
Hilbert

ДАВИД ГИЛЬБЕРТ

ИЗБРАННЫЕ ТРУДЫ

ТОМ I

ТЕОРИЯ ИНВАРИАНТОВ
ТЕОРИЯ ЧИСЕЛ
АЛГЕБРА
ГЕОМЕТРИЯ
ОСНОВАНИЯ МАТЕМАТИКИ

Под общей редакцией А. Н. ПАРШИНА

ИЗДАТЕЛЬСТВО «ФАКТОРИАЛ»
МОСКВА 1998

ББК 22.1
Г 47
УДК 51

СЕРИЯ «КЛАССИКИ МАТЕМАТИКИ»

Г 47 **Гильберт Д.** Избранные труды. Т. I. Теория инвариантов. Теория чисел. Алгебра. Геометрия. Основания математики. — М.: Изд-во «Факториал», 1998. — 575 с.

В собрание сочинений выдающегося немецкого ученого Д. Гильберта включены все основные работы, содержащие его наиболее выдающиеся результаты. В первом томе публикуются работы Д. Гильберта по теории инвариантов, теории чисел, алгебре, геометрии и основаниям математики. Почти все работы впервые публикуются на русском языке.

Книга предназначена для математиков, физиков и историков науки.

При участии Удмуртского государственного университета (г. Ижевск)

РФФИ

Издание осуществлено при финансовой поддержке Российского фонда фундаментальных исследований. Проект № 96-01-14195.

ISBN 5-88688-028-3
ISBN 5-88688-029-1 (том I)

СОДЕРЖАНИЕ

ТЕОРИЯ ЧИСЕЛ

АЛГЕБРА

ГЕОМЕТРИЯ

ОСНОВАНИЯ МАТЕМАТИКИ

ПРИЛОЖЕНИЯ И КОММЕНТАРИИ

ПРЕДИСЛОВИЕ

Давид Гильберт — крупнейший математик XX века и один из крупнейших математиков в истории нашей науки. Он внес огромный вклад во все основные разделы математики, и его исследования в значительной степени определили лицо математики нашего столетия. В работах Гильберта сочетается решение труднейших, долгое время неприступных, математических задач с созданием новых понятий и концепций, оказывающих определяющее влияние на развитие математики вплоть до настоящего времени. Гильберт поставил новые математические задачи почти во всех областях математики — это знаменитые проблемы Гильберта. Он также оказал существенное влияние на развитие теоретической физики в ее переломную эпоху — первую четверть нашего века.

Кроме того, Гильберт является создателем большой математической школы. Среди его учеников — выдающие немецкие математики: О. Блюменталь, М. Ден, Э. Шмидт, Э. Хеллингер, Г. Вейль, А. Шпайзер, А. Хаар, Р. Курант, Э. Гекке, Х. Штейнгауз, Х. Кнезер, В. Аккерманн. Время с 90-х годов прошлого века по 20-е нашего, когда Гильберт, и вместе с ним Ф. Клейн и Г. Минковский, работали в Гёттингене, можно без каких-либо преувеличений назвать золотым веком немецкой математики и физики. Рядом с Гильбертом и под его влиянием находились Дж. фон Нейман, Э. Нётер, М. Борн, Т. фон Карман, К. Каратеодори и многие другие.

Научная деятельность Гильберта распадается на периоды, когда он занимался какой-либо одной областью математики. Решив основные проблемы в этой области, он прекращал ею интересоваться и переходил к следующей. Впрочем, имеется и ряд отклонений от этой общей линии. Так, в 1909 г. будучи поглощенным теорией интегральных уравнений, Гильберт публикует работу по аналитической теории чисел, содержащую весьма изощренное решение проблемы Варинга.

Тем не менее, следуя Герману Вейлю, можно, в первом приближении, выделить такие основные периоды творчества Гильберта:

теория инвариантов (1885–1893);
теория алгебраических чисел (1893–1898);
основания геометрии (1898–1902);
анализ (1902–1912);
физика (1910–1922);
основания математики (1922–1930).

В настоящем издании представлены все основные работы Гильберта, содержащие его наиболее выдающиеся результаты. Включена также книга «Основы общей теории линейных интегральных уравнений». Все они (за исключением трех приложений из «Оснований геометрии», первого сообщения «Оснований физики» и «Математических проблем») никогда не переводились на русский язык. Упомянутая выше особенность математической биографии Гильберта предопределила структуру нашего издания. Тексты Гильберта разбиты на разделы, относящиеся к той или иной области математики, которые почти полностью повторяют приведенную выше периодизацию его деятельности. Не представлены лишь исследования по основаниям геометрии, вошедшие в одноименную книгу и имеющиеся в русском

переводе. Мы выделили также в отдельный раздел работы по алгебре: по теории положительных форм и о суперпозициях алгебраических функций (связанные соответственно с его семнадцатой и тринадцатой проблемами), и геометрии: алгебраической и дифференциальной. Внутри разделов работы даются, как правило, в хронологическом порядке.

Это издание имеет долгую предысторию. Еще в 60-е годы А. Н. Колмогоров предлагал издать работы Гильберта по математической логике и основаниям математики в серии «Классики науки» издательства «Наука». Новая попытка издать Гильберта в той же серии была предпринята в 80-е гг. Предполагалось выпустить избранные труды по алгебре, теории чисел, геометрии, теории инвариантов и логике. Значительная часть работ была тогда же переведена и снабжена комментариями. На разных этапах этой работы поддержка и помощь изданию были оказаны В. И. Арнольдом, А. Н. Колмогоровым, А. И. Кострикиным, Д. В. Юзнобишиным и А. П. Юшкевичем.

В 1994 г. работа над изданием была возобновлена по инициативе ректора Удмуртского государственного университета В. А. Журавлёва Далее ее приняло на себя издательство «Факториал» (директор издательства — И. Е. Калиниченко). Было решено издать избранные труды Гильберта, представляющие его деятельность в целом.

В настоящем издании приняли участие в качестве переводчиков: Г. В. Белый, А. П. Василевич, Ю. А. Данилов, И. В. Долгачев, Ю. Г. Зархин, З. А. Кузичева, Л. В. Кузьмин, Б. Л. Лаптев, Е. М. Матвеев, Н. М. Нагорный, И. Б. Пенков, В. Л. Попов, Н. И. Фельдман, В. М. Харламов, С. А. Харламова.

Кроме того, в издании помещены ранее опубликованные переводы И. С. Градштейна, А. В. Дорофеевой, Д. В. Жаркова, М. Е. Новодворского и М. Г. Шестопал.

Авторами комментариев являются: И. Г. Башмакова, А. А. Болибрух, Вл. П. Визгин, С. В. Востоков, С. С. Демидов, М. И. Зеликин, А. А. Карацуба, Ю. Л. Климонтович, Л. Д. Кудрявцев, Л. В. Кузьмин, Б. Л. Лаптев, В. Я. Лин, А. С. Меркурьев, Ю. В. Нестеренко, С. С. Петрова, А. Н. Паршин, В. Л. Попов, С. А. Степанов, В. М. Тихомиров, Н. И. Фельдман, В. М. Харламов, А. А. Шкаликов,

Редакторы издания: В. И. Авербух, Ю. Н. Торхов, Г. М. Цукерман.

От издательства «Факториал» в работе принимали участие: О. А. Васильева, М. И. Гринчук, Е. А. Коноваленко, Е. А. Макарова, И. Н. Мельникова, К. Е. Панкратьев, Н. А. Шихова.

Выход трудов Гильберта был бы совершенно невозможен без самоотверженной работы главного редактора издательства «Факториал» Ю. Н. Торхова.

Финансовая поддержка изданию была оказана Российским Фондом Фундаментальных Исследований (проект № 96–01–14195).

А. Н. Паршин

ТЕОРИЯ ИНВАРИАНТОВ

О КОНЕЧНОСТИ СИСТЕМЫ ИНВАРИАНТОВ ДЛЯ БИНАРНЫХ БАЗИСНЫХ ФОРМ*)

Как доказал ранее П. Гордан, для заданной системы бинарных базисных форм найдется такой конечный набор инвариантов, что любой другой инвариант этих базисных форм выражается целым рациональным образом через инварианты из этого набора. Ниже мы дадим другое доказательство этого фундаментального утверждения; в нем можно обнаружить, с одной стороны, близкую аналогию с первоначальным методом П. Гордана[1)], а с другой — параллели с ходом рассуждений Ф. Мертенса[2)].

Это доказательство опирается на следующие две известные и легко доказываемые теоремы:

I.

Всякая система, состоящая из произвольного числа линейных однородных диофантовых уравнений, обладает таким конечным набором положительных решений, что любое другое положительное решение представляется в виде линейной однородной комбинации решений из этого набора с целыми положительными коэффициентами[3)] [1].

II.

Рассмотрим для N произвольных величин $\omega, \ldots$ суммы их 1-х, 2-х, ..., N-х степеней

$$\omega + \ldots, \quad \omega^2 + \ldots, \quad \ldots, \quad \omega^N + \ldots$$

и обозначим через p какое-либо целое положительное число. Тогда всегда имеет место тождество вида

$$\omega^p = G + G^{(1)}\omega + \ldots + G^{(N-1)}\omega^{N-1}, \tag{1}$$

где $G, G^{(1)}, \ldots, G^{(N-1)}$ — целые функции от этих N степенных сумм.

В некотором смысле в обеих этих теоремах речь идет о том же, о чем и в теореме об инвариантах, поскольку в них, как и в теореме об инвариантах, содержится *некоторое утверждение о конечности в замкнутой системе.* Вместе с тем отметим то обстоятельство, что в обеих этих теоремах отдельные члены замкнутых систем входят в характеристическое редукционное равенство *линейным* образом.

---

*) Über die Endlichkeit des Invariantensystems für binäre Grundformen. — Math. Ann., 1889, Bd. 33, S. 223–226. *Перевод В. Л. Попова.*

1) *Gordan P.* Vorlesungen über Invariantentheorie. Bd. 2. — 1885, S. 231.

2) *Mertens F.* — Crelles J., Bd. 100, S. 223.

3) См. *Gordan P.*, loc. cit., Bd. 1. — 1885, S. 199.

Разложим заданную базисную форму f порядка n от однородных переменных x, y в произведение линейных множителей:

$$f = (\alpha^{(1)}x + \beta^{(1)}y)(\alpha^{(2)}x + \beta^{(2)}y) \ldots (\alpha^{(n)}x + \beta^{(n)}y),$$

и введем краткое обозначение

$$(k, l) = \alpha^{(k)}\beta^{(l)} - \alpha^{(l)}\beta^{(k)}.$$

Хорошо известно, что каждый инвариант формы f представляется в виде симметрического выражения

$$J = (1,2)^{e^{1,2}}(1,3)^{e^{1,3}}(2,3)^{e^{2,3}} \ldots (n-1,n)^{e^{n-1,n}} + \ldots, \tag{2}$$

где последующие члены суммы получаются из выписанного начального члена с помощью всевозможных перестановок стоящих в скобках чисел $1, 2, \ldots, n$. Кроме того, необходимо, чтобы каждое из чисел $1, 2, \ldots, n$ встречалось в этом начальном члене *одинаково часто*, т. е. для целых чисел, служащих показателями степени, должны выполняться равенства

$$\left.\begin{aligned} e^{1,2} + e^{1,3} + \ldots + e^{1,n} &= \\ = e^{2,1} + e^{2,3} + \ldots + e^{2,n} &= \\ \ldots\ldots\ldots\ldots\ldots\ldots & \\ = e^{n,1} + e^{n,2} + \ldots + e^{n,n-1}, & \end{aligned}\right\} \tag{3}$$

где $e^{k,l}$ и $e^{l,k}$ — одинаковые числа.

По теореме I каждое положительное решение диофантовых уравнений (3) представляется в виде линейного однородного выражения с целыми положительными коэффициентами $p_1, p_2, \ldots, p_m$ от определенного конечного числа m специальных положительных решений:

$$\left.\begin{aligned} e^{1,2} &= p_1 e_1^{1,2} + p_2 e_2^{1,2} + \ldots + p_m e_m^{1,2}, \\ e^{1,3} &= p_1 e_1^{1,3} + p_2 e_2^{1,3} + \ldots + p_m e_m^{1,3}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ e^{n-1,n} &= p_1 e_1^{n-1,n} + p_2 e_2^{n-1,n} + \ldots + p_m e_m^{n-1,n}. \end{aligned}\right\} \tag{4}$$

Воспользуемся краткими обозначениями

$$\left.\begin{aligned} \omega_1 &= (1,2)^{e_1^{1,2}}(1,3)^{e_1^{1,3}}(2,3)^{e_1^{2,3}} \ldots (n-1,n)^{e_1^{n-1,n}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \omega_m &= (1,2)^{e_m^{1,2}}(1,3)^{e_m^{1,3}}(2,3)^{e_m^{2,3}} \ldots (n-1,n)^{e_m^{n-1,n}} \end{aligned}\right\} \tag{5}$$

и построим всевозможные инварианты вида

$$J_{\pi_1\pi_2\ldots\pi_m} = \omega_1^{\pi_1}\omega_2^{\pi_2} \ldots \omega_m^{\pi_m} + \ldots, \tag{6}$$

где ни один из показателей степеней $\pi_1, \pi_2, \ldots, \pi_m$ не превышает числа

$$N = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

и где последующие члены суммы получаются из начального члена так же, как и выше в (2).

При перестановках стоящих в скобках чисел $1, 2, \ldots, n$ каждое из m произведений (5) порождает $N-1$ других выражений; поэтому ввиду редукционной формулы (1) из теоремы II имеют место равенства следующего вида:

$$\left.\begin{aligned} \omega_1^{p_1} &= G_1 + G_1^{(1)}\omega_1 + \ldots + G_1^{(N-1)}\omega_1^{N-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \omega_m^{p_m} &= G_m + G_m^{(1)}\omega_m + \ldots + G_m^{(N-1)}\omega_m^{N-1}, \end{aligned}\right\} \tag{7}$$

где коэффициенты G — целые функции от степенных сумм

$$\left.\begin{aligned} &\omega_1 + \ldots, \quad \omega_1^2 + \ldots, \quad \ldots, \quad \omega_1^N + \ldots, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\omega_m + \ldots, \quad \omega_m^2 + \ldots, \quad \ldots, \quad \omega_m^N + \ldots \end{aligned}\right\} \tag{8}$$

Все степенные суммы (8) принадлежат системе инвариантов (6).

Принимая во внимание равенства (4) и (5), мы видим, что общее выражение для инварианта (2) может быть представлено в виде

$$J = \omega_1^{p_1}\omega_2^{p_2}\ldots\omega_m^{p_m} + \ldots$$

Отсюда ввиду (7) легко получается, что J является целой функцией от инвариантов системы (6), т. е. что *инварианты* (6) *образуют систему, обладающую требующимся в нашей теореме свойством.*

В случае когда исходным является произвольный набор форм $f, g, h, \ldots$, вместо (2) следует рассмотреть симметрическое выражение, начальный член которого содержит все определители линейных множителей форм $f, g, h, \ldots$, причем таким образом, что коэффициенты линейных множителей одной и той же базисной формы встречаются в одинаковой степени. Это характеристическое свойство совместного инварианта выражается в виде некоторой системы диофантовых уравнений, играющих в этом случае роль системы (3). В остальном рассуждения остаются точно такими же.

Гёттинген, 30 марта 1888 г.

О ТЕОРИИ АЛГЕБРАИЧЕСКИХ ФОРМ*)[1)]

I. Конечность произвольной системы форм

Как обычно, мы понимаем под алгебраической формой целую *однородную* рациональную функцию от нескольких переменных и считаем, что коэффициенты формы являются числами из некоторой области рациональности [1]. Если теперь с помощью некоторого правила задана система, состоящая из какого-либо количества форм произвольных порядков, то возникает вопрос, всегда ли можно так выбрать из этой системы конечное число форм, чтобы всякая другая форма из этой системы могла быть представлена в виде линейной комбинации выбранных форм, или, иначе говоря, каждая ли форма в этой системе может быть выражена в виде

$$F = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

где F_1, $F_2, \ldots$, F_m — определенным образом выбранные из данной системы формы, а A_1, $A_2, \ldots$, A_m — какие-нибудь формы от тех же переменных и над той же областью рациональности. Чтобы решить этот вопрос, мы докажем сначала следующую теорему, являющуюся основой наших дальнейших исследований.

Теорема I. *Если задана необрывающаяся последовательность форм от n переменных x_1, $x_2, \ldots$, x_n, скажем, F_1, F_2, $F_3, \ldots$, то всегда существует такое число m, что каждая форма в этой последовательности может быть выражена в виде*

$$F = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

где A_1, $A_2, \ldots$, A_m — подходящие формы от тех же n переменных [2].

Ни на порядки форм из последовательности, ни на их коэффициенты не налагается никаких ограничений. Однако если мы предполагаем, что последние являются числами из какой-либо определенной области рациональности, то можем считать, что коэффициенты форм A_1, $A_2, \ldots$, A_m принадлежат той же области рациональности. Что же касается порядков форм A_1, $A_2, \ldots$, A_m, то они должны удовлетворять условию, что выражение

$$A_1F_1 + A_2F_2 + \ldots + A_mF_m$$

снова представляет собой *однородную* функцию от n переменных. Для удобства дальнейшего изложения здесь же условимся, что в тех случаях, когда мы имеем дело с линейной комбинацией нескольких форм, порядки

---

*) Über die Theorie der algebraischen Formen. — Math. Ann., 1890, Bd. 36, S. 473–534. *Перевод В. Л. Попова.*

1) См. также предварительные работы автора: Zur Theorie der algebraischen Gebilde. — Nachr. Ges. Wiss. Göttingen, 1888, S. 450–457 (первая заметка), 1889, S. 25–34, 423–430 (вторая и третья заметки).

форм выбраны так, что результирующее выражение является по-прежнему *однородным*.

В простейшем случае $n = 1$ каждая форма в данной последовательности состоит только из одного члена вида cx^r, где c обозначает константу. Пусть $c_1x^{r_1}$ — первая форма в данной последовательности, коэффициент c_1 которой отличен от 0. Рассмотрим теперь следующую форму в последовательности, порядок которой меньше r_1; пусть это будет форма $c_2x^{r_2}$. Далее рассмотрим следующую форму в последовательности, порядок которой меньше r_2; пусть это будет форма $c_3x^{r_3}$. Продолжая таким способом, мы самое большее через r_1 шагов придем к форме F_m из данной последовательности, за которой не следует ни одна форма меньшего порядка. Поскольку каждая форма в рассматриваемой последовательности делится на эту форму F_m, число m обладает свойством, которое требуется в теореме [3].

Подобным же способом нашу теорему I легко можно доказать и в случае $n = 2$. Достаточно будет следующего краткого наброска этого доказательства. Если все бинарные формы в данной последовательности содержат одну и ту же бинарную форму в качестве общего множителя, то мы исключим этот множитель делением. Взяв линейную комбинацию, из получившейся последовательности всегда можно построить две бинарные формы G и H, не имеющие общего множителя [4]. Проделав это, получим, что каждая бинарная форма F, порядок которой не меньше суммы r порядков форм G и H, может быть выражена в виде

$$F = AG + BH,$$

где A и B — соответствующим образом определяемые формы. В частности, каждая форма в рассматриваемой последовательности, порядок которой $\geqslant r$, равна линейной комбинации форм G и H. Что касается форм из нашей последовательности, порядок которых $\leqslant r$, то всегда можно так выбрать конечное число таких форм, чтобы всякая другая такая форма из последовательности была равна линейной комбинации выбранных форм [5].

Чтобы аналогичным способом доказать теорему I в случае тернарных форм, следует воспользоваться фундаментальной теоремой Нётера[2]) об условиях представления тернарной формы с помощью двух заданных форм и проделать тщательное исследование всех возможных вырождений систем значений переменных, обращающих в нуль заданные формы. Поскольку трудности этого метода быстро растут с ростом числа переменных n, мы докажем теорему другим методом: покажем, как случай форм от n переменных может быть сведен к случаю $n - 1$ переменных.

Пусть F_1, F_2, $F_3, \ldots$ — заданная последовательность форм от n переменных x_1, $x_2, \ldots, x_n$, и пусть F_1 — форма порядка r, не равная тождественно нулю. Найдем сначала линейную подстановку переменных $x_1, \ldots, x_n$, имеющую ненулевой определитель и переводящую форму F_1 в форму G_1 от переменных y_1, $y_2, \ldots, y_n$, у которой коэффициент при y_n^r отличен от 0 [6]. Пусть G_2, $G_3, \ldots$ — результат применения той же самой линейной подстановки к формам F_2, $F_3, \ldots$ соответственно. Тогда соотношение

$$G_s = B_1G_1 + B_2G_2 + \ldots + B_mG_m,$$

---

[2]) См.: *Noether M.* — Math. Ann., Bd. 6, S. 351; Bd. 30, S. 410, а также: *Voss A.* — Math. Ann., Bd. 27, S. 527; *Stickelberger L.* — Math. Ann., Bd. 30, S. 401.

где s — какой-нибудь индекс, а B_1, $B_2, \ldots, B_m$ — формы от переменных y_1, $y_2, \ldots, y_n$, преобразуется обратной подстановкой в соотношение

$$F_s = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

где A_1, $A_2, \ldots, A_m$ — формы от исходных переменных x_1, $x_2, \ldots, x_n$. Следовательно, мы получим утверждение теоремы I для исходной последовательности форм F_1, F_2, $F_3, \ldots$, если докажем его для последовательности G_1, G_2, $G_3, \ldots$

Поскольку коэффициент при y_n^r в G_1 отличен от 0, степень любой формы G_s из данной последовательности относительно переменной y_n может быть сделана меньше r с помощью умножения формы G_1 на подходящую форму B_s и вычитания полученного произведения из G_s. Соответственно мы полагаем

$$G_s = B_sG_1 + g_{s1}\,y_n^{r-1} + g_{s2}\,y_n^{r-2} + \ldots + g_{sr},$$

где s — произвольный индекс, B_s — форма от n переменных $y_1, \ldots, y_n$ и g_{s1}, $g_{s2}, \ldots, g_{sr}$ — формы, содержащие только $n-1$ переменных y_1, $y_2, \ldots, y_{n-1}$.

Предположим теперь, что теорема I уже доказана для последовательностей форм от $n-1$ переменных, и применим ее к последовательности g_{11}, g_{21}, $g_{31}, \ldots$ По теореме I существует такое число μ, что для каждого s имеется соотношение

$$g_{s1} = b_{s1}\,g_{11} + b_{s2}\,g_{21} + \ldots + b_{s\mu}\,g_{\mu 1} = l_s(g_{11}, g_{21}, \ldots, g_{\mu 1}),$$

где b_{s1}, $b_{s2}, \ldots, b_{s\mu}$ — формы от $n-1$ переменных y_1, $y_2, \ldots, y_{n-1}$. Теперь рассмотрим формы

$$g_{st}^{(1)} = g_{st} - l_s(g_{1t}, g_{2t}, \ldots, g_{\mu t}) \qquad (t = 1, 2, \ldots, r). \tag{1}$$

В частности, для $t = 1$ мы имеем

$$g_{s1}^{(1)} = 0.$$

Применим теперь теорему I для случая $n-1$ переменных к последовательности форм $g_{12}^{(1)}$, $g_{22}^{(1)}$, $g_{32}^{(1)}, \ldots$ Мы получим, что существует такое число $\mu^{(1)}$, что для каждого s имеет место соотношение

$$g_{s2}^{(1)} = b_{s1}^{(1)}g_{12}^{(1)} + b_{s2}^{(1)}g_{22}^{(1)} + \ldots + b_{s\mu^{(1)}}^{(1)}g_{\mu^{(1)}2}^{(1)} = l_s^{(1)}\left(g_{12}^{(1)}, g_{22}^{(1)}, \ldots, g_{\mu^{(1)}2}^{(1)}\right),$$

где $b_{s1}^{(1)}$, $b_{s2}^{(1)}, \ldots, b_{s\mu^{(1)}}^{(1)}$ — формы от $n-1$ переменных y_1, $y_2, \ldots, y_{n-1}$. Положим теперь

$$g_{st}^{(2)} = g_{st}^{(1)} - l_s^{(1)}\left(g_{1t}^{(1)}, g_{2t}^{(1)}, \ldots, g_{\mu^{(1)}t}^{(1)}\right) \qquad (t = 1, 2, \ldots, r). \tag{2}$$

В частности, при $t = 1, 2$ это дает

$$g_{s1}^{(2)} = 0, \quad g_{s2}^{(2)} = 0.$$

Применение теоремы I к последовательности форм $g_{13}^{(2)}$, $g_{23}^{(2)}$, $g_{33}^{(2)}, \ldots$ приводит к соотношению

$$g_{s3}^{(2)} = l_s^{(2)}\left(g_{13}^{(2)}, g_{23}^{(2)}, \ldots, g_{\mu^{(2)}3}^{(2)}\right).$$

Положим теперь

$$g_{st}^{(3)} = g_{st}^{(2)} - l_s^{(2)}\left(g_{1t}^{(2)}, g_{2t}^{(2)}, \ldots, g_{\mu^{(2)}t}^{(2)}\right) \qquad (t = 1, 2, \ldots, r), \tag{3}$$

так что, в частности,

$$g_{s1}^{(3)} = 0, \quad g_{s2}^{(3)} = 0, \quad g_{s3}^{(3)} = 0.$$

Повторение этого процесса дает соотношения

$$g_{st}^{(r-1)} = g_{st}^{(r-2)} - l_s^{(r-2)}\left(g_{1t}^{(r-2)}, g_{2t}^{(r-2)}, \ldots, g_{\mu^{(r-2)}t}^{(r-2)}\right) \qquad (t = 1, 2, \ldots, r) \qquad (4)$$

и

$$g_{s1}^{(r-1)} = 0, \quad g_{s2}^{(r-1)} = 0, \quad \ldots, \quad g_{s,r-1}^{(r-1)} = 0.$$

И, наконец, получаем

$$g_{sr}^{(r-1)} = l_s^{(r-1)}\left(g_{1r}^{(r-1)}, g_{2r}^{(r-1)}, \ldots, g_{\mu^{(r-1)}r}^{(r-1)}\right),$$

откуда следует, что

$$0 = g_{st}^{(r-1)} - l_s^{(r-1)}\left(g_{1t}^{(r-1)}, g_{2t}^{(r-1)}, \ldots, g_{\mu^{(r-1)}t}^{(r-1)}\right) \qquad (t = 1, 2, \ldots, r). \qquad (5)$$

Сложение равенств (1), (2), (3), ..., (4), (5) дает

$$g_{st} = l_s(g_{1t}, g_{2t}, \ldots, g_{\mu t}) + l_s^{(1)}\left(g_{1t}^{(1)}, g_{2t}^{(1)}, \ldots, g_{\mu^{(1)}t}^{(1)}\right) + \ldots$$
$$\ldots + l_s^{(r-1)}\left(g_{1t}^{(r-1)}, g_{2t}^{(r-1)}, \ldots, g_{\mu^{(r-1)}t}^{(r-1)}\right) \qquad (t = 1, 2, \ldots, r).$$

Теперь формы

$$g_{1t}^{(1)}, \; g_{2t}^{(1)}, \; \ldots, \; g_{\mu^{(1)}t}^{(1)}, \; \ldots, \; g_{1t}^{(r-1)}, \; g_{2t}^{(r-1)}, \; \ldots, \; g_{\mu^{(r-1)}t}^{(r-1)}$$

в правой части последней формулы могут быть заменены на линейные комбинации форм $g_{1t}, g_{2t}, \ldots, g_{mt}$, где m — наибольшее из чисел $\mu, \mu^{(1)}, \ldots, \mu^{(r-1)}$. Таким способом мы получаем из последней формулы систему уравнений

$$g_{st} = c_{s1}g_{1t} + c_{s2}g_{2t} + \ldots + c_{sm}g_{mt} = k_s(g_{1t}, g_{2t}, \ldots, g_{mt}) \qquad (t = 1, 2, \ldots, r),$$

где $c_{s1}, c_{s2}, \ldots, c_{sm}$ — снова формы от $n-1$ переменных $y_1, y_2, \ldots, y_{n-1}$. Если мы умножим последнюю формулу на y_n^{r-t} и сложим получившиеся уравнения для $t = 1, 2, \ldots, r$, то ввиду того, что

$$g_{s1}y_n^{r-1} + g_{s2}y_n^{r-2} + \ldots + g_{sr} = G_s - B_sG_1,$$

получим

$$G_s - B_sG_1 = k_s(G_1 - B_1G_1, G_2 - B_2G_1, \ldots, G_m - B_mG_1),$$

или

$$G_s = C_sG_1 + k_s(G_1, G_2, \ldots, G_m) = L_s(G_1, G_2, \ldots, G_m),$$

где C_s — форма от n переменных $y_1, y_2, \ldots, y_n$. Таким образом, m — как раз такое число, как требуется в теореме I для последовательности $G_1, G_2, G_3, \ldots$, а значит, также и для последовательности $F_1, F_2, F_3, \ldots$ Итак, наша теорема I доказана в случае n переменных в предположении, что она имеет место для форм от $n-1$ переменных. Поскольку справедливость теоремы I для форм от одной переменной уже была установлена, эта теорема доказана теперь и в общем случае.

С помощью теоремы I можно ответить на вопрос, поставленный в начале этой работы. В самом деле, пусть задана произвольная система форм от n переменных $x_1, x_2, \ldots, x_n$, причем неизвестно, можно ли упорядочить эти

формы в некоторую последовательность или же они составляют несчетное множество. Задание такой системы форм предполагает задание некоторого правила, с помощью которого можно решить, принадлежит произвольно взятая форма системе или нет. Предположим теперь, что из данной системы невозможно выбрать конечное число форм так, чтобы каждую другую форму из этой системы можно было получить в виде линейной комбинации выбранных форм. Выберем теперь произвольную не равную тождественно нулю форму из заданной системы и обозначим ее через F_1. Пусть F_2 — форма из данной системы, не равная произведению A_1F_1, где A_1 — произвольная форма от n переменных $x_1, x_2, \ldots, x_n$. Точно так же пусть F_3 — форма из данной системы, которая не может быть записана в виде $A_1F_1 + A_2F_2$, где A_1 и A_2 — снова формы от $x_1, x_2, \ldots, x_n$. Аналогично пусть F_4 — форма из системы, которую нельзя записать в виде $A_1F_1 + A_2F_2 + A_3F_3$. Продолжая так и далее, мы получим последовательность форм F_1, F_2, $F_3, \ldots$, которая по нашему предположению не может оборваться после конечного числа шагов и в которой никакую из форм нельзя получить с помощью взятия линейной комбинации предыдущих форм. Но это противоречит теореме I, и поэтому наше предыдущее предположение неверно. Таким образом, мы получили следующее утверждение:

Из любой заданной системы форм всегда можно выделить конечное число форм так, чтобы любая другая форма из этой системы представлялась в виде линейной комбинации выбранных форм [7].

Рассмотрим, в частности, системы форм, обладающие тем свойством, что любое произведение формы из такой системы на произвольную форму (не обязательно лежащую в этой системе) снова принадлежит системе, равно как и каждая сумма таких произведений, являющаяся однородной относительно переменных $x_1, x_2, \ldots, x_n$; иначе говоря, каждая линейная комбинация форм из системы снова принадлежит этой системе. Такая система, состоящая из произвольного количества форм, называется *модулем* [8]. Таким образом, наши дальнейшие рассмотрения в той мере, в какой они касаются теории модулей, основаны на обозначениях и понятиях, использованных Л. Кронекером в теории систем модулей, которую он создал и недавно систематически развил[3]. Нужно, однако, отметить, что в отличие от вопросов, рассмотренных Л. Кронекером, в наших исследованиях, а особенно в разд. III и IV этой работы, существенным и необходимым предположением является *однородность* функций из модуля. Формулируя только что доказанное предложение для частного случая модуля, получаем следующее предложение:

Среди форм произвольного модуля всегда можно выбрать конечное число таких, что всякая другая форма из этого модуля представляется в виде линейной комбинации выбранных [9].

Чтобы получить наглядный пример, иллюстрирующий это предложение, предположим, что задана пространственная алгебраическая кривая и что

---

[3] См.: *Kronecker L.* — Crelles J., Bd. 92, S. 1–122; Bd. 93, S. 365–366; Bd. 99, S. 329–371; Bd. 100, S. 490–510; Berl. Sitzgsber., 1888, S. 429–438, 447–465, 557–578, 595–612, 983–1016; а также *Dedekind R., Weber H.* — Crelles J., Bd. 92, S. 181–290, и *Molk J.* — Acta math., Bd. 6, S. 50–165.

мы интересуемся полной системой алгебраических поверхностей, содержащих эту пространственную кривую [10]. Так как левые части уравнений этих поверхностей являются кватернарными формами, линейные комбинации которых принадлежат той же самой системе, то эти формы образуют модуль, и предыдущее предложение интерпретируется в этом частном случае следующим образом:

Через данную пространственную алгебраическую кривую можно провести конечное число m таких поверхностей

$$F_1 = 0, \quad F_2 = 0, \quad \ldots, \quad F_m = 0,$$

что всякая другая алгебраическая поверхность, содержащая эту кривую, может быть задана уравнением

$$A_1F_1 + A_2F_2 + \ldots + A_mF_m = 0,$$

где $A_1, A_2, \ldots, A_m$ обозначают кватернарные формы[4].

Например, пусть пространственная кубическая кривая задается уравнениями [11]

$$\left.\begin{aligned} x_1 &= \xi_1^3, \\ x_2 &= \xi_1^2\xi_2, \\ x_3 &= \xi_1\xi_2^2, \\ x_4 &= \xi_2^3, \end{aligned}\right\} \tag{6}$$

где x_1, x_2, x_3, x_4 — однородные координаты ее точек, а ξ_1, ξ_2 — однородные параметры. Через эту пространственную кривую проходят три поверхности $F_1 = 0$, $F_2 = 0$, $F_3 = 0$, где

$$F_1 = x_1x_3 - x_2^2, \quad F_2 = x_2x_3 - x_1x_4, \quad F_3 = x_2x_4 - x_3^2$$

— квадратичные формы, ни одна из которых не может быть получена из двух других с помощью взятия линейной комбинации. Чтобы показать, что всякая другая поверхность, содержащая эту пространственную кривую, может быть задана уравнением [12]

$$A_1F_1 + A_2F_2 + A_3F_3 = 0,$$

мы предположим, что

$$F = \sum C_{r_1r_2r_3r_4}x_1^{r_1}x_2^{r_2}x_3^{r_3}x_4^{r_4}$$

— форма, превращающаяся в тождественный нуль, если применить подстановку (6). Используя сравнения [13]

$$\begin{aligned} x_1x_3 &\equiv x_2^2, && (F_1, F_2, F_3), \\ x_1x_4 &\equiv x_2x_3, && (F_1, F_2, F_3), \\ x_2x_4 &\equiv x_3^2, && (F_1, F_2, F_3), \end{aligned}$$

---

[4] Вопрос о конечности числа поверхностей, содержащих пространственную кривую, уже поднимался Г. Сальмоном в его учебнике: *Salmon G.* Analytische Geometrie des Raumes. Bd. II. S. 79.

мы можем положить

$$F \equiv \sum C_{\varkappa_1\varkappa_2} x_1^{\varkappa_1} x_2^{\varkappa_2} + \sum C_{\lambda_2\lambda_3} x_2^{\lambda_2} x_3^{\lambda_3} + \sum C_{\mu_3\mu_4} x_3^{\mu_3} x_4^{\mu_4}, \quad (F_1, F_2, F_3), \quad (7)$$

где $C_{\varkappa_1\varkappa_2}$, $C_{\lambda_2\lambda_3}$, $C_{\mu_3\mu_4}$ — некоторые числовые коэффициенты. Кроме того, можно считать, что ни один из двух показателей λ_2 и λ_3 не равен нулю, поскольку в противном случае такой член мог бы быть перемещен из второй суммы либо в первую, либо в третью. Так как правая часть формулы (7) однородна, то

$$\varkappa_1 + \varkappa_2 = \lambda_2 + \lambda_3 = \mu_3 + \mu_4,$$

откуда следует, что [14]

$$3\varkappa_1 + 2\varkappa_2 > 2\lambda_2 + \lambda_3 > \mu_3.$$

Вводя в правую часть формулы (7) параметры ξ_1, ξ_2 с помощью уравнений (6), мы видим, что ни один из получающихся членов $C\xi_1^{\varrho_1}\xi_2^{\varrho_2}$ не может быть объединен ни с каким членом той же самой или другой суммы. Поскольку после подстановки (6) выражение в правой части (7) должно обратиться в нуль, все коэффициенты $C_{\varkappa_1\varkappa_2}$, $C_{\lambda_2\lambda_3}$, $C_{\mu_3\mu_4}$ должны быть нулевыми. Таким образом, мы получаем из сравнения (7), что

$$F = 0, \quad (F_1, F_2, F_3)$$

или, иначе говоря, что

$$F = A_1F_1 + A_2F_2 + A_3F_3.$$

Наши общие рассмотрения имеют и другое приложение в теории уравнений, касающееся целых однородных функций от коэффициентов уравнения, обращающихся в нуль в случае, когда уравнение имеет некоторое количество кратных корней [15]. Поскольку система всех таких функций образует модуль, мы получаем следующее утверждение:

Существует конечное число целых однородных функций от коэффициентов алгебраического уравнения, обращающихся в нуль, когда уравнение имеет заданное количество кратных корней, и таких, что любая другая целая функция с тем же свойством является их линейной комбинацией.

Например, предположим, что следует найти все однородные функции от коэффициентов x_1, x_2, x_3, x_4, x_5 бинарной формы четвертого порядка

$$\varphi = x_1\xi_1^4 + 4x_2\xi_1^3\xi_2 + 6x_3\xi_1^2\xi_2^2 + 4x_4\xi_1\xi_2^3 + x_5\xi_2^4,$$

которые обращаются в нуль, когда форма φ является четвертой степенью. Рассмотрим следующие шесть квадратичных форм:

$$F_1 = x_1x_3 - x_2^2,$$
$$F_2 = x_1x_4 - x_2x_3,$$
$$F_3 = x_1x_5 - x_2x_4,$$
$$F_4 = x_1x_5 - x_3^2,$$
$$F_5 = x_2x_5 - x_3x_4,$$
$$F_6 = x_3x_5 - x_4^2.$$

Тогда легко, как и раньше, убедиться, что любая функция F с требуемым свойством может быть записана в виде

$$F = A_1F_1 + A_2F_2 + \ldots + A_6F_6,$$

где A_1, $A_2, \ldots, A_6$ — однородные функции от x_1, x_2, x_3, x_4, x_5 [16].

В качестве второго примера найдем все однородные функции от коэффициентов формы φ, обращающиеся в нуль, когда бинарная форма φ является полным квадратом. Для этого следует рассмотреть такие семь функций:

$$\begin{aligned}
F_1 &= x_1^2x_4 \quad - 3x_1x_2x_3 + 2x_2^3,\\
F_2 &= x_1^2x_5 \quad + 2x_1x_2x_4 - 9x_1x_3^2 + 6x_2^2x_3,\\
F_3 &= x_1x_2x_5 - 3x_1x_3x_4 + 2x_2^2x_4,\\
F_4 &= x_1x_4^2 \quad - x_2^2x_5,\\
F_5 &= x_1x_4x_5 - 3x_2x_3x_5 + 2x_2x_4^2,\\
F_6 &= x_1x_5^2 \quad + 2x_2x_4x_5 - 9x_3^2x_5 + 6x_3x_4^2,\\
F_7 &= x_2x_5^2 \quad - 3x_3x_4x_5 + 2x_4^2.
\end{aligned}$$

По существу эти семь функций совпадают с коэффициентами коварианта порядка шесть и степени три формы φ, и поэтому, используя методы теории инвариантов, можно показать, что любая другая однородная функция с требующимся свойством может быть записана в виде

$$A_1F_1 + A_2F_2 + \ldots + A_7F_7,$$

где A_1, $A_2, \ldots, A_7$ — снова однородные функции.

Следующее предложение имеет более общий характер, а также фундаментальное значение для наших последующих исследований.

Если F_1, $F_2, \ldots, F_{m^{(1)}}$ — *заданные формы от* n *переменных* x_1, $x_2, \ldots, x_n$, *то существует конечное число* $m^{(2)}$ *систем форм*

$$\begin{array}{llll}
X_1 = X_{11}, & X_2 = X_{21}, & \ldots, & X_{m^{(1)}} = X_{m^{(1)}1},\\
X_1 = X_{12}, & X_2 = X_{22}, & \ldots, & X_{m^{(1)}} = X_{m^{(1)}2},\\
\ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots\ldots,\\
X_1 = X_{1m^{(2)}}, & X_2 = X_{2m^{(2)}}, & \ldots, & X_{m^{(1)}} = X_{m^{(1)}m^{(2)}},
\end{array}$$

которые все тождественно удовлетворяют уравнению

$$F_1X_1 + F_2X_2 + \ldots + F_{m^{(1)}}X_{m^{(1)}} = 0$$

и с помощью которых любая другая система форм, удовлетворяющих этому уравнению, может быть выражена в виде

$$\begin{aligned}
X_1 &= A_1X_{11} \quad + A_2X_{12} \quad + \ldots + A_{m^{(2)}}X_{1m^{(2)}},\\
X_2 &= A_1X_{21} \quad + A_2X_{22} \quad + \ldots + A_{m^{(2)}}X_{2m^{(2)}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X_{m^{(1)}} &= A_1X_{m^{(1)}1} + A_2X_{m^{(1)}2} + \ldots + A_{m^{(2)}}X_{m^{(1)}m^{(2)}},
\end{aligned}$$

где A_1, $A_2, \ldots, A_{m^{(2)}}$ — *также формы от переменных* x_1, $x_2, \ldots, x_n$ [17].

Доказательство этого предложения основано на наших общих результатах о конечности для форм из произвольной системы. Пусть $X_1, X_2, \ldots, X_{m^{(1)}}$ — любая система, являющаяся решением уравнения

$$F_1X_1 + F_2X_2 + \ldots + F_{m^{(1)}}X_{m^{(1)}} = 0.$$

В каждой такой системе-решении рассмотрим последнюю форму $X_{m^{(1)}}$. В силу наших предыдущих общих предложений можно выбрать конечное число μ форм $X_{m^{(1)}1}, X_{m^{(1)}2}, \ldots, X_{m^{(1)}\mu}$ из всей совокупности этих форм $X_{m^{(1)}}$, таких, что всякую другую такую форму можно представить в виде

$$X_{m^{(1)}} = A'_1X_{m^{(1)}1} + A'_2X_{m^{(1)}2} + \ldots + A'_\mu X_{m^{(1)}\mu}.$$

Если теперь мы построим формы

$$X'_t = X_t - A'_1X_{t1} - A'_2X_{t2} - \ldots - A'_\mu X_{t\mu} \qquad (t = 1, 2, \ldots, m^{(1)}),$$

так что, в частности, $X'_{m^{(1)}} = 0$ при $t = m^{(1)}$, то увидим, что каждое решение $X_1, X_2, \ldots, X_{m^{(1)}}$ исходного уравнения соответствует решению $X'_1, X'_2, \ldots, X'_{m^{(1)}-1}$ уравнения

$$F_1X'_1 + F_2X'_2 + \ldots + F_{m^{(1)}-1}X'_{m^{(1)}-1} = 0.$$

Очевидно, что и, наоборот, каждое решение исходного уравнения может быть получено из μ систем-решений

$$X_1 = X_{1s}, \quad X_2 = X_{2s}, \quad \ldots, \quad X_{m^{(1)}} = X_{m^{(1)}s} \qquad (s = 1, \ldots, \mu)$$

и из системы-решения только что указанного уравнения. Это последнее уравнение содержит, однако, только $m^{(1)} - 1$ форм, подлежащих определению. Поэтому если сформулированное выше предложение считать верным для такого уравнения, то оно будет доказано и для данного уравнения. Но наше предложение действительно справедливо для $m^{(1)} = 1$, поскольку в этом случае соответствующее уравнение

$$F_1X_1 = 0,$$

очевидно, не имеет решений. Это завершает доказательство.

В качестве примера рассмотрим уравнение

$$(x_1x_3 - x_2^2)X_1 + (x_2x_3 - x_1x_4)X_2 + (x_2x_4 - x_3^2)X_3 = 0,$$

коэффициенты которого — те самые три квадратичные формы, к которым мы пришли, рассматривая выше пространственную кубическую кривую. Мы без труда получаем, что из двух систем-решений

$$X_1 = x_3, \quad X_2 = x_2, \quad X_3 = x_1,$$
$$X_1 = x_4, \quad X_2 = x_3, \quad X_3 = x_2$$

может быть получена любая другая система-решение этого уравнения. В самом деле, если X_1, X_2, X_3 — произвольная система-решение, то можно сначала исключить из формы X_1 все члены, содержащие в качестве множителя x_3, используя для этого первую из двух указанных систем-решений; после этого можно исключить из X_1 все члены, содержащие в качестве множителя x_4, используя для этого вторую систему-решение; в полученной

в результате системе-решении X_1', X_2', X_3' форма X_1' не зависит от x_3 и x_4. Если теперь мы положим $x_3 = 0$ и $x_4 = 0$ в тождестве

$$(x_1x_3 - x_2^2)X_1' + (x_2x_3 - x_1x_4)X_2' + (x_2x_4 - x_3^2)X_3' = 0,$$

то получим $X_1' = 0$ и, следовательно,

$$X_2' = A(x_2x_4 - x_3^2), \quad X_3' = A(x_1x_4 - x_2x_3),$$

где A — произвольная форма от переменных x_1, x_2, x_3, x_4. Легко видеть, что полученная таким способом система-решение представляется также как комбинация двух предыдущих систем-решений, а именно нужно умножить первую систему-решение на Ax_4, вторую — на $-Ax_3$ и затем сложить соответствующие формы.

В качестве второго примера мы выберем уравнение

$$F_1X_1 + F_2X_2 + \ldots + F_6X_6 = 0,$$

где F_1, $F_2, \ldots, F_6$ — указанные выше шесть квадратичных форм от пяти переменных x_1, x_2, x_3, x_4, x_5. Мы имеем следующие восемь решений:

$$\begin{array}{llllll}
X_1 = x_3, & X_2 = -x_2, & X_3 = -x_1, & X_4 = x_1, & X_5 = 0, & X_6 = 0, \\
X_1 = x_4, & X_2 = -x_3, & X_3 = -x_2, & X_4 = x_2, & X_5 = 0, & X_6 = 0, \\
X_1 = x_5, & X_2 = 0, & X_3 = -x_3, & X_4 = 0, & X_5 = x_2, & X_6 = 0, \\
X_1 = 0, & X_2 = x_3, & X_3 = 0, & X_4 = -x_2, & X_5 = x_1, & X_6 = 0, \\
X_1 = 0, & X_2 = x_4, & X_3 = -x_3, & X_4 = 0, & X_5 = 0, & X_6 = x_1, \\
X_1 = 0, & X_2 = x_5, & X_3 = -x_4, & X_4 = 0, & X_5 = 0, & X_6 = x_2, \\
X_1 = 0, & X_2 = 0, & X_3 = x_4, & X_4 = -x_4, & X_5 = x_3, & X_6 = -x_2, \\
X_1 = 0, & X_2 = 0, & X_3 = x_5, & X_4 = -x_5, & X_5 = x_4, & X_6 = -x_3,
\end{array}$$

и, как и в первом примере, может быть показано, что всякое другое решение является комбинацией этих.

Мы доказали выше конечность полной системы решений в случае одного уравнения. Но использованные там аргументы непосредственно переносятся на тот случай, когда должны удовлетворяться несколько уравнений того вида, о котором идет речь. Таким образом, мы получаем более общее утверждение:

Если дана система m уравнений

$$F_{t1}X_1 + F_{t2}X_2 + \ldots + F_{tm^{(1)}}X_{m^{(1)}} = 0 \qquad (t = 1, 2, \ldots, m),$$

где коэффициенты F_{t1}, $F_{t2}, \ldots, F_{tm^{(1)}}$ являются заданными формами от n переменных, а X_1, $X_2, \ldots, X_{m^{(1)}}$ — подлежащие определению $m^{(1)}$ форм, то такая система всегда обладает конечным числом $m^{(2)}$ таких систем-решений

$$X_1 = X_{1s}, \quad X_2 = X_{2s}, \quad \ldots, \quad X_{m^{(1)}} = X_{m^{(1)}s} \qquad (s = 1, 2, \ldots, m^{(2)}),$$

что всякая другая система-решение исходной системы может быть выражена в виде

$$X_l = A_1 X_{l1} + A_2 X_{l2} + \ldots + A_{m^{(2)}} X_{lm^{(2)}} \qquad (l = 1, 2, \ldots, m^{(1)}),$$

где A_1, $A_2, \ldots, A_{m^{(2)}}$ *— также формы от* n *переменных*[5].

II. Конечность для форм с целыми коэффициентами

Все утверждения, полученные до сих пор, основывались по существу на теореме I предыдущего раздела. Мы рассмотрели там случай, когда коэффициенты форм являются числами из произвольной области рациональности; теперь же мы хотим рассмотреть случай, когда все они — целые числа. Соответственно может быть дана более точная формулировка теоремы I, делающая ее пригодной в теоретико-числовых исследованиях, а именно:

Теорема II. *Для любой бесконечной последовательности* F_1, F_2, $F_3, \ldots$ *форм произвольных порядков с целыми коэффициентами от* n *однородных переменных* x_1, $x_2, \ldots, x_n$ *всегда найдется такое число* m, *что каждая форма из этой последовательности может быть представлена в виде*

$$F = A_1 F_1 + A_2 F_2 + \ldots + A_m F_m,$$

где A_1, $A_2, \ldots, A_m$ *— формы с целыми коэффициентами от тех же самых* n *переменных.*

Мы видим, что в отличие от предыдущей формулировки этой теоремы здесь требуется, чтобы как данные формы F_1, F_2, $F_3, \ldots$, так и формы A_1, $A_2, \ldots, A_m$, использующиеся в указанном представлении, были формами с *целыми* коэффициентами.

Аргументы, использованные для доказательства теоремы I, не достаточны для доказательства теоремы II. Дело в том, что предыдущие рассуждения основывались на изменении порядков форм F_2, $F_3, \ldots$ по переменной x_n с помощью подходящей комбинации с формой F_1 так, чтобы они стали меньше порядка r формы F_1. Теперь же, когда мы не используем дробей, для осуществления такой процедуры нужно, чтобы коэффициент при x_n^r в F_1 был равен ± 1, что в общем случае не так и не может быть достигнуто целочисленной линейной заменой переменных. Поэтому для доказательства теоремы II нужны новые соображения; в то же время они дадут нам и второе доказательство теоремы I.

Обозначим через f_s члены формы F_s, не зависящие от переменной x_n. Если теперь все члены бесконечной последовательности f_1, f_2, $f_3, \ldots$ тождественно равны нулю, то мы положим

$$F_s^{(1)} = F_s \qquad (s = 1, 2, 3, \ldots);$$

в противном случае пусть f_α — первая ненулевая форма в последовательности f_1, f_2, $f_3, \ldots$; пусть, далее, f_β — первая форма этой последовательности,

---

[5] В случае *одной* неоднородной переменной это предложение было использовано Л. Кронекером в его доказательстве конечности системы целых алгебраических величин в роде (Gattung); см.: *Kronecker L.* — Crelles J., Bd. 92, S. 16.

не равная произведению $a_\alpha f_\alpha$, где a_α — форма с целыми коэффициентами от переменных $x_1, x_2, \ldots, x_{n-1}$; пусть f_γ — первая форма в этой последовательности, которая не может быть представлена в виде $a_\alpha f_\alpha + a_\beta f_\beta$, где a_α и a_β — снова формы с целыми коэффициентами от $x_1, x_2, \ldots, x_{n-1}$, и т. д. Если считать теперь, что теорема II уже доказана для случая $n-1$ однородных переменных, и если заметить, что в последовательности форм $f_\alpha, f_\beta, f_\gamma, \ldots$ ни одна не может быть представлена как линейная комбинация предыдущих, то мы получим, что эта последовательность форм должна оборваться через конечное число шагов. Пусть f_λ будет последней формой в этой последовательности, так что

$$f_s = a_{\alpha s} f_\alpha + a_{\beta s} f_\beta + \ldots + a_{\lambda s} f_\lambda = l_s(f_\alpha, f_\beta, \ldots, f_\lambda) \qquad (s = 1, 2, 3, \ldots),$$

где $a_{\alpha s}, a_{\beta s}, \ldots, a_{\lambda s}$ — целочисленные формы от $x_1, \ldots, x_{n-1}$. Если теперь мы образуем выражения

$$F_s^{(1)} = F_s - l_s(F_\alpha, F_\beta, \ldots, F_\lambda) \qquad (s = 1, 2, 3, \ldots),$$

то получим формы от n переменных $x_1, x_2, \ldots, x_n$, каждая из которых содержит x_n в качестве множителя. Обозначим через $x_n f_s^{(1)}$ те члены формы $F_s^{(1)}$, которые содержат только первую степень x_n, и рассмотрим формы $f_1^{(1)}$, $f_2^{(1)}, f_3^{(1)}, \ldots$ от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Если все эти формы равны нулю, то положим

$$F_s^{(2)} = F_s^{(1)} \qquad (s = 1, 2, 3, \ldots).$$

В случае когда каждая форма в последовательности $f_1^{(1)}, f_2^{(1)}, f_3^{(1)}, \ldots$ является линейной комбинацией форм $f_\alpha, f_\beta, \ldots, f_\lambda$, скажем

$$f_s^{(1)} = a_{\alpha s}^{(1)} f_\alpha + a_{\beta s}^{(1)} f_\beta + \ldots + a_{\lambda s}^{(1)} f_\lambda = l_s^{(1)}(f_\alpha, f_\beta, \ldots, f_\lambda) \qquad (s = 1, 2, 3, \ldots),$$

положим

$$F_s^{(2)} = F_s^{(1)} - l_s^{(1)}(x_n F_\alpha, x_n F_\beta, \ldots, x_n F_\lambda).$$

Во всех остальных случаях пусть $f_{\alpha^{(1)}}^{(1)}$ — первая форма в последовательности $f_1^{(1)}, f_2^{(1)}, f_3^{(1)}, \ldots$, не являющаяся линейной комбинацией форм $f_\alpha, f_\beta, \ldots, f_\lambda$; пусть $f_{\beta^{(1)}}^{(1)}$ — первая форма в этой последовательности, не являющаяся линейной комбинацией форм $f_\alpha, f_\beta, \ldots, f_\lambda, f_{\alpha^{(1)}}^{(1)}$; аналогично, пусть $f_{\gamma^{(1)}}^{(1)}$ — первая форма в этой последовательности, не являющаяся линейной комбинацией форм $f_\alpha, f_\beta, \ldots, f_\lambda, f_{\alpha^{(1)}}^{(1)}, f_{\beta^{(1)}}^{(1)}$, и т. д. В силу нашего предположения последовательность форм $f_\alpha, f_\beta, \ldots, f_\lambda, f_{\alpha^{(1)}}^{(1)}, f_{\beta^{(1)}}^{(1)}, f_{\gamma^{(1)}}^{(1)}, \ldots$, получающихся таким образом, должна оборваться через конечное число шагов, и если обозначить через $f_{\lambda^{(1)}}^{(1)}$ последнюю форму в этой последовательности, то мы получим

$$f_s^{(1)} = l_s^{(1)}\left(f_\alpha, f_\beta, \ldots, f_\lambda, f_{\alpha^{(1)}}^{(1)}, f_{\beta^{(1)}}^{(1)}, \ldots, f_{\lambda^{(1)}}^{(1)}\right) \qquad (s = 1, 2, 3, \ldots),$$

где $l_s^{(1)}$ — линейная однородная функция от форм, коэффициенты которых

являются целочисленными формами от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Значит, если мы положим

$$F_s^{(2)} = F_s^{(1)} - l_s^{(1)}\left(x_n F_\alpha, x_n F_\beta, \ldots, x_n F_\lambda, F_{\alpha^{(1)}}^{(1)}, F_{\beta^{(1)}}^{(1)}, \ldots, F_{\lambda^{(1)}}^{(1)}\right),$$

то все получающиеся в результате формы $F_s^{(2)}$ от n переменных $x_1, x_2, \ldots, x_n$ имеют в качестве множителя x_n^2. Обозначим через $x_n^2 f_s^{(2)}$ те члены формы $F_s^{(2)}$, которые содержат только вторую степень x_n, и рассмотрим формы $f_1^{(2)}$, $f_2^{(2)}$, $f_3^{(2)}, \ldots$ от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Если не все эти формы равны нулю или являются линейными комбинациями форм $f_\alpha, f_\beta, \ldots, f_\lambda$, $f_{\alpha^{(1)}}^{(1)}, f_{\beta^{(1)}}^{(1)}, \ldots, f_{\lambda^{(1)}}^{(1)}$, то обозначим через $f_{\alpha^{(2)}}^{(2)}$ первую из этих форм, не являющуюся линейной комбинацией форм этой последовательности; аналогично, пусть $f_{\beta^{(2)}}^{(2)}$ — первая форма в указанной последовательности, не являющаяся линейной комбинацией форм $f_\alpha, f_\beta, \ldots, f_\lambda, f_{\alpha^{(1)}}^{(1)}, f_{\beta^{(1)}}^{(1)}, \ldots, f_{\lambda^{(1)}}^{(1)}, f_{\alpha^{(2)}}^{(2)}$. Этот процесс должен оборваться через конечное число шагов, если считать, что теорема II верна для $n-1$ переменных. Пусть в соответствии с этим $f_{\lambda^{(2)}}^{(2)}$ — последняя форма, получающаяся с помощью этого процесса; тогда

$$f_s^{(2)} = l_s^{(2)}\left(f_\alpha, f_\beta, \ldots, f_\lambda, f_{\alpha^{(1)}}^{(1)}, f_{\beta^{(1)}}^{(1)}, \ldots, f_{\lambda^{(1)}}^{(1)}, f_{\alpha^{(2)}}^{(2)}, f_{\beta^{(2)}}^{(2)}, \ldots, f_{\lambda^{(2)}}^{(2)}\right) \quad (s = 1, 2, 3, \ldots),$$

где $l_s^{(2)}$ — линейная однородная функция, коэффициенты которой являются целочисленными формами от $x_1, x_2, \ldots, x_{n-1}$. Значит, если мы положим

$$F_s^{(3)} = F_s^{(2)} - l_s^{(2)}\Big(x_n^2 F_\alpha, x_n^2 F_\beta, \ldots, x_n^2 F_\lambda, x_n F_{\alpha^{(1)}}^{(1)}, x_n F_{\beta^{(1)}}^{(1)}, \ldots, x_n F_{\lambda^{(1)}}^{(1)}, F_{\alpha^{(2)}}^{(2)}, F_{\beta^{(2)}}^{(2)}, \ldots, F_{\lambda^{(2)}}^{(2)}\Big) \qquad (s = 1, 2, 3, \ldots),$$

то все получающиеся в результате формы $F_s^{(3)}$ содержат множитель x_n^3. Обозначим через $x_n^3 f_s^{(3)}$ те члены формы $F_s^{(3)}$, которые содержат не более чем третью степень x_n; тогда мы получим последовательность форм $f_1^{(3)}$, $f_2^{(3)}$, $f_3^{(3)}, \ldots$, с которой следует поступить аналогично предыдущему. Ясно, что повторение указанного процесса приведет к последовательности форм

$$f_{\alpha^{(\pi)}}^{(\pi)}, \quad f_{\beta^{(\pi)}}^{(\pi)}, \quad \ldots, \quad f_{\lambda^{(\pi)}}^{(\pi)}, \quad f_{\alpha^{(\tau)}}^{(\tau)}, \quad f_{\beta^{(\tau)}}^{(\tau)}, \quad \ldots, \quad f_{\lambda^{(\tau)}}^{(\tau)}, \quad \ldots, \quad \ldots,$$

где $\pi, \tau, \ldots$ — некоторые положительные целые числа и ни одна из форм не является линейной комбинацией предыдущих. Ввиду последнего обстоятельства эта последовательность также должна оборваться через конечное число шагов, если считать, что теорема II верна для $n-1$ переменных. Обозначим последнюю форму этой последовательности через $f_{\lambda^{(\omega)}}^{(\omega)}$ и покажем, что каждая форма в исходной последовательности $F_1, F_2, F_3, \ldots$ является линейной комбинацией форм

$$F_{\alpha^{(\pi)}}^{(\pi)}, F_{\beta^{(\pi)}}^{(\pi)}, \ldots, F_{\lambda^{(\pi)}}^{(\pi)}, F_{\alpha^{(\tau)}}^{(\tau)}, F_{\beta^{(\tau)}}^{(\tau)}, \ldots, F_{\lambda^{(\tau)}}^{(\tau)}, \ldots, F_{\alpha^{(\omega)}}^{(\omega)}, F_{\beta^{(\omega)}}^{(\omega)}, \ldots, F_{\lambda^{(\omega)}}^{(\omega)}. \quad (8)$$

В самом деле, если F_s — какая-либо форма из исходной последовательности,

а r — ее порядок относительно переменных $x_1, x_2, \ldots, x_n$, то рассмотрим уравнения

$$\begin{aligned} F_s^{(r+1)} &= F_s^{(r)} - l_s^{(r)}, \\ F_s^{(r)} &= F_s^{(r-1)} - l_s^{(r-1)}, \\ &\cdots\cdots\cdots\cdots \\ F_s^{(1)} &= F_s - l_s, \end{aligned}$$

где $l_s^{(r)}$, $l_s^{(r-1)}, \ldots, l_s$ — линейные комбинации форм (8). Теперь ввиду того, что форма $F_s^{(r+1)}$ является однородной функцией порядка r и делится в силу построения на x_n^{r+1}, она должна быть тождественно равна нулю, и из указанных выше уравнений следует, что F_s также линейная комбинация форм (8). Но эти формы (8) являются линейными комбинациями форм

$$F_{\alpha^{(\pi)}},\ F_{\beta^{(\pi)}},\ \ldots,\ F_{\lambda^{(\pi)}},\ F_{\alpha^{(\tau)}},\ F_{\beta^{(\tau)}},\ \ldots,\ F_{\lambda^{(\tau)}},\ \ldots,\ F_{\alpha^{(\omega)}},\ F_{\beta^{(\omega)}},\ \ldots,\ F_{\lambda^{(\omega)}},$$

откуда, очевидно, следует, что $m = \lambda^{(\omega)}$ — число, обладающее указанным в теореме II свойством. Это доказывает теорему II для n переменных, если считать ее доказанной для $n-1$ переменных.

Остается доказать, что теорема II справедлива для форм без переменных, т. е. для бесконечной последовательности целых чисел $c_1, c_2, c_3, \ldots$ [18]. Чтобы получить это доказательство, обозначим через c_μ первое ненулевое целое число в этой последовательности; далее пусть $c_{\mu'}$ — ближайшее целое число из этой последовательности, не делящееся на c_μ. Определим тогда наибольший общий делитель $c_{\mu\mu'}$ чисел c_μ и $c_{\mu'}$; он меньше абсолютной величины числа c_μ. Если теперь в последовательности имеется число $c_{\mu''}$, не делящееся на $c_{\mu\mu'}$, то определим наибольший общий делитель $c_{\mu\mu'\mu''}$ чисел $c_{\mu\mu'}$ и $c_{\mu''}$; при этом число $c_{\mu\mu'\mu''}$ будет меньше, чем $c_{\mu\mu'}$. Таким способом получается последовательность целых чисел c_μ , $c_{\mu\mu'}$, $c_{\mu\mu'\mu''}, \ldots$, в которой каждое число меньше, чем предыдущее. Такая последовательность должна оборваться через конечное число шагов; пусть $c_{\mu\mu'\ldots\mu^{(\varkappa)}}$ — последний член этой последовательности. Это число является наибольшим общим делителем чисел c_μ, $c_{\mu'}, \ldots, c_{\mu^{(\varkappa)}}$, и, значит, имеются такие целые числа a, $a', \ldots, a^{(\varkappa)}$, что

$$c_{\mu\mu'\ldots\mu^{(\varkappa)}} = ac_\mu + a'c_{\mu'} + \ldots + a^{(\varkappa)}c_{\mu^{(\varkappa)}}.$$

Ввиду того что каждое число в исходной последовательности $c_1, c_2, c_3, \ldots$ кратно числу $c_{\mu\mu'\ldots\mu^{(\varkappa)}}$, мы получаем теперь, что $m = \mu^{(\varkappa)}$ — число, обладающее указанным в теореме II свойством.

Из только что доказанной теоремы можно вывести все утверждения, соответствующие утверждениям, которые были выведены из теоремы I в первом разделе. Но мы не намерены продолжать исследования в этом направлении и в дальнейшем ограничимся вопросами, охватываемыми теоремой I.

III. Соотношения между формами из произвольной системы форм

Мы возобновим теперь рассмотрения, начатые в разд. I, и будем считать далее, что коэффициенты форм, с которыми мы имеем дело, являются числами из произвольной области рациональности.

Если задан модуль $(F_1, F_2, \ldots, F_{m^{(1)}})$, то мы получаем все остальные формы из этого модуля, т. е. все формы, сравнимые по этому модулю с нулем, образуя выражения

$$A_1F_1 + A_2F_2 + \ldots + A_{m^{(1)}}F_{m^{(1)}},$$

в которых порядки форм $A_1, A_2, \ldots, A_{m^{(1)}}$ выбраны так, что все произведения $A_1F_1, A_2F_2, \ldots, A_{m^{(1)}}F_{m^{(1)}}$ имеют один и тот же порядок, чтобы их сумма являлась однородной функцией. Две *различные* системы форм $A_1, A_2, \ldots, A_{m^{(1)}}$ и $B_1, B_2, \ldots, B_{m^{(1)}}$ дадут *одну и ту же* форму из рассматриваемого модуля, если

$$A_1F_1 + A_2F_2 + \ldots + A_{m^{(1)}}F_{m^{(1)}} = B_1F_1 + B_2F_2 + \ldots + B_{m^{(1)}}F_{m^{(1)}},$$

или

$$(A_1 - B_1)F_1 + (A_2 - B_2)F_2 + \ldots + (A_{m^{(1)}} - B_{m^{(1)}})F_{m^{(1)}} = 0,$$

так что из системы форм $A_1, A_2, \ldots, A_{m^{(1)}}$ мы получаем все прочие системы $B_1, B_2, \ldots, B_{m^{(1)}}$, задающие ту же самую форму из этого модуля, с помощью формул

$$B_1 = A_1 + X_1, \quad B_2 = A_2 + X_2, \quad \ldots, \quad B_{m^{(1)}} = A_{m^{(1)}} + X_{m^{(1)}},$$

где $X_1, X_2, \ldots, X_{m^{(1)}}$ — любое решение системы уравнений

$$F_1X_1 + F_2X_2 + \ldots + F_{m^{(1)}}X_{m^{(1)}} = 0. \tag{9}$$

Таким образом, чтобы глубже разобраться в структуре данного модуля, нужно исследовать это уравнение, рассматривая $F_1, F_2, \ldots, F_{m^{(1)}}$ как заданные коэффициенты, а $X_1, X_2, \ldots, X_{m^{(1)}}$ — как искомые формы. Из результатов разд. I следует, что такое уравнение обладает конечным числом $m^{(2)}$ решений

$$X_1 = F_{1s}^{(1)}, \quad X_2 = F_{2s}^{(1)}, \quad \ldots, \quad X_{m^{(1)}} = F_{m^{(1)}s}^{(1)} \qquad (s = 1, 2, \ldots, m^{(2)}),$$

из которых всякое другое решение получается в виде

$$X_t = A_1^{(1)}F_{t1}^{(1)} + A_2^{(1)}F_{t2}^{(1)} + \ldots + A_{m^{(2)}}^{(1)}F_{tm^{(2)}}^{(1)} \qquad (t = 1, 2, \ldots, m^{(1)}), \tag{10}$$

где $A_1^{(1)}, A_2^{(1)}, \ldots, A_{m^{(2)}}^{(1)}$ — формы от тех же самых переменных $x_1, x_2, \ldots, x_n$. Можно считать, что среди этих $m^{(2)}$ решений не имеется такого, которое получается из остальных как их линейная комбинация. Если, далее, мы изменим в формуле (10) формы $A_1^{(1)}, A_2^{(1)}, \ldots, A_{m^{(2)}}^{(1)}$, то не всегда получим *другое* решение уравнения (9); две различные системы форм $A_1^{(1)}, A_2^{(1)}, \ldots, A_{m^{(2)}}^{(1)}$ и $B_1^{(1)}, B_2^{(1)}, \ldots, B_{m^{(2)}}^{(1)}$ дают *одно и то же* решение $X_1, X_2, \ldots, X_{m^{(1)}}$, если

$$A_1^{(1)}F_{t1}^{(1)} + A_2^{(1)}F_{t2}^{(1)} + \ldots + A_{m^{(2)}}^{(1)}F_{tm^{(2)}}^{(1)} = \\ = B_1^{(1)}F_{t1}^{(1)} + B_2^{(1)}F_{t2}^{(1)} + \ldots + B_{m^{(2)}}^{(1)}F_{tm^{(2)}}^{(1)} \qquad (t = 1, 2, \ldots, m^{(1)}),$$

или

$$(A_1^{(1)} - B_1^{(1)})F_{t1}^{(1)} + (A_2^{(1)} - B_2^{(1)})F_{t2}^{(1)} + \ldots + (A_{m^{(2)}}^{(1)} - B_{m^{(2)}}^{(1)})F_{tm^{(2)}}^{(1)} = 0 \\ (t = 1, 2, \ldots, m^{(1)}),$$

так что мы приходим к рассмотрению системы уравнений

$$F_{t1}^{(1)}X_1^{(1)} + F_{t2}^{(1)}X_2^{(1)} + \ldots + F_{tm^{(2)}}^{(1)}X_{m^{(2)}}^{(1)} = 0 \qquad (t = 1, 2, \ldots, m^{(1)}), \qquad (11)$$

где $F_{t1}^{(1)}$, $F_{t2}^{(1)}, \ldots, F_{tm^{(2)}}^{(1)}$ — заданные коэффициенты, а $X_1^{(1)}$, $X_2^{(1)}, \ldots, X_{m^{(2)}}^{(1)}$ — подлежащие определению формы. Эта система уравнений (11) называется *производной системой* для (9).

Отметим, что при построении производной системы уравнений мы начали с полной системы форм, в которой ни одно из решений не может быть получено из остальных в виде линейной комбинации. Легко видеть, что число и порядок таких решений однозначно определены, а формы, входящие в системы-решения, определены так, что всякое другое решение с тем же свойством получается как линейная комбинация систем-решений исходной системы и других решений равного или меньшего порядка. Ввиду этого производная система уравнений также в аналогичном смысле определяется исходной системой уравнений.

Мы видим, что коэффициенты производной системы состоят из форм от решений исходного уравнения, так что, решая производную систему (11), мы получаем соотношения между решениями исходного уравнения (9). Соответственно определим полную систему решений

$$X_1^{(1)} = F_{1s}^{(2)}, \quad X_2^{(1)} = F_{2s}^{(2)}, \quad \ldots, \quad X_{m^{(2)}}^{(1)} = F_{m^{(2)}s}^{(2)} \qquad (s = 1, 2, \ldots, m^{(3)})$$

производной системы как такую систему, что ни одно из входящих в нее решений не может быть получено в виде линейной комбинации остальных, а любая другая система-решение может быть представлена в виде

$$X_t^{(1)} = A_1^{(2)}F_{t1}^{(2)} + A_2^{(2)}F_{t2}^{(2)} + \ldots + A_{m^{(3)}}^{(2)}F_{tm^{(3)}}^{(2)} \qquad (t = 1, 2, \ldots, m^{(2)}),$$

где $A_1^{(2)}$, $A_2^{(2)}, \ldots, A_{m^{(3)}}^{(2)}$ — произвольные формы. Второе условие приводит к системе уравнений

$$F_{t1}^{(2)}X_1^{(2)} + F_{t2}^{(2)}X_2^{(2)} + \ldots + F_{tm^{(3)}}^{(2)}X_{m^{(3)}}^{(2)} = 0 \qquad (t = 1, 2, \ldots, m^{(2)}), \qquad (12)$$

где $F_{t1}^{(2)}$, $F_{t2}^{(2)}, \ldots, F_{tm^{(3)}}^{(2)}$ — заданные коэффициенты, а $X_1^{(2)}$, $X_2^{(2)}, \ldots, X_{m^{(3)}}^{(3)}$ — подлежащие определению формы. Эта третья система уравнений (12) получена из второй системы уравнений (11) таким же способом, как вторая система уравнений получена из исходной системы уравнений (9). Продолжая этот процесс, мы получим цепь производных систем уравнений, в каждой из которых количество подлежащих определению форм совпадает с числом уравнений в следующей системе.

Чтобы представить дальнейшие рассмотрения в единообразной форме, нужно заменить исходное уравнение на произвольную систему уравнений вида

$$F_{t1}X_1 + F_{t2}X_2 + \ldots + F_{tm^{(1)}}X_{m^{(1)}} = 0 \qquad (t = 1, 2, \ldots, m). \qquad (13)$$

Тогда указанный выше процесс приводит к общей теории таких систем уравнений, ядром которой служит следующая

Теорема III. *Если задана система уравнений* (13), *то задача нахождения соотношений между ее решениями приводит к второй системе такого же типа; аналогичным способом из этой второй,*

производной, системы получается третья производная система. Начавшийся таким образом процесс должен закончиться и, самое большее, n-я система цепи не будет иметь решений.

Доказательство этой теоремы не просто; оно начинается со следующих соображений.

Среди уравнений данной системы некоторые могут быть следствиями остальных в том смысле, что им удовлетворяет каждая система форм, которая удовлетворяет остальным. Мы предположим, что такие уравнения уже исключены, так что в случае, когда решения есть, число m уравнений в системе (13) меньше числа $m^{(1)}$ форм, подлежащих определению, и, кроме того, m-строчные определители

$$D_{i_1 i_2 \ldots i_m} = \begin{vmatrix} F_{1i_1} & F_{1i_2} & \ldots & F_{1i_m} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ F_{mi_1} & F_{mi_2} & \ldots & F_{mi_m} \end{vmatrix},$$

где $i_1, i_2, \ldots, i_m$ обозначают любые m чисел из $1, 2, \ldots, m^{(1)}$, отличны от нуля [19]. Пусть, скажем, $D = D_{12\ldots m}$ — такая отличная от тождественного нуля форма порядка r и определитель D выбран так, что порядки других определителей от переменных $x_1, x_2, \ldots, x_n$ не превосходят r. Кроме того, мы предположим, что осуществлена такая однородная линейная замена переменных $x_1, x_2, \ldots, x_n$, что коэффициент при x_n^r в D стал отличным от нуля. Очевидно, что система уравнений (13) имеет следующие решения:

$$\left.\begin{array}{llll} X_1 = D_{m+1,2,\ldots,m}, & \ldots, & X_m = D_{1,2,\ldots,m-1,m+1}, & X_{m+1} = D, \\ & & X_{m+2} = 0, \quad \ldots, & X_{m^{(1)}} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & & \\ X_1 = D_{m^{(1)},2,\ldots,m}, & \ldots, & X_m = D_{1,2,\ldots,m-1,m^{(1)}}, & X_{m+1} = 0, \\ & & X_{m+2} = 0, \quad \ldots, & X_{m^{(1)}} = D. \end{array}\right\} \quad (14)$$

Если теперь задано решение $X_1, X_2, \ldots, X_{m^{(1)}}$ системы уравнений (13), то, комбинируя его с первым из решений (14), можно получить другое решение $X_1, X_2, \ldots, X_{m^{(1)}}$, в котором вместо формы X_{m+1} будет форма, степень которой по x_n меньше порядка r определителя D, а формы $X_{m+2}, X_{m+3}, \ldots, X_{m^{(1)}}$ останутся неизменными. Полученное решение можно затем скомбинировать со вторым из решений (14), так что на месте X_{m+2} будет форма, степень которой по x_n меньше r. Используя другие решения из (14) аналогичным способом, мы в итоге получим решение $\Xi_1, \Xi_2, \ldots, \Xi_{m^{(1)}}$, в котором степени по x_n каждой из форм $\Xi_{m+1}, \Xi_{m+2}, \ldots, \Xi_{m^{(1)}}$ меньше r. Покажем, что тогда степени по x_n форм $\Xi_1, \Xi_2, \ldots, \Xi_m$ также меньше r. Для этого умножим уравнение

$$F_{t1}\Xi_1 + F_{t2}\Xi_2 + \ldots + F_{tm^{(1)}}\Xi_{m^{(1)}} = 0$$

на определенный элементом F_{ts} минор в D размера $m-1$, а затем сложим все уравнения, которые получаются таким образом при $t = 1, 2, \ldots, m$. Тогда мы приходим к соотношению вида

$$D\Xi_s + D_{1,2,\ldots,m+1,\ldots,m}\Xi_{m+1} + D_{1,2,\ldots,m+2,\ldots,m}\Xi_{m+2} + \ldots$$
$$\ldots + D_{1,2,\ldots,m^{(1)},\ldots,m}\Xi_{m^{(1)}} = 0 \qquad (s = 1, 2, \ldots, m).$$

Поскольку порядки встречающихся в нем определителей не больше, чем порядок r определителя D, отсюда получается, что степени по x_n всех форм Ξ_s меньше r.

Ввиду этого

$$\Xi_s = \xi_{s1}x_n^{r-1} + \xi_{s2}x_n^{r-2} + \ldots + \xi_{sr} \qquad (s = 1, 2, \ldots, m^{(1)}), \tag{15}$$

где $\xi_{s1}, \xi_{s2}, \ldots, \xi_{sr}$ — формы, содержащие только переменные $x_1, x_2, \ldots, x_{n-1}$. Если мы подставим вместо $X_1, X_2, \ldots, X_{m^{(1)}}$ в исходные уравнения (13) эти $m^{(1)}$ выражений (15) для $\Xi_1, \Xi_2, \ldots, \Xi_{m^{(1)}}$, затем упорядочим левые части по степеням x_n, а затем приравняем нулю те выражения, которые умножаются на одинаковые степени x_n, то получим некоторое число μ уравнений для определения $m^{(1)}r$ форм $\xi_{11}, \xi_{12}, \ldots, \xi_{m^{(1)}r}$. Если для краткости обозначить эти формы через $\xi_1, \xi_2, \ldots, \xi_{\mu^{(1)}}$, то указанные μ уравнений могут быть переписаны в виде

$$\varphi_{t1}\xi_1 + \varphi_{t2}\xi_2 + \ldots + \varphi_{t\mu^{(1)}}\xi_{\mu^{(1)}} = 0 \qquad (t = 1, 2, \ldots, \mu), \tag{16}$$

где коэффициенты $\varphi_{t1}, \varphi_{t2}, \ldots, \varphi_{t\mu^{(1)}}$ являются известными формами от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Пусть теперь

$$\xi_1 = \varphi_{1s}^{(1)}, \quad \xi_2 = \varphi_{2s}^{(1)}, \quad \ldots, \quad \xi_{\mu^{(1)}} = \varphi_{\mu^{(1)}s}^{(1)} \qquad (s = 1, 2, \ldots, \mu^{(2)})$$

— полная система решений уравнений (16), в которой ни одно из решений не является линейной комбинацией остальных. Из каждого решения этой системы можно построить с помощью (15) решение исходных уравнений (13). Пусть соответствующими решениями для (13) будут

$$\Xi_1 = \Phi_{1s}^{(1)}, \quad \Xi_2 = \Phi_{2s}^{(1)}, \quad \ldots, \quad \Xi_{m^{(1)}} = \Phi_{m^{(1)}s}^{(1)} \qquad (s = 1, 2, \ldots, \mu^{(2)}). \tag{17}$$

Подводя итог нашим рассмотрениям, мы получаем, что каждое решение $X_1, X_2, \ldots, X_{m^{(1)}}$ исходной системы (13) может быть выражено в виде

$$\begin{aligned}
X_1 = {} & a_1^{(1)}\Phi_{11}^{(1)} + a_2^{(1)}\Phi_{12}^{(1)} + \ldots + a_{\mu^{(2)}}^{(1)}\Phi_{1\mu^{(2)}}^{(1)} + A_1^{(1)}D_{m+1,2,\ldots,m} + \\
& + A_2^{(1)}D_{m+2,2,\ldots,m} + \ldots + A_{m^{(1)}-m}^{(1)}D_{m^{(1)},2,\ldots,m}, \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_m = {} & a_1^{(1)}\Phi_{m1}^{(1)} + a_2^{(1)}\Phi_{m2}^{(1)} + \ldots + a_{\mu^{(2)}}^{(1)}\Phi_{m\mu^{(2)}}^{(1)} + A_1^{(1)}D_{1,2,\ldots,m-1,m+1} + \\
& + A_2^{(1)}D_{1,2,\ldots,m-1,m+2} + \ldots + A_{m^{(1)}-m}^{(1)}D_{1,2,\ldots,m-1,m^{(1)}}, \\
X_{m+1} = {} & a_1^{(1)}\Phi_{m+1,1}^{(1)} + a_2^{(1)}\Phi_{m+1,2}^{(1)} + \ldots + a_{\mu^{(2)}}^{(1)}\Phi_{m+1,\mu^{(2)}}^{(1)} + A_1^{(1)}D + 0 + \ldots + 0, \\
X_{m+2} = {} & a_1^{(1)}\Phi_{m+2,1}^{(1)} + a_2^{(1)}\Phi_{m+2,2}^{(1)} + \ldots + a_{\mu^{(2)}}^{(1)}\Phi_{m+2,\mu^{(2)}}^{(1)} + 0 + A_2^{(1)}D + \ldots + 0, \\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{m^{(1)}} = {} & a_1^{(1)}\Phi_{m^{(1)}1}^{(1)} + a_2^{(1)}\Phi_{m^{(1)}2}^{(1)} + \ldots + a_{\mu^{(2)}}^{(1)}\Phi_{m^{(1)}\mu^{(2)}}^{(1)} + 0 + 0 + \ldots + A_{m^{(1)}-m}^{(1)}D,
\end{aligned}$$

где $a_1^{(1)}, a_2^{(1)}, \ldots, a_{\mu^{(2)}}^{(1)}$ — формы от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$, а $A_1^{(1)}, A_2^{(1)}, \ldots, A_{m^{(1)}-m}^{(1)}$ — формы от n переменных $x_1, x_2, \ldots, x_n$. В частности, и решения

$$X_1 = x_n\Phi_{1s}^{(1)}, \quad X_2 = x_n\Phi_{2s}^{(1)}, \quad \ldots, \quad X_{m^{(1)}} = x_n\Phi_{m^{(1)}s}^{(1)} \qquad (s = 1, 2, \ldots, \mu^{(2)})$$

могут быть представлены в указанном виде. Мы положим соответственно

$$\left.\begin{aligned}
x_n\Phi^{(1)}_{1s} &= \psi^{(2)}_{1s}\Phi^{(1)}_{11} + \ldots + \psi^{(2)}_{\mu^{(2)}s}\Phi^{(1)}_{1\mu^{(2)}} + \chi^{(2)}_{1s}D_{m+1,2,\ldots,m} + \ldots \\
&\qquad \ldots + \chi^{(2)}_{m^{(1)}-m,s}D_{m^{(1)},1,2,\ldots,m}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_n\Phi^{(1)}_{ms} &= \psi^{(2)}_{1s}\Phi^{(1)}_{m1} + \ldots + \psi^{(2)}_{\mu^{(2)}s}\Phi^{(1)}_{m\mu^{(2)}} + \chi^{(2)}_{1s}D_{1,2,\ldots,m-1,m+1} + \ldots \\
&\qquad \ldots + \chi^{(2)}_{m^{(1)}-m,s}D_{1,2,\ldots,m-1,m^{(1)}}, \\
x_n\Phi^{(1)}_{m+1,s} &= \psi^{(2)}_{1s}\Phi^{(1)}_{m+1,1} + \ldots + \psi^{(2)}_{\mu^{(2)}s}\Phi^{(1)}_{m+1,\mu^{(2)}} + \chi^{(2)}_{1s}D + 0 + \ldots + 0, \\
x_n\Phi^{(1)}_{m+2,s} &= \psi^{(2)}_{1s}\Phi^{(1)}_{m+2,1} + \ldots + \psi^{(2)}_{\mu^{(2)}s}\Phi^{(1)}_{m+2,\mu^{(2)}} + 0 + \chi^{(2)}_{2s}D + \ldots + 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_n\Phi^{(1)}_{m^{(1)}s} &= \psi^{(2)}_{1s}\Phi^{(1)}_{m^{(1)}1} + \ldots + \psi^{(2)}_{\mu^{(2)}s}\Phi^{(1)}_{m^{(1)}\mu^{(2)}} + 0 + 0 + \ldots + \chi^{(2)}_{m^{(1)}-m,s}D \\
&\qquad (s = 1, 2, \ldots, \mu^{(2)}),
\end{aligned}\right\} \quad (18)$$

где формы $\psi^{(2)}_{1s}, \ldots, \psi^{(2)}_{\mu^{(2)}s}$, а значит, и формы $\chi^{(2)}_{1s}, \ldots, \chi^{(2)}_{m^{(1)}-m,s}$ содержат только $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$.

Взяв вместе решения (14) и (17), образуем полную систему решений для (13). Рассмотрение соотношений между этими решениями приводит к системе уравнений вида

$$\left.\begin{aligned}
&\Phi^{(1)}_{11}X^{(1)}_1 + \ldots + \Phi^{(1)}_{1\mu^{(2)}}X^{(1)}_{\mu^{(2)}} + D_{m+1,2,\ldots,m}Y^{(1)}_1 + \ldots \\
&\qquad \ldots + D_{m^{(1)},2,\ldots,m}Y^{(1)}_{m^{(1)}-m} = 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\Phi^{(1)}_{m1}X^{(1)}_1 + \ldots + \Phi^{(1)}_{m\mu^{(2)}}X^{(1)}_{\mu^{(2)}} + D_{1,2,\ldots,m-1,m+1}Y^{(1)}_1 + \ldots \\
&\qquad \ldots + D_{1,2,\ldots,m-1,m^{(1)}}Y^{(1)}_{m^{(1)}-m} = 0, \\
&\Phi^{(1)}_{m+1,1}X^{(1)}_1 + \ldots + \Phi^{(1)}_{m+1,\mu^{(2)}}X^{(1)}_{\mu^{(2)}} + DY^{(1)}_1 + 0 + \ldots + 0 = 0, \\
&\Phi^{(1)}_{m+2,1}X^{(1)}_1 + \ldots + \Phi^{(1)}_{m+2,\mu^{(2)}}X^{(1)}_{\mu^{(2)}} + 0 + DY^{(1)}_2 + \ldots + 0 = 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&\Phi^{(1)}_{m^{(1)}1}X^{(1)}_1 + \ldots + \Phi^{(1)}_{m^{(1)}\mu^{(2)}}X^{(1)}_{\mu^{(2)}} + 0 + 0 + \ldots + DY^{(1)}_{m^{(1)}-m} = 0,
\end{aligned}\right\} \quad (19)$$

где $X^{(1)}_1, \ldots, X^{(1)}_{\mu^{(2)}}$, $Y^{(1)}_1, \ldots, Y^{(1)}_{m^{(1)}-m}$ — подлежащие определению формы.

Отметим, что некоторые из решений (14) и (17) могут быть линейными комбинациями остальных и поэтому нельзя утверждать, что (19) является *производной* системой для (13) в смысле, который был определен выше и который имеется в виду в теореме III. Поэтому, чтобы преобразовать систему (19) в *производную* систему для (13), нужно ее еще редуцировать, что мы и проделаем ниже.

Из (18) следует, что система (19) имеет решения

$$\left.\begin{array}{llll} X_1^{(1)} = \psi_{11}^{(2)} - x_n, & X_2^{(1)} = \psi_{21}^{(2)}, & \ldots, & X_{\mu^{(2)}}^{(1)} = \psi_{\mu^{(2)}1}^{(2)}, \\ & Y_1^{(1)} = \chi_{11}^{(2)}, & \ldots, & Y_{m^{(1)}-m}^{(1)} = \chi_{m^{(1)}-m,1}^{(2)}, \\ X_1^{(1)} = \psi_{12}^{(2)}, & X_2^{(1)} = \psi_{22}^{(2)} - x_n, & \ldots, & X_{\mu^{(2)}}^{(1)} = \psi_{\mu^{(2)}2}^{(2)}, \\ & Y_1^{(1)} = \chi_{12}^{(2)}, & \ldots, & Y_{m^{(1)}-m}^{(1)} = \chi_{m^{(1)}-m,2}^{(2)}, \\ \ldots & \ldots & \ldots & \ldots \\ X_1^{(1)} = \psi_{1\mu^{(2)}}^{(2)}, & X_2^{(1)} = \psi_{2\mu^{(2)}}^{(2)}, & \ldots, & X_{\mu^{(2)}}^{(1)} = \psi_{\mu^{(2)}\mu^{(2)}}^{(2)} - x_n, \\ & Y_1^{(1)} = \chi_{1\mu^{(2)}}^{(2)}, & \ldots, & Y_{m^{(1)}-m}^{(1)} = \chi_{m^{(1)}-m,\mu^{(2)}}^{(2)}. \end{array}\right\} \quad (20)$$

Теперь можно, комбинируя любое решение $X_1^{(1)}, \ldots, X_{\mu^{(2)}}^{(1)}, Y_1^{(1)}, \ldots, Y_{m^{(1)}-m}^{(1)}$ системы (19) с решениями (20), построить другое решение

$$X_1^{(1)} = \xi_1^{(1)}, \quad \ldots, \quad X_{\mu^{(2)}}^{(1)} = \xi_{\mu^{(2)}}^{(1)}, \quad Y_1^{(1)} = \mathrm{H}_1^{(1)}, \quad \ldots, \quad Y_{m^{(1)}-m}^{(1)} = \mathrm{H}_{m^{(1)}-m}^{(1)},$$

где $\xi_1^{(1)}, \ldots, \xi_{\mu^{(2)}}^{(1)}$ — формы, содержащие только $n-1$ переменных $x_1, x_2, \ldots$ $\ldots, x_{n-1}$. Подставляя это решение $\xi_1^{(1)}, \ldots, \xi_{\mu^{(2)}}^{(1)}, \mathrm{H}_1^{(1)}, \ldots, \mathrm{H}_{m^{(1)}-m}^{(1)}$ в последние $m^{(1)} - m$ уравнений (19), мы видим, что формы $\mathrm{H}_1^{(1)}, \ldots, \mathrm{H}_{m^{(1)}-m}^{(1)}$ тождественно равны нулю, так что мы получаем следующие уравнения для определения форм $\xi_1^{(1)}, \ldots, \xi_{\mu^{(2)}}^{(1)}$:

$$\Phi_{t1}^{(1)}\xi_1^{(1)} + \Phi_{t2}^{(1)}\xi_2^{(1)} + \ldots + \Phi_{t\mu^{(2)}}^{(1)}\xi_{\mu^{(2)}}^{(1)} = 0 \qquad (t = 1, 2, \ldots, m^{(1)}).$$

Формы $\Phi_{t1}^{(1)}, \Phi_{t2}^{(1)}, \ldots, \Phi_{t\mu^{(2)}}^{(1)}$ содержат переменную x_n в степени не более чем $r-1$. Следовательно, если мы приравняем нулю коэффициенты при степенях x_n в левой части последних уравнений, то получим систему уравнений

$$\varphi_{t1}^{(1)}\xi_1^{(1)} + \varphi_{t2}^{(1)}\xi_2^{(1)} + \ldots + \varphi_{t\mu^{(2)}}^{(1)}\xi_{\mu^{(2)}}^{(1)} = 0 \qquad (t = 1, 2, \ldots, \mu^{(1)}), \qquad (21)$$

в которой как коэффициенты, так и подлежащие определению формы содержат только $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Мы видим, что система (21) является производной системой для (16). Пусть теперь

$$\xi_1^{(1)} = \varphi_{1s}^{(2)}, \quad \xi_2^{(1)} = \varphi_{2s}^{(2)}, \quad \ldots, \quad \xi_{\mu^{(2)}}^{(1)} = \varphi_{\mu^{(2)}s}^{(2)} \qquad (s = 1, 2, \ldots, \mu^{(3)})$$

— полная система решений для (21), в которой ни одно из решений не является линейной комбинацией остальных.

Объединяя последние утверждения, мы видим, что каждое решение системы (19) может быть выражено в виде

$$\left.\begin{aligned}
X_1^{(1)} &= a_1^{(2)}\varphi_{11}^{(2)} + \ldots + a_{\mu^{(3)}}^{(2)}\varphi_{1\mu^{(3)}}^{(2)} + A_1^{(2)}(\psi_{11}^{(2)} - x_n) + \\
&\quad + A_2^{(2)}\psi_{12}^{(2)} + \ldots + A_{\mu^{(2)}}^{(2)}\psi_{1\mu^{(2)}}^{(2)}, \\
X_2^{(1)} &= a_1^{(2)}\varphi_{21}^{(2)} + \ldots + a_{\mu^{(3)}}^{(2)}\varphi_{2\mu^{(3)}}^{(2)} + A_1^{(2)}\psi_{21}^{(2)} + \\
&\quad + A_2^{(2)}(\psi_{22}^{(2)} - x_n) + \ldots + A_{\mu^{(2)}}^{(2)}\psi_{2\mu^{(2)}}^{(2)}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_{\mu^{(2)}}^{(1)} &= a_1^{(2)}\varphi_{\mu^{(2)}1}^{(2)} + \ldots + a_{\mu^{(3)}}^{(2)}\varphi_{\mu^{(2)}\mu^{(3)}}^{(2)} + A_1^{(2)}\psi_{\mu^{(2)}1}^{(2)} + \\
&\quad + A_2^{(2)}\psi_{\mu^{(2)}2}^{(2)} + \ldots + A_{\mu^{(2)}}^{(2)}(\psi_{\mu^{(2)}\mu^{(2)}}^{(2)} - x_n), \\
Y_1^{(1)} &= 0 + \ldots + 0 + A_1^{(2)}\chi_{11}^{(2)} + \\
&\quad + A_2^{(2)}\chi_{12}^{(2)} + \ldots + A_{\mu^{(2)}}^{(2)}\chi_{1\mu^{(2)}}^{(2)}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
Y_{m^{(1)}-m}^{(1)} &= 0 + \ldots + 0 + A_1^{(2)}\chi_{m^{(1)}-m,1}^{(2)} + \\
&\quad + A_2^{(2)}\chi_{m^{(1)}-m,2} + \ldots + A_{\mu^{(2)}}^{(2)}\chi_{m^{(1)}-m,\mu^{(2)}}^{(2)},
\end{aligned}\right\} \quad (22)$$

где $a_1^{(2)}, \ldots, a_{\mu^{(3)}}^{(2)}$ — формы от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$, а $A_1^{(2)}, \ldots, A_{\mu^{(2)}}^{(2)}$ — формы от n переменных $x_1, x_2, \ldots, x_n$. В частности, в указанном виде могут быть выражены решения

$$X_1^{(1)} = x_n\varphi_{1s}^{(2)},\ X_2^{(1)} = x_n\varphi_{2s}^{(2)},\ \ldots,\ X_{\mu^{(2)}}^{(1)} = x_n\varphi_{\mu^{(2)}s}^{(2)},\ Y_1^{(1)} = 0,\ \ldots,\ Y_{m^{(1)}-m}^{(1)} = 0$$
$$(s = 1, 2, \ldots, \mu^{(3)}).$$

Соответственно этому положим

$$\left.\begin{aligned}
x_n\varphi_{1s}^{(2)} &= \psi_{1s}^{(3)}\varphi_{11}^{(2)} + \ldots + \psi_{\mu^{(3)}s}^{(3)}\varphi_{1\mu^{(3)}}^{(2)} + \chi_{1s}^{(3)}(\psi_{11}^{(2)} - x_n) + \ldots \\
&\quad \ldots + \chi_{\mu^{(2)}s}^{(3)}\psi_{1\mu^{(2)}}^{(2)}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
x_n\varphi_{\mu^{(2)}s}^{(2)} &= \psi_{1s}^{(3)}\varphi_{\mu^{(2)}1}^{(2)} + \ldots + \psi_{\mu^{(3)}s}^{(3)}\varphi_{\mu^{(2)}\mu^{(3)}}^{(2)} + \chi_{1s}^{(3)}\psi_{\mu^{(2)}1}^{(2)} + \ldots \\
&\quad \ldots + \chi_{\mu^{(2)}s}^{(3)}(\psi_{\mu^{(2)}\mu^{(2)}}^{(2)} - x_n), \\
0 &= 0 + \ldots + 0 + \chi_{1s}^{(3)}\chi_{11}^{(2)} + \ldots \\
&\quad \ldots + \chi_{\mu^{(2)}s}^{(3)}\chi_{1\mu^{(2)}}^{(2)}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
0 &= 0 + \ldots + 0 + \chi_{1s}^{(3)}\chi_{m^{(1)}-m,1}^{(2)} + \ldots \\
&\quad \ldots + \chi_{\mu^{(2)}s}^{(3)}\chi_{m^{(1)}-m,\mu^{(2)}}^{(2)}, \\
&(s = 1, 2, \ldots, \mu^{(3)})
\end{aligned}\right\} \quad (23)$$

где формы $\psi_{1s}^{(3)},\ldots,\psi_{\mu^{(3)}s}^{(3)}$, а значит, и формы $\chi_{1s}^{(3)},\ldots,\chi_{\mu^{(2)}s}^{(3)}$ содержат только переменные $x_1,\ x_2,\ldots,x_{n-1}$. Ввиду (22) решения (20), взятые вместе с решениями

$$X_1^{(1)}=\varphi_{1s}^{(2)},\ X_2^{(1)}=\varphi_{2s}^{(2)},\ \ldots,\ X_{\mu^{(2)}}^{(1)}=\varphi_{\mu^{(2)}s}^{(2)},\ Y_1^{(1)}=0,\ \ldots,\ Y_{m^{(1)}-m}^{(1)}=0$$
$$(s=1,2,\ldots,\mu^{(3)}),$$

дают полную систему решений для (19). Рассмотрение соотношений между этими решениями приводит к системе уравнений

$$\left.\begin{array}{l}
\varphi_{11}^{(2)}X_1^{(2)}+\ldots+\varphi_{1\mu^{(3)}}^{(2)}X_{\mu^{(3)}}^{(2)}+(\psi_{11}^{(2)}-x_n)Y_1^{(2)}+\ldots+\psi_{1\mu^{(2)}}^{(2)}Y_{\mu^{(2)}}^{(2)}=0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\varphi_{\mu^{(2)}1}^{(2)}X_1^{(2)}+\ldots+\varphi_{\mu^{(2)}\mu^{(2)}}^{(2)}X_{\mu^{(3)}}^{(2)}+\psi_{\mu^{(2)}1}^{(2)}Y_1^{(2)}+\ldots+(\psi_{\mu^{(2)}\mu^{(2)}}^{(2)}-x_n)Y_{\mu^{(2)}}^{(2)}=0,\\
0+\ldots+0+\chi_{11}^{(2)}Y_1^{(2)}+\ldots+\chi_{1\mu^{(2)}}^{(2)}Y_{\mu^{(2)}}^{(2)}=0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
0+\ldots+0+\chi_{m^{(1)}-m,1}^{(2)}Y_1^{(2)}+\ldots+\chi_{m^{(1)}-m,\mu^{(2)}}^{(2)}Y_{\mu^{(2)}}^{(2)}=0,
\end{array}\right\}\quad(24)$$

где $X_1^{(2)},\ldots,X_{\mu^{(3)}}^{(2)},\ Y_1^{(2)},\ldots,Y_{\mu^{(2)}}^{(2)}$ — подлежащие определению формы. Из (23) следует, что (24) имеет решения

$$\left.\begin{array}{l}
X_1^{(2)}=\psi_{11}^{(3)}-x_n,\ \ldots,\ X_{\mu^{(3)}}^{(2)}=\psi_{\mu^{(3)}1}^{(3)},\ Y_1^{(2)}=\chi_{11}^{(3)},\ \ldots\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\ldots,\ Y_{\mu^{(2)}}^{(2)}=\chi_{\mu^{(2)}1}^{(3)},\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
X_1^{(2)}=\psi_{1\mu^{(3)}}^{(3)},\ \ldots,\ X_{\mu^{(3)}}^{(2)}=\psi_{\mu^{(3)}\mu^{(3)}}^{(3)}-x_n,\ Y_1^{(2)}=\chi_{1\mu^{(3)}}^{(3)},\ \ldots,\\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\ldots,\ Y_{\mu^{(2)}}^{(2)}=\chi_{\mu^{(2)}\mu^{(3)}}^{(3)}.
\end{array}\right\}\quad(25)$$

Комбинируя произвольное решение $X_1^{(2)},\ldots,X_{\mu^{(3)}}^{(2)},\ Y_1^{(2)},\ldots,Y_{\mu^{(2)}}^{(2)}$ системы (24) с решениями (25), можно получить другое решение $\xi_1^{(2)},\ldots,\xi_{\mu^{(3)}}^{(2)}$, $\mathrm{H}_1^{(2)},\ldots,\mathrm{H}_{\mu^{(2)}}^{(2)}$, где формы $\xi_1^{(2)},\ldots,\xi_{\mu^{(3)}}^{(2)}$ содержат лишь переменные $x_1,\ x_2,\ldots,x_{n-1}$. Подставляя это решение $\xi_1^{(2)},\ldots,\xi_{\mu^{(3)}}^{(2)},\ \mathrm{H}_1^{(2)},\ldots,\mathrm{H}_{\mu^{(2)}}^{(2)}$ в первые $\mu^{(2)}$ уравнений (24), легко убедиться, что формы $\mathrm{H}_1^{(2)},\ldots,\mathrm{H}_{\mu^{(2)}}^{(2)}$ тождественно равны нулю. Следовательно, мы получаем уравнения

$$\varphi_{s1}^{(2)}\xi_1^{(2)}+\varphi_{s2}^{(2)}\xi_2^{(2)}+\ldots+\varphi_{s\mu^{(3)}}^{(2)}\xi_{\mu^{(3)}}^{(2)}=0\qquad(s=1,2,\ldots,\mu^{(2)})\qquad(26)$$

для определения форм $\xi_1^{(2)},\ldots,\xi_{\mu^{(3)}}^{(2)}$. В этих уравнениях как коэффициенты, так и подлежащие определению формы содержат лишь $n-1$ переменных $x_1,\ x_2,\ldots,x_{n-1}$. Система (26) является, как мы видели, производной для системы (21).

Полная система решений для (24) может быть образована из решений (25) и решений вида

$$X_1^{(2)} = \xi_1^{(2)}, \quad \ldots, \quad X_{\mu^{(3)}}^{(2)} = \xi_{\mu^{(3)}}^{(2)}, \quad Y_1^{(2)} = 0, \quad \ldots, \quad Y_{\mu^{(2)}}^{(2)} = 0,$$

где $\xi_1^{(2)}, \ldots, \xi_{\mu^{(3)}}^{(2)}$ — решения системы (26).

Продолжение только что описанного процесса даст цепь систем уравнений (13), (19), (24), ... и одновременно цепь производных систем (16), (21), (26), ... Эти две цепи систем уравнений очень тесно между собой связаны: полная система решений π-й системы в цепи (13), (19), (24), ... может быть образована из решений вида

$$\left.\begin{aligned}
X_1^{(\pi-1)} &= \psi_{11}^{(\pi)} - x_n, \quad \ldots, \quad X_{\mu^{(\pi)}}^{(\pi-1)} = \psi_{\mu^{(\pi)}1}^{(\pi)}, \\
Y_1^{(\pi-1)} &= \chi_{11}^{(\pi)}, \quad \ldots, \quad Y_{\mu^{(\pi-1)}}^{(\pi-1)} = \chi_{\mu^{(\pi-1)}1}^{(\pi)}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_1^{(\pi-1)} &= \psi_{1\mu^{(\pi)}}^{(\pi)}, \quad \ldots, \quad X_{\mu^{(\pi)}}^{(\pi-1)} = \psi_{\mu^{(\pi)}\mu^{(\pi)}}^{(\pi)} - x_n, \\
Y_1^{(\pi-1)} &= \chi_{1\mu^{(\pi)}}^{(\pi)}, \quad \ldots, \quad Y_{\mu^{(\pi-1)}}^{(\pi-1)} = \chi_{\mu^{(\pi-1)}\mu^{(\pi)}}^{(\pi)}
\end{aligned}\right\} \qquad (27)$$

и решений вида

$$X_1^{(\pi-1)} = \xi_1^{(\pi-1)}, \quad \ldots, \quad X_{\mu^{(\pi)}}^{(\pi-1)} = \xi_{\mu^{(\pi)}}^{(\pi-1)}, \quad Y_1^{(\pi-1)} = 0, \quad \ldots, \quad Y_{\mu^{(\pi-1)}}^{(\pi-1)} = 0,$$

где $\xi_1^{(\pi-1)}, \ldots, \xi_{\mu^{(\pi)}}^{(\pi-1)}$ — решения π-й системы уравнений в цепи (16), (21), (26), ... В системе (27) $\psi_{11}^{(\pi)}, \ldots, \psi_{\mu^{(\pi)}\mu^{(\pi)}}^{(\pi)}$, $\chi_{11}^{(\pi)}, \ldots, \chi_{\mu^{(\pi-1)}\mu^{(\pi)}}^{(\pi)}$ обозначают формы от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Легко видеть, что между решениями (27) нет соотношений, т. е. следующая система уравнений (28) не имеет решения:

$$\left.\begin{aligned}
(\psi_{11}^{(\pi)} - x_n)Y_1^{(\pi)} + \ldots + \psi_{1\mu^{(\pi)}}^{(\pi)} Y_{\mu^{(\pi)}}^{(\pi)} &= 0, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\psi_{\mu^{(\pi)}1}^{(\pi)} Y_1^{(\pi)} + \ldots + (\psi_{\mu^{(\pi)}\mu^{(\pi)}}^{(\pi)} - x_n)Y_{\mu^{(\pi)}}^{(\pi)} &= 0, \\
\chi_{11}^{(\pi)} Y_1^{(\pi)} + \ldots + \chi_{1\mu^{(\pi)}}^{(\pi)} Y_{\mu^{(\pi)}}^{(\pi)} &= 0, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\
\chi_{\mu^{(\pi-1)}1}^{(\pi)} Y_1^{(\pi)} + \ldots + \chi_{\mu^{(\pi-1)}\mu^{(\pi)}}^{(\pi)} Y_{\mu^{(\pi)}}^{(\pi)} &= 0.
\end{aligned}\right\} \qquad (28)$$

В системах уравнений (16), (21), (26), ... второй цепи рассматриваются лишь формы, не зависящие от переменной x_n. Значит, если мы предположим, что теорема III справедлива в случае $n-1$ переменных, то цепь (16), (21), (26), ... содержит — самое позднее, на $(n-1)$-м месте — систему, не имеющую решения. Ввиду этого цепь (13), (19), (24), ... должна содержать систему, имеющую полную систему решений, каждое из которых имеет вид (27), и притом не позднее, чем на $(n-1)$-м месте. Но тогда следующая система уравнений в цепи (13), (19), (24), ... имеет вид (28)

(и расположена, самое позднее, на n-м месте), и такая система не имеет решений в силу справедливости теоремы III для $n-1$ переменных — таким образом, мы показали, что цепь систем уравнений (13), (19), (24), ... должна оборваться, самое позднее, на n-й системе.

π-я система в цепи систем уравнений (13), (19), (24), ... получается с помощью построения описанным выше способом полной системы решений $(\pi-1)$-й системы и последующего рассмотрения линейных комбинаций этих решений с неопределенными коэффициентами, равных нулю. Поскольку полная система решений, получающаяся с помощью нашего процесса, вообще говоря, содержит решения, являющиеся линейными комбинациями остальных, π-я система уравнений в цепи (13), (19), (24), ... может и не быть *производной* системой $(\pi-1)$-й системы в определенном выше и предполагаемом теоремой III смысле. Однако нетрудно получить цепь *производных* систем для (13) из цепи (13), (19), (24), ...; это можно сделать, найдя те системы форм в цепи систем уравнений (13), (19), (24), ..., которые определяются именно лишними решениями, и удалив их или же заменив их на линейные комбинации остальных систем форм. Это замечание показывает также, что количество уравнений и неизвестных форм в системах цепи (13), (19), (24), ... не возрастет при получении цепи *производных* систем уравнений для (13) из цепи (13), (19), (24), ... А поскольку, согласно нашему предыдущему результату, цепь (13), (19), (24), ... обрывается, самое большее, на n-й системе, цепь производных систем для (13) также должна обладать этим свойством. Это доказывает теорему III для форм от n переменных в предположении, что она справедлива в случае $n-1$ переменных.

Чтобы доказать справедливость теоремы III для случая $n=2$, мы предположим, что дана система уравнений типа

$$F_{t1}X_1 + F_{t2}X_2 + \ldots + F_{tm^{(1)}}X_{m^{(1)}} = 0 \qquad (t = 1, 2, \ldots, m), \tag{29}$$

где F_{t1}, $F_{t2}, \ldots, F_{tm^{(1)}}$ — бинарные формы от переменных x_1, x_2. Пусть

$$X_1 = F^{(1)}_{1,s}, X_2 = F^{(1)}_{2,s}, \ldots, X_{m^{(1)}} = F^{(1)}_{m^{(1)},s} \qquad (s = 1, 2, \ldots, m^{(2)})$$

— полная система решений для (29), ни одно из которых не является линейной комбинацией остальных. Тогда производной системой для (29) является система уравнений типа

$$F^{(1)}_{t1}X^{(1)}_1 + F^{(1)}_{t2}X^{(1)}_2 + \ldots + F^{(1)}_{tm^{(2)}}X^{(1)}_{m^{(2)}} = 0 \qquad (t = 1, 2, \ldots, m^{(1)}), \tag{30}$$

и следует доказать, что эта система не имеет решений. Предположим, что это не так, и пусть $X^{(1)}_1$, $X^{(1)}_2, \ldots, X^{(1)}_{m^{(2)}}$ — бинарные формы порядков r_1, $r_2, \ldots, r_{m^{(2)}}$ соответственно, удовлетворяющие системе (30). Предположим, что эти формы занумерованы так, что

$$r_1 \leqslant r_2 \leqslant r_3 \leqslant \ldots \leqslant r_{m^{(2)}},$$

и пусть l — бинарная форма, не являющаяся делителем $x_1X^{(1)}_1$. Определим тогда константы c_2, $c_3, \ldots, c_{m^{(2)}}$ так, чтобы все формы

$$Y^{(1)}_s = X^{(1)}_s + c_s x_1^{r_s - r_1} X^{(1)}_1 \qquad (s = 2, 3, \ldots, m^{(2)})$$

делились на l. Если мы положим

$$G_{t1}^{(1)} = F_{t1}^{(1)} - c_2 x_1^{r_2-r_1} F_{t2}^{(1)} - c_3 x_1^{r_3-r_1} F_{t3}^{(1)} - \ldots$$
$$\ldots - c_{m^{(2)}} x_1^{r_{m^{(2)}}-r_1} F_{tm^{(2)}}^{(1)} \qquad (t = 1, 2, \ldots, m^{(1)}), \quad (31)$$

то

$$G_{t1}^{(1)} X_1^{(1)} + F_{t2}^{(1)} Y_2^{(1)} + F_{t3}^{(1)} Y_3^{(1)} + \ldots + F_{tm^{(2)}}^{(1)} Y_{m^{(2)}}^{(1)} = 0 \quad (t = 1, 2, \ldots, m^{(1)}).$$

Отсюда следует, что все формы $G_{t1}^{(1)}$ делятся на l. В соответствии с этим положим

$$G_{t1}^{(1)} = l H_{t1}^{(1)} \qquad (t = 1, 2, \ldots, m^{(1)}). \quad (32)$$

Формы

$$X_1 = G_{11}^{(1)}, \quad X_2 = G_{21}^{(1)}, \quad \ldots, \quad X_{m^{(1)}} = G_{m^{(1)}1}^{(1)}$$

удовлетворяют исходной системе уравнений (29), а значит, этим же свойством обладают и формы

$$X_1 = H_{11}^{(1)}, \quad X_2 = H_{21}^{(1)}, \quad \ldots, \quad X_{m^{(1)}} = H_{m^{(1)}1}^{(1)}.$$

Отсюда вытекает, что это последнее решение также может быть получено как линейная комбинация указанных выше $m^{(2)}$ решений. А поскольку формы $H_{t1}^{(1)}$ имеют меньший порядок, чем формы $F_{t1}^{(1)}$ соответственно, то

$$H_{t1}^{(1)} = A_2 F_{t2}^{(1)} + A_3 F_{t3}^{(1)} + \ldots + A_{m^{(2)}} F_{tm^{(2)}}^{(1)} \qquad (t = 1, 2, \ldots, m^{(1)})$$

для некоторых бинарных форм $A_2, A_3, \ldots, A_{m^{(2)}}$. Из этих формул и из формул (31) и (32) мы непосредственно получаем

$$F_{t1}^{(1)} = A_2^{(1)} F_{t2}^{(1)} + A_3^{(1)} F_{t3}^{(1)} + \ldots + A_{m^{(2)}}^{(1)} F_{tm^{(2)}}^{(1)} \qquad (t = 1, 2, \ldots, m^{(1)}),$$

где $A_2^{(1)}, A_3^{(1)}, \ldots, A_{m^{(2)}}^{(1)}$ — некоторые другие бинарные формы; иначе говоря, первые $m^{(2)}$ решений являются линейными комбинациями остальных. Это — противоречие, и поэтому наше предположение, что система (30) имеет решение, недопустимо. Это доказывает теорему III для бинарных форм, а значит, и в общем случае.

Мы уже объясняли, в какой степени формы из полной системы решений, не содержащей лишних решений, определяются данной системой уравнений. Очевидно, что цепь производных систем уравнений также ею по существу определяется в похожем смысле.

Исследуя модуль $(F_1, F_2, \ldots, F_m)$, мы берем

$$F_1 X_1 + F_2 X_2 + \ldots + F_m X_m = 0$$

в качестве первой системы уравнений. Построение цепи производных систем для этой системы позволяет, как мы увидим позже, глубоко проникнуть в алгебраическую структуру данного модуля.

Чтобы проиллюстрировать наши общие рассмотрения, мы приведем теперь несколько примеров.

Модуль (F_1, F_2, F_3), построенный по трем квадратичным формам

$$F_1 = x_1 x_3 - x_2^2,$$
$$F_2 = x_2 x_3 - x_1 x_4,$$
$$F_3 = x_2 x_4 - x_3^2,$$

рассмотренным в разд. I, приводит к уравнению

$$F_1X_1 + F_2X_2 + F_3X_3 = 0.$$

Как показано выше, каждое решение этого уравнения может быть выражено в виде

$$\begin{aligned} X_1 &= x_3Y_1 + x_4Y_2, \\ X_2 &= x_2Y_1 + x_3Y_2, \\ X_3 &= x_1Y_1 + x_2Y_2, \end{aligned}$$

где Y_1, Y_2 — квадратичные формы. Это приводит к производной системе

$$\begin{aligned} x_3Y_1 + x_4Y_2 &= 0, \\ x_2Y_1 + x_3Y_2 &= 0, \\ x_1Y_1 + x_2Y_2 &= 0, \end{aligned}$$

которая не имеет решений. Таким образом, в этом случае цепь обрывается на второй системе уравнений.

В качестве примера рассмотрим модуль $(F_1, F_2, \ldots, F_6)$, где F_1, $F_2, \ldots, F_6$ — формы второго порядка от пяти переменных x_1, $x_2, \ldots, x_5$, рассмотренные в разд. I. Уравнение

$$F_1X_1 + F_2X_2 + \ldots + F_6X_6 = 0$$

имеет восемь указанных там решений, причем ни одно из них не является линейной комбинацией остальных, а всякое другое решение этого уравнения может быть получено из этих восьми. Значит, общее решение данного уравнения имеет вид

$$\begin{aligned} X_1 = {} & x_3Y_1 + x_4Y_2 + x_5Y_3, \\ X_2 = {} & -x_2Y_1 - x_3Y_2 + x_3Y_4 + x_4Y_5 + x_5Y_6, \\ X_3 = {} & -x_1Y_1 - x_2Y_2 - x_3Y_3 - x_3Y_5 - x_4Y_6 + x_4Y_7 + x_5Y_8, \\ X_4 = {} & x_1Y_1 + x_2Y_2 - x_2Y_4 - x_4Y_7 - x_5Y_8, \\ X_5 = {} & x_2Y_3 + x_1Y_4 + x_3Y_7 + x_4Y_8, \\ X_6 = {} & x_1Y_5 + x_2Y_6 - x_2Y_7 - x_3Y_8, \end{aligned}$$

где $Y_1, Y_2, \ldots, Y_8$ — произвольные формы. Теперь мы можем получить производную систему уравнений, приравнивая нулю выражения, стоящие в правых частях предыдущих формул, и эта производная система имеет три решения

$$\begin{array}{llllll} Y_1 = x_4, & Y_2 = -x_3, & Y_3 = 0, & Y_4 = -x_3, & Y_5 = x_2, & Y_6 = 0, \\ & & & & Y_7 = x_1, & Y_8 = 0, \\ Y_1 = x_5, & Y_2 = 0, & Y_3 = -x_3, & Y_4 = -x_4, & Y_5 = x_3, & Y_6 = x_2, \\ & & & & Y_7 = x_2, & Y_8 = x_1, \\ Y_1 = 0, & Y_2 = x_5, & Y_3 = -x_4, & Y_4 = 0, & Y_5 = 0, & Y_6 = x_3, \\ & & & & Y_7 = 0, & Y_8 = x_2. \end{array}$$

Любое другое решение производной системы может быть получено из этих, и, значит, следующей производной системой является

$$\begin{aligned}
x_4Z_1 + x_5Z_2 &= 0,\\
-x_3Z_1 + x_5Z_3 &= 0,\\
-x_3Z_2 - x_4Z_3 &= 0,\\
-x_3Z_1 - x_4Z_2 &= 0,\\
x_2Z_1 + x_3Z_2 &= 0,\\
x_2Z_2 + x_3Z_3 &= 0,\\
x_1Z_1 + x_2Z_2 &= 0,\\
x_1Z_2 + x_2Z_3 &= 0.
\end{aligned}$$

Эта система не имеет решений, и поэтому цепь, определенная данным модулем, обрывается на третьей системе уравнений.

В качестве более общего примера мы рассмотрим модуль $(x_1, x_2, \ldots, x_n)$ и докажем следующее предложение:

В цепи производных систем уравнений для уравнения

$$x_1X_1 + x_2X_2 + \ldots + x_nX_n = 0 \tag{33}$$

s-я система состоит из $\binom{n}{s-1}$ уравнений, число подлежащих определению форм этой системы равно $\binom{n}{s}$, а число решений в полной системе решений этой системы равно $\binom{n}{s+1}$. Все коэффициенты производных уравнений являются линейными формами.

Для небольших значений n это предложение легко проверяется с помощью непосредственного нахождения производных систем. Например, в случае $n = 4$ получаем, что уравнение

$$x_1X_1 + x_2X_2 + x_3X_3 + x_4X_4 = 0$$

имеет шесть решений

$$\begin{aligned}
&X_1 = x_2, && X_2 = -x_1, && X_3 = 0, && X_4 = 0,\\
&X_1 = x_3, && X_2 = 0, && X_3 = -x_1, && X_4 = 0,\\
&X_1 = x_4, && X_2 = 0, && X_3 = 0, && X_4 = -x_1,\\
&X_1 = 0, && X_2 = x_3, && X_3 = -x_2, && X_4 = 0,\\
&X_1 = 0, && X_2 = x_4, && X_3 = 0, && X_4 = -x_2,\\
&X_1 = 0, && X_2 = 0, && X_3 = x_4, && X_4 = -x_3,
\end{aligned}$$

и поэтому производной системой является

$$\begin{aligned}
x_2Y_1 + x_3Y_2 + x_4Y_3 &= 0,\\
-x_1Y_1 + x_3Y_4 + x_4Y_5 &= 0,\\
-x_1Y_2 - x_2Y_4 + x_4Y_6 &= 0,\\
-x_1Y_3 - x_2Y_5 - x_3Y_6 &= 0.
\end{aligned}$$

Решения этой системы имеют вид

$$\begin{array}{llllll}
Y_1 = x_3, & Y_2 = -x_2, & Y_3 = 0, & Y_4 = x_1, & Y_5 = 0, & Y_6 = 0,\\
Y_1 = -x_4, & Y_2 = 0, & Y_3 = x_2, & Y_4 = 0, & Y_5 = -x_1, & Y_6 = 0,\\
Y_1 = 0, & Y_2 = x_4, & Y_3 = -x_3, & Y_4 = 0, & Y_5 = 0, & Y_6 = x_1,\\
Y_1 = 0, & Y_2 = 0, & Y_3 = 0, & Y_4 = -x_4, & Y_5 = x_3, & Y_6 = -x_2.
\end{array}$$

Следовательно, третьей системой в цепи будет

$$\begin{aligned}
x_3Z_1 - x_4Z_2 &= 0,\\
-x_2Z_1 + x_4Z_3 &= 0,\\
x_2Z_2 - x_3Z_3 &= 0,\\
x_1Z_1 - x_4Z_4 &= 0,\\
-x_1Z_2 + x_3Z_4 &= 0,\\
x_1Z_3 - x_2Z_4 &= 0.
\end{aligned}$$

Поскольку эта система имеет только одно решение

$$Z_1 = x_4, \quad Z_2 = x_3, \quad Z_3 = x_2, \quad Z_4 = x_1,$$

то четвертой системой в цепи является

$$\begin{aligned}
x_4U_1 &= 0,\\
x_3U_1 &= 0,\\
x_2U_1 &= 0,\\
x_1U_1 &= 0,
\end{aligned}$$

и эта система, очевидно, не имеет решений. Таким образом, цепь производных систем обрывается на четвертой системе.

Для доказательства предложения в общем случае мы воспользуемся теми же соображениями, на которых основывалось доказательство теоремы III. Уравнение (33) допускает $n-1$ решений

$$\begin{array}{llllll}
X_1 = x_n, & X_2 = 0, & X_3 = 0, & \ldots, & X_{n-1} = 0, & X_n = -x_1,\\
X_1 = 0, & X_2 = x_n, & X_3 = 0, & \ldots, & X_{n-1} = 0, & X_n = -x_2,\\
X_1 = 0, & X_2 = 0, & X_3 = x_n, & \ldots, & X_{n-1} = 0, & X_n = -x_3,\\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots\\
X_1 = 0, & X_2 = 0, & X_3 = 0, & \ldots, & X_{n-1} = x_n, & X_n = -x_{n-1}.
\end{array}$$

Возьмем теперь произвольное решение $X_1, X_2, \ldots, X_n$ уравнения (33) и, комбинируя его соответствующим образом с $n-1$ указанными частными решениями, преобразуем в такое решение, у которого $X_1, X_2, \ldots, X_{n-1}$ будут формами, не содержащими переменной x_n. Поскольку в уравнении (33) форма X_n умножается на переменную x_n, форма, возникшая после преобразования на месте X_n, будет тождественным нулем. Предположим теперь, что наше предложение доказано для случая $n-1$ переменных; тогда уравнение

$$x_1X_1 + x_2X_2 + \ldots + x_{n-1}X_{n-1} = 0 \tag{34}$$

имеет ровно $\binom{n-1}{2}$ решений, ни одно из которых не является линейной комбинацией остальных и из которых получается всякое другое решение. Кроме того, поскольку, согласно этому предложению, все решения являются линейными формами, общее решение уравнения (34) выражается в виде

$$\begin{aligned} X_1 &= l_{11}y_1 + l_{12}y_2 + \ldots + l_{1,\binom{n-1}{2}}y_{\binom{n-1}{2}}, \\ X_2 &= l_{21}y_1 + l_{22}y_2 + \ldots + l_{2,\binom{n-1}{2}}y_{\binom{n-1}{2}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_{n-1} &= l_{n-1,1}y_1 + l_{n-1,2}y_2 + \ldots + l_{n-1,\binom{n-1}{2}}y_{\binom{n-1}{2}}, \end{aligned}$$

где $l_{11}, l_{12}, \ldots, l_{n-1,\binom{n-1}{2}}$ — линейные формы от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$, а $y_1, y_2, \ldots, y_{\binom{n-1}{2}}$ — произвольные формы от тех же переменных. Мы видим из предыдущего, что каждое решение исходного уравнения (33) может быть выражено в виде

$$\begin{aligned} X_1 &= x_nY_1 + 0 + \ldots + l_{11}y_1 + \ldots + l_{1,\binom{n-1}{2}}y_{\binom{n-1}{2}}, \\ X_2 &= 0 + x_nY_2 + \ldots + l_{21}y_1 + \ldots + l_{2,\binom{n-1}{2}}y_{\binom{n-1}{2}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_n &= -x_1Y_1 - x_2Y_2 - \ldots + 0 + \ldots + 0, \end{aligned}$$

где $Y_1, Y_2, \ldots, Y_{n-1}$ — формы от n переменных $x_1, x_2, \ldots, x_n$, а $y_1, \ldots, y_{\binom{n-1}{2}}$ — формы от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. А поскольку ни одно из использованных частных решений не является линейной комбинацией остальных решений, общее число решений уравнения (33) равно $n-1+\binom{n-1}{2}$, т. е. — в согласии с предложением — равно $\binom{n}{2}$, а производная система для (33) имеет вид

$$\left.\begin{aligned} x_nY_1 + \ldots + l_{11}Y_n + \ldots + l_{1,\binom{n-1}{2}}Y_{\binom{n}{2}} &= 0, \\ x_nY_2 + \ldots + l_{21}Y_n + \ldots + l_{2,\binom{n-1}{2}}Y_{\binom{n}{2}} &= 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ -x_1Y_1 - x_2Y_2 - \ldots + 0 + \ldots + 0 &= 0. \end{aligned}\right\} \qquad (35)$$

Чтобы найти следующую производную систему, заметим, что производная система (35) обладает решениями

$$\begin{aligned} &Y_1 = l_{11}, \quad Y_2 = l_{21}, \quad \ldots, Y_{n-1} = l_{n-1,1}, \quad Y_n = -x_n, \; Y_{n+1} = 0, \quad \ldots \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots, \quad Y_{\binom{n}{2}} = 0, \\ &Y_1 = l_{12}, \quad Y_2 = l_{22}, \quad \ldots, Y_{n-1} = l_{n-1,2}, \quad Y_n = 0, \quad Y_{n+1} = -x_n, \ldots \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots, \quad Y_{\binom{n}{2}} = 0, \\ &Y_1 = l_{1,\binom{n-1}{2}}, \; Y_2 = l_{2,\binom{n-1}{2}}, \ldots, Y_{n-1} = l_{n-1,\binom{n-1}{2}}, \; Y_n = 0, \quad Y_{n+1} = 0, \quad \ldots \\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \ldots, \quad Y_{\binom{n}{2}} = -x_n. \end{aligned}$$

Используя соображения, примененные ранее в доказательстве теоремы III, легко убедиться, что каждое решение системы (35) может быть получено

из $\binom{n-1}{2}$ данных решений и решения

$$Y_1 = 0, \quad \ldots, \quad Y_{n-1} = 0, \quad Y_n = y_1, \quad Y_{n+1} = y_2, \quad \ldots, \quad Y_{\binom{n}{2}} = y_{\binom{n-1}{2}},$$

где $y_1, y_2, \ldots, y_{\binom{n-1}{2}}$ — решение системы уравнений

$$l_{s1}y_1 + l_{s2}y_2 + \ldots + l_{s,\binom{n-1}{2}}y_{\binom{n-1}{2}} = 0 \qquad (s = 1, 2, \ldots, n-1).$$

Последняя система есть производная система для (34), а значит, ввиду нашего предложения имеет ровно $\binom{n-1}{3}$ решений, ни одно из которых не является линейной комбинацией остальных и из которых может быть получено любое другое решение. Общее число рассматриваемых решений производной системы (35) уравнения (33) равно поэтому $\binom{n-1}{2} + \binom{n-1}{3}$, т. е. $\binom{n}{3}$, что снова согласуется с нашим предложением. Продолжая рассуждать таким образом и предполагая, что предложение справедливо для $n-1$ переменных, мы убедимся в справедливости нашего предложения в случае n переменных. Поскольку предложение непосредственно очевидно для $n = 2$, оно справедливо и в общем случае.

Это исследование уравнения (33) *особенно важно с принципиальной точки зрения, поскольку оно доставляет случай, когда цепь производных систем обрывается лишь на n-й системе.*

IV. Характеристическая функция модуля

Рассмотрения предыдущего раздела дают нам возможность найти число условий, которым должны удовлетворять коэффициенты формы, если она сравнима с нулем по данному модулю [20]. Чтобы убедиться в этом, рассмотрим модуль $(F_1, F_2, \ldots, F_m)$, где $F_1, F_2, \ldots, F_m$ — однородные формы от переменных $x_1, x_2, \ldots, x_n$ порядков $r_1, r_2, \ldots, r_m$ соответственно. Найдем сначала число линейно независимых форм F порядка R, сравнимых с нулем по этому модулю. Полагая

$$F = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

где $A_1, A_2, \ldots, A_m$ — формы порядков $R - r_1, R - r_2, \ldots, R - r_m$ соответственно, мы получаем, согласно рассмотрениям из начала предыдущего раздела, что число, о котором идет речь, равно общему числу коэффициентов форм $A_1, A_2, \ldots, A_m$ минус число тех линейно независимых решений уравнения

$$F_1X_1 + F_2X_2 + \ldots + F_mX_m = 0, \tag{36}$$

для которых $X_1, X_2, \ldots, X_m$ — формы порядков $R - r_1, R - r_2, \ldots, R - r_m$ соответственно. Согласно результатам, полученным в конце разд. I, каждое решение уравнения (36) может быть получено из конечного числа решений с помощью формул

$$X_t = A_1^{(1)}F_{t1}^{(1)} + A_2^{(1)}F_{t2}^{(1)} + \ldots + A_{m^{(1)}}^{(1)}F_{tm^{(1)}}^{(1)} \qquad (t = 1, 2, \ldots, m).$$

Если мы обозначим порядки форм $F_{11}^{(1)}, F_{12}^{(1)}, \ldots, F_{1m^{(1)}}^{(1)}$ через $r_1^{(1)}, r_2^{(1)}, \ldots, r_{m^{(1)}}^{(1)}$ соответственно, то $A_1^{(1)}, A_2^{(1)}, \ldots, A_{m^{(1)}}^{(1)}$ — формы порядков $R - r_1 - r_1^{(1)}$, $R - r_1 - r_2^{(1)}, \ldots, R - r_1 - r_{m^{(1)}}^{(1)}$ соответственно. Следовательно, мы получим нужное нам число линейно независимых решений уравнения (36), если вычтем

из общего числа коэффициентов форм $A_1^{(1)}$, $A_2^{(1)},\ldots,A_{m^{(1)}}^{(1)}$ число линейно независимых систем форм $X_1^{(1)}$, $X_2^{(1)},\ldots,X_{m^{(1)}}^{(1)}$ порядков $R-r_1-r_1^{(1)}$, $R-r_1-r_2^{(1)},\ldots,R-r_1-r_{m^{(1)}}^{(1)}$, удовлетворяющих уравнениям

$$X_1^{(1)}F_{t1}^{(1)}+X_2^{(1)}F_{t2}^{(1)}+\ldots+X_{m^{(1)}}^{(1)}F_{tm^{(1)}}^{(1)}=0 \qquad (t=1,2,\ldots,m). \tag{37}$$

Чтобы найти это последнее число, мы должны вспомнить, что все решения уравнений (37) могут быть получены из конечного числа таких решений. Значит, это число, очевидно, получается вычитанием из общего числа коэффициентов рассматриваемых форм числа линейно независимых решений производной системы для (37). Этот процесс следует продолжать до тех пор, пока цепь производных систем для (36) не оборвется [21]. Если теперь порядок R формы F выбран настолько большим, что все встречающиеся в этом процессе числа $R-r_1$, $R-r_2,\ldots,R-r_m$, $R-r_1-r_1^{(1)}$, $R-r_1-r_2^{(1)},\ldots,R-r_1-r_{m^{(1)}}^{(1)},\ldots$ положительны, то все эти числа являются линейными комбинациями с целыми коэффициентами чисел членов общих форм порядков $R-r_1$, $R-r_2,\ldots,R-r_m$, $R-r_1-r_1^{(1)}$, $R-r_1-r_2^{(1)},\ldots,R-r_1-r_{m^{(1)}}^{(1)},\ldots$ Эти последние числа задаются следующими выражениями:

$$\frac{(R-r_1+1)(R-r_1+2)\ldots(R-r_1+n-1)}{1\cdot 2\cdot\ldots\cdot(n-1)},\ldots,$$

$$\frac{(R-r_m+1)(R-r_m+2)\ldots(R-r_m+n-1)}{1\cdot 2\cdot\ldots\cdot(n-1)},\ldots,$$

$$\frac{(R-r_1-r_1^{(1)}+1)(R-r_1-r_1^{(1)}+2)\ldots(R-r_1-r_1^{(1)}+n-1)}{1\cdot 2\cdot\ldots\cdot(n-1)},\ldots,$$

$$\frac{(R-r_1-r_{m^{(1)}}^{(1)}+1)(R-r_1-r_{m^{(1)}}^{(1)}+2)\ldots(R-r_1-r_{m^{(1)}}^{(1)}+n-1)}{1\cdot 2\cdot\ldots\cdot(n-1)},\ldots,$$

. . . . . .

и, значит, являются целыми рациональными функциями от R степени $n-1$. В силу этого число форм, сравнимых с нулем по данному модулю, есть для достаточно больших значений R значение некоторой целой рациональной функции от R, коэффициенты которой являются рациональными числами, зависящими только от модуля $(F_1,F_2,\ldots,F_m)$. Вычитая это число из числа членов общей формы порядка R, мы получаем число независимых условий, которым должны удовлетворять коэффициенты формы порядка R, чтобы она была сравнима с нулем по модулю $(F_1,F_2,\ldots,F_m)$. Значит, определенное таким способом число является для достаточно больших значений R целой рациональной функцией от R с рациональными коэффициентами. Мы обозначим эту целую рациональную функцию через $\chi(R)$ и назовем ее *характеристической функцией* модуля $(F_1,F_2,\ldots,F_m)$ [22]. *Данное доказательство существования характеристической функции основывается на конечности цепи производных систем уравнений и, следовательно, существенно зависит от теоремы* III *предыдущего раздела* [23].

Что касается границы, начиная с которой характеристическая функция $\chi(R)$ дает число условий, о которых идет речь, то из предыдущих рассмотрений сразу видно, как она может быть вычислена по порядкам форм, встречающихся в качестве решений в цепи производных систем для (36) [24].

Наш результат может быть также выражен и следующим образом. Если мы обозначим через c_R число линейно независимых условий, которым должна удовлетворять форма порядка R, чтобы быть сравнимой с нулем по модулю $(F_1, F_2, \ldots, F_m)$, то бесконечная последовательность целых чисел c_1, c_2, $c_3, \ldots$ является с некоторого места арифметической последовательностью порядка, меньшего n. В самом деле, для достаточно большого R

$$c_R = \chi(R) \text{ [25]}.$$

Это служит основой для следующего разбиения модулей: мы относим два модуля к одному *классу*, если они порождают одну и ту же последовательность c_1, c_2, $c_3, \ldots$ [26].

Чтобы определить общий вид характеристической функции, мы положим

$$\chi(R) = (a_0 + a_1 R + a_2 R^2 + \ldots + a_d R^d)/a,$$

где a_0, a_1, $a_2, \ldots, a_d$ — целые положительные или отрицательные числа, а степень d меньше числа n переменных в заданных формах. В соответствии с интерпретацией характеристической функции $\chi(R)$ принимает целые значения для всех целых значений аргумента R, превосходящих некоторую границу; отсюда следует, что $\chi(R)$ принимает целые значения для всех целых значений аргумента. В самом деле, если бы нашлось целое число r, для которого выражение

$$a_0 + a_1 r + a_2 r^2 + \ldots + a_d r^d$$

не делилось бы на знаменатель a, то выражение

$$a_0 + a_1(r + ka) + a_2(r + ka)^2 + \ldots + a_d(r + ka)^d$$

не делилось бы на a ни для каких целых значений k и, значит, $\chi(r + ka)$ было бы дробью. Но это приводит к противоречию, если мы возьмем k таким, чтобы $r + ka$ превышало границу, выше которой $\chi(R)$ обязательно является целым числом.

Положим теперь

$$\chi(R) = \chi_0 + \chi_1 \binom{R}{1} + \chi_2 \binom{R}{2} + \ldots + \chi_d \binom{R}{d},$$

где, как обычно,

$$\binom{R}{s} = \frac{R(R-1)\ldots(R-s+1)}{1 \cdot 2 \cdot \ldots \cdot s} \quad (s = 1, 2, \ldots, d) \text{ [27]}.$$

Поскольку, согласно предыдущему, $\chi(R)$ — целое число при $R = 0$, то χ_0 — целое число; аналогично, последовательно полагая $R = 1, 2, \ldots, d$, мы видим, что другие коэффициенты χ_1, $\chi_2, \ldots, \chi_d$ также являются целыми числами. А поскольку биномиальные коэффициенты $\binom{R}{s}$ всегда являются целыми числами для всех значений R, предыдущее выражение с целыми χ_0, $\chi_1, \ldots, \chi_d$ является наиболее общей целой рациональной функцией, обладающей тем

свойством, что она принимает целые значения для всех целых значений аргумента.

Объединим все полученные в этом разделе результаты в виде теоремы.

Теорема IV. *Число линейно независимых условий, которым должны удовлетворять коэффициенты формы порядка R, чтобы она была сравнима с нулем по заданному модулю $(F_1, F_2, \ldots, F_m)$, дается при R, большем некоторой определенной границы, формулой*

$$\chi(R) = \chi_0 + \chi_1 \binom{R}{1} + \chi_2 \binom{R}{2} + \ldots + \chi_d \binom{R}{d},$$

где $\chi_0, \chi_1, \ldots, \chi_d$ — некоторые целочисленные характеристики модуля $(F_1, F_2, \ldots, F_m)$. Целая функция $\chi(R)$ степени d относительно R, называется характеристической функцией модуля $(F_1, F_2, \ldots, F_m)$.

Предыдущие рассмотрения доставляют также и общий метод определения характеристической функции. Чтобы проиллюстрировать этот метод, мы рассмотрим сначала модуль (F_1, F_2, F_3), где F_1, F_2, F_3 — те же самые три квадратичные формы от четырех переменных x_1, x_2, x_3, x_4, которые рассматривались в разд. I и III. Число коэффициентов в кватернарной форме порядка R равно

$$\tfrac{1}{6}(R+1)(R+2)(R+3).$$

Из этого числа следует вычесть число линейно независимых форм F порядка R, которые могут быть представлены формулой

$$F = A_1F_1 + A_2F_2 + A_3F_3;$$

это последнее число мы получим, вычитая из общего количества членов в трех формах A_1, A_2, A_3 порядка $R-2$, равного $3 \cdot \frac{1}{6}(R-1)R(R+1)$, число линейно независимых систем форм X_1, X_2, X_3 порядка $R-2$, удовлетворяющих уравнению

$$F_1X_1 + F_2X_2 + F_3X_3 = 0.$$

Как было показано в конце разд. I, общее решение этого уравнения может быть записано в виде

$$X_1 = A_1^{(1)}x_3 + A_2^{(1)}x_4,$$
$$X_2 = A_1^{(1)}x_2 + A_2^{(1)}x_3,$$
$$X_3 = A_1^{(1)}x_1 + A_2^{(1)}x_2.$$

Значит, последнее нужное нам число равно общему числу членов в двух формах $A_1^{(1)}$, $A_2^{(1)}$ порядка $R-3$, т. е. $2 \cdot \frac{1}{6}(R-2)(R-1)R$. Поскольку, согласно полученным в разд. III результатам, производная система

$$x_3X_1^{(1)} + x_4X_2^{(1)} = 0,$$
$$x_2X_1^{(1)} + x_3X_2^{(1)} = 0,$$
$$x_1X_1^{(1)} + x_2X_2^{(1)} = 0$$

не имеет решений, эти $2 \cdot \frac{1}{6}(R-2)(R-1)R$ решений линейно независимы, а число, которое мы искали с самого начала, равно

$$\chi(R) = \tfrac{1}{6}(R+1)(R+2)(R+3) - 3 \cdot \tfrac{1}{6}(R-1)R(R+1) + \\ + 2 \cdot \tfrac{1}{6}(R-2)(R-1)R = 1 + 3R.$$

Этот результат соответствует тому факту, что поверхность степени R должна удовлетворять в точности $1+3R$ условиям, чтобы содержать заданную пространственную кривую порядка 3.

Чтобы вычислить характеристическую функцию модуля $(F_1, F_2, \ldots, F_6)$, где $F_1, F_2, \ldots, F_6$ — квадратичные формы от пяти переменных $x_1, x_2, \ldots, x_5$, рассмотренные в разд. I, воспользуемся цепью производных систем этого модуля, найденной в разд. III. Рассматривая порядки форм, являющихся коэффициентами этих систем уравнений, мы получаем следующее выражение для характеристической функции модуля $(F_1, F_2, \ldots, F_6)$:

$$\chi(R) = \frac{(R+1)(R+2)(R+3)(R+4)}{1\cdot 2\cdot 3\cdot 4} - \\ -6\frac{(R-1)R(R+1)(R+2)}{1\cdot 2\cdot 3\cdot 4} + 8\frac{(R-2)(R-1)R(R+1)}{1\cdot 2\cdot 3\cdot 4} - \\ - 3\frac{(R-3)(R-2)(R-1)R}{1\cdot 2\cdot 3\cdot 4} = 1 + 4R.$$

Поступая аналогично с цепью производных систем модуля $(x_1, x_2, \ldots, x_n)$, которая была указана выше, приходим к следующему виду характеристической функции этого модуля:

$$\chi(R) = \frac{(R+1)(R+2)\ldots(R+n-1)}{1\cdot 2\cdot \ldots \cdot (n-1)} - \\ - \binom{n}{1}\frac{R(R+1)\ldots(R+n-2)}{1\cdot 2\cdot \ldots \cdot (n-1)} + \binom{n}{2}\frac{(R-1)R\ldots(R+n-3)}{1\cdot 2\cdot \ldots \cdot (n-1)} - \ldots \\ \ldots + (-1)^n \frac{(R-n+1)(R-n+2)\ldots(R-1)}{1\cdot 2\cdot \ldots \cdot (n-1)} = 0.$$

И действительно, каждая форма сравнима с нулем по модулю $(x_1, x_2, \ldots, x_n)$.

Если F — произвольная тернарная форма порядка r, то характеристическая функция определенного ею модуля (F) имеет вид

$$\chi(R) = \frac{(R+1)(R+2)}{1\cdot 2} - \frac{(R-r+1)(R-r+2)}{1\cdot 2} = -\tfrac{1}{2}(r-1)(r-2) + 1 + rR.$$

Если F_1, F_2 — две произвольные тернарные формы порядков r_1, r_2, не имеющие общего множителя, то для модуля (F_1, F_2)

$$\chi(R) = \frac{(R+1)(R+2)}{1\cdot 2} - \frac{(R-r_1+1)(R-r_1+2)}{1\cdot 2} - \\ - \frac{(R-r_2+1)(R-r_2+2)}{1\cdot 2} + \frac{(R-r_1-r_2+1)(R-r_1-r_2+2)}{1\cdot 2} = r_1 r_2.$$

Наконец, если F_1, F_2 — две кватернарные формы порядков r_1, r_2 без общего множителя, то для модуля (F_1, F_2)

$$\chi(R) = \frac{(R+1)(R+2)(R+3)}{1\cdot 2\cdot 3} - \frac{(R-r_1+1)(R-r_1+2)(R-r_1+3)}{1\cdot 2\cdot 3} - \frac{(R-r_2+1)(R-r_2+2)(R-r_2+3)}{1\cdot 2\cdot 3} + \frac{(R-r_1-r_2+1)(R-r_1-r_2+2)(R-r_1-r_2+3)}{1\cdot 2\cdot 3} = 2r_1r_2 - \tfrac{1}{2}r_1r_2(r_1+r_2) + r_1r_2R.$$

Установленные в этом и предыдущих разделах общие принципы позволяют нам исчерпывающим образом разобрать частный случай произвольного модуля бинарных форм. Чтобы убедиться в этом, рассмотрим модуль $(F_1, F_2, \ldots, F_m)$, где $F_1, F_2, \ldots, F_m$ — бинарные формы. Предположим для простоты, что эти формы не имеют общего множителя и все имеют один и тот же порядок r. Ввиду первого предположения характеристическая функция модуля $(F_1, F_2, \ldots, F_m)$ равна нулю. В самом деле, при этом предположении каждая бинарная форма F достаточно высокого порядка R может быть выражена в виде

$$F = A_1F_1 + A_2F_2 + \ldots + A_mF_m,$$

где все $A_1, A_2, \ldots, A_m$ — формы порядка $R - r$. Доказательство было кратко намечено в начале разд. I. С другой стороны, вычислим ту же характеристическую функцию, пользуясь общим методом, развитым выше, т. е. рассматривая полную систему решений уравнения

$$F_1X_1 + F_2X_2 + \ldots + F_mX_m = 0,$$

в которой ни одно из решений не может быть получено из остальных в виде линейной комбинации. Пусть

$$X_1 = G_{1s}, \quad X_2 = G_{2s}, \quad \ldots, \quad X_m = G_{ms} \qquad (s = 1, 2, \ldots, m^{(1)})$$

— эта система решений, и пусть r_s — общий порядок форм $G_{1s}, G_{2s}, \ldots, G_{ms}$. Между этими решениями нет соотношений. Действительно, производная система

$$G_{t1}X_1^{(1)} + G_{t2}X_2^{(1)} + \ldots + G_{tm^{(1)}}X_{m^{(1)}}^{(1)} = 0 \qquad (t = 1, 2, \ldots, m)$$

указанного выше уравнения не имеет решений ввиду теоремы III предыдущего раздела. Значит, характеристическая функция, о которой идет речь, имеет вид

$$\chi(R) = R + 1 - m(R - r + 1) + \sum_s (R - r - r_s + 1) = R(m^{(1)} - m + 1) - (r-1)(m^{(1)} - m + 1) + r - \sum_s r_s,$$

где сумма берется по всем $s = 1, 2, \ldots, m^{(1)}$. Если приравнять нулю как коэффициент при R, так и член, не зависящий от R, стоящие в правой

части, то мы получим

$$m^{(1)} = m - 1,$$

$$r = r_1 + r_2 + \ldots + r_{m-1},$$

откуда вытекает следующее утверждение:

Если m бинарных форм $F_1, F_2, \ldots, F_m$ порядка r не имеют общего множителя, то полная система решений уравнения

$$F_1X_1 + F_2X_2 + \ldots + F_mX_m = 0$$

всегда состоит из $m-1$ решений

$$X_1 = G_{1s}, \quad X_2 = G_{2s}, \quad \ldots, \quad X_m = G_{ms} \qquad (s = 1, 2, \ldots, m-1),$$

между которыми нет соотношений, и сумма порядков этих $m-1$ решений равна r [6].

Из $m-1$ уравнений

$$G_{1s}F_1 + G_{2s}F_2 + \ldots + G_{ms}F_m = 0 \qquad (s = 1, 2, \ldots, m-1)$$

следует, что

$$F_1 : F_2 : \ldots : F_m = D_1 : D_2 : \ldots : D_m,$$

где $D_1, D_2, \ldots, D_m$ обозначают соответствующие $(m-1)$-строчные определители матрицы

$$\begin{pmatrix} G_{11} & G_{21} & G_{31} & \ldots & G_{m1} \\ G_{12} & G_{22} & G_{32} & \ldots & G_{m2} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ G_{1,m-1} & G_{2,m-1} & G_{3,m-1} & \ldots & G_{m,m-1} \end{pmatrix}.$$

Поскольку, согласно доказанному только что утверждению, порядки этих определителей по переменным x_1, x_2 равны r, данные формы равны с точностью до несущественного числового множителя соответствующим определителям этой матрицы, и поэтому мы положим

$$F_1 = D_1, \quad F_2 = D_2, \quad \ldots, \quad F_m = D_m.$$

Наоборот, если даны $m-1$ решений

$$X_1 = G_{1s}, \quad X_2 = G_{2s}, \quad \ldots, \quad X_m = G_{ms} \qquad (s = 1, 2, \ldots, m-1),$$

то эти формулы позволяют нам определить формы $F_1, F_2, \ldots, F_m$. В то же время мы видим, что порядки $r_1, r_2, \ldots, r_{m-1}$ не связаны никакими ограничениями, кроме того, что их сумма равна r.

Легко видеть, что числа $r_1, r_2, \ldots, r_{m-1}$ полностью определяют описанную выше последовательность целых чисел $c_1, c_2, c_3, \ldots$ для данного модуля $(F_1, F_2, \ldots, F_m)$, а значит, и класс, к которому принадлежит этот модуль. Для всех значений R, бóльших $2r-1$, мы имеем $c_R = \chi(R) = 0$. Наконец, отметим, что нетрудно снять оба сделанных выше предположения о том, что все формы данного модуля имеют одинаковый порядок и не имеют общего делителя, соответствующим образом изменив результаты.

Эти рассмотрения существенно относятся к теории бинарных модулей. Следующая задача — соответствующее исследование модулей, содержащих

---

[6] Это утверждение уже высказывалось в качестве предположения Ф. Мейером, который рассматривал его как гипотезу в своих исследованиях приводимых функций, см. *Meyer F.* — Math. Ann., Bd. 30, S. 38.

формы с тремя и большим числом переменных. Здесь мы, однако, лишь отметим, что для такого развития теории необходимо прежде всего обобщение фундаментальной теоремы Нётера[7] на формы от многих переменных, равно как и более глубокое исследование всех возможных исключительных случаев.

Цитированные в разд. I исследования систем модулей содержат обсуждение ряда других фундаментальных понятий теории модулей. После тривиальных модификаций соответствующие определения приложимы также и к модулям однородных форм, исследованным здесь. Рассмотрим, в частности, понятия «*наименьшего содержащего*» и «*наибольшего общего*» модулей[8]. Если заданы любые два однородных модуля $(F_1, F_2, \ldots, F_m)$ и $(H_1, H_2, \ldots, H_h)$, то рассматривается сначала полная система решений уравнения

$$F_1X_1 + F_2X_2 + \ldots + F_mX_m = H_1Y_1 + H_2Y_2 + \ldots + H_hY_h,$$

скажем

$$\left.\begin{aligned} X_1 = F_{1s},\ X_2 = F_{2s},\ \ldots,\ X_m = F_{ms} \\ Y_1 = H_{1s},\ Y_2 = H_{2s},\ \ldots,\ Y_h = H_{hs} \end{aligned}\right\} \qquad (s = 1, 2, \ldots, k).$$

Затем строятся формы

$$K_s = F_1F_{1s} + F_2F_{2s} + \ldots + F_mF_{ms} = H_1H_{1s} + H_2H_{2s} + \ldots + H_hH_{hs}$$
$$(s = 1, 2, \ldots, k).$$

Модуль $(K_1, K_2, \ldots, K_k)$ и есть наименьший содержащий модуль. С другой стороны, располагая формы двух данных модулей рядом друг с другом, получаем наибольший общий модуль

$$(F_1, F_2, \ldots, F_m, H_1, H_2, \ldots, H_h) = (G_1, G_2, \ldots, G_g)\ [28].$$

Имеется очень простое соотношение между характеристическими функциями χ_F, χ_H двух данных модулей и характеристическими функциями χ_K, χ_G их наименьшего содержащего и наибольшего общего модулей. Чтобы получить это соотношение, построим сначала систему S_F линейно независимых форм порядка R, такую, что каждая из этих форм сравнима с нулем по модулю $(F_1, F_2, \ldots, F_m)$ и любая другая форма порядка R получается из них в виде линейной комбинации. Если R больше некоторой границы, то число форм в этой системе S_F равно $\varphi(R) - \chi_F(R)$, где $\varphi(R)$ — число членов в общей форме порядка R. Построим, далее, полную систему S_K линейно независимых форм порядка R, которые сравнимы с нулем по обоим модулям $(F_1, F_2, \ldots, F_m)$ и $(H_1, H_2, \ldots, H_h)$. Все эти формы являются линейными комбинациями форм системы S_F. Для достаточно большого R число форм в системе S_K равно $\varphi(R) - \chi_K(R)$. И, наконец, построим систему S форм, которая дополняет формы системы S_K до полной системы S_H линейно независимых форм, сравнимых с нулем по модулю $(H_1, H_2, \ldots, H_h)$. Число форм

---

[7] См.: *Noether M.* — Math. Ann., Bd. 6, S. 351; Bd. 30, S. 410, а также: *Voss A.* — Math. Ann., Bd. 27, S. 527, и *Stickelberger L.* — Math. Ann., Bd. 30, S. 401.

[8] См. определения у Л. Кронекера (*Kroneker L.* — Crelles J., Bd. 92, S. 78), а также у Р. Дедекинда и Г. Вебера (*Dedekind R., Weber .* — Crelles J., Bd. 92, S. 197).

в системе S_H равно $\varphi(R) - \chi_H(R)$; поскольку формы в системах S и S_K вместе дают формы из системы S_H, число форм в системе S равно

$$\{\varphi(R) - \chi_H(R)\} - \{\varphi(R) - \chi_K(R)\} = \chi_K(R) - \chi_H(R).$$

Из указанной конструкции следует, что формы в обеих системах S_F и S взаимно линейно независимы и что все формы, являющиеся линейными комбинациями форм систем S_F и S_H, могут быть построены как линейные комбинации форм из обеих систем S_F и S. Поэтому, взятые вместе, формы из обеих систем S_F и S образуют полную систему S_G линейно независимых форм порядка R, сравнимых с нулем по модулю $(G_1, G_2, \ldots, G_g)$. Из предыдущих рассмотрений следует, что общее число форм в системах S_F и S равно $\varphi(R) - \chi_F(R) + \chi_K(R) - \chi_H(R)$, а общее число форм в системе S_G равно $\varphi(R) - \chi_G(R)$. Значит, эти два числа совпадают, т. е.

$$\varphi(R) - \chi_F(R) + \chi_K(R) - \chi_H(R) = \varphi(R) - \chi_G(R)$$

или

$$\chi_F + \chi_H = \chi_K + \chi_G \text{ [29]}.$$

Мы сформулируем этот результат в виде следующего предложения:

Сумма характеристических функций двух произвольных модулей равна сумме характеристических функций их наименьшего содержащего и наибольшего общего модулей.

В заключение этого раздела мы кратко укажем, как полученные здесь общие результаты могут быть применены в теории алгебраических многообразий (algebraischen Gebilde).

Пусть сначала дана кривая или система кривых и точек в трехмерном пространстве [30]. Согласно утверждению, доказанному в разд. I, имеется конечное число таких проходящих через это многообразие поверхностей

$$F_1 = 0, \quad F_2 = 0, \quad \ldots, \quad F_m = 0,$$

что всякая другая поверхность, содержащая это многообразие, может быть задана уравнением

$$A_1F_1 + A_2F_2 + \ldots + A_mF_m = 0.$$

Вследствие этого всякому алгебраическому многообразию соответствует модуль $(F_1, F_2, \ldots, F_m)$ и, значит, определенная характеристическая функция $\chi(R)$. Эта функция показывает нам, скольким линейно независимым условиям должна удовлетворять поверхность степени R, если R достаточно велико, чтобы она содержала данное многообразие [31]. Таким образом, характеристическая функция пространственной кривой порядка r и рода p без двойных точек имеет следующий вид[9]:

$$\chi(R) = -p + 1 + rR.$$

Например, можно взять пространственную кубическую кривую, характеристическая функция которой имеет вид $1+3R$, согласно уже проделанным в этом разделе вычислениям.

---

[9] См.: *Noether M.* — Crelles J., Bd. 93, S. 295.

Для кривой, являющейся пересечением двух поверхностей степеней r_1 и r_2, с помощью предыдущих вычислений получаем характеристическую функцию [32]

$$\chi(R) = 2r_1r_2 - \tfrac{1}{2}r_1r_2(r_1 + r_2) + r_1r_2R.$$

Чтобы проиллюстрировать значение установленного раньше общего утверждения о характеристических функциях в связи с этими последними рассмотрениями, применим его к решению одной задачи из теории пространственных кривых. Допустим, что две пространственные кривые без двойных точек порядков ϱ_1, ϱ_2 и родов p_1, p_2 соответственно составляют вместе полное пересечение поверхностей $K_1 = 0$, $K_2 = 0$ степеней r_1, r_2. Пусть $(F_1, F_2, \ldots, F_m)$ и $(H_1, H_2, \ldots, H_h)$ — модули, связанные с этими пространственными кривыми. Тогда наименьшим содержащим модулем этих двух модулей является (K_1, K_2), а наибольшим общим модулем — модуль $(F_1, F_2, \ldots, F_m, H_1, H_2, \ldots, H_h)$, представленный геометрически общими точками этих двух пространственных кривых. Пусть ϱ — число этих точек. Участвующие в рассмотрении характеристические функции имеют вид

$$\chi_F(R) = -p_1 + 1 + \varrho_1 R,$$
$$\chi_H(R) = -p_2 + 1 + \varrho_2 R,$$
$$\chi_K(R) = 2r_1r_2 - \tfrac{1}{2}r_1r_2(r_1 + r_2) + r_1r_2R,$$
$$\chi_G(R) = \varrho,$$

и, используя наше утверждение, что

$$\chi_F + \chi_H = \chi_K + \chi_G,$$

получаем, что число общих точек этих двух кривых равно

$$\varrho = -2r_1r_2 + \tfrac{1}{2}r_1r_2(r_1 + r_2) - p_1 - p_2 + 2.$$

Что касается обобщения этих рассмотрений на пространства произвольно большой размерности, то здесь следует отметить следующие результаты. Пусть задано алгебраическое многообразие в пространстве сколь угодно большой размерности, и пусть модуль, принадлежащий этому алгебраическому многообразию, имеет характеристическую функцию

$$\chi(R) = \chi_0 + \chi_1\binom{R}{1} + \chi_2\binom{R}{2} + \ldots + \chi_d\binom{R}{d};$$

тогда степень d этой характеристической функции дает размерность многообразия, а коэффициент χ_d дает его степень, в то время как остальные коэффициенты $\chi_0, \chi_1, \ldots, \chi_{d-1}$ тесно связаны с родовыми числами (Geschlechtszahlen), определенными и изученными М. Нётером[10]. Общее доказательство этого основывается на переходе от $n-1$ к n переменным [33]. Как можно убедиться, указанное утверждение справедливо в случае кривых в трехмерном пространстве.

В какой степени модуль определяется системой значений, обращающих в нуль одновременно все формы из этого модуля [34], — это вопрос, удовлетворительный и общий ответ на который может быть получен только

---

[10] См. Math. Ann.. Bd. 2. S. 293: Bd. 8. S. 495.

после систематического исследования, охватывающего все возможные исключительные случаи фундаментальной теоремы Нётера для произвольной размерности.

Отметим, наконец, теорию так называемых ограниченных систем уравнений (beschränkten Gleichungssysteme), развитую А. Кэли, Г. Сальмоном, С. Робертсом и А. Бриллем[11], поскольку наше понятие характеристической функции доставляет как плодотворные вопросы, так и единую точку зрения для этой ветви алгебры. Например, если задана пространственная кривая и мы рассматриваем три содержащие ее поверхности $F_1 = 0$, $F_2 = 0$, $F_3 = 0$ соответственно степеней r_1, r_2, r_3, то число точек пересечения этих трех поверхностей, не лежащих на данной пространственной кривой, равно характеристической функции соответствующего модуля минус характеристическая функция этой пространственной кривой. Это соображение приводит в действительности к допускающему обобщение доказательству известного утверждения о том, что число точек пересечения этих трех поверхностей, поглощенных общей пространственной кривой, равно $\varrho(r_1 + r_2 + r_3) - \alpha$, где ϱ — порядок пространственной кривой, а α — другая константа, связанная с этой пространственной кривой, — так называемый ранг.

Этих указаний достаточно, чтобы показать, что развитая в этом разделе теория характеристической функции приводит к единой и ясной трактовке чисел, относящихся к алгебраическому многообразию (размерность, степень, род, ранг и т. д.). Дальнейшей задачей теории является теперь фактическое осуществление тех алгебраических процессов, на которых основываются определения этих чисел [35].

V. Теория алгебраических инвариантов

В особой степени развитые в разд. I принципы демонстрируют свою силу в той части алгебры, которая имеет дело с формами, инвариантными относительно линейных подстановок. П. Гордан[12] как известно, впервые показал, что все инварианты системы бинарных базисных форм (Grundformen) от набора переменных x_1, x_2 являются целыми рациональными функциями от конечного их числа. Использованные для этого методы недостаточны, однако, для доказательства соответствующего утверждения для форм от многих переменных или в случае, когда базисные формы содержат несколько наборов переменных, каждый из которых подвергается различным преобразованиям. Мы разработаем далее средства, необходимые для решения этих более общих проблем [36].

Для того, чтобы сделать существенные моменты доказательства как можно более ясными, мы рассмотрим сначала простой случай одной бинарной базисной формы f с единственным набором переменных x_1, x_2 [37].

---

[11] См.: *Salmon G.* Algebra der linearen Transformationen. — 1887, лекции 22, 23 и библиография.

[12] См.: *Gordan P.* Vorlesungen über Invariantentheorie, Bd. II. 1885, — S. 231. Другие доказательства были даны Ф. Мертенсом (*Mertens F.* — Crelles J., Bd. 100, S. 223) и автором (Math. Ann., Bd. 33, S. 223).

В соответствии с доказанным в разд. I утверждением, из любой заданной системы форм можно выбрать такое конечное число форм, что всякая другая форма из этой системы может быть получена из выбранных форм в виде их линейной комбинации. Мы рассмотрим, в частности, систему всех инвариантов бинарной базисной формы f; согласно упомянутому утверждению, должно найтись конечное число m таких инвариантов $i_1, i_2, \ldots, i_m$, что всякий другой инвариант i базисной формы f может быть выражен в виде

$$i = A_1 i_1 + A_2 i_2 + \ldots + A_m i_m, \tag{38}$$

где $A_1, A_2, \ldots, A_m$ — целые однородные функции от коэффициентов базисной формы f. Этот результат, очевидно, может быть также непосредственно выведен из теоремы I разд. I. Чтобы вкратце объяснить это, выберем прежде всего произвольный инвариант i_1 из совокупности всех инвариантов базисной формы f; пусть далее i_2 будет инвариантом базисной формы f, не равным произведению $A_1 i_1$, где A_1 — целая однородная функция от коэффициентов базисной формы f; пусть затем i_3 будет инвариантом, не представимым в виде $A_1 i_1 + A_2 i_2$, где A_1 и A_2 — снова целые однородные функции от коэффициентов базисной формы f. Подобным же образом пусть i_4 — инвариант базисной формы f, не представимый в виде $A_1 i_1 + A_2 i_2 + A_3 i_3$. Продолжая в этом духе, мы получим последовательность форм $i_1, i_2, i_3, \ldots$, в которой ни одна из форм не может быть получена из предыдущих в виде линейной комбинации. Согласно теореме I разд. I, такая последовательность должна оборваться через конечное число шагов. Если мы обозначим последнюю форму в этой последовательности через i_m, то всякий инвариант заданной базисной формы f будет линейной комбинацией m инвариантов $i_1, i_2, \ldots, i_m$. Полученный таким образом результат служит *первым* шагом в доказательстве конечности полной системы инвариантов.

Второй шаг состоит в том, чтобы установить, что в выражении $A_1 i_1 + A_2 i_2 + \ldots + A_m i_m$ функции $A_1, A_2, \ldots, A_m$ всегда можно, не меняя значения i самого этого выражения, заменить на инварианты $J_1, J_2, \ldots, J_m$. Этот второй шаг можно осуществить особенно просто в случае бинарной базисной формы от одного набора переменных, если воспользоваться следующим утверждением, доказанным в диссертации (Inauguraldissertation) автора[13]:

Всякая однородная и изобарная (т. е. с членами равных весов) функция от коэффициентов бинарной формы

$$a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n,$$

имеющая по коэффициентам $a_0, a_1, \ldots, a_n$ степень r и вес $p = \frac{1}{2}nr$, преобразуется в инвариант этой базисной формы с помощью следующего дифференциального процесса:

$$[\ ] = 1 - \frac{\Delta}{1!}\frac{D}{2!} + \frac{\Delta^2}{2!}\frac{D^2}{3!} - \frac{\Delta^3}{3!}\frac{D^3}{4!} + \ldots = 1 - \frac{D}{1!}\frac{\Delta}{2!} + \frac{D^2}{2!}\frac{\Delta^2}{3!} - \frac{D^3}{3!}\frac{\Delta^3}{4!} + \ldots,$$

[13] См.: Über die invarianten Eigenschaften spezieller binärer Formen, insbesondere der Kugelfunktionen. — Königsberg i. Pr., 1885, а также: Über eine Darstellungsweise der invarianten Gebilde im binären Formengebiete — Math. Ann., Bd. 30, S. 15.

где

$$D = a_0\frac{\partial}{\partial a_1} + 2a_1\frac{\partial}{\partial a_2} + 3a_2\frac{\partial}{\partial a_3} + \ldots,$$

$$\Delta = na_1\frac{\partial}{\partial a_0} + (n-1)a_2\frac{\partial}{\partial a_1} + (n-2)a_3\frac{\partial}{\partial a_2} + \ldots\ [38].$$

Обозначим теперь веса инвариантов i, i_1, $i_2, \ldots, i_m$ соответственно через p, p_1, $p_2, \ldots, p_m$ и, собрав вместе все члены веса $p - p_s$ в выражении A_s, обозначим их через B_s. Поскольку в левой части формулы (38) имеются только члены веса p, то мы можем удалить из правой части этой формулы все члены произведений $A_s i_s$, имеющие больший или меньший, чем p, вес, и таким образом получим для i выражение

$$i = B_1 i_1 + B_2 i_2 + \ldots + B_m i_m, \tag{39}$$

где B_1, B_2, $\ldots, B_m$ — однородные и изобарные функции от коэффициентов базисной формы [39]. Заметим теперь, что результат применения дифференциального процесса D или дифференциального процесса Δ к инварианту является тождественным нулем [40] и что, согласно предыдущему утверждению, однородные и изобарные функции B_s преобразуются дифференциальным процессом [ ] в некоторые инварианты J_s базисной бинарной формы f. Следовательно,

$$[i] = i,$$

$$[B_s i_s] = [B_s]\, i_s = J_s i_s \qquad (s = 1, 2, \ldots, m)$$

и применение процесса [ ] к каждому члену в (39) дает уравнение

$$i = J_1 i_1 + J_2 i_2 + \ldots + J_m i_m.$$

Все инварианты J_1, J_2, $\ldots$, J_m имеют меньшую степень относительно коэффициентов базисной формы, чем инвариант i, и мы поступим теперь с ними точно так же, как и с инвариантом i; в конце концов мы получим выражение инварианта i в виде целой рациональной функции от m инвариантов i_1, $i_2, \ldots, i_m$. Значит, эти последние m инвариантов образуют полную систему инвариантов для данной бинарной базисной формы f.

Второй шаг в этом доказательстве состоял в том, чтобы показать, как в исходном выражении (38) заменить функции A_1, $A_2, \ldots, A_m$ на инварианты. Этот второй шаг не может быть, однако, осуществлен для базисных форм от многих переменных точно так же, как и выше, поскольку пока неизвестно утверждения теории инвариантов форм от многих переменных, соответствующего сформулированному ранее утверждению о бинарных формах [41]. Однако в этом более общем случае тот же результат может быть достигнут с помощью утверждения, совпадающего по существу с одним утверждением, доказанным П. Горданом[14] и Ф. Мертенсом[15], которое для случая тернарных форм формулируется так:

---

[14] *Gordan P.* Vorlesungen über Invariantentheorie, Bd. 2, 1885, § 9; см. также: *Clebsch A.* Über symbolische Darstellung algebraischer Formen. — Crelles J., Bd. 59, S. 1.

[15] *Mertens F.* Über invariante Gebilde ternärer Formen. — Sitzgsber. Akad. Wiss. Wien, Math.-Phys. Kl., Bd. 95.

Пусть дана система тернарных базисных форм $f^{(1)}$, $f^{(2)},\ldots,f^{(k)}$ от переменных x_1, x_2, x_3 ; пусть $f_a^{(1)}$, $f_a^{(2)}$, $\ldots$, $f_a^{(k)}$ — соответственно результаты применения к этой системе форм линейной подстановки

$$\begin{aligned} x_1 &= a_{11}y_1 + a_{12}y_2 + a_{13}y_3, \\ x_2 &= a_{21}y_1 + a_{22}y_2 + a_{23}y_3, \\ x_3 &= a_{31}y_1 + a_{32}y_2 + a_{33}y_3, \end{aligned} \qquad a = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}. \tag{40}$$

Пусть, далее, $F(f_a)$ — целая функция от коэффициентов этих преобразованных форм $f_a^{(1)}$, $f_a^{(2)}$, $\ldots$, $f_a^{(k)}$, однородная отдельно по коэффициентам каждой из форм. Умножим теперь эту функцию $F(f_a)$ на a^q, где a — определитель подстановки, а q — произвольное неотрицательное целое число, и будем применять к произведению $a^qF(f_a)$ дифференциальный процесс

$$\Omega_a = \frac{\partial^3}{\partial a_{11}\partial a_{22}\partial a_{33}} - \frac{\partial^3}{\partial a_{11}\partial a_{23}\partial a_{32}} + \frac{\partial^3}{\partial a_{12}\partial a_{23}\partial a_{31}} - \frac{\partial^3}{\partial a_{12}\partial a_{21}\partial a_{33}} + \frac{\partial^3}{\partial a_{13}\partial a_{21}\partial a_{32}} - \frac{\partial^3}{\partial a_{13}\partial a_{22}\partial a_{31}}$$

последовательно до тех пор, пока не получится выражение, свободное от коэффициентов a_{11}, $a_{12},\ldots,a_{33}$ подстановки. Тогда полученное выражение является инвариантом системы форм $f^{(1)}$, $f^{(2)},\ldots,f^{(k)}$.

Это утверждение немедленно вытекает из того факта, что инварианты не изменяются при линейных преобразованиях. Чтобы убедиться в этом, рассмотрим базисные формы $f^{(1)}$, $f^{(2)},\ldots,f^{(k)}$ в записи, в которой переменные обозначаются через y_1, y_2, y_3, и применим затем к этим переменным линейное преобразование

$$\begin{aligned} y_1 &= b_{11}z_1 + b_{12}z_2 + b_{13}z_3, \\ y_2 &= b_{21}z_1 + b_{22}z_2 + b_{23}z_3, \\ y_3 &= b_{31}z_1 + b_{32}z_2 + b_{33}z_3, \end{aligned} \qquad b = \begin{vmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{vmatrix}. \tag{41}$$

Пусть при этом базисные формы $f^{(1)}$, $f^{(2)},\ldots,f^{(k)}$ перейдут соответственно в $f_b^{(1)}$, $f_b^{(2)},\ldots,f_b^{(k)}$. Наконец, линейные подстановки (40) и (41) дают составную линейную подстановку

$$\begin{aligned} x_1 &= c_{11}z_1 + c_{12}z_2 + c_{13}z_3, \\ x_2 &= c_{21}z_1 + c_{22}z_2 + c_{23}z_3, \\ x_3 &= c_{31}z_1 + c_{32}z_2 + c_{33}z_3, \end{aligned} \qquad c = \begin{vmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{vmatrix} = ab, \tag{42}$$

где c_{11}, $c_{12},\ldots,c_{33}$ — известные билинейные сочетания подстановочных коэффициентов a_{11}, $a_{12},\ldots,a_{33}$ и b_{11}, $b_{12},\ldots,b_{33}$. Пусть базисные формы $f^{(1)}$, $f^{(2)},\ldots,f^{(k)}$ преобразуются линейной подстановкой (42) в $f_c^{(1)}$, $f_c^{(2)},\ldots,f_c^{(k)}$.

Подстановка (41) относится к дифференциальному процессу

$$\Omega_b = \frac{\partial^3}{\partial b_{11}\partial b_{22}\partial b_{33}} - \frac{\partial^3}{\partial b_{11}\partial b_{23}\partial b_{32}} + \frac{\partial^3}{\partial b_{12}\partial b_{23}\partial b_{31}} - \\ - \frac{\partial^3}{\partial b_{12}\partial b_{21}\partial b_{33}} + \frac{\partial^3}{\partial b_{13}\partial b_{21}\partial b_{32}} - \frac{\partial^3}{\partial b_{13}\partial b_{22}\partial b_{31}},$$

а составная подстановка (42) — к дифференциальному процессу

$$\Omega_c = \frac{\partial^3}{\partial c_{11}\partial c_{22}\partial c_{33}} - \frac{\partial^3}{\partial c_{11}\partial c_{23}\partial c_{32}} + \frac{\partial^3}{\partial c_{12}\partial c_{23}\partial c_{31}} - \\ - \frac{\partial^3}{\partial c_{12}\partial c_{21}\partial c_{33}} + \frac{\partial^3}{\partial c_{13}\partial c_{21}\partial c_{32}} - \frac{\partial^3}{\partial c_{13}\partial c_{22}\partial c_{31}}.$$

Пусть p обозначает число раз, которое нужно применить Ω_a, чтобы избавиться в выражении $a^q F(f_a)$ от подстановочных коэффициентов a_{11}, $a_{12}, \ldots, a_{33}$. Тогда наша задача состоит в том, чтобы показать, что выражение

$$J(f) = \Omega_a^p\{a^q F(f_a)\}$$

является инвариантом базисных форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$. Поскольку выражение справа должно быть свободно от подстановочных коэффициентов a_{11}, $a_{12}, \ldots, a_{33}$, то

$$J(f) = \Omega_b^p\{b^q F(f_b)\}.$$

Мы заменим в этой формуле коэффициенты форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ на соответствующие коэффициенты преобразованных форм $f_a^{(1)}, f_a^{(2)}, \ldots, f_a^{(k)}$. Тогда коэффициенты форм $f_b^{(1)}, f_b^{(2)}, \ldots, f_b^{(k)}$ перейдут в коэффициенты форм $f_c^{(1)}, f_c^{(2)}, \ldots, f_c^{(k)}$ и мы получим

$$J(f_a) = \Omega_b^p\{b^q F(f_c)\},$$

или [42]

$$a^q J(f_a) = \Omega_b^p\{c^q F(f_c)\}. \tag{43}$$

Выражение $c^q F(f_c)$ зависит от коэффициентов базисных форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ и от подстановочных коэффициентов $a_{11}, a_{12}, \ldots, a_{33}$, $b_{11}, b_{12}, \ldots, b_{33}$, хотя и содержит эти подстановочные коэффициенты только в билинейных сочетаниях $c_{11}, c_{12}, \ldots, c_{33}$. Как легко следует из теоремы об умножении определителей, для любой функции G от этих билинейных сочетаний c_{11}, $c_{12}, \ldots, c_{33}$

$$\Omega_b G = a\Omega_c G,$$

и применение этого p раз дает

$$\Omega_b^p\{c^q F(f_c)\} = a^p \Omega_c^p\{c^q F(f_c)\}. \tag{44}$$

С другой стороны,

$$J(f) = \Omega_c^p\{c^q F(f_c)\},$$

и из (43) и (44) следует, что

$$J(f_a) = a^{p-q} J(f).$$

Эта формула показывает, что $J(f)$ является инвариантом.

Доказанное утверждение позволяет нам построить сколь угодно много инвариантов данной системы форм. Чтобы показать, что с помощью этого процесса могут быть найдены все инварианты, рассмотрим выражение $\Omega_a^p a^p$. Дифференциальный символ Ω_a возникает из определителя a при замене в каждом члене $\pm a_{11'} a_{22'} a_{33'}$ произведения $a_{11'} a_{22'} a_{33'}$ на дифференциальное частное

$$\frac{\partial^3}{\partial a_{11'} \partial a_{22'} \partial a_{33'}},$$

где $1'$, $2'$, $3'$ обозначают числа 1, 2, 3, расположенные в каком-либо порядке. Аналогично мы получаем из a^p дифференциальный символ Ω_a^p, заменяя $a_{11}^{p_{11}} a_{12}^{p_{12}} \dots a_{33}^{p_{33}}$ в разложении a^p на дифференциальное частное

$$\frac{\partial^{3p}}{\partial a_{11}^{p_{11}} \partial a_{12}^{p_{12}} \dots \partial a_{33}^{p_{33}}},$$

где $p_{11}, p_{12} \dots, p_{33}$ обозначают некоторые показатели, сумма которых равна $3p$. Отсюда, в частности, следует, что знак члена $a_{11}^{p_{11}} a_{12}^{p_{12}} \dots a_{33}^{p_{33}}$ в a^p такой же, как и знак члена

$$\frac{\partial^{3p}}{\partial a_{11}^{p_{11}} \partial a_{12}^{p_{12}} \dots \partial a_{33}^{p_{33}}}$$

в Ω_a^p. Поэтому применение Ω_a^p к a^p дает сумму строго положительных чисел [43], т. е. $\Omega_a^p a^p$ — *ненулевое* число[16]; мы обозначим его через N_p.

Пусть теперь $J(f)$ — произвольный заданный инвариант, умножающийся при преобразовании на p-ю степень определителя подстановки. Соотношение [44]

$$\Omega_a^p \left\{ \frac{1}{N_p} J(f_a) \right\} = \frac{1}{N_p} J(f) \Omega_a^p a^p = J(f)$$

показывает тогда, что инвариант $J(f)$ получается указанным процессом, откуда и следует справедливость сделанного выше утверждения.

Эти рассмотрения являются основой доказательства конечности полной системы инвариантов тернарных форм, которое мы хотим получить. *Первый* шаг, ведущий к этому доказательству, — тот же самый, что и раньше в случае бинарных форм: мы снова рассматриваем m инвариантов $i_1, i_2, \dots, i_m$ совокупности базисных форм $f^{(1)}, f^{(2)}, \dots, f^{(k)}$, обладающих тем свойством, что всякий другой инвариант i этих базисных форм может быть выражен в виде

$$i = A_1 i_1 + A_2 i_2 + \dots + A_m i_m, \tag{45}$$

где $A_1, A_2, \dots, A_m$ — целые однородные функции от коэффициентов базисных форм.

Второй шаг состоит в том, чтобы показать, что, не меняя значения i выражения $A_1 i_1 + A_2 i_2 + \dots + A_m i_m$, всегда можно заменить функции $A_1, A_2, \dots, A_m$ на инварианты. Заметим сначала, что по определению инвариант однороден по коэффициентам каждой из базисных форм. Пусть степени

---

[16] См.: *Clebsch A.*, loc. cit., S. 12, где этот последний факт доказан по существу тем же способом.

инвариантов i, i_1, $i_2, \ldots, i_m$ по коэффициентам первой базисной формы $f^{(1)}$ равны соответственно r, r_1, $r_2, \ldots, r_m$. Поскольку теперь левая часть формулы (45) содержит только члены степени r по коэффициентам $f^{(1)}$, то из правой части этой формулы можно убрать все члены функций A_s, степени которых по коэффициентам формы $f^{(1)}$ меньше или больше, чем $r - r_s$. Приравнивая аналогичным образом степени по коэффициентам других базисных форм, мы придем в итоге к равенству

$$i = B_1 i_1 + B_2 i_2 + \ldots + B_m i_m,$$

где B_1, $B_2, \ldots, B_m$ — функции, однородные по коэффициентам каждой из базисных форм в отдельности. Заменим в этом равенстве коэффициенты базисных форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ на соответствующие коэффициенты преобразованных форм $f_a^{(1)}, f_a^{(2)}, \ldots, f_a^{(k)}$ и воспользуемся инвариантностью i, i_1, $i_2, \ldots, i_m$. Мы получим тогда, что

$$a^p i = a^{p_1} B_1(f_a) i_1 + a^{p_2} B_2(f_a) i_2 + \ldots + a^{p_m} B_m(f_a) i_m,$$

где p, p_s — веса инвариантов i, i_s, а $B_s(f_a)$ — соответствующие функции от коэффициентов преобразованных базисных форм $f_a^{(1)}, f_a^{(2)}, \ldots, f_a^{(k)}$. Применяя p раз к этому соотношению дифференциальный символ Ω_a, получим

$$\Omega_a^p\{a^p\} \cdot i = \Omega_a^p\{a^{p_1} B_1(f_a)\} \cdot i_1 + \Omega_a^p\{a^{p_2} B_2(f_a)\} \cdot i_2 + \ldots$$
$$\ldots + \Omega_a^p\{a^{p_m} B_m(f_a)\} \cdot i_m.$$

Разделив обе части на ненулевое число $N_p = \Omega_a^p\{a^p\}$, мы приходим к равенству

$$i = J_1 i_1 + J_1 i_1 + \ldots + J_m i_m,$$

где, согласно доказанному выше утверждению, выражения

$$J_s = \frac{1}{N_p} \Omega_a^p\{a^{p_s} B_s(f_a)\} \qquad (s = 1, 2, \ldots, m)$$

являются инвариантами заданных базисных форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$.

Поступая с этими инвариантами J_1, $J_2, \ldots, J_m$ так же, как мы поступили выше с инвариантом i, мы видим, что эти инварианты тоже могут быть представлены в виде линейных комбинаций инвариантов i_1, $i_2, \ldots, i_m$, причем функции, являющиеся коэффициентами этих линейных комбинаций, снова будут инвариантами. Однако поскольку при каждом повторении этой процедуры веса представляемых инвариантов убывают, этот процесс закончится и в итоге мы получим представление инварианта i в виде целой рациональной функции от инвариантов i_1, $i_2, \ldots, i_m$. Этим завершается доказательство для тернарных базисных форм от одного набора переменных.

Однако выше мы ограничились лишь этим случаем исключительно ради сокращения изложения, и мы легко убеждаемся теперь, что наши рассуждения могут быть непосредственно перенесены на случай базисных форм от n переменных. Вместо указанного выше дифференциального процесса следует воспользоваться общим дифференциальным процессом

$$\Omega_a = \sum \pm \frac{\partial^n}{\partial a_{11'} \partial a_{22'} \ldots \partial a_{nn'}} \qquad (1', 2' \ldots, n' = 1, 2, \ldots, n),$$

где через $a_{11}, a_{12}, \ldots, a_{nn}$ обозначены n^2 коэффициентов линейной подстановки n переменных.

Если базисные формы содержат несколько наборов переменных, которые подвергаются тому же линейному преобразованию, то предыдущий процесс остается тем же самым. И даже в том случае, когда базисные формы содержат несколько наборов переменных, которые частично подвергаются различным линейным преобразованиям, теперь уже достаточно лишь краткого указания, как следует обобщить предыдущие рассуждения.

Поэтому пусть заданы базисные формы $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ от набора трех переменных x_1, x_2, x_3 и набора двух переменных ξ_1, ξ_2, которые преобразуются одновременно с помощью формул

$$\begin{aligned} x_1 &= a_{11}y_1 + a_{12}y_2 + a_{13}y_3, \\ x_2 &= a_{21}y_1 + a_{22}y_2 + a_{23}y_3, \\ x_3 &= a_{31}y_1 + a_{32}y_2 + a_{33}y_3, \end{aligned} \qquad a = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix},$$

$$\begin{aligned} \xi_1 &= \alpha_{11}\eta_1 + \alpha_{12}\eta_2, \\ \xi_2 &= \alpha_{21}\eta_1 + \alpha_{22}\eta_2, \end{aligned} \qquad \alpha = \begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix}.$$

Пусть это преобразование переводит формы $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ в формы $f_{a\alpha}^{(1)}, f_{a\alpha}^{(2)}, \ldots, f_{a\alpha}^{(k)}$, коэффициенты которых содержат как подстановочные коэффициенты $a_{11}, a_{12}, \ldots, a_{33}$, так и подстановочные коэффициенты $\alpha_{12}, \alpha_{12}, \alpha_{21}, \alpha_{22}$. Мы понимаем под инвариантом этого преобразования такое выражение, которое однородно по коэффициентам каждой из базисных форм и изменяется лишь на степени определителей подстановок a и α, когда коэффициенты базисных форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ заменяются на соответствующие коэффициенты преобразованных форм $f_{a\alpha}^{(1)}, f_{a\alpha}^{(2)}, \ldots, f_{a\alpha}^{(k)}$.

В рассматриваемом случае доказанное выше утверждение соответствует следующему предложению:

Пусть $F(f_{a\alpha})$ — любая целая функция от коэффициентов преобразованных форм $f_{a\alpha}^{(1)}, f_{a\alpha}^{(2)}, \ldots, f_{a\alpha}^{(k)}$, однородная по коэффициентам каждой из них. Умножим эту функцию $F(f_{a\alpha})$ на $a^q\alpha^\varkappa$, где q и $\varkappa$ — произвольные неотрицательные целые числа, и применим к произведению $a^q\alpha^\varkappa F(f_{a\alpha})$ оба процесса

$$\Omega_a = \frac{\partial^3}{\partial a_{11}\partial a_{22}\partial a_{33}} - \frac{\partial^3}{\partial a_{11}\partial a_{23}\partial a_{32}} + \frac{\partial^3}{\partial a_{12}\partial a_{23}\partial a_{31}} - \frac{\partial^3}{\partial a_{12}\partial a_{21}\partial a_{33}} + \frac{\partial^3}{\partial a_{13}\partial a_{21}\partial a_{32}} - \frac{\partial^3}{\partial a_{13}\partial a_{22}\partial a_{31}}$$

и

$$\Omega_\alpha = \frac{\partial^2}{\partial \alpha_{11}\partial \alpha_{22}} - \frac{\partial^2}{\partial \alpha_{12}\partial \alpha_{21}}$$

столько раз, пока не получится выражение, свободное от подстановочных коэффициентов $a_{11}, a_{12}, \ldots, a_{33}, \alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$. Тогда полученное в результате выражение является инвариантом базисных форм $f^{(1)}, f^{(2)}, \ldots, f^{(k)}$ в требующемся смысле.

Доказательство этого предложения полностью соответствует предыдущему подробно проведенному доказательству для форм с тернарным набором переменных; как и там, легко видеть что и, обратно, всякий инвариант может быть получен применением дифференциальных процессов Ω_a и Ω_α указанным в предложении способом к соответствующим образом подобранной функции от коэффициентов преобразованных форм.

Чтобы установить теперь конечность полной системы инвариантов рассматриваемого вида, предположим снова, что выбраны m инвариантов i_1, $i_2, \ldots, i_m$, через которые каждый другой инвариант i можно выразить в виде

$$i = A_1 i_1 + A_2 i_2 + \ldots + A_m i_m,$$

где A_1, $A_2, \ldots, A_m$ — целые однородные функции от коэффициентов базисных форм. Из этого соотношения тем же способом, что и выше, мы получаем соотношение

$$i = B_1 i_1 + B_2 i_2 + \ldots + B_m i_m,$$

где функции B_1, $B_2, \ldots, B_m$ однородны по коэффициентам каждой из базисных форм. Если мы заменим в этом равенстве коэффициенты базисных форм $f^{(1)}$, $f^{(2)}, \ldots, f^{(k)}$ на соответствующие коэффициенты преобразованных базисных форм $f_{a\alpha}^{(1)}$, $f_{a\alpha}^{(2)}, \ldots, f_{a\alpha}^{(k)}$, то получим

$$a^p \alpha^\pi i = a^{p_1} \alpha^{\pi_1} B_1(f_{a\alpha}) i_1 + \ldots a^{p_m} \alpha^{\pi_m} B_m(f_{a\alpha}) i_m.$$

Наконец, применение дифференциального процесса $\Omega_a^p \Omega_\alpha^\pi$ и последующее деление на ненулевое число

$$\Omega_a^p \Omega_\alpha^\pi \{a^p \alpha^\pi\} = N_p N_\pi$$

приводит к равенству

$$i = J_1 i_1 + J_2 i_2 + \ldots + J_m i_m,$$

где J_1, $J_2, \ldots, J_m$ — инварианты базисных форм в требующемся смысле. Повторное применение этой формулы приводит к целому рациональному представлению инварианта i через m инвариантов i_1, $i_2, \ldots, i_m$.

Легко видеть, что использованные в разборе этого случая соображения немедленно переносятся на случай, когда базисные формы содержат любое число наборов переменных, подвергающихся одному и тому же или разным преобразованиям. Мы приходим к следующему общему утверждению:

Теорема V. *Для любой системы базисных форм от любого числа наборов переменных, подвергающихся предписанным способом одинаковым или различным линейным преобразованиям, всегда существует конечное число таких целых рациональных инвариантов, что всякий другой целый рациональный инвариант является рациональной функцией от них.*

Что касается так называемых ковариантов и комбинантов систем форм, то все эти конструкции являются частными случаями понятия инварианта, рассмотренного выше. Поэтому из теоремы V следует конечность полных систем для этих инвариантных конструкций. То же самое справедливо для так называемых контравариантов и всех других инвариантных конструкций,

содержащих в качестве переменных некоторые составные определители, образованные из нескольких наборов переменных[17]. Эти конструкции могут быть охвачены данным выше понятием инварианта с помощью присоединения к уже имеющимся базисным формам подходящих форм от нескольких наборов переменных. Если это сделано, то непосредственно применимы все предыдущие рассмотрения, и, следовательно, для таких инвариантных конструкций также устанавливается конечность полных систем. В качестве примера такого случая можно взять систему базисных форм, в которой переменными являются шесть координат p_{ik} прямой [45].

Однако ситуация становится иной при попытке обобщить понятие инварианта в направлении, указанном исследованиями Ф. Клейна[18] и С. Ли[19]. До сих пор мы определяли инвариант как целую рациональную функцию от коэффициентов базисных форм, которая инвариантна относительно *всех* линейных преобразований переменных. Но теперь, следуя более общей концепции, мы выбираем определенную подгруппу в общей группе линейных преобразований и интересуемся целыми однородными функциями от коэффициентов базисных форм, инвариантными только относительно подстановок из выбранной подгруппы. Хотя все инварианты в предыдущем смысле содержатся, очевидно, среди этих новых инвариантов, из наших предыдущих утверждений о конечности полной системы инвариантов не следует, что всегда можно выбрать конечное число инвариантов в указанном расширенном смысле так, что всякий другой инвариант такого же типа является целой рациональной функцией от них [46].

Предыдущие рассмотрения и результаты непосредственно переносятся на теорию инвариантов в расширенном смысле, если коэффициенты подстановок из группы являются целыми рациональными функциями от некоторого числа параметров, причем параметры подстановки, составленной из двух подстановок, являются билинейными функциями от параметров этих подстановок, и если, кроме того, имеется дифференциальный процесс, точно так же порождающий инварианты, принадлежащие данной группе, как и дифференциальный процесс Ω в случае инвариантов общей линейной группы. Конечность системы инвариантов для таких групп подстановок получается с помощью наших аргументов.

Чтобы показать, как в такого рода случае может быть проведено доказательство, рассмотрим группу тернарных ортогональных подстановок, т. е. группу всех линейных подстановок трех однородных переменных, сохраняющих сумму квадратов этих переменных. Известно, что формулы преобразований для этих подстановок имеют вид

$$\begin{aligned}
x_1 &= (a_1^2 + a_2^2 - a_3^2 - a_4^2)y_1 - 2(a_1a_3 + a_2a_4)y_2 - 2(a_1a_4 - a_2a_3)y_3,\\
x_2 &= 2(a_1a_3 - a_2a_4)y_1 + (a_1^2 - a_2^2 - a_3^2 + a_4^2)y_2 - 2(a_1a_2 + a_3a_4)y_3,\\
x_3 &= 2(a_1a_4 + a_2a_3)y_1 + 2(a_1a_2 - a_3a_4)y_2 + (a_1^2 - a_2^2 + a_3^2 - a_4^2)y_3,
\end{aligned}$$

---

[17] См.: *Study E.* — Über den Begriff der Invariante algebraischer Formen. — Ber. kgl. sächs. Ges. Wiss., 1887, S. 142.

[18] См. его программу в: *Klein F.* Vergleichende Betrachtungen über neuere geometrische Forschungen. — Erlangen, 1872; см. также: Ges. Abh., Bd. I, 1921, S. 460.

[19] См. предисловие к книге: *Lie S.* Theorie der Transformationsgruppen. — Leipzig, 1888.

где через a_1, a_2, a_3, a_4 обозначены однородные параметры группы подстановок. Групповое свойство этих подстановок легко проверяется, если заменить в указанных формулах параметры a_1, a_2, a_3, a_4 на другие величины и образовать составную подстановку из полученной подстановки и исходной. Что касается инвариантов этой группы подстановок, то имеет место следующее предложение:

Если подвергнуть систему тернарных базисных форм линейному преобразованию с помощью указанных формул, а затем применить к произвольной однородной функции от коэффициентов преобразованных базисных форм дифференциальный символ

$$\Omega = \frac{\partial^2}{\partial a_1^2} + \frac{\partial^2}{\partial a_2^2} + \frac{\partial^2}{\partial a_3^2} + \frac{\partial^2}{\partial a_4^2}$$

столько раз, пока не получится выражение, свободное от параметров a_1, a_2, a_3, a_4, то это выражение будет инвариантом относительно группы подстановок, заданных указанными формулами. То же самое справедливо, если умножить прежде однородную функцию от преобразованных коэффициентов на произвольную целую степень выражения $a_1^2 + a_2^2 + a_3^2 + a_4^2$.

Применение этого предложения позволяет доказать конечность полной системы инвариантов; в этом легко убедиться, перенеся на рассматриваемый случай рассуждения из предыдущего доказательства.

Другой пример дает группа, содержащая следующие кватернарные подстановки:

$$\begin{aligned}
x_1 &= a_1^3 y_1 + 3a_1^2 a_2 y_2 + 3a_1 a_2^2 y_3 + a_2^3 y_4,\\
x_2 &= a_1^2 a_3 y_1 + (a_1^2 a_4 + 2a_1 a_2 a_3) y_2 + (2a_1 a_2 a_4 + a_2^2 a_3) y_3 + a_2^2 a_4 y_4,\\
x_3 &= a_1 a_3^2 y_1 + (2a_1 a_3 a_4 + a_2 a_3^2) y_2 + (a_1 a_4^2 + 2a_2 a_3 a_4) y_3 + a_2 a_4^2 y_4,\\
x_4 &= a_3^2 y_1 + 3a_3^2 a_4 y_2 + 3a_3 a_4^2 y_3 + a_4^3 y_4.
\end{aligned}$$

Если мы интерпретируем переменные как однородные координаты точки в пространстве, то эти формулы с переменными параметрами a_1, a_2, a_3, a_4 задают все линейные преобразования пространства, которые сохраняют пространственную кривую третьего порядка. Рассуждения, аналогичные приведенным выше, показывают, что и в этом случае имеет место конечность полной системы инвариантов [47].

После нахождения всех инвариантов данной системы базисных форм возникает следующий вопрос о взаимной зависимости инвариантов полной системы. И опять основу для такого исследования доставляют теоремы I и III. В самом деле, если мы положим во встречающихся в них формах одну из n однородных переменных равной единице, то немедленно увидим, что обе эти теоремы имеют также место и для неоднородных функций и, в частности, их можно применить к соотношениям между инвариантами [48]. Будем теперь, как обычно, понимать под неприводимой сизигией соотношение между инвариантами системы базисных форм, левая часть которого не представима в виде линейной комбинации сизигий меньшей степени. Тогда из теоремы I вытекает следующее предложение:

Конечная система инвариантов имеет лишь к о н е ч н о е число неприводимых сизигий.

Рассмотрим в качестве примера полную систему инвариантов трех бинарных квадратичных базисных форм, состоящую, как известно, из семи инвариантов и шести ковариантов. Можно показать, что для этой системы инвариантов имеется 14 неприводимых сизигий, из которых всякая другая сизигия получается как линейная комбинация.

Однако в соответствии с общими принципами разд. I, III и IV нахождение полной системы неприводимых сизигий является лишь первым шагом на пути полного описания общих зависимостей между инвариантами, ибо, вообще говоря, между сизигиями также имеются линейные соотношения, коэффициенты которых являются инвариантами, — так называемые сизигии второго рода, а они, в свою очередь, сами связаны линейными соотношениями — так называемыми сизигиями третьего рода [49]. Согласно теореме III, переформулированной, как указано выше, для неоднородных функций, этот процесс должен завершиться после конечного числа повторений. Таким образом, мы приходим к следующему утверждению:

Система неприводимых сизигий первого, второго и т.д. рода образует цепь производных систем уравнений. Эта цепь сизигий обрывается после конечного числа шагов, а именно, не существует сизигий более чем $(m+1)$*-го рода, где* m *— число инвариантов в полной системе* [50].

В каждом частном случае полное исследование системы инвариантов требует нахождения всей цепи сизигий. В соответствии со сказанным в разд. IV в этом случае можно найти линейно независимые инварианты заранее указанной степени, а именно найти их выражение в виде целых рациональных функций от инвариантов из полной системы.

Кёнигсберг в Пруссии, 15 февраля 1890.

О ПОЛНОЙ СИСТЕМЕ ИНВАРИАНТОВ*)

ВВЕДЕНИЕ

В моей работе «О теории алгебраических форм»[1] содержится несколько теорем, важных для теории инвариантов. С помощью этих теорем в разд. V указанной работы я, в частности, доказал *конечность* полной системы инвариантов для произвольной базисной формы. *Эта теорема о конечности полной системы инвариантов является отправной точкой и основой исследований настоящей работы*[2]. Развитые ниже методы существенно отличаются от тех, которые использовались раньше в теории инвариантов. А именно, теория алгебраических инвариантов рассматривается в дальнейшем в рамках общей теории полей алгебраических функций. Таким образом, теория инвариантов появляется просто как особенно замечательный пример в теории полей алгебраических функций многих переменных подобно тому, как в теории чисел теория круговых полей рассматривается как особенно важный пример, для которого были впервые обнаружены и доказаны наиболее важные утверждения теории общих числовых полей.

Используемые далее методы пригодны для систем базисных форм от произвольного числа переменных или наборов переменных, которые подвергаются одному и тому же линейному преобразованию или различным линейным преобразованиям предписанным заранее способом. Тем не менее, в дальнейшем ради краткости и наглядности я буду чаще всего рассматривать в качестве базисных форм лишь бинарные или тернарные формы от одного набора переменных.

Всюду далее под *инвариантом* без каких бы то ни было уточнений всегда понимается целый рациональный инвариант, т. е. целая рациональная однородная функция от коэффициентов a базисной формы или системы базисных форм, которая при замене коэффициентов a на соответствующие коэффициенты b линейно преобразованной базисной формы умножается на степень определителя преобразования [1]. Известно, что эти инварианты обладают следующими элементарными свойствами:

1. Инварианты сохраняются линейными преобразованиями из некоторой непрерывной группы [2].

---

*) Über die vollen Invariantensysteme. — Math. Ann., 1893, Bd. 42, S. 313–373. *Перевод В. Л. Попова.*

1) Über die Theorie der algebraischen Formen. — Math. Ann., 1890, Bd. 36, S. 473–534 [имеется перевод на с. 16–66 настоящего издания. — *Ред.*].

2) См. три заметки автора: Über die Theorie der algebraischen Invarianten. — Nachr. Ges. Wiss. Göttingen, 1891, S. 232 (первая заметка); 1892, S. 6, 439 (вторая и третья заметки).

2. Инварианты удовлетворяют некоторым линейным дифференциальным уравнениям в частных производных [3].

3. Всякая алгебраическая и, в частности, всякая рациональная функция от произвольного количества инвариантов, являющаяся целой рациональной однородной функцией от коэффициентов a базисных форм, также является инвариантом [4].

4. Если произведение двух целых рациональных функций от коэффициентов a является инвариантом, то и каждый из сомножителей является инвариантом [5].

Утверждения 1 и 2 допускают обращение. По утверждению 3 система всех инвариантов образует замкнутую область целых функций, которую нельзя расширить алгебраическими конструкциями. Утверждение 4 говорит о том, что в этой области функций имеют место обычные законы делимости, т. е. каждый инвариант может быть однозначно представлен в виде произведения неразложимых инвариантов.

Для вычисления инвариантов и дальнейшего развития теории нам нужна одна лемма[3)], касающаяся фундаментального свойства так называемого Ω-процесса; вкратце она может быть сформулирована так:

Если образовать произвольную целую рациональную функцию от коэффициентов b линейно преобразованной базисной формы и применить к ней Ω-процесс столько раз, сколько нужно, чтобы получить выражение, не содержащее коэффициентов примененной подстановки, то полученное в итоге выражение будет инвариантом.

Завершим список этих элементарных утверждений теории инвариантов формулировкой упомянутого выше утверждения о конечности:

5. Существует такое конечное множество инвариантов, что любой инвариант может быть представлен в виде целой рациональной функции от них. Этот конечный набор инвариантов мы называем *полной системой инвариантов*.

Вместе все эти пять утверждений приводят к вопросу о том, какие из перечисленных свойств системы функций связаны друг с другом, а какие выполняются независимо от других. В первой из цитированных выше моих заметок «Über die Theorie der algebraischen Invarianten»[4)] я привел пример бесконечной системы целых рациональных однородных функций, которая обладает свойствами 2, 3 и 5, но не обладает свойством 4.

Отметим в заключение, что из общих теорем моей работы «О теории алгебраических форм», цитированной в начале, следуют еще два утверждения о конечности в теории инвариантов, а именно предложение о конечности числа неприводимых сизигий и предложение о том, что цепь сизигий обрывается через конечное число шагов.

[3)] См. мою работу, цитированную выше, с. 58 [страницы указываются по настоящему изданию. — *Ред.*]; это утверждение по существу соответствует одному результату П. Гордана и Ф. Мертенса. Недавно Стори (Math. Ann., Bd. 41, S. 469) указал указал дифференциальный процесс [ ], непосредственно образованный из дифференцирований по коэффициентам a и способный заменить Ω-процесс; этот процесс является обобщением процесса [ ] для бинарных форм, указанного мною в моей диссертации, см. Math. Ann., Bd. 30, S. 20.

[4)] S. 233

I. ПОЛЕ ИНВАРИАНТОВ

§ 1. Одно вспомогательное алгебраическое утверждение

Рациональные инварианты базисной формы или системы базисных форм образуют поле функций, а целые рациональные инварианты являются целыми алгебраическими функциями указанного поля функций. Чтобы убедиться в этом, воспользуемся следующим простым вспомогательным предложением:

Если заданы m целых рациональных однородных функций $f_1, \ldots, f_m$ от n переменных $x_1, \ldots, x_n$, то всегда можно образовать из них некоторое число $\varkappa$ таких целых рациональных однородных функций $F_1, \ldots, F_\varkappa$ от тех же самых переменных, что между ними не существует алгебраических соотношений с постоянными коэффициентами, а каждая из данных функций представляется в виде *целой* алгебраической функции от $F_1, \ldots, F_\varkappa$ [6].

Для доказательства обозначим через $\nu_1, \ldots, \nu_m$ степени функций $f_1, \ldots, f_m$ относительно переменных $x_1, \ldots, x_n$, и пусть ν — произведение этих степеней. Тогда m функций

$$f_1' = f_1^{\nu/\nu_1}, \quad \ldots, \quad f_m' = f_m^{\nu/\nu_m}$$

имеют одинаковую степень ν. Если между этими m функциями не имеется алгебраических соотношений с постоянными коэффициентами [7], то таких соотношений нет и между исходными функциями $f_1, \ldots, f_m$, и, значит, уже эти функции образуют систему требующегося типа. В противном случае имеется соотношение вида

$$G(f_1', \ldots, f_m') = 0,$$

где G — целая рациональная однородная функция от $f_1', \ldots, f_m'$ [8]. Осуществим теперь линейное преобразование этих m функций, полагая

$$f_1' = \alpha_{11} f_1'' + \ldots + \alpha_{1m} f_m'',$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$f_m' = \alpha_{m1} f_1'' + \ldots + \alpha_{mm} f_m'',$$

где определитель преобразования отличен от нуля, а само преобразование выбрано так, чтобы в преобразованной функции $H(f_1'', \ldots, f_m'')$ коэффициент при старшей степени f_m'' был равен 1 [9]. Тогда f_m'', очевидно, является целой алгебраической функцией от $f_1'', \ldots, f_{m-1}''$; поэтому функции $f_1', \ldots, f_m'$, а значит, и исходные функции $f_1, \ldots, f_m$ могут быть представлены как целые алгебраические функции от $m-1$ функций $f_1'', \ldots, f_{m-1}''$. Если теперь между этими $m-1$ функциями нет алгебраических соотношений, то они образуют систему функций требующегося типа. В противном случае мы поступим с однородным соотношением между этими $m-1$ функциями так же, как мы поступили выше с соотношением $G = 0$. Повторяя этот процесс, мы придем в конце концов к системе однородных функций $F_1, \ldots, F_\varkappa$ одинаковой степени ν по переменным $x_1, \ldots, x_n$, которая обладает указанным в предложении свойством.

§ 2. Инварианты J, J_1, ..., $J_\varkappa$

Пусть $i_1, \ldots, i_m$ — полная система инвариантов. Они являются целыми рациональными однородными функциями от коэффициентов базисной формы и поэтому из доказанного в § 1 вспомогательного предложения вытекает следующее утверждение:

Если задана произвольная базисная форма или система форм, то всегда имеется некоторое число $\varkappa$ таких инвариантов $J_1, \ldots, J_\varkappa$, не связанных никакими алгебраическими соотношениями, что всякий другой инвариант может быть представлен в виде целой алгебраической функции от них.

Например, $\varkappa = n - 2$ в случае одной бинарной базисной формы порядка n, а в случае тернарной базисной формы порядка n имеем $\varkappa = \frac{1}{2}(n+1)(n+2) - 8$ [10].

Можно считать, что все инварианты $J_1, \ldots, J_\varkappa$ имеют одинаковую степень по коэффициентам базисной формы; обозначим эту степень через ν.

Помимо этого, имеется следующее утверждение:

К инвариантам $J_1, \ldots, J_\varkappa$ всегда можно присоединить такой инвариант J, что любой инвариант базисной формы рационально выражается через J, $J_1, \ldots, J_\varkappa$ [11].

Чтобы найти инвариант J, выберем любые два инварианта из полной системы, скажем i_1 и i_2, степеней ν_1 и ν_2 соответственно, а затем положим

$$i_1' = i_1^{\alpha_1} i_2^{\alpha_2},$$
$$i_2' = i_1^{\beta_1} i_2^{\beta_2} J_1^{\gamma},$$

где показатели α_1, α_2, β_1, β_2, γ являются положительными целыми числами, удовлетворяющими условиям

$$\alpha_1\nu_1 + \alpha_2\nu_2 = \beta_1\nu_1 + \beta_2\nu_2 + \gamma\nu,$$
$$\alpha_1\beta_2 - \alpha_2\beta_1 = 1.$$

Чтобы найти такие числа, возьмем сначала три положительных целых числа δ_1, δ_2, γ, обладающих следующими свойствами:

$$\delta_1\nu_1 + \delta_2\nu_2 = \gamma\nu,$$

а δ_1 и δ_2 взаимно просты. Затем возьмем два положительных целых числа β_1, β_2, для которых

$$\delta_1\beta_2 - \delta_2\beta_1 = 1.$$

Тогда пять чисел $\alpha_1 = \delta_1 + \beta_1$, $\alpha_2 = \delta_2 + \beta_2$, β_1, β_2, γ обладают нужным нам свойством.

Как показывают формулы

$$i_1 = i_1'^{\beta_2} i_2'^{-\alpha_2} J_1^{\alpha_2\gamma},$$
$$i_2 = i_1'^{-\beta_1} i_2'^{\alpha_1} J_1^{-\alpha_1\gamma},$$

i_1 и i_2 могут быть рационально выражены через i_1', i_2', J_1. Поскольку инварианты i_1', i_2' имеют одинаковую степень по коэффициентам базисной формы, всякая линейная комбинация

$$i'' = c_1 i_1' + c_2 i_2'$$

является инвариантом. Согласно известному предложению теории алгебраических функций, можно так определить константы c_1 и c_2 в этом выражении, что оба инварианта i_1' и i_2' будут рациональными функциями от i'', $J_1, \ldots, J_\varkappa$. Значит, все инварианты базисной формы могут быть выражены в виде рациональных функций от i'', $J_1, \ldots, J_\varkappa$, i_3, $i_4, \ldots, i_m$. Если снова выбрать два инварианта, скажем i'' и i_3, из i'', i_3, $i_4, \ldots, i_m$, то, как и выше, можно найти такой инвариант i''', что i'' и i_3 являются рациональными функциями от i''', $J_1, \ldots, J_\varkappa$ и, таким образом, все инварианты являются рациональными функциями от i''', $J_1, \ldots, J_\varkappa$, i_4, $i_5, \ldots, i_m$. Продолжая этот процесс, мы в конце концов придем к инварианту $i^{(m)} = J$ с требующимся свойством.

Согласно доказанным утверждениям, каждый инвариант является рациональной функцией от J, $J_1, \ldots, J_\varkappa$ и целой алгебраической функцией от $J_1, \ldots, J_\varkappa$; обратно, каждая функция i, являющаяся рациональной функцией от J, $J_1, \ldots, J_\varkappa$ и целой алгебраической функцией от $J_1, \ldots, J_\varkappa$, является инвариантом базисной формы. Действительно, поскольку функция i рационально зависит от инвариантов J, $J_1, \ldots, J_\varkappa$, она должна быть рациональной функцией от коэффициентов базисной формы; положим $i = g/h$, где g и h — целые рациональные функции от коэффициентов базисной формы, не имеющие общих множителей. Далее, i удовлетворяет уравнению вида

$$i^k + G_1 i^{k-1} + \ldots + G_k = 0,$$

где $G_1, \ldots, G_k$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$. Подставляя в это уравнение $i = g/h$ и умножая полученное уравнение на h^{k-1}, получаем, что g^k/h является целой рациональной функцией от коэффициентов базисной формы. Но поскольку g и h взаимно просты, h должна быть константой, т. е. i — целая рациональная функция от коэффициентов базисной формы и, значит, целый рациональный инвариант. Отсюда вытекает следующее утверждение:

Инварианты J, $J_1, \ldots, J_\varkappa$ определяют поле функций, в котором целые алгебраические функции являются в точности всеми целыми рациональными инвариантами; это поле в дальнейшем будет коротко называться полем инвариантов [12].

Теперь, согласно одному фундаментальному утверждению, принадлежащему Л. Кронекеру, в любом поле функций всегда имеется конечное число таких целых функций, что любая целая функция из этого поля представляется в виде их линейной комбинации с коэффициентами, являющимися целыми рациональными функциями из этого поля [13]; кроме того, общая теория алгебраических функций, развитая Л. Кронекером, показывает, как определить целые алгебраические функции из поля. В соответствии с этими результатами для того, чтобы получить полную систему инвариантов $i_1, \ldots, i_m$ из инвариантов J, $J_1, \ldots, J_\varkappa$, нужно прежде всего вычислить дискриминант D уравнения степени k для J [14]. Все инварианты базисной формы, т. е. целые алгебраические функции из поля инвариантов, имеют тогда следующий вид [15]:

$$i = \frac{\Gamma_1 J^{k-1} + \Gamma_2 J^{k-2} + \ldots + \Gamma_k}{D}.$$

Применяя к бесконечному ряду, построенному из функций $\Gamma_1, \Gamma_2, \ldots, \Gamma_k$, теорему I из разд. I моей работы, цитированной выше[5]), мы видим, что имеется конечное число таких инвариантов $j_1, \ldots, j_M$, что любой инвариант представляется в виде

$$i = A_1 j_1 + \ldots + A_M j_M,$$

где $A_1, \ldots, A_M$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$ [16]. Тогда инварианты $J_1, \ldots, J_\varkappa, j_1, \ldots, j_M$ образуют полную систему инвариантов.

Итак, для построения полной системы инвариантов, помимо знания инвариантов $J, J_1, \ldots, J_\varkappa$, требуется лишь решить элементарную задачу из арифметической теории алгебраических функций [17].

II. ОБРАЩЕНИЕ ИНВАРИАНТОВ В НУЛЬ

§ 3. Одна общая теорема об алгебраических формах

Поскольку все инварианты базисной формы являются целыми алгебраическими функциями от $J_1, \ldots, J_\varkappa$, мы непосредственно получаем следующее утверждение:

Если коэффициентам базисной формы приданы такие специальные значения, что все $\varkappa$ инвариантов $J_1, \ldots, J_\varkappa$ обращаются в нуль, то это же верно для всех инвариантов базисной формы.

Большое значение для теории, которая будет здесь построена, имеет тот факт, что в действительности указанное свойство системы инвариантов $J_1, \ldots, J_\varkappa$ характеризует эти инварианты. Чтобы доказать это, мы докажем сначала утверждение, являющееся третьим общим фактом теории алгебраических функций после теорем I и III из моей работы, цитированной выше[6]). Оно гласит:

Пусть $f_1, \ldots, f_m$ — набор m целых рациональных однородных функций от n переменных $x_1, \ldots, x_n$, и пусть $F, F', F'', \ldots$ — произвольные целые рациональные однородные функции от тех же самых переменных, обращающиеся в нуль при любых значениях переменных [18], *при которых обращаются в нуль все $f_1, \ldots, f_m$. Тогда всегда можно указать такое число r, что каждое произведение $\Pi^{(r)}$ любых r функций из последовательности $F, F', F'', \ldots$ может быть представлено в виде*

$$\Pi^{(r)} = a_1 f_1 + a_2 f_2 + \ldots + a_m f_m,$$

где $a_1, a_2, \ldots, a_m$ — подходящие целые рациональные однородные функции от переменных $x_1, \ldots, x_n$ [19].

В следующем ниже доказательстве этой теоремы мы предположим сначала, что последовательность $F, F', F'', \ldots$ состоит только из *конечного* числа форм.

---

[5]) Math. Ann., Bd. 36, S. 474 [с. 16 настоящего издания. — *Ред.*].

[6]) См. Math. Ann., Bd. 36, S. 474, 492 [с. 16, 31–32 настоящего издания. — *Ред.*].

Доказательство распадается на две части: в *первой* мы докажем теорему в частном случае, когда m заданных форм $f_1, \ldots, f_m$ имеют лишь конечное число общих нулей [20]. Чтобы получить это доказательство, мы предположим, что теорема уже доказана для некоторого количества общих нулей, и покажем тогда, что она справедлива также с дополнительным общим нулем.

Пусть общими нулями форм $f_1, \ldots, f_m$ будут

$$\begin{aligned} &x_1 = \alpha_1, \quad x_2 = \alpha_2, \quad \ldots, \quad x_n = \alpha_n, \\ &x_1 = \beta_1, \quad x_2 = \beta_2, \quad \ldots, \quad x_n = \beta_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &x_1 = \varkappa_1, \quad x_2 = \varkappa_2, \quad \ldots, \quad x_n = \varkappa_n. \end{aligned}$$

Заменим теперь переменные $x_1, \ldots, x_n$ на выражения $x_1\xi_1, x_2\xi_1, \ldots$ $\ldots, x_{n-1}\xi_1, \xi_2$, преобразовав тем самым формы $f_1, \ldots, f_m$ в бинарные формы от переменных ξ_1, ξ_2 порядков $\nu_1, \ldots, \nu_m$. Построим далее выражения

$$\begin{aligned} F_1 &= u_1 f_1 + u_2 f_2 + \ldots u_m f_m, \\ F_2 &= v_1 f_1 + v_2 f_2 + \ldots v_m f_m, \end{aligned}$$

где $u_1, \ldots, u_m, v_1, \ldots, v_m$ — бинарные формы от переменных ξ_1, ξ_2 с неопределенными коэффициентами таких порядков, чтобы F_1 и F_2 были однородными по этим переменным. Тогда результант двух бинарных форм F_1, F_2 относительно переменных ξ_1, ξ_2 является целой рациональной функцией от неопределенных коэффициентов форм $u_1, \ldots, u_m, v_1, \ldots, v_m$, а степени и произведения этих неопределенных коэффициентов оказываются умноженными на формы, содержащие только $n-1$ переменных $x_1, \ldots, x_{n-1}$; обозначим эти формы через $f'_1, \ldots, f'_{m'}$. Из свойств результанта двух бинарных форм легко вытекает, что формы $f'_1, \ldots, f'_{m'}$ имеют только следующие общие нули:

$$\begin{aligned} &x_1 = \alpha_1, \quad x_2 = \alpha_2, \quad \ldots, \quad x_{n-1} = \alpha_{n-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &x_1 = \varkappa_1, \quad x_2 = \varkappa_2, \quad \ldots, \quad x_{n-1} = \varkappa_{n-1}, \end{aligned}$$

и что, кроме того, все эти формы являются линейными комбинациями форм $f_1, \ldots, f_m$, т. е.

$$\left.\begin{aligned} f'_1 &\equiv 0, \\ &\ldots\ldots \\ f'_{m'} &\equiv 0, \end{aligned}\right\} \quad (f_1, \ldots, f_m).$$

Применяя снова этот процесс исключения — на этот раз к формам $f'_1, \ldots$ $\ldots, f'_{m'}$, — мы получим систему форм $f''_1, \ldots, f''_{m''}$ от $n-2$ переменных $x_1, \ldots$ $\ldots, x_{n-2}$, общими нулями которых являются только

$$\begin{aligned} &x_1 = \alpha_1, \quad x_2 = \alpha_2, \quad \ldots, \quad x_{n-2} = \alpha_{n-2}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &x_1 = \varkappa_1, \quad x_2 = \varkappa_2, \quad \ldots, \quad x_{n-2} = \varkappa_{n-2} \end{aligned}$$

и которые все сравнимы с нулем по модулю $(f'_1, \ldots, f'_{m'})$, а значит, и по модулю $(f_1, \ldots, f_m)$. Продолжая этот процесс, мы приходим в итоге к систе-

ме бинарных форм $f_1^{(n-2)}, \ldots, f_{m^{(n-2)}}^{(n-2)}$ от переменных x_1, x_2, имеющих лишь следующие общие нули:

$$x_1 = \alpha_1, \quad x_2 = \alpha_2,$$
$$\ldots\ldots\ldots\ldots$$
$$x_1 = \varkappa_1, \quad x_2 = \varkappa_2,$$

и сравнимых с нулем по модулю $(f_1, \ldots, f_m)$. Выберем одну из этих бинарных форм и представим ее в виде $(\alpha_2 x_1 - \alpha_1 x_2)^{\rho_{12}} \varphi_{12}$, где ρ_{12} — целое положительное число, а φ_{12} — бинарная форма, не обращающаяся в нуль при $x_1 = \alpha_1$, $x_2 = \alpha_2$. Здесь предполагается, что α_1, α_2 одновременно не равны нулю [21].

Таким же способом, когда α_1, α_3 одновременно не равны нулю, мы найдем целое число ρ_{13} и бинарную форму φ_{13} от переменных x_1, x_3, не обращающуюся в нуль при $x_1 = \alpha_1$, $x_3 = \alpha_3$, для которых

$$(\alpha_3 x_1 - \alpha_1 x_3)^{\rho_{13}} \varphi_{13} \equiv 0, \qquad (f_1, \ldots, f_m),$$

и, наконец, целое число $\rho_{n-1,n}$ и бинарную форму $\varphi_{n-1,n}$ от переменных x_{n-1}, x_n, отличную от нуля при $x_{n-1} = \alpha_{n-1}$, $x_n = \alpha_n$, для которых

$$(\alpha_n x_{n-1} - \alpha_{n-1} x_n)^{\rho_{n-1,n}} \varphi_{n-1,n} \equiv 0, \qquad (f_1, \ldots, f_m).$$

Поскольку по предположению каждая форма в последовательности $F, F', F'', \ldots$ обращается в нуль при $x_1 = \alpha_1$, $x_2 = \alpha_2, \ldots, x_n = \alpha_n$, можно положить

$$F^{(i)} = F_{12}^{(i)} (\alpha_2 x_1 - \alpha_1 x_2) + F_{13}^{(i)} (\alpha_3 x_1 - \alpha_1 x_3) + \ldots + F_{n-1,n}^{(i)} (\alpha_n x_{n-1} - \alpha_{n-1} x_n),$$

где $F_{12}^{(i)}$, $F_{13}^{(i)}, \ldots, F_{n-1,n}^{(i)}$ — формы от n переменных $x_1, \ldots, x_n$. Если воспользоваться указанными выше сравнениями и положить для краткости

$$\rho = \rho_{12} + \rho_{13} + \ldots + \rho_{n-1,n},$$
$$\Phi = \varphi_{12} \varphi_{13} \ldots \varphi_{n-1,n},$$

то отсюда следует, что

$$\Phi \Pi^{(\rho)} \equiv 0, \qquad (f_1, \ldots, f_m),$$

где Φ — форма, не обращающаяся в нуль при $x_1 = \alpha_1$, $x_2 = \alpha_2, \ldots, x_n = \alpha_n$, а $\Pi^{(\rho)}$ — произведение любых ρ форм из последовательности $F, F', F'', \ldots$

Формы Φ, $f_1, \ldots, f_m$ имеют меньше общих нулей, чем формы $f_1, \ldots, f_m$ исходной системы. Значит, поскольку мы предположили, что теорема доказана для систем форм с меньшим числом нулей, найдется такое число r, что

$$\Pi^{(r)} \equiv 0, \qquad (\Phi, f_1, \ldots, f_m),$$

где $\Pi^{(r)}$ — произведение любых r форм из последовательности $F, F', F'', \ldots$ Используя предыдущее сравнение, мы получаем отсюда, что

$$\Pi^{(\rho+r)} \equiv 0, \qquad (f_1, \ldots, f_m),$$

где $\Pi^{(\rho+r)}$ — произведение любых $\rho + r$ функций из последовательности $F, F', F'', \ldots$ Тем самым для систем форм $f_1, \ldots, f_m$, удовлетворяющих сделанным предположениям, теорема доказана.

Теорема верна, далее, в случае, когда данные формы вообще *не имеют* общих нулей [22]. Действительно, в этом случае бинарные формы $f_1^{(n-2)}, \ldots, f_{m^{(n-2)}}^{(n-2)}$ не имеют общих нулей; значит, каждая бинарная форма от x_1, x_2 достаточно большого порядка и, в частности, формы $x_1^{\rho_1}$, $x_2^{\rho_2}$ для достаточно больших показателей ρ_1 и ρ_2 сравнимы с нулем по модулю $(f_1, \ldots, f_m)$. Таким же образом устанавливается, что формы $x_3^{\rho_3}, \ldots, x_n^{\rho_n}$ для достаточно больших показателей $\rho_3, \ldots, \rho_n$ сравнимы с нулем по модулю $(f_1, \ldots, f_m)$. Следовательно, любая форма от переменных $x_1, \ldots, x_n$ порядка, большего $\rho_1 + \rho_2 + \ldots + \rho_n$, сравнима с нулем по модулю $(f_1, \ldots, f_m)$, что и доказывает наше утверждение.

Вторая часть посвящена доказательству теоремы в общем случае. Чтобы получить его, мы предположим, что утверждение верно для произвольных форм от $n-1$ переменных, и покажем, что оно верно для случая n переменных.

Если положить $x_1 = tx_2$, то формы $f_1, \ldots, f_m, F, F', \ldots$ станут формами от $n-1$ переменных $x_2, \ldots, x_n$, коэффициенты которых являются целыми рациональными функциями от параметра t. Обозначим эти формы соответственно через $g_1, \ldots, g_m, G, G', \ldots$ Если теперь мы придадим параметру t произвольное определенное конечное значение, то, очевидно, каждая форма в последовательности $G, G', \ldots$ обратится в нуль при тех значениях переменных $x_2, \ldots, x_n$, которые обращают в нуль все m форм $g_1, \ldots, g_m$. Мы считаем сейчас теорему доказанной для случая $n-1$ переменных и будем предполагать вдобавок, что в этом случае число r можно выбрать меньшим некоторой границы, зависящей лишь от порядков и числа форм $g_1, \ldots, g_m, G, G', \ldots$, но не от их коэффициентов. Тогда нам известно, что имеется некоторое число $r = \sigma_{12}$, обладающее тем свойством, что для каждого конкретного значения t произведение $\Pi^{(\sigma_{12})}$ любых σ_{12} форм из последовательности $G, G', \ldots$ допускает представление

$$\Pi^{(\sigma_{12})} = b_1 g_1 + b_2 g_2 + \ldots + b_m g_m,$$

где $b_1, \ldots, b_m$ — целые рациональные однородные функции от $n-1$ переменных $x_2, \ldots, x_n$. Если мы рассмотрим коэффициенты u форм $b_1, \ldots, b_m$ в этой формуле как неопределенные величины и сравним коэффициенты при одинаковых степенях и произведениях переменных $x_2, \ldots, x_n$ в обеих ее частях, то получим неоднородную систему линейных уравнений для определения коэффициентов u. Коэффициенты в этих линейных уравнениях являются целыми рациональными функциями от параметра t, и мы, кроме того, знаем, что эта система линейных уравнений обладает решением для каждого частного конечного значения t.

Воспользуемся следующим легко доказываемым вспомогательным утверждением:

Если задана система линейных уравнений вида

$$\begin{aligned} c_{11}u_1 + \ldots c_{1p}u_p &= c_1, \\ \cdots\cdots\cdots\cdots & \\ c_{q1}u_1 + \ldots c_{qp}u_p &= c_q, \end{aligned}$$

где $c_{11}, c_{12}, \ldots, c_{qp}, c_1, \ldots, c_q$ — целые рациональные функции от параметра t, и если она имеет решение для каждого частного значения t, то всегда можно

определить такие рациональные функции от t [23], что при подстановке их вместо неизвестных $u_1, \ldots, u_p$ указанные уравнения преобразуются в тождества относительно параметра t.

Применяя это утверждение к полученным выше уравнениям, полагая $t = x_1/x_2$ и затем избавляясь от знаменателей, мы получаем следующее сравнение:

$$\psi_{12}\Pi^{(\sigma_{12})} \equiv 0, \qquad (f_1, \ldots, f_m),$$

где ψ_{12} — бинарная форма от пары переменных x_1, x_2, а $\Pi^{(\sigma_{12})}$ — произведение любых σ_{12} форм из последовательности $F, F', F'', \ldots$

Точно так же мы получаем сравнение вида

$$\psi_{13}\Pi^{(\sigma_{13})} \equiv 0, \qquad (f_1, \ldots, f_m),$$

где ψ_{13} — бинарная форма от пары переменных x_1, x_3, а $\Pi^{(\sigma_{13})}$ — произведение σ_{13} форм из последовательности $F, F', \ldots$ Пусть, наконец, $\sigma_{n-1,n}$ и $\psi_{n-1,n}$ — такие целое число и форма от двух переменных x_{n-1}, x_n, что имеет место сравнение

$$\psi_{n-1,n}\Pi^{(\sigma_{n-1,n})} \equiv 0, \qquad (f_1, \ldots, f_m).$$

Поскольку, очевидно, имеется лишь конечное число систем значений, для которых все формы $\psi_{12}, \psi_{13}, \ldots, \psi_{n-1,n}$, $f_1, \ldots, f_m$ обращаются в нуль, эта система форм имеет как раз такой вид, для которого теорема считается доказанной. Значит, можно найти такое число r, что

$$\Pi^{(r)} \equiv 0, \qquad (\psi_{12}, \psi_{13}, \ldots, \psi_{n-1,n}, f_1, \ldots, f_m).$$

С помощью предыдущего сравнения отсюда получаем, что

$$\Pi^{(\sigma+r)} \equiv 0, \qquad . (f_1, \ldots, f_m),$$

где σ — наибольшее из чисел $\sigma_{12}, \sigma_{13}, \ldots, \sigma_{n-1,n}$.

Поскольку во всяком случае бинарные формы могут иметь лишь конечное число нулей, то, согласно первой части доказательства, наша теорема верна в частном случае $n = 2$, а значит, также и в общем случае для форм от n переменных. Если теперь заданная последовательность $F, F', \ldots$ содержит бесконечно много форм [24], то можно найти такое число μ, что каждая форма из последовательности $F, F', \ldots$ является линейной комбинацией [25] μ форм $F, F', \ldots, F^{(\mu-1)}$, — это всегда возможно ввиду теоремы I моей работы, цитированной выше. Если теперь произведение любых r форм из $F, F', \ldots, F^{(\mu-1)}$ сравнимо с нулем по модулю $(f_1, \ldots, f_m)$, то, очевидно, это же верно и для произведения любых r форм из последовательности $F, F', \ldots$ Этим завершается доказательство теоремы.

Согласно только что доказанной теореме, r-я степень любой из форм $F, F', \ldots$ сравнима с нулем по модулю $(f_1, \ldots, f_m)$ [26]; в частном случае двух неоднородных переменных это утверждение было сформулировано и доказано Э. Нетто[7] [27].

---

[7] См. Acta math., Bd. 7, S. 101.

§ 4. Фундаментальная теорема об инвариантах, обращение которых в нуль влечет за собой обращение в нуль всех инвариантов

Продолжим теперь развитие теории инвариантов одной базисной формы или системы нескольких базисных форм, прерванное в начале предыдущего параграфа, и докажем следующее фундаментальное предложение:

Если μ инвариантов $I_1, \ldots, I_\mu$ обладают тем свойством, что их обращение в нуль влечет за собой обращение в нуль всех инвариантов, то все инварианты являются целыми алгебраическими функциями от $I_1, \ldots, I_\mu$.

По предположению μ инвариантов $I_1, \ldots, I_\mu$ являются такими функциями от коэффициентов базисной формы, что в том случае, когда этим коэффициентам придаются частные значения, обращающие $I_1, \ldots, I_\mu$ в нуль, все инварианты базисной формы тоже обращаются в нуль. Поэтому из общей теоремы § 3 следует, что имеется такое число r, что каждое произведение $\Pi^{(r)}$ любых r или большего числа инвариантов базисной формы может быть представлено в виде

$$\Pi^{(r)} = a_1 I_1 + a_2 I_2 + \ldots + a_\mu I_\mu,$$

где a_1, $a_2, \ldots, a_\mu$ — целые рациональные однородные функции от коэффициентов базисной формы. Как и выше, обозначим через $i_1, \ldots, i_m$ полную систему инвариантов; пусть ν — максимальная степень этих инвариантов. Тогда, очевидно, любой инвариант i базисной формы, имеющий степень $\geqslant \nu r$, может быть представлен как сумма произведений $\Pi^{(r)}$ и, значит,

$$i = a_1' I_1 + a_2' I_2 + \ldots a_\mu' I_\mu,$$

где a_1', $a_2', \ldots, a_\mu'$ — снова целые рациональные однородные функции от коэффициентов базисной формы. Следуя рассуждениям из моей работы «О теории алгебраических форм»[8)], цитированной выше, выражения a_1', $a_2', \ldots$ $\ldots, a_\mu'$ можно заменить на инварианты i_1', $i_2', \ldots, i_\mu'$ [28]:

$$i = i_1' I_1 + i_2' I_2 + \ldots i_\mu' I_\mu.$$

Все инварианты i_1', $i_2', \ldots, i_\mu'$ имеют по коэффициентам базисной формы меньшую степень, чем i. Они аналогичным образом могут быть заменены на линейные комбинации инвариантов I_1, $I_2, \ldots, I_\mu$, и эту процедуру можно продолжать до тех пор, пока не получатся инварианты степени меньше νr. Пусть j_1, $j_2, \ldots, j_w$ — полный набор линейно независимых инвариантов степени меньше νr [29]. Тогда для произвольного инварианта i базисной формы получается система w уравнений вида

$$\begin{aligned}
ij_1 &= G_1^{(1)} j_1 + G_2^{(1)} j_2 + \ldots + G_w^{(1)} j_w, \\
ij_2 &= G_1^{(2)} j_1 + G_2^{(2)} j_2 + \ldots + G_w^{(2)} j_w, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
ij_w &= G_1^{(w)} j_1 + G_2^{(w)} j_2 + \ldots + G_w^{(w)} j_w,
\end{aligned}$$

---

8) См. Math. Ann., Bd. 36, S. 527 [с. 60–61 настоящего издания. — *Ред.*].

где $G_1^{(1)}, G_2^{(1)}, \ldots, G_w^{(w)}$ — целые рациональные функции от инвариантов $I_1, \ldots, I_\mu$. Исключая $j_1, j_2, \ldots, j_w$, мы получаем уравнение

$$\begin{vmatrix} G_1^{(1)} - i & G_2^{(1)} & \ldots & G_w^{(1)} \\ G_1^{(2)} & G_2^{(2)} - i & \ldots & G_w^{(2)} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ G_1^{(w)} & G_2^{(w)} & \ldots & G_w^{(w)} - i \end{vmatrix} = 0,$$

показывающее, что i — целая алгебраическая функция от $I_1, \ldots, I_\mu$.

Теперь становится ясно, что для изучения инвариантов базисной формы особую важность представляет нахождение необходимых и достаточных условий обращения всех инвариантов этой базисной формы в нуль. Интерпретируя известным способом N коэффициентов базисной формы как координаты в $(N-1)$-мерном пространстве [30], мы приходим к задаче исследования алгебраического многообразия (Gebilde) Z в этом пространстве, определенного равенством нулю всех инвариантов. Обозначая, как и выше, через $\varkappa$ число алгебраически независимых инвариантов, мы получаем из предыдущих рассмотрений, что имеется в точности $\varkappa$ инвариантов $I_1, \ldots, I_\varkappa$, обращение которых в нуль полностью определяет алгебраическое многообразие Z. Из доказанного только что предложения следует, что $\mu \geqslant \varkappa$ [31], т. е. что невозможно определить многообразие Z обращением в нуль меньшего числа инвариантов.

§ 5. Обращение в нуль всех инвариантов бинарной базисной формы

Доказанное только что в § 4 предложение является ядром всей теории алгебраических инвариантов, которая будет здесь построена. Сначала мы применим его к теории бинарных форм; для них алгебраическое многообразие Z может быть найдено без особого труда, а именно:

Если все инварианты бинарной базисной формы порядка $n = 2h+1$ *или* $n = 2h$ *равны нулю, то эта базисная форма имеет линейный множитель кратности* $h+1$*; если, обратно, базисная форма имеет линейный множитель кратности* $h+1$*, то все ее инварианты равны нулю* [32].

Чтобы доказать первую часть этого предложения, построим из данной базисной формы

$$f = a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n$$

следующие трансвектанты (Überschiebungen) [33]:

$$F_1 = [a_0 a_2 - a_1^2]\, x_1^{2(n-2)} + \ldots,$$

$$F_2 = [a_0 a_4 - 4a_1 a_3 + 3a_2^2]\, x_1^{2(n-4)} + \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$F_h = \left[a_0 a_{2h} - \binom{2h}{1} a_1 a_{2h-1} + \ldots \pm \frac{1}{2}\binom{2h}{h} a_h^2\right] x_1^{2(n-2h)} + \ldots$$

Выпишем теперь условия того, чтобы формы f, $F_1, \ldots, F_h$ или соответственно f, $F_1, \ldots, F_{h-1}$ имели общий линейный множитель. Это можно сделать так. Пусть M — наименьшее общее кратное чисел n, $2(n-2)$, $2(n-4), \ldots$ $\ldots, 2(n-2h)$ и

$$M = mn = 2m_1(n-2) = \ldots = 2m_h(n-2h)$$

или соответственно

$$M = mn = 2m_1(n-2) = \ldots = 2m_{h-1}(n-2h+2),$$

в зависимости от того, является n нечетным или четным. Построим, далее, формы

$$U = uf^m + u_1 F_1^{m_1} + \ldots + u_h F_h^{m_h},$$
$$V = vf^m + v_1 F_1^{m_1} + \ldots + v_h F_h^{m_h}$$

или соответственно формы

$$U = uf^m + u_1 F_1^{m_1} + \ldots + u_{h-1} F_{h-1}^{m_{h-1}},$$
$$V = vf^m + v_1 F_1^{m_1} + \ldots + v_{h-1} F_{h-1}^{m_{h-1}},$$

где u, $u_1, \ldots, u_h$ и v, $v_1, \ldots, v_h$ — неопределенные параметры. Результантом этих двух форм U и V является форма

$$R(U, V) = J_1 P_1 + \ldots + J_\mu P_\mu,$$

где $P_1, \ldots, P_\mu$ — некоторые степени и произведения неопределенных параметров u, v, а $J_1, \ldots, J_\mu$ — инварианты базисной формы [34]. Уравнения

$$J_1 = 0, \quad \ldots, \quad J_\mu = 0$$

являются необходимыми и достаточными условиями для того, чтобы формы f, $F_1, \ldots, F_h$ или соответственно формы f, $F_1, \ldots, F_{h-1}$ имели в качестве общего множителя линейную форму. Действительно, если бы у них не было общего линейного множителя, то параметрам u, v можно было бы приписать такие численные значения, что две формы U, V не имели бы общего множителя, а это противоречит условию $R(U, V) = 0$.

Преобразуем теперь бинарную форму f с помощью подстановки

$$y_1 = \alpha_1 x_1 + \alpha_2 x_2,$$
$$y_2 = \beta_1 x_1 + \beta_2 x_2,$$

где $\beta_1 x_1 + \beta_2 x_2$ — общий линейный множитель, а α_1 и α_2 подобраны так, чтобы определитель $\alpha_1\beta_2 - \alpha_2\beta_1$ был отличен от нуля. Обозначим коэффициенты преобразованной формы g через b_0, $b_1, \ldots, b_n$. Поскольку преобразованная форма g и ее трансвектанты содержат множитель y_2, коэффициенты должны удовлетворять следующим уравнениям:

$$b_0 = 0,$$
$$b_0 b_2 - b_1^2 = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$b_0 b_{2h} - \binom{2h}{1} b_1 b_{2h-1} + \ldots \pm \frac{1}{2}\binom{2h}{h} b_h^2 = 0,$$

или соответственно уравнениям

$$b_0 = 0,$$

$$b_0 b_2 - b_1^2 = 0,$$

. . . . . .

$$b_0 b_{2h-2} - \binom{2h-2}{1} b_1 b_{2h-3} + \ldots \pm \frac{1}{2}\binom{2h-2}{h-1} b_{h-1}^2 = 0.$$

Если в случае четного n мы присоединим еще уравнение $F_h = 0$, то получим как для нечетного, так и для четного n уравнения

$$b_0 = 0, \quad b_1 = 0, \quad \ldots, \quad b_h = 0,$$

из которых следует, что форма g содержит множитель y_2 с кратностью по меньшей мере $h+1$. Конечно, в частных случаях вычисление условий, при которых формы f, $F_1, \ldots, F_h$ имеют общий множитель, может быть значительно сокращено.

Справедливость второй части нашего предложения непосредственно устанавливается с помощью такого преобразования базисной формы, чтобы первые $h+1$ коэффициентов b_0, $b_1, \ldots, b_h$ стали равны нулю. В самом деле, если e_{h+1}, $e_{h+2}, \ldots, e_n$ — произвольные положительные целые числа, то наиболее общий член, который можно образовать из оставшихся коэффициентов b_{h+1}, $b_{h+2}, \ldots, b_n$, имеет вид

$$b_{h+1}^{e_{h+1}} b_{h+2}^{e_{h+2}} \ldots b_n^{e_n}.$$

Но для такого члена удвоенный вес больше n-кратного порядка. Значит, каждый член инварианта должен содержать по меньшей мере один из коэффициентов b_0, $b_1, \ldots, b_h$ в качестве множителя и потому его значение на нашей специальной базисной форме равно нулю.

Эти инварианты $J_1, \ldots, J_\mu$ или соответственно $J_1, \ldots, J_\mu$, F_h образуют, как мы показали, такую систему инвариантов базисной формы f, что их обращение в нуль влечет за собой обращение в нуль всех инвариантов этой базисной формы, а поэтому *из доказанного в* § 4 *утверждения вытекает, что все инварианты базисной формы* f *являются целыми алгебраическими функциями этих найденных инвариантов. При вычислении этой системы инвариантов мы использовали лишь построение результантов* [35].

§ 6. Приложения к специальным бинарным базисным формам и системам базисных форм

Полученные до сих пор общие результаты могут быть, как показывают следующие примеры, прекрасно проверены во всех просчитанных частных случаях.

Для бинарной формы порядка 5 условия доказанного в § 4 утверждения выполнены для трех инвариантов A, B, C степеней 4, 8 и 12 соответственно [36]. Действительно, их одновременное обращение в нуль означает существование у f линейного множителя кратности 3, и, обратно, это условие в соответствии с доказанным в § 5 утверждением означает, что все инварианты этой бинарной формы равны нулю. Значит, все инварианты

должны быть *целыми* алгебраическими функциями от A, B, C; и на самом деле полная система содержит лишь один дополнительный инвариант, а именно, косой (schiefe) инвариант R, квадрат которого является целой рациональной функцией от A, B, C.

Бинарная форма порядка 6 имеет четыре инварианта A, B, C, D степеней 2, 4, 6, 10 соответственно, одновременное обращение в нуль которых влечет за собой наличие линейного множителя кратности 4. В свою очередь, это условие влечет за собой равенство нулю всех инвариантов. И действительно, в соответствии с доказанным в § 4 утверждением единственный остающийся косой инвариант R нашей базисной формы является *целой* алгебраической функцией от A, B, C, D, а именно квадратным корнем из целой рациональной функции от этих четырех инвариантов.

Рассмотрим далее бинарную базисную форму f порядка 5 и линейную базисную форму l. Если шесть их совместных инвариантов A, B, C, $(f, l^5)_5$, $(h, l^6)_6$, $(i, l^2)_2$, где $h = (f, f)_2$, а $i = (f, f)_4$ [37] обращаются одновременно в нуль, то либо линейная форма l является множителем кратности 3 формы f, либо f имеет некоторый множитель кратности 3, а все коэффициенты линейной формы l равны нулю, либо все коэффициенты формы f равны нулю. Легко видеть, что в каждом из этих трех случаев все совместные инварианты двух заданных базисных форм равны нулю, и поэтому обращение в нуль заданных шести совместных инвариантов влечет за собой обращение в нуль всех прочих совместных инвариантов. Согласно доказанному в § 4 утверждению, отсюда следует, что все совместные инварианты двух базисных форм f и l являются целыми алгебраическими функциями от этих шести данных инвариантов.

Поскольку совместные инварианты совпадают с системой инвариантов и ковариантов одной бинарной формы порядка 5, отсюда следует, что все 23 инвариантные формы бинарной базисной формы порядка 5 могут быть выражены в виде целых алгебраических функций от трех инвариантов A, B, C и трех ковариантов f, h, i. Если мы заметим теперь, что все инварианты и коварианты бинарной базисной формы порядка 5 являются рациональными функциями от f, h, i, $(f, h)_1$, $(f, h)_3$, то в соответствии с нашими общими результатами из разд. I получим, что известная система 23 инвариантов может быть построена только с помощью этих данных. Для этого нужно лишь найти все такие функции, которые одновременно являются *целыми* алгебраическими функциями от A, B, C, f, h, i и рациональными функциями от ковариантов f, h, i, $(f, h)_1$, $(f, h)_3$.

Чтобы найти совместные инварианты двух бинарных кубических форм f, g, рассмотрим их линейную комбинацию $\varkappa f + \lambda g$ и разложим дискриминант этой формы по неопределенным параметрам $\varkappa$ и λ:

$$D(\varkappa f + \lambda g) = D_0\varkappa^4 + D_1\varkappa^3\lambda + D_2\varkappa^2\lambda^2 + D_3\varkappa\lambda^3 + D_4\lambda^4.$$

Очевидно, что пять инвариантов D_0, D_1, D_2, D_3, D_4 обращаются в нуль одновременно лишь в том случае, когда кубические формы f и g имеют общий линейный множитель кратности 2 для каждой из них, и, в свою очередь, это условие влечет за собой равенство нулю всех совместных инвариантов. Из нашего предложения следует, что все совместные инварианты пары кубических форм f и g являются целыми алгебраическими функциями от D_0, D_1, D_2, D_3, D_4. Далее, полная система инвариантов содержит, помимо этих

пяти инвариантов. лишь два дополнительных инварианта, а именно, трансвектант $(f,g)_3$ и результант R этих двух форм, и вычисления показывают, что, действительно, эти два инварианта являются целыми алгебраическими функциями от указанных пяти инвариантов.

Чтобы исследовать совместные инварианты системы, состоящей из кубической формы f, квадратичной формы g и линейной формы l, обозначим через d_1 и d_2 дискриминанты форм f и g соответственно, а через r их результант, и образуем также инварианты $(f,l^3)_3$, $(h,l^2)_2$, $(g,l^2)_2$ и $(h,g)_2$, где h — ковариант Гессе для f. Если эти семь совместных инвариантов одновременно обращаются в нуль, то, как легко показать, соответствующие три базисные формы должны иметь вид

$$f = cp^2q, \quad g = c'p^2, \quad l = c''p,$$

где p, q — линейные формы, а c, c', c'' — константы. Поскольку все совместные инварианты этой системы, очевидно, обращаются на этих специальных базисных формах в нуль, то ввиду доказанного в § 4 предложения все совместные инварианты указанных трех базисных форм являются целыми алгебраическими функциями описанных семи совместных инвариантов, или, что то же самое, все совместные инварианты и ковариантны кубической формы f и квадратичной формы g являются целыми алгебраическими функциями от четырех инвариантов d_1, d_2, r, $(h,g)_2$ и трех форм f, h, g.

В заключение рассмотрим более общий пример, а именно систему ν бинарных линейных форм

$$l_1 = a_1x + b_1y, \quad l_2 = a_2x + b_2y, \quad \ldots, \quad l_\nu = a_\nu x + b_\nu y.$$

Полная система инвариантов состоит из определителей

$$p_{ik} = a_ib_k - a_kb_i \qquad (i,k = 1,2,\ldots,\nu).$$

Построим две бинарные формы порядка $\nu - 1$

$$\varphi = a_1\xi^{\nu-1} + a_2\xi^{\nu-2}\eta + \ldots + a_\nu\eta^{\nu-1},$$

$$\psi = b_1\xi^{\nu-1} + b_2\xi^{\nu-2}\eta + \ldots + b_\nu\eta^{\nu-1}$$

и вычислим их функциональный определитель:

$$(\varphi,\psi)_1 = p_0\xi^{2\nu-4} + p_1\xi^{2\nu-5}\eta + \ldots + p_{2\nu-4}\eta^{2\nu-4}.$$

Поскольку коэффициенты p_0, $p_1,\ldots,p_{2\nu-4}$ являются линейными комбинациями определителей p_{ik}, они также являются инвариантами базисных линейных форм, и легко видеть, что если все эти инварианты p_0, $p_1,\ldots,p_{2\nu-4}$ обращаются в нуль, то либо все коэффициенты формы φ обращаются в нуль, либо все коэффициенты формы ψ обращаются в нуль, либо же эти две формы совпадают друг с другом с точностью до числового множителя. Во всех этих случаях все определители p_{ik} равны нулю, а ввиду нашего предложения отсюда следует, что определители p_{ik} являются целыми алгебраическими функциями от p_0, $p_1,\ldots,p_{2\nu-4}$[9], откуда мы в то же время получаем, что последние $2\nu - 3$ инвариантов независимы.

---

[9] Совершенно другим способом этот результат был получен мною в работе: Über Büschel von binären Formen mit vorgeschriebener Funktionaldeterminante. — Math. Ann., Bd. 33, S. 233.

§ 7. Системы базисных форм

Чтобы распространить полученные в § 5 для бинарной базисной формы результаты на систему бинарных базисных форм, мы поступим следующим образом. Рассмотрим пару бинарных форм одинакового порядка n

$$f = a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n,$$

$$g = b_0 x_1^n + \binom{n}{1} b_1 x_1^{n-1} x_2 + \ldots + b_n x_2^n$$

и образуем их линейную комбинацию $\lambda f + \mu g$, где λ и μ — два параметра. Если теперь инварианты формы $\lambda f + \mu g$ обращаются в нуль для всех значений λ и μ, то, согласно доказанному в § 5 предложению, форма $\lambda f + \mu g$ должна иметь для всех значений параметров λ и μ линейный множитель кратности $n/2+1$ или $(n+1)/2$. Отсюда легко следует, что сами формы f и g должны содержать ту же самую линейную форму в качестве множителя кратности $n/2+1$ или $(n+1)/2$; обратно, это условие влечет за собой равенство нулю всех совместных инвариантов пары форм f и g. Таким образом, имеет место следующий результат:

Если $J_1, \ldots, J_\mu$ — инварианты базисной формы f, через которые все инварианты этой базисной формы могут быть выражены в виде целых алгебраических функций, то последовательное применение к этим инвариантам процесса Аронгольда

$$b_0 \frac{\partial}{\partial a_0} + b_1 \frac{\partial}{\partial a_1} + \ldots + b_n \frac{\partial}{\partial a_n}$$

приводит к системе совместных инвариантов, обладающей тем свойством, что каждый совместный инвариант пары форм f и g является целой алгебраической функцией совместных инвариантов из этой системы.

Это предложение обнаруживает новое фундаментальное свойство процесса Аронгольда.

Частный случай $n = 3$ был уже разобран выше. В случае двух биквадратичных базисных форм мы должны рассмотреть два инварианта i и j и положить

$$i(\lambda f + \mu g) = i_0 \lambda^2 + i_1 \lambda\mu + i_2 \mu^2,$$

$$j(\lambda f + \mu g) = j_0 \lambda^3 + j_1 \lambda^2\mu + j_2 \lambda\mu^2 + j_3 \mu^3.$$

Тогда по тем же причинам, что и выше, каждый совместный инвариант пары форм f и g является целой алгебраической функцией от семи инвариантов i_0, i_1, i_2, j_0, j_1, j_2, j_3, и эти семь совместных инвариантов алгебраически независимы, поскольку число $\varkappa$ для данной системы базисных форм равно семи.

Заменяя бинарную форму g на n-ю степень линейной формы, получаем следующий результат:

Применяя последовательно к инвариантам $J_1, \ldots, J_\mu$ бинарной базисной формы f процесс

$$x_2^n \frac{\partial}{\partial a_0} - x_1 x_2^{n-1} \frac{\partial}{\partial a_1} + \ldots \pm x_1^n \frac{\partial}{\partial a_n},$$

мы получим систему ковариантов, обладающую тем свойством, что все коварианты базисной формы f являются целыми алгебраическими функциями от ковариантов из полученной системы и инвариантов $J_1, \ldots, J_\mu$.

Например, применяя этот процесс в случае бинарной кубической базисной формы f к ее дискриминанту два раза, мы получаем два коварианта $t = (f,h)_1$ и f^2; и действительно, ковариант Гессе $h = (f,f)_2$ является целой алгебраической функцией от D, t и f, поскольку его третья степень есть целая рациональная функция от этих инвариантов. Если, далее, мы применим этот процесс к инвариантам i и j биквадратичной бинарной формы f, то получим коварианты f и $h = (f,f)_2$; и действительно, квадрат единственного остающегося коварианта $t = (f,h)_1$ является целой рациональной функцией от i, j, f и h.

Все эти рассмотрения можно легко перенести на теорию комбинантов двух или более бинарных базисных форм. Таким способом устанавливается, что комбинанты пары форм f и g одновременно все обращаются в нуль тогда и только тогда, когда в семействе $\lambda f + \mu g$ содержатся две формы, одна из которых имеет линейный множитель кратности r, а другая содержит тот же самый множитель с кратностью $n + 1 - r$. Отсюда вытекает такое утверждение:

Каждый комбинант двух бинарных форм f и g является целой алгебраической функцией от инвариантов их функционального определителя $(f,g)_1$.

Предыдущие исследования могут быть распространены и на теорию форм от многих переменных; при этом следует позаботиться только об описании особенностей тех форм, на которых все инварианты обращаются в нуль. Например, в случае тернарных форм порядка 3 условие обращения в нуль всех инвариантов состоит в том, что кривая, определенная равенством нулю соответствующей формы, имеет точку возврата (Rückkehrpunkt). Если мы возьмем теперь линейную комбинацию пары тернарных кубических форм и два инварианта

$$S(\lambda f + \mu g) = S_0\lambda^4 + \ldots + S_4\mu^4,$$

$$T(\lambda f + \mu g) = T_0\lambda^6 + \ldots + T_6\mu^6,$$

то аналогичные предыдущим соображения показывают, что все совместные инварианты пары форм f и g являются целыми алгебраическими функциями от 12 инвариантов $S_0, \ldots, S_4$, $T_0, \ldots, T_6$, и, поскольку число $\varkappa$ равно 12, мы видим, что эти 12 инвариантов алгебраически независимы.

С помощью вычислений подобным же образом могут быть исследованы тернарные биквадратичные формы, но высшие случаи требуют новых и более общих методов[10].

---

[10] См. разд. IV и V этой работы.

III. СТЕПЕНЬ ПОЛЯ ИНВАРИАНТОВ

§ 8. Представление асимптотического значения числа $\varphi(\sigma)$

В § 2 была определена система инвариантов $J, J_1, \ldots, J_\varkappa$, обладающая тем свойством, что все инварианты базисной формы могут быть представлены как целые алгебраические функции от $J_1, \ldots, J_\varkappa$ и рациональные функции от $J, J_1, \ldots, J_\varkappa$.

Неприводимое уравнение, которому удовлетворяет J, имеет вид

$$J^k + G_1 J^{k-1} + G_2 J^{k-2} + \ldots + G_k = 0,$$

где $G_1, G_2, \ldots, G_k$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$. Степень k этого уравнения является вместе с тем и степенью поля инвариантов [38].

Чтобы определить величину k для бинарной базисной формы f порядка n, рассмотрим число $\varphi(\sigma)$ тех инвариантов базисной формы f, степени которых по коэффициентам базисной формы не превосходят σ и между которыми нет линейных соотношений с постоянными коэффициентами [39]. Это число $\varphi(\sigma)$ может быть вычислено двумя различными способами, и сравнение двух соответствующих результатов для предельного значения $\sigma = \infty$ дает интересующее нас значение k.

В § 2 каждый инвариант i был представлен в виде

$$i = \frac{\Gamma_1 J^{k-1} + \Gamma_2 J^{k-2} + \ldots + \Gamma_k}{D},$$

где $\Gamma_1, \ldots, \Gamma_k$, D — целые рациональные функции от $J_1, \ldots, J_\varkappa$. Мы можем получить из этого представления верхнюю и нижнюю границы для числа $\varphi(\sigma)$. А именно, если мы заметим, что в рассматриваемом случае число $\varkappa$ равно $n-2$ [40], и обозначим через ν, $\nu_1, \ldots, \nu_{n-2}$, δ степени инвариантов J, $J_1, \ldots, J_{n-2}$, D, а через $\lambda(\sigma)$ число систем целых положительных чисел $\xi_1, \xi_2, \ldots, \xi_{n-2}$, удовлетворяющих неравенству

$$\nu_1\xi_1 + \nu_2\xi_2 + \ldots + \nu_{n-2}\xi_{n-2} \leqslant \sigma,$$

то легко найдем, что [41]

$$\lambda(\sigma) + \lambda(\sigma - \nu) + \lambda(\sigma - 2\nu) + \ldots + \lambda(\sigma - [k-1]\nu) \leqslant \varphi(\sigma),$$

$$\varphi(\sigma) \leqslant \lambda(\sigma + \delta) + \lambda(\sigma + \delta - \nu) + \lambda(\sigma + \delta - 2\nu) + \ldots + \lambda(\sigma + \delta - [k-1]\nu).$$

Далее [42], для числа $\lambda(\sigma)$ имеется формула

$$\lim_{\sigma\to\infty} \frac{\lambda(\sigma)}{\sigma^{n-2}} = \frac{1}{(n-2)!} \frac{1}{\nu_1\nu_2 \ldots \nu_{n-2}},$$

и, значит, из предыдущих неравенств вытекает, что

$$\lim_{\sigma\to\infty} \frac{\varphi(\sigma)}{\sigma^{n-2}} = \frac{1}{(n-2)!} \frac{1}{\nu_1\nu_2 \ldots \nu_{n-2}}.$$

§ 9. Вычисление степени k поля инвариантов для бинарной базисной формы порядка n

Этот предел можно определить другим способом, а именно с помощью методов, использованных Кэли и Сильвестром для подсчета инвариантов данной степени. Известно, что число линейно независимых инвариантов степени σ относительно коэффициентов бинарной базисной формы порядка n равно коэффициенту при $r^{n\sigma/2}$ в разложении выражения[11)]

$$f(r) = \frac{(1-r^{\sigma+1})(1-r^{\sigma+2})\dots(1-r^{\sigma+n})}{(1-r^2)(1-r^3)\dots(1-r^n)}.$$

Это выражение может быть представлено в виде

$$f(r) = f_0(r) + r^\sigma f_1(r) + r^{2\sigma} f_2(r) + \dots + r^{n\sigma} f_n(r),$$

где $f_0(r)$, $f_1(r), \dots, f_n(r)$ — рациональные функции от r, определенные тождеством

$$u^n f_0 + u^{n-1} f_1 + \dots + f_n = \frac{(u-r)(u-r^2)\dots(u-r^n)}{(1-r^2)(1-r^3)\dots(1-r^n)}.$$

Чтобы осуществить подсчет, следует разделить случаи нечетного и четного n.

Пусть сначала n будет нечетным. Поскольку в этом случае имеются лишь инварианты четной степени, мы получим, очевидно, искомое число $\varphi(\sigma)$, определив коэффициенты

при r^n в выражении $f_0 + r^2 f_1 + r^4 f_2 + \dots$,

при r^{2n} в выражении $f_0 + r^4 f_1 + r^8 f_2 + \dots$,

. . . . . .

при $r^{(\sigma/2)n}$ в выражении $f_0 + r^\sigma f_1 + r^{2\sigma} f_2 + \dots$,

а затем образовав сумму этих коэффициентов, или, что то же самое, сложив коэффициенты

при $r^n, r^{2n}, r^{3n}, \dots, r^{(\sigma/2)n}$ в f_0,

при $r^{n-2}, r^{2(n-2)}, r^{3(n-2)}, \dots, r^{(\sigma/2)(n-2)}$ в f_1,

при $r^{n-4}, r^{2(n-4)}, r^{3(n-4)}, \dots, r^{(\sigma/2)(n-4)}$ в f_2,

. . . . . .

при $r, r^2, r^3, \dots, r^{(\sigma/2)}$ в $f_{(n-1)/2}$,

Если ε_n — примитивный корень n-й степени из единицы, то мы видим, что сумма коэффициентов при $r^n, r^{2n}, r^{3n}, \dots, r^{(\sigma/2)n}$ в f_0 равна n-й части суммы первых $(\sigma/2)n$ коэффициентов в разложении выражения

$$f_0'(r) = f_0(r) + f_0(\varepsilon_n r) + f_0(\varepsilon_n^2 r) + \dots + f_0(\varepsilon_n^{n-1} r).$$

---

11) См. *Faà di Bruno*. Theorie der binären Formen. — Leipzig, 1881, S. 194.

Если ε_{n-2} — примитивный корень $(n-2)$-й степени из единицы, то сумма соответствующих коэффициентов в f_1 равна $(n-2)$-й части суммы первых $(\sigma/2)(n-2)$ коэффициентов в разложении выражения

$$f_1'(r) = f_1(r) + f_1(\varepsilon_{n-2}r) + f_1(\varepsilon_{n-2}^2 r) + \ldots + f_1(\varepsilon_{n-2}^{n-3} r).$$

Наконец, положим

$$f'_{(n-1)/2}(r) = f_{(n-1)/2}(r).$$

Теперь, заменяя r в f_0', $f_1', \ldots, f'_{(n-1)/2}$ соответственно на величины

$$t^{1\cdot 3\cdot 5\cdot \ldots \cdot n/n}, \quad t^{1\cdot 3\cdot 5\cdot \ldots \cdot n/(n-2)}, \quad \ldots, \quad t^{1\cdot 3\cdot 5\cdot \ldots \cdot n},$$

мы видим, что искомое число $\varphi(\sigma)$ равно сумме первых $(\sigma/2)\cdot 1\cdot 3\cdot 5\cdot \ldots \cdot n$ коэффициентов в разложении выражения

$$h(t) = \frac{1}{n} f_0'\left(t^{1\cdot 3\cdot 5\cdot \ldots \cdot n/n}\right) + \frac{1}{n-2} f_1'\left(t^{1\cdot 3\cdot 5\cdot \ldots \cdot n/(n-2)}\right) + \ldots + f'_{(n-1)/2}\left(t^{1\cdot 3\cdot 5\cdot \ldots \cdot n}\right).$$

Из одного хорошо известного результата Абеля легко выводится следующий факт.

Если коэффициенты степенного ряда

$$\mathfrak{P} = a_0 + a_1 t + a_2 t^2 + \ldots$$

обладают тем свойством, что для некоторого целого числа $\varkappa$ выражение

$$\frac{a_0 + a_1 + a_2 + \ldots + a_\rho}{\rho^\varkappa}$$

сходится к конечному пределу при неограниченном увеличении ρ, то этот предел равен

$$\frac{1}{\varkappa!} \lim_{t\to 1} \left[(1-t)^\varkappa \mathfrak{P}(t)\right].$$

Используя это утверждение, получаем

$$\lim_{\sigma\to\infty} \frac{\varphi(\sigma)}{\left(\frac{\sigma}{2} 1\cdot 3\cdot 5\cdot \ldots \cdot n\right)^{n-2}} = \frac{1}{(n-2)!} \lim_{t\to 1} \left[(1-t)^{n-2} h(t)\right].$$

Теперь, если $n > 3$, можно положить

$$h(t) = \frac{1}{n} f_0\left(t^{1\cdot 3\cdot 5\cdot \ldots \cdot n/n}\right) + \frac{1}{n-2} f_1\left(t^{1\cdot 3\cdot 5\cdot \ldots \cdot n/(n-2)}\right) + \ldots$$
$$\ldots + f_{(n-1)/2}\left(t^{1\cdot 3\cdot 5\cdot \ldots \cdot n}\right) + h'(t),$$

где $h'(t)$ — такая рациональная функция от t, что выражение $(1-t)^{n-2}h'(t)$ является бесконечно малой величиной при стремлении t к 1. Далее, для любого индекса i

$$(1-t)^{n-1} f_i(r) = \frac{g_i(r)}{\left[2\cdot \frac{1\cdot 3\cdot 5\cdot \ldots \cdot n}{n-2i}\right]\left[3\cdot \frac{1\cdot 3\cdot 5\cdot \ldots \cdot n}{n-2i}\right]\ldots\left[n\cdot \frac{1\cdot 3\cdot 5\cdot \ldots \cdot n}{n-2i}\right]},$$

где

$$[M] = 1 + t + t^2 + \ldots + t^{M-1},$$

а $g_i(r)$ — рациональные функции от r, определенные тождеством

$$(u-r)(u-r^2)\dots(u-r^n)=g_0(r)u^n+g_1(r)u^{n-1}+\dots+g_n(r).$$

Теперь с помощью простого вычисления мы приходим к формуле

$$\lim_{t\to 1}[(1-t)^{n-2}h(t)]=$$
$$=\sum\frac{1}{n-2i}\,\frac{g_i(1)\left[\dfrac{dN(t)}{dt}\right]_{t=1}-\left[\dfrac{dg_i(r)}{dr}\right]_{r=1}\dfrac{1\cdot 3\cdot 5\cdot\dots\cdot n}{n-2i}N(1)}{N^2(1)},$$

где сумма берется по всем $i=0,\ 1,\ 2,\dots,(n-1)/2$ и где

$$N(t)=\left[2\cdot\frac{1\cdot 3\cdot 5\cdot\dots\cdot n}{n-2i}\right]\left[3\cdot\frac{1\cdot 3\cdot 5\cdot\dots\cdot n}{n-2i}\right]\dots\left[n\cdot\frac{1\cdot 3\cdot 5\cdot\dots\cdot n}{n-2i}\right].$$

Переписывая сумму, стоящую справа, получаем

$$\lim_{t\to 1}[(1-t)^{n-2}h(t)]=-\frac{1}{2\cdot n!\,(1\cdot 3\cdot 5\cdot\dots\cdot n)^{n-2}}\sum(-1)^i\binom{n}{i}(n-2i)^{n-3},$$

где сумма снова берется по $i=0,\ 1,\ 2,\dots,(n-1)/2$.

Сравнивая это с формулой, полученной в конце § 8, мы приходим к следующему *результату*[12]:

$$\frac{k}{\nu_1\nu_2\dots\nu_{n-2}}=-\frac{1}{4}\frac{1}{n!}\sum_i(-1)^i\binom{n}{i}\left(\frac{n}{2}-i\right)^{n-3}\qquad(i=0,1,\dots,(n-1)/2).$$

Эту формулу для степени k поля инвариантов легко проверить в случае бинарной базисной формы порядка 5. В самом деле, поскольку степени инвариантов A, B, C равны, соответственно 4, 8, 12, то мы полагаем $\nu_1=4$, $\nu_2=8$, $\nu_3=12$, что дает $k=2$. И действительно, косой инвариант R удовлетворяет уравнению степени 2, а поле инвариантов полностью определяется этими четырьмя инвариантами A, B, C, R.

Пусть теперь порядок n четен. Как и выше, мы получаем искомое число, складывая коэффициенты

при $r^0, r^{1(n/2)}, r^{2(n/2)}, r^{3(n/2)}, \dots, r^{\sigma(n/2)}$ в f_0,

при $r^0, r^{1(n/2-1)}, r^{2(n/2-1)}, r^{3(n/2-1)}, \dots, r^{\sigma(n/2-1)}$ в f_1,

при $r^0, r^{1(n/2-2)}, r^{2(n/2-2)}, r^{3(n/2-2)}, \dots, r^{\sigma(n/2-2)}$ в f_2,

. . . . . .

при $r^0, r^1, r^2, r^3, \dots, r^\sigma$ в $f_{n/2-1}$,

Используя примитивные корни из единицы $\varepsilon_{n/2}$, $\varepsilon_{n/2-1},\dots$ порядков $n/2$, $n/2-1,\dots$ мы, как и выше, получаем функции f_0', $f_1',\dots,f_{n/2-1}'$. Заменяя параметр r в этих функциях на

$$t^{(n/2)!/(n/2)},\quad t^{(n/2)!/(n/2-1)},\quad \dots,\quad t^{(n/2)!},$$

[12] Эту формулу и соответствующую формулу для четного n я уже приводил в докладе на Обществе естествоиспытателей и медиков в Халле в 1891 г.; см. Jahresbericht der deutschen Mathematiker-Vereinigung, 1892, S. 62.

мы видим, что искомое число $\varphi(\sigma)$ равно сумме первых $\sigma(n/2)!$ коэффициентов в разложении

$$h(t) = \frac{1}{n/2} f_0'\left(t^{(n/2)!/(n/2)}\right) + \frac{1}{n/2-1} f_1'\left(t^{(n/2)!/(n/2-1)}\right) + \ldots + f_{n/2-1}'(t^{(n/2)!}).$$

С помощью тех же соображений, что и выше, отсюда получается, что

$$\lim_{\sigma\to\infty} \frac{\varphi(\sigma)}{(\sigma(n/2)!)^{n-2}} = \frac{1}{(n-2)!} \lim_{t\to 1}[(1-t)^{n-2}h(t)].$$

Теперь при $n > 4$ можно положить

$$h(t) = \frac{1}{n/2} f_0\left(t^{(n/2)!/(n/2)}\right) + \frac{1}{n/2-1} f_1\left(t^{(n/2)!/(n/2-1)}\right) + \ldots$$
$$\ldots + f_{n/2-1}(t^{(n/2)!}) + h'(t),$$

где $h'(t)$ — такая рациональная функция от t, что выражение $(1-t)^{n-2}h'(t)$ является бесконечно малым при t, стремящемся к 1. Далее, используя введенную выше сокращенную запись, мы имеем для любого индекса i

$$(1-t)^{n-1} f_i(r) = \frac{g_i(r)}{\left[2\cdot\frac{(n/2)!}{n/2-i}\right]\left[3\cdot\frac{(n/2)!}{n/2-i}\right]\ldots\left[n\cdot\frac{(n/2)!}{n/2-i}\right]}.$$

Обозначая знаменатель правой части через $N(t)$, получаем

$$\lim_{t\to 1}[(1-t)^{n-2}h(t)] =$$
$$= \sum \frac{1}{n-2i} \frac{g_i(1)\left[\frac{dN(t)}{dt}\right]_{t=1} - \left[\frac{dg_i(r)}{dr}\right]_{r=1} \frac{(n/2)!}{n/2-i} N(1)}{N^2(1)} =$$
$$= -\frac{1}{2\cdot n!\left((n/2)!\right)^{n-2}} \sum (-1)^i \binom{n}{i} \left(\frac{n}{2}-i\right)^{n-3},$$

где сумма берется по $i = 0, 1, 2, \ldots, n/2-1$.

Сравнение этого соотношения с формулой, полученной в конце § 8, дает следующий *результат*:

$$\frac{k}{\nu_1\nu_2\ldots\nu_{n-2}} = -\frac{1}{2}\frac{1}{n!}\sum_i (-1)^i \binom{n}{i}\left(\frac{n}{2}-i\right)^{n-3} \quad (i = 0, 1, \ldots, n/2-1).$$

Эту формулу легко проверить в случае бинарной базисной формы порядка 6. Поскольку четыре ее инварианта A, B, C, D имеют степени 2, 4, 6, 10 соответственно, мы должны положить $\nu_1 = 2$, $\nu_2 = 4$, $\nu_3 = 6$, $\nu_4 = 10$, что дает $k = 2$. И действительно, косой инвариант R удовлетворяет уравнению степени 2, а поле инвариантов полностью определяется этими пятью инвариантами.

§ 10. Типичное представление бинарной базисной формы

Использованные в §§ 8 и 9 методы обеспечивают новое доказательство возможности типичного представления бинарной базисной формы [43].

Чтобы показать это, допустим *сначала*, что порядок n бинарной базисной формы нечетен. Тогда все линейные ковариванты базисной формы имеют нечетную степень по ее коэффициентам; пусть $\varphi_1(\sigma)$ — число таких линейных ковариантов, степень которых по коэффициентам базисной формы не превосходит σ и которые не связаны линейными соотношениями с постоянными коэффициентами. Для нахождения типичного представления базисной формы нужны два линейных ковариванта l и m, не связанные никаким соотношением вида

$$A\,l + B\,m = 0,$$

где A и B — соответствующим образом подобранные инварианты. Существование таких двух ковариантов может быть установлено так. Если бы у рассматриваемой базисной формы не было линейных ковариантов, то $\varphi_1(\sigma)$ было бы равно нулю для всех σ. С другой стороны, если бы нашелся такой ковариант l, что все прочие ковариванты базисной формы имеют вид $A\,l$, где A — инвариант, то имелось бы соотношение

$$\varphi_1(\sigma) = \varphi(\sigma - \lambda),$$

где λ — степень ковариванта l, и, значит,

$$\lim_{\sigma\to\infty} \frac{\varphi_1(\sigma)}{\varphi(\sigma)} = 1.$$

Наконец, если мы предположим, что существуют два линейных ковариванта l и m с требующимся свойством, и обозначим оставшиеся линейные ковариванты из полной системы форм через $p_1, p_2, \ldots, p_r$, то каждый из этих ковариантов может быть представлен в виде

$$p_i = \frac{A_i\,l + B_i\,m}{C_i},$$

где A_i, B_i, C_i — инварианты, и, значит, каждый линейный ковариант p может быть представлен в виде

$$p = \frac{A\,l + B\,m}{C_1 C_2 \ldots C_r}.$$

Если мы обозначим теперь степень линейного ковариванта m через μ, а степень инварианта $C_1 C_2 \ldots C_r$ через γ, то получим для $\varphi_1(\sigma)$ неравенство

$$\varphi(\sigma - \lambda) + \varphi(\sigma - \mu) \leqslant \varphi_1(\sigma) \leqslant \varphi(\sigma - \lambda + \gamma) + \varphi(\sigma - \mu + \gamma),$$

и, значит,

$$\lim_{\sigma\to\infty} \frac{\varphi_1(\sigma)}{\varphi(\sigma)} = 2.$$

Чтобы определить теперь, чему же в действительности равно число $\lim\limits_{\sigma\to\infty} (\varphi_1(\sigma)/\varphi(\sigma))$, мы снова воспользуемся перечислительной теоремой Кэли — Сильвестра. В соответствии с ней число линейных ковариантов степени σ равно коэффициенту при $r^{(n\sigma-1)/2}$ в разложении f; следовательно,

мы получаем интересующее нас число $\varphi_1(\sigma)$, складывая коэффициенты

при $r^{(n-1)/2}$, $r^{(3n-1)/2}$, $r^{(5n-1)/2}$, ..., $r^{(\sigma n-1)/2}$ в f_0,

при $r^{(n-1)/2-1}$, $r^{(3n-1)/2-3}$, $r^{(5n-1)/2-5}$, ..., $r^{(\sigma n-1)/2-\sigma}$ в f_1,

при $r^{(n-1)/2-2}$, $r^{(3n-1)/2-6}$, $r^{(5n-1)/2-10}$, ..., $r^{(\sigma n-1)/2-2\sigma}$ в f_2,

. . . . . .

при r^0, r^1, r^2, ..., $r^{(\sigma-1)/2}$ в $f_{(n-1)/2}$.

Если $n > 3$, это вычисление дает для $\lim\limits_{\sigma\to\infty}(\varphi_1(\sigma)/\varphi(\sigma))$ значение 2, что и завершает доказательство.

Теперь предположим, что порядок n четен, и пусть $\varphi_2(\sigma)$ — число квадратичных ковариантов, степени которых по коэффициентам базисной формы не превосходят σ и между которыми нет линейных соотношений с постоянными коэффициентами.

Чтобы найти типичное представление базисной формы, нужны три квадратичных коварианта l, m, p, между которыми нет соотношений вида

$$A\,l + B\,m + C\,p = 0,$$

где A, B, C — инварианты. С помощью таких же, как и выше, рассуждений мы получаем, что три таких коварианта найдутся, если предел частного $\varphi_2(\sigma)/\varphi(\sigma)$ при $\sigma \to \infty$ равен 3. Но это действительно так при $n > 4$, как показывают вычисления, подобные предыдущим.

До сих пор результаты настоящего разд. III получались с помощью чисто арифметических средств и лишь в начале § 8 мы использовали известный алгебраический факт, что число $\varkappa$ алгебраически независимых инвариантов бинарной базисной формы порядка n равно $n-2$ [44]. Однако даже этот факт может быть установлен нашими методами, и мы теперь это вкратце покажем.

Как показывают рассмотрения § 8, частное $\varphi(\sigma)/\sigma^{\varkappa}$ имеет конечный ненулевой предел при $\sigma \to \infty$. В § 9 мы показали, что выражение $\lim\limits_{\sigma\to\infty}(\varphi(\sigma)/\sigma^{n-2})$ отличается лишь ненулевым числовым множителем от суммы

$$\sum_i (-1)^i \binom{n}{i} \left(\frac{n}{2} - i\right)^{n-3} \quad (i = 0, 1, \ldots, (n-1)/2) \text{ или } n/2 - 1).$$

Отсюда следует, что $\varkappa = n-2$, если только доказать, что указанная сумма отлична от нуля. Чтобы показать это, определим число ковариантов l, $m, \ldots, p$, имеющих порядок ν по переменным и не связанных никаким линейным соотношением вида

$$A\,l + B\,m + \ldots + E\,p = 0,$$

где A, $B, \ldots, E$ — инварианты. Мы получаем, что это число равно $\lim\limits_{\sigma\to\infty}(\varphi_\nu(\sigma)/\varphi(\sigma))$, где $\varphi_\nu(\sigma)$ — число ковариантов, имеющих порядок ν по переменным и степень, не превосходящую σ, по коэффициентам базисной формы, между которыми нет линейных соотношений с постоянными коэффициентами. Если мы подсчитаем, как и выше для $\nu = 1$ и $\nu = 2$, этот предел с помощью перечислительной теоремы Кэли — Сильвестра, то полу-

чим выражение, снова содержащее сумму

$$\sum_i (-1)^i \binom{n}{i} \left(\frac{n}{2} - i\right)^{n-3}.$$

Если мы заменим в этом выражении указанную сумму нулем и придадим затем ν достаточно большое значение, то, как показывает вычисление, значение полученного выражения будет больше $\nu+1$, а это противоречит тому факту, что число ковариантов l, $m, \ldots, p$ порядка ν по переменным не превосходит $\nu+1$. Поэтому предположение о том, что указанная сумма равна нулю, невозможно, и *доказательство закончено.*

Используя типичное представление бинарной базисной формы, А. Клебш доказал следующее предложение[13]:

Если для двух данных бинарных форм порядка $n > 4$ с числовыми коэффициентами все соответствующие инварианты принимают одно и то же значение и если инвариант N в знаменателе типично представленных коэффициентов отличен от нуля, то эти две формы принадлежат к одному и тому же классу.

Под утверждением, что две бинарные формы принадлежат к одному классу, мы понимаем следующее: одна из них может быть преобразована в другую с помощью линейной подстановки с ненулевым определителем [45]. Далее, если мы выберем значения инвариантов $J_1, \ldots, J_{n-2}$ таким образом, чтобы дискриминант D уравнения для J был отличен от нуля, то k равно числу значений инварианта J, совместимых с выбранными значениями $J_1, \ldots, J_{n-2}$, откуда вытекает такое утверждение:

Степень k поля инвариантов в общем случае равна числу различных классов бинарных форм, для которых инварианты $J_1, \ldots, J_{n-2}$ равны заданным величинам [46].

§ 11. Система ν линейных бинарных форм

Методы разд. III могут быть применены к совместным инвариантам бинарных базисных форм. Мы рассмотрим в качестве простейшего примера систему ν линейных бинарных форм

$$a_1 x + b_1 y, \quad a_2 x + b_2 y, \quad \ldots, \quad a_\nu x + b_\nu y,$$

которая уже рассматривалась в § 6. Полная система инвариантов состоит из определителей p_{ik}. Кроме того, каждый из этих инвариантов удовлетворяет дифференциальному уравнению

$$a_1 \frac{\partial J}{\partial b_1} + a_2 \frac{\partial J}{\partial b_2} + \ldots + a_\nu \frac{\partial J}{\partial b_\nu} = 0;$$

обратно, каждая функция J вида

$$J = \sum C a_1^{r_1} a_2^{r_2} \ldots a_\nu^{r_\nu} b_1^{s_1} b_2^{s_2} \ldots b_\nu^{s_\nu},$$

$$r_1 + r_2 + \ldots + r_\nu = s_1 + s_2 + \ldots + s_\nu = \rho,$$

---

[13] *Clebsch A.* Theorie der binaren Formen. 1872.

удовлетворяющая этому дифференциальному уравнению, является инвариантом веса ρ указанных линейных форм. Отсюда можно извлечь доказательство того, что число инвариантов веса ρ, не связанных линейными соотношениями с постоянными коэффициентами, равно

$$\chi(\rho) = [\psi(\rho)]^2 - \psi(\rho-1)\psi(\rho+1),$$

где $\psi(\rho)$ — число целых положительных решений уравнения

$$r_1 + r_2 + \ldots + r_\nu = \rho,$$

которое равно $\dfrac{(\rho+\nu-1)!}{\rho!(\nu-1)!}$. Подстановка этого значения дает

$$\chi(\rho) = \frac{(\rho+1)(\rho+2)^2(\rho+3)^2\ldots(\rho+\nu-2)^2(\rho+\nu-1)}{(\nu-1)!(\nu-2)!}.$$

Мы нашли в § 6 такую систему инвариантов $p_0, p_1, \ldots, p_{2\nu-4}$, что все инварианты базисных форм выражаются в виде целых алгебраических функций от инвариантов этой системы. Мы определили, кроме того, линейную функцию p с постоянными коэффициентами от инвариантов p_{ik}, обладающую тем свойством, что все инварианты p_{ik} являются рациональными функциями от $p, p_0, p_1, \ldots, p_{2\nu-4}$. Поскольку ввиду этого инварианты $p, p_0, p_1, \ldots, p_{2\nu-4}$ образуют систему инвариантов рассматривавшегося в § 2 вида, мы можем вычислить с помощью использованных в § 8 методов степень поля инвариантов, определенного этими инвариантами. На этом пути мы получаем

$$k = (2\nu-4)! \lim_{\rho\to\infty} \frac{\chi(\rho)}{\rho^{2\nu-4}} = \frac{(2\nu-4)!}{(\nu-1)!(\nu-2)!}.$$

В то же время, можно также показать, что $2\nu-3$ инвариантов $p_0, p_1, \ldots, p_{2\nu-4}$ алгебраически независимы.

Возвращаясь к методу определения $p_0, p_1, \ldots, p_{2\nu-4}$ из § 6, мы видим, что k также равно числу семейств бинарных форм, функциональный определитель которых является предписанной бинарной формой порядка $2\nu-4$ [14].

Отметим в заключение, что $\chi(\rho)$ является так называемой «характеристической функцией» алгебраического многообразия, получающегося, если положить

$$p_{ik} = a_i b_k - a_k b_i \qquad (i, k = 1, 2, \ldots, \nu)$$

и рассматривать p_{ik} как переменные, а a_i, b_i как произвольные параметры [47]. Этот пример показывает также, как развитые в этой работе методы соотносятся с пригодными для общих модулей методами, которые я развил в разд. III и IV моей работы «О теории алгебраических форм». В соответствии с общими утверждениями из этой работы [15] степень $2\nu-4$ характеристической функции по ρ равна размерности указанного алгебраического многообразия, а умноженный на $(2\nu-4)!$ коэффициент при $\rho^{2\nu-4}$ дает степень этого многообразия.

---

[14] См. мою работу: Über Büschel von binären Formen mit vorgeschriebener Funktionaldeterminante. — Math. Ann., Bd. 33, S. 227, и литературу, цитированную там.

[15] См. мою работу: Über die Theorie der algebraischen Formen. — Math. Ann., Bd. 36, S. 520 [с. 54 настоящего издания. — *Ред.*].

IV. ПОНЯТИЕ НУЛЬ-ФОРМЫ

§ 12. Определитель подстановки как функция коэффициентов преобразованной базисной формы

Согласно результатам разд. I и II, для построения и исследования полной системы инвариантов базисной формы необходимо прежде всего знать такую конечную систему инвариантов, что обращение в нуль инвариантов этой системы влечет за собой обращение в нуль всех инвариантов. Задача нахождения такой системы инвариантов была решена в § 5 для бинарной базисной формы f, однако способом, непригодным для распространения на базисные формы от многих переменных. Существование такой системы инвариантов немедленно вытекает из теоремы I в разд. I моей работы «О теории алгебраических форм»[16]. Однако эта общая теорема не дает никаких средств для построения такой системы инвариантов с помощью конечного числа процессов, произведя которые перед началом вычислений, можно было бы, например, получить верхнюю границу для числа инвариантов системы или для их степеней по коэффициентам базисной формы. Эта трудность будет теперь полностью преодолена. Ради краткости мы ограничимся случаем одной базисной формы, хотя методы и результаты сохраняют силу и в полной общности.

Пусть задана тернарная базисная форма f порядка n от переменных x_1, x_2, x_3, все $N = \frac{1}{2}(n+1)(n+2)$ коэффициентов a_1, $a_2, \ldots, a_N$ которой имеют определенные числовые значения. Нам следует прежде всего выяснить, имеется ли инвариант J, который отличен от нуля на данной форме f, или же все инварианты равны на ней нулю. Чтобы сделать это, преобразуем f с помощью линейной подстановки

$$\begin{aligned} x_1 &= \alpha_{11}y_1 + \alpha_{12}y_2 + \alpha_{13}y_3, \\ x_2 &= \alpha_{21}y_1 + \alpha_{22}y_2 + \alpha_{23}y_3, \\ x_3 &= \alpha_{31}y_1 + \alpha_{32}y_2 + \alpha_{33}y_3, \end{aligned} \qquad \delta = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix},$$

где коэффициенты α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$ являются неопределенными величинами. Обозначим коэффициенты преобразованной формы $g(y_1, y_2, y_3)$ через b_1, $b_2, \ldots, b_N$; они являются целыми рациональными функциями степени n от α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$ с определенными числовыми коэффициентами. Предположим теперь, что имеется инвариант J, отличный от нуля на данной форме f; тогда

$$J(g) = \delta^p J(f),$$

где p — вес инварианта J, а $J(f)$ — отличное от нуля число. Разделив последнее уравнение на это число, мы видим, что определитель подстановки δ удовлетворяет уравнению, первый коэффициент которого равен 1, а остальные коэффициенты являются целыми рациональными функциями от b_1, $b_2, \ldots, b_N$; иначе говоря, при нашем предположении δ — *целая* алгебраическая функция от коэффициентов b_1, $b_2, \ldots, b_N$.

---

[16] Math. Ann., Bd. 36, S. 474 [с. 16 настоящего издания. — *Ред.*].

Существенно знать, что верно утверждение, обратное этому. Чтобы доказать это, предположим, что δ — целая алгебраическая функция от b_1, $b_2, \ldots, b_N$; пусть, скажем, она удовлетворяет уравнению

$$\delta^p + G_1(b)\delta^{p-1} + \ldots + G_p(b) = 0,$$

где G_1, $G_2, \ldots, G_p$ — целые рациональные функции от b_1, $b_2, \ldots, b_N$ с числовыми коэффициентами. Это уравнение должно выполняться тождественно, если мы подставим вместо δ и b_1, $b_2, \ldots, b_N$ их выражения через α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$. Далее, так как δ — однородная функция степени 3, а b_1, $b_2, \ldots, b_N$ — однородные функции степени n по α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$, то мы можем предположить, что те коэффициенты G_s в указанном выше уравнении, для которых $3s/n$ — дробное число, равны нулю, а остальные коэффициенты G_s однородны степени $3s/n$ по b_1, $b_2, \ldots, b_N$. Будем теперь временно рассматривать коэффициенты a_1, $a_2, \ldots, a_N$ в форме f как неопределенные величины, а b_1, $b_2, \ldots, b_N$ соответственно как функции не только от коэффициентов подстановки α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$, но и как функции, линейно зависящие от a_1, $a_2, \ldots, a_N$. Левая часть предыдущего уравнения, т. е. выражение

$$\delta^p + G_1(b)\delta^{p-1} + \ldots + G_p(b),$$

будет тогда тождественно равна нулю для всех значений α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$, если заменить величины a_1, $a_2, \ldots, a_N$ на заданные числовые коэффициенты нашей конкретной базисной формы f. Если мы применим теперь к этому выражению p раз процесс

$$\Omega = \begin{vmatrix} \dfrac{\partial}{\partial\alpha_{11}} & \dfrac{\partial}{\partial\alpha_{12}} & \dfrac{\partial}{\partial\alpha_{13}} \\ \dfrac{\partial}{\partial\alpha_{21}} & \dfrac{\partial}{\partial\alpha_{22}} & \dfrac{\partial}{\partial\alpha_{23}} \\ \dfrac{\partial}{\partial\alpha_{31}} & \dfrac{\partial}{\partial\alpha_{32}} & \dfrac{\partial}{\partial\alpha_{33}} \end{vmatrix},$$

то в соответствии с доказанным в разд. V моей работы «О теории алгебраических форм»[17] предложением получим выражение вида

$$C_p + J_1(a) + J_2(a) + \ldots + J_p(a),$$

где C_p — ненулевое число, а $J_1(a)$, $J_2(a), \ldots, J_p(a)$ — инварианты базисной формы f с неопределенными коэффициентами a_1, $a_2, \ldots, a_N$. Это выражение должно обратиться в нуль, когда a_1, $a_2, \ldots, a_N$ заменяются на данные числовые коэффициенты нашей формы f, откуда следует, что не все инварианты J_1, $J_2, \ldots, J_p$ обращаются в нуль на нашей базисной форме f. Мы сформулируем этот результат в виде следующего предложения:

Базисная форма с определенными числовыми коэффициентами тогда и только тогда не обращает в нуль некоторый инвариант, когда определитель подстановки δ является целой алгебраической функцией от коэффициентов линейно преобразованной формы [48].

---

[17] См. Math. Ann., Bd. 36, S. 524 [с. 58 настоящего издания. — *Ред.*].

§ 13. Выяснение того, имеет ли данная базисная форма ненулевой инвариант

Мы укажем теперь, как выяснить с помощью конечного и полностью обозримого процесса, является ли δ целой алгебраической функцией от b_1, $b_2, \ldots, b_N$. Прежде всего, согласно доказанному в § 1 вспомогательному утверждению, мы всегда можем найти такие числовые коэффициенты $c_{11}, c_{12}, \ldots, c_{rN}$, что b_1, $b_2, \ldots, b_N$ будут целыми алгебраическими функциями от r линейных выражений

$$B_1 = c_{11}\, b_1 + c_{12}\, b_2 + \ldots + c_{1N}\, b_N,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$B_r = c_{r1}\, b_1 + c_{r2}\, b_2 + \ldots + c_{rN}\, b_N,$$

между которыми нет алгебраических соотношений. В этом случае как $B_1, \ldots$ $\ldots, B_r$, так и b_1, $b_2, \ldots, b_N$ являются целыми рациональными однородными функциями степени n от α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$ с числовыми коэффициентами, и, поскольку между любыми десятью такими функциями от α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$ должно быть алгебраическое соотношение [49], мы видим, что r во всяком случае не превосходит 9.

Чтобы исследовать условия, при которых $r < 9$, будем считать, что переменные y_1, y_2, y_3 преобразованной формы $g(y_1, y_2, y_3)$ заменены восемью системами значений

$$\begin{aligned} &y_1 = y_1', \quad y_1 = y_1'', \quad \ldots, \quad y_1 = y_1^{(8)}, \\ &y_2 = y_2', \quad y_2 = y_2'', \quad \ldots, \quad y_2 = y_2^{(8)}, \\ &y_3 = y_3', \quad y_3 = y_3'', \quad \ldots, \quad y_3 = y_3^{(8)}. \end{aligned}$$

Это дает восемь линейных выражений g', $g'', \ldots, g^{(8)}$ такого же вида, как выражения B. Предположим теперь, что между g и этими восемью выражениями имеется алгебраическое соотношение

$$G\big(g, g', \ldots, g^{(8)}\big) = 0,$$

причем производные целой рациональной функции G по g, $g', \ldots, g^{(8)}$ не равны тождественно нулю при всех α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$. Дифференцируя предыдущее тождество по α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$, получаем

$$\frac{\partial G}{\partial g}\frac{\partial g}{\partial \alpha_{11}} + \frac{\partial G}{\partial g'}\frac{\partial g'}{\partial \alpha_{11}} + \ldots + \frac{\partial G}{\partial g^{(8)}}\frac{\partial g^{(8)}}{\partial \alpha_{11}} = 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\frac{\partial G}{\partial g}\frac{\partial g}{\partial \alpha_{33}} + \frac{\partial G}{\partial g'}\frac{\partial g'}{\partial \alpha_{33}} + \ldots + \frac{\partial G}{\partial g^{(8)}}\frac{\partial g^{(8)}}{\partial \alpha_{33}} = 0,$$

и, значит,

$$\begin{vmatrix} \dfrac{\partial g}{\partial \alpha_{11}} & \dfrac{\partial g'}{\partial \alpha_{11}} & \cdots & \dfrac{\partial g^{(8)}}{\partial \alpha_{11}} \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{\partial g}{\partial \alpha_{33}} & \dfrac{\partial g'}{\partial \alpha_{33}} & \cdots & \dfrac{\partial g^{(8)}}{\partial \alpha_{33}} \end{vmatrix} = 0.$$

Используя при разложении этого определителя по первому столбцу равенства

$$\frac{\partial g}{\partial \alpha_{ik}} = y_k \frac{\partial f}{\partial x_i} \qquad (i,k = 1,2,3),$$

мы получаем соотношение вида

$$\begin{aligned} &D_{11}\, y_1 \frac{\partial f}{\partial x_1} + D_{21}\, y_2 \frac{\partial f}{\partial x_1} + D_{31}\, y_3 \frac{\partial f}{\partial x_1} + \\ &+ D_{12}\, y_1 \frac{\partial f}{\partial x_2} + D_{22}\, y_2 \frac{\partial f}{\partial x_2} + D_{32}\, y_3 \frac{\partial f}{\partial x_2} + \\ &+ D_{13}\, y_1 \frac{\partial f}{\partial x_3} + D_{23}\, y_2 \frac{\partial f}{\partial x_3} + D_{33}\, y_3 \frac{\partial f}{\partial x_3} = 0, \end{aligned}$$

где $D_{11}, D_{21}, \ldots, D_{33}$ — целые рациональные функции от величин $\alpha_{11}, \alpha_{12}, \ldots$ $\ldots, \alpha_{33}, y_1', y_2', y_3', \ldots, y_1^{(8)}, y_2^{(8)}, y_3^{(8)}$. Предположим, что не все субопределители $D_{11}, D_{21}, \ldots, D_{33}$ тождественно равны нулю при всех значениях этих параметров, и пусть теперь эти параметры имеют такие числовые значения, что хотя бы один из этих субопределителей отличен от нуля. Ввиду того что y_1, y_2, y_3 являются линейными функциями от x_1, x_2, x_3, предыдущее соотношение дает дифференциальное уравнение для f вида

$$l_1 \frac{\partial f}{\partial x_1} + l_2 \frac{\partial f}{\partial x_2} + l_3 \frac{\partial f}{\partial x_3} = 0,$$

где l_1, l_2, l_3 — линейные однородные функции от x_1, x_2, x_3. С другой стороны, если сделать предыдущее предположение нельзя, т. е. если все субопределители указанного выше определителя тождественно равны нулю, то к любому из этих субопределителей можно применить те же соображения и мы снова придем к линейному дифференциальному уравнению для f.

Применяя подходящее линейное преобразование переменных, можно легко исследовать полученное линейное дифференциальное уравнение для f более подробно, что дает следующий результат:

Число r в общем случае < 9, когда заданная форма f обладает тем специальным свойством, что имеются непрерывные преобразования, переводящие ее в себя [50].

Вернемся теперь к рассмотрениям из начала этого параграфа и в случае $r < 9$ определим $9 - r$ функций $B_{r+1}, \ldots, B_9$ степени n по $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}$ с числовыми коэффициентами как-либо так, чтобы девять функций $B_1, \ldots$ $\ldots, B_9$ не были связаны алгебраическими соотношениями. Тот факт, что при данных условиях это всегда возможно, легко установить с помощью хорошо известного свойства функционального определителя. Рассмотрим

теперь неприводимое уравнение, связывающее δ, $B_1, \ldots, B_9$; пусть оно имеет вид

$$\Gamma_0\delta^\pi + \Gamma_1\delta^{\pi-1} + \ldots + \Gamma_\pi = 0,$$

где $\Gamma_0, \Gamma_1, \ldots, \Gamma_\pi$ — целые рациональные функции от $B_1, \ldots, B_9$. Если предположить, что δ — целая алгебраическая функция от b_1, $b_2, \ldots, b_N$, то δ должна также быть целой алгебраической функцией от $B_1, \ldots, B_r$ и потому должна удовлетворять уравнению вида

$$\delta^\rho + E_1\delta^{\rho-1} + \ldots + E_\rho = 0,$$

где $E_1, \ldots, E_\rho$ — целые рациональные функции от $B_1, \ldots, B_r$. Однако левая часть этого уравнения должна содержать левую часть предыдущего уравнения в качестве множителя [51]; отсюда легко прийти к заключению, что Γ_0 — отличная от нуля константа, а остальные коэффициенты $\Gamma_1, \ldots, \Gamma_\pi$ — целые рациональные функции только от $B_1, \ldots, B_r$. По этой причине для того, чтобы сделать интересующее нас заключение [52], требуется лишь выяснить, обладает ли связывающее δ, $B_1, \ldots, B_9$ неприводимое соотношение указанным только что свойством.

§ 14. Верхняя граница для весов инвариантов

Наряду с этим мы можем, используя следующее наблюдение, найти верхнюю границу для степени π неприводимого уравнения.

Пусть заданы $h+1$ форм $H_1, \ldots, H_{h+1}$ степени m от h однородных переменных $u_1, \ldots, u_h$. Образуем все степени и произведения форм $H_1, \ldots, H_{h+1}$, имеющие относительно них степень R, и рассмотрим уравнение

$$\sum C_{s_1, s_2, \ldots, s_{h+1}} H_1^{s_1} H_2^{s_2} \ldots H_{h+1}^{s_{h+1}} = 0 \qquad (s_1 + s_2 + \ldots + s_{h+1} = R).$$

Если теперь мы положим в левой части все степени и произведения переменных $u_1, \ldots, u_h$ равными нулю, то получим систему из

$$\frac{(mR+1)(mR+2)\ldots(mR+h-1)}{1\cdot 2\cdot \ldots \cdot (h-1)}$$

линейных однородных уравнений для определения

$$\frac{(R+1)(R+2)\ldots(R+h)}{1\cdot 2\cdot \ldots \cdot h}$$

коэффициентов $C_{s_1, s_2, \ldots, s_{h+1}}$. Если

$$\frac{(R+1)\ldots(R+h)}{1\cdot 2\cdot \ldots \cdot h} > \frac{(mR+1)\ldots(mR+h-1)}{1\cdot 2\cdot \ldots \cdot (h-1)},$$

то эти уравнения всегда имеют решения, а значит, это тем более так, если

$$(R+1)^h > h(mR+h-1)^{h-1}.$$

Это неравенство во всяком случае имеет место, если мы возьмем $R = h(m+1)^{h-1}$. Отсюда следует, что между функциями $H_1, \ldots, H_{h+1}$ должно существовать соотношение степени, меньшей или равной $h(m+1)^{h-1}$.

Применим это утверждение к десяти формам δ^n, $B_1^3, \ldots, B_9^3$, каждая из которых однородна степени $3n$ по девяти переменным α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$; таким образом, мы полагаем $h = 9$ и $m = 3n$. Значит, степень π указанного выше уравнения должна быть не больше числа $9n(3n+1)^8$. Поэтому, пользуясь тем же методом доказательства, что и в § 12, получаем следующее утверждение:

Если определитель подстановки δ является целой алгебраической функцией от коэффициентов линейно преобразованной базисной формы, то она обладает не обращающимся в нуль инвариантом веса, не превосходящего $9n(3n+1)^8$.

Это утверждение вместе с доказанными в § 4 и § 12 предложениями немедленно приводит к следующему утверждению:

Всякий инвариант тернарной базисной формы n-го порядка можно представить в виде целой алгебраической функции от инвариантов веса $\leqslant 9n(3n+1)^8$.

Ввиду этого инварианты $J_1, \ldots, J_\varkappa$, с которыми мы имели дело в разд. I, всегда можно выбрать так, чтобы их веса были меньше некоторой границы, зависящей лишь от n; из верхней же границы для весов немедленно получается верхняя граница для степеней инвариантов $J_1, \ldots, J_\varkappa$ [53].

Чтобы короче сформулировать как результаты настоящего разд. IV, так и следствия из них, которые будут получены позже, мы введем понятие нуль-формы.

Базисная форма называется нуль-формой, если ее коэффициенты имеют такие специальные числовые значения, что все ее инварианты равны нулю [54].

Если задана нуль-форма, то, как показывают предыдущие рассмотрения, имеется конечное число значений $B_1, \ldots, B_\tau$, определенных условием $\Gamma_0 = 0$, для которых определитель δ становится бесконечным. Поскольку все $b_1, \ldots, b_N$ имеют конечное значение, когда этим свойством обладают $B_1, \ldots, B_\tau$, то можно также сказать, что (в правильно понимаемом смысле) *нуль-форма — это форма f, коэффициенты которой остаются конечными, когда она подвергается некоторой линейной подстановке с бесконечным определителем.*

Точная алгебраическая формулировка этого свойства нуль-форм будет дана в следующем параграфе.

V. ПОСТРОЕНИЕ НУЛЬ-ФОРМ

§ 15. Линейное преобразование, соответствующее нуль-форме

В разд. IV было показано, как с помощью конечного числа рациональных операций найти систему инвариантов $J_1, \ldots, J_\varkappa$, обладающую указанными в разд. I свойствами [55]. Что касается практического вычисления такой системы в конкретных случаях, то, очевидно, эта задача будет существенно облегчена, если заранее знать, где обращаются в нуль все инварианты данной базисной формы. Для бинарной базисной формы такое описание общих нулей всех инвариантов было получено в § 5, и с его помощью я получил

там систему инвариантов, через которые все инварианты бинарной базисной формы могут быть выражены в виде целых алгебраических функций. Если попытаться искать нуль-формы в случае многих переменных таким же способом, как и для бинарных форм, или же с помощью вычислений, то сталкиваешься с существенными трудностями; таким способом без мучительных вычислений мне удалось найти нуль-формы только для кубической и биквадратичной тернарных базисных форм. В этом разделе задача нахождения нуль-форм будет полностью решена с помощью нового и общего метода. Излагая этот метод, я буду снова, простоты ради, рассматривать случай одной тернарной базисной формы. Метод основывается на следующем вспомогательном утверждении:

Пусть задана тернарная нуль-форма f порядка n с коэффициентами $a_1, \ldots, a_N$. Тогда всегда можно найти линейную подстановку вида

$$(\alpha) = \begin{pmatrix} \tau^{\mu_1}\mathfrak{P}_{11} & \tau^{\mu_1}\mathfrak{P}_{12} & \tau^{\mu_1}\mathfrak{P}_{13} \\ \tau^{\mu_2}\mathfrak{P}_{21} & \tau^{\mu_2}\mathfrak{P}_{22} & \tau^{\mu_2}\mathfrak{P}_{23} \\ \tau^{\mu_3}\mathfrak{P}_{31} & \tau^{\mu_3}\mathfrak{P}_{32} & \tau^{\mu_3}\mathfrak{P}_{33} \end{pmatrix},$$

где μ_1, μ_2, μ_3 — целые числа, а $\mathfrak{P}_{11}, \mathfrak{P}_{12}, \ldots, \mathfrak{P}_{33}$ — обычные степенные ряды по целым положительным [56] степеням переменной τ, обладающую тем свойством, что все коэффициенты $b_1, \ldots, b_N$ преобразованной нуль-формы g остаются конечными при $\tau = 0$, тогда как определитель подстановки

$$\delta = \begin{vmatrix} \tau^{\mu_1}\mathfrak{P}_{11} & \tau^{\mu_1}\mathfrak{P}_{12} & \tau^{\mu_1}\mathfrak{P}_{13} \\ \tau^{\mu_2}\mathfrak{P}_{21} & \tau^{\mu_2}\mathfrak{P}_{22} & \tau^{\mu_2}\mathfrak{P}_{23} \\ \tau^{\mu_3}\mathfrak{P}_{31} & \tau^{\mu_3}\mathfrak{P}_{32} & \tau^{\mu_3}\mathfrak{P}_{33} \end{vmatrix} = \tau^{\mu}\mathfrak{Q}$$

становится при $\tau = 0$ бесконечным.

Чтобы доказать это [57], преобразуем данную нуль-форму f с помощью линейной подстановки

$$\begin{aligned} x_1 &= \alpha_{11}y_1 + \alpha_{12}y_2 + \alpha_{13}y_3, \\ x_2 &= \alpha_{21}y_1 + \alpha_{22}y_2 + \alpha_{23}y_3, \\ x_3 &= \alpha_{31}y_1 + \alpha_{32}y_2 + \alpha_{33}y_3, \end{aligned} \qquad \delta = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{vmatrix},$$

где $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}$ — неопределенные параметры. Мы получим форму g, коэффициенты $b_1, \ldots, b_N$ которой являются целыми рациональными функциями n-й степени от $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}$ с определенными числовыми коэффициентами. Построим теперь, как указано в конце § 13, такие девять алгебраически независимых функций $B_1, \ldots, B_9$, через которые все $b_1, \ldots, b_N$ могут быть выражены в виде целых алгебраических функций, и, как и там, построим связывающее δ, $B_1, \ldots, B_9$ неприводимое уравнение. Оно имеет вид

$$\Gamma_0\delta^{\pi} + \Gamma_1\delta^{\pi-1} + \ldots + \Gamma_{\pi} = 0,$$

где $\Gamma_0, \Gamma_1, \ldots, \Gamma_{\pi}$ — целые рациональные однородные функции от $B_1, \ldots, B_9$ и где, в частности, первый коэффициент Γ_0 в действительности обязательно содержит некоторые из величин $B_1, \ldots, B_9$. В самом деле, в противном случае δ была бы целой алгебраической функцией от $b_1, \ldots, b_N$, а тогда f не могла бы, вопреки предположению, быть нуль-формой.

Определим теперь девять чисел $B_1^0, \ldots, B_9^0$ таким образом, чтобы при их подстановке вместо $B_1, \ldots, B_9$ выражение Γ_0 обращалось в нуль, а по крайней мере один из остальных коэффициентов $\Gamma_1, \ldots, \Gamma_\pi$ нашего неприводимого уравнения был отличен от нуля. Определим, далее, девять чисел $B_1^{00}, \ldots, B_9^{00}$ таким образом, чтобы при подстановке

$$\begin{aligned} B_1 &= B_1^0 + B_1^{00} t, \\ &\cdots\cdots\cdots \\ B_9 &= B_9^0 + B_9^{00} t \end{aligned}$$

в указанное неприводимое уравнение оно стало уравнением от δ и t, которое по-прежнему неприводимо[18]. Пусть это уравнение имеет вид

$$\Gamma_0^0 \delta^\pi + \Gamma_1^0 \delta^{\pi-1} + \ldots + \Gamma_\pi^0 = 0,$$

где $\Gamma_0^0, \Gamma_1^0, \ldots, \Gamma_\pi^0$ — целые рациональные функции от t.

Мы рассмотрим теперь девять уравнений

$$\begin{aligned} B_1(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}) &= B_1^0 + B_1^{00} t, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ B_9(\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}) &= B_9^0 + B_9^{00} t. \end{aligned}$$

Поскольку между девятью функциями $B_1, \ldots, B_9$ не имеется алгебраических соотношений, их функциональный определитель

$$\begin{vmatrix} \dfrac{\partial B_1}{\partial \alpha_{11}} & \cdots & \dfrac{\partial B_9}{\partial \alpha_{11}} \\ \cdots & \cdots & \cdots \\ \dfrac{\partial B_1}{\partial \alpha_{33}} & \cdots & \dfrac{\partial B_9}{\partial \alpha_{33}} \end{vmatrix}$$

не обращается тождественно в нуль для всех $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}$. Эти уравнения поэтому определяют девять величин $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}$ как алгебраические функции от t. Система ветвей этих алгебраических функций в окрестности $t = 0$ представляется разложениями

$$\alpha_{ik} = t^{\nu_{ik}} P_{ik}(t^{1/m}) \qquad (i, k = 1, 2, 3),$$

где m — целое положительное число, ν_{ik} — рациональные числа, а P_{ik} — обычные степенные ряды по целым положительным [56] степеням аргумента $t^{1/m}$. Определитель, составленный из этих девяти разложений,

$$\delta = |t^{\nu_{ik}} P_{ik}(t^{1/m})| = t^\nu Q(t^{1/m}),$$

имеет такой же вид и представляет ветвь алгебраической функции $\delta(t)$, определенной уравнением

$$\Gamma_0^0 \delta^\pi + \Gamma_1^0 \delta^{\pi-1} + \ldots + \Gamma_\pi^0 = 0.$$

Поскольку это уравнение неприводимо, остальные $\pi - 1$ ветвей алгебраической функции $\delta(t)$ можно получить из данной ветви $\delta = t^\nu Q(t^{1/m})$ с по-

---

[18] Я доказал существование таких $B_1^{00}, \ldots, B_9^{00}$ в моей работе Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. — Crelles J., Bd. 110, S. 104.

мощью аналитического продолжения. Пусть этими ветвями являются

$$\delta' = t^{\nu'} Q'(t^{1/m'}),$$
$$\delta'' = t^{\nu''} Q''(t^{1/m''}),$$
$$\cdots\cdots\cdots\cdots$$
$$\delta^{(\pi-1)} = t^{\nu^{(\pi-1)}} Q^{(\pi-1)}(t^{1/m^{(\pi-1)}}),$$

и пусть исходная ветвь δ переходит в ветви $\delta', \delta'', \ldots, \delta^{(\pi-1)}$ соответственно по путям $W', W'', \ldots, W^{(\pi-1)}$, а эти $\pi-1$ путей выбраны на комплексной плоскости переменного t так, что все точки разрыва алгебраических функций $\alpha_{ik}(t)$ и $\delta(t)$ расположены снаружи этих путей. Поскольку Γ_0^0 обращается в нуль при $t = 0$, а остальные коэффициенты $\Gamma_1^0, \ldots, \Gamma_\pi^0$ не все обращаются в нуль при $t = 0$, то по меньшей мере одна из ветвей $\delta, \delta', \ldots, \delta^{(\pi-1)}$ должна принимать значение ∞ при $t = 0$; пусть, скажем, это будет ветвь $\delta' = t^{\nu'} Q'$. Поскольку Q' — сходящийся степенной ряд по целым положительным степеням аргумента $t^{1/m'}$, а m' — целое положительное число, ν' должно быть отрицательным целым числом. Продолжим теперь вдоль пути W' значения ветвей, представленных системой степенных рядов

$$\alpha_{ik} = t^{\nu_{ik}} P_{ik}(t^{1/m}) \qquad (i, k = 1, 2, 3),$$

и получим тем самым другую систему ветвей алгебраических функций $\alpha_{ik}(t)$; пусть система этих ветвей в окрестности точки $t = 0$ представлена степенными рядами

$$\alpha'_{ik} = t^{\nu'_{ik}} P'_{ik}(t^{1/m'}).$$

Если M — целое положительное число, делящееся на m' и на знаменатель рационального числа ν'_{ik}, то подстановка $t = \tau^M$ дает систему разложений в степенные ряды для алгебраических функций α_{ik} вида

$$\alpha_{ik} = \tau^{\mu_i} \mathfrak{P}_{ik}(\tau) \qquad (i, k = 1, 2, 3),$$

где μ_i — целые числа, и эта система обладает свойством, которое требуется в нашем утверждении. В самом деле, при $t = 0$ величины $B_1, \ldots, B_9$ принимают значения $B_1^0, \ldots, B_9^0$ и поэтому $b_1, \ldots, b_N$, будучи целыми алгебраическими функциями от $B_1, \ldots, B_9$, остаются конечными при $\tau = 0$.

Обращение только что доказанного утверждения установить несложно. В самом деле, если для величин $\alpha_{11}, \alpha_{12}, \ldots, \alpha_{33}$ можно определить обладающие требуемым свойством степенные ряды, то δ не является целой алгебраической функцией от $b_1, \ldots, b_N$, а потому базисная форма f не является нуль-формой.

§ 16. Одно вспомогательное предложение о линейных подстановках, коэффициенты которых являются степенными рядами

Чтобы применить к вычислению нуль-форм доказанное в § 15 утверждение, нам нужно следующее вспомогательное предложение о нормализации

линейных подстановок, коэффициентами которых являются степенные ряды от переменной τ. Пусть, как и в § 15, задана подстановка

$$(\alpha) = \begin{pmatrix} \tau^{\mu_1}\mathfrak{P}_{11} & \tau^{\mu_1}\mathfrak{P}_{12} & \tau^{\mu_1}\mathfrak{P}_{13} \\ \tau^{\mu_2}\mathfrak{P}_{21} & \tau^{\mu_2}\mathfrak{P}_{22} & \tau^{\mu_2}\mathfrak{P}_{23} \\ \tau^{\mu_3}\mathfrak{P}_{31} & \tau^{\mu_3}\mathfrak{P}_{32} & \tau^{\mu_3}\mathfrak{P}_{33} \end{pmatrix}$$

с определителем

$$\delta = \tau^{\mu}\,\mathfrak{Q},$$

где μ_1, μ_2, μ_3, μ — целые числа, а $\mathfrak{P}_{11}, \mathfrak{P}_{12}, \ldots, \mathfrak{P}_{33}$ [58] — обычные степенные ряды по целым положительным [56] степеням переменной τ. Всегда можно определить две линейные подстановки

$$(\beta) = \begin{pmatrix} \beta_{11} & \beta_{12} & \beta_{13} \\ \beta_{21} & \beta_{22} & \beta_{23} \\ \beta_{31} & \beta_{32} & \beta_{33} \end{pmatrix}, \qquad (\gamma) = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} \end{pmatrix},$$

обладающие следующими свойствами.

1. Коэффициенты этих двух подстановок (β) и (γ) являются обычными степенными рядами по целым положительным [56] степеням переменной τ,

$$\beta_{ik} = (\beta_{ik})_0 + (\beta_{ik})_1\,\tau + (\beta_{ik})_2\,\tau^2 + \ldots,$$

$$\gamma_{ik} = (\gamma_{ik})_0 + (\gamma_{ik})_1\,\tau + (\gamma_{ik})_2\,\tau^2 + \ldots,$$

постоянные члены которых удовлетворяют условиям

$$\begin{vmatrix} (\beta_{11})_0 & (\beta_{12})_0 & (\beta_{13})_0 \\ (\beta_{21})_0 & (\beta_{22})_0 & (\beta_{23})_0 \\ (\beta_{31})_0 & (\beta_{32})_0 & (\beta_{33})_0 \end{vmatrix} = 1, \qquad \begin{vmatrix} (\gamma_{11})_0 & (\gamma_{12})_0 & (\gamma_{13})_0 \\ (\gamma_{21})_0 & (\gamma_{22})_0 & (\gamma_{23})_0 \\ (\gamma_{31})_0 & (\gamma_{32})_0 & (\gamma_{33})_0 \end{vmatrix} = 1.$$

2. Последовательное применение подстановок (β), (α), (γ) дает подстановку вида

$$(\gamma)(\alpha)(\beta) = \begin{pmatrix} \tau^{\lambda_1} & 0 & 0 \\ 0 & \tau^{\lambda_2} & 0 \\ 0 & 0 & \tau^{\lambda_3} \end{pmatrix},$$

где λ_1, λ_2, λ_3 — некоторые целые числа [59].

Чтобы доказать это, положим

$$\mathfrak{P}_{ik} = (\mathfrak{P}_{ik})_0 + (\mathfrak{P}_{ik})_1\tau + (\mathfrak{P}_{ik})_2\tau^2 + \ldots,$$

$$\mathfrak{Q} = (\mathfrak{Q})_0 \quad + \quad (\mathfrak{Q})_1\tau + \quad (\mathfrak{Q})_2\tau^2 + \ldots$$

Можно считать, что $(\mathfrak{Q})_0$ отлично от нуля, поскольку в противном случае целое число μ можно было бы увеличить. Предположим также, что $\mu_1 \geqslant \mu_2 \geqslant \mu_3$. Если теперь $\mu_1 + \mu_2 + \mu_3 = \mu$, то определитель

$$\begin{vmatrix} (\mathfrak{P}_{11})_0 & (\mathfrak{P}_{12})_0 & (\mathfrak{P}_{13})_0 \\ (\mathfrak{P}_{21})_0 & (\mathfrak{P}_{22})_0 & (\mathfrak{P}_{23})_0 \\ (\mathfrak{P}_{31})_0 & (\mathfrak{P}_{32})_0 & (\mathfrak{P}_{33})_0 \end{vmatrix}$$

будет ненулевой константой и, значит, обратной к подстановке

$$(\mathfrak{P}) = \begin{pmatrix} \mathfrak{P}_{11} & \mathfrak{P}_{12} & \mathfrak{P}_{13} \\ \mathfrak{P}_{21} & \mathfrak{P}_{22} & \mathfrak{P}_{23} \\ \mathfrak{P}_{31} & \mathfrak{P}_{32} & \mathfrak{P}_{33} \end{pmatrix}$$

будет подстановка $(\mathfrak{P})^{-1}$, коэффициенты которой являются обычными степенными рядами по целым положительным $[^{56}]$ степеням переменной τ. Полагая тогда

$$(\beta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad (\gamma) = (\mathfrak{P})^{-1}, \quad \mu_1 = \lambda_1, \quad \mu_2 = \lambda_2, \quad \mu_3 = \lambda_3,$$

мы немедленно получаем две подстановки с требуемыми свойствами.

С другой стороны, если $\mu_1 + \mu_2 + \mu_3 < \mu$, то определитель $|(\mathfrak{P}_{ik})_0|$ должен быть равен нулю, и тогда можно найти три не равных одновременно нулю числа ε_1, ε_2, ε_3, для которых

$$\varepsilon_1(\mathfrak{P}_{1i})_0 + \varepsilon_2(\mathfrak{P}_{2i})_0 + \varepsilon_3(\mathfrak{P}_{3i})_0 = 0 \qquad (i = 1, 2, 3).$$

Мы должны теперь исследовать три случая.

1. Предположим, что $\varepsilon_1 \neq 0$; положим тогда $\varepsilon_1 = 1$. В этом случае

$$(\varepsilon) = \begin{pmatrix} \varepsilon_1 & \tau^{\mu_1 - \mu_2}\varepsilon_2 & \tau^{\mu_1 - \mu_3}\varepsilon_3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

— подстановка с определителем $\varepsilon_1 = 1$, коэффициенты которой являются целыми рациональными функциями от τ, и поэтому

$$(\alpha') = (\alpha)(\varepsilon) = \begin{pmatrix} \tau^{\mu_1'}\mathfrak{P}'_{11} & \tau^{\mu_1'}\mathfrak{P}'_{12} & \tau^{\mu_1'}\mathfrak{P}'_{13} \\ \tau^{\mu_2}\mathfrak{P}_{21} & \tau^{\mu_2}\mathfrak{P}_{22} & \tau^{\mu_2}\mathfrak{P}_{23} \\ \tau^{\mu_3}\mathfrak{P}_{31} & \tau^{\mu_3}\mathfrak{P}_{32} & \tau^{\mu_3}\mathfrak{P}_{33} \end{pmatrix},$$

где μ_1' — целое число, большее μ_1, а $\mathfrak{P}'_{11}$, $\mathfrak{P}'_{12}$, $\mathfrak{P}'_{13}$ — снова обычные степенные ряды по целым положительным $[^{56}]$ степеням переменной τ.

2. Предположим, что $\varepsilon_1 = 0$, а $\varepsilon_2 \neq 0$; положим тогда $\varepsilon_2 = 1$. В этом случае подстановка

$$(\varepsilon) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon_2 & \tau^{\mu_2 - \mu_3}\varepsilon_3 \\ 0 & 0 & 1 \end{pmatrix}$$

снова имеет определитель $\varepsilon_2 = 1$, ее коэффициенты являются целыми рациональными функциями от τ и для нее

$$(\alpha') = (\alpha)(\varepsilon) = \begin{pmatrix} \tau^{\mu_1}\mathfrak{P}_{11} & \tau^{\mu_1}\mathfrak{P}_{12} & \tau^{\mu_1}\mathfrak{P}_{13} \\ \tau^{\mu_2'}\mathfrak{P}'_{21} & \tau^{\mu_2'}\mathfrak{P}'_{22} & \tau^{\mu_2'}\mathfrak{P}'_{23} \\ \tau^{\mu_3}\mathfrak{P}_{31} & \tau^{\mu_3}\mathfrak{P}_{32} & \tau^{\mu_3}\mathfrak{P}_{33} \end{pmatrix},$$

где μ_2' — целое число, большее μ_2, а $\mathfrak{P}'_{21}$, $\mathfrak{P}'_{22}$, $\mathfrak{P}'_{23}$ — обычные степенные ряды по целым положительным $[^{56}]$ степеням переменной τ.

3. Предположим, что $\varepsilon_1 = 0$, $\varepsilon_2 = 0$, а $\varepsilon_3 \neq 0$; положим тогда $\varepsilon_3 = 1$. В этом случае

$$(\mathfrak{P}_{31})_0 = 0, \quad (\mathfrak{P}_{32})_0 = 0, \quad (\mathfrak{P}_{33})_0 = 0,$$

так что можно положить

$$(\alpha') = (\alpha) = \begin{pmatrix} \tau^{\mu_1}\mathfrak{P}_{11} & \tau^{\mu_1}\mathfrak{P}_{12} & \tau^{\mu_1}\mathfrak{P}_{13} \\ \tau^{\mu_2}\mathfrak{P}_{21} & \tau^{\mu_2}\mathfrak{P}_{22} & \tau^{\mu_2}\mathfrak{P}_{23} \\ \tau^{\mu_3'}\mathfrak{P}'_{31} & \tau^{\mu_3'}\mathfrak{P}'_{32} & \tau^{\mu_3'}\mathfrak{P}'_{33} \end{pmatrix},$$

где μ_3' — целое число, большее μ_3, а $\mathfrak{P}'_{31}$, $\mathfrak{P}'_{32}$, $\mathfrak{P}'_{33}$ — снова обычные степенные ряды по целым положительным [56] степеням переменной τ.

Если теперь сумма показателей $\mu_1' + \mu_2 + \mu_3$, $\mu_1 + \mu_2' + \mu_3$ или $\mu_1 + \mu_2 + \mu_3'$ соответственно равна μ, то из доказанного следует, что наше предложение верно для подстановки (α'), а потому вследствие равенства

$$(\gamma)(\alpha')(\beta) = (\gamma)(\alpha)\{(\varepsilon)(\beta)\}$$

оно верно также и для подстановки (α). Если же сумма показателей меньше μ, то нужно применить к подстановке (α') процедуру, примененную только что к подстановке (α). Так как после этого дополнительного шага сумма показателей возрастает по крайней мере на единицу, то после конечного числа r повторений этого процесса мы получим подстановку $(\alpha^{(r)})$, для которой сумма показателей равна μ. Это доказывает наше вспомогательное предложение.

§ 17. Каноническая нуль-форма

Коэффициенты подстановки

$$(\beta_0) = \begin{pmatrix} (\beta_{11})_0 & (\beta_{12})_0 & (\beta_{13})_0 \\ (\beta_{21})_0 & (\beta_{22})_0 & (\beta_{23})_0 \\ (\beta_{31})_0 & (\beta_{32})_0 & (\beta_{33})_0 \end{pmatrix}$$

являются константами, и, поскольку определитель $|(\beta_{ik})_0|$ равен 1, эта подстановка имеет обратную. Мы преобразуем теперь данную нуль-форму f с помощью этой подстановки и получим тем самым нуль-форму $f' = (\beta_0)^{-1}f$, коэффициенты которой снова являются константами. Согласно формуле из § 16,

$$\lim_{\tau\to 0}\left[\begin{pmatrix} \tau^{\lambda_1} & 0 & 0 \\ 0 & \tau^{\lambda_2} & 0 \\ 0 & 0 & \tau^{\lambda_3} \end{pmatrix} f'\right] = \lim_{\tau\to 0}[(\gamma)(\alpha)(\beta)f'].$$

С другой стороны,

$$\lim_{\tau\to 0}[(\gamma)(\alpha)(\beta)f'] = \lim_{\tau\to 0}[(\gamma)(\alpha)\lim_{\tau\to 0}\{(\beta)f'\}] = \lim_{\tau\to 0}[(\gamma)(\alpha)f].$$

Согласно § 15, применение к f подстановки (α) дает форму, все коэффициенты которой остаются конечными при $\tau = 0$. А поскольку коэффициенты подстановки (γ) являются обычными степенными рядами по целым положительным [56] степеням переменной τ, то $(\gamma)(\alpha)f$ также является формой, коэффициенты которой остаются конечными при $\tau = 0$. Поэтому то же

самое верно и для формы

$$\begin{pmatrix} \tau^{\lambda_1} & 0 & 0 \\ 0 & \tau^{\lambda_2} & 0 \\ 0 & 0 & \tau^{\lambda_3} \end{pmatrix} f' = f'(\tau^{\lambda_1} x_1, \tau^{\lambda_2} x_2, \tau^{\lambda_3} x_3).$$

Так как определитель подстановки (α) становится бесконечным при $\tau = 0$, то сумма $\lambda_1 + \lambda_2 + \lambda_3$ должна быть отрицательной.

Обратно, если для формы f с числовыми коэффициентами найдутся три целых числа $\lambda_1, \lambda_2, \lambda_3$ с указанным свойством, то, очевидно, f является нуль-формой; ввиду этого мы примем следующее определение:

Тернарная форма $f = \sum a_{n_1 n_2 n_3} x_1^{n_1} x_2^{n_2} x_3^{n_3}$ *порядка* n *называется канонической нуль-формой, если найдутся такие три целых числа* $\lambda_1, \lambda_2, \lambda_3$, *что их сумма отрицательна и коэффициент* $a_{n_1 n_2 n_3}$ *равен нулю, когда отрицательно число* $\lambda_1 n_1 + \lambda_2 n_2 + \lambda_3 n_3$ [60].

Из предшествующего обсуждения вытекает следующее предложение:

Каждая нуль-форма может быть преобразована с помощью линейной подстановки с определителем 1 *в каноническую нуль-форму* [61].

Если понимать под классом форм совокупность всех форм, которые могут быть преобразованы друг в друга с помощью линейной подстановки с ненулевым определителем, то это предложение может быть переформулировано так:

в каждом классе нуль-форм имеется каноническая нуль-форма.

Задача построения всех нуль-форм сведена, таким образом, к нахождению всех канонических нуль-форм, а это требует лишь построения всех систем целых чисел λ_1, λ_2, λ_3 описанного выше вида.

§ 18. Построение канонических нуль-форм

Для решения сформулированной в конце предыдущего параграфа задачи выберем на плоскости в качестве координатного треугольника равносторонний треугольник ABC с длиной стороны, равной n, и определим координаты точки P на этой плоскости следующим образом: проведем через P прямые, параллельные сторонам AC, BA, CB, и пусть A', B', C' — точки их пересечения со сторонами BC, CA, AB соответственно; тогда отрезки $\xi_1 = PA'$, $\xi_2 = PB'$, $\xi_3 = PC'$ и будут координатами точки P. Если теперь мы разобьем каждую из трех сторон треугольника на n равных частей и для каждой из сторон проведем через эти точки деления $n - 1$ параллельных ей прямых, то координатный треугольник будет разбит на равные треугольники, стороны которых равны 1. Каждая из возникающих таким образом вершин $\xi_1 = n_1$, $\xi_2 = n_2$, $\xi_3 = n_3$ лежит либо внутри, либо на стороне координатного треугольника и соответствует члену $a_{n_1 n_2 n_3} x_1^{n_1} x_2^{n_2} x_3^{n_3}$ тернарной формы n-го порядка; и обратно, каждому члену тернарной формы соответствует вершина построенных треугольников.

Если теперь u_1, u_2, u_3 — произвольные вещественные константы, сумма $u_1+u_2+u_3$ которых отлична от нуля, то уравнение

$$u_1\xi_1+u_2\xi_2+u_3\xi_3=0$$

задает прямую, не проходящую через середину M координатного треугольника. Рассмотрим все вершины n_1, n_2, n_3, лежащие вне прямой $u_1\xi_1+u_2\xi_2+u_3\xi_3=0$ и с той же стороны от нее, что и M, и, приравняв нулю в тернарной форме n-го порядка соответствующие коэффициенты $a_{n_1n_2n_3}$, придадим остальным коэффициентам произвольные числовые значения. Обозначим полученную форму через $f_{u_1u_2u_3}$; это — каноническая нуль-форма. Чтобы убедиться в этом, определим три таких рациональных числа u_1', u_2', u_3' с ненулевой суммой, чтобы все вершины, лежащие с той же, что и M, стороны от прямой $u_1\xi_1+u_2\xi_2+u_3\xi_3=0$, лежали бы также с той же, что и M, стороны от прямой $u_1'\xi_1+u_2'\xi_2+u_3'\xi_3=0$ и наоборот. Легко видеть, что это всегда можно сделать: нужно рассмотреть три случая, когда на прямой $u_1\xi_1+u_2\xi_2+u_3\xi_3=0$ либо не лежит ни одной вершины, либо лежит одна, либо лежит больше одной вершины, и затем взять u_1', u_2', u_3' достаточно близкими к u_1, u_2, u_3. Определим теперь такое положительное или отрицательное целое число u, чтобы произведения uu_1', uu_2', uu_3' были целыми числами с отрицательной суммой. Полагая эти целые числа равными соответственно λ_1, λ_2, λ_3, мы видим, что $f_{u_1u_2u_3}$ действительно является канонической нуль-формой, поскольку для нее $a_{n_1n_2n_3}=0$ при

$$\lambda_1n_1+\lambda_2n_2+\lambda_3n_3<0.$$

Если, далее, v_1, v_2, v_3 — вещественные константы, сумма которых равна нулю, то уравнение $v_1\xi_1+v_2\xi_2+v_3\xi_3=0$ определяет прямую, проходящую через точку M. В этом случае мы рассмотрим все вершины u_1, u_2, u_3, лежащие на прямой $v_1\xi_1+v_2\xi_2+v_3\xi_3=0$, а также вершины, лежащие с той же стороны от этой прямой, что и координатная вершина A, после чего в тернарной форме n-го порядка приравняем нулю коэффициенты $a_{n_1n_2n_3}$, соответствующие этим вершинам n_1, n_2, n_3, а остальным коэффициентам придадим произвольные значения. Обозначим полученную форму через $f_{v_1v_2v_3}$; это каноническая нуль-форма. Чтобы убедиться в этом, перенесем прямую $v_1\xi_1+v_2\xi_2+v_3\xi_3=0$ параллельно ей самой в направлении от вершины A таким образом, чтобы при этом переносе прямая не прошла ни через какую вершину. Если новое положение этой прямой задается уравнением $u_1\xi_1+u_2\xi_2+u_3\xi_3=0$, то форма $f_{v_1v_2v_3}$, очевидно, совпадает с формой $f_{u_1u_2u_3}$, а потому в силу предыдущего является канонической нуль-формой.

Определяя каноническую нуль-форму $f_{v_1v_2v_3}$, мы могли бы точно так же воспользоваться вершинами с той стороны от прямой $v_1\xi_1+v_2\xi_2+v_3\xi_3=0$, с которой не лежит точка A. Получающаяся таким способом каноническая нуль-форма понятным образом соответствует первой форме.

Далее, канонические нуль-формы $f_{u_1u_2u_3}$ являются частным случаем канонических нуль-форм $f_{v_1v_2v_3}$, которые мы только что рассмотрели. Чтобы доказать это, предположим, что точки M и A лежат по одну сторону от прямой $u_1\xi_1+u_2\xi_2+u_3\xi_3=0$, и проведем через M прямую, параллельную ей; пусть $v_1\xi_1+v_2\xi_2+v_3\xi_3=0$, где $v_1+v_2+v_3=0$, — уравнение этой последней прямой. Тогда форма $f_{u_1u_2u_3}$ получается из формы $f_{v_1v_2v_3}$ приравниванием

нулю всех коэффициентов этой последней формы, соответствующих лежащим между указанными параллельными прямыми вершинам.

Если же точки M и A не лежат по одну сторону от прямой $u_1\xi_1 + u_2\xi_2 + u_3\xi_3 = 0$, то необходимо предварительно сменить координаты.

Итак, чтобы получить полный список канонических нуль-форм, нужно только определить канонические нуль-формы $f_{v_1v_2v_3}$, и потому мы получаем следующее правило для получения такого списка:

Нужно провести через точку M прямую и определить вершины, лежащие либо на этой прямой, либо по ту же сторону от нее, что и точка A. Затем нужно приравнять нулю коэффициенты $a_{n_1n_2n_3}$ тернарной формы n-го порядка, соответствующие этим вершинам n_1, n_2, n_3, а оставшимся коэффициентам придать произвольные значения [62].

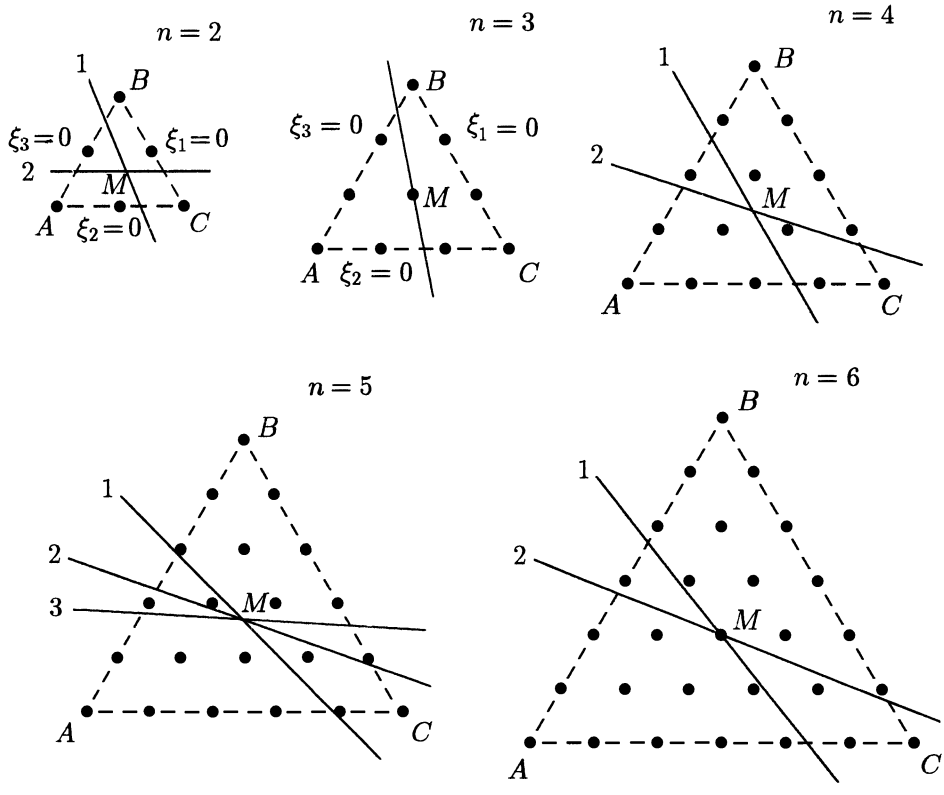
Поскольку таким способом получаются все канонические нуль-формы, число различных типов нуль-форм совпадает с числом существенно различных положений, которые может занимать относительно вершин луч, проходящий через M [63]; при этом можно игнорировать те положения, для которых соответствующие формы являются *специальными* каноническими нуль-формами [64].

Чтобы проиллюстрировать найденное правило, я построил диаграммы, с помощью которых можно определить тернарные канонические нуль-формы вплоть до порядка 6. Мы получаем следующий список, в котором для краткости $x_1 = 1$, $x_2 = x$, $x_3 = y$, через a обозначена произвольная величина, а $(xy)_s$ — однородное выражение степени s по x и y с произвольными коэффициентами:

$n = 2$: 1) $(xy)_2$,
2) $ax + x(xy)_1$;
$n = 3$: $ay^2 + (xy)_3$;
$n = 4$: 1) $(xy)_3 + (xy)_4$,
2) $x\{ax + x(xy)_1 + (xy)_3\}$;
$n = 5$: 1) $ax^3 + (xy)_4 + (xy)_5$,
2) $x\{x(xy)_1 + x(xy)_2 + (xy)_4\}$,
3) $x^2\{a + (xy)_1 + (xy)_2 + (xy)_3\}$;
$n = 6$: 1) $x^3(xy)_1 + (xy)_5 + (xy)_6$,
2) $x\{ax^2 + x^2(xy)_1 + x(xy)_3 + (xy)_5\}$.

Отметим, что при $n = 2$ указанные две канонические нуль-формы могут быть преобразованы одна в другую с помощью линейного преобразования, так что в этом случае в действительности имеется только одна нуль-форма.

После нахождения нуль-форм легко указать вырождения плоских кривых, определенных обращением в нуль этих нуль-форм. Так, с помощью предыдущего списка легко проверить результаты для тернарных кубических форм, приведенные в § 7. Далее, мы получаем, например, что все инварианты биквадратичной формы f обращаются в нуль в точности в том случае, когда кривая $f = 0$ либо содержит точку кратности три, либо распадается на кубическую кривую и касательную в ее точке перегиба.



§ 19. Кватернарные кубические нуль-формы

Данный метод нахождения всех тернарных нуль-форм непосредственно применим и в случае форм или систем форм от любого числа переменных или наборов переменных.

Например, чтобы найти кватернарные нуль-формы порядка три, построим в пространстве правильный тетраэдр с длиной стороны, равной трем, затем разобьем каждую его сторону на три равных отрезка и для каждой из четырех граней тетраэдра проведем через точки деления две параллельные ей плоскости; они разобьют тетраэдр на правильные тетраэдры со стороной 1. Каждой вершине (n_1, n_2, n_3, n_4) этого тетраэдра соответствует член кватернарной кубической формы. Чтобы определить все канонические нуль-формы, мы должны найти все возможные расположения плоскости, проходящей через центр M тетраэдра, по отношению к вершинам. Для этого используем исходный тетраэдр для определения в пространстве координатной системы точно таким же образом, как выше использовали равносторонний треугольник на плоскости. Тогда каждая плоскость, проходящая

через центр $M = (1,1,1,1)$, задается уравнением вида $u_1\xi_1 + u_2\xi_2 + u_3\xi_3 + u_4\xi_4 = 0$, где $u_1 + u_2 + u_3 + u_4 = 0$. Предположим, что $u_1 \geqslant u_2 \geqslant u_3 \geqslant u_4$, и будем говорить, что точка пространства $(\xi_1^0, \xi_2^0, \xi_3^0, \xi_4^0)$ лежит слева или справа от плоскости $u_1\xi_1 + u_2\xi_2 + u_3\xi_3 + u_4\xi_4 = 0$ в зависимости от того, какое неравенство выполнено: $u_1\xi_1^0 + u_2\xi_2^0 + u_3\xi_3^0 + u_4\xi_4^0 \geqslant 0$ или $u_1\xi_1^0 + u_2\xi_2^0 + u_3\xi_3^0 + u_4\xi_4^0 < 0$. Из равенства $u_1 + u_2 + u_3 + u_4 = 0$ и принятых неравенств следует, что $u_1 > 0$. Будем теперь различать два случая: 1) $u_2 \leqslant 0$; 2) $u_2 > 0$. В случае 1) легко видеть, что девять точек $(3,0,0,0)$, $(2,1,0,0)$, $(2,0,1,0)$, $(2,0,0,1)$, $(1,2,0,0)$, $(1,0,2,0)$, $(1,1,1,0)$, $(1,1,0,1)$, $(1,0,1,1)$ должны лежать слева от плоскости, и уравнение $5\xi_1 - \xi_2 - \xi_3 - 3\xi_4 = 0$ определяет такую плоскость, что указанные девять точек лежат слева от нее, а оставшиеся 11 — справа. В случае 2) следует выделить два подслучая, 2а) и 2б), в зависимости от того, какое неравенство выполнено: $u_3 \leqslant 0$ или $u_3 > 0$. В случае 2а) восемь вершин $(3,0,0,0)$, $(2,1,0,0)$, $(2,0,1,0)$, $(2,0,0,1)$, $(1,2,0,0)$, $(1,1,1,0)$, $(1,1,0,1)$, $(0,3,0,0)$ лежат слева от плоскости, а уравнение $5\xi_1 + \xi_2 - 3\xi_3 - 3\xi_4 = 0$ задает такую плоскость, слева от которой лежат эти 8 точек, а справа — остальные 12. В случае 2б) слева от плоскости лежат 10 вершин, у которых $\xi_4 = 0$, а справа — остальные 10 вершин. Положим далее для краткости $x_1 = 1$, $x_2 = x$, $x_3 = y$, $x_4 = z$. Пусть через a обозначена произвольная величина, а через $(xyz)_s$ и $(yz)_s$ — однородные выражения степени s по x, y, z и по y, z соответственно, имеющие произвольные коэффициенты. Мы получаем тогда следующий список нуль-форм:

1) $z^2 + (xyz)_3$;

2а) $(yz)_2 + (yz)_3 + x(yz)_2 + x^2(yz)_1$;

2б) $az + z(xyz)_1 + z(xyz)_2$.

Легко видеть, что с помощью соответствующей линейной подстановки нуль-форма 2б) может быть преобразована к такому виду, что станет частным случаем формы 2а); отсюда следует, что имеется лишь два существенно различных типа нуль-форм. Определяя вырождения кубических поверхностей, заданных обращением этих нуль-форм в нуль, мы получаем следующее предложение:

Все инварианты кватернарной кубической формы f обращаются в нуль в том и только в том случае, когда поверхность $f = 0$ имеет либо двойную точку, вторая поляра которой является двойной плоскостью, либо двойную точку, вторая поляра которой состоит из двух разных плоскостей, пересекающихся по прямой, лежащей на этой поверхности.

Аналогичным способом может быть развита теория квадратичных и билинейных форм от произвольного числа переменных.

Далее, мы располагаем теперь средствами перенести на формы от трех или большего числа переменных все утверждения, которые установлены в разд. II лишь для бинарных форм. *В частности, утверждение из* § 7, *описывающее одно фундаментальное свойство процесса Аронгольда, верно и в общем случае.*

Наши результаты о тернарных нуль-формах допускают следующую геометрическую интерпретацию. Если мы представим тернарную форму f точкой $(N-1)$-мерного пространства, то условие обращения в нуль всех инвариантов определяет в этом пространстве алгебраическое многообразие, непри-

водимые компоненты которого могут быть, в соответствии с предыдущим обсуждением, заранее описаны [65]. Мы видим, кроме того, что эти многообразия рациональны, т. е. координаты их точек являются рациональными функциями от параметров [66].

Рассматривая все инварианты тернарной базисной формы как модуль, мы можем определить все содержащиеся в нем неприводимые модули.

§ 20. Обращение в нуль инвариантов нуль-формы и порядок их обращения в нуль

Тот факт, что все инварианты канонической нуль-формы обращаются в нуль, может быть также непосредственно выведен из определения канонической нуль-формы, и на этом пути мы, кроме того, получаем замечательную информацию о кратности обращения в нуль инвариантов произвольной нуль-формы.

Инвариант базисной формы

$$f = \sum a_{n_1 n_2 n_3}\, x_1^{n_1} x_2^{n_2} x_3^{n_3}$$

есть целая рациональная функция от коэффициентов $a_{n_1 n_2 n_3}$, все члены которой имеют одну и ту же степень g и один и тот же вес $p = \frac{1}{3}ng$. Поэтому если мы запишем его в виде

$$J = \sum C \prod a_{n_1 n_2 n_3}^{e_{n_1 n_2 n_3}},$$

где через C обозначен соответствующий числовой коэффициент, то показатели $e_{n_1 n_2 n_3}$ удовлетворяют следующим уравнениям [67]:

$$\sum n_1 e_{n_1 n_2 n_3} = \frac{1}{3}ng,$$

$$\sum n_2 e_{n_1 n_2 n_3} = \frac{1}{3}ng,$$

$$\sum n_3 e_{n_1 n_2 n_3} = \frac{1}{3}ng,$$

где суммирование осуществляется по всем системам чисел n_1, n_2, n_3, сумма которых равна n. Пусть теперь λ_1, λ_2, λ_3 — система трех чисел, определяющая в соответствии с данным выше определением каноническую нуль-форму. Пусть сумма этих трех чисел равна $-\lambda$, где λ — положительное число. Из предыдущих уравнений мы получаем

$$\sum (\lambda_1 n_1 + \lambda_2 n_2 + \lambda_3 n_3) e_{n_1 n_2 n_3} = \frac{1}{3}ng(\lambda_1 + \lambda_2 + \lambda_3) = -\frac{1}{3}\lambda ng.$$

Опуская в сумме из левой части все члены, которые $\geqslant 0$, мы приходим к неравенству

$$\sum{}' (\lambda_1 n_1 + \lambda_2 n_2 + \lambda_3 n_3)\, e_{n_1 n_2 n_3} \leqslant -\frac{1}{3}\lambda ng,$$

или

$$\sum{}' |\lambda_1 n_1 + \lambda_2 n_2 + \lambda_3 n_3|\, e_{n_1 n_2 n_3} \geqslant \frac{1}{3}\lambda ng,$$

где сумма $\sum'$ берется по всем системам чисел n_1, n_2, n_3, для которых число

$\lambda_1 n_1 + \lambda_2 n_2 + \lambda_3 n_3$ отрицательно. Обозначая, далее, через Λ наибольшее из чисел $|\lambda_1|$, $|\lambda_2|$, $|\lambda_3|$, получаем

$$|\lambda_1 n_1 + \lambda_2 n_2 + \lambda_3 n_3| \leqslant n\Lambda,$$

что дает

$$\sum{}' e_{n_1 n_2 n_3} \geqslant \frac{\lambda g}{3\Lambda},$$

т. е. в каждом члене $C \prod a_{n_1 n_2 n_3}^{e_{n_1 n_2 n_3}}$ инварианта сумма показателей тех коэффициентов $a_{n_1 n_2 n_3}$, которые равны нулю для канонической нуль-формы, не меньше некоторого положительного числа $\lambda g/(3\Lambda)$. Значит, *для канонической нуль-формы в нуль обращаются не только все инварианты, но и их производные по* $a_{n_1 n_2 n_3}$ *вплоть до некоторого порядка* G, *где* G — *наибольшее из чисел, не превосходящих* $\lambda g/(3\Lambda)$ (так что G неограниченно растет с ростом степени g). Ввиду предыдущего произвольная нуль-форма может быть преобразована в каноническую нуль-форму; поэтому *обнаруженное свойство имеет место для любой нуль-формы.* На этом может быть основано новое доказательство конечности полной системы инвариантов, но мы не станем здесь этим заниматься.[19)]

VI. ПОСТРОЕНИЕ ПОЛНОЙ СИСТЕМЫ ИНВАРИАНТОВ

§ 21. Три этапа построения полной системы инвариантов

Чтобы получить с помощью развитых в разд. I и II методов полную систему инвариантов, нужно последовательно решить следующие три задачи.

1. Найти систему инвариантов S_1, через которые все инварианты базисной формы выражаются как целые алгебраические функции.

2. Найти систему инвариантов S_2, через которые все инварианты выражаются рационально.

3. Вычислить полную систему целых алгебраических функций S_3 в поле инвариантов, определенном системами S_1 и S_2. Функции из этой системы S_3 являются инвариантами и образуют вместе с инвариантами из S_1 искомую полную систему инвариантов.

Наиболее трудной из этих трех задач является первая. Согласно доказанному в § 4 утверждению, система S_1 получается с помощью нахождения инвариантов, обладающих тем свойством, что их совместное обращение в нуль влечет за собой обращение в нуль всех инвариантов. Из утверждения, доказанного в § 14, следует, что для этого достаточно рассмотреть инварианты, веса которых не превосходят некоторого числа [^{68}]. Наконец, действительное вычисление такой системы S_1 в конкретных случаях существенно облегчается за счет описания нуль-форм, которое получено в § 18; дело в том, что это описание позволяет в конкретном случае легко решить,

---

[19)] Это доказательство я привел в моей третьей заметке, цитированной выше (S. 445); оно не использует теорему I из моей работы «О теории алгебраических форм» (Math. Ann., Bd. 36, S. 474) [с. 16 настоящего издания. — *Ред.*]).

обладают ли уже найденные инварианты тем свойством, что их одновременное обращение в нуль влечет за собой обращение в нуль всех инвариантов.

Систему S_2 можно найти, либо используя типичное представление, либо с помощью вычислений *ad hoc*. В следующем параграфе мы покажем, как найти полную систему инвариантов, не зная системы S_2.

§ 22. Получение полной системы инвариантов из $J_1, \ldots, J_\varkappa$

Пусть $i_1, \ldots, i_m$ — система инвариантов, через которые все инварианты выражаются в виде целых алгебраических функций. Тогда доказанное в § 1 вспомогательное утверждение показывает, как, исходя из этой системы, вычислить такую систему $\varkappa$ инвариантов $J_1, \ldots, J_\varkappa$, что сами они не связаны никакими алгебраическими соотношениями, а все инварианты базисной формы выражаются через них в виде целых алгебраических функций. Если это сделано, то из функций $b_1, \ldots, b_N$ [69] выбирается некоторое число τ функций — пусть это будут функции $b_1, \ldots, b_\tau$ — таким образом, чтобы $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$ не были связаны никаким алгебраическим соотношением, а оставшиеся функции $b_{\tau+1}$, $b_{\tau+2}, \ldots, b_N$ были алгебраическими функциями от $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$[20]. Если p_1 — вес инварианта J_1, то

$$\delta^{p_1} J_1(a_1, \ldots, a_N) = J_1(b_1, \ldots, b_N).$$

В силу этого δ является алгебраической функцией от J_1, $b_1, \ldots, b_N$. Поэтому можно, согласно хорошо известному утверждению [71], так выбрать константы $c, c_{\tau+1}$, $c_{\tau+2}, \ldots, c_N$ в выражении

$$B = c\delta + c_{\tau+1} b_{\tau+1} + c_{\tau+2} b_{\tau+2} + \ldots + c_N b_N,$$

чтобы $\delta, b_{\tau+1}, b_{\tau+2}, \ldots, b_N$ стали рациональными функциями от B, $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$. Функция B удовлетворяет уравнению вида

$$B^\mu + R_1 B^{\mu-1} + \ldots + R_\mu = 0,$$

где $R_1, \ldots, R_\mu$ — рациональные функции от $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$.

Рассмотрим теперь $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$ как независимые переменные и найдем в поле функций, определенном функцией B, фундаментальную систему, т. е. такую систему целых алгебраических функций $B_1, \ldots, B_M$ этого поля, что всякая другая целая функция этого поля может быть записана в виде

$$G_1 B_1 + G_2 B_2 + \ldots + G_M B_M,$$

где G_1, $G_2, \ldots, G_M$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$ [72]. Поскольку функция B_s является целой алгебраической функцией от $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$, она удовлетворяет уравнению вида

$$B_s^\mu + \Gamma_{1s} B_s^{\mu-1} + \ldots + \Gamma_{\mu s} = 0 \qquad (s = 1, 2, \ldots, M),$$

где $\Gamma_{1s}, \ldots, \Gamma_{\mu s}$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$. А поскольку B_s являются рациональными функциями от B, $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$,

---

[20] В предыдущем случае тернарной базисной формы n-го порядка мы имеем $\varkappa = N - 8$, $\tau = 9$ [70].

они становятся целыми рациональными функциями от $a_1, \ldots, a_N$, $\alpha_{11}, \alpha_{12}, \ldots$ $\ldots, \alpha_{33}$, когда $b_1, \ldots, b_N$ заменяются на их выражения через $a_1, \ldots, a_N$, α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$.

Пусть $[A]$ обозначает постоянный член любого целого рационального выражения A от α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$. Очевидно тогда, что $[B_1], \ldots, [B_M]$ являются инвариантами базисной формы. Действительно, $[B_s]$ удовлетворяет уравнению

$$[B_s]^\mu + [\Gamma_{1s}][B_s]^{\mu-1} + \ldots + [\Gamma_{\mu s}] = 0,$$

и так как теперь лишь $b_1, \ldots, b_\tau$ содержат подстановочные коэффициенты α_{11}, $\alpha_{12}, \ldots, \alpha_{33}$, то ясно, что $[\Gamma_{11}], \ldots, [\Gamma_{1s}], \ldots, [\Gamma_{\mu s}]$ являются целыми рациональными функциями от инвариантов $J_1, \ldots, J_\varkappa$. Ввиду указанного во введении третьего свойства системы инвариантов отсюда следует, что $[B_1], \ldots, [B_M]$ являются инвариантами.

С другой стороны, в силу уравнения

$$\delta^p J(a_1, \ldots, a_N) = J(b_1, \ldots, b_N).$$

любой инвариант J базисной формы f является рациональной функцией от δ, $b_1, \ldots, b_N$. Так как он является также целой алгебраической функцией от $J_1, \ldots, J_\varkappa$, то он — целая алгебраическая функция поля и в этом качестве может быть представлен в виде

$$J = G_1 B_1 + \ldots + G_M B_M,$$

где $G_1, \ldots, G_M$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$, $b_1, \ldots, b_\tau$. Из этой формулы мы получаем равенство

$$J = [G_1][B_1] + \ldots + [G_M][B_M],$$

где $[G_1], \ldots, [G_M]$ — целые рациональные функции от $J_1, \ldots, J_\varkappa$. Это равенство показывает, что $J_1, \ldots, J_\varkappa$, $[B_1], \ldots, [B_M]$ образуют систему инвариантов, через которые любой инвариант базисной формы f выражается в виде целой рациональной функции.

Изложенный метод нахождения полной системы инвариантов требует привлечения лишь рациональных и целиком обозримых процессов, а более детальное исследование доставляет также и верхнюю границу на веса инвариантов в полной системе, зависящую только от n [73]. Таким образом, я полагаю, нами достигнута наиболее важная общая цель теории функциональных полей, образованных инвариантами.

Кёнигсберг в Пруссии, 29 сентября 1892 г.

ТЕОРИЯ ЧИСЕЛ

О ДИОФАНТОВЫХ УРАВНЕНИЯХ РОДА НУЛЬ

(совместно с А. Гурвицем)*)

Ниже обсуждается задача о нахождении всех целочисленных решений уравнения

$$f(x_1, x_2, x_3) = 0 \tag{1}$$

в предположении, что $f(x_1, x_2, x_3)$ — однородный многочлен (ganzzahlige homogene Funktion) степени n от переменных x_1, x_2, x_3 с целыми коэффициентами, и плоская кривая, определенная этим уравнением, имеет род нуль. Вопрос обо всех точках кривой (1) с рациональными координатами — это, по существу, та же самая задача.

При решении этой задачи мы опираемся на работу M. Нётера «Rationale Ausführung der Operationen in der Theorie der algebraischen Funktionen»[1]. Прежде всего, согласно полученным в ней результатам мы можем выяснить посредством конечного числа рациональных операций, выполняется ли предположение о нулевом роде предъявленного уравнения. Затем, тоже посредством рациональных операций можно построить $n-1$ линейно независимых тернарных целочисленных форм $\varphi_1, \varphi_2, \ldots \varphi_{n-1}$ порядка $n-2$ таких, что для любых параметров $\lambda_1, \lambda_2, \ldots \lambda_{n-1}$ кривая (1) пересекается с кривой

$$\lambda_1\varphi_1 + \lambda_2\varphi_2 + \ldots + \lambda_{n-1}\varphi_{n-1} = 0 \tag{2}$$

зависящей от параметров $\lambda_1, \lambda_2, \ldots, \lambda_{n-1}$, в $n-2$ различных точках. Уравнение (2) задает кривую $(n-2)$-го порядка, присоединенную к кривой (1).

Теперь положим

$$\left.\begin{aligned} \Phi_1 &= \lambda_{11}\varphi_1 + \lambda_{12}\varphi_2 + \ldots + \lambda_{1,n-1}\varphi_{n-1}, \\ \Phi_2 &= \lambda_{21}\varphi_1 + \lambda_{22}\varphi_2 + \ldots + \lambda_{2,n-1}\varphi_{n-1}, \\ \Phi_3 &= \lambda_{31}\varphi_1 + \lambda_{32}\varphi_2 + \ldots + \lambda_{3,n-1}\varphi_{n-1}, \end{aligned}\right\} \tag{3}$$

где $\lambda_{11}, \lambda_{12}, \ldots, \lambda_{3,n-1}$ обозначают неопределенные параметры. Преобразуя уравнение (1) с помощью формул

$$y_1 : y_2 : y_3 = \Phi_1 : \Phi_2 : \Phi_3, \tag{4}$$

получим, уравнение

$$g(y_1, y_2, y_3) = 0, \tag{5}$$

---

*) Über die diophantischen Gleichungen vom Geschlecht Null. (Zusammen mit A. Hurwitz.) — Acta Math., 1891, Bd. 14, S. 217–224. *Перевод Ю. Г. Зархина.*

[1]) Math. Ann., Bd. 23, S. 311.

левая часть которого является целочисленной формой от y_1, y_2, y_3 и параметров λ_{11}, $\lambda_{12}, \ldots, \lambda_{3,n-1}$. Далее, используя формулы преобразования, приходим к формулам вида

$$x_1 : x_2 : x_3 = \Psi_1 : \Psi_2 : \Psi_3, \tag{6}$$

где Ψ_1, Ψ_2, Ψ_3 — тоже целочисленные формы от y_1, y_2, y_3 и параметров λ_{11}, $\lambda_{12}, \ldots, \lambda_{3,n-1}$. Мы предполагаем, что эти формы не имеют общих делителей. Форма $g(y_1, y_2, y_3)$ обязана быть неприводимой и однородной степени $n-2$, как это непосредственно вытекает из известных теорем о рациональных однозначно обратимых преобразованиях алгебраических кривых. Теперь придадим параметрам λ_{11}, $\lambda_{12}, \ldots, \lambda_{3,n-1}$ такие целочисленные значения, что форма $g(y_1, y_2, y_3)$ остается неприводимой. Такое всегда возможно, так как значения параметров λ_{11}, $\lambda_{12}, \ldots, \lambda_{3,n-1}$, при которых форма $g(y_1, y_2, y_3)$ приводима, должны удовлетворять определенным алгебраическим уравнениям. Теперь каждой точке кривой (1) с рациональными координатами отвечает согласно формулам (4) и (6) точка кривой (5) с рациональными координатами, и наоборот. Итак, мы вновь приходим к нашей первоначальной задаче для уравнения $g(y_1, y_2, y_3) = 0$, которое также является целочисленным рода нуль, зато степень его на два ниже степени уравнения $f(x_1, x_2, x_3) = 0$.

Продолжая действовать указанным способом, пока это возможно, т. е. пока степень уравнения выше трех, мы приходим к уравнению третьей или второй степени, в зависимости от того, нечетна или четна степень n первоначального уравнения. Но уравнение третьей степени немедленно сводится к уравнению первой степени. Дело в том, что такое уравнение задает кривую третьей степени с двойной точкой или точкой возврата, координаты которой обязаны быть рациональными числами, и такая кривая может быть переведена в прямую линию посредством рационального однозначного обратимого преобразования. В зависимости от того, нечетна или четна степень предъявленного нам уравнения, мы приходим к уравнению первой или второй степени. Разберем отдельно эти случаи.

В п е р в о м случае пусть

$$l(u_1, u_2, u_3) = 0 \tag{7}$$

— получившееся линейное уравнение. Тогда, очевидно, можно указать три целочисленные формы w_1, w_2, w_3 от однородных параметров t_1, t_2 такие, что пропорция

$$u_1 : u_2 : u_3 = w_1 : w_2 : w_3 \tag{8}$$

доставляет все рациональные решения уравнения (7), когда параметры t_1, t_2 принимают всевозможные целочисленные значения. Возвращаясь посредством последовательного применения выведенных выше преобразований к первоначально предъявленному уравнению (1), получаем пропорцию вида

$$x_1 : x_2 : x_3 = \rho_1 : \rho_2 : \rho_3, \tag{9}$$

где ρ_1, ρ_2, ρ_3 — целозначные формы степени n от переменных t_1, t_2. За возможным исключением конечного числа решений, которые мы будем называть *особыми* и которыми займемся чуть позже, все остальные, неособые, решения уравнения (1) можно найти из пропорции (9), придавая параметрам t_1, t_2 всевозможные целочисленные значения. Отсюда очевидно, что, считая в формулах для ρ_1, ρ_2, ρ_3 параметры t_1, t_2 всевозможными взаимно

простыми целыми числами и деля вычисленные значения на их наибольший общий делитель, мы получим все неособые целочисленные *собственные* решения x_1, x_2, x_3 уравнения (1). Для того чтобы получить явные формулы для этих целочисленных собственных решений, образуем результант двух форм

$$\lambda_1\rho_1 + \lambda_2\rho_2 + \lambda_3\rho_3, \quad \mu_1\rho_1 + \mu_2\rho_2 + \mu_3\rho_3,$$

где через λ_1, λ_2, λ_3, μ_1, μ_2, μ_3 обозначены неопределенные параметры. Наш результант является многочленом с целыми коэффициентами от параметров λ_1, λ_2, λ_3, μ_1, μ_2, μ_3; он не может тождественно равняться нулю, так как формы ρ_1, ρ_2, ρ_3 не имеют общего множителя. Пусть R — наибольшее положительное целое число, на которое делятся все коэффициенты этого многочлена. Считая t_1, t_2 произвольной парой взаимно простых целых чисел, легко усмотреть, что каждое число, на которое нацело делятся три числа

$$\rho_1(t_1, t_2), \quad \rho_2(t_1, t_2), \quad \rho_3(t_1, t_2),$$

должно быть делителем R. Поэтому, заставляя оба параметра t_1, t_2 независимо друг от друга пробегать полную систему вычетов по модулю R, мы приходим с помощью простого умозаключения к следующему результату:

Конечная система формул

$$\left.\begin{aligned} &x_1 = \alpha_1(\tau_1, \tau_2), \quad x_2 = \alpha_2(\tau_1, \tau_2), \quad x_3 = \alpha_3(\tau_1, \tau_2);\\ &x_1 = \beta_1(\tau_1, \tau_2), \quad x_2 = \beta_2(\tau_1, \tau_2), \quad x_3 = \beta_3(\tau_1, \tau_2);\\ &\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\\ &x_1 = \varkappa_1(\tau_1, \tau_2), \quad x_2 = \varkappa_2(\tau_1, \tau_2), \quad x_3 = \varkappa_3(\tau_1, \tau_2); \end{aligned}\right\} \tag{10}$$

доставляет все неособые целочисленные собственные решения уравнения (1), когда параметры τ_1, τ_2 принимают всевозможные целочисленные значения. При этом α_1, α_2, $\alpha_3, \ldots$, $\varkappa_1$, $\varkappa_2$, $\varkappa_3$ являются неоднородными многочленами с целыми коэффициентами от параметров τ_1, τ_2.

Предыдущее изложение существенно основывалось на том обстоятельстве, что использовавшиеся нами преобразования однозначно обратимы. Однако эта однозначность гарантирована нам лишь для неособых точек кривой (1), так что особые точки еще нуждаются в специальном рассмотрении. Эти точки отвечают общим решениям трех уравнений

$$\frac{df}{dx_1} = 0, \quad \frac{df}{dx_2} = 0, \quad \frac{df}{dx_3} = 0. \tag{11}$$

Поэтому всегда можно с помощью конечного числа рациональных операций выяснить, имеются ли среди особых точки с рациональными координатами. Так найденные «*особые*» решения диофантова уравнения (1) не обязаны получаться из формул (10), как легко увидеть из примеров.

Во втором случае, когда степень n предъявленного уравнения четна, мы, как было указано выше, приходим к квадратному уравнению

$$q(u_1, u_2, u_3) = 0. \tag{12}$$

Мы всегда можем привести это уравнение подходящим линейным преобразованием с целыми рациональными коэффициентами к виду

$$a_1u_1^2 + a_2u_2^2 + a_3u_3^2 = 0, \tag{13}$$

где все a_1, a_2, a_3 свободны от квадратов и попарно взаимно просты. Известно, что уравнение (13) имеет целочисленные решения тогда и только тогда, когда не все числа a_1, a_2, a_3 одного знака, и числа $-a_2a_3$, $-a_3a_1$, $-a_1a_2$ являются квадратичными вычетами по модулю a_1, a_2, a_3 соответственно[2)].

Таким образом, когда это условие выполнено, на коническом сечении, определяемом уравнением (13), имеются точки с рациональными координатами, что позволяет нам с помощью рационального однозначно обратимого преобразования перевести это коническое сечение в прямую линию, или, что то же самое, уравнение (13) в линейное уравнение. К последнему применим тот же самый подход, который был развит нами выше в связи с уравнением (7). Таким образом, и в рассматриваемом сейчас случае наше диофантово уравнение (1) имеет бесконечное число решений, определяемых системой формул типа (10), к которым возможно, добавляется конечное число особых решений.

Если же вышеприведенное условие не выполнено, то на коническом сечении (13) нет точек с рациональными координатами. Следовательно, таких точек нет и на кривой (1), разве только одна или несколько особых точек этой кривой имеют рациональные координаты. Значит, наше уравнение (1) или имеет конечное число (особых) решений или вообще не имеет решений, смотря по тому, допускают или нет уравнения

$$\frac{df}{dx_1} = 0, \quad \frac{df}{dx_2} = 0, \quad \frac{df}{dx_3} = 0$$

общие рациональные решения. Как показывает следующий пример, первая из указанных двух возможностей действительно встречается, т. е. на кривой (1) может лежать особая точка с рациональными координатами и не лежать никаких других точек с рациональными координатами. Пусть φ, ψ_1, ψ_2, ψ_3 — четыре целочисленные квадратичные формы и l — целочисленная линейная форма от переменных u_1, u_2, u_3. Эти формы можно выбрать так, чтобы выполнялись следующие условия: коническое сечение, определенное уравнением

$$\varphi = 0, \tag{14}$$

не имеет точек с рациональными координатами, далее, конические сечения

$$\psi_1 = 0, \quad \psi_2 = 0 \tag{15}$$

проходят через обе точки пересечения конического сечения $\varphi = 0$ и прямой $l = 0$, причем $\varphi = 0$ не принадлежит тому же пучку, что и сечения (15); и, наконец, коническое сечение

$$\psi_3 = 0 \tag{16}$$

[2)] *Legendre A. M.*. Theorie des nombres, 3me éd., T. 1, § III, IV (имеется перевод на немецкий, выполненный Г. Мазером (H. Maser): Leipzig, 1886). См. также *Lejeune-Dirichlet.* Vorlesungen über Zahlentheoric, heransgegeben von R. Dedekind, 3 Aufl., § 157 des X Supplementes.

не содержит вышеупомянутых точек пересечения. Очевидно, можно бесконечным числом способов образовать перечисленные формы, удовлетворяющие указанным условиям. Преобразуя теперь уравнение (14) с помощью формул

$$x_1 : x_2 : x_3 = \psi_1 : \psi_2 : \psi_3, \tag{17}$$

получаем целочисленное уравнение

$$f(x_1, x_2, x_3) = 0, \tag{18}$$

описывающее кривую четвертого порядка и рода нуль. Точкам пересечения прямой $l = 0$ с коническим сечением $\varphi = 0$ соответствует двойная точка нашей кривой четвертого порядка; координаты этой точки имеют рациональные значения

$$\frac{x_1}{x_3} = 0, \quad \frac{x_2}{x_3} = 0.$$

Зато среди неособых точек кривой (18) не найдется имеющих рациональные координаты, потому что такие точки соответствуют точкам конического сечения (14), также имеющим рациональные координаты. Мы хотели бы еще заметить, что при подходящем выборе формы ψ_3 можно, при желании, добиться того, чтобы либо только одна, либо все особые точки кривой (18) имели рациональные координаты.

Из вышеприведенного изложения вытекает следующий окончательный результат для диофантова уравнения

$$f(x_1, x_2, x_3) = 0$$

произвольной степени и рода нуль. *У такого уравнения либо вообще нет решений, либо их конечное число и тогда они являются общими целочисленными решениями уравнений* (11), *либо, наконец, имеется бесконечное число решений, которые, за возможным исключением общих целочисленных решений уравнений* (11), *находятся по системе формул* (10). В случае, когда степень нашего уравнения нечетна, реализуется последний случай. Таким образом, диофантово уравнение нечетной степени и рода нуль всегда имеет бесконечное число решений.

Кёнигсберг в Пруссии, 14 марта 1889 года.

О ДИОФАНТОВЫХ УРАВНЕНИЯХ*)

Дискриминант D уравнения n-ой степени относительно t

$$x_0t^n + x_1t^{n-1} + \ldots + x_n = 0 \tag{1}$$

с неопределенными коэффициентами $x_0, x_1, \ldots, x_n$ и корнями $t_1, t_2, \ldots, t_n$ определяется формулой

$$D = x_0^{2n-2} \prod_{i,k} (t_i - t_k)^2 \quad (i = 1, 2, \ldots, n;\ k = i+1, i+2, \ldots, n);$$

дискриминант D является многочленом степени $2n-2$ от $x_0, x_1, \ldots, x_n$ с целыми рациональными коэффициентами. Ниже мы обсудим диофантово уравнение

$$D = \pm 1. \tag{2}$$

I. *Диофантово уравнение* (2) *всегда имеет рациональные решения* $x_0, x_1, \ldots, x_n$.

Чтобы убедиться в этом, положим в уравнении (1) $x_1 = 0, x_2 = 0, \ldots, x_{n-2} = 0$; тогда уравнение (1) становится трехчленным и мы получаем следующее значение для нашего дискриминанта:

$$D = (-1)^{n(n-1)/2}\{n^n x_0^{n-1} x_n^{n-1} + (1-n)^{n-1} x_0^{n-2} x_{n-1}^n\}.$$

Выражение в фигурных скобках равно ± 1, если мы положим:

$$x_0 = (1-n)^{(n-1)/2}, \quad x_{n-1} = (1-n)^{(-n+1)/2}, \quad x_n = 0,$$

для нечетного n, и

$$x_0 = (1-n)^{(n/2)-1}, \quad x_{n-1} = (1-n)^{-(n/2)+1}, \quad x_n = n^{-1}(1-n)^{-(n/2)+1}.$$

для четного n.

Мне представляется весьма интересным вопрос о *целых* рациональных решениях диофантова уравнения (2); ответ на этот вопрос дает следующая теорема:

II. *При* $n > 3$ *диофантово уравнение* (2) *неразрешимо в целых рациональных числах* $x_0, x_1, \ldots, x_n$. *Единственными уравнениями с целыми рациональными коэффициентами и дискриминантом* ± 1 *являются: квадратное уравнение*

$$(ut + v)(u't + v') = 0$$

и кубическое уравнение

$$(ut + v)(u't + v')([u + u']t + [v + v']t) = 0,$$

---

*) Über diophantische Gleichungen. — Nachr. Ges. Wiss. Göttingen, 1897, S. 48–54. *Перевод Ю. Г. Зархина.*

где u, u', v, v' — любые целые рациональные числа, удовлетворяющие соотношению

$$uv' - u'v = \pm 1.$$

Прежде всего мы докажем следующий факт:

Пусть над полем рациональных чисел имеется неприводимое уравнение n-й степени относительно t

$$a_0 t^n + a_1 t^{n-1} + \ldots + a_n = 0, \tag{3}$$

коэффициенты которого $a_0, a_1, \ldots, a_n$ суть целые рациональные числа; пусть α — корень нашего уравнения и k — определяемое корнем α числовое поле степени n; тогда дискриминант D нашего уравнения (3) всегда является целым рациональным числом, которое содержит дискриминант d поля k в качестве делителя.

Для доказательства запишем α в виде $\alpha = \alpha_1/\alpha_2$, где α_1, α_2 — целые числа из поля k; далее, обозначим через $\mathfrak{a}$ идеал в поле k, являющийся наибольшим общим делителем чисел α_1 и α_2, а через $\mathfrak{a}_1$ и $\mathfrak{a}_2$ — такие идеалы поля k, что

$$\alpha_1 = \mathfrak{a}\,\mathfrak{a}_1, \qquad \alpha_2 = \mathfrak{a}\,\mathfrak{a}_2.$$

Наконец, пусть β_2 — делящееся на $\mathfrak{a}_2$ целое число из k, такое что частное $\beta_2/\mathfrak{a}_2$ взаимно просто с дискриминантом d поля k. Произведение $\alpha\beta_2$ является целым числом из поля k, потому что $\alpha_1\beta_2$ делится на идеал $\alpha_2 = \mathfrak{a}\mathfrak{a}_2$; положив $\beta_1 = \alpha\beta_2$, имеем $\alpha = \beta_1/\beta_2$. Определим идеал $\mathfrak{b}$ как наибольший общий делитель целых чисел β_1, β_2. Обозначая соответствующие этим числам главные идеалы поля k также через β_1, β_2, получаем

$$\beta_1 = \frac{\beta_2}{\mathfrak{a}_2}\,\mathfrak{a}_1, \qquad \beta_2 = \frac{\beta_2}{\mathfrak{a}_2}\,\mathfrak{a}_2.$$

Поскольку $\mathfrak{a}_1$ и $\mathfrak{a}_2$ имеют в качестве наибольшего общего делителя идеал 1, мы видим, что наибольший общий делитель $\mathfrak{b}$ целых чисел β_1 и β_2 равен частному $\beta_2/\mathfrak{a}_2$ и, следовательно, идеал $\mathfrak{b}$ взаимно прост с дискриминантом d поля k.

Обозначая числа, сопряженные к α, β_1, β_2 через $\alpha', \ldots, \alpha^{(n-1)}$, $\beta_1', \ldots$ $\ldots, \beta_1^{(n-1)}, \beta_2', \ldots, \beta_2^{(n-1)}$ соответственно, мы получаем следующее выражение для дискриминанта D уравнения (3):

$$D = a_0^{2n-2} \begin{vmatrix} 1 & \alpha & \ldots & \alpha^{n-1} \\ 1 & \alpha' & \ldots & \alpha'^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \alpha^{(n-1)} & \ldots & \left(\alpha^{(n-1)}\right)^{n-1} \end{vmatrix}^2.$$

Подставляя сюда $\alpha = \beta_1/\beta_2, \alpha' = \beta_1'/\beta_2', \ldots, \alpha^{(n-1)} = \beta_1^{(n-1)}/\beta_2^{(n-1)}$, приходим к равенству

$$D = \frac{a_0^{2n-2} B}{(n(\beta_2))^{2n-2}}, \tag{4}$$

где $\mathfrak{n}(\beta_2)$ обозначает норму числа β_2 в k и где

$$B = \begin{vmatrix} \beta_1^{n-1} & \beta_1^{n-2}\beta_2 & \dots & \beta_2^{n-1} \\ \beta_1'^{n-1} & \beta_1'^{n-2}\beta_2' & \dots & \beta_2'^{n-1} \\ \dots\dots & \dots\dots & \dots\dots & \dots\dots \\ \left(\beta_1^{(n-1)}\right)^{n-1} & \left(\beta_1^{(n-1)}\right)^{n-2}\beta_2^{(n-1)} & \dots & \left(\beta_2^{(n-1)}\right)^{n-1} \end{vmatrix}^2. \tag{5}$$

Произведение

$$(\beta_2 t - \beta_1)(\beta_2' t - \beta_1') \dots (\beta_2^{(n-1)} t - \beta_1^{(n-1)}),$$

где t — независимая переменная, есть многочлен с целыми рациональными коэффициентами. По теореме, впервые сформулированной и доказанной Кронекером[1], наибольший общий делитель целых рациональных коэффициентов этого многочлена равен норме $n(\mathfrak{b})$ идеала $\mathfrak{b}$. В нашем доказательстве мы можем, не ограничивая общности, считать, что наибольший общий делитель коэффициентов $a_0, a_1, \dots, a_n$ в (3) равен 1. При этом предположении проведенные выше рассуждения дают тождественное по t соотношение

$$(\beta_2 t - \beta_1)(\beta_2' t - \beta_1') \dots (\beta_2^{(n-1)} t - \beta_1^{(n-1)}) = \pm n(b)(a_0 t^n + a_1 t^{n-1} + \dots + a_n).$$

Приравнивая коэффициенты при t^n, получаем

$$n(\beta_2) = \pm a_0 n(\mathfrak{b}).$$

Ввиду этого равенства формула (4) приобретает вид

$$D = \frac{B}{n(\mathfrak{b})^{2n-2}}.$$

Поскольку B, как немедленно следует из (5), делится на дискриминант d поля k и, поскольку $\mathfrak{b}$, а значит и $n(\mathfrak{b})$ взаимно просты с d, отсюда вытекает справедливость сформулированного нами утверждения.

Чтобы теперь доказать теорему II для диофантова уравнения (2), мы привлечем теорему Г. Минковского[2], согласно которой дискриминант алгебраического числового поля всегда отличен от ± 1. Поэтому, с учетом ранее доказанного нами факта любое неприводимое уравнение (3) над полем рациональных чисел обязано иметь дискриминант, отличный от ± 1. С другой стороны, дискриминант приводимого уравнения с целыми рациональными коэффициентами должен, в силу известных теорем, делиться на дискриминанты всех целочисленных делителей левой части. Отсюда следует, что дискриминант D уравнения (3) только тогда может быть равен ± 1, когда левая часть этого уравнения полностью разлагается на линейные множители с целыми рациональными коэффициентами.

Далее, для того чтобы дискриминант уравнения n-й степени

$$(ut + v)(u't + v') \dots (u^{(n-1)} t + v^{(n-1)}) = 0, \tag{6}$$

---

[1] Grundzuge einer arithmetischen Theorie der algebraischen Großen. — J. Math., Bd. 92, S. 1. См. в связи с этим мое сообщение «Die Theorie der algebraischen Zahlkörper», представленное Немецкому математическому объединению (Bd. 4, S. 190, Satz 20).

[2] Geometrie der Zahlen. — Leipzig, 1896, S. 130. См. также мое упомянутое в предыдущем подстрочном примечании сообщение (S. 211, Satz 44).

где $u, v, u', v', \ldots, u^{(n-1)}, v^{(n-1)}$ — целые рациональные числа, равнялся ± 1, необходимо, чтобы все $n(n-1)/2$ определителей

$$uv' - u'v, \quad uv'' - u''v, \ \ldots, \ u^{(n-2)}v^{(n-1)} - u^{(n-1)}v^{(n-2)} \tag{7}$$

равнялись ± 1. Подставим в (6)

$$t = \frac{-v + v't'}{u - u't'}$$

и умножим затем на $(u - u't')^n$; левая часть получившегося уравнения имеет тот же самый вид, что и в исходном уравнении (6); однако теперь

$$u = \pm 1, \quad v = 0, \quad u' = 0, \quad v' = \pm 1.$$

Так как выражения (7) должны принимать значения ± 1, мы заключаем, что степень n может быть равна лишь 2 или 3, причем в последнем случае должны выполняться равенства

$$u'' = \pm 1, \quad v'' = \pm 1.$$

Тем самым теорема II полностью доказана.

В заключение приведем еще несколько общих замечаний о диофантовых уравнениях.

Когда хотят доказать, что данное диофантово уравнение неразрешимо в рациональных числах, то во многих случаях это удается сделать, переходя от исходного уравнения к соответствующему сравнению и показывая, что это сравнение неразрешимо по модулю некоторого простого числа или по модулю степени простого числа. В случае квадратного уравнения с двумя неизвестными верно и обратное: из разрешимости всех сравнений, получающихся из данного уравнения, вытекает разрешимость этого уравнения в рациональных числах. А именно, используя известный критерий разрешимости тернарного квадратного диофантова уравнения, мы можем получить следующую *теорему*[3]:

Пусть m, n — произвольные целые рациональные числа. Диофантово уравнение

$$mx^2 + ny^2 = 1$$

всегда разрешимо в рациональных числах x, y, если по модулю любого простого числа и любой степени такого числа разрешимо в целых рациональных числах x, y сравнение

$$mx^2 + ny^2 \equiv 1.$$

Как показывают примеры уравнений

$$y^2 + 7(x^2+1)(x^2-2)^2(x^2+2)^2 = 0, \tag{8}$$

$$y^2 - 3(x^2+1)^2(x^2-2)^2(x^2+2)^2(x^2+7) = 0 \tag{9}$$

эта теорема непосредственно не переносится на уравнения высших степеней. Левые части уравнений (8), (9) являются неприводимыми многочленами от x, y. Ни одно из уравнений (8), (9) не имеет рациональных решений x, y. Обозначим через p произвольное нечетное простое число. Среди трех

[3] Ср. с моим упомянутым выше сообщением (S. 299, Satz 102).

чисел $-1, +2, -2$ по крайней мере одно является квадратичным вычетом по модулю p; обозначим это число через r, и пусть e — произвольный целочисленный показатель. Тогда можно найти целое рациональное число a, для которого $a^2 \equiv r$ по модулю p^e и, следовательно, сравнение

$$y^2 + 7(x^2+1)(x^2-2)^2(x^2+2)^2 \equiv 0, \quad (p^e)$$

имеет решение $x = a, y = 0$. Далее, пусть 2^e — произвольная степень двойки. Как легко видеть, всегда найдется целое рациональное число b, такое что $b^2 + 7 \cdot 2^4 \equiv 0$ по модулю 2^e и, следовательно, $x = 0, y = b$ — решение сравнения

$$y^2 + 7(x^2+1)(x^2-2)^2(x^2+2)^2 \equiv 0, \quad (2^e).$$

Аналогично устанавливается справедливость нашего утверждения для уравнения (9).

Только что рассмотренная ситуация дает основания для предположения о том, что может существовать многочлен от t с целыми рациональными коэффициентами, неприводимый над полем рациональных чисел и все же приводимый по модулю любого простого числа и любой его степени. И в самом деле, например, произведение

$$\left(t + \frac{\sqrt{5}+\sqrt{-31}}{2}\right)\left(t + \frac{-\sqrt{5}+\sqrt{-31}}{2}\right)\left(t + \frac{\sqrt{5}-\sqrt{-31}}{2}\right)\times$$
$$\times \left(t + \frac{-\sqrt{5}-\sqrt{-31}}{2}\right) = t^4 + 13t^2 + 81 \quad (10)$$

является неприводимым многочленом четвертой степени с целыми рациональными коэффициентами, в то время как по модулю любого простого числа и любой степени такого числа этот многочлен распадается в произведение двух многочленов с целыми рациональными коэффициентами. Доказательство этого факта легко получается следующим способом. Простое число 31 в квадратичном поле $k_1 = k(\sqrt{5})$, определяемом посредством $\sqrt{5}$, и простое число 5 в квадратичном поле $k_2 = k(\sqrt{-31})$, определяемом посредством $\sqrt{-31}$, распадаются каждое на два отличных друг от друга простых идеала. Далее, как нетрудно проверить, каждое простое число, отличное от 5 и 31, может быть представлено как произведение двух отличных друг от друга простых идеалов по крайней мере в одном из трех квадратичных полей k_1, k_2 или $k_3 = k(\sqrt{-5 \cdot 31})$. Обозначим теперь через p произвольное простое число, и пусть k — одно из полей k_1, k_2, k_3, такое что в нем p распадается в произведение двух отличных друг от друга идеалов $\mathfrak{p}, \mathfrak{p}'$; затем выберем из произведения в левой части (10) два множителя, таких что их произведение есть квадратный многочлен

$$t^2 + \alpha t + \beta,$$

коэффициенты которого — целые алгебраические числа, лежащие в k. Произведение остальных двух множителей представляет собой некоторый многочлен

$$t^2 + \alpha' t + \beta',$$

где α', β' — тоже целые числа из k. Тогда $\mathfrak{p}$, входя в разложение числа p лишь с показателем 1, оказывается простым идеалом первой степени в k, откуда видно, что при любом показателе e существует четверка целых рациональных чисел a, b, a', b', таких что $\alpha \equiv a$, $\beta \equiv b$, $\alpha' \equiv a'$, $\beta' \equiv b'$ по модулю $\mathfrak{p}^e$. Отсюда вытекает сравнение

$$(t^2 + \alpha t + \beta)(t^2 + \alpha' t + \beta') \equiv (t^2 + at + b)(t^2 + a't + b'), \quad (\mathfrak{p}^e),$$

из которого следует, что

$$t^4 + 13t^2 + 81 \equiv (t^2 + at + b)(t^2 + a't + b'), \quad (\mathfrak{p}^e).$$

Гёттинген, 20 февраля 1897 г.

О НЕПРИВОДИМОСТИ МНОГОЧЛЕНОВ С ЦЕЛОЧИСЛЕННЫМИ КОЭФФИЦИЕНТАМИ*)

Если задан многочлен (ganze rationale Funktion) с целочисленными коэффициентами от переменных $x, y, \ldots, w; t, r, \ldots, q$ и мы, оставив часть из них, скажем $x, y, \ldots, w$, переменными, будем присваивать остальным переменным $t, r, \ldots, q$ произвольные целые, положительные или отрицательные, значения, возникнет бесконечная система многочленов от переменных $x, y, \ldots, w$ с целыми коэффициентами. Поставим вопрос: обязательно ли в этой системе найдутся неприводимые многочлены от переменных $x, y, \ldots, w$, если исходный многочлен от переменных $x, y, \ldots, w; t, r, \ldots, q$ был неприводимым? Многочлен с целыми коэффициентами называется неприводимым, если он не представим в виде произведения двух многочленов с целыми рациональными коэффициентами. Изучение этого вопроса и его обобщение на случай произвольной области рациональности проливают новый свет на понятие неприводимости; кроме того, полученные ниже результаты допускают разнообразные применения, в частности, в теории уравнений и областей рациональности.

Наши результаты основываются на следующей лемме:

Пусть задана бесконечная последовательность $a_1, a_2, a_3, \ldots$, каждый элемент которой есть целое положительное число, не превосходящее некоторого фиксированного числа a, т. е. одно из чисел $1, 2, \ldots, a$, и пусть задано некоторое целое положительное число m. Тогда можно определить m целых положительных чисел $\mu^{(1)}, \mu^{(2)}, \ldots, \mu^{(m)}$ таким образом, чтобы для бесконечного множества значений μ все 2^m элементов

$$a_\mu,$$

$$a_{\mu+\mu^{(1)}},$$

$$a_{\mu+\mu^{(2)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(2)}},$$

$$a_{\mu+\mu^{(3)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(3)}}, \quad a_{\mu+\mu^{(2)}+\mu^{(3)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(2)}+\mu^{(3)}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{\mu+\mu^{(m)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(m)}}, \quad a_{\mu+\mu^{(2)}+\mu^{(m)}}, \ldots, a_{\mu+\mu^{(1)}+\mu^{(2)}+\ldots+\mu^{(m)}}$$

совпадали с одним и тем же числом G, где G — одно из чисел $1, 2, \ldots, a$. При этом, индекс $\mu+\mu^{(1)}$ второго элемента получается прибавлением числа $\mu^{(1)}$ к индексу μ первого элемента, индексы третьего и четвертого элементов получаются прибавлением числа $\mu^{(2)}$ к индексам первого и второго элементов; индексы пятого, шестого, седьмого и восьмого элементов — прибавлением

---

*) Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. — J. reine und angew. Math., 1892, Bd. 110, S. 104–129. *Перевод Г. В. Белого.*

числа $\mu^{(3)}$ к индексам первых четырех элементов; и, наконец, индексы последних 2^{m-1} элементов получаются, если к уже определенным индексам первых 2^{m-1} элементов прибавить число $\mu^{(m)}$.

Для доказательства надо будет рассмотреть отдельные части заданной последовательности. В частности, если взять i следующих друг за другом элементов последовательности, скажем $a_\mu, a_{\mu+1}, a_{\mu+2}, \ldots, a_{\mu+i-1}$, то я буду называть такие i элементов интервалом длины i. Рассмотрим какой-нибудь интервал длины $a+1$. В нем хотя бы одно из чисел $1, 2, \ldots, a$ должно встретиться не менее двух раз; пусть это будет число G. Это означает, что в нашем интервале длины $a+1$ найдется хотя бы один из следующих подынтервалов («цепочек»):

$$G_2^{(1)} = GG$$

$$G_3^{(1)} = G.G$$

$$G_4^{(1)} = G..G$$

$$\ldots\ldots\ldots$$

$$G_{a+1}^{(1)} = G\ldots\ldots G.$$

Здесь мы для краткости обозначили через $G_s^{(1)}$ интервал длины s, у которого начало и конец равны числу G. Очевидно, что количество всех таких возможных цепочек $G_s^{(1)}$ равно a^2 и потому всегда меньше числа $(a+1)^2$. Теперь рассмотрим $(a+1)^2$ следующих друг за другом без перекрытий интервалов, каждый из которых имеет длину $a+1$. Вместе они образуют интервал длины $(a+1)^3$, в котором хотя бы одна из цепочек $G_s^{(1)}$ должна встретиться не менее двух раз. Обозначим такую цепочку через $G_{\nu^{(1)}}^{(1)}$. Это означает, что в интервале длины $(a+1)^3$ встретится хотя бы одна из следующих цепочек:

$$G_{2\nu^{(1)}}^{(2)} = G_{\nu^{(1)}}^{(1)} G_{\nu^{(1)}}^{(1)},$$

$$G_{2\nu^{(1)}+1}^{(2)} = G_{\nu^{(1)}}^{(1)} . G_{\nu^{(1)}}^{(1)},$$

$$G_{2\nu^{(1)}+2}^{(2)} = G_{\nu^{(1)}}^{(1)} .. G_{\nu^{(1)}}^{(1)},$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$G_{(a+1)^3}^{(2)} = G_{\nu^{(1)}}^{(1)} \ldots\ldots G_{\nu^{(1)}}^{(1)}.$$

Здесь $G_s^{(2)}$ обозначает интервал длины s, который начинается цепочкой $G_{\nu^{(1)}}^{(1)}$ и такой же цепочкой заканчивается. Очевидно, что количество всех попарно различных цепочек $G_s^{(2)}$ меньше произведения длины $(a+1)^3$ этого интервала на количество всех возможных цепочек $G_s^{(1)}$, и следовательно, меньше, чем $(a+1)^5$. Если теперь в нашей последовательности мы выберем $(a+1)^5$ следующих друг за другом интервалов длины $(a+1)^3$, то в совокупном интервале длины $(a+1)^8$ хотя бы одна из цепочек $G_s^{(2)}$, скажем $G_{\nu^{(2)}}^{(2)}$, встретится не менее двух раз. Это означает, что в интервале длины $(a+1)^8$ хотя

бы один раз встретится одна из следующих цепочек:

$$G^{(3)}_{2\nu^{(2)}} = G^{(2)}_{\nu^{(2)}} G^{(2)}_{\nu^{(2)}},$$

$$G^{(3)}_{2\nu^{(2)}+1} = G^{(2)}_{\nu^{(2)}} . G^{(2)}_{\nu^{(2)}},$$

$$G^{(3)}_{2\nu^{(2)}+2} = G^{(2)}_{\nu^{(2)}} \,..\, G^{(2)}_{\nu^{(2)}},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$G^{(3)}_{(a+1)^s} = G^{(2)}_{\nu^{(2)}} \,\ldots\ldots\, G^{(2)}_{\nu^{(2)}}.$$

Здесь $G^{(3)}_s$ обозначает интервал длины s, который начинается и заканчивается цепочкой $G^{(2)}_{\nu^{(2)}}$.

После m-кратного применения этой процедуры мы приходим к цепочкам, имеющим вид

$$G^{(m)} = G^{(m-1)} \,\ldots\ldots\, G^{(m-1)},$$

и видим, что в каждом интервале нашей последовательности достаточно большой длины l должна обязательно встретиться одна из цепочек $G^{(m)}$. При этом l зависит только от a и m. С другой стороны, количество всех различных цепочек $G^{(m)}$ не превосходит некоторого достаточно большого числа k, которое можно легко выразить через a и m. В заданной последовательности мы можем выбрать бесконечно много следующих друг за другом интервалов длины l, и следовательно, хотя бы одна из цепочек $G^{(m)}$ встречается в последовательности бесконечно часто. Пусть это будет следующая цепочка:

$$G^{(m)}_{\nu^{(m)}} = G^{(m-1)}_{\nu^{(m-1)}} \,\ldots\ldots\, G^{(m-1)}_{\nu^{(m-1)}},$$

где $G^{(m)}_{\nu^{(m)}}$ и $G^{(m-1)}_{\nu^{(m-1)}}$ обозначают интервалы длины $\nu^{(m)}$ и $\nu^{(m-1)}$ соответственно.

Теперь уже легко установить справедливость сформулированной выше леммы. А именно, найденная цепочка $G^{(m)}_{\nu^{(m)}}$ представляется рекурсивно в следующем виде:

$$G^{(1)}_{\nu^{(1)}} = G \,\ldots\ldots G,$$

$$G^{(2)}_{\nu^{(2)}} = G^{(1)}_{\nu^{(1)}} \,\ldots\ldots G^{(1)}_{\nu^{(1)}},$$

$$G^{(3)}_{\nu^{(3)}} = G^{(2)}_{\nu^{(2)}} \,\ldots\ldots G^{(2)}_{\nu^{(2)}},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$G^{(m)}_{\nu^{(m)}} = G^{(m-1)}_{\nu^{(m-1)}} \,\ldots\ldots G^{(m-1)}_{\nu^{(m-1)}},$$

где нижние индексы указывают количество элементов в соответствующих интервалах. Я полагаю

$$\mu^{(1)} = \nu^{(1)} - 1,$$

$$\mu^{(2)} = \nu^{(2)} - \nu^{(1)},$$

$$\mu^{(3)} = \nu^{(3)} - \nu^{(2)},$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\mu^{(m)} = \nu^{(m)} - \nu^{(m-1)}.$$

и утверждаю, что определенные таким образом целые положительные числа $\mu^{(1)}, \mu^{(2)}, \ldots, \mu^{(m)}$ обладают тем свойством, которое требуется в нашей лемме. Действительно, уже доказано, что в заданной последовательности $a_1, a_2, a_3, \ldots$ цепочка $G^{(m)}_{\nu^{(m)}}$ встречается бесконечно часто, т. е. существует бесконечно много целых μ, для которых

$$a_\mu a_{\mu+1} \ldots a_{\mu+\nu^{(m)}-1} = G^{(m)}_{\nu^{(m)}}.$$

Из построения цепочки $G^{(m)}_{\nu^{(m)}}$ следует, что

$$a_\mu = G,$$

$$a_{\mu+\mu^{(1)}} = G,$$

$$a_{\mu+\mu^{(2)}} = a_{\mu+\mu^{(1)}+\mu^{(2)}} = G,$$

$$a_{\mu+\mu^{(3)}} = a_{\mu+\mu^{(1)}+\mu^{(3)}} = a_{\mu+\mu^{(2)}+\mu^{(3)}} = a_{\mu+\mu^{(1)}+\mu^{(2)}+\mu^{(3)}} = G,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{\mu+\mu^{(m)}} = a_{\mu+\mu^{(1)}+\mu^{(m)}} = a_{\mu+\mu^{(2)}+\mu^{(m)}} = \ldots = a_{\mu+\mu^{(1)}+\mu^{(2)}+\ldots+\mu^{(m)}} = G,$$

и тем самым наша лемма доказана.

Теперь мы вернемся к поставленному вначале вопросу и докажем следующую теорему:

I. *Пусть $f(x,t)$ — неприводимый многочлен от переменных x и t с целочисленными коэффициентами. Существует бесконечно много способов подставить в $f(x,t)$ вместо t целое рациональное число так, что многочлен $f(x,t)$ окажется неприводимым многочленом от одной переменной x.* (При этом многочлен с целочисленными коэффициентами называется неприводимым, если его нельзя представить в виде произведения нескольких таких же многочленов с целочисленными коэффициентами.)

Запишем $f(x,t)$ в виде

$$f(x,t) = Tx^n + T_1x^{n-1} + \ldots + T_n,$$

где $T, T_1, \ldots, T_n$ — многочлены от t с целочисленными коэффициентами, и приведем доказательство от противного. Допустим, что многочлен $f(x,t)$ становится равным произведению двух или нескольких многочленов от x с целыми коэффициентами, если только вместо t подставить целое положительное число, большее некоторого достаточно большого фиксированного числа C. Сделав подстановку $x = y/T$, мы получаем

$$f(x,t) = \frac{1}{T^{n-1}}(y^n + S_1y^{n-1} + S_2y^{n-2} + \ldots + S_n),$$

где $S, S_1, \ldots, S_n$ опять обозначают многочлены от t с целочисленными коэффициентами. Тогда многочлен

$$g(y,t) = y^n + S_1y^{n-1} + S_2y^{n-2} + \ldots + S_n$$

является приводимым для всех целых положительных значений t, больших определенной границы C', где $C' \geqslant C$, которую можно выбрать так, чтобы для всех таких значений t многочлен T был отличен от нуля.

Рассмотрим теперь для n корней $y_1, y_2, \ldots, y_n$ уравнения

$$y^n + S_1 y^{n-1} + S_2 y^{n-2} + \ldots + S_n = 0$$

разложение Пюизё[1] по целым степеням $\tau = t^{1/k}$, где k есть определяемое известным способом целое положительное число и где под $t^{1/k}$ мы понимаем положительное вещественное значение корня. Такое разложение начинается с конечного числа целых положительных степеней τ. Пусть h — наибольшая из этих положительных степеней. Тогда мы имеем разложения

$$\begin{aligned}
y_1 &= \alpha_1\tau^h + \beta_1 t^{h-1} + \ldots + \lambda_1 + \frac{\pi_1}{\tau} + \frac{\rho_1}{\tau^2} + \frac{\sigma_1}{\tau^3} + \ldots,\\
y_2 &= \alpha_2\tau^h + \beta_2 t^{h-1} + \ldots + \lambda_2 + \frac{\pi_2}{\tau} + \frac{\rho_2}{\tau^2} + \frac{\sigma_2}{\tau^3} + \ldots,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
y_n &= \alpha_n\tau^h + \beta_n t^{h-1} + \ldots + \lambda_n + \frac{\pi_n}{\tau} + \frac{\rho_n}{\tau^2} + \frac{\sigma_n}{\tau^3} + \ldots,
\end{aligned}$$

где коэффициенты $\alpha, \beta, \ldots, \lambda, \pi, \rho, \sigma, \ldots$ представляют собой вполне определенные рациональные или иррациональные, вещественные или комплексные числа. Эти степенные ряды сходятся, когда $t = \tau^k$ больше некоторого достаточно большого положительного числа C''.

Выберем теперь из n корней $y_1, y_2, \ldots, y_n$ какую-нибудь пару, скажем y_1 и y_2, и построим степенные ряды для двух элементарных симметрических функций:

$$y_1 + y_2 = (\alpha_1 + \alpha_2)\tau^h + (\beta_1 + \beta_2)\tau^{h-1} + \ldots,$$

$$y_1 y_2 = \alpha_1\alpha_2\tau^{2h} + (\alpha_1\beta_2 + \alpha_2\beta_1)\tau^{2h-1} + \ldots$$

Так как существует $\frac{n(n-1)}{1\cdot 2} = \binom{n}{2}$ способов выбрать два из n корней $y_1, y_2, \ldots, y_n$, мы получаем $\binom{n}{2}$ систем, каждая из которых состоит из пары степенных рядов. Затем выберем из n корней $y_1, y_2, \ldots, y_n$ тройку, скажем, y_1, y_2, y_3, и построим степенные ряды для трех элементарных симметрических функций:

$$\begin{aligned}
y_1 + y_2 + y_3 &= (\alpha_1 + \alpha_2 + \alpha_3)\tau^h + (\beta_1 + \beta_2 + \beta_3)\tau^{h-1} + \ldots,\\
y_1y_2 + y_2y_3 + y_3y_1 &= (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)\tau^{2h} +\\
&\quad + (\alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_2\beta_3 + \alpha_3\beta_2 + \alpha_3\beta_1 + \alpha_1\beta_3)\tau^{2h-1} + \ldots,\\
y_1y_2y_3 &= \alpha_1\alpha_2\alpha_3\tau^{3h} + (\alpha_1\alpha_2\beta_3 + \alpha_1\alpha_3\beta_2 + \alpha_2\alpha_3\beta_1)\tau^{3h-1} + \ldots
\end{aligned}$$

Так как имеется $\binom{n}{3}$ способов выбрать три из n корней $y_1, y_2, \ldots, y_n$, мы получаем $\binom{n}{3}$ систем, состоящих из троек степенных рядов. Аналогично мы получаем $\binom{n}{4}$ систем по четыре степенных ряда, $\binom{n}{5}$ систем по пять степенных рядов и т. д. Наконец, выберем $n-1$ из n корней $y_1, y_2, \ldots, y_n$,

---

[1] Оригинальную работу Пюизё (Puiseux) можно найти в Liouvilles J., 1850, vol. 15; 1851, vol. 16. Используя эти степенные разложения, С. Рунге показал, что при некоторых определенных условиях уравнение с двумя неизвестными имеет бесконечно много целочисленных решений, см.: J. reine und angew. Math., Bd. 100, S. 425.

скажем $y_1, y_2, \ldots, y_{n-1}$, и построим степенные ряды для $n-1$ элементарных симметрических функций:

$$y_1 + y_2 + \ldots + y_{n-1} = (\alpha_1 + \alpha_2 + \ldots + \alpha_{n-1})\tau^h + \\ + (\beta_1 + \beta_2 + \ldots + \beta_{n-1})\tau^{h-1} + \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_{n-1} = \alpha_1\alpha_2 \ldots \alpha_{n-1}\tau^{(n-1)h} + \\ + (\alpha_1\alpha_2 \ldots \alpha_{n-2}\beta_{n-1} + \ldots + \alpha_2\alpha_3 \ldots \alpha_{n-1}\beta_1)\tau^{h(n-1)-1} + \ldots$$

Таким образом, получим $\binom{n}{n-1} = n$ систем, каждая из которых состоит из $n-1$ степенных рядов.

Если теперь мы возьмем еще и n исходных рядов, считая каждый из них системой, мы получим всего $n + \binom{n}{2} + \binom{n}{3} + \ldots + \binom{n}{n-1} = 2^n - 2$ систем степенных рядов. Выстроим эти системы одну за другой и занумеруем числами $1, 2, \ldots, 2^n - 2$.

После того как это будет сделано, выберем простое число p, которое больше обоих чисел C' и C'', и подставим во все степенные ряды наших 2^n-2 систем вместо τ положительное вещественное значение корня $p^{1/k}$. Из нашего предположения следует, что многочлен с целочисленными коэффициентами $g(y, p)$ приводим, т. е. может быть разложен в произведение двух таких же многочленов. Поэтому среди наших $2^n - 2$ систем существует хотя бы одна, у которой все степенные ряды принимают целые рациональные значения, если τ положить равным $p^{1/k}$. Пусть номером первой из таких систем будет a_1. Положим, далее, $\tau = 2p^{1/k}$. Многочлен $g(y, 2^k p)$ приводим, и среди наших $2^n - 2$ систем должна найтись хотя бы одна, у которой степенные ряды при $\tau = 2p^{1/k}$ принимают целочисленные значения. Пусть a_2 есть номер первой из таких систем. После подстановки $\tau = 3p^{1/k}$ найдем такую же систему с номером a_3, и так далее.

Таким образом получается бесконечная числовая последовательность $a_1, a_2, a_3, \ldots$, в которой любое a_s равно одному из чисел $1, 2, \ldots, 2^n - 2$. Мы применим к этой последовательности доказанную ранее лемму, полагая $a = 2^n - 2$, $m = (n-1)h + 1$. Из леммы следует существование m чисел $\mu^{(1)}, \mu^{(2)}, \ldots, \mu^{(m)}$, для которых все 2^m элементов

$$a_\mu,$$

$$a_{\mu+\mu^{(1)}},$$

$$a_{\mu+\mu^{(2)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(2)}},$$

$$a_{\mu+\mu^{(3)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(3)}}, \quad a_{\mu+\mu^{(2)}+\mu^{(3)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(2)}+\mu^{(3)}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{\mu+\mu^{(m)}}, \quad a_{\mu+\mu^{(1)}+\mu^{(m)}}, \quad a_{\mu+\mu^{(2)}+\mu^{(m)}}, \ \ldots, \ a_{\mu+\mu^{(1)}+\mu^{(2)}+\ldots+\mu^{(m)}}$$

равны одному и тому же числу G для бесконечного количества значений μ. Здесь G обозначает одно из чисел $1, 2, \ldots, 2^n - 2$, так что G есть номер одной из наших систем, которая состоит из ν степенных рядов. Эти ряды можно

представить в следующем виде:

$$y_1 + y_2 + \ldots + y_\nu = \mathsf{A}_1\tau^{m-1} + \mathsf{B}_1\tau^{m-2} + \ldots + \Lambda_1 + \frac{\Pi_1}{\tau} + \frac{\mathsf{P}_1}{\tau^2} + \frac{\Sigma_1}{\tau^3} + \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = \mathsf{A}_\nu\tau^{m-1} + \mathsf{B}_\nu\tau^{m-2} + \ldots + \Lambda_\nu + \frac{\Pi_\nu}{\tau} + \frac{\mathsf{P}_\nu}{\tau^2} + \frac{\Sigma_\nu}{\tau^3} + \ldots,$$

где коэффициенты $\mathsf{A}, \mathsf{B}, \ldots, \Lambda, \Pi, \mathsf{P}, \Sigma, \ldots$ суть вполне определенные рациональные или иррациональные, вещественные или комплексные числа; некоторые из них, возможно, равны нулю. Положительные степени τ в этих рядах не превосходят числа $m-1=(n-1)h$. Полагая во всех этих ν степенных рядах $\tau = \sigma p^{1/k}$, получаем

$$y_1 + y_2 + \ldots + y_\nu = A_1\sigma^{m-1} + B_1\sigma^{m-2} + \ldots + L_1 + \frac{P_1}{\sigma} + \frac{R_1}{\sigma^2} + \frac{S_1}{\sigma^3} + \ldots,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = A_\nu\sigma^{m-1} + B_\nu\sigma^{m-2} + \ldots + L_\nu + \frac{P_\nu}{\sigma} + \frac{R_\nu}{\sigma^2} + \frac{S_\nu}{\sigma^3} + \ldots,$$

где коэффициенты $A, B, \ldots, L, P, R, S$ опять представляют собой некоторые определенные числа.

Как показывают наши разложения, существует бесконечно много таких целых чисел μ, таких что правые части последних формул дают целые числа, если подставить вместо σ одно из чисел

$$\mu,$$

$$\mu + \mu^{(1)},$$

$$\mu + \mu^{(2)}, \quad \mu + \mu^{(1)} + \mu^{(2)},$$

$$\mu + \mu^{(3)}, \quad \mu + \mu^{(1)} + \mu^{(3)}, \quad \mu + \mu^{(2)} + \mu^{(3)}, \quad \mu + \mu^{(1)} + \mu^{(2)} + \mu^{(3)},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mu + \mu^{(m)}, \quad \mu + \mu^{(1)} + \mu^{(m)}, \quad \mu + \mu^{(2)} + \mu^{(m)}, \ldots, \mu + \mu^{(1)} + \mu^{(2)} + \ldots + \mu^{(m)}.$$

Выберем теперь один из ν степенных рядов рассматриваемой системы, скажем степенной ряд

$$\mathfrak{P}(\sigma) = A_1\sigma^{m-1} + B_1\sigma^{m-2} + \ldots + L_1 + \frac{P_1}{\sigma} + \frac{R_1}{\sigma^2} + \frac{S_1}{\sigma^3} + \ldots$$

и построим из него следующие m степенных рядов:

$$\mathfrak{P}^{(1)}(\sigma) = \mathfrak{P}(\sigma) - \mathfrak{P}(\sigma + \mu^{(1)}),$$

$$\mathfrak{P}^{(2)}(\sigma) = \mathfrak{P}^{(1)}(\sigma) - \mathfrak{P}^{(1)}(\sigma + \mu^{(2)}),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathfrak{P}^{(m)}(\sigma) = \mathfrak{P}^{(m-1)}(\sigma) - \mathfrak{P}^{(m-1)}(\sigma + \mu^{(m)}).$$

Из уже доказанных фактов следует, что каждый из этих m степенных рядов для бесконечного количества целых аргументов $\sigma = \mu$ принимает целочисленные значения. Положим для краткости

$$\varphi_{m-1}(\sigma) = A_1\sigma^{m-1} + B_1\sigma^{m-2} + \ldots + L_1.$$

Пусть последующие коэффициенты $P_1, R_1, S_1, \ldots$ степенного ряда $\mathfrak{P}(\sigma)$ не все равны нулю, и пусть V_1/σ^v обозначает первое ненулевое слагаемое. Тогда мы имеем:

$$\mathfrak{P}^{(1)}(\sigma) = \varphi_{m-1}(\sigma) - \varphi_{m-1}(\sigma + \mu^{(1)}) + V_1 \left[\frac{1}{\sigma^v} - \frac{1}{(\sigma + \mu^{(1)})^v} \right] + \ldots$$

Первая стоящая справа разность является многочленом от σ степени $m-2$; положим

$$\varphi_{m-2}(\sigma) = \varphi_{m-1}(\sigma) - \varphi_{m-1}(\sigma + \mu^{(1)}).$$

Разлагая остальные слагаемые правой части по убывающим степеням σ, получим

$$\mathfrak{P}^{(1)}(\sigma) = \varphi_{m-2}(\sigma) + \mu^{(1)} v \frac{V_1}{\sigma^{v+1}} + \ldots$$

Тем же способом получим

$$\mathfrak{P}^{(2)}(\sigma) = \varphi_{m-3}(\sigma) + \mu^{(1)}\mu^{(2)} v(v+1) \frac{V_1}{\sigma^{v+2}} + \ldots,$$

где $\varphi_{m-3}(\sigma)$ обозначает многочлен от σ степени $m-3$. После m-кратного повторения этих рассуждений приходим к формуле

$$\mathfrak{P}^{(m)}(\sigma) = \mu^{(1)}\mu^{(2)} \ldots v(v+1) \ldots (v+m-1) \frac{V_1}{\sigma^{v+m}} + \ldots$$

Так как этот степенной ряд начинается с отрицательной степени σ, должно существовать такое положительное число Γ, что для всех σ, превосходящих Γ, сумма этого ряда по абсолютной величине меньше единицы. С другой стороны, для бесконечного количества целых аргументов σ эта сумма равна целому числу. Так как нуль — единственное целое число, абсолютная величина которого меньше единицы, мы заключаем, что существует бесконечно много целых σ, для которых сумма этого ряда равна нулю.

Но из последней формулы следует, что

$$\lim_{\sigma \to \infty} [\sigma^{m+v} \mathfrak{P}^{(m)}(\sigma)] = \mu^{(1)}\mu^{(2)} \ldots \mu^{(m)} v(v+1) \ldots (v+m-1) V_1.$$

Выражение в правой части отлично от нуля. Это обстоятельство находится в противоречии с уже доказанными фактами, если только не все коэффициенты $P_1, R_1, S_1, \ldots$ равны нулю. Подобным же образом устанавливается, что и все коэффициенты $P_2, R_2, S_2, \ldots, P_\nu, R_\nu, S_\nu, \ldots$ одновременно равны нулю. Мы получаем

$$y_1 + y_2 + \ldots + y_\nu = A_1 \sigma^{m-1} + B_1 \sigma^{m-2} + \ldots + L_1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = A_\nu \sigma^{m-1} + B_\nu \sigma^{m-2} + \ldots + L_\nu.$$

Так как правые части принимают целые значения для бесконечного количества целых аргументов σ, отсюда легко вывести, что все коэффициенты $A, B, \ldots, L$ являются рациональными числами[2]. Возвращаясь к переменной

[2] Нельзя, однако, сделать отсюда вывод, что эти коэффициенты будут *целыми* рациональными числами; действительно, как хорошо известно, существуют многочлены от одной переменной, принимающие целые значения для всех целочисленных значений аргумента и,

$\tau = \sigma p^{1/k}$, мы получаем

$$y_1 + y_2 + \ldots + y_\nu = A_1 p^{-\frac{m-1}{k}} \tau^{m-1} + B_1 p^{-\frac{m-2}{k}} \tau^{m-2} + \ldots + L_1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = A_\nu p^{-\frac{m-1}{k}} \tau^{m-1} + B_\nu p^{-\frac{m-2}{k}} \tau^{m-2} + \ldots + L_\nu.$$

Предыдущие рассмотрения приводят к следующему результату: если взять простое число p, большее некоторой определенной границы, то среди построенных выше $2^n - 2$ систем найдется хотя бы одна, которая имеет только что указанный вид и у которой все коэффициенты $A, B, \ldots, L$ суть рациональные числа.

Выберем еще $2^n - 2$ различных простых чисел $p', p'', \ldots, p^{2^n-2}$, больших, чем простое число p. Для каждого из этих простых чисел хотя бы одна из наших $2^n - 2$ систем имеет аналогичный вид. Так как количество чисел $p, p', p'', \ldots, p^{2^n-2}$ равно $2^n - 1$, а систем у нас всего $2^n - 2$, одна из этих систем должна допускать два представления. Пусть это будут, как и выше,

$$y_1 + y_2 + \ldots + y_\nu = A_1 p^{-\frac{m-1}{k}} \tau^{m-1} + B_1 p^{-\frac{m-2}{k}} \tau^{m-2} + \ldots + L_1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = A_\nu p^{-\frac{m-1}{k}} \tau^{m-1} + B_\nu p^{-\frac{m-2}{k}} \tau^{m-2} + \ldots + L_\nu$$

и

$$y_1 + y_2 + \ldots + y_\nu = A'_1 p'^{-\frac{m-1}{k}} \tau^{m-1} + B'_1 p'^{-\frac{m-2}{k}} \tau^{m-2} + \ldots + L'_1,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = A'_\nu p'^{-\frac{m-1}{k}} \tau^{m-1} + B'_\nu p'^{-\frac{m-2}{k}} \tau^{m-2} + \ldots + L'_\nu.$$

Сравнивая одинаковые степени τ в правых частях, получаем

$$A_1 p^{-\frac{m-1}{k}} = A'_1 p'^{-\frac{m-1}{k}}, \quad \ldots, \quad A_\nu p^{-\frac{m-1}{k}} = A'_\nu p'^{-\frac{m-1}{k}},$$

$$B_1 p^{-\frac{m-2}{k}} = B'_1 p'^{-\frac{m-2}{k}}, \quad \ldots, \quad B_\nu p^{-\frac{m-2}{k}} = B'_\nu p'^{-\frac{m-2}{k}},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$L_1 = L'_1, \quad \ldots, \quad L_\nu = L'_\nu.$$

Здесь коэффициенты $A, B, \ldots, L, A', B', \ldots, L'$ все являются рациональными числами, а p и p' — два различных простых числа. Поэтому из наших равенств вытекает, что коэффициенты при дробных степенях p равны нулю, т. е. все функции в этой системе являются многочленами от τ^k с рациональными коэффициентами, так что, полагая $\tau^k = t$, получаем

$$y_1 + y_2 + \ldots + y_\nu = F_1(t),$$

$$\ldots\ldots\ldots\ldots$$

$$y_1 y_2 \ldots y_\nu = F_\nu(t),$$

где $F_1(t), \ldots, F_\nu(t)$ — целые рациональные функции от t с рациональными коэффициентами.

несмотря на это, имеющие дробные коэффициенты; см. Math. Ann., 1890, Bd. 36, S. 512, где мною описаны самые общие многочлены с таким свойством [с. 47–48 настоящего издания. — *Ред.*].

Этот результат показывает, что многочлен $g(y,t)$ должен делиться на многочлен

$$\Psi(y,t) = y^{\nu} - F_1(t)y^{\nu-1} + F_2(t)y^{\nu-2} + \ldots + (-1)^{\nu}F_{\nu}(t),$$

т. е.

$$g(y,t) = \Psi(y,t)\Psi'(y,t),$$

где Ψ и Ψ' — многочлены от y и t с рациональными коэффициентами. Сделав подстановку $y = xT$, получим для исходного многочлена равенство

$$f(x,t) = \frac{\Phi(x,t)\Phi'(x,t)}{AT^{n-1}},$$

где $\Phi(x,t)$ и $\Phi'(x,t)$ — многочлены от x и t с *целыми* коэффициентами, A — целое число, а T — многочлен от переменной t с целыми коэффициентами. Отметим еще, что, если P — простой делитель числа A или общий простой делитель всех коэффициентов многочлена T, то частное

$$\frac{\Phi(x,t)\Phi'(x,t)}{P}$$

будет многочленом с целочисленными коэффициентами от переменных x и t, откуда стандартным образом легко выводится, что все коэффициенты либо многочлена $\Phi(x,t)$, либо $\Phi'(x,t)$ должны делиться на P. Если $U(t)$ обозначает неприводимый многочлен с целочисленными коэффициентами от t, и частное

$$\frac{\Phi(x,t)\Phi'(x,t)}{U(t)}$$

равно многочлену от x и t с целыми коэффициентами, то аналогичным образом мы получаем, что все коэффициенты при степенях переменной x (эти коэффициенты являются многочленами от t) либо у $\Phi(x,t)$, либо у $\Phi'(x,t)$ должны делиться на $U(t)$. Сократив последовательно нашу дробь на все простые множители знаменателя, мы придем к равенству

$$f(x,t) = \varphi(x,t)\varphi'(x,t),$$

где $\varphi(x,t)$ и $\varphi'(x,t)$ — многочлены с *целочисленными* коэффициентами. Это равенство означает, что исходный многочлен является приводимым. Но это противоречит предположению нашей теоремы, следовательно, не существует такого числа C, что для всех целочисленных значений t, больших C, многочлен $f(x,t)$ является приводимым, чем наша теорема и доказана.

Ради краткости я провел доказательство так, что установлено только *существование* числа t, удовлетворяющего требованиям нашей теоремы. Однако, это доказательство можно без труда дополнить и указать, как найти нужное t с помощью *конечного* количества арифметических операций, при условии что многочлен $f(x,t)$ явно задан.

Далее мы займемся обобщениями и применениями доказанной теоремы I. Что касается доказательств приводимых ниже утверждений, мы ограничимся кратким указанием на используемые факты.

Прежде всего пусть вместо одного неприводимого многочлена $f(x,t)$ задано несколько неприводимых многочленов $f(x,t), g(x,t), \ldots, k(x,t)$. Несложное видоизменение приведенного выше доказательства показывает справедливость следующего предложения:

Если все многочлены $f(x,t), g(x,t), \ldots, k(x,t)$ от переменных x и t с целочисленными коэффициентами неприводимы, то существует бесконечно много способов подставить вместо t целое рациональное число так, чтобы все эти многочлены $f(x,t), g(x,t), \ldots, k(x,t)$ перешли в неприводимые многочлены от одной переменной x.

Это предложение можно следующим образом переформулировать в терминах произведения $F(x,t)$ всех фигурирующих в нем многочленов $f(x,t), g(x,t), \ldots, k(x,t)$:

Для произвольного заданного многочлена $F(x,t)$ от переменных x и t с целочисленными коэффициентами существует бесконечно много способов подставить целое рациональное число вместо t таким образом, чтобы разложение на простые множители получившегося многочлена от одной переменной x содержало ровно столько неприводимых многочленов с целочисленными коэффициентами, сколько и разложение исходного многочлена $F(x,t)$ с неопределенным параметром t.

Более сложная ситуация получается в случае, когда многочлен из теоремы I зависит не от одной переменной x, а от нескольких переменных $x, y \ldots, w$ и не от одного параметра, а от нескольких параметров $t, r, \ldots, q$. Прежде чем переходить к этому общему случаю, мы докажем следующее предложение:

Пусть $F(x,t,r,\ldots,q)$ — неприводимый многочлен с целочисленными коэффициентами от переменной x и параметров $t, r, \ldots, q$. Вместо этих параметров можно так подставить линейные многочлены с целочисленными коэффициентами от одного параметра u, что многочлен $F(x,t,r,\ldots,q)$ будет неприводимым многочленом от двух переменных x и u[3]).

Пусть

$$F(x,t,r,\ldots,q) = fx^n + f_1x^{n-1} + \ldots + f_n,$$

где $f, f_1, \ldots, f_n$ — многочлены с целочисленными коэффициентами от $t, r, \ldots, q$. Делая подстановку $x = y/f$ и умножая затем на f^{n-1}, получаем многочлен, который также неприводим и имеет вид

$$G(y,t,r,\ldots,q) = y^n + g_1y^{n-1} + \ldots + g^n,$$

где $g_1, \ldots, g_n$ — опять многочлены с целочисленными коэффициентами от $t, r, \ldots, q$. Возьмем дискриминант D этого многочлена, который является многочленом от $t, r, \ldots, q$ и не равен тождественно нулю (иначе многочлен $G(y,t,r,\ldots,q)$ делился бы на квадрат некоторого многочлена и не был бы неприводимым). Подберем систему рациональных чисел

$$t = t_0, \quad r = r_0, \quad \ldots, \quad q = q_0,$$

для которой дискриминант D не равен нулю, и подставим эти значения в многочлен $G(y,t,r,\ldots,q)$. Получившийся многочлен от y разложим на неприводимые множители с целочисленными коэффициентами, скажем

$$G(y,t_0,r_0,\ldots,q_0) = \varphi(y) \ldots \chi(y),$$

---

[3]) Ср. с подстановкой, использованной с аналогичной целью в работе Л. Кронекера «Grundzüge einer arithmetischen Theorie der algebraischen Größen», см.: J. reine und angew. Math., Bd. 92, S. 11.

где $\varphi(y),\ldots,\chi(y)$ — многочлены с целочисленными коэффициентами от y степеней $\nu,\ldots,\mu$ соответственно.

Рассмотрим, далее, алгебраическую функцию y, заданную уравнением

$$G(y,t,r,\ldots,q)=0.$$

В точке $t=t_0, r=r_0,\ldots,q=q_0$ она определяет n степенных рядов по положительным степеням переменных

$$t'=t-t_0,\quad r'=r-r_0,\quad \ldots,\quad q'=q-q_0,$$

имеющих следующий вид:

$$\begin{gathered}
y_1=\sum \alpha_1^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa},\\
\ldots\ldots\ldots\ldots\ldots\ldots\\
y_\nu=\sum \alpha_\nu^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa},\\
\ldots\ldots\ldots\ldots\ldots\ldots\\
y_{n-\mu+1}=\sum \gamma_1^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa},\\
\ldots\ldots\ldots\ldots\ldots\ldots\\
y_n=\sum \gamma_\mu^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa};\\
(\tau,\rho,\ldots,\varkappa=0,1,2,3,\ldots).
\end{gathered}$$

Здесь постоянными членами $\alpha_1^{(0,0,\ldots,0)},\ldots,\alpha_\nu^{(0,0,\ldots,0)}$ первых ν степенных рядов служат ν корней уравнения $\varphi(y)=0$, а постоянными членами $\gamma_1^{(0,0,\ldots,0)},\ldots,\gamma_\mu^{(0,0,\ldots,0)}$ последних μ рядов являются μ корней уравнения $\chi(y)=0$. Теперь мы можем построить элементарные симметрические функции от ν первых степенных рядов и получить следующие ν степенных рядов

$$\begin{gathered}
y_1+y_2+\ldots+y_\nu=\sum \mathrm{A}_1^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa},\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
y_1y_2\ldots y_\nu=\sum \mathrm{A}_\nu^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa}\\
(\tau,\rho,\ldots,\varkappa=0,1,2,3,\ldots).
\end{gathered}$$

Продолжая так же, получим в конце концов μ элементарных симметрических функций от последних μ рядов:

$$\begin{gathered}
y_{n-\mu+1}+\ldots+y_n=\sum \Gamma_1^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa},\\
\ldots\ldots\ldots\ldots\ldots\ldots\\
y_{n-\mu+1}\ldots y_n=\sum \Gamma_\mu^{(\tau,\rho,\ldots,\varkappa)}t'^{\tau}r'^{\rho}\ldots q'^{\varkappa}\\
(\tau,\rho,\ldots,\varkappa=0,1,2,3,\ldots).
\end{gathered}$$

Таким образом, мы пришли к системам степенных рядов, первая из которых состоит из ν рядов, последняя — из μ рядов. Коэффициенты $\mathrm{A},\ldots,\Gamma$ этих рядов являются рациональными числами, и ни одна из этих систем не может состоять только из многочленов, т. е. в каждой системе имеются бесконечные ряды (иначе многочлен $G(y,t,r,\ldots,q)$ был бы приводим). Рассмотрим еще всевозможные комбинации этих систем, например, возьмем

разложения для $y_1, \ldots, y_\nu$ и для $y_{n-\mu+1}, \ldots, y_n$ и построим общую систему из $\nu + \mu$ элементарных симметрических функций. Окончательно, для каждого множителя многочлена $G(y, t_0, r_0, \ldots, q_0)$, приводимого или неприводимого, мы получаем систему степенных рядов, причем все эти системы обладают следующим свойством: коэффициенты всех рядов суть рациональные числа и хотя бы один ряд в каждой системе бесконечен.

После этого мы полагаем

$$t' = t_1 u, \quad r' = r_1 u, \quad \ldots, \quad q' = q_1 u,$$

и все наши ряды превращаются в степенные ряды от одной переменной u. Возникает следующая задача: подобрать целые рациональные значения для $t_1, r_1, \ldots, q_1$ таким образом, чтобы в каждой системе остался хотя бы один бесконечный ряд. Чтобы доказать, что такая задача разрешима, обозначим через E число, которое больше суммы наибольших степеней параметров $t, r, \ldots, q$, входящих в выражение $G(y, t, r, \ldots, q)$. Пусть теперь $At'^{\tau_\alpha} r'^{\rho_\alpha} \ldots \ldots q'^{\varkappa_\alpha}$ — такое слагаемое из подходящего ряда первой системы, у которого коэффициент A отличен от нуля, а сумма степеней $\tau_\alpha + \rho_\alpha + \ldots + \varkappa_\alpha$ больше числа E. Выберем такие же слагаемые для каждой системы; пусть, скажем, $\Gamma t'^{\tau_\gamma} r'^{\rho_\gamma} \ldots q'^{\varkappa_\gamma}$ — слагаемое из системы рядов, относящейся ко множителю χ, такое что коэффициент Γ не равен нулю и сумма $\tau_\gamma + \rho_\gamma + \ldots + \varkappa_\gamma$ больше числа E. Как показывает несложное рассуждение, можно найти такие целые числа $t_1, r_1, \ldots, q_1$, что ряды от переменной u, которые получаются нашей подстановкой, содержат степени

$$u^{\tau_\alpha + \rho_\alpha + \varkappa_\alpha}, \quad \ldots, \quad u^{\tau_\gamma + \rho_\gamma + \varkappa_\gamma}, \quad \ldots$$

с ненулевыми коэффициентами. Но отсюда следует, что в каждой системе хотя бы один из рядов от переменной u не является многочленом. Действительно, в противном случае многочлен от переменных y и u, который получается из многочлена $G(y, t, r, \ldots, q)$ подстановкой

$$t = t_0 + t_1 u, \quad r = r_0 + r_1 u, \quad \ldots, \quad q = q_0 + q_1 u,$$

был бы приводимым, причем в каждый сомножитель переменная u входила бы в степени, большей числа E, что, как легко видеть, невозможно. Этим мы доказали, что ни одна из наших систем при этой подстановке не может перейти в систему многочленов, а это означает, что многочлен от y и u, получающийся из многочлена $G(y, t, r, \ldots, q)$, должен быть неприводимым. Значит, если мы вернемся к многочлену $F(x, t, r, \ldots, q)$ и сделаем ту же подстановку, то получим многочлен от x и u, который не распадается на несколько сомножителей, зависящих от x. Возможно, правда, что получится многочлен, у которого есть сомножитель, зависящий только от переменной u. Но, как легко видеть, целые числа $t_1, r_1, \ldots, q_1$ можно подобрать таким образом, чтобы и этого не случилось. Тем самым предложение доказано.

Теперь с помощью этих предложений мы докажем следующую общую теорему:

II. *Пусть* $F(x, y, \ldots, w, t, r, \ldots, q)$ — *неприводимый многочлен от переменных* $x, y, \ldots, w$ *и параметров* $t, r, \ldots, q$ *с целочисленными коэффициентами. Существует бесконечно много способов присвоить параметрам* $t, r, \ldots, q$ *целые рациональные значения так, чтобы*

многочлен $F(x, y, \ldots, w, t, r, \ldots, q)$ *перешел в неприводимый многочлен от переменных* $x, y, \ldots, w$.

Если в заданном многочлене $F(x, y, \ldots, w, t, r, \ldots, q)$ сделать подстановку

$$y = \eta x, \quad \ldots, \quad w = \omega x$$

и поделить на соответствующую степень x, то получится многочлен $G(x, \eta, \ldots, \omega, t, r, \ldots, q)$ от переменной x и параметров $\eta, \ldots \omega, t, r, \ldots, q$, который также будет неприводимым. Используя доказанное предложение, заменяем эти параметры на линейные целочисленные многочлены от одного параметра u

$$\eta = \eta_1 u + \eta_0, \quad \ldots, \quad \omega = \omega_1 u + \omega_0,$$
$$t = t_1 u + t_0, \quad \ldots, \quad q = q_1 u + q_0,$$

так, чтобы этот многочлен перешел в неприводимый многочлен $g(x, u)$ от двух переменных x и u. Тогда, по теореме I, для переменной u найдется такое целое рациональное значение u_0, что многочлен $g(x, u_0)$ будет неприводимым многочленом одной переменной x. Мы видим, что заданный многочлен $F(x, y, \ldots, w, t, r, \ldots, q)$ переходит в неприводимый многочлен от переменных $x, y, \ldots, w$, если параметрам присвоить целые значения

$$t = t_1 u_0 + t_0, \quad r = r_1 u_0 + r_0, \quad \ldots, \quad q = q_1 u_0 + q_0.$$

Действительно, если в полученном многочлене сделать еще подстановку

$$y = (\eta_1 u_0 + \eta_0)x, \quad \ldots, \quad w = (\omega_1 u_0 + \omega_0)x,$$

то получим неприводимый многочлен $g(x, u_0)$, умноженный на некоторую степень переменной x. Тем самым доказательство закончено.

До сих пор все наши рассуждения о неприводимости велись в предположении, что в основе лежит область рациональных чисел: многочлен мы называли неприводимым, если он не распадается в произведение нескольких многочленов с целочисленными коэффициентами. Теперь мы хотим распространить полученные результаты на случай, когда область рациональности определяется некоторым алгебраическим числом. В соответствии с этим будем, как это принято, называть многочлен с коэффициентами из области рациональности, определенной данным алгебраическим числом, неприводимым в этой области, если его нельзя представить в виде произведения нескольких многочленов с коэффициентами, которые лежат в той же области рациональности. Справедлива следующая теорема:

III. *Пусть многочлен* $F(x, y, \ldots, w, t, r, \ldots, q)$ *неприводим над областью рациональности, которая определена некоторым алгебраическим числом. Существует бесконечно много способов так присвоить параметрам* $t, r, \ldots, q$ *целые рациональные значения, чтобы этот многочлен перешел в многочлен, неприводимый над той же областью рациональности.*

Теорему III можно вывести из теоремы II с помощью того же метода, который использовал Л. Кронекер[4] для разложения многочлена на неприводимые сомножители над произвольной областью рациональности. Умножив

[4] См. его работу «Grundzüge einer arithmetischen Theorie der algebraischen Größen», J. reine und angew. Math., Bd. 92, S. 12, 13.

сначала наш многочлен на некоторое число из заданной области и сделав подходящую линейную замену переменных, добьемся того, чтобы в многочлен входило хоть одно слагаемое с целым рациональным коэффициентом и чтобы все многочлены, сопряженные с F, были попарно различны. Перемножив все эти сопряженные многочлены и помножив на подходящее целое рациональное число, получим многочлен $G(x, y, \ldots, w, t, r, \ldots, q)$ с целыми рациональными коэффициентами, который неприводим над областью рациональных чисел. По теореме II найдутся такие целые рациональные значения параметров $t, r, \ldots, q$, что многочлен G перейдет в многочлен от переменных $x, y, \ldots, w$, неприводимый над областью рациональных чисел. Легко показать, что эти же значения параметров переводят заданный многочлен $F(x, y, \ldots, w, t, r, \ldots, q)$ в многочлен от $x, y, \ldots, w$, который неприводим над заданной областью рациональности.

А теперь мы применим полученные результаты к теории уравнений. Пусть уравнение n-й степени от x задано в следующем виде:

$$F_0 x^n + F_1 x^{n-1} + \ldots + F_n = 0,$$

где коэффициенты $F_0, F_1, \ldots, F_n$ суть многочлены с целыми рациональными коэффициентами от параметров $t, r, \ldots, q$. Пусть Г есть группа этого уравнения относительно определенной рациональными числами и параметрами $t, r, \ldots, q$ области рациональности.

Рассмотрим произведение

$$\prod (u + x_{i_1} u_1 + \ldots + x_{i_n} u_n),$$

взятое по всем перестановкам $i_1, i_2, \ldots, i_n$ множества из n чисел $1, 2, \ldots, n$, где $u, u_1, \ldots, u_n$ — неопределенные параметры, а $x_1, x_2, \ldots, x_n$ — корни заданного уравнения. Умножив это произведение на $F_0^{n!}$, получим многочлен с целочисленными коэффициентами от переменных $u, u_1, \ldots, u_n, t, r, \ldots, q$. Пусть $G(u, u_1, \ldots, u_n, t, r, \ldots, q)$ — неприводимый над областью рациональных чисел множитель этого многочлена. Тогда указанная группа Г определяется теми перестановками, которые сохраняют множитель G. Покажем с помощью полученых выше результатов, что *можно бесконечным количеством способов подставить вместо параметров $t, r, \ldots, q$ в заданное уравнение целые рациональные числа так, чтобы группа полученного целочисленного уравнения совпадала с группой* Г. Чтобы сделать это, мы вычислим дискриминант заданного уравнения: после умножения на некоторую степень F_0 он станет не равным тождественно нулю многочленом с целочисленными коэффициентами от параметров $t, r, \ldots, q$. По теореме II мы можем найти неограниченно много значений для t, при подстановке которых в G будут получаться неприводимые над областью рациональных чисел многочлены от переменных $u, u_1 \ldots, u_n, r, \ldots, q$. Среди этих целых рациональных t выберем одно, для которого дискриминант D не обращается тождественно в нуль. Затем определим целое рациональное число r, при подстановке которого в G получается неприводимый над областью рациональных чисел многочлен и для которого дискриминант D не обращается в нуль. Продолжая таким же образом, найдем целые рациональные значения $t, r, \ldots, q$, при подстановке которых в G получается неприводимый многочлен $g(u, u_1, \ldots, u_n)$, а дискриминант D становится равным некоторому отличному от нуля числу. Теперь, с одной стороны, очевидно, что переста-

новки, сохраняющие G, сохраняют также и многочлен g; с другой стороны, кроме этих перестановок никакие другие не могут сохранять многочлен g, так как порядок группы получаемого целочисленного уравнения не может превышать порядок группы Г. Следовательно, группа Г совпадает с группой целочисленного уравнения, которое получается при замене параметров на найденные целые числа.

Возьмем для примера сами коэффициенты уравнения в качестве неопределенных параметров $t, r, \ldots, q$, так что группой уравнения будет симметрическая группа. Из нашей теоремы следует, *что существует бесконечно много уравнений n-й степени с целочисленными коэффициентами, у которых группа над областью рациональных чисел есть симметрическая группа.*

Для таких уравнений можно доказать и более сильное утверждение — для случая, когда позволен свободный выбор лишь последнего коэффициента. Пусть в уравнении

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + t = 0$$

коэффициенты $a_0, a_1, \ldots, a_{n-1}$ суть любые целые рациональные числа, такие что у уравнения

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \ldots + a_{n-1} = 0$$

все корни различны и функция $f(x)$ в этих корнях принимает попарно различные значения. Тогда дискриминантом первого уравнения будет многочлен степени $n-1$ от t, корни которого попарно различны. Из этого факта с помощью того же принципа, который использовал А. Гурвиц[5], можно вывести, что группа монодромии этого уравнения относительно параметра t есть симметрическая группа[6]. Из доказанного ранее общего предложения следует, что существует бесконечно много способов выбрать целочисленное значение последнего коэффициента t так, чтобы группа получающегося целочисленого уравнения над областью рациональных чисел совпадала с симметрической группой.

Подобным же образом мы в состоянии показать, что *существует бесконечно много уравнений с целочисленными коэффициентами, у которых группа над областью рациональных чисел совпадает со знакопеременной группой.* Для доказательства воспользуемся двумя предложениями, справедливость которых без труда можно установить теми же методами, развитыми Гурвицем в уже упоминавшейся работе. Первое из этих предложений гласит:

Пусть $f(x)$ — многочлен *четной* степени n от переменной x, который делится на x^2 и производная которого имеет вид

$$f'(x) = n(x-a)^2(x-b)^2 \ldots (x-k)^2x,$$

где $a, b, \ldots, k$ — попарно различные не равные нулю числа, причем все значе-

---

[5] Math. Ann., Bd. 39, S. 1.

[6] См. также его работу: *Hurwitz A.* Über diejenigen algebraischen Gebilde, welche eindeutige Transformationen in sich zulassen. — Nachr. Ges. Wiss. Göttingen, 1887, S. 103, где также играет роль использованный мною выше факт.

ния $f(a), f(b), \ldots, f(k)$ также попарно различны. Тогда группой монодромии уравнения

$$f(x) + (-1)^{n/2} t^2 = 0$$

относительно параметра t будет знакопеременная группа.

Прежде всего вычислим дискриминант этого уравнения, представив его в виде результанта двух многочленов. Именно, если $\varphi(x)$ и $\psi(x)$ — два многочлена от x степеней ν и μ, а $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ и $\beta_1, \beta_2, \ldots, \beta_\mu$ — их корни, то

$$\varphi(x) = \alpha(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_\nu),$$
$$\psi(x) = \beta(x - \beta_1)(x - \beta_2) \ldots (x - \beta_\mu)$$

и результант, как известно, имеет вид

$$R(\varphi, \psi) = \beta^\nu \varphi(\beta_1)\varphi(\beta_2) \ldots \varphi(\beta_\mu) = (-1)^{\nu\mu} \alpha^\mu \psi(\alpha_1)\psi(\alpha_2) \ldots \psi(\alpha_\nu).$$

Отсюда находим дискриминант указанного уравнения, т. е. произведение квадратов разностей корней многочлена:

$$D = n^n t^2 \left(f(a) + (-1)^{n/2} t^2\right)^2 \left(f(b) + (-1)^{n/2} t^2\right)^2 \ldots \left(f(k) + (-1)^{n/2} t^2\right)^2,$$

откуда следует, что произведение самих разностей равно

$$D^{1/2} = n^{\frac{n}{2}} t \left(f(a) + (-1)^{n/2} t^2\right) \left(f(b) + (-1)^{n/2} t^2\right) \ldots \left(f(k) + (-1)^{n/2} t^2\right).$$

Выберем теперь для $a, b, \ldots, k$ какие-нибудь рациональные положительные попарно различные значения. Выбором этих значений многочлен $f(x)$ полностью определяется, и значения $f(a), f(b), \ldots, f(k)$ будут попарно различны. Действительно, разность $f(b) - f(a)$, например, равна интегралу от a до b от положительной функции $f'(x)$. Так как n — четное число, найденное выражение для $D^{1/2}$ равно многочлену от t с рациональными коэффициентами и, следовательно, группой этого уравнения над областью рациональности, определенной рациональными числами и параметром t, будет знакопеременная группа. Значит, по доказанному выше предложению, можно бесконечным количеством способов присвоить t целое значение так, чтобы полученное целочисленное уравнение имело группу над областью рациональных чисел, совпадающую со знакопеременной группой. Тем самым наше утверждение для уравнений четной степени доказано.

Соответствующее утверждение для уравнений нечетной степени устанавливается с помощью предложения, которое без труда может быть получено методами, развитыми Гурвицем. Это утверждение гласит:

Пусть $f(x)$ — многочлен от переменной x *нечетной* степени, производная которого удовлетворяет уравнению

$$xf'(x) - f(x) = (n-1)(x-a)(x-b)^2(x-c)^2 \ldots (x-k)^2,$$

где $a, b, c, \ldots, k$ — попарно различные числа, не равные нулю, и пусть значения $f'(b), f'(c), \ldots, f'(k)$ также попарно различны. Тогда группой монодромии уравнения

$$f(x) + \left((-1)^{\frac{n-1}{2}} t^2 - f'(a)\right) x = 0$$

относительно параметра t будет знакопеременная группа.

Используя вышеприведенную формулу для вычисления результанта двух многочленов, а также формулу

$$R(\varphi - x\psi, \psi) = R(\varphi, \psi),$$

получим для дискриминанта нашего уравнения, т. е. для произведения квадратов разностей корней, значение

$$D = (n-1)^{n-1}t^2\left((-1)^{\frac{n-1}{2}}t^2 + f'(b) - f'(a)\right)^2 \ldots \left((-1)^{\frac{n-1}{2}}t^2 + f'(k) - f'(a)\right)^2,$$

откуда получаем произведение самих разностей

$$D^{1/2} = (n-1)^{\frac{n-1}{2}}t\left((-1)^{\frac{n-1}{2}}t^2 + f'(b) - f'(a)\right) \ldots \left((-1)^{\frac{n-1}{2}}t^2 + f'(k) - f'(a)\right).$$

Выберем для $b, c, \ldots, k$ какие-нибудь рациональные положительные и попарно различные значения и положим

$$a = -\frac{1}{2\left(\frac{1}{b} + \frac{1}{c} + \ldots + \frac{1}{k}\right)}.$$

Из последнего предположения следует, что коэффициент при первой степени x в правой части формулы

$$xf'(x) - f(x) = (n-1)(x-a)(x-b)^2(x-c)^2 \ldots (x-k)^2$$

равен нулю, как и в левой части. Поэтому эта формула определяет единственным образом многочлен $f(x)$ с рациональными коэффициентами n-й степени. Этот многочлен обладает тем свойством, что все значения $f'(b), f'(c), \ldots, f'(k)$ попарно различны. Действительно, возьмем, скажем,

$$f'(c) - f'(b) = \frac{f(c)}{c} - \frac{f(b)}{b} = \int_b^c \frac{xf'(x) - f(x)}{x^2}dx;$$

интеграл справа не равен нулю, так как подынтегральная функция положительна. Поскольку n — число нечетное, найденное выражение для $D^{1/2}$ дает многочлен от t с целочисленными коэффициентами, и, следовательно, наше уравнение над областью рациональности, определенной рациональными числами и параметром t, дает знакопеременную группу. Применяя доказанное выше предложение, заключаем, что существует бесконечно много целочисленных значений параметра t, таких что при их подстановке в наше уравнение получающееся целочисленное уравнение над областью рациональных чисел имеет знакопеременную группу. Тем самым наше утверждение доказано для уравнений нечетной степени.

С помощью теоремы III мы можем обобщить наши результаты о группе уравнения на случай произвольных областей рациональности, задаваемых любым алгебраическим числом. Именно, справедливо следующее предложение:

IV. *Пусть заданы алгебраическое число* $\mathfrak{R}$ *и уравнение* n*-й степени*

$$F_0x^n + F_1x^{n-1} + \ldots + F_n = 0,$$

где коэффициенты $F_0, F_1, \ldots, F_n$ *суть многочлены от параметров* $t, r, \ldots, q$, *имеющие коэффициенты из области рациональности,*

определенной числом $\mathfrak{R}$. *Пусть* Γ — *группа этого уравнения над областью рациональности, определенной числом* $\mathfrak{R}$ *и параметрами* $t, r, \ldots, q$. *Тогда существует бесконечно много способов так подставить вместо параметров* $t, r, \ldots, q$ *целые рациональные числа, чтобы получающееся числовое уравнение над областью рациональности, определенной числом* $\mathfrak{R}$, *имело ту же группу* Γ.

Этот результат принципиально важен, так как показывает, что все параметры, формально входящие в выражения для коэффициентов уравнения и в определение области рациональности, можно заменить на целые рациональные *числа*, покуда речь идет лишь о теоретико-групповых свойствах уравнений, и тем самым обойтись без использования алгебраических *функций*.

Опираясь на полученные результаты, мы можем прояснить понятие группы монодромии в арифметическом случае. Пусть дано уравнение, коэффициенты которого суть многочлены от одного параметра t с коэффициентами из области рациональности, определенной некоторым алгебраическим числом $\mathfrak{R}$. Мы подставляем в это уравнение целочисленные значения параметра t и рассматриваем группы всех получаемых таким образом численных уравнений над областью рациональности, определенной числом $\mathfrak{R}$. Пусть, далее, $\mathfrak{A}$ — алгебраическое число, после присоединения которого к области рациональности все эти группы уменьшаются, максимальное в том смысле, что в результате дополнительного присоединения любых других чисел уменьшатся будут уже не все группы [1]. Тогда та из уменьшенных групп, которая имеет максимальный порядок, совпадает с группой монодромии нашего уравнения относительно параметра t.

Опираясь на теорему IV, мы можем обобщить ранее полученные предложения, касающиеся симметрических и знакопеременных групп. Именно, справедлив следующий факт: *для произвольной области рациональности, заданной любым алгебраическим числом, можно построить уравнения с рациональными коэффициентами, группой которых над этой областью служит симметрическая группа, равно как и уравнения со знакопеременной группой*. Таким образом, для области рациональности, заданной алгебраическим числом, мы можем построить уравнение любой степени n с рациональными числовыми коэффициентами, которое будет неразложимым в заданной области.

Легко также показать, что *существует бесконечно много попарно различных областей рациональности заданной степени* n (областей рода n-го порядка, числовых полей n-й степени), *не содержащих областей меньшей степени, кроме области рациональных чисел*. Действительно, если бы существовало лишь конечное число таких областей, то их объединение дало бы новую область рациональности $\mathfrak{R}$, которая их содержит. Из полученных результатов следует существование уравнения n-й степени с рациональными коэффициентами, имеющего над областью $\mathfrak{R}$ симметрическую группу. Это уравнение определяет, очевидно, область n-й степени, не содержащую областей меньшей степени и отличную от исходных областей. Аналогично доказывается более общий факт, что существует бесконечно много областей степени $n = \nu\mu$, которые содержат заданную область ν-й степени и не содержат никаких других областей рациональности, кроме области рациональных чисел.

Предыдущие рассуждения доказывают лишь *существование* уравнений и областей с указанными свойствами. Но, как уже говорилось в замечании к теореме I, наши рассуждения можно дополнить таким образом, чтобы стало ясно, что эти уравнения и области можно было построить, используя конечное число арифметических действий.

В заключение я приведу еще одно предложение, которое также может быть получено с помощью изложенных выше методов, хотя его легко доказать и непосредственно, рассматривая соответствующие степенные разложения. Это предложение гласит:

Если алгебраическая функция от t для всех рациональных чисел из сколь угодно малого интервала принимает рациональные значения, то она должна быть рациональной[7].

[7] Как показал недавно Э. Штраусс, *аналитическая* функция вполне может принимать при всех рациональных аргументах рациональные значения и не быть рациональной.

О ТРАНСЦЕНДЕНТНОСТИ ЧИСЕЛ e И π*)

Предположим, что число e удовлетворяет уравнению степени n

$$a + a_1 e + a_2 e^2 + \ldots + a_n e^n = 0$$

с целыми рациональными коэффициентами $a, a_1, \ldots, a_n$.

Если левую часть этого уравнения умножить на интеграл

$$\int_0^\infty = \int_0^\infty z^\rho \left[(z-1)(z-2)\cdots(z-n)\right]^{\rho+1} e^{-z} dz,$$

где ρ — целое положительное число, то получится выражение

$$a\int_0^\infty + a_1 e \int_0^\infty + a_2 e^2 \int_0^\infty + \ldots + a_n e^n \int_0^\infty .$$

Это выражение разлагается в сумму следующих двух:

$$P_1 = a\int_0^\infty + a_1 e \int_1^\infty + a_2 e^2 \int_2^\infty + \ldots + a_n e^n \int_n^\infty ,$$

$$P_2 = a_1 e \int_0^1 + a_2 e^2 \int_0^2 + \ldots + a_n e^n \int_0^n .$$

Формула

$$\int_0^\infty z^\rho e^{-z} dz = \rho!$$

показывает, что интеграл $\int_0^\infty$ представляет собой целое рациональное число, делящееся на $\rho!$. Аналогично, применяя соответственно подстановки $z = z' + 1$, $z = z' + 2$, …, $z = z' + n$, получим, что $e\int_1^\infty$, $e^2\int_2^\infty$, …, $e^n\int_n^\infty$ — целые рациональные числа, делящиеся на $(\rho+1)!$. Отсюда следует, что и P_1 — целое рациональное число, делящееся на $\rho!$, причем выполняется сравнение по модулю $\rho + 1$

$$\frac{P_1}{\rho!} \equiv \pm a (n!)^{\rho+1}, \quad (\rho + 1). \tag{1}$$

---

*) Über die Transzendenz der Zahlen e und π. — Nachr. Ges. Wiss. Gött., 1893, S. 113–116; Math. Ann., 1893, Bd. 43, S. 216–219. *Перевод* Н. И. Фельдмана.

С другой стороны, если обозначить через K и k максимумы модуля на промежутке $[0, n]$ функций

$$z(z-1)(z-2)\cdots(z-n)$$

и

$$(z-1)(z-2)\cdots(z-n)e^{-z}$$

соответственно, то

$$\left|\int_0^1\right| < kK^\rho, \quad \left|\int_0^2\right| < 2kK^\rho, \quad \ldots, \quad \left|\int_0^n\right| < nkK^\rho.$$

Отсюда следует неравенство

$$|P_2| < \varkappa K^\rho, \tag{2}$$

где для краткости положено

$$\varkappa = \left\{|a_1 e| + 2|a_2 e^2| + \ldots + n|a_n e^n|\right\} k.$$

Теперь выберем целое положительное число ρ, которое, во-первых, делится на целое число $a \cdot n!$ и для которого, во-вторых, $\varkappa K^\rho/\rho! < 1$. Вследствие сравнения (1) целое число $P_1/\rho!$ не делится на $\rho + 1$ и поэтому отлично от нуля, а так как, далее, ввиду неравенства (2) абсолютная величина числа $P_2/\rho!$ меньше 1, то равенство

$$\frac{P_1}{\rho!} + \frac{P_2}{\rho!} = 0$$

невозможно.

Предположим, что π — алгебраическое число и что число $\alpha_1 = i\pi$ удовлетворяет некоторому уравнению степени n с целыми коэффициентами. Обозначим через $\alpha_2, \ldots, \alpha_n$ остальные корни этого уравнения. Из равенства $1 + e^{i\pi} = 0$ следует, что и выражение

$$(1 + e^{\alpha_1})(1 + e^{\alpha_2})\cdots(1 + e^{\alpha_n}) = 1 + e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_N}$$

равно нулю. Здесь N показателей $\beta_1, \ldots, \beta_N$ являются, как легко видеть [1], корнями некоторого уравнения степени N с целыми рациональными коэффициентами. Пусть, скажем, M показателей $\beta_1, \ldots, \beta_M$ отличны от нуля, а остальные равны нулю. Эти M показателей являются корнями некоторого уравнения M-й степени вида

$$f(z) = bz^M + b_1 z^{M-1} + \ldots + b_M = 0$$

тоже с целыми рациональными коэффициентами, причем свободный член b_M отличен от нуля. Вышеупомянутое выражение принимает теперь вид

$$a + e^{\beta_1} + \ldots + e^{\beta_M},$$

где a — целое положительное число.

Умножим это выражение на интеграл

$$\int_0^\infty = \int_0^\infty z^\rho \left[g(z)\right]^{\rho+1} e^{-z} dz,$$

где снова ρ — некоторое целое положительное число, а $g(z) = b^M f(z)$. Получим

$$a\int_0^\infty + e^{\beta_1}\int_0^\infty + e^{\beta_2}\int_0^\infty + \ldots + e^{\beta_M}\int_0^\infty .$$

Это выражение разлагается в сумму следующих двух:

$$P_1 = a\int_0^\infty + e^{\beta_1}\int_{\beta_1}^\infty + e^{\beta_2}\int_{\beta_2}^\infty + \ldots + e^{\beta_M}\int_{\beta_M}^\infty ,$$

$$P_2 = e^{\beta_1}\int_0^{\beta_1} + e^{\beta_2}\int_0^{\beta_2} + \ldots + e^{\beta_M}\int_0^{\beta_M} ,$$

где интеграл $\int_{\beta_i}^\infty$ взят по лучу в комплексной плоскости, идущему из точки $z = \beta_i$ параллельно вещественной оси к $z = +\infty$, а интеграл $\int_0^{\beta_i}$ взят по отрезку, соединяющему точки $z = 0$ и $z = \beta_i$.

Этот интеграл $\int_0^\infty$ опять равен некоторому целому рациональному числу, делящемуся на $\rho!$, причем справедливо сравнение по модулю $\rho + 1$

$$\frac{1}{\rho!}\int_0^\infty \equiv b^{\rho M+M} b_M^{\rho+1}, \quad (\rho+1).$$

Так как $g(\beta_i) = 0$, то с помощью подстановки $z = z' + \beta_i$ получим

$$e^{\beta_i}\int_{\beta_i}^\infty = \int_0^\infty (z'+\beta_i)^\rho \left[g(z'+\beta_i)\right]^{\rho+1} e^{-z'} dz' = (\rho+1)!G(\beta_i).$$

Здесь $G(\beta_i)$ — многочлен с целыми коэффициентами от β_i, степень которого меньше числа $\rho M + M$, а все коэффициенты делятся на $b^{\rho M+M}$. Поскольку $\beta_1, \ldots, \beta_M$ являются корнями уравнения с целыми коэффициентами $f(z) = 0$, то их произведения на старший коэффициент b будут *целыми* алгебраическими числами, поэтому величина

$$G(\beta_1) + G(\beta_2) + \ldots + G(\beta_M)$$

обязательно является *целым рациональным* числом. Отсюда следует, что выражение P_1 равно целому рациональному числу, делящемуся на $\rho!$, причем выполняется сравнение по модулю $\rho + 1$

$$\frac{P_1}{\rho!} \equiv ab^{\rho M+M} b_M^{\rho+1}, \quad (\rho+1). \tag{3}$$

С другой стороны, если K и k — максимумы модуля функций $zg(z)$

и $g(z)e^{-z}$ на отрезках, соединяющих точки $z = 0$ и $z = \beta_i$, то

$$\left| \int_0^{\beta_i} \right| < |\beta_i| k K^\rho \qquad (i = 1, 2, \ldots, M).$$

Отсюда вытекает неравенство

$$|P_2| < \varkappa K^\rho, \tag{4}$$

где для краткости положено

$$\varkappa = \left\{ |\beta_1 e^{\beta_1}| + |\beta_2 e^{\beta_2}| + \ldots + |\beta_M e^{\beta_M}| \right\} k.$$

Теперь выберем целое положительное число ρ, которое, во-первых, делится на abb^M и для которого, во-вторых, $\varkappa K^\rho < \rho!$. Вследствие сравнения (3), целое число $P_1/\rho!$ не делится на $\rho+1$ и поэтому отлично от нуля, а так как, далее, ввиду неравенства (4) абсолютная величина числа $P_2/\rho!$ меньше 1, то равенство

$$\frac{P_1}{\rho!} + \frac{P_2}{\rho!} = 0$$

невозможно.

Легко видеть, что предложенным способом можно так же просто доказать общую теорему Линдемана о показательной функции.

Кёнигсберг в Пруссии, 5 января 1893 г.

О БИКВАДРАТИЧНЫХ ЧИСЛОВЫХ ПОЛЯХ ДИРИХЛЕ*)

ВВЕДЕНИЕ

После того как Гауссом были введены в арифметику целые мнимые числа, Дирихле в ряде работ[1]) исследовал те биквадратичные числовые поля, которые содержат мнимую единицу i, а следовательно, и все другие гауссовы мнимые числа. Такие биквадратичные поля называют полями Дирихле. Дирихле применил к этим полям свой общий аналитический метод для определения числа классов идеалов и, в частности, рассмотрел случай, когда биквадратичное поле, кроме квадратичного поля, определенного с помощью i, содержит еще два других квадратичных поля. Он показал, что число классов идеалов этого специального поля Дирихле по существу равно произведению чисел классов идеалов последних двух квадратичных полей. Этот полученный аналитическими средствами чисто арифметический результат Дирихле отметил как один из самых красивых в теории мнимых чисел, прежде всего потому, что тем самым была обнаружена связь между числами классов идеалов этих двух квадратичных полей, определяемых квадратными корнями из противоположных по знаку вещественных чисел.

Цель данной работы состоит в том, чтобы чисто арифметическим путем развить теорию биквадратичных полей Дирихле до того же уровня, на котором находится теория квадратичных полей после работ Гаусса. Для этого прежде всего необходимо ввести понятие рода и исследовать основанное на этом понятии разбиение классов идеалов. Эта задача решается для произвольных полей Дирихле в первых восьми параграфах данной работы, после чего в последних двух параграфах рассматриваются упомянутые выше специальные поля Дирихле. При этом оказывается, что в таком поле классы идеалов из некоторых просто характеризуемых родов составлены из классов идеалов квадратичных полей, содержащихся в этом поле. Этот результат, полученный чисто арифметическим путем, содержит в себе упомянутую выше теорему Дирихле о числе классов идеалов специального поля Дирихле.

§ 1. Целые числа поля Дирихле

Обозначим через k квадратичное числовое поле, определяемое мнимой единицей i. Целые числа этого поля, т. е. числа вида $a+bi$, где a и b — целые

---

*) Über den Dirichletischen Zahlenkörper. — Math. Ann., 1894, Bd. 45, S. 309–340. *Перевод Л. В. Кузьмина.*

[1]) Untersuchungen über die Theorie der komplexen Zahlen; Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. — *Dirichlet L.* Werke, Bd. 1, S. 505, 511, 533.

рациональные числа, будем называть целыми мнимыми числами. Обозначим через δ целое мнимое число, которое не делится ни на какой квадрат целого мнимого числа и отлично от ± 1. Тогда совокупность всех чисел, которые рационально выражаются через i и $\sqrt{\delta}$, образует биквадратичное поле Дирихле. Обозначим это поле через K; это самое общее биквадратичное поле, содержащее мнимую единицу i.

Любое число поля K может быть представлено в виде

$$\mathsf{A} = \frac{\alpha + \beta\sqrt{\delta}}{\gamma},$$

где α, β, γ — целые мнимые числа. Преобразование, переводящее $\sqrt{\delta}$ в $-\sqrt{\delta}$, будет обозначаться символом S [1].

Пусть теперь A — некоторое целое число в K. Тогда числа

$$\mathsf{A} + S\mathsf{A} = \frac{2\alpha}{\gamma} \quad \text{и} \quad \mathsf{A} \cdot S\mathsf{A} = \frac{\alpha^2 - \beta^2\delta}{\gamma^2}$$

должны быть целыми мнимыми числами. Обозначим через λ некоторое отличное от $1+i$ простое число k, делящее γ. Тогда, как легко видеть, и α и β должны делиться на λ и, следовательно, можно сократить на λ числитель и знаменатель A. Далее, если γ делится на $(1+i)^3$, то таким же способом получаем, что α и β делятся на $1+i$, так что числитель и знаменатель A можно сократить на множитель $1+i$. Следовательно, остается рассмотреть только два случая $\gamma = 1+i$ и $\gamma = 2$. В этих двух случаях число $\alpha^2 - \beta^2\delta$ должно делиться на 2 и на 4 соответственно. Если бы β делилось на $1+i$, то это же было бы верно и для α и тогда снова числитель и знаменатель A сокращались бы на $1+i$. С другой стороны, предположим, что β не делится на $1+i$. Тогда $\delta \equiv \alpha^2/\beta^2$ по модулю 2 (соответственно по модулю 4), т. е. в поле k число δ должно быть квадратичным вычетом по модулю 2 (соответственно по модулю 4). Если $\delta \equiv \pm 1$ по модулю 4, то δ является квадратичным вычетом по модулю 4. Если $\delta \equiv \pm 3 + 2i$ по модулю 4, то δ будет квадратичным вычетом по модулю 2 и одновременно квадратичным невычетом по модулю 4. Во всех остальных случаях, а именно когда $\delta \equiv i$ по модулю 2 и $\delta \equiv 0$ по модулю $1+i$, δ будет квадратичным невычетом по модулю 2. Заметим, что мы получим то же самое биквадратичное поле K, если заменим под знаком корня δ на $-\delta$, так как эта замена соответствует умножению корня на i; поэтому мы можем, очевидно, выбрать δ таким, чтобы в обоих случаях имела место первая возможность, т. е. чтобы $\delta \equiv 1$ (соответственно $\equiv 3 + 2i$) по модулю 4. Отсюда мы легко получаем следующий результат.

В поле Дирихле K базис целых чисел образуют числа $1, i, \Omega, i\Omega$, *где* Ω *задается так*:

$$\begin{aligned}
&\text{если } \delta \equiv 1, && (4), && \text{то} \quad \Omega = \frac{1+\sqrt{\delta}}{2},\\
&\text{если } \delta \equiv 3+2i, && (4), && \text{то} \quad \Omega = \frac{1+\sqrt{\delta}}{1+i},\\
&\text{если } \delta \equiv i, && (2), && \text{то} \quad \Omega = 1+\sqrt{\delta},\\
&\text{если } \delta \equiv 0, && (1+i), && \text{то} \quad \Omega = \sqrt{\delta}.
\end{aligned}$$

Вычислим выражение $d = (\Omega - S\Omega)^2$, которое будем называть *частичным дискриминантом поля* K:

$$\left.\begin{array}{ll} \text{если } \delta \equiv 1, & (4), \\ \text{если } \delta \equiv 3+2i, & (4), \\ \text{если } \delta \equiv i, & (2) \\ \text{если } \delta \equiv 0, & (1+i) \end{array}\right\}, \quad \text{то} \quad \begin{array}{l} d = \delta, \\ d = -2i\,\delta, \\ d = 4\delta. \end{array}$$

Обычный дискриминант D *биквадратичного поля* K *оказывается равным* $2^4|d|^2$, где $|d|$ обозначает абсолютную величину частичного дискриминанта d.

§ 2. Простые идеалы поля Дирихле

Сначала мы рассмотрим простые числа поля k, отличные от $1+i$ и не делящие δ, среди которых следует различать два типа: во-первых, те простые числа π, относительно которых δ является квадратичным вычетом в поле k, и, во-вторых, те простые числа $\varkappa$, относительно которых δ является квадратичным невычетом.

Простые числа π первого типа допускают разложение на два простых идеала поля K, которые взаимно просты. Обозначим через η какое-либо число в k, удовлетворяющее сравнению $\delta \equiv \eta^2$ по модулю π. Применяя введенный мною ранее[2] способ записи, когда последовательность $(\mathsf{A}, \mathsf{B}, \ldots)$ обозначает идеал, являющийся наибольшим общим делителем чисел $\mathsf{A}, \mathsf{B}, \ldots$, получаем

$$(\pi, \eta+\sqrt{\delta})(\pi, \eta-\sqrt{\delta}) = (\pi^2, \pi[\eta+\sqrt{\delta}], \pi[\eta-\sqrt{\delta}], \eta^2-\delta) = (\pi, \eta^2-\delta) = \pi.$$

Таким образом, мы получаем искомое разложение

$$\pi = \mathfrak{P} \cdot S\mathfrak{P}, \quad \mathfrak{P} = (\pi, \eta+\sqrt{\delta}),$$

где $\mathfrak{P}$ — простой идеал; в силу того что $(\pi, \eta+\sqrt{\delta}, \eta-\sqrt{\delta}) = 1$, сопряженный простой идеал $S\mathfrak{P}$ должен быть отличен от $\mathfrak{P}$.

Простые числа $\varkappa$ второго типа остаются простыми в поле K. Действительно, если бы число $\varkappa$ было разложимым, то в K можно было бы выбрать целое число $\mathsf{A} = \alpha + \beta\sqrt{\delta}$, которое не делится на $\varkappa$, но делится на простой идеал, делящий $\varkappa$. Тогда β должно быть взаимно простым с $\varkappa$, в то время как $\mathsf{A} \cdot S\mathsf{A} = \alpha^2 - \beta^2\delta$ делится на $\varkappa$, а значит, $\delta \equiv (\alpha/\beta)^2$ по модулю $\varkappa$, вопреки нашему предположению.

Чтобы получить разложение на идеальные множители для простых чисел поля k, делящих δ и отличных от $1+i$, обозначим их через $\lambda_1, \ldots, \lambda_r$. Таким образом, $\delta = \lambda_1 \ldots \lambda_r$ или $\delta = (1+i)\lambda_1 \ldots \lambda_r$ в зависимости от того, не делится δ на $1+i$ или делится. Легко видеть, что

$$\mathfrak{L}_1 = S\mathfrak{L}_1 = (\lambda_1, \sqrt{\delta}), \quad \ldots, \quad \mathfrak{L}_r = S\mathfrak{L}_r = (\lambda_r, \sqrt{\delta})$$

являются простыми идеалами в поле K и что

$$\lambda_1 = \mathfrak{L}_1^2, \quad \ldots, \quad \lambda_r = \mathfrak{L}_r^2.$$

---

[2] Math. Ann.. Bd. 44. S. 1.

Наконец, чтобы получить разложение числа $1+i$, рассмотрим сначала случай $\delta \equiv 1$ по модулю 4. В этом случае $1+i$ остается простым, если $\delta \equiv 1+4i$ по модулю $(1+i)^5$. Если же $\delta \equiv 1$ по модулю $(1+i)^5$, то

$$1+i=(1+i,\ \Omega)(1+i,\ S\Omega),$$

где обе скобки справа представляют простые идеалы поля K, которые должны быть взаимно простыми в силу условия $(\Omega,\ S\Omega)=1$. Во всех остальных случаях, как показывает простое вычисление, $(1+i)$ совпадает с квадратом идеала $(1+i,\ \Omega)=(1+i,\ S\Omega)$. Итак, мы получаем, что $1+i$ тогда и только тогда будет квадратом некоторого простого идеала, когда $1+i$ входит множителем в частичный дискриминант d поля K. Разложение числа $1+i$ на множители представлено в следующей таблице:

при $\delta \equiv 1$, $(1+i)^5$ имеем $1+i=\mathfrak{P}\cdot S\mathfrak{P}$, $\mathfrak{P}=(1+i,\ \Omega)$, $S\mathfrak{P}\neq\mathfrak{P}$,

при $\delta \equiv 1+4i$, $(1+i)^5$ имеем $1+i=\mathfrak{P}$,

при $\delta \equiv 3+2i$, (4)
при $\delta \equiv i$, (2)
при $\delta \equiv 0$, $(1+i)$
} имеем $1+i=\mathfrak{L}^2$, $\mathfrak{L}=S\mathfrak{L}=(1+i,\ \Omega)$.

Полученные результаты о разложении чисел в k можно наглядно представить, если воспользоваться символом, который использовал Дирихле. Именно, если α — произвольное число и τ — простое число в k, то под $\left[\frac{\alpha}{\tau}\right]$ мы понимаем $+1$, -1 или 0 в зависимости от того, является ли α в поле k квадратичным вычетом или квадратичным невычетом по модулю τ или делится на τ; далее, $\left[\frac{\alpha}{1+i}\right]$ принимает значения $+1$, -1, 0 в зависимости от того, является ли α квадратичным вычетом или невычетом по модулю $(1+i)^5$ или делится на $1+i$. Тогда справедлива следующая теорема.

Простое число τ поля k в поле K распадается на два различных простых идеала, или остается простым, или равно квадрату простого идеала [2] *в зависимости от того, какое значение,* $+1$, -1 *или* 0, *принимает символ* $\left[\frac{d}{\tau}\right]$.

§ 3. Распределение классов идеалов по родам

Если A — произвольное целое или дробное число поля K, то $\nu(\mathrm{A})=\mathrm{A}\cdot S\mathrm{A}$ называется *частичной нормой* A. Эта частичная норма является, очевидно, числом поля k. Пусть теперь λ — отличное от $1+i$ простое число поля k, делящее δ, и пусть частичная норма $\nu(\mathrm{A})$ является целым числом, не делящимся на λ, или дробным числом, числитель и знаменатель которого не делятся на λ. Тогда в области целых мнимых чисел $\nu(\mathrm{A})$ является квадратичным вычетом относительно λ.

Чтобы убедиться в этом, запишем $\mathsf{A} = \dfrac{\alpha + \beta\sqrt{\delta}}{\gamma}$, где α, β, γ — целые мнимые числа. Тогда $\nu(\mathsf{A}) = \dfrac{\alpha^2 - \beta^2\delta}{\gamma^2}$. Если γ содержит простой множитель λ, то в силу нашего предположения относительно $\nu(\mathsf{A})$ и число $\alpha^2 - \beta^2\delta$ должно делиться на λ^2, а следовательно, и α и β должны содержать множитель λ; тем самым числитель и знаменатель дроби A сократимы. Далее, если α содержит множитель λ, то в силу предположения относительно $\nu(\mathsf{A})$ и γ и β должны делиться на λ, и тогда снова множитель λ в числителе и знаменателе дроби A сократим. Поэтому мы можем считать, что ни одно из чисел α и γ не содержит множитель λ. Но тогда $\nu(\mathsf{A}) \equiv \alpha^2/\gamma^2$ по модулю λ, чем и доказано наше утверждение.

Теперь мы введем новый символ $\left[\dfrac{\sigma}{\lambda : \delta}\right]$, где σ — произвольное число в k, сначала для случая, когда λ — отличное от $1 + i$ простое число, делящее δ. Если $\sigma = \alpha$ — целое число, не делящееся на λ, или дробь, числитель и знаменатель которой не делятся на λ, то наш символ определяется равенством

$$\left[\frac{\alpha}{\lambda : \delta}\right] = \left[\frac{\alpha}{\lambda}\right].$$

Если же $\sigma = \nu$ — частичная норма некоторого числа из K, то полагаем

$$\left[\frac{\nu}{\lambda : \delta}\right] = +1.$$

Утверждение, доказанное в начале этого параграфа, показывает, что последняя формула согласована с нашим прежним определением. В дальнейшем нам потребуется утверждение о том, что любое число σ в k можно представить как произведение двух чисел α и ν, где α — целое не делящееся на λ число в k или дробь, числитель и знаменатель которой не делятся на λ, а ν — частичная норма некоторого числа из K. Чтобы доказать это утверждение, очевидно, достаточно получить такое разложение для простого числа λ. С этой целью выберем в K число A, которое делится на $\mathfrak{L}$, но не на $\lambda = \mathfrak{L}^2$. Положим $\nu = \nu(\mathsf{A})$ и учтем, что $\lambda/\nu = \alpha$ можно представить в виде дроби, числитель которой равен 1, а знаменатель не делится на λ. Отсюда и следует искомое разложение $\lambda = \alpha\nu$.

В общем случае, если произвольное число $\sigma = \alpha\nu$ разложено указанным образом, то мы определяем наш символ равенством

$$\left[\frac{\sigma}{\lambda : \delta}\right] = \left[\frac{\alpha}{\lambda}\right].$$

Без труда устанавливается, что этот символ однозначно определен и обладает свойством

$$\left[\frac{\sigma\sigma'}{\lambda : \delta}\right] = \left[\frac{\sigma}{\lambda : \delta}\right]\left[\frac{\sigma'}{\lambda : \delta}\right],$$

где σ, σ' — произвольные числа поля k.

В случае когда $1 + i$ делит d, необходимо более точно исследовать поведение частичной нормы и ее вычетов по степеням $1 + i$. Чтобы получить обозримое представление соответствующей системы вычетов, положим

$$i' = 3 + 2i, \quad i'' = 1 + 4i.$$

Простое вычисление показывает, что, когда t, t', t'' принимают значения 0 или 1, все 8 вычетов по модулю $(1 + i)^4$, взаимно простых с $1 + i$, имеют

вид $\pm i^t i'^{t'}$, а все 16 вычетов по модулю $(1+i)^5$, взаимно простых с $1+i$, имеют вид $\pm i^t i'^{t'} i''^{t''}$. Для краткости мы будем обозначать эти выражения через (tt') и $(tt't'')$ соответственно.

Так как в случае $\delta \equiv (00)$ по модулю $(1+i)^4$ частичный дискриминант d не делится на $1+i$, остается рассмотреть 7 случаев $\delta \equiv (01), (10), (11)$ по модулю $(1+i)^4$ и $\delta \equiv (1+i)(00)$, $(1+i)(01)$, $(1+i)(10)$, $(1+i)(11)$ по модулю $(1+i)^5$. Вычисление показывает, что из вычетов по модулю $(1+i)^5$, взаимно простых с $1+i$, частичными нормами чисел из поля K представляются лишь те, которые стоят в столбце «α» в следующей таблице; их показатели t, t', t'' удовлетворяют условию, приведенному в последнем столбце:

$\delta \equiv$	$\alpha \equiv$	
(01)	$(000), (001), (010), (011)$	t четно
(10)	$(000), (001), (100), (101)$	t' четно
(11)	$(000), (001), (110), (101)$	$t+t'$ четно
$(1+i)(00)$	$(000), (011), (100), (111)$	$t'+t''$ четно
$(1+i)(01)$	$(000), (011), (101), (110)$	$t+t'+t''$ четно
$(1+i)(10)$	$(000), (010), (100), (110)$	t'' четно
$(1+i)(11)$	$(000), (010), (101), (111)$	$t+t''$ четно

Чтобы представить эту таблицу в более обозримом виде, запишем $\delta \equiv (t_\delta t'_\delta)$ (соответственно $\equiv (1+i)(t_\delta t'_\delta)$) и $\alpha \equiv (t_\alpha t'_\alpha t''_\alpha)$. Как легко убедиться, число α тогда и только тогда сравнимо с некоторой частичной нормой по модулю $(1+i)^5$, когда число $t_\alpha t'_\delta + t'_\alpha t_\delta$ (соответственно $t_\alpha t'_\delta + t'_\alpha t_\delta + t'_\alpha + t''_\alpha$) четно. Отметим также, что число α, если оно удовлетворяет этому условию, сравнимо и по модулю любой более высокой степени $1+i$ с частичной нормой некоторого числа из K.

Символ $\left[\frac{\sigma}{1+i:\delta}\right]$ мы определим сначала для случая, когда $\sigma = \alpha$ — число, не делящееся на $1+i$, или дробь, числитель и знаменатель которой не делятся на $1+i$. В этом случае мы будем считать, что $\alpha \equiv (t_\alpha t'_\alpha t''_\alpha)$, и положим

$$\left[\frac{\alpha}{1+i:\delta}\right] = (-1)^{t_\alpha t'_\delta + t'_\alpha t_\delta} \quad \text{или} \quad (-1)^{t_\alpha t'_\delta + t'_\alpha t_\delta + t'_\alpha + t''_\alpha}$$

в зависимости от того, сравнимо δ с $(t_\delta t'_\delta)$ по модулю $(1+i)^4$ или с $(1+i)(t_\delta t'_\delta)$ по модулю $(1+i)^5$. Если теперь $\sigma = \nu$ — частичная норма произвольного числа поля K, то мы полагаем

$$\left[\frac{\nu}{1+i:\delta}\right] = +1.$$

Наконец, чтобы определить наш символ для произвольного σ, мы воспользуемся разложением $\sigma = \alpha\nu$, где α — число, не делящееся на $1+i$, или дробь, числитель и знаменатель которой не делятся на $1+i$, и где ν — некоторая частичная норма, и положим

$$\left[\frac{\sigma}{1+i:\delta}\right] = \left[\frac{\alpha}{1+i:\delta}\right].$$

Снова легко проверяется, что так определенный символ обладает свойством

$$\left[\frac{\sigma\sigma'}{1+i:\delta}\right] = \left[\frac{\sigma}{1+i:\delta}\right]\left[\frac{\sigma'}{1+i:\delta}\right],$$

где σ, σ' — произвольные числа поля K.

В дальнейшем мы будем обозначать через $\lambda_1, \ldots, \lambda_s$ все простые числа, входящие множителями в частичный дискриминант d. Тогда наш символ сопоставляет каждому числу σ из поля k набор из s знаков

$$\left[\frac{\sigma}{\lambda_1:\delta}\right], \quad \ldots, \quad \left[\frac{\sigma}{\lambda_s:\delta}\right],$$

который мы назовем *системой характеров числа* σ в поле Дирихле K. Чтобы в дальнейшем сопоставить любому идеалу $\mathfrak{I}$ в K некоторый определенный набор знаков при помощи нашего символа, мы рассмотрим $\mathfrak{I}\cdot S\mathfrak{I}$. Это произведение равно некоторому числу $\nu(\mathfrak{I})$ в k, которое называется *частичной нормой идеала* $\mathfrak{I}$. Так как эта частичная норма определена лишь с точностью до умножения на единицу, для нашей цели приходится различать два случая в зависимости от того, состоит система характеров

$$\left[\frac{i}{\lambda_1:\delta}\right], \quad \ldots, \quad \left[\frac{i}{\lambda_s:\delta}\right]$$

единичного множителя i только из знаков плюс или содержит хотя бы один минус. Очевидно, что в *первом случае все* s *знаков*

$$\left[\frac{\nu(\mathfrak{I})}{\lambda_1:\delta}\right], \quad \ldots, \quad \left[\frac{\nu(\mathfrak{I})}{\lambda_s:\delta}\right],$$

отвечающих идеалу $\mathfrak{I}$, *определены однозначно*. Эта система s знаков называется *системой характеров идеала* $\mathfrak{I}$. Во *втором случае* будем считать, что $\left[\frac{i}{\lambda_s:\delta}\right] = -1$. Тогда можно выбрать такое значение частичной нормы $\nu(\mathfrak{I})$, что $\left[\frac{\nu(\mathfrak{I})}{\lambda_s:\delta}\right] = +1$. В этом случае $s-1$ *знаков*

$$\left[\frac{\nu(\mathfrak{I})}{\lambda_1:\delta}\right], \quad \ldots, \quad \left[\frac{\nu(\mathfrak{I})}{\lambda_{s-1}:\delta}\right]$$

однозначно определяются идеалом $\mathfrak{I}$ и называются *системой характеров этого идеала.*

Идеалы из одного класса обладают одинаковыми системами характеров.

Действительно, пусть $\mathfrak{J}'$ и $\mathfrak{J}$ эквивалентны. Тогда в K существует такое целое или дробное число A, что $\mathfrak{J}' = A\mathfrak{J}$. Отсюда следует, что $\nu(\mathfrak{J}') = \nu(A)\nu(\mathfrak{J})$ и поэтому $\left[\frac{\nu(\mathfrak{J}')}{\lambda : \delta}\right] = \left[\frac{\nu(\mathfrak{J})}{\lambda : \delta}\right]$.

Изложенным способом каждому классу идеалов ставится в соответствие некоторая определенная система характеров. *Мы будем считать классы идеалов с одинаковыми системами характеров принадлежащими к одному роду и, в частности, определим главный род, как совокупность всех классов, система характеров которых состоит из одних знаков плюс. Так как система характеров главного класса обладает, очевидно, последним свойством, главный класс принадлежит к главному роду* [3].

§ 4. Построение классов идеалов главного рода

Из свойства нашего символа, выражаемого формулой

$$\left[\frac{\sigma\sigma'}{\lambda : \delta}\right] = \left[\frac{\sigma}{\lambda : \delta}\right]\left[\frac{\sigma'}{\lambda : \delta}\right],$$

легко вытекает тот факт, что произведение классов идеалов, принадлежащих некоторым двум родам, представляет класс идеалов рода, система характеров которого получается перемножением характеров соответствующих двух родов. В частности, отсюда следует, что система характеров квадрата класса идеалов произвольного рода состоит из одних плюс единиц. Тем самым квадрат любого класса идеалов принадлежит главному роду. Важно, что выполняется следующее обратное утверждение.

Любой класс идеалов главного рода равен квадрату некоторого класса идеалов [4].

В справедливости этого утверждения мы убедимся, доказав ряд теорем.

Теорема 1. *Если ν является частичной нормой некоторого идеала в поле Дирихле K_δ, получаемом с помощью $\sqrt{\delta}$, и система характеров ν в поле K_δ состоит из одних плюс единиц, то и δ является частичной нормой некоторого идеала в поле Дирихле K_ν, получаемом с помощью $\sqrt{\nu}$, и обладает в K_ν системой характеров, состоящей из одних плюс единиц.*

Очевидно, мы можем предположить, что ν не содержит множителей, являющихся квадратами в поле k. Так как ν — частичная норма, любой простой делитель π числа ν, не входящий множителем в частичный дискриминант d поля K_δ, распадается в поле K_δ на два простых идеала. Тогда в силу результатов § 2 дискриминант d должен быть квадратичным вычетом по модулю π, т. е. при π, отличном от $1 + i$, мы имеем

$$\left[\frac{\delta}{\pi : \nu}\right] = +1.$$

Теперь мы рассмотрим отличные от $1 + i$ содержащиеся в d простые делители λ числа ν. В поле K_δ имеет место разложение $\lambda = \mathfrak{L}^2$ и вместе

с тем $\lambda+\sqrt{\delta}$ является делящимся на $\mathfrak{L}$, но не на λ числом поля K_δ. Полагая $\nu=\lambda\nu'$, $\delta=\lambda\delta'$, мы заключаем, что

$$\left[\frac{\nu}{\lambda:\delta}\right]=\left[\frac{\nu\cdot\nu\left(\frac{1}{\lambda+\sqrt{\delta}}\right)}{\lambda:\delta}\right]=\left[\frac{\frac{\nu}{\lambda^2-\delta}}{\lambda:\delta}\right]=\left[\frac{\frac{\nu'}{\lambda-\delta'}}{\lambda}\right]=\left[\frac{\nu'\delta'}{\lambda}\right].$$

Таким же образом получаем

$$\left[\frac{\delta}{\lambda:\nu}\right]=\left[\frac{\nu'\delta'}{\lambda}\right],$$

а так как по предположению символ $\left[\frac{\nu}{\lambda:\delta}\right]$ принимает значение $+1$, то и

$$\left[\frac{\delta}{\lambda:\nu}\right]=+1.$$

Наконец, что касается простого множителя $1+i$, то для дальнейшего изучения мы выделим четыре основных случая.

I. Ни ν, ни δ не делятся на $1+i$.

II. ν делится на $1+i$, а δ не делится.

III. ν не делится на $1+i$, а δ делится.

IV. Как ν, так и δ делятся на $1+i$.

В случае I мы положим $\nu\equiv(t_\nu t'_\nu)$ и $\delta\equiv(t_\delta t'_\delta)$ по модулю $(1+i)^4$ и будем различать два подслучая.

В случае I мы положим $\nu\equiv(t_\nu t'_\nu)$ и $\delta\equiv(t_\delta t'_\delta)$ по модулю $(1+i)^4$ и будем различать два подслучая.

1. t_ν, t'_ν оба четны. При этом условии $1+i$ не входит множителем в частичный дискриминант n поля Дирихле K_ν и, следовательно, в поле K_ν нет символа, соответствующего множителю $1+i$.

2. t_ν, t'_ν не являются одновременно четными. При этом условии $1+i$ входит множителем в n и мы имеем

$$\left[\frac{\delta}{1+i:\nu}\right]=(-1)^{t_\delta t'_\nu+t'_\delta t_\nu}.$$

Если t_δ, t'_δ оба четны, тогда правая часть равна $+1$. Если t_δ, t'_δ не являются одновременно четными, то в поле K_δ существует символ, соответствующий $1+i$, и при этом

$$\left[\frac{\nu}{1+i:\delta}\right]=(-1)^{t_\nu t'_\delta+t'_\nu t_\delta}.$$

Так как этот символ должен по предположению иметь значение $+1$, мы заключаем, что и

$$\left[\frac{\delta}{1+i:\nu}\right]=+1.$$

В случае II мы запишем $\nu\equiv(1+i)(t_\nu t'_\nu)$ и $\delta\equiv(t_\delta t'_\delta t''_\delta)$ по модулю $(1+i)^5$ и будем различать следующие два подслучая.

1. t_δ, t'_δ четны. При этом предположении $1+i$ не входит в частичный дискриминант d поля K_δ. Так как ν должно быть частичной нормой некоторого идеала в K_δ, то число $1+i$ должно распадаться в поле K_δ на два простых

идеала. Условие для этого, установленное в § 2, состоит в том, что $\delta \equiv (000)$ по модулю $(1+i)^5$, и тогда

$$\left[\frac{\delta}{1+i:\nu}\right] = +1.$$

2. t_δ, t'_δ не являются одновременно четными. Тогда $1+i$ является множителем частичного дискриминанта d. Полагая $\omega = \dfrac{\Omega \cdot S\Omega}{1+i}$, имеем

$$\left[\frac{\nu}{1+i:\delta}\right] = \left[\frac{\nu \cdot \nu\left(\frac{1}{\Omega}\right)}{1+i:\delta}\right] = \left[\frac{(t_\nu t'_\nu)\omega}{1+i:\delta}\right] = \left[\frac{(t_\nu t'_\nu)}{1+i:\delta}\right]\left[\frac{\omega}{1+i:\delta}\right];$$

но

$$\left[\frac{(t_\nu t'_\nu)}{1+i:\delta}\right] = (-1)^{t_\nu t'_\delta + t'_\nu t_\delta},$$

и простое вычисление показывает, что

$$\left[\frac{\omega}{1+i:\delta}\right] = (-1)^{t'_\delta + t''_\delta}.$$

Следовательно,

$$\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t_\nu t'_\delta + t'_\nu t_\delta + t'_\delta + t''_\delta}.$$

С другой стороны,

$$\left[\frac{\delta}{1+i:\delta}\right] = (-1)^{t_\delta t'_\nu + t'_\delta t_\nu + t'_\delta + t''_\delta},$$

а так как предпоследний символ имеет значение $+1$, то и последний тоже:

$$\left[\frac{\delta}{1+i:\nu}\right] = +1.$$

В случае III запишем $\nu \equiv (t_\nu t'_\nu t''_\nu)$ и $\delta \equiv (1+i)(t_\delta t'_\delta)$ по модулю $(1+i)^5$ и будем различать два подслучая.

1. t_ν, t'_ν оба четны. При этом условии $1+i$ не содержится множителем в частичном дискриминанте n поля K_ν. В силу нашего предположения,

$$\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t''_\nu} = +1.$$

Следовательно, t''_ν четно, т. е. $\nu \equiv (000)$ по модулю $(1+i)^5$; ввиду результатов § 2 отсюда следует, что $1+i$ распадается в поле K_ν на два простых идеала.

2. t_ν, t'_ν не являются четными одновременно. Тогда $1+i$ содержится в n в качестве множителя и мы имеем

$$\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t_\nu t'_\delta + t'_\nu t_\delta + t'_\nu + t''_\nu}.$$

Как и ранее в подслучае 2 случая II, мы получаем такое же значение для символа $\left[\frac{\delta}{1+i:\nu}\right]$, а так как первое значение равно $+1$, мы заключаем, что и

$$\left[\frac{\delta}{1+i:\nu}\right]=+1.$$

В случае IV запишем $\nu\equiv(\iota+i)(t_\nu t'_\nu t''_\nu)$ и $\delta\equiv(1+i)(t_\delta t'_\delta t''_\delta)$ по модулю $(1+i)^6$. Тогда

$$\left[\frac{\nu}{1+i:\delta}\right]=\left[\frac{\nu\cdot\nu\left(\frac{1}{\sqrt{\delta}}\right)}{1+i:\delta}\right]\left[\frac{(t_\nu t'_\nu t''_\nu)(t_\delta t'_\delta t''_\delta)}{1+i:\delta}\right]=$$

$$=(-1)^{(t_\nu+t_\delta)t'_\delta+(t'_\nu+t'_\delta)t_\delta+t'_\nu+t'_\delta+t''_\nu+t''_\delta}=(-1)^{t_\nu t'_\delta+t'_\nu t_\delta+t'_\nu+t'_\delta+t''_\nu+t''_\delta}.$$

Такое же значение мы получаем и для $\left[\frac{\delta}{1+i:\nu}\right]$, а так как первый символ имеет значение $+1$, мы заключаем, что и

$$\left[\frac{\delta}{1+i:\delta}\right]=+1.$$

Только что проведенные рассмотрения показывают, что система характеров числа δ в поле K_ν состоит из одних знаков плюс.

С другой стороны, δ должно быть частичной нормой некоторого идеала в K_ν. Действительно, если λ — отличный от $1+i$ простой множитель δ, не содержащийся в n, то в силу того, что все характеры ν относительно поля K_δ равны $+1$, мы должны иметь

$$\left[\frac{\nu}{\lambda:\delta}\right]=\left[\frac{\nu}{\lambda}\right]=+1,$$

и, следовательно, в силу результатов § 2, λ распадается в поле K_ν на два простых идеала. Далее, если $1+i$ входит в качестве множителя в δ и не входит в частичный дискриминант n, то должно выполняться сравнение $\nu\equiv(00)$ по модулю $(1+i)^4$, а тогда, как было доказано в подслучае 1 случая III, $1+i$ распадается в поле K_ν. Итак, все простые множители числа δ распадаются в поле K_ν. Значит, δ является частичной нормой некоторого идеала в K_ν, и тем самым наша теорема полностью доказана.

Теорема 2. *Если ν является частичной нормой некоторого целого или дробного числа из поля Дирихле K_δ, получаемого с помощью $\sqrt{\delta}$, то и δ является частичной нормой некоторого целого или дробного числа из поля Дирихле K_ν, получаемого с помощью $\sqrt{\nu}$.*

Действительно, пусть

$$\nu=\nu(\alpha+\beta\sqrt{\delta})=\alpha^2-\beta^2\delta,$$

где α и β — числа поля k. Тогда

$$\delta=\left(\frac{\alpha}{\beta}\right)^2-\left(\frac{1}{\beta}\right)^2\nu,$$

т. е. δ равно частичной норме числа $\dfrac{\alpha+\sqrt{\nu}}{\beta}$, принадлежащего полю K_ν.

Теорема 3. *Если ν является частичной нормой некоторого идеала из K_δ и система характеров ν в K_δ состоит из одних плюс единиц, то ν равно частичной норме некоторого целого или дробного числа поля K_δ.*

Применив принадлежащую Г. Минковскому теорему о дискриминанте произвольного поля алгебраических чисел[3] к биквадратичному полю Дирихле K_δ, получим, что в каждом классе идеалов поля Дирихле K_δ существует идеал $\mathfrak{J}$, норма которого $N(\mathfrak{J})$ по абсолютной величине меньше, чем $3|\sqrt{D}|/(2\pi^2)$, где D обозначает дискриминант поля K_δ. Так как $D \leqslant 2^8|\delta|^2$ и $3 \cdot 2^3/\pi^2 < \sqrt{6}$ и, кроме того, норма $N(\mathfrak{J})$ равна по абсолютной величине квадрату абсолютного значения частичной нормы $\nu = \nu(\mathfrak{J})$, мы заключаем, что в любом классе идеалов поля K_δ можно найти идеал $\mathfrak{J}$, для которого $|\nu(\mathfrak{J})|^2 < \sqrt{6}|\delta|$.

Сначала мы докажем непосредственным вычислением, что теорема 3 выполняется для всех полей Дирихле K_δ, для которых $|\delta| < \sqrt{6}$. Используя неравенство, полученное только что с помощью теоремы Минковского, мы представим это доказательство в виде следующей таблицы, в которой в столбце «δ» приведены все значения δ, по абсолютной величине меньшие $\sqrt{6}$, в столбце «ν» представлены ν, удовлетворяющие условиям теоремы 3 и неравенству $|\nu|^2 < \sqrt{6}|\delta|$, а в последнем столбце стоит число из поля K_δ, частичная норма которого равна ν:

δ	ν	
$1 \pm 2i$	$1 \mp i$	$\frac{1+i\sqrt{1\pm 2i}}{1\pm i}$
$2 \pm i$	$2 \mp i$	$1 \mp i + i\sqrt{2 \pm i}$
	$1 \pm i$	$i + i\sqrt{2 \pm i}$
$1 \pm i$	$\pm i$	$i + i\sqrt{1 \pm i}$
i	$1 + i$	$1 + i\sqrt{i}$

Пусть теперь δ — некоторое целое мнимое число с абсолютной величиной $|\delta| > \sqrt{6}$. Будем предполагать, что теорема 3 уже доказана для всех полей $K_{\delta'}$, для которых $|\delta'| < |\delta|$. Итак, пусть ν — частичная норма некоторого идеала $\mathfrak{J}$, система характеров которого в K_δ состоит из одних плюс единиц. Тогда в K_δ можно указать эквивалентный $\mathfrak{J}$ идеал $\mathfrak{J}'$ с частичной нормой ν', квадрат абсолютной величины которой меньше $\sqrt{6}|\delta|$. Так как $\sqrt{6} < |\delta|$, мы заключаем, что $|\nu'| < |\delta|$. С другой стороны, ν' является частичной нормой некоторого идеала в K_δ, система характеров которого состоит из одних плюс единиц, поэтому, в силу теоремы 1, целое мнимое число δ

[3] См. C. R. за 1891 г. Для наших целей вполне достаточно и неравенства, установленного Г. Минковским (J. Math., 1891, Bd. 107, S. 296).

является частичной нормой некоторого идеала из поля $K_{\nu'}$, определенного с помощью $\sqrt{\nu'}$, и система характеров этого идеала состоит из одних плюс единиц. Ввиду условия $|\nu'| < |\delta|$ теорема 3 выполняется в $K_{\nu'}$ и, следовательно, δ является частичной нормой некоторого целого или дробного числа поля $K_{\nu'}$, откуда по теореме 2 вытекает, что и ν' является частичной нормой некоторого числа из K_δ. Так как идеал $\mathfrak{J}$ эквивалентен $\mathfrak{J}'$, частное этих двух идеалов является числом поля K_δ; следовательно, частное чисел ν и ν', а значит, и само ν являются частичными нормами некоторых чисел из K_δ. Итак, теорема 3 выполняется для поля K_δ, откуда следует ее справедливость в общем случае[4].

Наконец, из теоремы 3 очень просто следует высказанное в начале этого параграфа утверждение о классах идеалов главного рода. Именно, если $\mathfrak{J}$ — идеал из главного рода, то его частичная норма $\nu(\mathfrak{J})$ — при условии, что в отношении множителя i мы следуем рецепту, указанному на с. 158, — удовлетворяет всем условиям теоремы 3. Из этой теоремы следует, что в поле K_δ существует такое число A, что $\nu(\mathfrak{J}) = \nu(\mathsf{A})$. Пусть $\frac{\mathfrak{J}}{\mathsf{A}} = \frac{\mathfrak{H}}{\mathfrak{H}'}$, где $\mathfrak{H}$ и $\mathfrak{H}'$ — взаимно простые идеалы. Тогда должно выполняться равенство $\frac{\mathfrak{H} \cdot S\mathfrak{H}}{\mathfrak{H}' \cdot S\mathfrak{H}'} = 1$ и, следовательно, $\mathfrak{H}' = S\mathfrak{H}$. Так как $\mathfrak{H} \cdot S\mathfrak{H}$ можно считать равным некоторому числу α поля k, мы заключаем, что $\mathfrak{J} = \frac{\mathsf{A}}{\alpha}\mathfrak{H}^2$, т. е. $\mathfrak{J}$ должен быть эквивалентен квадрату идеала $\mathfrak{H}$.

§ 5. Амбивалентные идеалы

Идеал $\mathfrak{J}$ поля Дирихле K называется *амбивалентным* (ambige), если он не меняется под действием операции S и не содержит в качестве множителя никакого числа поля k. Чтобы получить все амбивалентные идеалы, мы обозначим, как и в § 3, через $\lambda_1, \ldots, \lambda_s$ все простые числа, входящие в частичный дискриминант d поля K, и положим $\lambda_1 = \mathfrak{L}_1^2, \ldots, \lambda_s = \mathfrak{L}_s^2$. Тогда ввиду условия $\mathfrak{L} = S\mathfrak{L}$ все s идеалов $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$ будут амбивалентны, равно как будут амбивалентны и все 2^s произведений $\mathfrak{U} = \prod \mathfrak{L}$, которые могут быть образованы из s идеалов $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$. Легко доказать, что в поле K нет других амбивалентных идеалов. Именно, если $\mathfrak{J} = \mathfrak{P}\mathfrak{Q} \ldots \mathfrak{R}$ — амбивалентный идеал, где $\mathfrak{P}, \mathfrak{Q}, \ldots, \mathfrak{R}$ — простые идеалы, то в силу условия $\mathfrak{J} = S\mathfrak{J}$ простые идеалы $S\mathfrak{P}, S\mathfrak{Q}, \ldots, S\mathfrak{R}$ должны совпадать с $\mathfrak{P}, \mathfrak{Q}, \ldots, \mathfrak{R}$ с точностью до порядка следования. Если бы выполнялось равенство $S\mathfrak{P} = \mathfrak{Q}$, то $\mathfrak{J}$ содержал бы множитель $\mathfrak{P}S\mathfrak{P}$, равный целому мнимому числу, а так как это противоречит нашему предположению, мы заключаем, что $\mathfrak{P} = S\mathfrak{P}$, равно как и $\mathfrak{Q} = S\mathfrak{Q}, \ldots, \mathfrak{R} = S\mathfrak{R}$, т. е. все идеалы $\mathfrak{P}, \mathfrak{Q}, \ldots, \mathfrak{R}$ являются амбивалентными простыми идеалами, а так как квадрат любого такого идеала

---

[4] Только что доказанная теорема 3 позволяет также сформулировать необходимые и достаточные условий разрешимости в целых мнимых числах ξ, η, ζ тернарного диофантова уравнения

$$\alpha\xi^2 + \beta\eta^2 + \gamma\zeta^2 = 0$$

с произвольными целыми мнимыми коэффициентами α, β, γ.

равен целому мнимому числу, мы одновременно приходим к выводу, что идеалы $\mathfrak{P}, \mathfrak{Q}, \ldots, \mathfrak{R}$ должны быть попарно различны. Оформим полученный результат в виде следующей теоремы.

Теорема 1. *Простыми амбивалентными идеалами в поле Дирихле K являются s простых идеалов $\mathfrak{L}_1, \ldots, \mathfrak{L}_s$, входящих множителями в частичный дискриминант d, и только они. Совокупность всех амбивалентных идеалов поля K образована 2^s построенными из них произведениями $\mathfrak{U} = \prod \mathfrak{L}$.*

§ 6. Амбивалентные классы

Если $\mathfrak{J}$ — идеал из класса C, то класс идеалов, содержащий идеал $S\mathfrak{J}$, будет обозначаться через SC. В частности, если $C = SC$, то класс идеалов C называется *амбивалентным*. Так как произведение $\mathfrak{J} \cdot S\mathfrak{J}$ эквивалентно 1, то $C \cdot SC = 1$ и, следовательно, квадрат любого амбивалентного класса равен главному классу 1. Обратно, если квадрат некоторого класса C равен 1, то $C = \dfrac{1}{C} = SC$ и, следовательно, C — амбивалентный класс [5].

Возникает задача описания всех амбивалентных классов. Так как, очевидно, любой амбивалентный идеал $\mathfrak{J}$, в силу своего свойства $\mathfrak{J} = S\mathfrak{J}$, принадлежит некоторому амбивалентному классу, нам нужно прежде всего выяснить, сколько попарно различных амбивалентных классов возникает из 2^s амбивалентных идеалов.

Произведение всех входящих множителями в δ идеалов $\mathfrak{L}$ равно $\sqrt{\delta}$ и, следовательно, является главным идеалом. Выберем теперь в поле K какую-нибудь основную единицу E, т. е. единицу, обладающую тем свойством, что любая другая единица поля равна $\varrho \mathsf{E}^m$, где ϱ — некоторый корень из единицы, а m — некоторое положительное или отрицательное целое число. Так как неприводимое уравнение, которому удовлетворяет ϱ, должно быть 2-й или 4-й степени, то ϱ может быть только корнем из единицы 2-й, 3-й, 4-й, 5-й или 8-й степени либо же является произведением таких корней из единицы. Корень из единицы 3-й степени появляется в поле K только при $\delta = 3$. Далее, легко показать, что корень 5-й степени из единицы никогда не появляется в поле K. Наконец, корень 8-й степени из единицы появляется в поле K в случае $\delta = i$. Оба случая $\delta = 3$ и $\delta = i$ будут особо рассмотрены ниже, а пока исключим их из рассмотрения, так что далее мы считаем, что $\varrho = \pm 1$ или $\pm i$.

Основная единица E определена с точностью до некоторого множителя ϱ. Содержит ли K другие амбивалентные главные идеалы, кроме 1 и $\sqrt{\delta}$, зависит только от того, чему равняется $\nu(\mathsf{E})$: ± 1 или $\pm i$.

Действительно, предположим сначала, что $\nu(\mathsf{E}) = \pm 1$. Так как мы можем выбрать в качестве основной единицы $i\mathsf{E}$ вместо E, мы можем считать, что $\nu(\mathsf{E}) = +1$. Положим[5)] $1 + \mathsf{E} = \alpha \mathsf{A}$, где α — целое мнимое число и A — целое число поля K, которое не делится ни на одно целое мнимое число.

[5)] Подоплекой этого подхода является частный случай одного выражения, рассмотренного Куммером (J. Math., 1855, Bd. 50, S. 212).

Из равенства $\frac{\mathsf{A}}{S\mathsf{A}} = \mathsf{E}$ вытекает, что A — амбивалентный главный идеал. Далее, этот главный идеал отличен от 1 и от $\sqrt{\delta}$. Действительно, если бы $\mathsf{A} = \varrho\mathsf{E}^m$ или $\varrho\mathsf{E}^m\sqrt{\delta}$, то выполнялось бы равенство

$$\frac{\mathsf{A}}{S\mathsf{A}} = \pm\left(\frac{\mathsf{E}}{S\mathsf{E}}\right)^m = \pm\mathsf{E}^{2m},$$

а эта единица не может быть равна E, так как m — целое число и E не является корнем из единицы. Далее, очевидно, что любой другой амбивалентный главный идеал поля K может быть получен как произведение $\sqrt{\delta}$ и A. В самом деле, если B — произвольный амбивалентный главный идеал, то должно быть $\frac{\mathsf{B}}{S\mathsf{B}} = \varrho\mathsf{E}^m$. Из равенства $\nu\left(\frac{\mathsf{B}}{S\mathsf{B}}\right) = +1$ следует, что $\varrho = \pm 1$; положим $\varrho = (-1)^n$, где n принимает значения 0 или 1. Тогда число $\Gamma = \mathsf{B}(\sqrt{\delta})^n\mathsf{A}^{-m}$ удовлетворяет равенству $\frac{\Gamma}{S\Gamma} = +1$ и, следовательно, является числом поля k, что делает наше утверждение очевидным.

Если, с другой стороны, частичная норма $\nu(\mathsf{E})$ равна i, то не существует амбивалентных главных идеалов, отличных от 1 и $\sqrt{\delta}$. В самом деле, если бы $\mathfrak{U} = \mathsf{A}$ был таким идеалом, то должно было бы выполняться равенство $\frac{\mathsf{A}}{S\mathsf{A}} = \varrho\mathsf{E}^m$. Но так как $\nu\left(\frac{\mathsf{A}}{S\mathsf{A}}\right) = 1$, отсюда вытекает, что $[\nu(\mathsf{E})]^m = \pm 1$ и, следовательно, m должно быть четным числом. Ввиду того что $\mathsf{E}^2 = \frac{i\mathsf{E}}{S\mathsf{E}}$, число $\mathsf{B}{=}\mathsf{A}\mathsf{E}^{-m/2}$ удовлетворяет равенству $\frac{\mathsf{B}}{S\mathsf{B}}{=}\varrho$, а так как $\nu\left(\frac{\mathsf{B}}{S\mathsf{B}}\right) = +1$, мы заключаем, что $\varrho = \pm 1$. С учетом того, что B не может делиться ни на какое целое мнимое число, предположение, что $\frac{\mathsf{B}}{S\mathsf{B}} = +1$, влечет $\mathsf{B} = \varrho$, а предположение, что $\frac{\mathsf{B}}{S\mathsf{B}} = -1$, влечет $\mathsf{B} = \varrho\sqrt{\delta}$, чем наше утверждение и доказано.

Теперь мы выразим один из s простых амбивалентных идеалов через $s-1$ остальных амбивалентных простых идеалов и через $\sqrt{\delta}$ и далее, если частичная норма основной единицы равна ± 1, выразим один из этих $s-1$ амбивалентных идеалов через $s-2$ остальных и через A. Будем называть некоторое число классов идеалов *независимыми* друг от друга, если ни один из них не равен 1 или некоторому произведению остальных. Очевидно, справедлив следующий результат.

Теорема 2. *s амбивалентных простых идеалов определяют $s-2$ или $s-1$ независимых друг от друга амбивалентных классов в зависимости от того, равна ли частичная норма основной единицы ± 1 или $\pm i$. Все 2^s амбивалентных идеалов определяют в первом случае 2^{s-2}, а во втором — 2^{s-1} попарно различных амбивалентных классов идеалов.*

Что касается исключенных выше случаев $\delta = 3$ и $\delta = i$, то в первом из них только что приведенная теорема остается справедливой, так как единственный амбивалентный идеал $\mathfrak{L} = \sqrt{3}$ является главным и норма основной

единицы равна $\pm i$. Во втором же случае, когда $\delta = i$, приведенный в теореме критерий перестает быть применимым, так как частичная норма корня из единицы $\sqrt{i}$ равна $-i$. Можно проверить, что и в случае $\delta = i$ единственный имеющийся амбивалентный идеал, возникающий из разложения $1 + i$, является главным.

Отметим здесь еще тот более общий случай, когда δ — простое число и, кроме того, $\delta \equiv \pm 1$ по модулю $(1 + i)^4$. В этом случае снова $s = 1$ и из вышеизложенного следует, что частичная норма основной единицы должна быть равна $\pm i$.

Остается еще ответить на вопрос, имеются ли в поле K амбивалентные классы, которые не содержат амбивалентных идеалов. С этой целью выберем в амбивалентном классе C произвольный идеал $\mathfrak{J}$. Тогда частное $\frac{\mathfrak{J}}{S\mathfrak{J}}$ равно некоторому числу A поля K. Так как мы вольны выбрать iA вместо A, мы можем предполагать, что $\nu(\mathsf{A}) = +1$ или $+i$.

В первом случае рассмотрим число $\mathsf{B} = 1 + S\mathsf{A}$. Ввиду того что $\frac{\mathsf{B}}{S\mathsf{B}} = \frac{1}{\mathsf{A}}$, мы имеем $\frac{\mathsf{B}\mathfrak{J}}{S(\mathsf{B}\mathfrak{J})} = 1$, т. е. $\mathsf{B}\mathfrak{J} = S(\mathsf{B}\mathfrak{J})$. Тогда мы можем записать $\mathsf{B}\mathfrak{J} = \frac{\alpha}{\beta}\mathfrak{U}$, где α и β — целые мнимые числа, а идеал $\mathfrak{U}$ не делится ни на какое целое мнимое число; отсюда следует, что $\mathfrak{U}$ — амбивалентный идеал. Таким образом, класс C содержит амбивалентный идеал.

Обратимся ко второму случаю, когда $\nu(\mathsf{A}) = i$. Мы видим прежде всего, что в этом случае система характеров числа i должна состоять из одних плюс единиц. Ответ на поставленный выше вопрос зависит от того, чему равняется частичная норма нашей основной единицы: $+1$ или $+i$. В последнем случае мы просто поставим $\frac{\mathsf{A}}{\mathsf{E}}$ вместо A. Тогда только что проведенные рассуждения показывают, что в классе идеалов C содержится амбивалентный идеал. Если же $\nu(\mathsf{E}) = +1$, то класс C не содержит ни одного амбивалентного идеала. Действительно, если бы $\mathfrak{U} = \mathsf{B}\mathfrak{J}$, где B означает некоторое число из K, был таким идеалом, то мы имели бы $\frac{\mathfrak{U}}{S\mathfrak{U}} = \frac{\mathsf{B}}{S\mathsf{B}}\mathsf{A}$. Но, с другой стороны, $\frac{\mathfrak{U}}{S\mathfrak{U}}$ должно быть равно некоторой единице, скажем $\varrho\mathsf{E}^m$, а так как $\nu(\mathsf{E}) = 1$, отсюда следовало бы, что $\nu(\mathsf{A}) = \pm 1$, вопреки нашему предположению.

Предположим теперь, что система характеров числа i в поле K состоит из одних плюс единиц. Тогда по теореме 3 § 4 существует число A, частичная норма которого равна i, и если мы предположим еще, что $\nu(\mathsf{E}) = 1$, то число A должно быть обязательно дробным. Запишем $\mathsf{A} = \frac{\mathfrak{J}}{\mathfrak{J}'}$, где $\mathfrak{J}$ и $\mathfrak{J}'$ — взаимно простые идеалы. Тогда $\frac{\mathfrak{J} \cdot S\mathfrak{J}}{\mathfrak{J}' \cdot S\mathfrak{J}'} = 1$, откуда следует, что $\mathfrak{J}' = S\mathfrak{J}$, т. е. $\mathfrak{J}$ эквивалентен $S\mathfrak{J}$ и, следовательно, определяет некоторый амбивалентный класс C; по только что доказанному этот класс C не содержит амбивалентных идеалов. Объединим полученные результаты в виде следующей теоремы.

Теорема 3. *В поле K тогда и только тогда существует амбивалентный класс, не содержащий амбивалентных идеалов, когда система характеров числа i состоит из одних плюс единиц и частичная норма основной единицы равна* ± 1.

Та же техника позволяет описать все амбивалентные классы с указанным свойством. Именно, предположим, что существуют два амбивалентных класса идеалов, не содержащих амбивалентных идеалов, и выберем из них по одному идеалу $\mathfrak{J}$ и $\mathfrak{J}'$. Из предыдущего изложения вытекает, что частичные нормы обоих чисел $\mathsf{A} = \dfrac{\mathfrak{J}}{S\mathfrak{J}}$ и $\mathsf{A}' = \dfrac{\mathfrak{J}'}{S\mathfrak{J}'}$ должны быть равны $\pm i$ и, следовательно, $\nu\left(\dfrac{\mathsf{A}}{\mathsf{A}'}\right) = \pm 1$. Предположим, на что мы имеем право, что в этих равенствах имеют место верхние знаки. Тогда мы получаем, что $\mathsf{B} = 1 + \dfrac{S\mathsf{A}}{S\mathsf{A}'}$ удовлетворяет равенству $\dfrac{\mathsf{B}}{S\mathsf{B}} = \dfrac{\mathsf{A}'}{\mathsf{A}}$. Это дает нам $\mathsf{B}\dfrac{\mathfrak{J}}{\mathfrak{J}'} = S\left(\mathsf{B}\dfrac{\mathfrak{J}}{\mathfrak{J}'}\right)$; мы можем, следовательно, записать $\mathsf{B}\dfrac{\mathfrak{J}}{\mathfrak{J}'} = \dfrac{\alpha}{\beta}\mathfrak{U}$, где α и β — целые мнимые числа, а идеал $\mathfrak{U}$ не делится ни на какое целое мнимое число. Таким образом, $\mathfrak{U}$ — амбивалентный идеал, и, следовательно, частное идеалов $\mathfrak{J}$ и $\mathfrak{J}'$ эквивалентно некоторому амбивалентному идеалу. Мы доказали следующую теорему.

Теорема 4. *Если в поле K имеется амбивалентный класс, который не содержит амбивалентных идеалов, то для того, чтобы получить все другие классы с тем же свойством, следует данный класс умножить поочередно на все классы, порожденные амбивалентными идеалами.*

Полученные выше результаты позволяют найти число всех амбивалентных классов. Рассмотрим тот случай, когда система характеров числа i состоит из одних плюс единиц. Из теорем 2, 3 и 4 следует, что в этом случае существует ровно 2^{s-1} амбивалентных классов, где s означает число простых делителей частичного дискриминанта d. Среди этих 2^{s-1} амбивалентных классов либо все, либо лишь половина порождены амбивалентными идеалами, в зависимости от того, равна ли частичная норма основной единицы $\pm i$ или ± 1. Если же в систему характеров числа i входит хоть одна минус единица, то норма основной единицы должна быть равна ± 1; тогда по теоремам 2 и 3 существует только 2^{s-2} амбивалентных классов и все они порождаются амбивалентными идеалами. Положим теперь $c = s$ или $s-1$ в зависимости от того, состоит система характеров числа i из одних плюс единиц или нет. Тогда, как было объяснено в § 3, c есть число тех характеров, которые определяют род идеала, и мы получаем такую теорему.

Теорема 5. *Существует ровно $c-1$ независимых друг от друга амбивалентных классов, где c означает число характеров, которые определяют род любого класса. Следовательно, число всех попарно различных амбивалентных классов идеалов равно* 2^{c-1}.

Легко проверяется, что эта общая теорема верна и для особого случая поля Дирихле, определенного с помощью $\sqrt{i}$, которое было выше исключено из рассмотрения.

§ 7. Число существующих родов

Результаты, полученные в §§ 4, 5 и 6, позволяют нам вычислить число родов, имеющихся в заданном числовом поле Дирихле K. Так как система характеров некоторого класса идеалов поля K состоит из c отдельных характеров, каждый из которых может принимать значение $+1$ или -1, то возникает важный вопрос, для любой ли из этих возможных 2^c систем характеров существует некоторый род или только часть этих систем характеров действительно представлена некоторыми родами? Чтобы получить ответ на этот вопрос, мы обозначим число имеющихся попарно различных родов через g, а число классов главного рода — через f [6]. Тогда, очевидно, любой другой род также должен содержать f классов, т. е. число всех классов поля равно gf.

Обозначим теперь классы главного рода через $H_1, \ldots, H_f$. В силу утверждения, доказанного в § 4, мы можем записать $H_1 = Q_1^2, \ldots, H_f = Q_f^2$, где $Q_1, \ldots, Q_f$ — некоторые классы поля. Пусть теперь C — произвольный класс поля K. Тогда, поскольку C^2, очевидно, принадлежит главному роду, имеем $C^2 = Q_r^2$, где Q_r — один из только что определенных классов $Q_1, \ldots, Q_f$. Следовательно, $\dfrac{C}{Q_r}$ является амбивалентным классом идеалов A, т. е. $C = AQ_r$. Так как по теореме 5 из § 6 число амбивалентных классов равно 2^{c-1}, то выражение AQ представляет ровно $2^{c-1}f$ классов идеалов. Все они отличны друг от друга. Действительно, если бы $AQ_r = A'Q_{r'}$, где A' — некоторый амбивалентный класс и $Q_{r'}$ обозначает один из ранее определенных классов $Q_1, \ldots, Q_f$, то было бы $Q_r^2 = Q_{r'}^2$, т. е. $H_r = H_{r'}$ и, следовательно, $r = r'$. Из $Q_r = Q_{r'}$, сразу следует $A = A'$, чем наше утверждение и доказано [7].

Приравнивая найденное число $2^{c-1}f$ всех классов и ранее полученное число gf, мы получаем $g = 2^{c-1}$. Тем самым мы ответили на вопрос, поставленный в начале этого параграфа, и получили следующий результат.

Число имеющихся родов равно половине возможных систем характеров, а именно равно 2^{c-1}, где c обозначает число характеров, определяющих род.

§ 8. Закон взаимности

После того как в предыдущем параграфе было показано, что лишь половина всех возможных систем характеров действительно представлена некоторыми родами, возникает вопрос об условиях, которым должна удовлетворять система характеров, чтобы для нее существовал соответствующий род. Мы ответим на этот вопрос с помощью установленного Дирихле закона взаимности для квадратичных вычетов и невычетов в области целых мнимых чисел.

Прежде всего, чтобы выяснить характер вычетов числа i, будем считать, что $\varkappa$ — простое число поля k, отличное от $1+i$, и что, кроме того, $\varkappa \equiv (00)$ по модулю $(1+i)^4$. Тогда, согласно сделанному в § 6 замечанию, в поле $K_\varkappa$, полученном с помощью $\sqrt{\varkappa}$, частичная норма основной единицы равна $\pm i$,

поэтому по теореме, доказанной в начале § 3, i должно быть квадратичным вычетом относительно $\varkappa$. Если $\varkappa$ — простое число и $\varkappa \equiv (10)$ по модулю $(1+i)^4$, то $i\varkappa \equiv (00)$ и, следовательно, в этом случае опять будет $\left[\frac{i}{\varkappa}\right] = +1$.

Далее, рассмотрим поле Дирихле K_i, полученное с помощью $\sqrt{i}$. Очевидно, в нем $1+i$ — единственный простой множитель частичного дискриминанта. Символ $\left[\frac{i}{1+i:i}\right]$ равен $+1$, и в поле K_i существует только один характер $\left[\frac{\nu}{1+i:i}\right]$. Следовательно, число возможных систем характеров в K_i равно 2, а так как только половина из них представлена родами, то имеется только один род и потому $\left[\frac{\nu}{1+i:i}\right] = +1$, где ν обозначает частичную норму произвольного идеала. Пусть теперь $\varkappa$ — некоторое простое число, причем $\varkappa \equiv (t_\varkappa t'_\varkappa)$ по модулю $(1+i)^4$. Тогда если i — квадратичный вычет по модулю $\varkappa$, то согласно § 2, $\varkappa$ — частичная норма некоторого простого идеала, откуда следует, что $\left[\frac{\varkappa}{1+i:i}\right] = (-1)^{t'_\varkappa} = +1$, т. е. $t'_\varkappa = 0$. Этот результат обратен предыдущему. Вместе оба эти результата дают такую теорему.

Если $\varkappa$ — простое число и $\varkappa \equiv (t_\varkappa t'_\varkappa)$ по модулю $(1+i)^4$, то характер числа i как квадратичного вычета относительно $\varkappa$ определяется формулой

$$\left[\frac{i}{\varkappa}\right] = (-1)^{t'_\varkappa}.$$

Чтобы определить характер числа $1+i$ как квадратичного вычета, рассмотрим сначала поле $K_\varkappa$, полученное с помощью $\sqrt{\varkappa}$, где $\varkappa$ — простое число и $\varkappa \equiv (000)$ по модулю $(1+i)^5$. Так как в этом поле может существовать только один род и, как было показано выше, характер $\left[\frac{i}{\varkappa:\varkappa}\right]$ равен $+1$, мы заключаем, что норма любого идеала также должна иметь характер $+1$. Поскольку согласно § 2 число $1+i$ распадается на два идеала в поле $K_\varkappa$ и, следовательно, является частичной нормой некоторого идеала, то $\left[\frac{1+i}{\varkappa:\varkappa}\right] = \left[\frac{1+i}{\varkappa}\right] = +1$. Если $\varkappa \equiv (100)$, то $i\varkappa \equiv (000)$ по модулю $(1+i)^5$ и, следовательно, в этом случае мы снова имеем $\left[\frac{1+i}{\varkappa}\right] = +1$.

Пусть теперь $\varkappa$ — простое число и $\varkappa \equiv (t_\varkappa 0 t''_\varkappa)$ по модулю $(1+i)^5$. Предположим, что $\left[\frac{1+i}{\varkappa}\right] = +1$. Тогда $\varkappa$ распадается в поле, полученном с помощью $\sqrt{1+i}$, а так как в этом поле существует только один род и число i имеет характер $+1$, мы заключаем что и $\left[\frac{\varkappa}{1+i:1+i}\right] = (-1)^{t''_\varkappa} = +1$, т. е. $t''_\varkappa = 0$.

Вместе взятые, эти два результата определяют характер числа $1+i$ как квадратичного вычета относительно $\varkappa$ при $t'_\varkappa = 0$, а именно, при этом пред-

положении справедлива формула

$$\left[\frac{1+i}{\varkappa}\right] = (-1)^{t''_\varkappa}.$$

Наконец, пусть $\varkappa$ — простое число и $\varkappa \equiv (t_\varkappa 1 t''_\varkappa)$ по модулю $(1+i)^5$. Легко проверить, что в поле, полученном с помощью $\sqrt{(1+i)\varkappa}$, оба характера числа i равны -1 и, следовательно, существует только один род. Поэтому если ν — частичная норма некоторого идеала, то оба характера числа ν, т. е. символы $\left[\frac{\nu}{\varkappa : (1+i)\varkappa}\right]$ и $\left[\frac{\nu}{1+i : (1+i)\varkappa}\right]$ должны быть одновременно или оба положительны, или оба отрицательны. Отсюда, если принять $\nu = \varkappa$, получается формула

$$\left[\frac{1+i}{\varkappa}\right] = (-1)^{1+t''_\varkappa}.$$

Две только что полученные формулы можно объединить в одну, и таким образом мы получаем следующую теорему.

Если $\varkappa$ — простое число и $\varkappa = (t_\varkappa t'_\varkappa t''_\varkappa)$ по модулю $(1+i)^5$, то характер числа $1+i$ как квадратичного вычета относительно $\varkappa$ определяется формулой

$$\left[\frac{1+i}{\varkappa}\right] = (-1)^{t'_\varkappa + t''_\varkappa}.$$

Наконец, чтобы вывести закон взаимности для двух произвольных отличных от $1+i$ простых чисел, мы примем во внимание то обстоятельство, что из двух целых мнимых чисел α и $i\alpha$ всегда одно $\equiv (0 t_\alpha)$ по модулю $(1+i)^4$. Ниже мы всегда будем брать простые числа $\varkappa$ и π в таком виде, чтобы $t_\varkappa = 0, t_\pi = 0$.

Пусть сначала $\varkappa$ — простое число и $\varkappa \equiv (00)$ по модулю $(1+i)^4$. Тогда если π — такое простое число, что $\left[\frac{\varkappa}{\pi}\right] = +1$, то π может быть разложено в поле $K_\varkappa$, полученном с помощью $\sqrt{\varkappa}$, и, следовательно, является частичной нормой некоторого идеала. С помощью тех же рассуждений, что и выше, получаем, что должно быть $\left[\frac{\pi}{\varkappa}\right] = +1$. Итак, мы знаем следующие два факта.

Если $\varkappa \equiv (00), \pi \equiv (00)$ по модулю $(1+i)^4$ и $\left[\frac{\varkappa}{\pi}\right] = +1$, то $\left[\frac{\pi}{\varkappa}\right] = +1$, (1)

если $\varkappa \equiv (00), \pi \equiv (01)$ по модулю $(1+i)^4$ и $\left[\frac{\varkappa}{\pi}\right] = +1$, то $\left[\frac{\pi}{\varkappa}\right] = +1$. (2)

Далее, пусть $\varkappa \equiv (01)$ по модулю $(1+i)^4$. Тогда в поле $K_\varkappa$, полученном с помощью $\sqrt{\varkappa}$, имеются два характера, но только один род, потому что система характеров числа i, как легко обнаружить непосредственным вычислением, состоит из двух минус единиц. Поэтому если π — такое простое число, что $\left[\frac{\varkappa}{\pi}\right] = +1$, то характеры $\left[\frac{\pi}{1+i : \varkappa}\right]$ и $\left[\frac{\pi}{\varkappa : \varkappa}\right]$ должны быть либо оба положительны, либо оба отрицательны; отсюда следует, что

$\left[\frac{\pi}{\varkappa}\right] = +1$, и мы получаем, таким образом, следующие два факта.

Если $\varkappa \equiv (01), \pi \equiv (00)$ по модулю $(1+i)^4$ и $\left[\frac{\varkappa}{\pi}\right] = +1$, то $\left[\frac{\pi}{\varkappa}\right] = +1$, (3)

если $\varkappa \equiv (01), \pi \equiv (01)$ по модулю $(1+i)^4$ и $\left[\frac{\varkappa}{\pi}\right] = +1$, то $\left[\frac{\pi}{\varkappa}\right] = +1$. (4)

Эти четыре утверждения показывают, что, вообще, в предположении $t_\varkappa = 0$, $t_\pi = 0$, выполняется равенство $\left[\frac{\varkappa}{\pi}\right] = \left[\frac{\pi}{\varkappa}\right]$. Действительно, пусть сначала $t'_\varkappa = 0, t'_\pi = 0$. В силу (1) из $\left[\frac{\varkappa}{\pi}\right] = +1$ следует обязательно $\left[\frac{\pi}{\varkappa}\right] = +1$. Если же $\left[\frac{\varkappa}{\pi}\right] = -1$, то должно быть также $\left[\frac{\pi}{\varkappa}\right] = -1$, поскольку, меняя местами $\varkappa$ и π, мы получаем из (1), что из $\left[\frac{\pi}{\varkappa}\right] = +1$ должно следовать $\left[\frac{\varkappa}{\pi}\right] = +1$.

Далее, пусть $t'_\varkappa = 0, t'_\pi = 1$. Тогда по (2) из $\left[\frac{\varkappa}{\pi}\right] = +1$ должно следовать $\left[\frac{\pi}{\varkappa}\right] = +1$. Если же $\left[\frac{\varkappa}{\pi}\right] = -1$, то должно быть также $\left[\frac{\pi}{\varkappa}\right] = -1$, поскольку согласно (3) из $\left[\frac{\pi}{\varkappa}\right]=+1$ следовало бы, что и $\left[\frac{\varkappa}{\pi}\right]=+1$.

Наконец, пусть $t'_\varkappa = 1, t'_\pi = 1$. Согласно (4) из $\left[\frac{\varkappa}{\pi}\right]=+1$ должно следовать $\left[\frac{\pi}{\varkappa}\right]=+1$. Если же $\left[\frac{\varkappa}{\pi}\right]=-1$, то должно быть также $\left[\frac{\pi}{\varkappa}\right] = -1$, поскольку, снова согласно (4), из равенства $\left[\frac{\pi}{\varkappa}\right] = +1$ следовало бы, что и $\left[\frac{\varkappa}{\pi}\right] = +1$.

Чтобы применить установленную нами формулу $\left[\frac{\varkappa}{\pi}\right] = \left[\frac{\pi}{\varkappa}\right]$ к двум произвольным простым числам $\varkappa, \pi$, для которых не обязательно $t_\varkappa$ и t_π равны 0, мы должны в этой формуле вместо $\varkappa, \pi$ подставить $i^{t_\varkappa}\varkappa, i^{t_\pi}\pi$ соответственно, и тогда мы приходим к следующей теореме.

Если $\varkappa$ и π — отличные от $1+i$ простые числа, которые сравнимы по модулю $(1+i)^4$ с $(t_\varkappa t'_\varkappa)$ и $(t_\pi t'_\pi)$ соответственно, то выполняется закон взаимности

$$\left[\frac{\varkappa}{\pi}\right]\left[\frac{\pi}{\varkappa}\right] = (-1)^{t_\varkappa t'_\pi + t'_\varkappa t_\pi}.$$

Теперь мы определим общий символ $\left[\frac{\alpha}{\beta}\right]$, где $\alpha = \prod_\varkappa \varkappa$ и $\beta = \prod_\pi \pi$ — два произвольных числа, взаимно простых между собой и с $1+i$, равенством

$$\left[\frac{\alpha}{\beta}\right] = \prod_{\varkappa,\pi}\left[\frac{\varkappa}{\pi}\right];$$

здесь произведение берется по всем простым множителям $\varkappa$ и π чисел α и β соответственно, как они входят в разложение этих чисел в произведение. Из определения непосредственно вытекает следующая теорема.

Если α и β — произвольные взаимно простые между собой и с $1+i$ целые числа и если $\alpha \equiv (t_\alpha t'_\alpha)$, $\beta \equiv (t_\beta t'_\beta)$ по модулю $(1+i)^4$, то

$$\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = (-1)^{t_\alpha t'_\beta + t'_\alpha t_\beta}.$$

Эта формула дает нам возможность получить условие, которое должно связывать c характеров произвольного поля Дирихле для того, чтобы данная система характеров образовывала реально существующий род.

Будем сперва считать, что δ не делится на $1+i$, и положим тогда в вышеуказанной формуле $\alpha = \delta$ и $\beta = \nu$, где ν — частичная норма некоторого идеала в поле K_δ, взаимно простая с δ и с $1+i$. Тогда, поскольку согласно § 2 число δ должно быть квадратичным вычетом относительно всех простых чисел, входящих в ν в нечетных степенях, мы получаем $\left[\frac{\delta}{\nu}\right] = +1$ и, следовательно,

$$\left[\frac{\nu}{\delta}\right] = (-1)^{t_\delta t'_\nu + t'_\delta t_\nu}.$$

Если теперь $\delta \equiv (00)$ по модулю $(1+i)^4$, то частичный дискриминант d равен δ, и если мы обозначим все входящие в него простые числа через $\lambda_1, \ldots, \lambda_s$, то будет

$$\left[\frac{\nu}{\lambda_1}\right] \cdots \left[\frac{\nu}{\lambda_s}\right] = \left[\frac{\nu}{\lambda_1 : \delta}\right] \cdots \left[\frac{\nu}{\lambda_s : \delta}\right] = +1.$$

Если же $\delta \not\equiv (00)$ по модулю $(1+i)^4$, то $1+i$ входит в качестве множителя в частичный дискриминант d поля K_δ. Тогда мы обозначим входящие в δ простые числа через $\lambda_1, \ldots, \lambda_{s-1}$ и положим $1+i = \lambda_s$. В силу того что $\left[\frac{\nu}{1+i:\delta}\right] = (-1)^{t_\delta t'_\nu + t'_\delta t_\nu}$, мы снова получим

$$\left[\frac{\nu}{\lambda_1 : \delta}\right] \cdots \left[\frac{\nu}{\lambda_s : \delta}\right] = +1.$$

Наконец, пусть δ делится на $1+i$; положим $\delta = (1+i)\delta'$ и придадим ν то же значение, что и выше. Так как снова δ должно быть квадратичным вычетом относительно всех простых чисел, входящих в ν в нечетных степенях, то при вычислении множителей символа $\left[\frac{\delta'}{\nu}\right]$ число δ' можно заменить на $1+i$; тогда найденная выше формула для характера $1+i$ как квадратичного вычета дает нам $\left[\frac{\delta'}{\nu}\right] = (-1)^{t'_\nu + t''_\nu}$. Далее, полагая в общем уравнении взаимности $\alpha = \delta', \beta = \nu$ и используя только что найденное значение символа $\left[\frac{\delta'}{\nu}\right]$, получим $\left[\frac{\nu}{\delta'}\right] = (-1)^{t_{\delta'} t'_\nu + t'_{\delta'} t_\nu + t'_\nu + t''_\nu}$. Но символ $\left[\frac{\nu}{1+i:\delta}\right]$ имеет точно такое же значение, откуда снова, обозначив все делящие δ простые числа через $\lambda_1, \ldots, \lambda_s$, получаем равенство

$$\left[\frac{\nu}{\lambda_1 : \delta}\right] \cdots \left[\frac{\nu}{\lambda_s : \delta}\right] = +1.$$

Итак, во всех случаях справедлив следующий результат.

Данная система характеров тогда и только тогда представлена некоторым родом, когда произведение всех этих характеров равно $+1$.

§ 9. Специальные поля Дирихле

Если поле Дирихле K, полученное с помощью $\sqrt{\delta}$, содержит, кроме поля k, еще какое-нибудь квадратичное поле, то, как легко проверить, δ должно быть равно некоторому вещественному или чисто мнимому числу. В этом случае мы будем называть биквадратичное поле Дирихле, полученное с помощью $\sqrt{\delta}$, *специальным полем Дирихле*, и положим $\partial = \pm\delta$ (соответственно $\partial = \pm 2i\delta$), так что ∂ всегда означает вещественное положительное число, которое не делится ни на какой квадрат вещественного числа. Специальное поле Дирихле K является полем Галуа. Произвольное число из этого поля может быть представлено в виде

$$\mathsf{A} = a + bi + c\sqrt{\partial} + di\sqrt{\partial},$$

где a, b, c, d — рациональные числа, и мы получаем три сопряженных с A числа применением трех подстановок:

$$S = (\sqrt{\partial} : -\sqrt{\partial}),$$

$$S' = (i : -i),$$

$$S'' = SS' = (\sqrt{\partial} : -\sqrt{\partial}, i : -i).$$

Этим трем подстановкам соответствуют три содержащихся в K квадратичных поля; именно, все числа, которые остаются на месте при применении S, образуют квадратичное поле k, полученное с помощью i, а все числа поля K, которые остаются на месте при применении подстановок S' (соответственно S'') образуют еще два квадратичных поля — квадратичные поля, полученные с помощью $\sqrt{\partial}$ и $\sqrt{-\partial}$ соответственно. Первое из них мы будем обозначать через k', а второе — через k''.

Сделаем еще одно замечание, которое будет использовано в следующем параграфе.

Если некоторый идеал поля K может быть представлен как наибольший общий делитель таких чисел, которые все являются числами подполя k' (соответственно k''), то мы будем говорить, что этот идеал «*лежит*» в поле k', соответственно в k''. Если $\mathfrak{J}$ — какой-то идеал в K, то произведение $\mathfrak{J}S'\mathfrak{J}$ всегда лежит в поле k'. Действительно, выберем какое-нибудь число A, делящееся на $\mathfrak{J}$, и затем найдем число B, также делящееся на $\mathfrak{J}$ и такое, что $\dfrac{\mathsf{B}}{\mathfrak{J}}$ взаимно просто с $\dfrac{\mathsf{A}}{\mathfrak{J}}S'\left(\dfrac{\mathsf{A}}{\mathfrak{J}}\right)$. Тогда и $S'\left(\dfrac{\mathsf{B}}{\mathfrak{J}}\right)$, а следовательно, и $\dfrac{\mathsf{B}}{\mathfrak{J}}S'\left(\dfrac{\mathsf{B}}{\mathfrak{J}}\right)$ будет взаимно просто с $\dfrac{\mathsf{A}}{\mathfrak{J}}S'\left(\dfrac{\mathsf{A}}{\mathfrak{J}}\right)$, откуда следует $\mathfrak{J}\cdot S'\mathfrak{J} = (\mathsf{A}\cdot S'\mathsf{A}, \mathsf{B}\cdot S'\mathsf{B})$, что и доказывает наше утверждение. Аналогичным образом можно показать, что $\mathfrak{J}\cdot S''\mathfrak{J}$ всегда лежит в поле k''.

§ 10. Число классов идеалов специального поля Дирихле K

В этом последнем параграфе будет вкратце указан путь, приводящий к чисто арифметическому доказательству упомянутой во введении теоремы Дирихле о числе классов идеалов в K.

Для этой цели изложим сначала следующие соображения. Пусть c' и c'' — некоторые классы идеалов из квадратичных полей k' и k'' соответственно. Выберем в каждом из этих двух классов по идеалу $\mathfrak{j}', \mathfrak{j}''$. Тогда эти два идеала, рассматриваемые как идеалы биквадратичного поля K, принадлежат некоторым классам идеалов в K; эти два класса идеалов биквадратичного поля K, определенные таким образом через c' и c'', и их произведение мы будем обозначать через $\overline{c'}, \overline{c''}$ и $\overline{c'c''}$ соответственно. Прежде всего, справедлива следующая теорема.

Любой класс главного рода в биквадратичном поле K равен некоторому произведению $\overline{c'c''}$, где c', c'' — классы идеалов квадратичных полей k' и k'' соответственно.

Для доказательства этой теоремы мы воспользуемся тем обстоятельством, что любой идеал $\mathfrak{H}$ главного рода эквивалентен в биквадратичном поле квадрату некоторого идеала $\mathfrak{J}$. С другой стороны, выполняется тождество

$$\mathfrak{J}^2 = \frac{(\mathfrak{J} \cdot S'\mathfrak{J})(\mathfrak{J} \cdot S''\mathfrak{J})}{S'\mathfrak{J} \cdot S''\mathfrak{J}}.$$

Так как произведение $S'\mathfrak{J} \cdot S''\mathfrak{J}$ остается на месте при применении подстановки S, оно само равно некоторому числу в k и, следовательно, является главным идеалом. Так как $\mathfrak{J} \cdot S'\mathfrak{J}$ и $\mathfrak{J} \cdot S''\mathfrak{J}$ лежат в полях k' и k'' соответственно, мы заключаем, что идеал $\mathfrak{J}^2$, а тем самым и $\mathfrak{H}$, эквивалентен произведению некоторого идеала, лежащего в k', и некоторого идеала, лежащего в k''.

Пусть теперь $p_1, \ldots, p_\pi$ — входящие множителями в ∂ простые числа, удовлетворяющие сравнению $p \equiv 1$ по модулю 4, а $q_1, \ldots, q_\varkappa$ — входящие в ∂ простые числа, удовлетворяющие сравнению $q \equiv 3$ по модулю 4. Первые из этих простых чисел допускают представление в виде произведения двух целых мнимых чисел, скажем $p_1 = \alpha_1\beta_1, \ldots, p_\pi = \alpha_\pi\beta_\pi$.

Мы будем теперь называть *родами главного типа* [8] те роды в биквадратичном поле K, для которых характеры нормы ν удовлетворяют условиям

$$\left[\frac{\nu}{\alpha_1 : \partial}\right]\left[\frac{\nu}{\beta_1 : \partial}\right] = +1, \quad \ldots, \quad \left[\frac{\nu}{\alpha_\pi : \partial}\right]\left[\frac{\nu}{\beta_\pi : \partial}\right] = +1$$

и

$$\left[\frac{\nu}{q_1 : \partial}\right] = +1, \quad \ldots, \quad \left[\frac{\nu}{q_\varkappa : \partial}\right] = +1.$$

Непосредственно из этого определения следует утверждение, что роды главного типа составляют $2^{\pi+\varkappa-1}$-ю часть (соответственно $2^{\pi+\varkappa}$-ю часть) всех родов поля K в зависимости от того, нечетно ∂ или четно. Далее, справедлива следующая теорема.

В биквадратичном поле K любое произведение $\overline{c'c''}$ принадлежит некоторому роду главного типа, и, обратно, любой класс C биквадратичного поля K, принадлежащий роду главного типа, равен некоторому произведению $\overline{c'c''}$ [9].

Чтобы доказать первую часть этой теоремы, вспомним, что частичная норма любого идеала, лежащего в k' или в k'', является целым рациональным числом, и воспользуемся затем следующими двумя утверждениями.

1. Если $p = \alpha\beta$ — простое рациональное число, разложимое в k, то в области целых мнимых чисел любое рациональное число является одновременно квадратичным вычетом или невычетом относительно обоих сопряженных комплексных множителей α и β.

2. Если q — некоторое простое рациональное число, неразложимое в k, то в области целых мнимых чисел любое рациональное число является квадратичным вычетом относительно q.

Чтобы убедиться в справедливости второго, обратного утверждения теоремы, заметим, что в любом случае либо дискриминант квадратичного поля k', либо дискриминант квадратичного поля k'' должен содержать множитель 2. Тогда, как следует из теории квадратичных полей, в одном из этих двух квадратичных полей должен существовать род, характеры которого относительно простых чисел $p_1, \ldots, p_\pi$ совпадают со значениями символов $\left[\frac{\nu}{\alpha_1 : \partial}\right], \ldots, \left[\frac{\nu}{\alpha_\pi : \partial}\right]$ в том же порядке. Если a — некоторый класс такого рода в квадратичном поле k' или k'', то, как легко проверить, класс $C\bar{a}$ принадлежит главному роду в биквадратичном поле K и, следовательно, по доказанной ранее теореме равен $\overline{c'c''}$; откуда следует, что $C = \dfrac{\overline{c'c''}}{\bar{a}}$.

Следующая наша цель состоит в вычислении числа тех пар классов c', c'' из квадратичных полей k', k'' соответственно, для которых $\overline{c'c''} = 1$. Для этого нам потребуются следующие понятия и результаты из теории квадратичных полей.

Идеал квадратичного поля, который совпадает со своим сопряженным и который, кроме того, не делится ни на какое целое рациональное число, называется *амбивалентным идеалом*. Амбивалентные идеалы состоят из простых амбивалентных идеалов, которые определяются тем свойством, что их квадраты равны рациональным простым числам, содержащимся в качестве множителей в дискриминанте поля.

Любой класс квадратичного поля, квадрат которого является главным классом, называется *амбивалентным классом*. Если квадратичное поле мнимо, то любой амбивалентный класс содержит амбивалентный идеал и число амбивалентных классов равно $2^{\sigma-1}$, где σ — число простых рациональных чисел, делящих дискриминант.

Пусть c' и c'' — такие два класса квадратичных полей k' и k'' соответственно, что $\overline{c'c''} = 1$. Выберем из классов c' и c'' по одному идеалу $\mathfrak{j}'$ и $\mathfrak{j}''$ соответственно, и пусть $\mathfrak{j}'\mathfrak{j}'' = \mathsf{A}$, где A — некоторое число биквадратичного поля K. Применяя подстановку S'', получаем без труда, что $(\mathfrak{j}' \cdot S''\mathfrak{j}')\mathfrak{j}''^2 = \mathsf{A}S''\mathsf{A}$, т. е. $\mathfrak{j}''^2 = \alpha''$, где α'' — некоторое число квадратичного поля k''. Из этого следует, что $\mathfrak{j}''$ принадлежит некоторому амбивалентному классу a'' в k'', а так как k'' — мнимое квадратичное поле, то согласно только что приведенной теореме идеал $\mathfrak{j}''$ эквивалентен в k'' некоторому амбивалентному идеалу $\mathfrak{a}''$. Но, как легко проверить, все амбивалентные простые идеалы поля k'' лежат одновременно и в квадратичном поле k'; исключение составляет только случай $\partial \equiv 1$ по модулю 4; в этом случае амбивалентный простой идеал $\mathfrak{l}''$, возникающий из разложения числа 2, лежит в поле k'',

но не лежит в k'. Так как $\mathfrak{l}''$ равняется $1+i$ и, следовательно, является главным идеалом биквадратичного поля K, то, обозначая класс, определяемый $\mathfrak{l}''$, через $\overline{\mathfrak{l}''}$, получаем, очевидно, $\overline{\mathfrak{l}''}=1$. Пусть теперь $\mathfrak{a}''$ не делится на $\mathfrak{l}''$ и $\mathfrak{a}'$ — такой амбивалентный идеал в k', который, рассматриваемый как идеал в K, совпадает с идеалом $\mathfrak{a}''$; пусть, далее, a' — амбивалентный класс в k', определяемый идеалом $\mathfrak{a}'$; тогда, очевидно, $\overline{a'a''}=1$. Итак, имеет место следующая теорема.

Для любого из амбивалентных классов a'' в k'' и только для таких классов можно найти такой класс a' в k', что $\overline{a'a''}=1$.

Остается еще разрешить вопрос, когда для данного класса a'' поля k'' существует более одного класса c', удовлетворяющего условию $\overline{c'a''}=1$. Для этого, очевидно, необходимо, чтобы в поле k' существовал отличный от 1 класс c', для которого бы $\overline{c'}=1$.

Чтобы разобраться в этом вопросе, предположим, что $\mathfrak{h}'$ — некоторый идеал в k', становящийся главным в биквадратичном поле K. Пусть $\mathfrak{h}'=\mathsf{A}$, где A — некоторое число в K, тогда, очевидно, $\dfrac{\mathsf{A}}{S'\mathsf{A}}$ — единица поля K, которая по абсолютной величине равна 1 и которая, следовательно, является некоторым корнем ϱ из единицы. Положим теперь $\mathsf{B}=\mathsf{A}, i\mathsf{A}, \dfrac{\mathsf{A}}{1-i}$ или $\dfrac{\mathsf{A}}{1+i}$ в зависимости от того, принимает ли ϱ значение $+1,-1,+i$, или $-i$. Тогда получаем $\dfrac{\mathsf{B}}{S'\mathsf{B}}=1$, т. е. B является вещественным числом. Следовательно, $\mathfrak{h}'$ либо равен некоторому вещественному числу, т. е. некоторому главному идеалу в k', либо равен вещественному числу, умноженному на некоторый идеал $\mathfrak{l}'$, который, рассматриваемый как идеал в K, равен $1+i$. Так как в этом последнем случае должно быть $\mathfrak{l}'^2=2$, то он возникает только при условии $\partial\equiv 3$ по модулю 4 или $\partial\equiv 0$ по модулю 2. Обратно, идеал $\mathfrak{l}'$, заданный равенством $\mathfrak{l}'^2=2$, всегда определяет в k' некоторый класс $\mathfrak{l}'$, для которого $\overline{\mathfrak{l}'}=1$. Случай, когда K содержит еще и другие корни из единицы, также разбирается без труда.

Из сказанного вытекает следующий результат.

Число пар классов c', c'' в полях k' и k'' соответственно, для которых $\overline{c'c''}=1$, в случае нечетного ∂ равно $2^{\pi+\varkappa-1}$ или $2^{\pi+\varkappa}$, а в случае четного ∂ равно $2^{\pi+\varkappa}$ или $2^{\pi+\varkappa+1}$ в зависимости от того, является число 2, с точностью до умножения на единицу, квадратом некоторого числа из вещественного квадратичного поля k' или нет [10].

Обозначим теперь число классов идеалов c' и c'' в квадратичных полях k' и k'' через h' и h'' соответственно. Комбинаций вида $\overline{c'c''}$ имеется $h'h''$, и когда мы разделим это число $h'h''$ на только что найденное число пар классов, удовлетворяющих условию $\overline{c'c''}=1$, то получится число всех попарно различных классов $\overline{c'c''}$ нашего биквадратичного поля, принадлежащих главному типу. Но поскольку, как было показано выше, ровно $2^{\pi+\varkappa-1}$-я часть (соответственно $2^{\pi+\varkappa}$-я часть) всех родов поля K принадлежит главному типу в зависимости от того, нечетно ∂ или четно, мы получаем такую теорему [11].

Число классов идеалов специального поля Дирихле K равно произведению чисел классов идеалов квадратичных полей k' и k'' либо же равно половине этого произведения в зависимости от того, является число 2, с точностью до умножения на единицу, квадратом некоторого числа в вещественном квадратичном поле или нет.

Пусть α' обозначает число в k', квадрат которого, с точностью до умножения на единицу, дает число 2. Тогда $\frac{1+i}{\alpha'}$ — единица биквадратичного поля K, частичная норма которой равна $\pm i$. Справедливо и обратное утверждение, что число 2, с точностью до умножения на единицу, должно быть равно квадрату некоторого числа в k', коль скоро в K существует единица, частичная норма которой равна $\pm i$. Используя это обстоятельство, мы можем сформулировать полученную теорему еще и следующим образом:

Число классов идеалов в поле K равно произведению чисел классов в k' и k'' либо равно половине этого произведения в зависимости от того, равна частичная норма основной единицы этого поля $\pm i$ или ± 1.

Эта теорема совпадает по своему содержанию с теоремой, доказанной Дирихле[6], что становится ясным, если принять во внимание, что в теореме Дирихле речь идет о числе *классов форм* с заданным определителем, а в нашей теореме — о числе *классов идеалов* поля.

Кёнигсберг, 14 апреля 1894.

[6] *Dirichlet L.* Werke. Bd. 1. S. 618.

О ТЕОРИИ ОТНОСИТЕЛЬНО КВАДРАТИЧНЫХ ЧИСЛОВЫХ ПОЛЕЙ*)

ВВЕДЕНИЕ

Пусть за основу взято произвольное числовое поле k, степень этого поля k обозначим через m, а $m-1$ сопряженных с k полей будем обозначать через k', k'', ..., $k^{(m-1)}$. Число классов идеалов поля k будем обозначать через h.

Обозначим через μ некоторое число в k, которое не равно квадрату никакого числа из k. Тогда $\sqrt{\mu}$ вместе с числами поля k определяет некоторое поле степени $2m$, которое является квадратичным относительно k и будет обозначаться через $K(\sqrt{\mu})$ или, кратко, через K. Возникает проблема разработки и обоснования теории таких относительно квадратичных числовых полей. Эта проблема представляется нам естественным обобщением тех проблем, которые составляют предмет «disquisitiones arithmeticae» Гаусса.

Теория относительно квадратичных полей привела меня к открытию общего закона взаимности для квадратичных вычетов, согласно которому обычный закон взаимности между простыми рациональными числами — это всего лишь отдельное звено в цепи самых удивительных и разнообразных числовых соотношений.

Методы, которые я применяю в дальнейшем для изучения относительно квадратичных полей, с равным успехом применимы, будучи надлежащим образом обобщены, также и в теории относительно абелевых полей произвольной относительной степени и, в частности, приводят в этом случае к наиболее общим законам взаимности для произвольных высших степенных вычетов в произвольных алгебраических числовых областях[1]).

Если изложенное в данной работе доказательство общего закона взаимности для квадратичных вычетов перенести на развитую Куммером теорию l-х степенных вычетов в поле l-го корня из единицы, то получится новое доказательство закона взаимности Куммера для l-х степенных вычетов, которое существенно отличается как от доказательства Куммера, так и от данного мною ранее доказательства тем, что в нем *не* используется связанный с делением круга частный закон взаимности Эйзенштейна.

Среди приложений моей теории назову здесь установление критерия разрешимости квадратичного диофантова уравнения с произвольными алгебраическими коэффициентами в области рациональности, определенной этими коэффициентами.

---

*) Über die Theorie des relativquadratischen Zahlkörpres. — Math. Ann., 1899, Bd. 51, S. 1–127. *Перевод Л. В. Кузьмина.*

[1]) Ср. с конкурсной темой, предложенной на 1891 год Гёттингенским научным обществом (K. Gesellschaft der Wiss. zu Göttingen).

Данная работа состоит из *двух глав*. В *первой* главе излагаются *общие определения* и *предварительные результаты* теории относительно квадратичных полей для *произвольного* основного поля k; во *второй* главе дано *полное* построение теории относительно квадратичных полей над таким полем k, которое вместе со всеми своими сопряженными полями является *мнимым* и, кроме того, имеет *нечетное число классов* h. Что касается случая произвольного основного поля k, то я собираюсь в скором времени опубликовать в Göttinger Nachrichten наиболее важные теоремы соответствующей теории с краткими указаниями по поводу доказательств[2].

ГЛАВА 1

ОБЩИЕ ОПРЕДЕЛЕНИЯ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

§ 1. Квадратичные вычеты и невычеты в основном поле k и символ $\left(\frac{\alpha}{\mathfrak{p}}\right)$

Определение 1. Пусть $\mathfrak{p}$ — простой идеал поля k, не делящий числа 2, и α — произвольное взаимно простое с $\mathfrak{p}$ целое число поля k. Число α называется *квадратичным вычетом* по модулю $\mathfrak{p}$ в k, если α сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{p}$, т. е. если сравнение

$$\xi^2 \equiv \alpha, \qquad (\mathfrak{p})$$

выполняется при некотором целом числе ξ из поля k; в противном случае α называется *квадратичным невычетом* по модулю $\mathfrak{p}$. Определим теперь *символ* $\left(\frac{\alpha}{\mathfrak{p}}\right)$, полагая

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1,$$

если α — квадратичный вычет в k по модулю $\mathfrak{p}$, и

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = -1$$

в противном случае.

Теорема 1. *Если $\mathfrak{p}$ — произвольный простой идеал поля k, не делящий 2, и α — целое число в k, взаимно простое с $\mathfrak{p}$, то по модулю $\mathfrak{p}$ выполняется сравнение*

$$\alpha^{(n(\mathfrak{p})-1)/2} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right), \qquad (\mathfrak{p}),$$

где $n(\mathfrak{p})$ обозначает норму простого идеала $\mathfrak{p}$ поля k.

---

[2] См. мой доклад «Über die Theorie der relativquadratischen Zahlkörper», сделанный в 1897 г. на заседании Брауншвейгского союза математиков (Mathematiker-Vereinigung zu Braunschweig).

Доказательство. Пусть $\alpha \equiv \beta^2$ по модулю $\mathfrak{p}$, где β — некоторое целое число из поля k. Из теоремы Ферма[3)] немедленно следует, что

$$\alpha^{(n(\mathfrak{p})-1)/2} \equiv \beta^{n(\mathfrak{p})-1} \equiv +1, \qquad (\mathfrak{p}).$$

Предположим, с другой стороны, что α — квадратичный невычет по модулю $\mathfrak{p}$. Обозначим в таком случае через ρ примитивное число по модулю $\mathfrak{p}$ в поле k, и пусть $\alpha \equiv \rho^a$ по модулю $\mathfrak{p}$. Очевидно, что здесь показатель a должен быть нечетным числом. Но по теореме Ферма

$$\rho^{n(\mathfrak{p})-1} \equiv +1, \qquad (\mathfrak{p})$$

и, следовательно,

$$\rho^{(n(\mathfrak{p})-1)/2} \equiv \pm 1, \qquad (\mathfrak{p}). \tag{1}$$

Так как в последовательности степеней ρ, ρ^2, ρ^3, ... степень $\rho^{n(\mathfrak{p})-1}$ — первая, сравнимая с $+1$ по модулю $\mathfrak{p}$, то в правой части сравнения (1) должен быть отрицательный знак и, значит,

$$\alpha^{(n(\mathfrak{p})-1)/2} \equiv \rho^{a(n(\mathfrak{p})-1)/2} \equiv -1, \qquad (\mathfrak{p}).$$

Из только что доказанной теоремы 1 легко вытекает следующее утверждение.

Теорема 2. *Если α, β — целые числа поля k, взаимно простые с простым идеалом $\mathfrak{p}$, то справедливо равенство*

$$\left(\frac{\alpha\beta}{\mathfrak{p}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\beta}{\mathfrak{p}}\right).$$

Полная система из $n(\mathfrak{p}) - 1$ чисел, взаимно простых с $\mathfrak{p}$ и попарно не сравнимых по модулю $\mathfrak{p}$, разбивается на две подсистемы, первая из которых состоит из $\frac{1}{2}(n(\mathfrak{p}) - 1)$ квадратичных вычетов по модулю $\mathfrak{p}$, а вторая — из $\frac{1}{2}(n(\mathfrak{p}) - 1)$ квадратичных невычетов по модулю $\mathfrak{p}$.

§ 2. Понятия относительной нормы, относительной дифференты и относительного дискриминанта

Определение 2. Любое число A поля $K(\sqrt{\mu})$ может быть представлено в виде

$$\mathrm{A} = \alpha + \beta\sqrt{\mu},$$

где α, β — целые или дробные числа поля k. При этом говорят, что число

$$S\mathrm{A} = \alpha - \beta\sqrt{\mu}$$

получено из A с помощью подстановки

$$S = (\sqrt{\mu} : -\sqrt{\mu})$$

[3)] См. мое сообщение «Теория полей алгебраических чисел» [см.: *Hilbert D.* Die Theorie der algebraischen Zahlkörper. — Jber. der Deutschen Mathematiker-Vereinigung, 1897, Bd. 4, S. 175–546. — *Ред.*], представленное Немецкому Союзу Математиков (1897 г.), теоремы 22 и 24. В данной работе я буду ссылаться на это мое сообщение кратко как на «Поля алгебраических чисел».

или что $S\mathsf{A}$ — *относительно сопряженное* с A *число* в $K(\sqrt{\mu})$. Число

$$\mathsf{A} - S\mathsf{A}$$

называется *относительной дифферентой числа* A в поле $K(\sqrt{\mu})$. Наибольший общий делитель относительных дифферент всех *целых* чисел $\Omega_1, \Omega_2, \ldots$ поля $K(\sqrt{\mu})$, т. е. идеал

$$\mathfrak{D} = (\Omega_1 - S\Omega_1,\ \Omega_2 - S\Omega_2, \ldots)$$

называется *относительной дифферентой поля* $K(\sqrt{\mu})$ над полем k.

Произведение данного числа A поля K на относительно сопряженное с ним число $S\mathsf{A}$ называется *относительной нормой числа* A и будет обозначаться через $N(\mathsf{A})$; итак,

$$N(\mathsf{A}) = \mathsf{A} \cdot S\mathsf{A}.$$

Относительная норма $N(\mathsf{A})$ числа A в K всегда является числом из k.

Пусть $\mathfrak{J} = (\mathsf{I}_1, \mathsf{I}_2, \ldots)$ — произвольный идеал поля K, и пусть ко всем целым числам $\mathsf{I}_1, \mathsf{I}_2, \ldots$ этого идеала применена подстановка S. Полученный таким образом идеал называется *идеалом, относительно сопряженным* с $\mathfrak{J}$, и обозначается через $S\mathfrak{J}$; итак,

$$S\mathfrak{J} = (S\mathsf{I}_1,\ S\mathsf{I}_2, \ldots).$$

Произведение данного идеала $\mathfrak{J}$ поля K на относительно сопряженный с ним идеал $S\mathfrak{J}$ называется *относительной нормой идеала* $\mathfrak{J}$ и будет обозначаться через $N(\mathfrak{J})$; итак,

$$N(\mathfrak{J}) = \mathfrak{J} \cdot S\mathfrak{J}.$$

Относительная норма идеала $\mathfrak{J}$ в K всегда является идеалом в k.

Квадрат относительной дифференты данного числа A поля K, т. е. число $(\mathsf{A} - S\mathsf{A})^2$, называется *относительным дискриминантом числа* A. Относительный дискриминант числа A в K всегда является числом из k.

Квадрат относительной дифференты поля K

$$\mathfrak{d} = \mathfrak{D}^2 = (\Omega_1 - S\Omega_1,\ \Omega_2 - S\Omega_2, \ldots)^2$$

называется *относительным дискриминантом поля* K. Так как относительная дифферента $\mathfrak{D}$ поля K — это такой идеал поля K, который равен относительно сопряженному с ним идеалу, то относительный дискриминант $\mathfrak{d}$ равен относительной норме относительной дифференты $\mathfrak{D}$ поля K. Следовательно, относительный дискриминант $\mathfrak{d}$ всегда является идеалом в k.

§ 3. Амбивалентные идеалы

Определение 3. Идеал $\mathfrak{A}$ поля K называется *амбивалентным идеалом*, если он остается неизменным при операции S, т. е. если

$$S\mathfrak{A} = \mathfrak{A},$$

и если, кроме того, $\mathfrak{A}$ не содержит в качестве множителя никакого отличного от 1 идеала поля k. В частности, простой идеал поля K называется

амбивалентным простым идеалом, если он не меняется при применении подстановки S и в то же время не лежит в поле k. Каждый амбивалентный идеал является произведением простых амбивалентных идеалов. Квадрат амбивалентного простого идеала равен его относительной норме и сам представляет собой простой идеал в поле k.

Теорема 3[4]. *Относительная дифферента $\mathfrak{D}$ относительного квадратичного поля K содержит в качестве множителей все те и только те простые идеалы, которые являются амбивалентными.*

§ 4. Простые множители относительного дискриминанта

Наша следующая задача состоит в том, чтобы определить все имеющиеся простые множители относительного дискриминанта $\mathfrak{d}$ поля $K(\sqrt{\mu})$. Эта задача решается следующей теоремой.

Теорема 4. *Пусть $\mathfrak{p}$ — взаимно простой с 2 простой идеал поля k, и пусть a — точный показатель степени, с которой $\mathfrak{p}$ входит в число μ. Тогда если показатель a нечетен, то относительный дискриминант $\mathfrak{d}$ поля $K(\sqrt{\mu})$ всегда содержит множитель $\mathfrak{p}$. Напротив, если показатель a четен, то относительный дискриминант $\mathfrak{d}$ взаимно прост с $\mathfrak{p}$.*

Пусть $\mathfrak{l}$ — простой идеал поля k, который входит множителем в 2 и притом в степени ровно l; далее, пусть $\mathfrak{l}$ входит множителем в μ в степени ровно a. Тогда относительный дискриминант поля $K(\sqrt{\mu})$ взаимно прост с $\mathfrak{l}$ в том и только том случае, если в поле k имеется целое число α, удовлетворяющее сравнению

$$\mu \equiv \alpha^2, \qquad (\mathfrak{l}^{2l+a}). \tag{1}$$

Доказательство. Займемся сначала первой частью теоремы. Пусть π — целое число поля k, которое делится на $\mathfrak{p}$, но не делится на $\mathfrak{p}^2$, и пусть, далее, ν — целое число поля k, которое делится на $\pi/\mathfrak{p}$, но взаимно просто с $\mathfrak{p}$.

Если показатель a нечетен, то $\mu^* = \dfrac{\mu \cdot \nu^{a-1}}{\pi^{a-1}}$ представляет собой целое число в k, которое делится на $\mathfrak{p}$, но не на $\mathfrak{p}^2$, и для которого $\sqrt{\mu^*}$ лежит в поле $K(\sqrt{\mu})$. Если мы обозначим через $\mathfrak{P}$ общий идеальный делитель $\mathfrak{p}$ и $\sqrt{\mu^*}$, то

$$\mathfrak{P} = S\mathfrak{P}, \qquad \mathfrak{p} = \mathfrak{P}^2.$$

Итак, идеал $\mathfrak{P}$ является амбивалентным простым идеалом и, следовательно, по теореме 3 содержится в качестве множителя в относительной дифференте $\mathfrak{D}$ поля $K(\sqrt{\mu})$; а значит, относительный дискриминант $\mathfrak{d}$ делится на $\mathfrak{p}$.

---

[4] См. «Поля алгебраических чисел», теорему 93, где эта теорема сформулирована и доказана в общем случае для относительно циклических полей простой степени.

Наоборот, пусть показатель a четный. Тогда $\mu^* = \frac{\mu\nu^a}{\pi^a}$ представляет собой взаимно простое с $\mathfrak{p}$ целое число в k, такое что $\sqrt{\mu^*}$ лежит в $K(\sqrt{\mu})$. Так как относительный дискриминант числа $\sqrt{\mu^*}$ равен $2^2\mu^*$, то он взаимно прост с $\mathfrak{p}$. Это же верно и для относительного дискриминанта $\mathfrak{d}$ поля $K(\sqrt{\mu})$.

Теперь мы рассмотрим, как обстоит дело с простым множителем $\mathfrak{l}$. Если выполняется сравнение (1), то $\mathfrak{l}$ должен входить множителем в число α^2 в степени точно a и, следовательно, показатель a является четным числом. Пусть теперь λ — некоторое целое число поля k, делящееся на $\mathfrak{l}$, но не на $\mathfrak{l}^2$, и пусть, далее, ν — целое число в k, делящееся на $\lambda/\mathfrak{l}$, но взаимно простое с $\mathfrak{l}$. Тогда выражение

$$\Omega = \left(\frac{\nu}{\lambda}\right)^{l+a/2}(\alpha + \sqrt{\mu})$$

представляет собой некоторое целое число поля $K(\sqrt{\mu})$, так как, очевидно, выражения

$$\Omega + S\Omega = \left(\frac{\nu}{\lambda}\right)^{l+a/2} \cdot 2\alpha,$$

$$\Omega \cdot S\Omega = \left(\frac{\nu}{\lambda}\right)^{2l+a}(\alpha^2 - \mu)$$

оба являются целыми числами в k. С другой стороны, относительный дискриминант числа Ω равен

$$(\Omega - S\Omega)^2 = \left(\frac{\nu}{\lambda}\right)^{2l+a} \cdot 2^2\mu$$

и, следовательно, взаимно прост с $\mathfrak{l}$; это же верно и для относительного дискриминанта поля $K(\sqrt{\mu})$.

Наоборот, предположим, что относительный дискриминант $\mathfrak{d}$ поля $K(\sqrt{\mu})$ взаимно прост с $\mathfrak{l}$. Из того что

$$\mathfrak{d} = (\Omega_1 - S\Omega_1, \Omega_2 - S\Omega_2, \ldots)^2 = ([\Omega_1 - S\Omega_1]^2, [\Omega_2 - S\Omega_2]^2, \ldots),$$

следует, что в поле $K(\sqrt{\mu})$ должно существовать целое число Ω, относительный дискриминант которого $[\Omega - S\Omega]^2$ взаимно прост с $\mathfrak{l}$. Положим

$$\Omega = \frac{\alpha^* + \beta^*\sqrt{\mu}}{\gamma^*},$$

где α^*, β^*, γ^* обозначает целые числа из k, которые делятся в точности на a^*-ю, b^*-ю и c^*-ю степень $\mathfrak{l}$ соответственно. Так как

$$[\Omega - S\Omega]^2 = \frac{2^2\beta^{*2}\mu}{\gamma^{*2}}$$

должно быть целым числом, взаимно простым с $\mathfrak{l}$, мы заключаем, что

$$2l + 2b^* + a = 2c^*, \tag{2}$$

а так как, с другой стороны, относительная норма $N(\Omega) = \frac{\alpha^{*2} - \beta^{*2}\mu}{\gamma^{*2}}$ является целым числом, то либо числа α^{*2} и $\beta^{*2}\mu$ оба в точности делятся на одну и ту же степень $\mathfrak{l}$, либо каждое из этих двух чисел делится по крайней мере на $\mathfrak{l}^{2c^*}$. Последний случай не может иметь места, так как в силу только что

доказанного равенства (2) в любом случае $2b^* + a < 2c^*$ и, следовательно, $\beta^{*2}\mu$ никак не может делиться на $\mathfrak{l}^{2c^*}$. Значит, должно быть $2a^* = 2b^* + a$, а тогда согласно (2) должно быть также $2l + 2a^* = 2c^*$, или $l + a^* = c^*$. Из $2a^* = 2b^* + a$ следует, далее, что $a^* \geqslant b^*$, а из $l + a^* = c^*$ следует $c^* > a^*$, а значит и $c^* > b^*$. Так как $\dfrac{\alpha^{*2} - \beta^{*2}\mu}{\gamma^{*2}}$ должно быть целым числом, мы имеем сравнение

$$\mu \equiv \left(\frac{\alpha^*}{\beta^*}\right)^2, \qquad (\mathfrak{l}^{2c^*-2b^*}).$$

Ввиду того что $a^* \geqslant b^*$, дробь α^*/β^* может быть записана в виде дроби, знаменатель которой взаимно прост с $\mathfrak{l}$ и, следовательно, α^*/β^* должно быть сравнимо с некоторым целым числом α поля k по модулю $\mathfrak{l}^{2c^*-2b^*}$, так что имеет место сравнение

$$\mu \equiv \alpha^2, \qquad (\mathfrak{l}^{2c^*-2b^*}).$$

Этим, если принять во внимание вытекающее из (2) равенство $2c^* - 2b^* = 2l + a$, полностью доказана справедливость теоремы 4.

Из теоремы 4 мы легко получаем следующий частный результат.

Теорема 5. *Если μ — произвольное взаимно простое с 2 целое число поля k, которое не является квадратом никакого числа в k, то относительный дискриминант поля $K(\sqrt{\mu})$ тогда и только тогда взаимно прост с 2, когда μ сравнимо с квадратом некоторого целого числа в k по модулю 2^2.*

§ 5. Разложение простых идеалов основного поля k в относительном квадратичном поле K

Вопрос о том, как получить простые идеалы относительного квадратичного поля K из разложения простых идеалов поля k, решается следующими теоремами.

Теорема 6. *Простой идеал $\mathfrak{p}$ поля k тогда и только тогда равен квадрату некоторого простого идеала $\mathfrak{P}$ в поле K, когда $\mathfrak{p}$ входит множителем в относительный дискриминант поля K.*

Доказательство. Из равенства $\mathfrak{p} = \mathfrak{P}^2$ следует, что $\mathfrak{p} = (S\mathfrak{P})^2$, а значит, и $\mathfrak{P} = S\mathfrak{P}$, т. е. $\mathfrak{P}$ — амбивалентный идеал поля K и как таковой содержится, по теореме 3, в относительной дифференте поля K, а значит, $\mathfrak{p}$ входит множителем в относительный дискриминант.

Обратно, предположим, что $\mathfrak{p}$ входит в относительный дискриминант поля K, и обозначим через $\mathfrak{P}$ некоторый простой идеал поля K, входящий множителем в $\mathfrak{p}$. Очевидно, что $\mathfrak{P}$ входит множителем в относительную дифференту поля K и, следовательно, является, по теореме 3, амбивалентным идеалом, т. е., согласно определению 3, $\mathfrak{P} = S\mathfrak{P}$ и $\mathfrak{p} \neq \mathfrak{P}$. Ввиду этого условия мы имеем также $\mathfrak{p}^2 \neq \mathfrak{P} \cdot S\mathfrak{P}$, откуда следует, что $\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P} = \mathfrak{P}^2$. Этим теорема 6 доказана.

Теорема 7. *Если* $\mathfrak{p}$ *— простой идеал поля* k*, который не входит множителем ни в* 2*, ни в* μ*, то* $\mathfrak{p}$ *распадается или не распадается в поле* $K(\sqrt{\mu})$ *на два различных простых идеала в зависимости от того, является* μ *в поле* k *квадратичным вычетом или невычетом по модулю* $\mathfrak{p}$*.*

Доказательство. Пусть μ — квадратичный вычет в k по модулю $\mathfrak{p}$, и пусть α — такое целое число в k, что выполняется сравнение

$$\mu \equiv \alpha^2, \qquad (\mathfrak{p}).$$

Рассмотрим два взаимно относительно сопряженных идеала поля $K(\sqrt{\mu})$:

$$\mathfrak{P} = (\mathfrak{p}, \alpha - \sqrt{\mu}),$$
$$S\mathfrak{P} = (\mathfrak{p}, \alpha + \sqrt{\mu}).$$

Без труда находим, что

$$\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P}.$$

Поскольку

$$(\mathfrak{p}, \alpha - \sqrt{\mu}, \alpha + \sqrt{\mu}) = 1,$$

$\mathfrak{P}$ и $S\mathfrak{P}$ отличны друг от друга.

Наоборот, пусть простой идеал $\mathfrak{p}$ поля k разложим на два простых идеала $\mathfrak{P}$ и $S\mathfrak{P}$. Тогда если обозначить через N норму в поле $K(\sqrt{\mu})$, а через n — норму в поле k, то выполняются равенства

$$N(\mathfrak{p}) = N(\mathfrak{P}) \cdot N(S\mathfrak{P}) = (N(\mathfrak{P}))^2,$$
$$N(\mathfrak{p}) = (n(\mathfrak{p}))^2$$

и, следовательно,

$$N(\mathfrak{P}) = n(\mathfrak{p}).$$

Равенство норм $N(\mathfrak{P})$ и $n(\mathfrak{p})$ позволяет сделать заключение, что для каждого целого числа поля $K(\sqrt{\mu})$ может быть найдено сравнимое с ним по модулю $\mathfrak{P}$ целое число поля k, так как любые $n(\mathfrak{p})$ не сравнимых друг с другом по модулю $\mathfrak{p}$ чисел должны образовывать и полную систему вычетов по модулю $\mathfrak{P}$ в $K(\sqrt{\mu})$. В частности, $\sqrt{\mu} \equiv \alpha$ по модулю $\mathfrak{P}$ для некоторого α, лежащего в k. Отсюда следует, что $\mu \equiv \alpha^2$ по модулю $\mathfrak{P}$, а так как $\mu - \alpha^2$ — число поля k, то сравнение $\mu \equiv \alpha^2$ должно выполняться также по модулю $\mathfrak{p}$, т. е. μ — квадратичный вычет по модулю $\mathfrak{p}$. Этим теорема 7 полностью доказана.

Теорема 8. *Пусть* $\mathfrak{l}$ *— некоторый содержащийся множителем в* 2 *простой идеал поля* k*, а именно* $\mathfrak{l}$ *входит множителем в* 2 *точно в* l*-й степени. Далее, пусть* μ *— некоторое взаимно простое с* $\mathfrak{l}$ *целое число в* k*, сравнимое с квадратом некоторого целого числа в* k *по модулю* $\mathfrak{l}^{2l}$*, так что, согласно теореме* 4*, простой идеал* $\mathfrak{l}$ *не входит множителем в относительный дискриминант поля* $K(\sqrt{\mu})$*. Тогда* $\mathfrak{l}$ *распадается или не распадается в поле* $K(\sqrt{\mu})$ *на два различных простых идеала в зависимости от того, сравнимо* μ *с квадратом некоторого целого числа в* k *по модулю* $\mathfrak{l}^{2l+1}$ *или нет.*

Доказательство. Пусть $\mathfrak{l}$ распадается в $K(\sqrt{\mu})$, и пусть $\mathfrak{L}$ — простой множитель $\mathfrak{l}$. На основании равенства норм $N(\mathfrak{L})$ в $K(\sqrt{\mu})$ и $n(\mathfrak{l})$ в k мы заключаем, как и в доказательстве теоремы 7, что любое целое число в $K(\sqrt{\mu})$ должно быть сравнимо с некоторым целым числом в k по модулю $\mathfrak{L}$. По предположению в k существует такое целое число α, что $\mu \equiv \alpha^2$ по модулю $\mathfrak{l}^{2l}$. Пусть λ — какое-нибудь целое число поля k, делящееся на $\mathfrak{l}$, но не на $\mathfrak{l}^2$, и пусть, далее, ν — целое число в k, делящееся на $\lambda/\mathfrak{l}$, но взаимно простое с $\mathfrak{l}$. Тогда, как следует из доказательства теоремы 4, выражение $\dfrac{\nu^l(\alpha+\sqrt{\mu})}{\lambda^l}$ представляет собой некоторое целое число в $K(\sqrt{\mu})$. Итак, по только что доказанному, в k существует целое число β, для которого

$$\frac{\nu^l(\alpha+\sqrt{\mu})}{\lambda^l} \equiv \beta, \qquad (\mathfrak{L}).$$

Из этого сравнения следует, что

$$\sqrt{\mu} \equiv -\alpha + \frac{\beta\lambda^l}{\nu^l}, \qquad (\mathfrak{l}^l\mathfrak{L}).$$

С учетом того обстоятельства, что ν взаимно просто с $\mathfrak{l}$, мы можем в этом сравнении выражение, стоящее в правой части, заменить некоторым целым числом γ поля k и получить

$$\sqrt{\mu} \equiv \gamma \quad \text{или} \quad \sqrt{\mu} - \gamma \equiv 0, \qquad (\mathfrak{l}^l\mathfrak{L}). \tag{1}$$

Далее, так как $-\gamma \equiv +\gamma$ по модулю 2, а следовательно, также и по модулю $\mathfrak{l}^l$, то выполняется сравнение

$$\sqrt{\mu} + \gamma \equiv 0, \qquad (\mathfrak{l}^l). \tag{2}$$

Наконец, при помощи умножения мы получаем из сравнений (1) и (2) сравнение

$$\mu - \gamma^2 \equiv 0, \qquad (\mathfrak{l}^{2l}\mathfrak{L}).$$

Так как левая часть этого сравнения является целым числом в k, мы имеем также

$$\mu - \gamma^2 \equiv 0 \quad \text{или} \quad \mu \equiv \gamma^2, \qquad (\mathfrak{l}^{2l+1}),$$

чем доказано одно из утверждений теоремы 8.

Наоборот, предположим, что $\mu \equiv \alpha^2$ по модулю $\mathfrak{l}^{2l+1}$, где α — некоторое целое число в k. Тогда, как проверяется без труда, справедливо равенство

$$\mathfrak{l} = \left(\mathfrak{l}, \frac{\nu^l[\alpha+\sqrt{\mu}]}{\lambda^l}\right)\left(\mathfrak{l}, \frac{\nu^l[\alpha-\sqrt{\mu}]}{\lambda^l}\right),$$

причем здесь оба простые идеала в правой части действительно различны, ввиду того что

$$\left(\mathfrak{l}, \frac{\nu^l[\alpha+\sqrt{\mu}]}{\lambda^l}, \frac{\nu^l[\alpha-\sqrt{\mu}]}{\lambda^l}\right) = 1,$$

что полностью доказывает теорему 8.

§ 6. Символ $\left(\frac{\mu}{\mathfrak{a}}\right)$

Определение 4. Обобщим введенное в определении 1 понятие *символа* следующим образом.

Пусть $\mathfrak{w}$ — какой-либо простой идеал в k. Мы полагаем

$$\left(\frac{\mu}{\mathfrak{w}}\right) = +1, \quad \text{или} \quad = -1, \quad \text{или} \quad = 0,$$

в зависимости от того, распадается ли $\mathfrak{w}$ в поле $K(\sqrt{\mu})$ на два различных простых идеала, или не распадается, или равен квадрату некоторого простого идеала. Если μ — квадрат некоторого числа в k, то мы всегда полагаем

$$\left(\frac{\mu}{\mathfrak{w}}\right) = +1.$$

Теоремы 6, 7 и 8 позволяют вычислить значение символа $\left(\frac{\mu}{\mathfrak{w}}\right)$ во всех случаях. В случае, когда идеал $\mathfrak{w}$ взаимно прост с 2 и μ, теорема 7 гарантирует согласованность нашего определения с определением 1. Что касается случая, когда идеал $\mathfrak{w}$ равен некоторому делящему 2 простому идеалу $\mathfrak{l}$ поля k, то прежде всего определим наибольшую степень $\mathfrak{l}$, делящую μ. Если показатель a этой степени нечетен, то мы имеем $\left(\frac{\mu}{\mathfrak{l}}\right) = 0$. Если же a четен, то пусть μ^* — целое число поля k, взаимно простое с $\mathfrak{l}$ и такое, что

$$\mu \equiv \lambda^a \mu^*, \qquad (\mathfrak{l}^{2l+a+1}),$$

где λ означает некоторое число, делящееся на $\mathfrak{l}$, но не на $\mathfrak{l}^2$. Если μ^* не сравнимо по модулю $\mathfrak{l}^{2l}$ ни с каким квадратом целого числа в k, то, принимая во внимание теоремы 4 и 6, мы также имеем $\left(\frac{\mu}{\mathfrak{l}}\right) = 0$; в противном случае μ^* либо сравнимо с квадратом некоторого целого числа в k также и по модулю $\mathfrak{l}^{2l+1}$, либо нет, и по теореме 8 мы имеем соответственно $\left(\frac{\mu}{\mathfrak{l}}\right) = +1$ или $= -1$.

Определение 5. Пусть $\mathfrak{a}$ — произвольный идеал поля k, и пусть $\mathfrak{a} = \mathfrak{p}\mathfrak{q} \ldots \mathfrak{w}$, где $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{w}$ — простые идеалы в k. Тогда *символ* $\left(\frac{\mu}{\mathfrak{a}}\right)$, где μ — произвольное целое число в k, может быть определен следующим равенством:

$$\left(\frac{\mu}{\mathfrak{a}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right)\left(\frac{\mu}{\mathfrak{q}}\right) \ldots \left(\frac{\mu}{\mathfrak{w}}\right).$$

Пусть $\mathfrak{a}$, $\mathfrak{b}$ — произвольные идеалы в k. Тогда, очевидно, выполняется равенство

$$\left(\frac{\mu}{\mathfrak{a}\mathfrak{b}}\right) = \left(\frac{\mu}{\mathfrak{a}}\right)\left(\frac{\mu}{\mathfrak{b}}\right).$$

Этими правилами символ $\left(\frac{\mu}{\mathfrak{a}}\right)$ определен для любого целого числа μ в k и любого идеала $\mathfrak{a}$ в k. Символ $\left(\frac{\mu}{\mathfrak{a}}\right)$ может принимать лишь значения $+1$, -1, 0.

§ 7. Норменный вычет и норменный невычет в поле K и символ $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$

Определение 6. Пусть $\mathfrak{w}$ — некоторый простой идеал в k, и пусть ν, μ — произвольные целые числа в k, с тем единственным ограничением, что μ не равно квадрату никакого числа в k. Тогда если ν сравнимо по модулю $\mathfrak{w}$ с относительной нормой некоторого целого числа поля $K(\sqrt{\mu})$ и если, сверх того, для любой степени $\mathfrak{w}$ всегда можно найти такое целое число A в поле $K(\sqrt{\mu})$, что $\nu \equiv N(\mathrm{A})$ по модулю этой степени $\mathfrak{w}$, то я называю ν *норменным вычетом* поля $K(\sqrt{\mu})$ относительно $\mathfrak{w}$. Во всех остальных случаях я называю ν *норменным невычетом* поля $K(\sqrt{\mu})$ относительно $\mathfrak{w}$. Я определяю *символ* $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$, полагая

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = +1 \quad \text{или} \quad = -1$$

в зависимости от того, является ν норменным вычетом или невычетом относительно $\mathfrak{w}$. Если μ равно квадрату некоторого целого числа в k, то я полагаю

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = +1.$$

Этими правилами новый символ $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ определен для любых целых чисел ν, μ поля k и любого простого идеала $\mathfrak{w}$ поля k. Символ $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ может принимать лишь два значения: $+1$ или -1.

§ 8. Свойства символа $\left(\frac{\nu,\mu}{\mathfrak{p}}\right)$

В следующих теоремах мы выявим некоторые свойства символа $\left(\frac{\nu,\mu}{\mathfrak{p}}\right)$ в случае, когда $\mathfrak{p}$ — простой идеал, не делящий 2.

Теорема 9. *Если ν, μ — произвольные целые числа в k и $\mathfrak{p}$ — простой идеал поля k, который взаимно прост с 2 и ν, но входит множителем в μ ровно в первой степени, то выполняется равенство*

$$\left(\frac{\nu,\mu}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{p}}\right).$$

Доказательство. Если $\left(\frac{\nu}{\mathfrak{p}}\right) = +1$, то по определению 1 в k существует целое число α, для которого $\nu \equiv \alpha^2$ по модулю $\mathfrak{p}$. Покажем, что сравнение $\nu \equiv \xi^2$ разрешимо также по модулю любой произвольной степени $\mathfrak{p}$ при подходящем выборе ξ. Пусть

$$\frac{\nu}{\alpha^2} \equiv 1 + 2\mathfrak{w}, \qquad (\mathfrak{p}^2),$$

где $\mathfrak{w}$ — некоторое целое делящееся на $\mathfrak{p}$ число в k. Тогда целое число $\alpha' = \alpha(1+\mathfrak{w})$ удовлетворяет условию

$$\nu \equiv \alpha'^2, \qquad (\mathfrak{p}^2).$$

Продолжая в том же духе, мы получаем, что для любого показателя e существует такое целое число $\alpha^{(e-1)}$, что

$$\nu \equiv (\alpha^{(e-1)})^2, \qquad (\mathfrak{p}^e).$$

Положим $\mathsf{A} = \alpha^{(e-1)}$. Тогда

$$\nu \equiv N(\mathsf{A}), \qquad (\mathfrak{p}^e),$$

т. е. при сделанном выше предположении символ $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ имеет значение $+1$.

Наоборот, предположим, что $\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = +1$. Тогда по определению 6 в $K(\sqrt{\mu})$ существует целое число A, для которого $\nu \equiv N(\mathsf{A})$ по модулю $\mathfrak{p}$. Так как по теореме 4 простой идеал $\mathfrak{p}$ входит множителем в относительный дискриминант поля $K(\sqrt{\mu})$, то по теореме 6 простой идеал $\mathfrak{p}$ равен квадрату некоторого простого идеала $\mathfrak{P}$ поля $K(\sqrt{\mu})$. Из равенства $\mathfrak{p} = \mathfrak{P}^2$ следует равенство норм $n(\mathfrak{p})$ в k и $N(\mathfrak{P})$ в $K(\sqrt{\mu})$, и, как и в доказательстве теоремы 7, мы заключаем, что любое целое число поля $K(\sqrt{\mu})$ должно быть сравнимым с некоторым целым числом поля k по модулю $\mathfrak{P}$. Пусть $\mathsf{A} \equiv \alpha$ по модулю $\mathfrak{P}$, где α — некоторое целое число в k. Тогда

$$\nu \equiv N(\mathsf{A}) \equiv \alpha^2, \qquad (\mathfrak{P})$$

и, следовательно, также $\nu \equiv \alpha^2$ по модулю $\mathfrak{p}$, т. е. при сделанном предположении мы получаем $\left(\frac{\nu}{\mathfrak{p}}\right) = +1$, что вместе с установленным ранее полностью доказывает теорему 9.

Теорема 10. *Если ν, μ — два произвольных целых числа в k и $\mathfrak{p}$ — простой идеал поля k, который не делит ни ν, ни μ, ни 2, то всегда выполняется равенство*

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = +1.$$

Доказательство. По теореме 4 идеал $\mathfrak{p}$ не входит множителем в относительный дискриминант поля $K(\sqrt{\mu})$, поэтому остается рассмотреть только две возможности: идеал $\mathfrak{p}$ распадается на два различных простых идеала поля $K(\sqrt{\mu})$ или неразложим также и в $K(\sqrt{\mu})$.

Предположим сначала, что $\mathfrak{p}$ разложим, скажем $\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P}$, где $\mathfrak{P}$ — некоторый простой идеал поля $K(\sqrt{\mu})$. Тогда в $K(\sqrt{\mu})$ должна существовать система из двух целых чисел A_1, A_2, для которых выполняются два линейных по A_1, A_2 сравнения

$$\left.\begin{aligned} \mathsf{A}_1 + \mathsf{A}_2\sqrt{\mu} &\equiv \nu, \\ \mathsf{A}_1 - \mathsf{A}_2\sqrt{\mu} &\equiv 1, \end{aligned}\right\} \qquad (\mathfrak{P}). \tag{1}$$

Ввиду равенства норм $n(\mathfrak{p})$ и $N(\mathfrak{P})$ мы можем теперь, как и в доказательстве теорем 7 и 9, для любого целого числа в $K(\sqrt{\mu})$ найти сравнимое с ним по модулю $\mathfrak{P}$ целое число поля k. Пусть

$$A_1 \equiv \alpha_1, \qquad A_2 \equiv \alpha_2, \qquad (\mathfrak{P}), \tag{2}$$

где α_1, α_2 — целые числа поля k. Если мы положим для краткости

$$\mathsf{A} = \alpha_1 + \alpha_2\sqrt{\mu},$$

то, перемножая сравнения (1), получим в силу (2) сравнение

$$\nu \equiv N(\mathsf{A}), \qquad (\mathfrak{P}),$$

а так как обе части этого сравнения являются целыми числами в k, то оно выполняется также по модулю $\mathfrak{p}$. Чтобы доказать, что сравнение $\nu \equiv N(\Xi)$ удовлетворяется также по модулю каждой степени $\mathfrak{p}^e$ при надлежащем выборе целого числа Ξ в $K(\sqrt{\mu})$, мы убеждаемся, как и в доказательстве теоремы 9, в существовании числа ξ, удовлетворяющего сравнению

$$\frac{\nu}{N(\mathsf{A})} \equiv \xi^2, \qquad (\mathfrak{p}^e).$$

Очевидно, что тогда $\nu \equiv N(\xi\mathsf{A})$ по модулю $\mathfrak{p}^e$.

С другой стороны, пусть $\mathfrak{p}$ не разлагается и в поле $K(\sqrt{\mu})$ и тем самым, в силу теоремы 7, число μ является квадратичным невычетом по модулю $\mathfrak{p}$. По теореме 2 в k существует ровно $f = \frac{1}{2}(n(\mathfrak{p}) - 1)$ квадратичных вычетов по модулю $\mathfrak{p}$. Пусть они представлены квадратами чисел $\alpha_1^2, \alpha_2^2, \ldots, \alpha_f^2$. Мы будем различать теперь два случая в зависимости от того, является число -1 квадратичным вычетом или невычетом по модулю $\mathfrak{p}$. В первом случае в силу нашего предположения о μ все $n(\mathfrak{p}) - 1$ чисел

$$\alpha_1^2,\ \alpha_2^2,\ \ldots,\ \alpha_f^2,\ -\alpha_1^2\mu,\ -\alpha_2^2\mu,\ \ldots,\ -\alpha_f^2\mu \tag{3}$$

попарно не сравнимы по модулю $\mathfrak{p}$. Следовательно, любое целое число в k, взаимно простое с $\mathfrak{p}$, сравнимо с одним из чисел (3) по модулю $\mathfrak{p}$. Числа (3) являются относительными нормами чисел

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_f,\ \alpha_1\sqrt{\mu},\ \alpha_2\sqrt{\mu},\ \ldots,\ \alpha_f\sqrt{\mu}$$

соответственно, и, следовательно, любое взаимно простое с $\mathfrak{p}$ число в k сравнимо по модулю $\mathfrak{p}$ с относительной нормой некоторого подходящего целого числа в $K(\sqrt{\mu})$.

Если же -1 является квадратичным невычетом по модулю $\mathfrak{p}$, то $-\mu$ будет квадратичным вычетом по модулю $\mathfrak{p}$; пусть $-\mu \equiv \beta^2$ по модулю $\mathfrak{p}$, где β — некоторое целое число в k. В последовательности положительных целых рациональных чисел

$$1,\ 2,\ 3,\ \ldots,\ n(\mathfrak{p}) - 1$$

последнее число является невычетом по модулю $\mathfrak{p}$. Пусть r — первое число этой последовательности, за которым следует невычет простого идеала $\mathfrak{p}$, и пусть $r \equiv \alpha^2$ по модулю $\mathfrak{p}$, где α — некоторое целое число в k. Тогда ввиду того, что

$$\alpha^2\beta^2 - \mu \equiv r\beta^2 + \beta^2 \equiv (r+1)\beta^2, \qquad (\mathfrak{p}),$$

целое число $\alpha^2\beta^2 - \mu$ непременно будет квадратичным невычетом по модулю $\mathfrak{p}$, и, следовательно, все $n(\mathfrak{p}) - 1$ чисел

$$\alpha_1^2,\ \alpha_2^2,\ \ldots,\ \alpha_f^2,\ \alpha_1^2(\alpha^2\beta^2 - \mu),\ \alpha_2^2(\alpha^2\beta^2 - \mu),\ \ldots,\ \alpha_f^2(\alpha^2\beta^2 - \mu) \tag{4}$$

попарно не сравнимы по модулю $\mathfrak{p}$. Однако числа (4) являются относительными нормами чисел

$$\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_f,\ \alpha_1(\alpha\beta + \sqrt{\mu}),\ \alpha_2(\alpha\beta + \sqrt{\mu}),\ \ldots,\ \alpha_f(\alpha\beta + \sqrt{\mu})$$

соответственно, и, следовательно, любое взаимно простое с $\mathfrak{p}$ целое число в k сравнимо с относительной нормой некоторого целого числа в $K(\sqrt{\mu})$. Далее, отсюда следует, как и в первой части этого доказательства, что для любого не делящегося на $\mathfrak{p}$ числа ν поля k и для любой сколь угодно высокой степени $\mathfrak{p}^e$ простого идеала $\mathfrak{p}$ всегда можно найти целое число в $K(\sqrt{\mu})$, относительная норма которого сравнима с числом ν по модулю $\mathfrak{p}^e$. Этим теорема 10 доказана во всех случаях.

Теорема 11. *Если ν, μ — два произвольных целых числа в k и $\mathfrak{p}$ — простой идеал поля k, взаимно простой с 2 и μ и входящий множителем в ν ровно в первой степени, то выполняется равенство*

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right).$$

Доказательство. Пусть $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$. Тогда по теореме 7 простой идеал $\mathfrak{p}$ поля k разлагается в поле $K(\sqrt{\mu})$ на два различных простых идеала $\mathfrak{P}$ и $S\mathfrak{P}$. Найдем целое число A в $K(\sqrt{\mu})$, которое делится на $\mathfrak{P}$, но не делится ни на $\mathfrak{P}^2$, ни на $S\mathfrak{P}$. Тогда относительная норма $\alpha = N(\mathrm{A})$ числа A делится ровно на первую степень $\mathfrak{p}$. Пусть ϱ — целое число в k, делящееся на $\alpha/\mathfrak{p}$, но взаимно простое с $\mathfrak{p}$. Тогда $\nu\varrho^2/\alpha$ является взаимно простым с $\mathfrak{p}$ целым числом и, следовательно, по теореме 10, норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$. Рассмотрим произвольную степень $\mathfrak{p}^e$ идеала $\mathfrak{p}$, и пусть

$$\frac{\nu\varrho^2}{\alpha} \equiv N(\mathrm{P}), \qquad (\mathfrak{p}^e),$$

где P — некоторое целое число в $K(\sqrt{\mu})$. Определим теперь ϱ^* как такое целое число в k, что $\varrho\varrho^* \equiv 1$ по модулю $\mathfrak{p}^e$. Тогда, очевидно,

$$\nu \equiv N(\varrho^* \mathrm{PA}), \qquad (\mathfrak{p}^e),$$

т. е. ν является норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$.

Наоборот, если ν — норменный вычет поля $K(\sqrt{\mu})$ и, скажем, $\nu \equiv N(\Omega)$ по модулю $\mathfrak{p}^2$, где Ω — некоторое целое число в $K(\sqrt{\mu})$, то, в силу сделанного относительно ν предположения, $N(\Omega)$ делится только на первую степень $\mathfrak{p}$. Отсюда мы получаем, очевидно,

$$\mathfrak{p} = (\mathfrak{p}, \Omega) \cdot (\mathfrak{p}, S\Omega),$$

т. е. $\mathfrak{p}$ распадается в $K(\sqrt{\mu})$ в произведение двух идеалов, а тогда, по теореме 7, $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$. Этим теорема 11 полностью доказана.

Теорема 12. *Пусть $\mathfrak{p}$ — взаимно простой с 2 простой идеал поля k, и пусть, далее, ν, μ, ν^*, μ^* — четыре целых числа в k, обладающие тем свойством, что μ/μ^* является квадратом некоторого целого или дробного числа в k, а ν/ν^* — относительной нормой некоторого целого или дробного числа поля $K(\sqrt{\mu})$. Тогда выполняется равенство*

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right).$$

Доказательство. Прежде всего заметим, что в силу определения 6 для символа $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ всегда выполнено равенство

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu, \mu^*}{\mathfrak{p}}\right), \tag{5}$$

так как очевидно, что относительное квадратичное поле, определенное с помощью $\sqrt{\mu^*}$, совпадает с полем $K(\sqrt{\mu})$.

Далее, мы утверждаем, что если число γ есть относительная норма $N(\Gamma)$ некоторого целого числа Γ поля $K(\sqrt{\mu})$, то

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\gamma\nu, \mu}{\mathfrak{p}}\right). \tag{6}$$

В самом деле, ясно, что если ν — норменный вычет поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$, то и $\gamma\nu$ будет норменным вычетом этого поля относительно $\mathfrak{p}$. Наоборот, предположим, что $\gamma\nu$ — норменный вычет поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$. Мы рассуждаем следующим образом. Пусть ν делится ровно на b-ю степень $\mathfrak{p}$, а γ — ровно на c-ю степень $\mathfrak{p}$. Далее, пусть Ω — такое целое число в $K(\sqrt{\mu})$, что выполняется сравнение

$$\nu\gamma \equiv N(\Omega), \qquad (\mathfrak{p}^{c+e}), \tag{7}$$

где e — какой-нибудь показатель, больший b. Мы будем различать три случая в зависимости от того, остается ли $\mathfrak{p}$ простым идеалом и в поле $K(\sqrt{\mu})$, либо же распадается на два одинаковых или на два различных простых идеала поля $K(\sqrt{\mu})$.

В первом случае ввиду условия $\gamma = N(\Gamma)$ показатель c должен быть четным и $\mathfrak{p}$ входит множителем в Γ ровно в $(c/2)$-й степени. Тогда, в силу (7), число Ω должно делиться ровно на $((c+b)/2)$-ю степень $\mathfrak{p}$. Пусть теперь α — некоторое делящееся на $\frac{\gamma}{\mathfrak{p}^c}$, но взаимно простое с $\mathfrak{p}$ целое число в k. Тогда, конечно, $\mathsf{A} = \frac{\alpha\Omega}{\Gamma}$ — целое число в $K(\sqrt{\mu})$, и мы получаем $\alpha^2\nu \equiv N(\mathsf{A})$ по модулю $\mathfrak{p}^e$. Определим теперь такое целое число α^* в k, что выполняется $\alpha\alpha^* \equiv 1$ по модулю $\mathfrak{p}^e$. Тогда $\nu \equiv N(\alpha^*\mathsf{A})$ по модулю $\mathfrak{p}^e$, т. е. ν является норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$.

Во втором случае положим $\mathfrak{p} = \mathfrak{P}^2$, где $\mathfrak{P}$ — простой идеал поля $K(\sqrt{\mu})$. Ввиду условия $\gamma = N(\Gamma)$ в Γ входит ровно c-я степень $\mathfrak{P}$, а в силу сравнения (7) в Ω входит ровно $(c+b)$-я степень $\mathfrak{P}$. Определим теперь число α поля k, как и в первом случае, и после надлежащих рассуждений снова придем к выводу, что ν должно быть норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$.

Наконец, в третьем случае положим $\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P}$, где $\mathfrak{P}$ — простой идеал поля $K(\sqrt{\mu})$, который отличен от своего относительно сопряженного простого идеала $S\mathfrak{P}$. Пусть теперь в Γ простой идеал $\mathfrak{P}$ входит множителем ровно в C-й, а простой идеал $S\mathfrak{P}$ — ровно в C'-й степени. Далее, пусть в Ω простой идеал $\mathfrak{P}$ входит ровно в U-й степени, а $S\mathfrak{P}$ — ровно в U'-й степени. Тогда $c = C + C'$, $c + b = U + U'$ и, следовательно,

$$U + U' \geqslant C + C'. \tag{8}$$

Возьмем целое число A в $K(\sqrt{\mu})$, которое делится ровно на C-ю степень $\mathfrak{P}$ и U-ю степень $S\mathfrak{P}$, и, наконец, определим целое число α в k, которое делится на $\dfrac{\Gamma \cdot S\mathsf{A}}{\mathfrak{P}^{U+C} S\mathfrak{P}^{C+C'}}$, но взаимно просто с $\mathfrak{p}$. Из неравенства (8) следует, что $\mathsf{B} = \dfrac{\alpha\Omega\mathsf{A}}{\Gamma \cdot S\mathsf{A}}$ — целое число в $K(\sqrt{\mu})$, и мы получаем $\alpha^2\nu \equiv N(\mathsf{B})$ по модулю $\mathfrak{p}^e$. Теперь определим еще такое целое число α^* в k, что $\alpha\alpha^* \equiv 1$ по модулю $\mathfrak{p}^e$. Тогда $\nu \equiv N(\alpha^*\mathsf{B})$ по модулю $\mathfrak{p}^e$, т. е. ν является нормменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$. Этим справедливость свойства, выражаемого формулой (6), доказана во всех случаях.

В силу сделанного относительно ν/ν^* предположения мы можем положить $\nu/\nu^* = \gamma^*/\gamma$ или $\nu\gamma = \nu^*\gamma^*$, где γ, γ^* — относительные нормы некоторых целых чисел из $K(\sqrt{\mu})$. С помощью только что доказанной формулы (6) получаем

$$\left(\frac{\nu, \mu^*}{\mathfrak{p}}\right) = \left(\frac{\gamma\nu, \mu^*}{\mathfrak{p}}\right) \quad \text{и} \quad \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right) = \left(\frac{\gamma^*\nu^*, \mu^*}{\mathfrak{p}}\right).$$

Следовательно, также

$$\left(\frac{\nu, \mu^*}{\mathfrak{p}}\right) = \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right).$$

Последняя формула вместе с формулой (5) доказывает справедливость теоремы 12.

§ 9. Общие основные формулы для символа $\left(\dfrac{\nu, \mu}{\mathfrak{p}}\right)$

Из полученных в § 8 свойств символа $\left(\dfrac{\nu, \mu}{\mathfrak{p}}\right)$ можно вывести систему основных формул для этого символа в предположении, что $\mathfrak{p}$ — простой идеал, не делящий 2.

Теорема 13. *Пусть $\mathfrak{p}$ — взаимно простой с 2 простой идеал поля k и ν, μ — два произвольных целых числа в k. Пусть простой идеал $\mathfrak{p}$ входит множителем в числа ν и μ ровно в b-й и a-й степенях соответственно. Рассмотрим число ν^a/μ^b и представим его в виде дроби ϱ/σ, числитель которой ϱ и знаменатель σ не делятся на $\mathfrak{p}$. Тогда выполняется равенство*

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{(-1)^{ab}\varrho\sigma}{\mathfrak{p}}\right).$$

Доказательство. Теоремы 9, 10 и 11 немедленно показывают, что теорема 13 верна для $a = 1$, $b = 0$, для $a = 0$, $b = 0$ и для $a = 0$, $b = 1$. В случае $a = 1$, $b = 1$ имеем $\nu/\mu = \varrho/\sigma$, и

$$\frac{\nu}{-\varrho\sigma} = -\frac{\mu}{\sigma^2}$$

является относительной нормой числа $\sqrt{\mu}/\sigma$, поэтому, по теореме 12,

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{-\varrho\sigma, \mu}{\mathfrak{p}}\right),$$

а так как, с другой стороны, по теореме 9

$$\left(\frac{-\varrho\sigma, \mu}{\mathfrak{p}}\right) = \left(\frac{-\varrho\sigma}{\mathfrak{p}}\right),$$

мы заключаем о справедливости теоремы 13 для этого случая.

Пусть теперь a, b — произвольные целые рациональные неотрицательные показатели. Положим a^* равным 0 или 1 в зависимости от того, четно или нечетно a, и аналогично определим b^*. Найдем в поле k целое число ν^*, в которое $\mathfrak{p}$ входит множителем ровно в степени b^*, и число μ^*, в которое $\mathfrak{p}$ входит множителем ровно в степени a^*, такие что ν/ν^* и μ/μ^* являются квадратами некоторых чисел в k. Пусть ν^{*a^*}/μ^{*b^*} равно некоторой дроби ϱ^*/σ^*, числитель которой ϱ^* и знаменатель σ^* являются целыми взаимно простыми с $\mathfrak{p}$ числами в k. Тогда, как легко проверить, в последовательности чисел

$$\varrho^*\sigma^*, \quad \frac{\varrho^*}{\sigma^*}, \quad \frac{\nu^{*a^*}}{\mu^{*b^*}}, \quad \frac{\nu^{*a}}{\mu^{*b}}, \quad \frac{\nu^a}{\mu^b}, \quad \frac{\varrho}{\sigma}, \quad \varrho\sigma$$

каждое число, поделенное на следующее, равно квадрату некоторого числа поля k. Отсюда мы заключаем, что и частное первого $(\varrho^*\sigma^*)$ и последнего $(\varrho\sigma)$ чисел в этой последовательности должно быть равно квадрату некоторого числа $\varkappa$ поля k. С другой стороны, так как оба этих числа взаимно просты с $\mathfrak{p}$, то $\varkappa$ допускает представление в виде дроби ψ/ψ^*, числитель ψ и знаменатель ψ^* которой являются целыми взаимно простыми с $\mathfrak{p}$ числами в k. Таким образом, мы получаем $\psi^{*2}\varrho^*\sigma^* = \psi^2\varrho\sigma$ и, следовательно, $\left(\frac{\varrho^*\sigma^*}{\mathfrak{p}}\right) = \left(\frac{\varrho\sigma}{\mathfrak{p}}\right)$; а так как $(-1)^{ab} = (-1)^{a^*b^*}$, то мы имеем также

$$\left(\frac{(-1)^{a^*b^*}\varrho^*\sigma^*}{\mathfrak{p}}\right) = \left(\frac{(-1)^{ab}\varrho\sigma}{\mathfrak{p}}\right). \tag{1}$$

Но по теореме 12

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right), \tag{2}$$

а так как, в силу первой части данного доказательства, наша теорема верна для чисел ν^*, μ^*, то выполняется равенство

$$\left(\frac{\nu^*, \mu^*}{\mathfrak{p}}\right) = \left(\frac{(-1)^{a^*b^*}\varrho^*\sigma^*}{\mathfrak{p}}\right). \tag{3}$$

Из формул (1), (2), (3) следует справедливость теоремы 13 в общем случае.

Из теоремы 13 вытекает ряд важных формул для символа $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$, которые собраны в следующей теореме.

Теорема 14. *Пусть ν, ν_1, ν_2, μ, μ_1, μ_2 — произвольные целые числа поля k. Для любого простого идеала $\mathfrak{p}$ поля k, взаимно простого*

с 2, имеют место формулы

$$\left(\frac{\nu,\mu}{\mathfrak{p}}\right)=\left(\frac{\mu,\nu}{\mathfrak{p}}\right),$$
$$\left(\frac{\nu_1\nu_2,\mu}{\mathfrak{p}}\right)=\left(\frac{\nu_1,\mu}{\mathfrak{p}}\right)\left(\frac{\nu_2,\mu}{\mathfrak{p}}\right),$$
$$\left(\frac{\nu,\mu_1\mu_2}{\mathfrak{p}}\right)=\left(\frac{\nu,\mu_1}{\mathfrak{p}}\right)\left(\frac{\nu,\mu_2}{\mathfrak{p}}\right).$$

Доказательство. Первая формула немедленно следует из теоремы 13.

Чтобы доказать вторую формулу, предположим, что простой идеал $\mathfrak{p}$ входит множителем в ν_1, ν_2 и μ ровно в b_1-й, b_2-й и a-й степенях соответственно, и положим

$$\frac{\nu_1^a}{\mu^{b_1}}=\frac{\varrho_1}{\sigma_1},\qquad \frac{\nu_2^a}{\mu^{b_2}}=\frac{\varrho_2}{\sigma_2},$$

так что ϱ_1, σ_1, ϱ_2, σ_2 являются целыми взаимно простыми с $\mathfrak{p}$ числами в k. По теореме 13

$$\left(\frac{\nu_1,\mu}{\mathfrak{p}}\right)=\left(\frac{(-1)^{ab_1}\varrho_1\sigma_1}{\mathfrak{p}}\right),$$
$$\left(\frac{\nu_2,\mu}{\mathfrak{p}}\right)=\left(\frac{(-1)^{ab_2}\varrho_2\sigma_2}{\mathfrak{p}}\right),$$
$$\left(\frac{\nu_1\nu_2,\mu}{\mathfrak{p}}\right)=\left(\frac{(-1)^{a(b_1+b_2)}\varrho_1\varrho_2\sigma_1\sigma_2}{\mathfrak{p}}\right),$$

и эти равенства доказывают справедливость второй формулы.

Третья формула — непосредственное следствие первой и второй.

В ходе дальнейшего исследования мы обнаружим, что формулы теоремы 14 выполняются также для любого входящего множителем в 2 простого идеала поля k.

§ 10. Число норменных вычетов относительно некоторого не входящего в 2 простого идеала

Теорема 15. *Если $\mathfrak{p}$ — взаимно простой с 2 простой идеал поля k, который не входит множителем в относительный дискриминант относительного квадратичного поля $K(\sqrt{\mu})$, то любое взаимно простое с $\mathfrak{p}$ число ν является норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{p}$.*

Напротив, если $\mathfrak{p}$ — взаимно простой с 2 простой идеал поля k, который входит множителем в относительный дискриминант поля $K(\sqrt{\mu})$, и e — произвольный положительный показатель, то из всех имеющихся в k попарно не сравнимых по модулю $\mathfrak{p}^e$ и взаимно простых с $\mathfrak{p}$ чисел ровно половина являются норменными вычетами поля $K(\sqrt{\mu})$.

Доказательство. Пусть $\mathfrak{p}$ входит множителем в μ ровно в a-й степени, и пусть $\mathfrak{p}$ взаимно прост с относительным дискриминантом поля $K(\sqrt{\mu})$. Тогда по теореме 4 a должно быть четным числом. Далее, так как по предположению ν взаимно просто с $\mathfrak{p}$, мы можем при использовании теоремы 13 для вычисления символа $\left(\frac{\nu, \mu}{\mathfrak{p}}\right)$ положить просто $\varrho = \nu^a$ и $\sigma = 1$. Тогда мы получим

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^a}{\mathfrak{p}}\right) = +1,$$

что доказывает первую часть теоремы 15.

С другой стороны, пусть $\mathfrak{p}$ входит множителем в относительный дискриминант поля $K(\sqrt{\mu})$. Тогда по теореме 4 показатель a является нечетным числом. Следовательно, по теореме 13 мы имеем

$$\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = \left(\frac{\nu^a}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{p}}\right),$$

откуда, принимая во внимание теорему 2, легко получаем вторую часть теоремы 15.

Позже мы увидим, что теорема 15, равно как и теорема 14, выполняются для любого входящего множителем в 2 простого идеала, хотя доказать это уже значительно труднее. Тогда мы остановимся на роли, которую теорема 15 и ее обобщение на случай произвольного простого идеала играют в нашей теории.

§ 11. Связки единиц поля k

Определение 7. Если ε — некоторая единица поля k, то система всех единиц вида $\varepsilon\xi^2$, где ξ пробегает все единицы поля k, называется *связкой единиц* поля k. Связка единиц, определяемая единицей $\varepsilon = 1$, т. е. связка, состоящая из квадратов всех единиц поля, называется *главной связкой* и будет обозначаться через 1. Если V, V' — две произвольные связки единиц в k, то при умножении каждой единицы из V на каждую единицу из V' все такие произведения снова образуют связку единиц в k, которая будет называться *произведением связок* V и V' и обозначаться через VV'. Если представлено некоторое число связок в k, ни одна из которых не является главной и ни одна из которых не может быть получена из других при помощи умножения, то такие связки называются *независимыми* друг от друга.

Можно построить полную систему основных единиц[5] поля k из r единиц $\varepsilon_1, \ldots, \varepsilon_r$. Далее, пусть ζ — корень из единицы, который содержится в k, в то время как $\sqrt{\zeta}$ не лежит в k. Полагая $\varepsilon_{r+1} = \zeta$, легко убеждаемся, что $\varepsilon_1, \ldots, \varepsilon_{r+1}$ образуют такую систему из $r+1$ единиц, что произвольная единица ε в k может быть представлена, и притом только одним способом, в виде

$$\varepsilon = \varepsilon_1^{u_1} \varepsilon_2^{u_2} \ldots \varepsilon_{r+1}^{u_{r+1}} \xi^2,$$

[5] См. «Поля алгебраических чисел».

где показатели $u_1, u_2, \ldots, u_{r+1}$ принимают лишь значения 0 или 1 и ξ — некоторая подходящая единица в k. Очевидно, что единицы $\varepsilon_1, \ldots, \varepsilon_{r+1}$ определяют систему из $r+1$ независимых связок в k, умножением которых можно получить вообще все имеющиеся в k связки. Отсюда мы заключаем, что всего поле k обладает ровно 2^{r+1} различными связками единиц.

§ 12. Комплексы относительного квадратичного поля K

Определение 8. Пусть $\mathfrak{C}$ — идеал из некоторого класса идеалов C относительного квадратичного поля K над k. Тогда класс идеалов, определенный относительно сопряженным идеалом $S\mathfrak{C}$, будет обозначаться через SC и называться *относительно сопряженным* с C *классом*. Класс идеалов A поля $K(\sqrt{\mu})$ называется *амбивалентным классом*, если он равен своему относительно сопряженному классу SA, т. е. если

$$A = SA.$$

В частности, очевидно, что амбивалентен любой класс поля K, который содержит амбивалентный идеал поля K. Однако, как будет показано позже, вполне возможно существование амбивалентных классов в K, не содержащих амбивалентных идеалов.

Квадрат амбивалентного класса A всегда является таким классом в K, который обязательно содержит среди своих идеалов и идеалы, лежащие в k; это легко следует из равенства $A^2 = A \cdot SA$.

Определение 9. Если C — произвольный класс в K, то я называю систему всех классов вида cC, где c пробегает классы поля k, *комплексом* поля K. Комплекс, состоящий из всех классов c в k, называется *главным комплексом* и будет обозначаться через 1.

Если P и P' — два произвольных комплекса и каждый класс в P умножить на каждый класс в P', то все такие произведения снова образуют комплекс, который называется *произведением комплексов* P и P' и обозначается через PP'.

Если C — некоторый класс комплекса P, то тот комплекс, которому принадлежит относительно сопряженный класс SC, называется *относительно сопряженным* с P *комплексом* и обозначается через SP.

Любой комплекс, который совпадает со своим относительно сопряженным комплексом, называется *амбивалентным комплексом*. Если P — амбивалентный комплекс, то из равенства $P = SP$ следует равенство

$$P^2 = P \cdot SP = 1,$$

т. е. квадрат любого амбивалентного комплекса является главным комплексом. Наоборот, если квадрат некоторого комплекса P представляет собой главный комплекс 1, то P — амбивалентный комплекс. В самом деле, так как комплекс $P \cdot SP$ всегда равен 1, из $P^2 = 1$ следует $P = SP$.

Любой комплекс P, содержащий амбивалентный класс A, является амбивалентным комплексом; такой комплекс называется комплексом, порожденным амбивалентным классом A. Если, в частности, амбивалентный класс A

содержит амбивалентный идеал $\mathfrak{A}$, то P называется комплексом, порожденным амбивалентным идеалом $\mathfrak{A}$.

Если имеется некоторое число комплексов поля K, среди которых нет главного комплекса 1 и ни один из которых нельзя получить из остальных при помощи умножения, то такие комплексы называются *независимыми* друг от друга.

§ 13. Простые идеалы поля k с предписанными квадратичными характерами

Мы получим здесь одно весьма ценное вспомогательное средство для дальнейшего развития теории относительно квадратичных полей, исследовав вопрос о том, всегда ли в поле k существует простой идеал, относительно которого некоторые данные числа имеют предписанные квадратичные характеры. Мы проведем исследование этого вопроса следующим образом.

Теорема 16 (лемма). *Пусть α — целое число в k, которое не является квадратом в k. Положим*

$$f(1) = \sum_{(\mathfrak{p})} \left(\frac{\alpha}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{p})^s} \qquad (s > 1),$$

где сумма в правой части распространяется на все простые идеалы $\mathfrak{p}$ поля k. Так определенная функция $f(s)$ вещественной переменной s стремится к некоторому конечному пределу, когда s, убывая, стремится к 1.

Доказательство. Помимо заданного поля k степени m, рассмотрим определенное с помощью $\sqrt{\alpha}$ относительное квадратичное поле $K(\sqrt{\alpha})$ степени $2m$. Далее, введем в рассмотрение функции

$$\zeta_k(s) = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}} \quad \text{и} \quad \zeta_K(s) = \prod_{(\mathfrak{P})} \frac{1}{1 - N(\mathfrak{P})^{-s}},$$

где первое произведение распространяется на все простые идеалы $\mathfrak{p}$ поля k, а второе — на все простые идеалы $\mathfrak{P}$ поля $K(\sqrt{\alpha})$ и где $n(\mathfrak{p})$ означает норму идеала $\mathfrak{p}$ в k, а $N(\mathfrak{P})$ — норму $\mathfrak{P}$ в $K(\sqrt{\alpha})$. Известно[6], что эти бесконечные произведения сходятся при $s > 1$ и пределы

$$\lim_{s \to 1}\{(s-1)\zeta_k(s)\}, \qquad \lim_{s \to 1}\{(s-1)\zeta_K(s)\}$$

конечны и отличны от нуля. Отсюда следует, что и предел

$$\lim_{s \to 1} \frac{\zeta_K(s)}{\zeta_k(s)} \tag{1}$$

---

[6] См. «Поля алгебраических чисел», § 26.

имеет конечное отличное от нуля значение. Теперь мы сгруппируем произведение

$$\zeta_K(s) = \prod_{(\mathfrak{P})} \frac{1}{1 - N(\mathfrak{P})^{-s}} \tag{2}$$

по простым идеалам $\mathfrak{p}$ поля k, от которых «происходят» простые идеалы $\mathfrak{P}$. Учитывая определение 4, получим, что любому простому идеалу $\mathfrak{p}$ соответствует в произведении (2) член

$$\frac{1}{(1 - n(\mathfrak{p})^{-s})^2}, \quad \text{или} \quad \frac{1}{1 - n(\mathfrak{p})^{-s}}, \quad \text{или} \quad \frac{1}{1 - n(\mathfrak{p})^{-2s}} \tag{3}$$

в зависимости от того,

$$\left(\frac{\alpha}{\mathfrak{p}}\right) = +1, \quad \text{или} \quad = 0, \quad \text{или} \quad = -1.$$

Поэтому мы можем записать все три выражения (3) в виде

$$\frac{1}{1 - n(\mathfrak{p})^{-s}} \cdot \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}}$$

и получить

$$\zeta_K(s) = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}} \prod_{(\mathfrak{p})} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}} = \zeta_k(s) \prod_{(\mathfrak{p})} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}},$$

а так как предел (1) конечен и отличен от 0, то это же верно и для предела

$$\lim_{s \to 1} \prod_{(\mathfrak{p})} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}}.$$

Переходя стандартным способом к логарифмам, мы заключаем отсюда, что предел

$$\lim_{s \to 1} \sum_{(\mathfrak{p})} \left(\frac{\alpha}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{p})^s}$$

имеет конечное значение, что и доказывает теорему 16.

Теорема 17 (лемма). *Пусть $\alpha_1, \ldots, \alpha_z$ — какие-нибудь z целых чисел в k, обладающие тем свойством, что никакое составленное из них произведение не равно квадрату никакого числа в k. Далее, пусть $c_1, \ldots, c_z$ — произвольно заданные единицы ± 1. Тогда выполняется равенство*

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} = \frac{1}{2^z} \log \frac{1}{s - 1} + f(s) \qquad (s > 1),$$

где сумма слева распространяется на все простые идеалы $\mathfrak{p}$ поля k, удовлетворяющие условиям

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right) = c_1, \qquad \left(\frac{\alpha_2}{\mathfrak{p}}\right) = c_2, \qquad \ldots, \qquad \left(\frac{\alpha_z}{\mathfrak{p}}\right) = c_z,$$

а $f(s)$ справа — функция вещественной переменной s, стремящаяся к некоторому конечному пределу при s, стремящемся к 1.

Доказательство. Имеем

$$\log \zeta_k(s) = \sum_{(\mathfrak{p})} \log \frac{1}{1 - n(\mathfrak{p})^{-s}} = \sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + \varphi(s) \qquad (s > 1),$$

где обе суммы распространены на все простые идеалы $\mathfrak{p}$ в k, а $\varphi(s)$ — некоторая функция вещественной переменной s, остающаяся конечной при $s = 1$. Далее, так как выражение $(s-1)\zeta_k(s)$ остается конечным и отличным от 0 при $s = 1$, мы заключаем, что в равенстве

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} = \log \frac{1}{s-1} + \psi(s) \qquad (s > 1) \tag{4}$$

$\psi(s)$ снова представляет собой функцию от s, остающуюся конечной при $s=1$.

Теперь подставим в сумму

$$\sum_{(\mathfrak{p})} \left(\frac{\alpha}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{p})^s} \qquad (s > 1), \tag{5}$$

распространенную на все простые идеалы $\mathfrak{p}$, значение $\alpha = \alpha_1^{u_1}\alpha_2^{u_2} \dots \alpha_z^{u_z}$ и умножим полученное выражение на множитель $c_1^{u_1}c_2^{u_2}\dots c_z^{u_z}$. Придадим затем всем z показателям $u_1, u_2, \dots, u_z$ поочередно значения 0 и 1, исключив, однако, систему значений $u_1 = 0, u_2 = 0, \dots, u_z = 0$. Согласно теореме 16 все $2^z - 1$ полученных таким способом из (5) выражений остаются конечными при $s = 1$. Если сложить их с (4), то получится равенство вида

$$\sum_{(\mathfrak{p})} \left\{1 + c_1\left(\frac{\alpha_1}{\mathfrak{p}}\right)\right\}\left\{1 + c_2\left(\frac{\alpha_2}{\mathfrak{p}}\right)\right\} \dots \left\{1 + c_z\left(\frac{\alpha_z}{\mathfrak{p}}\right)\right\} \frac{1}{n(\mathfrak{p})^s} = \\ = \log \frac{1}{s-1} + \chi(s), \tag{6}$$

где снова $\chi(s)$ — некоторая функция, остающаяся конечной при $s = 1$.

Справедливость нашей теоремы немедленно следует из соотношения (6), если заметить, что выражение

$$\left\{1 + c_1\left(\frac{\alpha_1}{\mathfrak{p}}\right)\right\}\left\{1 + c_2\left(\frac{\alpha_2}{\mathfrak{p}}\right)\right\} \dots \left\{1 + c_z\left(\frac{\alpha_z}{\mathfrak{p}}\right)\right\}$$

принимает значение 2^z для всех простых идеалов $\mathfrak{p}$, которые удовлетворяют условию теоремы, и что это выражение обращается в нуль для всех остальных простых идеалов $\mathfrak{p}$ поля k, за исключением конечного числа простых идеалов, входящих множителями в $\alpha_1\alpha_2 \dots \alpha_z$.

Из только что доказанной равенства теоремы тотчас следует, с учетом того факта, что $\log \dfrac{1}{s-1}$ неограничен при $s = 1$, следующий результат.

Теорема 18. *Пусть $\alpha_1, \alpha_2, \dots, \alpha_z$ — какие-либо z целых чисел в k, удовлетворяющих условию, что никакое составленное из них произведение не равно квадрату никакого числа в k. Далее, пусть c_1, $c_2, \dots, c_z$ — произвольно заданные единицы ± 1. Тогда в поле k существует бесконечно много простых идеалов $\mathfrak{p}$, удовлетворяющих условиям*

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right) = c_1, \qquad \left(\frac{\alpha_2}{\mathfrak{p}}\right) = c_2, \qquad \dots, \qquad \left(\frac{\alpha_z}{\mathfrak{p}}\right) = c_z.$$

ГЛАВА 2

ТЕОРИЯ ОТНОСИТЕЛЬНО КВАДРАТИЧНЫХ ПОЛЕЙ ДЛЯ ОСНОВНОГО ПОЛЯ С ОДНИМИ МНИМЫМИ СОПРЯЖЕННЫМИ И НЕЧЕТНЫМ ЧИСЛОМ КЛАССОВ

Чтобы выразить возможно более простым и понятным способом дальнейшие утверждения теории относительно квадратичных числовых полей и изложить их доказательства наиболее естественным и последовательным образом, я ограничусь ниже рассмотрением частного случая: я всегда буду предполагать, что положенное в основу поле k удовлетворяет двум условиям:

1. *Это поле m-й степени k вместе со всеми сопряженными полями $k', \ldots, k^{(m-1)}$ является мнимым.*
2. *Число h классов идеалов поля k нечетно.*

§ 14. Относительные основные единицы поля K

Вследствие первого из только что сделанных двух предположений число единиц, образующих полную систему основных единиц в k, равно $m/2-1$. Пусть $\varepsilon_1, \ldots, \varepsilon_{m/2-1}$ — полная система основных единиц в k. Докажем сначала следующее утверждение:

Теорема 19 (лемма). *В относительном квадратичном поле $K(\sqrt{\mu})$ всегда можно найти $m/2$ единиц $\mathsf{H}_1, \ldots, \mathsf{H}_{m/2}$, таких что для любой единицы E в $K(\sqrt{\mu})$ справедливо равенство вида*

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \ldots \mathsf{H}_{m/2}^{U_{m/2}} [\xi],$$

где показатель u — нечетное число, показатели $U_1, \ldots, U_{m/2}$ принимают нулевые или целые рациональные значения, а $[\xi]$ — некоторая единица поля k или же единица поля $K(\sqrt{\mu})$, квадрат которой является единицей в k. Итак, в любом случае $[\xi]$ представляет собой некоторую единицу в k и может быть корнем из некоторой единицы в k тогда и только тогда, когда μ является единицей в k или равно произведению таковой на квадрат некоторого числа поля k.

Единицы $\mathsf{H}_1, \ldots, \mathsf{H}_{m/2}$ независимы друг от друга в том смысле, что между ними невозможно никакое соотношение вида

$$\mathsf{H}_1^{U_1} \ldots \mathsf{H}_{m/2}^{U_{m/2}} [\xi] = 1$$

с целыми рациональными показателями $U_1, \ldots, U_{m/2}$, за исключением случая, когда все эти показатели обращаются в нуль и $[\xi] = 1$.

Доказательство. В поле $K(\sqrt{\mu})$ существует полная система из $m-1$ основных единиц $\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}$. Рассмотрим систему из $3m/2-2$ единиц

$$\mathsf{H}_1, \ \ldots, \ \mathsf{H}_{m-1}, \ \varepsilon_1, \ \ldots, \ \varepsilon_{m/2-1}.$$

Коль скоро $m/2-1>0$, между этими единицами всегда существует соотношение вида

$$\mathsf{H}_1^{A_1}\dots\mathsf{H}_{m-1}^{A_{m-1}}\varepsilon_1^{a_1}\dots\varepsilon_{m/2-1}^{a_{m/2-1}}=1, \tag{1}$$

где $A_1,\dots,A_{m-1}$, $a_1,\dots,a_{m/2-1}$ — целые рациональные показатели, причем не все $A_1,\dots,A_{m-1}$ равны нулю. Положим

$$A_1=2^eA'_1,\qquad\dots,\qquad A_{m-1}=2^eA'_{m-1},$$

где 2^e — наибольшая степень 2, делящая все числа $A_1,\dots,A_{m-1}$, и пусть, скажем, A'_{m-1} — нечетное число. Далее, положим для краткости

$$\varepsilon=\varepsilon_1^{-a_1}\dots\varepsilon_{m/2-1}^{-a_{m/2-1}}.$$

Из соотношения (1) вытекает следующее равенство:

$$\mathsf{H}_1^{A'_1}\dots\mathsf{H}_{m-1}^{A'_{m-1}}=\sqrt[2^e]{\varepsilon}. \tag{2}$$

Так как правая часть здесь является корнем степени 2^e из некоторой единицы ε в k и должна совпадать с некоторой единицей в K в силу соотношения (2), эта правая часть является либо единицей в k, либо квадратным корнем из некоторой единицы в k. Таким образом, мы можем записать соотношение (2) в виде

$$\mathsf{H}_1^{A'_1}\dots\mathsf{H}_{m-1}^{A'_{m-1}}=[\xi],$$

откуда следует, что

$$\mathsf{H}_{m-1}^{A'_{m-1}}=\mathsf{H}_1^{-A'_1}\dots\mathsf{H}_{m-2}^{-A'_{m-2}}[\xi], \tag{3}$$

где $[\xi]$ понимается, как указано в формулировке теоремы.

Теперь мы исключим единицу H_{m-1} из первоначальной системы основных единиц и рассмотрим систему из $3m/2-3$ единиц

$$\mathsf{H}_1,\ \dots,\ \mathsf{H}_{m-2},\ \varepsilon_1,\ \dots,\ \varepsilon_{m/2-1}.$$

В случае если $m/2-2>0$, между этими единицами существует соотношение вида

$$\mathsf{H}_1^{B_1}\dots\mathsf{H}_{m-2}^{B_{m-2}}\varepsilon_1^{b_1}\dots\varepsilon_{m/2-1}^{b_{m/2-1}}=1, \tag{4}$$

где $B_1,\dots,B_{m-2}$, $b_1,\dots,b_{m/2-1}$ — целые рациональные показатели, причем не все $B_1,\dots,B_{m-2}$ равны нулю. Положим

$$B_1=2^fB'_1,\qquad\dots,\qquad B_{m-2}=2^fB'_{m-2},$$

где 2^f — наибольшая степень 2, делящая все числа $B_1,\dots,B_{m-2}$, и пусть, скажем, B'_{m-2} — нечетное число. Далее, положим для краткости

$$\overline{\varepsilon}=\varepsilon_1^{-b_1}\dots\varepsilon_{m/2-1}^{-b_{m/2-1}}.$$

Тогда соотношение (4) принимает вид

$$\mathsf{H}_1^{B'_1}\dots\mathsf{H}_{m-2}^{B'_{m-2}}=\sqrt[2^f]{\overline{\varepsilon}},$$

откуда получаем, как и раньше, равенство

$$\mathsf{H}_{m-2}^{B'_{m-2}}=\mathsf{H}_1^{-B'_1}\dots\mathsf{H}_{m-3}^{-B'_{m-3}}[\xi], \tag{5}$$

где снова $[\xi]$ понимается, как указано в формулировке теоремы. Рассмотрим теперь систему единиц

$$\mathsf{H}_1, \quad \ldots, \quad \mathsf{H}_{m-3}, \quad \varepsilon_1, \quad \ldots, \quad \varepsilon_{m/2-1}.$$

Очевидно, что можно продолжать в том же духе до тех пор, пока от первоначальных основных единиц $\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}$ не останется всего лишь $m/2$ единиц, скажем $\mathsf{H}_1, \ldots, \mathsf{H}_{m/2}$. Легко проверить, что эти единицы обладают требуемым свойством. Действительно, так как $\mathsf{H}_1, \ldots, \mathsf{H}_{m-1}$ образуют систему основных единиц поля K, то произвольная единица E в K может быть представлена в виде

$$\mathsf{E} = \mathsf{H}_1^{U_1} \ldots \mathsf{H}_{m-1}^{U_{m-1}} \mathsf{Z}, \tag{6}$$

где $U_1, \ldots, U_{m-1}$ — целые рациональные показатели и Z — некоторый корень из единицы. Очевидно, что Z — либо корень из единицы, лежащий в k, либо квадратный корень из некоторого корня из единицы, лежащего в k, умноженный на некоторый корень Z^* нечетной степени u^* из единицы. Следовательно, мы можем положить $\mathsf{Z} = [\xi]\mathsf{Z}^*$, где $[\xi]$ понимается, как указано в формулировке теоремы. Если теперь мы возведем равенство (6) в $u = u^* A'_{m-1} B'_{m-2} \ldots$ степень, то, используя равенства (3), (5) и их дальнейшие аналоги, получим соотношение, которое ввиду нечетности u доказывает справедливость нашей теоремы.

О п р е д е л е н и е 10. Я называю единицы $\mathsf{H}_1, \ldots, \mathsf{H}_{m/2}$, обладающие свойством, указанным в теореме 19, системой *относительных основных единиц поля* $K(\sqrt{\mu})$ над k.

Т е о р е м а 20 (лемма). *Пусть* $\mathsf{H}_1, \ldots, \mathsf{H}_{m/2}$ *образуют систему относительных основных единиц поля* K *и*

$$\eta_1 = N(\mathsf{H}_1), \qquad \ldots, \qquad \eta_{m/2} = N(\mathsf{H}_{m/2})$$

— их относительные нормы. Тогда любая единица ε *в* k, *являющаяся относительной нормой некоторой единицы* E *поля* K, *может быть представлена в виде*

$$\varepsilon = \eta_1^{u_1} \ldots \eta_{m/2}^{u_{m/2}} N([\xi]),$$

где показатели $u_1, \ldots, u_{m/2}$ *принимают значения* 0 *или* 1, *а* $[\xi]$ *— некоторая единица в* k *или лежащий в* K *корень квадратный из некоторой единицы в* k.

Д о к а з а т е л ь с т в о. По теореме 19 для единицы E выполняется равенство

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \ldots \mathsf{H}_{m/2}^{U_{m/2}} [\xi],$$

где обозначения следует понимать, как и в теореме 19. Если мы возьмем теперь относительные нормы от обеих частей этого равенства, то получим

$$\varepsilon^u = \eta_1^{U_1} \ldots \eta_{m/2}^{U_{m/2}} N([\xi]).$$

Отсюда следует, что

$$\varepsilon = \eta_1^{u_1} \ldots \eta_{m/2}^{u_{m/2}} N([\xi^*]),$$

где $u_i = 0$ или $= 1$ в зависимости от того, четно U_i или нечетно, и где, далее,

$$[\xi^*] = \eta_1^{(U_1-u_1)/2} \dots \eta_{m/2}^{(U_{m/2}-u_{m/2})/2} \varepsilon^{(1-u)/2}[\xi].$$

Тем самым теорема 20 доказана.

§ 15. Число амбивалентных комплексов в K, порождаемых амбивалентными идеалами

Теорема 21. *Амбивалентный комплекс P относительного квадратичного поля K содержит только амбивалентные классы. Число амбивалентных классов в K в точности равно умноженному на h числу амбивалентных комплексов.*

Доказательство. Если C — некоторый класс амбивалентного комплекса P, то из равенства $P = SP$ следует, очевидно, что $C = c \cdot SC$, где C — один из h классов поля k. Взяв относительную норму от обеих частей последнего равенства, легко получаем, что $1 = c^2$, а так как, с другой стороны, и $c^h = 1$, где число классов h должно быть нечетным, то $c = 1$, т. е. $C = SC$; следовательно, C — амбивалентный класс. Если теперь $C = cC$, где c — некоторый класс в k, то точно так же получаем $c = 1$, откуда следует второе утверждение теоремы.

Теорема 22. *Пусть число всех амбивалентных идеалов поля $K(\sqrt{\mu})$ равно 2^t, и пусть те единицы в k, которые являются относительными нормами единиц из $K(\sqrt{\mu})$, составляют все вместе 2^{v^*} связок единиц в k. Тогда число амбивалентных комплексов поля $K(\sqrt{\mu})$, порожденных амбивалентными идеалами, в точности равно 2^{a^*}, где*

$$a^* = t + v^* - m/2 - 1.$$

Доказательство. Предположим сначала, что число μ не является произведением единицы на квадрат некоторого числа в поле k. Тогда любое выражение $[\xi]$ должно быть единицей, лежащей в k.

Пусть теперь, как и в теореме 20, $\mathsf{H}_1, \dots, \mathsf{H}_{m/2}$ — система относительных основных единиц поля $K(\sqrt{\mu})$ и

$$\eta_1 = N(\mathsf{H}_1), \qquad \dots, \qquad \eta_{m/2} = N(\mathsf{H}_{m/2})$$

— их относительные нормы. В силу нашего предположения и теоремы 20 любая единица ε в k, которая является относительной нормой некоторой единицы в $K(\sqrt{\mu})$, может быть представлена в виде

$$\varepsilon = \eta_1^{u_1} \dots \eta_{m/2}^{u_{m/2}} \xi^2,$$

где показатели $u_1, \dots, u_{m/2}$ имеют значения 0 или 1 и ξ — некоторая единица в k. Так как число связок единиц в k, являющихся относительными нормами единиц в $K(\sqrt{\mu})$, по предположению равняется 2^{v^*}, то можно среди этих $m/2$ единиц $\eta_1, \dots, \eta_{m/2}$ выбрать какие-то v^* штук, скажем $\eta_1, \dots, \eta_{v^*}$,

таких что любая единица ε в k, являющаяся относительной нормой некоторой единицы в $K(\sqrt{\mu})$, может быть представлена, и притом единственным способом, в виде

$$\varepsilon = \eta_1^{u_1} \ldots \eta_{v^*}^{u_{v^*}} \xi^2,$$

где показатели $u_1, \ldots, u_{v^*}$ снова принимают значения 0 или 1 и ξ — некоторая единица в k.

В частности, мы представим в таком виде единицы $\eta_{v^*+1}, \ldots, \eta_{m/2}$; таким образом,

$$\eta_i = \eta_1^{u_1^{(i)}} \ldots \eta_{v^*}^{u_{v^*}^{(i)}} (\xi^{(i)})^2 \qquad (i = v^* + 1,\, v^* + 2,\, \ldots,\, m/2),$$

где $u_1^{(i)}, \ldots, u_{v^*}^{(i)}$ принимают значения 0 или 1 и $\xi^{(i)}$ — единицы в k. Тогда $m/2 - v^*$ выражений

$$\mathsf{H}'_i = \mathsf{H}_i \mathsf{H}_1^{-u_1^{(i)}} \ldots \mathsf{H}_{v^*}^{-u_{v^*}^{(i)}} (\xi^{(i)})^{-1} \qquad (i = v^* + 1,\, v^* + 2,\, \ldots,\, m/2) \tag{1}$$

являются, очевидно, единицами в $K(\sqrt{\mu})$, относительные нормы которых равны 1, и, следовательно, $m/2 - v^*$ целых чисел

$$\mathsf{M}_1 = 1 + \mathsf{H}'_{v^*+1}, \qquad \ldots, \qquad \mathsf{M}_{m/2-v^*} = 1 + \mathsf{H}'_{m/2}$$

удовлетворяет равенствам

$$\mathsf{M}_1 = \mathsf{H}'_{v^*+1} \cdot S\mathsf{M}_1, \qquad \ldots, \qquad \mathsf{M}_{m/2-v^*} = \mathsf{H}'_{m/2} \cdot S\mathsf{M}_{m/2-v^*}. \tag{2}$$

Положим, далее, $\mathsf{M} = \sqrt{\mu}$ и рассмотрим определенные числами

$$\mathsf{M},\ \mathsf{M}_1,\ \ldots,\ \mathsf{M}_{m/2-v^*}$$

главные идеалы

$$(\mathsf{M}) = \mathfrak{M}, \qquad (\mathsf{M}_1) = \mathfrak{M}_1, \qquad \ldots, \qquad (\mathsf{M}_{m/2-v^*}) = \mathfrak{M}_{m/2-v^*}.$$

Так как в силу (2) каждый из этих главных идеалов совпадает со своим относительно сопряженным идеалом и, следовательно, является произведением амбивалентного идеала и идеала из k, мы можем согласно определению 3 записать

$$\begin{aligned}
\mathfrak{M} &= \mathfrak{V}_1^{a_1} \ldots \mathfrak{V}_t^{a_t}, && (\mathfrak{j}),\\
\mathfrak{M}_1 &= \mathfrak{V}_1^{a_1^{(1)}} \ldots \mathfrak{V}_t^{a_t^{(1)}}, && (\mathfrak{j}^{(1)}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\mathfrak{M}_{m/2-v^*} &= \mathfrak{V}_1^{a_1^{(m/2-v^*)}} \ldots \mathfrak{V}_t^{a_t^{(m/2-v^*)}}, && (\mathfrak{j}^{(m/2-v^*)}),
\end{aligned} \tag{3}$$

где $\mathfrak{V}_1, \ldots, \mathfrak{V}_t$ — это t амбивалентных простых идеалов поля $K(\sqrt{\mu})$; $\mathfrak{j}, \mathfrak{j}^{(1)}, \ldots$ $\ldots, \mathfrak{j}^{(m/2-v^*)}$ — идеалы в k и $a_1, a_2, \ldots, a_t^{m/2-v^*}$ — заданные показатели 0 или 1.

Мы хотим доказать, что между идеалами

$$\mathfrak{M},\quad \mathfrak{M}_1,\quad \ldots,\quad \mathfrak{M}_{m/2-v^*}$$

не может иметь места никакое соотношение вида

$$\mathfrak{M}^e \mathfrak{M}_1^{e_1} \ldots \mathfrak{M}_{m/2-v^*}^{e_{m/2-v^*}} = \mathfrak{j}^*, \tag{4}$$

где показатели $e, e_1, \ldots, e_{m/2-v^*}$ имеют некие значения 0 или 1, а $\mathfrak{j}^*$ — идеал поля k, за исключением случая, когда все эти показатели равны 0 и $\mathfrak{j}^* = 1$.

С этой целью возведем соотношение (4) в h-ю степень и положим $\mathfrak{j}^h = (\iota)$, где ι — некоторое целое число в k. Мы получим соотношение вида

$$\mathsf{M}^{eh}\mathsf{M}_1^{e_1 h} \dots \mathsf{M}_{m/2-v^*}^{e_{m/2-v^*}h} = \iota\mathsf{E},$$

где E — некоторая единица поля $K(\sqrt{\mu})$. Применяя к этому соотношению подстановку S и деля исходное соотношение на полученное таким образом новое, приходим к равенству

$$\left(\frac{\mathsf{M}}{S\mathsf{M}}\right)^{eh}\left(\frac{\mathsf{M}_1}{S\mathsf{M}_1}\right)^{e_1 h} \dots \left(\frac{\mathsf{M}_{m/2-v^*}}{S\mathsf{M}_{m/2-v^*}}\right)^{e_{m/2-v^*}h} = \frac{\mathsf{E}}{S\mathsf{E}}$$

или, в силу (2),

$$(-1)^{eh}\mathsf{H}'^{e_1 h}_{v^*+1} \dots \mathsf{H}'^{e_{m/2-v^*}h}_{m/2} = \frac{\mathsf{E}}{S\mathsf{E}}.$$

Запишем это соотношение в виде

$$\mathsf{H}'^{e_1 h}_{v^*+1} \dots \mathsf{H}'^{e_{m/2-v^*}h}_{m/2} = \mathsf{E}^2\xi, \tag{5}$$

где $\xi = (-1)^{eh}/N(\mathsf{E})$ — единица в k.

По теореме 19 для любой единицы E существует нечетный показатель u, такой что

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \dots \mathsf{H}_{m/2}^{U_{m/2}}\xi', \tag{6}$$

где показатели $U_1, \dots, U_{m/2}$ принимают целые рациональные значения и ξ' — единица в k. Принимая во внимание (1), получаем из (5) и (6) равенство вида

$$\mathsf{H}_1^{E_1} \dots \mathsf{H}_{v^*}^{E_{v^*}}\mathsf{H}_{v^*+1}^{e_1 hu-2U_{v^*+1}} \dots \mathsf{H}_{m/2}^{e_{m/2-v^*}hu-2U_{m/2}} \cdot \xi'' = 1, \tag{7}$$

где $E_1, \dots, E_{v^*}$ — целые рациональные показатели и ξ'' — снова единица в k. Так как h и u — нечетные числа, то в случае, если бы хоть одно из чисел $e_1, \dots, e_{m/2-v^*}$ равнялось 1, соответствующий показатель в последовательности

$$e_1 hu - 2U_{v^*+1}, \quad \dots, \quad e_{m/2-v^*}hu - 2U_{m/2}$$

был бы обязательно нечетным и тем самым отличным от 0. Но тогда соотношение (7) противоречило бы второму утверждению теоремы 19. Этим показано, что в соотношении (4) все показатели $e_1, \dots, e_{m/2-v^*}$ должны быть равны 0.

Теперь легко проверить, что в (4) и показатель e должен обращаться в нуль. Действительно, если бы e равнялось 1, то идеал $\mathfrak{M} = \sqrt{\mu}$ совпадал бы с некоторым идеалом $\mathfrak{j}$ в k и, следовательно, мы имели бы $\mu = \mathfrak{j}^2$. Возводя это равенство в h-ю степень, получим $\mu^h = \mathfrak{j}^{2h}$, и если $\mathfrak{j}^h = (\iota)$, где ι — некоторое целое число в k, то мы получаем $\mu^h = \varepsilon\iota^2$ или $\mu = \varepsilon\alpha^2$, где ε — единица в k и $\alpha = \iota/\mu^{(h-1)/2}$ — число, принадлежащее k. Эта возможность, однако, исключается предположением, сделанным в начале доказательства. Тем самым доказано, что соотношение вида (4) может выполнятся, лишь если все показатели e, $e_1, \dots, e_{m/2-v^*}$ равны 0.

Теперь вернемся к равенствам (3) и выберем среди t амбивалентных простых идеалов $\mathfrak{D}_1, \dots, \mathfrak{D}_t$ такие $m/2 - v^* + 1$ штук — пусть это будут, скажем, $\mathfrak{D}_1, \dots, \mathfrak{D}_{m/2-v^*+1}$, — которые можно выразить с помощью равенств (3)

через идеалы $\mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{m/2-v^*}$, через остальные амбивалентные простые идеалы $\mathfrak{D}_{m/2-v^*+2}, \ldots, \mathfrak{D}_t$ и через некоторые идеалы $\mathfrak{m}^{(i)}$ поля k следующим образом:

$$\mathfrak{D}_i = \mathfrak{M}^{b^{(i)}} \mathfrak{M}_1^{b_1^{(i)}} \ldots \mathfrak{M}_{m/2-v^*}^{b_{m/2-v^*}^{(i)}} \mathfrak{D}_{m/2-v^*+2}^{d_{m/2-v^*+2}^{(i)}} \ldots \mathfrak{D}_t^{d_t^{(i)}} \mathfrak{m}^{(i)} \quad (i=1, 2, \ldots, m/2-v^*+1), \quad (8)$$

где показатели $b^{(i)}, b_1^{(i)}, \ldots, b_{m/2-v^*}^{(i)}, d_{m/2-v^*+2}^{(i)}, \ldots, d_t^{(i)}$ принимают значения 0 или 1. То, что это возможно, вытекает из ранее доказанного утверждения, что соотношение вида (4) может выполнятся лишь в случае, когда все показатели $e, e_1, \ldots, e_{m/2-v^*}$ обращаются в нуль. Кроме того, следует учесть то обстоятельство, что квадраты амбивалентных простых идеалов $\mathfrak{D}_1, \ldots, \mathfrak{D}_t$, а вместе с ними и квадраты идеалов

$$\mathfrak{M}, \quad \mathfrak{M}_1, \quad \ldots, \quad \mathfrak{M}_{m/2-v^*}$$

являются идеалами в k.

Так как идеалы $\mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{m/2-v^*}$ — главные, то равенства (8) немедленно показывают, что амбивалентные комплексы, определенные идеалами $\mathfrak{D}_1, \ldots, \mathfrak{D}_{m/2-v^*+1}$, представляют собой произведения комплексов, определенных идеалами $\mathfrak{D}_{m/2-v^*+2}, \ldots, \mathfrak{D}_t$. Итак, число независимых друг от друга комплексов, порождаемых амбивалентными идеалами, заведомо не превосходит $a^* = t + v^* - m/2 - 1$, а число всех вообще комплексов, порожденных амбивалентными идеалами, не превосходит поэтому 2^{a^*}.

Теперь мы докажем, что a^* комплексов, порождаемых a^* амбивалентными простыми идеалами $\mathfrak{D}_{m/2-v^*+2}, \ldots, \mathfrak{D}_t$, независимы друг от друга. Действительно, если бы один из этих комплексов, например, комплекс, порожденный $\mathfrak{D}_{m/2-v^*+2}$, можно было выразить через остальные, то имела бы место эквивалентность вида

$$\mathfrak{D}_{m/2-v^*+2} \sim \mathfrak{D}_{m/2-v^*+3}^{e_{m/2-v^*+3}} \ldots \mathfrak{D}_t^{e_t} \mathfrak{j},$$

где показатели $e_{m/2-v^*+3}, \ldots, e_t$ принимают значения 0 или 1 и $\mathfrak{j}$ — идеал в k. Будем понимать под $\mathfrak{j}'$ идеал в k, для которого в k выполняется эквивалентность $\mathfrak{j}' \mathfrak{D}_{m/2-v^*+2}^2 \sim \mathfrak{j}$. Тогда имеет место следующая эквивалентность:

$$\mathfrak{D}_{m/2-v^*+2} \mathfrak{D}_{m/2-v^*+3}^{e_{m/2-v^*+3}} \ldots \mathfrak{D}_t^{e_t} \mathfrak{j}' \sim 1,$$

и мы можем поэтому положить

$$\mathfrak{D}_{m/2-v^*+2} \mathfrak{D}_{m/2-v^*+3}^{e_{m/2-v^*+3}} \ldots \mathfrak{D}_t^{e_t} \mathfrak{j}' = (\mathsf{A}), \quad (9)$$

где A — некоторое целое число поля K.

Так как в силу равенства (9) главный идеал (A) должен совпадать со своим относительно сопряженным, выполняется равенство вида

$$\mathsf{A} = \mathsf{E} \cdot S\mathsf{A}, \quad (10)$$

где E — некоторая единица в K. Применим теперь к этой единице E теорему 19. Итак, пусть u — нечетный показатель, такой что

$$\mathsf{E}^u = \mathsf{H}_1^{U_1} \ldots \mathsf{H}_{m/2}^{U_{m/2}} \xi,$$

где показатели $U_1, \ldots, U_{m/2}$ принимают некоторые целые рациональные значения и ξ — единица в k. Используя (1), мы можем также записать

$$\mathsf{E}^u = \mathsf{H}_1^{U_1'} \ldots \mathsf{H}_{v^*}^{U_{v^*}'} \mathsf{H}'^{U_{v^*+1}}_{v^*+1} \ldots \mathsf{H}'^{U_{m/2}}_{m/2} \xi', \tag{11}$$

где $\mathsf{H}'_{v^*+1}, \ldots, \mathsf{H}'_{m/2}$ — определенные в (1) единицы, $U_1', \ldots, U_{v^*}'$ — некоторые целые рациональные показатели и ξ' — снова некоторая единица в k. Если мы возьмем относительную норму от обеих частей этого равенства и учтем, что, в силу (10), $N(\mathsf{E}) = 1$ и что относительные нормы единиц (1) равны 1, то легко получим, что

$$1 = \eta_1^{U_1'} \ldots \eta_{v^*}^{U_{v^*}'} \xi'^2.$$

Так как связки единиц в k, определенные с помощью $\eta_1, \ldots, \eta_v$, должны быть независимы друг от друга, отсюда следует, что все показатели $U_1', \ldots, U_{v^*}'$ четны. Теперь подставим в формулу (11) значения

$$\mathsf{E} = \frac{\mathsf{A}}{S\mathsf{A}},$$

$$\mathsf{H}_1^{U_1'} = \left(\frac{\mathsf{H}_1}{S\mathsf{H}_1}\eta_1\right)^{U_1'/2}, \quad \ldots, \quad \mathsf{H}_{v^*}^{U_{v^*}'} = \left(\frac{\mathsf{H}_{v^*}}{S\mathsf{H}_{v^*}}\eta_{v^*}\right)^{U_{v^*}'/2},$$

$$\mathsf{H}'_{v^*+1} = \frac{\mathsf{M}_1}{S\mathsf{M}_1}, \quad \ldots, \quad \mathsf{H}'_{m/2} = \frac{\mathsf{M}_{m/2-v^*}}{S\mathsf{M}_{m/2-v^*}}.$$

Полагая для краткости

$$\mathsf{B} = \mathsf{A}^{-u}\mathsf{H}_1^{U_1'/2} \ldots \mathsf{H}_{v^*}^{U_{v^*}'/2}\mathsf{M}_1^{U_{v^*+1}} \ldots \mathsf{M}_{m/2-v^*}^{U_{m/2}}, \tag{12}$$

получим из (11) равенство

$$\frac{\mathsf{B}}{S\mathsf{B}} = \xi'', \tag{13}$$

где ξ'' снова означает некоторую единицу в k. Взяв относительную норму от (13), находим, что $\xi''^2 = 1$, так что $\xi'' = (-1)^a$, где a принимает одно из значений 0, 1. Таким образом, мы можем записать (13) в виде

$$\frac{\mathsf{B}(\sqrt{\mu})^a}{S\{\mathsf{B}(\sqrt{\mu})^a\}} = 1, \quad \text{или} \quad \mathsf{B}(\sqrt{\mu})^a = S\{\mathsf{B}(\sqrt{\mu})^a\},$$

т. е. $\mathsf{B}(\sqrt{\mu})^a$ является числом из k. Ввиду этого обстоятельства, используя значения (9) и (12) для A и B и вспоминая, что u — нечетное число, мы без труда получаем соотношение вида

$$\mathfrak{D}_{m/2-v^*+2} = \mathfrak{M}^b\mathfrak{M}_1^{b_1} \ldots \mathfrak{M}_{m/2-v^*}^{b_{m/2-v^*}}\mathfrak{D}_{m/2-v^*+3}^{d_{m/2-v^*+3}} \ldots \mathfrak{D}_t^{d_t}\mathfrak{m}, \tag{14}$$

где $b, b_1, \ldots, b_{m/2-v^*}, d_{m/2-v^*+3}, \ldots, d_t$ принимают значения 0 или 1, а $\mathfrak{m}$ — некоторый идеал в k. Подставим это значение для $\mathfrak{D}_{m/2-v^*+2}$ в правую часть формулы (8) и присоединим к полученным таким образом $m/2 - v^* + 1$ уравнениям еще уравнение (14). Тогда мы получим систему из $m/2 - v^* + 2$

уравнений вида

$$\mathfrak{D}_i = \mathfrak{M}^{B^{(i)}}\mathfrak{M}_1^{B_1^{(i)}} \dots \mathfrak{M}_{m/2-v^*}^{B_{m/2-v^*}^{(i)}}\mathfrak{D}_{m/2-v^*+3}^{D_{m/2-v^*+3}^{(i)}} \dots \mathfrak{D}_t^{D_t^{(i)}}\mathfrak{n}^{(i)} \quad (i = 1, 2, \dots, m/2 - v^* + 2), \tag{15}$$

где показатели $B^{(i)}, B_1^{(i)}, \dots, B_{m/2-v^*}^{(i)}, D_{m/2-v^*+3}^{(i)}, \dots, D_t^{(i)}$ принимают значения 0 или 1, а $\mathfrak{n}^{(i)}$ — некоторые идеалы в k. Однако уравнения (15) выполняться не могут. В самом деле, пусть $m/2 - v^* + 2$ целых рациональных чисел

$$a^{(1)}, \dots, a^{m/2-v^*+2}$$

не все четны и по модулю 2 удовлетворяют сравнениям

$$\sum_{(i)} a^{(i)}B^{(i)} \equiv 0, \quad \sum_{(i)} a^{(i)}B_1^{(i)} \equiv 0, \quad \dots, \quad \sum_{(i)} a^{(i)}B_{m/2-v^*}^{(i)} \equiv 0, \quad (2), \quad (i = 1, 2, \dots, m/2 - v^* + 2).$$

Если мы возведем (15) в $a^{(i)}$-степень и перемножим между собой полученные таким образом для $i = 1, 2, \dots, m/2 - v^* + 2$ равенства, то получится равенство вида

$$\mathfrak{D}_1^{a^{(1)}} \dots \mathfrak{D}_{m/2-v^*+2}^{a^{(m/2-v^*+2)}} = \mathfrak{D}_{m/2-v^*+3}^{E^{(m/2-v^*+3)}} \dots \mathfrak{D}_t^{E^{(t)}}\mathfrak{n}, \tag{16}$$

где показатели $E^{(m/2-v^*+3)}, \dots, E^{(t)}$ имеют значения 0, 1 и $\mathfrak{n}$ — некоторый идеал в k. Однако такое равенство (16) невозможно, потому что его левая часть содержит хотя бы один из простых множителей $\mathfrak{D}_1, \dots, \mathfrak{D}_{m/2-v^*+2}$ в нечетной степени, в то время как справа эти простые множители входят только в $\mathfrak{n}$ и, следовательно, появляются в четных степенях. Таким образом, мы должны отказаться от нашего первоначального предположения о том, что комплекс, порожденный $\mathfrak{D}_{m/2-v^*+2}$, может быть выражен через комплексы, порожденные $\mathfrak{D}_{m/2-v^*+3}, \dots, \mathfrak{D}_t$. Тем самым мы показали, что в $K(\sqrt{\mu})$ существует ровно 2^{a^*} комплексов такого рода, как и утверждается в теореме.

В только что проведенном доказательстве теоремы был с самого начала исключен случай, когда μ равно произведению единицы на квадрат некоторого числа поля k; однако не составляет труда указать те видоизменения, которые следует внести в только что приведенное доказательство в этом специальном случае.

Так как число комплексов, порожденных амбивалентными идеалами, во всяком случае не меньше 1, то из теоремы 22 следует, в частности, неравенство

$$t + v^* - m/2 > 0.$$

§ 16. Число всех амбивалентных комплексов в K

Теорема 23. *Пусть число всех амбивалентных идеалов поля $K(\sqrt{\mu})$ равно 2^t и пусть те единицы поля, которые являются относительными нормами единиц или дробных чисел поля $K(\sqrt{\mu})$, составляют вместе ровно 2^v связок единиц. Тогда число всех амбивалентных комплексов поля $K(\sqrt{\mu})$ равно в точности 2^a, где*

$$a = t + v - m/2 - 1.$$

Доказательство. Прежде всего, мы снова примем то же предположение о числе μ, что и в начале доказательства теоремы 22, и будем постоянно использовать введенные там обозначения. Так как число связок единиц в k, являющихся относительными нормами каких-либо чисел из K, должно равняться 2^v, то можно к единицам $\eta_1, \ldots, \eta_{v^*}$, определенным в предыдущем доказательстве, добавить $v - v^*$ единиц $\theta_1, \ldots, \theta_{v-v^*}$, таких что единицы $\theta_1, \ldots, \theta_{v-v^*}$ являются относительными нормами некоторых дробных чисел $\Theta_1, \ldots, \Theta_{v-v^*}$ поля K, так что выполняются равенства

$$\theta_1 = N(\Theta_1), \qquad \ldots, \qquad \theta_{v-v^*} = N(\Theta_{v-v^*}) \tag{1}$$

и, сверх того, любая единица ε в k, являющаяся относительной нормой единицы или некоторого дробного числа в K, может быть представлена, и притом единственным способом, в виде

$$\varepsilon = \eta_1^{e_1} \ldots \eta_{v^*}^{e_{v^*}} \theta_1^{f_1} \ldots \theta_{v-v^*}^{f_{v-v^*}} \xi^2,$$

где показатели $e_1, \ldots, e_{v^*}, f_1, \ldots, f_{v-v^*}$ принимают значения 0 или 1, а ξ — единица в k. Тогда связки единиц, порождаемые $\eta_1, \ldots, \eta_{v^*}, \theta_1, \ldots, \theta_{v-v^*}$, независимы друг от друга.

Положим теперь

$$\Theta_i = \frac{\mathfrak{A}_i}{\mathfrak{B}_i} \qquad (i = 1, 2, \ldots, v - v^*),$$

где $\mathfrak{A}_i$ и $\mathfrak{B}_i$ — взаимно простые идеалы поля K для каждого данного i. Тогда в силу (1) $\mathfrak{B}_i = S\mathfrak{A}_i$, откуда

$$\Theta_i = \frac{\mathfrak{A}_i}{S\mathfrak{A}_i} \qquad (i = 1, 2, \ldots, v - v^*), \tag{2}$$

и на основании равенств (2) мы снова заключаем, что $\mathfrak{A}_i \sim S\mathfrak{A}_i$, т. е. все комплексы, определенные идеалами $\mathfrak{A}_i$, являются амбивалентными.

Теперь мы хотим доказать, что эти $v - v^*$ комплексов, определенных идеалами $\mathfrak{A}_i$, вместе с найденными в доказательстве теоремы 22

$$a^* = t + v^* - m/2 - 1$$

амбивалентными комплексами, порожденными амбивалентными идеалами $\mathfrak{D}_{m/2-v^*+2}, \ldots, \mathfrak{D}_t$, образуют систему независимых друг от друга комплексов и что, вообще, любой амбивалентный комплекс поля K является произведением некоторых

$$a = v - v^* + a^* = t + v - m/2 - 1$$

амбивалентных комплексов, порожденных $\mathfrak{A}_1, \ldots, \mathfrak{A}_{v-v^*}, \mathfrak{D}_{m/2-v^*+2}, \ldots, \mathfrak{D}_t$.

В самом деле, предположим, что эти комплексы зависимы. Тогда для соответствующих идеалов должно выполняться соотношение вида

$$\mathfrak{A}_1^{a_1} \dots \mathfrak{A}_{v-v^*}^{a_{v-v^*}} \mathfrak{D}_{m/2-v^*+2}^{e_1} \dots \mathfrak{D}_t^{e_{a^*}} \cdot \mathfrak{j} = \Theta, \tag{3}$$

где показатели $a_1, \dots, a_{v-v^*}, e_1, \dots, e_{a^*}$ принимают значения 0 или 1, не все из которых равны 0, $\mathfrak{j}$ — идеал в k и Θ — некоторое целое число из K. В силу (2) из (3) легко следует равенство

$$\frac{\Theta}{S\Theta} = \Theta_1^{a_1} \dots \Theta_{v-v^*}^{a_{v-v^*}} \mathsf{H}, \tag{4}$$

где H — некоторая единица в $K(\sqrt{\mu})$. Взяв относительную норму от обеих частей (4) и принимая во внимание (1), получаем

$$N(\mathsf{H}) = \theta_1^{-a_1} \dots \theta_{v-v^*}^{-a_{v-v^*}},$$

откуда видим, что единица

$$\theta = \theta_1^{-a_1} \dots \theta_{v-v^*}^{-a_{v-v^*}} \tag{5}$$

является относительной нормой некоторой единицы из K. Мы можем, следовательно, записать

$$\theta = \eta_1^{b_1} \dots \eta_{v^*}^{b_{v^*}} \xi^2, \tag{6}$$

где $b_1, \dots, b_{v^*}$ принимают значения 0 или 1, а ξ — некоторая единица в k. Из (5) и (6) мы получаем равенство

$$\eta_1^{b_1} \dots \eta_{v^*}^{b_{v^*}} \theta_1^{a_1} \dots \theta_{v-v^*}^{a_{v-v^*}} \xi^2 = 1.$$

В силу независимости связок единиц, определенных с помощью $\eta_1, \dots, \eta_{v^*}, \theta_1, \dots, \theta_{v-v^*}$, это равенство возможно только в том случае, когда все показатели $b_1, \dots, b_{v^*}, a_1, \dots, a_{v-v^*}$ четны и, тем самым, равны 0. Поэтому соотношение (3) приобретает вид

$$\mathfrak{D}_{m/2-v^*+2}^{e_1} \dots \mathfrak{D}_t^{e_{a^*}} \mathfrak{j} = \Theta.$$

В силу независимости комплексов, порожденных $\mathfrak{D}_{m/2-v^*+2}, \dots, \mathfrak{D}_t$, это соотношение требует, чтобы все показатели $e_1, \dots, e_{a^*}$ были равны 0, в противоречие нашим первоначальным предположениям о показателях в соотношении (3).

Остается еще привести доказательство того, что любой амбивалентный комплекс A может быть представлен как произведение комплексов, порожденных идеалами $\mathfrak{A}_1, \dots, \mathfrak{A}_{v-v^*}, \mathfrak{D}_{m/2-v^*+2}, \dots, \mathfrak{D}_t$. Если $\mathfrak{A}$ — произвольный идеал комплекса A, то в силу теоремы 21 выполняется равенство вида

$$\frac{S\mathfrak{A}}{\mathfrak{A}} = \Theta, \tag{7}$$

где Θ — некоторое число из поля K. Если мы возьмем относительную норму от обеих частей равенства (7), то получим, что относительной нормой

числа Θ служит некоторая единица θ в k. Таким образом, мы можем записать

$$\theta = N(\Theta) = \eta_1^{e_1} \dots \eta_{v^*}^{e_{v^*}} \theta_1^{f_1} \dots \theta_{v-v^*}^{f_{v-v^*}} \xi^2,$$

где показатели $e_1, \dots, e_{v^*}, f_1, \dots, f_{v-v^*}$ принимают значения 0 или 1, а ξ — единица в k. Отсюда мы получаем для числа

$$\Theta' = \pm\Theta \mathsf{H}_1^{-e_1} \dots \mathsf{H}_{v^*}^{-e_{v^*}} \Theta_1^{-f_1} \dots \Theta_{v-v^*}^{-f_{v-v^*}} \xi^{-1},$$

где знак выбирается так, чтобы $\Theta' \neq -1$, равенство

$$N(\Theta') = 1.$$

В силу этого равенства мы имеем

$$\Theta' = \frac{\Theta' + 1}{S(\Theta' + 1)}. \tag{8}$$

Далее, из равенства

$$\pm\Theta'\Theta^{-1}\mathsf{H}_1^{e_1} \dots \mathsf{H}_{v^*}^{e_{v^*}} \Theta_1^{f_1} \dots \Theta_{v-v^*}^{f_{v-v^*}} \xi = 1$$

вытекает, в силу (2), (7) и (8), следующее равенство для идеалов:

$$\frac{(\Theta' + 1)\,\mathfrak{A}\,\mathfrak{A}_1^{f_1} \dots \mathfrak{A}_{v-v^*}^{f_{v-v^*}}}{S(\Theta' + 1)\,S\mathfrak{A}\,S\mathfrak{A}_1^{f_1} \dots S\mathfrak{A}_{v-v^*}^{f_{v-v^*}}} = 1,$$

и, полагая здесь для краткости

$$\mathfrak{D} = (\Theta' + 1)\,\mathfrak{A}\,\mathfrak{A}_1^{f_1} \dots \mathfrak{A}_{v-v^*}^{f_{v-v^*}}, \tag{9}$$

получаем, наконец,

$$\mathfrak{D} = S\mathfrak{D},$$

т. е. $\mathfrak{D}$ — произведение некоторого амбивалентного идеала на некоторый идеал поля k. Следовательно, равенство (9) показывает, что идеал $\mathfrak{A}$ эквивалентен произведению некоторых идеалов из последовательности $\mathfrak{A}_1, \dots, \mathfrak{A}_{v-v^*}, \mathfrak{D}_1, \dots, \mathfrak{D}_t$ на идеал поля k. Так как амбивалентные идеалы $\mathfrak{D}_1, \dots, \mathfrak{D}_{m/2-v^*+1}$ могут быть представлены как произведения идеалов $\mathfrak{D}_{m/2-v^*+2}, \dots, \mathfrak{D}_t$, этим доказательство теоремы 23 полностью закончено.

В случае, когда μ равно произведению единицы на квадрат некоторого числа в k, данное доказательство потребует лишь незначительных видоизменений.

§ 17. Системы характеров чисел и идеалов поля K

Теперь мы обсудим вопрос о распределении классов идеалов относительного квадратичного поля $K(\sqrt{\mu})$ по родам. С этой целью обозначим через $\mathfrak{d}_1, \dots, \mathfrak{d}_t$ t простых идеалов поля k, входящих множителями в относительный дискриминант поля $K(\sqrt{\mu})$, и во всех последующих определениях и доказательствах с § 17 по § 19 *будем временно считать, что все эти простые идеалы* $\mathfrak{d}_1, \dots, \mathfrak{d}_t$ *взаимно просты с* 2, или, что в силу теоремы 5, по существу, равносильно, что число μ взаимно просто с 2 и в то же время сравнимо с квадратом некоторого целого числа из k по модулю 2^2. В ходе дальнейшего исследования мы отбросим это ограничение.

Определение 11. Любому целому отличному от 0 числу ν поля k соответствуют определенные значения t отдельных символов

$$\left(\frac{\nu,\mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\nu,\mu}{\mathfrak{d}_t}\right),$$

т. е., согласно определению 6, некоторые t единиц ± 1. Эти единицы называются *системой характеров числа ν в поле $K(\sqrt{\mu})$*.

Для того чтобы определенным образом сопоставить каждому идеалу $\mathfrak{J}$ поля $K(\sqrt{\mu})$ некоторую систему характеров, возьмем относительную норму $N(\mathfrak{J}) = \mathfrak{j}$. Ее h-я степень $\mathfrak{j}^h = (\nu)$, где ν — некоторое целое число в k. Будем далее обозначать через ξ_1 некоторую единицу в k. Тогда если для произвольной единицы ξ_1 все t символов

$$\left(\frac{\xi_1,\mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\xi_1,\mu}{\mathfrak{d}_t}\right)$$

имеют значение $+1$, то мы полагаем $r = t$ и будем называть r корней из единицы

$$\left(\frac{\nu,\mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\nu,\mu}{\mathfrak{d}_t}\right),$$

(которые определены идеалом $\mathfrak{J}$ вполне однозначно) *системой характеров идеала $\mathfrak{J}$*.

Если же в k имеется единица ε_1, для которой хотя бы один из t символов

$$\left(\frac{\varepsilon_1,\mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\varepsilon_1,\mu}{\mathfrak{d}_t}\right),$$

равен -1, то мы строим определение так. Не ограничивая общности, можно считать, что $\left(\frac{\varepsilon_1,\mu}{\mathfrak{d}_t}\right) = -1$. Рассмотрим все те единицы ξ_2 в k, для которых $\left(\frac{\xi_2,\mu}{\mathfrak{d}_t}\right) = +1$. Пусть среди них снова имеется такая единица $\xi_2 = \varepsilon_2$, для которой хотя бы один из $t-1$ символов

$$\left(\frac{\varepsilon_2,\mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\varepsilon_2,\mu}{\mathfrak{d}_{t-1}}\right)$$

равен -1; пусть, скажем, $\left(\frac{\varepsilon_2,\mu}{\mathfrak{d}_1}\right) = -1$. Далее, рассмотрим все те единицы ξ_3, для которых выполняется как равенство $\left(\frac{\xi_3,\mu}{\mathfrak{d}_1}\right) = +1$, так и равенство $\left(\frac{\xi_3,\mu}{\mathfrak{d}_{t-1}}\right) = +1$, и посмотрим, имеется ли среди них единица $\xi_3 = \varepsilon_3$, для которой хотя бы один из $t-2$ символов

$$\left(\frac{\varepsilon_3,\mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\varepsilon_3,\mu}{\mathfrak{d}_{t-2}}\right)$$

равен -1. Поступая и дальше таким же образом, мы в конце концов получим для некоторого числа r^* систему из r^* таких единиц $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r^*}$ поля k, что

после надлежащей перенумерации простых идеалов $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ выполняются равенства

$$\left.\begin{array}{llll} \left(\frac{\varepsilon_1, \mu}{\mathfrak{d}_t}\right) = -1, & & & \\ \left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_t}\right) = +1, & \left(\frac{\varepsilon_2, \mu}{\mathfrak{d}_{t-1}}\right) = -1, & & \\ \left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_t}\right) = +1, & \left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_{t-1}}\right) = +1, & \left(\frac{\varepsilon_3, \mu}{\mathfrak{d}_{t-2}}\right) = -1, & \\ \cdots & \cdots & \cdots & \cdots \\ \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_t}\right) = +1, & \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_{t-1}}\right) = +1, & \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_{t-2}}\right) = +1, \ldots & \left(\frac{\varepsilon_{r^*}, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = -1 \end{array}\right\} \quad (1)$$

и, помимо этого, для любой единицы ξ, удовлетворяющей r^* равенствам

$$\left(\frac{\xi, \mu}{\mathfrak{d}_t}\right) = +1, \quad \left(\frac{\xi, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \quad \ldots, \quad \left(\frac{\xi, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = +1,$$

обязательно и все $t - r^*$ символов

$$\left(\frac{\xi, \mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\xi, \mu}{\mathfrak{d}_{t-r^*}}\right)$$

имеют значение $+1$.

Теперь, принимая во внимание вторую формулу теоремы 14, мы можем число ν из поля k, построенное ранее по идеалу $\mathfrak{J}$, умножить на некоторые единицы $\varepsilon_1, \ldots, \varepsilon_{r^*}$ так, чтобы полученное произведение $\bar{\nu}$ удовлетворяло равенствам

$$\left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_t}\right) = +1, \quad \left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \quad \ldots, \quad \left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = +1.$$

Если $\bar{\nu}$ определено таким образом, то я буду называть $r = t - r^*$ единиц ± 1

$$\left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_1}\right), \quad \ldots, \quad \left(\frac{\bar{\nu}, \mu}{\mathfrak{d}_r}\right)$$

системой характеров идеала $\mathfrak{J}$. Эта система определяется идеалом $\mathfrak{J}$ вполне однозначно. В § 19 будет показано, что всегда $r^* < t$ и, следовательно, $r \geqslant 1$.

§ 18. Понятие рода

Мы немедленно убеждаемся в том, что все идеалы из данного класса поля $K(\sqrt{\mu})$ обладают одинаковыми системами характеров. Тем самым любому классу идеалов поля $K(\sqrt{\mu})$ соответствует некоторая определенная система характеров.

Определение 12. Мы объединяем в один *род* все те классы идеалов, которым соответствует одна и та же система характеров и все идеалы которых, следовательно, обладают одной и той же системой характеров. В частности, *главный род* определяется как совокупность всех тех классов, системы характеров которых состоят только из $+1$. Так как система

характеров главного класса обладает, очевидно, этим свойством, то главный класс всегда принадлежит главному роду.

Из второй формулы теоремы 14 мы легко получаем следующие утверждения. Если G и G' — два произвольных рода и классы G перемножить на классы G', то все такие произведения снова образуют род, который называется *произведением родов* G и G'. Его система характеров получается перемножением соответствующих характеров родов G и G'.

Любой род поля K содержит одно и то же число классов, а именно столько же классов, сколько содержит главный род. Для любого класса C относительно сопряженный класс SC принадлежит тому же роду, что и сам C. Квадрат любого класса C всегда принадлежит главному роду.

Очевидно, что все h классов произвольного комплекса P принадлежат одному и тому же роду. Я называю этот род *родом комплекса* P.

§ 19. Верхняя граница для числа родов в K

Возникает важный вопрос о том, всегда ли произвольно заданная система из r единиц ± 1 является системой характеров некоторого рода в K. Мы докажем сначала ряд вспомогательных утверждений, которые понадобятся нам, чтобы получить ответ на этот вопрос.

Теорема 24 (лемма). *Если t и v имеют тот же смысл, что и в теореме* 23, *и r, как и в* § 17, *обозначает число характеров, определяющих род класса идеалов в K, то всегда*

$$t + v - m/2 \leqslant r.$$

Доказательство. При доказательстве теорем 22 и 23 были построены v^* единиц $\eta_1, \ldots, \eta_{v^*}$ и $v - v^*$ единиц $\theta_1, \ldots, \theta_{v-v^*}$ с указанными там свойствами. Далее, пусть $\varepsilon_1, \ldots, \varepsilon_{r^*}$ — те специальные r^* единиц поля k, которые были введены в § 17; тогда $r = t - r^*$. Мы докажем сначала, что $r^* + v$ связок единиц, порожденных единицами

$$\varepsilon_1, \ldots, \varepsilon_r, \eta_1, \ldots, \eta_{v^*}, \theta_1, \ldots, \theta_{v-v^*},$$

независимы друг от друга. В самом деле, предположим, что между указанными $r^* + v$ единицами существует соотношение вида

$$\varepsilon_1^{a_1} \ldots \varepsilon_{r^*}^{a_{r^*}} \eta_1^{b_1} \ldots \eta_{v^*}^{b_{v^*}} \theta_1^{c_1} \ldots \theta_{v-v^*}^{c_{v-v^*}} = \xi^2, \tag{1}$$

в котором показатели $a_1, \ldots, a_{r^*}, b_1, \ldots, b_{v^*}, c_1, \ldots, c_{v-v^*}$ принимают значения 0 или 1, но не все равны 0, а ξ представляет собой некоторую подходящую единицу в k. Тогда для любого простого идеала $\mathfrak{w}$ поля k должно выполняться равенство

$$\left(\frac{\varepsilon_1^{a_1} \ldots \varepsilon_{r^*}^{a_{r^*}} \eta_1^{b_1} \ldots \eta_{v^*}^{b_{v^*}} \theta_1^{c_1} \ldots \theta_{v-v^*}^{c_{v-v^*}}, \mu}{\mathfrak{w}} \right) = +1,$$

и если мы учтем, что все единицы

$$\eta_1, \ldots, \eta_{v^*}, \theta_1, \ldots, \theta_{v-v^*}$$

являются относительными нормами чисел из K и, следовательно, всегда должно быть

$$\left(\frac{\eta_x, \mu}{\mathfrak{w}}\right) = +1, \qquad \left(\frac{\eta_y, \mu}{\mathfrak{w}}\right) = +1$$
$$(x = 1, 2, \ldots, v^*; \quad y = 1, 2, \ldots, v - v^*),$$

то получим

$$\left(\frac{\varepsilon_1^{a_1} \ldots \varepsilon_{r^*}^{a_{r^*}}, \mu}{\mathfrak{w}}\right) = +1.$$

Подставив здесь в качестве $\mathfrak{w}$ последовательно каждый из r^* простых идеалов $\mathfrak{d}_{t-r^*+1}, \ldots, \mathfrak{d}_t$, входящих множителями в относительный дискриминант K, придем к равенствам

$$\left(\frac{\varepsilon_1^{a_1} \ldots \varepsilon_{r^*}^{a_{r^*}}, \mu}{\mathfrak{d}_i}\right) = +1 \qquad (i = t - r^* + 1, \ldots, t). \tag{2}$$

В силу выведенной в § 17 системы формул (1) для единиц $\varepsilon_1, \ldots, \varepsilon_{r^*}$, равенства (2) могут осуществляться только в том случае, когда все показатели $a_1, \ldots, a_{r^*}$ четны и, следовательно, равны 0. Тогда соотношение (1) приобретает вид

$$\eta_1^{b_1} \ldots \eta_{v^*}^{b_{v^*}} \theta_1^{c_1} \ldots \theta_{v-v^*}^{c_{v-v^*}} = \xi^2.$$

Так как, однако, согласно § 16 порожденные $\eta_1, \ldots, \eta_{v^*}$, $\theta_1, \ldots, \theta_{v-v^*}$ связки единиц независимы, такое соотношение возможно только в том случае, когда все показатели $b_1, \ldots, b_{v^*}, c_1, \ldots, c_{v-v^*}$ четны и, следовательно, равны 0. Отсюда следует, что предположенное нами соотношение вида (1) не может иметь места, т. е. что связки, порожденные единицами $\varepsilon_1, \ldots, \varepsilon_{r^*}, \eta_1, \ldots, \eta_{v^*}$, $\theta_1, \ldots, \theta_{v-v^*}$, независимы друг от друга. При помощи умножения мы получаем из этих связок ровно 2^{r^*+v} попарно различных связок единиц в k, а так как согласно § 11 всего в k существует только $2^{m/2}$ связок единиц, то мы имеем $r^* + v \leqslant m/2$, чем и доказано утверждение теоремы 24.

Поскольку, как было замечено в конце § 15, всегда $t + v^* - m/2 > 0$ и, следовательно, тем более $t+v-m/2 > 0$, из теоремы 24 следует, в частности, что $r \geqslant 1$ и, следовательно $r^* < t$.

Теорема 25 (лемма). *Число g различных родов в поле $K(\sqrt{\mu})$ не превосходит числа* A *амбивалентных комплексов поля $K(\sqrt{\mu})$.*

Доказательство. Если g — число родов, на которые распадаются идеалы или классы идеалов поля K, то в соответствии с последним замечанием в § 18 и комплексы поля K распадаются ровно на g родов. Следовательно, если обозначить через f число комплексов главного рода, то число всех вообще комплексов, которое мы обозначим через M, равно в точности

$$M = gf.$$

Как было уже отмечено в § 18, квадрат произвольного класса C всегда принадлежит главному роду и, следовательно, квадрат произвольного комплекса является всегда комплексом главного рода. Сосредоточим теперь

наше внимание на тех комплексах главного рода, которые являются квадратами комплексов. Пусть их число равно f'. Обозначим их через $P_1, \ldots, P_{f'}$, так что $P_1 = Q_1^2, \ldots, P_{f'} = Q_{f'}^2$, где $Q_1, \ldots, Q_{f'}$ — некоторые комплексы. Очевидно, что $f' \leqslant f$. Далее, если P — произвольный комплекс, то P^2 обязательно будет совпадать с одним из уже определенных f' комплексов $P_1, \ldots, P_{f'}$, скажем с P_i. Тогда $P^2 = Q_i^2$, т. е. $(PQ_i^{-1})^2 = 1$, и в силу результатов § 12 PQ_i^{-1} совпадает с некоторым амбивалентным комплексом A. Тогда $P = AQ_i$, и, следовательно, выражение AQ_i представляет все вообще комплексы, коль скоро A пробегает все амбивалентные комплексы, а Q_i пробегает f' комплексов $Q_1, \ldots, Q_{f'}$. Ясно также, что такое представление для любого комплекса единственно. Следовательно, число всех вообще имеющихся комплексов равно

$$M = \mathrm{A}f'.$$

Сопоставление этого равенства с ранее найденным $M = gf$ дает $gf = \mathrm{A}f'$, и, поскольку $f' \leqslant f$, отсюда следует, что $g \leqslant \mathrm{A}$, чем теорема 25 и доказана.

Теперь мы в состоянии доказать следующее утверждение, которое будет играть важную роль в дальнейшем изложении.

Теорема 26 (лемма). *Если число характеров, которые определяют род классов в поле K, равно r, то число родов этого поля g всегда удовлетворяет условию*

$$g \leqslant 2^{r-1}.$$

Доказательство. По теореме 23 число A всех амбивалентных комплексов в K равно

$$\mathrm{A} = 2^a = 2^{t+v-m/2-1}.$$

По теореме 24 выполняется неравенство

$$t + v - m/2 \leqslant r,$$

следовательно,

$$\mathrm{A} \leqslant 2^{r-1}$$

откуда, в силу теоремы 25, и следует справедливость теоремы 26.

§ 20. Примарные простые идеалы $\mathfrak{p}$ и символ $\left(\frac{j}{\mathfrak{p}}\right)$

Для дальнейшего полезно ввести специальное название для одного типа простых идеалов в k.

Определение 13. *Примарным простым идеалом* поля k называется такой взаимно простой с 2 простой идеал поля k, относительно которого каждая единица k является квадратичным вычетом. Напротив, каждый простой идеал, относительно которого хотя бы одна единица в k является квадратичным невычетом, называется *непримарным*.

Для примарных простых идеалов мы введем еще один символ:

Определение 14. Пусть $\mathfrak{p}$ — примарный простой идеал и $\mathfrak{j}$ — произвольный идеал в k. Запишем $\mathfrak{j}^h = (\iota)$, где ι — некоторое целое число в k. Это число определено идеалом $\mathfrak{j}$ однозначно с точностью до некоторого единичного множителя. Поэтому значение символа $\left(\frac{\iota}{\mathfrak{p}}\right)$, равное $+1$, -1 или 0, полностью определяется идеалами $\mathfrak{p}$ и $\mathfrak{j}$. Это значение будет обозначаться через $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$, так что наш новый символ $\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)$ определен равенством

$$\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) = \left(\frac{\iota}{\mathfrak{p}}\right).$$

Если $\mathfrak{j}_1, \mathfrak{j}_2$ — некоторые взаимно простые с $\mathfrak{p}$ идеалы в k, то, очевидно, всегда выполняется равенство

$$\left(\frac{\mathfrak{j}_1\mathfrak{j}_2}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{j}_1}{\mathfrak{p}}\right)\left(\frac{\mathfrak{j}_2}{\mathfrak{p}}\right).$$

Если η — целое число в k и $\mathfrak{h} = (\eta)$ — главный идеал, представленный числом η, то, очевидно,

$$\left(\frac{\eta}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{h}}{\mathfrak{p}}\right),$$

потому что ввиду нечетности h обе стороны этого равенства имеют значение $\left(\frac{\eta^h}{\mathfrak{p}}\right)$.

В § 21 мы изучим некоторую систему из $m/2$ непримарных простых идеалов поля k, а в § 23 докажем важнейшее свойство примарных простых идеалов.

§ 21. Система из $m/2$ непримарных простых идеалов поля k

Пусть, как и в начале § 14, $\varepsilon_1, \ldots, \varepsilon_{m/2-1}$ — полная система основных единиц поля k. Далее, пусть $\varepsilon_{m/2} = \xi$ — некий определенный как в § 11 корень из единицы в k, так что, согласно § 11, произвольная единица ε поля k допускает представление, и притом единственное, в виде

$$\varepsilon = \varepsilon_1^{e_1}\varepsilon_2^{e_2}\ldots\varepsilon_{m/2}^{e_{m/2}}\xi^2,$$

где $e_1, \ldots, e_{m/2}$ принимают значения 0 или 1, а ξ — некоторая единица в k. Тогда связки поля k, порожденные $\varepsilon_1, \ldots, \varepsilon_{m/2}$, независимы, и эти $m/2$ связок образуют посредством умножения все $2^{m/2}$ связок единиц поля k.

Теорема 27[7]. *Относительный дискриминант относительного квадратичного поля $K(\sqrt{\mu})$ над k всегда отличен от 1.*

---

[7] См. «Поля алгебраических чисел», теорема 94 и замечание к ней.

Доказательство. В соответствии с замечанием, сделанным в конце § 15, мы имеем, в обозначениях теоремы 22,

$$t + v^* - m/2 > 0.$$

Так как число всех связок единиц в поле k составляет ровно $2^{m/2}$, то должно быть $m/2 \geqslant v^*$ и, следовательно, мы получаем $t > 0$. Но это и означает, что выполнено утверждение теоремы.

Теорема 28. *Если единица ε поля k сравнима с квадратом некоторого целого числа по модулю 2^2, то она сама является квадратом некоторой единицы в k.*

Доказательство. Предположим противное, т. е. что ε не является квадратом никакого числа из k. Тогда $\sqrt{\varepsilon}$ определяет некоторое относительное квадратичное поле. В силу теорем 4 и 5 это поле должно было бы иметь относительный дискриминант 1, а так как это невозможно по теореме 27, то наше предположение неверно.

Область действия теорем 27 и 28 существенно ограничена двумя специальными предположениями о поле k, сделанными в начале этой главы (с. 202). Если они не выполняются, например если k^* — числовое поле, являющееся само вещественным или обладающее вещественным сопряженным, либо если k^* имеет четное число классов, то вполне может существовать относительное квадратичное поле K^*, имеющее над k^* относительный дискриминант 1, и, более того, нахождение и изучение всех таких полей оказывается важнейшей и труднейшей из проблем, которые возникают при попытке распространения нашей теории на произвольное основное поле k^*.

Теорема 29. *Пусть $\varepsilon_1, \ldots, \varepsilon_{m/2}$ — система единиц в k, определенная в начале этого параграфа, и пусть, далее, $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$ — такие взаимно простые с 2 простые идеалы поля k, что*

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1, \qquad \left(\frac{\varepsilon_k}{\mathfrak{q}_i}\right) = +1, \qquad (i \neq k, \quad i, k = 1, 2, \ldots, m/2).$$

Запишем

$$\mathfrak{q}_1^h = (\varkappa_1), \qquad \ldots, \qquad \mathfrak{q}_{m/2}^h = (\varkappa_{m/2}),$$

где $\varkappa_1, \ldots, \varkappa_{m/2}$ — некоторые целые числа поля k. Тогда для произвольного взаимно простого с 2 целого числа ω в k выполняется по модулю 2^2 сравнение вида

$$\omega \equiv \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \alpha^2, \qquad (2^2),$$

где показатели $u_1, \ldots, u_{m/2}, v_1, \ldots, v_{m/2}$ принимают значения 0 или 1, а α — некоторая подходящая единица в k.

Доказательство. Прежде всего исследуем возможность того, что существует m таких показателей $u_1, \ldots, u_{m/2}, v_1, \ldots, v_{m/2}$, которые принимают значения 0 или 1 и притом не все равны 0, что построенное с их помощью число

$$\mu = \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \tag{1}$$

сравнимо с квадратом некоторого целого числа в k по модулю 2^2. Легко убедиться, что число $\sqrt{\mu}$ определяет относительное квадратичное поле $K(\sqrt{\mu})$ над k. Согласно теореме 5 относительный дискриминант поля $K(\sqrt{\mu})$ взаимно прост с 2, а по теореме 4 его множителями являются те из простых идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$, для которых соответствующие показатели $v_1, \ldots, v_{m/2}$ в (1) равны 1. В силу теоремы 27 число t таких простых идеалов по меньшей мере равно 1. Пусть, например, $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ — те t простых идеалов, которые содержатся в качестве множителей в относительном дискриминанте поля $K(\sqrt{\mu})$.

Пусть теперь ε — некоторая единица в k, равная относительной норме некоторой единицы из $K(\sqrt{\mu})$. Представим ε в виде

$$\varepsilon = \varepsilon_1^{e_1} \ldots \varepsilon_{m/2}^{e_{m/2}} \xi^2,$$

где показатели $e_1, \ldots, e_{m/2}$ принимают значения 0 или 1, а ξ — единица в k. Тогда, как немедленно следует из определения 6,

$$\left(\frac{\varepsilon, \mu}{\mathfrak{q}_i}\right) = +1$$

при $i = 1, 2, \ldots, t$, а так как согласно теореме 9, с учетом сделанных нами относительно $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$ предположений,

$$\left(\frac{\varepsilon, \mu}{\mathfrak{q}_i}\right) = \left(\frac{\varepsilon}{\mathfrak{q}_i}\right) = (-1)^{e_i} \qquad (i = 1, 2, \ldots, t),$$

отсюда следует, что

$$e_1 = 0, \qquad e_2 = 0, \qquad \ldots, \qquad e_t = 0,$$

т. е. единица ε должна быть произведением некоторых из $m/2 - t$ единиц $\varepsilon_{t+1}, \varepsilon_{t+2}, \ldots, \varepsilon_{m/2}$ на квадрат некоторой единицы поля k. Итак, все единицы в k, которые являются относительными нормами единиц из $K(\sqrt{\mu})$, образуют не более $2^{m/2-t}$ связок в k, откуда, в обозначениях теоремы 22, получаем

$$v^* \leqslant m/2 - t, \quad \text{или} \quad t + v^* - m/2 \leqslant 0,$$

что противоречит факту, отмеченному в конце § 15. Следовательно, наше ранее выдвинутое предположение неверно, т. е. не существует числа μ вида (1), сравнимого с квадратом некоторого целого числа в k по модулю 2^2, за исключением случая, когда все показатели

$$u_1, \ldots, u_{m/2}, v_1, \ldots, v_{m/2}$$

равны 0.

Пусть теперь $\alpha_1, \alpha_2, \ldots, \alpha_{\varphi(2)}$ — какая-нибудь полная система взаимно простых с 2 чисел в k, попарно не сравнимых по модулю 2. Тогда

$$\begin{gathered} \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \alpha_i^2 \\ (u_1, \ldots, u_{m/2}, v_1, \ldots, v_{m/2} = 0, 1; \quad i = 1, 2, 3, \ldots, \varphi(2)) \end{gathered} \tag{2}$$

представляет собой систему из $2^m \varphi(2)$ чисел, которые попарно не сравнимы по модулю 2^2. Действительно, если бы два из этих $2^m \varphi(2)$ чисел были

сравнимы по модулю 2^2, например если бы было

$$\varepsilon_1^{u_1}\dots\varepsilon_{m/2}^{u_{m/2}}\varkappa_1^{v_1}\dots\varkappa_{m/2}^{v_{m/2}}\alpha_i^2\equiv\varepsilon_1^{u'_1}\dots\varepsilon_{m/2}^{u'_{m/2}}\varkappa_1^{v'_1}\dots\varkappa_{m/2}^{v'_{m/2}}\alpha_{i'}^2,\qquad(2^2),$$

то ввиду того, что α_i и $\alpha_{i'}$ взаимно просты с 2, из ранее доказанного немедленно следовало бы, что все показатели $u_1,\dots,u_{m/2},v_1,\dots v_{m/2}$ совпадают с $u'_1,\dots,u'_{m/2},v'_1,\dots,v'_{m/2}$ соответственно, а тогда мы имели бы и

$$\alpha_i^2\equiv\alpha_{i'}^2,\qquad(2^2).\tag{3}$$

Рассмотрим теперь простой идеал $\mathfrak{l}$, входящий в 2 в качестве множителя, и предположим, что он входит в 2 точно в l-й степени. Тогда из (3) следует, что

$$(\alpha_i-\alpha_{i'})(\alpha_i+\alpha_{i'})\equiv 0,\qquad(\mathfrak{l}^{2l})$$

и, значит, либо $\alpha_i-\alpha_{i'}$, либо $\alpha_i+\alpha_{i'}$ делится на $\mathfrak{l}^l$, а так как, очевидно,

$$\alpha_i-\alpha_{i'}\equiv\alpha_i+\alpha_{i'},\qquad(2),$$

то в обоих случаях получаем

$$\alpha_i\equiv\alpha_{i'},\qquad(\mathfrak{l}^l).$$

Те же соображения остаются в силе и для любого другого входящего множителем в 2 простого идеала, поэтому мы заключаем, что

$$\alpha_i\equiv\alpha_{i'},\qquad(2),$$

откуда

$$\alpha_i=\alpha_{i'},$$

т. е. эти два числа системы (2) не были различны. Обозначим через $\mathfrak{l}_1,\dots,\mathfrak{l}_z$ различные простые идеалы поля k, входящие множителем в 2. Тогда[8)]

$$\varphi(2)=2^m\left(1-\frac{1}{n(\mathfrak{l}_1)}\right)\dots\left(1-\frac{1}{n(\mathfrak{l}_z)}\right),$$

$$\varphi(2^2)=2^{2m}\left(1-\frac{1}{n(\mathfrak{l}_1)}\right)\dots\left(1-\frac{1}{n(\mathfrak{l}_z)}\right).$$

Значит, $2^m\varphi(2)=\varphi(2^2)$, и, следовательно, числа вида (2), число которых равно $\varphi(2^2)$, образуют полную систему вычетов по модулю 2^2, взаимно простых с 2. Но это и утверждается в теореме 29.

§ 22. Бесконечный ряд $\sum_{\mathfrak{w}}\left(\frac{\mathfrak{w}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{w})^s}$

Прежде чем заняться более глубоким исследованием природы простых примарных идеалов, мы приведем два утверждения, которые примыкают к рассмотрениям § 13.

Теорема 30 (лемма). *Будем трактовать вещественные переменные $x_1,\dots,x_m$ как прямоугольные координаты в m-мерном пространстве, и пусть в этом пространстве задано конечное число*

[8)] См. «Поля алгебраических чисел», теорему 23.

семейств $(m-1)$-мерных поверхностей, описываемых уравнениями вида

$$f_1(x_1,\ldots,x_m,\tau)=0, \qquad f_2(x_1,\ldots,x_m,\tau)=0,\ldots,$$

где $f_1, f_2, \ldots$ — аналитические функции аргументов $x_1,\ldots,x_m,\tau$, регулярные в окрестности значения параметра $\tau=0$. Пусть при каждом фиксированном положительном или нулевом значении параметра τ эти поверхности ограничивают некоторую конечную часть R_τ m-мерного пространства. Зафиксируем теперь какое-нибудь положительное значение параметра τ и рассмотрим в m-мерном пространстве все точки с координатами вида

$$x_1=u_1\tau, \qquad x_2=u_2\tau, \qquad \ldots, \qquad x_m=u_m\tau,$$

где $u_1, u_2, \ldots, u_m$ пробегают все рациональные числа. Тогда число T всех таких точек, лежащих в области R_τ, дается формулой

$$T=\frac{J}{\tau^m}+\frac{M}{\tau^{m-1}},$$

где J — объем, отвечающий при $\tau=0$ области R_0, и M — некоторая зависящая от τ величина, которая изменяется лишь в конечных пределах при τ, стремящемся к 0.

Доказательство. Эта лемма представляет собой обобщение аналогичной теоремы, сформулированной и доказанной Г. Минковским[9] и Г. Вебером[10], и не составляет труда найти те видоизменения в доказательствах, которые требуются для того, чтобы установить справедливость высказанного мною только что обобщения.

Теорема 31. *Пусть $\mathfrak{p}$ — фиксированный примарный простой идеал. Тогда бесконечная сумма*

$$\sum_{(\mathfrak{w})}\left(\frac{\mathfrak{w}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{w})^s} \qquad (s>1),$$

распространенная на все простые идеалы $\mathfrak{w}$ поля k, представляет такую функцию вещественной переменной s, которая всегда остается меньше некоторой конечной положительной границы, когда вещественная переменная s приближается к 1.

Доказательство. Выберем из m сопряженных полей $k, k', \ldots, k^{(m-1)}$ такие $m/2-1$, никакие два из которых не являются комплексно-сопряженными друг к другу, и обозначим их через $k_1,\ldots,k_{m/2-1}$. Далее, если α — некоторое отличное от 0 число в k, то мы обозначим сопряженные с α лежащие в полях $k_1,\ldots,k_{m/2-1}$ числа через $\alpha_1,\ldots,\alpha_{m/2-1}$ соответственно

---

[9] Geometrie der Zahlen. — Teubner, 1896, S. 62.

[10] Über einen in der Zahlentheorie angewandten Satz der Integralrechnung. Nachr. Ges. Wiss. Göttingen, 1896, S. 275. Эту теорему Г. Вебер применил в своем исследовании «Über Zahlengruppen in algebraischen közpern» (Math. Ann., 1897, Bd. 49, S. 83) к одной задаче теории чисел, близкой к той, которую рассматриваю я.

и для краткости будем называть $m/2-1$ вещественных чисел

$$l_1(\alpha)=2\log|\alpha_1|,$$
$$l_2(\alpha)=2\log|\alpha_2|,$$
$$\dots\dots\dots\dots$$
$$l_{m/2-1}(\alpha)=2\log|\alpha_{m/2-1}|$$

логарифмами числа α. Наконец, обозначим через $\varepsilon_1,\dots,\varepsilon_{m/2-1}$ какую-нибудь систему из $m/2-1$ основных единиц в k и определим $m/2-1$ вещественных величин $e_1(\alpha),\dots,e_{m/2-1}(\alpha)$ из равенств

$$l_1(\alpha)-\frac{2}{m}\log n(\alpha)=e_1(\alpha)l_1(\varepsilon_1)+\dots+e_{m/2-1}(\alpha)l_1(\varepsilon_{m/2-1}),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$l_{m/2-1}(\alpha)-\frac{2}{m}\log n(\alpha)=e_1(\alpha)l_{m/2-1}(\varepsilon_1)+\dots+e_{m/2-1}(\alpha)l_{m/2-1}(\varepsilon_{m/2-1}).$$

Эти $m/2-1$ величин будем для краткости называть показателями числа α. Ясно, что путем умножения на целые степени единиц $\varepsilon_1,\dots,\varepsilon_{m/2-1}$ любое число α можно превратить одним и только одним способом в такое число α^*, показатели которого $e_1,\dots,e_{m/2-1}$ удовлетворяют условиям

$$0\leqslant e_1<1,\qquad 0\leqslant e_2<1,\qquad\dots,\qquad 0\leqslant e_{m/2-1}<1.$$

Наоборот, легко видеть, что две единицы с одинаковыми показателями могут отличаться только на множитель, являющийся корнем из единицы. Будем обозначать число всех лежащих в k корней из единицы через w.

Пусть теперь C — произвольный класс идеалов в k и $\mathfrak{a}$ — некоторый взаимно простой с $\mathfrak{p}$ идеал из обратного к C класса C^{-1}. Возьмем полную систему квадратичных вычетов по модулю $\mathfrak{p}$, скажем, $\varrho,\varrho',\varrho'',\dots$, и причем такую, что все $\frac{1}{2}(n(\mathfrak{p})-1)$ чисел $\varrho,\varrho',\varrho'',\dots$ делятся на $\mathfrak{a}$. Очевидно, что тогда каждое делящееся на $\mathfrak{a}$ целое число в k, которое является квадратичным вычетом по модулю $\mathfrak{p}$, может быть представлено в одной из $\frac{1}{2}(n(\mathfrak{p})-1)$ форм

$$\left.\begin{aligned}&u_1\varkappa^{(1)}+\dots+u_m\varkappa^{(m)}+\varrho,\\&u_1\varkappa^{(1)}+\dots+u_m\varkappa^{(m)}+\varrho',\\&u_1\varkappa^{(1)}+\dots+u_m\varkappa^{(m)}+\varrho'',\\&\dots\dots\dots\dots\dots\dots\end{aligned}\right\}\qquad(1)$$

где $u_1,\dots,u_m$ — некоторые целые рациональные числа и $\varkappa^{(1)},\dots,\varkappa^{(m)}$ — базисные числа идеала $\mathfrak{pa}$. Далее, пусть α — некоторый делящийся на $\mathfrak{a}$ квадратичный вычет по модулю $\mathfrak{p}$. Так как $\mathfrak{p}$ является примарным идеалом, то тем же свойством обладает число α^*, полученное умножением числа α на произвольную единицу, следовательно, α^* также представляется в одной из форм (1).

Собирая вместе эти результаты, приходим к следующему заключению: помноженное на w число $F(t)$ всех главных идеалов $\mathfrak{h}$, делящихся на $\mathfrak{a}$, для которых $\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right)=+1$ и нормы которых не превосходят вещественного

положительного числа t, равно числу T различных систем рациональных целочисленных значений $u_1,\ldots,u_m$, удовлетворяющих неравенствам

$$\left.\begin{aligned} n(u_1\varkappa^{(1)}+\ldots+u_m\varkappa^{(m)}+\varrho)&\leqslant t,\\ 0\leqslant e_1(u_1\varkappa^{(1)}+\ldots+u_m\varkappa^{(m)}+\varrho)&<1,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ 0\leqslant e_{m/2-1}(u_1\varkappa^{(1)}+\ldots+u_m\varkappa^{(m)}+\varrho)&<1,\end{aligned}\right\}\tag{2}$$

сложенному с соответствующими числами $T',T'',\ldots$, где $T^{(i)}$ обозначает число различных рациональных целочисленных систем значений $u_1,\ldots,u_m$, удовлетворяющих неравенствам

$$\left.\begin{aligned} n(u_1\varkappa^{(1)}+\ldots+u_m\varkappa^{(m)}+\varrho^{(s)})&\leqslant t,\\ 0\leqslant e_1(u_1\varkappa^{(1)}+\ldots+u_m\varkappa^{(m)}+\varrho^{(s)})&<1,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots&\\ 0\leqslant e_{m/2-1}(u_1\varkappa^{(1)}+\ldots+u_m\varkappa^{(m)}+\varrho^{(s)})&<1.\end{aligned}\right\}$$

Таким образом,

$$wF(t)=T+T'+T''\ldots$$

Прежде всего оценим T. Подставим в неравенства (2)

$$u_1=\frac{x_1}{\tau},\qquad\ldots,\qquad u_m=\frac{x_m}{\tau},\qquad \tau=t^{-1/m},$$

тогда они превратятся в следующие неравенства:

$$\left.\begin{aligned} n(x_1\varkappa^{(1)}+\ldots+x_m\varkappa^{(m)}+\varrho\tau)&\leqslant 1,\\ 0\leqslant e_1&<1,\\ \ldots\ldots\ldots&\\ 0\leqslant e_{m/2}&<1,\end{aligned}\right\}\tag{3}$$

где величины $e_1,\ldots,e_{m/2}$ определены как функции от $x_1,\ldots,x_m,\tau$ уравнениями

$$\left.\begin{aligned} &e_1l_1(\varepsilon_1)+\ldots+e_{m/2-1}l_1(\varepsilon_{m/2-1})=\\ &\quad=2\log|x_1\varkappa_1^{(1)}+\ldots+x_m\varkappa_1^{(m)}+\varrho_1\tau|-\\ &\qquad-\frac{2}{m}\log n(x_1\varkappa^{(1)}+\ldots+x_m\varkappa^{(m)}+\varrho\tau),\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &e_1l_{m/2-1}(\varepsilon_1)+\ldots+e_{m/2-1}l_{m/2-1}(\varepsilon_{m/2-1})=\\ &\quad=2\log|x_1\varkappa_{m/2-1}^{(1)}+\ldots+x_m\varkappa_{m/2-1}^{(m)}+\varrho_{m/2-1}\tau|-\\ &\qquad-\frac{2}{m}\log n(x_1\varkappa^{(1)}+\ldots+x_m\varkappa^{(m)}+\varrho\tau).\end{aligned}\right\}\tag{4}$$

Здесь $\varkappa_1^{(i)},\ldots,\varkappa_{m/2-1}^{(i)}$, $\varrho_1,\ldots,\varrho_{m/2-1}$ означают сопряженные с $\varkappa^{(i)},\varrho$ числа, лежащие в полях $k_1,\ldots,k_{m/2-1}$ соответственно. Таким образом, число T равно числу всех точек с координатами

$$x_1=u_1\tau,\qquad\ldots,\qquad x_m=u_m\tau,$$

которые попадают в область пространства $x_1, \ldots, x_m$, определенную неравенствами (3). Эта область занимает конечную часть пространства и ограничена конечным числом аналитических поверхностей. Уравнения этих поверхностей содержат еще один параметр τ, а так как их левые части регулярны при $\tau = 0$ в упомянутой области, то выполняются все предположения теоремы 30. Обозначим через J объем этой области пространства при $\tau = 0$, т. е. объем той области, которая задается неравенствами

$$n(x_1\varkappa^{(1)} + \ldots + x_m\varkappa^{(m)}) \leqslant 1,$$
$$0 \leqslant e_1 < 1,$$
$$\ldots\ldots\ldots\ldots$$
$$0 \leqslant e_{m/2-1} < 1,$$

где теперь величины $e_1, \ldots, e_{m/2-1}$ определяются как функции от $x_1, \ldots, x_m$ из уравнений

$$e_1 l_1(\varepsilon_1) + \ldots + e_{m/2-1} l_1(\varepsilon_{m/2-1}) =$$
$$= 2\log|x_1\varkappa_1^{(1)} + \ldots + x_m\varkappa_1^{(m)}| - \frac{2}{m}\log n(x_1\varkappa^{(1)} + \ldots + x_m\varkappa^{(m)}),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$e_1 l_{m/2-1}(\varepsilon_1) + \ldots + e_{m/2-1} l_{m/2-1}(\varepsilon_{m/2-1}) =$$
$$= 2\log|x_1\varkappa_{m/2-1}^{(1)} + \ldots + x_m\varkappa_{m/2-1}^{(m)}| - \frac{2}{m}\log n(x_1\varkappa^{(1)} + \ldots + x_m\varkappa^{(m)}).$$

По теореме 30 число T точек с координатами

$$x_1 = u_1\tau, \qquad \ldots, \qquad x_m = u_m\tau,$$

попадающих в задаваемую посредством (3) область пространства $x_1 \ldots x_m$, представляется формулой

$$T = \frac{J}{\tau^m} + \frac{M}{\tau^{m-1}} = Jt + Mt^{1-1/m},$$

где M — некоторая зависящая от t величина, которая остается заключенной между некоторыми конечными границами при бесконечно возрастающем t. Равным образом

$$T' = Jt + M't^{1-1/m},$$
$$T'' = Jt + M''t^{1-1/m},$$
$$\ldots\ldots\ldots\ldots$$

где $M', M'', \ldots$ — также величины, зависящие от t и остающиеся заключенными между некоторыми конечными границами при бесконечно возрастающем t. Складывая все эти формулы, находим, что

$$T + T' + T'' + \ldots = \frac{n(\mathfrak{p}) - 1}{2} Jt + (M + M' + M'' + \ldots)\, t^{1-1/m}$$

и, следовательно,

$$F(t) = \frac{1}{w}\frac{n(\mathfrak{p}) - 1}{2} Jt + \frac{1}{w}(M + M' + M'' + \ldots)\, t^{1-1/m}. \qquad (5)$$

Таким же способом мы получаем для числа $G(t)$ всех делящихся на $\mathfrak{a}$ главных идеалов $\mathfrak{h}$ поля k, с нормами, не превосходящими вещественного положительного числа t, для которых $\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) = -1$, равенство

$$G(t) = \frac{1}{w}\frac{n(\mathfrak{p})-1}{2}Jt + \frac{1}{w}(N + N' + N'' + \ldots)t^{1-1/m}, \tag{6}$$

где $N, N', N'', \ldots$ снова суть зависящие от t величины, которые при бесконечно растущем t остаются заключенными между некоторыми конечными границами. Вычитая формулу (6) из (5), приходим к равенству

$$\Phi(t) = F(t) - G(t) = Dt^{1-1/m}, \tag{7}$$

где D — снова некоторая зависящая от t величина, изменяющаяся лишь в конечных пределах при неограниченно растущем t.

Очевидно, что

$$\sum_{(\mathfrak{h})}\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{h})^s} = \sum_{(\mathfrak{h}^{(+)})}\frac{1}{n(\mathfrak{h}^{(+)})^s} - \sum_{(\mathfrak{h}^{(-)})}\frac{1}{n(\mathfrak{h}^{(-)})^s} \qquad (s>1),$$

где сумма слева распространяется на все взаимно простые с $\mathfrak{p}$ и делящиеся на $\mathfrak{a}$ главные идеалы $\mathfrak{h}$ поля k, а справа первая сумма берется по всем взаимно простым с $\mathfrak{p}$ и делящимся на $\mathfrak{a}$ главным идеалам $\mathfrak{h}^{(+)}$, обладающим свойством $\left(\frac{\mathfrak{h}^{(+)}}{\mathfrak{p}}\right) = +1$, а вторая сумма — по всем взаимно простым с $\mathfrak{p}$ и делящимся на $\mathfrak{a}$ главным идеалам $\mathfrak{h}^{(-)}$ со свойством $\left(\frac{\mathfrak{h}^{(-)}}{\mathfrak{p}}\right) = -1$. С другой стороны, принимая во внимание смысл чисел $F(t)$, $G(t)$, мы имеем

$$\sum_{(\mathfrak{h}^{(+)})}\frac{1}{n(\mathfrak{h}^{(+)})^s} = \sum_{(t)}\frac{F(t)-F(t-1)}{t^s} \qquad (s>1),$$

$$\sum_{(\mathfrak{h}^{(-)})}\frac{1}{n(\mathfrak{h}^{(-)})^s} = \sum_{(t)}\frac{G(t)-G(t-1)}{t^s} \qquad (s>1)$$

и, следовательно,

$$\sum_{(\mathfrak{h})}\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{h})^s} = \sum_{(t)}\frac{\Phi(t)-\Phi(t-1)}{t^s} \qquad (s>1), \tag{8}$$

где сумма справа берется по $t = 1, 2, 3, \ldots$ и считается, что $F(0)$, $G(0)$, $\Phi(0)$ равны нулю. Но

$$\sum_{(t)}\frac{\Phi(t)-\Phi(t-1)}{t^s} = \sum_{(t)}\Phi(t)\left(\frac{1}{t^s} - \frac{1}{(t+1)^s}\right),$$

а так как при $t > 0$, $s > 1$

$$\frac{1}{t^s} - \frac{1}{(t+1)^s} = \frac{1}{t^s}\left\{1 - \left(1 + \frac{1}{t}\right)^{-s}\right\},$$

$$\left(1 + \frac{1}{t}\right)^{-s} = 1 - \frac{s\theta}{t} \qquad (0 < \theta < 1),$$

то мы получаем, далее,

$$\sum_{(t)} \frac{\Phi(t) - \Phi(t-1)}{t^s} = \sum_{(t)} \Phi(t) \frac{s\theta}{t^{s+1}} \qquad (0 < \theta < 1),$$

откуда в силу (7) и (8) следует, что

$$\sum_{(\mathfrak{h})} \left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{h})^s} = \sum_{(t)} \frac{s\theta D}{t^{s+1/m}} \qquad (s > 1). \tag{9}$$

Так как по ранее доказанному величина D остается заключенной между некоторыми конечными границами при неограниченно возрастающем t, и значение бесконечного ряда

$$\sum_{(t)} \frac{1}{t^{s+1/m}}$$

стремится к некоторому конечному пределу при s, стремящемуся к 1, из (9) следует, что бесконечная сумма

$$\sum_{(\mathfrak{h})} \left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{h})^s} \qquad (s > 1) \tag{10}$$

также представляет функцию от s, стремящуюся к некоторому конечному значению при s, стремящемся к 1.

Запишем $\mathfrak{h}$ в (10) в виде $\mathfrak{h} = \mathfrak{a} \cdot \mathfrak{j}$. Взаимно простой с $\mathfrak{p}$ идеал $\mathfrak{j}$ принадлежит классу C, и, учитывая, что

$$\left(\frac{\mathfrak{h}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{a}}{\mathfrak{p}}\right)\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right),$$

мы заключаем на основании только что доказанного факта, что бесконечная сумма

$$\sum_{(\mathfrak{j})} \left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{j})^s} \qquad (s > 1), \tag{11}$$

распространенная на все идеалы $\mathfrak{j}$ класса C, взаимно простые с $\mathfrak{p}$, снова представляет функцию от s, стремящуюся к некоторому конечному значению при s, стремящемся к 1. Образуем теперь бесконечные суммы, аналогичные выражению (11), используя h различных классов поля k, и сложим все полученные таким образом h бесконечных сумм. Тогда мы убедимся, что и бесконечная сумма

$$\sum_{(\mathfrak{j})} \left(\frac{\mathfrak{j}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{j})^s} \qquad (s > 1), \tag{12}$$

распространенная на все взаимно простые с $\mathfrak{p}$ идеалы $\mathfrak{j}$ поля k, сходится к некоторому конечному предельному значению при s, стремящемся к 1.

Наконец,

$$\sum_{(\mathfrak{j})}\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{j})^s}=\prod_{(\mathfrak{w})}\frac{1}{1-\left(\frac{\mathfrak{w}}{\mathfrak{p}}\right)n(\mathfrak{w})^{-1}},$$

где произведение $\prod_{(\mathfrak{w})}$ распространено на все простые идеалы $\mathfrak{w}$ поля k, и, следовательно, мы получаем

$$\log\sum_{(\mathfrak{j})}\left(\frac{\mathfrak{j}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{j})^s}=\sum_{(\mathfrak{w})}\left(\frac{\mathfrak{w}}{\mathfrak{p}}\right)\frac{1}{n(\mathfrak{w})^s}+f(s)\qquad(s>1),\tag{13}$$

где сумма $\sum_{(\mathfrak{w})}$ снова распространяется на все простые идеалы $\mathfrak{w}$ поля k и где $f(s)$ представляет собой величину, стремящуюся к некоторому конечному пределу при s, стремящемся к 1. Так как (12) стремится к конечному предельному значению при s, стремящемся к 1, то и (13) должно при s, стремящемся к 1, либо тоже стремиться к некоторому конечному предельному значению, либо становиться меньше любого отрицательного числа. В обоих случаях ясно, что доказываемое утверждение справедливо.

§ 23. Одно свойство примарных простых идеалов

Теоремы 29 и 31 приводят нас к следующей важной теореме о простых примарных идеалах.

Теорема 32. *Если $\mathfrak{p}$ — примарный простой идеал, то всегда возможно найти в поле k такое целое число π, что идеал (π) равен $\mathfrak{p}^h$ и, сверх того, число π удовлетворяет по модулю 2^2 сравнению вида*

$$\pi\equiv\alpha^2,\qquad(2^2),$$

где α — некоторое подходящее целое число поля k.

Доказательство. Пусть $\varepsilon_1,\ldots,\varepsilon_{m/2}$ — система единиц в k, построенная в начале § 21. Далее, пусть, как и в теореме 29, $\mathfrak{q}_1,\ldots,\mathfrak{q}_{m/2}$ — такие простые идеалы поля k, взаимно простые с 2, для которых выполняется

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right)=-1,\qquad\left(\frac{\varepsilon_k}{\mathfrak{q}_i}\right)=+1,\qquad(i\neq k,\quad i,k=1,2,\ldots,m/2).$$

Существование таких простых идеалов следует из теоремы 18. Запишем

$$\mathfrak{p}^h=(\pi^*),\qquad\mathfrak{q}_1^h=(\varkappa_1),\qquad\ldots,\qquad\mathfrak{q}_{m/2}^h=(\varkappa_{m/2}),$$

так что $\pi^*,\varkappa_1,\ldots,\varkappa_{m/2}$ — некоторые целые числа поля k. Теперь мы применим теорему 29 к этому целому числу π^*. Получим, что π^* удовлетворяет сравнению вида

$$\pi^*\equiv\varepsilon\varkappa_1^{v_1}\ldots\varkappa_{m/2}^{v_{m/2}}\alpha^2,\qquad(2^2),\tag{1}$$

где ε — некоторая подходящая единица в k и где, далее, показатели $v_1, \ldots, v_{m/2}$ принимают значения 0 или 1, а α — подходящее целое число в k. В случае когда все показатели $v_1, \ldots, v_{m/2}$ в правой части сравнения (1) имеют нулевые значения, уже $\pi = \pi^*\varepsilon$ было бы числом такого вида, как требуется в теореме. Итак, мы предположим, что число e тех из показателей $v_1, \ldots, v_{m/2}$, которые равны 1, больше 0.

Запишем

$$\mu = \pi^*\varepsilon\varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}}.$$

По теореме 5 относительное квадратичное поле $K(\sqrt{\mu})$ обладает взаимно простым с 2 относительным дискриминантом. Для этого случая мы располагаем уже теоремой 26. Сохраняя обозначения, использованные в определении 11, имеем, очевидно,

$$t = e + 1, \qquad r^* = e, \qquad r = t - r^* = 1.$$

Следовательно, по теореме 26 число родов g поля $K(\sqrt{\mu})$ не превосходит 1 и, значит, равно 1, т. е. все классы идеалов поля $K(\sqrt{\mu})$ принадлежат главному роду.

Из только что доказанного обстоятельства мы выводим следующее заключение. Пусть $\mathfrak{r}$ — некоторый взаимно простой с 2 простой идеал в k, обладающий свойством

$$\left(\frac{\mu}{\mathfrak{r}}\right) = +1,$$

так что по теореме 7 $\mathfrak{r}$ распадается в $K(\sqrt{\mu})$ в произведение двух простых идеалов $\mathfrak{R}$ и $S\mathfrak{R}$. Если $\mathfrak{R}$ принадлежит главному роду, то система характеров этого простого идеала в поле $K(\sqrt{\mu})$ должна состоять из одних единиц $+1$. Следовательно, и система характеров числа $\xi\varrho$, где ξ — некоторая подходящая единица в k и ϱ — целое число в k со свойством $\mathfrak{r}^h = (\varrho)$, должна состоять из одних единиц $+1$. Взяв, в частности, характер числа относительно простого идеала $\mathfrak{p}$, входящего множителем в относительный дискриминант $K(\sqrt{\mu})$, получим

$$\left(\frac{\xi\varrho, \mu}{\mathfrak{p}}\right) = \left(\frac{\xi\varrho}{\mathfrak{p}}\right) = +1,$$

а если мы учтем, что $\mathfrak{p}$ — примарный простой идеал, то придем к равенству

$$\left(\frac{\xi\varrho}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{r}}{\mathfrak{p}}\right) = +1,$$

т. е. любой простой идеал $\mathfrak{r}$, для которого $\left(\frac{\mu}{\mathfrak{r}}\right) = +1$, обладает также тем свойством, что $\left(\frac{\mathfrak{r}}{\mathfrak{p}}\right) = +1$.

Теперь мы определим вместо простых идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$ какие-либо другие $m/2$ простых идеалов $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{m/2}$ с аналогичными свойствами

$$\left(\frac{\varepsilon_i}{\mathfrak{q}'_i}\right) = -1, \qquad \left(\frac{\varepsilon_k}{\mathfrak{q}'_i}\right) = +1 \qquad (i \neq k, \quad i, k = 1, 2, \ldots, m/2)$$

и снова запишем $\mathfrak{q}_1'^h = (\varkappa'_1), \ldots, \mathfrak{q}_{m/2}'^h = (\varkappa'_{m/2})$, где $\varkappa'_1, \ldots, \varkappa'_{m/2}$ — целые числа в k. Проводя те же рассуждения для этой новой системы простых

идеалов $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{m/2}$, мы приходим к сравнению

$$\mu' = \pi^* \varepsilon' \varkappa_1'^{v'_1} \ldots \varkappa_{m/2}'^{v'_{m/2}} \equiv \alpha'^2, \qquad (2^2),$$

в котором ε' — некоторая единица и показатели $v'_1, \ldots, v'_{m/2}$ принимают значения 0 или 1. Если бы здесь все показатели имели значение 0, то число $\pi = \pi^* \varepsilon'$ снова было бы такого вида, как требуется в теореме 32. Итак, мы предположим, что не все показатели $v'_1, \ldots, v'_{m/2}$ равны 0, и в таком случае придем, как и раньше, к выводу, что любой простой идеал $\mathfrak{r}$, для которого $\left(\frac{\mu'}{\mathfrak{r}}\right) = +1$, обладает также тем свойством, что $\left(\frac{\mathfrak{r}}{\mathfrak{p}}\right) = +1$.

Обозначим теперь для краткости через $\mathfrak{r}_\mu$ все те простые идеалы в k, для которых

$$\left(\frac{\mu}{\mathfrak{r}_\mu}\right) = +1,$$

а через $\mathfrak{r}_{\mu\mu'}$ — все те простые идеалы в k, для которых одновременно

$$\left(\frac{\mu}{\mathfrak{r}_{\mu\mu'}}\right) = -1 \quad \text{и} \quad \left(\frac{\mu'}{\mathfrak{r}_{\mu\mu'}}\right) = +1.$$

Далее, через $\mathfrak{r}_\mathfrak{p}^{(+)}$, $\mathfrak{r}_\mathfrak{p}^{(-)}$ обозначим те простые идеалы, для которых

$$\left(\frac{\mathfrak{r}_\mathfrak{p}^{(+)}}{\mathfrak{p}}\right) = +1 \quad \text{и} \quad \left(\frac{\mathfrak{r}_\mathfrak{p}^{(-)}}{\mathfrak{p}}\right) = -1$$

соответственно. Так как числа μ и μ' заведомо не являются квадратами целых чисел в k и в силу наших предположений то же верно и для произведения $\mu\mu'$, из теоремы 17 следуют равенства

$$\left.\begin{aligned} \sum_{(\mathfrak{r}_\mu)} \frac{1}{n(\mathfrak{r}_\mu)^s} &= \frac{1}{2} \log \frac{1}{s-1} + f_\mu(s), \\ \sum_{(\mathfrak{r}_{\mu\mu'})} \frac{1}{n(\mathfrak{r}_{\mu\mu'})^s} &= \frac{1}{4} \log \frac{1}{s-1} + f_{\mu\mu'}(s). \end{aligned}\right\} \qquad (s > 1). \qquad (2)$$

Здесь бесконечные суммы распространяются на все простые идеалы $\mathfrak{r}_\mu$ и $\mathfrak{r}_{\mu\mu'}$ соответственно, а $f_\mu(s)$, $f_{\mu\mu'}(s)$ суть функции вещественной переменной s, которые остаются заключенными между некоторыми конечными границами, когда s приближается к значению 1.

Очевидно, что все простые идеалы $\mathfrak{r}_\mu$ отличны от простых идеалов $\mathfrak{r}_{\mu\mu'}$, а так как по ранее доказанному все простые идеалы $\mathfrak{r}_\mu$, $\mathfrak{r}_{\mu\mu'}$ входят в число простых идеалов $\mathfrak{r}_\mathfrak{p}^{(+)}$, то мы имеем

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} \geqslant \sum_{(\mathfrak{r}_\mu)} \frac{1}{n(\mathfrak{r}_\mu)^s} + \sum_{(\mathfrak{r}_{\mu\mu'})} \frac{1}{n(\mathfrak{r}_{\mu\mu'})^s}$$

и, следовательно, в силу (2)

$$\sum_{(\mathfrak{r}_\mathfrak{p}^{(+)})} \frac{1}{n(\mathfrak{r}_\mathfrak{p}^{(+)})^s} \geqslant \frac{3}{4} \log \frac{1}{s-1} + f_\mu(s) + f_{\mu\mu'}(s); \qquad (3)$$

здесь снова бесконечная сумма распространяется на все простые идеалы с соответствующими свойствами.

Очевидно, что простыми идеалами $\mathfrak{r}_{\mathfrak{p}}^{(+)}, \mathfrak{r}_{\mathfrak{p}}^{(-)}$ исчерпываются все простые идеалы $\mathfrak{w}$ в k, помимо простого идеала $\mathfrak{p}$, и, следовательно,

$$\sum_{(\mathfrak{r}_{\mathfrak{p}}^{(+)})} \frac{1}{n(\mathfrak{r}_{\mathfrak{p}}^{(+)})^s} + \sum_{(\mathfrak{r}_{\mathfrak{p}}^{(-)})} \frac{1}{n(\mathfrak{r}_{\mathfrak{p}}^{(-)})^s} = -\frac{1}{n(\mathfrak{p})^s} + \sum_{(\mathfrak{w})} \frac{1}{n(\mathfrak{w})^s} = \log \frac{1}{s-1} + f(s), \quad (4)$$

где сумма $\sum_{(\mathfrak{w})}$ распространяется на все простые идеалы в k и снова $f(s)$ — величина, остающаяся заключенной между конечными границами при s, стремящемся к 1. Из (3) и (4) следует неравенство

$$\sum_{(\mathfrak{r}_{\mathfrak{p}}^{(+)})} \frac{1}{n(\mathfrak{r}_{\mathfrak{p}}^{(+)})^s} - \sum_{(\mathfrak{r}_{\mathfrak{p}}^{(-)})} \frac{1}{n(\mathfrak{r}_{\mathfrak{p}}^{(-)})^s} \geqslant \frac{1}{2} \log \frac{1}{s-1} + 2f_{\mu}(s) + 2f_{\mu\mu'}(s) - f(s). \quad (5)$$

Ввиду того что

$$\sum_{(\mathfrak{r}_{\mathfrak{p}}^{(+)})} \frac{1}{n(\mathfrak{r}_{\mathfrak{p}}^{(+)})^s} - \sum_{(\mathfrak{r}_{\mathfrak{p}}^{(-)})} \frac{1}{n(\mathfrak{r}_{\mathfrak{p}}^{(-)})^s} = \sum_{(\mathfrak{w})} \left(\frac{\mathfrak{w}}{\mathfrak{p}}\right) \frac{1}{n(\mathfrak{w})^s},$$

неравенство (5) непосредственно противоречит теореме 31, и, следовательно, наши предположения следует отвергнуть, т. е. либо показатели $v_1, \ldots, v_{m/2}$ в сравнении (1) все равны 0, либо же все показатели $v_1', \ldots, v_{m/2}'$ в соответствующем сравнении равны 0, но тогда, как было уже отмечено, либо $\pi = \pi^* \varepsilon$ либо $\pi = \pi^* \varepsilon'$ является таким числом, какое требуется в нашей теореме. Тем самым справедливость теоремы установлена.

Теорема, обратная к теореме 32, тоже справедлива.

Теорема 33. *Если π — целое число в k, сравнимое с квадратом некоторого целого числа в k по модулю 2^2, и если, сверх того, идеал (π) равен $\mathfrak{p}^h$, где $\mathfrak{p}$ — некоторый простой идеал в k, то $\mathfrak{p}$ — примарный простой идеал.*

Доказательство. Рассмотрим поле $K(\sqrt{\pi})$. По теоремам 4 и 5 относительный дискриминант этого поля обладает лишь одним простым множителем $\mathfrak{p}$. В силу теоремы 22 и замечания в конце § 15 получаем, используя обозначения указанной теоремы 22 для поля $K(\sqrt{\pi})$ и учитывая, что $t = 1$, неравенство

$$1 + v^* - m/2 > 0, \quad \text{т. е.} \quad v^* \geqslant m/2.$$

Так как с другой стороны, согласно результатам § 11 v^* не может быть больше чем $m/2$, заключаем, что $v^* = m/2$. Следовательно, каждая единица ξ в k является относительной нормой некоторой единицы поля $K(\sqrt{\pi})$, откуда по теореме 9 следует, что

$$\left(\frac{\xi, \pi}{\mathfrak{p}}\right) = \left(\frac{\xi}{\mathfrak{p}}\right) = +1,$$

т. е. $\mathfrak{p}$ является примарным простым идеалом.

§ 24. Два частных случая закона взаимности для квадратичных вычетов в поле k

На основании теоремы 32 мы можем ввести следующее новое определение.

Определение 15. Если $\mathfrak{p}$ — примарный простой идеал в k и $\mathfrak{p}^h = (\pi)$, где π — целое число в k, сравнимое с квадратом некоторого целого числа в k по модулю 2^2, то я называю π *примарным числом примарного простого идеала* $\mathfrak{p}$. В силу теоремы 28 это примарное число π определяется примарным простым идеалом $\mathfrak{p}$ с точностью до квадрата некоторой единицы в k.

Теорема 34. *Пусть* $\mathfrak{p}$ — *примарный простой идеал в* k *и* $\mathfrak{r}$ — *произвольный простой идеал в* k; *далее, пусть* π — *примарное число идеала* $\mathfrak{p}$ *и* ϱ — *такое целое число в* k, *что* $(\varrho) = \mathfrak{r}^h$. *Тогда если* $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$, *то и* $\left(\frac{\varrho}{\mathfrak{p}}\right) = +1$.

Доказательство. Учитывая определение 15, получаем в силу теорем 4 и 5, что относительный дискриминант поля $K(\sqrt{\pi})$ обладает единственным простым множителем $\mathfrak{p}$. Следовательно, по теореме 26, число родов в этом относительном поле равно 1, т. е. все идеалы поля $K(\sqrt{\pi})$ принадлежат главному роду. Ввиду предположения $\left(\frac{\pi}{\mathfrak{r}}\right) = +1$ идеал $\mathfrak{r}$ распадается в $K(\sqrt{\pi})$, по теореме 7, в произведение двух простых идеалов. Для характера любого из этих двух простых идеалов мы получаем значение

$$\left(\frac{\varrho, \pi}{\mathfrak{p}}\right) = \left(\frac{\varrho}{\mathfrak{p}}\right) = +1,$$

чем теорема 34 и доказана.

Теорема 35. *Если* $\mathfrak{p}, \mathfrak{p}^*$ — *два примарных простых идеала в* k *и* π, π^* — *примарные числа для* $\mathfrak{p}, \mathfrak{p}^*$ *соответственно, то имеет место равенство*

$$\left(\frac{\pi}{\mathfrak{p}^*}\right) = \left(\frac{\pi^*}{\mathfrak{p}}\right).$$

Доказательство. В случае когда $\left(\frac{\pi}{\mathfrak{p}^*}\right) = +1$, справедливость этой теоремы непосредственно следует из теоремы 34. Итак, $\left(\frac{\pi}{\mathfrak{p}^*}\right) = -1$. Тогда обязательно должно быть и $\left(\frac{\pi^*}{\mathfrak{p}}\right) = -1$; действительно, если бы было $\left(\frac{\pi^*}{\mathfrak{p}}\right) = +1$, то по той же теореме 34 мы должны были бы иметь $\left(\frac{\pi}{\mathfrak{p}^*}\right) = +1$, что противоречит нашему предположению.

§ 25. Произведение $\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ для ν, взаимно простого с 2, и при некоторых предположениях относительно μ

Теперь мы в состоянии получить еще одну важную составную часть закона взаимности для квадратичных вычетов в поле k.

Теорема 36. *Если ν, μ — два целых числа в k, взаимно простых с 2, и, сверх того, число μ сравнимо с квадратом некоторого целого числа в k по модулю 2^2, то всегда*

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = +1,$$

где произведение распространяется на все взаимно простые с 2 простые идеалы $\mathfrak{w}$ поля k.

Доказательство. В качестве *первого* шага рассмотрим случай, когда ν есть некоторое число $\varkappa$ поля k, обладающее тем свойством, что идеал $(\varkappa)$ является h-й степенью некоторого непримарного простого идеала q в k; число же μ пусть представляет собой произведение исключительно степеней примарных идеалов. Пусть, далее, $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ — те из простых множителей μ, которые входят в μ в нечетной степени. Тогда, обозначая через $\delta_1, \ldots, \delta_t$ примарные числа для $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ соответственно и применяя теорему 28, мы без труда получаем равенство

$$\mu^h = \delta_1 \ldots \delta_t \alpha^2, \tag{1}$$

где α — некоторое подходящее целое число в k. Рассмотрим поле $K(\sqrt{\mu})$; по теореме 4 идеалы $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ являются простыми идеалами, входящими в качестве множителей в относительный дискриминант поля $K(\sqrt{\mu})$. Так как все эти t простых идеалов примарны и, следовательно, для любой единицы ξ

$$\left(\frac{\xi,\mu}{\mathfrak{d}_i}\right) = \left(\frac{\xi}{\mathfrak{d}_i}\right) = +1 \qquad (i = 1, 2, \ldots, t),$$

то число $r = t$ совпадает с числом характеров, определяющих род данного класса в поле $K(\sqrt{\mu})$. По теореме 26 в $K(\sqrt{\mu})$ существует не более 2^{t-1} родов.

Покажем теперь, что в поле $K(\sqrt{\mu})$ действительно имеется 2^{t-1} родов. С этой целью обозначим через $c_1, \ldots, c_t$ какие-либо t единиц ± 1, произведение которых равно $+1$, и рассмотрим простой идеал $\mathfrak{p}$ в k, удовлетворяющий условиям

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = +1, \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right) = +1, \tag{2}$$

или

$$\left(\frac{\delta_1}{\mathfrak{p}}\right) = c_1, \quad \ldots, \quad \left(\frac{\delta_t}{\mathfrak{p}}\right) = c_t, \tag{3}$$

где $\varepsilon_1, \ldots, \varepsilon_{m/2}$ — система единиц в k, построенная в начале § 21; существование простого идеала $\mathfrak{p}$ с требуемыми свойствами обеспечивается теоремой 18. Ввиду (2) $\mathfrak{p}$ является примарным простым идеалом; пусть π —

примарное число для $\mathfrak{p}$. Согласно теореме 35, из равенств (3) следуют равенства

$$\left(\frac{\pi}{\mathfrak{d}_1}\right)=c_1,\qquad \ldots,\qquad \left(\frac{\pi}{\mathfrak{d}_t}\right)=c_t. \tag{4}$$

Перемножив равенства (3) между собой, получим ввиду (1) и ввиду того, что $c_1\ldots c_t=+1$,

$$\left(\frac{\delta_1\ldots\delta_t}{\mathfrak{p}}\right)=\left(\frac{\mu}{\mathfrak{p}}\right)=+1,$$

т. е. $\mathfrak{p}$ распадается в поле $K(\sqrt{\mu})$ на два простых множителя. В силу (4) характеры любого из этих простых множителей совпадают с $c_1,\ldots,c_t$. Очевидно, что число возможных систем единиц $c_1,\ldots,c_t$ с $c_1\ldots c_t=+1$ равно 2^{t-1}; следовательно, столько родов существует на самом деле, а так как по ранее доказанному большего числа родов быть не может, мы заключаем, что система характеров $c_1,\ldots,c_t$ произвольного рода в поле $K(\sqrt{\mu})$ должна удовлетворять условию $c_1\ldots c_t=+1$.

Выведем из этого факта утверждение теоремы при сделанных в начале данного первого шага доказательства предположениях. Пусть сначала $\left(\frac{\mu}{\mathfrak{q}}\right)=+1$. Тогда $\mathfrak{q}$ распадается в $K(\sqrt{\mu})$ на два простых множителя и система характеров каждого из этих простых множителей совпадает с

$$\left(\frac{\varkappa,\mu}{\mathfrak{d}_1}\right)=\left(\frac{\varkappa}{\mathfrak{d}_1}\right),\qquad \ldots,\qquad \left(\frac{\varkappa,\mu}{\mathfrak{d}_t}\right)=\left(\frac{\varkappa}{\mathfrak{d}_t}\right).$$

Так как по ранее доказанному произведение этих характеров должно быть равно $+1$ и так как

$$\left(\frac{\varkappa,\mu}{\mathfrak{q}}\right)=\left(\frac{\mu}{\mathfrak{q}}\right)=+1,$$

должно выполняться равенство

$$\prod_{(\mathfrak{w})}'\left(\frac{\varkappa,\mu}{\mathfrak{w}}\right)=+1,$$

где произведение распространяется на все взаимно простые с 2 простые идеалы $\mathfrak{w}$ поля k. Тем самым справедливость нашего утверждения доказана.

Теперь пусть $\left(\frac{\mu}{\mathfrak{q}}\right)=-1$. Найдем примарный простой идеал $\mathfrak{p}$, отличный от $\mathfrak{d}_1,\ldots,\mathfrak{d}_t$ и такой, что $\left(\frac{\varkappa}{\mathfrak{p}}\right)=-1$; это всегда возможно в силу теоремы 18. Обозначим через π примарное число для $\mathfrak{p}$. Тогда обязательно должно быть также $\left(\frac{\pi}{\mathfrak{q}}\right)=-1$, так как в противном случае из теоремы 34 следовало бы, что $\left(\frac{\varkappa}{\mathfrak{p}}\right)=+1$. Далее, $\left(\frac{\mu\pi}{\mathfrak{q}}\right)=+1$, и если мы в предыдущем рассуждении заменим μ на $\mu\pi$, то точно так же получим равенство

$$\prod_{(w)}'\left(\frac{\varkappa,\mu\pi}{\mathfrak{w}}\right)=+1.$$

Однако

$$\prod_{(w)}{}'\left(\frac{\varkappa, \pi}{\mathfrak{w}}\right) = \left(\frac{\varkappa}{\mathfrak{p}}\right)\left(\frac{\pi}{\mathfrak{q}}\right) = +1$$

и, следовательно,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa, \mu}{\mathfrak{q}}\right) = +1, \tag{5}$$

чем и доказано утверждение нашей теоремы при сделанных на данном шаге предположениях.

Применяя формулу (5), в частности, к случаю, когда μ есть примарное число π некоторого примарного простого идеала $\mathfrak{p}$, получим равенство

$$\prod_{(\mathfrak{w})}\left(\frac{\varkappa, \pi}{\mathfrak{w}}\right) = \left(\frac{\varkappa}{\mathfrak{p}}\right)\left(\frac{\pi}{\mathfrak{q}}\right) = +1; \tag{6}$$

следовательно, всегда

$$\left(\frac{\varkappa}{\mathfrak{p}}\right) = \left(\frac{\pi}{\mathfrak{q}}\right). \tag{7}$$

На втором шаге рассмотрим случай, когда ν есть примарное число π некоторого примарного простого идеала $\mathfrak{p}$, а число μ может содержать в качестве множителя как примарные, так и непримарные простые идеалы. Запишем $(\mu) = \mathfrak{r}_1, \mathfrak{r}_2, \ldots$, где $\mathfrak{r}_1, \mathfrak{r}_2, \ldots$ — простые идеалы, и обозначим через $\varrho_1, \varrho_2, \ldots$ такие целые числа в k, что

$$(\varrho_1) = \mathfrak{r}_1^h, \qquad (\varrho_2) = \mathfrak{r}_2^h, \qquad \ldots$$

Тогда

$$\mu^h = \eta\varrho_1\varrho_2\ldots,$$

где η — некоторая единица в k. Применяя третью формулу теоремы 14, получаем

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu^h}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \eta}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \varrho_1}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \varrho_2}{\mathfrak{w}}\right)\ldots \tag{8}$$

С другой стороны, в силу теоремы 13

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \eta}{\mathfrak{w}}\right) = \left(\frac{\eta}{\mathfrak{p}}\right) = +1. \tag{9}$$

Далее, имеют место равенства

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \varrho_i}{\mathfrak{r}}\right) = \left(\frac{\varrho_i}{\mathfrak{p}}\right)\left(\frac{\pi}{r_i}\right) = +1 \qquad (i = 1, 2, \ldots), \tag{10}$$

что для примарных $\mathfrak{r}_i$ следует из теоремы 35, а для непримарных — из формулы (6). Равенство (8) вместе с (9) и (10) приводит к равенству

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\pi, \mu}{\mathfrak{w}}\right) = +1, \tag{11}$$

чем и доказана справедливость теоремы 36 для рассматриваемого случая.

В качестве третьего шага разберем случай, когда ν равно некоторой единице ε в k, а μ может включать в себя как множители произвольные, примарные или непримарные, простые идеалы. Рассмотрим относительное поле $K(\sqrt{\mu})$. Обозначим, как и на первом шаге, через $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ те из простых множителей μ, которые входят в μ в нечетной степени, и пусть $\delta_1, \ldots \delta_t$ — такие целые числа в k, что

$$(\delta_1) = \mathfrak{d}_1^h, \qquad \ldots, \qquad (\delta_t) = \mathfrak{d}_t^h.$$

Тогда мы можем записать

$$\mu^h = \eta\delta_1 \ldots \delta_t\alpha^2, \tag{12}$$

где η — единица в k и α — некоторое целое число в k. По теореме 4 простые идеалы $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ входят в относительный дискриминант поля $K(\sqrt{\mu})$. Обозначим через r число характеров, определяющих род классов в $K(\sqrt{\mu})$, и пусть идеалы $\mathfrak{d}_t, \mathfrak{d}_{t-1}, \ldots, \mathfrak{d}_{r+1}$ выбраны из простых идеалов $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ способом, указанным в определении 11. Тогда справедливо следующее утверждение: если $c_1, \ldots, c_r$ — какие-либо r единиц ± 1, для которых $c_1 \ldots c_r = 1$, то в поле $K(\sqrt{\mu})$ всегда существует идеал, характеры которого совпадают с $c_1, \ldots, c_r$. В самом деле, по теореме 18 в k должен существовать простой идеал $\mathfrak{p}$, удовлетворяющий равенствам

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = +1, \qquad \ldots, \qquad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right) = +1, \tag{13}$$

$$\left.\begin{aligned} \left(\frac{\delta_1}{\mathfrak{p}}\right) = c_1\ , \qquad \ldots, \qquad \left(\frac{\delta_r}{\mathfrak{p}}\right) = c_r, \\ \left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = +1, \qquad \ldots, \qquad \left(\frac{\delta_t}{\mathfrak{p}}\right) = +1. \end{aligned}\right\} \tag{14}$$

Ввиду (13), $\mathfrak{p}$ является примарным простым идеалом; пусть π — его примарное число. В силу теоремы 35 и соотношения (7) из (14) следуют равенства

$$\left(\frac{\pi}{\mathfrak{d}_1}\right) = c_1, \quad \ldots, \quad \left(\frac{\pi}{\mathfrak{d}_r}\right) = c_r, \quad \left(\frac{\pi}{\mathfrak{d}_{r+1}}\right) = +1, \quad \ldots, \quad \left(\frac{\pi}{\mathfrak{d}_t}\right) = +1. \tag{15}$$

Так как должно быть $c_1, \ldots, c_r = +1$, то мы получаем из (14)

$$\left(\frac{\delta_1 \ldots \delta_t}{\mathfrak{p}}\right) = +1$$

и, следовательно, ввиду (12)

$$\left(\frac{\mu^h}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right) = +1,$$

т. е. $\mathfrak{p}$ распадается в $K(\sqrt{\mu})$ на два простых множителя. В силу (15) характеры любого из этих простых множителей совпадают с $c_1, \ldots, c_r$.

Так как число наборов по r единиц $c_1, \ldots, c_r$ с $c_1 \ldots c_r = +1$ равно 2^{r-1}, а с другой стороны, по теореме 26, в поле $K(\sqrt{\mu})$ не может существовать более 2^{r-1} родов, мы заключаем, как и на первом шаге, что система характеров $c_1, \ldots, c_r$ любого имеющегося в $K(\sqrt{\mu})$ рода должна удовлетворять условию $c_1 \ldots c_r = +1$.

Для того чтобы доказать с помощью этого утверждения нашу теорему 36 в рассматриваемом третьем случае, предположим, что $\mathfrak{p}$ — простой идеал, удовлетворяющий условиям

$$\left(\frac{\mu}{\mathfrak{p}}\right) = +1, \tag{16}$$

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\mathfrak{p}}\right) = +1, \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right) = +1, \tag{17}$$

$$\left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_{r+1}}\right), \quad \left(\frac{\delta_{r+2}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_{r+2}}\right), \quad \ldots, \quad \left(\frac{\delta_t}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_t}\right), \tag{18}$$

Ввиду равенства (16) $\mathfrak{p}$ распадается в поле $K(\sqrt{\mu})$ на два простых множителя, а ввиду равенства (17) $\mathfrak{p}$ является примарным простым идеалом; пусть π — примарное число для $\mathfrak{p}$. В силу (18) мы получаем, используя теорему 35 и соотношение (7), равенства

$$\left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_i}\right) = \left(\frac{\varepsilon\pi}{\mathfrak{d}_i}\right) = \left(\frac{\varepsilon}{\mathfrak{d}_i}\right)\left(\frac{\pi}{\mathfrak{d}_i}\right) = +1 \qquad (i = r+1, r+2, \ldots, t), \tag{19}$$

и, следовательно, r характеров простого множителя $\mathfrak{p}$ имеют следующие значения

$$\left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_1}\right), \quad \left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_2}\right), \quad \ldots, \quad \left(\frac{\varepsilon\pi, \mu}{\mathfrak{d}_r}\right).$$

Далее, по ранее доказанному произведение этих характеров должно быть равно $+1$, что, с учетом (16) и (19), влечет равенство

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\varepsilon\pi, \mu}{\mathfrak{w}}\right) = +1,$$

а так как согласно утверждению, доказанному на втором шаге, должно быть

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\pi, \mu}{\mathfrak{w}}\right) = +1,$$

то получаем также

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\varepsilon, \mu}{\mathfrak{w}}\right) = +1, \tag{20}$$

что доказывает нашу теорему при предположениях, сделанных на данном третьем шаге. Здесь, как и в дальнейшем, произведение $\prod_{(\mathfrak{w})}{}'$ распространяется на все взаимно простые с 2 простые идеалы $\mathfrak{w}$ поля k.

В качестве *четвертого* шага разберем случай, когда ν есть h-я степень некоторого непримарного простого идеала $\mathfrak{q}$, и запишем $(\varkappa) = \mathfrak{q}^h$, где $\varkappa$ — некоторое целое число в k; μ же пусть содержит в качестве множителей сколь угодно много примарных или непримарных простых идеалов. Рассмотрим поле $K(\sqrt{\mu})$, используя те же обозначения, что и на предыдущем шаге.

Как было установлено на том шаге, произведение r характеров любого рода в $K(\sqrt{\mu})$ должно быть равно $+1$.

Пусть сначала $\left(\frac{\mu}{\mathfrak{q}}\right) = +1$. Тогда $\mathfrak{q}$ распадается в поле $K(\sqrt{\mu})$ на два простых множителя. Для каждого из этих простых множителей его r характеров суть

$$\left(\frac{\xi\varkappa,\mu}{\mathfrak{d}_1}\right),\quad \left(\frac{\xi\varkappa,\mu}{\mathfrak{d}_2}\right),\quad \ldots,\quad \left(\frac{\xi\varkappa,\mu}{\mathfrak{d}_r}\right), \tag{21}$$

где ξ — некоторая подходящая единица в k, а в остальном сохраняются те же обозначения, что были использованы на третьем шаге. Помимо этого, имеют еще место равенства

$$\left(\frac{\xi\varkappa,\mu}{\mathfrak{d}_{r+1}}\right) = +1,\qquad \left(\frac{\xi\varkappa,\mu}{\mathfrak{d}_{r+2}}\right) = +1,\qquad \left(\frac{\xi\varkappa,\mu}{\mathfrak{d}_t}\right) = +1. \tag{22}$$

Перемножением равенств (21) и (22) легко получаем, что

$$\prod'_{(\mathfrak{w})}\left(\frac{\xi\varkappa,\mu}{\mathfrak{w}}\right) = \left(\frac{\mu}{\mathfrak{q}}\right) = +1,$$

а в силу доказанного на третьем шаге соотношения (20) отсюда следует, что

$$\prod'_{(\mathfrak{w})}\left(\frac{\varkappa,\mu}{\mathfrak{w}}\right) = +1. \tag{23}$$

Если же $\left(\frac{\mu}{\mathfrak{q}}\right) = -1$, то возьмем такой примарный простой идеал $\mathfrak{p}$, что $\left(\frac{\varkappa}{\mathfrak{p}}\right) = -1$. Пусть π — примарное число для $\mathfrak{p}$. Тогда ввиду (7) $\left(\frac{\pi}{\mathfrak{q}}\right) = -1$ и, следовательно, $\left(\frac{\pi\mu}{\mathfrak{q}}\right) = +1$. Из только что доказанной формулы (23), если мы подставим в нее теперь $\pi\mu$ вместо μ, вытекает, что

$$\prod'_{(\mathfrak{w})}\left(\frac{\varkappa,\pi\mu}{\mathfrak{w}}\right) = +1,$$

откуда, привлекая (11), снова получаем

$$\prod'_{(\mathfrak{w})}\left(\frac{\varkappa,\mu}{\mathfrak{w}}\right) = +1, \tag{24}$$

что доказывает нашу теорему 36 и для этого четвертого случая.

Наконец, докажем теорему 36 в общем случае. С этой целью запишем

$$\nu^h = \varepsilon\varrho_1\varrho_2\ldots,$$

где ε — единица в k и $\varrho_1,\varrho_2,\ldots$ — либо примарные числа примарных простых идеалов, либо такие целые числа в k, которые представляют h-е степени непримарных простых идеалов. Тогда из (20), (11) и (24) мы получаем доказываемое равенство

$$\prod'_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = \prod'_{(\mathfrak{w})}\left(\frac{\nu^h,\mu}{\mathfrak{w}}\right) = +1.$$

Теорема 36 уже содержит важную составную часть квадратичного закона взаимности, связывающего между собой взаимно простые с 2 числа в поле k. В приводимой ниже теореме собраны некоторые важные следствия из теоремы 36.

Теорема 37. *Пусть ν, μ, ν^*, μ^* — взаимно простые с 2 целые числа в k, удовлетворяющие по модулю 2^2 сравнениям*

$$\nu \equiv \nu^*, \qquad \mu = \mu^*, \qquad (2^2)$$

и пусть, сверх того, ν взаимно просто с μ, а ν^* взаимно просто с μ^*. Тогда справедлива формула

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right) = \left(\frac{\nu^*}{\mu^*}\right)\left(\frac{\mu^*}{\nu^*}\right).$$

Пусть ν, μ — взаимно простые и взаимно простые с 2 целые числа в k, хотя бы одно из которых сравнимо с квадратом некоторого целого числа в k по модулю 2^2. Тогда справедлива формула

$$\left(\frac{\nu}{\mu}\right) = \left(\frac{\mu}{\nu}\right).$$

Доказательство. При предположениях, сделанных в первой части теоремы, имеем по теореме 36

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu\nu^*, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \mu}{\mathfrak{w}}\right) = +1,$$

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \mu\mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \mu}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \mu^*}{\mathfrak{w}}\right) = +1$$

и, следовательно,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*, \mu^*}{\mathfrak{w}}\right),$$

откуда легко получаем первое утверждение теоремы. Второе утверждение получается непосредственным применением теоремы 36.

Формулы теоремы 37 могут быть проиллюстрированы разнообразными численными примерами.

§ 26. Примарные идеалы и их свойства

Расширим определение 13 следующим образом.

Определение 16. Взаимно простой с 2 идеал $\mathfrak{a}$ поля k, относительно которого для любой единицы ξ выполняется условие

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1,$$

называется *примарным идеалом*; напротив, идеал называется *непримарным*, если указанное равенство выполняется не для каждой единицы ξ.

Опираясь на теорему 36, мы можем теперь обобщить теорему 32 следующим образом.

Теорема 38. *Пусть $\mathfrak{a}$ — произвольный примарный идеал в k. Всегда можно найти такое целое число α в k, что идеал (α) равен $\mathfrak{a}^h$ и, кроме того, число α сравнимо по модулю 2^2 с квадратом некоторого целого числа в поле k.*

Доказательство. Пусть α^* — такое целое число в k, что $(\alpha^*) = \mathfrak{a}^h$. Далее, пусть $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$ и $\varkappa_1, \ldots, \varkappa_{m/2}$ обозначают те же $m/2$ идеалов и $m/2$ целых чисел соответственно, что и в теореме 29. Как было установлено при доказательстве этой теоремы, любое целое взаимно простое с 2 число представимо по модулю 2^2 некоторым определенным образом (см. с. 220). В частности, мы можем записать

$$\alpha^* \equiv \varepsilon^* \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \beta^2, \qquad (2^2), \tag{1}$$

где ε^* — некоторая подходящая единица в k, показатели $v_1, \ldots, v_{m/2}$ принимают значения 0 или 1, а β — подходящее целое число в k. Так как в силу (1) число

$$\alpha^* \varepsilon^* \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}}$$

сравнимо с квадратом некоторого целого числа в k по модулю 2^2, по теореме 36 для любой единицы ξ в k

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\xi, \alpha^* \varepsilon^* \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}}}{\mathfrak{w}} \right) = +1$$

и, следовательно,

$$\left(\frac{\xi}{\alpha^* \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}}} \right) = \left(\frac{\xi}{\mathfrak{a}} \right) \left(\frac{\xi}{\mathfrak{q}_1} \right)^{v_1} \ldots \left(\frac{\xi}{\mathfrak{q}_{m/2}} \right)^{v_{m/2}} = +1,$$

а так как по предположению должно быть $\left(\frac{\xi}{\mathfrak{a}} \right) = +1$, мы заключаем, что для любой единицы ξ в k должно выполняться равенство

$$\left(\frac{\xi}{\mathfrak{q}_1} \right)^{v_1} \ldots \left(\frac{\xi}{\mathfrak{q}_{m/2}} \right)^{v_{m/2}} = +1.$$

Если подставить в него вместо ξ поочередно единицы $\varepsilon_1, \ldots, \varepsilon_{m/2}$, определенные в § 21, то из формул на стр. 220 мы получим, что все показатели $v_1, \ldots, v_{m/2}$ равны 0, и поэтому, ввиду (1), $\alpha = \alpha^* \varepsilon^*$ является целым числом в k с требуемыми свойствами.

Обратное к теореме 38 утверждение представляет собой обобщение теоремы 33 и звучит следующим образом.

Теорема 39. *Пусть $\mathfrak{a}$ — взаимно простой с 2 идеал в k. Если существует целое число α в k, сравнимое по модулю 2^2 с квадратом некоторого целого числа поля k и такое, что идеал (α) равен $\mathfrak{a}^h$, то α — примарный идеал в k.*

Доказательство. В равенстве из теоремы 36 положим ν равным произвольной единице ξ в k, а μ — равным числу α.

§ 27. Примеры к теоремам 32, 33, 38, 39

Теоремы 32, 33 соответствуют известным утверждениям теории рациональных чисел, согласно которым -1 является квадратичным вычетом или невычетом относительно данного рационального положительного простого числа в зависимости от того, имеет ли это число вид $4n+1$ или $4n+3$. Следующие примеры могут служить иллюстрацией к названным теоремам 32 и 33, равно как и к более общим теоремам 38 и 39.

Пример 1. У квадратичного поля $k(\sqrt{-7})$ число классов $h = 1$; это поле обладает двумя связками единиц, а именно теми, которые определяются единицами $+1$ и -1. Числа

$$3, \qquad \sqrt{-7}, \qquad 2+\sqrt{-7}, \qquad 4+\sqrt{-7}, \qquad 1+2\sqrt{-7}$$

являются простыми с нормами

$$3^2, \qquad 7, \qquad 11, \qquad 23, \qquad 29$$

соответственно. Далее, выполняются сравнения

$$-1 \equiv (\sqrt{-7})^2, \qquad (3) \quad \text{и} \quad -1 \equiv 12^2, \qquad (1+2\sqrt{-7});$$

таким образом, в поле $k(\sqrt{-7})$

$$\left(\frac{-1}{3}\right) = +1 \quad \text{и} \quad \left(\frac{-1}{1+2\sqrt{-7}}\right) = +1,$$

т. е. простые идеалы (3) и $(1+2\sqrt{-7})$ являются примарными. Далее, с помощью теоремы 1 мы находим, что

$$\left(\frac{-1}{\sqrt{-7}}\right) = (-1)^{(7-1)/2} = -1, \qquad \left(\frac{-1}{2+\sqrt{-7}}\right) = (-1)^{(11-1)/2} = -1,$$

$$\left(\frac{-1}{4+\sqrt{-7}}\right) = (-1)^{(23-1)/2} = -1;$$

т. е. простые идеалы $(\sqrt{-7})$, $(2+\sqrt{-7})$, $(4+\sqrt{-7})$ непримарны. И действительно, в полном согласии с теоремой 32 мы имеем

$$-3 \equiv 1^2, \qquad (2^2) \quad \text{и} \quad -1-2\sqrt{-7} \equiv 1^2, \qquad (2^2),$$

т. е. -3 и $-1-2\sqrt{-7}$ являются примарными числами простых идеалов (3) и $(1+2\sqrt{-7})$ соответственно. Напротив, ни одно из шести чисел

$$\pm\sqrt{-7}, \qquad \pm(2+\sqrt{-7}), \qquad \pm(4+\sqrt{-7})$$

не сравнимо с квадратом целого числа в $k(\sqrt{-7})$ по модулю 2^2, как и утверждается теоремой 33.

Согласно определению 16 идеалы

$$(\sqrt{-7})(2+\sqrt{-7}) = (-7+2\sqrt{-7}),$$

$$(\sqrt{-7})(4+\sqrt{-7}) = (-7+4\sqrt{-7})$$

являются примарными; и действительно, в согласии с теоремы 38 имеют место сравнения по модулю 2^2

$$-(-7+2\sqrt{-7}) \equiv 1^2, \qquad (2^2),$$
$$-7+4\sqrt{-7} \equiv 1^2, \qquad (2^2).$$

Пример 2. У биквадратичного поля $k(\sqrt{-1}, \sqrt{5})$ число классов $h=1$. Положим $i=\sqrt{-1}$ и $\theta=\frac{1}{2}(1+\sqrt{5})$ так что $i^2+1=0$ и $\theta^2-\theta-1=0$. Поле $k(i,\theta)$ имеет 4 связки единиц, а именно те, которые определяются единицами $1, i, \theta, i\theta$.

Числа

$$i+\theta, \quad 3+2i, \quad 2i+\theta, \quad 1-2\theta+i\theta, \quad 1+2i+2\theta, \quad 3i+\theta \qquad (1)$$

являются примарными числами с нормами

$$5, \quad 13^2, \quad 29, \quad 41, \quad 89, \quad 109$$

соответственно. С помощью теоремы 1 мы легко обнаруживаем, что в поле $k(i,\theta)$ выполняются равенства

$$\left(\frac{i}{i+\theta}\right) = i^{(5-1)/2} = -1, \qquad \left(\frac{\theta}{i+\theta}\right) = \left(\frac{-i}{i+\theta}\right) = -1,$$
$$\left(\frac{i}{3+2i}\right) = +1, \qquad \left(\frac{\theta}{3+2i}\right) = +1,$$
$$\left(\frac{i}{2i+\theta}\right) = -1, \qquad \left(\frac{\theta}{2i+\theta}\right) = +1,$$
$$\left(\frac{i}{1-2\theta+i\theta}\right) = +1, \qquad \left(\frac{\theta}{1-2\theta+i\theta}\right) = -1,$$
$$\left(\frac{i}{1+2i+2\theta}\right) = +1, \qquad \left(\frac{\theta}{1+2i+2\theta}\right) = +1,$$
$$\left(\frac{i}{3i+\theta}\right) = -1, \qquad \left(\frac{\theta}{3i+\theta}\right) = -1.$$

В силу теоремы 33 ни одно из четырех простых чисел $i+\theta$, $2i+\theta$, $1-2\theta+i\theta$, $3i+\theta$ не может быть сравнимым по модулю 2^2 ни с каким числом вида $i^u\theta^v\alpha^2$, где u, v могут принимать значения 0 или 1, а α — какое-либо целое число в $k(i,\theta)$. Напротив, по теореме 32 каждое из остальных двух чисел последовательности (1) должно удовлетворять такому сравнению. И в самом деле,

$$3+2i \equiv \theta(1-i-\theta)^2, \qquad (2^2) \quad \text{и} \quad 1+2i+2\theta \equiv (1+\theta+i\theta)^2, \qquad (2^2).$$

Далее, из вышеприведенных равенств вытекает, что идеалы

$$(i+\theta)(3i+\theta) =, (-2+\theta+4i\theta),$$
$$(i+\theta)(2i+\theta)(1-2\theta+i\theta) = (-6-5i-2\theta-3i\theta)$$

примарны; и действительно, в согласии с теоремами 38 и 39, имеют место равенства

$$-2+\theta+4i\theta \equiv -(1-\theta)^2, \qquad (2^2)$$
$$-6-5i-2\theta-3i\theta \equiv -i(1+i-\theta)^2, \qquad (2^2).$$

Пример 3. У биквадратичного поля $k(\sqrt{1+4\sqrt{-1}})$ число классов $h=1$; положим $i=\sqrt{-1}$ и $\theta=\frac{1}{2}(1+\sqrt{1+4i})$, так что $\theta^2-\theta-i=0$. Поле $k(\sqrt{\theta})$ обладает четырьмя связками единиц, а именно теми, которые определяются единицами $1, i, \theta, i\theta$.

Разлагая число 5 на множители, мы получаем три простых числа в $k(\sqrt{\theta})$

$$2+i, \quad 1+\theta, \quad 2-\theta. \qquad (2)$$

Произведение двух последних равно $2-i$, а произведение всех трех простых чисел равно 5. Мы легко обнаруживаем, что в поле $k(\theta)$

$$\left(\frac{i}{2+i}\right)=i^{(5^2-1)/2}=+1, \quad \left(\frac{i}{1+\theta}\right)=i^{(5-1)/2}=-1, \quad \left(\frac{i}{2-\theta}\right)=-1 \qquad (3)$$

и

$$\left(\frac{\theta}{2+i}\right)=-1, \qquad \left(\frac{\theta}{1+\theta}\right)=+1, \qquad \left(\frac{\theta}{2-\theta}\right)=-1. \qquad (4)$$

И в самом деле, ни одно из трех простых чисел (2) не сравнимо по модулю 2^2 с числом вида $i^u\theta^v\alpha^2$, где u, v принимают значения 0 или 1, а α — некоторое целое число в $k(\theta)$. Напротив, $5\equiv 1^2$ по модулю 2^2, и в силу (3), (4) мы имеем

$$\left(\frac{i}{5}\right)=\left(\frac{i}{2+i}\right)\left(\frac{i}{1+\theta}\right)\left(\frac{i}{2-\theta}\right)=+1,$$
$$\left(\frac{\theta}{5}\right)=\left(\frac{\theta}{2+i}\right)\left(\frac{\theta}{1+\theta}\right)\left(\frac{\theta}{2-\theta}\right)=+1,$$

т. е. идеал (5) примарен в полном соответствии с теоремой 39.

Число 37 равно в $k(\theta)$ произведению трех простых чисел

$$6+i, \quad -3+\theta, \quad 2+\theta.$$

Мы без труда находим

$$\left(\frac{i}{6+i}\right)=+1, \qquad \left(\frac{i}{3-\theta}\right)=-1, \qquad \left(\frac{i}{2+\theta}\right)=-1 \qquad (5)$$

и

$$\left(\frac{\theta}{6+i}\right)=-1, \qquad \left(\frac{\theta}{3-\theta}\right)=+1, \qquad \left(\frac{\theta}{2+\theta}\right)=-1. \qquad (6)$$

У числа 37, равно как и у 5, все простые множители непримарны. Напротив, идеал (37) примарен. Далее, ввиду (3), (4), (5), (6) идеалы

$$\big((2+i)(6+i)\big), \quad \big((1+\theta)(3-\theta)\big), \quad \big((2-\theta)(2+\theta)\big)$$

примарны; и действительно, в полном соответствии с теоремой 38 имеют место сравнения

$$\begin{aligned}(2+i)(6+i) &\equiv (2+i)^2 \qquad (2^2),\\ -(1+\theta)(3-\theta) &\equiv (1-\theta)^2 \qquad (2^2),\\ -(2-\theta)(2+\theta) &\equiv \theta^2 \qquad (2^2).\end{aligned}$$

Числа 3 и 7 остаются неразложимыми в $k(\theta)$, и так как $-3 \equiv 1^2$ и $-7 \equiv 1^2$ по модулю 2^2, то согласно теореме 33, (3) и (7) должны быть примарными простыми идеалами с примарными числами -3 и -7. И в самом деле, обе единицы i, θ являются квадратичными вычетами в $k(\theta)$ по модулю (3) и (7), ибо

$$\left(\frac{i}{3}\right) = i^{(3^4-1)/2} = +1 \quad \text{и} \quad \left(\frac{i}{7}\right) = i^{(7^4-1)/2} = +1,$$

а также

$$\theta \equiv (1-\theta+i\theta)^2, \qquad (3) \qquad \text{и} \qquad \theta \equiv (1-3i-3\theta-i\theta)^2, \qquad (7).$$

Пример 4. У биквадратичного поля $k(\sqrt[4]{-2})$ число классов $h = 1$; мы положим $\theta = \sqrt[4]{-2}$, так что $\theta^2 + 2 = 0$. Поле $k(\theta)$ обладает четырьмя связками единиц, а именно теми, которые определены единицами 1, -1, ε, $-\varepsilon$, где для краткости мы положили

$$\varepsilon = 1 - \theta^2 + \theta^3.$$

Числа

$$\left.\begin{array}{ccc} 1-\theta, & 1+\theta, & 1+\theta-2\theta^2+2\theta^3,\\ & 1+\theta+2\theta^2+\theta^3, & 1+2\theta-\theta^2 \end{array}\right\} \qquad (7)$$

являются в $k(\theta)$ простыми числами первой степени с нормами

$$\begin{array}{ccc} 3, & 3, & 19,\\ & 59, & 73, \end{array}$$

соответственно. Отсюда мы заключаем на основании теоремы 1, что

$$\left.\begin{array}{cc} \left(\dfrac{-1}{1-\theta}\right) = -1, \quad \left(\dfrac{-1}{1+\theta}\right) = -1, & \left(\dfrac{-1}{1+\theta-2\theta^2+2\theta^3}\right) = -1,\\ \left(\dfrac{-1}{1+\theta+2\theta^2+\theta^3}\right) = -1, & \left(\dfrac{-1}{1+2\theta-\theta^2}\right) = +1. \end{array}\right\} \qquad (8)$$

Относительно простых чисел (7) число θ удовлетворяет сравнениям

$$\begin{array}{ccc} \theta \equiv 1, & \theta \equiv -1, & \theta \equiv -5,\\ & \theta \equiv 6, & \theta \equiv -31, \end{array}$$

соответственно, и, следовательно, для ε имеют место сравнения относительно этих простых чисел

$$\begin{array}{ccc} \varepsilon \equiv 1, & \varepsilon \equiv -1, & \varepsilon \equiv 3,\\ & \varepsilon \equiv 4, & \varepsilon \equiv -18. \end{array}$$

Так как в области рациональных чисел 1 является квадратичным вычетом по модулю 3, -1 — невычетом по модулю 3, 3 — невычетом по модулю 19, 4 — вычетом по модулю 59 и -18 — вычетом по модулю 73, то в поле $k(\theta)$ выполняются равенства

$$\left.\begin{gathered}\left(\frac{\varepsilon}{1-\theta}\right)=+1,\quad \left(\frac{\varepsilon}{1+\theta}\right)=-1,\quad \left(\frac{\varepsilon}{1+\theta-2\theta^2+2\theta^3}\right)=-1,\\ \left(\frac{\varepsilon}{1+\theta+2\theta^2+\theta^3}\right)=+1,\qquad \left(\frac{\varepsilon}{1+2\theta-\theta^2}\right)=+1.\end{gathered}\right\} \tag{9}$$

Ввиду (8) и (9) только последнее из пяти простых чисел (7) примарно. И в самом деле, в согласии с теоремой 32 имеет место сравнение по модулю 2^2

$$-(1+2\theta-\theta^2)\equiv(1+\theta+\theta^2+\theta^3)^2,\qquad (2^2),$$

так что $-1-2\theta+\theta^2$ есть примарное число простого идеала $(1+2\theta+\theta^2)$.

Числа

$$1-2\theta+2\theta^2,\qquad\qquad 1-4\theta^2+2\theta^3$$

являются простыми числами второй степени в $k(\theta)$ с нормами

$$7^2,\qquad\qquad 31^2,$$

соответственно. Имеем

$$\left(\frac{-1}{1-2\theta+2\theta^2}\right)=(-1)^{(7^2-1)/2}=+1.$$

Далее, используя сравнение

$$\theta^2\equiv\theta+3,\qquad (1-2\theta+2\theta^2),$$

легко находим, что ε — квадратичный невычет по модулю $1-2\theta+2\theta^2$, т. е.

$$\left(\frac{\varepsilon}{1-2\theta+2\theta^2}\right)=-1,$$

и, следовательно, простое число $1-2\theta+2\theta^2$ непримарно. Напротив,

$$-1+4\theta^2-2\theta^3\equiv(1+\theta^2+\theta^3),\qquad (2^2),$$

и поэтому простой идеал $(1-4\theta^2+2\theta^3)$ должен быть примарным по теореме 33. И в самом деле, мы имеем

$$\left(\frac{-1}{1-4\theta^2+2\theta^3}\right)=(-1)^{(31^2-1)/2}=+1$$

и, кроме того, выполняется сравнение

$$\varepsilon\equiv(3-2\theta)^2,\qquad (1-4\theta^2+2\theta^3).$$

Наконец, в силу (8) и (9) идеалы

$$\big((1+\theta)(1+\theta-2\theta^2+2\theta^3)\big),\qquad \big((1-\theta)(1+\theta+2\theta^2+\theta^3)\big)$$

примарны. И в самом деле, в согласии с теоремой 38 мы обнаруживаем, что

$$-(1+\theta)(1+\theta-2\theta^2+2\theta^3)\equiv(1+\theta+\theta^2+\theta^3)^2, \qquad (2^2),$$
$$-\varepsilon(1-\theta)(1+\theta+2\theta^2+\theta^3)\equiv\varepsilon^2, \qquad (2^2).$$

Число 5 неразложимо в $k(\theta)$, и ввиду сравнения $5\equiv 1^2$ по модулю 2^2 простой идеал (5) примарен, по теореме 33. И в самом деле, ввиду сравнения

$$\varepsilon\equiv(1+2\theta+\theta^2+\theta^3)^2, \qquad (5),$$

ε является квадратичным вычетом по модулю 5.

Пример 5. Поле, определенное корнем 5-й степени из единицы, является биквадратичным циклическим полем с числом классов $h=1$; пусть θ — некоторый отличный от 1 корень 5-й степени из единицы, так что

$$\theta^4+\theta^3+\theta^2+\theta+1=0.$$

Поле $k(\theta)$ имеет 4 связки единиц, а именно те, которые определяются единицами $+1$, -1, $1+\theta$, $1-\theta$.

Числа

$$\left.\begin{array}{lll} 1+2\theta^2, & 2-\theta^2, & 3+2\theta+\theta^2, \\ 3+\theta, & 3+4\theta^2, & 1+5\theta^2 \end{array}\right\} \qquad (10)$$

являются простыми числами первой степени в $k(\theta)$ с нормами

$$\begin{array}{lll} 11, & 31, & 41, \\ 61, & 181, & 521 \end{array}$$

соответственно. С помощью теоремы 1 мы легко получаем отсюда, что

$$\left.\begin{array}{lll} \left(\frac{-1}{1+2\theta^2}\right)=-1, & \left(\frac{-1}{2-\theta^2}\right)=-1, & \left(\frac{-1}{3+2\theta+\theta^2}\right)=+1, \\ \left(\frac{-1}{3+\theta}\right)=+1, & \left(\frac{-1}{3+4\theta^2}\right)=+1, & \left(\frac{-1}{1+5\theta^2}\right)=+1. \end{array}\right\} \qquad (11)$$

Относительно простых чисел (10) единица $1+\theta$ удовлетворяет сравнениям

$$\begin{array}{lll} 1+\theta\equiv 5, & \equiv 9, & \equiv 11, \\ \equiv -2, & \equiv 43, & \equiv 26, \end{array}$$

соответственно. Так как в области рациональных чисел 5 является квадратичным вычетом по модулю 11, 9 — квадратичным вычетом по модулю 31, 11 — невычетом по модулю 41, -2 — невычетом по модулю 61, 43 — вычетом по модулю 181 и 26 — вычетом по модулю 521, то в $k(\theta)$ мы имеем равенства

$$\left.\begin{array}{lll} \left(\frac{1+\theta}{1+2\theta^2}\right)=+1, & \left(\frac{1+\theta}{2-\theta^2}\right)=+1, & \left(\frac{1+\theta}{3+2\theta+\theta^2}\right)=-1, \\ \left(\frac{1+\theta}{3+\theta}\right)=-1, & \left(\frac{1+\theta}{3+4\theta^2}\right)=+1, & \left(\frac{1+\theta}{1+5\theta^2}\right)'=+1. \end{array}\right\} \qquad (12)$$

Ввиду (11) и (12) только два последние из шести простых чисел (10) примарны, и в самом деле, в согласии с теоремой 32 и 33 имеют место сравнения по модулю 2^2

$$3+4\theta^2\equiv -1, \qquad (2^2),$$

$$1+5\theta^2\equiv -\frac{\theta^4}{1+\theta}, \qquad (2^2),$$

так что

$$-3-4\theta^2 \quad \text{и} \quad -(1+\theta)(1+5\theta^2)=-1-\theta-5\theta^2-5\theta^3$$

суть примарные числа соответствующих двух простых идеалов.

Из равенств (11), (12) легко получаются равенства

$$\left(\frac{-1}{(1+2\theta^2)(2-\theta^2)}\right)=+1, \qquad \left(\frac{-1}{(3+2\theta+\theta^2)(3+\theta)}\right)=+1,$$

$$\left(\frac{1+\theta}{(1+2\theta^2)(2-\theta^2)}\right)=+1, \qquad \left(\frac{1+\theta}{(3+2\theta+\theta^2)(3+\theta)}\right)=+1.$$

Следовательно, по теореме 38 числа $(1+2\theta^2)(2-\theta^2)$ и $(3+2\theta+\theta^2)(3+\theta)$ должны быть сравнимы по модулю 2^2 с произведением некоторой единицы на квадрат целого числа поля $k(\theta)$. И в самом деле, имеют место сравнения

$$(1+2\theta^2)(2-\theta^2)\equiv 2\theta+\theta^2+2\theta^3\equiv(1+\theta)(1+\theta^4)^2, \qquad (2^2),$$

$$(3+2\theta+\theta^2)(3+\theta)\equiv -\theta^4, \qquad (2^2).$$

Пример 6. Поле, определенное корнем θ уравнения

$$\theta^4+\theta+1=0,$$

является биквадратичным полем без квадратичных подполей с числом классов $h=1$ и обладает четырьмя связками единиц, а именно теми, которые определяются единицами $+1$, -1, θ, $-\theta$. Числа 3 и 5 в $k(\theta)$ имеют разложения

$$3=(1-\theta)(2+\theta+\theta^2+\theta^3),$$

$$5=(1+\theta+\theta^2+\theta^3)(2-4\theta+2\theta^2-\theta^3),$$

где в обоих случаях первый множитель справа является простым числом первой степени, а второй множитель — простым числом третьей степени. Сообразно с этим мы без труда получаем с помощью теоремы 1, что

$$\left.\begin{aligned}\left(\frac{-1}{1-\theta}\right)=-1, \quad \left(\frac{-1}{2+\theta+\theta^2+\theta^3}\right)=(-1)^{(3^3-1)/2}=-1,\\ \left(\frac{-1}{1+\theta+\theta^2+\theta^3}\right)=+1, \quad \left(\frac{-1}{2-4\theta+2\theta^2-\theta^3}\right)=(-1)^{(5^3-1)/2}=+1.\end{aligned}\right\} \qquad (13)$$

С другой стороны, из сравнений

$$\theta \equiv 1, \qquad (1-\theta) \quad \text{и} \quad \theta \equiv -2, \qquad (1+\theta+\theta^2+\theta^3)$$

вытекают равенства

$$\left(\frac{\theta}{1-\theta}\right) = +1, \qquad \left(\frac{\theta}{1+\theta+\theta^2+\theta^3}\right) = -1. \tag{14}$$

Поскольку $-3 \equiv 1^2$ и $5 \equiv 1^2$ по модулю 2^2, мы заключаем на основании теоремы 39, что (3) и (5) являются примарными идеалами, и, следовательно,

$$\left(\frac{\theta}{3}\right) = \left(\frac{\theta}{1-\theta}\right)\left(\frac{\theta}{2+\theta+\theta^2+\theta^3}\right) = +1,$$

$$\left(\frac{\theta}{5}\right) = \left(\frac{\theta}{1+\theta+\theta^2+\theta^3}\right)\left(\frac{\theta}{2-4\theta+2\theta^2-\theta^3}\right) = +1,$$

откуда, учитывая (14), получаем

$$\left(\frac{\theta}{2+\theta+\theta^2+\theta^3}\right) = +1 \quad \text{и} \quad \left(\frac{\theta}{2-4\theta+2\theta^2-\theta^3}\right) = -1. \tag{15}$$

И в самом деле, первое равенство подтверждается сравнением

$$\theta \equiv (\theta-\theta^2)^2, \qquad (2+\theta+\theta^2+\theta^3).$$

Чтобы подтвердить второе равенство, заметим, что

$$\theta^3 \equiv 2(1-\theta)^2, \qquad (2-4\theta+2\theta^2-\theta^3),$$

а потому

$$\left(\frac{\theta}{2-4\theta+2\theta^2-\theta^3}\right) = \left(\frac{2}{2-4\theta+2\theta^2-\theta^3}\right),$$

а поскольку

$$2^{(5^3-1)/2} \equiv -1, \qquad (5),$$

по теореме 1

$$\left(\frac{2}{2-4\theta+2\theta^2-\theta^3}\right) = -1.$$

Число 7 неразложимо в $k(\theta)$, и, ввиду того что $-7 \equiv 1^2$ по модулю 2^2, число θ должно быть квадратичным вычетом по модулю 7 в $k(\theta)$. И в самом деле,

$$\theta \equiv (\theta+\theta^2+3\theta^3)^2, \qquad (7).$$

Числа $2-\theta$ и $2-\theta^2$ являются простыми числами первой степени в $k(\theta)$ с нормами 19 и 23 соответственно. Мы получаем без труда

$$\left(\frac{-1}{2-\theta}\right) = -1, \qquad \left(\frac{\theta}{2-\theta}\right) = -1,$$

$$\left(\frac{-1}{2-\theta^2}\right) = -1, \qquad \left(\frac{\theta}{2-\theta^2}\right) = +1.$$

Отсюда, а также из (13), (14), (15) вытекают равенства

$$\left(\frac{-1}{(1-\theta)(2-\theta)(2-4\theta+2\theta^2-\theta^3)}\right)=+1, \qquad \left(\frac{-1}{(1-\theta)(2-\theta^2)}\right)=+1.$$

По теореме 38 каждое из этих двух фигурирующих здесь произведений простых чисел после умножения на подходящие единицы должно стать сравнимым с квадратом некоторого целого числа в $k(\theta)$ по модулю 2^2. И в самом деле,

$$-(1-\theta)(2-\theta)(2-4\theta+2\theta^2-\theta^3)\equiv(1-\theta)^2, \qquad (2^2),$$
$$-\theta(1-\theta)(2-\theta^2)\equiv(\theta+\theta^2+\theta^3)^2, \qquad (2^2).$$

Пример 7. Поле, определенное корнем 7-й степени из единицы, является абелевым полем 6-й степени с числом классов $h=1$; оно может быть составлено из квадратичного и кубического полей. Будем понимать под θ фиксированный отличный от 1 корень 7-й степени из единицы и положим

$$\zeta=\theta+\theta^2+\theta^4 \quad \text{и} \quad \eta=\theta+\theta^6.$$

Тогда

$$\zeta^2+\zeta+2=0 \quad \text{и} \quad \eta^3+\eta^2-2\eta-1=0.$$

Поле $k(\theta)$ имеет 8 связок единиц, а именно те, которые определяются единицами $+1$, -1, $+\eta$, $-\eta$, $2-\eta^2$, $-2+\eta^2$, $\eta(2-\eta^2)$, $-\eta(2-\eta^2)$.

Числа

$$1-\theta+2\theta^3, \qquad 1+3\theta+\theta^2+\theta^3 \tag{16}$$

суть простые числа первой степени в $k(\theta)$ с нормами

$$113, \quad 197$$

соответственно. Далее, так как относительно этих простых чисел выполняются сравнения

$$\left.\begin{aligned}\eta&\equiv 9,\\ 2-\eta^2&\equiv 34,\end{aligned}\right\} \qquad \left.\begin{aligned}\eta&\equiv -39,\\ 2-\eta^2&\equiv 57\end{aligned}\right\}$$

соответственно, мы без труда находим, что

$$\left(\frac{-1}{1-\theta+2\theta^3}\right)=+1, \qquad \left(\frac{\eta}{1-\theta+2\theta^3}\right)=+1, \qquad \left(\frac{2-\eta^2}{1-\theta+2\theta^3}\right)=-1,$$
$$\left(\frac{-1}{1+3\theta+\theta^2+\theta^3}\right)=+1, \qquad \left(\frac{\eta}{1+3\theta+\theta^2+\theta^3}\right)=+1, \qquad \left(\frac{2-\eta^2}{1+3\theta+\theta^2+\theta^3}\right)=-1.$$

Таким образом, в соответствии с определением 16 произведение двух простых чисел (16) является примарным идеалом поля $k(\theta)$. И в самом деле, в согласии с теоремами 38 и 39 имеет место сравнение по модулю 2^2

$$(1-\theta+2\theta^3)(1+3\theta+\theta^2+\theta^3)\equiv(2-\eta^2)\theta^2.$$

Число 37 допускает разложение

$$37=(1-4\zeta)(5+4\zeta),$$

где оба множителя справа суть простые числа третьей степени в $k(\theta)$. Так как они сравнимы с 1^2 по модулю 2^2, то по теореме 33 они представляют

примарные простые идеалы. В полном согласии с этим мы находим

$$\left(\frac{-1}{1-4\zeta}\right)=+1,$$

$$\eta\equiv(14+17\eta+19\eta^2)^2, \qquad (37),$$

$$-2+\eta^2\equiv(19\eta+2\eta^2)^2, \qquad (37).$$

Число 3 является простым в $k(\theta)$, и ввиду того что $-3\equiv 1^2$ по модулю 2^2, идеал (3) является примарным простым идеалом (по теореме 33). И в самом деле, мы имеем

$$\left(\frac{-1}{3}\right)=(-1)^{(3^6-1)/2}=+1,$$

$$\eta\equiv(\eta-\eta^2)^2, \qquad (3),$$

$$-2+\eta^2\equiv(1+\eta-\eta^2)^2, \qquad (3).$$

Приведенные примеры показывают, какое богатство арифметических фактов заключено в теоремах 32, 33, 38, 39, — а эти теоремы составляют лишь часть *первого дополнения* к общему закону взаимности для квадратичных вычетов, который будет позже изложен мною. В своем полном виде это первое дополнение появится только в § 36 (теорема 53). Напомним еще о том, что для облегчения понимания мы всюду во второй главе этого сочинения предполагаем, что основное поле k удовлетворяет специальным условиям, приведенным на стр. 202. Пока мы вынуждены отказаться от того, чтобы сообщить формулировку первого дополнения к общему закону взаимности и объяснить, сколь глубоко оно касается самого существа понятия класса идеалов в случае, когда положенное в основу поле k имеет четное число классов.

§ 28. Произведение $\prod_{(\mathfrak{w})}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ для произвольного ν и при некоторых предположениях относительно μ

Для дальнейшего нам необходимо обобщить теорему 36 следующим образом.

Теорема 40. *Пусть* $\mathfrak{l}_1,\mathfrak{l}_2,\ldots,\mathfrak{l}_z$ — *все* (*попарно различные*) *простые множители числа* 2, *и пусть* $\mathfrak{l}_1$ *входит множителем в* 2 *точно в* l_1*-й степени,* $\mathfrak{l}_2$ — *точно в* l_2*-й степени,...,* $\mathfrak{l}_z$ — *точно в* l_z*-й степени, так что*

$$2=\mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}\ldots\mathfrak{l}_z^{l_z}.$$

Тогда если ν — *произвольное целое число и* μ — *целое число в* k, *взаимно простое с* 2 *и сравнимое с квадратом некоторого целого числа в* k *по модулю* $\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\ldots\mathfrak{l}_z^{2l_z+1}$, *то*

$$\prod_{(\mathfrak{w})}'\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=+1,$$

где произведение распространяется на все взаимно простые с 2 *простые идеалы* $\mathfrak{w}$ *поля* k.

Доказательство. Запишем

$$\nu = \mathfrak{n}\mathfrak{l}_1^{e_1} \dots \mathfrak{l}_z^{e_z},$$

где $e_1, \dots, e_z$ — некоторые целые рациональные показатели и $\mathfrak{n}$ — идеал, взаимно простой с 2. По теореме 8 все идеалы $\mathfrak{l}_1, \dots, \mathfrak{l}_z$ разлагаются далее в поле $K(\sqrt{\mu})$; возьмем по одному простому множителю $\mathfrak{L}_1, \dots, \mathfrak{L}_z$ в $K(\sqrt{\mu})$ идеалов $\mathfrak{l}_1, \dots, \mathfrak{l}_z$, соответственно; наконец, пусть A — такое целое число поля $K(\sqrt{\mu})$, делящееся на идеал $\mathfrak{L}_1^{e_1} \dots \mathfrak{L}_z^{e_z}$, что частное $\dfrac{\mathsf{A}}{\mathfrak{L}_1^{e_1} \dots \mathfrak{L}_z^{e_z}}$ взаимно просто с 2. Тогда относительная норма α числа A представима в виде

$$\alpha = N(\mathsf{A}) = \mathfrak{a}\mathfrak{l}_1^{e_1} \dots \mathfrak{l}_s^{e_z},$$

где $\mathfrak{a}$ — некоторый взаимно простой с 2 идеал поля k, так что частное $\dfrac{\nu}{\alpha}$ можно представить в виде дроби $\dfrac{\varrho}{\sigma}$, числитель ϱ и знаменатель σ которой суть целые взаимно простые с 2 числа. Ввиду определения 6, для любого простого идеала $\mathfrak{w}$

$$\left(\frac{N(\mathsf{A}\mathsf{A}), \mu}{\mathfrak{w}}\right) = +1$$

и, следовательно, также

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\alpha, \mu}{\mathfrak{w}}\right) = +1,$$

где произведение $\prod'$ распространено на все простые идеалы $\mathfrak{w}$ в k, взаимно простые с 2. Далее, учитывая, что по теореме 36 имеют место равенства

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\sigma, \mu}{\mathfrak{w}}\right) = +1, \qquad \prod_{(\mathfrak{w})}{}' \left(\frac{\varrho, \mu}{\mathfrak{w}}\right) = +1,$$

мы получаем, принимая во внимание вторую формулу из теоремы 14, что

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu\sigma, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\alpha\varrho, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\alpha, \mu}{\mathfrak{w}}\right) = +1,$$

как и утверждается в доказываемой теореме.

§ 29. Основная теорема о числе родов в относительном квадратичном поле

В § 19 нами была доказана для случая, когда относительный дискриминант поля $K(\sqrt{\mu})$ взаимно прост с 2, теорема 26, дающая верхнюю границу для числа родов в $K(\sqrt{\mu})$. Теперь мы в состоянии доказать при том же ограничении следующую важную теорему.

Теорема 41. *Пусть r — число характеров, определяющих род в относительном квадратичном поле $K(\sqrt{\mu})$, и пусть задана система из r произвольных единиц ± 1. Эта система тогда и только тогда является системой характеров некоторого рода в $K(\sqrt{\mu})$,*

когда произведение всех единиц равно $+1$. *Число* g *всех имеющихся в* $K(\sqrt{\mu})$ *родов равно, таким образом,* 2^{r-1}.

Доказательство. Пусть $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ — простые идеалы поля $K(\sqrt{\mu})$, входящие множителями в относительный дискриминант $K(\sqrt{\mu})$. Запишем

$$\mathfrak{d}_1^h = (\delta_1), \ldots, \mathfrak{d}_t^h = (\delta_t),$$

где $\delta_1, \ldots, \delta_t$ — некоторые целые числа в k. Очевидно, что

$$\delta_1 \ldots \delta_t = \varepsilon\alpha^2\mu, \tag{1}$$

где ε — некоторая единица и α — некоторое целое число в k. Далее, согласно предписанию из § 17 выберем $r = t - r^*$ из наших t простых идеалов; пусть это будут, скажем, $\mathfrak{d}_1, \ldots, \mathfrak{d}_r$. Наконец, пусть $c_1, \ldots, c_r$ — произвольные r единиц ± 1, удовлетворяющие условию

$$c_1 \ldots c_r = +1. \tag{2}$$

Согласно теореме 18 в k существует примарный идеал $\mathfrak{p}$, для которого

$$\left(\frac{\delta_1}{\mathfrak{p}}\right) = c_1, \quad \ldots, \quad \left(\frac{\delta_r}{\mathfrak{p}}\right) = c_r, \quad \left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = +1, \quad \ldots, \quad \left(\frac{\delta_t}{\mathfrak{p}}\right) = +1. \tag{3}$$

Пусть π — примарное число для $\mathfrak{p}$. Тогда по теореме 37

$$\left(\frac{\pi}{\mathfrak{d}_i}\right) = \left(\frac{\delta_i}{\mathfrak{p}}\right) \qquad (i = 1, 2, \ldots, t).$$

Ввиду (1), (2), (3) мы имеем

$$\left(\frac{\delta_1 \ldots \delta_t}{\mathfrak{p}}\right) = \left(\frac{\varepsilon\alpha^2\mu}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right) = +1,$$

т. е. $\mathfrak{p}$ распадается в $K(\sqrt{\mu})$ на два простых множителя. Поскольку

$$\left(\frac{\pi, \mu}{\mathfrak{d}_{r+1}}\right) = \left(\frac{\pi}{\mathfrak{d}_{r+1}}\right) = +1, \qquad \ldots, \qquad \left(\frac{\pi, \mu}{\mathfrak{d}_t}\right) = \left(\frac{\pi}{\mathfrak{d}_t}\right) = +1,$$

каждый из этих двух множителей имеет в поле $K(\sqrt{\mu})$ характеры

$$\left(\frac{\pi, \mu}{\mathfrak{d}_1}\right) = \left(\frac{\pi}{\mathfrak{d}_1}\right) = c_1, \qquad \ldots, \qquad \left(\frac{\pi, \mu}{\mathfrak{d}_r}\right) = \left(\frac{\pi}{\mathfrak{d}_r}\right) = c_r.$$

Далее, очевидно, что единицы $c_1, \ldots, c_r$ можно выбрать 2^{r-1} способами так, чтобы выполнялось условие $c_1 \ldots c_r = +1$. По только что доказанному любая такая система из r единиц действительно соответствует некоторому роду в $K(\sqrt{\mu})$, а так как по теореме 26 число родов g в $K(\sqrt{\mu})$ не превосходит 2^{r-1}, то теорема 41 доказана для случая, когда относительный дискриминант поля $K(\sqrt{\mu})$ взаимно прост с 2. Доказательство теоремы 41 в общем случае будет приведено только в § 41.

§ 30. Одна система из $m/2+z$ взаимно простых с 2 простых идеалов поля k

Мы выведем теперь теорему, которая будет использоваться в последующих параграфах и которая является обобщением теоремы 20.

Теорема 42. *Пусть* $\varepsilon_1, \ldots, \varepsilon_{m/2}$, $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$, $\varkappa_1, \ldots, \varkappa_{m/2}$ — *те же, что и в теореме* 29; *далее, запишем*

$$r = \mathfrak{l}_1^{l_1} \ldots \mathfrak{l}_z^{l_z},$$

где $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ — *попарно различные простые множители числа* 2 *в* k *и* $l_1, \ldots, l_z$ — *показатели степеней, в которых каждый из этих простых множителей входит в* 2. *Запишем*

$$\mathfrak{l}_1^h = (\lambda_1), \qquad \ldots, \qquad \mathfrak{l}_z^h = (\lambda_z),$$

где $\lambda_1, \ldots, \lambda_z$ — *некоторые целые числа в* k; *наконец, пусть* $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$ — *такие примарные простые идеалы, что*

$$\left(\frac{\lambda_i}{\mathfrak{p}_i}\right) = -1, \qquad \left(\frac{\lambda_k}{\mathfrak{p}_i}\right) = +1 \qquad (i \neq k, \quad i, k = 1, 2, \ldots, z)$$

и пусть $\pi_1, \ldots, \pi_z$ — *примарные числа примарных простых идеалов* $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$ *соответственно. Тогда для произвольного взаимно простого с* 2 *целого числа* ω *в* k *имеет место сравнение вида*

$$\omega \equiv \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \pi_1^{w_1} \ldots \pi_z^{w_z} \alpha^2, \qquad (\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}),$$

где показатели $u_1, \ldots, u_{m/2}$, $v_1, \ldots, v_{m/2}$, $w_1, \ldots, w_z$ *принимают значения* 0 *или* 1, *а* α — *подходящее целое число в* k.

Доказательство. Прежде всего рассмотрим такое предположение: существуют $m+z$ показателей $u_1, \ldots, u_{m/2}$, $v_1, \ldots, v_{m/2}$, $w_1, \ldots, w_z$, которые принимают значения 0 или 1, но не все равны 0, и которые удовлетворяют условию: построенное с помощью этих показателей число

$$\mu = \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \pi_1^{w_1} \ldots \pi_z^{w_z} \tag{1}$$

сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$. Тогда число $\sqrt{\mu}$ определяет, очевидно, относительное квадратичное поле $K(\sqrt{\mu})$, и по теореме 5 относительный дискриминант этого поля взаимно прост с 2. Из доказательства теоремы 29 следует, что все показатели $u_1, \ldots, u_{m/2}$, $v_1, \ldots, v_{m/2}$ в выражении (1) равны 0. Учитывая теорему 4, получаем, что относительный дискриминант $K(\sqrt{\mu})$ не содержит в качестве множителей ни одного из простых идеалов $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$, $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$, а из простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_z$ содержит только те, для которых соответствующие показатели $w_1, \ldots, w_z$ в (1) равны 1; пусть это будут, скажем, t простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$. Тогда вследствие наших предположений должно быть $t > 0$.

Теперь мы можем применить теорему 41, так как она была доказана в § 29 как раз для соответствующего случая. Согласно этой теореме, поскольку здесь $r = t$, в поле $K(\sqrt{\mu})$ имеется ровно 2^{t-1} родов, и для любого

рода произведение всех характеров равно $+1$. Так как μ сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}$, то, в частности, простой идеал $\mathfrak{l}_1$ распадается в поле $K(\sqrt{\mu})$ на два простых множителя. Очевидно, характеры каждого из этих простых множителей суть

$$\left(\frac{\lambda_1,\mu}{\mathfrak{p}_1}\right),\quad \dots,\quad \left(\frac{\lambda_1,\mu}{\mathfrak{p}_t}\right),$$

а так как их произведение должно равняться $+1$, мы заключаем, что

$$\left(\frac{\lambda_1}{\mathfrak{p}_1}\right)\dots\left(\frac{\lambda_1}{\mathfrak{p}_t}\right)=+1.$$

Но это противоречит нашим предположениям относительно простых идеалов $\mathfrak{p}_1,\dots,\mathfrak{p}_z$ (см. формулировку теоремы), и тем самым предположение, сделанное в начале доказательства, должно быть отвергнуто, т. е. выражение вида (1) может быть сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}$ только тогда, когда все показатели $u_1,\dots,u_{m/2}$, $v_1,\dots,v_{m/2}$, $w_1,\dots,w_z$ равны 0.

Теперь положим для краткости

$$L_1=n(\mathfrak{l}_1)^{l_1}(n(\mathfrak{l}_1)-1)$$

и будем понимать под

$$\alpha_1^{(1)},\quad \dots,\quad \alpha_1^{(L_1)}$$

какую-нибудь полную систему целых чисел в k, взаимно простых с $\mathfrak{l}_1$, попарно не сравнимых по модулю $\mathfrak{l}_1^{l_1+1}$ и сравнимых с 1 по модулю $\mathfrak{l}_2^{l_2+1}\mathfrak{l}_3^{l_3+1}\dots\mathfrak{l}_z^{l_z+1}$. Так как

$$\alpha_1^{(i)}\not\equiv-\alpha_1^{(i)},\qquad (\mathfrak{l}_1^{l_1+1})\qquad (i=1,2,\dots,L_1),$$

то мы можем считать, что, скажем,

$$-\alpha_1^{(i)}\equiv\alpha_1^{(L_1/2+i)},\qquad (\mathfrak{l}_1^{l_1+1})\qquad (i=1,2,\dots,L_1/2).$$

Тогда, очевидно, $L_1/2$ чисел $\alpha_1^{(1)},\dots,\alpha_1^{(L_1/2)}$ обладают тем свойством, что ни сумма, ни разность никаких двух из них не делится на $\mathfrak{l}_1^{l_1+1}$. Далее, положим для краткости

$$L_2=n(\mathfrak{l}_2)^{l_2}(n(\mathfrak{l}_2)-1),$$

$$\dots\dots\dots\dots\dots\dots$$

$$L_z=n(\mathfrak{l}_z)^{l_z}(n(\mathfrak{l}_z)-1)$$

и построим таким же способом, как и выше, систему из $L_2/2$ целых взаимно простых с $\mathfrak{l}_2$ чисел

$$\alpha_2^{(1)},\quad \dots,\quad \alpha_2^{(L_2/2)},$$

которые все сравнимы с 1 по модулю $\mathfrak{l}_1^{l_1+1}\mathfrak{l}_3^{l_3+1}\dots\mathfrak{l}_z^{l_z+1}$ и обладают тем свойством, что ни сумма, ни разность никаких двух из них не делится на $\mathfrak{l}_2^{l_2+1}$, и т. д. Под конец построим систему из $L_z/2$ целых взаимно простых с $\mathfrak{l}_z$ чисел

$$\alpha_z^{(1)},\quad \dots,\quad \alpha_z^{(L_z/2)},$$

которые все сравнимы с 1 по модулю $\mathfrak{l}_1^{l_1+1}\mathfrak{l}_2^{l_2+1}\dots\mathfrak{l}_{z-1}^{l_{z-1}+1}$ и обладают тем свойством, что ни сумма, ни разность никаких двух из них не делится на $\mathfrak{l}_z^{l_z+1}$.

Числа

$$\begin{gathered}\varepsilon_1^{u_1}\dots\varepsilon_{m/2}^{u_{m/2}}\varkappa_1^{v_1}\dots\varkappa_{m/2}^{v_{m/2}}\pi_1^{w_1}\dots\pi_z^{w_z}(\alpha_1^{(i_1)})^2\dots(\alpha_z^{(i_z)})^2 \qquad (2)\\ (u_1,\ \dots,\ u_{m/2},\ v_1,\ \dots,\ v_{m/2},\ w_1,\ \dots,\ w_z=0,1,\\ i_1=1,\ 2,\ \dots,\ L_1/2,\ \dots,\quad i_z=1,\ 2,\ \dots,\ L_z/2)\end{gathered}$$

образуют систему из $2^mL_1\dots L_z$ целых чисел в k, которые все взаимно просты с 2 и попарно не сравнимы по модулю $\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}$. В самом деле, если бы два числа вида (2) были сравнимы друг с другом по модулю $\mathfrak{l}_1^{2l_1+1}\dots$ $\dots\mathfrak{l}_z^{2l_z+1}$, например, если бы было

$$\begin{gathered}\varepsilon_1^{u_1}\dots\varepsilon_{m/2}^{u_{m/2}}\varkappa_1^{v_1}\dots\varkappa_{m/2}^{v_{m/2}}\pi_1^{w_1}\dots\pi_z^{w_z}(\alpha_1^{(i_1)})^2\dots(\alpha_z^{(i_z)})^2\equiv\varepsilon_1^{u'_1}\dots\varepsilon_{m/2}^{u'_{m/2}}\times\\ \times\varkappa_1^{v'_1}\dots\varkappa_{m/2}^{v'_{m/2}}\pi_1^{w'_1}\dots\pi_z^{w'_z}(\alpha_1^{(i'_1)})^2\dots(\alpha_z^{(i'_z)})^2,\qquad(\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\dots\mathfrak{l}_z^{2l_z+1}),\end{gathered}\qquad(3)$$

то ввиду того, что все числа $\alpha_1^{(i)},\dots,\alpha_z^{(i)}$ взаимно просты с 2, из ранее доказанного немедленно следовало бы, что показатели $u_1,\dots,u_{m/2}$, $v_1,\dots,v_{m/2}$, $w_1,\dots,w_z$ совпадают с показателями $u'_1,\dots,u'_{m/2}$, $v'_1,\dots,v'_{m/2}$, $w'_1,\dots,w'_z$ соответственно, и, следовательно, мы имели бы

$$(\alpha_1^{(i_1)})^2\dots(\alpha_z^{(i_z)})^2\equiv(\alpha_1^{(i'_1)})^2\dots(\alpha_z^{(i'_z)})^2,\qquad(\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}).$$

Из этого сравнения последовательно получаем z сравнений

$$\begin{gathered}(\alpha_1^{(i_1)})^2\equiv(\alpha_1^{(i'_1)})^2\quad(\mathfrak{l}_1^{2l_1+1}),\\ \dots\dots\dots\dots\dots\\ (\alpha_z^{(i_z)})^2\equiv(\alpha_z^{(i'_z)})^2\quad(\mathfrak{l}_z^{2l_z+1}).\end{gathered}$$

Первое из этих сравнений показывает, что либо $\alpha_1^{(i_1)}+\alpha_1^{(i'_1)}$, либо $\alpha_1^{(i_1)}-\alpha_1^{(i'_1)}$ должно делиться на $\mathfrak{l}_1^{l_1+1}$ и, значит, должно быть $i_1=i'_1$. Равным образом, мы заключаем, что $i_2=i'_2,\dots,i_z=i'_z$, и, таким образом, выражения в левой и правой частях сравнения (3) не отличаются друг от друга.

Однако по модулю $\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}$ существует ровно

$$n(\mathfrak{l}_1)^{2l_1}\dots n(\mathfrak{l}_z)^{2l_z}(n(\mathfrak{l}_1)-1)\dots(n(\mathfrak{l}_z)-1)=2^mL_1\dots L_z$$

взаимно простых с 2 попарно не сравнимых чисел, и, следовательно, целые числа вида (2) образуют полную систему вычетов указанного вида по модулю $\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}$, в чем и состоит утверждение теоремы 42.

§ 31. Одно свойство некоторых специальных идеалов поля k

Мы продолжим теперь изучение примарных идеалов поля k, начатое в §§ 23 и 26, и выведем следующие две теоремы.

Теорема 43. *Пусть $\mathfrak{a}$ — произвольный взаимно простой с 2 идеал в k, для которого выполняются равенства*

$$\left(\frac{\varepsilon_1}{\mathfrak{a}}\right)=+1, \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{a}}\right)=+1,$$
$$\left(\frac{\lambda_1}{\mathfrak{a}}\right)=+1, \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{a}}\right)=+1.$$

Тогда можно найти целое число α в k, такое что идеал (α) равен $\mathfrak{a}^h$ и, сверх того, α сравнимо по модулю $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ с квадратом некоторого целого числа поля k. Здесь $\varepsilon_1,\ldots,\varepsilon_{m/2}$, $l_1,\ldots,l_{m/2}$, $\lambda_1,\ldots,\lambda_{m/2}$, имеют тот же смысл, что и в теореме 42.

Доказательство. Пусть α^* — какое-либо целое число в k, такое что $(\alpha^*)=\mathfrak{a}^h$. Далее, пусть $\mathfrak{q}_1,\ldots,\mathfrak{q}_{m/2}$, $\mathfrak{p}_1,\ldots,\mathfrak{p}_z$, $\varkappa_1,\ldots,\varkappa_{m/2}$, $\pi_1,\ldots,\pi_z$ означают те же идеалы и те же целые числа поля k, что и в теореме 42. Тогда, как было нами доказано, любое целое взаимно простое с 2 число представимо по модулю $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$ в виде, указанном в теореме 42. Таким образом, мы можем, в частности, записать

$$\alpha^*\equiv\varepsilon^*\varkappa_1^{v_1}\ldots\varkappa_{m/2}^{v_{m/2}}\pi_1^{w_1}\ldots\pi_z^{w_z}\beta^2, \qquad (\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}) \tag{1}$$

где ε^* — подходящая единица в k, показатели $v_1,\ldots,v_{m/2}$, $w_1,\ldots,w_z$ принимают значения 0 или 1, а β — подходящее целое число в k. Отсюда следует, что число

$$\mu=\alpha^*\varepsilon^*\varkappa_1^{v_1}\ldots\varkappa_{m/2}^{v_{m/2}}\pi_1^{w_1}\ldots\pi_z^{w_z}$$

сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$, и по теореме 40 мы получаем равенства

$$\left.\begin{aligned}
&\prod_{(\mathfrak{w})}{}'\left(\frac{\varepsilon_1,\mu}{\mathfrak{w}}\right)=+1, \quad \ldots, \quad \prod_{(\mathfrak{w})}{}'\left(\frac{\varepsilon_{m/2},\mu}{\mathfrak{w}}\right)=+1,\\
&\prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_1,\mu}{\mathfrak{w}}\right)=+1, \quad \ldots, \quad \prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_z,\mu}{\mathfrak{w}}\right)=+1,
\end{aligned}\right\} \tag{2}$$

где произведение $\prod'$ распространяется на все взаимно простые с 2 простые идеалы $\mathfrak{w}$ поля k. Из равенств (2) вытекает, что

$$\left(\frac{\varepsilon_i}{\alpha^*\varkappa_1^{v_1}\ldots\varkappa_{m/2}^{v_{m/2}}\pi_1^{w_1}\ldots\pi_z^{w_z}}\right)=\left(\frac{\varepsilon_i}{\mathfrak{a}}\right)\left(\frac{\varepsilon_i}{\mathfrak{q}_1}\right)^{v_1}\ldots\left(\frac{\varepsilon_i}{\mathfrak{q}_{m/2}}\right)^{v_{m/2}}\left(\frac{\varepsilon_i}{\mathfrak{p}_1}\right)^{w_1}\ldots\left(\frac{\varepsilon_i}{\mathfrak{p}_z}\right)^{w_z}=+1$$
$$(i=1,2,\ldots,m/2), \tag{3}$$

$$\left(\frac{\lambda_k}{\alpha^* \varkappa_1^{v_1} \dots \varkappa_{m/2}^{v_{m/2}} \pi_1^{w_1} \dots \pi_z^{w_z}}\right) = \left(\frac{\lambda_k}{\mathfrak{a}}\right)\left(\frac{\lambda_k}{\mathfrak{q}_1}\right)^{v_1} \dots \left(\frac{\lambda_k}{\mathfrak{q}_{m/2}}\right)^{v_{m/2}} \left(\frac{\lambda_k}{\mathfrak{p}_1}\right)^{w_1} \dots \left(\frac{\lambda_k}{\mathfrak{p}_z}\right)^{w_z} = +1$$
$$(k = 1, 2, \dots, z). \quad (4)$$

Используя предположения теоремы, последовательно заключаем на основании (3) и (4), что все показатели $v_1, \dots, v_{m/2}$, $w_1, \dots, w_z$ равны 0. Следовательно, ввиду (1), число $\alpha = \varepsilon^* \alpha^*$ имеет требуемый в теореме вид.

Утверждение, обратное к теореме 43, гласит следующее.

Теорема 44. *Если α — взаимно простое с 2 целое число в k, сравнимое с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1} \dots \mathfrak{l}_z^{2l_z+1}$, то имеют место равенства*

$$\left(\frac{\varepsilon_1}{\alpha}\right) = +1, \quad \dots, \quad \left(\frac{\varepsilon_{m/2}}{\alpha}\right) = +1,$$
$$\left(\frac{\lambda_1}{\alpha}\right) = +1, \quad \dots, \quad \left(\frac{\lambda_z}{\alpha}\right) = +1,$$

где $\varepsilon_1, \dots, \varepsilon_{m/2}$, $\mathfrak{l}_1, \dots, \mathfrak{l}_z$, $l_1, \dots, l_z$, $\lambda_1, \dots, \lambda_z$ имеют тот же смысл, что и в теореме 42.

Доказательство. Это немедленно следует из теоремы 40, если в утверждаемое этой теоремой равенство подставить в качестве ν по очереди числа $\varepsilon_1, \dots, \varepsilon_{m/2}$, $\lambda_1, \dots, \lambda_z$, а в качестве μ брать каждый раз число α.

Теоремы 43 и 44 образуют существенную составную часть *второго дополнения* к общему закону взаимности для квадратичных вычетов, который будет установлен позже. Благодарная задача — подыскать для теорем 43 и 44 численные примеры в том же роде, как это было сделано в § 27 для соответствующих утверждений первого дополнения. Ввиду большого числа возможных типов разложения числа 2 в различных полях k, утверждения второго дополнения дают даже еще больше конкретных арифметических фактов, чем в случае первого дополнения.

§ 32. Символ $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ для произвольных взаимно простых с 2 чисел ν, μ

Мы в состоянии теперь установить и доказать теоремы, отвечающие теоремам 14 и 15, если в качестве $\mathfrak{w}$ взять входящий множителем в 2 простой идеал поля k. Для достижения этой цели мы вводим новый символ $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$; однако этот символ послужит нам только для временного использования, так как позже будет установлено, что он совпадает с символом $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$.

Определение 17. Пусть ν, μ — взаимно простые с 2 целые числа в k. Далее, пусть $\mathfrak{l}$ — входящий множителем в 2 простой идеал поля k. Запишем $2 = \mathfrak{l}^l \mathfrak{L}$, где l — некоторый положительный показатель степени

и $\mathfrak{L}$ — взаимно простой с $\mathfrak{l}$ идеал поля k. Наш новый символ определяется равенством

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right).$$

Здесь произведение $\prod_{(\mathfrak{w})}{}'$ распространяется на все простые идеалы $\mathfrak{w}$, взаимно простые с 2, а μ^* — какое-либо взаимно простое с 2 целое число в k, удовлетворяющее сравнениям

$$\mu^* \equiv \mu, \qquad (\mathfrak{l}^{2l}),$$
$$\mu^* \equiv \alpha^2, \qquad (\mathfrak{L}^2),$$

где α — какое-либо взаимно простое с $\mathfrak{L}$ целое число в k.

Символ $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ определен этим правилом однозначно. Действительно, если μ_0^* — целое число в k, удовлетворяющее сравнениям

$$\mu_0^* \equiv \mu, \qquad (\mathfrak{l}^{2l}),$$
$$\mu_0^* \equiv \alpha_0^2, \qquad (\mathfrak{L}^2),$$

где α_0 — некоторое взаимно простое с $\mathfrak{L}$ и отличное от α целое число в k, то можно найти два целых числа ξ, ξ_0 в k, удовлетворяющих сравнениям

$$\xi\xi_0\mu \equiv 1, \qquad (\mathfrak{l}^{2l}),$$
$$\left.\begin{aligned} \xi\alpha &\equiv 1, \\ \xi_0\alpha &\equiv 1, \end{aligned}\right\} \qquad (\mathfrak{L}^2).$$

Тогда для числа $\zeta = \xi^2\xi_0^2\mu^*\mu_0^*$ выполняется сравнение $\zeta \equiv 1$ по модулю 2^2, и, следовательно, по теореме 36, мы получаем

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \zeta}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*\mu_0^*}{\mathfrak{w}}\right) = +1$$

и тем самым

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu_0^*}{\mathfrak{w}}\right),$$

где произведение $\prod'$ распространяется на все взаимно простые с 2 простые идеалы $\mathfrak{w}$ в k.

Привлекая две последние формулы теоремы 14, из определения символа $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ мы немедленно получаем две соответствующие формулы для этого нового символа. Мы отразим этот факт в виде следующей теоремы.

Теорема 45 (лемма). *Если ν, ν_1, ν_2, μ, μ_1, μ_2 — произвольные взаимно простые с 2 целые числа поля k, то для любого входящего множителем в 2 простого идеала $\mathfrak{l}$ имеют место формулы*

$$\left(\frac{\nu_1\nu_2, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu_1, \mu}{\mathfrak{l}}\right)\left(\frac{\nu_2, \mu}{\mathfrak{l}}\right), \qquad \left(\frac{\nu, \mu_1\mu_2}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu_1}{\mathfrak{l}}\right)\left(\frac{\nu, \mu_2}{\mathfrak{l}}\right).$$

§ 33. Совпадение символов $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ и $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ для произвольных взаимно простых с 2 чисел ν, μ

Доказательство того факта, что символы $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ и $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ совпадают друг с другом, мы дадим в виде следующей цепочки лемм.

Теорема 46 (лемма). *Пусть, как и в определении* 17, $\mathfrak{l}$ — *простой множитель числа* 2 *в поле* k, *и пусть* $\mathfrak{l}$ *входит в* 2 *точно в* l-*й степени. Далее, пусть* ϱ — *целое или дробное число в* k, *для которого имеет место сравнение*

$$\varrho \equiv \alpha^2, \qquad (\mathfrak{l}^{2l+1}),$$

где α — *некоторое целое взаимно простое с* 2 *число в* k. *Тогда и для любой степени* $\mathfrak{l}^L$ *с бо́льшим показателем* L *всегда можно найти в* k *целое число* α_L, *удовлетворяющее сравнению*

$$\varrho \equiv \alpha_L^2, \qquad (\mathfrak{l}^L).$$

Доказательство. Предположим, что для степени $\mathfrak{l}^{2l+a}$ $(a \geqslant 1)$ уже найдено число α_{2l+a} с требуемым свойством. Мы получим число α_{2l+a+1} для степени $\mathfrak{l}^{2l+a+1}$ следующим способом. Выберем сначала целое число λ в k, которое делится на $\mathfrak{l}$, но не на $\mathfrak{l}^2$, и положим

$$\alpha_{2l+a+1} = \alpha_{2l+a} + 2\lambda^a\xi,$$

где ξ — целое число в k, подлежащее определению. Из сравнения

$$\varrho \equiv \alpha_{2l+a+1}^2 = \alpha_{2l+a}^2 + 4\alpha_{2l+a}\lambda^a\xi + 4\lambda^{2a}\xi^2, \qquad (\mathfrak{l}^{2l+a+1}),$$

вытекает, что

$$\varrho \equiv \alpha_{2l+a}^2 + 4\alpha_{2l+a}\lambda^a\xi, \qquad (\mathfrak{l}^{2l+a+1}).$$

Поэтому если мы определим ξ из сравнения

$$\xi \equiv \frac{\varrho - \alpha_{2l+a}^2}{4\alpha_{2l+a}\lambda^a}, \qquad (\mathfrak{l}),$$

то α_{2l+a+1} будет числом с требуемым свойством, чем теорема и доказана.

Теорема 47 (лемма). *Пусть* $\mathfrak{l}$ — *простой множитель числа* 2 *в поле* k, *и пусть* $\mathfrak{l}$ *входит в* 2 *ровно в* l-*й степени. Тогда, если* ν_1, ν_2, μ_1, μ_2 — *взаимно простые с* 2 *целые числа в* k, *такие что дроби* $\frac{\nu_1}{\nu_2}$ *и* $\frac{\mu_1}{\mu_2}$ *сравнимы с квадратами некоторых целых чисел в* k *по модулю* $\mathfrak{l}^{2l+1}$, *то*

$$\left(\frac{\nu_1,\mu_1}{\mathfrak{l}}\right) = \left(\frac{\nu_2,\mu_2}{\mathfrak{l}}\right).$$

Доказательство. Предположим сначала, что μ_1 не является квадратом никакого числа в k, а ν_1 является норменным вычетом в поле $K(\sqrt{\mu_1})$ относительно $\mathfrak{l}$. Будем понимать под L какой-либо показатель, а под A — такое целое число в $K(\sqrt{\mu_1})$, что $\nu_1 \equiv N(\mathrm{A})$ по модулю $\mathfrak{l}^L$. Так как $\frac{\nu_1}{\nu_2}$,

а следовательно, и $\frac{\nu_2}{\nu_1}$ сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}^{2l+1}$, то по теореме 46 для произвольного показателя L должно существовать целое число α_L в k, квадрат которого сравним с дробью $\frac{\nu_2}{\nu_1}$ по модулю $\mathfrak{l}^L$. Тем самым мы имеем

$$\nu_2 \equiv \alpha_L^2 \nu_1 \equiv N(\alpha_L \mathsf{A}), \qquad (\mathfrak{l}^L), \tag{1}$$

т. е. ν_2 является норменным вычетом относительно $\mathfrak{l}$ в поле $K(\sqrt{\mu_1})$.

Запишем теперь

$$\alpha_L \mathsf{A} = \frac{\alpha + \beta\sqrt{\mu_1}}{\gamma}. \tag{2}$$

Здесь α, β, γ — некоторые целые числа в k, причем $\mathfrak{l}$ входит в γ точно в c-й степени. Ввиду сделанного относительно $\frac{\mu_1}{\mu_2}$ предположения мы можем, согласно теореме 46, найти такое число β_L, что

$$\frac{\mu_1}{\mu_2} \equiv \beta_L^2, \quad \text{т. е.} \quad \mu_1 \equiv \mu_2 \beta_L^2, \qquad (\mathfrak{l}^{L+2c}). \tag{3}$$

Из (1), (2), (3) получаем

$$\nu_2 \gamma^2 \equiv \alpha^2 - \beta^2 \mu_1 \equiv \alpha^2 - \beta^2 \beta_L^2 \mu_2, \qquad (\mathfrak{l}^{L+2c}). \tag{4}$$

Пусть теперь δ — какое-либо взаимно простое с $\mathfrak{l}$ и делящееся на $\frac{\gamma}{\mathfrak{l}^c}$ число в k. Тогда

$$\mathsf{A}^* = \frac{\delta(\alpha + \beta\beta_L\sqrt{\mu_2})}{\gamma}$$

является целым числом в $K(\sqrt{\mu_2})$, так как, очевидно, сумма и произведение числа A^* и его относительно сопряженного $S\mathsf{A}^*$ являются целыми числами в k. Используя (4), получаем

$$N(\mathsf{A}^*) \equiv \delta^2 \nu_2, \qquad (\mathfrak{l}^L),$$

а так как δ взаимно просто с $\mathfrak{l}$, то тем самым ν_2 оказывается норменным вычетом поля $K(\sqrt{\mu_2})$ относительно $\mathfrak{l}$.

Итак, мы доказали, что всякий раз, когда $\left(\frac{\nu_1,\mu_1}{\mathfrak{l}}\right) = +1$, должно быть и $\left(\frac{\nu_2,\mu_2}{\mathfrak{l}}\right) = +1$. Наоборот, на том же основании из равенства $\left(\frac{\nu_2,\mu_2}{\mathfrak{l}}\right) = +1$, где μ_2 не является квадратом никакого числа в k, всякий раз следует, что и $\left(\frac{\nu_1,\mu_1}{\mathfrak{l}}\right) = +1$. Тем самым установлена справедливость нашей теоремы в случае, когда ни одно из чисел μ_1, μ_2 не является квадратом в k.

Предположим теперь, что одно из этих двух чисел, например μ_2, является квадратом целого числа в k, а μ_1 — нет. Тогда, согласно определению 6, $\left(\frac{\nu_2,\mu_2}{\mathfrak{l}}\right) = +1$, и из предположений доказываемой теоремы вытекает, что μ_1 должно быть сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}^{2l+1}$. Мы хотим доказать, что в этом случае и $\left(\frac{\nu_1,\mu_1}{\mathfrak{l}}\right) = +1$.

С этой целью обозначим, как и в теореме 40, через $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ все (попарно различные) простые идеалы, входящие множителем в 2, и будем считать, что $\mathfrak{l}_i$ входит в 2 точно в l_i-й степени, так что

$$2 = \mathfrak{l}_1^{l_1} \mathfrak{l}_2^{l_2} \ldots \mathfrak{l}_z^{l_z}.$$

Возьмем $\mathfrak{l} = \mathfrak{l}_1$, $l = l_1$ и найдем целое число μ_1^* в k, удовлетворяющее сравнениям

$$\left.\begin{aligned} \mu_1^* &\equiv \mu_1, \qquad (\mathfrak{l}_1^{2l_1+1}), \\ \mu_1^* &\equiv 1, \qquad (\mathfrak{l}_2^{2l_2} \ldots \mathfrak{l}_z^{2l_z}). \end{aligned}\right\} \tag{5}$$

а затем найдем простой идеал $\mathfrak{p}$ в k, для которого выполняются равенства

$$\left.\begin{aligned} \left(\frac{\varepsilon_1}{\mathfrak{p}}\right) &= \left(\frac{\varepsilon_1}{\mu_1^*}\right), \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_{m/2}}{\mu_1^*}\right), \\ \left(\frac{\lambda_1}{\mathfrak{p}}\right) &= \left(\frac{\lambda_1}{\mu_1^*}\right), \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\mu_1^*}\right). \end{aligned}\right\} \tag{6}$$

Здесь $\varepsilon_1, \ldots, \varepsilon_{m/2}$, $\lambda_1, \ldots, \lambda_z$ имеют тот же смысл, что и в теореме 42. Так как, ввиду (6),

$$\left(\frac{\varepsilon_1}{\mathfrak{p}\mu_1^*}\right) = +1, \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}\mu_1^*}\right) = +1,$$

$$\left(\frac{\lambda_1}{\mathfrak{p}\mu_1^*}\right) = +1, \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{p}\mu_1^*}\right) = +1,$$

в силу теоремы 43 мы можем указать такое целое число α, что идеал (α) равен $\mathfrak{p}^h \mu_1^{*h}$ и, кроме того, число α сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$. Мы положим $\pi = \dfrac{\alpha}{\mu_1^{*h}}$. Тогда $(\pi) = \mathfrak{p}^h$.

Теперь мы возьмем простой идеал $\mathfrak{q}$ в k, для которого выполняются равенства

$$\left.\begin{aligned} \left(\frac{\varepsilon_1}{\mathfrak{q}}\right) &= \left(\frac{\varepsilon_1}{\nu_1}\right), \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_{m/2}}{\nu_1}\right), \\ \left(\frac{\lambda_1}{\mathfrak{q}}\right) &= \left(\frac{\lambda_1}{\nu_1}\right), \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{q}}\right) = \left(\frac{\lambda_z}{\nu_1}\right), \\ \left(\frac{\pi}{\mathfrak{q}}\right) &= +1. \end{aligned}\right\} \tag{7}$$

Поступая, как и выше, мы можем согласно теореме 43 найти такое целое число β, что идеал (β) равен $\mathfrak{q}^h \nu_1^h$ и, кроме того, число β сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$. Полагая $\varkappa = \dfrac{\beta}{\nu_1^h}$, имеем $(\varkappa) = \mathfrak{q}^h$.

Учитывая свойства чисел α, β и применяя теорему 47 для уже разобранного нами случая, получаем

$$\left(\frac{\nu_1, \mu_1}{\mathfrak{l}}\right) = \left(\frac{\varkappa, \pi}{\mathfrak{l}}\right). \tag{8}$$

Теперь рассмотрим поле $K(\sqrt{\pi})$ и докажем, что $\varkappa$ равно относительной норме некоторого числа из этого поля, имеющего знаменатель, взаимно простой с 2. Ввиду сравнений (5) μ_1^*, а следовательно, и π сравнимо с квадратом некоторого целого числа в k по модулю 2^2. Значит, по теоремам 4 и 5 относительный дискриминант поля $K(\sqrt{\pi})$ содержит только один простой множитель $\mathfrak{p}$. Если мы применим к полю $K(\sqrt{\pi})$ замечание, сделанное в конце § 15, и соответственно положим $t = 1$, то приведенное там неравенство примет вид

$$v^* > m/2 - 1,$$

а так как v^*, очевидно, не может быть больше чем $m/2$, то мы должны иметь $v^* = m/2$, т. е. любая единица в k является относительной нормой некоторой единицы в $K(\sqrt{\pi})$. Число, обозначенное в теореме 23 через v, заведомо не меньше v^*, и, следовательно, тоже равно $m/2$. Поэтому теорема 23 говорит нам, что число всех амбивалентных комплексов в поле $K(\sqrt{\pi})$ равно 1, т. е. главный комплекс является единственным амбивалентным комплексом в поле $K(\sqrt{\pi})$.

Из только что установленных фактов мы легко получаем, что число классов H поля $K(\sqrt{\pi})$ обязательно должно быть нечетным. В противном случае в $K(\sqrt{\pi})$ существовал бы такой идеал $\mathfrak{J}$, что

$$\mathfrak{J} \not\sim 1, \qquad \mathfrak{J}^2 \sim 1.$$

Однако этот идеал $\mathfrak{J}$ не может принадлежать главному комплексу, ибо если бы $\mathfrak{J}$ был эквивалентен некоторому идеалу $\mathfrak{j}$ в k, то должно было бы быть

$$\mathfrak{J}^h \sim \mathfrak{j}^h \sim 1,$$

а так как h — нечетное число, то из этой эквивалентности следовало бы, что $\mathfrak{J} \sim 1$, чего не может быть. С другой стороны, если положить $N(\mathfrak{J}) = \mathfrak{J} \cdot S\mathfrak{J} = \mathfrak{n}$, то $\mathfrak{n} \cdot \mathfrak{J} \sim S\mathfrak{J}$ и, следовательно, идеал $\mathfrak{J}$ определял бы амбивалентный комплекс в поле $K(\sqrt{\pi})$, отличный от главного комплекса, что противоречит ранее доказанному.

Ввиду равенства (7) идеал $\mathfrak{q}$ распадается в поле $K(\sqrt{\pi})$. Пусть $\mathfrak{Q}$ — один из двух простых множителей $\mathfrak{q}$. Положим $\mathfrak{Q}^{hH} = (\mathsf{A})$, где A — некоторое целое число поля $K(\sqrt{\pi})$. Тогда главный идеал $\mathfrak{q}^{hH}$ равен относительной норме главного идеала (A), и, следовательно,

$$\varepsilon \varkappa^H = N(\mathsf{A}),$$

где ε — некоторая подходящая единица в k. Но так как по уже доказанному каждая единица в k является относительной нормой некоторой единицы из $K(\sqrt{\pi})$, то и $\varkappa^H$ будет относительной нормой некоторого целого числа A^* в $K(\sqrt{\pi})$. Следовательно, $\varkappa$ — относительная норма числа $\frac{\mathsf{A}^*}{\varkappa^{(H-1)/2}}$, и знаменатель этой дроби взаимно прост с 2. Отсюда по определению 6 следует, что $\left(\frac{\varkappa,\pi}{\mathfrak{l}}\right) = +1$ и, следовательно, ввиду (8) и $\left(\frac{\nu_1,\mu_1}{\mathfrak{l}}\right) = +1$, чем теорема для рассматриваемого случая и доказана.

Наконец, предположим, что каждое из μ_1, μ_2 является квадратом целого числа в k. Тогда по определению 6 мы получим для обоих символов значение $+1$. Тем самым, теорема доказана полностью.

Теорема 48 (лемма). *Пусть* $\mathfrak{l}$ *— некоторый входящий множителем в* 2 *простой идеал и пусть, далее,* ν, μ *— произвольные взаимно простые с* 2 *целые числа в* k. *Тогда если* $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=+1$, *то и* $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=+1$.

Доказательство. Обозначим, как и в теореме 40, через $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ все (попарно различные) входящие множителем в 2 простые идеалы, и пусть $\mathfrak{l}_i$ входит в 2 точно в l_i-й степени, так что

$$2 = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}\ldots\mathfrak{l}_z^{l_z}.$$

Пусть, скажем, $\mathfrak{l}=\mathfrak{l}_1$, и пусть $l=l_1$, $\mathfrak{L}=\mathfrak{l}_2^{l_2}\ldots\mathfrak{l}_z^{l_z}$, так что

$$2 = \mathfrak{l}^l\mathfrak{L},$$

где $\mathfrak{L}$ — некоторый идеал, не делящийся на $\mathfrak{l}$.

Пусть, далее, μ^* — целое число поля k, удовлетворяющее сравнениям

$$\mu^* \equiv \mu, \qquad (\mathfrak{l}^{2l+1}),$$
$$\mu^* \equiv 1, \qquad (\mathfrak{L}^2).$$

Прежде всего возьмем какой-нибудь простой идеал $\mathfrak{p}$ в k, для которого

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right)=\left(\frac{\varepsilon_1}{\mu^*}\right), \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right)=\left(\frac{\varepsilon_{m/2}}{\mu^*}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{p}}\right)=\left(\frac{\lambda_1}{\mu^*}\right), \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{p}}\right)=\left(\frac{\lambda_z}{\mu^*}\right).$$

Здесь $\varepsilon_1,\ldots,\varepsilon_{m/2}$, $\lambda_1,\ldots,\lambda_z$ имеют тот же смысл, что и в теореме 42. Так как тогда

$$\left(\frac{\varepsilon_1}{\mathfrak{p}\mu^*}\right)=+1, \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}\mu^*}\right)=+1,$$
$$\left(\frac{\lambda_1}{\mathfrak{p}\mu^*}\right)=+1, \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{p}\mu^*}\right)=+1,$$

то по теореме 43 мы можем найти такое целое число α, что идеал (α) равен $\mathfrak{p}^h\mu^{*h}$ и, кроме того, число α сравнимо с квадратом некоторого целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\ldots\mathfrak{l}_z^{2l_z+1}$. Полагая $\pi=\frac{\alpha}{\mu^{*h}}$, имеем $(\pi)=\mathfrak{p}^h$.

Теперь возьмем простой идеал $\mathfrak{q}$, для которого

$$\left.\begin{aligned}
&\left(\frac{\varepsilon_1}{\mathfrak{q}}\right)=\left(\frac{\varepsilon_1}{\nu}\right),\ldots,\left(\frac{\varepsilon_{m/2}}{\mathfrak{q}}\right)=\left(\frac{\varepsilon_{m/2}}{\nu}\right),\\
&\left(\frac{\lambda_1}{\mathfrak{q}}\right)=\left(\frac{\lambda_1}{\nu}\right),\ldots,\left(\frac{\lambda_z}{\mathfrak{q}}\right)=\left(\frac{\lambda_z}{\nu}\right),\\
&\left(\frac{\pi}{\mathfrak{q}}\right)=+1.
\end{aligned}\right\} \qquad (1)$$

Поступая, как и прежде, мы можем согласно теореме 43 найти такое целое число β, что идеал (β) равен $\mathfrak{q}^h\nu^h$ и, кроме того, число β сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1},\ldots,\mathfrak{l}_z^{2l_z+1}$. Полагая $\varkappa=\frac{\beta}{\nu^h}$, имеем $(\varkappa)=\mathfrak{q}^h$.

По теореме 40

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\alpha}{\mathfrak{w}}\right)=+1,\qquad \prod_{(\mathfrak{w})}{}'\left(\frac{\beta,\pi}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\pi,\beta}{\mathfrak{w}}\right)=+1,$$

где произведение $\prod'$ распространяется на все простые идеалы $\mathfrak{w}$ поля k, взаимно простые с 2. Учитывая определение 17, получаем отсюда

$$\left(\frac{\nu,\alpha}{\overline{\mathfrak{l}}}\right)=+1,\qquad \left(\frac{\beta,\pi}{\overline{\mathfrak{l}}}\right)=+1,$$

и, следовательно, в силу формул из теоремы 45

$$\left(\frac{\nu,\mu}{\overline{\mathfrak{l}}}\right)=\left(\frac{\nu,\mu^*}{\mathfrak{l}}\right)=\left(\frac{\nu,\mu^{*h}}{\mathfrak{l}}\right)=\left(\frac{\nu,\pi}{\mathfrak{l}}\right)$$

и

$$\left(\frac{\nu,\pi}{\overline{\mathfrak{l}}}\right)=\left(\frac{\nu^h,\pi}{\mathfrak{l}}\right)=\left(\frac{\varkappa,\pi}{\mathfrak{l}}\right).$$

Таким образом, мы получаем окончательно

$$\left(\frac{\nu,\mu}{\overline{\mathfrak{l}}}\right)=\left(\frac{\varkappa,\pi}{\mathfrak{l}}\right),$$

а значит, согласно предположению теоремы,

$$\left(\frac{\varkappa,\pi}{\overline{\mathfrak{l}}}\right)=+1. \tag{2}$$

Так как число μ^*, а следовательно, и число π сравнимо с квадратом целого числа в k по модулю $\mathfrak{L}^2$, то с учетом определения 17 равенство (2) принимает вид

$$\left(\frac{\varkappa,\pi}{\overline{\mathfrak{l}}}\right)=\left(\frac{\pi}{\mathfrak{q}}\right)\left(\frac{\varkappa}{\mathfrak{p}}\right)=+1.$$

На основании (1) мы заключаем, что должно быть

$$\left(\frac{\varkappa}{\mathfrak{p}}\right)=+1. \tag{3}$$

Теперь рассмотрим поле $K(\sqrt{\pi})$ и докажем, что $\varkappa$ равно относительной норме числа из этого поля, у которого знаменатель взаимно прост с 2. С этой целью будем различать три случая.

Первый случай: простой идеал $\mathfrak{p}$ примарен и π — примарное число идеала $\mathfrak{p}$. Тогда относительный дискриминант поля $K(\sqrt{\pi})$ содержит только один простой множитель $\mathfrak{p}$, и в этом случае можно показать, точно так же, как во второй части доказательства теоремы 47, что $\varkappa$ является относительной нормой некоторого числа поля $K(\sqrt{\pi})$, знаменатель которого взаимно прост с 2.

Второй случай: $\mathfrak{p}$ — примарный простой идеал, но π не является примарным числом для $\mathfrak{p}$; пусть $\pi = \varepsilon\pi^*$, где π^* — примарное число для $\mathfrak{p}$, а ε — единица в k, которая не равна квадрату никакой единицы в k. Так как π сравнимо с квадратом целого числа в k по модулю $\mathfrak{L}^2$, то согласно теореме 4 относительный дискриминант поля $K(\sqrt{\pi})$ содержит только два простых идеала $\mathfrak{l}$ и $\mathfrak{p}$. Применяя теорему 23 с $t = 2$ и учитывая, что $v \leqslant m/2$, получим, что $a \leqslant 1$, т. е. число $A = 2^a$ всех амбивалентных комплексов в поле $K(\sqrt{\pi})$ не превосходит 2.

Пусть теперь $\mathfrak{J}$ — какой-либо идеал в $K(\sqrt{\pi})$ и $\mathfrak{j} = N(\mathfrak{J})$ — относительная норма $\mathfrak{J}$. Пусть, далее, $\mathfrak{j}^h = (\iota)$, где ι — некоторое целое число в k. Тогда $\frac{\iota}{\mathfrak{p}} = +1$, так что тот комплекс поля $K(\sqrt{\pi})$, которому принадлежит $\mathfrak{J}$, является комплексом главного рода в $K(\sqrt{\pi})$. Легко показать, что не все комплексы в $K(\sqrt{\pi})$ являются комплексами главного рода. Именно, пусть $\mathfrak{r}$ — простой идеал в k, для которого

$$\left(\frac{\pi}{\mathfrak{r}}\right) = +1 \quad \text{и} \quad \left(\frac{\pi^*}{\mathfrak{r}}\right) = -1.$$

Ввиду первого из этих равенств идеал $\mathfrak{r}$ разложим в $K(\sqrt{\pi})$. Обозначим через $\mathfrak{R}$ простой множитель $\mathfrak{r}$ в $K(\sqrt{\pi})$. Полагая $\mathfrak{r}^h = (\varrho)$, где ϱ — целое число в k, по теореме 37 получаем

$$\left(\frac{\varrho}{\mathfrak{p}}\right) = \left(\frac{\pi^*}{\mathfrak{r}}\right) = -1,$$

и это равенство показывает, что комплекс, определяемый $\mathfrak{R}$ в $K(\sqrt{\pi})$, не является комплексом главного рода.

Обозначим теперь через f' число тех комплексов в $K(\sqrt{\pi})$, которые являются квадратами комплексов из $K(\sqrt{\pi})$, а через f — число всех комплексов главного рода в $K(\sqrt{\pi})$. Тогда точно так же, как в доказательстве теоремы 25, мы убеждаемся в справедливости равенства

$$Af' = 2f. \tag{4}$$

Поскольку $A \leqslant 2$, из этого равенства следует неравенство $f \leqslant f'$. Далее, так как квадрат любого комплекса должен быть комплексом главного рода, то также $f' \leqslant f$ и, следовательно, мы имеем $f = f'$, т. е. каждый комплекс главного рода равен квадрату некоторого комплекса. Ввиду (4) из $f = f'$ следует, что $A = 2$ и $a = 1$. Отсюда, учитывая теорему 23, мы заключаем, что $v = m/2$, т. е. любая единица поля k равна относительной норме некоторого целого или дробного числа поля $K(\sqrt{\pi})$.

Теперь покажем, что $\varkappa$ равно относительной норме некоторого числа из $K(\sqrt{\pi})$. Для этого заметим, что ввиду (1) простой идеал $\mathfrak{q}$ разложим в $K(\sqrt{\pi})$. Тогда равенство (3) показывает, что любой входящий множителем в $\mathfrak{q}$ простой идеал $\mathfrak{Q}$ поля $K(\sqrt{\pi})$ принадлежит комплексу главного рода, а так как по ранее доказанному любой такой комплекс равен квадрату некоторого комплекса, идеал $\mathfrak{q}$ удовлетворяет равенству вида

$$\mathfrak{Q} = \mathfrak{J}^2\mathfrak{A}\mathfrak{j},$$

где $\mathfrak{J}$ — идеал в $K(\sqrt{\pi})$, A — некоторое число в $K(\sqrt{\pi})$ и $\mathfrak{j}$ — некоторый идеал в k. Если мы возьмем относительную норму обеих частей этого равенства и возведем ее в h-ю степень, то получится равенство вида

$$(\varkappa) = N(\mathsf{A})\{N(\mathfrak{J})\mathfrak{j}\}^{2h} = N(\mathsf{A})(\gamma)^2,$$

где γ — подходящее целое число в k; из этого равенства вытекает, что

$$\xi\varkappa = N(\gamma\mathsf{A}),$$

где ξ — некоторая единица в k. Так как по ранее доказанному любая единица в k является относительной нормой некоторого числа из $K(\sqrt{\pi})$, мы заключаем, что и $\varkappa$ должно быть относительной нормой некоторого числа из $K(\sqrt{\pi})$. Наконец, несложное рассуждение показывает, что $\varkappa$ может быть также представлено как относительная норма такого числа, знаменатель которого взаимно прост с 2.

Третий случай: $\mathfrak{p}$ — непримарный простой идеал в k и ζ — единица, для которой $\left(\frac{\zeta}{\mathfrak{p}}\right) = -1$. В этом случае ζ безусловно не может быть относительной нормой никакого целого или дробного числа из $K(\sqrt{\pi})$. Следовательно, здесь число, обозначаемое в теореме 23 через v, меньше или равно $m/2-1$. Так как π сравнимо с квадратом целого числа в k по модулю $\mathfrak{L}^2$, по теореме 4 относительный дискриминант поля $K(\sqrt{\pi})$ взаимно прост с $\mathfrak{L}$, и, следовательно, снова содержит только два простых множителя $\mathfrak{p}$ и $\mathfrak{l}$. Применяя теорему 23 с $t = 2$, получим, ввиду неравенства $v \leqslant m/2 - 1$, что $a \leqslant 0$, т. е. $a = 0$ и $v = m/2 - 1$. Итак, совокупность всех единиц ξ, для которых $\left(\frac{\xi}{\mathfrak{p}}\right) = +1$, образует, очевидно, ровно $2^{m/2-1}$ связок единиц в поле k, а так как те $2^{m/2-1}$ связок единиц η, для которых $\left(\frac{\eta}{\mathfrak{p}}\right) = -1$, не могут содержать единиц, являющихся относительными нормами каких-либо чисел, то мы видим, что все единицы ξ со свойством $\left(\frac{\xi}{\mathfrak{p}}\right) = +1$ должны быть относительными нормами чисел из поля $K(\sqrt{\pi})$.

Далее, из равенства $a = 0$ следует, что единственным амбивалентным комплексом в поле $K(\sqrt{\pi})$ является главный комплекс, откуда, как и во второй части доказательства теоремы 47, мы заключаем, что число классов H поля $K(\sqrt{\pi})$ должно быть нечетным. Снова, как и там, приходим к выводу, что число $\varepsilon\varkappa^H$, где ε — некоторая подходящая единица в k, должно быть равно относительной норме целого числа из $K(\sqrt{\pi})$. Таким образом, имеет место равенство

$$\left(\frac{\varepsilon\varkappa^H}{\mathfrak{p}}\right) = +1,$$

поэтому ввиду (3) должно быть также $\left(\frac{\varepsilon}{\mathfrak{p}}\right) = +1$, а тогда, согласно предыдущему, ε должно быть относительной нормой некоторого числа из $K(\sqrt{\pi})$. Отсюда мы заключаем, что и $\varkappa^H$ должно быть относительной нормой некоторого числа из $K(\sqrt{\pi})$, и, следовательно, $\varkappa$ — относительная норма некоторого числа из $K(\sqrt{\pi})$, а значит и такого числа, знаменатель которого взаимно прост с 2.

Таким образом, во всех трех только что разобранных случаях мы получаем, согласно определению 6,

$$\left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = +1.$$

В начале доказательства мы выбирали $\alpha = \pi\mu^{*h}$ и $\beta = \varkappa\nu^h$ как такие целые числа в k, которые сравнимы с квадратами целых чисел в k по модулю $\mathfrak{l}_1^{2l_1+1} \ldots \mathfrak{l}_z^{2l_z+1}$. Так как $\mu^* \equiv \mu$ по модулю $\mathfrak{l}^{2l+1}$, то из теоремы 47 следует, что

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\varkappa, \pi}{\mathfrak{l}}\right) = +1,$$

чем наша теорема полностью доказана.

Теорема 49 (лемма). *Пусть $\mathfrak{l}$ — входящий множителем в 2 простой идеал, и пусть ν, μ — произвольные взаимно простые с 2 целые числа в k. Тогда если $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$, то и $\left(\frac{\nu, \mu}{\overline{\mathfrak{l}}}\right) = +1$.*

Доказательство. Будем использовать обозначения, введенные в начале доказательства теоремы 48. Подберем целое число μ^*, которое удовлетворяет сравнениям

$$\begin{aligned} \mu^* &\equiv \mu, \qquad (\mathfrak{l}_1^{2l_1+1}), \\ \mu^* &\equiv 1, \qquad (\mathfrak{l}_2^{2l_2+1}\mathfrak{l}_3^{2l_3+1} \ldots \mathfrak{l}_z^{2l_z+1}), \end{aligned}$$

и в то же время не равно квадрату целого числа в k. Тогда согласно теореме 47

$$\begin{aligned} \left(\frac{\nu, \mu^*}{\mathfrak{l}_1}\right) &= \left(\frac{\nu, \mu}{\mathfrak{l}_1}\right) = +1, \\ \left(\frac{\nu, \mu^*}{\mathfrak{l}_i}\right) &= \left(\frac{\nu, 1}{\mathfrak{l}_i}\right) = +1 \qquad (i = 2, 3, \ldots, z), \end{aligned}$$

а значит, в поле $K(\sqrt{\mu^*})$ существуют целые числа $\mathsf{A}_1, \ldots, \mathsf{A}_z$, такие что

$$\begin{aligned} \nu &\equiv N(\mathsf{A}_1), \qquad (\mathfrak{l}_1^{2l_1}), \\ &\cdots\cdots\cdots \qquad \cdots\cdot \\ \nu &\equiv N(\mathsf{A}_z), \qquad (\mathfrak{l}_z^{2l_z}). \end{aligned}$$

Следовательно, если мы возьмем целое число A в $K(\sqrt{\mu^*})$, которое удовлетворяет z сравнениям

$$\begin{aligned} \mathsf{A} &\equiv \mathsf{A}_1, \qquad (\mathfrak{l}_1^{2l_1}), \\ &\cdots\cdots\cdot \qquad \cdots\cdot \\ \mathsf{A} &\equiv \mathsf{A}_z, \qquad (\mathfrak{l}_z^{2l_z}), \end{aligned}$$

то мы будем иметь также

$$\nu \equiv N(\mathsf{A}), \qquad (\mathfrak{l}_1^{2l_1}\mathfrak{l}_2^{2l_2} \ldots \mathfrak{l}_z^{2l_z}),$$

откуда ввиду теоремы 36 вытекает

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu^*}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{N(\mathsf{A}),\mu^*}{\mathfrak{w}}\right),$$

где произведение $\prod'$ распространено на все взаимно простые с 2 простые идеалы $\mathfrak{w}$ в k. Согласно определению 17 произведение слева равно $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$. Согласно же определению 6 все множители правого произведения равны $+1$; отсюда следует, что $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=+1$, чем наша теорема и доказана.

В совокупности теоремы 48 и 49 дают следующий результат:

Теорема 50 (лемма). *Если* $\mathfrak{l}$ *— входящий множителем в* 2 *простой идеал и* ν,μ *— взаимно простые с* 2 *целые числа в* k, *то всегда имеет место равенство*

$$\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=\left(\frac{\nu,\mu}{\overline{\mathfrak{l}}}\right).$$

§ 34. Свойства символа $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ для любых взаимно простых с 2 целых чисел ν,μ

С помощью теоремы 50 мы можем доказать важный факт, что представленные в теореме 14 формулы справедливы также для любого входящего множителем в 2 простого идеала $\mathfrak{l}$. Сформулируем соответствующую теорему.

Теорема 51. *Пусть* $\nu,\nu_1,\nu_2,\mu,\mu_1,\mu_2$ *— произвольные взаимно простые с* 2 *целые числа в* k. *Относительно любого входящего множителем в* 2 *простого идеала* $\mathfrak{l}$ *поля* k *имеют место формулы*

$$\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=\left(\frac{\mu,\nu}{\mathfrak{l}}\right),$$
$$\left(\frac{\nu_1\nu_2,\mu}{\mathfrak{l}}\right)=\left(\frac{\nu_1,\mu}{\mathfrak{l}}\right)\left(\frac{\nu_2,\mu}{\mathfrak{l}}\right),$$
$$\left(\frac{\nu,\mu_1\mu_2}{\mathfrak{l}}\right)=\left(\frac{\nu,\mu_1}{\mathfrak{l}}\right)\left(\frac{\nu,\mu_2}{\mathfrak{l}}\right).$$

Доказательство. Пусть $\mathfrak{l}$ и $\mathfrak{L}$ имеют тот же смысл, что и в определении 17. Для того, чтобы доказать первую из наших формул, подберем два таких целых числа ν^*,μ^* в k, что

$$\left.\begin{aligned}\nu^*&\equiv\nu,\\ \mu^*&\equiv\mu,\end{aligned}\right\}\quad(\mathfrak{l}^{2l+1}),$$

$$\left.\begin{aligned}\nu^*&\equiv 1,\\ \mu^*&\equiv 1,\end{aligned}\right\}\quad(\mathfrak{L}^2).$$

Тогда по теореме 47

$$\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=\left(\frac{\nu^*,\mu}{\mathfrak{l}}\right),\qquad \left(\frac{\mu,\nu}{\mathfrak{l}}\right)=\left(\frac{\mu^*,\nu}{\mathfrak{l}}\right),$$

и, следовательно ввиду теоремы 50 также

$$\left(\frac{\nu,\mu}{\overline{\mathfrak{l}}}\right)=\left(\frac{\nu^*,\mu}{\overline{\mathfrak{l}}}\right),\qquad \left(\frac{\mu,\nu}{\overline{\mathfrak{l}}}\right)=\left(\frac{\mu^*,\nu}{\overline{\mathfrak{l}}}\right). \tag{1}$$

Теперь по определению 17

$$\left(\frac{\nu^*,\mu}{\overline{\mathfrak{l}}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\mu^*}{\mathfrak{w}}\right),\qquad \left(\frac{\mu^*,\nu}{\overline{\mathfrak{l}}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\mu^*,\nu^*}{\mathfrak{w}}\right), \tag{2}$$

а так как согласно первой формуле теоремы 14

$$\left(\frac{\nu^*,\mu^*}{\mathfrak{w}}\right)=\left(\frac{\mu^*,\nu^*}{\mathfrak{w}}\right)$$

для любого простого идеала $\mathfrak{w}$ взаимно простого с 2, из (2) следует, что и

$$\left(\frac{\nu^*,\mu}{\overline{\mathfrak{l}}}\right)=\left(\frac{\mu^*,\nu}{\overline{\mathfrak{l}}}\right),$$

а значит, ввиду (1)

$$\left(\frac{\nu,\mu}{\overline{\mathfrak{l}}}\right)=\left(\frac{\mu,\nu}{\overline{\mathfrak{l}}}\right).$$

Тем самым, ввиду теоремы 50, справедливость первой из доказываемых формул установлена.

Две другие формулы немедленно следуют из теорем 45 и 50.

§ 35. Произведение $\prod_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$ для произвольных взаимно простых с 2 чисел ν,μ

Мы в состоянии теперь доказать теорему, представляющую собой существенное обобщение теоремы 36.

Теорема 52. *Для любых взаимно простых с 2 целых чисел ν,μ в k*

$$\prod_{(\mathfrak{w})}\left(\frac{\nu,\mu}{\mathfrak{w}}\right)=+1,$$

где произведение распространяется на все простые идеалы $\mathfrak{w}$ поля k.

Доказательство. Будем использовать обозначения, введенные в теореме 40. Возьмем z таких целых чисел $\mu_1,\mu_2,\ldots,\mu_z$ в k, что имеют место

сравнения

$$\left.\begin{array}{lllll} \mu_1 \equiv \mu, & \mu_2 \equiv 1, & \ldots, & \mu_z \equiv 1, & (\mathfrak{l}_1^{2l_1}), \\ \mu_1 \equiv 1, & \mu_2 \equiv \mu, & \ldots, & \mu_z \equiv 1, & (\mathfrak{l}_2^{2l_2}), \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots & \ldots \\ \mu_1 \equiv 1, & \mu_2 \equiv 1, & \ldots, & \mu_z \equiv \mu, & (\mathfrak{l}_z^{2l_z}). \end{array}\right\} \tag{1}$$

Очевидно, что произведение этих z чисел удовлетворяет сравнению

$$\mu_1\mu_2 \ldots \mu_z \equiv \mu, \qquad (2^2). \tag{2}$$

С учетом сравнений (1) определение (17) дает равенства

$$\left(\frac{\nu, \mu}{\mathfrak{l}_i}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu_i}{\mathfrak{w}}\right) \qquad (i = 1, 2, \ldots, z),$$

откуда ввиду теоремы 50 вытекает следующая система равенств

$$\left(\frac{\nu, \mu}{\mathfrak{l}_i}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu_i}{\mathfrak{w}}\right) \qquad (i = 1, 2, \ldots, z), \tag{3}$$

где произведение $\prod'$ распространяется на все простые идеалы $\mathfrak{w}$ в k, взаимно простые с 2. Перемножая z равенств (3), получаем равенство

$$\left(\frac{\nu, \mu}{\mathfrak{l}_1}\right)\left(\frac{\nu, \mu}{\mathfrak{l}_2}\right) \cdots \left(\frac{\nu, \mu}{\mathfrak{l}_z}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu_1\mu_2 \ldots \mu_z}{\mathfrak{w}}\right),$$

а умножая его на $\prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu}{\mathfrak{w}}\right)$, мы приходим к равенству

$$\prod_{(\mathfrak{w})} \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu\mu_1\mu_2 \ldots \mu_z}{\mathfrak{w}}\right), \tag{4}$$

где справа стоит произведение по всем простым идеалам $\mathfrak{w}$, взаимно простым с 2, а слева — произведение по всем простым идеалам $\mathfrak{w}$ в k. Далее, ввиду сравнения (2) число $\mu\mu_1\mu_2 \ldots \mu_z$ сравнимо с квадратом целого числа в k по модулю 2^2, а следовательно, согласно теореме 36 правая часть (4) равна $+1$, чем теорема 52 и доказана.

§ 36. Общий закон взаимности для квадратичных вычетов и первое дополнение к нему

Отметим два особенно важных следствия теоремы 52.

Теорема 53. *Пусть* $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ — *простые идеалы поля* k, *входящие множителем в* 2, *и* ε — *некоторая единица в* k. *Пусть, далее,* $\mathfrak{p}$ — *простой идеал, взаимно простой с* 2, *и* π — *такое целое число в* k, *что* $(\pi) = \mathfrak{p}^h$. *Тогда справедливо равенство*

$$\left(\frac{\varepsilon}{\mathfrak{p}}\right) = \left(\frac{\varepsilon, \pi}{\mathfrak{l}_1}\right)\left(\frac{\varepsilon, \pi}{\mathfrak{l}_2}\right) \cdots \left(\frac{\varepsilon, \pi}{\mathfrak{l}_z}\right).$$

Эту теорему мы будем называть *первым дополнением к общему закону взаимности для квадратичных вычетов в поле k.*

Теорема 54. *Пусть $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ — простые идеалы поля k, входящие множителем в 2. Далее, пусть $\mathfrak{p}$, $\mathfrak{q}$ — некоторые простые идеалы, взаимно простые с 2, и $\pi, \varkappa$ — целые числа в k, такие что $(\pi) = \mathfrak{p}^h$, $(\varkappa) = \mathfrak{q}^h$. Тогда имеет место равенство*

$$\left(\frac{\pi}{\mathfrak{q}}\right)\left(\frac{\varkappa}{\mathfrak{p}}\right) = \left(\frac{\pi, \varkappa}{\mathfrak{l}_1}\right)\left(\frac{\pi, \varkappa}{\mathfrak{l}_2}\right) \ldots \left(\frac{\pi, \varkappa}{\mathfrak{l}_z}\right).$$

Эту теорему будем называть *общим законом взаимности для квадратичных вычетов в поле k.*

Теоремы 53 и 54 немедленно следуют из теоремы 52, если положить в ней сначала $\nu = \varepsilon$, $\mu = \pi$, а затем $\nu = \pi$, $\mu = \varkappa$.

§ 37. Символ $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ для произвольных целых чисел ν, μ

Теперь мы обобщим определение 17 символа $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ на случай, когда ν, μ — произвольные целые числа в k. Окажется, что этот обобщенный символ снова будет совпадать с символом $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$.

Определение 18. Пусть, как и прежде, $\mathfrak{l}_1 = \mathfrak{l}, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ — попарно различные простые множители числа 2, и пусть простой идеал $\mathfrak{l}_1 = \mathfrak{l}$ входит в 2 точно в $l_1 = l$-й степени, а простые идеалы $\mathfrak{l}_2, \ldots, \mathfrak{l}_z$ входят в 2 в степенях $l_2, \ldots, l_z$ соответственно. Наконец, пусть ν, μ — произвольные целые числа в k, и пусть в μ входит множителем ровно a-я степень $\mathfrak{l}$. Тогда *символ* $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ определяется равенством

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\nu, \mu^*}{\mathfrak{w}}\right).$$

Здесь произведение $\prod_{(\mathfrak{w})}{}'$ распространено на все простые идеалы $\mathfrak{w}$, взаимно простые с 2, а μ^* — любое целое число, удовлетворяющее сравнениям

$$\mu^* \equiv \mu, \qquad (\mathfrak{l}^{2l+1+a}),$$

$$\mu^* \equiv \alpha^2, \qquad (\mathfrak{l}_2^{2l_2+1} \ldots \mathfrak{l}_z^{2l_z+1}),$$

где α — какое-либо целое число в k, взаимно простое с $\mathfrak{l}_2, \mathfrak{l}_3, \ldots, \mathfrak{l}_z$.

Как и в § 32, только вместо используемой там теоремы 36 применяя теорему 40, мы видим, что символ $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ однозначно определен этим правилом.

Из определения 18, привлекая две последние формулы теоремы 14, легко получаем следующее утверждение, соответствующее теореме 45.

Теорема 55 (лемма). *Пусть $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ — произвольные целые числа в k. Для любого входящего множителем в 2 простого идеала $\mathfrak{l}$ имеют место формулы*

$$\left(\frac{\nu_1\nu_2,\mu}{\mathfrak{l}}\right) = \left(\frac{\nu_1,\mu}{\mathfrak{l}}\right)\left(\frac{\nu_2,\mu}{\mathfrak{l}}\right),$$

$$\left(\frac{\nu,\mu_1\mu_2}{\mathfrak{l}}\right) = \left(\frac{\nu,\mu_1}{\mathfrak{l}}\right)\left(\frac{\nu,\mu_2}{\mathfrak{l}}\right).$$

§ 38. Совпадение символов $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ и $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ для произвольных целых чисел ν, μ

Доказательство того факта, что символы $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ и $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ совпадают для произвольных целых чисел ν, μ, мы оформим в виде следующей цепочки лемм.

Теорема 56 (лемма). *Пусть $\mathfrak{l}$ — простой множитель числа 2 в поле k, и пусть $\mathfrak{l}$ входит в 2 точно в l-й степени. Далее, пусть $\nu_1, \nu_2, \mu_1, \mu_2$ — целые числа в k, и пусть простой идеал $\mathfrak{l}$ входит множителем в эти числа точно в b_1-й, b_2-й, a_1-й и a_2-й степенях соответственно, причем $b_2 \leqslant b_1$ и $a_2 \leqslant a_1$. Тогда если в k имеются целые числа α, β, для которых выполняются сравнения*

$$\nu_1 \equiv \alpha^2\nu_2, \qquad (\mathfrak{l}^{2l+1+b_1}),$$

$$\mu_1 \equiv \beta^2\mu_2, \qquad (\mathfrak{l}^{2l+1+a_1}),$$

то

$$\left(\frac{\nu_1,\mu_1}{\mathfrak{l}}\right) = \left(\frac{\nu_2,\mu_2}{\mathfrak{l}}\right).$$

Доказательство. Доказательство этой леммы легко устанавливается теми же рассуждениями, что и в доказательстве аналогичной теоремы 47.

Теорема 57 (лемма). *Пусть $\mathfrak{l}$ — входящий множителем в 2 простой идеал поля k, и пусть ν, μ — произвольные целые числа ($\neq 0$) в k. Тогда если $\left(\frac{\nu,\mu}{\mathfrak{l}}\right) = +1$, то и $\left(\frac{\nu,\mu}{\mathfrak{l}}\right) = +1$.*

Доказательство. Воспользуемся обозначениями, введенными в определении 18. Следует разобрать отдельно два случая в зависимости от того, четен или нечетен показатель a, с которым $\mathfrak{l}$ входит в μ.

В *первом случае* мы обозначим через $\bar{\lambda}$ какое-либо взаимно простое с $\mathfrak{l}_2, \mathfrak{l}_3, \ldots, \mathfrak{l}_z$ целое число в k, делящееся на $\mathfrak{l}^{a/2}$, но не делящееся ни на какую более высокую степень $\mathfrak{l}$, и подберем целое число μ^* в k, удовлетворяющее сравнениям

$$\begin{aligned} \bar{\lambda}^2\mu^* &\equiv \mu, \qquad (\mathfrak{l}^{2l+1+a}), \\ \mu^* &\equiv 1, \qquad (\mathfrak{l}_2^{2l_2+1}\mathfrak{l}_3^{2l_3+1}\ldots\mathfrak{l}_z^{2l_z+1}) \end{aligned} \tag{1}$$

и не являющееся квадратом никакого числа в k. Тогда μ^* взаимно просто с 2, и согласно определению 18

$$\left(\frac{\nu,\mu}{\mathfrak{l}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\bar{\lambda}^2\mu^*}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu^*}{\mathfrak{w}}\right),$$

где произведение $\prod_{(\mathfrak{w})}{}'$ распространяется на все простые идеалы $\mathfrak{w}$ в k, взаимно простые с 2. Следовательно, согласно предположению теоремы, мы имеем

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\mu^*}{\mathfrak{w}}\right)=+1. \tag{2}$$

Мы хотим теперь вывести из (2), что когда идеал $\mathfrak{l}$ поля k остается простым идеалом в $K(\sqrt{\mu^*})$, показатель b, с которым $\mathfrak{l}$ входит в ν, должен быть четным. Итак, предположим, что $\mathfrak{l}$ остается простым идеалом в $K(\sqrt{\mu^*})$. Подберем простой идеал $\mathfrak{p}$, для которого выполняются равенства

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right)=\left(\frac{\varepsilon_1}{\mu^*}\right),\qquad\ldots,\qquad\left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right)=\left(\frac{\varepsilon_{m/2}}{\mu^*}\right), \tag{3}$$

$$\left(\frac{\lambda_1}{\mathfrak{p}}\right)=\left(\frac{\lambda_1}{\mu^*}\right),\qquad\ldots,\qquad\left(\frac{\lambda_z}{\mathfrak{p}}\right)=\left(\frac{\lambda_z}{\mu^*}\right), \tag{4}$$

где $\varepsilon_1,\varepsilon_2,\ldots,\varepsilon_{m/2}$, $\lambda_1,\lambda_2,\ldots,\lambda_z$ такие же, как в теореме 42. Поскольку идеал $\mathfrak{l}$ неразложим в поле $K(\sqrt{\mu^*})$, то, согласно теоремам 4 и 6, μ^* должно быть сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l}$, и, следовательно, ввиду (1), также по модулю 2^2. Значит, по теореме 39 имеют место равенства

$$\left(\frac{\varepsilon_1}{\mu^*}\right)=+1,\qquad\ldots,\qquad\left(\frac{\varepsilon_{m/2}}{\mu^*}\right)=+1,$$

и, следовательно, ввиду (3), $\mathfrak{p}$ является примарным простым идеалом. Обозначим через π примарное число для $\mathfrak{p}$. Тогда, как видно из равенств (3), (4) и теорем 43 и 28, $\pi\mu^*$ сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\ldots\mathfrak{l}_z^{2l_z+1}$. Следовательно, ввиду (1), само π сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_2^{2l_2+1}\ldots\mathfrak{l}_z^{2l_z+1}$, а тогда по теореме 8 каждый из простых идеалов $\mathfrak{l}_2,\mathfrak{l}_3,\ldots,\mathfrak{l}_z$ распадается в поле $K(\sqrt{\pi})$ на два простых множителя. В доказательстве теоремы 34 было показано, что все идеалы поля $K(\sqrt{\pi})$ принадлежат главному роду. Таким образом, характеры простых множителей в поле $K(\sqrt{\pi})$, входящих в $\mathfrak{l}_2,\mathfrak{l}_3,\ldots,\mathfrak{l}_z$, должны быть все равны $+1$, т. е. имеют место равенства

$$\left(\frac{\lambda_2}{\mathfrak{p}}\right)=+1,\qquad\left(\frac{\lambda_3}{\mathfrak{p}}\right)=+1,\qquad\ldots,\qquad\left(\frac{\lambda_z}{\mathfrak{p}}\right)=+1.$$

Если бы было также $\left(\frac{\lambda_1}{\mathfrak{p}}\right)=+1$, то по теореме 43 примарное число π, а следовательно, и число μ^*, должны были быть сравнимы с квадратами

целых чисел в k по модулю $\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\dots\mathfrak{l}_z^{2l_z+1}$, а тогда по теореме 8 простой идеал $\mathfrak{l}=\mathfrak{l}_1$ распадался бы в поле $K(\sqrt{\mu^*})$ на два простых множителя, что противоречит нашему предположению. Следовательно, должно быть

$$\left(\frac{\lambda_1}{\mathfrak{p}}\right)=-1. \tag{5}$$

Теперь запишем идеал ν в виде

$$(\nu)=\mathfrak{n}\mathfrak{l}^b\mathfrak{l}_2^{b_2}\dots\mathfrak{l}_z^{b_z},$$

где идеал $\mathfrak{n}$ взаимно прост с 2 и $b_2,\dots,b_z$ — целые рациональные показатели. Тогда

$$\nu^h=\nu^*\lambda_1^b\lambda_2^{b_2}\lambda_3^{b_3}\dots\lambda_z^{b_z},$$

где ν^* — некоторое целое число в k, взаимно простое с 2. По теореме 40 имеем

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\pi\mu^*}{\mathfrak{w}}\right)=+1.$$

Далее, учитывая (2), получаем

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\pi\mu^*}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\pi}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\mu^*}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\pi}{\mathfrak{w}}\right),$$

следовательно,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\pi}{\mathfrak{w}}\right)=+1. \tag{6}$$

С другой стороны, так как по теореме 36

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\pi}{\mathfrak{w}}\right)=+1,$$

мы имеем равенство

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^h,\pi}{\mathfrak{w}}\right)=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\pi}{\mathfrak{w}}\right)\prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_1,\pi}{\mathfrak{w}}\right)^b\prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_2,\pi}{\mathfrak{w}}\right)^{b_2}\dots\prod_{(\mathfrak{w})}{}'\left(\frac{\lambda_z,\pi}{\mathfrak{w}}\right)^{b_z}=$$

$$=\prod_{(\mathfrak{w})}{}'\left(\frac{\nu^*,\pi}{\mathfrak{w}}\right)\cdot\left(\frac{\lambda_1}{\mathfrak{p}}\right)^b\left(\frac{\lambda_2}{\mathfrak{p}}\right)^{b_2}\dots\left(\frac{\lambda_z}{\mathfrak{p}}\right)^{b_z}=\left(\frac{\lambda_1}{\mathfrak{p}}\right)^b.$$

Ввиду (5) и (6) мы заключаем отсюда, что

$$(-1)^b=+1$$

т. е. b является четным числом.

Этим наше утверждение относительно показателя b доказано. Итак, либо простой идеал $\mathfrak{l}$ поля k распадается в $K(\sqrt{\mu^*})$, либо показатель b, с которым $\mathfrak{l}$ входит в ν, четен. Однако, как легко видеть, в обоих случаях можно найти такое целое число A в поле $K(\sqrt{\mu^*})$, что $\frac{\nu}{N(\mathrm{A})}$ равно некоторой дро-

би $\frac{\varrho}{\sigma}$, числитель ϱ и знаменатель σ которой взаимно просты с 2, а тогда на основании (2) мы заключаем, что

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varrho\sigma, \mu^*}{\mathfrak{w}}\right) = +1.$$

С учетом определения 17 это равенство приобретает вид

$$\left(\frac{\varrho\sigma, \mu^*}{\mathfrak{l}}\right) = +1,$$

и, следовательно по теореме 50 также

$$\left(\frac{\varrho\sigma, \mu^*}{\mathfrak{l}}\right) = +1,$$

т. е. $\varrho\sigma$ является норменным вычетом в поле $K(\sqrt{\mu^*})$ относительно $\mathfrak{l}$, а значит, по теореме 56 мы имеем также $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$. Этим наша теорема доказана в случае, когда показатель a четен.

Обратимся ко *второму случаю*, когда показатель a нечетен. Снова будем использовать обозначения из теоремы 42. Подберем целое взаимно простое с 2 число μ^* в k, для которого выполняются сравнения

$$\lambda_1^a \mu^* \equiv \mu^h, \qquad (\mathfrak{l}^{2l+1+ah}),$$
$$\lambda_1^a \mu^* \equiv 1, \qquad (\mathfrak{l}_2^{2l_2+1}\mathfrak{l}_3^{2l_3+1}\dots\mathfrak{l}_z^{2l_z+1}).$$

Пусть, далее, $\mathfrak{p}$ — простой идеал в k, удовлетворяющий условиям

$$\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_1}{\mu^*}\right), \quad \dots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_{m/2}}{\mu^*}\right),$$
$$\left(\frac{\lambda_1}{\mathfrak{p}}\right) = \left(\frac{\lambda_1}{\mu^*}\right), \quad \dots, \quad \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\mu^*}\right).$$

Тогда согласно теореме 43 в k существует такое целое число π^*, что главный идеал (π^*) равен $\mathfrak{p}^h$ и произведение $\pi^*\mu^*$ сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\dots\mathfrak{l}_z^{2l_z+1}$. Далее, как легко показать, используя теоремы 4, 6 и 8, в поле $K(\sqrt{\lambda_1\mu^*})$ можно найти такое число A, что $\frac{\nu}{N(\mathrm{A})}$ равно дроби $\frac{\varrho}{\sigma}$, числитель ϱ и знаменатель σ которой взаимно просты с 2. Наконец, возьмем какой-нибудь простой идеал $\mathfrak{q}$ в k, который удовлетворяет условиям

$$\left.\begin{aligned}
&\left(\frac{\varepsilon_1}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_1}{\varrho\sigma}\right), \quad \dots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{q}}\right) = \left(\frac{\varepsilon_{m/2}}{\varrho\sigma}\right),\\
&\left(\frac{\lambda_1}{\mathfrak{q}}\right) = \left(\frac{\lambda_1}{\varrho\sigma}\right), \quad \dots, \quad \left(\frac{\lambda_z}{\mathfrak{q}}\right) = \left(\frac{\lambda_z}{\varrho\sigma}\right),\\
&\left(\frac{\lambda_1\pi^*}{\mathfrak{q}}\right) = +1.
\end{aligned}\right\} \qquad (7)$$

Согласно теореме 43 в k существует такое целое число $\varkappa$, что $(\varkappa) = \mathfrak{q}^h$ и $\varkappa\varrho\sigma$ сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1} \dots \mathfrak{l}_z^{2l_z+1}$.

На основании определения 18 мы имеем

$$\left(\frac{\nu,\mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\lambda_1^a\mu^*}{\mathfrak{w}}\right).$$

Далее,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\nu,\lambda_1^a\mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\varrho\sigma,\lambda_1^a\mu^*}{\mathfrak{w}}\right).$$

Наконец, применяя теоремы 36 и 40, мы получаем

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varrho\sigma,\lambda_1^a\mu^*}{\mathfrak{w}}\right) = \prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa,\lambda_1\pi^*}{\mathfrak{w}}\right),$$

и, следовательно, в силу предположений нашей теоремы,

$$\prod_{(\mathfrak{w})}{}'\left(\frac{\varkappa,\lambda_1\pi^*}{\mathfrak{w}}\right) = +1,$$

т. е.

$$\left(\frac{\varkappa}{\mathfrak{p}}\right)\left(\frac{\lambda_1\pi^*}{\mathfrak{q}}\right) = +1,$$

а значит, ввиду (7), также и

$$\left(\frac{\varkappa}{\mathfrak{p}}\right) = +1. \tag{8}$$

Теперь рассмотрим поле $K(\sqrt{\lambda_1\pi^*})$ и применим тот же способ рассуждений, который был использован при доказательстве теоремы 48. Из (7) следует, что простой идеал $\mathfrak{q}$ поля k разложим в $K(\sqrt{\lambda_1\pi^*})$. Мы будем различать далее два случая в зависимости от того, является ли $\mathfrak{p}$ непримарным или примарным простым идеалом.

В первом случае при помощи рассуждений, аналогичных тем, которые были проведены при рассмотрении третьего случая в доказательстве теоремы 48 (с. 267), мы устанавливаем, что число классов поля $K(\sqrt{\lambda_1\pi^*})$ нечетно, откуда, привлекая (8), получаем, как и в только что упомянутом доказательстве, что $\varkappa$ является относительной нормой некоторого числа из $K(\sqrt{\lambda_1\pi^*})$.

Во втором случае мы разобьем, как и во втором случае из доказательства теоремы 48 (с. 265–267), комплексы поля $K(\sqrt{\lambda_1\pi^*})$ на два рода и покажем, как и там, что любой комплекс главного рода равен квадрату некоторого комплекса. Заметим, что ввиду (8) любой простой идеал в $K(\sqrt{\lambda_1\pi^*})$, возникающий в результате разложения $\mathfrak{q}$, принадлежит главному роду, откуда снова следует, что $\varkappa$ является относительной нормой некоторого числа из $K(\sqrt{\lambda_1\pi^*})$.

Следовательно, в обоих указанных случаях мы получаем

$$\left(\frac{\varkappa,\lambda_1\pi^*}{\mathfrak{l}}\right) = +1,$$

а так как числа $\pi^*\mu^*$ и $\varkappa\varrho\sigma$ сравнимы с квадратами целых чисел в k по модулю $\mathfrak{l}^{2l+1}$, то на основании теоремы 56 мы заключаем, наконец, что

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1.$$

Теорема доказана.

Теорема 58 (лемма). *Пусть $\mathfrak{l}$ — простой идеал в k, входящий множителем в 2, и пусть ν, μ — произвольные целые числа $\neq 0$ в k. Тогда если $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$, то и $\left(\frac{\nu, \mu}{\overline{\mathfrak{l}}}\right) = +1$.*

Доказательство. Воспользуемся обозначениями, введенными в определении 18. Подберем целое число μ^*, которое удовлетворяет сравнениям

$$\begin{aligned} \mu^* &\equiv \mu, \qquad (\mathfrak{l}_1^{2l_1+1+a}), \\ \mu^* &\equiv 1, \qquad (\mathfrak{l}_2^{2l_2+1} \dots \mathfrak{l}_z^{2l_z+1}), \end{aligned}$$

и не является квадратом никакого целого числа в k. Тогда по теореме 56

$$\left.\begin{aligned} \left(\frac{\nu, \mu^*}{\mathfrak{l}_1}\right) &= \left(\frac{\nu, \mu}{\mathfrak{l}_1}\right) = +1, \\ \left(\frac{\nu, \mu^*}{\mathfrak{l}_i}\right) &= \left(\frac{\nu, 1}{\mathfrak{l}_i}\right) = +1 \qquad (i = 2, 3, \dots, z). \end{aligned}\right\} \tag{9}$$

Пусть теперь простые идеалы $\mathfrak{l}_1, \dots, \mathfrak{l}_z$ входят в число ν точно в степенях $b_1, \dots, b_z$ соответственно. Вследствие равенств (9) в поле $K(\sqrt{\mu^*})$ существуют такие числа $\mathfrak{A}_1, \dots \mathfrak{A}_z$, что

$$\begin{aligned} \nu &\equiv N(\mathfrak{A}_1), \qquad (\mathfrak{l}_1^{2l_1+1+b_1}), \\ &\dots\dots\dots \qquad\quad \dots\dots\dots \\ \nu &\equiv N(\mathfrak{A}_z), \qquad (\mathfrak{l}_z^{2l_z+1+b_z}). \end{aligned}$$

Построив по числам $\mathfrak{A}_1, \dots, \mathfrak{A}_z$ число $\mathfrak{A}$ точно так же, как и при доказательстве теоремы 49, и рассуждая далее, как и в том доказательстве, без труда убедимся в справедливости нашей теоремы.

Взятые вместе, теоремы 57 и 58 дают следующий результат.

Теорема 59 (лемма). *Для любого входящего множителем в 2 простого идеала $\mathfrak{l}$ и любых отличных от нуля целых чисел ν, μ в k выполняется равенство*

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu, \mu}{\overline{\mathfrak{l}}}\right).$$

С помощью теоремы 59 легко доказать, что три формулы, для символа $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$, приведенные в теореме 51, справедливы также и в случае, когда ν, μ — произвольные целые числа в k. Ход рассуждений при выводе

первой формулы аналогичен тому, который был применен для доказательства первой формулы теоремы 51. Справедливость двух остальных формул немедленно следует из теорем 55 и 59. Соответственно *формулы для символа* $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$, приведенные в теореме 14, справедливы в общем случае произвольных целых чисел ν, μ в k и произвольного простого идеала $\mathfrak{w}$ в k.

§ 39. Произведение $\prod_{(\mathfrak{w})}\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ для произвольных целых чисел ν, μ

Теперь мы в состоянии сформулировать и доказать теорему, которая представляет собой далеко идущее обобщение теорем 36, 40 и 52 и в которой, как мне кажется, закон взаимности для квадратичных вычетов в поле k находит свое наиболее простое и полное выражение.

Теорема 60. *Для произвольных отличных от нуля целых чисел ν, μ в k*

$$\prod_{(\mathfrak{w})}\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1,$$

где произведение распространено на все простые идеалы $\mathfrak{w}$ в k.

Доказательство. Эта теорема доказывается при помощи рассуждений, аналогичных использованным при доказательстве теоремы 52.

Отметим одно важное следствие теоремы 60.

Теорема 61. *Пусть $\mathfrak{l}_1(=\mathfrak{l}), \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ — входящие множителями в 2 простые идеалы поля k и λ — целое число в k, такое что идеал (λ) совпадает с h-й степенью $\mathfrak{l}$. Далее, пусть $\mathfrak{p}$ — простой идеал, взаимно простой с 2, и π — целое число в k, такое что $(\pi) = \mathfrak{p}^h$. Тогда выполняется равенство*

$$\left(\frac{\lambda}{\mathfrak{p}}\right) = \left(\frac{\lambda, \pi}{\mathfrak{l}_1}\right)\left(\frac{\lambda, \pi}{\mathfrak{l}_2}\right)\cdots\left(\frac{\lambda, \pi}{\mathfrak{l}_z}\right).$$

Доказательство. Для доказательства достаточно взять в предыдущей теореме $\nu = \lambda$ и $\mu = \pi$.

Теорему 61 мы будем называть *вторым дополнением к общему закону взаимности для квадратичных вычетов в поле k.*

§ 40. Число норменных вычетов относительно некоторого простого идеала, входящего множителем в 2

Теперь мы в состоянии распространить утверждение теоремы 15 на простые множители числа 2. Справедлива следующая теорема.

Теорема 62. *Пусть $\mathfrak{l}$ — простой множитель числа 2, причем $\mathfrak{l}$ входит в 2 точно в l-й степени. Тогда если относительный дискриминант поля $K(\sqrt{\mu})$ не делится на $\mathfrak{l}$, то любое целое взаимно простое с $\mathfrak{l}$ число ν в k является норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{l}$.*

Напротив, если относительный дискриминант поля $K(\sqrt{\mu})$ *содержит множитель* $\mathfrak{l}$ *и* L *— произвольный показатель, больший чем* $2l$*, то среди всех имеющихся в* k *чисел* ν*, взаимно простых с* $\mathfrak{l}$ *и не сравнимых между собой по модулю* $\mathfrak{l}^L$*, ровно половину составляют норменные вычеты поля* $K(\sqrt{\mu})$ *относительно* $\mathfrak{l}$.

Доказательство. Если $\mathfrak{l}$ не входит множителем в относительный дискриминант $K(\sqrt{\mu})$, то, принимая во внимание теоремы 4 и 6, мы можем считать, что μ сравнимо с квадратом целого взаимно простого с $\mathfrak{l}$ числа по модулю $\mathfrak{l}^{2l}$. Тогда число μ^*, отвечающее числу μ согласно определению 17, сравнимо с квадратом целого числа в k по модулю 2^2 и, следовательно, по теореме 36 мы получаем $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$, а значит, по теореме 50 и $\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = +1$, чем и доказана справедливость первого утверждения теоремы.

Для того чтобы доказать второе утверждение, мы предположим сначала, что μ взаимно просто с 2. Пусть снова μ^* — целое число в k, отвечающее числу μ согласно определению 17. Рассмотрим фигурирующие в теореме 29 $m/2$ простых идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2}$ и связанные с ними целые числа $\varkappa_1, \ldots, \varkappa_{m/2}$. Согласно этой теореме любое взаимно простое с 2 целое число поля k представимо по модулю 2^2 в указанном там виде. В частности, мы можем записать

$$\mu^* \equiv \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varkappa_1^{v_1} \ldots \varkappa_{m/2}^{v_{m/2}} \beta^2, \qquad (2^2),$$

где показатели $u_1, \ldots, u_{m/2}, v_1, \ldots, v_{m/2}$ принимают значения 0 или 1, а β — подходящее целое число в k.

Мы будем различать в дальнейшем два случая соответственно тому, равны все показатели $v_1, \ldots, v_{m/2}$ нулю или хотя бы один из этих показателей отличен от нуля. В первом случае показатели $u_1, \ldots, u_{m/2}$ не могут все одновременно обращаться в нуль, так как в этом случае было бы $\mu^* \equiv \mu \equiv \beta^2$ по модулю $\mathfrak{l}^{2l}$ и, следовательно, в противоречие с нашим предположением, относительный дискриминант $K(\sqrt{\mu})$ был бы взаимно прост с $\mathfrak{l}$. Пусть, скажем, $u_i = 1$. Тогда в силу теорем 50 и 36

$$\left(\frac{\varkappa_i, \mu}{\mathfrak{l}}\right) = \left(\frac{\varkappa_i, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\varkappa_i, \mu^*}{\mathfrak{w}}\right) = \left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1.$$

Во втором случае пусть, например, $v_i = 1$. Тогда мы заключаем таким же способом, что

$$\left(\frac{\varepsilon_i, \mu}{\mathfrak{l}}\right) = \left(\frac{\varepsilon_i, \mu}{\mathfrak{l}}\right) = \prod_{(\mathfrak{w})}{}' \left(\frac{\varepsilon_i, \mu^*}{\mathfrak{w}}\right) = \left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1.$$

Полагая в первом случае $\nu = \varkappa_i$, а во втором $\nu = \varepsilon_i$, мы видим, что в поле k всегда существует число ν, которое является норменным невычетом в поле $K(\sqrt{\mu})$ относительно $\mathfrak{l}$.

Поскольку $L > 2l$, по теореме 47 любые два взаимно простые с $\mathfrak{l}$ целые числа в k, сравнимые по модулю $\mathfrak{l}^L$, одновременно являются норменными вычетами или невычетами относительно $\mathfrak{l}$. Обозначим через $\nu_1, \nu_2, \ldots, \nu_s$ какую-нибудь систему целых чисел в k со следующими свойствами: $\nu_1, \ldots$

$\ldots, \nu_s$ взаимно просты с $\mathfrak{l}$, попарно не сравнимы по модулю $\mathfrak{l}^L$ и являются норменными вычетами относительно $\mathfrak{l}$; кроме того, любое взаимно простое с $\mathfrak{l}$ число, являющееся норменным вычетом относительно $\mathfrak{l}$, сравнимо с одним из чисел $\nu_1, \ldots, \nu_s$ по модулю $\mathfrak{l}^L$. Если теперь ν — взаимно простой с $\mathfrak{l}$ норменный невычет относительно $\mathfrak{l}$, то ввиду второй формулы теоремы 51 все числа $\nu\nu_1, \nu\nu_2, \ldots, \nu\nu_s$ являются норменными невычетами относительно $\mathfrak{l}$, и легко показать, что произвольный взаимно простой с $\mathfrak{l}$ норменный невычет относительно $\mathfrak{l}$ сравним с одним из этих s чисел по модулю $\mathfrak{l}^L$. В самом деле, возьмем такое целое число ν^*, что $\nu\nu^* \equiv 1$ по модулю $\mathfrak{l}^L$. Поскольку $L > 2l$, в силу теоремы 47

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\nu^*, \mu}{\mathfrak{l}}\right) = -1,$$

и, следовательно, ν^* снова является норменным невычетом относительно $\mathfrak{l}$. Пусть теперь ν' означает какой-то произвольный норменный невычет относительно $\mathfrak{l}$. Тогда число $\nu'\nu^*$ представляет собой норменный вычет относительно $\mathfrak{l}$ и, следовательно, сравнимо с одним из чисел $\nu_1, \ldots, \nu_s$ по модулю $\mathfrak{l}^L$. Пусть, скажем, $\nu'\nu^* \equiv \nu_i$ по модулю $\mathfrak{l}^L$. Тогда $\nu\nu'\nu^* \equiv \nu' \equiv \nu\nu_i$ по модулю $\mathfrak{l}^L$.

Из этих рассмотрений немедленно следует справедливость второго утверждения теоремы 62 для случая, когда μ взаимно просто с 2. Доказательство этого утверждения для общего случая легко получается при помощи рассуждений, сходных с использованными при доказательстве теоремы 56.

Факт, выражаемый теоремами 15 и 62, в некотором смысле соответствует известной теореме о точках ветвления римановой поверхности, согласно которой алгебраическая функция в окрестности простой точки ветвления конформно отображает полный угол на его половину. Вследствие этого я называю простые идеалы $\mathfrak{d}$ поля k, входящие множителями в относительный дискриминант поля $K(\sqrt{\mu})$, *идеалами ветвления* для поля $K(\sqrt{\mu})$. Идеалы ветвления суть квадраты или относительные нормы амбивалентных простых идеалов поля $K(\sqrt{\mu})$.

§ 41. Доказательство основной теоремы о родах в произвольном относительном квадратичном поле

В параграфах с 17 по 19, равно как и в § 29 нами было принято временное предположение, что относительный дискриминант изучаемого поля K взаимно прост с 2. Так как мы выяснили, что все существенные свойства символа $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ сохраняются также и для простых идеалов $\mathfrak{w}$ поля k, входящих множителем в 2, мы можем теперь отбросить это предварительное предположение.

Как и прежде, обозначим через $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$ попарно различные простые множители числа 2 и запишем

$$2 = \mathfrak{l}_1^{l_1} \ldots \mathfrak{l}_z^{l_z}.$$

Заметим, что мы можем непосредственно распространить понятия «системы характеров» и «рода» из определений 11 и 12 на случай, когда относительный дискриминант K содержит множители из числа простых идеалов $\mathfrak{l}_1, \ldots, \mathfrak{l}_z$; надо только учесть при этом замечание, сделанное в конце § 38.

Равным образом мы можем немедленно перенести доказательство теорем 24, 25, 26 на рассматриваемый общий случай. Таким образом, в частности, теорема 26 справедливо для произвольного относительного квадратичного поля $K(\sqrt{\mu})$.

Наконец, возникает задача доказать основную теорему 41 также для случая, когда относительный дискриминант поля $K(\sqrt{\mu})$ содержит простые множители числа 2. Дадим такое доказательство. При этом мы будем придерживаться обозначений, введенных в § 29; нужно только помнить, что в настоящем случае в число простых идеалов $\mathfrak{d}_1, \ldots, \mathfrak{d}_t$ входят также те, которые делят число 2.

Пусть $\mathfrak{l}_1, \ldots, \mathfrak{l}_{z^*}$ — простые множители числа 2, входящие в число r идеалов $\mathfrak{d}_1, \ldots, \mathfrak{d}_r$; скажем, пусть

$$\mathfrak{l}_1 = \mathfrak{d}_{r-z^*+1}, \ldots, \mathfrak{l}_{z^*} = \mathfrak{d}_r,$$

так что $r - z^*$ простых идеалов $\mathfrak{d}_1, \ldots, \mathfrak{d}_{r-z^*}$ взаимно просты с 2. Пусть теперь $c_1, \ldots, c_r$ — какие-то r произвольных единиц ± 1, удовлетворяющих условию $c_1 \ldots c_r = +1$. В силу теоремы 62 можно найти z^* таких целых взаимно простых с 2 чисел $\nu_1, \ldots, \nu_{z^*}$, что

$$\left(\frac{\nu_1, \mu}{\mathfrak{l}_1}\right) = c_{r-z^*+1}, \quad \ldots, \quad \left(\frac{\nu_{z^*}, \mu}{\mathfrak{l}_{z^*}}\right) = c_r.$$

Выберем теперь целое число ν, такое что

$$\begin{aligned}
&\nu \equiv \nu_1, && (\mathfrak{l}_1^{2l_1+1}),\\
&\ldots\ldots && \ldots\ldots\\
&\nu \equiv \nu_{z^*}, && (\mathfrak{l}_{z^*}^{2l_{z^*}+1}),\\
&\nu \equiv 1, && (\mathfrak{l}_{z^*+1}^{2l_{z^*+1}+1}),\\
&\ldots\ldots && \ldots\ldots\\
&\nu \equiv 1, && (\mathfrak{l}_z^{2l_z+1}).
\end{aligned}$$

Тогда, согласно теореме 56, ν удовлетворяет условиям

$$\left.\begin{aligned}
&\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = c_{r-z^*+1}, \quad \ldots, \quad \left(\frac{\nu, \mu}{\mathfrak{l}_{z^*}}\right) = c_r,\\
&\left(\frac{\nu, \mu}{\mathfrak{l}_{z^*+1}}\right) = +1, \quad \ldots, \quad \left(\frac{\nu, \mu}{\mathfrak{l}_z}\right) = +1.
\end{aligned}\right\} \tag{1}$$

Теперь обозначим через $\mathfrak{d}_{r+1}, \ldots, \mathfrak{d}_{t^*}$ те из $t - r$ простых идеалов $\mathfrak{d}_{r+1}, \ldots, \mathfrak{d}_t$, которые взаимно просты с 2, и подберем затем простой идеал $\mathfrak{p}$, для которого, в обозначениях § 31, имеют место равенства

$$\left.\begin{aligned}
&\left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_1}{\nu}\right), \quad \ldots, \quad \left(\frac{\varepsilon_{m/2}}{\mathfrak{p}}\right) = \left(\frac{\varepsilon_{m/2}}{\nu}\right),\\
&\left(\frac{\lambda_1}{\mathfrak{p}}\right) = \left(\frac{\lambda_1}{\nu}\right), \quad \ldots, \quad \left(\frac{\lambda_z}{\mathfrak{p}}\right) = \left(\frac{\lambda_z}{\nu}\right),
\end{aligned}\right\} \tag{2}$$

$$\left.\begin{aligned}
&\left(\frac{\delta_1}{\mathfrak{p}}\right) = c_1\left(\frac{\nu}{\mathfrak{d}_1}\right)\left(\frac{\delta_1}{\nu}\right), \quad \ldots, \quad \left(\frac{\delta_{r-z^*}}{\mathfrak{p}}\right) = c_{r-z^*}\left(\frac{\nu}{\mathfrak{d}_{r-z^*}}\right)\left(\frac{\delta_{r-z^*}}{\nu}\right),\\
&\left(\frac{\delta_{r+1}}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{d}_{r+1}}\right)\left(\frac{\delta_{r+1}}{\nu}\right), \quad \ldots, \quad \left(\frac{\delta_{t^*}}{\mathfrak{p}}\right) = \left(\frac{\nu}{\mathfrak{d}_{t^*}}\right)\left(\frac{\delta_{t^*}}{\nu}\right).
\end{aligned}\right\} \tag{3}$$

Ввиду (2) мы можем, согласно теореме 43, найти такое целое число π, что $(\pi) = \mathfrak{p}^h$ и, кроме того, $\pi\nu$ сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1} \dots \mathfrak{l}_z^{2l_z+1}$. Поэтому мы заключаем на основании теоремы 56 (принимая во внимание (1)), что

$$\left.\begin{aligned} \left(\frac{\pi,\mu}{\mathfrak{l}_1}\right) = \left(\frac{\nu,\mu}{\mathfrak{l}_1}\right) = c_{r-z^*+1}, \quad \dots, \quad \left(\frac{\pi,\mu}{\mathfrak{l}_{z^*}}\right) = \left(\frac{\nu,\mu}{\mathfrak{l}_{z^*}}\right) = c_r, \\ \left(\frac{\pi,\mu}{\mathfrak{l}_{z^*+1}}\right) = \left(\frac{\nu,\mu}{\mathfrak{l}_{z^*+1}}\right) = +1, \quad \dots, \quad \left(\frac{\pi,\mu}{\mathfrak{l}_z}\right) = \left(\frac{\nu,\mu}{\mathfrak{l}_z}\right) = +1. \end{aligned}\right\} \tag{4}$$

С другой стороны, с учетом первой формулы теоремы 14, из теоремы 40 следует, что

$$\prod_{(\mathfrak{w})}{}' \left(\frac{\pi\nu, \delta_i}{\mathfrak{w}}\right) = +1 \qquad (i = 1, 2, \dots, r - z^*, r + 1, \dots, t^*),$$

и, следовательно, ввиду (3),

$$\left(\frac{\pi}{\mathfrak{d}_i}\right)\left(\frac{\nu}{\mathfrak{d}_i}\right)\left(\frac{\delta_i}{\mathfrak{p}}\right)\left(\frac{\delta_i}{\nu}\right) = \left(\frac{\pi}{\mathfrak{d}_i}\right) c_i = +1 \qquad (i = 1, 2, \dots, r - z^*),$$

$$\left(\frac{\pi}{\mathfrak{d}_i}\right)\left(\frac{\nu}{\mathfrak{d}_i}\right)\left(\frac{\delta_i}{\mathfrak{p}}\right)\left(\frac{\delta_i}{\nu}\right) = \left(\frac{\pi}{\mathfrak{d}_i}\right) = +1 \qquad (i = r + 1, \dots, t^*),$$

т. е. имеют место равенства

$$\left.\begin{aligned} \left(\frac{\pi}{\mathfrak{d}_i}\right) = \left(\frac{\pi,\mu}{\mathfrak{d}_i}\right) = c_i \qquad (i = 1, 2, \dots, r - z^*), \\ \left(\frac{\pi}{\mathfrak{d}_i}\right) = \left(\frac{\pi,\mu}{\mathfrak{d}_i}\right) = +1 \qquad (i = r + 1, \dots, t^*). \end{aligned}\right\} \tag{5}$$

Так как $\mathfrak{d}_1, \dots, \mathfrak{d}_{r-z^*}, \mathfrak{d}_{r+1}, \dots, \mathfrak{d}_{t^*}$ суть все взаимно простые с 2 делители относительного дискриминанта $K(\sqrt{\mu})$, то мы можем записать

$$\mu^h = \gamma\alpha^2\delta_1 \dots \delta_{r-z^*}\delta_{r+1}\delta_{t^*},$$

где γ — целое число в k, все простые множители которого входят множителями в 2, и где α — некоторое определенное целое число в k. По теореме 60

$$\prod_{(\mathfrak{w})}\left(\frac{\pi,\mu}{\mathfrak{w}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right)\left(\frac{\pi,\mu}{\mathfrak{d}_1}\right)\dots\left(\frac{\pi,\mu}{\mathfrak{d}_{r-z^*}}\right)\left(\frac{\pi,\mu}{\mathfrak{d}_{r+1}}\right)\dots\left(\frac{\pi,\mu}{\mathfrak{d}_{t^*}}\right)\left(\frac{\pi,\mu}{\mathfrak{l}_1}\right)\dots\left(\frac{\pi,\mu}{\mathfrak{l}_z}\right) = +1,$$

и, следовательно, ввиду (4) и (5) мы получаем

$$\left(\frac{\mu}{\mathfrak{p}}\right) c_1 \dots c_r = +1.$$

Так как по нашему предположению $c_1 \dots c_r = +1$, отсюда вытекает, что $\left(\frac{\mu}{\mathfrak{p}}\right) = +1$, т. е. $\mathfrak{p}$ распадается в $K(\sqrt{\mu})$ на два простых множителя. В силу (4) и (5) характеры каждого из этих простых множителей равны

$$\left(\frac{\pi,\mu}{\mathfrak{d}_1}\right) = c_1, \quad \dots, \quad \left(\frac{\pi,\mu}{\mathfrak{d}_r}\right) = c_r.$$

Отсюда точно так же, как и в проведенном в § 29 доказательстве, мы убеждаемся о справедливости теоремы 41 в общем случае.

Тем самым нами полностью решен важнейший вопрос о числе родов в произвольном относительном квадратичном поле $K(\sqrt{\mu})$.

§ 42. Классы главного рода

В этом и следующих параграфах мы укажем некоторые следствия, вытекающие из теоремы 41.

Теорема 63. *Число родов g в данном относительном квадратичном поле равно числу* A *его амбивалентных комплексов.*

Доказательство. Пусть t и v имеют тот же смысл, что и в теореме 23. Поскольку согласно теореме 41 $g = 2^{r-1}$, из теорем 23 и 25 следует, что

$$r \leqslant t + v - m/2,$$

а так как, с другой стороны, по теореме 24 должно быть

$$t + v - m/2 \leqslant r,$$

мы видим, что

$$r = t + v - m/2.$$

Следовательно, по теореме 23 число амбивалентных комплексов равно

$$\mathrm{A} = 2^a = 2^{r-1} = g.$$

Теорема 64. *Любой комплекс главного рода в данном относительном квадратичном поле K является квадратом некоторого комплекса в K, т. е. любой класс главного рода в относительном квадратичном поле K равен произведению квадрата некоторого класса на класс, содержащий идеал основного поля k.*

Доказательство. При доказательстве теоремы 25 было получено равенство $\mathrm{A}f' = gf$; здесь A и g имеют тот же смысл, что и в теореме 63, f' обозначает число тех комплексов, которые равны квадратам каких-либо комплексов, а f — число комплексов главного рода. Так как, согласно теореме 63, $\mathrm{A} = g$, то отсюда следует, что $f' = f$, чем и доказано, что любой комплекс главного рода является квадратом некоторого комплекса.

§ 43. Теорема об относительных нормах для относительного квадратичного поля

Теорема 65. *Пусть ν, μ — произвольные отличные от нуля целые числа поля k, причем μ не является квадратом никакого числа в k. Если для любого простого идеала $\mathfrak{w}$ в k*

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1,$$

то число ν равно относительной норме некоторого целого или дробного числа поля $K(\sqrt{\mu})$.

Доказательство. Сначала мы докажем эту теорему для случая, когда ν — единица в k. Пусть t и v имеют тот же смысл, что и в теореме 23. При доказательстве теоремы 63 было показано, что $r = t + v - m/2$, т. е. что $v = m/2 - t + r$. Итак, число связок единиц в k, которые состоят из единиц, являющихся относительными нормами, составляет $2^{m/2-t+r}$.

С другой стороны, рассмотрим $r^* = t - r$ единиц $\varepsilon_1, \ldots, \varepsilon_{r^*}$, которые были определены в § 17. Из равенств (1) § 17 мы легко получаем, что r^* связок единиц, порожденных $\varepsilon_1, \ldots, \varepsilon_{r^*}$, независимы друг от друга. Следовательно, можно найти такие $m/2 - r^*$ связок единиц, которые вместе с предыдущими образуют систему из $m/2$ независимых связок единиц. Пусть $\varepsilon_{r^*+1}, \ldots$ $\ldots, \varepsilon_{m/2}$ — единицы из этих $m/2 - r^*$ связок единиц, по одной из каждой. Очевидно, что тогда произвольная единица ξ поля k может быть представлена в виде

$$\xi = \varepsilon_1^{u_1} \ldots \varepsilon_{m/2}^{u_{m/2}} \varepsilon^2,$$

где показатели $u_1, \ldots, u_{m/2}$ принимают значения 0 или 1, а ε — подходящая единица в k. Рассмотрим теперь r^* равенств

$$\left(\frac{\varepsilon, \mu}{\mathfrak{d}_t}\right) = +1, \qquad \left(\frac{\varepsilon, \mu}{\mathfrak{d}_{t-1}}\right) = +1, \qquad \ldots, \qquad \left(\frac{\varepsilon, \mu}{\mathfrak{d}_{t-r^*+1}}\right) = +1. \qquad (1)$$

Для показателей $u_1, u_2, \ldots, u_{m/2}$ эти равенства дают r^* линейных сравнений по модулю 2, которые, как легко проверить, независимы друг от друга. Таким образом, мы получаем, что все единицы ξ, удовлетворяющие условиям (1), составляют в совокупности

$$2^{m/2-r^*} = 2^{m/2-t+r}$$

связок единиц.

В начале доказательства мы установили, что число связок единиц, которые состоят из единиц, являющихся относительными нормами, выражается тем же числом. Далее, так как любая единица в k, которая является относительной нормой некоторой единицы или дробного числа из $K(\sqrt{\mu})$, очевидно, есть норменный вычет относительно $\mathfrak{l}$ и, следовательно, должна удовлетворять уравнениям (1), любая связка первоначально рассмотренных единиц содержится среди тех связок, единицы ξ которых удовлетворяют равенствам (1). Так как обе системы состоят из одного и того же числа связок единиц, обе системы совпадают друг с другом. Согласно предположению заданная единица ν удовлетворяет условиям (1) и, следовательно, согласно только что доказанному, является относительной нормой некоторой единицы или дробного числа из $K(\sqrt{\mu})$.

Пусть теперь ν — произвольное число из $K(\sqrt{\mu})$, удовлетворяющее предположению нашей теоремы. Тогда если $\mathfrak{n}_1, \mathfrak{n}_2, \ldots$ — максимальные степени простых идеалов поля k, входящие в ν, то ввиду предположения теоремы 65 в $K(\sqrt{\mu})$ должны существовать такие целые числа $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$, что имеют место сравнения

$$\nu \equiv N(\mathfrak{A}_1), \qquad (\mathfrak{n}_1^2),$$

$$\nu \equiv N(\mathfrak{A}_2), \qquad (\mathfrak{n}_2^2),$$

Итак, если обозначить через A целое число в $K(\sqrt{\mu})$, которое сравнимо с A_1 по модулю $\mathfrak{n}_1^2$, сравнимо с A_2 по модулю $\mathfrak{n}_2^2$ и т. д., то мы получим

$$\nu \equiv N(\mathsf{A}), \qquad (\nu^2). \tag{2}$$

Рассмотрим теперь в $K(\sqrt{\mu})$ идеал

$$\mathfrak{H} = (\nu, \mathsf{A}).$$

Ввиду (2)

$$\mathfrak{H} \cdot S\mathfrak{H} = (\nu, \mathsf{A})(\nu, S\mathsf{A}) = (\nu^2, \nu\mathsf{A}, \nu S\mathsf{A}, \mathsf{A}S\mathsf{A}) = (\nu),$$

откуда следует, что ν должно быть относительной нормой идеала $\mathfrak{H}$ в $K(\sqrt{\mu})$.

В силу предположения теоремы $\mathfrak{H}$ обязательно принадлежит главному роду в $K(\sqrt{\mu})$, и, следовательно, мы можем, согласно теореме 64, записать

$$\mathfrak{H} \sim \mathfrak{j}\mathfrak{J}^2,$$

где $\mathfrak{j}$ — некоторый идеал в k, а $\mathfrak{J}$ — идеал в $K(\sqrt{\mu})$. Ввиду того что $\mathfrak{j}^h \sim 1$, $\mathsf{B} = \left(\dfrac{\mathfrak{H}}{\mathfrak{J}^2}\right)^h$ должно быть целым или дробным числом поля K. Очевидно, что относительная норма $N(\mathsf{B})$ этого числа имеет вид $\dfrac{\varepsilon\nu^h}{\alpha^2}$, где ε — единица в k и α — целое число в k. Отсюда следует, что для произвольного простого идеала $\mathfrak{w}$ должно быть

$$\left(\frac{\varepsilon\nu^h\alpha^2, \mu}{\mathfrak{w}}\right) = +1,$$

а, следовательно, и

$$\left(\frac{\varepsilon, \mu}{\mathfrak{w}}\right) = +1.$$

Как было показано в первой части доказательства, при данных условиях единица ε должна быть равной относительной норме некоторого числа из $K(\sqrt{\mu})$. Запишем $\varepsilon = N(\Gamma)$, где Γ — некоторое число из $K(\sqrt{\mu})$. Тогда

$$\nu = N\left(\frac{\mathsf{B}\cdot\alpha}{\Gamma\cdot\nu^{(h-1)/2}}\right),$$

чем теорема и доказана.

§ 44. Тернарное квадратное диофантово уравнение в поле k

Содержание теоремы 65 можно выразить также следующим способом.

Теорема 66. *Пусть ν, μ — произвольные отличные от нуля целые числа в k. Диофантово уравнение*

$$\nu\xi^2 + \mu\eta^2 = 1$$

разрешимо в целых или дробных числах ξ, η поля k, если для любого простого идеала $\mathfrak{w}$ в k выполнено условие

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1.$$

Теорема 67. *Пусть ν, μ — произвольные целые числа поля k. Диофантово уравнение*

$$\nu\xi^2 + \mu\eta^2 = 1$$

разрешимо в целых или дробных числах ξ, η поля k, если разрешимо в целых числах ξ, η поля k сравнение

$$\nu\xi^2 + \mu\eta^2 \equiv 1$$

по модулю любого простого идеала поля k и любой степени такого идеала.

Доказательство. В случае когда μ является квадратом некоторого целого числа в k, данное диофантово уравнение удовлетворяется значениями $\xi = 0$, $\eta = 1/\sqrt{\mu}$. Пусть теперь μ не является квадратом никакого целого числа в k. Далее, пусть $\mathfrak{w}$ — простой идеал в k и $\mathfrak{w}^L$ — произвольная степень $\mathfrak{w}$. Наконец, пусть ξ, η — целые числа в k, удовлетворяющие представленному в формулировке теоремы сравнению по модулю $\mathfrak{w}^L$. Так как, очевидно, ξ и η не могут оба одновременно делиться на $\mathfrak{w}$, то мы можем предположить, что, скажем, ξ взаимно просто с $\mathfrak{w}$. Тогда ввиду того, что

$$\nu \equiv N\left(\frac{1+\eta\sqrt{\mu}}{\xi}\right), \qquad (\mathfrak{w}^L),$$

число ν является норменным вычетом поля $K(\sqrt{\mu})$ относительно $\mathfrak{w}$ и, следовательно, числа ν и μ удовлетворяют условиям теоремы 65. Согласно этой теореме ν является относительной нормой некоторого числа A поля $K(\sqrt{\mu})$. Запишем A в виде

$$\mathrm{A} = \frac{\alpha+\beta\sqrt{\mu}}{\gamma},$$

где α, β, γ — целые числа в k. Тогда

$$\nu = \frac{\alpha^2 - \mu\beta^2}{\gamma^2}$$

и, следовательно, числа $\xi = \dfrac{\gamma}{\alpha}$, $\eta = \dfrac{\beta}{\alpha}$ удовлетворяют нашему уравнению. Теорема доказана.

Если дано однородное тернарное квадратное диофантово уравнение с произвольными лежащими в k коэффициентами, то возникает вопрос об условиях, при которых это уравнение разрешимо в целых числах поля k. Как легко видеть, теоремы 66 и 67 дают полный ответ и на этот вопрос.

О ТЕОРИИ ОТНОСИТЕЛЬНО АБЕЛЕВЫХ ЧИСЛОВЫХ ПОЛЕЙ*)[1)]

§ 1.

В теории относительно абелевых числовых полей наш интерес привлекают прежде всего поля *второй* относительной степени.

Пусть в основу положено в качестве области рациональности произвольное числовое поле k степени n. Тогда наша задача состоит в обосновании теории относительно квадратичных (или относительных квадратичных) полей $K(\sqrt{\mu})$, т. е. тех полей, которые определяются квадратным корнем из произвольного целого числа μ поля k. Гауссовы «disquisitiones arithmetical» содержатся здесь в качестве простейшего случая. Мы можем также обозначить нашу тему как теорию квадратных уравнений или квадратичных форм, коэффициенты которых являются числами из заданной области рациональности k.

Теория относительных квадратичных полей привела меня к открытию общего закона взаимности для квадратичных вычетов, для которых обычный закон взаимности между простыми рациональными числами выступает всего лишь как отдельное звено в цепи очень интересных и разнообразных числовых соотношений.

В моем сочинении «О теории относительных квадратичных числовых полей»[2)] теория относительных квадратичных полей была развита мной для произвольного алгебраического основного поля k в случае, когда основное поле k вместе со всеми своими сопряженными полями является мнимым и, кроме того, обладает нечетным числом классов. Важнейшими из установленных в названном сочинении теорем являются закон взаимности для квадратичных вычетов в k и теорема, согласно которой в любом относительном квадратичном поле над k всегда половина всех возможных систем характеров действительно представляется родами. Я попытался показать в этом сочинении, какое изобилие арифметических фактов содержится в этих теоремах. Тем не менее полное значение названных теорем становится очевидным, только когда мы распространим их на *произвольное* алгебраическое

---

*) Über die Theorie der relativ-Abelschen Zahlkörper. — Acta Math., 1902, Bd. 26, S. 99–132. *Перевод Л. В. Кузьмина.*

1) За прошедшее с момента выхода той работы время в в Гёттингене были опубликованы следующие диссертации по этой тематике: *Dörrie H.* Das quadratische Reziprozitätsgesetz im quadratischen Zahlkörper mit der Klassenzahl 1, 1898; *Reid L. W.* Tafel der Klassenzahl für kubische Zahlkörper, 1899; *Hilbert K. S.* Dar allgemeine quadratische Reziprozitätsgesetz in ausgewählten Kreiskörpern der 2^h-ten Einheitswurzeln, 1900; *Rückle L.* Quadratische Resiprozitätsgesetz in algebraischen Zahlkörpern, 1901. В частности, последняя диссертация содержит многочисленные интересные примеры, относящиеся к развиваемой здесь теории.

2) Math. Ann., 1899, Bd. 51, S. 1–127 [имеется перевод на с. 179–287 настоящего издания. — *Ред.*].

поле K. В докладе, прочитанном мною на заседании Брауншвейгского союза математиков[3], я сделал несколько кратких замечаний, относящихся к случаю, когда основное поле k вещественно, либо же обладает вещественным сопряженным полем или имеет число классов 2. В настоящей работе я намерен изложить наиболее важные теоремы из теории квадратичных относительных полей для произвольного основного поля k и одновременно указать те изменения, которые надо внести в доказательства из моего ранее названного сочинения, если мы хотим отбросить принятые там ограничительные предположения об основном поле k.

Наконец, в последнем параграфе (§ 16) данной работы я формулирую ряд гипотез — общих теорем для относительных абелевых числовых полей произвольной степени с относительным дискриминантом 1; это теоремы поразительной простоты и кристальной красоты; полное их доказательство и надлежащее обобщение на случай произвольного относительного дискриминанта представляется мне конечной целью чисто арифметической теории относительно абелевых числовых полей.

§ 2.

Пусть k — произвольное числовое поле. Обозначим степень этого поля через m и будем обозначать $m-1$ сопряженных с k полей через $k', k'', \ldots, k^{(m-1)}$. Число классов идеалов поля k будет обозначаться через h. Мы перенесем известное из теории рациональных чисел понятие символа на рассматриваемый здесь случай следующим образом[4].

Пусть $\mathfrak{p}$ — простой идеал поля k, не входящий множителем в 2, и α — произвольное взаимно простое с $\mathfrak{p}$ целое число в k. Тогда символ $\left(\frac{\alpha}{\mathfrak{p}}\right)$ принимает значения $+1$ или -1 в зависимости от того, сравнимо ли α с квадратом некоторого целого числа в k по модулю $\mathfrak{p}$ или нет. Далее, если $\mathfrak{a}$ — произвольный взаимно простой с 2 идеал в k и $\mathfrak{a} = \mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$, где $\mathfrak{a}, \mathfrak{q}, \ldots, \mathfrak{w}$ — простые идеалы в k, и если α — некоторое взаимно простое с $\mathfrak{a}$ целое число в k, то символ $\left(\frac{\alpha}{\mathfrak{a}}\right)$ может быть определен следующим равенством:

$$\left(\frac{\alpha}{\mathfrak{a}}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right)\left(\frac{\alpha}{\mathfrak{q}}\right)\ldots\left(\frac{\alpha}{\mathfrak{w}}\right).$$

Если $\mathfrak{a}, \mathfrak{b}$ — произвольные взаимно простые с 2 идеалы в k, и α — целое число в k, взаимно простое с $\mathfrak{a}\mathfrak{b}$, то, очевидно, выполняется равенство

$$\left(\frac{\alpha}{\mathfrak{a}\mathfrak{b}}\right) = \left(\frac{\alpha}{\mathfrak{a}}\right)\left(\frac{\alpha}{\mathfrak{b}}\right).$$

Пусть μ — целое число в k, которое не равно квадрату какого-либо числа из k. Тогда $\sqrt{\mu}$ вместе с числами поля k определяет некоторое поле степени $2m$, которое является квадратичным относительно k и будет обозначаться через $K(\sqrt{\mu})$ или кратко через K. Если задано несколько полей,

---

[3] Jber. der Deutschen Mathematiker-Vereinigung, 1897, Bd. 4, S. 88–94.

[4] Ср. с моей работой «Über die Theorie des relativquadratischen Zahlkörpers», определения 1 и 5 [см. с. 180 и 188 настоящего издания. — *Ред.*].

квадратичных относительно k, то они называются *независимыми друг от друга*, коль скоро ни одно из них не содержится в качестве подполя в том поле, которое получается композицией остальных.

Относительное квадратичное поле K называется *неразветвленным* относительно k, если относительный дискриминант K над k равен 1, или, что то же самое, если в k не существует простого идеала, который равен квадрату простого идеала в K.

§ 3.

Сначала мы будем считать, что для положенного в основу поля k выполняются те два предположения, при которых теория относительных квадратичных полей была подробно развита в моем упомянутом выше сочинении о квадратичных полях. Это следующие предположения.

1. Поле k степени m мнимо вместе со всеми сопряженными полями $k', k'', \ldots, k^{(m-1)}$.

2. Число классов идеалов h поля k равно 1.

Для дальнейшего нам будет удобно повторить здесь важнейшие относящиеся сюда определения и результаты в виде, который немного отличается от данного в том моем сочинении.

Определение 1. *Примарным идеалом* называется всякий такой взаимно простой с 2 идеал $\mathfrak{a}$ поля k, относительно которого для любой единицы ξ в k имеет место равенство

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1.$$

Определение 2. *Примарным числом* поля k называется всякое такое взаимно простое с 2 целое число α из k, которое сравнимо с квадратом целого числа в k по модулю 2^2.

Основное содержание *первого дополнения к закону взаимности* можно выразить следующим образом.

Теорема 1. *Если $\mathfrak{a}$ — примарный идеал в k, то всегда существует такое примарное число α, что $\mathfrak{a} = (\alpha)$, и, обратно, если α — примарное число в k, то $\mathfrak{a} = (\alpha)$ всегда является примарным идеалом.*

Теперь запишем разложение числа 2 в поле k на простые идеалы:

$$2 = \mathfrak{l}_1^{l_1}\mathfrak{l}_2^{l_2}\ldots\mathfrak{l}_z^{l_z},$$

где $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_z$ — попарно различные простые множители числа 2 в k и $l_1, l_2, \ldots, l_z$ — показатели степеней, в которых соответствующие простые идеалы входят в число 2.

Определение 3. *Гиперпримарным идеалом* называется всякий такой взаимно простой с 2 идеал $\mathfrak{a}$ поля k, что не только для любой единицы ξ в k, но и для любого целого числа λ поля k, делящего 2, выполняются условия

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1, \quad \left(\frac{\lambda}{\mathfrak{a}}\right) = +1.$$

Определение 4. *Гиперпримарным числом* поля называется всякое такое взаимно простое с 2 число α в k, которое сравнимо с квадратом целого числа в k по модулю $\mathfrak{l}_1^{2l_1+1}\mathfrak{l}_2^{2l_2+1}\dots\mathfrak{l}_z^{2l_z+1}$.

Основное содержание *второго дополнения к закону взаимности* можно выразить следующим образом.

Теорема 2. *Если* $\mathfrak{a}$ *— гиперпримарный идеал в* k, *то всегда существует такое гиперпримарное число* α, *что* $\mathfrak{a}=(\alpha)$, *и, обратно, если* α *— гиперпримарное число в* k, *то* $\mathfrak{a}=(\alpha)$ *всегда является гиперпримарным идеалом.*

Основное содержание *общего закона взаимности для квадратичных вычетов* в поле k состоит в следующем.

Теорема 3. *Если* ν,μ,ν',μ' *— такие взаимно простые с* 2 *целые числа в* k, *что оба произведения* $\nu\nu'$ *и* $\mu\mu'$ *примарны и* ν *взаимно просто с* μ, ν' *взаимно просто с* μ', *то всегда*

$$\left(\frac{\nu}{\mu}\right)\left(\frac{\mu}{\nu}\right)=\left(\frac{\nu'}{\mu'}\right)\left(\frac{\mu'}{\nu'}\right).$$

Если число классов h поля k равно не 1, а произвольному нечетному числу, то формулировки теорем 1–3 требуют лишь незначительных видоизменений, которые легко извлечь из моего сочинения о квадратичных полях.

Теорема 4. *Любая единица в* k, *которая является примарной* (*т. е. примарным числом*), *совпадает с квадратом некоторой единицы в* k.

Теорема 5. *Над* k *не существует относительно квадратичных неразветвленных полей.*

Последние две теоремы без изменения переносятся на случай, когда число классов h поля k является произвольным нечетным числом.

§ 4.

Теперь мы примем за основу следующие предположения о поле k.

1. Среди m сопряженных полей $k,k',k'',\dots,k^{(m-1)}$ имеется некое число s $(s>0)$ вещественных полей. Пусть таковыми будут поля $k,k',k'',\dots,k^{(s-1)}$.
2. Число h классов идеалов в поле k равно 1.

При этих предположениях определение примарного идеала (определение 1) остается без изменений, в то время как понятие примарного числа необходимо уточнить.

Определение 5. Число α поля k называется *всюду положительным* в k в случае, когда все s сопряженных с α чисел, лежащих в полях $k,k',\dots,k^{(s-1)}$ соответственно, положительны. Если взаимно простое с 2 число α поля k сравнимо с квадратом целого числа в k по модулю 2^2 и если, кроме того, α всюду положительно в k, то α называется *примарным числом* поля k.

При таком определении первое дополнение (теорема 1) и общий закон взаимности (теорема 3) остаются в силе в прежнем виде, а если соответствующим образом уточнить понятие гиперпримарного числа, то и второе дополнение (теорема 2) останется справедливым в том же виде.

§ 5.

Далее обсудим вопрос о том, существуют ли над k относительно квадратичные неразветвленные поля при принятых в § 4 предположениях о поле k. С этой целью мы прежде всего условимся, что в общем случае если ε — какая-то единица в k, то через $\varepsilon', \varepsilon'', \ldots, \varepsilon^{(s-1)}$ будут обозначаться сопряженные с ε единицы, лежащие в полях $k', k'', \ldots, k^{(s-1)}$, соответственно.

Теперь положим $\varepsilon_1 = -1$. Очевидно, что единица ε_1, равно как и все сопряженные с ε_1 единицы, отрицательна. Далее, пусть в k существует единица ε_2, которая положительна в k, но для которой хоть одна из сопряженных единиц $\varepsilon_2', \ldots, \varepsilon_2^{(s-1)}$ отрицательна. Пусть, например, отрицательна лежащая в k' единица ε_2'. Затем, пусть в k' существует единица ε_3, которая положительна и для которой ε_3' снова положительна, в то время как хоть одна из остальных сопряженных единиц $\varepsilon_3'', \varepsilon_3''', \ldots, \varepsilon_3^{(s-1)}$ отрицательна. Пусть, например, отрицательна лежащая в k'' единица ε_3''. Продолжая в том же духе, в конце концов мы получим единицу ε_p $(p \leqslant s)$ с тем свойством, что все $\varepsilon_p, \varepsilon_p', \varepsilon_p'', \ldots, \varepsilon_p^{(p-2)}$, в то время как единица $\varepsilon_p^{(p-1)}$ отрицательна, и дальше нельзя продолжать действовать тем же способом, т. е. если какая-либо единица ε в k вместе с $p-1$ сопряженными $\varepsilon', \varepsilon'', \ldots, \varepsilon^{(p-1)}$ положительна, то и все остальные $s-p$ сопряженных единиц $\varepsilon^{(p)}, \ldots, \varepsilon^{(s-1)}$ положительны.

Число $s-p$ получает особенно простой смысл, если ввести более узкие понятия классов и их эквивалентности, чем было до сих пор. Именно, отныне мы будем считать два идеала $\mathfrak{j}, \mathfrak{k}$ поля k эквивалентными только тогда, когда $\frac{\mathfrak{j}}{\mathfrak{k}} = \alpha$, где α — некоторое целое или дробное число в k, которое положительно вместе со всеми своими сопряженными числами $\alpha', \alpha'', \ldots, \alpha^{(s-1)}$, лежащими в полях $k', k'', \ldots, k^{(s-1)}$ соответственно, т. е. всюду положительно в k. Мы отнесем к одному классу все идеалы поля k, которые эквивалентны друг другу в этом более узком смысле. Тогда, как легко убедиться, поле k обладает ровно $\overline{h} = 2^{s-p}$ классами идеалов.

После этой подготовки мы можем ответить на поставленный выше вопрос о неразветвленных полях над k.

Теорема 6. *Для поля k существует система из $s-p$ независимых неразветвленных относительных квадратичных полей над k. Эти $s-p$ полей порождают поле Kk относительной степени $\overline{h} = 2^{s-p}$ над k, которое содержит все неразветвленные поля над k в качестве подполей. Это поле называется полем классов поля k. Число $\overline{H}$ классов идеалов поля Kk является всегда нечетным числом (если снова, как и для поля k, понимать классы в указанном выше узком смысле).*

Одно из наиболее замечательных свойств поля классов Kk состоит в том, что простые идеалы поля k, которые принадлежат одному и тому же классу идеалов k в узком смысле, одинаково разлагаются на простые идеалы в поле Kk, т. е. в их разложениях число различных простых идеалов и их степени совпадают. Таким образом, разложение простого идеала $\mathfrak{p}$ поля k в поле Kk зависит только от класса, которому принадлежит простой этот идеал в поле k.

§ 6.

Для того чтобы доказать перечисленные результаты и полностью построить теорию относительных квадратичных полей над k при сделанных в § 4 предположениях, нам будет нужен один символ, о котором я говорил в своем Брауншвейгском докладе.

Определение 6. Пусть $\mathfrak{w}$ — какой-либо простой идеал в k, и пусть ν, μ — произвольные целые числа в k, причем μ не равно квадрату никакого числа в k. Тогда если ν сравнимо по модулю $\mathfrak{w}$ с относительной нормой некоторого целого числа поля $K(\sqrt{\mu})$ и если, кроме того, для любой более высокой степени $\mathfrak{w}$ всегда можно найти такое целое число A в поле $K(\sqrt{\mu})$, что $\nu \equiv N(A)$ по модулю этой степени $\mathfrak{w}$, то я полагаю

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1,$$

а во всех остальных случаях

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = -1.$$

В случае когда μ равно квадрату целого числа ($\neq 0$) в k, будем считать, что всегда

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = +1.$$

Далее, мы определим еще s символов

$$\left(\frac{\nu, \mu}{1}\right), \quad \left(\frac{\nu, \mu}{1'}\right), \quad \ldots, \quad \left(\frac{\nu, \mu}{1^{(s-1)}}\right).$$

А именно, мы полагаем

$$\left(\frac{\nu, \mu}{1}\right) = +1,$$

если хотя бы одно из чисел ν, μ положительно; напротив, мы полагаем

$$\left(\frac{\nu, \mu}{1}\right) = -1,$$

если каждое из чисел ν, μ отрицательно. Далее, обозначая через $\nu^{(i)}, \mu^{(i)}$ сопряженные соответственно с ν, μ числа, лежащие в $k^{(i)}$, положим

$$\left(\frac{\nu, \mu}{1}\right) = \left(\frac{\nu', \mu'}{1}\right), \quad \left(\frac{\nu, \mu}{1''}\right) = \left(\frac{\nu'', \mu''}{1}\right), \quad \ldots, \quad \left(\frac{\nu, \mu}{1^{(s-1)}}\right) = \left(\frac{\nu^{(s-1)}, \mu^{(s-1)}}{1}\right).$$

Пусть теперь задано некоторое относительное квадратичное поле $K(\sqrt{\mu})$ над k. Тогда определение понятия рода получается естественным способом

из определения 12 моего сочинения о квадратичных полях, если использовать обобщенные символы $\left(\frac{\nu,\mu}{\omega}\right)$, где ω пробегает простые идеалы, входящие множителями в относительный дискриминант $K(\sqrt{\mu})$, и, кроме того, те знаки $1^{(i)}$, для которых сопряженное с μ число $\mu^{(i)}$, лежащее в $k^{(i)}$, отрицательно. Без особых затруднений удается полностью распространить теорию относительных квадратичных полей, развитую в том моем сочинении, на рассматриваемый здесь случай, когда поле k удовлетворяет предположениям, сделанным в § 4.

С использованием обобщенных символов $\left(\frac{\nu,\mu}{\omega}\right)$ закон взаимности для квадратичных вычетов в поле k приобретает следующий простой вид.

Теорема 7. *Если ν,μ — произвольные целые числа $\neq 0$ в k, то всегда*

$$\prod_{(\omega)}\left(\frac{\nu,\mu}{\omega}\right)=+1,$$

где произведение распространено на все простые идеалы $\omega=\mathfrak{w}$ в k и на s знаков $\omega=1,1',1'',\ldots,1^{(s-1)}$.

Теоремы 41, 64, 65, 67 из моего сочинения о квадратичных полях немедленно переносятся на случай рассматриваемого здесь основного поля k при указанном обобщенном понимании символа $\left(\frac{\nu,\mu}{\omega}\right)$.

Если понимаемое в первоначальном смысле число классов h поля k равно не 1, а какому-то нечетному числу, то теоремы §§ 4–6 нуждаются лишь в незначительных видоизменениях, которые легко извлечь из того моего сочинения.

§ 7.

Если, в частности, для поля k выполнено условие $s-p=0$, то $\overline{h}=1$ и теорема 6 говорит, что над k не существует ни одного неразветвленного поля. Мы хотим теперь рассмотреть следующий по простоте случай, когда $s-p=1$ и $\overline{h}=2$, и прежде всего детально обсудить намеченные в конце § 5 законы разложения простых идеалов в k. Итак, мы принимаем следующие специальные предположения об основном поле k.

1. Среди m сопряженных полей $k,k',k'',\ldots,k^{(m-1)}$ существует некое число s $(s>0)$ вещественных полей. Пусть таковыми являются поля $k,k',k'',\ldots,k^{(s-1)}$.

2. Число h классов идеалов поля k, понимаемое в первоначальном широком смысле, равно 1; число $\overline{h}$ классов идеалов поля k, понимаемое в узком смысле, равно 2.

При этих предположениях упомянутое в § 5 поле классов Kk является относительным квадратичным и обладает следующими свойствами.

Теорема 8а. *Поле классов Kk имеет относительный дискриминант 1, т. е. оно не разветвлено над k.*

Теорема 8b. *Число $\overline{H}$ классов поля классов Kk, понимаемое в узком смысле, нечетно.*

Теорема 8c. *Простые идеалы в k, являющиеся главными идеалами в k в узком смысле, распадаются в Kk в произведение двух простых идеалов. Что же касается простых идеалов в k, которые не являются главными в узком смысле, то они остаются в Kk простыми идеалами.*

Если для поля k выполнены наши предположения, то каждым из этих трех свойств поле классов Kk характеризуется однозначно.

Чтобы доказать существование поля классов Kk, необходимо показать, что при сделанных предположениях в k всегда существует единица ε, которая сравнима с квадратом целого числа по модулю 2^2, но не является сама квадратом единицы в k. Тогда искомым полем классов Kk будет поле $K(\sqrt{\varepsilon})$. Доказательство существования такой единицы ε можно провести способом, сходным с тем, которым мы воспользуемся ниже в § 9 для доказательства теорем 9a, 9b и 9c.

§ 8.

В качестве дальнейшего этапа нашего исследования мы хотим точно сформулировать законы разложения простых идеалов основного поля k в поле классов Kk для некоторых других случаев и привести доказательства сформулированных результатов. В этом параграфе считается, что для основного поля k выполнены следующие специальные предположения.

1. Среди m сопряженных полей $k, k', k'', \ldots, k^{(m-1)}$ существует некое число s вещественных полей.

2. Число h классов идеалов поля k в первоначальном широком смысле совпадает с числом классов $\overline{h}$, понимаемом в узком смысле, и равно 2.

При этих предположениях поле классов Kk является относительно квадратичным и обладает следующими свойствами.

Теорема 9a. *Поле классов Kk не разветвлено над k, т. е. оно имеет относительный дискриминант 1 над k.*

Теорема 9b. *Число классов H и $\overline{H}$ поля классов Kk, понимаемые как в широком, так и в узком смысле, нечетны ($H = \overline{H}$).*

Теорема 9c. *Простые идеалы в k, являющиеся главными в k, распадаются в Kk в произведение двух простых идеалов. Что же касается простых идеалов в k, которые не являются главными в k, то в Kk они остаются простыми, но становятся главными.*

Если для поля k выполнены наши предположения, то поле классов Kk характеризуется каждым из этих трех свойств однозначно. Таким образом, верны следующие теоремы.

Теорема 10a. *Кроме Kk не существует другого относительно квадратичного поля, не разветвленного над k.*

Теорема 10b. *Если некоторое относительно квадратичное поле над k имеет четное число классов, то оно совпадает с полем классов Kk.*

Теорема 10c. *Если все простые идеалы в k, которые являются главными в k, распадаются в некотором относительно квадратичном поле, или все простые идеалы в k, которые не являются главными в k, остаются простыми в некотором относительно квадратичном поле, то относительное квадратичное поле есть не что иное, как поле классов Kk.*

§ 9.

При доказательстве существования поля классов Kk, а затем и теорем 9a, 9b, 9c, мы для простоты будем предполагать, что основное поле k и все его сопряженные поля мнимы. При этом, как и в § 3, мы будем называть целое число в k примарным, если оно взаимно просто с 2 и сравнимо с квадратом целого числа в k по модулю 2^2.

Выберем теперь какую-нибудь систему основных единиц в k и обозначим их через $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m/2-1}$. Далее, пусть r — взаимно простой с 2 простой идеал поля k, который не принадлежит главному классу, и пусть $\mathfrak{r}^2 = (\varrho)$, где ϱ — некоторое число в k. Присоединим к вышеуказанным $m/2-1$ единицам еще следующие числа:

$$\varepsilon_{m/2} = -1, \quad \varepsilon_{m/2+1} = \varrho.$$

Тогда $m/2+1$ чисел $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m/2+1}$ образуют систему чисел со следующими свойствами: любое целое число ξ в k, которое является квадратом некоторого идеала в k, может быть представлено в виде

$$\xi = \varepsilon_1^{x_1} \varepsilon_2^{x_2} \ldots \varepsilon_{m/2+1}^{x_{m/2+1}} \alpha^2,$$

где показатели $x_1, x_2, \ldots, x_{m/2+1}$ принимают значения 0 или 1, а α — некоторое целое или дробное число в k.

Наконец, принимая во внимание теорему 18 моего сочинения о квадратичных полях, найдем в k систему простых идеалов $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_{m/2-1}$, взаимно простых с 2 и таких, что

$$\left(\frac{\varepsilon_i}{\mathfrak{q}_i}\right) = -1, \quad \left(\frac{\varepsilon_j}{\mathfrak{q}_i}\right) = +1 \qquad (i \neq j, \quad i,j = 1,2,\ldots,m/2+1), \tag{1}$$

выберем показатели $w_1, \ldots, w_{m/2+1}$ со значениями 0 или 1 так, чтобы произведения

$$\mathfrak{q}_1 \mathfrak{r}^{w_1}, \quad \mathfrak{q}_2 \mathfrak{r}^{w_2}, \quad \ldots, \quad \mathfrak{q}_{m/2+1} \mathfrak{r}^{w_{m/2+1}}$$

были главными идеалами в k. Пусть, скажем,

$$\mathfrak{q}_1 \mathfrak{r}^{w_1} = (\varkappa_1), \quad \ldots, \quad \mathfrak{q}_{m/2+1} \mathfrak{r}^{w_{m/2+1}} = (\varkappa_{m/2+1}),$$

где $\varkappa_1, \ldots, \varkappa_{m/2}$ — некоторые целые числа в k.

После этих приготовлений рассмотрим выражение

$$\varepsilon_1^{u_1} \ldots \varepsilon_{m/2+1}^{u_{m/2+1}} \varkappa_1^{v_1} \ldots \varkappa_{m/2+1}^{v_{m/2+1}}; \tag{2}$$

если допустить для показателей $u_1, \ldots, u_{m/2+1}$ произвольные значения 0 или 1, а для показателей $v_1, \ldots, v_{m/2+1}$ — любые значения 0 или 1, удовлетворяющие сравнению

$$v_1 w_1 + v_2 w_2 + \ldots + v_{m/2+1} w_{m/2+1} \equiv 0, \qquad (2), \tag{3}$$

то это выражение представляет 2^{m+1} чисел. Будем теперь считать два целых взаимно простых с 2 числа ω_1 и ω_2 в k принадлежащими одному типу, если их произведение $\omega_1\omega_2$ является примарным числом. Как показывают рассмотрения, проведенные в конце § 21 моего сочинения о квадратичных полях, в поле k существует ровно 2^m различных типов чисел. Итак, среди чисел вида (2) должно иметься по меньшей мере два числа, принадлежащих одному типу. Произведение таких чисел является примарным числом вида

$$\omega = \varepsilon_1^{u_1} \dots \varepsilon_{m/2+1}^{u_{m/2+1}} \varkappa_1^{v_1} \dots \varkappa_{m/2+1}^{v_{m/2+1}} \alpha^2, \tag{4}$$

где показатели $u_1, \dots, u_{m/2+1}, v_1, \dots, v_{m/2+1}$ принимают некоторые значения 0 или 1, но не все равны 0, а α — некоторое целое число в k.

Если бы в выражении (4) для числа ω показатели $v_1, \dots, v_{m/2+1}$ все обращались в 0, то согласно теоремам 4 и 5 моего сочинения о квадратичных полях поле $K(\sqrt{\omega})$ было бы неразветвленным относительно квадратичным полем над k, и тем самым существование поля классов со свойством из теоремы 9а было бы доказано.

Предположим теперь, что хотя бы один из показателей $v_1, \dots, v_{m/2+1}$ имеет значение 1, и пусть t — точное число таких показателей. Пусть, скажем, $v_{i_1} = 1, v_{i_2} = 1, \dots, v_{i_t} = 1$, где индексы $i_1, i_2, \dots, i_t$ — некоторые из чисел $1, 2, \dots, m/2+1$. В силу этого предположения в относительный дискриминант поля $K(\sqrt{\omega})$ должны входить t простых идеалов $\mathfrak{q}_{i_1}, \mathfrak{q}_{i_2}, \dots, \mathfrak{q}_{i_t}$. Ввиду условия (3) и ввиду примарности w отсюда следует, что, помимо этих t простых идеалов, не существует других, которые содержались бы в относительном дискриминанте поля $K(\sqrt{\omega})$. Указанные t простых идеалов поля k становятся в поле $K(\sqrt{\omega})$ квадратами некоторых t амбивалентных простых идеалов, и, следовательно, число всех амбивалентных идеалов поля $K(\sqrt{\omega})$ в точности равно 2^t. Нам понадобятся также следующие обозначения из теоремы 22 § 15 моего сочинения о квадратичных полях: пусть поле k обладает ровно 2^{v^*} связками единиц, порожденных относительными нормами единиц из $K(\sqrt{\omega})$, и пусть 2^{a^*} — число амбивалентных классов, в которых содержатся амбивалентные идеалы поля $K(\sqrt{\omega})$.

Что касается поведения идеалов поля k в поле $K(\sqrt{\omega})$, то возможны следующие два случая.

I. Идеалы поля k, которые не были главными в k, становятся главными в $K(\sqrt{\omega})$.

II. Идеалы поля k, которые не были главными в k, остаются неглавными в $K(\sqrt{\omega})$.

Перенося на поле $K(\sqrt{\omega})$ способ рассуждений, примененный мною при доказательстве теоремы 22 моего сочинения о квадратичных полях, без труда получим в первом случае равенство

$$a^* = t + v^* - m/2, \tag{5}$$

а во втором —

$$a^* = t + v^* - m/2 - 1. \tag{6}$$

§ 10.

Мы хотим получить для числа v^* некоторую оценку сверху, зависящую от t и m. С этой целью будем обозначать через $x_1, \ldots, x_{m/2}$ произвольные показатели, принимающие значения 0 или 1. Тогда если единица

$$\varepsilon = \varepsilon_1^{x_1} \ldots \varepsilon_{m/2}^{x_{m/2}}$$

является относительной нормой некоторой единицы из $K(\sqrt{\omega})$, то должны выполняться t условий

$$\left(\frac{\varepsilon}{\mathfrak{q}_{i_1}}\right) = +1, \quad \ldots, \quad \left(\frac{\varepsilon}{\mathfrak{q}_{i_t}}\right) = +1. \tag{7}$$

Теперь установим ряд лемм, которые имеют силу в обоих случаях I,II.

Лемма 1. *Любая единица ε поля k, удовлетворяющая условиям* (7), *должна быть относительной нормой некоторой единицы относительного поля $K(\sqrt{\omega})$.*

Для доказательства этой леммы мы будем различать два случая: входит в число индексов $i_1, \ldots, i_t$ число $m/2+1$, или нет. В первом случае пусть $i_t = m/2+1$. На основании (7), принимая во внимание (1), заключаем, что должны выполняться равенства

$$x_{i_1} = 0, \quad \ldots, \quad x_{i_{t-1}} = 0,$$

откуда видно, что число v^* независимых связок единиц, порождаемых относительными нормами единиц из $K(\sqrt{\omega})$, не превосходит $m/2 - t + 1$.

Если же число $m/2-1$ не входит в число индексов $i_1, \ldots, i_t$, то тем же способом мы получаем, что

$$x_{i_1} = 0, \quad \ldots, \quad x_{i_t} = 0$$

и, следовательно, число v^* независимых единиц, порождаемых относительными нормами единиц из $K(\sqrt{\omega})$, не превосходит в этом случае $m/2 - t$.

Без труда проверяется, что в случае I число $m/2+1$ не входит в число индексов $i_1, \ldots, i_t$. В противном случае относительный дискриминант поля $K(\sqrt{\omega})$ содержал бы простой идеал $\mathfrak{q}_{m/2+1}$, и если обозначить через P целое число из $K(\sqrt{\omega})$, представляющее идеал $\mathfrak{r}$, то относительная норма P должна была бы быть равна некоторому числу в k вида $\varepsilon\varrho$, где ε — некоторая единица в k, а $\varrho = \varepsilon_{m/2+1}$ имеет ранее указанный смысл. Вытекающее отсюда равенство

$$\left(\frac{\varepsilon\varrho}{\mathfrak{q}_{m/2+1}}\right) = \left(\frac{\varepsilon\varepsilon_{m/2+1}}{\mathfrak{q}_{m/2+1}}\right)$$

находится в противоречии с нашим выбором простого идеала $\mathfrak{q}m/2+1$ (см. (1)).

Предыдущие рассуждения приводят в случае I к неравенству

$$v^* \leqslant m/2 - t, \tag{8}$$

а в случае II — к неравенству

$$v^* \leqslant m/2 - t + 1. \tag{9}$$

Равенства (5) и (6) и неравенства (8) и (9) показывают, что в обоих случаях имеет место неравенство $a^* \leqslant 0$, а так как, конечно, должно быть $a^* \geqslant 0$, мы заключаем, что $a^* = 0$, т. е. в случае I

$$v^* = m/2 - t, \tag{10}$$

а в случае II

$$v^* = m/2 - t + 1. \tag{11}$$

Теперь мы можем констатировать, что в случае II простой идеал $\mathfrak{q}_{m/2+1}$ должен входить множителем в относительный дискриминант поля $K(\sqrt{\omega})$. Действительно, как показывают ранее проведенные рассуждения, в противном случае, т. е. если бы число $m/2+1$ не входило в число индексов $i_1, \ldots, i_t$, имело бы место неравенство (8), которое противоречит равенству (11).

Учитывая это, мы видим, что единицы ε в k, которые удовлетворяют условиям (7), составляют в случае I ровно $m/2 - t$, а в случае II — ровно $m/2 - t + 1$ независимых связок единиц. Так как согласно (10) и (11) это число в обоих случаях равно v^*, то такие единицы ε составляют в целом 2^{v^*} связки единиц, которые, следовательно, должны совпадать с теми связками единиц, единицы которых являются относительными нормами единиц из $K(\sqrt{\omega})$, т. е. в обоих случаях любая единица ε в k, удовлетворяющая условиям (7), должна быть относительной нормой некоторой единицы из $K(\sqrt{\omega})$, чем наша лемма и доказана.

Лемма 2. *Если $\mathfrak{J}$ — идеал в $K(\sqrt{\omega})$, квадрат которого эквивалентен некоторому идеалу в k, то и сам $\mathfrak{J}$ эквивалентен некоторому идеалу в k.*

Доказательство. Для доказательства обозначим через S относительную подстановку $(\sqrt{\omega} : -\sqrt{\omega})$, и пусть N обозначает относительную норму числа или идеала в $K(\sqrt{\omega})$. Так как в любом случае относительная норма идеала $\mathfrak{J}$

$$N(\mathfrak{J}) = \mathfrak{J} \cdot S\mathfrak{J}$$

является идеалом в k, а по предположению $\mathfrak{J}^2$ должен быть эквивалентен некоторому идеалу в k, отсюда следует, что частное $\mathfrak{J}/S\mathfrak{J}$ должно быть эквивалентно некоторому идеалу $\mathfrak{j}$ в k.

В случае I этот идеал $\mathfrak{j}$, конечно, является главным идеалом в $K(\sqrt{\omega})$. С другой стороны, мы докажем, что в случае II идеал $\mathfrak{j}$ — главный в поле k. Именно, если бы $\mathfrak{j}$ не был главным идеалом в k, то было бы $\mathfrak{j}\mathfrak{r} \sim 1$, где $\mathfrak{r}$ имеет ранее указанный смысл. Запишем

$$\frac{\mathfrak{J}}{S\mathfrak{J}}\,\mathfrak{r} = A,$$

где A — некоторое дробное число в $K(\sqrt{\omega})$. Взяв норму от обеих частей, заключаем, что

$$\varepsilon\varrho = N(A), \tag{12}$$

где ε — некоторая единица и $\varrho = \varepsilon_{m/2+1}$ обозначает ранее определенное число в k. Так как в случае II простой идеал $\mathfrak{q}_{m/2+1}$ входит множителем

в относительный дискриминант поля $K(\sqrt{\omega})$, то ввиду (12) мы получаем равенство

$$\left(\frac{\varepsilon\varepsilon_{m/2+1}}{\mathfrak{q}_{m/2+1}}\right) = 1,$$

которое противоречит нашему выбору простого идеала $\mathfrak{q}_{m/2+1}$ (См. (1)).

Итак, мы выяснили, что в обоих случаях I, II частное идеалов $\mathfrak{J}/S\mathfrak{J}$ эквивалентно 1 в $K(\sqrt{\omega})$. Поэтому мы можем записать

$$\frac{\mathfrak{J}}{S\mathfrak{J}} = A, \tag{13}$$

где A некоторое целое или дробное число в $K(\sqrt{\omega})$. Если теперь взять относительную норму этого числа

$$\varepsilon = N(A), \tag{14}$$

то ε будет единицей в k, которая должна удовлетворять условиям (7). Следовательно, в силу ранее доказанной леммы 1 эта единица ε равна относительной норме некоторой единицы в $K(\sqrt{\omega})$. Запишем

$$\varepsilon = N(E^{-1}), \tag{15}$$

где E — некоторая единица в $K(\sqrt{\omega})$. Из (14) и (15) следует, что

$$N(AE) = 1. \tag{16}$$

Положим

$$B = 1 + S(AE).$$

(Соответственно $B = 1$, если $AE = -1$). Тогда ввиду (16) будет выполнено равенство

$$\frac{SB}{B} = EA,$$

(соответственно $= 1$) откуда, учитывая (13), мы получаем равенство для идеалов

$$\frac{S(B\mathfrak{J})}{B\mathfrak{J}} = 1,$$

т. е. $B\mathfrak{J}$ является произведением амбивалентного идеала поля $K(\sqrt{\omega})$ и некоторого идеала поля k. Поскольку ранее для обоих случаев было доказано равенство $a^* = 0$ и, следовательно, все амбивалентные идеалы в $K(\sqrt{\omega})$ являются главными, мы видим, что и идеал $\mathfrak{J}$ должен быть эквивалентен некоторому идеалу поля k. Тем самым лемма доказана.

Лемма 3. *Для любого идеала $\mathfrak{J}$ в $K(\sqrt{\omega})$ существует такой нечетный показатель u, что идеал $\mathfrak{J}^u$ эквивалентен некоторому идеалу в k.*

Доказательство. В самом деле, пусть H — число классов поля $K(\sqrt{\omega})$, и пусть $H = 2^a u$, где a — некоторый показатель и u — нечетное число. Тогда должно быть $\mathfrak{J}^{2^a u} \sim 1$, откуда, принимая во внимание лемму 2, последовательно заключаем, что идеалы $\mathfrak{J}^{2^{a-1}u}, \mathfrak{J}^{2^{a-2}u}, \ldots, \mathfrak{J}^{2u}, J^u$ эквивалентны некоторым идеалам в k.

Лемма 4. *Если* $\mathfrak{p}$ *— простой идеал в поле* k*, для которого выполнено условие*

$$\left(\frac{\omega}{\mathfrak{p}}\right) = +1, \tag{17}$$

то $\mathfrak{p}$ *— всегда главный идеал в поле* k.

Доказательство. Для доказательства заметим, что ввиду предположения (17) простой идеал $\mathfrak{p}$ должен распадаться в поле $K(\sqrt{\omega})$. Запишем

$$\mathfrak{p} = \mathfrak{P} \cdot S\mathfrak{P},$$

где $\mathfrak{P}, S\mathfrak{P}$ — относительно сопряженные друг с другом идеалы в $K(\sqrt{\omega})$. В силу леммы 3 найдется такой нечетный показатель u, что идеал $\mathfrak{P}^u$ эквивалентен некоторому идеалу $\mathfrak{j}$ в k. Отсюда, очевидно, следует, что

$$\mathfrak{p}^u \sim \mathfrak{j}^2 \sim 1, \quad \text{т. е.} \quad \mathfrak{p} \sim 1.$$

§ 11.

Существование поля классов со свойствами 9a, 9b, 9c можно теперь установить при помощи следующих рассуждений. Вместо определенных в § 9 простых идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2+1}$, удовлетворяющих условиям (1), мы выберем какие-нибудь другие взаимно простые с 2 простые идеалы $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{m/2+1}$ с соответствующими свойствами

$$\left(\frac{\varepsilon_i}{\mathfrak{q}'_i}\right) = -1, \quad \left(\frac{\varepsilon_j}{\mathfrak{q}'_i}\right) = +1 \qquad (i \neq j, \quad i,j = 1,2,\ldots,m/2+1)$$

и снова подберем показатели $w'_1, \ldots, w'_{m/2+1}$ так, чтобы

$$\mathfrak{q}'_1 \mathfrak{r}^{w'_1} = (\varkappa'_1), \quad \ldots, \quad \mathfrak{q}'_{m/2+1} \mathfrak{r}^{w'_{m/2+1}} = (\varkappa'_{m/2+1}),$$

где $\varkappa'_1, \ldots, \varkappa'_{m/2+1}$ — целые числа в k. Затем повторим для новой системы простых идеалов $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{m/2+1}$ все рассуждения §§ 9, 10. В результате придем к выражению

$$\omega' = \varepsilon' \varkappa'^{v'_1}_1 \ldots \varkappa'^{v'_{m/2+1}}_{m/2+1}, \tag{18}$$

в котором ε' — некоторая единица из k и $v'_1, \ldots, v'_{m/2+1}$ — некоторые показатели, принимающие значения 0 или 1. В случае если мы предположим, как и прежде, что не все показатели $v'_1, \ldots, v'_{m/2+1}$ равны 0, мы снова получаем, что для поля $K(\sqrt{\omega'})$ верны леммы 1–4, и в соответствии с леммой 4 любой простой идеал $\mathfrak{p}$ поля k, для которого

$$\left(\frac{\omega'}{\mathfrak{p}}\right) = +1,$$

должен быть главным идеалом поля k.

Теперь обозначим кратко через $\mathfrak{w}_\omega$ все те простые идеалы в k, для которых

$$\left(\frac{\omega}{\mathfrak{w}_\omega}\right) = +1,$$

а через $\mathfrak{w}_{\omega\omega'}$ — те простые идеалы в k, для которых одновременно

$$\left(\frac{\omega}{\mathfrak{w}_{\omega\omega'}}\right) = -1 \quad \text{и} \quad \left(\frac{\omega'}{\mathfrak{w}_{\omega\omega'}}\right) = +1.$$

Далее, через $\mathfrak{w}^{(+)}$ обозначим те простые идеалы в k, которые являются главными в k, а через $\mathfrak{w}^{(-)}$ — те простые идеалы в k, которые не являются главными в k.

Так как числа ω, ω', безусловно, не являются квадратами целых чисел в k и при наших предположениях, ввиду различия простых идеалов $\mathfrak{q}_1, \ldots, \mathfrak{q}_{m/2+1}$ и $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{m/2+1}$, это же верно и для произведения $\omega\omega'$, то и из теоремы 17 моего сочинения о квадратичных полях следуют равенства

$$\begin{aligned} \sum_{(\mathfrak{w}_\omega)} \frac{1}{n(\mathfrak{w}_\omega)^s} &= \frac{1}{2}\log\frac{1}{s-1} + f_\omega(s) \qquad (s>1), \\ \sum_{(\mathfrak{w}_{\omega\omega'})} \frac{1}{n(\mathfrak{w}_{\omega\omega'})^s} &= \frac{1}{4}\log\frac{1}{s-1} + f_{\omega\omega'}(s) \qquad (s>1). \end{aligned} \tag{19}$$

Здесь бесконечные суммы распространяются на все простые идеалы $\mathfrak{w}_\omega$ и $\mathfrak{w}_{\omega\omega'}$ соответственно, а $f_\omega(s), f_{\omega\omega'}(s)$ обозначают функции вещественной переменной s, остающиеся заключенными в конечных пределах, когда s стремится к значению 1; наконец, n означает норму в поле k.

Очевидно, что все простые идеалы $\mathfrak{w}_\omega$ отличны от простых идеалов $\mathfrak{w}_{\omega\omega'}$, а так как по ранее доказанному все простые идеалы $\mathfrak{w}_\omega, \mathfrak{w}_{\omega\omega'}$ входят в число простых идеалов $\mathfrak{w}^{(+)}$, то мы имеем

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} \geqslant \sum_{(\mathfrak{w}_\omega)} \frac{1}{n(\mathfrak{w}_\omega)^s} + \sum_{(\mathfrak{w}_{\omega\omega'})} \frac{1}{n(\mathfrak{w}_{\omega\omega'})^s}, \qquad (s>1)$$

и, следовательно, ввиду (19),

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} \geqslant \frac{3}{4}\log\frac{1}{s-1} + f_\omega(s) + f_{\omega\omega'}(s). \tag{20}$$

Здесь снова все бесконечные суммы распространяются на все простые идеалы с соответствующими свойствами.

Очевидно, что идеалами $\mathfrak{w}^{(+)}$ и $\mathfrak{w}^{(-)}$ исчерпываются все простые идеалы $\mathfrak{w}$ в k, а значит,

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} + \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} = \sum_{(\mathfrak{w})} \frac{1}{n(\mathfrak{w})^s} = \log\frac{1}{s-1} + f(s), \tag{21}$$

где сумма $\sum_{(\mathfrak{w})}$ распространяется на все простые идеалы $\mathfrak{w}$ в k и $f(s)$ снова означает величину, которая при $s>1$ остается заключенной в конечных пределах при s, стремящемся к 1. Из (20) и (21) следует неравенство

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} - \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} \geqslant \frac{1}{2}\log\frac{1}{s-1} + 2f_\omega(s) + 2f_{\omega\omega'}(s) - f(s). \tag{22}$$

Теперь мы установим следующую лемму об идеалах поля k.

Лемма 5. *Выражение*

$$\sum_{(\mathfrak{w}^{(+)})} \frac{1}{n(\mathfrak{w}^{(+)})^s} - \sum_{(\mathfrak{w}^{(-)})} \frac{1}{n(\mathfrak{w}^{(-)})^s} \qquad (s > 1),$$

где первая сумма распространяется на все простые идеалы $\mathfrak{w}^{(+)}$, *а вторая сумма — на все простые идеалы* $\mathfrak{w}^{(-)}$, *представляет такую функцию вещественной переменной* s, *которая всегда остается меньше некоторой конечной положительной границы, когда* s *приближается к* 1.

Доказательство. Эта лемма доказывается с помощью тех же рассуждений, которые были применены в моем сочинении при доказательстве теоремы 31.

Сразу видно, что неравенство (22) противоречит лемме 5. Следовательно, наше первоначальное предположение должно быть отвергнуто, т. е. либо все показатели $v_1, \ldots, v_{m/2+1}$ в равенстве (4), либо все показатели $v_1', \ldots, v_{m/2+1}'$ в аналогичном равенстве (18) должны быть равны 0. Итак, в качестве одного из чисел ω, ω' мы имеем число в поле k, которое как идеал представляет собой квадрат некоторого идеала в k и, кроме того, сравнимо с квадратом некоторого числа в k по модулю 2^2, но не является квадратом никакого числа из k.

Тогда одно из полей $K(\sqrt{\omega})$, $K(\sqrt{\omega'})$ является искомым полем классов Kk над основным полем k, так как оно обладает свойством, выражаемым теоремой 9a. Тем самым решена самая трудная проблема в обсуждаемой здесь теории.

§ 12.

Доказательство теоремы 9b, равно как и второго утверждения теоремы 9c, легко получить из предыдущего. Не так просто доказать первое утверждение теоремы 9c — о том, что любой простой идеал поля k, принадлежащий главному классу в k, распадается в поле классов Kk, которое совпадает теперь с $K(\sqrt{\omega})$. Мы проведем это доказательство следующим образом.

Согласно доказанному в § 11, число ω имеет вид (4):

$$\omega = \varepsilon_1^{u_1} \varepsilon_2^{u_2} \ldots \varepsilon_{m/2+1}^{u_{m/2+1}},$$

где показатели $u_1, \ldots, u_{m/2+1}$ принимают значения 0 или 1, но не все равны 0. Пусть, например, $u_i = 1$. Тогда обозначим числа $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{i-1}, \varepsilon_{i+1}, \ldots, \varepsilon_{m/2}, \varepsilon_{m/2+1}$ через $\varepsilon_1^*, \ldots, \varepsilon_{m/2}^*$ соответственно и найдем $m/2$ отличных от $\mathfrak{r}$ простых идеалов $\mathfrak{p}_1, \ldots, \mathfrak{p}_{m/2}$ в k, таких что

$$\begin{aligned} &\left(\frac{\varepsilon_h^*}{\mathfrak{p}_h}\right) = -1, \quad \left(\frac{\varepsilon_h^*}{\mathfrak{p}_k}\right) = +1, \quad (h \neq k, \quad h, k = 1, 2, \ldots, m/2), \\ &\left(\frac{\omega}{\mathfrak{p}_h}\right) = +1 \quad (h = 1, 2, \ldots, m/2). \end{aligned} \tag{23}$$

Ввиду (23) все простые идеалы $\mathfrak{p}_1, \ldots, \mathfrak{p}_{m/2}$ являются, согласно второму утверждению теоремы 9c, главными идеалами в k. Запишем

$$\mathfrak{p}_1 = (\pi_1), \quad \ldots, \quad \mathfrak{p}_{m/2} = (\pi_{m/2}),$$

где $\pi_1, \ldots, \pi_{m/2}$ — целые числа в k. Мы утверждаем, что выражение вида

$$\omega^* = \varepsilon^{*\,u_1^*}_{1} \ldots \varepsilon^{*\,u_{m/2}^*}_{m/2}\, \pi_1^{v_1} \ldots \pi_{m/2}^{v_{m/2}} \qquad (u_1^*, \ldots, u_{m/2}^*, v_1, \ldots, v_{m/2} = 0, 1) \tag{24}$$

может тогда только представлять примарное число в k, когда все показатели $u_1^*, \ldots, u_{m/2}^*, v_1, \ldots, v_{m/2}$ имеют значение 0. В самом деле, если бы ω^* было примарным и хотя бы один из этих показателей равнялся бы 1, то, как и выше, используя лемму 4, мы получили бы, что все простые идеалы в k, которые распадаются в $K(\sqrt{\omega^*})$, являются главными идеалами в k, т. е. что все простые идеалы $\mathfrak{w}$, относительно которых ω^* — квадратичный вычет, являются главными в k. То обстоятельство, что в то же время и все простые идеалы $\mathfrak{w}$, относительно которых ω — квадратичный вычет, являются главными в k, приводит нас, как и ранее в § 11, к противоречию.

Из только что доказанного результата о том, что выражение (24) не может представлять ни одного примарного числа, кроме числа 1, при помощи рассуждений, сходных с применявшимися ранее, без труда выводится такое следствие: если $\varkappa$ — произвольное взаимно простое с 2 целое число в k, то всегда можно найти такую систему показателей $u_1^*, \ldots, u_{m/2}^*, v_1, \ldots, v_{m/2}$, что выражение

$$\varkappa \varepsilon^{*\,u_1^*}_{1} \ldots \varepsilon^{*\,u_{m/2}^*}_{m/2} \pi_1^{v_1} \ldots \pi_{m/2}^{v_{m/2}} \tag{25}$$

представляет примарное число в k.

Теперь пусть $\mathfrak{q}$ — какой-либо простой идеал в k из главного класса. Запишем $\mathfrak{q} = (\varkappa)$, где $\varkappa$ — целое число в k, и предположим в противоположность доказываемому утверждению, что $\mathfrak{q}$ неразложим в $K(\sqrt{\omega})$. Построим для числа $\varkappa$ выражение (25) и обозначим его через α. Наконец, возьмем в k простой идеал $\widetilde{\mathfrak{r}}$, отличный от $\mathfrak{r}$, и не являющийся главным в k, и такое число σ в k, что $\sigma = \mathfrak{r}\widetilde{\mathfrak{r}}$. Мы положим $\overline{\omega} = \omega\sigma^2/\varrho^2$ или $\overline{\omega} = \omega$ в зависимости от того, содержит ω множитель $\mathfrak{r}^2$ или нет.

Так как по теореме 9b поле $K(\sqrt{\omega})$ обладает нечетным числом классов, то с учетом того, что α примарно, мы получаем, согласно квадратичному закону взаимности, доказанному для этого случая в моем сочинении о квадратичных полях, формулу

$$\left\{\frac{\alpha}{\sqrt{\overline{\omega}}}\right\} = \left\{\frac{\sqrt{\overline{\omega}}}{\alpha}\right\}. \tag{26}$$

Здесь фигурные скобки означают для поля $K(\sqrt{\omega})$ то же, что обычные скобки — для поля k. Главный идеал $\sqrt{\overline{\omega}}$ в поле $K(\sqrt{\omega})$ либо равен 1, либо равен простому идеалу $\widetilde{\mathfrak{r}}$. Если теперь $\left(\frac{\alpha}{\widetilde{\mathfrak{r}}}\right) = +1$, то и $\left\{\frac{\alpha}{\widetilde{\mathfrak{r}}}\right\} = +1$. Если $\left(\frac{\alpha}{\widetilde{\mathfrak{r}}}\right) = -1$, то, поскольку $\left(\frac{\omega}{\widetilde{\mathfrak{r}}}\right) = -1$, должно быть $\left(\frac{\alpha\omega}{\widetilde{\mathfrak{r}}}\right) = +1$ и, тем более, $\left\{\frac{\alpha\omega}{\widetilde{\mathfrak{r}}}\right\} = +1$. С другой стороны, ввиду равенства $\omega = (\sqrt{\omega})^2$ должно быть

$\left\{\frac{\omega}{\widetilde{\mathfrak{r}}}\right\} = +1$ и, следовательно, также $\left\{\frac{\alpha}{\widetilde{\mathfrak{r}}}\right\} = +1$. Итак, в любом случае мы имеем $\left\{\frac{\alpha}{\sqrt{\overline{\omega}}}\right\} = +1$, и ввиду (26) отсюда следует, что

$$\left\{\frac{\sqrt{\overline{\omega}}}{\alpha}\right\} = +1. \tag{27}$$

Если A — какое-либо целое взаимное простое с $\mathfrak{q}$ число в $K(\sqrt{\omega})$, то по модулю простого идеала $\mathfrak{q}$ поля k, который остается простым и в $K(\sqrt{\omega})$, имеют место следующие сравнения:

$$\left\{\frac{A}{\mathfrak{q}}\right\} \equiv A^{(n(\mathfrak{q})^2-1)/2}, \qquad (\mathfrak{q}),$$

$$\left\{\frac{NA}{\mathfrak{q}}\right\} \equiv (NA)^{(n(\mathfrak{q})^2-1)/2}, \qquad (\mathfrak{q}),$$

а так как

$$SA \equiv A^{n(\mathfrak{q})}, \quad NA \equiv A^{n(\mathfrak{q})+1}, \qquad (\mathfrak{q}),$$

мы заключаем, что

$$\left\{\frac{A}{\mathfrak{q}}\right\} = \left(\frac{NA}{\mathfrak{q}}\right).$$

Взяв, в частности, что $A = \sqrt{\overline{\omega}}$, получим

$$\left\{\frac{\sqrt{\overline{\omega}}}{\varkappa}\right\} = \left(\frac{-\overline{\omega}}{\varkappa}\right). \tag{28}$$

С другой стороны, в общем случае ввиду (23) простой идеал $\mathfrak{p}_h$ распадается в $K(\sqrt{\omega})$. Запишем

$$\mathfrak{p}_h = \mathfrak{P}_h \cdot S\mathfrak{P}_h \qquad (h = 1, 2, \ldots, m/2),$$

где $\mathfrak{P}_h$ — некоторый простой идеал в $K(\sqrt{\omega})$. Так как

$$\left\{\frac{\sqrt{\overline{\omega}}}{\mathfrak{p}_h}\right\} = \left\{\frac{\sqrt{\overline{\omega}}}{\mathfrak{P}_h}\right\}\left\{\frac{\sqrt{\overline{\omega}}}{S\mathfrak{P}_h}\right\}, \qquad \left\{\frac{\sqrt{\overline{\omega}}}{\mathfrak{P}_h}\right\}\left\{\frac{\sqrt{-\overline{\omega}}}{S\mathfrak{P}_h}\right\},$$

мы имеем

$$\left\{\frac{\sqrt{\overline{\omega}}}{\mathfrak{p}_h}\right\} = \left\{\frac{-1}{\mathfrak{P}_h}\right\} = \left(\frac{-1}{\mathfrak{p}_h}\right). \tag{29}$$

Ввиду (27), (28), (29) мы получаем с учетом определения α, что

$$\left(\frac{-\overline{\omega}}{\varkappa}\right)\left(\frac{-1}{\pi_1}\right)^{v_1} \cdots \left(\frac{-1}{\pi_{m/2}}\right)^{v_{m/2}} = +1$$

и, следовательно,

$$\left(\frac{-1}{\alpha}\right)\left(\frac{\overline{\omega}}{\varkappa}\right) = +1. \tag{30}$$

Так как число α примарно, т. е. сравнимо с квадратом целого числа в k по модулю 2^2, то, как легко видеть, $n(\alpha) \equiv 1$ по модулю 2^2 и, следовательно, должно быть

$$\left(\frac{-1}{\alpha}\right) = (-1)^{(n(\alpha)-1)/2} = +1.$$

Таким образом, мы получаем из (30) равенство

$$\left(\frac{\overline{\omega}}{\varkappa}\right) = +1, \quad \text{а значит, и} \quad \left(\frac{\omega}{\varkappa}\right) = +1,$$

что противоречит нашему предположению, согласно которому идеал $\mathfrak{q}$ должен быть неразложим в k. Следовательно, это предположение неверно, т. е. любой простой идеал поля k, который принадлежит главному классу в k, распадается в $K(\sqrt{\omega})$ в произведение двух простых идеалов, как и утверждается в первой части теоремы 9c.

§ 13.

Теперь обсудим закон взаимности для квадратичных вычетов в поле k при специальном предположении, что $h = \overline{h} = 2$, которое было сделано об этом поле в § 8. Первое дополнение к закону взаимности снова формулируется в точности как теорема 1, коль скоро мы придадим следующий узкий смысл понятию примарного идеала: будем называть взаимно простой с 2 идеал $\mathfrak{a}$ из положенного в основу поля k *примарным*, в случае когда

$$\left(\frac{\xi}{\mathfrak{a}}\right) = +1$$

не только для любой единицы ξ, но и для тех целых чисел ξ в k, которые являются квадратами идеалов, т. е. когда

$$\left(\frac{\varepsilon_1}{\mathfrak{q}}\right) = +1, \quad \left(\frac{\varepsilon_2}{\mathfrak{q}}\right) = +1, \quad \ldots, \quad \left(\frac{\varepsilon_{m/2+1}}{\mathfrak{q}}\right) = +1.$$

Если сузить соответствующим образом понятие гиперпримарного идеала в нашем основном поле k, то сохраняет силу и второе дополнение в форме теоремы 2, равно как и общий закон взаимности в форме теоремы 3.

Что касается доказательства этого закона взаимности, то напомним, что поле классов $K(\sqrt{\omega})$ имеет нечетное число классов. Для любого такого поля закон взаимности был уже доказан в моем сочинении о квадратичных полях. После этого мы без затруднений получим только что упомянутый закон взаимности для поля k из закона взаимности для поля $K(\sqrt{\omega})$ при помощи надлежащих рассуждений.

В упомянутом сочинении я показал, при принятых в § 3 этой работы предположениях, как распределяются по родам классы идеалов произвольного относительного квадратичного поля над k. При действующем в данный момент предположении о том, что $h = \overline{h} = 2$, которое мы сделали о поле k в § 8, классы идеалов произвольного относительного квадратичного поля $K(\sqrt{\mu})$ над k распределяются по родам следующим образом. Пусть $\mathfrak{J}$ — произвольный идеал относительного квадратичного поля $K(\sqrt{\mu})$. Прежде всего мы определим, как и в случае, к которому относилось мое сочинение о квадратичных полях, систему характеров некоторого числа поля k. После этого будем понимать под r некоторый определенный взаимно простой с 2 идеал, который не принадлежит главному классу в k, и выберем такой показатель $u = 0, 1$, что в поле k относительная норма $\mathfrak{J}$ эквивалентна идеалу $\mathfrak{r}^u$. Пусть, скажем,

$$N(\mathfrak{J})\mathfrak{r}^u = (\iota),$$

где ι — подходящее целое число в k. Наконец, построим систему характеров числа ι и добавим к ней еще единицу $(-1)^u$. Так полученную систему из единиц ± 1 назовем системой характеров идеала $\mathfrak{J}$. Все идеалы, обладающие одной и той же системой характеров, образуют один род. Снова *имеет место фундаментальная теорема о том, что всегда точно половина всех возможных систем характеров действительно представляется родами из* $K(\sqrt{\mu})$.

Если для некоторого поля k значения числа классов h в первоначальном смысле и числа классов $\overline{h}$ в узком смысле совпадают, но равны не 2, а некоторому удвоенному нечетному числу, то теоремы, высказанные в §§ 8–13, нуждаются только в незначительных и легко усматриваемых из моего сочинения о квадратичных полях видоизменениях.

§ 14.

Наконец, следует кратко разобрать предположение о том, что основное поле k имеет число классов $h = \overline{h} = 4$. Тогда мы должны различать два случая.

A. В k существует такой класс C, что $C, C^2, C^3, C^4 = 1$ представляют четыре класса поля k.

B. В k существую т такие два класса C_1, C_2, что $C_1, C_2, C_1C_2 = C_3$, $C_1^2 = C_2^2 = 1$ представляют четыре класса поля k.

В случае A поле классов Kk поля k является относительно циклическим относительной степени 4 над k и обнаруживает следующие основные свойства.

Теорема 11a. *Поле классов* Kk *имеет относительный дискриминант* 1 *над* k.

Теорема 11b. *Числа классов* $H, \overline{H}$ *поля классов* Kk *как в первоначальном, так и в узком смысле представляют собой нечетное число. Поле классов* Kk *обладает одним и только относительным квадратичным подполем* UKk. *Число классов поля* UKk *равно удвоенному нечетному числу.*

Теорема 11c. *Те простые идеалы в* k, *которые являются главными в* k, *т. е. принадлежат классу* 1, *распадаются в* Kk *в произведение четырех простых идеалов. Те простые идеалы в* k, *которые принадлежат классу* C^2, *распадаются в* UKk *в произведение таких двух простых идеалов, которые остаются неразложимыми в* Kk. *Те простые идеалы в* k, *которые принадлежат классу* C *или* C^3, *остаются неразложимыми в* Kk. *Все идеалы поля* k *становятся главными в* Kk.

Любое из этих трех свойств 11a, 11b, 11c однозначно характеризует поле классов Kk, если для поля k выполнены наши предположения. В частности, справедливы следующие теоремы.

Теорема 12a. *Если некоторое относительное квадратичное поле имеет относительный дискриминант* 1 *над* k, *то оно совпадает с* UKk. *Если некоторое относительно абелево поле относи-*

тельной степени 4 *имеет относительный дискриминант* 1 *над* k, *то оно совпадает с* Kk.

Теорема 12b. *Если некоторое относительное квадратичное поле над* k *обладает числом классов, которое равно удвоенному нечетному числу, то это поле совпадает с* UKk.

Теорема 12c. *Если некоторое относительно абелево поле относительной степени* 4 *над* k *обладает нечетным числом классов, то оно совпадает с* Kk.

В случае B поле классов Kk поля k является относительно абелевым относительной степени 4 и обнаруживает следующие основные свойства.

Теорема 13a. *Поле классов* Kk *имеет относительный дискриминант* 1 *над полем* k.

Теорема 13b [1]. *Число классов поля* Kk *нечетно. Поле классов* Kk *обладает тремя относительно квадратичными подполями* UKk_1, UKk_2, UKk_3 *над* k. *Число классов каждого из этих трех подполей равно удвоенному нечетному числу.*

Теорема 13c. *Те простые идеалы в* k, *которые являются главными в* k, *т. е. принадлежат классу* 1, *распадаются в* Kk *в произведение четырех простых идеалов. Те простые идеалы в* k, *которые принадлежат классу* C_1, *распадаются в одном из трех подполей, скажем в* UKk_1, *в произведение двух простых идеалов и являются неразложимыми в каждом из двух других полей, т. е. в* UKk_2, UKk_3. *Те простые идеалы в* k, *которые принадлежат классу* C_2 (*соответственно классу* C_3), *распадаются, скажем в* UKk_2 (*соответственно в* UKk_3), *в произведение двух простых идеалов и являются неразложимыми в* UKk_1, UKk_3 (*соответственно в* UKk_1, UKk_2). *Все идеалы поля* k *становятся главными в каждом из трех относительных квадратичных полей* UKk_1, UKk_2, UKk_3.

Снова каждый из этих свойств полностью характеризуются поле классов Kk и его три подполя UKk_1, UKk_2, UKk_3.

Приведенные выше теоремы 11a, 11b, 11c, 12a, 12b, 12c, 13a, 13b, 13c подтверждают как легко проверить, справедливость формулируемых ниже в § 16 общих теорем 14 и 15 при ныне действующем предположении $h = \overline{h} = 4$ как в случае A, так и в случае B.

Для доказательства теорем 11–13 надо прежде всего показать, что при сделанных предположениях для основного поля k всегда существует хотя бы одно относительное квадратичное поле с относительным дискриминантом 1. Затем следует построить над ним еще одно относительное квадратичное поле с относительным дискриминантом 1, что всегда можно сделать на основании уже доказанной теоремы 9a.

Если для некоторого поля k общее значение числа классов h в первоначальном смысле и числа классов h в узком смысле равны не 4, а какому-либо учетверенному нечетному числу, то высказанные здесь теоремы нуждаются лишь в незначительных и легко усматриваемых из моего сочинения о квадратичных полях видоизменениях.

§ 15.

Доказанные выше теоремы и общие теоремы, формулируемые в следующем параграфе (§ 16), показывают, что для полного изучения арифметических свойств произвольного заданного основного поля k прежде всего необходимо знание отвечающего ему поля классов Kk. Развитая нами теория дает возможность арифметическим путем фактически найти поле классов Kk в каждом отдельном случае. Ниже мы указываем один трансцендентный метод определения этого поля классов, который соответствует известному методу трансцендентного определения числа классов, изобретенному на свет Дирихле.

Относительно основного поля k мы сделаем предположение, что $h = \overline{h} = 2$, и обозначим через $\varkappa$ соответствующее полю k число, которое было определено в § 25 моего сообщения «Über die Theorie der algebraischen Zahlkörper»[5]. Далее, пусть J обозначает число классов поля классов Kk и K — аналогичным образом определенное число для поля классов Kk. Тогда имеет место следующая формула:

$$\lim_{s\to 1}\left\{\sum_{(\mathfrak{j}^{(+)})}\frac{1}{n(\mathfrak{j}^{(+)})^s}-\sum_{(\mathfrak{j}^{(-)})}\frac{1}{n(\mathfrak{j}^{(-)})^s}\right\}=\frac{H\mathsf{K}}{h\varkappa}\qquad(s>1),\tag{31}$$

где сумма $\sum_{(\mathfrak{j}^{(+)})}$ распространена на все главные идеалы $\mathfrak{j}^{(+)}$ в k, а сумма $\sum_{(\mathfrak{j}^{(-)})}$ — на все неглавные идеалы в k. Выражение для K содержит логарифмы единиц поля классов Kk в определенной комбинации, так что с его помощью можно дать желаемое определение поля классов.

Для доказательства формулы (31) мы рассмотрим произведение

$$\zeta(s)=\prod_{(w)}\frac{1}{1-n(w)^{-s}},\tag{32}$$

в котором w пробегает все простые идеалы поля k. Оно сходится для вещественных значений $s>1$ и

$$\lim_{s\to 1}\{(s-1)\zeta(s)\}=h\varkappa.\tag{33}$$

Соответствующее произведение для поля Kk имеет вид

$$\mathsf{Z}(s)=\prod_{(\mathfrak{M})}\frac{1}{1-nN(\mathfrak{M})^{-s}}\qquad(s>1),$$

где $\mathfrak{M}$ пробегает все простые идеалы поля Kk и nN обозначает норму относительной нормы $\mathfrak{M}$ в k, т. е. норму в Kk. Имеем

$$\lim_{s\to 1}\{(s-1)\mathsf{Z}(s)\}=H\mathsf{K}.\tag{34}$$

Теперь мы будем различать среди простых идеалов $\mathfrak{M}$ те, которые возникают из разложения какого-либо простого идеала в k, и те, которые являются простыми идеалами в k. Ввиду теоремы 9c для первых $N(\mathfrak{M})$ равна

[5] См. Jber. der Deutschen Mathematiker-Vereinigung, 1894–95, Bd. 4, S. 229.

некоторому простому идеалу $\mathfrak{w}^{(+)}$ главного класса в k; для последних же она равна квадрату некоторого простого идеала $\mathfrak{w}^{(-)}$ в k, не принадлежащего главному классу. Поэтому

$$Z(s) = \prod_{(\mathfrak{w}^{(+)})} \frac{1}{\left(1 - n(\mathfrak{w}^{(+)})^{-s}\right)^2} \prod_{(\mathfrak{w}^{(-)})} \frac{1}{1 - n(\mathfrak{w}^{(-)})^{-2s}},$$

и ввиду (32) отсюда следует, что

$$\frac{Z(s)}{\zeta(s)} = \prod_{(\mathfrak{w}^{(+)})} \frac{1}{1 - n(\mathfrak{w}^{(+)})^{-s}} \prod_{(\mathfrak{w}^{(-)})} \frac{1}{1 + n(\mathfrak{w}^{(-)})^{-s}} = \sum_{(\mathfrak{j}^{(+)})} \frac{1}{n(\mathfrak{j}^{(+)})^s} - \sum_{(\mathfrak{j}^{(-)})} \frac{1}{n(\mathfrak{j}^{(-)})^s}.$$

С учетом (33) и (34) это равенство дает при переходе к пределу при $s \to 1$ утверждаемую формулу (31).

§ 16.

Наконец, пусть k — вполне произвольное числовое поле. Мы примем следующие соглашения, в которых нет никаких ограничительных предположений о поле k.

1. Среди m сопряженных полей $k, k', k'', \ldots, k^{(m-1)}$ имеется произвольное число s вещественных полей.

2. Число классов идеалов поля k, понимаемое в узком смысле, равно произвольному числу $\overline{h}$.

Относительно абелево поле K над k называется *неразветвленным*, если относительный дискриминант K над k равен 1, или, что то же самое, если в k не существует простых идеалов, которые делятся на квадрат простого идеала в K. Ниже мы формулируем две теоремы, которые были выше доказаны лишь для определенных частных случаев, хотя, как я убежден, с помощью развитых мною методов можно доказать их в полной общности.

Теорема 14. *Над k всегда существует однозначно определенное относительно абелево неразветвленное поле Kk относительной степени $\overline{h}$. Назовем это поле Kk полем классов поля k. Это поле классов Kk содержит все относительно абелевы неразветвленные поля над k в качестве подполей.*

Относительная группа поля классов Kk изоморфна абелевой группе, определяемой композицией классов идеалов в k[6]*.*

Те простые идеалы $\mathfrak{p}$ поля k, которые принадлежат одному и тому же классу идеалов, понимаемому в узком смысле, разлагаются в поле классов Kk на одно и то же число простых идеалов с одними и теми же степенями, так что характер разложения простого идеала $\mathfrak{p}$ поля k в поле Kk зависит только от класса, которому принадлежит этот простой идеал в поле k.

Определение 7. Целое число A поля классов Kk будем называть *амбивалентом* этого поля, если оно удовлетворяет следующим двум условиям:

---

[6] Ср. с исследованиями Г. Вебера: *Weber H.* Über Zahlengruppen in algebraischen Körpern. — Math. Ann., Bd. 48, S. 433; Bd. 49, S. 83.

a) это число A всюду положительно (см. определение 5), т. е. идеал, представляемый A, принадлежит главному классу в k в узком смысле;

b) каждое относительно сопряженное с A число отличается от A лишь множителем, который является единицей в Kk.

Амбивалент называется *простым амбивалентом*, если он не является единицей и если его нельзя представить как произведение двух амбивалентов, ни один из которых не является единицей.

Теорема 15. *Любой амбивалент поля классов Kk представляет идеал основного поля k, и, наоборот, любой идеал основного поля k может быть представлен амбивалентом поля классов Kk, который определяется данным идеалом с точностью до умножения на единицу.*

Следовательно, любой амбивалент поля классов Kk разлагается в произведение простых амбивалентов и притом, с точностью до единичных множителей, единственным способом.

Среди всех относительно абелевых полей над k свойствами, указанными в этой теореме, обладает только поле классов Kk.

И для произвольного поля k самый общий закон взаимности для квадратичных вычетов выражается формулой из теоремы 7. Закон взаимности для высших степенных вычетов допускает столь же простую и общую формулировку[7].

Наконец, следует заметить, что надлежащее обобщение изложенной здесь теории приводит к созданию теории «полей классов колец», т. е. таких относительно абелевых полей над k, которые находятся в некоторой тесной связи с классами идеалов некоторого кольца в k, подобно тому как рассматриваемые здесь поля классов Kk связаны с обычными классами идеалов поля k.

---

[7] См. конкурсную тему Гёттингенского научного общества на 1901 г. (Math. Ann., Bd. 51. S. 159). Удостоенная премии работа Фуртвенглера на эту тему была опубликована в Abh. Ges. Wiss. Göttingen, Math.-phys. Kl. (Neue Folge II, Nr. 3, 1902).

ДОКАЗАТЕЛЬСТВО ПРЕДСТАВИМОСТИ ЦЕЛЫХ ЧИСЕЛ С ПОМОЩЬЮ ФИКСИРОВАННОГО ЧИСЛА n-Х СТЕПЕНЕЙ (ПРОБЛЕМА ВАРИНГА)*)1)

Посвящается памяти Германа Минковского

Теорема. *Каждое положительное целое число допускает представление в виде суммы n-х степеней положительных целых чисел, количество которых не превосходит некоторой границы, определяемой только показателем n и не зависящей от представляемого числа.*

Эта теорема в общем виде была высказана в качестве гипотезы Варингом[2]; ее доказательство до сих пор удалось получить лишь в отдельных случаях, а именно для

$$n = 2, 3, 4, 5, 6, 7, 8, 10.$$

Математиками, которым мы должны быть признательны за эти доказательства, а также за остроумные исследования о минимальном количестве используемых в представлении степеней, являются Ж. Лиувилль [1] ($n = 4$), Майе (Maillet)[3] ($n = 3, n = 5, n = 8$), Флек (Fleck)[4] ($n = 6$), Ландау (Landau)[5] ($n = 3, n = 4$), И. Шур [2] ($n = 10$), Гурвиц (Hurwitz)[6] ($n = 8$), Виферих (Wieferich)[7] ($n = 3, n = 4, n = 5, n = 7$).

Общее доказательство теоремы, которое я привожу ниже, получилось с помощью *нового способа приложения анализа к теории чисел.* А именно, если в аналитической теории чисел из арифметических формул удается с помощью предельного перехода получить интегральные соотношения для арифметических величин — вспомним о нахождении числа классов — или, как в теории простых чисел, с помощью трансцендентных

---

*) Beweis für Darstellbarkeit der ganzen Zahlen durch eine feste Anzahl n-ter Potenzen (Waringsches Problem). — Math. Ann., 1909, Bd 67, S. 281–300. *Перевод Е. М. Матвеева.*

1) С некоторыми изменениями и дополнениями перепечатывается из Nachr. Ges. Wiss. Göttingen, Math.-phys. Kl., 1909, Sitzg. 6. Februar, S. 17–36.

2) Meditationes algebricae, ed. III. Cambridge 1782, S. 349–350.

3) Congres de Boddeaux 1895. — J. de Mathem., Ser. 5, 1896 vol. 2; C. r. Acad. Sci. Paris, 1907, vol. 145; Bull. Soc. math. France, 1908, vol. 36.

4) Sitzgsber. Berl. math. Ges. 1906; Math. Ann., 1907, Bd. 64.

5) Rendiconti Circ. mat. Palermo, 1907, vol. 23; Math. Ann., 1908, Bd. 66.

6) Math. Ann., 1908, Bd. 65.

7) Math. Ann., 1908–09, Bd. 66 (Abhandlengen).

функций ищут асимптотические выражения, я, наоборот, буду исходить из определенной интегральной формулы и из нее в конце получу чисто арифметическое соотношение.

Чтобы отчетливее выделить основные идеи, я предпошлю доказательству теоремы два утверждения.

Теорема I. *Пусть m — произвольное положительное целое число. Тогда тождественно по 5 переменным $x_1, \ldots, x_5$ справедлива интегральная формула*

$$(x_1^2 + \cdots + x_5^2)^m = C \int\limits_{(S)} \cdots \int (t_1 x_1 + \cdots + t_5 x_5)^{2m} dt_1 \ldots dt_5, \tag{1}$$

где C обозначает некоторую определяемую через m положительную константу, а именно

$$\frac{(2m+1)(2m+3)(2m+5)}{8\pi^2}$$

и 5-кратный интеграл справа распространен на шар S

$$t_1^2 + \cdots + t_5^2 \leqslant 1. \tag{2}$$

Для доказательства будем понимать под $x_1, \ldots, x_5$ произвольные вещественные величины и рассмотрим ортогональную замену пяти переменных $t_1, \ldots, t_5$ на пять переменных $t_1', \ldots, t_5'$

$$\begin{aligned} t_1' &= \alpha_{11} t_1 + \ldots + \alpha_{51} t_5, \\ &\ldots\ldots\ldots\ldots\ldots \\ t_5' &= \alpha_{15} t_1 + \ldots + \alpha_{55} t_5, \end{aligned} \tag{3}$$

где

$$\alpha_{11} = \frac{x_1}{\sqrt{x_1^2 + \cdots + x_5^2}}, \quad \ldots, \quad \alpha_{51} = \frac{x_5}{\sqrt{x_1^2 + \cdots + x_5^2}}. \tag{4}$$

Поскольку шар S при такой замене (3) остается неизменным, интеграл в формуле (1) после перехода к переменным интегрирования $t_1', \ldots, t_5'$ превращается в

$$(x_1^2 + \cdots + x_5^2)^m \int\limits_{(S)} \cdots \int t_1'^{2m} dt_1' \ldots dt_5';$$

очевидно, что последний 5-кратный интеграл представляет собой не зависящее от $x_1, \ldots, x_5$ положительное число; если обозначить его через $1/C$, то получается доказываемая формула (1).

Теорема II. *Пусть снова m — произвольное положительное целое число, тогда тождественно по 5 переменным $x_1, \ldots, x_5$ выполняется формула вида*

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} r_h (a_{1h} x_1 + \ldots + a_{5h} x_5)^{2m}. \tag{5}$$

Здесь для краткости положено

$$M = \frac{(2m+1)(2m+2)(2m+3)(2m+4)}{1 \cdot 2 \cdot 3 \cdot 4};$$

далее, $r_1, \ldots, r_M$ *обозначают некоторые положительные рациональные числа, зависящие от* m, *и* $a_{1h}, \ldots, a_{5h}$ *— некоторые целые числа, также зависящие от* m.

Доказательство основано на установленной в теореме I интегральной формуле; исходя из нее, мы после ряда шагов придем к утверждаемому арифметическому тождеству.

Первый шаг заключается в аппроксимации 5-кратного интеграла

$$C \int\limits_{(S)} \cdots \int (t_1 x_1 + \cdots + t_5 x_5)^{2m} dt_1 \ldots dt_5$$

некоторой конечной суммой. Разобьем наше 5-мерное пространство переменных t_h на 5-мерные кубики с ребром длины ε. Поскольку область S ограничена, внутри области S будет лежать лишь конечное число $H^{(\varepsilon)}$ этих кубов. Возьмем, далее, значение подынтегральной функции, т. е. $2m$-й степени линейного выражения

$$t_1 x_1 + \cdots + t_5 x_5,$$

в центре каждого из этих кубиков, умножим его на положительный корень $\sqrt[2m]{C}$, а затем [3] на объем кубика ε^5; тогда из интеграла возникнет сумма вида

$$\sum_{h=1,\ldots,H^{(\varepsilon)}} \left\{ P_h^{(\varepsilon)}(x) \right\}^{2m}, \tag{6}$$

где $P_h^{(\varepsilon)}$ суть $H^{(\varepsilon)}$ линейных функций от $x_1, \ldots, x_5$, коэффициенты которых зависят от ε. При этом выполняется предельное соотношение

$$C \int\limits_{(S)} \cdots \int (t_1 x_1 + \cdots + t_5 x_5)^{2m} dt_1 dt_2 \ldots dt_5 = \lim_{\varepsilon \to 0} \sum_{h=1,\ldots,H^{(\varepsilon)}} \left\{ P_h^{(\varepsilon)}(x) \right\}^{2m}.$$

В силу интегральной формулы из теоремы I имеем также

$$(x_1^2 + \cdots + x_5^2)^m = \lim_{\varepsilon \to 0} \sum_{h=1,\ldots,H^{(\varepsilon)}} \left\{ P_h^{(\varepsilon)}(x) \right\}^{2m}. \tag{7}$$

Второй существенный шаг состоит в том, что в последней сумме мы сводим число $H^{(\varepsilon)}$, которое при стремящемся к нулю ε неограниченно возрастает, к некоторому фиксированному, не зависящему от ε числу. Это удается сделать следующим образом. Вспомним, что имеется только M линейно независимых форм степени $2m$ от 5 переменных и что поэтому между первыми $M+1$ из наших форм степени $2m$

$$\left\{ P_h^{(\varepsilon)}(x) \right\}^{2m} \qquad (h = 1, \ldots, M+1)$$

обязательно должно существовать связывающее их тождество вида

$$c_1 P_1^{(\varepsilon)2m} + c_2 P_2^{(\varepsilon)2m} + \cdots + c_{M+1} P_{M+1}^{(\varepsilon)2m} = 0,$$

где $c_1, \ldots, c_{M+1}$ — вещественные постоянные, среди которых должны быть как положительные, так и отрицательные. Разделив это тождество на наибольший из положительных коэффициентов, получим тождество вида

$$c'_1 P_1^{(\varepsilon)2m} + c'_2 P_2^{(\varepsilon)2m} + \cdots + c'_{M+1} P_{M+1}^{(\varepsilon)2m} = 0,$$

где обязательно один из коэффициентов $c'_1, \ldots, c'_{M+1}$ равен $+1$, все же остальные $\leqslant 1$. Вычтем это тождество из суммы (6), тогда, очевидно, одна из $2m$-х степеней сократится и мы получим сумму из $H^{(\varepsilon)} - 1$ слагаемых, среди которых нет отрицательных, поскольку при всех $P_h^{(\varepsilon)2m}$ коэффициентами будут лишь положительные числа либо нуль. Если мы введем эти коэффициенты под знак $2m$-й степени, то придем к формуле вида

$$\sum_{h=1,\ldots,H^{(\varepsilon)}} \left\{P_h^{(\varepsilon)}(x)\right\}^{2m} = \sum_{h=1,\ldots,H^{(\varepsilon)}-1} \left\{P_h'^{(\varepsilon)}(x)\right\}^{2m},$$

где $P_h'^{(\varepsilon)}$ снова обозначает линейную форму от переменных $x_1, \ldots, x_5$, причем число слагаемых справа по сравнению с первоначальной суммой слева уменьшилось на 1.

Вышеприведенный метод редукции можно применять повторно, пока число слагаемых не станет равным M. Таким образом, мы получим формулу вида

$$\sum_{h=1,\ldots,H^{(\varepsilon)}} \left\{P_h^{(\varepsilon)}(x)\right\}^{2m} = \sum_{h=1,\ldots,M} \left\{Q_h{}^{(\varepsilon)}(x)\right\}^{2m}, \tag{8}$$

где снова

$$Q_h^{(\varepsilon)}(x) = q_{h1}^{(\varepsilon)} x_1 + \cdots + q_{h5}^{(\varepsilon)} x_5 \qquad (h = 1, \ldots, M)$$

— линейная форма от переменных $x_1, \ldots, x_5$, коэффициенты $q_{hk}^{(\varepsilon)}$ которой пока еще существенно зависят от ε.

Наш *следующий* шаг состоит в предельном переходе к $\varepsilon = 0$. Чтобы выполнить этот переход, запишем вытекающую из (7) и (8) формулу

$$(x_1^2 + \cdots + x_5^2)^m = \lim_{\varepsilon \to 0} \sum_{h=1,\ldots,M} \left\{Q_h^{(\varepsilon)}(x)\right\}^{2m}. \tag{9}$$

Прежде всего, совершенно ясно, что если ε достаточно мало, то все коэффициенты форм $Q_h^{(\varepsilon)}$ ограничены величиной, не зависящей от ε; это следует из предельных соотношений

$$1 = \lim_{\varepsilon \to 0} (q_{1k}^{(\varepsilon)2m} + q_{2k}^{(\varepsilon)2m} + \cdots + q_{Mk}^{(\varepsilon)2m}),$$

которые получаются путем приравнивания коэффициентов при x_k^{2m} в (9). Так как, в частности, величина $q_{11}^{(\varepsilon)}$ остается ограниченной, мы можем найти такую сходящуюся к 0 последовательность положительных значений $\varepsilon_1, \varepsilon_2, \ldots$, что существует предел

$$\lim_{r \to \infty} q_{11}^{(\varepsilon_r)} = q_{11}.$$

Далее, ограничено также и $q_{21}^{(\varepsilon)}$, что позволяет снова из последовательности

$\varepsilon_1, \varepsilon_2, \ldots$ выбрать такую подпоследовательность $\varepsilon_1', \varepsilon_2', \ldots$, что существует также предел

$$\lim_{r\to\infty} q_{21}^{(\varepsilon_r')} = q_{21}.$$

Продолжая таким образом, получим после $5M$-кратного применения этого приема сходящуюся к нулю последовательность $\bar{\varepsilon}_1, \bar{\varepsilon}_2, \ldots$, для которой имеют место одновременно все предельные соотношения

$$\lim_{r\to\infty} q_{hk}^{(\bar{\varepsilon}_r)} = q_{hk} \qquad (h = 1, \ldots, M, k = 1, \ldots, 5).$$

Положим теперь

$$Q_h(x) = q_{h1}x_1 + \cdots + q_{h5}x_5 \qquad (h = 1, \ldots, M).$$

Тогда, ввиду (9), тождественно по $x_1, \ldots, x_5$ справедлива формула

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} Q_h^{2m}(x). \tag{10}$$

Эта формула еще существенно отличается от указанной в теореме тем, что коэффициенты линейных форм Q_h не обязаны быть рациональными числами.

Последний, решающий шаг моего доказательства будет заключаться в том, чтобы от формулы (10) перейти к формуле, в которой все числовые коэффициенты были бы рациональными. Для этой цели подберем сначала M линейных форм

$$G_h(x) = a_{h1}x_1 + \cdots + a_{h5}x_5 \qquad (h = 1, \ldots, M)$$

с целочисленными коэффициентами a_{hk} таким образом, чтобы между их $2m$-ми степенями не существовало никакого линейного соотношения с постоянными коэффициентами. Это возможно, поскольку определитель

$$A = \begin{vmatrix} a_{11}^{2m} & a_{21}^{2m} & \ldots & a_{M1}^{2m} \\ a_{11}^{2m-1}a_{12} & a_{21}^{2m-1}a_{22} & \ldots & a_{M1}^{2m-1}a_{M2} \\ \ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots \\ a_{15}^{2m} & a_{25}^{2m} & \ldots & a_{M5}^{2m} \end{vmatrix},$$

очевидно, не равен тождественно нулю, и для выполнения нашего требования достаточно так подобрать целые рациональные числа a_{hk}, чтобы A получился отличным от нуля.

Далее, пусть в формуле (10), скажем, Q_1 есть линейная форма, среди коэффициентов которой имеются отличные от нуля, так что

$$q_{11}^2 + \cdots + q_{15}^2$$

является положительным числом. Положим для краткости

$$\alpha_h = \sqrt{\frac{q_{11}^2 + \cdots + q_{15}^2}{a_{h1}^2 + \cdots + a_{h5}^2}} \qquad (h = 1, \ldots, M).$$

Тогда у каждой из M линейных форм

$$\alpha_1 G_1, \quad \ldots, \quad \alpha_M G_M$$

суммы квадратов коэффициентов будут такими же, как у Q_1. Поэтому существует ортогональное преобразование переменных $x_1, \ldots, x_5$, которое пе-

реводит Q_1 в $\alpha_1 G_1$, далее, такое ортогональное преобразование, которое переводит Q_1 в $\alpha_2 G_2, \ldots$ и, наконец, в $\alpha_M G_M$. Применим все эти ортогональные преобразования по очереди к формуле (10), сложим возникающие формулы и поделим на M. Полагая

$$\rho_1 = \frac{\alpha_1^{2m}}{M}, \quad \ldots, \quad \rho_M = \frac{\alpha_M^{2m}}{M},$$

приходим к формуле

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} \rho_h G_h^{2m}(x) + \sum_{h=1,\ldots,M(M-1)} S_h^{2m}(x), \qquad (11)$$

где S_h являются некоторыми $M(M-1)$ линейными формами от $x_1, \ldots, x_5$, получающимися из $Q_2, \ldots, Q_M$ с помощью указанных ортогональных преобразований и умножения на $1/\sqrt[2m]{M}$. Рассмотрим теперь систему из M линейных уравнений с неизвестными $u_1, \ldots, u_M$, которая получается из тождества

$$\sum_{h=1,\ldots,M} u_h G_h^{2m}(x) = (x_1^2 + \cdots + x_5^2)^m - \sum_{h=1,\ldots,M(M-1)} S_h^{2m}(x)$$

после приравнивания коэффициентов при соответствующих степенях и произведениях степеней переменных $x_1, \ldots, x_5$. Поскольку определитель этой системы уравнений с точностью до отличного от нуля числового множителя совпадает с числом A, ее решения однозначно определены; в силу (11) они выглядят как

$$u_1 = \rho_1, \quad \ldots, \quad u_M = \rho_M$$

и, следовательно, все *положительны*. Решения системы линейных уравнений с отличным от нуля определителем являются непрерывными функциями от правых частей. Отсюда следует, что когда мы меняем коэффициенты линейных форм S_h, оставаясь внутри некоторой достаточно малой области, решения $u_1, \ldots, u_M$ видоизмененной системы уравнений остаются *положительными*. Выберем внутри этой области рациональные коэффициенты. Тогда решения $u_1, \ldots, u_M$ должны оказаться к тому же рациональными, поскольку все коэффициенты G_h являются целыми рациональными числами. Обозначим через S'_h формы с рациональными коэффициентами, выступающие вместо форм S_h, и пусть соответствующими положительными рациональными решениями будут

$$u_1 = r_1, \quad \ldots, \quad u_M = r_M.$$

Тогда справедливо тождество

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M} r_h G_h^{2m}(x) + \sum_{h=1,\ldots,M(M-1)} S'^{2m}_h(x).$$

Если мы теперь для каждой из форм S'_h приведем коэффициенты к общему знаменателю и вынесем его за скобку, а формы с целочисленными коэффициентами обозначим через $G_{M+1}, \ldots, G_{M^2}$, то получим

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,M^2} r_h G_h^{2m}(x), \qquad (12)$$

где $r_1, \ldots, r_{M^2}$ — положительные рациональные числа, а все коэффициенты форм G_h — целые числа.

В заключение мы можем применить к формуле (12) метод редукции, аналогичный тому, который привел нас выше к формуле (8). Между линейными формами $G_1, \ldots, G_{M+1}$ должно существовать тождество вида

$$c_1 G_1^{2m}(x) + \cdots + c_{M+1} G_{M+1}^{2m}(x) = 0, \tag{13}$$

где теперь $c_1, \ldots, c_{M+1}$ — рациональные числа. Определим рациональное число c таким образом, чтобы среди чисел

$$\frac{cc_1}{r_1}, \quad \ldots, \quad \frac{cc_{M+1}}{r_{M+1}}$$

одно равнялось 1 и остальные были $\leqslant 1$. Вычтем тождество (13), умноженное на c, из правой части формулы (12). В возникающей справа сумме один из коэффициентов будет нулевым и никакой из остальных не будет отрицательным, так что вновь получившаяся формула содержит справа на одно слагаемое меньше. Продолжая таким образом, мы в конце концов приходим к формуле, которая удовлетворяет всем требованиям теоремы, чем ее доказательство и завершается.

Следует еще добавить, что если мы в проведенном рассуждении в качестве Q_1 возьмем не какую попало из M линейных форм $Q_1, \ldots, Q_M$, а такую из них, для которой сумма квадратов коэффициентов получается наибольшей, то, используя тождества (10), для этой суммы квадратов

$$q_{11}^2 + \cdots + q_{15}^2$$

легко найти нижнюю границу, зависящую только от m, и что из этой нижней границы также без особого труда выводится верхняя граница σ для размеров области, внутри которой могут меняться коэффициенты форм S_h без того, чтобы соответствующие решения $u_1, \ldots, u_M$ стали отрицательными. Зная σ, можно найти верхнюю границу, зависящую только от m, для абсолютных значений числителя и знаменателя фигурирующих в формулировке теоремы II рациональных чисел r_h и для абсолютных значений целых чисел a_{kh}.

Формула из теоремы II — центральное ядро доказательства нашей главной теоремы. Именно она позволяет из справедливости теоремы Варинга для степени m сразу же заключить о ее справедливости для степени $2m$[8]. Если мы обозначим зависящий только от m общий знаменатель рациональных чисел r_h, входящих в правую часть формулы (5), через E, возьмем $x_5 = 0$ и заметим, что каждое целое положительное число допускает представление в виде суммы четырех квадратов, то формула (5) сразу показывает, что в предположении, что теорема Варинга верна для m-й степени, каждое делящееся на E положительное целое число может быть представлено в виде суммы некоторого количества $2m$-х степеней, ограниченного величиной, зависящей только от m. Поскольку каждое положительное целое число допускает представление в форме $HE + K$, где H и K — положительные целые числа [4] и $K < E$, отсюда следует справедливость теоремы Варинга для $2m$-й степени, ибо число K является суммой не более чем $E - 1$ чисел 1^{2m}.

Поскольку теорема Варинга верна для $m = 2$, то, в силу предыдущего, она верна для бесконечного множества показателей, а именно для всех

[8] Ср.: *Hurwitz A.* — Math. Ann., 1908, Bd. 65, S. 424–427.

показателей вида $m = 2^g$. Чтобы доказать ее для произвольного показателя, нам понадобится ряд лемм.

Лемма 1. *Каждому показателю m отвечают N положительных рациональных чисел*

$$r_1, r_2, \ldots, r_N,$$

а также два положительных целых числа a, A со следующими свойствами.

Пусть x и G — произвольные положительные целые числа и Γ — произвольное вещественное положительное число. Далее, пусть X — положительное целое число, удовлетворяющее неравенству

$$X < \Gamma^2 x^2. \tag{14}$$

Тогда для этих чисел x, G, Γ, X могут быть найдены таких N целых чисел

$$X_1, X_2, \ldots, X_N,$$

абсолютные значения которых удовлетворяют оценке

$$|X_h| < A\Gamma x \qquad (h = 1, \ldots, N),$$

что

$$(G^2x^2 + X)^m = \sum_{h=1,\ldots,N} r_h(aGx + X_h)^{2m}.$$

Для доказательства перепишем формулу из теоремы II следующим образом. Если в правой части этой формулы одна или более линейных форм, возводимых в $2m$-ю степень, имеют лишь нулевые коэффициенты, то отбросим эти степени. Тогда справа останется $N \leqslant M$ слагаемых, так что наша формула будет выглядеть следующим образом:

$$(x_1^2 + \cdots + x_5^2)^m = \sum_{h=1,\ldots,N} r_h(a_{1h}x_1 + \cdots + a_{5h}x_5)^{2m}. \tag{15}$$

Здесь мы можем принять, что каждое умножаемое на x_1 число a_{1h} отлично от нуля, поскольку в противном случае применение одного из подходящих ортогональных преобразований с рациональными коэффициентами превратит нашу формулу в такую, у которой все коэффициенты при первом аргументе отличны от нуля. Подставим в формулу (15) вместо $x_1, x_2, \ldots, x_5$ соответственно $Gx, x_1, \ldots, x_4$ и положим

$$a = |a_{11}a_{12} \ldots a_{1N}|,$$

$$\frac{aa_{2h}}{a_{1h}} = a'_{1h}, \quad \frac{aa_{3h}}{a_{1h}} = a'_{2h}, \quad \ldots, \quad \frac{aa_{5h}}{a_{1h}} = a'_{4h},$$

так что $a'_{1h}, \ldots, a'_{4h}$ снова будут целыми числами. В результате получим формулу

$$(G^2x^2 + x_1^2 + \cdots + x_4^2)^m = \sum_{h=1,\ldots,N} r_h(aGx + a'_{1h}x_1 + \cdots + a'_{4h}x_4)^{2m}, \tag{16}$$

где, как легко видеть, r_h претерпели лишь несущественные изменения.

Если мы теперь обозначим через A наибольшее из N чисел

$$|a'_{1h}| + \cdots + |a'_{4h}| \qquad (h = 1, \ldots, N),$$

то утверждение леммы I устанавливается следующим рассуждением. Представим наше целое число X как сумму четырех квадратов целых чисел:

$$X = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Из (14) следует, что

$$|x_h| < \Gamma x \qquad (h = 1, \ldots, 4).$$

Если мы возьмем

$$X_h = a'_{1h}x_1 + \cdots + a'_{4h}x_4,$$

то будем иметь

$$|X_h| \leqslant (|a'_{1h}| + \cdots + |a'_{4h}|)\Gamma x < A\Gamma x.$$

Лемма 2. *Каждому показателю m отвечает, как и в лемме* 1, *N положительных рациональных чисел*

$$r_1, \quad r_2, \quad \ldots, \quad r_N$$

и два положительных целых числа a, A со следующими свойствами.

Пусть x, G, Γ таковы же, как в лемме 1. *Пусть, далее, X — положительное целое число, удовлетворяющее неравенству*

$$X < \Gamma^2 x^2. \tag{17}$$

Тогда для этих величин x, G, Γ, X могут быть найдены N таких целых чисел

$$X_1, \quad X_2, \quad \ldots, \quad X_N,$$

абсолютные значения которых удовлетворяют оценке

$$|X_h| < A\Gamma x \qquad (h = 1, \ldots, N),$$

что

$$x(G^2x^2 + X)^m = \frac{1}{G} \sum_{h=1,\ldots,N} r_h(aGx + X_h)^{2m+1}.$$

Дифференцируя (16) по x, получаем формулу вида

$$x(G^2x^2 + x_1^2 + \cdots + x_4^2)^{m-1} = \frac{1}{G} \sum_{h=1,\ldots,N} r_h(aGx + a'_{1h}x_1 + \cdots + a'_{4h}x_4)^{2m-1},$$

где r_h имеют несущественно измененные значения. Заменив в ней m на $m + 1$ и повторив рассуждение, уже примененное выше к формуле (16), получим требуемое утверждение.

Из только что доказанных лемм 1 и 2 мы выведем сейчас две дальнейшие леммы, 3 и 4, в которых утверждаются равенства, отличающиеся от установленных в леммах 1 и 2 главным образом тем, что в левой стороне вместо положительных чисел X фигурируют числа Y, для которых допустимы и отрицательные значения.

Лемма 3. *Каждому показателю m отвечают N положительных рациональных чисел*

$$r_1, \quad r_2, \quad \ldots, \quad r_N,$$

вещественная всюду положительная функция $\varphi(\varkappa)$ вещественной переменной $\varkappa$ и функция $F(K, \varkappa)$ целочисленной переменной K и вещественной переменной $\varkappa$, принимающая лишь положительные целочисленные значения и при фиксированном $\varkappa$ и неограниченно возрастающем K монотонно стремящаяся к бесконечности, для которых (т. е. для отвечающих m величин r_h, φ, F) выполнено следующее свойство.

Пусть x — произвольное положительное целое число и K — произвольное положительное число > 16. Пусть, далее, $\varkappa$ — вещественная величина, удовлетворяющая неравенству

$$1 \leqslant \varkappa < \frac{1}{2}\sqrt{K} - 1, \tag{18}$$

и пусть

$$\varkappa' = \varphi(\varkappa), \quad K' = F(K, \varkappa). \tag{19}$$

Пусть, наконец, Y — произвольное целое число, абсолютное значение которого удовлетворяет неравенству

$$|Y| < \varkappa\sqrt{K}x^2. \tag{20}$$

Тогда для этих величин $x, K, \varkappa, Y$ могут быть найдены N таких целых чисел $Y_1', \ldots, Y_N'$, абсолютные значения которых удовлетворяют оценке

$$|Y_h'| < \varkappa'\sqrt{K'}x, \tag{21}$$

таких что имеет место равенство

$$(Kx^2 + Y)^m = \sum_{h=1,\ldots,N} r_h(K'x + Y_h')^{2m}.$$

Для доказательства найдем сначала положительное целое число G, удовлетворяющее неравенствам

$$(G + \varkappa)^2 < K \leqslant (G + \varkappa + 1)^2. \tag{22}$$

Тогда

$$K - G^2 > \varkappa(2G + \varkappa) \geqslant 2\varkappa\sqrt{K} - \varkappa(\varkappa + 2)$$

и в силу (18)

$$\sqrt{K} > \varkappa + 2;$$

таким образом, мы имеем также

$$K - G^2 > \varkappa\sqrt{K}. \tag{23}$$

С другой стороны, ввиду (22)

$$K - G^2 \leqslant (\varkappa + 1)(2G + \varkappa + 1) < 2(\varkappa + 1)\sqrt{K} \leqslant 4\varkappa\sqrt{K},$$

т. е.

$$K - G^2 < 4\varkappa\sqrt{K}. \tag{24}$$

Положим теперь

$$X = (K - G^2)x^2 + Y. \tag{25}$$

В силу (23), (24) и предположения (20) доказываемой леммы

$$0 < X < 5\varkappa\sqrt{K}x^2.$$

Применим теперь лемму 1 к числам x, G, X и к числу

$$\Gamma = \sqrt{5\varkappa}\sqrt[4]{K}.$$

Тогда условие (14) этой леммы выполнено, и мы заключаем, что справедливо равенство вида

$$(G^2x^2 + X)^m = \sum_{h=1,\ldots,N} r_h(aGx + Y_h')^{2m}, \tag{26}$$

где Y_h' (т. е. X_h в лемме 1) суть целые числа, удовлетворяющие оценке

$$|Y_h'| < A\sqrt{5\varkappa}\sqrt[4]{K}x. \tag{27}$$

Положим

$$\varphi(\varkappa) = \frac{A}{\sqrt{a}}\sqrt{10\varkappa}, \quad F(K, \varkappa) = aG.$$

Эти функции удовлетворяют всем условиям доказываемой леммы. Ввиду (19) имеем

$$\varkappa' = \frac{A}{\sqrt{a}}\sqrt{10\varkappa}, \quad K' = aG,$$

и формула (26) переходит с учетом (25) в утверждаемое в лемме равенство. Наконец, из (18), (22) вытекает, что

$$(2\varkappa + 2)^2 < K \leqslant (G + \varkappa + 1)^2,$$

следовательно,

$$\varkappa + 1 < G,$$

и поэтому

$$A\sqrt{5\varkappa}\sqrt[4]{K} \leqslant A\sqrt{5\varkappa}\sqrt{G + \varkappa + 1} < A\sqrt{10\varkappa}\sqrt{G},$$

т. е.

$$A\sqrt{5\varkappa}\sqrt[4]{K} < \varkappa'\sqrt{K'}.$$

В силу этого неравенства из (27) вытекает неравенство (21), чем наша лемма полностью и доказана.

Лемма 4. *Каждому показателю τ отвечают, как и в лемме* 3, *N положительных рациональных чисел*

$$r_1, \quad r_2, \quad \ldots, \quad r_N,$$

вещественная всюду положительная функция $\varphi(\varkappa)$ вещественной переменной $\varkappa$ и функция $F(K, \varkappa)$ целочисленной переменной K и вещественной переменной $\varkappa$, принимающая лишь положительные целочисленные значения и при фиксированном $\varkappa$ и неограниченно возрастающем K монотонно стремящаяся к бесконечности, для которых (т. е. для отвечающих τ величин r_h, φ, F) выполнено следующее свойство.

Пусть $x, K, \varkappa$ — *числа, удовлетворяющие условиям леммы* 3; *пусть, как и там,*

$$\varkappa' = \varphi(\varkappa), \quad K' = F(K, \varkappa);$$

пусть, далее, Y — *произвольное целое число, абсолютное значение которого удовлетворяет оценке*

$$|Y| < \varkappa\sqrt{K}x^2.$$

Тогда для этих величин $x, K, \varkappa, Y$ *могут быть найдены* N *таких целых чисел* $Y_1', \ldots, Y_N'$, *абсолютные значения которых удовлетворяют оценке*

$$|Y_h'| < \varkappa'\sqrt{K'}x,$$

что имеет место равенство

$$x(Kx^2 + Y)^m = \frac{1}{K'} \sum_{h=1,\ldots,N} r_h(K'x + Y_h')^{2m+1}.$$

Доказательство получится, если мы в рассуждениях, примененных при доказательстве леммы 3, будем ссылаться вместо леммы 1 на лемму 2.

Лемма 5. *Каждому показателю* n *отвечают два целых числа* p, q, *удовлетворяющих условиям*

$$n = p + q \tag{28}$$

и

$$0 \leqslant p < q, \tag{29}$$

положительное целое число K *и* N^* *положительных рациональных чисел*

$$k_1, \quad k_2, \quad \ldots, \quad k_{N^*},$$

для которых выполнено следующее утверждение.

Пусть x — *произвольное положительное целое число, и пусть* Y — *целое число, абсолютное значение которого удовлетворяет оценке*

$$|Y| < \sqrt{K}x^q.$$

Тогда для этих чисел x, Y *найдутся* N^* *таких положительных целых чисел*

$$P_1, \quad P_2, \quad \ldots, \quad P_{N^*},$$

что имеет место равенство

$$x^p(Kx^q + Y) = \sum_{h=1,\ldots,N^*} kP_h^n.$$

Для доказательства запишем показатель n в двоичной системе счисления:

$$n = 2^g + e_1 2^{g-1} + e_2 2^{g-2} + \cdots + e_{g-1}2 + e_g =$$

$$= 1e_1e_2 \ldots e_{g-1}e_g;$$

здесь g — некоторый целый показатель и $e_1, e_2, \ldots, e_g$ принимают значения нуль или единица. Теперь определим $g + 1$ чисел $n_0, n_1, n_2, \ldots, n_g$

следующими равенствами:

$$n_0 = 1,$$
$$n_1 = 2 + e_1 = 1e_1,$$
$$n_2 = 2^2 + e_1 2 + e_2 = 1e_1e_2,$$
$$n_3 = 2^3 + e_1 2^2 + e_2 2 + e_3 = 1e_1e_2e_3,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$n_g = 2^g + e_1 2^{g-1} + \dots + e_{g-1}2 + e_g = 1e_1e_2 \dots e_{g-1}e_g = n,$$

так что

$$n_{h+1} = 2n_h + e_{h+1}.$$

Далее, положим

$$\begin{aligned} p_0 &= e_1 2^{g-1} + e_2 2^{g-2} + \dots + e_g = e_1e_2 \dots e_g, \\ p_1 &= e_2 2^{g-2} + e_3 2^{g-3} + \dots + e_g = e_2e_3 \dots e_g, \\ p_2 &= e_3 2^{g-2} + \dots + e_g = e_3 \dots e_g, \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ p_{g-1} &= e_g, \\ p_g &= 0, \end{aligned}$$

так что

$$p_{h-1} - p_h = e_h 2^{g-h}.$$

Наконец, пусть еще

$$p = n - 2^g = e_1 2^{g-1} + e_2 2^{g-2} + \dots + e_g = p_0,$$
$$q = 2^g,$$

так что условия (28), (29) выполнены.

Применив теперь g раз леммы 3 и 4, соответственно, придем к равенствам

$$\left.\begin{aligned} x^{p_0}\left(Kx^{2^g}+Y\right) &= \frac{1}{K'^{e_1}} \sum_{h=1,\dots,N_1} r_h^{(1)} x^{p_1}\left(K'x^{2^{g-1}}+Y'^{(1)}\right)^{n_1}, \\ x^{p_1}\left(K_1x^{2^{g-1}}+Y_1\right)^{n_1} &= \frac{1}{K_1'^{e_2}} \sum_{h=1,\dots,N_2} r_h^{(2)} x^{p_2}\left(K_1'x^{2^{g-2}}+Y_h'^{(2)}\right)^{n_2}, \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ x^{p_{g-2}}\left(K_{g-2}x^{2^2}+Y_{g-2}\right)^{n_{g-2}} &= \frac{1}{K_{g-2}'^{e_{g-1}}} \sum_{h=1,\dots,N_{g-1}} r_h^{(g-1)} x^{p_{g-1}}\left(K_{g-2}'x^2+Y_h'^{(g-1)}\right)^{n_{g-1}}, \\ x^{p_{g-1}}\left(K_{g-1}x^2+Y_{g-1}\right)^{n_{g-1}} &= \frac{1}{K_{g-1}'^{e_q}} \sum_{h=1,\dots,N_g} r_h^{(g)}\left(K_{g-1}'x+Y_h'^{(g)}\right)^{n}. \end{aligned}\right\} \quad (30)$$

Каждое из этих равенств следует понимать так, что их левая часть, если подставить в нее вместо Y_s целое число, удовлетворяющее оценке

$$|Y_s| < \varkappa_s \sqrt{K_s} x^{2^{g-s}},$$

допускает представление в виде стоящей справа суммы, где $Y_h'^{(s+1)}$ обозначают подходящим образом выбранные целые числа, удовлетворяющие оценке

$$|Y_h'^{(s+1)}| < \varkappa_s' \sqrt{K_s'} x^{2^{g-s-1}}. \tag{31}$$

При этом величины $r_h^{(s)}, \varkappa_s, \varkappa_s', K_s, K_s'$ имеют смысл, указанный в леммах 3 и 4; таким образом (нижний индекс 0 опускается),

$$\left.\begin{aligned} \varkappa_s' &= \varphi_s(\varkappa_s), \\ K_s' &= F_s(K_s, \varkappa_s) \end{aligned}\right\} \qquad (s = 0, 1, \ldots, g-1), \tag{32}$$

где φ, F — функции, фигурирующие в леммах 3 и 4. Кроме того, отметим, что $\varkappa_s$ должно удовлетворять неравенствам

$$1 \leqslant \varkappa_s < \frac{1}{2}\sqrt{K_s} - 1, \tag{33}$$

поэтому и $K_s > 16$.

Теперь для завершения доказательства леммы нам нужно, чтобы можно было слагаемые, стоящие в правой части каждой из формул (30), взять в виде левой части последующей формулы, при этом левая часть первой формулы представится в конце концов как сумма величин, имеющих вид правой части последней формулы. Чтобы реализовать эту программу, положим

$$K_s = K_{s-1}' \qquad (s = 1, \ldots, g-1). \tag{34}$$

Тогда требуется только обеспечить выполнение условий

$$\varkappa' < \varkappa_1, \quad \varkappa_1' < \varkappa_2, \quad \ldots, \quad \varkappa_{g-2}' < \varkappa_{g-1}. \tag{35}$$

При первом применении леммы 3 (соответственно леммы 4) возьмем $\varkappa = 1$. Тогда формулой (32) определено значение

$$\varkappa' = \varphi(1),$$

в то время как выбор K пока свободен. Поскольку фигурирующая в леммах функция $F(K, \varkappa)$ при фиксированном $\varkappa$ монотонно стремится вместе с K к бесконечности и в силу (32), (34)

$$K_1 = F(K, \varkappa) = F(K, 1),$$

мы можем выбрать K настолько большим, чтобы было

$$\frac{1}{2}\sqrt{K_1} - 1 > \varkappa' + 1,$$

и это неравенство остается верным, если мы еще увеличим K. Теперь положим

$$\varkappa_1 = \varkappa' + 1$$

и тем самым удовлетворим первое из условий (35) и условие (33) для $s = 1$. После того как выбрано $\varkappa_1$, найдем $\varkappa_1'$ из равенства (см. (32))

$$\varkappa_1' = \varphi_1(\varkappa_1).$$

Поскольку снова функция $F_1(K_1, \varkappa_1)$ при фиксированном $\varkappa_1$ монотонно стремится к бесконечности вместе с K_1, и поскольку, в силу (32) и (34),

$$K_2 = F_1(K_1, \varkappa_1),$$

увеличив еще K, можно добиться, чтобы

$$\frac{1}{2}\sqrt{K_2} - 1 > \varkappa_1' + 1.$$

Это неравенство остается в силе при дальнейшем увеличении K. Теперь положим

$$\varkappa_2 = \varkappa_1' + 1$$

и удовлетворим тем самым второе из условий (35) и условие (33) для $s = 2$. Продолжим таким же образом, пока не придем к равенству

$$\varkappa_{g-1} = \varkappa_{g-2}' + 1.$$

Наконец, еще раз увеличим K, чтобы было выполнено неравенство

$$\sqrt{K_{g-1}'} > \varkappa_{g-1}'.$$

Тогда ввиду (31) для $s = g - 1$

$$|Y_h'^{(g)}| < \varkappa_{g-1}'\sqrt{K_{g-1}'}x,$$

и, следовательно,

$$|Y_h'^{(g)}| < K_{g-1}'x,$$

так что в правой части последней формулы (30) целые числа, возводимые в степень n, будут положительными.

Подставляя теперь левые части формул (30) в правую часть каждой предыдущей формулы, придем к формуле вида

$$x^p(Kx^q + Y) = \sum_{h=1,\ldots,N^*} k_h(K_{g-1}'x + Y_h'^{(g)})^n,$$

где справа стоят

$$N^* = N_1N_2 \ldots N_g$$

слагаемых и k_h являются положительными рациональными числами. Этим наша лемма доказана.

Располагая леммой 5, *мы теперь в состоянии доказать высказанную в начале теорему о представимости целых чисел через n-е степени.*

Пусть x — произвольное положительное целое число $\geqslant 2^n$. Пусть, далее, Y_1, Y_2 — два целых числа, удовлетворяющих неравенствам

$$\left.\begin{aligned} 0 \leqslant Y_1 &< \sqrt{K}x^q, \\ 0 \leqslant Y_2 &< \sqrt{K}(x+1)^q. \end{aligned}\right\} \tag{36}$$

Тогда по лемме 5 выполняются равенства

$$x^p[Kx^q - Y_1] = \sum_{h=1,\ldots,N^*} k_hP_h^n,$$

$$(x+1)^p[K(x+1)^q + Y_2] = \sum_{h=1,\ldots,N^*} k_hQ_h^n,$$

сложение которых дает

$$x^p[Kx^q - Y_1] + (x+1)^p[K(x+1)^q + Y_2] = \sum_{h=1,\ldots,N^*} k_h(P_h^n + Q_h^n), \qquad (37)$$

где P_h и Q_h — целые положительные числа. Левая часть формулы (37) имеет вид

$$K[x^n + (x+1)^n] + Z,$$

где положено

$$Z = (x+1)^p Y_2 - x^p Y_1.$$

Убедимся теперь в том, что выражение

$$(x+1)^p Y_2 - x^p Y_1$$

при подходящем выборе чисел Y_1, Y_2, удовлетворяющих неравенствам (36), может представить любое целое число Z, которое удовлетворяет неравенствам

$$0 \leqslant Z \leqslant x^n.$$

В самом деле, поскольку числа $(x+1)^p$ и x^p взаимно просты, то прежде всего для каждого целочисленного Z диофантово уравнение

$$Z = (x+1)^p Y_2 - x^p Y_1$$

обладает целочисленным решением Y_1, Y_2; но одновременно с Y_1, Y_2 будет решением и

$$Y_1 - T(x+1)^p,$$
$$Y_2 - Tx^p$$

для каждого целочисленного T, а отсюда очевидно, что мы можем взять Y_1 удовлетворяющим неравенствам

$$0 \leqslant Y_1 < (x+1)^p.$$

Поскольку $p < q$, будет выполнено неравенство $(x+1)^p < x^q$, если только выбрать x достаточно большим, например $\geqslant 2^n$; тогда мы имеем

$$0 \leqslant Y_1 < x^q.$$

Принимая во внимание неравенства $Y_1 < (x+1)^p$ и $0 \leqslant Z \leqslant x^n$, получаем далее

$$Y_2 = \frac{x^p Y_1 + Z}{(x+1)^p} < x^p + \frac{x^n}{(x+1)^p} < x^p + x^q.$$

Так как $q > p$ и $Y_2 \geqslant 0$, мы имеем

$$0 \leqslant Y_2 < (x+1)^q.$$

Поскольку $K > 16$, неравенства (36) выполнены.

Резюмируя все предыдущее, мы видим, что каждое целое число U, лежащее в интервале J_x, определяемом неравенствами

$$K[x^n + (x+1)^n] \leqslant U \leqslant K[x^n + (x+1)^n] + x^n,$$

допускает представление в виде

$$\sum_{h=1,\ldots,N^*} k_h(P_h^n + Q_h^n).$$

Начиная с некоторого достаточно большого x, интервалы, отвечающие x и $x+1$, перекрываются — наибольшее число из J_x будет больше, чем наименьшее число из J_{x+1}; в самом деле, очевидно, что

$$K[x^n+(x+1)^n]+x^n > K[(x+1)^n+(x+2)^n],$$

если

$$x > \frac{2\sqrt[n]{K}}{\sqrt[n]{K+1}-\sqrt[n]{K}}.$$

Таким образом, все целые числа U, превосходящие некоторую величину S, допускают представление в виде

$$\sum_{h=1,\ldots,N^*} k_h(P_h^n+Q_h^n),$$

где P_h и Q_h — некоторые положительные целые числа.

Обозначим через E общий знаменатель рациональных чисел k_h. Тогда из этого представления после умножения на E следует, что каждое превосходящее ES и делящееся на E целое число может быть представлено как сумма n-х степеней положительных целых чисел, количество которых не превосходит некоторой границы, зависящей только от n. Следовательно, это верно также для каждого целого числа, делящегося на E, а потому также и для каждого не делящегося на E целого числа, по соображениям, которые были приведены в конце доказательства теоремы II. Тем самым приведенная в начале теорема, высказанная в виде гипотезы Варингом, полностью доказана.

В заключение следует еще отметить, что с помощью вышеуказанного метода в действительности можно найти и верхнюю границу для количества n-х степеней, необходимых для представления произвольного числа; для этого надо принять во внимание сделанное в конце доказательства теоремы II замечание и в только что завершенном доказательстве оценивать все встречающиеся величины так, чтобы искомая граница в конце концов была выражена через n.

АЛГЕБРА

О ПРЕДСТАВЛЕНИИ ОПРЕДЕЛЕННЫХ ФОРМ В ВИДЕ СУММЫ КВАДРАТОВ ФОРМ*)

Алгебраическую форму четного порядка n с вещественными коэффициентами и m однородными переменными назовем *определенной*, если при любом вещественном наборе значений m переменных она принимает положительное значение и, кроме того, ее дискриминант отличен от нуля. Форму с вещественными коэффициентами будем для краткости называть вещественной формой.

Как известно, *каждая определенная квадратичная форма* от m переменных представима в виде суммы m квадратов вещественных линейных форм. Аналогичным образом *каждая определенная бинарная форма* представима в виде суммы двух квадратов вещественных форм, в чем нетрудно убедиться, разлагая форму на соответствующие множители. Так как представление, о котором идет речь, позволяет выявить определенность наиболее простым способом, то интересно исследовать возможность такого представления в общем случае. Что касается ближайшего ранее не рассмотренного случая $n = 4$, $m = 3$, то справедлива теорема:

каждая определенная биквадратичная тернарная форма представима в виде суммы трех квадратов вещественных квадратичных форм.

Для доказательства рассмотрим биквадратичную тернарную форму F, равную сумме квадратов трех квадратичных форм φ, ψ, χ. Если та же форма F представима в виде суммы квадратов трех квадратичных форм $\varphi+\varepsilon\varphi'$, $\psi+\varepsilon\psi'$, $\chi+\varepsilon\chi'$, где ε — бесконечно малая постоянная, то сравнение двух представлений с необходимостью приводит к соотношению

$$\varphi\varphi' + \psi\psi' + \chi\chi' = 0. \tag{1}$$

Три уравнения

$$\varphi = 0, \qquad \psi = 0, \qquad \chi = 0 \tag{2}$$

могут не иметь общей системы решений. В таком случае в силу тождества (1) четыре общих решения двух последних уравнений должны обращать в нуль квадратичную форму φ'; следовательно,

$$\varphi' = \alpha\psi + \gamma\chi$$

и аналогично

$$\psi' = \beta\varphi + \zeta\chi,$$
$$\chi' = \delta\varphi + \theta\psi.$$

---

*) Über die Darstellung definiter Formen als Summe von Formenquadraten. — Math. Ann., 1888, Bd. 32, S. 342–350. *Перевод Ю. А. Данилова.*

Подставляя эти выражения в тождество (1), получаем для введенных постоянных соотношения

$$\alpha+\beta=0, \qquad \gamma+\delta=0, \qquad \zeta+\theta=0.$$

Таким образом, если результант трех уравнений (2) отличен от нуля, то тождеству (1) удовлетворяет только линейная комбинация трех решений

$$\begin{array}{lll} \varphi'=0, & \varphi'=-\chi, & \varphi'=\psi, \\ \psi'=\chi, & \psi'=0, & \psi'=-\varphi, \\ \chi'=-\psi, & \chi'=\varphi, & \chi'=0, \end{array}$$

т. е. существует не более чем трехкратно бесконечное множество форм φ, ψ, χ, позволяющих представить данную форму F в виде суммы их квадратов. Так как система трех квадратичных форм содержит 18 коэффициентов, а биквадратичная форма F — только 15 коэффициентов, то из приведенных выше рассуждений следует, что каждая биквадратичная тернарная форма представима в виде суммы трех квадратов форм[1]).

Коэффициенты представляющих форм φ, ψ, χ содержат, кроме того, три произвольных параметра и поэтому принимают определенное значение лишь после того, как заданы любые три независимых условия. Если такие условия наложены, то существует только конечное число систем форм φ, ψ, χ, позволяющих представить данную биквадратичную форму F в виде суммы их квадратов. Если же из этих систем форм при любом выборе условий возникают две системы форм, то из приведенных выше рассуждений следует, что результант форм φ, ψ, χ, а значит, и дискриминант представляемой формы F равны нулю. Этот замечательный особый случай имеет значение для последующих выводов.

Действительно, пусть F, F', F'' — три определенные биквадратичные тернарные формы, а p, p', p'' — три переменные положительные величины, отношения которых можно представить в виде точки внутри координатного треугольника. Построим все точки p, p', p'', для которых уравнение

$$pF+p'F'+p''F''=0 \tag{3}$$

задает кривую четвертого порядка с двумя или более двойными точками. Как только две положительно определенные формы F и F' заданы, форму F'' всегда можно выбрать так, чтобы число точек p, p', p'' было конечным и мы могли бы соединить две вершины $p=1$, $p'=0$, $p''=0$ и $p=0$, $p'=1$, $p''=0$ кривой, целиком лежащей внутри координатного треугольника и не проходящей ни через одну из ранее построенных точек. Если мы рассмотрим теперь точку p, p', p'' кривой, соединяющей две указанные вершины, то соответствующая биквадратичная кривая (3) не будет иметь двойных точек. Действительно, так как кривая (3) вообще не имеет вещественных точек, то каждая существующая двойная точка этой кривой должна быть точкой с комплексными координатами; комплексно-сопряженная точка была бы второй двойной точкой той же кривой, что находится в очевидном противоречии со сделанными предположениями. Если величины p, p', p'' воспроизводят ход кривой, соединяющей две указанные вершины, то от

---

[1]) Общий принцип, лежащий в основе такого рода представлений, восходит к Л. Кронекеру.

определенной формы F мы путем непрерывного изменения ее вещественных коэффициентов переходим к определенной форме F', не проходя при этом через форму с нулевым дискриминантом. Положим форму F равной сумме квадратов трех вещественных квадратичных форм φ, ψ, χ. При непрерывном изменении вещественных коэффициентов формы F коэффициенты представляющих форм φ, ψ, χ остаются всегда вещественными, если заранее исключить отмеченный выше особый случай. Следовательно, если производить непрерывное изменение формы F в форму F' указанным выше образом, то получим, что последняя форма F' представима в виде суммы трех квадратов вещественных форм, что и требовалось. Тем самым наша теорема доказана.

Однако удовлетворительный ответ на вопрос, поставленный в начале этой работы, удается получить лишь после строгого обоснования следующей теоремы.

Среди определенных форм четного порядка n от m переменных всегда найдутся такие, которые непредставимы в виде суммы квадратов вещественных форм[2]. *Исключение составляют лишь три перечисленных выше случая*:

I. $n = 2$, m *произвольно*;

II. n *произвольно*, $m = 2$;

III. $n = 4$, $m = 3$.

Доказательство проведем сначала для случая тернарных форм 6-го порядка.

Выберем на плоскости восемь попарно несовпадающих точек (1), (2),... ..., (8), из которых никакие три не лежат на одной прямой и никакие шесть не лежат на одном коническом сечении. Через эти восемь точек проведем две вещественные кривые 3-го порядка, задаваемые уравнениями $\varphi = 0$ и $\psi = 0$. Эти две кривые пересекаются в еще одной, девятой, точке (9), которая также вещественна и, вообще говоря, не совпадает ни с одной из восьми ранее выбранных точек. Пусть $f = 0$ — уравнение конического сечения, проходящего через точки (1), (2), (3), (4), (5), а $g = 0$ — уравнение кривой 4-го порядка, также проходящей через точки (1), (2), (3), (4), (5), являющиеся для нее простыми, и, кроме того, через двойные точки (6), (7), (8). Тогда φ, ψ, f, g — тернарные формы с вещественными коэффициентами. Обозначим для краткости через (i) вещественные однородные координаты девяти точек (i) и покажем, что значения $f(9)$ и $g(9)$ отличны от нуля. Действительно, если бы значение $f(9)$ было равно нулю, то, образуя линейную комбинацию уравнений $\varphi = 0$ и $\psi = 0$, можно было бы получить уравнение кривой 3-го порядка, которая помимо шести точек (1), (2), (3), (4), (5), (9) имела бы с коническим сечением $f = 0$ еще одну, седьмую, общую точку. Такая кривая 3-го порядка должна была бы распадаться на коническое сечение и прямую, проходящую через точки (6), (7),

---

[2] На возможность существования таких форм указывал еще Г. Минковский; см. первый тезис его диссертации «Untersuchungen über quadratische Formen» по случаю вступления в должность профессора (Königsberg, 1885), а также работу: *Minkowski H.* — Ges. Abh., 1911, Bd. 1. S. VIII.

(8) (существование прямой следует из наших предположений относительно расположения восьми точек). Если бы значение $g(9)$ было равно нулю, то тем же способом можно было бы построить нераспадающуюся кривую 3-го порядка, проходящую через три двойные точки (6), (7), (8), а также через шесть простых точек (1), (2), (3), (4), (5), (9) и, кроме того, через еще одну произвольную простую точку кривой $g = 0$. Следовательно, кривая $g = 0$ должна была бы распадаться на эту кривую 3-го порядка и на прямую, проходящую через точки (6), (7), (8); это заключение также противоречит исходному предположению. Выбрав знак формы f так, чтобы произведение $f(9)g(9)$ было положительным, рассмотрим тернарную форму 6-го порядка

$$\varphi^2 + \psi^2 + pfg,$$

где p — положительная постоянная. Пусть p_i — наименьшая положительная величина, при которой кривая

$$\varphi^2 + \psi^2 + p_i fg = 0$$

имеет в точке (i) точку возврата или тройную точку. Если такой величины не существует, то будем считать, что $p_i = \infty$. Все величины p_i больше нуля, так как значению $p = 0$ соответствует кривая $\varphi^2 + \psi^2 = 0$, у которой все девять рассматриваемых нами точек — изолированные двойные точки. Если под $[p]$ понимать любую отличную от нуля величину, которая меньше наименьшей из величин p_i, то кривая

$$\varphi^2 + \psi^2 + [p]fg = 0$$

имеет только восемь изолированных двойных точек (1), (2),..., (8) и вообще не проходит через точку (9). Поэтому вокруг каждой из этих девяти точек можно описать малую окружность, обладающую тем свойством, что тернарная форма

$$\varphi^2 + \psi^2 + [p]fg$$

всюду внутри девяти проведенных окружностей положительна за исключением центров первых восьми окружностей, в которых она равна нулю. Так как вне этих девяти окружностей выражение $\varphi^2 + \psi^2$ всегда отлично от нуля, абсолютная величина отношения

$$\frac{\varphi^2 + \psi^2}{fg}$$

в области, лежащей вне этих девяти окружностей, достигает отличного от нуля минимума M. Если теперь под $[[p]]$ понимать отличную от нуля положительную величину, не совпадающую ни с $[p]$, ни с M, то *выражение*

$$F = \varphi^2 + \psi^2 + [[p]]fg \tag{4}$$

представляет собой тернарную форму 6*-го порядка, равную нулю в точках* (1), (2),..., (8), *но отличную от нуля и положительную при всех других вещественных наборах переменных.*

Пусть P — любая определенная тернарная форма 6-го порядка и p — снова отличная от нуля положительная величина; тогда форма $F+pP$ также

является определенной и представима в виде суммы 28 или меньшего числа квадратов форм:

$$F + pP = \rho^2 + \sigma^2 + \ldots + \tau^2, \tag{5}$$

где ρ, $\sigma, \ldots,$ τ — вещественные тернарные кубические формы, число которых не превосходит 28. Если подставить в тождество (5) координаты точки (9), то для одной из этих кубических форм, например, для формы ρ, выполняется неравенство

$$|\rho(9)| > \left|\sqrt{\frac{F(9)}{28}}\right|. \tag{6}$$

С другой стороны, из того же тождества (5) следуют восемь неравенств

$$\begin{aligned} \rho(1) &\leqslant \left|\sqrt{pP(1)}\right|, \\ \rho(2) &\leqslant \left|\sqrt{pP(2)}\right|, \\ &\ldots\ldots\ldots \\ \rho(8) &\leqslant \left|\sqrt{pP(8)}\right|. \end{aligned} \tag{7}$$

Так как рассматриваемые нами девять точек образуют полную систему точек пересечения двух кривых 3-го порядка, справедливо соотношение вида

$$c_1\rho(1) + c_2\rho(2) + \ldots + c_8\rho(8) + c_9\rho(9) = 0; \tag{8}$$

при этом величины c_1, $c_2, \ldots,$ c_8, c_9 не зависят от коэффициентов кубической формы ρ и, кроме того, все без исключения отличны от нуля. Из равенства (8) следует, что

$$|c_1\rho(1)| + |c_2\rho(2)| + \ldots + |c_8\rho(8)| \geqslant |c_9\rho(9)|,$$

и с учетом неравенств (6) и (7) мы получаем

$$\left|c_1\sqrt{pP(1)}\right| + \left|c_2\sqrt{pP(2)}\right| + \ldots + \left|c_8\sqrt{pP(8)}\right| > \left|c_9\sqrt{\frac{F(9)}{28}}\right|.$$

Выбирая в качестве p величину $\{p\}$, которая отлична от нуля, положительна и меньше отношения

$$\frac{c_9^2 F(9)}{28\left\{\left|c_1\sqrt{P(1)}\right| + \left|c_2\sqrt{P(2)}\right| + \ldots + \left|c_8\sqrt{P(8)}\right|\right\}^2},$$

мы убеждаемся, что наше предположение (5) в конечном счете приводит к противоречию, т. е. *определенная тернарная форма* $F + \{p\}P$ *6-го порядка непредставима в виде суммы* 28 *или меньшего числа квадратов вещественных форм.*

Если предположить, что форма $F + \{p\}P$ представима в виде суммы 29 квадратов вещественных форм, то и в этом случае между представляющими формами возникло бы линейное соотношение с постоянными положительными и отрицательными коэффициентами. Пусть γ — значение, принимаемое наибольшим положительным коэффициентом. Если соотношение, о котором идет речь, разделить на γ и вычесть из суммы 29 квадратов форм, то форма $F + \{p\}P$ окажется представленной в виде суммы 28 квадратов

форм, взятых со знаком плюс. Аналогичным образом предположение о представимости в виде суммы более чем 29 квадратов форм сводится в конечном счете к представлению в виде суммы 28 квадратов форм, т. е. *тернарная форма $F + \{p\}P$ 6-го порядка вообще непредставима в виде суммы квадратов вещественных форм.*

Убедимся в справедливости нашей теоремы для тернарных форм произвольного четного порядка n; пусть $f = 0$ — уравнение произвольной вещественной кривой порядка $n/2 - 3$, проходящей через девять точек (1), (2), ..., (8), (9). Выберем на этой кривой столько вещественных точек (10), (11), ..., чтобы каждая кривая порядка $n/2$, проходящая через все эти точки, распадалась на кривую $f = 0$ и кубическую кривую, но этого не происходило бы, если из набора точек (10), (11), ... выкинуть хотя бы одну точку. Из этого предположения и расположения девяти точек (1), (2), ..., (8), (9) следует, что выполняется соотношение вида

$$c_1\rho(1) + c_2\rho(2) + \ldots + c_8\rho(8) + c_9\rho(9) + c_{10}\rho(10) + c_{11}\rho(11) + \ldots = 0,$$

где ρ — произвольная тернарная форма порядка $n/2$. Коэффициенты c_1, $c_2, \ldots, c_8, c_9, c_{10}, c_{11}, \ldots$ не зависят от коэффициентов формы ρ, а коэффициенты $c_1, c_2, \ldots, c_8, c_9$, кроме того, отличны от нуля. Если P — определенная тернарная форма порядка n, то, рассуждая, как прежде, мы докажем, что *тернарная форма $Ff^2 + pP$ при достаточно малом положительном p непредставима в виде суммы $\frac{1}{2}(n+1)(n+2)$ квадратов вещественных форм и, следовательно, вообще непредставима в виде конечной суммы квадратов вещественных форм.*

Наконец, что касается форм с более чем тремя переменными, то прежде всего необходимо исследовать кватернарную биквадратичную форму.

Для этого выберем в трехмерном пространстве семь попарно несовпадающих точек (1), (2), ..., (7), никакие четыре из которых не лежат в одной плоскости. Кроме того, позаботимся о том, чтобы вершина любого конуса 2-го порядка, проходящего через любые шесть из выбранных нами точек, не совпала с седьмой точкой. Проведем через наши семь точек три вещественные квадратичные поверхности $\varphi = 0$, $\psi = 0$ и $\chi = 0$, которые помимо этого пересекаются в еще одной восьмой точке (8). Эта точка (8) также вещественна и не совпадает ни с одной из семи ранее выбранных точек. Пусть $f = 0$ — уравнение плоскости, проходящей через точки (1), (2), (3), а $g = 0$ — уравнение поверхности 3-го порядка, проходящей через точки (1), (2), (3), (4), (5), (6) и (7), причем точки (1), (2), (3) являются ее простыми точками, а точки (4), (5), (6), (7) — узловыми (Knotenpunkte). Обозначим для краткости через (i) вещественные однородные координаты восьми точек (i). Нетрудно видеть, что значение $f(8)$ отлично от нуля. То же самое относится и к $g(8)$. Действительно, если бы поверхность $g = 0$ также проходила через точку (8), то g можно было бы представить в виде

$$r\varphi + s\psi + t\chi,$$

где r, s, t — линейные формы. Определение поверхности $g = 0$ требует, чтобы в каждой из точек (4), (5), (6), (7) первые производные формы g по

каждой из четырех однородных переменных, т. е. выражения

$$r\frac{\partial\varphi}{\partial x_1}+s\frac{\partial\psi}{\partial x_1}+t\frac{\partial\chi}{\partial x_1},\qquad r\frac{\partial\varphi}{\partial x_3}+s\frac{\partial\psi}{\partial x_3}+t\frac{\partial\chi}{\partial x_3},$$
$$r\frac{\partial\varphi}{\partial x_2}+s\frac{\partial\psi}{\partial x_2}+t\frac{\partial\chi}{\partial x_2},\qquad r\frac{\partial\varphi}{\partial x_4}+s\frac{\partial\psi}{\partial x_4}+t\frac{\partial\chi}{\partial x_4},$$

обращались в нуль, а поскольку ни одна из линейных форм r, s, t не может обращаться в нуль во всех четырех точках (4), (5), (6), (7), мы заключаем, что по крайней мере в одной из этих четырех точек трехрядные определители матрицы

$$\begin{pmatrix} \frac{\partial\varphi}{\partial x_1} & \frac{\partial\psi}{\partial x_1} & \frac{\partial\chi}{\partial x_1} \\ \frac{\partial\varphi}{\partial x_2} & \frac{\partial\psi}{\partial x_2} & \frac{\partial\chi}{\partial x_2} \\ \frac{\partial\varphi}{\partial x_3} & \frac{\partial\psi}{\partial x_3} & \frac{\partial\chi}{\partial x_3} \\ \frac{\partial\varphi}{\partial x_4} & \frac{\partial\psi}{\partial x_4} & \frac{\partial\chi}{\partial x_4} \end{pmatrix}$$

обращаются в нуль. В последнем случае мы могли бы построить из одной из этих четырех точек конус 2-го порядка, проходящий через все остальные семь точек. Такое заключение противоречит доказанному ранее. Выбрав знак формы f так, чтобы произведение $f(8)g(8)$ было положительным, мы можем применить аналогичные рассуждения к тернарной форме 6-го порядка. Оказывается, *выражение*

$$F=\varphi^2+\psi^2+\chi^2+pfg$$

при достаточно малом положительном p задает форму, которая обращается в нуль в точках (1), (2),..., (7), *а при всех остальных вещественных наборах значений переменных отлична от нуля и положительна.*

Так как восемь точек, о которых идет речь, образуют полную систему точек пересечений трех поверхностей 2-го порядка, справедливо линейное тождество вида

$$c_1\rho(1)+c_2\rho(2)+\ldots+c_7\rho(7)+c_8\rho(8)=0,$$

где ρ — произвольная кватернарная квадратичная форма, а постоянные c_1, $c_2,\ldots,c_7$, c_8 зависят только от координат наших восьми точек. Пусть P — определенная кватернарная биквадратичная форма, а $\{p\}$ — величина, которая отлична от нуля, положительна и меньше отношения

$$\frac{c_8^2F(8)}{35\left\{\left|c_1\sqrt{P(1)}\right|+\left|c_2\sqrt{P(2)}\right|+\ldots+\left|c_7\sqrt{P(7)}\right|\right\}^2}.$$

Если предположить, что форма $F+\{p\}P$ представима в виде суммы 35 или меньшего числа вещественных форм, то мы снова придем к противоречию, хотя на этот раз речь идет о тернарной форме 6-го порядка. Таким образом, *определенная кватернарная биквадратичная форма* $F+\{p\}P$

непредставима в виде суммы 35 *или меньшего числа квадратов вещественных форм и, следовательно, вообще непредставима в виде суммы конечного числа квадратов вещественных форм.*

Пусть Φ — определенная тернарная форма 6-го порядка и Ψ — определенная кватернарная биквадратичная форма. Пусть ни Φ, ни Ψ не представимы в виде суммы квадратов вещественных форм. Тогда если n и m больше или равны четырем, то можно без труда построить определенную форму n-го порядка от m переменных, проходящую через нули по одной или нескольким переменным одной из форм Φ или Ψ. *Такая форма непредставима в виде суммы квадратов вещественных форм так же, как и сами формы* Φ *и* Ψ.

Тем самым правильность нашей теоремы полностью доказана.

Кёнигсберг в Пруссии, 20 февраля 1888 г.

О ТЕРНАРНЫХ ОПРЕДЕЛЕННЫХ ФОРМАХ*)

Целую рациональную однородную функцию f трех переменных x, y, z, порядок n которой является четным числом, а $N = \frac{1}{2}(n+1)(n+2)$ коэффициентов — вещественными числами, можно назвать тернарной определенной формой, если при вещественных значениях переменных x, y, z она всегда принимает положительные значения или обращается в нуль. Если существует вещественный отличный от $x = y = z = 0$ набор значений переменных, при котором определенная форма f обращается в нуль, то, как нетрудно показать, дискриминант формы f равен нулю.

Из приведенного выше определения непосредственно видно, что при сложении и умножении определенных форм всегда получаются формы, которые также являются определенными, т. е. совокупность всех определенных форм образует область форм, обладающую тем свойством, что каждая форма, получаемая с помощью сложения и умножения из форм этой области, также принадлежит этой области. Кроме того, каждый квадрат произвольной формы с вещественными коэффициентами есть определенная форма, и поэтому, складывая и умножая квадраты форм, мы всегда получаем определенные формы. Однако в своей работе «О представлении определенных форм в виде суммы квадратов форм»[1)] я показал, что не каждая определенная форма представима указанным образом в виде суммы квадратов форм. Доказанная мной в этой работе теорема гласит следующее:

Каждая тернарная квадратичная или биквадратичная определенная форма представима в виде суммы трех квадратов вещественных форм; среди определенных форм 6-го или более высокого порядка всегда найдутся такие, которые непредставимы в виде конечной суммы квадратов вещественных форм.

Чтобы получить представление, пригодное для всех определенных форм, необходимо прежде всего учесть, что всякий раз, когда один из множителей, на которые разлагается определенная форма, является определенным, дополнительный к нему множитель также должен быть определенным; поэтому определенный характер формы распознаваем и в том случае, когда форма представима в виде дроби, в числителе и знаменателе которой стоят суммы квадратов форм. Как будет показано ниже, *такое представление всегда возможно.* Доказательство этого утверждения сопряжено с большими трудностями; чтобы сделать его более удобообозримым, я разбиваю его на девять частей и в начале каждой части указываю цель, которой хочу достигнуть, а в конце — полученные в ней результаты.

---

*) Über ternäre definite Formen. — Acta. Math., 1893, Bd. 17, S. 169–197. *Перевод Ю. А. Данилова.*

1) Math. Ann., 1888, Bd. 32, S. 342–350 [имеется перевод на с. 331–338 настоящего издания. — *Ред.*].

1. Чтобы доказать существование определенных форм, особые свойства которых будут подробно изложены ниже, воспользуемся следующей леммой

Пусть тернарная форма F n-го порядка с вещественными коэффициентами обладает тем свойством, что кривая $F = 0$ имеет δ двойных точек $P_1, \ldots, P_\delta$ с несовпадающими касательными и, помимо них, какие-то другие двойные точки; пусть F' — форма того же порядка n с вещественными коэффициентами, обращающаяся в нуль в точках $P_1, \ldots, P_\delta$, но принимающая отличные от нуля значения во всех остальных двойных точках кривой $F = 0$; наконец, пусть на плоскости можно задать $N - \delta$ точек так, чтобы через них и через δ точек $P_1, \ldots, P_\delta$ нельзя было провести кривую n-го порядка. При этих предположениях всегда существует кривая $G = 0$ порядка n с коэффициентами, сколь угодно мало отличающимися от коэффициентов формы F, причем такая, что в произвольно малых окрестностях точек $P_1, \ldots, P_\delta$ эта кривая имеет обычную двойную точку с несовпадающими касательными, но не обладает более ни одной особой точкой.

Для простоты будем считать в дальнейшем третью координату z равной единице; пусть координаты δ точек $P_1, \ldots, P_\delta$ равны соответственно

$$\begin{aligned} x &= a_1, \quad \ldots, \quad x = a_\delta, \\ y &= b_1, \quad \ldots, \quad y = b_\delta. \end{aligned}$$

Предположим, что форма G, которую требуется найти, имеет вид

$$G = F + t\,(F' + \Omega),$$

где t — переменная, а Ω — форма n-го порядка; N коэффициентов $u_1, \ldots, u_N$ формы Ω мы зададим как функции от t таким образом, чтобы G при сколь угодно малых значениях t удовлетворяла условиям приведенной выше леммы. Для этого введем следующие выражения:

$$\left.\begin{aligned} \alpha_s &= a_s + t\,(A_s + \xi_s), \\ \beta_s &= b_s + t\,(B_s + \eta_s) \end{aligned}\right\} \qquad (s = 1, \ldots, \delta),$$

где ξ_s, η_s — пока неизвестные функции и

$$A_s = \left[\frac{\dfrac{\partial F'}{\partial y}\dfrac{\partial^2 F}{\partial x \partial y} - \dfrac{\partial F'}{\partial x}\dfrac{\partial^2 F}{\partial y^2}}{\dfrac{\partial^2 F}{\partial x^2}\dfrac{\partial^2 F}{\partial y^2} - \left(\dfrac{\partial^2 F}{\partial x \partial y}\right)^2}\right]_{\substack{x=a_s,\\ y=b_s}}, \qquad B_s = \left[\frac{\dfrac{\partial F'}{\partial x}\dfrac{\partial^2 F}{\partial x \partial y} - \dfrac{\partial F'}{\partial y}\dfrac{\partial^2 F}{\partial x^2}}{\dfrac{\partial^2 F}{\partial x^2}\dfrac{\partial^2 F}{\partial y^2} - \left(\dfrac{\partial^2 F}{\partial x \partial y}\right)^2}\right]_{\substack{x=a_s,\\ y=b_s}}.$$

Рассмотрим 3δ уравнений

$$\left.\begin{aligned} &G(\alpha_s, \beta_s) = 0, \\ &\frac{\partial G}{\partial x}(\alpha_s, \beta_s) = 0, \\ &\frac{\partial G}{\partial y}(\alpha_s, \beta_s) = 0 \end{aligned}\right\} \qquad (s = 1, \ldots, \delta).$$

Так как

$$\left.\begin{aligned} &F(a_s,b_s)=0, \quad \frac{\partial F}{\partial x}(a_s,b_s)=0, \quad \frac{\partial F}{\partial y}(a_s,b_s)=0,\\ &F'(a_s,b_s)=0 \end{aligned}\right\} \qquad (s=1,\ldots,\delta),$$

эти уравнения после отбрасывания множителя t в левых частях принимают вид

$$\Omega(a_s,b_s)+t\Gamma_1+t^2\Gamma_2+\ldots=0,$$

$$\frac{\partial\Omega}{\partial x}(a_s,b_s)+\xi_s\frac{\partial^2F}{\partial x^2}(a_s,b_s)+\eta_s\frac{\partial^2F}{\partial x\partial y}(a_s,b_s)+t\Gamma_t'+\ldots=0,$$

$$\frac{\partial\Omega}{\partial y}(a_s,b_s)+\xi_s\frac{\partial^2F}{\partial x\partial y}(a_s,b_s)+\eta_s\frac{\partial^2F}{\partial y^2}(a_s,b_s)+t\Gamma_t''+\ldots=0,$$

$$(s=1,2,\ldots,\delta),$$

где $\Gamma_1,\Gamma_2,\ldots,\Gamma_1',\ldots,\Gamma_1'',\ldots$ — целые рациональные выражения от $u_1,\ldots,u_N$; ξ_s,η_s.

Как известно, справедлива следующая теорема[2]):

Если заданы m уравнений вида

$$a_{11}x_1+\ldots+a_{1m}x_m+t\mathfrak{P}_{11}(x_1,\ldots,x_m)+t^2\mathfrak{P}_{12}(x_1,\ldots,x_m)+\ldots=0,$$

. . . . . .

$$a_{m1}x_1+\ldots+a_{mm}x_m+t\mathfrak{P}_{m1}(x_1,\ldots,x_m)+t^2\mathfrak{P}_{m2}(x_1,\ldots,x_m)+\ldots=0,$$

где в левых частях стоят степенные ряды от $m+1$ переменных $x_1,\ldots,x_m,t$, а определитель коэффициентов $a_{11},a_{12},\ldots,a_{mm}$ отличен от нуля, то для величин $x_1,\ldots,x_m$ можно найти однозначно определенные ряды по целым степеням переменной t, тождественно при всех значениях t удовлетворяющие приведенным выше m уравнениям.

Согласно предположению доказываемой леммы, на плоскости существует $N-\delta$ точек $P_{\delta+1},\ldots,P_N$, таких, что через N точек $P_1,\ldots,P_N$ невозможно провести ни одну кривую n-го порядка. Обозначим координаты таких $N-\delta$ точек соответственно через

$$x=a_{\delta+1}, \quad \ldots, \quad x=a_N,$$
$$y=b_{\delta+1}, \quad \ldots, \quad y=b_N.$$

К выписанным выше 3δ уравнениям присоединим $N-\delta$ уравнений

$$\Omega(a_s,b_s)=0 \qquad (s=\delta+1,\ldots,N)$$

и в получившейся системе $N+2\delta$ уравнений будем считать величину t независимой переменной, а $N+2\delta$ величин $u_1,\ldots,u_N;\ \xi_1,\eta_1;\ \xi_2,\eta_2;\ \ldots;\ \xi_\delta,\eta_\delta$ — неизвестными функциями от t. К этой системе уравнений применима сформулированная выше теорема, так как $N+2\delta$ уравнений имеют требуемый

---

[2]) *Königsberger L.* Theorie der Differentialgleichungen mit einer unabhängigen Variabeln. — Leipzig, 1889, S. 43.

вид и определитель коэффициентов при $u_1, \ldots, u_N$; ξ_1, η_1; ξ_2, η_2; $\ldots$; ξ_δ, η_δ принимает значение

$$\prod_{s=1,2,\ldots,\delta} \left[\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)\right]_{\substack{x=a_s \\ y=b_s}} \begin{vmatrix} a_1^n & a_1^{n-1}b_1 & a_1^{n-1} & \ldots & 1 \\ a_2^n & a_2^{n-1}b_2 & a_2^{n-1} & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_N^n & a_N^{n-1}b_N & a_N^{n-1} & \ldots & 1 \end{vmatrix}.$$

Все δ сомножителей произведения $\prod$ отличны от нуля, так как по предположению точки $P_1, \ldots, P_\delta$ для кривой $F = 0$ являются обычными двойными точками с несовпадающими касательными, а N-рядный определитель в силу сделанного выше предположения о точках $P_1, \ldots, P_N$ также отличен от нуля.

Тем самым коэффициенты формы Ω определены как функции переменной t, и остается лишь показать, что при достаточно малых значениях t кривая $G = 0$ не имеет других особых точек, кроме δ двойных точек α_1, $\beta_1; \ldots;$ α_δ, β_δ. Доказать это можно следующим образом. Координаты особых точек кривой $G = 0$ определяются из уравнений

$$G = 0, \quad \frac{\partial G}{\partial x} = 0, \quad \frac{\partial G}{\partial y} = 0$$

и поэтому, как нетрудно убедиться путем исключения, являются алгебраическими функциями от t. Следовательно, эти три уравнения при произвольном значении t помимо δ решений α_1, $\beta_1; \ldots;$ α_δ, β_δ имеют еще одно общее решение, которое должно разлагаться в ряды

$$x = a_0 + a_1 t^{\nu_1} + a_2 t^{\nu_2} + \ldots,$$
$$y = b_0 + b_1 t^{\mu_1} + b_2 t^{\mu_2} + \ldots,$$

где показатели $\nu_1, \nu_2, \ldots, \mu_1, \mu_2, \ldots$ — положительные рациональные числа и a_1, b_1 по предположению отличны от нуля. При $t = 0$ точка $x = a_0$, $y = b_0$ — особая точка кривой $F = 0$. По предположению леммы форма F' принимает в особых точках кривой $F = 0$ значения, отличные от нуля. Пусть $F'(a_0, b_0) = a$. Если начало системы координат поместить в точку $x = a_0$, $y = b_0$, то три выписанных выше уравнения принимают вид

$$xy + \ldots + t\,(a + a'x + a''y + \ldots) + \ldots = 0,$$
$$y + \ldots + t\,(a' + \quad \ldots \quad) + \ldots = 0,$$
$$x + \ldots + t\,(a'' + \quad \ldots \quad) + \ldots = 0,$$

и, как нетрудно убедиться, ряды

$$x = a_1 t^{\nu_1} + \ldots, \quad y = b_1 t^{\mu_1} + \ldots$$

не могут удовлетворять этим уравнениям тождественно при всех значениях t. Тем самым доказательство нашей леммы полностью завершено.

Доказанная лемма допускает обобщение в различных направлениях; кроме того, я хотел бы подчеркнуть, что она оказывается весьма полезной в теории алгебраических кривых и поверхностей для выяснения вопросов существования.

2. В этой части я построю тернарную определенную неприводимую форму G, такую, что уравнение $G = 0$ задает кривую с $\frac{1}{2}(n-1)(n-2)$ различными двойными точками, одна часть которых — вещественные изолированные точки, а другая — попарно комплексно-сопряженные точки.

Для этого предположим, что нами уже построена тернарная определенная неприводимая форма Γ порядка $n-2$ и что уравнение $\Gamma = 0$ задает кривую с $\frac{1}{2}(n-3)(n-4)$ различными двойными точками; пусть l и l' — две линейные формы с вещественными коэффициентами, такие, что комплексная прямая $l + il' = 0$ пересекает кривую $\Gamma = 0$ в $n-2$ попарно различных комплексных точках $Q_1, \ldots, Q_{n-2}$. Тогда комплексно-сопряженная прямая $l - il' = 0$ пересекает кривую $\Gamma = 0$ в $n-2$ комплексно-сопряженных с ними точках $Q'_1, \ldots, Q'_{n-2}$; последние попарно различны и не совпадают с точками $Q_1, \ldots, Q_{n-2}$. Выберем на $\Gamma = 0$ любые $3(n-2)$ попарно комплексно-сопряженных точек $R_1, \ldots, R_{3(n-2)}$ и две комплексные точки S_1, S_2 на прямой $l + il' = 0$; комплексно-сопряженные с ними точки S'_1, S'_2 лежат на прямой $l - il' = 0$. Наконец, пусть P — любая вещественная точка плоскости, не лежащая на кривой $\Gamma = 0$ и прямых $l + il' = 0$, $l - il' = 0$. Построим теперь форму F' порядка n, которая обращается в нуль в $\frac{1}{2}(n-3)(n-4)$ двойных точках кривой $\Gamma = 0$, в точках $Q_1, \ldots, Q_{n-3}, Q'_1, \ldots, Q'_{n-3}, R_1, \ldots, R_{3(n-2)}, S_1, S_2, S'_1, S'_2$, в точке P и в точке пересечения двух прямых $l = 0$, $l' = 0$. Такая форма всегда существует, так как общее число заданных точек равно $\frac{1}{2}n(n+3)$. Форма F' принимает в двух точках Q_{n-2}, Q'_{n-2} значения, отличные от нуля, так как в противном случае кривая $F' = 0$ имела бы с кривой $\Gamma = 0$ более $n(n-2)$, а с прямыми $l + il' = 0$, $l - il' = 0$ — более n общих точек и, следовательно, форма F' должна была бы совпадать с формой $F = (l^2 + l'^2)\Gamma$ с точностью до постоянного множителя. Но это невозможно, так как форма F принимает в точке P значение, отличное от нуля, тогда как форма F' в точке P обращается в нуль.

Применим теперь доказанную в части 1 лемму к кривой $F = 0$. Эта кривая имеет обычные двойные точки с несовпадающими касательными в $\frac{1}{2}(n-3)(n-4)$ двойных точках кривой $\Gamma = 0$, в точках $Q_1, \ldots, Q_{n-2}, Q'_1, \ldots, Q'_{n-2}$ и, кроме того, в точке $l = 0$, $l' = 0$. Во всех этих точках за исключением точек Q_{n-2}, Q'_{n-2} форма F' обращается в нуль. Следовательно, по нашей лемме существует кривая $G = 0$ порядка n, имеющая обычные двойные точки с несовпадающими касательными в окрестности двойных точек кривой $\Gamma = 0$, точек $Q_1, \ldots, Q_{n-3}, Q'_1, \ldots, Q'_{n-3}$ и точки $l = 0$, $l' = 0$, но не имеющая других двойных точек. Таким образом, число двойных точек в точности равно $\frac{1}{2}(n-1)(n-2)$.

Форма G при достаточно малых значениях параметра t является определенной формой. Действительно, если бы кривая $G = 0$ имела вещественную ветвь, то при $t = 0$ эта ветвь должна была бы стянуться в вещественную изолированную двойную точку кривой $F = 0$. С другой стороны, для каждой окрестности такой двойной точки можно найти такое отличное от нуля значение t, что соответствующая ему форма G в этой окрестности положительна или обращается в нуль. В этом нетрудно убедиться, если поместить начало системы координат в варьируемую двойную точку.

Тот факт, что полученная форма G при произвольных значениях t, заключенных в определенных пределах, неприводима, можно установить следующим образом. Предположим, что величина y задана уравнением $G = 0$ как алгебраическая функция от x и над плоскостью x построена соответствующая этой функции риманова поверхность. При $t = 0$ эта риманова поверхность распадается на три отдельные части, соответствующие уравнениям $\Gamma = 0$, $l+il' = 0$, $l-il' = 0$: первая часть, соответствующая уравнению $\Gamma = 0$, образует $(n-2)$-кратное накрытие комплексной плоскости x и связна, поскольку это уравнение неприводимо; каждая из двух остальных частей образует однократное накрытие плоскости x. При возрастании параметра t от нуля происходит разрешение двойных точек Q_{n-2}, Q'_{n-2}, в результате чего две последние части обретают те две точки ветвления, которые скрепляют их с первой частью в единую связную риманову поверхность. Тем самым наше утверждение доказано.

Мы построили неприводимую определенную форму G, такую, что уравнение $G = 0$ задает кривую с $\frac{1}{2}(n-1)(n-2)$ обычными различными двойными точками.

3. В этой части мы хотим представить только что построенную форму G в виде дроби, в числителе которой стоит сумма трех квадратов форм.

Для этого на кривой $G = 0$ выберем $n-4$ любых различных и попарно комплексно-сопряженных точек $A_1, \ldots, A_{n-4}$ и образуем три линейно независимые формы ρ, σ, $\varkappa$ порядка $n-2$ с вещественными коэффициентами, обращающиеся в нуль в $\frac{1}{2}(n-1)(n-2)$ двойных точках и в $n-4$ точках $A_1, \ldots, A_{n-4}$. Это всегда возможно, так как число наложенных условий ровно на три меньше, чем число коэффициентов формы $(n-2)$-го порядка. Если теперь мы преобразуем кривую $G(x, y, z) = 0$ по формулам

$$\xi : \eta : \zeta = \rho(x, y, z) : \sigma(x, y, z) : \varkappa(x, y, z),$$

то получим уравнение вида $g(\xi, \eta, \zeta) = 0$. Здесь g — неприводимая квадратичная форма от ξ, η, ζ, так как среди $n(n-2)$ точек пересечения двух кривых $G = 0$ и $u\rho + v\sigma + w\varkappa = 0$ имеются лишь две переменные точки с неопределенными параметрами u, v, w. Обращая преобразование, мы получаем формулы вида

$$x : y : z = r(\xi, \eta, \zeta) : s(\xi, \eta, \zeta) : k(\xi, \eta, \zeta),$$

где r, s, k — формы от переменных ξ, η, ζ с вещественными коэффициентами. Отсюда следует, что g — определенная форма; действительно, если бы $g(\xi, \eta, \zeta) = 0$ было бы уравнением вещественного конического сечения, то при вычислении форм r, s, k возникало бы бесконечно много вещественных наборов значений x, y, z, при которых G обращается в нуль. Из этого мы заключаем, что форма g представима в виде

$$g(\xi, \eta, \zeta) = (c_1\xi + d_1\eta + e_1\zeta)^2 + (c_2\xi + d_2\eta + e_2\zeta)^2 + (c_3\xi + d_3\eta + e_3\zeta)^2,$$

где c, d, e — вещественные числа, определитель которых отличен от нуля.

Если в форму g вместо переменных ξ, η, ζ подставить формы ρ, σ, $\varkappa$, то получится форма $(2n-4)$-го порядка по x, y, z, содержащая форму G в качестве множителя. Положим

$$g(\rho, \sigma, \varkappa) = h(x, y, z)G(x, y, z),$$

где h — определенная форма $(n-4)$-го порядка по x, y, z.

Девять вещественных постоянных c, d, e до некоторой степени произвольны: три постоянные c_1, d_1, e_1 необходимо выбрать так, чтобы кривая $(n-2)$-го порядка $c_1\rho + d_1\sigma + e_1\varkappa = 0$ пересекала кривую $G = 0$ в $\frac{1}{2}(n-1)(n-2)$ уже упоминавшихся двойных точках, $n-4$ выбранных нами точках $A_1, \ldots, A_{n-4}$ и, кроме того, еще в двух точках A и B, не совпадающих между собой и с только что указанными точками.

Полагая для краткости

$$c_1\rho + d_1\sigma + e_1\varkappa = \mathrm{P}(x, y, z),$$

$$c_2\rho + d_2\sigma + e_2\varkappa = \Sigma(x, y, z),$$

$$c_3\rho + d_3\sigma + e_3\varkappa = \mathrm{K}(x, y, z),$$

получаем

$$hG = \mathrm{P}^2 + \Sigma^2 + \mathrm{K}^2.$$

Из этой формулы непосредственно видно, что форма h обращается в нуль в $n-4$ точках $A_1, \ldots, A_{n-4}$; кроме того, для дальнейшего существенно, что h не обращается в нуль в двойных точках кривой $G = 0$. Чтобы доказать это, предположим противное и поместим начало системы координат в ту двойную точку, в которой $h = 0$. Рассматриваемые формы должны иметь вид

$$\begin{aligned}
h &= h_1x + h_2y + \ldots,\\
G &= G_{11}x^2 + 2G_{12}xy + G_{22}y^2 + \ldots,\\
\mathrm{P} &= \mathrm{P}_1x + \mathrm{P}_2y + \ldots,\\
\Sigma &= \Sigma_1x + \Sigma_2y + \ldots,\\
\mathrm{K} &= \mathrm{K}_1x + \mathrm{K}_2y + \ldots,
\end{aligned}$$

где выписаны члены только самого низкого порядка по x, y. Нетрудно видеть, что из приведенного выше тождества следует новое тождество

$$(\mathrm{P}_1x + \mathrm{P}_2y)^2 + (\Sigma_1x + \Sigma_2y)^2 + (\mathrm{K}_1x + \mathrm{K}_2y)^2 = 0,$$

из которого в свою очередь мы заключаем, что три линейные формы

$$\mathrm{P}_1x + \mathrm{P}_2y, \quad \Sigma_1x + \Sigma_2y, \quad \mathrm{K}_1x + \mathrm{K}_2y$$

либо тождественно равны нулю, либо отличаются одна от другой только постоянным множителем. И в том, и в другом случае из форм P, Σ, K можно составить две линейные комбинации Π_1, Π_2, не содержащие членов первого порядка по x, y. Выберем на $G = 0$ произвольную точку P и определим постоянные λ_1, λ_2 так, чтобы форма $\Pi = \lambda_1\Pi_1 + \lambda_2\Pi_2$ обращалась в нуль в точке P. Тогда кривая $\Pi = 0$ имеет двойную точку в начале системы координат и, кроме того, проходит через остальные двойные точки кривой $G = 0$ и через точки $A_1, \ldots, A_{n-4}$, P; таким образом, она пересекает кривую $G = 0$ более чем в $n(n-2)$ точках, что невозможно. Следовательно, предположение, в силу которого форма h обращается в нуль в перечисленных выше двойных точках, недопустимо.

В этой части мы показали, что построенная в части 2 форма G представима в виде

$$G = \frac{\mathrm{P}^2 + \Sigma^2 + \mathrm{K}^2}{h},$$

где P, Σ, K — формы $(n-2)$-го порядка с вещественными коэффициентами, которые обращаются в нуль в $\frac{1}{2}(n-1)(n-2)$ двойных точках и в $n-4$ попарно комплексно-сопряженных точках $A_1, \ldots, A_{n-4}$ кривой $G=0$. Кроме того, h — форма $(n-4)$-го порядка, отличная от нуля в указанных $\frac{1}{2}(n-1)(n-2)$ двойных точках и обращающаяся в нуль в $n-4$ точках $A_1, \ldots, A_{n-4}$. Кривая $\mathrm{P}=0$ пересекает кривую $G=0$ еще в двух комплексно-сопряженных точках A, B, в которых форму h можно считать отличной от нуля.

4. Форма G есть форма с нулевым дискриминантом. Построим теперь с помощью формы G форму f с отличным от нуля дискриминантом, допускающую такое же представление, как форма G.

Из соображений, приведенных в конце предыдущей части, следует, что в двойной точке кривой $G=0$ не все из трех определителей

$$\begin{vmatrix} \frac{\partial \mathrm{P}}{\partial x} & \frac{\partial \mathrm{P}}{\partial y} \\ \frac{\partial \Sigma}{\partial x} & \frac{\partial \Sigma}{\partial y} \end{vmatrix}, \quad \begin{vmatrix} \frac{\partial \mathrm{P}}{\partial x} & \frac{\partial \mathrm{P}}{\partial y} \\ \frac{\partial \mathrm{K}}{\partial x} & \frac{\partial \mathrm{K}}{\partial y} \end{vmatrix}, \quad \begin{vmatrix} \frac{\partial \Sigma}{\partial x} & \frac{\partial \Sigma}{\partial y} \\ \frac{\partial \mathrm{K}}{\partial x} & \frac{\partial \mathrm{K}}{\partial y} \end{vmatrix}$$

равны нулю; это позволяет определить три квадратичные формы p, q, m так, чтобы определитель

$$\begin{vmatrix} \frac{\partial \mathrm{P}}{\partial x} & \frac{\partial \mathrm{P}}{\partial y} & p \\ \frac{\partial \Sigma}{\partial x} & \frac{\partial \Sigma}{\partial y} & q \\ \frac{\partial \mathrm{K}}{\partial x} & \frac{\partial \mathrm{K}}{\partial y} & m \end{vmatrix}$$

был функцией, принимающей во всех двойных точках кривой $G=0$ отличные от нуля значения. Полагая

$$\varphi = \mathrm{P} + thp,$$
$$\psi = \Sigma + thq,$$
$$\chi = \mathrm{K} + thm,$$
$$f = G + 2t(\mathrm{P}p + \Sigma q + \mathrm{K}m) + t^2 h(p^2 + q^2 + m^2),$$

получаем из формулы для G тождество

$$hf = \varphi^2 + \psi^2 + \chi^2,$$

где все формы $h, f, \varphi, \psi, \chi$ в точках $A_1, \ldots, A_{n-4}$ очевидным образом обращаются в нуль.

Докажем теперь, что форма f при любом значении t, заключенном в определенных пределах, имеет отличный от нуля дискриминант. Предположим противное: пусть при любом значении t найдется пара значений x, y, удовлетворяющих уравнениям

$$f=0, \quad \frac{\partial f}{\partial x}=0, \quad \frac{\partial f}{\partial y}=0.$$

Исключая одну из переменных, нетрудно убедиться в том, что решения x, y — алгебраические функции от t и поэтому допускают разложение вида

$$x = a_0 + a_1 t^{\nu_1} + a_2 t^{\nu_2} + \ldots,$$
$$y = b_0 + b_1 t^{\mu_1} + b_2 t^{\mu_2} + \ldots,$$

где показатели $\nu_1, \nu_2, \ldots, \mu_1, \mu_2, \ldots$ — положительные рациональные числа, а коэффициенты a_1, b_1 можно считать отличными от нуля. При $t = 0$ мы получаем, что $x = a_0, y = b_0$ — двойная точка кривой $G = 0$. Если начало системы координат поместить в эту двойную точку, то рассматриваемые нами формы примут вид

$$G = G_{11}x^2 + 2G_{12}xy + G_{22}y^2 + \ldots,$$
$$\mathrm{P}p + \Sigma q + \mathrm{K}m = C_1 x + C_2 y + \ldots,$$
$$h(p^2 + q^2 + m^2) = c_0 + \ldots$$

и, следовательно,

$$\frac{1}{2}\frac{\partial f}{\partial x} = G_{11}x + G_{12}y + C_1 t + \ldots,$$
$$\frac{1}{2}\frac{\partial f}{\partial y} = G_{12}x + G_{22}y + C_2 t + \ldots,$$
$$f - \frac{x}{2}\frac{\partial f}{\partial x} - \frac{y}{2}\frac{\partial f}{\partial y} = C_1 xt + C_2 yt + c_0 t^2 + \ldots,$$

где в правых частях выписаны только члены самого низкого порядка по x, y, t. Эти три выражения должны тождественно, при всех значениях t, обращаться в нуль при подстановке

$$x = a_1 t^{\nu_1} + \ldots, \quad y = b_1 t^{\mu_1} + \ldots$$

Для этого, как нетрудно показать, необходимо, чтобы ряды для x, y были рядами по *целым* степеням t и определитель

$$\Delta = \begin{vmatrix} G_{11} & G_{12} & C_1 \\ G_{12} & G_{22} & C_2 \\ C_1 & C_2 & c_0 \end{vmatrix}$$

был равен нулю.

Для вычисления определителя Δ положим

$$\mathrm{P} = \mathrm{P}_1 x + \mathrm{P}_2 y + \ldots, \qquad p = p_0 t + \ldots,$$
$$\Sigma = \Sigma_1 x + \Sigma_2 y + \ldots, \qquad q = q_0 t + \ldots,$$
$$\mathrm{K} = \mathrm{K}_1 x + \mathrm{K}_2 y + \ldots, \qquad m = m_0 t + \ldots,$$
$$h = h_0 + \ldots,$$

где коэффициент h_0 отличен от нуля по доказанному ранее свойству формы h. Из формулы

$$hG = \mathrm{P}^2 + \Sigma^2 + \mathrm{K}^2$$

следует, что

$$h_0 G_{11} = \mathrm{P}_1^2 + \Sigma_1^2 + \mathrm{K}_1^2,$$
$$h_0 G_{12} = \mathrm{P}_1\mathrm{P}_2 + \Sigma_1\Sigma_2 + \mathrm{K}_1\mathrm{K}_2,$$
$$h_0 G_{22} = \mathrm{P}_2^2 + \Sigma_2^2 + \mathrm{K}_2^2,$$

и поэтому определитель Δ с точностью до множителя h_0 равен дискриминанту квадратичной формы

$$(\mathrm{P}_1 X + \mathrm{P}_2 Y + h_0 p_0 T)^2 + (\Sigma_1 X + \Sigma_2 Y + h_0 q_0 T)^2 + (\mathrm{K}_1 X + \mathrm{K}_2 Y + h_0 m_0 T)^2;$$

этот дискриминант с точностью до множителя h_0 равен квадрату определителя

$$\begin{vmatrix} \mathrm{P}_1 & \mathrm{P}_2 & p_0 \\ \Sigma_1 & \Sigma_2 & q_0 \\ \mathrm{K}_1 & \mathrm{K}_2 & m_0 \end{vmatrix},$$

который, в свою очередь, в силу произведенного нами ранее выбора квадратичных форм p, q, m равен отличному от нуля числу. Тем самым мы приходим к противоречию. Следовательно, предположение о том, что дискриминант формы f при всех значениях t должен быть равен нулю, недопустимо.

Вернемся к формам, построенным в предыдущей части. Так как форма P обращается в нуль в точке A, одна из двух форм $\Sigma + i\mathrm{K}$ или $\Sigma - i\mathrm{K}$ также обращается в нуль в точке A; пусть это будет, например, форма $\Sigma + i\mathrm{K}$. Но тогда комплексно-сопряженная форма $\Sigma - i\mathrm{K}$ обращается в нуль в комплексно-сопряженной с A точке B, а форма $\Sigma + i\mathrm{K}$ принимает в точке B, равно как и форма $\Sigma - i\mathrm{K}$ в точке A, отличное от нуля значение; в противном случае формы Σ и K были бы равны нулю в точке A, а так как форма h отлична от нуля в точке A, то отсюда следовало бы, что кривая $G = 0$ имеет в точке A двойную точку, а это не так.

Докажем, далее, что кривая $\Sigma + i\mathrm{K} = 0$ и кривая $G = 0$ касаются в точке A. Для этого поместим начало системы координат в точку A и возьмем касательную к кривой $G = 0$ в точке A за ось y; рассматриваемые формы примут при этом вид

$$\mathrm{P} = \mathrm{P}_1 x + \mathrm{P}_2 y + \ldots, \quad G = G_1 x + \ldots,$$
$$\Sigma + i\mathrm{K} = T_1 x + T_2 y + \ldots, \quad h = h_0 + \ldots,$$
$$\Sigma - i\mathrm{K} = T_0' + \ldots,$$

где T_0', G_1, h_0 — отличные от нуля числа. Из соотношения

$$hG = \mathrm{P}^2 + (\Sigma + i\mathrm{K})(\Sigma - i\mathrm{K})$$

следует, что $T_2 = 0$; тем самым утверждение доказано.

Формы f, φ, ψ, χ содержат еще переменную t. Выбирая достаточно малое значение t, мы можем, очевидно, добиться, чтобы точка пересечения кривой $f = 0$ с кривыми $\psi + i\chi = 0$, $\psi - i\chi = 0$ оказалась в сколь угодно малой окрестности соответствующей точки пересечения кривой $G = 0$ с кривыми $\Sigma + i\mathrm{K} = 0$, $\Sigma - i\mathrm{K} = 0$, причем расстояние между этими двумя точками пересечения можно измерять, например, по сумме абсолютных величин разностей координат. Приняв именно такое определение расстояния, выберем вокруг $\frac{1}{2}(n-1)(n-2)$ двойных точек кривой $G = 0$ небольшие

области так, чтобы форма h в каждой точке такой области была отлична от нуля и, кроме того, не существовало формы $(n-3)$-го порядка, которая имела бы нули внутри всех этих $\frac{1}{2}(n-1)(n-2)$ областей. Последнее всегда возможно, так как не существует кривой $(n-3)$-го порядка, которая проходила бы через все $\frac{1}{2}(n-1)(n-2)$ двойных точек кривой $G=0$. Выберем, кроме того, вокруг обеих точек A и B по области, в которой форма h отлична от нуля. Возьмем теперь параметр t столь малым, чтобы все точки пересечения кривых $\psi+i\chi=0$ и $\psi-i\chi=0$ с кривой $f=0$ оказались в выбранных областях за исключением $n-4$ точек пересечения $A_1,\ldots,A_{n-4}$, остающихся неподвижными. Учитывая тождество

$$pf=\varphi^2+\psi^2+\chi^2$$

и тот факт, что кривая $f=0$ не имеет двойных точек, приходим с помощью рассуждения, аналогичного приведенному нами чуть выше, к следующему результату: кривая $\psi+i\chi=0$ касается кривой $f=0$ в некоторой точке области, выбранной вокруг точки A, и в какой-то точке каждой из областей вокруг $\frac{1}{2}(n-1)(n-2)$ двойных точек кривой $G=0$. Обозначим точки касания через A, $U_1,\ldots,U_{\frac{1}{2}(n-1)(n-2)}$. Кривая $\psi-i\chi=0$ касается кривой $f=0$ в некоторой точке области, выбранной вокруг точки B, и в какой-то точке каждой из областей вокруг $\frac{1}{2}(n-1)(n-2)$ двойных точек; обозначим точки касания через B, $V_1,\ldots,V_{\frac{1}{2}(n-1)(n-2)}$ соответственно.

Тем самым мы построили определенную форму f с отличным от нуля дискриминантом, допускающую представление

$$f=\frac{\varphi^2+\psi^2+\chi^2}{h};$$

при этом φ, ψ, χ — формы $(n-2)$-го порядка с вещественными коэффициентами и следующими свойствами: кривые $\varphi=0$, $\psi=0$, $\chi=0$ имеют с кривой $f=0$ заведомо $n-4$ попарно комплексно-сопряженных точек пересечения $A_1,\ldots,A_{n-4}$; кроме того, кривая $\psi+i\chi=0$ касается кривой $f=0$ в $1+\frac{1}{2}(n-1)(n-2)$ комплексных точках A, $U_1,\ldots,U_{\frac{1}{2}(n-1)(n-2)}$; кривая $\psi-i\chi=0$ касается кривой $f=0$ в комплексно-сопряженных к ним точках B, $V_1,\ldots,V_{\frac{1}{2}(n-1)(n-2)}$; кривая $\varphi=0$ пересекает кривую $f=0$, кроме того, в точках A, $U_1,\ldots,U_{\frac{1}{2}(n-1)(n-2)}$, B, $V_1,\ldots,V_{\frac{1}{2}(n-1)(n-2)}$. Все перечисленные выше точки различны, а точки касания $U_1,\ldots,U_{\frac{1}{2}(n-1)(n-2)}$, так же как и точки касания $V_1,\ldots,V_{\frac{1}{2}(n-1)(n-2)}$, не лежат ни на какой кривой $(n-3)$-го порядка.

5. В последующих частях мы будем подвергать непрерывному изменению как коэффициенты построенной выше формы f, так и лежащие на кривой $f=0$ точки A, B, U, V, с таким расчетом, чтобы все коэффициенты формы f и координаты точек $A_1,\ldots,A_{n-4},A$ можно было рассматривать как независимые переменные, а координаты точек $U_1,\ldots,U_{\frac{1}{2}(n-1)(n-2)}$ — как функции этих независимых переменных. При этом мы будем использовать некоторые факты из теории абелевых функций, сформулировав их для наших целей следующим образом.

Пусть F — произвольная форма n-го порядка с вещественными коэффициентами и отличным от нуля дискриминантом. Уравнение $F=0$ задает y

как алгебраическую функцию от x. Так как кривая $F = 0$ не имеет двойных точек, ее род равен

$$p = \frac{1}{2}(n-1)(n-2);$$

p всюду конечных интегралов этой кривой имеют вид

$$w = \int \frac{x^\mu y^\nu}{\partial F/\partial x} dx,$$

где сумма показателей μ, ν не превосходит число $n-3$.

Для нашей цели необходимо рассмотреть задачу о построении кривой $(n-2)$-го порядка, пересекающей заданную кривую $F = 0$ в заданных точках $A_1, \ldots, A_{n-4}$ и касающейся той же кривой в заданной точке A и p других точках, которые требуется определить. Эта задача приводит к подзадаче, которая решается с помощью проблемы обращения Якоби.

Пусть p всюду определенных конечных интегралов выбраны так, как это предложено Риманом; обозначим их $w_1, \ldots, w_p$ и условимся понимать под $w(P)$ значение любого такого интеграла в точке P.

I. Если $P_1, \ldots, P_{n(n-2)}$ — точки пересечения произвольной кривой $(n-2)$-го порядка с кривой $F = 0$, то по теореме Абеля

$$w_s(P_1) + \ldots + w_s(P_{n(n-2)}) \equiv \beta_s \qquad (s = 1, 2, \ldots, p),$$

где $\beta_1, \ldots, \beta_p$ — суммы всюду конечных интегралов, зависящих не от точек $P_1, \ldots, P_{n(n-2)}$, а от коэффициентов формы F.

Обращение теоремы Абеля приводит к следующей теореме:

II. Если в $n(n-2)$ точках $P_1, \ldots, P_{n(n-2)}$ кривой $F = 0$ выполняются сравнения, приведенные в теореме I, то эти точки могут быть получены как точки пересечения кривой $F = 0$ с некоторой кривой $(n-2)$-го порядка.

Условимся в дальнейшем понимать под $w(x)$ значение, принимаемое интегралом w в точке с координатами x, y. Для функции Θ от p переменных, соответствующей нашей алгебраической кривой, справедливы следующие теоремы:

III. Если p точек $U_1, \ldots, U_p$ *не лежат* на кривой $(n-3)$-го порядка, то функция

$$\Theta[w_1(x) - w_1(U_1) - \ldots - w_1(U_p), \ldots, w_p(x) - w_p(U_1) - \ldots - w_p(U_p)]$$

не равна тождественно нулю при всех значениях x.

IV. Если функция Θ, о которой говорится выше, не равна тождественно нулю при всех значениях x, то как функция от x она имеет нули в p точках $U_1, \ldots, U_p$ и только в этих точках, и при подстановке в Θ выражений

$$w_s(U_1) + \ldots + w_s(U_p) \equiv$$

$$\equiv \frac{\beta_s}{2} - \frac{1}{2}[w_s(A_1) + \ldots + w_s(A_{n-4})] - w_s(A) \qquad (s = 1, 2, \ldots, p)$$

эти p нулей переходят в точки касания кривой $(n-2)$-го порядка, пересекающей кривую $F = 0$ в заданных точках $A_1, \ldots, A_{n-4}$ и касающейся ее в заданной точке A.

V. Функция Θ тождественно равна нулю, если в любой сколь угодно малой окрестности p точек $U_1, \ldots, U_p$ можно найти p других точек $U_1', \ldots, U_p'$, которые являются точками касания кривой $(n-2)$-го порядка, пересекающей кривую $F = 0$ в заданных точках $A_1, \ldots, A_{n-4}$ и касающейся ее в заданной точке A.

VI. Обратно, если функция Θ, о которой говорилось выше, тождественно равна нулю при всех значениях x, то в любой сколь угодно малой окрестности точек $U_1, \ldots, U_p$ всегда существует p других точек $U_1', \ldots, U_p'$, которые являются точками касания кривой $(n-2)$-го порядка, проходящей через точки $A_1, \ldots, A_{n-4}$ и касающейся кривой $F = 0$ в точке A.

6. Приведенные выше утверждения позволяют осуществить непрерывное изменение коэффициентов формы f так, как это предполагалось в начале предыдущей части. Для этого образуем для интересующей нас формы f функцию

$$\Theta[w_1(x) - w_1(U_1) - \ldots - w_1(U_p), \ldots, w_p(x) - w_p(U_1) - \ldots - w_p(U_p)]$$

и заменим относящиеся к точке U суммы интегралов известными величинами так, как это сделано в теореме IV предыдущей части. Так как по построению функции f в части 4 точки касания $U_1, \ldots, U_p$ не лежат на кривой $(n-3)$-го порядка, то по теореме III предыдущей части функция Θ не равна тождественно нулю при всех значениях x. Следовательно, по теореме IV функция Θ принимает нулевое значение только в p точках $U_1, \ldots, U_p$. Периоды и аргументы функции Θ составляются по вполне определенному закону из соответствующих кривой $f = 0$ всюду конечных интегралов. Значит, подвергая непрерывному изменению коэффициенты формы f и заданные точки $A_1, \ldots, A_{n-4}, A$, мы тем самым непрерывно изменяем периоды и аргументы функции Θ (лишь до тех пор, пока дискриминант формы f не обратится в нуль). Функция Θ допускает разложение по степеням периодов и амплитуд, и по известной теореме Вейерштрасса[3] нули функции Θ — непрерывные функции периодов и аргументов. Тем самым показано, что эти нули изменяются непрерывно при непрерывном изменении коэффициентов формы f и заданных точек $A_1, \ldots, A_{n-4}, A$.

Нули $U_1, \ldots, U_p$ функции Θ, как показано выше, являются точками касания некоторой кривой $(n-2)$-го порядка. Так как этими p точками касания и заданными точками $A_1, \ldots, A_{n-4}, A$ соприкасающаяся кривая $\psi + i\chi = 0$ полностью определена, то отсюда следует, что при их непрерывном изменении коэффициенты формы $\psi + i\chi$ также претерпевают непрерывное изменение и что то же самое относится и к коэффициентам форм ψ и χ.

По существу нам остается доказать, что всякая форма F, возникающая при непрерывном изменении из формы f, допускает такое же представление, как и сама форма f. Для этого мы прежде всего построим по p нулям функции Θ соответствующую соприкасающуюся кривую для кривой $F = 0$; пусть $\Psi + i\mathrm{X} = 0$ — уравнение этой кривой; $n-4$ простых точек пересечения соприкасающейся кривой с кривой $F = 0$ следует выбрать попарно комплексно-сопряженными; обозначим их, как и прежде,

---

[3] См.: *Weierstrass K.* Einige auf die Theorie der analytischen Funktionen mehrer Veränderlichen sich beziehende Sätze. — Ges. Werke. 1895. Bd. 11. S. 135.

$A_1, \ldots, A_{n-4}$. Точки касания мы обозначим также по-старому: $A, U_1, \ldots, U_p$; комплексно-сопряженными с ними, как нетрудно видеть, будут точки $B, V_1, \ldots, V_p$, в которых проходящая через точки $A_1, \ldots, A_{n-4}$ кривая $\Psi - i\mathrm{X} = 0$ касается кривой $F = 0$.

По теореме I

$$w_s(A_1) + \ldots + w_s(A_{n-4}) + 2[w_s(A) + w_s(U_1) + \ldots + w_s(U_p)] \equiv \beta_s,$$

$$w_s(A_1) + \ldots + w_s(A_{n-4}) + 2[w_s(B) + w_s(V_1) + \ldots + w_s(V_p)] \equiv \beta_s$$

$$(s = 1, 2, \ldots, p),$$

и если сложить обе эти формулы и получившееся сравнение разделить на 2, то

$$w_s(A_1) + \ldots + w_s(A_{n-4}) + w_s(A) + w_s(U_1) + \ldots + w_s(U_p) +$$

$$+ w_s(B) + w_s(V_1) + \ldots + w_s(V_p) \equiv \beta_s + \frac{\varepsilon}{2}\Pi_s \qquad (s = 1, 2, \ldots, p),$$

где $\Pi_1, \ldots, \Pi_p$ — система периодов, а ε равно либо 0, либо 1. Чтобы решить, какой из этих двух случаев имеет место, необходимо учесть следующее: все лежащие на кривой $f = 0$ точки $A_1, \ldots, A_{n-4}$, A, $U_1, \ldots, U_p$, B, $V_1, \ldots, V_p$ получены как точки пересечения ее с кривой $(n-2)$-го порядка, а именно с кривой $\varphi = 0$, и поэтому по теореме I

$$w_s(A_1) + \ldots + w_s(A_{n-4}) + w_s(A) + w_s(U_1) + \ldots + w_s(U_p) +$$

$$+ w_s(B) + w_s(V_1) + \ldots + w_s(V_p) \equiv \beta_s \qquad (s = 1, 2, \ldots, p).$$

Но так как при непрерывном изменении коэффициентов формы F и координат точек $A_1, \ldots, A_{n-4}$, A предпоследняя формула переходит в последнюю, а периоды $\Pi_1, \ldots, \Pi_p$ при этом не могут все обратиться в нуль, мы заключаем, что в первой формуле $\varepsilon = 0$ и поэтому по теореме II расположенные на кривой $F = 0$ точки $A_1, \ldots, A_{n-4}$, A, $U_1, \ldots, U_p$, B, $V_1, \ldots, V_p$ также являются точками пересечения этой кривой с кривой $(n-2)$-го порядка; пусть $\Phi = 0$ — уравнение последней кривой, где Φ — форма $(n-2)$-го порядка с вещественными коэффициентами.

Каждая из двух кривых $\Phi^2 = 0$ и $\Psi^2 + \mathrm{X}^2 = 0$ пересекает кривую $F = 0$ в $n(n-2)$ точках $A_1, \ldots, A_{n-4}$, A, $U_1, \ldots, U_p$, B, $V_1, \ldots, V_p$; при этом каждую из перечисленных точек надлежит, очевидно, считать двукратной точкой пересечения. Если определить постоянную λ так, чтобы форма $\lambda\Phi^2 + \Psi^2 + \mathrm{X}^2$ имела с формой F еще один общий нуль, то форма $\lambda\Phi^2 + \Psi^2 + \mathrm{X}^2$ будет содержать форму F в качестве множителя. Постоянная λ — вещественное число; действительно, если бы она была комплексным числом и мы обозначили бы комплексно-сопряженное число через λ', то форма $\lambda'\Phi^2 + \Psi^2 + \mathrm{X}^2$ должна была бы делиться на F, что невозможно. Если квадратный корень из абсолютной величины λ включить в форму Φ, то получится соотношение вида

$$HF = \pm\Phi^2 + \Psi^2 + \mathrm{X}^2.$$

Так как путем непрерывного изменения коэффициентов форм F, Φ, Ψ, X мы можем вернуться к соответствующим коэффициентам форм f, φ, ψ, χ

и между последними формами возникает соотношение

$$hf = \varphi^2 + \psi^2 + \chi^2,$$

в приведенной выше формуле следует выбрать знак плюс; тем самым показано, что форма F может быть представлена в виде

$$F = \frac{\Phi^2 + \Psi^2 + \mathrm{X}^2}{H}.$$

Здесь F — форма с вещественными коэффициентами, возникающая из формы f при произвольном непрерывном изменении коэффициентов (при том, однако, ограничении, что изменение коэффициентов не приводит к формам с нулевым дискриминантом или с функцией Θ, тождественно равной нулю при всех значениях x).

7. В этой части мы исследуем, при каких условиях из формы f при непрерывном изменении коэффициентов может возникнуть форма, для которой функция Θ тождественно равна нулю. Для этого нам понадобится одна лемма из теории исключения, которая гласит следующее.

Пусть имеется m уравнений вида

$$G_1(x, y, \ldots, p, q, \ldots) = 0,$$

$$\ldots\ldots\ldots\ldots\ldots$$

$$G_m(x, y, \ldots, p, q, \ldots) = 0,$$

где $G_1, \ldots, G_m$ — целые рациональные функции от неизвестных $x, y, \ldots$ и параметров $p, q, \ldots$, пусть эти уравнения выполняются при $x = 0$, $y = 0, \ldots$ $\ldots, p = 0$, $q = 0, \ldots$, и пусть существует положительная величина δ, такая, что всякий раз, когда значения параметров $p, q, \ldots$ по абсолютной величине не превосходят величину δ, можно найти одну и только одну систему величин $x, y, \ldots$, которые удовлетворяют уравнениям и по абсолютной величине не превосходят δ; тогда величины $x, y, \ldots$ — алгебраические функции параметров $p, q, \ldots$, т. е. каждая функция $x, y, \ldots$ удовлетворяет алгебраическому уравнению с коэффициентами, рационально зависящими от $p, q, \ldots$

Доказательство этого не представляет особого труда, но я не буду приводить его здесь.

Сформулированная только что теорема позволяет доказать, что координаты точек касания $U_1, \ldots, U_p$ — алгебраические функции коэффициентов формы F и координат точек $A_1, \ldots, A_{n-4}, A$. Действительно, если наложить условия, при которых $U_1, \ldots, U_p$ — точки касания кривой $(n-2)$-го порядка, пересекающей кривую $F = 0$ в заданных точках $A_1, \ldots, A_{n-4}$ и касающейся ее в заданной точке A, то получится система алгебраических уравнений; если коэффициенты формы F и координаты точек $A_1, \ldots, A_{n-4}, A$ подвергнуть непрерывному изменению, то каждой возникающей при этом системе коэффициентов и координат соответствует определенная функция Θ, нули которой служат для кривой $F = 0$ точками касания. Таким образом (если учесть теоремы IV и V из части 5), все условия нашей леммы выполнены; тем самым доказано, что координаты точек касания $U_1, \ldots, U_p$ удовлетворяют алгебраическим уравнениям, коэффициенты которых являются целыми рациональными функциями заданных величин, а именно коэффициентов формы F и координат точек $A_1, \ldots, A_{n-4}, A$. Мы считаем эти алгебраические

уравнения известными и предполагаем, что не все их коэффициенты содержат в качестве общего множителя целую рациональную функцию заданных величин.

Если форма F обладает той особенностью, что соответствующая ей функция Θ при всех значениях x и всех значениях координат точек $A_1, \ldots, A_{n-4}$ тождественно равна нулю, то по теореме VI из части 5 в любой сколь угодно малой окрестности точек $U_1, \ldots, U_p$ существуют другие точки $U_1', \ldots, U_p'$, координаты которых удовлетворяют тем же уравнениям, т. е. рассматриваемые уравнения имеют бесконечно много решений и поэтому по крайней мере у одного из них все коэффициенты должны быть равны нулю. Нули этих коэффициентов задают систему уравнений вида

$$C_1 = 0, \quad \ldots, \quad C_M = 0,$$

где $C_1, \ldots, C_M$ — целые рациональные функции коэффициентов $a_1, \ldots, a_N$ формы F. Все эти функции не могут содержать один и тот же множитель, так как в противном случае левые части выписанных уравнений вопреки доказанному также должны были бы содержать общий множитель. В силу обнаруженного свойства эти уравнения, если коэффициенты $a_1, \ldots, a_N$ формы F интерпретировать как однородные координаты точки в $(N-1)$-мерном пространстве R, задают некоторое алгебраическое многообразие (Gebilde) размерности меньше $N-2$. Таким образом, функция Θ при произвольном выборе точек $A_1, \ldots, A_{n-4}$, A тождественно обращается в нуль только в том случае, когда коэффициенты $a_1, \ldots, a_N$ соответствующей формы F задают в $(N-1)$-мерном пространстве R точку, принадлежащую некоторому алгебраическому многообразию размерности меньше $N-2$.

8. Теперь мы уже в состоянии распространить результаты, полученные в конце части 6, на все определенные формы. Докажем для этого предварительно следующую теорему.

Пусть $f_1, f_2, \ldots$ — бесконечная последовательность определенных форм, каждая из которых допускает полученное выше представление и имеет коэффициенты, переходящие в пределе в коэффициенты формы F. Тогда форма F также допускает представление, о котором идет речь.

Для доказательства положим

$$f_s = \frac{\varphi_s^2 + \psi_s^2 + \chi_s^2}{h_s} \qquad (s = 1, 2, \ldots)$$

и дробь в правой части при каждом значении s будем считать устроенной так, что наибольший по абсолютной величине коэффициент в формах φ_s, ψ_s, χ_s равен единице (этого всегда, очевидно, можно добиться, разделив числитель и знаменатель дроби на абсолютную величину наибольшего коэффициента). Так как по предположению все коэффициенты форм f_s по абсолютной величине также заключены в определенных пределах, то же справедливо и относительно коэффициентов формы h_s. Если рассмотреть бесконечную последовательность коэффициентов форм φ_s, ψ_s, χ_s, h_s, то по известной теореме существует по крайней мере *одна* система соответствующих значений, в окрестности которых значения коэффициентов последовательности форм сгущаются. Формы, построенные по этим точкам уплотнения, обозначим Φ, Ψ, X, H. Тогда для любого сколь угодно малого

числа δ всегда найдется число s, такое, что

$$|\Phi - \varphi_s| < \delta, \quad |\Psi - \psi_s| < \delta, \quad |\mathrm{X} - \chi_s| < \delta, \quad |H - h_s| < \delta.$$

Отсюда, как нетрудно доказать, следует, что

$$HF = \Phi^2 + \Psi^2 + \mathrm{X}^2;$$

действительно, если бы $HF - \Phi^2 - \Psi^2 - \mathrm{X}^2 = \Delta$, где Δ — форма, у которой по крайней мере один из коэффициентов отличен от нуля, то мы бы подставили в последнее равенство

$$H_s = h_s + \pi_s, \quad F = f_s + \varkappa_s, \quad \Phi = \varphi_s + \delta_s,$$
$$\Psi = \psi_s + \varepsilon_s, \quad \mathrm{X} = \chi_s + \eta_s$$

и заметили бы, что при подходящем выборе s все коэффициенты форм π_s, $\varkappa_s$, δ_s, ε_s, η_s могут быть сделаны меньше сколь угодно малого числа. Но это было бы несовместимо с предположением о том, что форма Δ имеет по крайней мере один отличный от нуля коэффициент.

Как показывают несложные рассуждения, отсюда с необходимостью следует, что при каждом s три формы φ_s, ψ_s, χ_s имеют некоторое число общих нулей и столько же общих нулей имеют предельные формы Φ, Ψ, X.

Для большей наглядности мы будем интерпретировать в дальнейшем N коэффициентов $a_1, \ldots, a_N$ формы F как однородные координаты в пространстве R размерности $N-1$ и рассмотрим в этом пространстве сначала поверхность, задаваемую уравнением $D = 0$, где D — дискриминант формы F. Эта поверхность имеет размерность $N-2$ и делит пространство на различные области. Затем мы рассмотрим в пространстве R алгебраическое многообразие, задаваемое уравнениями $C_1 = 0, \ldots, C_M = 0$; как следует из предыдущей части, его размерность меньше, чем $N-2$. Нас будут особенно интересовать те точки пространства R, которые соответствуют определенным формам. Нетрудно видеть (это было доказано в моей работе «О представлении определенных форм в виде суммы квадратов форм»[4]), что путем непрерывного изменения вещественных коэффициентов одну определенную форму можно перевести в другую, не проходя при этом через определенную форму с нулевым дискриминантом, т. е. соответствующие определенным формам точки пространства R заполняют некоторую связную область. На границе этой области лежат точки, соответствующие определенным формам с нулевым дискриминантом; кроме того, в область определенных форм вкраплены изолированные многообразия размерности $N-3$ и меньше, точки которых также соответствуют формам с нулевым дискриминантом. Так как многообразие, задаваемое уравнениями $C_1 = 0, \ldots, C_M = 0$, также имеет размерность не выше $N-3$, то оно не может нарушить связность области определенных форм; следовательно, если f и F — две определенные формы, то всегда можно путем непрерывного изменения вещественных коэффициентов перевести форму f в форму F, не проходя при этом через точку дискриминантной поверхности $D = 0$ или точку многообразия, задаваемого уравнениями $C_1 = 0, \ldots, C_M = 0$.

---

[4] Math. Ann., 1888, Bd. 32, S. 342–350 [имеется перевод на с. 331–338 настоящего издания. — *Ред.*].

Будем теперь понимать под f определенную форму, построенную в части 4. Так как точки касания $U_1, \ldots, U_p$ не лежат на кривой $(n-3)$-го порядка, функция Θ не равна тождественно нулю и соответствующая точка в пространстве R не лежит на многообразии, задаваемом уравнениями $C_1 = 0, \ldots, C_M = 0$, и расположена вне дискриминантной поверхности. Пусть F — произвольная определенная форма, такая, что соответствующая точка лежит либо вне этих специальных многообразий, либо на каком-то из них. Соединим форму f с формой F так же, как это делалось выше, путем, по которому f непрерывно преобразуется в F, не проходя через точки, лежащие на специальных многообразиях.

Докажем, что каждая точка этого пути соответствует форме, допускающей требуемое представление в виде дроби. Действительно, если проведенный путь пройден до некоторой точки и всем пройденным точкам соответствуют формы, допускающие указанное представление, то, как следует из теоремы, приведенной в начале этой части, последней точке также соответствует форма, допускающая такое представление. С другой стороны, из части 6 мы заключаем: если для какой-нибудь формы F, соответствующей точке построенного пути, доказана представимость в требуемом виде, то путь всегда можно продолжить на конечный отрезок за эту точку так, чтобы все формы, соответствующие новому отрезку пути, допускали аналогичное представление, и так как форма, соответствующая конечной точке пути, есть произвольная определенная форма, то тем самым доказана следующая теорема.

Любая произвольная тернарная определенная форма F порядка n представима в виде

$$F = \frac{\Phi^2 + \Psi^2 + \mathrm{X}^2}{H},$$

где Φ, Ψ, X — формы с вещественными коэффициентами $(n-2)$-го порядка, а H — форма $(n-4)$-го порядка.

9. Полученный только что результат позволяет немедленно доказать теорему, сформулированную во введении; действительно, форма H порядка $n-4$, стоящая в знаменателе правой части, есть, в свою очередь, определенная форма, и поэтому к ней применима теорема о представимости в виде дроби, в числителе которой стоит сумма трех квадратов форм, а в знаменателе — определенная форма $(n-8)$-го порядка. Продолжая таким образом, мы в конечном итоге приходим к дроби, в знаменателе которой стоит константа или квадратичная определенная форма. Так как последняя равна сумме квадратов форм, после выполнения операций умножения приходим к представлению исходной формы F в виде отношения сумм квадратов. Сформулируем доказанную теорему следующим образом:

любая тернарная определенная форма F представима в виде

$$F = \frac{\Phi_1^2 + \Phi_2^2 + \ldots + \Phi_P^2}{\varphi_1^2 + \varphi_2^2 + \ldots + \varphi_\rho^2},$$

где $\Phi_1, \Phi_2, \ldots, \Phi_P, \varphi_1, \varphi_2, \ldots, \varphi_\rho$ — формы с вещественными коэффициентами.

Кёнигсберг в Пруссии, 18 февраля 1892 г.

ОБ УРАВНЕНИИ ДЕВЯТОЙ СТЕПЕНИ*)

Большинство проблем, упомянутых мною в докладе «Математические проблемы»[1] и относящихся к различным областям математики, с тех пор успешно исследовались различными методами. В приводимом ниже сообщении я хотел бы обратиться к некоторым из этих проблем, а именно к задачам, требующим для своего решения алгебраических средств и методов, хотя по своей постановке они происходят из других, неалгебраических, дисциплин.

К первому классу таких проблем относится вопрос о конечности некоторой полной системы функций — задача, постановкой которой мы обязаны теории инвариантов. Простейшей задачей этого класса представляется мне следующая.

Пусть задано m целых рациональных функций $X_1, \ldots, X_m$ от переменной x с определенными численными коэффициентами; тогда, как нетрудно видеть, каждое целое рациональное соотношение между $X_1, \ldots, X_m$ после подстановки этих функций всегда превращается в целую рациональную функцию от x. Однако вполне могут встретиться дробно-рациональные функции от $X_1, \ldots, X_m$, которые после подстановки $X_1, \ldots, X_m$ также превращаются в целые функции от x. Проблема состоит в следующем: показать возможность выбора такого *конечного* числа дробных функций от $X_1, \ldots$ $\ldots, X_m$ с этим свойством, чтобы любая другая такая дробная функция была представима в виде целой рациональной функции от этих функций и самих функций $X_1, \ldots, X_m$[2].

Указанная проблема служит примером того, что столь распространенное в арифметике явление, когда ответ на весьма простой по своей постановке и, казалось бы, очевидный вопрос наталкивается на серьезные трудности, может встречаться и в области чистой алгебры.

Другой класс алгебраических проблем указанного рода возникает при попытке алгебраически реализовать топологически важные и интересные кривые, поверхности или специфические геометрические объекты, наделенные особенностями, которые стали предметом топологических исследований нового времени[3].

Весьма простым примером этого служит задача о взаимно однозначном и всюду регулярном проектировании проективной плоскости в ее конечную

---

*) Über die Gleichung der neunten Grades. — Math. Ann., 1927, Bd. 97, S. 243–250. *Перевод Ю. А. Данилова.*

[1] Доклад на Международном математическом конгрессе в Париже: *Hilbert D.* Mathematische Probleme. — Nachr. Ges. Wiss. Göttingen, 1900, S. 253–297; Arch. Mathematik und Physik, 1901, 3. Reihe, Bd. 1, S. 44–63, 213–237 [имеется перевод в т. 2 настоящего издания. — *Ред.*].

[2] См. четырнадцатую проблему в упомянутом докладе.

[3] Такую постановку вопроса следует рассматривать как обобщение и углубление шестнадцатой проблемы из моего доклада.

часть. Как известно, в трехмерном пространстве она решается с помощью поверхности, приведенной в диссертации Боя, — поверхности, пересекающей себя по некоторой пространственной кривой с тройной точкой. Возникает вопрос, существует ли, например, в четырехмерном пространстве двумерные поверхности без особенностей такой же связности [1] и *без* самопересечения?

Ответ на поставленный вопрос оказывается утвердительным и получается проще всего, если понять, что искомое отображение проективной плоскости порождается поверхностью, задаваемой квадратичными функциями, а именно поверхностью, задаваемой формулами

$$x = \eta\zeta,$$
$$y = \zeta\xi,$$
$$z = \xi\eta,$$
$$t = \xi^2 - \eta^2,$$
$$\xi^2 + \eta^2 + \zeta^2 = 1,$$

где x, y, z, t — прямоугольные координаты в четырехмерном пространстве, а параметры ξ, η, ζ — прямоугольные координаты в трехмерном пространстве. Задаваемая этими формулами поверхность, очевидно, всюду регулярна в четырехмерном пространстве, а так как точке ξ, η, ζ сферы в трехмерном пространстве всегда соответствует та же точка x, y, z, t поверхности, что и диаметрально противоположной точке $-\xi, -\eta, -\zeta$, то эта поверхность в четырехмерном пространстве обладает требуемой связностью [1] проективной плоскости. Остается лишь доказать, что рассматриваемая поверхность не имеет самопересечений, т. е. каждой точке x, y, z, t поверхности соответствует лишь *одна* пара троек ξ, η, ζ и $-\xi, -\eta, -\zeta$.

Для доказательства воспользуемся тем, что по формуле

$$t^2 + 4z^2 = (\xi^2 + \eta^2)^2$$

величина $\xi^2 + \eta^2$ однозначно определяется заданием t и z, а так как t есть не что иное, как $\xi^2 - \eta^2$, значения t и z однозначно определяют значения ξ^2 и η^2, например, $\xi^2 = p$ и $\eta^2 = q$.

Если предположить, что $p > 0$, то с учетом соотношений

$$z = \xi\eta \qquad \text{и} \qquad y = \zeta\xi$$

мы получаем для ξ, η, ζ две тройки значений

$$\xi = \sqrt{p}, \qquad \eta = \frac{z}{\sqrt{p}}, \qquad \zeta = \frac{y}{\sqrt{p}}$$

и

$$\xi = -\sqrt{p}, \qquad \eta = -\frac{z}{\sqrt{p}}, \qquad \zeta = -\frac{y}{\sqrt{p}},$$

что соответствует утверждению, которое требуется доказать. С другой стороны, при $p = 0$ рассмотрим значение q величины η^2. Если $q > 0$, то из соотношения

$$x = \eta\zeta$$

мы получаем две тройки значений

$$\xi = 0, \qquad \eta = \sqrt{q}, \qquad \zeta = \frac{x}{\sqrt{q}}$$

и

$$\xi = 0, \qquad \eta = -\sqrt{q}, \qquad \zeta = -\frac{x}{\sqrt{q}},$$

что также соответствует утверждению, которое требуется доказать. Наконец, если $q = 0$, то из соотношения

$$\xi^2 + \eta^2 + \zeta^2 = 1$$

мы получаем для ξ, η, ζ две тройки значений

$$\xi = 0, \qquad \eta = 0, \qquad \zeta = 1$$

и

$$\xi = 0, \qquad \eta = 0, \qquad \zeta = -1.$$

Тем самым доказано, что наше утверждение выполняется всегда.

Весьма изящное и наглядное представление упоминавшейся выше поверхности в трехмерном пространстве, построенной Боем, недавно было найдено Ф. Шиллингом; задача о наиболее простой алгебраической реализации этой поверхности относится к кругу рассматриваемых нами задач.

Третий класс задач указанного выше рода возникает в связи с нуждами номографии[4]. Эта дисциплина наводит на мысль характеризовать функции произвольно большого числа аргументов тем, представимы ли они в виде суперпозиции функций определенного числа аргументов.

Из функций одного аргумента мы получаем при подстановках только функции одного аргумента. Если же мы хотим перейти к функциям нескольких переменных, то к области функций одного аргумента необходимо присоединить по крайней мере одну функцию двух переменных. Выберем для этого сумму $u+v$ двух переменных u, v и убедимся, что три остальные арифметические операции (вычитание, умножение и деление) попадают в область выполнимых операций, т. е. могут быть получены как суперпозиции функций *одного* аргумента и суммы следующим образом:

$$u - v = u + (-v),$$

$$u \cdot v = \frac{1}{4}\{(u+v)^2 - (u-v)^2\},$$

$$\frac{u}{v} = u \cdot \frac{1}{v}.$$

Возникает вопрос: имеются ли вообще помимо суммы другие аналитические функции двух существенных аргументов, т. е. аналитические функции, не представимые в виде суперпозиции функций одного аргумента и суммы? Доказать существование таких функций можно в действительности различными способами. Наиболее далеко идущий результат в этом направлении

---

[4] См. тринадцатую проблему моего доклада.

получил А. Островский[5]. Из его работы, в частности, следует, что функция двух переменных u, v

$$\zeta(u, v) = \sum_{n=1,2,3\ldots} \frac{u^n}{n^v}$$

не представима в виде суперпозиции аналитических функций одной переменной и алгебраических функций произвольного числа аргументов.

Следующий вопрос — о существовании *алгебраических* функций такого рода, т. е. вопрос о том, существует ли алгебраическая функция, не представимая в виде суперпозиции функций одного аргумента и суммы.

Некоторые важные моменты в указанном направлении позволяет прояснить метод преобразования Чирнгаузена. Как известно, этот метод состоит в следующем.

Пусть имеется уравнение n-й степени

$$x^n + u_1 x^{n-1} + u_2 x^{n-2} + \ldots + u_n = 0.$$

Чтобы представить корень x как функцию от n переменных u_1, $u_2, \ldots$, u_n, составим выражение

$$X = x^{n-1} + t_1 x^{n-2} + \ldots + t_{n-1}$$

с неопределенными коэффициентами $t_1, \ldots, t_{n-1}$ и запишем уравнение для X; последнее имеет вид

$$X^n + U_1 X^{n-1} + \ldots + U_n = 0,$$

где, вообще говоря,

$$U_h = U_h(t_1, \ldots, t_{n-1})$$

— функция h-й степени относительно $t_1, \ldots, t_{n-1}$. Если параметры $t_1, \ldots$ $\ldots, t_{n-1}$ выбрать так, чтобы

$$U_1 = 0, \qquad U_2 = 0, \qquad U_3 = 0,$$

то оказывается, что исходное уравнение с помощью одних лишь рациональных операций и извлечения корней приводится к виду

$$X^n + U_4 X^{n-4} + U_5 X^{n-5} + \ldots + U_n = 0.$$

Наконец, если подставить

$$X = \sqrt[n]{U_n}\, Y,$$

то для новой переменной Y возникает уравнение n-й степени, в котором не только равны нулю коэффициенты при Y^{n-1}, Y^{n-2}, Y^{n-3}, но первый и последний коэффициенты равны единице.

---

[5] *Ostrovski A.* Über Dirichletsche Reihen und algebraische Differentialgleichungen. — Math. Z., Bd. 8. S. 241.

В результате уравнения от пятой до девятой степени приводятся к следующим нормальным формам:

$$x^5 + ux + 1 = 0,$$

$$x^6 + ux^2 + vx + 1 = 0,$$

$$x^7 + ux^3 + vx^2 + wx + 1 = 0,$$

$$x^8 + ux^4 + vx^3 + wx^2 + px + 1 = 0,$$

$$x^9 + ux^5 + vx^4 + wx^3 + px^2 + qx + 1 = 0.$$

Так как операция извлечения корня также есть функция одного аргумента, тем самым показано, что приведение к каждой из этих нормальных форм требует только функций одного аргумента и операции взятия суммы. Что же касается нашего вопроса об алгебраической функции двух существенных (в указанном смысле) аргументов, то, как нетрудно видеть, уравнение пятой степени не может породить такую функцию; действительно, приведенная выше нормальная форма содержит только один параметр u, вследствие чего общее уравнение пятой степени также разрешимо с помощью функций одного аргумента и операции взятия суммы.

Для нормальной формы уравнения шестой степени

$$x^6 + ux^2 + vx + 1 = 0$$

попытки решить ее с помощью функций одного аргумента и операции взятия суммы, как нетрудно видеть, обречены на неудачу, и возникает предположение, что корень этого уравнения шестой степени есть функция, обладающая требуемыми свойствами.

Что же касается уравнения седьмой степени

$$x^7 + ux^3 + vx^2 + wx + 1 = 0,$$

то в докладе, о котором упоминалось в начале моего сообщения, я высказал предположение, что оно неразрешимо даже с помощью произвольных непрерывных функций двух аргументов; это утверждение также еще предстоит доказать.

Равным образом можно предположить, что корень уравнения восьмой степени непредставим в виде суперпозиции функций трех аргументов; более того, имеются основания полагать, что приведенная выше нормальная форма уравнения восьмой степени является функцией четырех существенных аргументов u, v, w, p.

Тем более замечательным кажется мне то обстоятельство, что в силу стечения различных обстоятельств *общее уравнение девятой степени разрешимо в функциях только четырех аргументов*, так как пять коэффициентов u, v, w, p, q приведенной выше нормальной формы могут быть сведены к четырем и, следовательно, не являются существенными аргументами в нашем смысле.

Чтобы убедиться в этом, воспользуемся методом преобразования Чирнгаузена и получим для X уравнение следующего вида:

$$X^9 + U_1X^8 + U_2X^7 + \ldots + U_9 = 0,$$

где U_1, $U_2, \ldots$, U_9 — целые рациональные функции от $t_1, \ldots, t_8$.

Выразим с помощью линейного по $t_1, \ldots, t_8$ уравнения

$$U_1(t_1, \ldots, t_8) = 0$$

параметр t_8 через остальные параметры $t_1, \ldots, t_7$. Если полученное выражение для t_8 подставить в U_2, U_3, U_4, то эти выражения перейдут в выражения U_2', U_3', U_4' соответственно второй, третьей и четвертой степеней по $t_1, \ldots, t_7$. Представив затем U_2' в виде суммы квадратов восьми линейных функций $L_1, \ldots, L_8$ параметров $t_1, \ldots, t_7$,

$$U_2'(t_1, \ldots, t_7) = L_1^2 + L_2^2 + \ldots + L_8^2,$$

мы увидим, что уравнению

$$U_2'(t_1, \ldots, t_7) = 0$$

можно удовлетворить, положив

$$L_1 + iL_2 = 0, \qquad L_5 + iL_6 = 0,$$
$$L_3 + iL_4 = 0, \qquad L_7 + iL_8 = 0.$$

Это — четыре линейных уравнения относительно параметров $t_1, \ldots, t_7$. Они позволяют выразить t_4, t_5, t_6, t_7 через t_1, t_2, t_3 и, подставив полученные выражения, линейные по t_1, t_2, t_3, в U_3', U_4', получить кубическое и биквадратное по t_1, t_2, t_3 выражения

$$U_3''(t_1, t_2, t_3) \qquad \text{и} \qquad U_4''(t_1, t_2, t_3).$$

Естественно попытаться определить t_1, t_2, t_3 так, чтобы оба эти выражения обратились в нуль.

Для этого вспомним, что уравнение

$$U_3''(t_1, t_2, t_3) = 0$$

задает в трехмерном пространстве с координатами t_1, t_2, t_3 кубическую двумерную поверхность. На такой поверхности лежат 27 прямых. Чтобы найти их, необходимо решить уравнение 27-й степени с коэффициентами, рационально зависящими от коэффициентов уравнения $U_3'' = 0$.

Исследуем теперь, насколько можно уменьшить число коэффициентов уравнения $U_3'' = 0$. Как известно, целая рациональная функция третьей степени от трех переменных всегда представима в виде суммы пяти кубов:

$$U_3''(t_1, t_2, t_3) = M_1^3 + M_2^3 + M_3^3 + M_4^3 + M_5^3,$$

где M_1, M_2, M_3, M_4, M_5 — линейные функции от t_1, t_2, t_3. Это представление в существенном однозначно: кубы M_1^3, M_2^3, M_3^3, M_4^3, M_5^3 — корни уравнения пятой степени, коэффициенты которого рационально выражаются через коэффициенты кубической функции U_3''. Отсюда мы заключаем, что для представления кубов M_1^3, M_2^3, M_3^3, M_4^3, M_5^3 и тем самым линейных функций M_1, M_2, M_3, M_4, M_5 помимо операции взятия суммы требуются только функции *одного* аргумента. Если теперь вместо t_1, t_2, t_3 ввести в качестве новых переменных дробно-линейные выражения

$$m_1 = \frac{M_1}{M_4}, \qquad m_2 = \frac{M_2}{M_4}, \qquad m_3 = \frac{M_3}{M_4},$$

то из уравнения $U_3'' = 0$ мы получим уравнение вида

$$m_1^3 + m_2^3 + m_3^3 + 1 + (V_1 m_1 + V_2 m_2 + V_3 m_3 + V_4)^3 = 0,$$

коэффициенты которого содержат четыре параметра V_1, V_2, V_3, V_4. Отсюда следует, что если уравнения

$$t_1 = \rho_1 s + \sigma_1,$$

$$t_2 = \rho_2 s + \sigma_2,$$

$$t_3 = \rho_3 s + \sigma_3$$

с переменной s задают 27 прямых, лежащих на нашей поверхности $U_3'' = 0$, то коэффициенты ρ_1, ρ_2, ρ_3, σ_1, σ_2, σ_3 — также алгебраические функции тех же четырех параметров V_1, V_2, V_3, V_4.

Наконец, если в U_4'' вместо t_1, t_2, t_3 подставить приведенные выше линейные функции от s, то уравнение

$$U_4''(t_1, t_2, t_3) = 0$$

переходит в биквадратное уравнение

$$U_4'''(s) = 0$$

для s, для решения которого помимо операции взятия суммы требуются только функции одного аргумента.

Найденное преобразование Чирнгаузена позволяет также, если произвести в U_5, U_6, U_7, U_8, U_9 соответствующие подстановки, переводящие исходное уравнение девятой степени в уравнение вида

$$X^9 + U_5^* X^4 + U_6^* X^3 + U_7^* X^2 + U_8^* X + U_9^* = 0,$$

и, кроме того, воспользоваться подстановкой

$$X = \sqrt[9]{U_9^*}\, Y,$$

получить уравнение вида

$$Y^9 + W_1 Y^4 + W_2 Y^3 + W_3 Y^2 + W_4 Y + 1 = 0$$

в которое входят только четыре параметра W_1, W_2, W_3, W_4. Следовательно, *общее уравнение девятой степени разрешимо в алгебраических функциях четырех аргументов*, причем в их число наряду с функциями одной переменной и суммой входят еще две специальные функции четырех аргументов. Маловероятно, что для общего уравнения девятой степени число аргументов удастся понизить еще больше.

Аналогичная редукция числа аргументов существует и для уравнений более высокой степени.

Д. ГИЛЬБЕРТ

ГЕОМЕТРИЯ

О ВЕЩЕСТВЕННЫХ ВЕТВЯХ АЛГЕБРАИЧЕСКИХ КРИВЫХ*)

А. Гарнак[1)] доказал, что число вещественных ветвей плоской алгебраической кривой n-го порядка не превосходит $\frac{1}{2}(n-1)(n-2)+1$, и указал способ построения плоских кривых n-го порядка с $\frac{1}{2}(n-1)(n-2)+1$ вещественными ветвями. Так как никакая кривая с максимальным числом вещественных ветвей не имеет двойных точек, то никакая ее ветвь не может пересечь себя или другую ветвь, и потому, если n четно, такая кривая состоит только из парных ветвей [1]. Если n нечетно, то такая кривая имеет одну непарную ветвь; остальные ветви все парные.

Для того чтобы можно было ясно выделить существенные свойства парной и непарной ветвей[2)], мы возьмем трехмерные однородные координаты x_1, x_2, x_3 в качестве координат точек пространства в прямоугольной системе координат, так что каждой точке исходной плоскости будет соответствовать прямая, проходящая через начальную точку O, а каждой ветви плоской кривой — конус, вершина которого находится в начальной точке O. Такой конус делит пространство на две или три области. В *первом* случае любую проходящую через начальную точку O прямую можно перевести, вращая ее вокруг O, в любую другую проходящую через O прямую, не выходя из конуса, т. е. без совмещения этой прямой с образующей конуса. Тогда конус и соответствующая ветвь называются непарными. Во *втором* случае две пространственные области составляют пару вертикальных областей, поскольку все прямые, которые заполняют первую область, при продолжении попадают во вторую область. Тогда конус и соответствующая ветвь кривой называются парными. Обе связанные так пространственные области и соответствующая область плоскости составляют *внутренности* конуса и кривой. Все остальные проходящие через O прямые заполняют третью пространственную область. Она и соответствующая ей область плоскости называются *внешними* областями. Две непарные ветви пересекаются в нечетном числе точек; две парные ветви, как и одна непарная и одна парная ветви, пересекаются в четном числе точек. Каждая непарная ветвь, проходящая через внутренность парной ветви, пересекает парную ветвь по меньшей мере в двух точках.

Согласно приведенным выше рассуждениям, внутренность и внешность парной ветви различаются вполне определенным образом, и потому если задана кривая с несколькими ветвями, то мы можем для каждой парной ветви

---

*) Über die reellen Züge algebraisher Kurven. — Math. Ann., 1891, Bd. 38, S. 115–138. *Перевод Харламова В. М. и Харламовой С. А.*

1) *Harnak A.* — Math. Ann., Bd. 10, S. 189.

2) Ср. *Möbius A.* Über die Grundformen der Linien der dritten Ordnung. — Ges. Werke, Bd. 2. — Leipzig, 1886, S. 89, и *von Staudt K.* Geometrie der Lage. — Nürnberg, 1847, S. 81.

указать, какие ветви лежат вне или внутри нее, а какие охватывают ее. При этом, что касается различных возможностей, то прежде всего необходимо рассмотреть крайние случаи расположения ветвей; поэтому ниже мы исследуем вопрос, каково наибольшее число ветвей у кривой с максимальным числом вещественных ветвей, которые вложены друг в друга, т. е. сколько ветвей могут располагаться таким образом, что первая ветвь полностью лежит внутри второй, вторая — внутри третьей и т. д. [2]

Легко показать, *что для четного* n (>4) *описанным выше образом вложено, самое большее,* $n/2-1$ *ветвей.* [3] Если бы имелось $n/2$ вложенных ветвей, то можно было бы взять на одной из остальных ветвей произвольную точку A и соединить прямой эту точку A с точкой самой внутренней ветви. Так как эта прямая пересекала бы ветвь, на которой лежит A, и, кроме того, каждую из $n/2$ вложенных ветвей по меньшей мере в двух точках, то она имела бы с кривой в совокупности не менее $n+2$ общих точек, что невозможно.

Если предположить, что кривая четного порядка n с максимальным числом вещественных ветвей имеет $n/2-1$ ветвей, вложенных друг в друга описанным выше способом, то легко убедиться, что все остальные $\frac{1}{2}(n^2-4n+6)$ ее ветвей расположены вне друг друга. Если бы одна из этих остальных ветвей охватывала другую, то прямая, соединяющая точку последней с точкой самой внутренней ветви [4], имела бы не меньше $n+2$ общих точек с кривой, а это невозможно. Напротив, ничто не мешает тому, чтобы остальные $\frac{1}{2}(n^2-4n+6)$ ветвей различными способами распределялись в кольцевых областях, которые образованы $n/2-1$ вложенными ветвями [5].

Если n нечетно, то кривая имеет непарную ветвь и, *самое большее,* $\frac{1}{2}(n-3)$ *парных ветвей кривой вложены друг в друга* [6]. Если бы имелось $\frac{1}{2}(n-1)$ вложенных ветвей, то можно было бы взять на одной из остальных ветвей произвольную точку и соединить прямой эту точку с точкой самой внутренней ветви. Так как эта прямая обязательно пересекла бы еще и непарную ветвь кривой по меньшей мере в одной точке, то она имела бы с кривой не менее $n+2$ общих точек, что невозможно. Остальные $\frac{1}{2}(n^2-4n+7)$ ветвей, как и раньше, расположены вне друг друга.

Теперь мы докажем, *что кривые описанного выше вида действительно существуют.* Для этого предположим, что $f=0$ — уравнение кривой порядка n с максимальным числом вещественных ветвей, среди которых, в зависимости от того, четно или нечетно n, $n/2-1$ ветвей $Z_1, Z_2, \ldots$ $\ldots, Z_{n/2-1}$, соответственно $\frac{1}{2}(n-3)$ ветвей $Z_1, Z_2, \ldots, Z_{\frac{1}{2}(n-3)}$, требуемым образом вложены друг в друга. Пусть, кроме того, дан эллипс $k=0$, который или охватывает самую внешнюю ветвь $Z_{n/2-1}$, соответственно $Z_{\frac{1}{2}(n-3)}$, или полностью лежит в самой внутренней ветви Z_1, или, более общим образом, охватывает ветвь Z_ν и одновременно лежит внутри ветви $Z_{\nu+1}$, где ν — одно из чисел $1, 2, \ldots, \frac{1}{2}(n-4)$, соответственно $1, 2, \ldots, \frac{1}{2}(n-5)$. Пусть этот эллипс $k=0$ пересекает одну из остальных $\frac{1}{2}(n^2-4n+6)$, соответственно $\frac{1}{2}(n^2-4n+7)$, ветвей в $2n$ точках $A_1, A_2, \ldots, A_{2n}$ именно таким образом, что последние как точки эллипса следуют друг за другом в таком же порядке,

как на кривой. Выберем теперь на эллипсе между какими-нибудь двумя из этих точек , например между A_1 и A_2, произвольным образом $2n+4$ точек $B_1, B_2, \ldots, B_{2n+4}$ и соединим прямыми B_1 с B_2, B_3 с B_4, ..., B_{2n+3} с B_{2n+4}. Перемножим левые части уравнений этих прямых и обозначим через g полученное произведение, которое является тернарной формой порядка $n+2$. Если теперь придать величине δ достаточно малое значение, то при подходящим образом выбранном знаке

$$fk \pm \delta g = 0$$

является уравнением кривой порядка $n+2$, которая имеет

$$\frac{1}{2}(n-1)(n-2)+1+(2n-1)=\frac{1}{2}(n+1)n+1$$

ветвей, т. е. она имеет максимальное число ветвей, причем среди них на самом деле $n/2$, соответственно $\frac{1}{2}(n-1)$, ветвей вложены друг в друга. Дело в том, что каждая из вложенных ветвей $Z_1, Z_2, \ldots, Z_{n/2-1}$, соответственно $Z_1, Z_2, \ldots, Z_{\frac{1}{2}(n-3)}$, приводит к близко расположенной ветви новой кривой. Обозначим так возникшие ветви новой кривой через $Z'_1, Z'_2, \ldots, Z'_{n/2-1}$, соответственно $Z'_1, Z'_2, \ldots, Z'_{\frac{1}{2}(n-3)}$. Одновременно из эллипса $k=0$ возникает особая ветвь Z', которая или охватывает эллипс снаружи, или прижимается к нему изнутри, причем так, что эллипс вложен или между ветвями Z'_ν и Z', или между ветвями Z' и $Z'_{\nu+1}$. Эллипс $k=0$ пересекает одну из возникших ветвей в $2n+4$ точках $B_1, B_2, \ldots, B_{2n+4}$, причем именно так, что порядок следования этих точек пересечения на эллипсе и на ветви кривой один и тот же. Таким образом, мы доказали, что эллипс $k=0$ занимает относительно возникшей кривой порядка $n+2$ точно такое же положение, как и относительно первоначальной кривой порядка n. Поэтому описанный метод можно применить снова, и на каждом новом шаге мы получаем новую кривую с требуемыми свойствами, порядок которой больше на два. Поскольку, как легко доказать, для низких порядков кривые с требуемыми свойствами существуют, то они существуют и в общем случае [7].

Указанным методом мы пришли в случаях $n=6$, $n=7$, $n=8$ к следующим кривым с упомянутым выше свойством:

$n=6$.[3)]

1. Ветвь Z, внутри нее еще одна ветвь, а снаружи ветви Z 9 ветвей, расположенных вне друг друга.

2. Ветвь Z, внутри нее 9 ветвей, расположенных вне друг друга, а снаружи ветви Z одна ветвь.

[3)] [Примечание из собр. соч. Д. Гильберта 1930 г.] Я подверг этот случай $n=6$ дальнейшему подробному исследованию; при этом я нашел, — правда, чрезвычайно сложным путем — что одиннадцать ветвей кривой 6-го порядка никогда не могут располагаться все вне друг друга. Этот результат мне кажется интересным, потому что оказывается, что для кривых с максимальным числом ветвей топологически простейший случай не всегда возможен [8]. Одновременно из упомянутого обстоятельства следует, что поверхности 4-го порядка с двенадцатью компонентами *не* может существовать; ср. конкурсную работу К. Роона: *Rohn K.* Die Flächen 4-ter Ordnung hinsichtlich ihrer Knotenpunkte und ihrer Gestaltung, S. 42, где число 12 указано как верхняя граница числа компонент; см. также статью «О форме поверхности четвертого порядка» [имеется перевод на с. 386–389 настоящего издания. — *Ред.*].

$n = 7$.

1. Ветвь Z, внутри нее 2 ветви, расположенные вне друг друга, а снаружи ветви Z 12 парных ветвей, лежащих вне друг друга, и одна непарная ветвь.

2. Ветвь Z, внутри нее 12 ветвей, лежащих вне друг друга, а снаружи ветви Z 2 парные ветви и одна непарная ветвь.

3. Ветвь Z, внутри нее 3 ветви, расположенные вне друг друга, а снаружи ветви Z 11 парных ветвей и одна непарная ветвь.

4. Ветвь Z, внутри нее 13 ветвей, расположенных вне друг друга, а снаружи ветви Z одна парная и одна непарная ветви.

$n = 8$.

1. Ветвь Z_1, внутри нее одна ветвь, а снаружи две ветви, лежащих вне друг друга; эти две последние вместе с ветвью Z_1 охвачены ветвью Z_2, а снаружи ветви Z_2 17 ветвей, расположенных вне друг друга.

2. Ветвь Z_1, внутри нее 17 ветвей, лежащих вне друг друга, снаружи ветви Z_1 две ветви, расположенные вне друг друга, причем две последние вместе с ветвью Z_1 охвачены ветвью Z_2; снаружи ветви Z_2 одна ветвь.

3. Ветвь Z_1, внутри нее одна ветвь, а снаружи ветви Z_1 14 ветвей, лежащих вне друг друга, и эти последние 14 ветвей вместе с ветвью Z_1 охвачены ветвью Z_2; снаружи ветви Z_2 5 ветвей, расположенных вне друг друга.

4. Ветвь Z_1, внутри нее 5 ветвей, расположенных вне друг друга, а снаружи ветви Z_1 14 ветвей; эти 14 ветвей вместе с ветвью Z_1 охвачены ветвью Z_2, а снаружи ветви Z_2 одна ветвь [9].

Вопрос о максимальном числе вещественных ветвей допускает полное решение также для алгебраических пространственных кривых.

Мы исследуем прежде всего, из какого числа ветвей может состоять неприводимая пространственная кривая порядка n. Альфан[4] и М. Нётер[5] показали, что неприводимая неплоская кривая порядка n максимального рода обязательно лежит на поверхности порядка 2. Этот максимальный род равен $\frac{1}{4}(n-2)^2$ или соответственно $\frac{1}{4}(n-1)(n-3)$, в зависимости от того, четно n или нечетно. Пусть теперь задана неплоская кривая порядка n с максимальным числом вещественных ветвей; если мы спроектируем ее из какой-нибудь точки на плоскость, то каждой ветви пространственной кривой будет соответствовать ветвь плоской кривой и род пространственной кривой совпадает с родом плоской кривой. Число вещественных ветвей произвольной плоской кривой, как также доказал А. Гарнак в цитированной выше работе [10], не превосходит рода кривой, увеличенного на 1, и потому число ветвей проекции и, следовательно, также число ветвей исходной кривой не больше $\frac{1}{4}(n-2)^2+1$ или соответственно $\frac{1}{4}(n-1)(n-3)+1$, в зависимости от того четно n или нечетно. Одновременно получается, что любая неплоская кривая порядка n, которая имеет в точности $\frac{1}{4}(n-2)^2+1$, соответственно $\frac{1}{4}(n-1)(n-3)+1$, ветвей, обязательно лежит на поверхности порядка 2.

---

[4] *Halphen G.* — Bull. Soc. Franc. Math., vol. 2, p. 42.

[5] *Noether M.* Zur Grundlegung der Theorie der algebraischen Raumkurven. — Crelles J., Bd. 93, S. 293.

Теперь мы покажем, что найденная выше верхняя граница для числа ветвей действительно достигается. Для этого мы предположим, что кривая C_n четного порядка n задана как пересечение однополостного гиперболоида $H = 0$ и поверхности $F = 0$ порядка $n/2$ и что эта кривая C_n имеет максимальное число $\frac{1}{4}(n-2)^2 + 1$ вещественных ветвей. Кроме того, пусть плоскость $E = 0$ высекает на гиперболоиде $H = 0$ эллипс, который пересекает одну из ветвей кривой C_n последовательно в точках $A_1, A_2, \ldots, A_n$. На этом эллипсе между точками A_1 и A_2 мы выберем произвольно $n+2$ точек $B_1, B_2, \ldots, B_{n+2}$ и построим $\frac{1}{2}(n+2)$ плоскостей, из которых первая проходит через B_1 и B_2, вторая — через B_3 и B_4, ..., $\frac{1}{2}(n+2)$-я — через B_{n+1} и B_{n+2}; ни одна из этих плоскостей не должна совпадать с плоскостью $E = 0$. Произведение левых частей уравнений этих $\frac{1}{2}(n+2)$ плоскостей является кватернарной формой G порядка $\frac{1}{2}(n+2)$. Если величине δ придать достаточно малое значение, то при подходящим образом выбранном знаке

$$FE \pm \delta G = 0$$

является уравнением поверхности порядка $\frac{1}{2}(n+2)$, которая высекает на гиперболоиде $H = 0$ пространственную кривую C_{n+2} порядка $n+2$ с

$$\frac{1}{4}(n-2)^2 + 1 + (n-1) = \frac{1}{4}n^2 + 1$$

вещественными ветвями; дело в том, что таким методом из каждой ветви кривой C_n возникает ветвь кривой C_{n+2}, а эллипс вместе с пересекающей его в n точках ветвью кривой C_n приводит к n новым ветвям кривой C_{n+2}. Полученное число ветвей максимальное. Кроме того, одна из n возникших ветвей пересекает эллипс $E = 0$ последовательно в $n+2$ точках $B_1, B_2, \ldots$ $\ldots, B_{n+2}$, так что примененный выше к C_n метод применим также к возникшей кривой C_{n+2}. Так как для $n = 2$ максимальное число равно 1, то для описанного выше метода в качестве исходного шага можно взять произвольный эллипс на гиперболоиде $H = 0$, и тогда переходом от n к $n+2$ мы получаем для каждого четного порядка n существование пространственных кривых с $\frac{1}{4}(n-2)^2 + 1$ вещественными ветвями [11].

Для того чтобы доказать аналогичное утверждение для кривых нечетного порядка n, мы предположим, что поверхность $F = 0$ порядка $\frac{1}{2}(n+1)$ пересекает однополостный гиперболоид $H = 0$ по вспомогательной прямой L и по кривой C_n порядка n, которая имеет $\frac{1}{4}(n-1)(n-3)+1$ ветвей. Пусть, кроме того, плоскость $E = 0$ высекает на гиперболоиде $H = 0$ эллипс, который пересекает одну из ветвей кривой C_n в n точках $A_1, A_2, \ldots, A_n$. Пусть все эти точки лежат на расположенной в конечной области части ветви, причем при пробегании этого конечного куска точки встречаются именно в указанной последовательности. Пусть вспомогательная прямая L пересекает эллипс в точке A и положение точки A на эллипсе таково, что при пробегании эллипса точки $A, A_1, A_2, \ldots, A_n$ следуют по очереди друг за другом. Теперь произвольным образом выберем на эллипсе $n+2$ точек $B_1, B_2, \ldots, B_{n+2}$ между точками A и A_1 и построим плоскость, которая проходит через прямую L и через точку B_1, а затем построим еще $\frac{1}{2}(n+1)$

плоскостей, первая из которых проходит через B_2 и B_3, вторая — через B_4 и B_5, а $\frac{1}{2}(n+1)$-я — через B_{n+1} и B_{n+2}. Обозначим произведение левых частей уравнений этих $\frac{1}{2}(n+3)$ плоскостей через G. Если мы придадим величине δ достаточно малое значение, то при подходящем выборе знака

$$FE \pm \delta G = 0$$

является уравнением поверхности порядка $\frac{1}{2}(n+3)$, которая высекает на гиперболоиде $H=0$ прямую L и, кроме того, пространственную кривую C_{n+2} порядка $n+2$ с

$$\frac{1}{4}(n-1)(n-3)+1+(n-1)=\frac{1}{4}(n+1)(n-1)+1$$

ветвями, т. е. с максимальным числом ветвей. Кроме того, одна из этих ветвей пересекает эллипс $E=0$ в $n+2$ точках $B_1, B_2, \ldots, B_{n+2}$. Эти последние опять все лежат на куске кривой, целиком расположенном в конечной области, и если при пробегании этого конечного куска кривой указанные точки встречаются в порядке $B_1, B_2, \ldots, B_{n+2}$, то порядок следования точек на эллипсе есть $A, B_1, B_2, \ldots, B_{n+2}$. Поэтому метод, примененный выше к C_n, будет применим и к возникающей кривой C_{n+2}. Так как для $n=1$ максимальное число равно 1, то для описанного выше метода в качестве исходной может служить любая прямая гиперболоида $H=0$, и тогда, если в качестве вспомогательной прямой L взять прямую из другого семейства образующих гиперболоида, то переходом от произвольного n к $n+2$ устанавливается, что существуют пространственные кривые нечетного порядка n с $\frac{1}{4}(n-1)(n-3)+1$ ветвями. На основании этого мы высказываем такую теорему.

Число вещественных ветвей неприводимой пространственной кривой порядка n не превосходит $\frac{1}{4}(n-2)^2+1$, соответственно $\frac{1}{4}(n-1)(n-3)+1$, в зависимости от того четно n или нечетно, и в обоих случаях существуют пространственные кривые, которые действительно состоят из такого числа ветвей [12].

Мы исследуем теперь положение и форму пространственных кривых с максимальным числом вещественных ветвей. Согласно изложенному выше, такие кривые лежат на поверхности второго порядка, а тогда невозможно, чтобы какая-нибудь ветвь этой кривой была зацеплена за какую-нибудь из остальных ветвей. Напротив, ветви пространственной кривой все разделены в пространстве таким образом, что каждую ветвь можно стянуть в точку непрерывным изменением, не пересекая при этом ни одну из других ветвей [13]. Однако с этим очень хорошо совмещается тот факт, что одна из ветвей кривой на поверхности второго порядка охватывает какую-то из других ветвей, и в общем случае для данного порядка n кривой на поверхности второго порядка возможны различные группировки ветвей.

Далее мы легко убедимся, что пространственная кривая с максимальным числом вещественных ветвей не может иметь никаких настоящих (wirklichen) [14] двойных точек. А именно, если мы предположим противное и вне пространственной кривой на поверхности второго порядка, несущей эту кривую, так выберем точку P, что никакая из двух пересекающихся

в этой точке прямых поверхности не проходит через двойную точку кривой, то проекция пространственной кривой из этой точки даст плоскую кривую порядка n, которая имеет обычную двойную точку и, кроме того, одну n_1-кратную и одну n_2-кратную точки, причем $n_1 + n_2 = n$. Следовательно, род этой плоской кривой должен быть меньше, чем $\frac{1}{4}(n-2)^2$, соответственно $\frac{1}{4}(n-1)(n-3)$. Но так как число ветвей кривой не больше чем на 1 превосходит ее род, то эта плоская кривая имеет не больше, чем $\frac{1}{4}(n-2)^2$, соответственно $\frac{1}{4}(n-1)(n-3)$, ветвей, и то же самое верно тогда для исходной пространственной кривой. Это противоречит нашему предположению о том, что пространственная кривая имеет максимальное число вещественных ветвей. Одновременно это рассуждение позволяет узнать значения чисел n_1 и n_2. Так как спроектированная плоская кривая обязательно имеет род $\frac{1}{4}(n-2)^2$, соответственно $\frac{1}{4}(n-1)(n-3)$, то получаем $n_1 = n/2$, $n_2 = n/2$, соответственно $n_1 = \frac{1}{2}(n+1)$, $n_2 = \frac{1}{2}(n-1)$, в зависимости от того, четно n или нечетно.

Как мы видим, построенные выше пространственные кривые с максимальным числом вещественных ветвей не имеют ни одной или имеют ровно одну непарную ветвь, в зависимости от того, четно n или нечетно. Возникает следующий вопрос (так же, как и для плоских кривых): исключает ли требование максимальности числа вещественных ветвей появление *нескольких* непарных ветвей или помимо построенных выше пространственных кривых имеются еще другие виды пространственных кривых с максимальным числом ветвей?

Для того чтобы определить верхнюю границу для числа непарных ветвей пространственной кривой порядка n с максимальным числом вещественных ветвей, мы прежде всего спроектируем, как выше, пространственную кривую из точки P квадратичной поверхности на плоскость: сама точка P не должна лежать на рассматриваемой пространственной кривой. Возникающая плоская кривая порядка n имеет две $n/2$-кратные или одну $\frac{1}{2}(n+1)$-кратную и одну $\frac{1}{2}(n-1)$-кратную точки, в зависимости от того, четно n или нечетно. Мы обозначим эти две точки через A и B. Помимо этих двух особенностей указанная плоская кривая, как было показано выше, не имеет никаких кратных точек. Каждой непарной ветви пространственной кривой соответствует также непарная ветвь плоской кривой и наоборот. В самом деле, если проведена плоскость через точку — центр проекции — и если эта плоскость пересекает ветвь пространственной кривой в нечетном числе точек, то определенная этой плоскостью прямая пересекает соответствующую ветвь плоской кривой в том же самом нечетном числе точек. Итак, мы возвращаемся к исследованию плоской кривой, образованной проектированием.

Мы легко докажем, что плоская кривая может иметь не больше *одной* непарной ветви, которая проходит через каждую из точек A и B нечетное число раз. Действительно, предположим, что имеются две такие ветви, и если мы примем во внимание, что эти две непарные ветви нигде, кроме точек A и B, друг с другом не пересекаются, то получится, что в конечном счете эти непарные ветви пересекаются друг с другом четное число раз, что невозможно [15]. Аналогичным образом устанавливается, что при наличии нескольких непарных ветвей ни одна из них не может проходить

четное число раз как через A, так и через B. Следовательно, если плоская кривая имеет несколько непарных ветвей, то среди них всегда существует непарная ветвь Z, которая проходит через одну из двух особых точек, например через A, нечетное число раз, а через другую особую точку B четное число раз. Но тогда остальные непарные ветви кривой обязательно также должны проходить через указанную точку A нечетное число раз, а через точку B четное число раз — за исключением, разве что, одной непарной ветви, которая проходит через каждую из точек A и B нечетное число раз. Действительно, если бы существовала непарная ветвь, которая пересекала бы A четное, а B нечетное число раз, то эта непарная ветвь должна была бы пересечь непарную ветвь Z в четном числе точек, а это невозможно.

Предыдущие рассуждения показывают, что каждая непарная ветвь проходит через одну из особых точек, например через A, нечетное число раз, а следовательно, по меньшей мере один раз. Так как сейчас A — это $n/2$-кратная, соответственно $\frac{1}{2}(n \pm 1)$-кратная точка, в зависимости от того четно n или нечетно, то во всяком случае кривая не может иметь больше, чем $n/2$, соответственно $\frac{1}{2}(n+1)$, непарных ветвей. Однако, как показывается ниже, эта верхняя граница для числа непарных ветвей не достигается.

Во-первых, положим $n = 4\nu$, где ν обозначает целое число, и предположим, что существует кривая порядка n с максимальным числом ветвей, для которой A и B являются 2ν-кратными точками; пусть 2ν ветвей этой кривой непарные и каждая из них один раз проходит через точку A. Согласно изложенному выше, среди 2ν непарных ветвей могла бы существовать, самое большее, одна ветвь, которая проходит через точку B нечетное число раз. Так как точка B является 2ν-кратной точкой кривой, то кроме этих непарных ветвей еще нечетное число вещественных локальных ветвей данной кривой проходит через точку B. Остальные непарные ветви кривой все пробегают через B четное число раз, и поэтому должна была бы существовать по меньшей мере одна парная ветвь, которая проходит через B нечетное число раз. Эта парная ветвь не может пробегать также через A, потому что в A уже пересекаются 2ν непарных ветвей. Так как парная ветвь кроме точек A и B нигде не может пересечь другую ветвь, то она должна была бы пересечь нечетное число раз ту непарную ветвь, которая пробегает через B нечетное число раз, а это невозможно. Тем самым доказано, что каждая из 2ν непарных ветвей пробегает через B четное число раз. Предположим теперь, что $n > 4$; тогда кроме 2ν непарных ветвей существует по крайней мере одна парная ветвь. Мы проведем из произвольной точки парной ветви кривой прямую к точке B. Так как эта прямая пересекает в B каждую из непарных ветвей четное число раз, то, следовательно, она должна помимо точки B встретить каждую из непарных ветвей еще в нечетном числе точек, т. е. каждую по меньшей мере в одной точке. Ну а B является 2ν-кратной точкой кривой, и, следовательно, указанная прямая имела бы с кривой по меньшей мере $4\nu + 1$ общих точек. Этот вывод противоречит предполагаемой неприводимости кривой. Поэтому кривая не может иметь 2ν непарных ветвей, а так как кривая четного порядка должна иметь и четное число непарных ветвей, то, следовательно, наша плоская кривая, а значит, также и первоначально рассмотренная пространственная кривая порядка $n = 4\nu$ с максимальным числом вещественных ветвей может иметь не больше чем $2\nu - 2$ непарных ветвей. Исключением является кривая 4-го

порядка, для которой предположение допускает две непарные ветви.

Во-вторых, положим $n = 4\nu + 2$ и покажем, что в этом случае наша кривая не может иметь ни одной непарной ветви. Ведь, согласно предыдущим рассуждениям, каждая из имеющихся непарных ветвей должна была бы пройти через одну из двух особых точек, например, через A, нечетное число раз. В рассматриваемом случае число всех непарных ветвей обязательно четно, и так как A является $2\nu+1$-кратной точкой кривой, то должна была бы существовать по меньшей мере одна парная ветвь Z, которая проходит через точку A нечетное число раз. С другой стороны, не больше, чем *одна* непарная ветвь может пробегать также через B нечетное число раз, и вследствие этого, во всяком случае, должна была бы существовать одна непарная ветвь, которая пробегает через B четное число раз. Эта непарная ветвь пересекала бы указанную парную ветвь Z нечетное число раз, а это невозможно.

Пусть, *в-третьих*, $n = 4\nu + 1$; найденная ранее для числа непарных ветвей верхняя граница в этом случае равна $2\nu + 1$. Эта граница опять не достигается. Чтобы это понять, мы предположим что имеется кривая с максимальным числом ветвей; пусть $2\nu+1$ из этих ветвей непарные и пробегают по разу $2\nu+1$-кратную точку A. Не больше чем одна из этих $2\nu+1$ непарных ветвей может проходить также через B нечетное число раз. Но поскольку B является 2ν-кратной точкой кривой, в этом случае должна была бы существовать по меньшей мере *одна* парная ветвь, которая пересекала бы B нечетное число раз. Эта парная ветвь не может пробегать через A, так как в точке A уже пересекаются $2\nu + 1$ локальных ветвей кривой; следовательно, она должна была бы нечетное число раз пересекать ту непарную ветвь, которая проходит через B нечетное число раз. Это невозможно, и тем самым доказано, что никакая из $2\nu + 1$ непарных ветвей не может проходить через B нечетное число раз. Если $n > 5$, то кроме $2\nu + 1$ непарных ветвей существует еще парная ветвь, и, как в первом случае, легко понять, что проведенная через B и произвольную точку этой парной ветви прямая имела бы с кривой более чем n общих точек. Итак, кривая не может иметь $2\nu + 1$ непарных ветвей, а так как кривая нечетного порядка обязательно имеет нечетное число непарных ветвей, то, следовательно, пространственная кривая порядка $n = 4\nu+1$ с максимальным числом вещественных ветвей может иметь не более чем $2\nu - 1$ непарных ветвей. Исключением является кривая 5-го порядка, для которой предположение допускает три непарные ветви.

Наконец, *в-четвертых*, положим $n = 4\nu + 3$. Тогда, согласно предыдущим рассуждениям, кривая может иметь не более чем $2\nu + 2$, а так как она нечетного порядка, то не более чем $2\nu+1$ непарных ветвей. Это число также не достигается. Мы предположим, что существует кривая требуемого вида с $2\nu + 1$ непарными ветвями, и будем различать случаи, когда каждая из этих непарных ветвей пробегает один раз через $2\nu+2$-кратную точку A и когда — через $2\nu + 1$-кратную точку B. В первом случае, кроме того, должна была бы существовать еще парная ветвь Z кривой, которая один раз проходит через точку A. При $n > 3$ имеем $2\nu + 1 > 1$ и поэтому существует во всяком случае одна непарная ветвь, которая пробегает через B четное число раз. Эта непарная ветвь пересекала бы указанную парную ветвь Z нечетное число раз, что невозможно. Если же мы предположим, что все $2\nu + 1$ непарных ветвей по разу проходят через $2\nu + 1$-кратную точку B,

то, прежде всего, как легко понять, исключается возможность, что одна из этих непарных ветвей также проходит через A нечетное число раз. Тогда если опять принять, что $n > 3$, то наша кривая имеет во всяком случае еще одну парную ветвь, и мы получаем так же, как выше при обсуждении случаев $n = 4\nu$ и $n = 4\nu + 1$, что проведенная через A и произвольную точку парной ветви прямая имела бы с кривой более чем n общих точек, что невозможно. Следовательно, пространственная кривая порядка $n = 4\nu + 3$ с максимальным числом вещественных ветвей может иметь не более чем $2\nu - 1$ непарных ветвей. Исключением является кривая 3-го порядка; она состоит из одной непарной ветви.

Мы резюмируем полученные результаты следующим образом:

Неприводимая пространственная кривая порядка n с максимальным числом вещественных ветвей при $n = 4\nu, 4\nu + 1, 4\nu + 3$ имеет соответственно не более чем $2\nu - 2, 2\nu - 1, 2\nu - 1$ непарных ветвей. В случае $n = 4\nu + 2$ все ветви обязательно парные. Исключением являются кривые порядков 3, 4 и 5, для которых допускается предположение об 1, 2 и 3 непарных ветвях соответственно.

Ниже доказывается, что высказанные в этой теореме ограничения на число непарных ветвей являются также достаточными, т. е. если выбрать четное или нечетное число, не превышающее найденных границ, то всегда существуют пространственные кривые четного или соответственно нечетного порядка с максимальным числом вещественных ветвей и с тем самым выбранным числом непарных ветвей. Это доказательство составляет наиболее трудную часть нашей работы.

Прежде всего необходимо построить пространственную кривую 4-го порядка с двумя непарными ветвями. Для этого мы возьмем на однополостном гиперболоиде $H = 0$ две пары прямых, из которых одна пара L, M принадлежит одному семейству образующих, а другая пара L', M' — другому семейству. Затем мы проведем как через прямые L и L', так и через прямые L и M' по одной плоскости и обозначим через P произведение левых частей уравнений этих двух плоскостей. Тогда квадратичная форма P в одной части поверхности гиперболоида, ограниченной прямыми L' и M', всегда будет нулевой или положительной, а в другой — нулевой или отрицательной. Затем мы проведем через прямые M и L' и через прямые M и M' по плоскости и возьмем произведение Q левых частей уравнений обеих плоскостей. Поскольку полученная таким образом квадратичная форма Q может изменять свой знак на гиперболоиде только при переходе через прямые L' и M', то при подходящем выборе знака $P \pm Q$ является квадратичной формой, которая обращается в нуль на L' и M', а во всех других точках гиперболоида имеет отличное от нуля значение. Поэтому если мы обозначим через G произвольную кватернарную квадратичную форму, то для достаточно малых значений δ

$$F = P \pm Q + \delta G = 0$$

будет уравнением квадратичной поверхности, которая высекает из гиперболоида неприводимую кривую C_4 порядка 4 с двумя непарными ветвями. В то же время ясно, что два семейства образующих гиперболоида ведут себя по-разному относительно ветвей кривой: прямые одного семейства или пересекают одну из двух ветвей в двух вещественных точках, или вообще

не пересекают кривую, а прямые другого семейства пересекают каждую из двух непарных ветвей в одной точке.

Построенная выше кривая C_4 4-го порядка имеет род 1, и потому координаты ее точек можно представить как эллиптические функции параметра t таким образом, что значения параметра t от 0 до ω дают все точки первой ветви, а значения параметра t от $i\omega'/2+0$ до $i\omega'/2+\omega$ — все точки другой ветви. При этом ω, ω' — вещественные величины и $\omega, i\omega'$ являются двумя периодами кривой[6]. Пусть параметр t нормирован таким образом, что сумма значений этого параметра для четырех точек пересечения кривой с какой-либо плоскостью равна $i\omega'/2$. По теореме Абеля сравнение

$$t_1+t_2+\ldots+t_{4m}\equiv\frac{mi\omega'}{2}, \qquad (\omega, i\omega')$$

является необходимым и достаточным условием того, чтобы поверхность порядка m могла высечь $4m$ точек $t_1, t_2, \ldots, t_{4m}$ на пространственной кривой C_4. Пусть L — прямая на гиперболоиде $H=0$, которая пересекает каждую из двух непарных ветвей кривой C_4 в одной вещественной точке. Пусть параметры этих двух точек суть λ_1 и $i\omega'/2+\lambda_2$, где λ_1 и λ_2 — вещественные величины. Пусть, далее, L' — образующая гиперболоида, которая принадлежит другому семейству и пересекает одну из непарных ветвей в двух точках $t=\lambda_1'$ и $t=\lambda_2'$, где λ_1' и λ_2' также вещественны. Для краткости положим

$$\tau=-\lambda_1-\lambda_2\equiv\lambda_1'+\lambda_2', \qquad (\omega).$$

Если мы проведем теперь через прямую L поверхность нечетного порядка m, то она пересечет нашу кривую C_4 еще в $4m-2$ других точках и, согласно цитированной теореме, для параметров $t_1, t_2, \ldots, t_{4m-2}$ этих точек имеет место соотношение

$$t_1+t_2+\ldots+t_{4m-2}\equiv\tau, \qquad (\omega, i\omega').$$

Обратно, если для нечетного числа m выполнено последнее условие, то всегда существует поверхность порядка m, которая содержит прямую L и высекает на кривой C_4 те самые $4m-2$ точек $t_1, t_2, \ldots, t_{4m-2}$. Действительно, если уравнение $G=0$ задает поверхность порядка m, которая на кривой C_4 высекает $4m$ точек $t_1, t_2, \ldots, t_{4m-2}, \lambda_1, i\omega'/2+\lambda_2$, то всегда возможно так определить кватернарную форму K порядка $m-2$, чтобы поверхность $G+KF=0$ имела с прямой L еще $m-1$ других общих точек и, следовательно, полностью содержала эту прямую.

Тем же образом проверяется, что если m — четное число, то условие

$$t_1+t_2+\ldots+t_{4m-2}\equiv-\tau, \qquad (\omega, i\omega')$$

является необходимым и достаточным для существования поверхности порядка m, которая содержит прямую L' и высекает на кривой C_4 еще $4m-2$ других точек $t_1, t_2, \ldots, t_{4m-2}$.

Постоянная τ, как легко выяснить, не зависит от конкретного выбора прямых L и L' из соответствующих семейств образующих. Поэтому установленное условие

$$t_1+t_2+\ldots+t_{4m-2}\equiv\pm\tau, \qquad (\omega, i\omega')$$

---

[6] Ср. *Clebsch A.* — *Lindemann F.* Vorlesungen über Geometrie, Bd. I, S. 610.

является вообще необходимым и достаточным для существования поверхности порядка m, которая на кривой C_4 высекает $4m-2$ точек $t_1, t_2, \ldots, t_{4m-2}$ и, кроме того, содержит произвольно заданную прямую одного, соответственно другого, семейства.

Напротив, постоянная τ изменит значение, если вместо гиперболоида $H=0$ взять, например, гиперболоид $H+F=0$, который также содержит кривую C_4, но не имеет общих образующих с гиперболоидом $H=0$. Вследствие этого обстоятельства мы можем считать, что постоянная τ не равна нулю и не является кратным периода ω.

После этих приготовлений мы перейдем к доказательству существования возможных видов пространственных кривых.

Во-первых, мы положим $n=4\nu$ и возьмем 8 вещественных величин $t_1^{(1)}, t_2^{(1)}, \ldots, t_8^{(1)}$, которые удовлетворяют условиям

$$t_1^{(1)} < 0 < t_2^{(1)} < t_3^{(1)} < \ldots < t_8^{(1)},$$
$$t_1^{(1)} + t_2^{(1)} + t_3^{(1)} + \ldots + t_8^{(1)} = 0.$$

Пусть, кроме того, $t=0$ — точка пространственной кривой C_4, лежащая в конечной области, и для большей наглядности предположим, что величины $t_1^{(1)}$ и $t_8^{(1)}$ настолько малы по абсолютной величине, что, в то время как параметр t растет от $t_1^{(1)}$ до $t_8^{(1)}$, соответствующая точка пробегает отрезок кривой C_4, полностью лежащий в конечной области. Затем возьмем 16 вещественных величин $t_1^{(2)}, t_2^{(2)}, \ldots, t_{16}^{(2)}$, которые удовлетворяют условиям

$$t_1^{(1)} < t_1^{(2)} < 0 < t_2^{(2)} < t_3^{(2)} < \ldots < t_{16}^{(2)} < t_2^{(1)},$$
$$t_1^{(2)} + t_2^{(2)} + t_3^{(2)} + \ldots + t_{16}^{(2)} = 0,$$

потом 24 вещественные величины $t_1^{(3)}, t_2^{(3)}, \ldots, t_{24}^{(3)}$, удовлетворяющие условиям

$$t_1^{(2)} < t_1^{(3)} < 0 < t_2^{(3)} < t_3^{(3)} < \ldots < t_{24}^{(3)} < t_2^{(2)},$$
$$t_1^{(3)} + t_2^{(3)} + t_3^{(3)} + \ldots + t_{24}^{(3)} = 0,$$

и т. д., пока не придем к системе из $8(\nu-1)$ величин

$$t_1^{(\nu-1)},\ t_2^{(\nu-1)},\ \ldots,\ t_{8(\nu-1)}^{(\nu-1)},$$

для которой выполнены условия

$$t_1^{(\nu-2)} < t_1^{(\nu-1)} < 0 < t_2^{(\nu-1)} < t_3^{(\nu-1)} < \ldots < t_{8(\nu-1)}^{(\nu-1)} < t_2^{(\nu-2)},$$
$$t_1^{(\nu-1)} + t_2^{(\nu-1)} + t_3^{(\nu-1)} + \ldots + t_{8(\nu-1)}^{(\nu-1)} = 0.$$

Согласно изложенному выше, значения $t_1^{(1)}, t_2^{(1)}, \ldots, t_8^{(1)}$ параметра t определяют на одной из двух непарных ветвей кривой C_4 такие 8 точек, которые могут быть высечены на ней поверхностью 2-го порядка. Пусть $G^{(1)}=0$ —

уравнение этой поверхности 2-го порядка. Тогда для достаточно малых значений $\delta^{(1)}$ уравнение

$$F^{(1)} = F + \delta^{(1)} G^{(1)} = 0$$

определяет квадратичную поверхность, пересечение которой с гиперболоидом $H = 0$ также является кривой 4-го порядка с двумя непарными ветвями. Одна из этих двух непарных ветвей пересекает соответствующую ветвь первоначальной кривой C_4 в 8 точках $t_1^{(1)}, t_2^{(1)}, \ldots, t_8^{(1)}$ таким образом, что при прохождении непарной ветви новой кривой эти самые 8 точек $t_1^{(1)}, t_2^{(1)}, \ldots$ $\ldots, t_8^{(1)}$ появляются в той же последовательности, что и при прохождении кривой C_4. Вторая ветвь возникшей кривой располагается вдоль соответствующей ветви первоначальной кривой, не пересекая ее. Пусть теперь $G^{(2)} = 0$ — уравнение поверхности 4-го порядка, которая высекает 16 точек $t_1^{(2)}, t_2^{(2)}, \ldots, t_{16}^{(2)}$ на первоначальной кривой C_4. Тогда уравнение

$$F^{(2)} = FF^{(1)} \pm \delta^{(2)} G^{(2)} = 0$$

при надлежаще выбранном знаке и для достаточно малых значений $\delta^{(2)}$ дает поверхность 4-го порядка, высекающую на гиперболоиде $H = 0$ кривую 8-го порядка с двумя непарными и восьмью парными ветвями, потому что из четырех непарных ветвей, определенных уравнениями $F = 0$ и $F^{(1)} = 0$, при указанной вариации остаются непарными только две взаимно непересекающиеся непарные ветви, в то время как бесконечные части двух других непарных ветвей дают единственную парную ветвь, уходящую на бесконечность. Все остальные возникшие семь парных ветвей располагаются в конечной части пространства. Среди них имеется одна, которая пересекает одну из непарных ветвей кривой C_4 в 16 точках $t_1^{(2)}, t_2^{(2)}, \ldots, t_{16}^{(2)}$, причем так, что при пробегании указанной парной ветви эти 16 точек появляются в такой же последовательности $t_1^{(2)}, t_2^{(2)}, \ldots, t_{16}^{(2)}$, как и при пробегании непарной ветви кривой C_4. Далее, если $G^{(3)} = 0$ — уравнение поверхности 6-го порядка, высекающей 24 точки $t_1^{(3)}, t_2^{(3)}, \ldots, t_{24}^{(3)}$ на первоначальной кривой C_4, то

$$F^{(3)} = FF^{(2)} \pm \delta^{(3)} G^{(3)} = 0$$

при надлежаще выбранном знаке и для достаточно малых значений $\delta^{(3)}$ является уравнением поверхности 6-го порядка, высекающей на гиперболоиде $H = 0$ кривую 12-го порядка с четырьмя непарными и $8 + 14 = 22$ парными ветвями, потому что одна из непарных ветвей кривой C_4 и пересекаемая ею в 16 точках парная ветвь вместе дают одну непарную ветвь и 15 парных ветвей. Одна из этих 15 парных ветвей пересекает одну из непарных ветвей первоначальной кривой C_4 в 24 последовательных точках $t_1^{(3)}, t_2^{(3)}, \ldots, t_{24}^{(3)}$. Продолжая таким образом, мы получим на следующем шаге поверхность 8-го порядка $F^{(4)}$, которая высекает на гиперболоиде $H = 0$ кривую 16-го порядка с шестью непарными и $8 + 14 + 22 = 44$ парными ветвями. Видно, что с каждым следующим шагом к имеющимся добавляются еще две непарные ветви, в то время как увеличение числа парных ветвей оказывается на 8 большим, чем при предыдущем шаге. Следовательно, мы дойдем через

$\mu - 1$ шагов до поверхности

$$F^{(\mu)} = FF^{(\mu-1)} \pm \delta^{(\mu)} G^{(\mu)} = 0$$

порядка 2μ, высекающей на гиперболоиде $H = 0$ кривую порядка 4μ с $2\mu - 2$ непарными и

$$8 + 14 + 22 + 30 + \ldots + (8\mu - 10) = 4\mu^2 - 6\mu + 4$$

парными ветвями. При этом число μ не превосходит числа ν.

Поверхность $G^{(\mu)} = 0$ порядка 2μ пересекает одну из двух непарных ветвей кривой C_4 в 8μ точках $t_1^{(\mu)}, t_2^{(\mu)}, \ldots, t_{8\mu}^{(\mu)}$. Пусть теперь $G'^{(\mu)} = 0$ — уравнение поверхности указанного порядка 2μ, высекающей 8μ каких-нибудь вещественных точек на *другой* непарной ветви кривой C_4. Тогда при надлежащем выборе знака и для достаточно малых значений $\delta'^{(\mu)}$ уравнение

$$F'^{(\mu)} = FF^{(\mu-1)} \pm \delta'^{(\mu)} G'^{(\mu)} = 0$$

дает поверхность, высекающую на гиперболоиде $H = 0$ кривую 4μ-го порядка того же вида, что и кривая, высекаемая поверхностью $F^{(\mu)} = 0$. Эта высеченная кривая порядка 4μ также пересекает первоначальную кривую C_4 в 8μ последовательных точках; но сейчас высекающая 8μ точек на кривой C_4 ветвь непарна. Пусть теперь $G^{(\mu+1)} = 0$ — уравнение поверхности порядка $2\mu+2$, которая высекает на *первой* непарной ветви кривой C_4 какие-нибудь $8\mu + 8$ вещественных точек; тогда уравнение

$$F^{(\mu+1)} = FF'^{(\mu)} \pm \delta^{(\mu+1)} G^{(\mu+1)} = 0$$

при надлежащем выборе знака и для достаточно малых значений $\delta^{(\mu+1)}$ дает поверхность, высекающую на гиперболоиде $H = 0$ кривую порядка $4\mu + 4$ с $2\mu - 2$ непарными ветвями и $(4\mu^2 - 6\mu + 4) + 8\mu$ парными ветвями, — ведь уходящие в бесконечность части обеих пересекающихся непарных ветвей при возмущении дают единственную парную ветвь, так что общее число непарных ветвей остается неизменным. Одна из непарных ветвей построенной выше кривой порядка $4\mu + 4$ пересекает одну из двух непарных ветвей кривой C_4 в $8\mu + 8$ последовательных точках, и поэтому следующий шаг приведет к поверхности $F^{(\mu+2)} = 0$, которая высекает на гиперболоиде $H = 0$ кривую с тем же самым числом $2\mu - 2$ непарных ветвей и $(4\mu^2 - 6\mu + 4) + 8\mu + (8\mu + 8)$ парными ветвями. Точки пересечения с кривой C_4 при каждом следующем шаге мы выбираем попеременно на одной, а затем на другой непарной ветви кривой C_4 так, чтобы это всегда была непарная ветвь построенной кривой, которая пересекает одну из непарных ветвей кривой C_4, и вследствие этого число непарных ветвей при всех следующих шагах остается неизменным. С другой стороны, прирост числа парных ветвей на каждом шаге, как и прежде, увеличивается на 8. Так, после $\nu - \mu$ шагов мы придем к кривой порядка $n = 4\nu$ с $2\mu - 2$ непарными и

$$(4\mu^2 - 6\mu + 4) + 8\mu + (8\mu + 8) + \ldots + \{8(\nu - 1)\} = 4\nu^2 - 4\nu - 2\mu + 4$$

парными ветвями; итак, эта кривая имеет в сумме

$$4\nu^2 - 4\nu + 2 = \frac{1}{4}(n-2)^2 + 1$$

ветвей, а это, как указывалось ранее, максимальное число. Если мы положим по очереди $\mu = 2, 3, \ldots, \nu$, то получим пространственные кривые порядка 4ν с максимальным числом вещественных ветвей, среди которых соответственно $2, 4, \ldots, 2\nu - 2$ ветвей являются непарными. Так как существование пространственных кривых с максимальным числом ветвей без непарной ветви уже было доказано выше, то тем самым поставленная задача в первом случае $n = 4\nu$ выполнена.

Во *втором* случае $n = 4\nu + 2$, согласно нашим предыдущим рассмотрениям, кривая с максимальным числом вещественных ветвей вообще не может иметь непарной ветви, и мы сразу перейдем к исследованию *третьего* случая $n = 4\nu + 1$. Для этого мы вспомним установленное выше условие существования поверхности порядка m, высекающей $4m - 2$ заданных точек на кривой C_4 и одновременно содержащей заданную прямую гиперболоида. Пусть определенная там с точностью до кратного периода ω постоянная τ выбрана так, чтобы ее значение лежало между 0 и ω. Посредством линейного преобразования гиперболоида $H = 0$ мы можем легко сделать так, чтобы тот отрезок кривой C_4, который описывает точка, когда параметр t растет от 0 до τ, целиком лежал в конечной области. Пусть далее ε — положительная величина, которая меньше, чем каждое из двух чисел $9/17$ и $\tau/2$, так что выполнены неравенства

$$0 < \frac{\varepsilon^{\nu-1}}{9} < \frac{\varepsilon^{\nu-2}}{17} < \ldots < \frac{\varepsilon}{8\nu - 7},$$

$$\frac{\varepsilon}{8\nu - 7} < \tau - \varepsilon < \tau - \varepsilon^2 < \ldots < \tau - \varepsilon^{\nu-1} < \tau.$$

Мы выберем сейчас 9 вещественных величин

$$t_1^{(1)},\ t_2^{(1)},\ \ldots,\ t_9^{(1)},$$

затем 17 величин

$$t_1^{(2)},\ t_2^{(2)},\ \ldots,\ t_{17}^{(2)}$$

и, наконец, $8\nu - 7$ величин

$$t_1^{(\nu-1)},\ t_2^{(\nu-1)},\ \ldots,\ t_{8\nu-7}^{(\nu-1)},$$

которые удовлетворяют условиям

$$\begin{gathered}
0 < t_1^{(1)} < t_2^{(1)} < \ldots < t_9^{(1)} < t_1^{(2)}, \\
t_1^{(2)} < t_2^{(2)} < \ldots < t_{17}^{(2)} < t_1^{(3)}, \\
t_1^{(3)} < t_2^{(3)} < \ldots < t_{25}^{(3)} < t_1^{(4)}, \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
t_1^{(\nu-1)} < t_2^{(\nu-1)} < \ldots < t_{8\nu-7}^{(\nu-1)} < \tau - \varepsilon;
\end{gathered}$$

$$\begin{gathered}
t_1^{(1)} + t_2^{(1)} + \ldots + t_9^{(1)} = \varepsilon^{\nu-1}, \\
t_1^{(2)} + t_2^{(2)} + \ldots + t_{17}^{(2)} = \varepsilon^{\nu-2}, \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
t_1^{(\nu-1)} + t_2^{(\nu-1)} + \ldots + t_{8\nu-7}^{(\nu-1)} = \varepsilon.
\end{gathered}$$

Очевидно, что такие величины можно легко найти, если взять каждую из величин $t_1^{(1)}, t_2^{(1)}, \ldots, t_9^{(1)}$ достаточно близкой к значению $\varepsilon^{\nu-1}/9$, затем каждую из величин

$$t_1^{(2)}, t_2^{(2)}, \ldots, t_{17}^{(2)}$$

достаточно близкой к $\varepsilon^{\nu-2}/17$ и, наконец, каждую из величин

$$t_1^{(\nu-1)}, t_2^{(\nu-1)}, \ldots, t_{8\nu-7}^{(\nu-1)}$$

достаточно близкой к значению $\varepsilon/(8\nu-7)$. Если мы положим, кроме того,

$$t_{10}^{(1)} = \tau - \varepsilon^{\nu-1},\ t_{18}^{(2)} = \tau - \varepsilon^{\nu-2}, \ldots, t_{8\nu-6}^{(\nu-1)} = \tau - \varepsilon,$$

то будут выполнены условия

$$0 < t_1^{(1)} < t_2^{(1)} < \ldots < t_9^{(1)} < t_{10}^{(1)} < \tau,$$

$$t_9^{(1)} < t_1^{(2)} < t_2^{(2)} < \ldots < t_{17}^{(2)} < t_{18}^{(2)} < t_{10}^{(1)},$$

$$t_{17}^{(2)} < t_1^{(3)} < t_2^{(3)} < \ldots < t_{25}^{(3)} < t_{26}^{(3)} < t_{18}^{(2)},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$t_{8\nu-15}^{(\nu-2)} < t_1^{(\nu-1)} < t_2^{(\nu-1)} < \ldots < t_{8\nu-7}^{(\nu-1)} < t_{8\nu-6}^{(\nu-1)} < t_{8\nu-14}^{(\nu-2)};$$

$$t_1^{(1)} + t_2^{(1)} + \ldots + t_9^{(1)} + t_{10}^{(1)} = \tau,$$

$$t_1^{(2)} + t_2^{(2)} + \ldots + t_{17}^{(2)} + t_{18}^{(2)} = \tau,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$t_1^{(\nu-1)} + t_2^{(\nu-1)} + \ldots + t_{8\nu-7}^{(\nu-1)} + t_{8\nu-6}^{(\nu-1)} = \tau.$$

Пусть теперь L — прямая на гиперболоиде, которая пересекает каждую из обеих непарных ветвей кривой C_4. Пусть, кроме того, эта прямая L выбрана так, чтобы она не пересекала тот отрезок кривой C_4, который описывает точка, когда параметр растет от 0 до τ. Затем мы выберем из другого семейства образующих прямую L', которая вообще не пересекает кривую C_4. Пусть плоскость, которая содержит прямые L и L', представлена уравнением $E = 0$. Согласно предыдущим рассуждениям, существует поверхность 3-го порядка, которая пересекает в 10 точках $t_1^{(1)}, t_2^{(1)}, \ldots, t_{10}^{(1)}$ одну из ветвей кривой C_4 и в то же время содержит прямую L. Пусть $G^{(1)} = 0$ — уравнение этой поверхности. Тогда для достаточно малых значений $\delta^{(1)}$ уравнение

$$F^{(1)} = FE + \delta^{(1)} G^{(1)} = 0$$

дает поверхность 3-го порядка, содержащую прямую L и при этом высекающую на гиперболоиде $H = 0$ кривую 5-го порядка с тремя непарными ветвями. Одна из этих непарных ветвей пересекает соответствующую непарную ветвь кривой C_4 в 10 точках $t_1^{(1)}, t_2^{(1)}, \ldots, t_{10}^{(1)}$ именно таким образом, что при

прохождении непарной ветви этой кривой 5-го порядка указанные 10 точек появляются в той же последовательности, что и при прохождении кривой C_4. Пусть теперь $G^{(2)} = 0$ — уравнение поверхности 5-го порядка, содержащей прямую L и высекающей на кривой C_4 18 точек $t_1^{(2)}, t_2^{(2)}, \ldots, t_{18}^{(2)}$. Тогда уравнение

$$F^{(2)} = FF^{(1)} \pm \delta^{(2)} G^{(2)} = 0$$

при надлежаще выбранном знаке и для достаточно малых значений $\delta^{(2)}$ дает поверхность 5-го порядка, высекающую на гиперболоиде $H = 0$ прямую L и, кроме того, кривую 9-го порядка с тремя непарными и 10 парными ветвями, так как только 3 взаимно непересекающиеся ветви остаются при этой вариации непарными, в то время как бесконечные части двух других непарных ветвей дают единственную уходящую в бесконечность парную ветвь. Остальные 9 возникших парных ветвей все лежат в конечной части пространства. Среди них имеется одна, которая пересекает соответствующую непарную ветвь кривой C_4 в 18 последовательных точках $t_1^{(2)}, t_2^{(2)}, \ldots, t_{18}^{(2)}$. Если теперь $G^{(3)} = 0$ является поверхностью 7-го порядка, содержащей прямую L и высекающей на кривой C_4 26 точек $t_1^{(3)}, t_2^{(3)}, \ldots, t_{26}^{(3)}$, то

$$F^{(3)} = FF^{(2)} \pm \delta^{(3)} G^{(3)} = 0$$

при надлежаще выбранном знаке и для достаточно малых значений $\delta^{(3)}$ является уравнением поверхности 7-го порядка, высекающей на гиперболоиде $H = 0$ прямую L и, кроме того, кривую 13-го порядка с 5 непарными и $10 + 16 = 26$ парными ветвями. Продолжая таким образом, мы получаем на следующем шаге поверхность 9-го порядка $F^{(4)} = 0$, которая высекает на гиперболоиде $H = 0$ прямую L и кривую 17-го порядка с 7 непарными и $10 + 16 + 24 = 50$ парными ветвями. Видно, что на каждом следующем шаге добавляются к имеющимся еще две непарные ветви, в то время как прирост числа парных ветвей на каждом следующем шаге на 8 больше, чем на предыдущем. Тогда после $\nu - 1$ шагов мы придем к поверхности $F^{(\nu)} = 0$ порядка $2\nu + 1$, которая высекает на гиперболоиде $H = 0$ прямую $L = 0$ и кривую порядка $4\nu + 1$ с $2\nu - 1$ непарными и

$$10 + 16 + 24 + 32 + \ldots + 8(\nu - 1) = 4\nu^2 - 4\nu + 2$$

парными ветвями. Итак, эта последняя кривая порядка $n = 4\nu + 1$ имеет в сумме

$$4\nu^2 - 2\nu + 1 = \frac{1}{4}(n-1)(n-3) + 1$$

вещественных ветвей, а это, как указывалось ранее, максимальное число.

Теперь не представляет никакого труда доказать также существование кривых порядка $4\nu + 1$ с максимальным числом ветвей, среди которых менее чем $2\nu - 1$ непарных. Обозначим через μ число, меньшее чем ν. Тогда описанный выше метод через $\mu - 1$ шагов приведет к кривой порядка $4\mu + 1$ с $2\mu - 1$ непарными ветвями. К этой кривой мы применим тот же метод, что и ранее в первом случае $n = 4\nu$, используя попеременно обе непарные ветви кривой C_4 так, чтобы каждый раз непарная ветвь построенной кривой пересекала одну из непарных ветвей кривой C_4 только в последовательных точках и вследствие этого на всех следующих шагах число непарных

ветвей не будет изменяться. Положение точек на обеих ветвях кривой C_4 нужно выбирать так, чтобы после вариации возникло максимально возможное число новых ветвей. После $\nu - \mu$ шагов получается кривая порядка $n = 4\nu + 1$ с максимальным числом вещественных ветвей, среди которых $2\mu - 1$ непарных. При этом предполагается, что $\mu > 1$. Однако уже раньше было доказано, что существуют также кривые порядка $n = 4\nu + 1$ с максимальным числом вещественных ветвей, среди которых только одна ветвь непарная.

Наконец, для изучения *последнего* случая $n = 4\nu+3$ положим $\tau' = \omega - \tau$ и применим линейное преобразование координат для того, чтобы тот отрезок кривой C_4, который описывает точка при увеличении параметра t от 0 до τ', целиком лежал в конечной части пространства. Пусть, далее, ε' обозначает положительную величину, которая меньше, чем каждое из чисел $5/13$ и $\tau'/2$, так что выполнены неравенства

$$0 < \frac{\varepsilon'^{\nu}}{5} < \frac{\varepsilon'^{\nu-1}}{13} < \ldots < \frac{\varepsilon'}{8\nu - 3},$$

$$\frac{\varepsilon'}{8\nu - 3} < \tau' - \varepsilon' < \tau' - \varepsilon'^{2} < \ldots < \tau' - \varepsilon'^{\nu} < \tau'.$$

Принимая во внимание эти неравенства, так же, как выше в случае $n = 4\nu+1$, легко найти 6 величин $t_1^{(1)}, t_2^{(1)}, \ldots, t_6^{(1)}$, затем 14 величин $t_1^{(2)}, t_2^{(2)}, \ldots, t_{14}^{(2)}$ и, наконец, $8\nu - 2$ величин $t_1^{(\nu)}, t_2^{(\nu)}, \ldots, t_{8\nu-2}^{(\nu)}$, которые удовлетворяют следующим условиям:

$$0 < t_1^{(1)} < t_2^{(1)} < \ldots < t_5^{(1)} < t_6^{(1)} < \tau',$$

$$t_5^{(1)} < t_1^{(2)} < t_2^{(2)} < \ldots < t_{13}^{(2)} < t_{14}^{(2)} < t_6^{(1)},$$

$$t_{13}^{(2)} < t_1^{(3)} < t_2^{(3)} < \ldots < t_{21}^{(3)} < t_{22}^{(3)} < t_{14}^{(2)},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$t_{8\nu-11}^{(\nu-1)} < t_1^{(\nu)} < t_2^{(\nu)} < \ldots < t_{8\nu-3}^{(\nu)} < t_{8\nu-2}^{(\nu)} < t_{8\nu-10}^{(\nu-1)};$$

$$t_1^{(1)} + t_2^{(1)} + \ldots + t_6^{(1)} = \tau',$$

$$t_1^{(2)} + t_2^{(2)} + \ldots + t_{14}^{(2)} = \tau',$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$t_1^{(\nu)} + t_2^{(\nu)} + \ldots + t_{8\nu-2}^{(\nu)} = \tau'.$$

Пусть L' — образующая гиперболоида $H = 0$, которая не пересекает ни одну из двух непарных ветвей кривой C_4. Тогда вследствие предыдущих рассуждений существует поверхность 2-го порядка, которая содержит прямую L' и высекает на одной из ветвей кривой C_4 6 точек $t_1^{(1)}, t_2^{(1)}, \ldots, t_6^{(1)}$. Пусть $F^{(1)} = 0$ — уравнение этой поверхности. Пусть, далее, $G^{(2)} = 0$ — уравнение поверхности 4-го порядка, которая содержит прямую L' и высекает на кривой C_4 14 точек $t_1^{(2)}, t_2^{(2)}, \ldots, t_{14}^{(2)}$. Тогда при подходящим образом

выбранном знаке и для достаточно малых значений $\delta^{(2)}$ уравнение

$$F^{(2)} = FF^{(1)} \pm \delta^{(2)} G^{(2)} = 0$$

дает поверхность 4-го порядка, которая высекает на гиперболоиде $H = 0$ прямую L' и кривую 7-го порядка с одной непарной и 6 парными ветвями. Одна из этих парных ветвей пересекает непарную ветвь кривой C_4 в 14 последовательных точках. Далее, если $G^{(3)} = 0$ — уравнение поверхности 6-го порядка, которая содержит прямую L' и высекает на кривой C_4 22 точки $t_1^{(3)}, t_2^{(3)}, \ldots, t_{22}^{(3)}$, то при надлежаще выбранном знаке и для достаточно малых значений $\delta^{(3)}$ уравнение

$$F^{(3)} = FF^{(2)} \pm \delta^{(3)} G^{(3)} = 0$$

дает поверхность 6-го порядка, которая содержит прямую L' и высекает на гиперболоиде $H = 0$ кривую 11-го порядка с тремя непарными и 18 парными ветвями. Так мы дойдем, наконец, до поверхности $F^{(\nu+1)} = 0$ порядка $2\nu+2$, которая содержит прямую L' и высекает на гиперболоиде $H = 0$ кривую порядка $n = 4\nu + 3$ с $2\nu - 1$ непарными и $4\nu^2 + 2$ парными ветвями. Эта кривая имеет в сумме

$$4\nu^2 + 2\nu + 1 = \frac{1}{4}(n-1)(n-3) + 1$$

вещественных ветвей, а это, как указывалось раньше, максимальное число.

Доказательство существования кривых порядка $n = 4\nu + 3$ с максимальным числом вещественных ветвей, среди которых меньше чем $2\nu - 1$ непарных ветвей, проводится так же, как для случаев $n = 4\nu$ и $n = 4\nu + 1$.

Видно, что проведенные выше построения дают все виды неприводимых пространственных кривых, которые в приведенной выше теореме не были исключены как невозможные. *Следовательно, выше полностью решен вопрос о различных видах форм пространственных кривых произвольного порядка n с максимальным числом вещественных ветвей.*

Кёнигсберг в Пруссии, 19 ноября 1890 г.

О ФОРМЕ ПОВЕРХНОСТИ ЧЕТВЕРТОГО ПОРЯДКА*)

При исследовании форм алгебраических поверхностей особенно важно знать формы тех неособых поверхностей, которые топологически наиболее разносторонни [1].

В случае когда

$$F(x, y, z, t) = 0$$

— уравнение с вещественными коэффициентами в однородных координатах x, y, z, t, под *компонентой* (Mantel) поверхности, определяемой этим уравнением, понимается непрерывно связная система [2] вещественных точек $(x : y : z : t)$, так что при использовании обычной прямоугольной системы координат x, y, z $(t = 1)$ те части поверхности в пространстве, которые соединяются только на бесконечности, нужно считать принадлежащими одной компоненте [3]. Компоненту называют, как это обычно принято, поверхностью рода p, если она допускает p и не более чем p попарно непересекающихся замкнутых разрезов, которые не приводят к распадению компоненты. Компоненте рода p я приписываю ранг $p + 1$ и в дальнейшем под *рангом* какой-либо алгебраической поверхности всегда подразумеваю сумму рангов ее компонент.

Что касается поверхности 4-го порядка, то из исследований К. Роона[1)] следует, что она не может иметь ранг выше 12. С другой стороны, среди известных до сих пор поверхностей 4-го порядка можно выделить поверхности, имеющие самый высокий ранг: они состоят из 10 отдельных овалоидов [4] и, следовательно, имеют ранг 10. Ниже я укажу *неособую поверхность 4-го порядка, которая действительно имеет максимальный ранг, а именно ранг* 12, *и, таким образом, представляет собой экстремум в многообразии форм поверхностей 4-го порядка.*

С этой целью мы построим окружность радиуса 1 с центром в начале координат координатной системы (x, y) и затем эллипс, который пересекает эту окружность в четырех вещественных точках A, B, C, D. Положим

$$k(x, y) = x^2 + y^2 - 1$$

и обозначим через E левую часть уравнения эллипса, выбрав это уравнение так, чтобы многочлен E внутри эллипса был отрицательным. Далее, определим на xy-плоскости четыре прямые

$$l_1 = 0, \quad l_2 = 0, \quad l_3 = 0, \quad l_4 = 0,$$

---

*) Über die Gestalt einer Fläche vierter Ordnung. — Nachr. Ges. Wiss. Göttingen, 1909, S. 308–313. *Перевод Харламова В. М. и Харламовой С. А.*

1) *Rohn K.* — В кн.: Preisschriften, herausgegeben von der Fürstlich Jäblonowskischen Gesellschaft. — Leipzig, 1886.

каждая из которых пересекает в двух точках дугу окружности AB, лежащую вне эллипса; тогда можно выбрать положительную или отрицательную постоянную ε, столь малую, что определяемая уравнением

$$C(x, y) \equiv kE + \varepsilon l_1 l_2 l_3 l_4 = 0$$

кривая 4-го порядка оказывается состоящей из четырех замкнутых ветвей, как показано на рис. 1: одна из ветвей пересекает дугу AB в 8 следую-

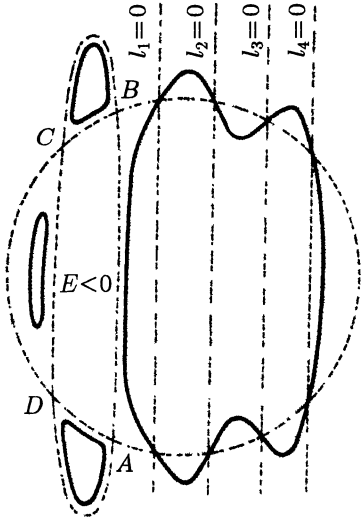


Рис. 1

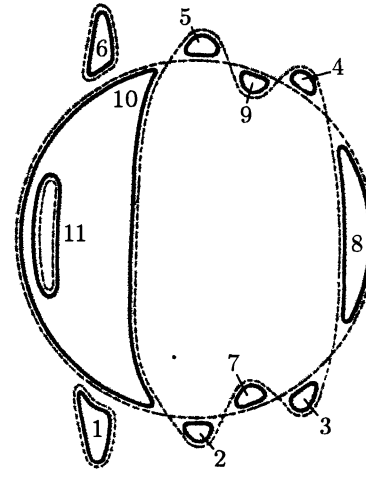


Рис. 2

щих друг за другом точках. Наконец, пусть положительная постоянная π выбрана столь малой, что определяемая уравнением

$$D(x, y) \equiv kC + \pi^2 = 0$$

кривая 6-го порядка имеет 11 замкнутых ветвей, как это показано на рис. 2: из них шесть ветвей $1, 2, 3, \ldots, 6$ расположены вне друг друга и вне окружности $k = 0$, в то время как пять других $7, 8, \ldots, 11$ лежат внутри окружности так, что одна из ветвей, а именно 10, содержит внутри себя ветвь 11, в то время как три других $7, 8, 9$ расположены вне ветви 10. В соответствии с этим функция D отрицательна внутри ветвей $1, 2, \ldots, 9$ и в кольцевой области, образованной ветвями 10 и 11.

Мы исследуем теперь форму такой поверхности 4-го порядка, уравнение которой в xyz-пространстве имеет вид

$$F \equiv kz^2 + 2\pi z - C = 0$$

Согласно этому уравнению, значению системы координат x, y тогда и только тогда отвечают два вещественных значения координаты z, когда $D > 0$, и эти значения оба конечны, за исключением случая $k = 0$; в этом

случае один из двух корней z бесконечен, причем разложение по возрастающим степеням переменной k в виде

$$z = -\frac{2\pi}{k} + \mathfrak{P}(k)$$

показывает, что при приближении точки x, y в xy-плоскости к окружности $k = 0$ корень z становится неограниченно отрицательным, соответственно положительным, в зависимости от того, приближается точка x, y в xy-плоскости к окружности $k = 0$ снаружи или изнутри. Бесконечно удаленная плоскость пересекает нашу поверхность $F = 0$ по кривой, которая определена конусом

$$(x^2 + y^2)z^2 - (x, y)_4 = 0,$$

где $(x, y)_4$ — однородная составляющая степени 4 многочлена C от переменных x, y. Так как кривая 4-го порядка $C = 0$ полностью располагается в конечной части xy-плоскости, а многочлен C для достаточно больших значений положителен, то $(x, y)_4$ — положительно определенная форма. Отсюда следует, что высекаемая на конусе плоскостью $z = 1$ кривая 4-го порядка

$$x^2 + y^2 - (x, y)_4 = 0$$

состоит из одного овала и точки $x = 0$, $y = 0$, которая лежит внутри этой замкнутой ветви и является изолированной двойной точкой — в соответствие с тем, что для поверхности $F = 0$ бесконечно удаленная точка z-оси является узловой точкой [5]. Обозначим через Ω проекцию рассмотренного выше овала кривой 4-го порядка из начала координат, т. е. бесконечно удаленную ветвь (Kurvenzug) нашей поверхности 4-го порядка $F = 0$.

Этих результатов достаточно, чтобы наглядно представить поверхность $F = 0$. С бесконечности из Ω, располагаясь вначале полностью в отрицательном, лежащем ниже xy-плоскости полупространстве, приходит лист поверхности, который остается все время снаружи кругового цилиндра $k = 0$ и приближается к нему асимптотически снаружи вниз, когда z уходит на минус-бесконечность. Одновременно также с бесконечности из Ω приходит, располагаясь вначале полностью в положительном, лежащем над xy-плоскостью полупространстве, второй лист; он прорезает круговой цилиндр $k = 0$ и затем возвращается к нему, асимптотически прижимаясь к нему изнутри вверх, когда z уходит на плюс-бесконечность. Эти протянувшиеся друг над другом вне кругового цилиндра $k = 0$ листы поверхности соединяются вдоль тех кривых, проекции которых на xy-плоскость суть овалы $1, 2, \ldots, 6$: таким образом, на поверхности возникают шесть дыр, находящихся вне кругового цилиндра $k = 0$. Далее верхний лист доставляет благодаря тем кривым, проекции которых на xy-плоскость суть овалы $7, 8, 9, 10$ и вдоль которых он сам с собой соединяется, еще четыре дыры нашей поверхности. Наконец, овал 11 дает лежащую отдельно от описанных ранее листов новую компоненту — простой овалоид.

Если теперь разрезать нашу поверхность $F = 0$ вдоль всех десяти кривых, проекции которых суть овалы $1, \ldots, 10$, то тем самым в конечной области верхний лист полностью отделится от нижнего и, кроме того, проходящий внутри кругового цилиндра $k = 0$ и прижимающийся к нему кусок поверхности (Flächenstück) верхнего листа отделится также от остальной части этого листа [6].

Ранее было показано, что верхний лист нашей поверхности соединяется с нижним вдоль бесконечно удаленной кривой Ω; с другой стороны, нижний лист и отделившийся кусок поверхности верхнего листа встречаются друг с другом в бесконечно удаленной узловой точке поверхности. Следовательно, для того чтобы получить поверхность без узловой точки, которая не распадается при тех десяти разрезах, нам нужно так изменить F, чтобы кривая, которую высекает измененная поверхность на бесконечно удаленной плоскости, приобрела вместо двойной точки новый вещественный овал. Это достигается построением поверхности с уравнением

$$G \equiv -\varepsilon z^4 + kz^2 + 2\pi z - C = 0$$

где ε обозначает настолько малую положительную постоянную, что для всех еще меньших положительных ε многочлен G имеет отличный от нуля дискриминант. Действительно, бесконечно удаленная кривая этой поверхности задана конусом

$$-\varepsilon z^4 + (x^2 + y^2)z^2 - (x, y)_4 = 0,$$

а сечение этого конуса плоскостью $z = 1$ есть кривая 4-го порядка, которая состоит из двух ветвей. Внутренняя ветвь, которая образовалась из двойной точки $x = 0$, $y = 0$ предыдущей кривой, соединяет верхний, простирающийся в бесконечную область положительного полупространства, кусок поверхности с нижним, простирающимся также в бесконечную область отрицательного полупространства, листом новой поверхности $G = 0$.

Тем самым указана неособая поверхность 4-го порядка, которая состоит из двух компонент, одна их которых имеет род 10 *и, следовательно, ранг* 11, *а другая — род* 0 *и, следовательно, ранг* 1. *Эта поверхность имеет максимально возможный ранг* 12.

В заключение следует еще заметить, что *что напрашивающиеся сами собой случаи для реализации ранга* 12, *а именно* 12 *простых овалов или компонента с* 11 *дырами, для поверхности 4-го порядка невозможны.* Действительно заметим, что такая поверхность, если бы она существовала, подходящим изменением коэффициентов уравнения поверхности превращалась бы в поверхность 4-го порядка с изолированной узловой точкой в первом случае, а в последнем случае — в такую поверхность 4-го порядка, которая имеет узловую точку с вещественным касательным конусом, не превращаясь ранее [7] в поверхность с особенностью. Проектирование полученной поверхности из ее узловой точки на плоскость давало бы в обоих случаях плоскую кривую 6-го порядка, которая состояла бы из 11 овалов, располагающихся вне друг друга. Но то, что такой кривой не существует, является одной из глубоких теорем топологии плоских алгебраических кривых; ее недавно доказали Г. Кан и К. Лёбенштейн[2)] указанным мной способом [8].

[2)] Ср. гёттингенские диссертации этих авторов.

О ПОВЕРХНОСТЯХ ПОСТОЯННОЙ ГАУССОВОЙ КРИВИЗНЫ*)

Согласно Бельтрами[1], поверхность постоянной отрицательной кривизны представляет часть плоскости Лобачевского (неевклидовой плоскости), если рассматривать геодезические линии поверхности постоянной отрицательной кривизны как прямые плоскости Лобачевского, а за длины и углы плоскости Лобачевского принять подлинные длины и углы на этой поверхности. Среди исследованных до настоящего времени поверхностей постоянной отрицательной кривизны мы не находим *ни одной*, которая простиралась бы непрерывно и обладала бы непрерывно изменяющейся касательной плоскостью в окрестности каждой своей точки, если окрестность продолжать во все стороны; напротив, все известные поверхности постоянной отрицательной кривизны обладают сингулярными линиями, за которые непрерывное продолжение с непрерывно изменяющейся касательной плоскостью невозможно. Вследствие этого пока еще не удалось представить *всю* плоскость Лобачевского с помощью какой-либо из известных поверхностей постоянной отрицательной кривизны, и нам кажется принципиально интересным вопрос, *может ли вообще вся плоскость Лобачевского быть представлена с помощью интерпретации Бельтрами аналитической*[2] *поверхностью постоянной отрицательной кривизны.*

Чтобы ответить на этот вопрос, мы будем исходить из существования аналитической поверхности постоянной отрицательной кривизны, равной -1, которая в конечном ν [1] ведет себя регулярно и не допускает особых точек; мы покажем далее, что это предположение приводит к противоречию. Поверхность, соответствующая нашим допущениям, полностью характеризуется следующим высказыванием:

Каждая лежащая в конечном точка сгущения точек поверхности тоже является точкой поверхности.

---

*) Über Flächen von konstanter Gaußscher Krümmung. — In: *Hilbert D.* Grundlagen der Geometrie. — Leipzig ind Berlin: Verlag und Druck von B. G. Teubner, 1930, Anhang V. *Перевод Б. Л. Лаптева.*

1) *Beltrami E.* — Giornale di Matem., vol. 6, 1868.

2) Аналитический характер рассматриваемой поверхности я предполагаю лишь для того, чтобы облегчить изложение вывода, поскольку ход доказательства и достигаемый результат (с. 394) остаются пригодными также тогда, когда функция $\mathfrak{P}(x, y)$ в уравнении (I) является не аналитической функцией от x, y, но дифференцируемой до достаточно высокого порядка. Существование неаналитических поверхностей постоянной отрицательной кривизны, регулярных всмысле теории поверхностей (которые, в соответствии с доказываемой далее теоремой, не могут простираться всюду непрерывно с непрерывным изменением касательной плоскости), установил по моему предложению Г. Люткемейер в своей диссертации (*Lütkemeyer G.* Über den analytischen Charakter der Integrale von partiellen Differentialgleichungen. — Göttingen, 1902)

Пусть O обозначает произвольную точку рассматриваемой поверхности; всегда возможно так выбрать прямоугольную систему координатных осей x, y, z, что O будет началом системы координат и уравнение поверхности в окрестности этой точки примет следующий вид:

$$z = ax^2 + by^2 + \mathfrak{P}(x, y), \tag{I}$$

где константы a, b удовлетворяют соотношению

$$4ab = -1,$$

а степенной ряд $\mathfrak{P}(x, y)$ содержит только члены третьего или более высокого порядка. Очевидно, что ось z является нормалью к поверхности, а оси x и y идут по направлениям, определяемым главными кривизнами.

Уравнение

$$ax^2 + by^2 = 0$$

определяет две главные касательные к поверхности, проходящие через точку O в плоскости xy; следовательно, они всегда отличны друг от друга и определяют направления, в которых через произвольную точку O проходят обе асимптотические линии поверхности. Каждая из этих асимптотических линий принадлежит своему простому (однопараметрическому) семейству асимптотических линий, и каждое из этих семейств покрывает регулярно и без пробелов всю окрестность точки O поверхности. Поэтому если под u и v мы будем понимать достаточно малые числа, то сможем, конечно, выполнить следующее построение. Отложим на одной из проходящих через O асимптотических линий значение параметра u как длину дуги от O, через конец этой дуги проведем линию второго семейства и отложим на ней значение параметра v как длину дуги от этого конца. Полученная при этом точка является точкой поверхности, и она однозначно определяется значениями параметров u, v. Соответственно этому мы будем рассматривать прямоугольные координаты x, y, z точек поверхности как функции от u, v, положив

$$x = x(u, v), \quad y = y(u, v), \quad z = z(u, v), \tag{1}$$

и они будут тогда для достаточно малых значений u, v регулярными аналитическими функциями от u, v.

Из теории поверхностей постоянной кривизны, равной -1, известны следующие основные факты:

Пусть φ обозначает угол между двумя асимптотическими линиями, проходящими через точку u, v; тогда три коэффициента первой квадратичной формы получают следующие значения:

$$e \equiv \left(\frac{\partial x}{\partial u}\right)^2 + \left(\frac{\partial y}{\partial u}\right)^2 + \left(\frac{\partial z}{\partial u}\right)^2 = 1,$$

$$f \equiv \frac{\partial x}{\partial u}\frac{\partial x}{\partial v} + \frac{\partial y}{\partial u}\frac{\partial y}{\partial v} + \frac{\partial z}{\partial u}\frac{\partial z}{\partial v} = \cos\varphi,$$

$$g \equiv \left(\frac{\partial x}{\partial v}\right)^2 + \left(\frac{\partial y}{\partial v}\right)^2 + \left(\frac{\partial z}{\partial v}\right)^2 = 1.$$

Поэтому квадрат производной по параметру t от длины дуги произвольной кривой на поверхности запишется так:

$$\left(\frac{ds}{dt}\right)^2 = \left(\frac{du}{dt}\right)^2 + 2\cos\frac{du}{dt}\frac{dv}{dt} + \left(\frac{dv}{dt}\right)^2. \tag{2}$$

Угол φ, рассматриваемый как функция от u, v, удовлетворяет дифференциальному уравнению в частных производных[3)]

$$\frac{\partial^2\varphi}{\partial u\partial v} = \sin\varphi. \tag{3}$$

Если отказаться от однозначности сопоставления с любой точкой поверхности пары чисел u, v, то можно рассмотренное построение распространить на сколь угодно большие значения u, v. Вообще говоря, u-линия, проходящая через точку O, может замкнуться, но все же на ней по обе стороны от точки O можно откладывать сколь угодно большие длины. В итоге каждому значению u соответствует точка на асимптотической линии.

В каждой такой точке P мы рассматриваем вторую проходящую через P асимптотическую линию, на которой в качестве параметра v принимаем длину ее дуги (со знаком), отсчитываемую от P; и опять можно по обе стороны от P откладывать на асимптотической линии сколь угодно большие длины.

Таким образом, каждой паре значений u, v однозначно, но, вообще говоря, не взаимно однозначно, соответствует некоторая точка нашей поверхности. Итак, получено то, что на геометрическом языке называется отображением евклидовой плоскости u, v в целом на некоторую накрывающую поверхность нашей поверхности или ее части.

Прежде всего, надо показать, что каждая u-линия поверхности является асимптотической и что параметр u представляет длину ее дуги.

Для линии $v = 0$ это уже известно. Далее из формулы (2), представляющей линейный элемент, вытекает, что это верно в окрестности точки $(u, 0)$ и для кусков u-линий.

Для доказательства в общем случае достаточно убедиться в правильности следующего утверждения:

Если a — положительное число, а b — любое вещественное число, то каждый отрезок $-a \leqslant u \leqslant +a$, $v = b$ отображается на нашей поверхности в кусок асимптотической линии или в последовательность ее кусков, причем параметр u представляет при этом длину дуги этой линии.

При $b = 0$ эта теорема справедлива. Далее надо показать, что

1) если эта теорема справедлива при $b = b_0$, то она верна и при любом b, достаточно мало отличающемся от b_0;

[3)] Ранее в начальной своей работе Über Flächen von konstanter Gaußscher Krümmung. — Trans. Amer. Math. Soc., 1901, vol. 2, p. 87–99, я доказал невозможность существования поверхности постоянной отрицательной кривизны, не имеющей особых точек, опираясь именно на эту формулу [2], затем Хольмгрен дал более аналитическое доказательство того же факта, тоже используя формулу (3) (см.: *Holmgren E.* — C. R. Acad. de Paris, 1902, vol. 134). Приведенная здесь переработка доказательства Хольмгрена примыкает к изложению этого доказательства В. Бляшке (*Blaschke W.* Elementare Differential Geometrie. I, 1921, § 80; имеется перевод 3-го изд. 1930 г.: *Бляшке В.* Дифференциальная геометрия. — М.–Л.: ОНТИ, 1935, § 96). В связи с первоначальным моим доказательством см. также изложение Л. Бибербаха (*Bieberbach L.* — Acta Math., 1926, Bd. 48).

2) если эта теорема справедлива для всех b, удовлетворяющих условиям $b_1 < b < b_2$, то она справедлива также при $b = b_1$ и $b = b_2$.

Но доказательство этих предложений основывается на использовании непрерывности и применении теоремы Гейне — Бореля о конечном покрытии.

Итак, теорема справедлива для всех значений b.

Пусть теперь $\varphi = \varphi(u, v)$ обозначает (как и ранее) угол между двумя асимптотическими линиями, проходящими через точку (u, v) нашей поверхности, причем этот угол отсчитывается от положительного направления u-линии к положительному направлению v-линии. Эта функция должна быть определена и непрерывна для всех u, v и обладать непрерывными частными производными, удовлетворяющими дифференциальному уравнению (3).

С помощью надлежащего выбора положительных u-направления и v-направления можно всегда добиться, чтобы в точке $u = v = 0$ выполнялись неравенства

$$0 < \varphi < \pi \quad \text{и} \quad \frac{\partial \varphi}{\partial u} \geqslant 0.$$

Так как φ не может равняться ни 0, ни π, то вследствие непрерывности функции $\varphi(u, v)$ для всех значений u, v должны выполняться неравенства $0 < \varphi(u, v) < \pi$, а следовательно, и неравенство

$$\sin \varphi > 0.$$

Но функции $\varphi(u, v)$, обладающей такими свойствами, как мы сейчас убедимся, не существует.

Действительно, из дифференциального уравнения

$$\frac{\partial^2 \varphi}{\partial u \partial v} = \sin \varphi$$

следует, что $\partial^2 \varphi / \partial u \partial v > 0$, и поэтому функция $\partial \varphi / \partial u$ при возрастании v растет.

В частности,

$$\frac{\partial \varphi}{\partial u}(0, 1) > \frac{\partial \varphi}{\partial u}(0, 0) \geqslant 0,$$

и потому можно найти такое положительное число a, для которого при $0 \leqslant u \leqslant 3a$ выполняется неравенство

$$\frac{\partial \varphi}{\partial u}(u, 1) > 0,$$

Пусть m означает положительный минимум функции

$$\frac{\partial \varphi}{\partial u}(u, 1) \quad \text{при} \quad 0 \leqslant u \leqslant 3a.$$

Тогда при $v \geqslant 1$

$$\varphi(a, v) - \varphi(0, v) = a \frac{\partial \varphi}{\partial u}(\theta a, v) \geqslant a \frac{\partial \varphi}{\partial u}(\theta a, 1) \geqslant ma,$$

где $0 < \theta < 1$. Аналогично

$$\varphi(3a, v) - \varphi(2a, v) \geqslant ma.$$

Таким образом,

$$\varphi(a, v) \geqslant \varphi(0, v) + ma \geqslant ma, \quad \varphi(2a, v) \leqslant \varphi(3a, v) - ma < \pi - ma.$$

Далее, при $0 \leqslant u \leqslant 3a$ и $v \geqslant 1$ имеем

$$\frac{\partial \varphi}{\partial u}(u, v) \geqslant \frac{\partial \varphi}{\partial u}(u, 1) > 0;$$

поэтому $\varphi(u, v)$ растет монотонно вместе с u, а тогда при $a \leqslant u \leqslant 2a$ и $v \geqslant 1$

$$0 < ma < \varphi(a, v) \leqslant \varphi(u, v) \leqslant \varphi(2a, v) < \pi - ma$$

и, следовательно,

$$\sin \varphi(u, v) > \sin(ma) = M,$$

где M больше 0 и не зависит от u, v.

Вследствие этого величина двойного интеграла

$$\iint \sin \varphi(u, v)\, du\, dv,$$

распространенного по прямоугольнику с вершинами

$$(a, 1), \quad (2a, 1), \quad (2a, V), \quad (a, V), \qquad \text{где } V > 1,$$

будет больше $Ma(V - 1)$ и при надлежащем выборе V может быть сделана больше π.

Но, с другой стороны, из уравнения (3) получаем

$$\iint \sin \varphi\, du\, dv = \int_0^{2a} \int_1^{V} \frac{\partial^2 \varphi}{\partial u \partial v}\, du\, dv =$$

$$= \varphi(2a, V) - \varphi(a, V) - \{\varphi(2a, 1) - \varphi(a, 1)\} < \pi,$$

так как

$$\varphi(2a, V) - \varphi(a, V) < \varphi(2a, V) < \pi \quad \text{и} \quad \varphi(2a, 1) - \varphi(a, 1) > 0.$$

Мы пришли, таким образом, к противоречию. Иначе говоря, *мы вынуждены отвергнуть принятое вначале предположение.* То есть мы убедились, что *не существует аналитической поверхности постоянной отрицательной кривизны, не имеющей особенностей и везде регулярной.*

В частности, и на поставленный вначале вопрос, можно ли по методу Бельтрами представить всю плоскость Лобачевского с помощью регулярной аналитической поверхности, следует ответить отрицательно.

О поверхностях постоянной положительной кривизны[4)]

Мы начали это исследование с вопроса о существовании поверхности, всюду в конечном непрерывной и аналитической, который был поставлен

[4)] Вопрос о представлении неевклидовой эллиптической геометрии плоскости точками непрерывно искривленной поверхности изучал по моему предложению В. Бой в работе: *Boy W.* Über die Curvatura integra und die Topologie geschlossener Flächen. — Inaugural-dissertation, Göttingen, 1901; Math. Ann., 1903, Bd. 57, S. 151–184. В этой работе В. Бой нашел топологически очень интересную модель, а именно одностороннюю замкнутую поверхность, лежащую в конечном, которая не имеет других особенностей, кроме замкнутой двойной кривой с тройной точкой, в которой эта кривая пересекает полости поверхности, причем эта модель обладает связностью неевклидовой эллиптической плоскости [3].

для поверхностей постоянной отрицательной кривизны и на который мы в этом случае получили отрицательный ответ, т. е. установили, что таких поверхностей не существует. Теперь мы собираемся обсудить посредством соответствующих методов аналогичный вопрос для поверхностей постоянной положительной кривизны. Очевидно, что сфера — это замкнутая поверхность без особенностей постоянной положительной кривизны, и в силу доказательства, осуществленного по моему предложению Г. Либманном[5], никакой другой замкнутой поверхности с теми же свойствами не существует. Этот важный результат мы хотим вывести из одного предложения, которое верно для любого куска поверхности постоянной положительной кривизны, не имеющей особенностей[6]. Оно звучит так:

Пусть на поверхности постоянной положительной кривизны, равной $+1$, *имеется односвязная или многосвязная область без особенностей, ограниченная в конечном. Вообразим, что как в каждой точке этой области, так и в граничных точках, выделены главные радиусы кривизны; тогда ни максимум наибольшего, ни минимум наименьшего из обоих радиусов кривизны не может достигаться ни в одной из внутренних точек области и, значит, наша поверхность — это кусок сферы радиуса* 1.

Для доказательства заметим сначала, что вследствие нашего предположения произведение обоих главных радиусов кривизны везде равно 1, и поэтому больший из них должен быть постоянно больше или равен 1. На этом основании максимум большего радиуса кривизны только тогда равен 1, когда оба главных радиуса кривизны в каждой точке рассматриваемого куска данной поверхности равны 1. В этом примечательном случае каждая точка этого куска поверхности является точкой округления, а отсюда, как известно, можно заключить, что рассматриваемый кусок поверхности — кусок сферы радиуса 1.

Пусть теперь максимум наибольшего из обоих главных радиусов кривизны нашей поверхности > 1; допустим, в противоречие с упомянутым утверждением, что внутри этого куска поверхности имеется точка O, в которой достигается этот максимум. Так как очевидно, что точка O не может быть точкой округления и является притом регулярной точкой нашей поверхности, то окрестность этой точки покрывается без пробелов и регулярно каждым из двух семейств линий кривизны. Если мы используем эти линии кривизны как координатные линии и примем точку O за начало криволинейной координатной системы, то, как известно из теории поверхностей постоянной положительной кривизны, будут верны следующие факты[7]:

Пусть r_1 обозначает больший из обоих главных радиусов кривизны в окрестности начальной точки $O = (0, 0)$; в этой окрестности $r_1 > 1$. По-

---

[5] См. *Liebmann H.* — Nachr. Ges. Wiss. Göttingen, 1899, S. 44–55. См. далее интересные работы того же автора в Math. Ann., 1900, Bd. 53 и 1901, Bd. 54.

[6] Аналитический характер поверхностей постоянной положительной кривизны доказан Г. Люткемейером в диссертации, упомянутой в примечании на с. 390, и Э. Хольмгреном в Math. Ann., 1903, Bd. 57.

[7] *Darboux G.* Leçons sur la théorie générale des surfaces. Vol. 3, 1894, № 776; *Bianchi L.* Lezioni di geometria differenziale, 1902, § 264.

ложим [4]

$$\rho = \frac{1}{2}\log\frac{r_1+1}{r_1-1}.$$

Тогда эта положительная вещественная величина ρ удовлетворяет как функция от u, v уравнению в частных производных [5]

$$\frac{\partial^2\rho}{\partial u^2} + \frac{\partial^2\rho}{\partial v^2} = \frac{e^{-2\rho} - e^{+2\rho}}{4}. \tag{4}$$

Так как ρ (как функция от r_1) при уменьшении r_1 растет, то в точке $u = 0$, $v = 0$ она необходимо имеет минимум; поэтому разложение по степеням переменных u, v имеет следующий вид:

$$\rho = a + \alpha u^2 + 2\beta uv + \gamma v^2 + \ldots,$$

где a, α, β, γ — константы, и при этом квадратичная форма

$$\alpha u^2 + 2\beta uv + \gamma v^2$$

для вещественных u, v не должна иметь отрицательных значений. Из последнего обстоятельства для констант α и γ следуют необходимые неравенства

$$\alpha \geqslant 0 \quad \text{и} \quad \gamma \geqslant 0. \tag{5}$$

С другой стороны, если подставить разложение для ρ в дифференциальное уравнение (4), то, положив $u = 0$, $v = 0$, мы получим

$$2(\alpha+\gamma) = \frac{e^{-2a} - e^{2a}}{4}.$$

Так как константа a является значением ρ в точке $O = (0,0)$ и поэтому положительна, то здесь правая часть отрицательна, т. е. мы приходим к неравенству

$$\alpha + \gamma < 0,$$

что противоречит неравенствам (5).

Поэтому наше предположение, что точка максимума лежит во внутренней части куска поверхности, оказывается неверным и высказанное выше предложение доказано.

Отсюда непосредственно следует, что *замкнутая поверхность без особенностей постоянной положительной кривизны, равной* 1, *является обязательно сферой радиуса* 1. Этот результат выражает также тот факт, что сфера как целое неизгибаема, т. е. не может быть изогнута без того, чтобы на поверхности не появилась какая-либо особенность.

Наконец, для незамкнутой поверхности, из этих рассмотрений вытекает следующий результат: если мы вообразим произвольный кусок, вырезанный из сферы, и будем его произвольно изибать, то точка максимума большего из двух имеющихся главных радиусов кривизны будет находиться всегда на крае куска поверхности.

Гёттинген, 1900 г.

ОСНОВАНИЯ МАТЕМАТИКИ

ОБ ОСНОВАНИЯХ ЛОГИКИ И АРИФМЕТИКИ*)

В то время, как в исследованиях оснований геометрии сегодня мы в основном единодушны относительно избираемого пути и поставленных целей, с вопросом об основании арифметики ситуация совершенно иная: здесь в настоящее время резко противостоят друг другу самые различные мнения исследователей.

Трудности, встречающиеся при обосновании арифметики, частично действительно отличаются от тех, которые надо было преодолеть при обосновании геометрии. При исследовании основ геометрии можно было обойти некоторые затруднения чисто арифметической природы; но при обосновании арифметики ссылка на другую основную дисциплину становится уже недопустимой [2]. Подвергнув краткому критическому разбору взгляды отдельных исследователей я смогу с бóльшей четкостью выявить те существенные трудности, которые встречаются при обосновании арифметики.

Л. Кронекер, как известно, усматривал в понятии целого числа коренной фундамент арифметики; он составил себе мнение, что целое число, и притом как общее понятие (значение параметра), существует прямо и непосредственно; это помешало ему осознать, что понятие целого числа нуждается в обосновании и может быть обосновано. Поскольку это так, я позволю себе назвать его *догматиком*: он воспринимает целое число с его существенными свойствами как догму, и затем уже не оглядывается назад.

Г. Гельмгольц представляет точку зрения *эмпирика*; однако точка зрения чистого опыта опровергается, как мне кажется, указанием на то, что из опыта, т. е. посредством эксперимента, никогда нельзя придти к заключению о возможности или существовании сколь угодно большого числа, ибо число предметов, являющихся объектом нашего опыта, даже если оно велико, все же не превосходит некоторого конечного предела.

Э. Б. Кристоффеля и всех тех противников Кронекера, которые под влиянием правильного чувства, подсказывавшего им, что без понятия иррационального числа весь анализ оказывается осужденным на бесплодие, пытались спасти существование иррационального числа путем отыскания «положительных» свойств этого понятия или другими аналогичными способами, — я позволю себе назвать *оппортунистами*. Однако опровержение точки зрения Кронекера, по моему мнению, ими, по сути дела, не было достигнуто.

Из ученых, которые глубже проникли в существо понятия «целое число», я упомяну следующих.

Г. Фреге ставит себе задачу обосновать законы арифметики средствами *логики*, понимая эту последнюю в обычном смысле. Его заслугой являет-

---

*) Über die Grundlagen der Logik und Arifmetik. — Verhandl. des 3 intern. Math. Kongresses in Heidelberg. Leipzig, 1905, S. 174–185. [1] *Перевод З. А. Кузичевой.*

ся правильное понимание существенных свойств понятия «целое число», а также значения выводов посредством полной индукции.

Но, проводя последовательно свою точку зрения, он среди прочего принимает и тот основной закон, согласно которому понятие (множество) определено и может быть непосредственно применено, если только относительно каждого объекта известно, попадает ли он под это понятие или нет [3]; при этом он не налагает никаких ограничений на понятие «каждый» и, таким образом, оказывается под ударами тех теоретико-множественных парадоксов, которые заключаются, например, в понятии множества всех множеств и которые показывают, как мне кажется, что концепции и средства исследования логики, понятые в обычном смысле, не в состоянии удовлетворить тем строгим требованиям, которые ставит теория множеств. Напротив, *устранение подобных противоречий и объяснение этих парадоксов следует с самого начала рассматривать как главную цель при исследованиях, касающихся понятия числа.*

Р. Дедекинд ясно осознал те математические трудности, которые встречаются при обосновании понятия числа, и весьма проницательно начал с построения теории целого числа [4]. Все же его метод я позволю себе назвать *трансцендентальным*, поскольку он доказывает существование бесконечного путем, основная идея которого используется таким же образом и философами; этот путь я, однако, не могу признать удобопроходимым и надежным, так как при этом приходится пользоваться понятием совокупности всех вещей, а в этом понятии кроется неизбежное противоречие.

Г. Кантор чувствовал упомянутое противоречие, и это его чувство нашло свое выражение в том, что он различал «консистентные» и «неконсистентные» множества. Но так как Кантор не установил, по моему мнению, никаких строгих критериев для этого различия, то я его точку зрения по этому пункту должен характеризовать как оставляющую еще широкое поле для *субъективного* мнения и не дающую поэтому никакой объективной уверенности.

Я придерживаюсь того мнения, что все затронутые трудности могут быть преодолены и что можно прийти к строгому и вполне удовлетворительному обоснованию понятия числа, а именно, с помощью метода, который я называю *аксиоматическим*; основную его идею я хотел бы обрисовать в данном докладе; строгое и последовательное проведение и развитие этого метода я оставляю на будущее.

Обычно характеризуют арифметику как часть логики и при обосновании арифметики чаще всего предполагают традиционные основные понятия логики известными. Однако, присматриваясь более внимательно, мы замечаем, что при обычном изложении законов логики применяются уже некоторые основные понятия арифметики, например, понятие множества, отчасти понятие числа, особенно в смысле количества. Мы попадаем, таким образом, в порочный круг, а потому для избежания парадоксов необходимо в некоторой части одновременное развитие и законов логики, и законов арифметики,

Вследствие краткости доклада я могу только наметить то, как я представляю себе это совместное построение. Поэтому я прошу меня извинить, если мне удастся дать вам только приблизительное представление о том, в каком направлении продвигаются мои исследования. Кроме того, для облегчения

понимания я буду пользоваться обычным «словесным» языком и выраженными с его помощью законами логики более широко, чем это желательно при точном построении.

Некоторый объект нашего мышления мы будем называть *мыслимой вещью* или, короче, *вещью* и обозначать каким-либо знаком [5]. В основу нашего исследования мы кладем сначала мыслимую вещь 1 (единицу). Соединение этой вещи с самой собой, по два, по три или по нескольку раз, как-то:

$$11, \quad 111, \quad 1111,$$

мы будем называть *комбинацией* вещи 1 с самой собою; точно так же любые комбинации этих комбинаций, как-то:

$$(1)(11), \quad (11)(11)(11), \quad ((1)(11))(11), \quad ((111)(1))(1),$$

также называются комбинациями той же вещи 1 с самой собою. Эти комбинации опять-таки будут называться просто вещами, а положенная в основу мыслимая вещь 1, в отличие от них, будет называться *простой* вещью [6].

Присоединим теперь другую простую мыслимую вещь и обозначим ее символом $=$ (равно). Затем создадим комбинации этих двух мыслимых вещей, как-то:

$$1=, \ 11=, \ldots, \ (1)(=1)(===), \ ((11)(1)(=))(==), \ 1=1, (11)=(1)(1).$$

Мы говорим, что комбинация a простых вещей $1, =$ *отличается* от комбинации b этих же простых вещей, если они где-либо отклоняются друг от друга по способу комбинирования, по последовательности комбинаций или по выбору входящих в них вещей $1, =$, т. е. если комбинации a и b не *тождественны* друг другу.

Представим себе теперь, что комбинации этих двух простых вещей разбиты на два класса: на класс *существующих* комбинаций и на класс *несуществующих*. Каждая вещь, принадлежащая к классу существующих, отличается от любой вещи, принадлежащей к классу несуществующих. Каждая комбинация двух простых вещей $1, =$ принадлежит к одному из этих двух классов.

Если a является комбинацией двух положенных нами в основу вещей $1, =$, то мы будем обозначать тоже через a и *высказывание*: «a принадлежит к классу существующих вещей», а через $\overline{a}$ — *высказывание*: «a принадлежит к классу несуществующих вещей». Назовем высказывание a *истинным*, если a принадлежит к классу существующих; наоборот, высказывание $\overline{a}$ *истинно*, если a принадлежит к классу несуществующих. Высказывания a и $\overline{a}$ образуют *противоречие*.

Совокупность двух высказываний A и B, которую мы будем обозначать

$$A \mid B$$

и которая словесно выражается так: «из A следует B» или «если A истинно, то B также истинно», мы будем также называть высказыванием, называя при этом A *посылкой*, а B — *заключением*.

Посылка и заключение сами могут состоять опять-таки из нескольких высказываний: A_1, A_2 и, соответственно, B_1, B_2, B_3, и т. д.; символически

$$A_1 \ \textit{и} \ A_2 \mid B_1 \ \textit{л} \ B_2 \ \textit{л} \ B_3,$$

словами: «из A_1 и A_2 следует B_1 либо B_2, либо B_3» и т. д. Используя знак $л$ («либо»), можно было бы устранить знак $|$, так как отрицание нами уже было введено; однако я использую его в этом докладе исключительно для того, чтобы возможно ближе подойти к обычной речи.

Под $A_1, A_2, \ldots$ мы будем понимать те высказывания, которые, кратко выражаясь, возникают из высказывания $A(x)$ путем подстановки на место «произвольного» x мыслимых вещей 1, $=$ и их комбинаций. В таком случае высказывания

$A_1 \quad л \quad A_2 \quad л \quad A_3, \quad \ldots$ и, соответственно, $A_1 \quad и \quad A_2 \quad и \quad A_3, \quad \ldots$

мы будем записывать следующим образом:

$A(x^{(л)})$, словесно: «по крайней мере для одного x»

и, соответственно:

$A(x^{(и)})$, словесно: «для каждого отдельного x»,

усматривая в этой записи только сокращенный способ письма [7].

Из положенных нами в основу двух вещей 1, $=$ мы создадим следующие высказывания:

1. $x = x$,
2. $\{x = y \quad и \quad w(x)\} \mid w(y)$.

При этом x (в смысле $x^{(и)}$) может означать каждую из двух положенных в основу мыслимых вещей и каждую комбинацию этих последних; y (в смысле $y^{(и)}$) точно так же может быть каждой из этих вещей и каждой их комбинацией, а $w(x)$ — «произвольная» комбинация, содержащая «произвольное» x (в смысле $x^{(и)}$); 2-е высказывание словами выражается так: из $x = y$ и $w(x)$ следует $w(y)$ [8].

Высказывания 1 и 2 образуют *определение понятия* $=$ (равно) и в этом смысле называются также *аксиомами*.

Если в аксиомы 1, 2 вместо произвольных x и y подставить простые вещи 1, $=$ или их конкретные комбинации, то получатся конкретные высказывания, которые мы будем называть *следствиями* этих аксиом. Будем рассматривать последовательность некоторых выводов такого рода, что посылки последующего вывода в ней тождественны с заключениями предшествующих ему выводов. Если мы теперь примем посылки предшествующих выводов в качестве посылок, а в качестве заключения — заключение последнего вывода, то мы получим новое высказывание, которое опять-таки может быть названо *следствием* аксиом. Продолжая делать заключения этим методом, мы можем получать и дальнейшие следствия.

Выберем теперь из этих выводов те, которые имеют простую форму высказывания a (утверждения без посылки), и объединим все возникающие таким образом вещи a в класс существующих, в то же время отличающиеся от них вещи пусть принадлежат к классу несуществующих. Мы убеждаемся, что из высказываний 1 и 2 всегда получаются следствия только вида $\mathfrak{a} = \mathfrak{a}$, где $\mathfrak{a}$ есть некоторая комбинация вещей 1, $=$. Аксиомы 1 и 2, со своей стороны, выполняются относительно указанного разбиения вещей на два класса, т. е. являются истинными высказываниями; вследствие этого свойства аксиом 1 и 2 мы назовем определяемое ими понятие $=$ (равно) *непротиворечивым* понятием.

Я хотел бы обратить внимание на то, что аксиомы 1, 2 вообще не содержат высказывания вида $\overline{a}$, т. е. высказывания, благодаря которому некоторая комбинация попадает в класс несуществующих. Таким образом, мы могли бы также удовлетворить этим аксиом, если бы мы поместили в класс существующих все комбинации этих двух простых вещей, а класс несуществующих вещей оставили бы пустым. Ранее выбранное нами разделение на два класса все же лучше показывает, как следует поступать в дальнейшем, когда мы встречаемся с более трудными случаями.

Продолжая построение логических основ математического мышления, мы к двум основным мыслимым вещам 1, = присоединяем, далее, еще три мыслимые вещи: $б$ (бесконечное множество, бесконечное), c (следующее), c' (сопровождающая операция) [9]. Установим для этих последних следующие аксиомы:

3. $c(бx) = б(c'x)$,

4. $c(бx) = c(бy) \mid бx = бy$,

5. $\overline{c(бx) = б1}$.

При этом произвольное x (в смысле $x^{(u)}$) может означать каждое из пяти положенных нами теперь в основу мыслимых вещей и каждую их комбинацию. Мыслимую вещь $б$ мы будем кратко называть *бесконечным множеством*, а комбинацию $бx$ (например, $б1$, $б(11)$, $бc$) — *элементом* этого бесконечного множества [10]. В таком случае аксиома 3 выражает, что за каждым элементом $бx$ следует вполне определенная мыслимая вещь $c(бx)$, которая равна некоторому элементу $б(c'x)$, т. е. опять-таки принадлежит множеству $б$. Аксиома 4 говорит о том, что если за двумя элементами множества $б$ следует один и тот же элемент, то и эти первоначальные элементы равны друг другу. Согласно аксиоме 5, в $б$ не существует элемента, за которым следовал бы элемент $б1$; поэтому этот элемент $б1$ мы будем называть первым элементом в $б$.

Мы должны теперь подвергнуть соответствующему исследованию аксиомы 1–5, подобно тому, как мы это сделали раньше с аксиомами 1, 2; при этом надо отметить, что действие этих аксиом 1, 2 расширилось, поскольку теперь произвольные x, y означают любые комбинации пяти простых вещей, положенных нами в основу.

Мы снова ставим вопрос о том, находятся ли некоторые следствия из аксиом 1–5 в противоречии друг с другом, или же, напротив, положенные нами в основу пять мыслимых вещей $1, =, б, c, c'$ и их комбинации можно так распределить между классом существующих и классом несуществующих, что аксиомы 1–5 по отношению к этому распределению на классы выполняются, т. е. что всякое следствие из этих аксиом становится истинным высказыванием относительно этого распределения на классы. Чтобы ответить на этот вопрос, обратим внимание на то, что аксиома 5 является единственной аксиомой, дающей повод к высказываниям вида $\overline{a}$, т. е. дающей повод к тому, чтобы некоторая комбинация a из пяти положенных в основу мыслимых вещей принадлежала к классу несуществующих. Поэтому высказывания, которые вместе с аксиомой 5 образуют противоречие, во всяком случае должны иметь вид:

6. $c(бx^{(л)}) = б1$;

однако такое следствие из аксиом 1–4 ни в коем случае не может быть получено.

Чтобы усмотреть это, назовем равенство, т. е. мыслимую вещь $a = b$, *однородным равенством* в том случае, когда как a, так и b являются комбинациями двух простых вещей, или когда a и b оба являются комбинациями трех, или — оба четырех, или бóльшего числа простых вещей; например, равенства

$$(11) = (c\,б), \qquad (cc) = (б\,c'), \qquad (c11) = (б1 =),$$
$$(c1)(c1) = (1111), \qquad (c(cc'б)) = (1ббб1),$$
$$((cc)(111)) = ((1)(11)(11)), \qquad (cб111 =) = (ббб111б)$$

называются однородными. Из одних только аксиом 1, 2 следуют, как мы видели раньше, только однородные равенства, а именно равенства вида $\mathfrak{a} = \mathfrak{a}$. Точно так же аксиома 3, если мы в ней за x принимаем некоторую мыслимую вещь, дает нам только однородные равенства. В заключении аксиомы 4 опять-таки должны всегда находиться только однородные равенства, если только посылка представляет собою однородное равенство; таким образом, следствием аксиом 1–4 могут быть только однородные равенства. Между тем, равенство 6, которое как раз и должно быть доказано, безусловно не однородно, так как в нем вместо $x^{(л)}$ надо взять некоторую комбинацию, вследствие чего левая его часть будет представлять комбинацию трех или большего числа простых вещей, между тем как его правая часть попрежнему остается комбинацией двух простых вещей: $б$ и 1.

Тем самым, как мне кажется, указана основная идея, дающая возможность убедиться в правильности моего утверждения; для полного проведения доказательства необходимо понятие конечного порядкового числа и некоторые определенные теоремы, касающиеся понятия равночисленности, которые на этой стадии можно уже действительно без труда установить и вывести; для полного проведения указанной основной идеи надо принять во внимание еще и те точки зрения, на которые я кратко укажу в конце своего доклада (см. V).

Желаемое распределение на классы получается, таким образом, если все вещи a, где a есть вывод из аксиом 1–4, причислить к классу существующих, а все отличающиеся от них вещи, в частности, вещь $c(бx) = б1$, отнести к классу несуществующих. Благодаря найденному таким образом свойству установленных аксиом, мы убеждаемся в том, что эти последние никогда не приводят к противоречию, а потому определяемые ими мыслимые вещи $б$, c, c' называем понятиями или операциями, *непротиворечивыми* или *существующими без противоречий*. В частности, что касается понятия о бесконечном $б$, то посредством вышеизложенного истолкования утверждение *о существовании бесконечного* $б$ оказывается оправданным, так как оно получило теперь вполне определенное значение и постоянно применяемое в дальнейшем содержание.

Намеченное здесь исследование представляет собой первый случай, где удалось провести прямое доказательство непротиворечивости аксиом, в то время, как обычные до сих пор методы таких доказательств, особенно в геометрии — методы подходящей специализации или построения примеров, в данном случае отказываются служить.

Это прямое доказательство в данном случае удается, как видно, в значительной мере благодаря тому обстоятельству, что высказывание вида $\overline{a}$, т. е. высказывание, согласно которому некоторая определенная комбинация должна принадлежать к классу несуществующих, выступает в качестве утверждения только в одном месте, именно в аксиоме 5.

Переведя на выбранный мною язык известную аксиому о полной индукции, мы подобным же образом придем к заключению о непротиворечивости расширенной таким образом системы аксиом, т. е. к доказательству непротиворечивого *существования так называемой наименьшей бесконечности*[1] (т. е. *порядкового типа* $1, 2, 3, \ldots$).

Не представляет затруднения обосновать, исходя из вышеустановленных принципов, понятие конечного порядкового числа; такое обоснование зиждется на аксиоме о том, что каждое множество, которое содержит первый элемент порядкового числа и которое, всякий раз как оно, содержа некоторый элемент, содержит также и следующий за ним элемент, должно обязательно содержать и последний элемент. Доказательство непротиворечивости этой аксиомы получается здесь очень легко посредством использования какого-либо примера; таковым может служить хотя бы число два. В таком случае надо будет показать, что возможен такой порядок элементов конечного порядкового числа, при котором каждое подмножество этого последнего имеет как первый, так и последний элемент — этот факт мы доказываем, определяя мыслимую вещь $<$ аксиомой

$$(x < y \quad \text{и} \quad y < z) \mid x < z$$

и убеждаясь затем в непротиворечивости установленных аксиом после присоединения этой новой аксиомы, как только x, y, z обозначают произвольные элементы конечного порядкового числа. При использовании факта существования наименьшего бесконечного выводится также и теорема о том, что для всякого конечного порядкового числа может быть найдено бóльшее порядковое число.

Принципы, которыми следует руководствоваться при построении и дальнейшем выводе законов математического мышления в том духе, который мы имеем в виду, вкратце суть следующие.

I. Достигнув в развитии теории известного этапа, я имею право некоторое дальнейшее высказывание считать правильным, как только установлено, что оно, будучи присоединено в качестве аксиомы к высказываниям, которые были найдены до сих пор в качестве правильных, не приводит к противоречию, т. е. что оно приводит к следствиям, которые, по отношению к некоторому определенному разделению вещей на классы существующих и несуществующих, все являются правильными высказываниями.

II. Встречающиеся в аксиомах «произвольные» — которые заменяют понятия «каждый» или «все» обычной логики — могут представлять только те мыслимые вещи и комбинации этих последних, которые либо должны быть на известной ступени приняты в качестве основных, либо полностью определены. Поэтому при выводе следствий из аксиомы «произвольные», встречающиеся в аксиомах, следует замещать только такими мыслимыми

[1] См. раздел 2 (непротиворечивость аксиом арифметики) моего доклада «Математические проблемы», сделанного на Международном математическом конгрессе в Париже в 1900 году (имеется перевод в т. 2 наст. издания. — *Ред.*)

вещами и их комбинациями. Следует также надлежащим образом обратить внимание на то, что при присоединении и принятии в основу новой мыслимой вещи значение всех предшествующих аксиом расширяется и, соответственно, они должны быть подвергнуты целесообразному изменению [11].

III. *Множество* вообще определяется как мыслимая вещь m, а комбинации mx называются элементами множества m, так что, — в противоположность обычной трактовке, — понятие элемента появляется лишь как более позднее порождение понятия множества.

Как понятие «множество», так и понятия «*сопоставление*», «*преобразование*», «*соотношение*», «*функция*» суть мыслимые вещи, для которых так же, как это было сделано раньше с понятием «бесконечность», следует соответствующим образом выбрать подходящие аксиомы, а затем, в случае возможности разбиения соответствующих комбинаций на класс существующих и несуществующих, можно убедиться, что эти понятия существуют непротиворечиво [12].

В пункте I выражен тот *творческий* принцип, который позволяет нам свободно пользоваться созданием все новых и новых понятий, ограничивая это образование новых понятий одним только условием: избегать противоречия. Парадоксы, упомянутые в начале этого доклада, оказываются невозможными благодаря принципам II и III; в частности, это касается парадокса о множестве всех множеств, не содержащих самих себя в качестве элемента.

Чтобы сделать убедительным далеко идущее по своему содержанию совпадение понятия множества, определенного в пункте III, с обычным понятием множества, я докажу следующую теорему.

Пусть $1, \ldots, \mathfrak{a}, \ldots, \mathfrak{f}$ суть мыслимые вещи, положенные в основу на известной ступени построения теории, и пусть $a(\xi)$ является их комбинацией, содержащей произвольное ξ; далее, пусть $a(\alpha)$ — истинное высказывание (т. е. $a(\alpha)$ принадлежит к классу существующих); в таком случае безусловно существует мыслимая вещь m такого рода, что $a(mx)$ для произвольного x представляет только истинные высказывания (т. е. $a(mx)$ всегда находится в классе существующих), и обратно, всякая вещь ξ, для которой $a(\xi)$ есть истинное высказывание, будет равна некоторой комбинации $mx^{(л)}$, так что высказывание

$$\xi = mx^{(л)}$$

истинно, т. е. вещи ξ, для которых $a(\xi)$ есть истинное высказывание, образуют элементы множества m в смысле вышеприведенного определения.

Для доказательства установим следующую аксиому: пусть m есть мыслимая вещь, для которой высказывания

$$7.\quad a(\xi) \mid m\xi = \xi,$$

$$8.\quad \overline{a(\xi)} \mid m\xi = \alpha$$

истинны, т. е. если ξ есть такого рода вещь, что $a(\xi)$ принадлежит к классу существующих, то $m\xi = \xi$; в противоположном же случае $m\xi = \alpha$. Присоединим эту аксиому к аксиомам, которые имеют место для вещей $1, \ldots, \alpha, \ldots, \mathfrak{f}$, и положим, что при этом мы придем к противоречию, т. е. что

вещи $1, \ldots, \alpha, \ldots, \mathfrak{f}$ одновременно приводят к следующим следствиям:

$$p(m) \quad \text{и} \quad \overline{p(m)},$$

где $p(m)$ есть некоторая комбинация вещей $1, \ldots, \mathfrak{f}, m$. При этом аксиома 8, будучи выражена словами, сводится к утверждению, что $m\xi = \alpha$, если $a(\xi)$ принадлежит к классу несуществующих. Всюду, где в $p(m)$ вещь m выступает в комбинации $m\xi$, заменим, в соответствии с аксиомами 7 и 8 и принимая во внимание аксиому 2, комбинации $m\xi$ через ξ или, соответственно, через α; из $p(m)$ этим способом получается $q(m)$ (где $q(m)$ уже более не содержит вещь m в комбинации mx); в таком случае $q(m)$ должно было бы быть следствием из аксиом, положенных вначале для $1, \ldots, \alpha, \ldots, \mathfrak{f}$, и тем самым быть истинным, если мы в качестве m примем одну из этих вещей, например 1. Так как подобное же рассуждение справедливо и для высказывания $\overline{p(m)}$, то и для первоначальной ступени, когда в основу были положены вещи $1, \ldots, \alpha, \ldots, \mathfrak{f}$, должно было бы существовать противоречие

$$q(1) \quad \text{и} \quad \overline{q(1)}.$$

Но это невозможно, если сначала предположить, что существование вещей $1, \ldots, \mathfrak{f}$ непротиворечиво. Поэтому мы должны отбросить наше предположение о том, что может произойти противоречие, т. е. m существует непротиворечиво, что и требовалось доказать.

IV. Если хотят заданную определенным образом систему аксиом исследовать с помощью вышеуказанных принципов, то комбинации вещей, положенных в основу, надо разбить на указанные два класса — класс существующих и класс несуществующих; при этом на долю аксиом выпадает роль предписаний, которым это разбиение должно удовлетворять.

Главная трудность будет состоять в том, чтобы убедиться в возможности разбить все вещи на два класса — класс существующих и класс несуществующих [13]. Вопрос о возможности такого разбиения, по существу, равносилен вопросу о том, приводят или не приводят к противоречию следствия, которые могут быть получены из аксиом посредством их специализации и совместного их использования в ранее изложенном смысле, *если присоединить еще известные способы логических умозаключений, каковы*

$$\{(a \mid b) \quad и \quad (\overline{a} \mid b)\} \mid b$$

$$\{(a \quad л \quad b) \quad и \quad (a \quad л \quad c)\} \mid \{a \quad л \quad (b \quad и \quad c)\}.$$

В таком случае непротиворечивость аксиом может быть проверена либо тем, что будет показано, как предполагаемое противоречие должно было бы проявиться уже на более ранней ступени развития теории, либо путем предположения, что существует доказательство, которое, исходя из аксиом, приводит к противоречию, и последующего выяснения того факта, что такое доказательство невозможно, т. е. что оно содержит в себе противоречие. Так, например, набросанный ранее эскиз доказательства непротиворечивости существования бесконечного сводится к тому, что, исходя из аксиом 1–4, невозможно доказать равенство 6.

V. Когда до сих пор шла речь о *многих* мыслимых вещах, комбинациях, комбинациях *многократного* вида или *многих* произвольных, то при этом всегда понималось ограниченное число таких вещей. После того

как мы установили определение конечного числа, мы оказываемся в состоянии трактовать этот способ выражения в его общем значении. Теперь на основании определения конечного числа (в соответствии с идеей полной индукции) оказывается также возможным с помощью рекуррентного приема точно описать значение «произвольного» следствия и «отличия» некоторого высказывания от всех высказываний определенного рода. Именно так, в частности, нужно представлять себе полное определение ранее намеченного доказательства того, что высказывание $c(\mathfrak{b}x^{(a)}) = \mathfrak{b}1$ отличается от каждого высказывания, которое получено, как следствие, из аксиом 1–4 после конечного числа шагов; именно самое доказательство нужно рассматривать как некоторое математическое образование, именно, как конечное множество, элементы которого связаны высказываниями, выражающими, что доказательство ведет от аксиом 1–4 к равенству 6, и надо в таком случае показать, что такое доказательство содержит противоречие и, таким образом, не существует непротиворечиво в определенном нами смысле.

Подобно тому как может быть доказано существование наименьшей бесконечности, может быть доказано также и существование совокупности действительных чисел; действительно, аксиомы, как они были установлены мною для действительных чисел [14], могут быть выражены в точности такими же формулами, как и установленные до сих пор аксиомы. Что же касается, в частности, той аксиомы, которую я назвал аксиомой полноты, то она выражает, что совокупность действительных чисел содержит каждое множество, элементы которого равным образом удовлетворяют предшествующим аксиомам; при этом слово «содержит» надо понимать в смысле взаимно однозначного соответствия элементов. При таком толковании аксиома полноты представляет собою требование, тоже выражаемое с помощью формул вышеуказанного характера, а аксиомы для совокупности действительных чисел качественно ни в каком смысле не отличаются от аксиом, необходимых, например, для определения целых чисел. В познании этого факта, как мне думается, заключается объективное опровержение взгляда, который защищал *Кронекер* и который в начале моего доклада был квалифицирован как догматическая трактовка основ арифметики.

Точно так же доказывается, что основным понятиям канторовского учения о множествах и в частности канторовским алефам присуще непротиворечивое существование.

Гейдельберг, август 1904 г.

АКСИОМАТИЧЕСКОЕ МЫШЛЕНИЕ*)

Подобно тому как в жизни народов отдельный народ может процветать только в том случае, если и у соседних народов дела идут хорошо, и интересы государств требуют не только поддержания порядка внутри каждого отдельного государства, но и надлежащего упорядочения связей между государствами, так же обстоит дело и в жизни науки. Понимая это, наиболее выдающиеся представители математического мышления всегда проявляли большой интерес к законам и порядкам в смежных науках и — в первую очередь на благо самой математики — стремились к установлению связей со смежными науками, в особенности с обширными царствами физики и теории познания. Я полагаю, что сущность этих связей и причина их плодотворности предстанут перед нами наиболее отчетливо, если я попытаюсь охарактеризовать тот общий метод исследования, который, насколько можно судить, играет все более важную роль в математике последнего времени: я имею в виду *аксиоматический метод*.

Стоит нам собрать воедино факты любой более или менее обширной области знания, как мы сразу замечаем, что эти факты могут быть упорядочены. Такое упорядочение достигается всякий раз с помощью своего рода *каркаса понятий*, возведенного с таким расчетом, чтобы отдельному объекту данной области знания соответствовало понятие из этого каркаса, а каждому факту из этой области знания соответствовала некоторая логическая связь между понятиями. Такой каркас понятий есть не что иное, как *теория* данной области знания.

Например, геометрические факты при упорядочении выстраиваются в геометрию, арифметические факты — в теорию чисел, факты, касающиеся статических, механических, электродинамических явлений — в такие теории, как статика, механика, электродинамика, а факты из физики газов — в теорию газов. Аналогичным образом обстоит дело с такими областями знания, как термодинамика, геометрическая оптика, элементарная теория излучения, теория теплопроводности, а также теория вероятностей и теория множеств. Сказанное относится и к таким специальным чисто математическим областям знания, как теория поверхностей, теория Галуа разрешимости уравнений, теория простых чисел, ничуть не в меньшей степени, чем ко многим областям знания, лежащим далеко от математики, например, к некоторым разделам психофизики или теории денег.

Рассматривая ту или иную теорию более подробно, мы всякий раз обнаруживаем, что в основании каркаса лежит небольшое число утверждений из данной области науки, которых достаточно, чтобы из них с помощью логических законов построить весь каркас.

---

*) Axiomatisches Denken. — Math. Ann., 1918, Bd. 78, S. 405–415. (Доклад, прочитанный 11 сентября 1917 г. в Цюрихе на заседании Швейцарского математического общества.) *Перевод Ю. А. Данилова.*

Так, в геометрии теорем о линейности уравнения плоскости и об ортогональном преобразовании координат точки достаточно для того, чтобы средствами анализа полностью построить всю обширную науку геометрии евклидова пространства. Для построения, скажем, теории чисел достаточно законов, которым подчиняются арифметические действия над целыми числами. В статике такую же роль играет утверждение о параллелограмме сил, в механике — лагранжевы дифференциальные уравнения движения и в электродинамике — уравнения Максвелла, дополненные предположением, что электрон представляет собой твердую заряженную частицу. Термодинамику можно полностью построить на понятии функции энергии и определении температуры и давления как производных по аргументам этой функции — энтропии и объему. В центре элементарной теории излучения находится теорема Кирхгофа о взаимосвязи между испусканием и поглощением; в теории вероятностей основополагающей является теорема о гауссовом законе распределения, в теории газов — теорема об энтропии как взятом со знаком минус логарифме вероятности состояний, в теории поверхностей — представление элемента дуги в виде квадратичной дифференциальной формы, в теории уравнений — теорема о существовании корней, в теории простых чисел — теорема о вещественности и распределении нулей дзета-функции Римана $\zeta(s)$.

Такие основополагающие теоремы с определенной точки зрения можно рассматривать как *аксиомы данной отдельной области знания*: последующее развитие этой области знания сводится исключительно к логическим построениям на базе уже имеющегося каркаса понятий. В особенности в чистой математике такая точка зрения стала господствующей, и именно этому мы обязаны мощным развитием геометрии, арифметики, теории чисел и всего анализа.

Тем самым в названных случаях проблема обоснования отдельной области знания обрела свое решение; но это решение носило лишь предварительный характер. Действительно, в отдельных областях знания возникла потребность в обосновании самих упомянутых выше теорем, принятых в качестве аксиом и положенных в основу. Так были получены «доказательства» линейности уравнения плоскости и ортогональности преобразования, выражающего движение, законов арифметики, параллелограмма сил, лагранжевых уравнений движения и закона Кирхгофа, устанавливающего взаимосвязь между испусканием и поглощением, теоремы об энтропии и теоремы о существовании корней уравнения.

Но как показывает критическая проверка такого рода «доказательств», они сами по себе не являются доказательствами, а лишь позволяют осуществить сведение к некоторым лежащим более глубоко теоремам, которые в свою очередь могут быть приняты в качестве новых аксиом вместо доказываемых теорем. Так возникает то, что ныне принято называть собственно *аксиомами* геометрии, арифметики, статики, механики, теории излучения или термодинамики. Эти аксиомы образуют слой аксиом, лежащий более глубоко, чем тот слой, который характеризуется упоминавшимися выше теоремами, первоначально принятыми за основополагающие в отдельных областях знания. Тем самым использование аксиоматического метода в том виде, как он здесь изложен, оказывается эквивалентным *углублению фундамента* данной области знания, столь необходимому любому зданию по

мере того, как его надстраивают, увеличивают его высоту, не переставая при этом заботиться о его надежности.

Поскольку теория некоторой области знания (т. е. представляющий эту область каркас понятий) должна соответствовать своему предназначению, а именно служить целям ориентации и упорядочения, она должна прежде всего удовлетворять двум требованиям: *во-первых*, давать возможность судить о *зависимости* или *независимости* теорем теории и, *во-вторых*, гарантировать *непротиворечивость* всех теорем теории. Аксиомы каждой теории подлежат тщательной проверке с этих двух точек зрения.

Начнем с зависимости или независимости аксиом.

Классическим примером проверки независимости аксиомы может служить *аксиома о параллельных* в геометрии. На вопрос о том, не следует ли утверждение о параллельных из других аксиом, Евклид ответил отрицательно, включив его в число аксиом. Избранный Евклидом метод изучения предмета стал образцом аксиоматического исследования, и со времен Евклида геометрию вообще принято считать эталоном аксиоматизированной науки.

Другой пример исследования зависимости или независимости аксиом дает классическая механика. На первых порах в качестве аксиом механики можно, как я уже упоминал, взять уравнения движения в форме Лагранжа, т. е. эти уравнения в своей общей формулировке, для любых сил и любых дополнительных условий, вполне могут служить надежным фундаментом для обоснования механики. Но при более подробном анализе оказывается, что при построении механики нет необходимости предполагать наличие как любых сил, так и любых дополнительных условий, что позволяет сузить множество предположений. Осознание этого факта приводит, с одной стороны, к системе аксиом Больцмана, предполагающего наличие одних лишь сил, причем сил особого рода — центральных, но не вводящего никаких дополнительных условий, и к системе аксиом Герца, отвергающего силы и исходящего из дополнительных условий, а именно из предположения о жестких связях. Обе эти системы аксиом представляют собой более глубокий слой продолжающейся аксиоматизации механики.

Если при обосновании теории Галуа разрешимости уравнений мы примем в качестве аксиомы существование корней уравнения, то такая аксиома заведомо будет зависимой: теорема о существовании корней уравнения, как впервые показал Гаусс, может быть доказана, исходя из арифметических аксиом.

Аналогичным образом обстоит дело и в том случае, если мы примем, например, за аксиому в теории простых чисел теорему о вещественности нулей дзета-функции Римана $\zeta(s)$: при переходе на более глубокий уровень чисто арифметических аксиом доказательство этой теоремы стало бы необходимым; только оно гарантировало бы нам сохранение важных следствий, которые мы установили, постулировав вещественность нулей дзета-функции.

Особый интерес для аксиоматического подхода представляет вопрос о зависимости теорем той или иной области знания от аксиомы *непрерывности*.

В теории вещественных чисел доказывается, что аксиома измерения (так называемая аксиома Архимеда) не зависит от всех остальных арифметичес-

ких аксиом. Как известно, знание этого обстоятельства имеет существенное значение для геометрии, но, как мне кажется, оно представляет принципиальный интерес и для физики, ибо приводит к следующему результату: то, что мы путем сложения земных расстояний достигаем размеров космических тел и расстояний между ними, т. е. можем измерять земными мерами небесные длины, равно как и то, что расстояния внутри атома могут быть выражены в метрических мерах, отнюдь не является чисто логическим следствием теорем о конгруэнтности треугольников и геометрических конфигурациях, а представляет собой результат исследования эмпирии. Выполнимость аксиомы Архимеда в природе требует в этом смысле такого же экспериментального подтверждения, как, например, теорема о сумме углов треугольника.

В общем виде я мог бы сформулировать аксиому непрерывности в физике следующим образом: «Если некоторое физическое утверждение должно выполняться с любой, сколь угодно высокой степенью точности, то должно быть возможно указать малые области, свободное варьирование внутри которых предположений, сделанных при формулировке утверждения, не приведет к выходу за пределы предписанной точности». По существу эта аксиома лишь явно выражает то, что составляет самую сущность эксперимента; физики всегда принимали ее, но до сих пор не формулировали.

Например, аксиома непрерывности с необходимостью используется, когда, следуя Планку, из аксиомы невозможности *вечного двигателя второго рода* выводят второе начало термодинамики.

То что аксиома непрерывности необходима при обосновании статики для доказательства теоремы о *параллелограмме сил* (по крайней мере при том выборе остальных аксиом, который первым приходит в голову), показал Гамель — весьма интересным способом, используя теорему о полной упорядочиваемости континуума.

Аксиомы классической механики можно перевести на более глубокий уровень, если с помощью аксиомы непрерывности мысленно разложить непрерывное движение на короткие следующие один за другим участки равномерного прямолинейного движения под действием импульсов и использовать в качестве существенной аксиомы механики *принцип максимума Бертрана*, согласно которому движение, реально возникающее после каждого толчка, всегда есть то движение, кинетическая энергия которого максимальна по сравнению со всеми движениями, совместимыми с законом сохранения энергии.

Мне не хотелось бы вдаваться здесь в подробное изложение новейших работ по обоснованию физики, в частности электродинамики, которые целиком и полностью представляют собой континуальные теории и поэтому широчайшим образом используют требование непрерывности, поскольку эти исследования пока не доведены до конца [1].

Переходим теперь ко второму из названных выше требований, а именно к вопросу о *непротиворечивости* аксиом; ясно, что этот вопрос еще более важен, поскольку наличие противоречия в любой теории грозит опрокинуть ее всю.

Установление внутренней непротиворечивости даже давно признанных и доказавших свою плодотворность теорий сопряжено с немалыми трудностями; вспомним хотя бы возражения, связанные с *обращением скоростей* и *возвращаемостью* в кинетической теории газов.

Внутренняя непротиворечивость теории часто считается самоочевидной, в то время как в действительности для ее доказательства требуются глубокие математические соображения. В качестве примера рассмотрим задачу из элементарной теории *теплопроводности*, а именно задачу о распределении температуры внутри однородного тела, поверхность которого поддерживается при данной температуре, изменяющейся от точки к точке; в этом случае предположение о существовании состояния температурного равновесия не приводит к внутренним противоречиям в теории. Для установления же этого обстоятельства необходимо доказать, что соответствующая краевая задача теории потенциала всегда разрешима, ибо только решение этой краевой задачи показывает, что удовлетворяющее уравнению теплопроводности распределение температуры вообще невозможно.

Но в физике недостаточно еще, чтобы теоремы той или иной теории были самосогласованы; требуется также, чтобы они не противоречили теоремам из смежных областей.

Так, аксиомы элементарной теории излучения, как я недавно показал [2], позволяют не только обосновать *теорему Кирхгофа* об испускании и поглощении, но и приводят к одному специальному утверждению об отражении и преломлении лучей света, а именно к теореме: «Если два луча естественного света с одинаковой энергией падают в одно и то же место на поверхности раздела двух сред по таким направлениям, что один луч после прохождения через поверхность раздела, а другой — после отражения от нее идут в одном и том же направлении, то при их объединении снова возникает луч естественного света, причем с такой же энергией». Эта теорема (как оказалось в действительности) не противоречит оптике и может быть выведена как следствие из электромагнитной теории света.

Результаты *кинетической теории газов*, как известно, наилучшим образом согласуются с *термодинамикой*.

Аналогично, *инерция электромагнитного излучения* и *эйнштейновская гравитация* согласуются с соответствующими понятиями классических теорий, поскольку эти понятия можно рассматривать как предельные случаи более общих понятий новых теорий.

Наоборот, *современная квантовая теория* и успехи в познании строения атома привели к законам, прямо противоречащим всей предшествующей электродинамике, по существу построенной на уравнениях Максвелла; поэтому современная электродинамика, как всем известно, нуждается в новом обосновании и существенной переработке.

Как следует из всего сказанного, устранение установленных противоречий в физических теориях всегда должно происходить с помощью иного выбора аксиом, и проблема заключается в том, чтобы в результате такого выбора все наблюдаемые физические законы стали логическими следствиями выбранных аксиом.

С иной ситуацией мы сталкиваемся, когда противоречия встречаются в чисто теоретических областях знания. Классическим примером такого рода может служить теория множеств, в частности восходящий еще к Кантору *парадокс множества всех множеств*. Этот парадокс настолько существен, что побудил некоторых весьма уважаемых математиков, например Кронекера и Пуанкаре, вообще отказать всей теории множеств — одной из самых плодотворных и жизнеспособных областей математики — в праве на существование.

Но и из столь затруднительной ситуации удалось найти выход с помощью аксиоматического метода. Это сделал Цермело, который, введя подходящую аксиому, с одной стороны ограничил произвол в определениях множеств, а с другой стороны, в строго определенном смысле сузил круг допустимых утверждений об элементах множеств и развил теорию множеств таким образом, что отпали противоречия, о которых я упоминал, но значимость и применимость теории, несмотря на наложенные ограничения, сохранились.

До сих пор речь во всех случаях шла о противоречиях, которые были обнаружены в ходе развития теории и для устранения которых возникала необходимость внести изменения в систему аксиом. Но чтобы восстановить репутацию математики как эталона строгой науки, недостаточно просто избавляться от имеющихся противоречий: принципиальное требование аксиоматической теории должно простираться дальше, а именно надо знать, что внутри данной области знания, построенной на основе принятой системы аксиом, никакие противоречия *вообще невозможны*

Следуя этому требованию, я доказал в «Основаниях геометрии» непротиворечивость принятых там аксиом, продемонстрировав, что любое противоречие в следствиях из геометрических аксиом с необходимостью должно было бы означать некоторое противоречие в арифметике системы вещественных чисел.

И в физике, понятно, всегда достаточно свести вопрос о *внутренней непротиворечивости* к вопросу о непротиворечивости аксиом арифметики. Так, я доказал непротиворечивость аксиом *элементарной теории излучения*, построив для этой теории систему аксиом, состоящую из аналитически независимых фрагментов (непротиворечивость математического анализа при этом предполагается).

Аналогичным образом можно и должно поступать, сообразуясь с обстоятельствами, и при построении математической теории. Например, если в теории групп Галуа мы примем за аксиому теорему о существовании корней или в теории простых чисел — теорему о вещественности нулей римановой дзета-функции $\zeta(s)$, то и в том, и в другом случае доказательство непротиворечивости системы аксиом сводится к тому, чтобы доказать средствами анализа теорему о существовании корней или теорему Римана о дзета-функции, — и лишь этим обеспечивается завершенность теории.

Вопрос о непротиворечивости системы аксиом для *вещественных чисел* можно, используя теоретико-множественные понятия, свести к такому же вопросу для целых чисел; это — заслуга теорий иррациональных чисел Вейерштрасса и Дедекинда.

Лишь в двух случаях, а именно когда речь идет об аксиомах самих *целых чисел* и обосновании *теории множеств*, этот прием, состоящий в сведении к другой, более узкой области знания, становится явно неприменимым, ибо помимо логики нет уже ни одной дисциплины, которую при этом можно было бы привлечь.

Но поскольку доказательство непротиворечивости — вещь совершенно обязательная, представляется необходимым аксиоматизировать саму логику и показать, что теория чисел, равно как и теория множеств, составляют лишь части логики.

Этот путь, подготавливавшийся уже давно (не в последнюю очередь

глубокими исследованиями Фреге), наконец, был проложен с величайшим успехом тонким математиком и логиком Расселом. Завершение намеченной Расселом грандиозной программы по *аксиоматизации логики* можно было бы рассматривать как венец всех усилий по аксиоматизации науки.

Но пока завершение этой программы все еще требует новых и разносторонних усилий. По зрелом размышлении нетрудно понять, что вопрос о непротиворечивости теории целых чисел и теории множеств существует не сам по себе, а принадлежит к обширной области труднейших теоретико-познавательных вопросов со специфической математической окраской; чтобы кратко охарактеризовать эту область вопросов, назову проблему *принципиальной разрешимости* любой математической задачи, проблему *контролируемости* результатов математического исследования, вопрос *о критерии простоты* математического доказательства, проблему отношения *содержательности и формализма* в математике и логике и, наконец, проблему *разрешимости* математической задачи *за конечное число операций.*

Аксиоматизацию логики нельзя считать удовлетворительной до тех пор, пока все вопросы такого рода не будут поняты и выяснены.

Последний из названных вопросов, а именно вопрос о разрешимости за конечное число операций, — наиболее известный и чаще всего обсуждаемый, поскольку он глубоко затрагивает самую сущность математического мышления.

Я хотел бы попытаться еще более усилить интерес к нему, указав на некоторые математические проблемы более специального характера, в решении которых этот вопрос играет важную роль.

Как известно, в теории *алгебраических инвариантов* имеется фундаментальная теорема о том, что всегда существует конечное число целых рациональных инвариантов, через которые могут быть рационально выражены все остальные алгебраические инварианты. Данное мною первое общее доказательство этой теоремы полностью удовлетворяет, как я полагаю, нашим пожеланиям в том, что касается простоты и прозрачности; однако это доказательство невозможно видоизменить так, чтобы можно было с его помощью указать верхнюю границу числа элементов в полной системе инвариантов и уж тем более фактически найти само это число. Потребовались соображения совершенно иного рода и совершенно новые принципы, чтобы убедиться, что построение полной системы инвариантов осуществимо с помощью операций, число которых конечно и не превосходит границы, поддающейся вычислению [3].

Аналогичную ситуацию наблюдаем мы и в одном примере из *теории поверхностей.* В геометрии поверхностей четвертого порядка имеется фундаментальный вопрос: из скольких, самое большее, отдельных кусков может состоять такая поверхность?

При ответе на этот вопрос в первую очередь надо доказать, что число связных кусков поверхности должно быть конечно; это легко установить из теоретико-функциональных соображений следующим образом. Предположим, что кусков поверхности бесконечно много, и выберем в каждой части пространства, ограниченной таким куском, по точке. Точка накопления бесконечного множества выбранных точек была бы особой точкой такого типа, который исключен для алгебраических поверхностей.

Такой функционально-теоретический подход никоим образом не позволяет получить верхнюю границу числа кусков поверхности; для этого необходимы гораздо более конкретные рассуждения относительно числа точек пересечения, приводящие к заключению о том, что число кусков поверхности не может быть больше 12.

Этот второй метод, в корне отличный от первого, неприменим и не может быть видоизменен так, чтобы он стал применимым к решению вопроса о том, действительно ли существует поверхность четвертого порядка, состоящая ровно из 12 кусков.

Так как у кватернарной формы четвертого порядка 35 однородных коэффициентов, мы можем наглядно представить ее в виде точки в 34-мерном пространстве. Дискриминант кватернарной формы четвертого порядка имеет степень 108 по коэффициентам формы; если его положить равным нулю, то в 34-мерном пространстве он будет представлять поверхность 108-го порядка. Так как коэффициенты дискриминанта сами являются некоторыми целыми числами, топологический характер дискриминантной поверхности может быть точно установлен по правилам, знакомым нам по дву- и трехмерному пространству, что позволяет получить точное представление о природе и значении отдельных подобластей, на которые дискриминантная поверхность делит 34-мерное пространство. Все поверхности, представляемые точками одной подобласти, состоят из одного и того же числа кусков, что позволяет с помощью весьма трудоемких и нудных вычислений установить, существуют или не существуют поверхности четвертого порядка, состоящие из $n \leqslant 12$ кусков.

Намеченные выше в общих чертах геометрические соображения доставляют третий подход к решению поднятого нами вопроса о наибольшем числе кусков, из которых может состоять поверхность четвертого порядка. Они показывают, что этот вопрос разрешим за конечное число операций. Тем самым принципиально наше требование выполнено: исходная проблема сведена к проблеме типа задачи о вычислении $10^{(10^{10})}$-й цифры десятичного разложения числа π — задачи, разрешимость которой очевидна, хотя решение остается неизвестным.

Наконец, потребовалось (проведенное Рооном) глубокое и трудное алгебро-геометрическое исследование, чтобы доказать, что поверхность четвертого порядка не может состоять из 11 кусков, но может состоять из 10. Таким образом, лишь этот четвертый метод дает полное решение проблемы [4].

Приведенные специальные примеры показывают, сколь различными могут быть методы доказательства, применимые к одной и той же задаче, и заставляют задуматься над тем, сколь необходимо изучать самую сущность математического доказательства, если мы хотим успешно решать такие вопросы, как разрешимость за конечное число операций.

Мне представляется, что принципиальные вопросы такого рода, который я охарактеризовал выше (только что рассмотренный нами вопрос о разрешимости за конечное число операций — лишь последний из перечисленных мной), образуют новую важную область исследований, которую нам еще предстоит освоить, и для ее освоения мы должны — это мое глубокое убеждение — сделать предметом исследования самое понятие специфически математического доказательства точно так же, как астроном должен

учитывать движение точки, из которой он производит наблюдения, физик заботится о теории своего прибора, а философ критикует собственный разум.

Разумеется, выполнение этой программы — пока еще нерешенная задача.

В заключение я хотел бы в нескольких фразах подвести итог моих общих взглядов на сущность аксиоматического метода.

Я придерживаюсь следующей точки зрения. Все, что вообще может быть предметом научного мышления, подпадает, коль скоро созрели условия для формирования теории, под юрисдикцию аксиоматического метода и тем самым математики. При переходе к все более глубоким слоям аксиоматизации в указанном выше смысле мы достигаем и более глубокого проникновения в сущность научного мышления как такового и все более постигаем единство нашего знания. Под знаком аксиоматического метода математике, насколько можно судить, предстоит сыграть ведущую роль во всей науке вообще.

ЛОГИЧЕСКИЕ ОСНОВАНИЯ МАТЕМАТИКИ*)

Мои исследования по новому обоснованию математики[1]) имеют своей целью не что иное, как полностью устранить вошедшее в моду сомнение в надежности математических выводов. Насколько необходимо это исследование, мы видим, когда размышляем, как часто переменчивы и неточны были относящиеся к этому воззрения самых выдающихся математиков, или когда вспоминаем, что некоторыми известными математиками новейшего времени были отвергли выводы, до того считавшиеся незыблемыми.

Для полного разрешения принципиальных трудностей и необходима теория математического доказательства. В сотрудничестве с Паулем Бернайсом и при его существенной помощи я теперь развил эту теорию настолько далеко, что фактически получил безукоризненное обоснование анализа и теории множеств; я даже думаю, что теперь мы продвинулись достаточно, чтобы можно было приняться за великие классические проблемы теории множеств типа проблемы континуума и не менее важные все еще открытые проблемы математической логики.

Невозможно изложить здесь всю теорию с ее долгим и трудным развитием. Но в ходе исследований был выработан ряд новых точек зрения и установлены взаимосвязи, представляющие интерес сами по себе, независимо от всего остального. Я хотел бы рассмотреть здесь одну из таких, как я полагаю, новых точек зрения, которая, помимо всего прочего, тесно связана с самым ядром моей теории доказательств.

Вспомним об аксиоме выбора, которую Цермело впервые ввел для теории множеств, сформулировал и использовал как основу предложенного им гениального доказательства полной упорядоченности континуума [1]. Возражения против этого доказательства и связанного с ним прогресса в теории множеств по существу направлены против принципа выбора; даже сейчас в основном бытует мнение, что допустимость принципа выбора сомнительна, в то время как прочие умозаключения, используемые в теории множеств вообще и в доказательстве Цермело в частности, не вызвали таких возражений. Эту точку зрения я считаю ошибочной; более того, логический анализ, подобный тому, который осуществляется в моей теории доказательств, показывает, что наиболее существенная идея, лежащая в основе принципа выбора, является общим логическим принципом, необходимым и неизбежным для самых первых начал математического вывода. Обеспечив надежность этих первых начал, мы тем самым обретем почву для принципа выбора: и то, и другое реализуется с помощью моей теории доказательств.

Основная идея моей теории доказательств сводится к следующему.

---

*) Die logischen Grundlagen der Mathematik. — Math. Ann., 1923, Bd. 88, S. 151–166. (Доклад на Обществе немецких естествоиспытателей в сентябре 1922 г.) *Перевод Ю. А. Данилова под редакцией З. А. Кузичевой.*

[1]) См. мои доклады в Копенгагене и Гамбурге (Abhandlungen aus dem mathematischen Seminar der Hamburgschen Universität, 1922).

Все, что в прежнем смысле составляет математику, подлежит строгой формализации с тем, чтобы собственно математику, или математику в узком смысле, превратить в набор формул. Последние отличаются от обычных математических формул только тем, что помимо обычных знаков содержат логические знаки, в частности, знаки для «следует» ($\rightarrow$) и «не» ($\bar{}$)[2]. Формулы, служащие кирпичиками, из которых строится формальное здание математики, называются аксиомами. Доказательство есть фигура, которая как таковая должна зримо предстать перед нами; она состоит из умозаключений по схеме вывода

$$\frac{\mathfrak{S} \qquad \mathfrak{S} \rightarrow \mathfrak{T}}{\mathfrak{T}},$$

где всякий раз любая из посылок, т. е. соответствующих формул $\mathfrak{S}$ и $\mathfrak{S} \rightarrow \mathfrak{T}$, есть либо аксиома или получается непосредственно с помощью подстановки из аксиомы, либо совпадает с заключительной формулой $\mathfrak{T}$ вывода, уже встречавшейся ранее в доказательстве или полученной с помощью подстановки из одной из таких заключительных формул. Формула называется доказуемой, если она есть либо аксиома (или получается с помощью подстановки из какой-нибудь аксиомы), либо заключительная формула какого-нибудь доказательства.

Наряду с собственно математикой, формализованной указанным выше образом, возникает в определенной мере новая математика, метаматематика, необходимая для обеспечения надежности собственно математики, в которой (в отличие от чисто формальных выводов собственно математики) используются содержательные выводы, но только для доказательства непротиворечивости аксиом. В этой метаматематике оперируют доказательствами собственно математики, и эти доказательства и составляют предмет содержательного исследования. Таким образом, развитие математической науки в целом происходит в непрекращающемся обмене двоякого рода: получении новых доказуемых формул из аксиом посредством формального вывода — с одной стороны, и добавлении новых аксиом наряду с доказательством непротиворечивости посредством содержательного вывода — с другой.

Аксиомы и доказуемые теоремы, т. е. формулы, возникающие в ходе такой игры в обмен, отражают те идеи, которые лежат в основе обычных методов прежней математики, но сами по себе не являются истинами в абсолютном смысле. В качестве абсолютных истин скорее надлежит рассматривать те представления, которые были выработаны моей теорией доказательств относительно доказуемости и непротиворечивости таких систем формул.

Согласно этой программе выбор аксиом для нашей теории доказательств предопределен. Мы начинаем ряд аксиом следующим образом.

I. АКСИОМЫ СЛЕДОВАНИЯ.

1. $A \rightarrow (B \rightarrow A)$

(Добавление посылки)

---

[2] В цитированной выше работе я еще избегал употреблять эти знаки; оказалось, что в настоящем изложении моей теории, претерпевшем незначительные изменения, употребление знака «не» не таит в себе никакой опасности.

2. $\{A \to (A \to B)\} \to (A \to B)$
(Исключение посылки)

3. $\{A \to (B \to C)\} \to \{B \to (A \to C)\}$
(Перестановка посылок)

4. $(B \to C) \to \{(A \to B) \to (A \to C)\}$
(Исключение высказывания)

II. АКСИОМЫ ОТРИЦАНИЯ.

5. $A \to (\overline{A} \to B)$
(Теорема о противоречии)

6. $(A \to B) \to \{(\overline{A} \to B) \to B\}$
(Принцип исключенного третьего)

III. АКСИОМЫ РАВЕНСТВА.

7. $a = a$

8. $a = b \to (A(a) \to A(b))$

IV. АКСИОМЫ ЧИСЛА.

9. $a + 1 \neq 0$

10. $\delta(a + 1) = a$

По поводу аксиомы 9 следует заметить, что формальное отрицание равенства $a = b$, т. е. $\overline{a = b}$, может быть записано и как $a \neq b$, поэтому $a + 1 \neq 0$ есть формальное отрицание равенства $a + 1 = 0$.

На основе аксиом 1–10 мы легко получаем целые положительные числа и числовые равенства, которым они удовлетворяют. Из тех же начал средствами «финитной» логики с помощью чисто наглядных соображений, к числу которых относится рекурсия и наглядная индукция для рассматриваемых конечных совокупностей, мы получаем элементарную теорию чисел[3)], не прибегая к сомнительным или проблематичным процедурам вывода.

Все доказуемые формулы, полученные в рамках такого подхода, имеют характер финитного, т. е. идеи, отображениями которых они являются, могут быть получены без каких-либо аксиом содержательно и непосредственно из рассмотрения конечных совокупностей [2].

[3)] В окончательном варианте моей теории обоснование элементарной теории чисел производится и с помощью аксиом; здесь же я для краткости буду ссылаться на прямое наглядное обоснование.

В нашей теории доказательств мы хотим между тем выйти за рамки финитной логики и получить такие доказуемые формулы, которые являются образами трансфинитных теорем обычной математики. Если бы нам удалось доказать непротиворечивость теории, получающейся после присоединения нескольких дальнейших трансфинитных аксиом, мы усмотрели бы в этом силу и подтверждение нашей теории доказательств. В каком именно месте впервые происходит выход за рамки конкретно наглядного и финитного? Ясно, что уже при использовании понятий «все» и «существует». С этими понятиями дело обстоит следующим образом. Утверждение о том, что *все* предметы некоторой конечной конкретно заданной обозримой совокупности обладают определенным свойством, логически равнозначно цепочке из высказываний о каждом предмете в отдельности, соединенных связкой «и»; например, утверждение о том, что все скамьи в этой аудитории деревянные, означает то же самое, что и утверждение о том, что эта скамья деревянная и та скамья деревянная, и..., и вон та скамья деревянная. Аналогично, утверждение о том, что в конечной совокупности *существует* предмет с определенным свойством, равнозначно цепочке высказываний относительно отдельных предметов, соединенных связкой «или»; например, утверждение о том, что среди этих кусков мела существует красный мел, означает то же самое, что и утверждение «Этот кусок мела красный, или тот кусок мела красный, или..., или вон тот кусок мела красный».

На основании этого, принцип исключенного третьего для конечных совокупностей мы формулируем следующим образом: либо все предметы обладают определенным свойством, либо существует предмет, который этим свойством не обладает; одновременно при использовании обычных знаков «все» и «существует» ((a) — «для всех a», $\overline{(a)}$ — «не для всех a», $(\mathsf{E}a)$ — «существует a», $\overline{(\mathsf{E}a)}$ — «не существует a») мы достигаем строгого выполнения отношений эквивалентности

$$\overline{(a)}A(a) \quad \text{экв.} \quad (\mathsf{E}a)\overline{A}(a)$$

и

$$\overline{(\mathsf{E}a)}A(a) \quad \text{экв.} \quad (a)\overline{A}(a);$$

где $A(a)$ означает высказывание с переменной a, т. е. предикат.

Обычно в математике предполагается, что эти отношения эквивалентности остаются в силе без каких-либо ограничений и в случае бесконечно многих индивидов; но при этом мы покидаем территорию финитного и вступаем в область трансфинитных выводов. Если бы мы, не задумываясь, всегда применяли к бесконечным совокупностям метод, допустимый в финитной области, то тем самым мы бы дали волю заблуждениям. Источник ошибок был бы тем же самым, который нам хорошо известен из анализа: подобно тому, как в анализе перенос теорем, справедливых для конечных сумм и произведений, на бесконечные суммы и произведения допустим лишь в том случае, если правильность вывода подтверждается специальным исследованием сходимости, с бесконечными логическими суммами и произведениями

$$A_1 \;\&\; A_2 \;\&\; A_3 \;\&\; \ldots,$$
$$A_1 \vee A_2 \vee A_3 \vee \ldots$$

не следует обращаться, как с конечными; такое допустимо только в том случае, если это разрешает уже упоминавшаяся теория доказательств.

Рассмотрим приведенные выше эквивалентности. В случае бесконечно многих предметов отрицание общего суждения $(a)Aa$ поначалу не имеет точного содержания, равно как и отрицание суждения существования $(Ea)Aa$. Правда, иногда этим отрицаниям все же удается придать смысл, а именно: если приводится пример, противоречащий утверждению $(a)Aa$, или если из предположения $(a)Aa$ (соответственно, $(Ea)Aa$) выводится противоречие. Но эти случаи не находятся в контрадикторном противоречии, поскольку если $A(a)$ выполняется не для всех a, то нам не известно, как в действительности обстоит дело с предметом, обладающим свойством не A. Столь же мало мы можем сразу утверждать, что либо $(a)Aa$ (соответственно, $(Ea)Aa$), либо эти утверждения действительно находятся в противоречии. Для конечных совокупностей понятия «существует» и «имеется в наличии» равнозначны; в случае же бесконечных совокупностей значение, не требующее дополнительных оговорок, имеет только последнее понятие.

Итак, мы видим, что для строгого обоснования математики обычные выводы анализа нельзя использовать как логически самоочевидные. Более того, наша задача как раз и состоит в том, чтобы выяснить, почему и в какой мере использование трансфинитных выводов так, как оно происходит в анализе и теории множеств, все же приводит к правильным результатам. Тем самым в области финитного будет достигнуто свободное обращение с трансфинитными понятиями и полное овладение ими! Каким образом возможно решить эту проблему?

Согласно нашему плану, мы добавим к четырем рассмотренным выше группам финитных аксиом такие, которые выражают трансфинитный вывод. Я воспользуюсь идеями, лежащими в основе принципа выбора, и для этого введу логическую функцию

$$\tau(A), \quad \text{или} \quad \tau_a(A(a)),$$

которая каждому предикату $A(a)$, т. е. каждому высказыванию с переменной a, ставит в соответствие определенный предмет $\tau(A)$. Функция $\tau(a)$ должна удовлетворять следующей аксиоме:

V. ТРАНСФИНИТНАЯ АКСИОМА

$$11. \quad A(\tau A) \rightarrow A(a).$$

На обычном языке эта аксиома означает следующее: если предикат A оказывается верным для предмета a, то он оказывается верным для всех предметов a. Функция τ есть определенная индивидуальная функция переменной A, обладающая характером предиката; ее можно назвать *трансфинитной функцией*, а аксиому 11 — *трансфинитной аксиомой*. Чтобы сделать ее содержание более наглядным, предположим, что A — предикат «быть нечестным»; тогда под τA нам следовало бы понимать человека столь неподкупно честного, что если бы он оказался нечист на руку, то всех остальных людей подавно можно было бы считать нечестными.

Трансфинитную аксиому V следует рассматривать как источник всех трансфинитных понятий, принципов и аксиом. Именно, если мы добавим следующие аксиомы:

VI. АКСИОМЫ ОПРЕДЕЛЕНИЯ ЗНАКОВ «ВСЕ» И «СУЩЕСТВУЕТ»

$$A(\tau A) \to (a)A(a),$$
$$(a)A(a) \to A(\tau A),$$
$$A(\tau \overline{A}) \to (\mathsf{E}a)A(a),$$
$$(\mathsf{E}a)A(a) \to A(\tau \overline{A}),$$

то все чисто логические трансфинитные принципы получаются как доказуемые формулы, а именно:

$$(a)A(a) \to Aa$$
(принцип Аристотеля);

$$A(a) \to (\mathsf{E}a)Aa$$
(принцип существования);

$$\overline{(a)}Aa \to (\mathsf{E}a)\overline{A}a,$$
$$(\mathsf{E}a)\overline{A}a \to \overline{(a)}Aa,$$
$$\overline{(\mathsf{E}a)}Aa \to (a)\overline{A}a,$$
$$(a)\overline{A}a \to \overline{(\mathsf{E}a)}Aa.$$

Последние четыре формулы позволяют утверждать, что соотношения эквивалентности, равно как и принцип исключенного третьего, установленные ранее для конечных совокупностей, остаются в силе и для бесконечных совокупностей[4].

Из всего сказанного становится ясно, что все сводится к доказательству непротиворечивости аксиом I–V (1–11).

Общая основная идея относительно того, как надлежит проводить такое доказательство, всегда сводится к следующему. Мы предполагаем, что доказательство существует конкретно — в виде фигуры с заключительной формулой $0 \neq 0$; наличие противоречия в самом деле сводится к этому случаю. Затем с помощью содержательного финитного способа рассуждения мы показываем, что такое доказательство не может удовлетворять нашим требованиям.

Прежде всего необходимо провести доказательство непротиворечивости аксиом I–IV (1–10). Метод состоит в том, что доказательство, которое предполагается существующим, мы подвергаем последовательным трансформациям, придерживаясь следующих взглядов.

1. С помощью повторения и отбрасывания формул доказательство можно превратить в такое, в котором каждая формула имеет своим «адресатом» одну и только одну формулу доказательства, для обоснования которой оно служит. Таким образом, доказательство распадается на нити, исходящие из аксиом и «впадающие» в окончательную формулу [3].

2. Используемые в доказательстве переменные могут быть исключены.

---

[4] Я признателен П. Бернайсу, сообщившему мне, что для выводов всех этих формул достаточно *одной* формулы 11.

3. Можно сделать так, что каждая формула помимо логических знаков будет содержать только числовые знаки

$$0,\ 0+1,\ 0+1+1,\ \ldots,$$

тем самым каждая формула доказательства превратится в «числовую» формулу.

4. Каждая формула приводится к определенной логической «нормальной форме».

По выполнении указанных операций каждая формула доказательства может быть подвергнута в некоторой степени прямой проверке, т. е. может быть установлено, «правильна» она или «неправильна» в определенном строго указанном смысле. Если рассматриваемое доказательство удовлетворяет всем нашим требованиям, то, как нетрудно видеть, каждую формулу по порядку можно подвергнуть такой проверке и поэтому окончательная формула $0 \neq 0$ также должна быть «правильной», что невозможно.

Таким способом можно было бы доказать непротиворечивость групп аксиом I–IV (1–10), хотя точное проведение доказательства, намеченного здесь лишь в общих чертах, потребовало бы гораздо больше времени, чем отведено на мой доклад.

Но сейчас для нас особый интерес представляет именно непротиворечивость аксиомы V (11), поскольку именно через эту аксиому трансфинитные выводы обрели бы в математике свое обоснование.

Самую суть доказательства непротиворечивости аксиомы 11 я хотел бы изложить несколько более подробно для первого и простейшего случая. Этот первый случай предоставляется нам, как только мы расширим теорию чисел, остававшуюся до сих пор строго финитной. Расширение происходит, если мы в аксиоме V (11) возьмем в качестве предметов знаки чисел, т. е. целые положительные числа, включая 0, а в качестве предикатов $A(a)$ — уравнения $f(a) = 0$, где f — обычная целочисленная функция. Логическая функция τ ставит в соответствие каждому предикату некоторый предмет, т. е. сопоставляет каждой математической функции f — некоторое число. Следовательно, из τ мы получаем некоторую обычную целочисленную функцию от функций, так, что если f — некоторая определенная функция, то τ — некоторое определенное число; мы обозначим его $\tau(f)$; таким образом,

$$\tau(f) = \tau_a(f(a) = 0);$$

аксиома V (11) превращается в аксиому

$$12.\quad f(\tau(f)) = 0 \rightarrow f(a) = 0.$$

Свойство функции функций $\tau(f)$, запечатленное в этой формуле, мы реализуем проще всего, если условимся понимать под $\tau(f)$ число 0, если для каждого a выполняется уравнение $f(a) = 0$, а в противном случае полагать $\tau(f)$ равной первому числу a, для которого $f(a) \neq 0$[5] [4]. Функция $\tau(f)$ — трансфинитная и относится к числу тех функций, которые запрещены Брауэром и Вейлем [5]. Все сводится теперь к тому, чтобы доказать, что аксиома 12, добавленная к аксиомам 1–10, не приводит к противоречию.

---

[5] В дальнейшем при введении в формализм этой специализации (с. 427) вместо символа $\tau(f)$ используется символ $\mu(f)$.

Для этого мы обратимся к доказательству непротиворечивости аксиом 1–10 и попытаемся перенести его на интересующий нас сейчас случай. Теперь нам предстоит преодолеть новую трудность, которая заключается в том, что в имеющемся доказательстве встречается знак $\tau(f)$, в котором вместо переменной функции f можно подставлять произвольные конкретные функции $\varphi, \varphi', \ldots$ Но временно мы примем поясняющее суть дела и упрощающее предположение, согласно которому подставлять вместо f можно только такую конкретную функцию φ, что имеющееся доказательство в конце концов можно превратить в доказательство, которое помимо логических и числовых знаков содержит только $\tau(\varphi)$, где φ — конкретная функция, в определении которой не используется τ.

При доказательстве мы используем по порядку следующие операции.

1. Вместо $\tau(\varphi)$ мы всюду подставляем, разумеется, временно и в качестве пробы, числовой символ 0. Наше доказательство при этом переходит в последовательность «числовых» формул; все эти формулы «правильны» в указанном ранее смысле, за исключением, возможно, тех, которые вытекают из аксиомы 12. Но если вместо f мы подставим φ, произведем соответствующую подстановку вместо a и затем заменим $\tau(\varphi)$ числовым символом 0, из аксиомы 12 следуют только формулы вида

$$\varphi(0) = 0 \rightarrow \varphi(\zeta) = 0.$$

Так как ζ здесь означает какой-то числовой символ, а φ — функция, определяемая рекурсией (определение посредством рекурсии легко воспроизводится в нашем формализме), $\varphi(\zeta)$ также сводится к какому-то числовому символу. По существу речь будет идти: всюду ли в этих формулах из $\varphi(\zeta)$ после указанной редукции к числовым символам возникает числовой символ 0, или однажды появляется некоторый отличный от 0 числовой символ. В первом случае, если речь идет о доказательстве непротиворечивости, то мы уже достигли цели, так как все формулы, вытекающие из аксиомы 12, правильны сами по себе. Последовательность формул, получаемых из доказательства, снова подлежит доказательству, в ходе которого проверка шаг за шагом устанавливает правильность всех формул, в результате чего ложная формула $0 \neq 0$ не может возникнуть как заключительная формула.

2. Если имеет место вторая альтернатива, то мы получаем такое ζ, что

$$\varphi(\zeta) = 0$$

— ложная формула. В этом случае мы проделываем над рассматриваемым доказательством другую операцию: подставляем вместо $\tau(\varphi)$ во всем доказательстве не 0, а числовой символ ζ. Все формулы, вытекающие из аксиомы 12, приобретают при этом вид

$$\varphi(\zeta) = 0 \rightarrow \varphi(s) = 0,$$

и эти формулы сами по себе уже непременно являются истинными, так как стоящая перед знаком следования ($\rightarrow$) формула ложна. Доказательство снова становится доказательством с чисто числовыми формулами, которые истинны, поэтому заключительная формула, также истинная, не может заканчиваться формулой $0 \neq 0$.

Этим доказательство непротиворечивости трансфинитной функции $\tau(f)$ проведено полностью; тем самым доказан также и принцип исключенного третьего для понятия бесконечной числовой последовательности, так как

она представляет целочисленную переменную в f, а именно: из аксиом отрицания II (5–6) следует, что формальное отрицание равносильно контрадикторной противоположности; но $f\tau(f) \neq 0$ — формальное отрицание соотношения $f\tau(f) = 0$; с другой стороны, из аксиом VI, $f\tau(f) \neq 0$ эквивалентно $(\mathsf{E}a)(f(a) \neq 0)$, а $f\tau(f) = 0$ эквивалентно $(a)(f(a) = 0)$.

Решение отмеченной трудности, каким его дает моя теория доказательств, можно понять следующим образом. Наше мышление финитно; когда мы мыслим, происходит финитный процесс. Эта самодействующая истина в определенной мере используется в моей теории доказательств таким образом, что если бы где-то было обнаружено противоречие, то, располагая знанием этого противоречия, необходимо было бы произвести соответствующий выбор из бесконечно многих вещей. В моей теории доказательств поэтому не утверждается, что среди бесконечно многих предметов всегда можно найти предмет, хотя без риска можно всегда действовать так, как если бы такой выбор был возможен. Мы могли бы согласиться с Вейлем относительно существования круга, но этот круг отнюдь не является порочным. Более того, ничто не угрожает принципу исключенного третьего [6].

В моей теории доказательств к финитным аксиомам добавлены трансфинитные аксиомы и формулы, подобно тому, как в теории комплексных чисел к действительным элементам присоединены мнимые, а в геометрии к действительным образам добавлены идеальные. Побудительные мотивы для этого и успех метода в моей теории доказательств такие же, как там, а именно: дополнительное включение трансфинитных аксиом происходит во имя упрощения и законченности теории.

Из сказанного выше можно понять, что трансфинитная функция $\tau(f)$ применима во всей математике, идет ли речь об определении функций и образовании новых понятий или о проведении математических доказательств.

В качестве примера определения функции может служить функция [7]

$$\varphi(a) = [a^{\sqrt{a}}],$$

где скобки в правой части означают 0 или 1 в зависимости от того, рационально или иррационально число $a^{\sqrt{a}}$.

Что же касается применения в доказательстве, то в большинстве имеющихся в литературе доказательств нетрудно распознать, существенным образом или нет в них используется трансфинитная функция. Подходящими примерами могут служить оба приведенных мной совершенно отличных друг от друга доказательства конечности полной системы инвариантов. В первом находит применение трансфинитный вывод, во втором он не используется. Мое первое доказательство полной системы инвариантов носит такой характер, что трансфинитный вывод используется в нем существенным образом и обойтись без него невозможно. Правда, высказывается предположение, что конечную теорему всегда можно доказать, и не используя трансфинитный вывод (как это было продемонстрировано моим вторым доказательством конечности полной системы инвариантов), но это утверждение относится к числу утверждений того же рода, что и утверждение о том, что любая математическая теорема вообще либо доказуема как истинная, либо должна быть отвергнута. У П. Гордана было смутное ощущение, что в моем первом доказательстве конечности полной системы инвариантов используется трансфинитный вывод: свое впечатление он выразил, назвав

мое доказательство «теологическим». Затем он модифицировал мое доказательство, использовав свою символику, и полагал, что тем самым лишил доказательство «теологического» характера. В действительности же трансфинитность вывода лишь скрылась за формализмом символики [8].

Тем же методом, каким выше нами была доказана непротиворечивость трансфинитной функции функций $\tau(f)$, мы можем доказать и непротиворечивость функции функций $\mu(f)$, обладающей (как и $\tau(f)$) свойством быть равной 0, если $f(a)$ при всех значениях переменной a обращается в нуль, а в противоположном случае принимающей наименьшее значение, при котором $f(a)$ отлична от 0[6]. С помощью этой функции $\mu(f)$ мы получаем[7] принцип полной индукции

$$A(0) \to (a)(A(a) \to A(a+1)) \to A(a)$$

как доказуемую формулу.

Для обоснования анализа определим действительное число z, заключенное между 0 и 1, с помощью двоичной дроби, а двоичную дробь — с помощью функции $\varphi(n)$ (значения n-го знака), принимающей значения 0 или 1:

$$z = 0, a_1 a_2 a_3 \ldots \qquad (a_n = \varphi(n)).$$

Примером трансфинитно определяемой двоичной дроби может служить дробь

$$0, [2^{\sqrt{2}}][3^{\sqrt{3}}][4^{\sqrt{4}}]\ldots;$$

она представляет вполне определенное число, хотя при современном состоянии науки мы не можем вычислить даже первый двоичный знак после запятой.

Основой анализа служит теорема о верхней границе. Действительно, трансфинитная функция τ позволяет доказать теорему о том, что верхняя граница последовательности действительных чисел всегда существует.

Чтобы установить это, прежде всего целесообразно ввести логические знаки $\&$ для «и» и $\vee$ для «или». Мы делаем это, сводя их к логическим знакам $\to$ и $\bar{\ }$, которыми пользовались ранее, следующим образом:

$$\mathfrak{A} \ \& \ \mathfrak{B} \quad \text{и, соответственно,} \quad \mathfrak{A} \vee \mathfrak{B}$$

означает то же самое, что

$$\overline{\mathfrak{A} \to \overline{\mathfrak{B}}} \quad \text{и, соответственно,} \quad \overline{\mathfrak{A}} \to \mathfrak{B}.$$

Формулу

$$(a)(fa = 0 \vee fa = 1) \ \& \ (a)(\mathsf{E}b)(f(a+b) = 1)$$

для краткости запишем в виде $\mathfrak{R}f$, т. е. $\mathfrak{R}f$ означает, что функция fa посредством бесконечной двоичной дроби

$$0, f(1)f(2)f(3)\ldots$$

---

[6] Функция $\mu(f)$ удовлетворяет следующим аксиомам:

$$f(\mu(f)) = 0 \to f(a) = 0, \quad (a)(f(a) = 0) \to \mu(f) = 0, \quad f(a) \neq 0 \to \mu(f) \leqslant a.$$

[7] Если присоединим к аксиомам IV аксиому

$$a \neq 0 \to a = \delta(a) + 1.$$

задает некоторое действительное число, заключенное в интервале от 0 до 1, исключая 0 и включая 1. Тогда последовательность $\zeta_1, \zeta_2, \zeta_3, \ldots$, действительных чисел представима функцией $\varphi(a, n)$, для которой формула $R\varphi(a, n)$ доказуема при произвольном целочисленном n. Дальнейший ход доказательства основан на использовании следующих идей. Рассмотрим в схеме

$$\zeta_1 = 0, \varphi(1,1)\varphi(2,1)\varphi(3,1)\ldots$$
$$\zeta_2 = 0, \varphi(1,2)\varphi(2,2)\varphi(3,2)\ldots$$
$$\zeta_3 = 0, \varphi(1,3)\varphi(2,3)\varphi(3,3)\ldots$$

сначала цифры в первом столбце после запятой. Если все эти цифры 0, т. е. если $\varphi(1, n) = 0$ при всех n, то мы полагаем $\psi(1) = 0$, в противном случае $\psi(1) = 1$. Если во втором столбце равны 0 все цифры, у которых в той же строке в первом столбце стоит $\psi(1)$, то мы полагаем $\psi(2) = 0$, в противном случае $\psi(2) = 1$. Если в третьем столбце равны 0 все цифры, у которых в той же строке в первом и во втором столбцах стоят, соответственно, $\psi(1)$ и $\psi(2)$, то мы полагаем $\psi(3) = 0$, в противном случае $\psi(3) = 1$, и т. д. В результате этой процедуры мы приходим к заключению, что верхняя граница $\psi(a)$ последовательности $\varphi(a, n)$ действительных чисел определяется следующей системой рекурсивных соотношений:

$$\chi(0, n) = 0,$$
$$\psi(a+1) = \pi_n\{\chi(a, n) = 0 \to \varphi(a+1, n) = 0\},$$
$$\chi(a+1, n) = \chi(a, n) + \iota\{\psi(a+1), \varphi(a+1, n)\};$$

где $\iota(a, b)$ — функция от a, b, принимающая значения 0 или 1 в зависимости от того, какое из соотношений $a = b$ или $a \neq b$ выполняется, а π_n — трансфинитная функция, определяемая аксиомой

$$(n)\mathfrak{A}(n) \to \pi_n(\mathfrak{A}n) = 0,$$
$$\overline{(n)}\mathfrak{A}(n) \to \pi_n(\mathfrak{A}n) = 1,$$

или словами: $\pi(\mathfrak{A}n)$ равна 0 или 1 в зависимости от того, истинно или ложно высказывание $\mathfrak{A}$ для всех n.

В смысле моей теории доказательств можно строго доказать, что $\mathfrak{R}\psi$ выполняется и что, кроме того, действительное число $\psi(n)$ обладает свойством верхней границы, причем понятие «меньше» для двух действительных чисел f, g определяется формулой

$$(\mathsf{E}a)\{(b)(b < a \to fb = gb) \ \ \& \ \ fa = 0 \ \ \& \ \ ga = 1\}.$$

Пусть теперь вместо последовательности действительных чисел мы имеем произвольное множество действительных чисел, например, пусть для функциональной переменной f задано некоторое высказывание $\mathfrak{R}(f)$, которое, с одной стороны, характеризует f как функцию, представляющую некоторое действительное число, а кроме того указывает отличительные особенности действительных чисел этого множества. Верхняя граница $\psi(a)$ этого множества $\mathfrak{R}(f)$ действительных чисел определяется в данном случае

следующей общей рекурсией:

$$\chi(0,f)=0,$$
$$\psi(a+1)=\pi_f\{\mathfrak{R}(f)\to(\chi(a,f)=0\to f(a+1)=0)\},$$
$$\chi(a+1,f)=\xi(a,f)+\iota\{\psi(a+1),f(a+1)\},$$

где π_f — трансфинитная функция, определяемая аксиомами

$$(f)\mathfrak{A}(f)\to\pi_f(\mathfrak{A}f)=0,$$
$$\overline{(f)}\mathfrak{A}(f)\to\pi_f(\mathfrak{A}f)=1.$$

В заключение я хотел бы продемонстрировать применение принципа выбора Цермело к множеству множеств действительных чисел. Выше множество действительных чисел было задано определенным высказыванием $\mathfrak{R}(f)$ с f в качестве функциональной переменной; теперь мы дополнительно вводим аксиомы

$$\mathfrak{R}(f)\to\nu(f)=1,$$
$$\overline{\mathfrak{R}(f)}\to\nu(f)=0,$$

непротиворечивость которых легко устанавливается. Тем самым наше множество определено функцией $\nu(f)$, принимающей при действительных числах f из нашего множества значение 1, а при всех других действительных числах f значение 0 [9]. Из выполняющейся для $\mathfrak{R}$ формулы

$$\mathfrak{R}(f)\to\mathfrak{R}(f)$$

получаем:

$$\nu(f)=1\to\mathfrak{R}(f),$$

где ν — конкретная функция функций, пусть r — соответствующая переменная, т. е. переменная для функции функций, аргументом которой служит обыкновенная функция одного аргумента.

Конкретное множество множеств действительных чисел задается тогда конкретным содержащим r высказыванием $\mathfrak{M}(r)$, для которого имеет место формула

$$\mathfrak{M}(r)\ \&\ (rf=1)\to\mathfrak{R}(f).$$

Мы предполагаем, что это множество множеств обладает тем свойством, что любое множество действительных чисел, которое является его элементом, содержит по крайней мере одно действительное число, или — на языке формул:

$$\mathfrak{M}(r)\to(\mathsf{E}f)(r(f)=1).$$

Далее мы определяем трансфинитную функцию τ_f так же, как ранее τ_a, с тем лишь различием, что вместо числовой переменной a мы с самого начала используем функциональную переменную f, т. е. τ_f определяется аксиомой

$$12^*.\quad r(\tau_f(r))=0\to r(f)=0,$$

соответствующей нашей аксиоме 12 для τ_a и также получаемой из логической аксиомы V (11), если в последней в качестве предметов выбрать

функции f, а в качестве предикатов — уравнения $r(f) = 0$; при этом сама τ_f всегда представляет некоторую функцию, в то время как аргумент есть некоторая функция функций r.

Теперь мы располагаем следующими доказуемыми формулами:

$$(\mathsf{E}f)(r(f) = 1) \to \overline{(f)}(rf = 0),$$

$$\overline{(f)}(rf = 0) \to r(\tau_f(r)) \neq 0,$$

$$r(\tau_f(r)) \neq 0 \to r(\tau_f(r)) = 1,$$

а отсюда следует, что

$$\mathfrak{M}(r) \to r(\tau_f(r)) = 1;$$

т. е. каждому элементу r множества $\mathfrak{M}(r)$ ставится в соответствие некоторая целочисленная функция $\tau_f(r)$. Она представляет действительное число, так как из приведенной ранее формулы тотчас же следует $\mathfrak{R}(\tau_f(r))$. Функции $\tau_f(r)$ образуют некоторое множество, ибо, чтобы получить для этих функций (обозначим их $g(a)$) высказывание, определяющее их совокупность, нам необходимо лишь сформулировать, что каждая из функций совпадает с представителем $\tau_f r$ некоторого множества r, принадлежащего $\mathfrak{M}$, как это происходит по формуле

$$(\mathsf{E}r)\{\mathfrak{M}(r) \ \& \ (a)(g(a) = \tau_f r(a))\},$$

так что, в соответствии с обычным методом, множество действительно существует.

Тем самым приведено доказательство предложенного Цермело принципа выбора для множества множеств действительных чисел.

Поскольку мы использовали знак «существует» $(\mathsf{E}r)$, необходимо еще доказать непротиворечивость трансфинитной функции $\tau_f(r)$ с переменной r, принадлежащей новому сорту. Это доказательство, как и аналогичные доказательства для π_n и π_f, проводится по образцу доказательства для трансфинитной функции τ_a.

Остается еще задача — более точная реализация идей, намеченных выше лишь в общих чертах; с ее решением будет завершено обоснование анализа и положено начало основания теории множеств.

О БЕСКОНЕЧНОМ*)[1)]

Своею критикой, проведенной им с мастерской остротой, Вейерштрасс заложил прочные основы математического анализа. Внеся, в частности, ясность в понятия минимума, функции и частного дифференциалов, он устранил недочеты, еще имевшиеся в исчислении бесконечно малых, очистил это исчисление от всех туманных представлений о бесконечно малом и окончательно преодолел вытекающие из этого понятия трудности. И если теперь в умозаключениях, основанных на понятии иррационального числа, и вообще на понятии предела, в анализе, — даже в самых его запутанных вопросах, касающихся теории дифференциальных и интегральных уравнений, — царит полное единодушие и уверенность, если, несмотря на самые смелые и многообразные по своему характеру нагромождения и перекрещивания пределов, здесь все-таки наблюдается полная согласованность результатов, то в основном это — заслуга научной деятельности Вейерштрасса.

И все же в обосновании, данном Вейерштрассом анализу бесконечно малых, дискуссия об основаниях анализа еще не нашла своего окончательного завершения.

Причина этого кроется в том, что значение *бесконечного* для математики еще не стало бесповоротно ясным. Правда, *бесконечно малое* и *бесконечно большое* были из вейерштрассова анализа исключены таким образом, что относящиеся к ним высказывания были сведены к отношениям между конечными величинами, но бесконечное здесь все еще фигурирует в виде бесконечных числовых последовательностей, определяющих действительные числа, а затем и в понятии системы действительных чисел, которая рассматривается на равных правах с любой готовой и законченной совокупностью.

Схемы логической дедукции, в которых это воззрение находит свое выражение, — в частности те из них, которые трактуют о *всех* действительных числах, обладающих тем или иным конкретным свойством, или о *суще-*

---

*) Über das Unendlichte. — In: *D. Hilbert.* «Grundlagen der Geometrie», 7. Aufl., 1930, Leipzig–Berlin, B. G. Teubner. См. также Math. Ann., 1926, Bd. 95, S. 161–190. [1] *Перевод Н. М. Нагорного.*

1) Доклад, прочитанный 4-го июня 1925 г. на съезде математиков, организованном вестфальским математическим обществом в Мюнстере в память Вейерштрасса; ср. другие мои сообщения на эту же тему: Neubegründung der Mathematik. — Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität, 1922, Bd. I, S. 57; Die logischen Grundlagen der Mathematik. — Math. Ann., 1923, Bd. 88, S. 151–166 [имеется перевод на с. 418–430 наст. издания. — *Ред.*]; Die Grundlagen der Mathematik. — Abhandlungen aus dem mathematischen Seminar der Hamburgischen Universität, 1928, Bd. 65 (имеется перевод в кн.: *Д. Гильберт.* «Основания геометрии». — М.–Л., ГИТТЛ, 1948 (добавление IX) — *Ред.*); Probleme der Grundlegung der Mathematik. — Abhandlungen des Internationalen Mathematischen Kongresses zu Bologna, 1928, см. также Math. Ann., 1930, Bd. 102, S. 1–9 [имеется перевод на с. 449–456 наст. издания. — *Ред.*.]

ствовании таких чисел, — применяются в вейерштрассовом обосновании без каких-либо ограничений и в итерированном виде.

Тем самым бесконечное все-таки снова смогло, — в замаскированном виде, — продолжить свою игру в вейерштрассовой теории, не будучи задето острием вейерштрассовой критики, а отсюда следует, что *проблема бесконечного* как раз и есть то, что в смысле, на который мы выше намекнули, нам еще требуется прояснить до конца. И подобно тому, как в процессах предельного перехода исчисления бесконечно малых удалось обнаружить, что бесконечное в смысле бесконечно малого и бесконечно большого есть всего лишь способ выражаться, бесконечное в смысле бесконечной совокупности там, где оно еще и ныне встречается в рассуждениях, мы должны трактовать лишь как нечто кажущееся. И аналогично тому, как оперирование с бесконечно малыми было заменено операциями с конечным, дающими в точности те же самые результаты и приводящими к абсолютно тем же самым элегантным формальным соотношениям, рассуждения с использованием бесконечного должны быть вообще заменены оперированием конечными операциями, в итоге дающими то же самое, иначе говоря, позволяющими проводить те же самые доказательства и развивать те же самые методы получения формул и теорем.

В этом и заключается замысел моей теории. Она ставит своей целью сделать математические методы окончательно надежными, что еще не было достигнуто в критический период исчисления бесконечно малых. Она должна, таким образом, завершить то, к чему стремился в своем обосновании анализа Вейерштрасс и к достижению чего им был сделан необходимый и существенный шаг.

Однако, что касается вопроса о прояснении понятия бесконечности, то здесь следует принимать во внимание и другие, более общие точки зрения. Математическая литература, если повнимательней присмотреться к ней, изобилует бессмыслицами и нелепостями, в которых в большинстве случаев повинна бесконечность. Так, например, иногда в качестве ограничительного условия подчеркивается требование, чтобы в математике, если она хочет быть строгой, в доказательстве допускалось лишь *конечное* число умозаключений — как будто кому-то в один прекрасный день уже удалось сделать бесконечное число умозаключений.

Да и старые возражения, казалось, давно похороненные, тоже порой выступают в новом обличье. Так, недавно высказывалось мнение вроде того, что если даже какое-либо понятие может быть введено с соблюдением правил безопасности, то есть без риска получить противоречие, и если это даже может быть доказано, то и тогда оно еще не может считаться достаточно оправданным. Но не это ли в точности возражение в свое время выдвигалось и против комплексных (мнимых) чисел? В самом деле, говорили нам, пусть из-за них не возникает никаких противоречий, но ведь введение их все равно является незаконным, ибо мнимых величин все-таки не существует. Нет, если сверх доказательства непротиворечивости может возникнуть и еще какой-то другой вопрос о законности проводимого мероприятия, то таким вопросом может быть лишь вопрос о том, сопровождается ли это мероприятие соответствующим успехом. Действительно, успех здесь необходим; он и здесь является высшей инстанцией, перед которой преклоняется каждый.

Другой автор усматривает противоречия, — подобно привидениям, — по-видимому даже там, где никто вообще ничего не утверждал; а именно — в самом конкретном, чувственном мире, „непротиворечивое функционирование“ которого рассматривается как особая гипотеза. Я, конечно, всегда полагал, что противоречить друг другу могут только высказывания и допущения, поскольку эти последние через умозаключения снова ведут к высказываниям, и мне кажется, что мнение, будто факты и события сами могут впадать в противоречие друг с другом, является классическим примером бессмыслицы.

Этими замечаниями я хочу лишь показать, что окончательное раскрытие *сущности бесконечного* далеко выходит за пределы узких интересов специальных наук и что, более того, оно стало необходимым для *чести самого человеческого разума.*

С давних пор никакой другой вопрос не волновал человеческую *душу* так глубоко, как вопрос о бесконечном; бесконечное, как едва ли какая-либо другая *идея*, побуждающе и плодотворно действовало на наш разум; и однако ни одно другое *понятие* так сильно не нуждается в *разъяснении*, как нуждается в нем бесконечное.

Обращаясь теперь к этой задаче разъяснения сущности бесконечного, мы должны вкратце представить себе, какое содержательное значение соответствует бесконечному в действительности; мы сначала посмотрим, что́ дает нам в этом отношении физика.

Первым наивным впечатлением, производимым явлениями природы и материей, является впечатление чего-то непрерывного, континуального. Если мы имеем перед собою кусок металла или какой-то объем жидкости, то само собой напрашивается представление о том, что они неограниченно делимы, что сколь угодно малая часть этого куска или объема снова обладает тем же самым свойством. Но повсюду, где методы исследования по физике материи достаточно усовершенствованы, мы наталкиваемся на границы этой делимости, кроющиеся не в недостаточности наших попыток, а в природе самой вещи, так что тенденцию современной науки мы могли бы решительно воспринимать как освобождение от бесконечно малого, и вместо старого тезиса «natura non facit saltus»*) мы теперь могли бы утверждать его антитезу: «природа делает скачки».

Как мы знаем, вся материя составлена из маленьких кирпичиков, — из *атомов*, — и их комбинации и соединения образуют все многообразие макроскопических веществ.

Однако физика не остановилась на учении об атомном строении материи. Рядом с ним в конце прошлого столетия встало поначалу производящее гораздо более странное впечатление учение об атомном строении электричества. В то время как до тех пор электричество считалось жидкостью и было примером непрерывно действующего агента, теперь оказалось, что и оно построено из положительных и отрицательных *электронов*.

Помимо материи и электричества, в физике имеется и другая реальность, для которой тоже имеет место закон сохранения, а именно — энергия. Но, как установлено теперь, и энергия не допускает простого и неограниченного деления на части; Планк открыл *кванты энергии.*

---

*) Природа не делает скачков (*лат.*). — *Ред.*

И каждый раз мы в итоге получаем, что однородный континуум, который должен был бы неограниченно делиться и тем самым реализовать бесконечное в малом, в действительности нигде не встречается. Бесконечная делимость континуума — это только существующая в человеческом представлении операция, только идея, которая опровергается нашими наблюдениями над природой и опытом физики и химии.

Второй повод столкнуться в природе с вопросом о бесконечности дает нам рассмотрение Вселенной как целого. Здесь мы должны исследовать протяженность Вселенной, чтобы узнать, нет ли в ней чего-то бесконечно большого.

Мнение, что Вселенная бесконечна, долгое время господствовало; вплоть до Канта, и даже после него вопрос о бесконечности пространства не вызывал никаких сомнений.

Но опять-таки современная наука, и в частности астрономия, подняла этот вопрос еще раз и пытается решить его не с помощью недостаточных по своей силе средств метафизического умозрения, а опираясь на основы, покоящиеся на опыте и на применении законов природы. И при этом выявились веские возражения против бесконечности. К принятию бесконечности нас с необходимостью подводит *евклидова* геометрия. И хотя евклидова геометрия является непротиворечивой в самой себе системой понятий, отсюда еще не следует, что она имеет законную силу в действительности. Так это или не так — может решить лишь наблюдение и опыт. Попытки доказать бесконечность пространства умозрительно содержали порой просто очевидные ошибки. Из того, что вне любой части пространства всякий раз налицо снова оказывается пространство, следует только неограниченность пространства, а отнюдь не его бесконечность. Но неограниченность и конечность не исключают друг друга. Математические изыскания дают нам естественную модель конечной Вселенной в виде так называемой *эллиптической* геометрии. Вопрос об отказе от евклидовой геометрии сейчас уже не является предметом чисто математического или философского умозрения. Напротив, мы приходим к нему с другой стороны, первоначально не имевшей ничего общего с вопросом о конечности Вселенной. Эйнштейн показал необходимость отойти от геометрии Евклида. Опираясь на созданную им теорию гравитации, он принялся и за космологические проблемы и показал возможность конечности Вселенной. При этом все полученные астрономами результаты вполне согласуются с предположением об эллиптичности Вселенной.

Итак, конечность действительного мы установили в двух направлениях: в части бесконечно малого и в части бесконечно большого. И все же вполне могло бы случиться так, что бесконечное займет полноправное место *в нашем мышлении* и окажется в нем необходимым понятием. Давайте посмотрим, как обстоит с этим дело в математической науке, и первым долгом опросим арифметику — это чистейшее и наивнейшее дитя человеческого духа. Из великого множества имеющихся здесь элементарных формул мы выберем какую-нибудь одну, например,

$$1^1 + 2^2 + 3^2 + \ldots + n^2 = \frac{1}{6}n(n+1)(2n+1).$$

Так как в нее вместо n мы можем подставить любое целое число, например, 2 или 5, то в этой формуле на самом деле содержится *бесконечно много*

высказываний, и в этом, очевидным образом, и заключается ее суть. Благодаря этому она и представляет собой решение некоторой арифметической проблемы и требует доказательства по существу, в то время как частные числовые равенства

$$1^2 + 2^2 = \frac{1}{6} \cdot 2 \cdot 3 \cdot 5,$$

$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 = \frac{1}{6} \cdot 5 \cdot 6 \cdot 11$$

могут быть проверены путем вычисления, и потому в отдельности не представляют сколько-нибудь существенного интереса.

С абсолютно другим, совершенно своеобразным толкованием и принципиальным по своему характеру подходом к понятию бесконечного мы знакомимся на примере в высшей степени важного и плодотворного метода *идеальных элементов*. Этот метод находит себе применение уже в элементарной геометрии плоскости. Здесь реальными, действительно существующими предметами изначально являются лишь точки и прямые плоскости. Для них, в частности, выполняется аксиома соединения, гласящая, что через всякие две точки проходит одна и только одна прямая. Отсюда как следствие получается, что любые две прямые пересекаются не более чем в одной точке. Но теорема о том, что две прямые всегда пересекаются в одной точке, места не имеет: ведь взятые прямые могут быть и параллельны друг другу. Известно, однако, что введением идеальных элементов, а именно — бесконечно удаленных точек и одной бесконечно удаленной прямой можно добиться, чтобы теорема о том, что две прямые всегда пересекаются в одной и только одной точке, была справедлива во всех случаях.

Идеальные „бесконечно удаленные“ элементы выгодны тем, что они делают систему законов соединения максимально простой и обозримой. Отсюда, как известно, вследствие симметрии, имеющейся между точками и прямыми, получается оказавшийся столь плодотворным геометрический принцип двойственности.

Обычные *комплексно-мнимые* величины алгебры тоже служат примером идеальных элементов; они используются для придания простого вида теоремам о существовании и о числе корней уравнения.

Подобно тому как в геометрии бесконечно многие прямые, а именно, прямые, параллельные друг другу, используются для определения идеальной точки, в высшей арифметике определенные бесконечные системы чисел объединяются в единый *числовой идеал*, и именно в этом, пожалуй, и состоит самое гениальное применение принципа идеальных элементов. И если все это происходит внутри некоторого алгебраического числового поля, то мы снова обнаружим в нем простые и хорошо известные законы делимости, аналогичные тем, которые имеют место в случае обыкновенных целых чисел $1, 2, 3, \ldots$ Так мы оказываемся уже в области высшей арифметики.

Теперь мы подходим к анализу, этому искуснейшему творению математической науки с его тончайшим образом разветвленной структурой. Вы сами знаете, какую ведущую роль играет там бесконечное, поскольку математический анализ в известной мере представляет собой единую симфонию бесконечного.

Громадные успехи, достигнутые в исчислении бесконечно малых, большей частью основываются на действиях с математическими системами, состоящими из бесконечного числа элементов. Так как очень легко напрашивалось отождествление бесконечного с „очень большим", то вскоре возникли несогласованности — так называемые парадоксы исчисления бесконечно малых, которые отчасти были известны софистам уже в древности. Основополагающим открытием было обнаружение того факта, что многие утверждения, справедливые для конечного, — например, что часть меньше целого, существование минимума и максимума, перестановочность сложения и умножения, — не могут быть непосредственно перенесены на бесконечное. В начале своего доклада я уже упоминал, что именно благодаря проницательности Вейерштрасса вопросы эти были полностью прояснены, и теперь анализ стал в своей области непогрешимым руководством и практическим инструментом для использования бесконечного.

Однако один лишь анализ еще не ведет нас к глубочайшему постижению сущности бесконечного. Этой цели скорее может способствовать научная дисциплина, стоящая ближе к общефилософскому подходу и призванная представить в новом свете весь комплекс вопросов, касающихся бесконечного. Этой дисциплиной является учение о множествах, создателем которого был Георг Кантор, и здесь мы рассмотрим только то действительно единственное в своем роде и оригинальное, что составляет истинное ядро канторовского учения, — его *теорию трансфинитных чисел*. Она представляется мне достойным наибольшего удивления цветком математического духа и вообще одним из высших достижений трезвого человеческого разума. Что же это такое?

Если мы захотим кратко охарактеризовать то новое понимание бесконечного, начало которому положил Кантор, то, пожалуй, можно будет сказать, что в анализе нам приходится иметь дело с бесконечно малым и бесконечно большим только как с предельным понятием, как с чем-то становящимся, возникающим, порожденным, т. е., как говорится, с *потенциально бесконечным*. Но это еще не само настоящее бесконечное. С ним, например, мы имеем дело, когда рассматриваем самоё совокупность чисел $1, 2, 3, \ldots$ как некое завершенное, готовое целое или же точки какого-нибудь отрезка как совокупность вещей, лежащую перед нами в завершенном, готовом виде. Такого рода бесконечность мы будем называть *актуальной бесконечностью*.

Уже оба, и Фреге и Дедекинд, — математики, имеющие большие заслуги перед обоснованиями математики, — независимо друг от друга пользовались актуально бесконечным для обоснования арифметики. Они делали это независимым ни от каких наглядных представлений и опыта образом, на базе чистой логики чисто дедуктивным путем. Дедекинд стремился даже к тому, чтобы и конечное количество брать не из наглядных представлений, а выводить его чисто логически, существенно используя при этом понятие бесконечного множества. Но систематическую форму понятию бесконечного придал Кантор. Давайте пристально вглядимся в оба упомянутых выше примера бесконечного:

1) числа $1, 2, 3, \ldots$;

2) точки отрезка от 0 до 1, или, что то же самое, совокупность действительных чисел, заключенных между 0 и 1.

Прежде всего сама собой напрашивается мысль рассмотреть их чисто с точки зрения количества входящих в них чисел. При этом обнаруживаются поразительные факты, хорошо теперь известные каждому математику. А именно, если рассмотреть множество всех рациональных чисел, т. е. всех дробей $\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \ldots, \frac{3}{7}, \ldots$, то окажется, что с указанной точки зрения оно не больше множества всех целых чисел: мы говорим, что рациональные числа могут быть самым обычным способом пересчитаны, или что множество их счетно.

То же самое справедливо и в отношении множества всех чисел, получающихся с помощью радикалов, и даже для множества всех алгебраических чисел. Аналогично обстоит дело и с нашим вторым примером: неожиданным образом оказывается, что множество всех точек квадрата или куба, взятое только с точки зрения количества его элементов, не больше множества точек отрезка от 0 до 1; да и для множества всех непрерывных функций такое утверждение тоже еще справедливо. Тот, кто знакомится с этим впервые, может подумать, что с точки зрения количества элементов вообще существует только одна бесконечность. Но нет: множества в двух наших примерах — в первом и во втором, — как говорится, не «равномощны»; наоборот, множество из второго примера не может быть пересчитано, оно больше множества из первого примера. И вот здесь в идеях Кантора происходит характерный поворот. Точки нашего отрезка с помощью чисел $1, 2, 3, \ldots$ обычным способом пересчитать нельзя! Но допуская актуальную бесконечность, мы отнюдь не обязываемся ограничиться этим обычным способом счета, и ничто не принуждает нас прекратить этот счет. Когда мы уже пересчитали $1, 2, 3, \ldots$, то пересчитанные нами предметы мы можем рассматривать как некое в этом конкретном упорядочении завершенное бесконечное множество. Если мы, как это делает Кантор, обозначим данное упорядочение по его типу символом ω, то счет может быть естественно продолжен: $\omega+1$, $\omega+2, \ldots$ до $\omega+\omega$, или $\omega\cdot 2$, а затем он продолжается и дальше: $\omega\cdot 2+1$, $\omega\cdot 2+2$, $\omega\cdot 2+3, \ldots$, $\omega\cdot 2+\omega=\omega\cdot 3$, а затем и далее: $\omega\cdot 2$, $\omega\cdot 3$, $\omega\cdot 4, \ldots$, $\omega\cdot\omega=\omega^2$, $\omega^2+1, \ldots$

Таким образом, мы получаем следующую таблицу:

$$
\begin{array}{llll}
1, & 2, & 3, & \ldots \\
\omega, & \omega+1, & \omega+2, & \ldots \\
\omega\cdot 2, & \omega\cdot 2+1, & \omega\cdot 2+2, & \ldots \\
\omega\cdot 3, & \omega\cdot 3+1, & \omega\cdot 3+2, & \ldots \\
\cdots & \cdots & \cdots & \cdots \\
\omega^2, & \omega^2+1, & \ldots & \\
\omega^2+\omega, & \omega^2+\omega\cdot 2, & \omega^2+\omega\cdot 3, & \ldots \\
\omega^2\cdot 2, & \ldots & & \\
\omega^2\cdot 2+\omega, & \ldots & & \\
\omega^3, & \ldots & & \\
\omega^4, & \ldots & & \\
\cdots & \cdots & \cdots & \cdots \\
\omega^\omega, & \ldots & &
\end{array}
$$

Это — первые трансфинитные канторовы числа, числа второго числового класса, как называет их Кантор. Таким образом, мы приходим к ним, просто продолжая счет за пределы обыкновенного счетного бесконечного, то есть вполне естественно и однозначно, определенным образом продолжая обычный счет в конечном. Подобно тому, как мы до сих пор считали 1-ю, 2-ю, 3-ю, ... вещь множества, мы теперь считаем ω-ю, $(\omega + 1)$-ю, ..., ω^{ω}-ю его вещь.

В связи с этим немедленно напрашивается естественный вопрос — нельзя ли при помощи трансфинитных чисел на самом деле пересчитать и те множества, которые в обычном смысле несчетны?

Развивая эти идеи, Кантор благополучнейшим образом построил теорию трансфинитных чисел и создал для них некое полное исчисление. Так в итоге, в результате гигантской совместной работы Фреге, Дедекинда и Кантора, бесконечное было возведено на престол, и для него наступила пора упоения своим высочайшим триумфом. Бесконечное в своем отважном полете достигло головокружительной высоты.

Но реакция не заставила себя ждать, и она разыгралась весьма драматически. Произошло нечто совершенно аналогичное тому, что случилось в ходе развития исчисления бесконечно малых. На радостях по поводу новых и обильных результатов математики стали явно недостаточным образом критически относиться к вопросу о допустимости логических средств, потому что одни лишь постепенно ставшие обычными способы образования понятий и средства логического вывода стали приводить к противоречиям, поначалу одиночным, а затем исподволь становившимся все более резкими и серьезными: к так называемым парадоксам теории множеств. В особенности это относится к противоречию, найденному Цермело и Расселлом. Опубликование его оказало на математический мир прямо-таки катастрофическое воздействие. Оказавшись лицом к лицу с этими парадоксами, Дедекинд и Фреге фактически отказались от своей точки зрения и очистили поле битвы: Дедекинд долго колебался перед тем, как выпустить новое издание своей эпохальной работы «Что такое числа, и чем они должны быть»; Фреге тоже был вынужден признать тенденцию своей книги «Основные законы арифметики» («Grundgesetze der Arithmetik») ошибочной, в чем он признается в одном послесловии. И на учение Кантора с самых различных сторон посыпались ожесточеннейшие нападки. Это контрдвижение было столь стремительным, что общеупотребительнейшие и плодотворнейшие понятия математики, а также простейшие и важнейшие ее способы умозаключений оказались под угрозой, и применение их требовали запретить. Правда, не было недостатка и в защитниках старого, но оборонные мероприятия были довольно вялыми, и кроме того, они не были направлены единым фронтом в нужную сторону. Лекарств от парадоксов рекомендовалось слишком много, методы разъяснения их были слишком беспорядочны.

Перед лицом этих парадоксов надо согласиться, что положение, в котором мы пребываем сейчас, на длительное время невыносимо. Подумайте: в математике, — этом образце надежности и истинности, — понятия и умозаключения, как их всякий изучает, преподает и применяет, приводят к нелепостям. Где же тогда искать надежность и истинность, если даже само математическое мышление дает осечку?

Имеется, однако, вполне удовлетворительный путь, позволяющий избе-

жать парадоксов, не предавая при этом нашу науку. Позиции, исходя из которых мы будем разыскивать этот путь, и наши желания, которые будут указывать нам направление поиска, заключаются в следующем.

1. Мы будем повсюду, где открываются хотя бы малейшие перспективы, заботливо следить за плодотворными понятиями и способами умозаключений, будем ухаживать за ними, поддерживать их, делать их пригодными к использованию. Никто не сможет изгнать нас из рая, который создал нам Кантор.

2. Надо повсюду установить такую же надежность логических средств, как и та, что имеется в обыкновенной, элементарной арифметике, где никто не испытывает ни малейших сомнений и где противоречия и парадоксы возникают лишь в результате нашей невнимательности.

Достижение этой цели, очевидным образом, станет возможным лишь после того, как мы полностью уясним себе *сущность бесконечного*.

Выше мы убедились, что какие бы опыты и наблюдения и какую бы из наук мы ни подвергали рассмотрению, мы нигде в действительности не находим бесконечного. Так должны ли мысли о вещах быть столь непохожими на то, что происходит с вещами, должны ли они сами по себе идти другим путем, совершенно в стороне от действительности? Разве, напротив того, не ясно, что когда мы думаем, что в каком-то смысле постигаем реальность бесконечного, мы на самом деле всего лишь позволяем себе соблазниться тем, что в действительности так часто встречаемся и с чудовищно большими, и с чудовищно малыми размерами. А содержательные логические рассуждения, когда мы применяли их к действительным вещам или событиям, — разве они нас где-нибудь обманывали или где-либо нам изменяли? Нет — содержательная логика необходима и незаменима. И обманывала она нас только тогда, когда мы мирились с произвольными абстрактными понятиями, в том числе и с такими, под которые подпадает бесконечное число объектов. Именно тогда мы и применяли недозволенные содержательные умозаключения, то есть явным образом не обращали внимания на необходимые предпосылки применения содержательной логики. А в признании того, что такие предпосылки имеются и приниматься во внимание должны, мы согласны с философами, и особенно с Кантом. Уже Кант учил, — и это составляет неотъемлемую часть его учения, — что математика обладает абсолютно не зависящим от логики имманентным содержанием, и потому никогда не может быть обоснована с помощью одной лишь логики, отчего, между прочим, старания Дедекинда и Фреге и должны были потерпеть крушение. Более того, нам уже в нашем представлении кое-что дано как предварительное условие применения логических умозаключений и выполнения логических операций: определенные, внелогические конкретные объекты, имеющиеся в созерцании в качестве непосредственных переживаний до всякого мышления. Для того чтобы логические рассуждения были надежными, эти объекты должны быть полностью обозримы во всех их частях, и предъявление этих объектов, их различение, следование друг за другом или то, как один из них располагается относительно других, — все это должно даваться непосредственно наглядно вместе с самими объектами как нечто такое, что не может быть сведено к чему-либо другому и не нуждается в таком сведе́нии. Это — та основная философская предпосылка, которую я считаю необходимой как для математики, так и вообще

для всякого научного мышления, понимания и общения. И в частности, в математике предметом нашего рассмотрения являются сами эти конкретные знаки, облик которых, согласно нашей установке, непосредственно ясен и впоследствии может быть узнаваем снова и снова.

Теперь напомним, как устроена обычная финитная арифметика и какова методика ее изложения. Конечно, ее можно строить отдельно, конструируя числа с помощью содержательных наглядных соображений. Однако данная математическая наука никоим образом не исчерпывается числовыми равенствами и не сводится к ним одним. И тем не менее, пожалуй, можно утверждать, что она является аппаратом, который в применении к целым числам должен всегда давать верные числовые равенства. Но тогда возникает обязанность исследовать строение этого аппарата настолько, чтобы в этом можно было убедиться. При этом в качестве подсобного средства в нашем рассмотрении должен находиться только тот же самый конкретно-содержательный подход и тот же самый финитный способ мышления, которые в само́м построении арифметики применялись для получения числовых равенств. Это требование в действительности выполнимо, то есть возможно чисто наглядным и финитным способом, — в точности так же, как получаются сами арифметические истины, — провести и рассмотрения, гарантирующие надежность математического аппарата. А теперь давайте рассмотрим эту арифметику поближе.

В ней будут иметься числовые знаки:

$$1, \quad 11, \quad 111, \quad 11111, \quad \ldots,$$

где каждый из них характеризуется тем, что в нем за 1 всякий раз снова следует 1. Эти числовые знаки, — они-то и являются объектами нашего рассмотрения, — сами по себе не означают ничего. Кроме этих знаков в элементарной арифметике мы будем пользоваться еще и другими знаками, которые будут нечто означать и будут служить нам для сообщений. Так, мы пользуемся знаком 2 для сокращенной записи числового знака 11, знаком 3 — для сокращенной записи числового знака 111,... Затем мы будем применять знаки $+$, $=$, $>$, а также и некоторые другие для сообщений об утверждениях. Так, запись $2+3=3+2$ будет использоваться для сообщения о том, что $2+3$ и $3+2$ с учетом используемого нами сокращенного способа записи представляют собой один и тот же числовой знак, а именно 11111. Точно так же запись $3>2$ будет служить для сообщения о том, что знак 3 (то есть 111) появляется позже знака 2, (то есть 11), то есть что этот последний является частью первого.

Для сообщений мы также вместо числовых знаков будем пользоваться буквами a, b, c. В дальнейшем запись $b>a$ будет являться сообщением о том, что числовой знак b появляется позже числового знака a. Равным образом, в рамках данного подхода запись $a+b=b+a$ представляет собой сообщение о том, что числовой знак $a+b$ означает то же, что и числовой знак $b+a$. При этом содержательная верность этого сообщения может быть доказана с помощью содержательных рассуждений. Пользуясь этим наглядным, содержательным способом изложения арифметики, мы можем добиться серьезных продвижений.

А теперь я хотел бы продемонстрировать вам один пример, в котором происходит выход за рамки этого наглядного способа рассмотрения. Самым

большим из до сих пор известных простых чисел (39 цифр) является число [2]

$$\mathfrak{p} = 170141183460469231731687303715884105727.$$

Пользуясь известным приемом Евклида, мы можем, не выходя за рамки нашей установки, доказать, что между $\mathfrak{p}+1$ и $\mathfrak{p}!+1$ обязательно имеется новое простое число. Само это высказывание тоже вполне согласуется с нашей финитной установкой. Действительно, в данном случае слово «существует» служит лишь для сокращения высказывания о том, что одно из чисел

$$\mathfrak{p}+1 \quad \text{или} \quad \mathfrak{p}+2 \quad \text{или} \quad \mathfrak{p}+3 \quad \ldots \quad \text{или} \quad \mathfrak{p}!+1$$

непременно является простым. А теперь пойдем дальше: очевидно, что то же самое я могу выразить словами: существует такое простое число, что оно

$$1) \quad > \mathfrak{p}$$

и в то же самое время

$$2) \quad \leqslant \mathfrak{p}!+1,$$

а отсюда мы приходим к формулировке теоремы, представляющей собой лишь часть евклидова утверждения — а именно, к теореме о том, что существует простое число $> \mathfrak{p}$. И хотя содержательно эта последняя гораздо слабее теоремы Евклида, а переход к ней выглядит совершенно безобидным, это частичное высказывание, если начать рассматривать его как самостоятельное утверждение в отрыве от сказанного выше, все-таки станет определенным прыжком в трансфинитное.

Итак, в чем же тут дело? Мы встречаем здесь экзистенциальное высказывание „существует“! Правда, с этим выражением мы встречались уже в теореме Евклида. Однако там слово „существует“ представляло собою, как я уже говорил, другой, сокращенный способ сказать, что

$$\mathfrak{p}+1 \quad \text{или} \quad \mathfrak{p}+2 \quad \text{или} \quad \mathfrak{p}+3 \quad \ldots \quad \text{или} \quad \mathfrak{p}!+1$$

является простым числом, — подобно тому, как вместо фразы: «этот кусок мела или тот кусок мела или ... или вот тот кусок мела имеет красный цвет» мы бы короче сказали: «среди всех этих кусков мела имеется по меньшей мере один красного цвета». Подобного рода утверждение, что среди некоторой конечной совокупности „существует“ предмет, обладающий определенным свойством, вполне отвечает нашей финитной установке. Альтернатива же «$\mathfrak{p}+1$ или $\mathfrak{p}+2$ или $\mathfrak{p}+3\ldots$ и так далее до бесконечности», наоборот, является, так сказать, бесконечной связкой «или», и подобный переход к бесконечному без особых разъяснений (и может быть, необходимых мер предосторожности) так же мало позволителен, как и переход в анализе от конечных произведений к бесконечным; и конечно же, он, вообще говоря, прежде всего бессмыслен.

И вообще, с финитной точки зрения экзистенциальное высказывание вида «существует число, обладающее таким-то и таким-то свойством» имеет смысл лишь *частичного* высказывания, то есть части более детального высказывания, которое, однако, таково, что точное содержание его во многих случаях несущественно.

Таким образом, мы наталкиваемся здесь на трансфинитное в процессе разложения некоторого экзистенциального высказывания, которое не может быть истолковано как связка «или». Равным образом, мы приходим

к трансфинитному и тогда, когда отрицаем утверждение общности, то есть утверждение о произвольных числовых знаках. Так, например, высказывание о том, что если $\mathfrak{a}$ — произвольный числовой знак, то всегда должно выполняться равенство

$$\mathfrak{a} + 1 = 1 + \mathfrak{a},$$

с финитной точки зрения *не может обладать отрицанием*. Факт этот мы можем себе уяснить, обратив внимание на то, что это высказывание нельзя истолковывать как соединенное связкой «и» *бесконечное* число числовых равенств, а лишь как гипотетическое суждение, которое утверждает нечто для случая, когда нам задан некоторый числовой знак.

Отсюда, в частности, следует, что с позиций финитной установки мы не можем утверждать альтернативу, гласящую, что равенство, подобное вышеприведенному, с фигурирующим в нем неопределенным числовым знаком, либо выполняется для любого такого знака, либо опровергается на контрпримере. И действительно, эта альтернатива, — как частный случай закона исключенного третьего, — существенным образом опирается на предположение о том, что утверждение об общезначимости этого равенства обладает отрицанием.

Во всяком случае мы констатируем, что оставаясь в области финитных высказываний, — что нам и приходится делать, — мы попадаем в господствующую здесь с трудом поддающуюся обозрению логическую обстановку, и эта необозримость начинает доходить до нестерпимости, когда в теоремах слова «все» и «существует» комбинируются друг с другом и одно попадает в область действия другого. Во всяком случае, те логические законы, которыми люди пользовались, с тех пор как они стали мыслить, и которым учил еще Аристотель, оказываются здесь недействительными. Мы могли бы искать выход в том, чтобы установить законы логики, справедливые в области финитных высказываний; но, вероятно, это нам бы не подошло, так как мы как раз и не хотим отказываться от пользования законами аристотелевской логики по причине их простоты, и никто, говори он хоть ангельским голосом, не удержит людей от того, чтобы отрицать любые утверждения, образовывать экзистенциальные суждения и применять закон исключенного третьего. Так как же нам теперь быть?

Давайте все-таки вспомним, *что мы — математики* и что в качестве таковых мы уже не раз бывали в аналогичных трудных ситуациях, и что нас выводил из них гениальный метод идеальных элементов. Кое-какие блистательные образцы применения этого метода я уже приводил в начале моего доклада. Так же, как $i = \sqrt{-1}$ было введено для того, чтобы сохранить простейший вид законов алгебры, — например, теорему о существовании и числе корней уравнения; так же, как были введены идеальные сомножители, — опять-таки для того, чтобы сохранить в силе простейшие законы делимости для целых алгебраических чисел, где, например, вводится общий идеальный делитель чисел

$$2 \quad \text{и} \quad 1 + \sqrt{-5},$$

хотя настоящего делителя у них и нет; точно так же и здесь *к финитным высказываниям мы должны будем присоединить идеальные высказывания* для того, чтобы сохранить простую форму законов обычной аристотелевской логики. И странным образом получается так, что способы

умозаключений, против которых Кронекер возражал с такой страстью, оказываются точной копией того, что тот же Кронекер с таким энтузиазмом превозносил в теории чисел у Куммера и чем он восхищался как высшим достижением математики.

Так как же нам все-таки прийти к этим *идеальным высказываниям*? Тут замечательно то — и это, во всяком случае, является благоприятным и говорящим в нашу пользу обстоятельством, — что для того, чтобы напасть на путь к ним, нам потребуется всего лишь естественным и последовательным образом продолжить то развитие, которое наука об основаниях математики уже получила к настоящему времени. В самом деле, давайте вспомним, что уже элементарная математика переступает за пределы точки зрения наглядной арифметики. Содержательно-наглядная арифметика, как мы ее понимали до сих пор, не включает в себя метод алгебраических буквенных исчислений. Формулы всегда употребляются в ней только для сообщений; буквы означают числовые знаки, а с помощью знака равенства в ней сообщается о совпадении двух числовых знаков. Наоборот, в алгебре буквенные выражения мы рассматриваем как образы, которые самостоятельны сами по себе, а содержательные теоремы арифметики формализуются ими. Вместо высказываний о числовых знаках появляются формулы, в свою очередь являющиеся конкретными объектами наглядного созерцания, а вместо содержательного арифметического доказательства появляется вывод одной формулы из другой по определенным правилам.

Таким образом, как это показывает нам уже алгебра, происходит увеличение числа финитных объектов. До сих пор это были только числовые знаки, такие как $1, 11, \ldots, 11111$. Они были единственными объектами содержательного рассмотрения. Но уже в алгебре математическая практика выходит за эти пределы. Ведь если даже какое-нибудь высказывание — вроде теоремы о том, что при любых числовых знаках $\mathfrak{a}$ и $\mathfrak{b}$

$$\mathfrak{a} + \mathfrak{b} = \mathfrak{b} + \mathfrak{a},$$

в связи со ссылками содержательного характера еще допустимо с нашей финитной точки зрения, то и тогда мы пользуемся не сообщением этого вида, а формулой

$$a + b = b + a,$$

которая в данном случае является уже совсем не непосредственным сообщением о чем-то содержательном, а некоторым формальным образом, отношение которого к прежним финитным высказываниям

$$2 + 3 = 3 + 2,$$

$$5 + 7 = 7 + 5$$

заключается в том, что мы в эту формулу вместо a и b подставляем числовые знаки $2, 3, 5, 7$ и благодаря этому, то есть определенному, — хотя и очень простому, — доказательству, получаем конкретные финитные высказывания. Так мы приходим к представлению о том, что знаки a, b, $=$ и $+$, равно как и вся формула

$$a + b = b + a$$

в целом, сами по себе никакого смысла не имеют, как его не имели и числовые знаки; однако из нее можно вывести формулы, которым мы приписы-

ваем значение, рассматривая их как сообщения о финитных высказываниях. Если мы эту концепцию надлежащим образом обобщим, то математика сведется к совокупности некоторых формул — а именно: во-первых, таких, которым соответствуют содержательные сообщения о финитных высказываниях, и во-вторых, таких, которые сами по себе никакого смысла не имеют, а просто являются *идеальными образами нашей теории.*

Так в чем же состояла наша цель? С одной стороны, мы нашли в математике такие финитные высказывания, которые содержат только числовые знаки, как-то:

$$3 > 2, \quad 2 + 3 = 3 + 2, \quad 2 = 3, \quad 1 \neq 1;$$

эти высказывания, если исходить из нашей финитной точки зрения, оказываются непосредственно наглядными и понятными без разъяснений; мы можем строить их отрицания; они истинны или ложны; можно свободно, не задумываясь, рассуждать о них по правилам аристотелевской логики; закон противоречия для них справедлив, то есть никакое высказывание этого рода не может быть истинно одновременно с его отрицанием; для них имеет место закон исключенного третьего, то есть верно либо само данное высказывание, либо его отрицание. Когда мы говорим: «данное высказывание ложно», то это равносильно тому, что «отрицание этого высказывания истинно». Кроме этих элементарных высказываний вполне непроблематичного характера, мы встречались с финитными высказываниями проблематичного характера, например, с отрицательными. И наконец, мы ввели идеальные высказывания, которые должны способствовать тому, чтобы обычные законы логики снова все вместе имели силу. Но так как идеальные высказывания, — собственно говоря, формулы, — сами по себе ничего не означают, поскольку они не выражают финитных утверждений, логические операции над ними не могут производиться содержательно, как над финитными высказываниями. Таким образом, оказывается необходимым формализовать логические операции, а также и сами математические доказательства; для этого требуется превратить логические отношения в формулы, так что мы должны будем к математическим знакам добавить еще и логические — например:

$$\underset{\text{и}}{\&}, \quad \underset{\text{или}}{\vee}, \quad \underset{\text{следует}}{\rightarrow}, \quad \underset{\text{не}}{-},$$

а кроме математических переменных $a, b, c, \ldots$ использовать еще и логические — переменные высказывания $A, B, C, \ldots$

В какой мере все это осуществимо? К счастью для нас, здесь вступает в игру та самая предустановленная гармония, которую мы так часто встречаем в истории развития науки и которая пригодилась Эйнштейну, когда для нужд своей теории гравитации он обнаружил полностью разработанную общую теорию инвариантов. Здесь в качестве такой успешно проделанной предварительной работы мы обнаруживаем *логическое исчисление.* Правда, это последнее первоначально было создано совсем из других соображений, и потому знаки этого исчисления первоначально были введены тоже только для сообщений. Но мы проявим полную последовательность, если откажемся теперь от всякого значения логических знаков, как в свое время отказались от какого бы то ни было значения знаков математических, и объявим, что формулы логического исчисления тоже сами по себе не означают ничего, а являются идеальными высказываниями.

В этом исчислении мы располагаем неким знаковым языком, который способен математические теоремы выразить с помощью формул, а логический вывод с помощью формальных процессов. Аналогично тому, как это делалось при переходе от содержательной арифметики к формальной алгебре, мы и в логическом исчислении рассматриваем знаки и символы операций в отрыве от их содержательного значения. Тем самым мы в конце концов вместо содержательной математической науки, которая передается обыкновенным языком, получаем некоторый запас формул, построенных по определенным правилам из математических и логических знаков. Математическим аксиомам среди этих формул соответствуют некоторые конкретные формулы, а содержательным умозаключениям — правила, по которым эти формулы следуют друг за другом. Таким образом, содержательные рассуждения заменяются формальными действиями над внешним видом этих формул, проводимыми по определенным правилам, и тем самым совершается строгий переход от наивной трактовки к формальной, с одной стороны, самих аксиом, которые первоначально тоже наивно считались фундаментальными истинами и которые уже давно в современной аксиоматике рассматриваются только как фиксации связей между понятиями, а с другой стороны — логического исчисления, которому первоначально отводилась роль всего лишь некоего нового языка.

Теперь мы еще вкратце разъясним, ка́к будет формализоваться понятие *математического доказательства*. Как я уже говорил, определенные формулы, служащие кирпичами, из которых возводится формальное здание математики, называются аксиомами. Математическое доказательство представляет собой некую фигуру, которая как таковая должна быть нам наглядно предъявлена. Оно состоит из выводов, совершаемых по правилу вывода

$$\frac{\begin{array}{c}\mathfrak{S}\\ \mathfrak{S}\longrightarrow\mathfrak{T}\end{array}}{\mathfrak{T}},$$

где всякий раз каждая из посылок (то есть из формул $\mathfrak{S}$ и $\mathfrak{S}\to\mathfrak{T}$) есть либо аксиома (или получается из аксиомы в результате подстановки), либо совпадает с заключительной формулой другого вывода, уже встречавшегося в доказательстве ранее (или получается из этой формулы в результате подстановки). Формулу мы будем называть *доказуемой*, если она является либо аксиомой, либо заключительной формулой какого-либо доказательства.

Выбор аксиом для нашей теории доказательств нашей программой уже предрешен. Несмотря на некоторый произвол в их подборе, мы здесь, по аналогии с аксиоматикой геометрии, разобъем их на качественно различные обособленные группы, в каждой из которых приведем несколько примеров.

I. Аксиомы следования:

$$A\to(B\to A)$$

(присоединение посылки);

$$(B\to C)\to\{(A\to B)\to(A\to C)\}$$

(правило исключения).

II. Аксиомы отрицания:

$$\{A \to (B\&\overline{B})\} \to \overline{A}$$

(приведение к нелепости (reduction ad absurdum));

$$\overline{\overline{A}} \to A$$

(закон двойного отрицания).

Аксиомы групп I и II входят в состав аксиом исчисления высказываний.

III. Трансфинитные аксиомы:

$$(x)A(x) \to A(a)$$

(заключение от общего к частному, аксиома Аристотеля);

$$\overline{(x)}A(x) \to (\mathsf{E}x)\overline{A(x)}$$

(если свойство таково, что им обладают не все объекты, то для него существует контрпример);

$$\overline{(\mathsf{E}x)}A(x) \to (x)\overline{A(x)}$$

(если не существует примера, для которого свойство выполнялось бы, то оно тождественно ложно).

При этом обнаруживается одно весьма замечательное обстоятельство, а именно, что все эти трансфинитные аксиомы могут быть выведены из одной-единственной, — той, что заодно содержит в себе и ядро так называемой аксиомы выбора, до сих пор чаще всего оспаривавшейся в математической литературе:

$$A(a) \to A(\varepsilon(A))$$

(здесь ε — трансфинитная логическая функция выбора).

Ко всему этому добавляются чисто математические аксиомы.

IV. Аксиомы равенства:

$$a = a,$$

$$a = b \to (A(a) \to A(b)).$$

V. Аксиома числа:

$$a' \neq 0.$$

IV. Аксиома полной индукции:

$$\{(A(0)\&(x)(A(x) \to (A(x'))\} \to A(a).$$

На этом пути мы оказываемся в состоянии реализовать нашу теорию доказательств и построить систему доказуемых формул, т. е. математическую науку.

Но на радостях по поводу этой удачи вообще и по поводу логического исчисления в частности, которое мы без каких-либо усилий с нашей стороны получили в руки в качестве незаменимого оружия, мы все-таки не должны забывать о существенной предпосылке, лежащей в основе всего сделанного нами. А именно, речь идет об условии, — одном-единственном,

но зато абсолютно необходимом, — с которым связывается применение метода идеальных элементов, и это — *доказательство непротиворечивости*: расширение путем добавления идеального законно лишь тогда, когда в прежней, более узкой области из-за этого не возникает никаких противоречий, и значит если отношения, возникающие между старыми объектами при исключении идеальных, всегда имеют место и в прежней области.

Однако данная проблема, — проблема непротиворечивости, — при современном состоянии дел вполне доступна для разработки. Именно, подставив в логическую формулу $(A\&\overline{A}) \rightarrow B$, — которая, как легко показать, выводится из логических аксиом, — вместо B формулу $0 \neq 0$, мы выведем формулу

$$(A\&\overline{A}) \rightarrow 0 \neq 0,$$

так что для доказательства искомой непротиворечивости нам теперь остается только показать, что в математическом доказательстве, проведенном по сформулированным выше правилам, формула $0 \neq 0$ никогда не появится в качестве заключительной и что, таким образом, она недоказуема. А это является задачей, которая в принципиальном отношении так же относится к области наглядного рассмотрения, как, например, к ней относится и задача установления иррациональности числа $\sqrt{2}$ (то есть задача установления невозможности указать два числовых знака $\mathfrak{a}$ и $\mathfrak{b}$, которые были бы связаны неким вполне определенным соотношением, а именно — соотношением $\mathfrak{a}^2 = 2\mathfrak{b}^2$). Соответственно, речь для нас пойдет о том, чтобы доказать, что невозможно привести математическое доказательство, обладающее неким вполне определенным свойством. Но ведь формализированное доказательство так же, как и числовой знак, является конкретной и обозримой вещью. Оно сообщаемо от начала и до конца. Интересующее нас свойство заключительной формулы «быть формулой $0 \neq 0$» тоже является конкретно проверяемым свойством доказательства. Все это действительно можно пытаться показать, и тем самым введение наших идеальных высказываний оказывается оправданным.

Одновременно мы испытываем радостное волнение еще и от того, что принимаем тем самым участие в решении еще одной давней и жгучей проблемы. Речь идет о проблеме *непротиворечивости аксиом арифметики*. Эта проблема, — проблема установления непротиворечивости, — возникает всюду, где применяется аксиоматический метод. Ведь при выборе, толковании и использовании аксиом и правил вывода мы не хотим зависеть только от доброй веры и слепого доверия. В геометрии и в физических теориях установление их непротиворечивости удается провести путем сведения этого вопроса к вопросу о непротиворечивости арифметических аксиом. К самой арифметике этот метод очевидным образом не приложим. Наша теория доказательств, опираясь на метод идеальных элементов, позволяет сделать этот последний важный шаг и тем самым завершает создание учения об аксиоматике. И того, что мы пережили дважды, — один раз, когда речь шла о парадоксах исчисления бесконечно малых, и второй, когда мы говорили о парадоксах теории множеств, — этого в третий раз не случится и не произойдет больше никогда.

Однако наша эскизно набросанная здесь теория доказательств в состоянии дать не только надежную гарантию основаниям математической науки.

Я полагаю, что она вообще дает ключ к обсуждению общих вопросов принципиального характера, попадающих в область математического мышления, — вопросов, подступиться к которым раньше было просто невозможно.

Расширяясь, математика в известной степени превращается в третейский суд, в трибунал высшей инстанции, выносящий решения по принципиальным вопросам, причем на конкретной основе, на которой все должны иметь возможность договориться и где каждое утверждение может быть проверено.

И претензии новейшего так называемого „интуиционизма", — как бы скромны они ни были, — тоже, по моему мнению, должны сначала получить от этого трибунала свидетельство на свои права.

В качестве примера принципиального вопроса я хотел бы избрать для обсуждения тезис о разрешимости любой математической проблемы. Все мы в этом убеждены. Ведь главная притягательная сила при занятии математической проблемой в том и состоит, что мы слышим в себе непрерывный призыв: вот проблема, ищи ее решение; ты можешь найти его с помощью чистого мышления: ведь в математике нет Ignorabimus. И хотя моя теория доказательств в общем не может указать путь, на котором можно было бы найти решение любой проблемы — такого пути нет, но доказательство того, что допущение о разрешимости любой математической проблемы непротиворечиво, вполне попадает в область нашей теории.

И напоследок давайте еще раз вспомним о нашей исходной теме и подведем итог всем нашим рассуждениям о бесконечном. Наш общий вывод таков: в реализованном виде бесконечное не встречается нигде. Его нет в природе, и оно также недопустимо и в качестве основы нашего разумного мышления, — достойный внимания пример гармонии между бытием и мышлением. В противоположность предшествующим стремлениям Фреге и Дедекинда, мы пришли к убеждению, что как предварительное условие для возможности научного познания необходимы некоторые наглядные представления и благоразумие и что одной только логики для этого недостаточно. Оперирование с бесконечным может быть сделано надежным только через конечное.

Роль, которая остается здесь за бесконечным, это скорее роль всего лишь идеи, — если по Канту под идеей подразумевать понятие, образованное разумом, которое выходит за пределы всякого опыта и посредством которого конкретное дополняется в смысле цельности, — более того, идеи, которой мы можем вполне доверять в рамках, поставленных теорией, намеченной и представленной здесь.

И в заключение я хотел бы выразить мою благодарность П. Бернайсу за чуткое сотрудничество и ценную помощь, оказанную им мне как по существу вопроса, так и в части окончательной редакции текста.

ПРОБЛЕМЫ ОБОСНОВАНИЯ МАТЕМАТИКИ*)[1)]

Последние десятилетия были периодом наивысшего расцвета математической науки.

Напомню о том, что в арифметике, особенно в теории алгебраических числовых полей, были решены труднейшие проблемы и была завершена постройка этого прекрасного творения мысли. Вместе с тем открыты трансцендентные функции, связанные с числовыми полями, которые долго разыскивались и которые удалось выявить благодаря разнообразным, ранее скрытым теоретико-числовым истинам. С другой стороны, способы образования понятий в теории идеалов были с большим успехом перенесены далеко за пределы теории чисел, в алгебру и в теорию функций, и тем самым большой комплекс математических дисциплин был приведен в единую систему.

И в теории функций комплексного переменного за истекший промежуток времени также были достигнуты немалые успехи. В частности, благодаря развитию принципа конформного отображения, мы имеем теперь прекрасные методы построения автоморфных функций и решения проблемы униформизации. Столь трудные доказательства теорем существования в высшей степени упростились и стали прозрачными благодаря применению методов вариационного исчисления.

А какую полноту картины дает нам геометрия! Одна только топология настолько обогатилась новыми постановками вопросов и методами исследования, что в этом должно усмотреть возникновение новой самостоятельной ветви науки. Также и дисциплины, близкие старой геометрии, — теория групп и теория инвариантов — расширились и углубились сверх ожидания.

Наконец, физика воздвигла перед нашими глазами математические здания, палаты которых импонируют своим великолепием. Мы имеем в виду и приложения вообще: не худшие плоды пожинает математика на полях своих приложений, будь то ее приложения к смежным дисциплинам или к вопросам, возникающим из потребностей практики. Область, в которую проникает математика, постоянно расширяется.

Столь отрадное положение вещей особенно сильно обязывает математиков укреплять математику в ее основах.

Каково же широко распространенное мнение о математиках и математическом мышлении? Оно гласит: математические истины абсолютно надежны, так как они доказаны исходя из определений, посредством верных выводов. Поэтому они и должны всегда соответствовать действительности.

---

*) Probleme der Grundlegung der Mathematik. — Math. Ann., 1930, Bd. 102, S. 1–9. [1] *Перевод З. А. Кузичевой.*

1) Доклад, прочитанный на Международном математическом конгрессе в Болонье 3-го сентября 1928 г.

Согласно этому популярному мнению, математика должна служить образцом для науки вообще. Теперь посмотрим, так ли обстоит дело с математикой. Каким было состояние вопросов обоснования математики в последние тридцать лет? Великими классиками и авторами исследований по основаниям были Кантор, Фреге и Дедекинд; они нашли своего конгениального истолкователя в лице Цермело. Цермело предложил гипотезы, необходимые для аксиоматического построения теории множеств, и тем самым уточнил средства, которые Кантор и Дедекинд применяли неопределенно и отчасти бессознательно [2]. К тому же эти аксиомы Цермело таковы, что вряд ли могло появиться серьезное сомнение в их справедливости. Образ действий Цермело был вполне оправдан и соответствовал аксиоматическому методу. Все же пути, которыми шел Цермело, под влиянием авторитетных математических кругов были оставлены. Старые возражения Кронекера, направленные против Кантора и Дедекинда, которые мы считали уже давно преодоленными и которым сам Кронекер не следовал в своих работах, были выдвинуты вновь. Злополучное мнение Пуанкаре, касающееся заключения от n к $n+1$, которое уже за два десятилетия до того Дедекинд опроверг с помощью обстоятельного доказательства, — помешало продвижению вперед. Пуанкаре выдвинул и поддерживал новое запрещение, запрещение непредикативных высказываний, хотя Цермело тотчас же указал убедительный пример против этого запрета и, кроме того, этот запрет противоречил результатам Дедекинда [3]. К сожалению, в остальном превосходная логика Рассела, будучи применена к математике, также содействовала лжеучению. Таким образом, произошло то, что наша любимая наука в вопросах, касающихся ее арифметической сущности и ее основания, в продолжение двух десятилетий находилась в каком-то летаргическом сне.

Я приветствую как пробуждение, как сияющую зарю тот факт, что в последнее время ряд молодых математиков снова вернулся к идеям Цермело; эти математики дополнили аксиомы Цермело и успешно разработали при этом ряд важных, глубоких вопросов [4].

Правда, окончательное решение проблем обоснования с помощью этого аксиоматического способа никогда не будет возможно. Действительно, аксиомы, положенные Цермело в основание, содержат настоящие содержательные предположения, а в доказательстве их как раз и состоит, как мне кажется, главная задача исследований по обоснованию математики — ведь уже тогда доказательство непротиворечивости арифметических аксиом стало жгучим вопросом. Если же за исходный пункт и основание доказательства мы примем содержательные аксиомы, то математика тем самым потеряет характер чего-то абсолютно достоверного. Принимая предпосылки, мы переходим в область проблематичного, так как различия в мнениях людей основываются большей частью на том, что они исходят из различных предпосылок. Поэтому в последнее время в ряде докладов по обоснованиям математики я выбрал новый путь для разрешения проблем обоснования. С помощью этого нового обоснования математики, которое справедливо может быть названо теорией доказательства, я надеюсь с вопросами обоснования математики, как таковыми, покончить тем, что каждое математическое высказывание я превращу в конкретно предъявляемую и строго выводимую формулу и тем самым перемещу весь комплекс вопросов в область чистой математики.

Конечно, для полного проведения этой задачи необходимо преданное сотрудничество молодого поколения математиков.

В этом смысле я хотел бы сегодня высказаться несколько подробнее. Все важнейшие проблемы концентрируются вокруг выставленной мною так называемой ε-аксиомы, которая гласит:

$$A(a) \to A(\varepsilon(A)).$$

При применении этой аксиомы следует прежде всего обращать внимание на род тех переменных, к которым относится ε. Когда имеют дело с числами, они же служат для формулировки обычных выводов, содержащих слово «некоторые»: под $\varepsilon(\mathfrak{A})$ понимают некоторое число, для которого высказывание $\mathfrak{A}$ заведомо справедливо, если вообще существует число, для которого $\mathfrak{A}$ справедливо.

Я хотел бы теперь назвать некоторые проблемы.

В работах Аккермана[2] и Ноймана[3] проводится доказательство непротиворечивости ε-аксиомы для чисел; тем самым разрешены следующие три проблемы.

1. Закон исключенного третьего для чисел, т. е. утверждение: если некоторое высказывание имеет место не для всех целых чисел, то существует число, для которого это высказывание неверно. Например, согласно Кронекеру, целую рациональную функцию переменной x с целыми коэффициентами недопустимо определять как неприводимую, указывая, что не существует представления этой функции в виде произведения такого же рода двух функций. Я же, с помощью теории доказательств, показываю, что, наоборот, это определение является в чисто математическом смысле вполне строгим; поэтому утверждение Кронекера не только логически неправильно, но и чисто арифметически неверно — неверно в том смысле, в каком бывает неверна ложная арифметическая теорема или ложная теоретико-числовая формула.

2. Истолкование утверждения о существовании некоторого числа в смысле такого числа: «наименьшее число, которое...»

3. Заключение от n к $n+1$, при котором формулу

$$(\varepsilon(A) = b') \to \overline{A(b)}$$

присоединяют в качестве аксиомы.

Как вы уже заметили, существенным вспомогательным средством в моей теории доказательства служит символическая запись понятий. Этой классической системой записи мы обязаны Пеано, который ее ввел и тщательно разработал. Форма, в которой я ею пользуюсь, в основном совпадает с той, которую первоначально ввел Рассел.

До сих пор еще не решены следующие проблемы.

Проблема I.

Доказательство непротиворечивости ε-аксиомы для функциональной переменной f. Доказательство ее уже намечено: Аккерман продвинул его

---

[2] *Ackermann W.* Begründung des «tertium non datur» mittels der Hilbertschen Theorie der Widerspruchsfreiheit. — Math. Ann., 1925, Bd. 93, S. 1–36. С тех пор Аккерман упростил свое доказательство.

[3] *Neumann J.* Zur Hilbertschen Beweistheorie. — Math. Zeitschr., 1927, Bd. 26, S. 1–46.

так далеко, что оставшаяся задача сводится к доказательству только чисто арифметической, элементарной теоремы о конечности.

С решением проблемы I сразу же получаются ответы на большой комплекс основных вопросов; именно, это доказательство непротиворечивости дает:

1) закон исключенного третьего для функций целых аргументов и, тем самым, и для действительных чисел;

2) процессы определения, против которых Пуанкаре возражал как против непредикативных, которые Рассел и Уайтхед сумели обосновать только с помощью весьма проблематичной аксиомы сводимости [5] и в связи с которыми Вейль однажды сказал о существовании в анализе порочного круга (circulus vitiosus) [6];

3) аксиому выбора в ее более слабой формулировке.

Относительно пункта 3 сделаем следующее замечание. В новейших исследованиях аксиомы выбора были указаны многочисленные оттенки между слабыми и сильными формулировками принципа выбора. Эти оттенки преимущественно касаются мощности множества множеств и множества их представителей, особенно различия между счетными и несчетными множествами.

Руководствуясь теорией доказательства, мы считаем существенным иное различие; именно, мы будем отличать случай, когда требуется, чтобы выбор представителя некоторого множества был однозначно определен составом элементов множества, независимо от способа определения этого множества, от того случая, когда этого не требуется.

Пусть, например, дана некоторая однопараметрическая совокупность множеств $M(t)$, и пусть для каждого значения действительного параметра t множеством $M(t)$ служит вполне определенное множество действительных чисел, содержащее по крайней мере один элемент. Принцип выбора в своей более слабой формулировке требует, в таком случае, существования однозначной функции $f(t)$ такого рода, чтобы для каждого значения t значение $f(t)$ принадлежало бы к $M(t)$. Принцип выбора в своей более сильной формулировке требует, кроме того, существования такой функции $f(t)$, для которой

$$f(t_1) = f(t_2)$$

всякий раз, как множества $M(t_1)$ и $M(t_2)$ имеют один и тот же состав элементов.

С помощью ε-аксиомы для функциональной переменной f мы получаем для множеств действительных чисел принцип выбора в его более слабой формулировке.

В результате решения нашей проблемы I, мы овладеваем в первую очередь следующими теориями.

1. Теорией действительного числа (дедекиндово сечение, верхняя грань ограниченных множеств действительных чисел).

2. Пеановским обоснованием учения о числе. — Эта теория не требует никакого принципа выбора, но нуждается в непредикативных определениях, например, в определении для $a \leqslant b$; именно: всякое множество, которое содержит a и которое, содержа n, содержит также и $n+1$, содержит b. Раньше при теоретико-множественных обоснованиях теории чисел усматривали

проблематическое всегда только в предположении о бесконечности области индивидуумов. Можно убедиться в том, что это предположение не содержит противоречия, уже на основании доказательства о непротиворечивости его для чисел. Большую трудность представляет доказательство непротиворечивости непредикативного определения.

Решение проблемы I дает также полное оправдание гениальному методу Дедекинда, изложенному в его работе «Что такое числа и для чего они служат» [7].

3. Теорией Кантора о том, что числовой ряд есть вполне упорядоченное множество. Благодаря этой теории учение о числах второго числового класса, которое можно аксиоматически построить совершенно аналогично теории числа, сводится к теории функций числовых переменных.

Проблема II.

Для дальнейшего развития анализа, особенно для теории точечных множеств (теоретико-множественной топологии), а также для теории чисел второго и более высоких классов следует позаботиться о непротиворечивости ε-аксиомы для переменных более высоких порядков и в первую очередь — для переменных по функциям действительного переменного.

Далее, для доказательства теоремы о полном упорядочении, а также для некоторых доказательств в теории измеримости (доказательства для случаев неизмеримости) требуется аксиома выбора в ее более сильной формулировке, которая в теории доказательства выражается формулой

$$((f)(A(f) \rightleftarrows B(f))) \rightarrow (\varepsilon(A) = \varepsilon(B))$$

(аксиома равенства выбора); $\varepsilon(A)$ и $\varepsilon(B)$ в данном случае являются функциями числовых переменных, а равенство означает совпадение для всех значений аргументов. Для того, чтобы присоединить эту формулу, необходимо опять-таки доказать ее непротиворечивость.

Проблема III.

Утверждается, что система аксиом теории чисел и анализа вообще обладает полнотой; но обычные соображения, с помощью которых показывают, что любые две реализации системы аксиом теории чисел или анализа должны быть изоморфны, не удовлетворяют требованиям финитной строгости.

Речь идет о том, чтобы сначала для теории чисел, область которой может быть строго очерчена, перестроить финитным образом обычное доказательство изоморфизма так, чтобы тем самым было показано следующее.

Если можно доказать, что некоторое предложение $\mathfrak{S}$ не противоречит аксиомам теории чисел, то невозможно доказать, что предложение $\overline{\mathfrak{S}}$ (отрицание $\mathfrak{S}$) тоже не противоречит тем же аксиомам.

Также надо доказать положение, стоящее в тесной связи с предыдущим: если некоторое высказывание непротиворечиво, то оно также и доказуемо.

В более высоких областях допустим случай непротиворечивости $\mathfrak{S}$, или $\overline{\mathfrak{S}}$; тогда присоединение одного из этих двух высказываний в качестве аксиомы необходимо оправдать путем систематических предположений (принцип перманентности законов, возможность дальнейших построений и т. д.).

Против моей теории доказательства были выдвинуты возражения; они в основном базируются на ее непонимании. Поэтому я позволю себе сделать здесь еще некоторые пояснения.

Если имеется некоторое высказывание или доказательство, то оно должно быть обозримо во всех своих частях. Обнаружение, опознание, различие и следование одной за другой отдельных частей доказательства должно быть для нас непосредственно наглядным. Без этой установки вообще невозможно мышление и тем более научная деятельность. При исследовании вопроса о непротиворечивости речь идет о том, можно ли дать доказательство, которое привело бы к противоречию. Если такое доказательство не может быть мне предложено, то тем лучше, — в таком случае я избавлен от забот. Если же такое доказательство мне предложено, то я могу выбрать из него и рассмотреть внимательно некоторые определенные отдельные части, а следовательно, также и отдельные числовые знаки, которые в них встречаются и, следовательно, уже составлены и построены, и снова их разобрать. Этим, однако, собственно метод полной индукции не будет затронут; наоборот, сущность заключения по полной индукции — как это показал уже Дедекинд и как это снова подтверждает моя теория доказательства — в том и состоит, что оно применимо не только к отдельным, имеющим конечное значение случаям, но, прежде всего, к тем случаям, в которых рекурсия относится к выражениям с любыми связанными переменными (с «все» и «существует»); в таком случае оказывается, что полная индукция является источником понятия математической переменной, к которому с помощью только конечных методов невозможно подойти.

На той основе, которую я только что обсуждал, каждый раз должно проводиться доказательство непротиворечивости присоединения некоторого высказывания. Если такое доказательство удается провести, то для высказывания это означает, что в случае, когда из него может быть выведено числовое и имеющее конечное значение высказывание, это последнее каждый раз действительно верно. Доказательство непротиворечивости учит вместе с тем каждый раз, когда доказательство приводит к ложному результату, находить то место, в котором сделана ошибка.

Ясно, что чисто логические проблемы также попадают в область намеченной мною теории доказательства. Примером может служить следующая проблема.

Проблема IV.

Утверждение о полноте системы аксиом теории чисел может быть формулировано также и следующим образом. Если к аксиомам теории чисел присоединить формулу, принадлежащую теории чисел, но недоказуемую, то, исходя из этой расширенной системы аксиом, можно вывести противоречие.

Так как здесь, в теории доказательства, мы всегда имеем дело с формализированными доказательствами, то высказанные нами утверждения о полноте теории чисел заключают в себе вместе с тем и утверждение, что формализированные правила логического вывода достаточны, во всяком случае в области теории чисел.

Вопрос о полноте системы логических правил, поставленный в общем виде, представляет собою проблему теоретической логики. К этой более общей постановке вопроса мы придем, исходя из теории чисел, когда мы

из области рассматриваемых формул, в частности также и аксиом, исключим все те, в которые входит знак «′», но зато допустим появление предикатных переменных.

Реально это означает, что мы отвлекаемся от порядкового характера системы чисел и изучаем эту систему только как некоторую систему вещей, к которым могут быть отнесены предикаты с одним или несколькими аргументами. Среди этих предикатов только один, именно равенство (тождество), устанавливается как некоторое вполне определенное соотношение с помощью обычных аксиом равенства

$$a = a$$

$$a = b \rightarrow (A(a) \rightarrow A(b)),$$

в то время как остальные предикаты остаются произвольными.

В этой области формул отмечаются те, которые не опровергаются, какой бы смысл мы ни придавали произвольно избираемым предикатам, лишь бы этот смысл был вполне определен. Эти формулы представляют всегда справедливые логические предложения.

Тогда возникает вопрос, можно ли все эти формулы доказать, исходя из правил логических умозаключений с присоединением упомянутой аксиомы равенства, другими словами — является ли система обычных логических правил полной.

До сих пор мы убеждались в достаточности этих правил с помощью испытаний. Действительное доказательство этого имеется только в области чистой логики высказываний. В области логики предикатов с одним аргументом. доказательство полноты этих правил может быть получено из метода решения проблемы разрешимости (Entscheidungsproblem) (проблема элиминации Шредера) в том виде, в каком оно было дано, в связи с наметками Шредера, сначала Левенгеймом, а затем — в окончательной форме — Беманном [8].

Сегодняшний мой доклад показывает, как много проблем ждут еще своего решения. Но в общем принципиальном смысле даже малейшие следы неясности невозможны: на каждый из возникающих вопросов можно, на основании намеченной мною теории доказательства, ответить математически точным и однозначным образом. Соответствующие теоремы можно отчасти доказать уже теперь абсолютно надежным и чисто математическим методом, исходя из полученных до сих пор результатов; поэтому эти теоремы и не подвергались нападкам. Кто желает меня опровергнуть, должен, как это было до сих пор всегда принято в математике и как это останется и в будущем, указать мне точно то место, где находится предполагаемая ошибка. Возражения, в которых этого не сделано, я решительно отвергаю.

Я верю, что моя теория доказательства окажет нам еще более общую услугу. Ведь что́ бы было с истинностью наших знаний вообще, и ка́к обстояло бы с существованием и прогрессом науки, если бы даже в математике не было достоверной истины? И действительно, в наше время нередко даже в специальных изданиях и в открытых докладах высказывается скептицизм и уныние по поводу науки; это есть в некотором роде оккультизм, который я считаю вредным. Теория доказательства делает такую установку невозможной и дает нам возвышенное чувство убеждения в том, что по крайней мере для математического разума не поставлены никакие границы и что он

сам в состоянии проследить законы собственного мышления. Кантор сказал: «Сущность математики состоит в ее свободе», и я мог бы для склонных к сомнениям и впадающих в уныние добавить: в математике нет никаких Ignorabimus*); наоборот, мы всегда можем ответить на вопросы, имеющие смысл. Подтверждается то, что, возможно, предчувствовал уже Аристотель, именно, что наш разум не производит никаких таинственных фокусов, а наоборот, пользуется только вполне определенными, установленными правилами — что является вместе с тем порукой абсолютной объективности его суждений.

*) Мы не будем знать (*лат.*). — *Ред.*

ПОЗНАНИЕ ПРИРОДЫ И ЛОГИКА*)

Познание природы и жизни — первейшая наша задача. Все человеческие помыслы и вся наша воля направлены на ее решение, и с течением времени нам удается достичь все большего и большего успеха. За последние десятилетия мы смогли расширить и углубить наши познания о природе больше, чем за равное им число столетий в прошлом. Мы хотим сегодня воспользоваться представившейся возможностью, чтобы в соответствии с объявленной нами темой рассмотреть одну давнюю философскую проблему, а именно — вызывавший немалые споры вопрос о том, какая доля нашего знания приходится, с одной стороны, на мышление, а с другой — на опыт. Этот имеющий большую историю вопрос вполне обоснован, ибо ответить на него — по существу означает вынести решение о том, каков вообще характер нашего естественнонаучного познания и в каком смысле все знание, накапливаемое нами в процессе занятий естественными науками, является истиной.

На сегодняшний день имеются две причины, по которым мы, не проявляя при этом никакой заносчивости по отношению к философам и естествоиспытателям прошлого, можем с большей чем они уверенностью рассчитывать на правильное решение этого вопроса. И первая из них — это уже упоминавшийся быстрый темп, в котором развивается наша сегодняшняя наука.

Важнейшие открытия старых времен — открытия Коперника, Кеплера, Галилея, Ньютона, Максвелла — разделены огромными промежутками времени и растянулись почти на четыре столетия. Открытия нового времени начинаются с волн Герца, и тут события идут одно за другим: Рентген открывает свои лучи, Кюри — радиоактивность, Планк создает квантовую теорию. А в самое последнее время новые явления и неожиданные причинные связи стали сменять друг друга с такой скоростью, что обилие действующих лиц начинает вызывать едва ли не беспокойство: Резерфорд создает теорию радиоактивности, Эйнштейн открывает $h\nu$-закон, Бор выдвигает объяснение спектров, Мозли производит нумерацию химических элементов, Эйнштейн разрабатывает теорию относительности, Резерфорд осуществляет расщепление азота, Бор предлагает теорию строения атомов, Астон строит теорию изотопов.

Так что в одной только физике — и то мы стали свидетелями беспрерывной шеренги открытий, и каких открытий! По величию ни одно из них не уступает достижениям прошлого, но сверх того они во времени куда более компактно идут друг за другом, оставаясь внутренне столь же разнообразными, как и открытия прошлых времен. И здесь повсюду обнаруживается глубочайшая связь между теорией и практикой, мышлением и опытом. Время от времени то теория, то эксперимент вырываются вперед, но всякий раз они взаимно подтверждают, дополняют и стимулируют друг друга.

---

*) Naturerkennen und Logik. — Naturwissenschaften, 1930, S. 959–963. [1] *Перевод Н. М. Нагорного.*

И нечто сходное наблюдается также и в химии, и в астрономии, и в биологических науках.

Таким образом, в отличие от философов прошлого мы обладаем тем важным преимуществом, что нам довелось быть современниками многих из этих открытий и познакомиться с новыми воззрениями, возникшими в результате их появления. При этом среди сделанных открытий было немало и таких, которые радикально меняли старые, прочно укоренившиеся взгляды и представления, а то и вообще приводили к полному отказу от них. Вспомним хотя бы о новом понимании времени в теории относительности или о расщеплении химических элементов и о том, как благодаря этому были устранены предрассудки, даже прикоснуться к которым раньше никому не пришло бы и в голову.

Однако решению этой стародавней проблемы ныне способствует и еще одно немаловажное обстоятельство. В наше время на не досягаемую доныне высоту поднялись не только техника экспериментирования и искусные построения теоретической физики. Их антипод, — логическая наука, — тоже сделал существенный шаг вперед. Сегодня мы располагаем неким универсальным, — а именно, аксиоматическим — методом рассмотрения естественнонаучных проблем, и он обычно помогает нам уточнить проблематику, а зачастую способствует и подготовке решения поставленной задачи.

Давайте посмотрим, как обстоят ныне дела с аксиоматикой, вокруг которой сегодня ведется так много разговоров. Прежде всего отметим, что основная ее идея зиждется на том, что даже в самых обширных по своему размаху областях знания нередко бывает достаточно небольшого числа исходных положений, обычно называемых аксиомами, над которыми затем чисто логическим путем надстраивается все здание рассматриваемой теории. Однако одним лишь сказанным значение аксиоматики отнюдь не исчерпывается. Суть этого метода нам, пожалуй, лучше всего могли бы прояснить примеры, причем древнейшим, а также и самым известным из них, бесспорно, является геометрия Евклида, но я с гораздо большей охотой хотел бы совсем в немногих словах проиллюстрировать его на одном весьма впечатляющем примере из области современной биологии.

Дрозофила — крохотная мушка, но интерес наш к ней велик, и она стала объектом чрезвычайно многочисленных, весьма тщательных и успешных экспериментов по селекции. Обычно это мушка серого цвета, с красными глазами, без пятен, имеющая закругленные длинные крылья. Но встречаются мушки и с отклоняющимися признаками: желтые, а не серые, с белыми, а не красными глазами и т. д. Как правило, перечисленные пять характерных признаков сцеплены между собой: это значит, что если мушка желтая, то у нее тогда белые глаза, она пятнистая, крылья имеют вырезы и скошены, а если у мушки косые крылья, то она тогда желтая, у нее белые глаза и т. д. Однако при подходящих скрещиваниях у небольшой части потомства появляются отклонения от обычных комбинаций этих признаков, причем в постоянном процентном отношении. Числа, получаемые здесь экспериментальным путем, удовлетворяют евклидовым аксиомам конгруэнтности и аксиомам, которым подчиняется геометрическое отношение «между», так что законы наследственности оказываются одной из моделей аксиом линейной конгруэнтности, то есть теоремами элементарной геометрии об откладывании отрезков. Так просто и так точно! И вместе с тем все это выглядит

таким чудом, что об этом ранее, пожалуй, никто не смог бы даже помыслить в самых смелых своих мечтах.

Еще один пример аксиоматического метода мы возьмем из совершенно другой области знания.

В нашей теоретической науке мы привыкли к формальным приемам мышления и к абстрактным методам. Аксиоматический метод относится к области логики. При слове «логика» обычно нам представляется нечто очень скучное и трудное. Но сегодняшняя логика стала наукой легкой, доступной для понимания и весьма интересной. Мы, например, стали теперь понимать, что даже в повседневной жизни приходится пользоваться методами и понятиями, требующими высокой степени абстракции и проясняющимися лишь при условии допущения подсознательных применений аксиоматического метода. Таковы, например, общелогическая операция отрицания и в особенности понятие «бесконечного». Что касается этого последнего, то мы должны отчетливо уяснить себе, что «бесконечное» лишено наглядного — а без детального анализа и вообще какого бы то ни было — смысла. Ведь повсюду существуют лишь конечные вещи. Не существует ни бесконечной скорости, ни бесконечно быстро распространяющейся силы или действия. К тому же действие по природе своей даже дискретно и существует только квантами. Не существует ничего континуального, что могло бы быть бесконечно делимо. Даже свет, как и действие, обладает атомистической структурой. Да и сама наша Вселенная, по моему глубокому убеждению, имеет лишь конечную протяженность, и когда-нибудь астрономы смогут нам сказать, сколько километров мировое пространство имеет в длину, высоту и в ширину. И хотя в действительности очень большие числа встречаются часто, — например, расстояния до звезд в километрах или число различных потенциально возможных шахматных партий, — неисчерпаемость, или бесконечность, поскольку она представляет собой именно отрицание повсеместно господствующего положения вещей, представляет собой чудовищную абстракцию, которая реализуется лишь путем сознательного, а то и подсознательного применения аксиоматического метода. Эта трактовка бесконечного, обоснованная мной подробными исследованиями, решает ряд принципиальных вопросов; она, в частности, делает беспредметными кантовские антиномии, связанные с пространством и с безграничной делимостью, а стало быть, и снимает возникающие в связи с ними трудности.

Обращаясь теперь к самой нашей проблеме взаимосвязи между природой и мышлением, мы хотели бы зафиксировать три основных момента. Первый из них связан с только что обсуждавшейся проблемой бесконечности. Мы видели, что бесконечное не реализуется нигде; оно не присутствует в природе, а без специальных мер предосторожности оно не допустимо и в качестве основы нашего мышления. Уже в этом я усматриваю некий важный параллелизм природы и мышления, основополагающую согласованность между опытом и теорией.

Отметим и еще один параллелизм: наше мышление произрастает из единства и стремится создавать его; мы наблюдаем единство вещества в материи и всюду констатируем единство законов природы. При этом природа в наших исследованиях весьма предупредительно идет нам навстречу, как если бы она была готова охотно раскрыть нам свои тайны. Сильная разреженность распределения массы в небесном пространстве способствовала

открытию и более точной проверке ньютонова закона всемирного тяготения. Майкельсон, несмотря на огромную скорость света, как раз из-за достаточно быстрого обращения Земли вокруг Солнца смог достоверно констатировать несоблюдение закона сложения скоростей. Меркурий откровенно делает нам одолжение, двигая свой перигелий таким образом, что по этому движению мы можем проверять теорию Эйнштейна. И луч света от неподвижных звезд тоже проходит мимо Солнца так, что позволяет нам наблюдать его отклонение.

Но еще большее впечатление производит явление, которое, заимствуя терминологию у Лейбница, мы называем предустановленной гармонией. Она является прямым воплощением и реализацией математических идей. Древнейшими ее примерами служат конические сечения, которые были изучены намного раньше, чем мы успели составить себе представление о том, что планеты и даже электроны движутся по эллиптическим орбитам. Но самым великолепным и самым чудесным примером предустановленной гармонии является знаменитая эйнштейнова теория относительности. В ней дифференциальные уравнения для гравитационного потенциала с математической однозначностью выводятся из одного лишь общего требования инвариантности в сочетании с принципом максимальной простоты; и этот вывод был бы невозможен, не будь выполненных задолго до Эйнштейна глубоких и сложных математических исследований Римана. В новейший период все чаще встречаются случаи, когда важнейшие математические теории, стоящие в самом центре интересов математической науки, оказываются вместе с тем нужными и физике. Теорию уравнений с бесконечным числом переменных я развивал, исходя из чисто математической заинтересованности, и даже применял при этом терминологию спектрального анализа, не имея ни малейшего представления о том, что однажды в дальнейшем она будет реализоваться в реальных физических спектрах.

Эту согласованность природы и мышления, эксперимента и теории будет можно понять лишь в том случае, если мы с обеих сторон, — и со стороны природы, и со стороны нашего разума, — примем во внимание этот формальный элемент и некий тесно связанный с ним механизм. Процесс математического решения задачи дает, как нам кажется, те точки покоя и стоянки, в которых в равной мере пребывают как тела в реальном мире, так и идеи в мире духовном, становясь тем самым доступными контролю и сравнению.

Между тем и эта предустановленная гармония тоже не исчерпывает всех взаимосвязей между природой и мышлением, и она еще не снимает покрова с глубочайших тайн нашей проблемы. Чтобы получше разобраться в этих вещах, давайте внимательно присмотримся ко всему комплексу физико-астрономических знаний. Мы обнаружим тогда в современной науке наличие некой общей точки зрения, далеко выходящей за рамки старых подходов к постановке научных проблем и самих целей науки. Она заключается в том, что современная наука учит нас не только находить, — как это делается в классической механике, — по текущим исходным данным будущие движения и ожидаемые явления, но и показывает, что реально существующие ныне состояния материи и на Земле и во Вселенной отнюдь не случайны и не произвольны, а вытекают из физических законов.

Важнейшим тому доказательством служит и модель атома Бора, и струк-

тура звездного мира, и, наконец, вся история развития органической жизни. Следование такой методике, как кажется на первый взгляд, реально должно было бы привести к системе законов природы, в своей совокупности соответствующих действительности, а тогда и на самом деле потребовалось бы одно лишь мышление, — то есть дедукция в терминах понятий, — чтобы получить все физическое знание; и тогда был бы прав Гегель с его утверждением, что все явления природы можно вывести из понятий. Но вместе с тем такое заключение ошибочно. Ведь все-таки как обстоит дело с происхождением законов нашего мира? Как мы их получаем? И кто учит нас тому, что они соответствуют действительности? Ответ на эти вопросы гласит, что все это становится возможным единственно благодаря опыту. В противоположность Гегелю мы считаем, что законы окружающего нас мира не могут быть получены иначе, чем из опыта. В построении системы физических понятий могут участвовать и разного рода спекулятивные точки зрения, но только опыт в состоянии судить о том, верны ли сформулированные нами законы и построенная исходя из них логическая система понятий. Иногда первой, — в области чистого мышления, — возникала идея, как это было, например, с идеей атомистики Демокрита, когда существование атомов было экспериментальной физикой доказано лишь две тысячи лет спустя. А иногда впереди шел опыт, навязывая разуму выработанную им умозрительную концепцию. Так было, когда благодаря энергичному импульсу, сообщенному опытом Майкельсона, был устранен глубоко укоренившийся предрассудок об абсолютном времени и в итоге у Эйнштейна смогла возникнуть идея всеобщей относительности.

И если вопреки всему сказанному кто-нибудь захочет отрицать факт опытного происхождения законов окружающего мира, то он должен будет стать на ту точку зрения, что кроме дедукции и опыта имеется еще и некий третий источник познания.

Философы и в самом деле утверждали, — и Кант был классическим представителем этой точки зрения, — что помимо логики и опыта мы обладаем еще и некоторыми априорными знаниями о действительности. Я допускаю, что уже для построения теоретических каркасов различных теорий некоторые априорные представления необходимы и что именно они всегда лежат в основе осуществления нашего знания. Я полагаю, что и математическое знание в конечном счете тоже основывается на некоторой разновидности такого созерцательного понимания и что даже для построения арифметики нам необходима определенная априорная установка. Тем самым остается в силе самая общая из основных идей кантовской теории познания, а именно философская задача — a priori зафиксировать эту созерцательную установку и тем самым исследовать условия возможности любого познания в терминах понятий, а одновременно и возможности опыта. Я полагаю, что по существу именно это и делается в моих исследованиях по основаниям математики. Априорное оказывается при этом не более, но и не менее, чем основополагающей установкой, то есть выражением некоторых обязательных предпосылок мышления и опыта. Однако граница между тем, чем, с одной стороны, мы обладаем a priori, и тем, для чего, с другой стороны, необходим опыт, должна проводиться нами иначе, чем у Канта; Кант сильно переоценил роль и масштабы априорного.

Во времена Канта можно было думать, что существовавшие тогда пред-

ставления о пространстве и времени с той же общностью и так же непосредственно приложимы к действительности, как, например, и наши представления о количестве, очередности и величине, которыми мы постоянно и привычно пользуемся в математических и физических теориях. При таком подходе теория пространства и времени — а следовательно, в частности, и геометрия — должна быть чем-то таким, что, как и арифметика, предшествует всему естествознанию. Но еще до того, как нас к этому принудило развитие физики, от этой точки зрения Канта отказались, к примеру, Риман и Гельмгольц — и с полным правом, ибо геометрия есть не что иное, как та самая часть общего понятийного каркаса физики, которая отражает возможные отношения взаимного расположения твердых тел в мире реальных предметов. То, что движущиеся твердые тела вообще существуют, а также и то, каковы отношения их взаимного расположения, есть дело исключительно опыта. Утверждение, что сумма углов треугольника равна двум прямым, и факт выполнения аксиомы о параллельных также должны устанавливаться или опровергаться, как это было осознано еще Гауссом, исключительно экспериментом. Так, например, если бы оказалось, что все факты, выражаемые теоремами о конгруэнтности, находятся в соответствии с опытом, а сумма углов некоторого треугольника, состоящего из твердых стержней, оказалась бы меньше двух прямых, то никому бы и в голову не пришло утверждать, что в пространстве реальных тел должна выполняться аксиома о параллельных.

Занимая позицию априоризма, необходимо соблюдать крайнюю осторожность; ведь многое из того, что когда-то считалось априорно истинным, ныне признано просто ошибочным. Наиболее ярким тому примером является представление об абсолютном настоящем. Абсолютного настоящего не существует; мы просто с детства привыкли принимать представление о нем, потому что в повседневной жизни речь всегда идет лишь о небольших расстояниях и о медленных движениях. Если бы это было иначе, никому бы и в голову не пришло вводить абсолютное время. Но ведь даже таким глубоким мыслителям, как Ньютон и Кант, никогда не приходило на ум усомниться в абсолютном времени. Осторожный Ньютон формулировал это требование самым вопиющим образом — настолько, насколько это можно было сделать вообще: абсолютное, истинное время течет само по себе, причем, — в силу своей природы, — равномерно и безотносительно к каким бы то ни было обстоятельствам. Тем самым Ньютон честно отрезал себе все пути к отступлению или компромиссу. А Кант, этот критически мыслящий философ, в данном вопросе проявил себя настолько некритичным, что безоговорочно принял точку зрения Ньютона. И только Эйнштейн, — что навсегда останется одним из величайших достижений человеческого духа, — решительно освободил нас от этого предрассудка, а априорная теория с ее чрезмерно далеко зашедшими выводами ничем не могла быть более убедительно приведена ad absurdum*), чем этим продвижением физической науки. Именно: из принятия абсолютного времени вытекал, помимо прочего, и закон простого сложения скоростей при композиции двух движений. Вряд ли, впрочем, тогда можно было бы предложить закон, более очевидный и простой для понимания. Между тем из самых разнообразных экспе-

*) К нелепости (*лат.*). — *Ред.*

риментов в области оптики, астрономии и электродинамики в дальнейшем стало неопровержимо ясно, что закон простого сложения скоростей неверен; на деле выполняется другая, куда более сложная версия этого закона. Ныне мы можем сказать, что в новейшее время представленные Гауссом и Гельмгольцем взгляды на эмпирическую природу геометрии стали непреложным достижением науки, и сегодня они должны служить надежным отправным пунктом для всех философских построений, касающихся пространства и времени. В самом деле, эйнштейнова теория гравитации со всей очевидностью показала, что геометрия есть не что иное, как ветвь физики; геометрические истины ни в едином отношении принципиально не отличаются от физических и устанавливаются так же, как и они. Так, например, теорема Пифагора и закон всемирного тяготения Ньютона родственны по духу, поскольку ими обоими правит одно и то же фундаментальное физическое понятие — понятие потенциала. Но для каждого знатока эйнштейновой теории гравитации еще более ясно, что оба эти столь внешне различные и считавшиеся ранее далекими друг от друга закона, — один из которых известен с древних времен и с тех пор в каждой школе изучается в качестве теоремы элементарной геометрии, между тем как другой описывает взаимодействие масс, — не только однотипны по своему характеру, но и представляют собой всего лишь части одного и того же общего закона.

Едва ли можно привести более впечатляющий пример принципиального родства геометрических и физических фактов. Однако при обычном, логическом построении предмета и в силу повседневного опыта, привычного нам с детских лет, изложение геометрии и кинематики предшествует изложению динамики, и именно этим и объясняется то обстоятельство, что иногда об опыте забывают вообще. Итак, мы видим, что в кантовской теории априорного еще содержатся антропоморфные шлаки, от которых она должна быть очищена, и что после того, как они будут удалены, останется лишь та априорная установка, которая лежит в основе чисто математического знания. По существу она и есть та финитная установка, которую я охарактеризовал в ряде своих работ[1]).

Инструментом, осуществляющим посредничество между теорией и практикой, мышлением и наблюдениями, служит математика; она наводит между ними мосты и способствует тому, чтобы несущая способность этих последних постоянно возрастала. Отсюда следует, что в основе всей современной культуры, поскольку она направлена на постижение природы разумом и на подчинение ее человеку, лежит математика. Еще Галилей сказал: «Понять природу может лишь тот, кто знает язык, которым она говорит с нами, и его письмена; язык же этот — математика, а письмена — математические фигуры». Канту принадлежит изречение: «Я утверждаю, что в каждой отдельной естественной науке настоящей науки лишь столько, сколько в ней содержится математики». И действительно, любой естественнонаучной теорией мы овладеваем не прежде, чем освободим от скорлупы

---

[1]) См. Über das Unendliche. — Math. Ann., 1926, Bd. 95, S. 161 [имеется перевод на с. 431–448 наст. издания. — *Ред.*]; Die Grundlagen der Mathematik. — Abhandlungen a. d. math-em. Sem. d. Hamburgschen Universität, 1928, Bd. 6, S. 65. (Перепечатаны в качестве дополнений VIII и IX к «Grundlagen der Geometrie», 7. Auflage, 1930 [имеется перевод в кн.: *Д. Гильберт.* «Основания геометрии». — М.–Л., ГИТТЛ, 1948. — *Ред.*].)

ее математическое ядро и полностью раскроем его. Без математики невозможны ни современная астрономия, ни физика; теоретические части этих наук напрямую раскрываются математикой. Этим, а также многочисленным другим приложениям математика обязана своим авторитетом, в той мере, в какой она им пользуется в широкой аудитории.

Тем не менее, математики отказываются считать приложения мерилом ценности своей науки. Того же мнения придерживался и король математиков Гаусс, бывший прикладным математиком par excellence*), создавшим целые науки, такие как теорию ошибок и геодезию, в которых математика призвана была играть ведущую роль. Когда астрономы потеряли незадолго до того открытую ими малую планету Цереру, — одно из особенно важных и интересных небесных тел, — и никак не могли отыскать ее, Гаусс разработал новую математическую теорию, на основе которой правильно предсказал место, где она должна была оказаться. Гаусс изобрел также телеграф и ряд других практических устройств. Чистая теория чисел — это та область математики, которая пока еще никогда не находила себе применения. Но именно ее Гаусс называл Царицей математики, и именно она владела его умом и умами почти всех великих математиков. Гаусс говорил о волшебном очаровании, сделавшем теорию чисел любимой наукой первых математиков, о ее неисчерпаемых сокровищах, по богатству которых она далеко превосходит все остальные разделы математики. Гаусс вспоминал о том, как он еще в юные годы был настолько потрясен красотой теоретико-числовых исследований, что никогда уже не мог оставить их. Он восхвалял Ферма, Эйлера, Лагранжа и Лежандра как людей, покрывших себя неувядаемой славой, отворивших врата в святилище этой Божественной науки и показавших, какими несметными сокровищами оно заполнено. Столь же восторженно отзывались о теории чисел предшественники Гаусса, а также и математики, жившие после него, такие как Лежен Дирихле, Куммер, Эрмит, Кронекер и Минковский. Кронекер сравнивал тех, кто занимается теорией чисел, с лотофагами [2], которые «вкусив единожды от яства сего, более уже не могли от него отказаться».

Того же мнения придерживался и Пуанкаре, самый выдающийся математик своего поколения, бывший по существу не только математиком, но и физиком, а также небесным механиком. Пуанкаре резко выступил против Толстого, утверждавшего, что девиз «Наука ради науки» безрассуден. «Должны ли мы, — вопрошал Толстой, — при выборе рода занятий руководствоваться капризами нашей жажды знания? Не лучше ли было бы исходить из полезности, то есть из наших практических и моральных потребностей?» [3] Странно, что именно Толстого нам, математикам, приходится отвергать как плоского реалиста и бездушного утилитариста. Пуанкаре возразил Толстому, что если бы человечество следовало его, Толстого, рецепту, то наука вообще никогда не возникла бы. Достаточно раскрыть глаза, заключает Пуанкаре, чтобы увидеть, что достижения промышленности никогда не появились бы на свет, если бы в мире существовали одни лишь практики и если бы этим достижениям не способствовали незаинтересованные безумцы, никогда даже и не помышлявшие о какой-либо практической пользе. Того же мнения придерживаемся и все мы.

*) По преимуществу (*франц.*). — *Ред.*

Так же думал и наш великий кёнигсбергский математик Якоби, чье имя стоит рядом с именем Гаусса и с благоговением произносится всяким, кто занимается нашей наукой. Когда знаменитый Фурье однажды сказал, что основная цель математики заключается в объяснении явлений природы, Якоби отчитал его со всей страстностью своего темперамента. Такой философ, как Фурье, возмущенно воскликнул Якоби, должен был бы знать, что единственной целью всей науки является возвышение чести человеческого духа и что с этой точки зрения любая задача чистой теории чисел столь же достойна уважения, как и проблемы, служащие приложениям [4].

Тот, кто способен ощутить истинность возвышенного мышления и миросозерцания, явственно слышную в этих словах Якоби, тот не поддастся ретроградным и бесплодным сомнениям; он не поверит тем, кто ныне с философской миной глубокомысленным тоном пророчествует о закате культуры и поддается мысли о непознаваемости мира. Для математика не существует Ignorabimus*), как, по моему мнению, его не существует и для естествознания вообще. Философ Конт [5], пытаясь привести пример неразрешимой проблемы, однажды сказал, что науке никогда не удастся установить химический состав небесных тел. А всего через несколько лет Кирхгоф и Бунзен с помощью спектрального анализа решили эту проблему, и сегодня мы можем сказать, что даже самыми отдаленными звездами мы ныне пользуемся как важнейшими физическими и химическими лабораториями, равных которым нельзя найти и на Земле. Истинная же причина, по которой Конту не удалось найти неразрешимую проблему, заключается, по-моему, в том, что неразрешимых проблем не существует вообще. Так пусть же вместо безрассудного Ignorabimus и в противоположность ему наш лозунг гласит:

Мы должны знать.
Мы будем знать.

*) Мы не будем знать (*лат.*). — *Ред.*

Гёттингенский математический институт

ПРИЛОЖЕНИЯ И КОММЕНТАРИИ

ФРАГМЕНТ ПЕРВОГО ВАРИАНТА РАБОТЫ «О ПОВЕРХНОСТЯХ ПОСТОЯННОЙ ГАУССОВОЙ КРИВИЗНЫ» (1901 г.)*)

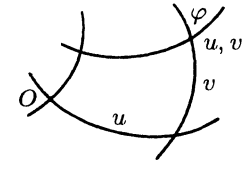
Формулы (2) и (3) доказывают известную теорему[1]:

В каждом четырехугольнике, образованном четырьмя асимптотическими линиями поверхности, длины дуг противоположных сторон равны.

Формула (3) позволяет выразить площадь четырехугольника, образованного асимптотическими линиями, через его углы; Дарбу[2] на этом пути пришел к следующей теореме:

Площадь четырехугольника, образованного асимптотическими линиями нашей поверхности, равна сумме углов четырехугольника, уменьшенной на 2π.

Формулы (1) дают параметрическое представление нашей поверхности, при котором координатные линии $u = \text{const}$, $v = \text{const}$ являются асимптотическими линиями. По приведенным выше соображениям прямоугольные координаты x, y, z являются, конечно, однозначно обратимыми функциями переменных u, v для достаточно малых значений u, v, т. е. формулы (1) осуществляют однозначное отображение *куска* uv-плоскости в окрестности точки $u = 0$, $v = 0$, на кусок нашей поверхности в окрестности точки O. Наша задача состоит в том, чтобы изучить отображение всей uv-плоскости на нашу поверхность, которое получается путем аналитического продолжения формул (1).



Если мы рассмотрим какую-либо асимптотическую линию нашей поверхности, то сразу выясняем, что в конечном она не может иметь особых точек. Действительно, если допустить существование такой особой точки, то ее можно принять за точку O, а тогда это приводит к противоречию с нашими предшествующими рассуждениями, поскольку через O всегда проходят две регулярные асимптотические линии и на поверхности достаточно малая окрестность точки O покрывается без пробелов регулярно проходящими асимптотическими линиями.

---

*) Часть статьи: Über Flächen von konstanter Gaußscher Krümmung. — Trans. Amer. Math. Soc., 1901, vol. 2, p. 87–99. Публикуется в качестве приложения к работе «О поверхностях постоянной гауссовой кривизны» по причинам, указанным в комментариях к этой статье. *Перевод* Б. Л. Лаптева.

[1] *Dini.* Annali di Mat., 1870, vol. 4, p. 175; *Darboux G.* Leçons sur la theorie générale des surfaces. Vol. 3, 1894, № 773; *Bianchi L.* Lezioni di geometria differenziale. — Bologna, 1927.

[2] *Darboux G.*, loc. cit., vol. 3, № 773 [1].

Из этих замечаний мы выведем аналитический факт, что функции x, y, z для всех вещественных u, v однозначно и безгранично продолжаемы. Чтобы это яснее понять, отложим от точки O на асимптотической линии $v = 0$ длину u в том или другом направлении соответственно тому, будет u положительным или отрицательным. Проведем затем через так полученную точку другую асимптотическую линию, далее отложим на ней длину v в том или другом направлении, смотря по тому, будет v положительным или отрицательным, и отнесем, наконец, полученной таким образом концевой точке, которая, скажем, имеет прямоугольные координаты x, y, z, значения параметров u, v. Таким образом каждой точке uv-плоскости будет сопоставлена определенная точка нашей поверхности, и функции x, y, z, осуществляющие это сопоставление, будут для всех вещественных значений переменных u, v однозначными и регулярными аналитическими функциями.

И тотчас доказывается, что, обратно, каждой точке нашей поверхности отвечает по меньшей мере одна пара значений u, v. Чтобы это усмотреть, обозначим буквой P точки, координаты которых представлены значениями функций

$$x(u, v), \quad y(u, v), \quad z(u, v),$$

а буквой Q точки, которые не охвачены нашим отображением, независимо от того, одна или несколько таких точек будут находиться в конечной области. Ясно, что имеется по меньшей мере одна точка A на поверхности, в произвольной близости к которой будут лежать как P, так и Q.

Из предыдущих рассуждений следует, что в окрестности точки A существует два семейства асимптотических линий, каждое из которых покрывает эту окрестность просто и без пробелов, и среди этих асимптотических линий должна быть по меньшей мере одна, содержащая как P, так и Q. Покажем это. Действительно, обратим внимание на одну из проходящих через точку A асимптотических линий и допустим, что она состоит только из точек P (соответственно Q); тогда асимптотические линии того семейства, к которому выбранная асимптотическая линия не принадлежит, будут содержать по меньшей мере одну точку P (соответственно Q), а именно точку пересечения с выбранной асимптотической линией. Но все линии этого семейства не могут, конечно, состоять только из точек P (соответственно Q), так как иначе вся окрестность точки A состояла бы только из точек P (соответственно Q).

Пусть теперь l будет длиной куска асимптотической линии, началом которого служит точка P, а концом Q. Рассмотрим обе проходящие через начальную точку P асимптотические линии; тогда этот кусок необходимо будет продолжением одной из этих двух асимптотических линий, и если u, v — координаты начальной точки P, то концевая точка Q рассматриваемого куска линии будет представлена следующими значениями параметров: $u \pm l, v$ или $u, v \pm l$, вопреки нашему предположению, что концевая точка Q не представима формулами (1).

Таким образом доказано, что формулы (1) дают представление всей поверхности, если u, v пробегают все вещественные значения.

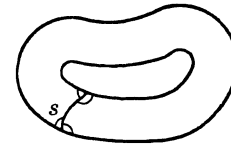
Наконец, для нашего исследования необходимо убедиться, что формулы (1) представляют какую-либо точку поверхности только *единственной* парой значений u, v, т. е. что найденное отображение нашей поверхности на

uv-плоскость будет взаимно однозначным не только для достаточно малой области, но и в целом.

Для этой цели мы последовательно докажем такой ряд предложений.

1. *На нашей поверхности не существует замкнутых, т. е. возвращающихся в себя асимптотических линий.*

Для доказательства допустим обратное, т. е. что такого рода асимптотическая линия на нашей поверхности имеется, и построим через каждую ее точку асимптотические линии другого семейства, отложив на них кусок дуги длины s в одну и ту же сторону. Полученные концевые точки тогда или образуют некоторую замкнутую асимптотическую линию, или же такая линия образуется впервые только после двукратного прохождения основной линии — это случай, который мог бы появиться, если бы наша поверхность являлась так называемой двойной поверхностью.



Рассмотрим теперь один из тех кусков асимптотических линий длины s, которые послужили нам для построения новой замкнутой асимптотической линии: будучи дважды взятым, он образует вместе с обеими замкнутыми асимптотическими линиями асимптотический четырехугольник, сумма углов которого точно равна 2π. Но это противоречит приведенному выше утверждению, по которому площадь четырехугольника из асимптотических линий равна избытку суммы его углов над 2π и потому этот избыток должен быть положительным.

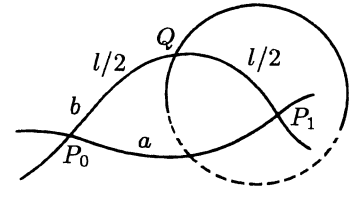
2. *Две асимптотические линии, проходящие через какую-либо точку поверхности, не пересекаются ни в какой другой точке нашей поверхности.*

Представим себе, что одна асимптотическая линия a продолжена в обоих направлениях до бесконечности и затем через одну ее точку P_0 в одну сторону проведена другая асимптотическая линия b. И допустим, что вопреки нашему предположению эта асимптотическая линия b, пересекающая a в первый раз в точке P_0, пересекает ее еще раз в точке P_1; тогда мыслимы два следующих случая:

первый: асимптотическая линия b может идти так, что, пересекая a, она войдет в точку P_1 с той же стороны относительно a, с которой вышла из P_0.

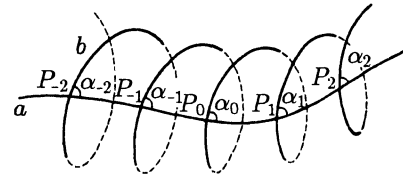
второй: асимптотическая линия b может идти так, что она войдет с другой стороны исходной асимптотической линии a и тогда, пройдя P_1, выйдет в ту же сторону относительно a, в которую выходила вначале из P_0.

Мы хотим показать, что оба случая невозможны. Что касается первого случая, то обозначим через l длину отрезка P_0P_1 на b, а середину этого отрезка обозначим через Q. Далее вообразим, что через каждую точку асимптотической линии a проведена другая асимптотическая линия в ту сторону, по которую лежит отрезок P_0P_1 на b, и на этой асимптотической линии отложен отрезок длины $l/2$. Для точек P_0 и P_1 кривой a мы получим таким образом именно точку Q как концевую. Вместе с тем все концевые точки образуют асимптотическую



линию, которая проходит через Q и туда же с той же касательной возвращается. Но это невозможно, так как по предложению 1 на нашей поверхности замкнутых геодезических не существует.

Этим доказано, что первый случай невозможен. Но и второй случай тоже невозможен. Пусть асимптотическая линия идет так, что после прохождения точки пересечения P_1 ее направление относительно a оказывается таким же, как ранее в P_0. Тогда мы могли бы получить продолжение этого куска P_0P_1 асимптотической линии b за P_1, построив, исходя из P_0, через каждую точку куска P_0P_1 линии b другие асимптотические линии и на всех этих других отложив в надлежащую сторону кусок, равный по длине куску P_0P_1 линии a. Полученные концевые точки образуют продолжение кривой b за P_1 до некоторой точки P_2 на a. Из этого куска P_1P_2 асимптотической линии b мы можем равным образом получить новый кусок асимптотической линии b, который исходит из точки P_2 и достигает точки P_3 на a, и т. д.



Также ясно, что мы можем продолжить с помощью соответствующего построения линию b в противоположном направлении от P_0 и получить последовательно куски P_0P_{-1}, $P_{-1}P_{-2}, \ldots$ линии b. Следовательно, асимптотическая линия b пересекает линию a в бесконечно большом числе точек

$$\ldots,\ P_{-3},\ P_{-2},\ P_{-1},\ P_0,\ P_1,\ P_2,\ P_3,\ \ldots,$$

причем соседние точки высекают равные по длине дуги асимптотической линии a. Обозначим углы, образованные асимптотической линией b с линией a в определенном направлении, соответственно через

$$\ldots, \alpha_{-3}, \alpha_{-2}, \alpha_{-1}, \alpha_0, \alpha_1, \alpha_2, \alpha_3, \ldots$$

Рассмотрим теперь четырехугольник $P_0P_1P_2P_1P_0$ из асимптотических линий, образованный кусками P_0P_1 на a, P_1P_2 на b, P_2P_1 на a, P_1P_0 на b. Четырьмя углами этого четырехугольника будут

$$\alpha_0, \quad \pi - \alpha_1, \quad \alpha_2, \quad \pi - \alpha_1;$$

поэтому по приведенной ранее теореме о четырехугольнике, образованном асимптотическими линиями, его площадь будет равна избытку его углов над 2π, причем этот избыток должен быть положительным. Значит,

$$\alpha_0 + \pi - \alpha_1 + \alpha_2 + \pi - \alpha_1 > 2\pi,$$

откуда

$$\alpha_0 - \alpha_1 > \alpha_1 - \alpha_2. \tag{4}$$

Таким же образом вообще

$$\alpha_k - \alpha_{k+1} > \alpha_{k+1} - \alpha_{k+2} \qquad (k = 0, \pm 1, \pm 2, \ldots). \tag{5}$$

Вследствие неравенства (4) $\alpha_0 - \alpha_1$ и $\alpha_1 - \alpha_2$ не могут быть оба равными нулю, т. е. мы должны принять

$$\alpha_0 - \alpha_1 \neq 0.$$

Из (5) следуют неравенства

$$\alpha_{-p} - \alpha_{-p+1} > \alpha_0 - \alpha_1 \qquad (p = 1, 2, 3, \ldots) \tag{6}$$

и

$$\alpha_0 - \alpha_1 > \alpha_p - \alpha_{p+1},$$

или

$$\alpha_{p+1} - \alpha_p > \alpha_1 - \alpha_0 \qquad (p = 1, 2, 3, \ldots). \tag{7}$$

Если мы выпишем неравенства (6) и (7) для $p = 1, 2, 3, \ldots$, то путем сложения получим

$$\alpha_{-n} > \alpha_0 + n(\alpha_0 - \alpha_1),$$
$$\alpha_{n+1} > \alpha_1 + n(\alpha_1 - \alpha_0).$$

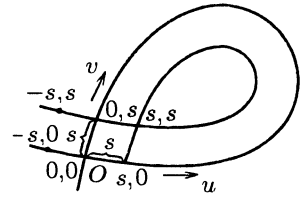
Если теперь случится, что $\alpha_0 - \alpha_1 > 0$, то для достаточно больших значений n первое из выписанных неравенств становится невозможным, так как углы α_k все меньше π; если же случится, что $\alpha_0 - \alpha_1 < 0$, то по тем же основаниям для достаточно больших n невозможно второе неравенство.

Поэтому для асимптотической линии b не может осуществиться ни один из рассмотренных возможных случаев, и, таким образом, доказательство предложения 2 завершено.

3. *Асимптотическая линия на нашей поверхности не может пересекать себя ни в одной точке, т. е. у нее нет двойных точек.*

Для доказательства мы допустим противоположное, т. е. что существует асимптотическая линия с двойной точкой, и поместим начало наших криволинейных координат u, v в эту двойную точку, выбрав обе ветви линии за координатные, направленные по ветвям в положительном направлении.

На координатной u-линии, начиная с точки $(-s, 0)$, проведем через каждую точку этой линии другие асимптотические линии и нанесем на них от этих точек в положительную сторону отрезки дуг длины s; если выбрать это s достаточно малым, то по упомянутой выше теореме о четырехугольнике, образованном асимптотическими линиями, все так полученные концевые точки тоже образуют асимптотическую линию. Эта асимптотическая линия исходит из точки $(-s, s)$ (соответственно $(-s, -s)$, если откладывать дуги в другую сторону), проходит через точку $(0, s)$ (соответственно $(0, -s)$) и оканчивается в точке $(s, 0)$ (соответственно $(-s, 0)$), пересекая себя в точке (s, s) (соответственно $(-s, -s)$ при продолжении).

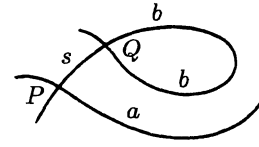


Таким образом, мы видим, что так построенная асимптотическая линия пересекает исходную асимптотическую линию в двух различных точках $(0, s)$ и $(s, 0)$ (соответственно $(0, -s)$ и $(-s, 0)$), что по предложению 2 невозможно.

4. *Если мы через каждую точку асимптотической линии a проведем другую асимптотическую линию и на ней по одну сторону отложим определенный отрезок s, то так полученные концевые точки образуют некоторую асимптотическую линию b, которая нигде не может пересечь линию a.*

Действительно, допустим, что точка P будет точкой пересечения так полученной асимптотической линии b с первоначальной линией a. Проведем

указанное в предложении построение, откладывая сначала от точки P по асимптотической линии b отрезок дуги длины s в соответствующую сторону от a. Перемещаясь от P по линии a, мы получим таким образом ветвь асимптотической линии b, проходящую через концевую точку Q. Таким образом, эта ветвь пересекает в точке Q первоначальный ход линии b; поэтому Q — двойная точка асимптотической линии b; но в силу предложения 3 появление двойной точки невозможно.



Из предложений 1 — 4 мы можем вывести следующие заключительные следствия.

Все асимптотические линии нашей поверхности распадаются на два семейства. Какие-либо две асимптотические линии, принадлежащие одному семейству, не пересекаются, тогда как две линии из различных семейств всегда пересекаются и притом только в одной точке.

Координатные линии $u = 0$, $v = 0$ являются двумя асимптотическими линиями, принадлежащими различным семействам. Из того что значения координат u, v выражают длины определенных отрезков координатных линий, мы на основании выясненных фактов выводим, что заданным значениям u, v всегда отвечает только одна точка нашей поверхности, т. е. *исследуемое отображение* (1) *нашей поверхности на uv-плоскость является с необходимостью однозначно обратимым. В частности, отсюда следует, что наша поверхность односвязна и не является двойной.*

После того как мы пришли к такому важному убеждению, мы вычислим площадь всей нашей поверхности двумя путями и придем тогда к противоречию.

Первый путь: мы рассмотрим на нашей поверхности образованный асимптотическими линиями четырехугольник, вершины которого определены следующими координатами

$$u, v; \quad -u, v; \quad -u, -v; \quad u, -v.$$

Так как каждый угол этого четырехугольника должен быть $< \pi$, то в любом случае сумма его углов $< 4\pi$, а площадь четырехугольника, т. е. избыток суммы углов над 2π обязательно $< 2\pi$. Заставим теперь значения u, v расти безгранично; тогда каждая фиксированная точка поверхности, очевидно, однажды попадет внутрь рассматриваемого четырехугольника и будет оставаться внутри всех последующих четырехугольников, так что безгранично растущий четырехугольник охватит всю поверхность. Отсюда заключаем, что вся площадь нашей поверхности $\leqslant 2\pi$.

С другой стороны, рассмотрим геодезические линии на нашей поверхности. Из-за отрицательности кривизны нашей поверхности каждая геодезическая линия между двумя своими точками является кратчайшей, т. е. имеет меньшую длину, чем всякая другая линия, проходящая на поверхности между этими двумя точками и такая, что ее непрерывным изменением можно перевести в упомянутую геодезическую.

Рассмотрим теперь на нашей поверхности какие-либо две геодезические, исходящие из точки O, и допустим, что они пересекаются еще в некоторой другой точке P поверхности. Но по доказанному ранее наша поверхность

односвязна, и поэтому каждая из этих геодезических линий OP может быть непрерывным изменением переведена в другую, так что по доказанному выше каждая из них короче другой, что невозможно. Поэтому наше допущение о существовании точки пересечения P следует также отбросить. Из этого заключения мы выводим также, что геодезическая линия на нашей поверхности не может ни пересекать себя, ни по себе возвращаться.

Представим себе теперь все исходящие из O геодезические линии, на которых отложены дуги равной длины r. Тогда концевые точки образуют на нашей поверхности замкнутую кривую [2] без двойных точек. Площадь области, ограниченной этой кривой, согласно известным формулам геометрии Лобачевского, равна

$$\pi\left(e^{r/2} - e^{-r/2}\right)^2.$$

Так как это выражение при бесконечно растущем значении r растет, превосходя все границы, то отсюда следует, что площадь нашей поверхности бесконечно велика. Но это следствие находится в противоречии с только что доказанным фактом, что эта площадь должна быть $\leqslant 2\pi$. Таким образом, мы вынуждены отбросить наше основное допущение и признать, что *регулярных поверхностей постоянной отрицательной кривизны без особенностей не существует*[3]. В частности, мы должны ответить отрицательно на поставленный в начале работы вопрос, можно ли по методу Бельтрами представить всю плоскость Лобачевского регулярной аналитической[4] поверхностью в евклидовом пространстве.

---

[3] (Примечание к изданию 1903 г.) Между тем Э. Хольмгрен в заметке *Holmgren E.* Sur les espaces a courbure constante négative. — C. R., Paris, 1902, вскрыл очень простое и тоже опирающееся на формулу (3), но более аналитическое доказательство.

[4] Ср. с замечанием об аналитичности в примечании в начале работы [3].

ГЕЛЬМУТ ХАССЕ

ИСТОРИЯ ТЕОРИИ ПОЛЕЙ КЛАССОВ*)[1)]

1. Понятие *поля классов* обычно связывается с именем Гильберта. На самом деле это понятие неявно присутствовало уже у Кронекера, а сам термин был введен Вебером до появления фундаментальной работы Гильберта.

Кронекер [23] в своем большом трактате «*Основания арифметической теории алгебраических чисел*» (1882) подробно обсуждает «zu assoziierenden Gattungen» («роды ассоциаций»). Под этим он подразумевает, если пользоваться современной терминологией, алгебраическое расширение K заданного поля алгебраических чисел k, такое, что все дивизоры[2)] из k становятся главными дивизорами в K. В этих исследованиях он обнаружил, что если k — мнимое квадратичное поле, то такое расширение K порождается «сингулярными модулями». Этим понятием Кронекер предвосхитил теорему о главных дивизорах теории полей классов, установленную и в частных случаях доказанную Гильбертом.

Вебер в работах [6] и [7] (1891, 1897, 1898, 1908), однако, определил понятие поля классов не на этой основе, которая, как мы знаем сегодня, не удобна для построения теории. То, что он постулировал, составляет часть *закона разложения*. Но в то время как Гильберт в своих более поздних определениях рассматривал только случай абсолютного поля классов, Вебер дал определение в полной общности:

Пусть k — поле алгебраических чисел и A/H — относительная группа классов дивизоров в k. Алгебраическое расширение K поля k называется полем классов для группы A/H, если в поле K вполне распадаются те и только те простые дивизоры из k первой степени, которые принадлежат главному классу H.

Чтобы определить веберовское понятие относительной группы классов дивизоров A/H поля k, рассмотрим целые модули дивизоров m поля k, т. е. формальные конечные произведения, составленные из конечного числа точек (простых дивизоров) поля k с целыми положительными показателями и вещественных бесконечных простых точек поля k с показателями единица. Назовем число (дивизор) поля k взаимно простым с модулем m, если оно (он) взаимно просто с каждым из простых дивизоров, входящих в m, и будем понимать сравнимость по модулю m как сравнимость по модулю

---

*) *Hasse H.* History of calss fields theory. — In: Algebraic number theory (eds. J. W. S. Cassels, A. Frölich). — London–New-york: Academic Press, 1967. Воспроизводится по книге «Алгебраическая теория чисел», М.: Мир, 1969. Перевод *М. Е. Новодворского*.

1) Подготовлено для печати Лю на основе рукописи автора.

2) Я всюду использую термин «дивизор» вместо классического термина «идеал», потому что теория нормирований, развившаяся из понятия дивизора Кронекера — Гензеля, сейчас широко распространена как более подходящий фундамент алгебраической теории чисел, чем теория идеалов Дедекинда.

степеней простых дивизоров, входящих в m, и равенство знака для всех вещественных простых точек, входящих в m. Рассмотрим далее факторгруппу A_m/H_m, где A_m — группа всех дивизоров поля k, взаимно простых с модулем m (для заданного целого модуля дивизоров m), и H_m — ее подгруппа, состоящая из всех чисел a, сравнимых с единицей по модулю m в поле k (рассматриваемых как главные дивизоры поля k). Назовем две факторгруппы A_{m_1}/H_{m_1} и A_{m_2}/H_{m_2} «равными» между собой, если для наименьшего общего кратного $m=[m_1,m_2]$ (и, значит, для любого общего кратного) модулей m_1 и m_2 имеет место равенство $H_{m_1}\cap A_m = H_{m_2}\cap A_m$, которое влечет за собой изоморфизм $A_{m_1}/H_{m_1}\cong A_{m_2}/H_{m_2}$. Любое множество факторгрупп $A_{m_1}/H_{m_1}, A_{m_2}/H_{m_2},\ldots$, которые «равны» между собой, определяет относительную группу классов дивизоров A/H в смысле Вебера. Индивидуальные факторгруппы $A_{m_1}/H_{m_1}, A_{m_2}/H_{m_2},\ldots$ называются *интерпретациями* (Erklärungen) по $\bmod m_1, \bmod m_2,\ldots$ группы A/H. Наименьший возможный *интерпретационный модуль* f (Erklärungsmodul), который оказывается наибольшим общим делителем всех возможных модулей $m_1, m_2,\ldots$, называется ведущим модулем (Führer) группы A/H. Иногда индивидуальные *интерпретации* также называют относительными группами классов дивизоров.

Кроме доказательства ряда теорем о полях классов, которые мы вскоре приведем, Вебер в рассматривавшихся им случаях установил основную *теорему изоморфизма*:

Группа Галуа $\mathfrak{G}\ (K/k)$ *изоморфна группе классов* A/H *и, значит, обязательно абелева.*

Уже Кронекер [21] (1853), [22] (1877) знал, что поля деления круга являются полями классов в указанном выше смысле. Он сформулировал знаменитую *теорему полноты:*

Всякое абелево расширение поля рациональных чисел является полем деления круга и, следовательно, полем классов.

Эта теорема была впервые полностью доказана Вебером [4] (1886, 1887) и позже, более просто, Гильбертом [12] (1896), [13] (1897); дальнейшие доказательства были даны Вебером [8] (1909), Шпейзером [53] (1919) и Делоне [20] (1923)[3)].

В дальнейшем Кронекер [24] (1883 — 1890) в своих исследованиях по модулярным и эллиптическим функциям с «сингулярными модулями» установил, что их преобразования и уравнения деления порождают относительно абелевы расширения K над мнимыми квадратичными полями k. Его «заветной мечтой юности» («liebster Jugendtraum») [25] (1880) было доказать также и в этом случае *теорему полноты*, а именно *любое абелево расширение* K *мнимого квадратичного поля* k получается из таких преобразований и уравнений деления. Она была доказана позже впервые в частном случае Вебером [7] (1908) и Фютером [38] (1914), затем полностью Такаги [28] (1920) и вновь Фютером (совместно с Гутом) [39] (1927).

Вебер [6] (1897, 1898) пришел к понятию поля классов из рассмотрения этих примеров. Используя аналитические методы Дирихле (L-ряды), он вы-

---

[3)] См. также: *Шафаревич И. Р.* Новое доказательство теоремы Кронекера — Вебера. — Тр. Матем. ин-та им. В. А. Стеклова, 1951, т. 38, с. 382–387. — *Прим. ред.*

вел из своего определения поля классов *первое*[4] *основное неравенство* теории полей классов:

$$[A : H] = h \leqslant n = [K : k],$$

а затем *теорему единственности*:

$$H = H' \Leftrightarrow K = K',$$

теорему вложения:

$$H \supseteq H' \Leftrightarrow K \subseteq K'$$

и следующую предпосылку к теореме изоморфизма:

K нормально над полем k.

Из введения к работе [6] (1897, 1898) Вебера можно с уверенностью заключить, что он был уверен в справедливости общей теоремы существования:

Всякой относительной группе классов дивизоров A/H поля k соответствует поле классов K над k.

Вебер заметил, что из существования поля классов K над k следует существование бесконечного множества простых дивизоров в единичном классе группы A/H; это представляет собой далеко идущее обобщение знаменитой теоремы Дирихле о простых числах в данном взаимно простом с модулем классе вычетов. Ему, однако, не было известно иных примеров существования полей классов, чем те, которые возникли в теории полей деления круга и в теории модулярных и эллиптических функций.

2. Подчеркивание роли Вебера в возникновении теории полей классов отнюдь не означает умаления огромных заслуг Гильберта в развитии этой теории, но лишь способствует их правильному освещению. Гильберт сам высоко ценил Вебера; он часто цитировал его и отмечал значение его идей и результатов, относящихся к полям классов.

Публикации Гильберта [14]–[17] (1898, 1899, 1900, 1902) по теории полей классов ограничивались только частным случаем абсолютного поля классов, т. е. случаем, когда главный класс H содержит все главные дивизоры (с условием на знак или без него). Более того, он проводил доказательства только для *относительно квадратичных* числовых полей, т. е. для $n = 2$, с числом классов $h = 2$. Перед его мысленным взором, однако, стоял более общий случай. В частности, в лекциях [15] (1899) перед собранием DMV (Немецкой математической Ассоциации), проходивших в Брауншвейге в 1897 г., он произнес (в вольном переводе) следующие слова: «В этой лекции мы ограничим наше рассмотрение относительно абелевыми полями второй степени. Однако это ограничение только временное, и так как все выводы в доказательствах теорем можно обобщить, то следует надеяться, что трудности создания теории относительно абелевых полей не будут непреодолимыми». Гильберт имел в виду при этом уже упоминавшиеся основные теоремы теории полей классов в их полной общности (*теорема существования*, *теорема единственности*, *теорема вложения*, *теорема изоморфизма* и *закон взаимности*).

---

[4] В современной терминологии — второе.

Для Гильберта теория полей классов не была, как для Кронекера и Вебера, только средством доказательства теоремы полноты или обобщения теоремы Дирихле о простых числах. Как ясно видно из отрывков, подобных цитированному выше, и из заголовка к его статьям [14] (1898, 1902) в Göttinger Nachrichten, он всегда рассматривал ее как «теорию относительно абелевых полей». Дальней целью его было нахождение *высшего закона взаимности* — задача, навеянная идеями Гаусса, Якоби, Эйзенштейна и Куммера и сформулированная в его знаменитой парижской лекции в 1900 г. как 9-я проблема. Действительно, одним из самых глубоких достижений Гильберта является установление закона взаимности в виде формулы произведения для его символа норменного вычета:

$$\prod_{\mathfrak{p}} \left(\frac{a,b}{\mathfrak{p}}\right)_n = 1.$$

Здесь предполагается, что поле k содержит корни n-й степени из единицы, а $\mathfrak{p}$ пробегает все простые дивизоры поля k, включая те, которые мы теперь называем бесконечными простыми точками и которые Гильберт ввел как символы $1, 1', 1'', \ldots$ Он подметил аналогию этой формулы (выведенной им только в специальных случаях) с теоремой о вычетах алгебраических функций — простые точки $\mathfrak{p}$ с символом норменного вычета $\neq 1$ соответствуют точкам ветвления на римановой поверхности[5]. Эта аналогия была позднее блестяще подтверждена объединением указанной формулы с формулой произведения для полей алгебраических функций с конечным полем констант в теореме о вычетах Шмидта [51] (1936) и Витта [10] (1937). Далее, Гильберт установил (опять только в частном случае) *теорему о нормах*:

Равенство $\left(\dfrac{a,b}{\mathfrak{p}}\right)_n = 1$ *имеет место для всех* $\mathfrak{p}$ *тогда и только тогда, когда* a *— относительная норма элемента из поля* $k(\sqrt[n]{b})$, столь важную для дальнейшего развития теории. Эта теорема была доказана позже в полной общности мною [42] (1930).

При уже указанном ограничении — для случая абсолютной группы классов дивизоров — гильбертовский список теорем о полях классов содержит, помимо уже упомянутых, теорему о дискриминанте:

Поле K *имеет относительный дискриминант*

$$\mathfrak{d} = 1 \text{ над полем } k.$$

Далее, он установил *теорему о главных дивизорах*, о которой уже говорилось ранее в этой главе:

Все дивизоры поля k *становятся главными дивизорами в* K.

Более того, он утверждал, что

число классов поля K *не делится на* 2,

---

[5] С сегодняшней точки зрения это не вполне точно. В числовом случае символ норменного вычета может быть отличен от единицы и без ветвления, а именно за счет инерции. В полях алгебраических функций над полем комплексных чисел это не так, там играет роль только ветвление.

причем это верно не только при его исходном ограничении, состоящем в том, что число классов h поля k равно 2, но и при $h = 4$.

За исключением этого последнего утверждения, которое оказалось верным лишь при $h = 2$, но не обязательно при $h = 4$, все утверждения Гильберта о полях классов были доказаны в общем случае. Однако что касается теоремы о главных дивизорах, то здесь положение оказалось гораздо более сложным, чем, по-видимому, думал Гильберт. Нельзя не испытывать величайшего восхищения перед остротой его мысли и проницательностью, которые позволили ему предугадать столь тонкий общий закон на основании довольно специальных случаев.

3. Что касается *закона взаимности*, то в 1899 г. Гёттингенское королевское научное общество, вероятно по предложению Гильберта, назначило премию за детальное рассмотрение к 1901 г. этого закона для случая простого показателя $l \neq 2$. Эта задача была решена Фуртвенглером. В трактате, удостоенном премии [33] (1902, 1904), он дал решение только для полей k, число классов которых не делится на l, причем он не делал различия между $l - 1$ разными классами невычетов. В позднейших работах [35, 36] (1909, 1912, 1913, 1928), однако, Фуртвенглер доказал закон взаимности для простого показателя l (включая $l = 2$) в полной общности. Он не только доказал его в классическом виде:

$$\left(\frac{a}{b}\right)_l = \left(\frac{b}{a}\right)_l, \quad \textit{если } a \textit{ и } b \textit{ примарны}$$

$$(\textit{и в случае } l = 2 \textit{ всюду положительны}),$$

но также и в виде гильбертовой формулы произведения для символа норменного вычета. Согласно его замечательной идее, закон в его классической форме — через переход к расширению $\overline{k} = k(\sqrt[l]{ab^{-1}})$, над которым поле $\overline{k}(\sqrt[l]{a}) = \overline{k}(\sqrt[l]{b})$ неразветвлено и потому содержится в абсолютном поле классов $\overline{K}$, — превращается в *закон разложения* в расширении $\overline{K}/\overline{k}$. Иными словами, $\left(\frac{a}{\mathfrak{p}}\right)_l = \left(\frac{b}{\mathfrak{p}}\right)_l$ над полем $\overline{k}$ зависит только от абсолютного класса в $\overline{k}$, к которому принадлежит дивизор $\mathfrak{p}$. Этот закон разложения уже был в его распоряжении, поскольку он ранее доказал теорему существования абсолютного поля классов [34] (1907).

4. Решающий шаг вперед был сделан Такаги [28], [29] (1920, 1922) в двух весьма важных работах по теории полей классов и закону взаимности. Такаги в начале века изучал работы Гильберта по теории чисел и исследовал относительно абелевы поля над полем гауссовых чисел. Результатом этого явилось решение им для этого поля [27] (1903) знаменитой проблемы полноты Кронекера средствами теории деления эллиптических функций в случае лемнискаты (т. е. когда параллелограмм периодов — квадрат).

В 1920 г. Такаги большой работой о полях классов ознаменовал новый решающий поворот в теории полей классов, введя новое определение понятия «поле классов». Это определение было более удачным, чем веберовское, потому что оно позволяло рассматривать важный вопрос о теореме полноты с самого начала.

Для произвольного расширения K поля k им было установлено соответствие между целыми модулями дивизоров m поля k и относительными группами классов дивизоров, *интерпретирующими* $\bmod m$; именно модулю m соответствует наименьшая факторгруппа A_m/H_m, главный класс H_m которой содержит все нормы $N(\mathfrak{U})$ над k дивизоров $\mathfrak{U}$ из поля K, взаимно простых с модулем m, и, значит, содержит все дивизоры $\mathfrak{a}$ поля k, взаимно простые с модулем m, для которых

$$\mathfrak{a} \sim N(\mathfrak{U}) \pmod m, \quad \text{т. е.} \quad \frac{\mathfrak{a}}{N(\mathfrak{U})} \cong a \equiv 1 \pmod m \qquad (a \in k).$$

Если модуль m достаточно высок, более точно, для всех m, кратных наименьшему $\mathfrak{f}$ (где $\mathfrak{f}$ — ведущий модуль расширения K поля k), то группы классов A_m/H_m становятся «равными» и, значит, образуют относительную группу классов дивизоров A/H в смысле Вебера с ведущим модулем $\mathfrak{f}$. Как и у Вебера, здесь выполняется уже упоминавшееся первое основное неравенство

$$[A : H] = h \leqslant n = [K : k],$$

доказанное аналитическими средствами. Теперь определение Такаги поля классов выглядит так:

Расширение K поля k называется полем классов, соответствующим относительной группе классов дивизоров A/H, если выполняется равенство $h = n$.

Основная теорема теории полей классов, доказанная Такаги и базирующаяся на этом определении, может быть сформулирована следующим образом:

Понятие поля классов устанавливает взаимно однозначное соответствие между всеми абелевыми расширениями поля k и всеми относительными группами классов дивизоров этого поля.

Это утверждение охватывает теорему существования, теорему единственности, теорему полноты в старой терминологии, а также *теорему ограничения*:

если расширение K поля k неабелево, то $h < n$,

которая была добавлена позже.

«Партнерами» описанного взаимно однозначного соответствия выступают далее следующие утверждения.

$$K \subseteq K' \Leftrightarrow H \supseteq H' \ (\textit{теорема вложения});$$

$$\mathfrak{G}(K/k) \simeq A/H \ (\textit{теорема изоморфизма});$$

дивизор $\mathfrak{p}$ вполне распадается в поле K на простые дивизоры относительной степени f с индексами ветвления e тогда и только тогда, когда $\mathfrak{p}^f$ является наименьшей степенью дивизора $\mathfrak{p}$, лежащей в $H_\mathfrak{p}$, где $A/H_\mathfrak{p}$ — максимальная факторгруппа группы A/H с ведущим модулем, взаимно простым с $\mathfrak{p}$, и $e = [H_\mathfrak{p} : H]$ (закон разложения).

Значит,

$$\mathfrak{p}/\mathfrak{d} \textit{ тогда и только тогда, когда } \mathfrak{p}|\mathfrak{f}$$

— утверждение, которое впоследствии было уточнено и дополнено мною [40], [43] (1926, 1927, 1930) и приняло следующий вид:

$$\delta = \prod_{\chi} \mathfrak{f}_\chi, \quad \mathfrak{f} = \mathop{\mathbf{M}}_{\chi} \mathfrak{f}_\chi$$

(*теорема о дискриминанте и ведущем модуле*), где χ пробегает все характеры группы A/H, через $\mathfrak{f}_\chi$ обозначены их ведущие модули, а через $\mathop{\mathbf{M}}_{\chi}$ — наименьшее общее кратное всех характеров χ.

В то время как теорема существования получается из теоремы единственности и теоремы полноты несложными преобразованиями, доказательство теоремы полноты нуждается во втором[6] основном неравенстве

$$h \geqslant n.$$

Оно является далеко идущим обобщением классической теории родов из «*Арифметических исследований*» Гаусса. В настоящее время теория когомологий позволяет систематизировать довольно сложную цепь заключений, ведущих к установлению этого неравенства.

5. Возвращаясь к закону взаимности, отметим, что упоминавшаяся выше работа Такаги (1922) уже дала довольно сильные упрощения сравнительно сложных рассуждений Фуртвенглера (всего лишь 40 страниц вместо 80!). Эти упрощения стали возможными благодаря использованию полной теории полей классов вместо теории только абсолютных полей классов. Однако, лишь Артину принадлежит совершенно новая идея фундаментальной важности, которая полностью вскрыла суть этого закона. Речь идет о том, что Артин понял значение явного выражения для *канонического изоморфизма группы классов A/H на группу Галуа $\mathfrak{G}(K/k)$*.

Артин [2] (1927) показал, что такой изоморфизм получается установлением соответствия между простыми дивизорами $\mathfrak{p} \nmid \mathfrak{d}$, или вернее их классами в A/H, и так называемыми автоморфизмами Фробениуса $F_\mathfrak{p}$ расширения K/k по отношению к дивизору $\mathfrak{p}$. Всякий такой автоморфизм определяется условием

$$a^{F_\mathfrak{p}} \equiv a^{\mathfrak{N}(\mathfrak{p})} \pmod{\mathfrak{p}} \qquad \text{для всех целых} \quad a \in K,$$

где $\mathfrak{N}(\mathfrak{p})$ — абсолютная норма дивизора $\mathfrak{p}$. Сейчас пишут

$$F_\mathfrak{p} = \left(\frac{K/k}{\mathfrak{p}}\right)$$

и отсюда определяют символ Артина $\dfrac{K/k}{\mathfrak{a}}$ как мультипликативную функцию на группе $A_\mathfrak{f}$ всех дивизоров $\mathfrak{a}$ поля k, взаимно простых с $\mathfrak{d}$ или, что то же самое, с ведущим модулем $\mathfrak{f}$. Изоморфизм между группами A/H и $\mathfrak{G}(K/k)$ можно выразить тогда *законом взаимности Артина*:

$$\left(\frac{K/k}{\mathfrak{A}}\right) = 1 \text{ } \textit{тогда и только тогда, когда} \text{ } a \in H_\mathfrak{f}.$$

Артин [1] (1924) получил этот закон взаимности четырьмя годами раньше и доказал его в несложных частных случаях. Однако, лишь когда Артин

[6] В современной терминологии — первое неравенство.

ознакомился с методом Чеботарева пересечения классов из группы A/H с относительными классами, соответствующими круговым расширениям, он достиг успеха в своих поисках общего доказательства. Чеботарев [47] (1926) разработал свой метод в целях усиления одной теоремы Фробениуса [32] (1896), а именно:

Простые дивизоры $\mathfrak{P}$ нормального расширения K поля k с автоморфизмом Фробениуса $F_{\mathfrak{P}}$ из заданного отдела (Abteilung) $S^{-1}F_{\mathfrak{P}}^{\nu}S$ (где ν взаимно просто с порядком автоморфизма $F_{\mathfrak{P}}$, а S пробегает всю группу $\mathfrak{G}(K/k)$) встречаются с плотностью, равной относительной частоте элементов из этого отдела во всей группе $\mathfrak{G}(K/k)$. Указанный метод позволил Чеботареву обобщить эту теорему на индивидуальный сопряженный класс $S^{-1}F_{\mathfrak{P}}^{\nu}S$.

Для расширения Куммера $K = k(\sqrt[n]{b})$ (где k содержит корни n-й степени из единицы) автоморфизм Фробениуса $\left(\frac{K/k}{\mathfrak{p}}\right)$ переводит элемент $\sqrt[n]{b}$ в $\left(\frac{b}{\mathfrak{p}}\right)_n \sqrt[n]{b}$, что очевидно из определения символа норменного вычета $\left(\frac{b}{\mathfrak{p}}\right)_n$ с помощью критерия Эйлера. Поэтому закон взаимности Артина дает нам следующее утверждение:

Значение символа $\left(\frac{b}{\mathfrak{p}}\right)_n$ зависит только от класса, к которому принадлежит идеал $\mathfrak{p}$ в группе относительных классов по $\bmod \mathfrak{f}_b$, *соответствующей полю $k(\sqrt[n]{b})$.*

Здесь $\mathfrak{f}_b$ обозначает ведущий модуль поля $k(\sqrt[n]{b})$.

С другой стороны, из определения символа $\left(\frac{b}{\mathfrak{p}}\right)_n$ ясно, что он зависит только от класса вычетов по $\bmod \mathfrak{p}$, к которому принадлежит b. Отсюда легко получить взаимность в ее классической форме, а также в форме гильбертовской формулы произведения. Таким образом, становится понятно, почему Артин назвал описанный выше изоморфизм «общим законом взаимности».

С помощью своего закона Артин [3] (1930) смог также свести теорему о главных дивизорах, предсказанную Гильбертом, но еще не доказанную Такаги, к чисто теоретико-групповому предложению, которое затем было доказано Фуртвенглером [37] (1930). В дальнейшем доказательства этого предложения были даны Магнусом [26] (1934), Янага [57] (1934), Виттом [9, 11] (1936, 1954) и Шуманом и Францем [54] (1938), в то время как Таусски и Шольц [31] (1932, 1934) исследовали более внимательно процесс превращения дивизоров из подполей в главные дивизоры в абсолютном поле классов. Окончательных результатов в этой последней задаче не получено, однако, по сей день.

6. Аналогично переходу от степенного символа вычета $\left(\frac{b}{\mathfrak{a}}\right)_n$ к более общему символу Артина $\left(\frac{K/k}{\mathfrak{A}}\right)$ я перешел от символа норменного вычета $\left(\frac{a,b}{\mathfrak{p}}\right)_n$ Гильберта (где поле k содержит корни n-й степени из единицы)

к символу $\left(\frac{a, K/k}{\mathfrak{p}}\right)$ над произвольным полем k (которое необязательно содержит корни n-й степени из единицы) [40], [41], (1926, 1927, 1930). Первоначально вместо всех простых точек $\mathfrak{p}$ поля k мое определение, следуя обходному пути Гильберта, вынуждено было использовать лишь простые дивизоры $\mathfrak{p}/n$. Как следствие этого, связь символа с норменным вычетом становилась видимой только в силу закона взаимности Артина. Вскоре, однако, мне удалось дать [46] (1933) новое определение, из которого эта связь стала ясной непосредственно. Мое новое определение основывалось на теории алгебр.

Предварительно я показал [45] (1931), что любая центральная простая алгебра степени n над локальным полем $k_\mathfrak{p}$ с простым элементом π допускает неразветвленное (и, значит, циклическое) поле разложения $Z_\mathfrak{p}$. Следовательно, такая алгебра имеет канонические образующие

$$u_\mathfrak{p}^n = \pi^{\nu\mathfrak{p}}, \quad u_\mathfrak{p}^{-1} Z_\mathfrak{p} u_\mathfrak{p} = Z_\mathfrak{p}^{F_\mathfrak{p}}$$

(где $F_\mathfrak{p}$ — автоморфизм Фробениуса). Таким образом, класс вычетов $\nu_\mathfrak{p}/n \pmod{+1}$ инвариантно связан с алгеброй. Для глобальных циклических расширений K поля k я положил

$$\left(\frac{a, K/k}{\mathfrak{p}}\right) = S^{-\nu\mathfrak{p}},$$

если циклическая алгебра над полем k, порожденная элементами

$$u^n = a, \quad u^{-1} K u = K^S,$$

после расширения до пополнения $k_\mathfrak{p}$ имеет инвариант $\nu_\mathfrak{p}/n \pmod{+1}$. В частности, для расширения Куммера $K = k(\sqrt[n]{b})$ (где поле k содержит корни n-й степени из единицы) автоморфизм $\left(\frac{a, K/k}{\mathfrak{p}}\right)$ переводит элемент $\sqrt[n]{b}$ в $\left(\frac{a, b}{\mathfrak{p}}\right)_n \sqrt[n]{b}$.

Из этого определения немедленно извлекается *локальное* свойство:

$$\left(\frac{a, K/k}{\mathfrak{p}}\right) = 1 \textit{ тогда и только тогда, когда } a \textit{ есть норма из } K^\mathfrak{p}/k_\mathfrak{p},$$

где $K^\mathfrak{p}$ обозначает тип (с точностью до изоморфизма) пополнения $K_\mathfrak{P}$ по простому дивизору $\mathfrak{P}/\mathfrak{p}$. Поэтому символ $\left(\frac{a, K/k}{\mathfrak{p}}\right)$ можно называть просто *норменным символом*. В *глобальном* случае мне удалось доказать [40, 41] (1926, 1927, 1930) *теорему о нормах*:

Равенство $\left(\frac{a, K/k}{\mathfrak{p}}\right) = 1$ *имеет место для всех дивизоров* $\mathfrak{p}$ *тогда и только тогда, когда* a *— норма элемента из расширения* K *поля* k.

Эта теорема была предвосхищена Гильбертом для своего символа, как уже упоминалось ранее. Таким образом, формула произведения Гильберта для его символа превратилась в формулу произведения для норменного

символа:

$$\prod_{\mathfrak{p}}\left(\frac{a, K/k}{\mathfrak{p}}\right) = 1.$$

Она эквивалентна моей *теореме о сумме для центральных простых алгебр* [46] (1933):

$$\sum_{\mathfrak{p}} \frac{\nu_{\mathfrak{p}}}{n} \equiv 0 \qquad (\mathrm{mod}^{+}1).$$

В то время как определение норменного символа обобщалось с циклических до произвольных абелевых расширений K/k с помощью формальных построений, я показал [44] (1931), что теорема о нормах становится в такой общности неверной.

В связи с локальным свойством норменного символа мне удалось установить [42] (1930) *основную теорему теории полей классов над локальными полями* $k_{\mathfrak{p}}$. Здесь существует взаимно однозначное соответствие между абелевыми расширениями $K^{\mathfrak{p}}$ поля $k_{\mathfrak{p}}$ и относительными группами классов чисел $A_{\mathfrak{p}}/H_{\mathfrak{p}}$ поля $k_{\mathfrak{p}}$, такое, что $\left(\frac{a, K^{\mathfrak{p}}/k_{\mathfrak{p}}}{\mathfrak{p}}\right)$ дает канонический изоморфизм группы $A_{\mathfrak{p}}/H_{\mathfrak{p}}$ на $\mathfrak{G}(K^{\mathfrak{p}}/k_{\mathfrak{p}})$. Связь с теорией полей классов над глобальным полем k устанавливается следующими предложениями:

1) расширение $K^{\mathfrak{p}}$ поля $k_{\mathfrak{p}}$ представляет тип (с точностью до изоморфизма) пополнения по дивизору $\mathfrak{P}/\mathfrak{p}$ расширения K поля k;

2) группа $\mathfrak{G}(K^{\mathfrak{p}}/k_{\mathfrak{p}})$ является группой разложения дивизора $\mathfrak{P}/\mathfrak{p}$ в поле K над k.

Впоследствии Шмид [52] (1930) и Шевалле [48] (1933) дали систематическое развитие локальной теории полей классов без ссылки, как сделал я, на эту связь с глобальной теорией полей классов. Здесь я должен также упомянуть особую роль работ Эрбрана [55], [56], (1931, 1932) о теоретико-групповом механизме некоторых доказательств в локальной, равно как и в глобальной теории полей классов и в теории высшего ветвления нормальных расширений.

7. В теории полей классов, развитой Такаги, характеризация абелевых расширений K поля k посредством групп классов дивизоров поля k обладает неприятным дефектом. Этот дефект проистекает от аппроксимации группы A/H группами A_m/H_m — некоего предельного процесса по возрастающим модулям дивизоров m. После того как $\mathfrak{p}$-адические понятия и методы описанным выше образом раскрыли сущность теории полей классов, Шевалле [49] (1933) пришел к счастливой идее заменить конструкцию Вебера — Такаги в терминах относительных групп классов дивизоров A/H более изящной $\mathfrak{p}$-адической конструкцией. Ему удалось добиться успеха путем введения *идеальных элементов* или сокращенно *иделей*, а именно векторов

$$\mathbf{a} = (\ldots, a_{\mathfrak{p}}, \ldots)$$

с компонентами $a_{\mathfrak{p}}$ из отдельных пополнений $k_{\mathfrak{p}}$, удовлетворяющих некоторым условиям конечности, а именно

$$a_{\mathfrak{p}} \cong 1 \quad \text{для почти всех } \mathfrak{p}.$$

Шевалле заменил относительные группы классов дивизоров Вебера — Такаги A/H факторгруппами $\mathbf{A}/\mathbf{H}$ *абсолютной группы классов иделей* $\mathbf{A}/k^*$, где k^* обозначает группу главных иделей $(\ldots, a, \ldots)$, соответствующих числам $a \neq 0$ из поля k. Он доказал, что символ

$$\left(\frac{K/k}{\mathbf{a}}\right) = \prod_{\mathfrak{p}} \left(\frac{a_{\mathfrak{p}}, K^{\mathfrak{p}}/k_{\mathfrak{p}}}{\mathfrak{p}}\right),$$

названный впоследствии *символом Шевалле*, осуществляет изоморфизм между группой классов иделей $\mathbf{A}/\mathbf{H}$ и группой Галуа $\mathfrak{J}(K/k)$. Здесь главный класс $\mathbf{H}$ состоит из всех тех абсолютных классов иделей из поля k, которые содержат нормы иделей из поля K. В теории полей классов Шевалле эти группы классов иделей играют роль относительных групп классов дивизоров A/H Такаги. Множеству всех абелевых расширений K поля k соответствует, таким образом, множество всех групп классов иделей $\mathbf{A}/\mathbf{H}$, где главный класс $\mathbf{H}$ открыт в подходящей топологии группы $\mathbf{A}$, а именно в той, для которой полную систему окрестностей единицы составляют идели единиц, сравнимых с единицей по модулю m для всевозможных модулей дивизоров m.

Таким образом, можно сказать, что идеи (но не идели) Шевалле позволили укорениться в теории полей классов *локально-глобальному принципу*.

При всей красоте построения теории полей классов Такаги в нем был один изъян, устраненный Шевалле [50] (1940). Этот изъян состоял в обращении к аналитическим средствам (L-ряды Дирихле) для доказательства первого основного неравенства $h \leqslant n$. Шевалле нашел чисто арифметическое доказательство этого неравенства.

8. Можно было бы еще много рассказать о дальнейшем развитии теории, возникшей из теории полей классов, обрисованной до этого. В частности, остались не затронутыми особенно дорогая моему сердцу *явная формула взаимности* (определение норменного символа $\left(\frac{a, b}{\mathfrak{p}}\right)_n$ для простых дивизоров $\mathfrak{p}/n$), затем *допущение бесконечных алгебраических расширений* K поля k, теория полей классов над функциональными полями (поля алгебраических функций с конечным полем констант), L-ряды Артина и ведущие модули и т. д. Я должен, однако, воздержаться здесь от обсуждения всех этих предметов, поскольку оно заставило бы перешагнуть границы данной лекции.

Я также не могу касаться дальнейшего развития теории полей классов после войны, так как полагаю, что должен закончить мой очерк исторического развития на этом месте.

Если я правильно понял, моей задачей было нарисовать для математиков послевоенного поколения яркую и живую картину великого и прекрасного здания теории полей классов, воздвигнутого предвоенными поколениями. Как мне кажется, четкий контур и яркие детали этого замечательного здания теряют что-то от их блеска и гибкости при проникновении в теорию полей классов когомологических понятий и методов, которые стали столь могущественными после войны.

Я был бы рад думать, что преуспел в какой-то степени в выполнении своей задачи.

ЛИТЕРАТУРА

Артин (Artin E.)

[1] Über eine neue Art von L-Reihen — Abh. Math. Semin. Univ. Hamburg, 1924, Bd. 3, S. 89–108. (Collected Papers. — Addison Wesley, 1965, p. 105–124.)

[2] Beweis des allgemeinen Reziprozitätsgesetzes — Abh. Math. Semin. Univ. Hamburg, 1927, Bd. 5, S. 353–363. (Collected Papers. — Addison Wesley, 1965, p. 131–141.)

[3] Idealklassen in Oberkörpern und allgemeines Reziprozitätsgesetz — Abh. Math. Semin. Univ. Hamburg, 1930, Bd. 7, S. 46–51. (Collected Papers. — Addison Wesley, 1965, p. 159–164.)

Вебер (Weber H.)

[4] Theorie der Abel'schen Zahlkörper, I, II. — Acta Math. Stockh., 1886, Bd. 8, S. 193–263; 1887, Bd. 9, S. 105–130.

[5] Elliptische Funktionen und algebraische Zahlen. — Braunschweig, 1891.

[6] Über Zahlengruppen in algebraischen Körper 1, 2, 3. — Math. Ann., 1897, Bd. 48, S. 433–473; Bd. 49, S. 83–100; 1898, Bd. 50, S. 1–26.

[7] Lehrbuch der Algebra 3. — Braunschweig, 1908.

[8] Zur Theorie der zyklischen Zahlkörper. — Math. Ann., 1909, S. 32–60.

Витт (Witt E.)

[9] Bemerkungen zum Beweis des Hauptidealsatzes von S. Iyanada. — Abh. Math. Semin. Univ. Hamburg, 1936, Bd. 11, S. 221.

[10] Zyklische Körper und Algebren der Charakteristik p vom Grade p^n. — J. reine und angew. Math., 1937, Bd. 176, S. 126–140.

[11] Verlagerung von Cruppen und Hauptidealsatz. — Proc. Internat. Math. Congress II, Amsterdam, 1954, p. 71–73.

Гильберт (Hilbert D.)

[12] Neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper. — Nachr. Ges. Wiss. Göttingen, 1896, S. 29–39.

[13] Bericht: Die Theorie der algebraischen Zahlkörper. — Jber. der Deutschen Mathematiker-Vereinigung, 1897, Bd. 4, S. 175–546.

[14] Über die Theorie der relativ-Abel'schen Zahlkörper. — Nachr. Ges. Wiss. Göttingen, 1898, S. 377–399; Acta Math., 1902, Bd. 26, S. 99–132 [имеется перевод на с. 288–311 настоящего издания].

[15] Über die Theorie der relativguadratischen Zahlkörper. — Jber. der Deutschen Mathematiker-Vereinigung, 1899, Bd. 6, S. 88–94.

[16] Über die Theorie der relativguadratischen Zahlkörpers. — Math. Ann., 1899, Bd. 51, S. 1–127 [имеется перевод на с. 179–287 настоящего издания].

[17] Theorie der algebraischen Zahlkörper. — Enzykl. math. Wiss., 1900, Bd. I (2), S. 675–698.

[18] Theorie des Kreiskörpers. — Enzykl. math. Wiss., 1900, Bd. I (2), S. 699–732.

[19] Mathematische Probleme. — Nachr. Ges. Wiss. Göttingen, 1900, 253–297 [имеется перевод в т. 2 настоящего издания].

Делоне (Delaunay B.)

[20] Zur Bestimmung algebraiscsher Zahlkörper durch Kongruenzen; eine Anwendung auf die Abelschen Gleichungen. — J. reine und angew. Math., 1923, Bd. 152, S. 120–123.

Кронекер (Kronecker L.)

[21] Über die algebraisch auflösbaren Gleichungen I. — Sber. preuss. Acad. Wiss., 1853, S. 365–374; Werke, Bd. IV, S. 1–11.

[22] Über Abel'sche Gleichungen. — Sber. preuss. Acad. Wiss., 1877, S. 845–851; Werke, Bd. IV, S. 63–72.

[23] Grundzüge einer arithmetischen Theorie der algebraischen Grösseń. — J. reine und angew. Math., 1882, Bd. 92, S. 1–2 (см. там же § 19, S. 65–68; S. 321–324).

[24] Zur Theorie der elliptischen Funktionen I–XXII. — Sber. preuss. Acad. Wiss.; Werke, Bd. IV, S. 345–496; Bd. V, S. 1–132, 1883–1890.

[25] Auszug aus Brief an R. Dedekind vom 15 März 1880. — Werke, Bd. 5, S. 453–458. См. также мое подробное «Zusatz», ibid., 510–515.

Магнус (Magnus W.)

[26] Über den Beweis des Hauptidealsatzes. — J. reine und angew. Math., 1934, Bd. 170, S. 235–240.

Такаги (Takagi T.)

[27] Über die im Bereich der rationalen komplexen Zahlen Abel'schen Zahlkörper. — J. Coll. Sci. imp. Univ. Tokyo, 1903, vol. 19, № 5, p. 1–42.

[28] Über eine Theorie des relativ-Abel'schen Zahlkörpers. — J. Coll. Sci. imp. Univ. Tokyo, 1920, vol. 41, № 9, p. 1–133.

[29] Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper. — J. Coll. Sci. imp. Univ. Tokyo, 1922, vol. 44, № 5, p. 1–50.

Таусски (Taussky O.)

[30] Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper. — J. reine und angew. Math., 1932, Bd. 168, S. 193–210.

Таусски, Шольц (Taussky O., Scholz A.)

[31] Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einflub auf deh Klassenkörperturm. — J. reine und angew. Math., 1934, Bd. 171, S. 19–41.

Фробениус (Frobenius G.)

[32] Über die Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. — Sber. preuss. Acad. Wiss., 1896, S. 689–703.

Фуртвенглер (Furtwängler Ph.)

[33] Über die Reziprozitätsgesetze zwischen l^{ten} Potenzresten in algebraischen Zahlkörpern, wenn L eine ingerade Primzahl bedeutet. — Nach. Ges. Wiss. Göttingen, 1902, Bd. 2, 3, S. 1–82; Math. Ann., 1904, Bd. 58, S. 1–50.

[34] Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebraischen Zahlkörpers. — Math. Ann., 1907, Bd. 63, S. 1–37.

[35] Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlkörpern, I, II, III. — Math. Ann., 1909, Bd. 67, S. 1–31; 1912, Bd. 72, S. 346–386; 1913, Bd. 74, S. 413–429.

[36] Über die Reziprozitätsgesetze für ungerade Primzahlexponenten. — Math. Ann., 1928, Bd. 98, S. 539–543.

[37] Beweis des Hauptidealsatzes für Klassenkörper algebraischer Zahlkörper. — Abh. Math. Semin. Univ. Hamburg, 1930, Bd. 7, S. 14–36.

Фютер (Fueter R.)

[38] Abel'sche Gleichungen in quadratisch-imaginären Zahlkörpern. — Math. Ann., 1914, Bd. 75, S. 177–255.

[39] Vorlesungen über die singulären Moduln und die komplexe Multiplikation der elliptischen Funktionen (unter Mitwirkung von M. Gut). — Leipzig–Berlin, 1927.

Хасце (Hasse H.)

[40] Bericht über neuere Untersuchungen und Probleme aus der algebraischen Zahlkörper, I, Ia, II. — Jber. der Deutschen Mathematiker-Vereinigung, 1926, Bd. 35, S. 1–55; 1927, Bd. 36, S. 233–311; Exg. 1930, Bd. 6, S. 1–204.

[41] Neue Begründung und Verallgemeinerung der Theorie des Normenrestsymbols. — J. reine und angew. Math., 1930, Bd. 162, S. 134–144.

[42] Die Normenresttheorie relativ-Abelscher Zahlkörper als Klassenkörpertheorie im Kleinen. — J. reine und angew. Math., 1930, Bd. 162, S. 145–154.

[43] Führer, Diskriminante und Verzweigungskörper relativ-Abelscher Zahlkörper. — J. reine und angew. Math., 1930, Bd. 162, S. 169–184.

[44] Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol. — Nachr. Ges. Wiss. Göttingen, 1931, S. 64–69.

[45] Über p-adische Schiefkörper und ihre Bedeutung für die Arithmetik hyperkomplexer Zahlsysteme. — Math. Ann., 1931, S. 495–534.

[46] Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper. — Math. Ann., 1933, Bd. 107, S. 731–760.

Чеботарев Н.Г. (Tchebotarev N.)
[47] Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. — Math. Ann., 1926, Bd. 95, S. 191–228.

Шевалле (Chevalley C.)
[48] La théorie du symbole de restes normiques. — J. reine und angew. Math., 1933, Bd. 169, S. 140–157.
[49] Sur la théorie du corps de classes dans les corps finis et les corps locaux. — J. Fac. Sci. Tokyo Univ., 1933, vol. 2, p. 365–476.
[50] La théorie du corps de classes. — Math. Ann., Bd. 41, S. 394–417.

Шмид (Schmid H.L.)
[51] Ziklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p. — J. reine und angew. Math., 1936, Bd. 175, S. 108–123.

Шмидт (Schmidt F.K.)
[52] Zur Klassenkörpertheorie im Kleinen. — J. reine und angew. Math., 1930, Bd. 162, S. 155–168.

Шпейзер (Speiser A.)
[53] Die Zerlegungsgruppe. — J. reine und angew. Math., 1919, Bd. 149, S. 174–188.

Шуман (Schumann H.G.)
[54] Zum Beweis des Hauptidealsatzes (unter Mitwirkung von W. Franz). — Abh. Math. Semin. Univ. Hamburg, 1938, Bd. 12, S. 42–47.

Эрбран (Herbrand J.)
[55] Sur la théorie des groupes de décomposition, d'inertie et de ramification. — J. Math. pures appl., 1931, vol. 10, p. 481–498.
[56] Sur le théorèmes du genre principal et des idéaux principaux. — Abh. Math. Semin. Univ. Hamburg, 1932, Bd. 9, S. 84–92.

Янага (Iyanaga S.)
[57] Zum Beweis des Hauptidealsatzes. — Abh. Math. Semin. Univ. Hamburg, 1934, Bd. 10, S. 349–357.

КОММЕНТАРИИ И ПРИМЕЧАНИЯ

О КОНЕЧНОСТИ СИСТЕМЫ ИНВАРИАНТОВ ДЛЯ БИНАРНЫХ БАЗИСНЫХ ФОРМ

Вершиной первого периода развития теории инвариантов явилось доказательство Горданом теоремы о конечной порожденности алгебры инвариантов бинарной формы степени (у Гильберта «порядка») n (см. подробности в комментариях к работе «О теории алгебраических форм», перевод которой на русский язык также включен в настоящее издание, с. 16–66). Это доказательство существенно использует специфику инвариантов бинарных форм (тот факт, что бинарная форма разлагается в произведение линейных форм) и не распространяется на инварианты от большего числа переменных. Доказательство теоремы в полной общности, т. е. для алгебр инвариантов любой системы форм от любых наборов переменных, было дано Гильбертом позже в работе «О теории алгебраических форм».

[1] (с. 13). Короткое доказательство этого факта см. в работе: *Данилов В. И.* — УМН, 1978, т. XXXIII, вып. 2(200), с. 85–134.

В. Л. Попов

О ТЕОРИИ АЛГЕБРАИЧЕСКИХ ФОРМ

Математическая деятельность Гильберта, как известно, четко делится на периоды, каждый из которых посвящен проблемам из одной конкретной области. Первый из них (1885–1893) связан с исследованиями по теории инвариантов. Они начались диссертацией Гильберта (Über die invarianten Eigenschaften specieller binärer Formen, insbesondere der Kugelfunktionen. — Inauguraldissertation, Königsberg i. Pr., 1885), а по существу закончились двумя его фундаментальными работами — настоящей статьей и статьей 1893 г. (Über die vollen Invariantensysteme. — Math. Ann., 1893, Bd. 42, S. 313–373), перевод которой на русский язык также включен в настоящее издание (с. 67–114).

С появлением этих работ завершился первый из трех этапов развития теории инвариантов. Как пишет Г. Вейль, характеризуя значение этих работ, в них Гильберт «решил основные проблемы и тем самым почти убил весь предмет» (*Вейль Г.* Классические группы, их инварианты и представления. — М., 1947, с. 46). Однако именно настоящая работа сделала Гильберта «знаменитым в одну ночь» (*Dieudonne J. A., Carrell J. B.* Invariant Theory. Old and new. — Acad. Press, 1971; имеется перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974): «ex ungue leonen [по когтям узнают льва] — молодой Гильберт показал свои когти» (*Weyl H.* — Scr. math., 1935, vol. 3, p. 201–220). Истинное же значение работы 1893 г. стало ясно только через 70 лет.

Первая основная проблема теории инвариантов, которую Гильберт решил (положительно) в полной общности в настоящей работе, называлась в те времена проблемой Гордана. Ее суть, в современной терминологии, сводится к следующему. Рассмотрим естественное действие группы $G = SL_n(\mathbb{C})$ на пространстве V, являющемся прямой суммой пространств вида $S^{d_1}\mathbb{C}^n \oplus \ldots \oplus S^{d_k}\mathbb{C}^n$. Является ли тогда алгебра $\mathbb{C}[V]^G$ G-инвариантных многочленов на V (так называемая алгебра инвариантов системы базисных форм от нескольких наборов переменных) конечно

порожденной? Гильберт решил (положительно) в настоящей статье и вторую основную проблему: если $\mathbb{C}[V]^G$ имеет конечное число однородных образующих $f_1, \ldots, f_m$, то можно ли найти такой конечный набор $F_1, \ldots, F_s$ алгебраических соотношений между ними (т. е. таких многочленов F_i от m переменных, что $F_i(f_1, \ldots, f_m) = 0$), что через эти соотношения любое алгебраическое соотношение F между указанными образующими выражается в виде $F = G_1F_1 + \ldots + G_sF_s$, где G_i — многочлены от тех же m переменных?

До появления настоящей работы Гильберта положительное решение этих проблем было получено лишь в весьма специальных случаях. Высшим достижением теории инвариантов до Гильберта считалось данное самим Горданом положительное решение проблемы конечной порожденности для алгебр инвариантов систем бинарных форм, т. е. для $G = SL_2$ (*Gordan P.* Vorlesungen über Invariantentheorie, Bd. 2. — 1885, S. 231). Доказательство Гордана было весьма сложным и носило формальный, вычислительный характер. Такой стиль написания работ, да и самый образ мышления был характерен для специалистов по теории инвариантов того времени. Г. Вейль писал о Гордане, «короле теории инвариантов» (*Weyl H.*, loc. cit): «Его сильной стороной было придумывание формальных процессов и проведение для них вычислительной работы. У него были такие труды, в которых на протяжении двадцати страниц беспрерывно идут формулы, совершенно без текста; говорят, что в своих работах он вообще писал одни формулы, а текст добавляли его друзья. Нётер говорил о нем: „Формула всегда и везде была необходимой поддержкой для формирования его мыслей, его заключений и его способа выражения... В своих лекциях он тщательно избегал всяких фундаментальных определений концептуального характера — даже таких, как предел“». (В заметке в Math. Ann., 1889, Bd. 32, S. 223–226, перевод которой на русский язык также включен в это издание (с. 13–15), Гильберт значительно упростил доказательство Гордана.)

В настоящей работе Гильберт дает положительное решение обеих проблем в самой полной (по тому времени) общности — для алгебр инвариантов любой системы базисных форм от любых наборов переменных. Он полностью отходит от прежнего формалистического подхода, развивая вместо него новые концепции (что так отталкивало Гордана), и именно это приводит к успеху. Эти концепции явились глубоким развитием «точки зрения Дедекинда и ...намеченных Кронекером идей» (*Клейн Ф.* Лекции о развитии математики в 19 веке. — М. — Л.: ОНТИ, 1937, гл. VII). Реакция на появление этой работы не была однозначной. Одни (как, например, Линдеман) нашли методы этой работы «unheimlich» [неудобный, чудовищный]. Гордан отозвался о ней довольно неодобрительно, заявив: «Das ist nicht Mathematik. Das ist Theologie» [Это не математика. Это теология]. Другие, напротив, сразу безоговорочно ее признали: Клейна, например, эта работа побудила пригласить Гильберта в Гёттинген. Однако со временем это отношение изменилось в сторону общего признания. Так, Гордан заявил, что считает доказательство «абсолютно верным» и что он «убедился, что и теология имеет свои преимущества» (*Клейн Ф.*, loc. cit.); в 1899 г. он дал собственный упрощенный вариант доказательства теоремы Гильберта о конечной порожденности алгебры инвариантов (невозможный, по его словам, «если бы господин Гильберт не применил к теории инвариантов понятий, развитых Дедекиндом, Кронекером и Вебером в другой части математики» (*Рид К.* Гильберт. — М.: Наука, 1977)).

Основная причина такого первоначального отношения к этой работе состояла в неконструктивности доказательства Гильберта: оно не давало способа получить образующие $f_1, \ldots, f_m$ алгебры инвариантов $\mathbb{C}[V]^G$ явно. Это было абсолютно непривычно по тем временам, поскольку предшественники Гильберта понимали основные проблемы теории инвариантов исключительно в конструктивном духе (в частности, конструктивным было и положительное решение первой основной проблемы для бинарных форм, данное Горданом). Указанное обстоятельство имело непосредст-

венное отношение к начатой Кронекером полемике о природе математического существования. Кронекер настаивал, что без построения нет и существования. Гильберт же полагал, что необходимо считать истинным любое утверждение, всякое следствие из которого непротиворечиво.

В действительности в полной мере оценить основополагающее значение настоящей работы Гильберта стало возможным не сразу, а лишь по мере дальнейшего развития алгебры. Дело в том, что, отправляясь от конкретной проблематики теории инвариантов, Гильберт получил в этой работе результаты фундаментального общеалгебраического значения, посвятив собственно теории инвариантов лишь последний, пятый раздел работы. А именно, в разд. I и II Гильберт по существу доказывает теорему о нётеровости (если пользоваться современной терминологией) кольца многочленов над нётеровым кольцом (сейчас она известна как теорема Гильберта о базисе), в разд. III — теорему о конечности цепи сизигий конечно порожденного градуированного модуля над кольцом многочленов над полем (известную ныне как теорема Гильберта о сизигиях), в разд. IV — теорему о существовании многочлена Гильберта для такого модуля. В наше время фундаментальная роль этих результатов в коммутативной алгебре и гомологической алгебре (а также алгебраической геометрии) общеизвестна. Именно с настоящей работы Гильберта и начинается самостоятельное развитие этих двух новых алгебраических дисциплин. Теорема о нётеровости позволила Гильберту не только сразу положительно решить вторую основную проблему теории инвариантов, но и автоматически доказать конечность числа базисных линейных соотношений между самими соотношениями (так называемых сизигий второго рода), затем, аналогично, — базисных сизигий третьего рода и т. д. При этом теорема о сизигиях гарантирует обрыв указанной цепочки. Решение же первой основной проблемы теории инвариантов основывается у Гильберта на решении второй, и это, как впервые отметил Г. Вейль (*Weyl H.* — Bull. Amer. Math. Soc., 1944, vol. 50, p. 612–654; имеется перевод в т. 2 наст. издания), с большим основанием позволяет считать, что в действительности Гильберт сначала решил вторую проблему (т. е. доказал теорему о нётеровости).

Хотя настоящей работой Гильберт подвел черту в исследованиях того времени по теории инвариантов, в ней же он явно или неявно поставил вопросы, определившие развитие этой теории в дальнейшем. Один из них связан с выяснением границ применимости его метода доказательства теоремы о конечной порожденности алгебры инвариантов. Конкретно этот вопрос сводился к разысканию общих процессов, обладающих некоторыми стандартными свойствами и позволяющих получать инвариантный многочлен из произвольного. Этот вопрос был полностью прояснен Г. Вейлем, который ввел процесс усреднения по компактной группе и с его помощью перенес доказательство Гильберта на любые компактные и (с помощью «унитарного трюка») любые комплексные редуктивные группы Ли (см.: *Вейль Г.* Теория представлений непрерывных полупростых групп при помощи линейных преобразований. — В кн.: *Вейль Г.* Избранные труды. — М.: Наука, 1984). Другой вопрос касается общего теоретико-группового описания класса тех линейных групп, для которых алгебра инвариантов конечно порождена. Ныне он известен как оригинальная четырнадцатая проблема Гильберта. Полной ясности в этом вопросе нет до сих пор (см. подробности в примечании [46] ниже).

[1] (с. 16). Гильберт понимает под этим числовое поле.

[2] (с. 16). В действительности отсюда следует аналогичное утверждение и для неоднородных многочленов F_1, F_2, ... (разумеется, в нем уже A_1, A_2, ... не обязаны быть формами). Дело в том, что неоднородный случай сводится к однородному введением новой переменной x, т. е. заменой каждого многочлена F от $x_1, \ldots, x_n$ на форму $x^{\deg F} F(x_1/x, \ldots, x_n/x)$; обратный переход осуществляется подстановкой $x = 1$. Гильберт указывает на это в самом конце статьи (это место отмечено примечанием [48]).

[3] (с. 17). Уже в этом простейшем случае проявляется неконструктивность доказательства существования числа m. Действительно, поскольку «правило задания» последовательности F_1, $F_2, \ldots$ позволяет лишь для каждого d указать форму F_d, а в остальном о нем больше ничего не известно, то с помощью последовательного сравнения степеней соседних форм F_d и F_{d+1} невозможно, вообще говоря, конструктивно (т. е. за конечное число шагов) решить вопрос, существует ли для наперед заданной формы F_s форма F_t с $s < t$, но с $\deg F_s > \deg F_t$. Иначе говоря, для произвольного конструктивного «правила задания» последовательности $F_1, F_2, \ldots$ множество $\{d \in \mathbb{N} \mid$ существует форма F_r с $d < r$ и $\deg F_d > \deg F_r\}$, вообще говоря, неразрешимо (хотя и перечислимо).

[4] (с. 17). Отличного от константы.

[5] (с. 17). С коэффициентами, лежащими в основной «области рациональности». Это следует из конечномерности пространства форм степени, не превосходящей заданную.

[6] (с. 17). Если «область рациональности» k, из которой берутся коэффициенты, считать не числовым, а любым полем, то такой подстановки, вообще говоря, может и не найтись. Например, если k — поле из двух элементов, $n = 2$ и $F_1 = x_1^3 x_2 + x_2^3 x_1$, то любая линейная невырожденная подстановка $x_1 \mapsto ay_1 + by_2$, $x_2 \mapsto cy_1 + dy_2$ переводит F_1 в форму, не содержащую ни y_1^4, ни y_2^4. Если k бесконечно, то искомая подстановка действительно существует и может быть найдена конструктивно, например, так. Пусть какая-либо переменная, скажем x_1, действительно входит в F_1. Тогда можно найти такое $\alpha \in k$, что при специализации $x_1 = \alpha$, $x_2 = \ldots = x_n = 1$ значение формы F_1 будет отлично от нуля (поскольку $\deg F_1 = r$, такое α найдется среди любых $r + 1$ различных элементов поля k, так как многочлен $F_1(x_1, 1, 1, \ldots, 1)$ от x_1 не может иметь больше, чем r, различных корней). Осуществляя линейную невырожденную подстановку $x_1 = \alpha z_1$, $x_2 = z_2, \ldots, x_n = z_n$, получим форму $\widetilde{F}_1$ от переменных $z_1, \ldots, z_n$, такую, что $\widetilde{F}_1(1, 1, \ldots, 1) \neq 0$. Рассмотрим теперь любую линейную невырожденную подстановку $z_i = \alpha_{i1} y_1 + \ldots + \alpha_{in} y_n$, $(1 \leqslant i \leqslant n)$, в которой $\alpha_{11} = \alpha_{21} = \ldots = \alpha_{n1} = 1$ (такие, очевидно, существуют). Она переводит $\widetilde{F}_1$ в форму G_1 от переменных $y_1, \ldots, y_n$, в которую одночлен y_1^r входит с коэффициентом $\widetilde{F}_1(1, 1, \ldots, 1) \neq 0$.

[7] (с. 20). На самом деле это верно для любых многочленов, а не только для форм, см. примечание [2]. Данное выше доказательство этого утверждения является чистым доказательством существования. Если оформлять его без приведения к противоречию, то указанное конечное множество форм находится следующей процедурой: берем F_1, затем присоединяем к F_1 форму F_2 (если такая найдется), затем присоединяем к ним F_3 (если такая найдется) и т. д. Этот процесс должен оборваться через конечное число шагов. Однако конструктивного способа находить такие F_2, $F_3, \ldots$ и узнавать на очередном шаге, закончилась ли процедура построения всех F_i, не предъявляется.

[8] (с. 20). В современной терминологии — идеалом. Этот последний термин ввел Дедекинд в своем XI дополнении к четвертому изданию «Лекций по теории чисел» Лежёна Дирихле (1894 г.): он дает аксиоматическое определение идеала, по существу пригодное для любого коммутативного кольца, хотя и рассматривает его только применительно к кольцам целых поля алгебраических чисел. См. подробности в гл. 2 сборника: Математика XIX века. Математическая логика, алгебра, теория чисел, теория вероятностей. — М.: Наука, 1978.

[9] (с. 20). В современной терминологии это означает, что кольцо многочленов над полем является нётеровым кольцом. Данное Гильбертом доказательство проходит для любого бесконечного основного поля, см. примечание [6]. В следующем разделе этой работы Гильберт приводит другое доказательство, пригодное в общей ситуации, т. е. позволяющее установить нётеровость кольца многочленов от конеч-

ного числа переменных над коммутативным нётеровым кольцом. Предположение об однородности в действительности не важно, см. примечание [2].

[10] (с. 21). Речь идет о проективной алгебраической кривой в проективном пространстве.

[11] (с. 21). Речь идет о кривой в трехмерном проективном пространстве.

[12] (с. 21). Это будет означать, что идеал I кривой порожден тремя элементами и не меньше. Интуитивно естественно предположить, что кривая в трехмерном пространстве есть пересечение двух алгебраических поверхностей. Если это так, то кривая называется теоретико-множественным полным пересечением. Если же идеал всех форм, обращающихся в нуль на некоторой кривой, порожден двумя элементами, то кривая называется алгебраическим полным пересечением. Пример Гильберта показывает, что не всякая кривая является алгебраическим полным пересечением. Будет ли всякая кривая теоретико-множественным полным пересечением — до сих пор (1996 г.) неизвестно.

[13] (с. 21). Запись «$f \equiv h, (F_1, F_2, F_3)$» и т. п. означает, что $f - h = A_1F_1 + A_2F_2 + A_3F_3$ для некоторых форм A_1, A_2, A_3.

[14] (с. 22). Аналогично предыдущему можно считать, что $\mu_4 \neq 0$.

[15] (с. 22). Здесь и в непосредственно следующем за этим абзацем тексте Гильберт имеет в виду уравнение вида $f(\xi_1, \xi_2) = 0$, где $f(\xi_1, \xi_2)$ — бинарная форма какого-либо порядка d от переменных ξ_1 и ξ_2. Такая форма всегда распадается (если, например, основное поле — это $\mathbb{C}$) в произведение линейных форм: $f = \prod_{i=1}^{d}(\alpha_i\xi_1 - \beta_i\xi_2)$. Точки $(\beta_i : \alpha_i)$ проективной прямой с однородными координатами ξ_1 и ξ_2 называются корнями уравнения $f = 0$. Это уравнение следует рассматривать как «однородную форму» уравнения от одной переменной $\varphi(t) = 0$, где $\varphi(t)$ — многочлен степени $\leqslant d$ от переменной t, получающийся из $f(\xi_1, \xi_2)$ подстановкой $\xi_1 = t$, $\xi_2 = 1$. Всякий многочлен $\psi(t)$ степени $\leqslant d$ получается таким способом: его однородной формой является $\xi_2^{d-\deg\psi}\psi(\xi_1/\xi_2)$. Если $\gamma_1, \ldots, \gamma_s$ — корни многочлена φ (взятые с их кратностями), то корни формы f — это $(\gamma_1 : 1), \ldots, (\gamma_s : 1)$ и $(1 : 0)$ с кратностью $d - \deg\varphi$ (т. е. корни формы f получаются добавлением к корням многочлена φ еще корня ∞ с кратностью $d - \deg\varphi$).

[16] (с. 23). Этот пример допускает значительное и важное обобщение (что стало ясно уже в наше время). А именно, рассмотрим естественное действие группы SL_2 на пространстве V_4 бинарных квартик от переменных ξ_1 и ξ_2 над полем $\mathbb{C}$. Пусть X — множество всех квартик, являющихся 4-й степенью линейной формы от ξ_1 и ξ_2. Тогда дополнение в X к нулевой квартике является одной орбитой группы SL_2, а X является замыканием этой орбиты в V_4. Квартика $\xi_1^4 \in X$ является старшим вектором для действия SL_2 на V_4 относительно борелевской подгруппы B, состоящей из нижнетреугольных матриц. Таким образом, X служит примером аффинного алгебраического многообразия специального вида, которое может быть определено в общей ситуации, когда задано алгебраическое представление редуктивной алгебраической группы G в конечномерном векторном пространстве V (скажем, над полем $\mathbb{C}$), а именно, многообразия Y, являющегося замыканием G-орбиты какого-либо старшего вектора v в V (относительно фиксированной борелевской подгруппы в G) или, более общо, суммы таких старших векторов. Теория таких многообразий была развита Э. Б. Винбергом и В. Л. Поповым в статье, опубликованной в Изв. АН СССР, сер. матем., 1972, т. 36, № 4, с. 749–763. Лихтенштейн (*Lichtenstein W.* — Proc. Amer. Math. Soc., 1982, vol. 84, № 4, p. 605–608) для неприводимого действия группы G на V и Брион (*Brion M.* — Ann. sci. Ec. Norm. Sup., 1985, 4$^{\text{e}}$ sér., vol. 18, p. 345–387) в общем случае дали описание минимальной системы однородных образующих идеала I_Y тех полиномиальных функций на V, которые обращаются в нуль на Y (в действительности первый результат в этом направлении

принадлежит Б. Константу; он опубликован в работе: *Lancaster G., Towber J.* — J. Algebra, 1979, vol. 59, p. 16–38). Ответ (мы ограничимся для краткости случаем неприводимого действия G на V) состоит в следующем. Пусть $V = V(\lambda)$ — простой G-модуль со старшим весом λ. Рассмотрим симметрический квадрат S^2V^* дуального G-модуля V^* (таким образом, S^2V^* состоит из всех однородных полиномиальных функций степени 2 на V). Известно, что G-модуль S^2V^* содержит единственный простой подмодуль, изоморфный $V(2\lambda)^*$. Ввиду редуктивности группы G в S^2V^* существует дополнительный к нему подмодуль M. Пусть $f_1, \ldots, f_m$ — базис линейного пространства M. Тогда набор функций $f_1, \ldots, f_m$ на V и будет минимальной системой образующих идеала I_Y. В примере, который рассматривает Гильберт, базисом в V^* являются x_1, x_2, x_3, x_4, x_5 (поскольку φ рассматривается как «общая» квартика), а в S^2V^* — всевозможные произведения x_ix_j и указанные Гильбертом элементы $F_1, \ldots, F_6 \in S^2V^*$ образуют базис в M.

Замыкания орбит старших векторов (так называемые HV-многообразия, см.: *Виньберг Э. Б., Попов В. Л.*, loc. cit.) играют важную роль в приложениях. Например, именно в классе таких многообразий были найдены алгебраические многообразия с некоторыми экстремальными геометрическими свойствами (с «малыми» многообразиями секущих): все так называемые многообразия Севери и многообразия Скорца оказываются HV-многообразиями (см.: *Zak F. L.* Tangent and Secant of Algebraic Varieties. — Transl. Math. Monographs, vol. 127, AMS, 1993). Другое приложение связано с рассмотрением аналогов HV-многообразий для представлений бесконечномерных групп G (см.: *Кац В.* Бесконечномерные алгебры Ли. — М.: Мир, 1994): например, уравнения HV-многообразия для базисного представления группы G аффинного типа оказываются эквивалентом иерархии Хироты билинейных уравнений Дейта — Джимбо — Касивары — Мивы, что в простейшем случае группы G типа $A_1^{(1)}$ дает знаменитую иерархию Кортевега — де Фриза.

[17] (с. 23). В сущности это утверждение является прообразом современной теоремы о том, что конечно порожденный модуль над коммутативным нётеровым кольцом является нётеровым модулем.

[18] (с. 29). До сих пор то, что коэффициенты — целые числа, никак не использовалось. Дальнейшие рассуждения — по существу доказательство нётеровости кольца целых чисел $\mathbb{Z}$, а предыдущие рассуждения — доказательство нётеровости кольца многочленов над нётеровым кольцом (к однородному случаю дело сводится введением новой переменной, см. примечание [2]).

[19] (с. 32). Эти ограничения получаются из стандартных утверждений теории систем линейных уравнений над полем, если считать коэффициенты системы (13) элементами поля частных кольца многочленов.

[20] (с. 45). Речь идет о нахождении для каждого натурального числа d разности между размерностью пространства всех форм степени d от n переменных и размерностью его подпространства, состоящего из форм, лежащих в $(F_1, \ldots, F_m)$. В современной терминологии это число интерпретируется так. Рассмотрим в $(n-1)$-мерном проективном пространстве с однородными координатами $x_1, \ldots, x_n$ замкнутую подсхему X, определенную идеалом $I_X = (F_1, \ldots, F_m)$. Ее координатным кольцом является факторалгебра $S(X)$ алгебры многочленов от переменных $x_1, \ldots, x_n$ (над основным полем) по идеалу I_X. Эта алгебра естественным образом $\mathbb{N}$-градуирована: $S(X) = \bigoplus_{d=0}^{\infty} S(X)_d$, и «число условий», о котором говорит Гильберт, — это $\dim S(X)_d$.

[21] (с. 46). По существу Гильберт использует здесь следующий простой, но важный факт: если $0 \leftarrow V_1 \leftarrow V_2 \leftarrow \ldots \leftarrow V_s \leftarrow 0$ — точная последовательность конечномерных линейных пространств, то $\sum_{i=1}^{s} (-1)^i \dim V_i = 0$.

[22] (с. 46). В настоящее время она называется многочленом Гильберта схемы X (см. выше примечание [20]). Коэффициенты этого многочлена доставляют важные инварианты как самой схемы X, так и ее вложения в проективное пространство (см. ниже примечание [33]). Реализованная здесь на примере идеала $(F_1, \ldots, F_m)$ идея Гильберта изучать рост целых чисел, естественно связанных с $\mathbb{N}$-градуированными и фильтрованными алгебраическими объектами (т. е. рост размерностей или, более общо, длин соответствующих подмодулей или фактормодулей), получила в дальнейшем широкое распространение и стала фундаментальным средством построения важных целочисленных инвариантов объектов коммутативной алгебры и алгебраической геометрии. Так, например, для случая конечно порожденного модуля M над нётеровым локальным кольцом A со стабильной относительно примарного идеала $\mathfrak{a} \subset A$ фильтрацией она позволяет аналогично ввести характеристическую функцию $\chi_{M,\mathfrak{a}}$ — так называемый многочлен Гильберта — Самюэля (см.: *Serre J.-P.* — Lect. Notes in Math., vol. 11, 1975).

[23] (с. 46). Для доказательства того, что $\dim S(X)_d$ (см. примечание [20]) является при $d \gg 0$ значением некоторого не зависящего от d многочлена с рациональными коэффициентами, Гильберт пользуется своей теоремой о конечности цепи сизигий конечно порожденного градуированного модуля над кольцом многочленов над полем (теоремой III). Сейчас, однако, известно и другое доказательство, не опирающееся на теорему III; оно было дано Серром. В этой связи утверждение о существовании характеристической функции (формулируемое в действительности в большей общности, чем в настоящей работе Гильберта) называют теоремой Гильберта — Серра (см.: *Зарисский О., Самюэль П.* Коммутативная алгебра, т. II. — М.: ИЛ, 1963, с. 269).

[24] (с. 47). В 1955 г. Серр (*Serre J.-P.* — Ann. of Math., 1955, vol. 61, p. 197–278) показал, что для любого $R \in \mathbb{Z}$ число $\chi(R)$ имеет следующий когомологический смысл: если X — подсхема в $\mathbb{P}^{n-1}$, определенная идеалом $(F_1, \ldots, F_m)$, то $\chi(R)$ — это эйлерова характеристика пучка $\mathcal{O}_X(R)$, т. е. $\chi(R) = \sum_{i=0}^{\infty} (-1)^i \dim H^i(X, \mathcal{O}_X(R))$. Он показал, что если $R \gg 0$, то $H^i(X, \mathcal{O}_X(R)) = 0$ при $i \geqslant 1$, а пространство $H^0(X, \mathcal{O}_X(R))$ изоморфно R-му градуирующему подпространству однородного координатного кольца $S(X)$ схемы X, так что число $\dim H^0(X, \mathcal{O}_X(R))$ при $R \gg 0$ как раз и равно, в терминологии Гильберта, «числу независимых условий, которым должны удовлетворять коэффициенты формы степени R, чтобы она была сравнима с нулем по модулю $(F_1, \ldots, F_m)$». Эти утверждения непосредственно переносятся на любые когерентные пучки $\mathcal{F}$ над X. Для ряда важных типов схем пространство $H^0(X, \mathcal{O}_X(R))$ изоморфно R-му градуирующему подпространству однородного координатного кольца схемы X при любом R, а не только при $R \gg 0$ (таковы, например, полные пересечения или, более общо, арифметически коэн-мэколеевские схемы). В этом случае $\chi(R)$ отличается от упомянутого «числа независимых условий» на поправку $\sum_{i \geqslant 0} (-1)^i \dim H^i(X, \mathcal{O}_X(R))$, указывающую на когомологическую природу той границы, о которой пишет Гильберт. Исторически в ряде случаев, наоборот, непосредственное исследование этой границы приводило к гипотезам (а затем к теоремам) о когомологических свойствах соответствующих схем. Так, Ходж, исследуя постулационную формулу для грассмановых многообразий (*Hodge W.* — Proc. Cambr. Philos. Soc., 1943, vol. 39, p. 22–30), обнаружил, что многочлен Гильберта дает размерность R-го градуирующего подпространства однородного координатного кольца для любого R. Это привело к предположению о тривиальности соответствующих когомологий, а точнее, об арифметической коэн-мэколеевости грассманианов, что и было затем доказано Хохстером, Лаксовом и Музили (*Hochster M.* — J. Algebra, 1973, vol. 25, p. 40–57; *Laksov D.* — Acta math., 1972, Bd. 1291, S. 1–9; *Musili C.* — J. Indian. Math. Soc., 1972, vol. 36, p. 143–171). См. также примечание [25].

[25] (с. 47). Помимо многочлена Гильберта χ важную информацию об идеале $(F_1, \ldots, F_m)$ и определяемой им схеме X доставляет производящая функция последовательности $c_0, c_1, \ldots$, т. е. формальный степенной ряд $\sum_{R=0}^{\infty} c_R t^R = P_X(t)$, называемый в наше время рядом Пуанкаре этой последовательности (или схемы X). Такие ряды рассматривал еще Кэли (*Cayley F.* Coll. Math. Papers, vol. II. — Cambr. Univ. Press, 1889, p. 250–275); систематически их изучал Мэколей (*Macaulay F. S.* The algebraic theory of modular systems. — Cambridge Tracts, 1916, vol. 19), а затем Островский (*Ostrowski A.* — Abh. Math. Sem. Univ. Hamburg, 1922, Bd. 1, S. 281–326), заметивший, что $P_X(t)$ сходится при $|t| < 1$ и является рациональной функцией вида $N(t)/(1-t)^n$, где $N(t)$ — многочлен с целыми коэффициентами. Более общо, можно аналогично определить ряд Пуанкаре $P_{M,A}(t)$ любого конечно порожденного градуированного модуля M над конечно порожденной градуированной алгеброй A над полем k. Он также сходится при $|t| < 1$ и является рациональной функцией вида $F(t)/D(t)$, где $F(t)$ — многочлен с целыми коэффициентами, а $D(t)$ имеет вид $\prod_{i=1}^{m}(1 - t^{d_i})$. Ряд $P_X(t)$ получается, если вместо A и M взять однородные координатные кольца соответственно проективного пространства и схемы X (специфика этого случая проявляется в том, что однородные образующие алгебры A имеют степень 1). По ряду Пуанкаре $P_X(t)$ могут быть найдены многочлен Гильберта χ и граница, начиная с которой $\chi(R) = c_R$. А именно, выполнив деление с остатком, можно записать $P_X(t)$ в виде $Q(t) + S(t)/(1-t)^n$, где $Q(t)$ и $S(t)$ — многочлены с целыми коэффициентами и $\deg S(t) \leqslant n-1$. Пусть $\deg Q(t) = d$, а разложение функции $S(t)/(1-t)^n$ в ряд по t в окрестности нуля имеет вид $a_0 + a_1 t + \ldots$. Тогда $\chi(R) = a_R$ для любого R и $\chi(R) = c_R$ при $R > d$ (но $\chi(d) \neq c_d$). Более того, отсюда вытекает, что числа c_R при $R > d$ связаны линейным рекуррентным соотношением $0 = \sum_{i=0}^{n}(-1)^i \binom{n}{i} c_{n+r-i}$, $r = d+1, d+2, \ldots$ В случае произвольного модуля M коэффициенты b_R ряда $P_{M,A}(t) = \sum_{R \geqslant 0} b_R t^R$ являются при $R \gg 0$ значениями не многочлена с рациональными коэффициентами, а квазимногочлена, т. е. функции от R вида $G_1(R)\alpha_1^R + \ldots + G_q(R)\alpha_q^R$, где G_i — многочлены от R с рациональными коэффициентами, а α_i — корни из 1. Эта функция играет в общем случае роль «многочлена Гильберта».

[26] (с. 47). Гильберт нигде дальше не изучает свойств этого разбиения. Поэтому тот факт, что он все-таки вводит понятие «класса модулей», свидетельствует о том, что он считал его важным. Это предвидение нашло в современной алгебраической геометрии точное подтверждение. Как показал Гротендик (*Grothendieck A.* Fondementes de la géometrie algébrique. — Seminaire Bourbaki, Exp. 221, Paris, 1962), замкнутые подсхемы проективного пространства, имеющие одинаковые многочлены Гильберта (это условие выполнено, если определяющие их идеалы принадлежат одному «классу модулей»), сами наделяются структурой схемы — так называемой схемы Гильберта. Теория схем Гильберта играет фундаментальную роль в современной алгебраической геометрии (в теории модулей алгебраических многообразий и схем).

[27] (с. 47). Возможность такого представления функции χ вытекает из того, что χ — многочлен с рациональными коэффициентами степени d, а $\binom{R}{s}$ — многочлен с рациональными коэффициентами степени s.

[28] (с. 52). Иначе говоря, «наименьший содержащий» и «наибольший общий» модули — это, в современной терминологии, соответственно пересечение и сумма идеалов $(F_1, \ldots, F_m)$ и $(H_1, \ldots, H_h)$.

[29] (с. 53). В сущности это есть элементарная формула линейной алгебры

$$\dim(V_1 + V_2) = \dim V_1 + \dim V_2 - \dim V_1 \cap V_2$$

(где V_i — конечномерные линейные подпространства некоторого линейного пространства), а предшествующие ей рассуждения — ее стандартное доказательство.

[30] (с. 53). Речь идет о проективном пространстве и проективных алгебраических кривых, а далее — о проективных алгебраических поверхностях.

[31] (с. 53). Количество этих условий называется постулацией соответствующего алгебраического многообразия, а формула, задающая это количество при всех R, — постулационной формулой.

[32] (с. 54). Требуется, чтобы эта кривая не просто являлась пересечением двух таких поверхностей $F_1 = 0$ и $F_2 = 0$, но чтобы (F_1, F_2) был «модулем», соответствующим этой кривой, т. е. чтобы всякая другая алгебраическая поверхность, содержащая эту кривую, задавалась уравнением $A_1F_1 + A_2F_2 = 0$, где A_1 и A_2 — многочлены (ср. с примечанием [12]).

[33] (с. 54). Если X — неприводимое d-мерное проективное алгебраическое многообразие в проективном пространстве $\mathbb{P}^n$ и χ — характеристическая функция идеала I_X, состоящего из форм, обращающихся на X в нуль, то χ_d — это, в современной терминологии, степень $\deg X$ многообразия X, т. е. число точек пересечения X с $(n-d)$-мерным линейным подпространством в $\mathbb{P}^n$ общего положения (основным полем является, как у Гильберта, $\mathbb{C}$ или, более общо, любое алгебраически замкнутое поле). Число $p_a(X) = (\chi_0 - 1)(-1)^d$ — это арифметический род многообразия X (или идеала I_X). Что касается остальных коэффициентов χ_i, то они связаны с арифметическими родами общих линейных сечений многообразия X размерностей $1, 2, \ldots, d-1$ с помощью следующей формулы Севери (*Severi F.* — Rend. Circ. Math. Palermo, 1909, vol. 28, p. 33–87):

$$\chi(R) = \frac{(R+d-1)\ldots R}{d!}\deg X + \frac{(R+d-2)\ldots R}{(d-1)!}[1 - p_a(X \cap H_1 \cap \ldots \cap H_{d-1})] + \ldots$$
$$\ldots + R[1 + (-1)^{d-1}p_a(X \cap H_1)] + [1 + (-1)^d p_a(X)],$$

где $H_1, H_2, \ldots, H_{d-1}$ — общий набор гиперплоскостей в $\mathbb{P}^n$. Гильберт ограничивается в этом месте лишь намеком как на сам характер связи коэффициентов $\chi_0, \ldots, \chi_{d-1}$ с «родовыми числами», так и на способ его доказательства; однако то, что речь идет о «переходе от $n-1$ к n переменным», позволяет предполагать, что он имеет в виду некоторые эквиваленты указанной формулы и ее геометрического доказательства с помощью последовательного рассмотрения гиперплоских сечений.

[34] (с. 54). То есть речь идет о том, в какой мере однородный идеал I в однородном координатном кольце проективного пространства $\mathbb{P}^n$ определяется своим «множеством нулей», — алгебраическим многообразием $X_I = \{p \in \mathbb{P}^n \mid f(p) = 0 \ \ \forall f \in I\}$. Ответ на этот вопрос был получен самим Гильбертом в работе 1893 г. (перевод которой на русский язык включен в настоящее издание, с. 67–114) единым методом, не связанным с использованием фундаментальной теоремы Нётера. Этот результат называется теперь теоремой Гильберта о корнях; она утверждает, что радикал $\sqrt{I}$ идеала I совпадает с идеалом всех форм, обращающихся на X_I в нуль.

[35] (с. 55). Гильберт, видимо, имеет в виду конструктивное нахождение этих чисел.

[36] (с. 55). Это решение будет опираться на доказанную в разд. I теорему I и поэтому будет неконструктивным (в отличие от данного Горданом решения в случае инвариантов бинарных форм).

[37] (с. 55). Таким образом, речь идет о следующей ситуации. Рассматривается «общая» (т. е. с буквенными коэффициентами a_i) бинарная форма

$f = \sum_{i=0}^{n} a_i \binom{n}{i} x_1^{n-i} x_2^i$. Если осуществить невырожденную линейную замену переменных $x_1 \mapsto \alpha x_1 + \beta x_2$, $x_2 \mapsto \gamma x_1 + \delta x_2$, то f преобразуется в форму $f' = \sum_{i=0}^{n} a_i' \binom{n}{i} x_1^{n-i} x_2^i$, где коэффициенты a_i' являются линейными комбинациями коэффициентов $a_0, \ldots, a_n$ формы f. Инвариант базисной формы f — это однородный многочлен от $a_0, \ldots, a_n$, не меняющийся при любой замене $(a_0, \ldots, a_n) \mapsto (a_0', \ldots, a_n')$, индуцированной унимодулярной линейной заменой переменных x_1, x_2. В современных терминах речь идет о естественном действии группы SL_2 на алгебре полиномиальных функций на пространстве $(n+1)$-мерного неприводимого представления группы SL_2 и инварианты — это функции, неподвижные относительно этого действия.

[38] (с. 57). Таким образом, речь идет о функции вида $F = \sum c_{i_0 \ldots i_n} a_0^{i_0} \ldots a_n^{i_n}$, где $c_{i_0, \ldots, i_n}$ — числовые коэффициенты, а суммирование ведется по таким наборам $(i_0, \ldots, i_n)$ целых неотрицательных индексов, что $i_0 + \ldots + i_n = r$ (однородность) и $1 \cdot i_1 + 2 \cdot i_2 + \ldots + n \cdot i_n = p$ (изобарность). Число p называется весом функции F. Тот факт, что $p = nr/2$, равносилен инвариантности однородной функции F относительно естественного действия одномерного тора T группы SL_2, состоящего из диагональных матриц, на алгебре многочленов от $a_0, \ldots, a_n$ (см. примечание [37]). В свою очередь, это эквивалентно тому, что F аннулируется естественным действием алгебры Ли этого тора. Эта алгебра Ли одномерна и ее образ в алгебре Ли дифференцирований алгебры многочленов от $a_0, \ldots, a_n$ натянут на дифференцирование $H = na_0 \dfrac{\partial}{\partial a_0} + (n-2)a_1 \dfrac{\partial}{\partial a_1} + \ldots + (-n)a_n \dfrac{\partial}{\partial a_n}$. Поэтому изобарность с $p = nr/2$ эквивалентна условию $HF = 0$. Пусть U_+ и U_- — соответственно подгруппа всех верхнетреугольных и подгруппа всех нижнетреугольных матриц из SL_2 с единицами на диагонали. Тогда пространства SL_2/TU_+ и SL_2/TU_- компактны, и отсюда несложно вывести, что инвариантность функции F эквивалентна ее неизменности относительно преобразований, взятых лишь из TU_+ или лишь из TU_-. Поэтому если F однородна степени r и изобарна веса $nr/2$, то она будет инвариантом в точности тогда, когда она не меняется под действием преобразований только из U_+ (или только из U_-). В свою очередь, это эквивалентно тому, что F аннулируется естественным действием алгебры Ли группы U_+ (или группы U_-). Но эти алгебры одномерны, и легко видеть, что их образы в алгебре Ли дифференцирований алгебры многочленов от $a_0, \ldots, a_n$ натянуты соответственно на D и Δ. Поэтому однородная степени r и изобарная веса $nr/2$ функция F будет инвариантом в точности тогда, когда $DF = 0$ (или, эквивалентно, $\Delta F = 0$). Пространства форм от $a_0, \ldots, a_n$ любой заданной степени инвариантны относительно линейных операторов D и Δ, и ограничения этих операторов на эти подпространства нильпотентны. Поэтому результат применения процесса [ ] к любой форме F является конечной суммой форм, а потому имеет смысл. Из сказанного и из вида [ ] непосредственно вытекает, что $[i] = i$ для любого инварианта i, — это будет использованно Гильбертом далее. Тот факт, что $[F]$ для однородной степени r и изобарной веса $nr/2$ функции F будет инвариантом, может быть выведен из указанного выше критерия инвариантности, если воспользоваться каноническими соотношениями в универсальной обертывающей алгебре алгебры Ли группы SL_2: $HD - DH = 2D$, $H\Delta - \Delta H = -2\Delta$ и $D\Delta - \Delta D = H$.

[39] (с. 57). Здесь использовано то, что при перемножении изобарных функций снова получается изобарная функция, вес которой равен сумме весов сомножителей. Более того, поскольку i, $i_1, \ldots, i_m$ — инварианты, вес каждого из них равен степени, умноженной на $n/2$. Отсюда следует, что этим же свойством обладает и вес каждой из функций $B_1, \ldots, B_m$, а значит, $[B_i]$ — инвариант. Это используется ниже.

[40] (с. 57). См. примечание [38].

[41] (с. 57). То есть речь идет о существовании в случае многих переменных аналога процесса [ ].

[42] (с. 59). Формула (43) получается, если умножить обе части предыдущей формулы на a^q и воспользоваться теоремой об умножении определителей $a^q b^q = c^q$.

[43] (с. 60). Следует учесть, что применение $\dfrac{\partial^{3p}}{\partial a_{11}^{p_{11}} \partial a_{12}^{p_{12}} \dots \partial a_{33}^{p_{33}}}$ к одночлену $a_{11}^{q_{11}} a_{12}^{q_{12}} \dots a_{33}^{q_{33}}$, где $p_{11} + p_{12} + \dots + p_{33} = q_{11} + q_{12} + \dots + q_{33} = 3p$, дает $q_{11}! q_{12}! \dots q_{33}!$, если $p_{11} = q_{11}, p_{12} = q_{12}, \dots, p_{33} = q_{33}$, и нуль в противном случае.

[44] (с. 60). В следующей формуле использован тот факт, что по определению $J(f_a)/N_p = a^p J(f)/N_p$, а $J(f)/N_p$ от a не зависит.

[45] (с. 64). Имеется в виду прямая в трехмерном проективном пространстве и ее плюккеровы координаты.

[46] (с. 64). Этот ход мысли привел к постановке четырнадцатой проблемы Гильберта: для любой ли подгруппы G в GL_n алгебра A^G инвариантных относительно G многочленов от n переменных конечно порождена? Точнее, на конгрессе 1900 г. в Париже Гильберт сформулировал свою четырнадцатую проблему несколько иначе, поскольку полагал, ссылаясь на работу Маурера (*Maurer L.* — Sitzungsber. der K. Akad. der Wiss. zu München, 1899, S. 147–175), что ответ на поставленный вопрос является положительным. Однако, как вскоре выяснилось, работа Маурера содержала ошибку, и с тех пор четырнадцатая проблема Гильберта рассматривается именно в сформулированном выше виде. До 1958 г. было установлено, что для многих важных классов групп G алгебра A^G конечно порождена: Фишер (*Fischer E.* — Crelles J., 1911, Bd. 140, S. 48–81) доказал это для комплексных групп G, которые (если их рассматривать как матричные группы) вместе с каждой матрицей B содержат и $\overline{B}^T$, Э. Нётер (*Noether E.* — Math. Ann., 1916, Bd. 77, S. 89–92; Nachr. Ges. Wiss. Göttingen, 1926, S. 28–35) — для конечных групп над любым полем, Вейценбек (*Weitzenböck R.* — Acta Math., 1932, vol. 58, p. 231–293) — для комплексных одномерных алгебраических групп, Г. Вейль (см.: *Вейль Г.* Классические группы. — М.: ИЛ, 1947; эта книга была впервые опубликована на английском языке в 1939 г.), обобщая результат и идеи настоящей работы Гильберта и важной работы Гурвица (*Hurwitz A.* Über die Erzengung der Invarianten durch Intergation. — Nachr. Ges. Wiss. Göttingen, 1897), доказавшего конечность числа базисных ортогональных инвариантов, — для компактных групп Ли G и комплексных редуктивных групп Ли G. Однако в 1958 г. на конгрессе в Эдинбурге Нагата — весьма неожиданно — привел пример коммутативной унипотентной группы G, для которой алгебра A^G не имеет конечного числа образующих (см.: *Nagata M.* — In: Proc. Int. Congress Math., 1958, Cambr. Univ. Press, 1960, p. 459–462). С тех пор под оригинальной четырнадцатой проблемой Гильберта стали понимать задачу теоретико-группового описания тех групп G, для которых алгебра A^G конечно порождена. При этом достаточно ограничиться лишь алгебраическими группами над алгебраически замкнутым полем. Интенсивное развитие за последние три десятилетия теории алгебраических групп преобразований (которая сейчас отождествляется с теорией инвариантов) привело к ясному пониманию недостаточности и неестественности рассмотрения лишь линейных действий: вместо них стали систематически изучать алгебраические действия алгебраических групп на произвольных аффинных алгебраических многообразиях или, эквивалентно, действия алгебраических групп на аффинных алгебрах — алгебрах регулярных функций на таких многообразиях (т. е. конечно порожденных приведенных алгебрах над полем). Соответственно этому Нагата сформулировал «обобщенную четырнадцатую проблему» (*Nagata M.* Lectures on the Fourteenth problem of Hilbert. — Tata Inst.,1965): найти теоретико-групповую характеризацию таких алгебраических групп G, что для любого алгебраического действия G на любой аффинной алгебре A алгебра инвариантов A^G конечно порож-

дена. В настоящее время эта проблема решена: указанное свойство будет выполнено тогда и только тогда, когда G редуктивна (т. е. имеет тривиальный унипотентный радикал). Доказательство достаточности в случае основного поля характеристики нуль по существу основывается на той же идее, которую использовал в настоящей работе Гильберт (роль процесса, переводящего неинварианты в инварианты, играет при этом так называемый оператор Рейнольдса, см. ниже примечание [47]); в случае положительной характеристики это доказательство значительно сложней и существенно использует структурную теорию алгебраических групп. Оно было получено совместными усилиями Нагаты (*Nagata M.* — J. Math. Kyoto Univ., 1964, vol. 3, p. 369–377), Хэбуша (*Haboush W. J.* — Ann. of Math., 1975, vol. 102, p. 67–83) и Мамфорда (*Mumford D.* Geometric Invariant Theory. — Ergebn. der Math. und ihrer Grenzg., Bd. 34, Springer-Verlag, 1965; имеется неполный перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974). Необходимость была доказана В. Л. Поповым (ДАН СССР, 1979, т. 249, № 3, с. 551–555). Этот результат объясняет, почему редуктивные группы играют в современной теории инвариантов ключевую роль. Что касается оригинальной четырнадцатой проблемы Гильберта, то она до сих пор не решена. Ситуация, рассматриваемая в ней, имеет важную особенность: действие группы G продолжается до действия некоторой редуктивной группы H (а именно GL_n). В этой проблеме всегда можно считать G так называемой обозримой подгруппой (это эквивалентно квазиаффинности многообразия H/G). Можно показать, что конечная порожденность алгебры инвариантов группы G зависит лишь от свойств пары (G, H): она эквивалентна конечной порожденности алгебры регулярных функций на (квазиаффинном) однородном пространстве H/G (*Grosshans F.* — Amer. J. Math., 1973, vol. XCV, № 1, p. 229–253). Обозримые алгебраические подгруппы G редуктивных алгебраических групп H с таким свойством называются подгруппами Гроссханса и оригинальная четырнадцатая проблема Гильберта — это проблема классификации подгрупп Гроссханса: простейшая из них, согласно упомянутому выше классическому результату Вейценбека, — одномерная унипотентная подгруппа. Однако к настоящему времени (1996 г.) их полная классификация неизвестна.

Вместе с тем недавно Р. Стейнбергу удалось упростить аргументы М. Нагаты и заменить в его контрпримере к четырнадцатой проблеме Гильберта тонкие соображения из алгебраической геометрии плоских кривых вполне элементарными рассуждениями (*Steinberg R.* Nagata's example. — In: Algebraic Groups and Lie Groups. A volume of papers in honour of the late R. W. Richardson. — Austral. Math. Soc. Lect. Series. 9, Cambr. Univ. Press, 1997, p. 375–384). Кроме того, П. Робертсом был найден новый подход к получению контрпримера к четырнадцатой проблеме Гильберта, использующий методы коммутативной алгебры (*Roberts P.* — J. Algebra, 1990, vol. 132, p. 461–473). В контексте теории инвариантов он был реализован А'Кампо (*A'Campo-Neuen A.* Note on a counterexample to Hilbert's fourteenth problem given by P. Roberts. — Indag. Math., N. S., 1994, vol. 5, p. 253–257).

[47] (с. 65). Эти примеры показывают, что Гильберт ясно осознавал универсальность своего метода доказательства конечности числа элементов фундаментальной системы инвариантов. В сущности, он подчеркивает здесь, что специфика выбора той или иной группы сказывается только в существовании некоторой процедуры, позволяющей получать из произвольного многочлена P инвариант $\overline{P}$ и обладающей несколькими простыми свойствами: а) отображение $P \mapsto \overline{P}$ является проектором алгебры всех многочленов A на алгебру инвариантов A^G; б) $\overline{PQ} = \overline{P}\,\overline{Q}$ для любых $P \in A$ и $Q \in A^G$. Если такая процедура имеется, то все остальное носит совершенно общий, не зависящий от группы характер, поскольку основывается только на теореме I. В рассматриваемых в тексте случаях Гильберт строит такую процедуру явно, но иначе в то время и не могло быть. Общая теория групп Ли должна была еще пройти долгий путь развития, прежде чем Г. Вейлю удалось найти в 1925–1926 гг. дока-

зательство существования указанной процедуры для всех компактных групп Ли G (и — с помощью «унитарного трюка» — для всех комплексных редуктивных групп Ли G) (см.: *Вейль Г.* Теория представлений непрерывных полупростых групп при помощи линейных преобразований. — В кн.: *Вейль Г.* Избранные труды. — М.: Наука, 1984): в качестве $\overline{P}$ следует взять результат усреднения P по G относительно инвариантной нормированной меры, $\overline{P}(x) = \int\limits_G P(ga)\,dg$. Вейль при этом развивал идеи Гурвица, получившего с помощью интегрирования инварианты ортогональной и унитарной групп и заметившего (это было первым примером «унитарного трюка»), что так получаются инварианты полной линейной группы (*Hurwitz A.* — Nachr. Ges. Wiss. Göttingen, 1897, S. 71–90). В случае конечной группы G процесс усреднения является простой конструктивной процедурой; она была использована Машке для доказательства теоремы о полной приводимости представлений таких групп (*Maschke H.* — Math. Ann., 1898, Bd. 50, S. 482–498). Фундаментальный результат Г. Вейля о полной приводимости представлений компактных и комплексных редуктивных групп Ли (полученный в цитированной выше работе) позволил понять и простой чисто алгебраический смысл отображения $P \mapsto \overline{P}$: оно является единственным G-инвариантным проектором A на A^G или, что то же самое, проектором A на A^G параллельно сумме всех отличных от A^G изотипных компонент G-модуля A (его называют оператором Рейнольдса). Это позволяет избежать в определении отображения $P \mapsto \overline{P}$ трансцендентных средств (типа интегрирования) и дает возможность дословно перенести утверждение и доказательство Гильберта на общую ситуацию алгебраических действий редуктивных алгебраических групп над алгебраически замкнутым полем характеристики нуль на аффинных алгебраических многообразиях (сейчас этот результат называется теоремой Гильберта об инвариантах). Возможности этого метода естественно ограничиваются классом редуктивных алгебраических групп над алгебраически замкнутым полем характеристики нуль, поскольку полная приводимость алгебраических представлений является характеристическим свойством таких групп. Существование в A^G-модуле A дополнительного к A^G подмодуля (ядра оператора Рейнольдса) играет ключевую роль не только в доказательстве теоремы о конечной порожденности алгебры A^G, но и в доказательстве других фундаментальных свойств этой алгебры. Так, сравнительно недавно Хохстер и Робертс показали, что из него вытекает коэн-мэколеевость алгебры A^G, если A — алгебра многочленов (*Hochster M., Roberts J.* — Adv. Math., 1974, vol. 13, p. 125–175), а Буто получил еще более тонкий результат: $\operatorname{Spec} A^G$ имеет рациональные особенности, если $\operatorname{Spec} A$ имеет рациональные особенности (в этих утверждениях характеристика основного поля равна нулю) (*Boutot J.-F.* — Invent. Math., 1987, vol. 88, p. 65–68). Эти результаты играют важную роль в современной теории инвариантов.

[48] (с. 65). Ср. с примечанием [2].

[49] (с. 66). Проблема явного описания неприводимых сизигий всех родов в каждом конкретном случае является, как правило, чрезвычайно сложной. Так, например, для инвариантов бинарной формы степени d она была решена классиками только при $d \leqslant 6$ (при $d \leqslant 4$ алгебра инвариантов свободна, т. е. не имеет сизигий, а при $d = 5, 6$ она является так называемой гиперповерхностью, т. е. имеет единственную неприводимую сизигию первого рода и не имеет высших сизигий). Случай $d = 8$ был исследован лишь в 1967 г. Шиодой (*Shioda T.* — Amer. J. Math., 1967, vol. 89, p. 1022–1046), а длина цепи сизигий при $d = 7$ была найдена лишь в 1985 г. Диксмье и Лазаром (*Dixmier J., Lazard D.* — Pörtugaliae Math., 1985–86, vol. 43, f. 3, p. 377–392): она равна 3 при $d = 8$ и 25 при $d = 7$. Полное исследование других случаев вряд ли возможно (и разумно), поскольку сложность алгебры инвариантов бинарной формы стремительно растет вместе с ее степенью d: В. Л. Попов (Изв. АН СССР, сер. матем., 1983, т. 47, № 3, с. 544–622) показал,

что при $d \to \infty$ длина цепи сизигий алгебры инвариантов растет быстрее любой степени d. Длину h цепи сизигий алгебры инвариантов (в современной терминологии h — это гомологическая размерность этой алгебры) естественно рассматривать как меру сложности алгебры инвариантов. С этой точки зрения первостепенный интерес представляет описание тех линейных групп (и тех алгебр инвариантов), у которых эта длина невелика. Эта задача тем более естественна, что, как было показано Поповым (loc. cit.), каждая связная полупростая или конечная группа имеет лишь конечное число представлений без ненулевых неподвижных векторов, алгебра инвариантов которых имеет наперед заданную гомологическую размерность h. В первую очередь по этой программе надлежит исследовать линейные группы со свободной алгеброй инвариантов ($h = 0$). Классификация комплексных конечных групп такого типа была получена Шевалле, Шепардом и Тоддом (*Chevalley C.* — Amer. J. Math., 1955, vol. 67, p. 778–786; *Shephard G. C., Todd J. A.* — Canad. J. Math., 1954, vol. 6, p. 274–304); они нашли как явный вид таких групп, так и их единообразную теоретико-групповую характеризацию: это в точности группы, порожденные псевдоотражениями. Метод классификации связных полупростых групп со свободной алгеброй инвариантов был найден в 1976 г. В. Г. Кацем, В. Л. Поповым и Э. Б. Винбергом (*Kac V. G., Popov V. L., Vinberg E. B.* — C. R. Acad. Sci. Paris, 1976, vol. 283, ser. A, p. 875–878); в качестве примера его применения они нашли список всех простых неприводимых комплексных групп такого типа. В настоящее время известны списки всех связных простых комплексных групп со свободной алгеброй инвариантов (*Schwarz G. W.* — Invent. Math., 1978, vol. 49, p. 167–191, и, независимо, Адамович О. М., Головина Е. О. — Вопросы теории групп и гомологической алгебры, вып. 2, 1979, Ярославль) и связных полупростых неприводимых комплексных групп со свободной алгеброй инвариантов (*Littelmann P.* — J. Algebra, 1989, vol. 123, № 1, p. 193–222). Получена классификация и в случае $h = 1$ (алгебра инвариантов является гиперповерхностью): Н. Л. Гордеев (Изв. АН СССР, сер. матем., 1986, т. 50, № 2, с. 345–352) и, независимо, Накадзима (*Nakajima H.* — J. Algebra, 1983, vol. 80, p. 279–294; Manuscr. Math., 1984, vol. 48, p. 163–187; Nagoya Math. J., 1985, vol. 98, p. 1–36) нашли списки конечных групп, а Накадзима (J. reine und angew. Math., 1986, Bd. 367, S. 115–138) — список связных простых групп с таким свойством. Для SL_2 классификация доведена до $h = 3$, а для алгебр инвариантов бинарных форм (т. е. для неприводимых представлений SL_2) — до $h = 10$ (*Popov V. L.* — J. reine und angew. Math., 1983, Bd. 341, S. 157–173).

[50] (с. 66). В действительности, поскольку, согласно теореме Хохстера — Робертса (см. примечание [47]), алгебра инвариантов является алгеброй Коэна — Мэколея, длина цепи сизигий равна $m - d$, где d — максимальное число алгебраически независимых базисных инвариантов.

В. Л. Попов

О ПОЛНОЙ СИСТЕМЕ ИНВАРИАНТОВ

Настоящая работа тесно связана с работой Гильберта 1890 г. «О теории алгебраических форм», перевод которой на русский язык также включен в это издание. Обе они являются наиболее значительными исследованиями Гильберта по теории инвариантов. Как и в работе 1890 г., Гильберт, имея в виду приложения в теории инвариантов, получает здесь ряд результатов фундаментального общеалгебраического значения: доказывает теорему, известную сейчас как теорема Гильберта о нулях (или о корнях), и теорему, являющуюся градуированным вариантом более поздней теоремы (или леммы) Нётер о нормализации. Вместе с теоремами о базисе, о цепях сизигий и о существовании характеристической функции (многочлена

Гильберта) из работы 1890 г. эти результаты положили начало современной коммутативной алгебре и гомологической алгебре.

Однако если в работе «О теории алгебраических форм» собственно теории инвариантов посвящен лишь последний раздел, то здесь ей уделено основное внимание. Известно, что неконструктивность доказательства конечной порожденности алгебры инвариантов, данного Гильбертом в работе 1890 г., вызвала (особенно поначалу) критику специалистов; см. подробности в комментариях к этой работе. Настоящая статья и явилась реакцией на эту критику: Гильберт ставит себе задачу дать конструктивное доказательство теоремы о конечной порожденности, т. е. указать способ, позволяющий в принципе за конечное число шагов с помощью явно осуществимых вычислений найти систему образующих.

Решение этой задачи эквивалентно нахождению априорной оценки сверху M на степени элементов из такой системы. В самом деле, имеются конструктивные способы нахождения базиса в пространстве однородных инвариантов любой фиксированной степени: это можно сделать либо с помощью символического метода, либо решая соответствующую систему линейных дифференциальных уравнений для инварианта (см. примечание [3]). Поэтому если число M заранее известно, то можно конструктивно найти (однородный) базис в пространстве инвариантов степени $\leqslant M$, и он будет системой образующих алгебры инвариантов. При необходимости из этой системы можно выделить минимальную такую систему — это также делается конструктивно (в нее войдут все элементы минимальной степени, затем те элементы следующей степени, которые не являются многочленами от элементов минимальной степени, и т. д.).

Занимаясь указанной задачей, Гильберт развивает замечательную теорию, вскрывающую тесную связь этой задачи с исследованием некоторого специального алгебраического многообразия — многообразия так называемых нуль-форм (т. е. форм, на которых обращаются в нуль все непостоянные однородные инварианты). Такое многообразие $\mathfrak{N}_{G,V}$ можно определить в самом общем контексте — когда редуктивная алгебраическая группа G, определенная над алгебраически замкнутым полем k, линейно действует на конечномерном векторном пространстве V. Если рассмотреть многообразие $V/\!/G := \operatorname{Spec} k[V]^G$ и естественный морфизм $\pi\colon V \to V/\!/G$, то $\mathfrak{N}_{G,V}$ — это слой $\pi^{-1}(\pi(0))$. Настоящая работа Гильберта не только впервые продемонстрировала (в контексте действия унимодулярной группы на пространстве форм) ключевую роль этого слоя в решении тонких задач теории инвариантов, но и содержит его замечательное геометрическое описание (см. примечание [61]).

Однако глубина проникновения Гильберта в существо дела была оценена по достоинству далеко не сразу: эта работа (в части, касающейся собственно теории инвариантов), по-видимому, опередила свое время и, в отличие от работы «О теории алгебраических форм», сразу имевшей широкий резонанс, долгое время не вызывала ощутимого интереса. Лишь в 1965 г. Мамфорд в книге: *Mumford D.* Geometric invariant theory. — Ergebn. der Math. und ihrer Grenzg., Bd. 34, Springer-Verlag, 1965 (имеется неполный перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974), распространив идеи этой работы Гильберта на общую ситуацию алгебраического действия редуктивной алгебраической группы G на алгебраическом многообразии (схеме) X, сумел применить их к решению классической алгебро-геометрической проблемы — построению многообразия модулей алгебраических кривых (а также абелевых многообразий и векторных расслоений на кривых). В общих чертах конструкция Мамфорда такова. Многообразия модулей возникают как так называемые геометрические факторы некоторых действий редуктивных алгебраических групп на подходящих алгебраических многообразиях. В общем случае геометрического фактора для действия G на X не существует; однако он существует для некоторого инвариантного открытого подмножества в X, и проблема состоит в точном описании такого подмножества. В контексте теории модулей это означает, что для того чтобы многообразие модулей

каких-либо геометрических объектов существовало, необходимо исключить некоторые «вырожденные» типы таких объектов. Эти исключительные типы и оказываются аналогом нуль-форм Гильберта. А именно, построение в X открытых подмножеств, допускающих геометрический фактор, основывается на следующем замечании: если G действует на неприводимом аффинном многообразии Y, то естественный морфизм $\pi\colon Y \to \operatorname{Spec} k[Y]^G$ является геометрическим фактором тогда и только тогда, когда все G-орбиты в Y имеют одинаковую размерность. Отсюда можно вывести, что если $U \subset \operatorname{Spec} k[Y]^G$ — такое открытое множество, что все орбиты в $\Omega = \pi^{-1}(U)$ имеют одинаковую размерность, то $\pi\colon \Omega \to U$ является геометрическим фактором. Это определяет интерес к нахождению в X инвариантных открытых подмножеств типа Ω: «склеивая» их геометрические факторы, можно получить геометрический фактор для открытого подмножества в X, являющегося их объединением. Построение же таких открытых множеств в X может быть осуществлено с помощью следующего приема. Предположим, что X неприводимо, обладает G-эквивариантным вложением в проективное пространство $\mathbb{P}^n$ и действие группы G на $\mathbb{P}^n$ поднимается до ее линейного действия на векторном пространстве V, проективизацией которого является $\mathbb{P}^n$. Поскольку все орбиты в любом инвариантном открытом подмножестве из X, обладающем геометрическим фактором, имеют одинаковую размерность, можно заменить X на $\{x \in X \mid \dim G x \geqslant \dim G y \ \forall y \in X\}$ и считать, что все орбиты в X имеют одинаковую размерность. (Можно показать, что все эти требования не слишком ограничительны.) Пусть теперь f — однородный G-инвариант для действия G на V. Тогда $\mathbb{P}^n_f = \mathbb{P}^n \setminus \{p \in \mathbb{P}^n \mid f(p) = 0\}$ — аффинное инвариантное открытое множество в $\mathbb{P}^n$, а $X \cap \mathbb{P}^n_f$ — множество типа Ω (оно допускает геометрический фактор). Ясно, что пересечение всех множеств вида $\{v \in V \mid f(v) = 0\}$ есть как раз многообразие $\mathfrak{N}_{G,V}$ (многообразие так называемых неполустабильных точек — аналогов нуль-форм). Таким образом, чтобы получить в X открытое подмножество, допускающее геометрический фактор, необходимо удалить подмногообразие $X \cap \mathbb{P}\mathfrak{N}_{G,V}$, где $\mathbb{P}\mathfrak{N}_{G,V}$ — образ множества $\mathfrak{N}_{G,V} \setminus \{0\}$ при каноническом морфизме $V \setminus \{0\} \to \mathbb{P}^n$.

В дальнейшем рядом математиков были даны различные модификации понятия стабильности и на основе этого получены новые яркие алгебро-геометрические приложения (например, к многообразиям модулей поверхностей общего типа, к векторным расслоениям на гладких проективных многообразиях и др.); см.: *Gieseker D.* — Proc. Intern. Congress Math., Helsinki, 1978, с. 525–528; *Богомолов Ф. А.* — Изв. АН СССР, сер. матем., 1978, т. 42, № 6, с. 1227–1287. Особая роль слоя $\mathfrak{N}_{G,V}$ и важность теории Гильберта — Мамфорда подтверждаются и многими современными исследованиями, посвященными проблемам собственно теории инвариантов; см., например, *Винберг Э. Б., Попов В. Л.* Теория инвариантов. — В кн.: Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 55. — М.: ВИНИТИ, 1989, с. 137–314, а также *Крафт Х.* Геометрические методы в теории инвариантов. — М.: Мир, 1987.

Что же касается исходной задачи о конструктивном доказательстве теоремы о конечной порожденности (или, иначе, о нахождении оценки M), то Гильберт сводит ее сначала к нахождению оценки сверху N на степени однородной системы параметров (в современной терминологии) алгебры инвариантов, а затем к «решению элементарной задачи из арифметической теории алгебраических функций», а точнее к методу Кронекера построения базиса целого замыкания конечно порожденной области целостности в конечном расширении ее поля частных. Он действительно получает оценку N, однако, ссылаясь на метод Кронекера, на самом деле комбинирует его со своей теоремой о базисе (см. примечания [16,17,72]), доказательство которой неконструктивно. Таким образом вопрос о явном нахождении M остается в неопределенном состоянии. Это обстоятельство было, по-видимому, причиной того, что авторы книги *Dieudonné F. A., Carrell F. B.* Invariant theory, old and new. — Acad. Press, 1971 (имеется перевод в кн.: *Дьедонне Ж., Кэррол Дж.*,

Мамфорд Д. Геометрическая теория инвариантов. — М.: Мир, 1974), излагая теорию Гильберта, изменили заключительную часть его общей стратегии и использовали вместо метода описания целых величин ссылку на теорему Гильберта о корнях. Их подход, однако, оказался ошибочным (см.: *Popov V. L.* — Astérisque, Soc. Math. de France, 1981, vol. 87–88, p. 303–334). Появление в 1974 г. нового важного результата Хохстера и Робертса об алгебрах инвариантов (см. примечание [47] к работе «О теории алгебраических форм») позволило избежать ссылки на метод Кронекера, см. *Popov V. L.*, loc. cit., и примечание [17]. Более того, константу M удалось найти в самой общей ситуации, т. е. для произвольной редуктивной алгебраической группы $G \subset GL(V)$ над алгебраически замкнутым полем k нулевой характеристики, естественно действующей на конечномерном векторном пространстве V. А именно, пусть $n = \dim V$, $s = \dim G$, $r = \operatorname{rk} G$, T — максимальный тор в G, $(k^*)^r \to T$ — фиксированный изоморфизм, заданный в координатах формулой $(t_1, \ldots, t_r) \mapsto (f_{ij}(t_1, \ldots, t_r))$, $f_{ij} \in k(t_1, \ldots, t_r)$. Пусть t — наибольшее из чисел $|m_l|$, взятое по всем l, $1 \leqslant l \leqslant r$, и всем одночленам $t_1^{m_1} \ldots t_r^{m_r}$, встречающимся хотя бы в одной из функций f_{ij}. Положим, далее, $C(h) = \text{НОК}\{a \in \mathbb{N} \mid 0 < a \leqslant h\}$ для любого $h > 0$. Тогда можно положить

(1) $M = |G|$, если группа G конечна;

(2) $M = nC(nt^s s!)$, если $G = T$ — тор;

(3) $M = nC\left(\dfrac{2^{r+s} n^{s+1} (n-1)^{s-r} t^r (s+1)!}{3^s (\left(\frac{s-r}{2}\right)!)^2}\right)$, если G связна и полупроста.

(Случай произвольной редуктивной группы G легко сводится к этим трем.)

Доказательство в случае (1) было дано еще Э. Нётер (*Noether E.* — Math. Ann., 1916, Bd. 7, S. 89–92). В случае (2) оно принадлежит Кемпфу (*Kempf G.* — Lect. Notes in Math., Springer-Verlag, vol. 1278, 1927, p. 81–94.), а в случае (3) — В. Л. Попову (*Popov V. L.*, loc. cit.).

[1] (с. 67). См. примечание [37] к работе «О теории алгебраических форм».

[2] (с. 67). А именно унимодулярной группы.

[3] (с. 68). Условие, что целая рациональная функция F от коэффициентов базисных форм сохраняется преобразованиями из унимодулярной группы, эквивалентно ввиду связности этой группы тому, что F аннулируется ее алгеброй Ли. Пусть $\Delta_1, \ldots, \Delta_s$ — образующие этой алгебры Ли. Они действуют как линейные дифференциальные операторы на алгебре всех целых рациональных функций от коэффициентов базисных форм. Поэтому функция F является инвариантом в точности в том случае, когда она является решением системы дифференциальных уравнений в частных производных $\Delta_1 F = \ldots = \Delta_s F = 0$. Для случая инвариантов одной базисной бинарной формы этот вопрос более подробно обсуждается в примечании [38] к работе «О теории алгебраических форм», где эти дифференциальные уравнения явно указаны (они имеют вид $HF = DF = 0$ и $HF = \Delta = 0$). Разумеется, все это очевидным образом переносится на инварианты любого представления любой связной алгебраической группы (или связной группы Ли).

[4] (с. 68). То есть, в современной терминологии, алгебра инвариантов алгебраически замкнута в алгебре всех многочленов от коэффициентов базисных форм. Это вытекает из связности унимодулярной группы (инварианты которой рассматривает Гильберт) и является частным случаем следующего простого общего утверждения: пусть V — конечномерное векторное пространство над алгебраически замкнутым полем k, G — связная алгебраическая подгруппа в группе $GL(V)$, $k[V]$ — алгебра полиномиальных функций на V и $k[V]^G$ — ее подалгебра G-инвариантов; тогда $k[V]^G$ алгебраически замкнута в $k[V]$. Действительно, пусть $f \in k[V]$ и $a_0 f^n + a_1 f^{n-1} + \ldots + a_n = 0$ для некоторых $a_i \in k[V]^G$. Для точки общего положения v в V все $a_i(v)$ отличны от нуля. Так как $a_i \in k[V]^G$, то все a_i постоянны на орбите Gv. Поэтому f

может принимать на Gv только конечное число значений (они должны быть корнями многочлена $a_0(v)t^n + a_1t^{n-1} + \ldots + a_n(v)$). Ввиду связности группы G орбита Gv является неприводимым алгебраическим многообразием, откуда следует, что f постоянна на Gv. Это и значит, что $f \in k[V]^G$.

[5] (с. 68). Это вытекает из связности унимодулярной группы и отсутствия у нее нетривиальных рациональных характеров. Вообще, пусть, в обозначениях примечания [4], группа G связна и не имеет нетривиальных рациональных характеров, и пусть $f \in k[V]^G$. Пусть $f = p_1 \cdot \ldots \cdot p_s$ — разложение на простые множители в факториальном кольце $k[V]$. Пусть $g \in G$. Тогда $gf = f = gp_1 \cdot \ldots \cdot gp_s$ — также разложение на простые множители. Ввиду связности G и факториальности $k[V]$ отсюда следует, что $gp_i = \lambda(g)p_i$, где $\lambda(g) \in k^*$. Поскольку отображение $G \to k^*$, $g \mapsto \lambda(g)$, является рациональным характером группы G, из условия на G следует, что $p_i \in k[V]^G$. Отсюда вытекает как свойство 4, так и то, что $k[V]^G$ — тоже факториальная алгебра.

[6] (с. 69). Это утверждение было затем обобщено Э. Нётер на неградуированный случай (*Noether E.* — Math. Ann., 1915, Bd. 76, S. 161–196); соответствующий результат относится к конечно порожденным целостным алгебрам над полем и называется теперь теоремой (или леммой) Э. Нётер о нормализации (см.: *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 2. — М.: ИЛ, 1963, и *Бурбаки Н.* Коммутативная алгебра. — М.: Мир, 1971). Сама Нётер в указанной работе рассматривает эту теорему, по-видимому, как незначительную модификацию утверждения Гильберта (*Noether E.*, loc. cit., подстрочное примечание на с. 184).

[7] (с. 69). Функции $f'_1, \ldots, f'_m$ алгебраически независимы в точности тогда, когда ранг матрицы $(\partial f'_i/\partial x_j)$ равен m, т. е. хотя бы один из ее миноров порядка m отличен от нуля (см.: *Ходж В., Пидо Д.* Методы алгебраической геометрии. Т. 1. — М.: ИЛ, 1954). Поэтому свойство функций быть алгебраически независимыми может быть проверено конструктивно, т. е. с помощью конечного числа явно осуществимых операций.

[8] (с. 69). Такую функцию G тоже можно найти конструктивно. А именно, будем последовательно рассматривать системы M_p, $p = 1, 2, \ldots$, всевозможных одночленов вида $f_1'^{s_1} \ldots f_m'^{s_m}$, $s_1 + \ldots + s_m = p$, и проверять линейную независимость элементов из M_p как функций от $x_1, \ldots, x_n$. Это сводится к вопросу о существовании ненулевого решения у соответствующей системы линейных уравнений, который, очевидно, может быть решен конструктивно. Ввиду алгебраической зависимости функций $f'_1, \ldots, f'_m$ через конечное число шагов будет найдено такое p, что система M_p линейно зависима. Решив соответствующую систему линейных уравнений, найдем явно коэффициенты $c_{s_1 \ldots s_m}$ этой линейной зависимости. Тогда

$$G(f'_1, \ldots, f'_m) = \sum c_{s_1 \ldots s_m} f_1'^{s_1} \ldots f_m'^{s_m}$$

[9] (с. 69). Это всегда можно сделать — и притом конструктивно, — если основное поле k бесконечно (Гильберт рассматривает случай, когда k — числовое поле, так что это условие выполнено), см. примечание [6] к работе «О теории алгебраических форм». Для конечного k такого преобразования может и не существовать (то же примечание). Тем не менее, теорема Нётер о нормализации (см. примечание [6]) может быть доказана и без каких-либо предположений о k (см.: *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 2, — М.; ИЛ, 1963).

[10] (с. 70). Это не совсем точно: указанные формулы имеют место только при $n \geqslant 3$ (в обоих случаях при $n = 1$ и $n = 2$ будет соответственно $\varkappa = 0$ и $\varkappa = 1$). Гильберт объясняет происхождение первой из них в § 10; скорее всего, и вторая была получена им аналогичными методами, т. е. по существу на основании того, что порядок в единице ряда Пуанкаре алгебры инвариантов равен степени трансцендентности $\varkappa$ этой алгебры (см. примечание [25] к работе «О теории алгебраических форм»).

В современной теории инвариантов подсчет числа $\varkappa$ осуществляется геометрическими методами на основе следующей теоремы Розенлихта (*Rosenlicht M.* — An. Bras. Cienc., 1963, vol. 35, p. 487–489). Пусть алгебраическая группа G действует на неприводимом алгебраическом многообразии X. Тогда степень трансцендентности поля инвариантных рациональных функций на X (над основным алгебраически замкнутым полем констант k) равна разности между размерностью многообразия X и размерностью G-орбиты точки общего положения в X (последняя равна максимуму размерностей G-орбит в X). Если X — конечномерное векторное пространство, а G — подгруппа в $GL(V)$, не имеющая нетривиальных рациональных характеров, то поле $k(V)^G$ инвариантных рациональных функций на V является полем частных алгебры $k[V]^G$ инвариантных целых рациональных функций (и потому степени трансцендентности $k(V)^G$ и $k[V]^G$ над k совпадают). Действительно, если $f = p/q \in k(V)^G$, где p и q — взаимно простые целые рациональные функции на V, то для любого $g \in G$ имеем $f = gf = gp/gq = p/q$, откуда ввиду факториальности алгебры целых рациональных функций на V следует, что $gp = \lambda(g)p$, $gq = \lambda(g)q$, где $\lambda(g) \in k$. Поскольку отображение $G \to k^*$, $g \mapsto \lambda(g)$, является рациональным характером, $\lambda(g) = 1$, т. е. $p, q \in k[V]^G$.

В классической ситуации, которую рассматривает Гильберт, G является унимодулярной группой (или произведением таких групп) и, значит, не имеет рациональных характеров. Это позволяет вычислить $\varkappa$ как разность между размерностью пространства V и размерностью G-орбиты точки общего положения v в V. Последняя же равна $\dim G - \dim G_v$, где $G_v = \{g \in G \mid gv = v\}$ — стабилизатор точки v. В настоящее время алгебра Ли группы G_v (а во многих случаях и сама G_v) явно описана для всех связных простых и неприводимых связных полупростых линейных групп G (см.: *Андреев Е. М., Винберг Э. Б., Элашвили А. Г.* — Функц. анализ и его прил., 1967, т. 1, вып. 4, с. 3–7; *Элашвили А. Г.* — Функц. анализ и его прил., 1972, т. 6, вып. 1, с. 51–62; 1972, т. 6, вып. 2, с. 65–78; *Андреев Е. М., Попов В. Л.* — Функц. анализ и его прил., 1971, т. 5, вып. 4, с. 1–8; *Попов А. М.* — Тр. ММО, 1985, т. 48, с. 7–59; 1987, т. 50, с. 209–248). Это позволяет найти $\varkappa$ во всех указанных случаях. Ситуация, когда $\dim G_v = 0$ и потому $\varkappa = \dim V - \dim G$, является при этом «типичной». Именно так и обстоит дело в том случае, который рассматривает Гильберт, т. е. когда V — пространство бинарных или тернарных форм степени n, а $G = SL_2$ или SL_3 соответственно: $\dim G_v = 0$ при $n \geqslant 3$ (и только тогда), откуда и следуют указанные в тексте формулы.

[11] (с. 70). Поле K всех рациональных инвариантов является конечным расширением поля частных L алгебры A, порожденной $J_1, \ldots, J_\varkappa$ над полем констант. По теореме о примитивном элементе $K = L(J)$ для некоторого рационального инварианта J, который можно считать целым над A (см., например, *Ленг С.* Алгебра. — М.: Мир, 1968, с. 269). Но тогда J — целый рациональный инвариант (см. соответствующее рассуждение в настоящей работе двумя абзацами ниже). Гильберт указывает ниже явный способ построения такого J.

[12] (с. 71). Таким образом, поле инвариантов — это, в терминологии комментариев к статье «О теории алгебраических форм», поле G-инвариантных рациональных функций на V. Оно является полем частных алгебры, порожденной инвариантами $J, J_1, \ldots, J_\varkappa$ над полем констант, а его «целые алгебраические функции» — это по определению элементы, целые над алгеброй B, порожденной $J_1, \ldots, J_\varkappa$. Целое замыкание алгебры B в поле инвариантов совпадает с алгеброй всех инвариантов.

[13] (с. 71). Это прообраз следующего общего утверждения современной коммутативной алгебры. Пусть A — конечно порожденная целостная алгебра над полем k и L — конечное расширение ее поля частных. Тогда целое замыкание алгебры A в L является A-модулем конечного типа (см.: *Бурбаки Н.* Коммутативная алгебра. — М.; Мир, 1971, с. 414).

[14] (с. 71). То есть минимального многочлена для J над полем, порожденным инвариантами $J_1, \ldots, J_\varkappa$. Поскольку J цел над алгеброй, порожденной $J_1, \ldots, J_\varkappa$, коэффициенты этого многочлена лежат в указанной алгебре (см.: *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 1. — М.; ИЛ, 1963).

[15] (с. 71). Здесь $\Gamma_1, \ldots, \Gamma_k$, D — многочлены от $J_1, \ldots, J_\varkappa$. Современное доказательство этого утверждения см., например, в книге *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 1. — М.; ИЛ, 1963, теорема 7 § 4 гл. V.

[16] (с. 72). По существу здесь Гильберт имеет в виду следующее. Рассматриваются такие наборы $(\Gamma_1, \ldots, \Gamma_k)$ элементов Γ_i из алгебры A, порожденной $J_1, \ldots, J_\varkappa$, что $(\Gamma_1 J^{k-1} + \ldots + \Gamma_k)/D$ — целый рациональный инвариант. Система всех таких наборов (которую Гильберт называет рядом, Reihe) образует подмодуль N свободного A-модуля A^k. Ввиду нётеровости A этот подмодуль конечно порожден (относительно доказательства этого факта Гильберт отсылает к теореме I своей работы «О теории алгебраических форм», однако собственно теорема I — это по существу теорема о нётеровости кольца многочленов над полем, так что для получения необходимого доказательства требуются, помимо нее, и еще некоторые рассуждения; они приведены в доказательстве последнего предложения в разд. I цитированной работы). Если теперь $(\Gamma_1^{(s)}, \ldots, \Gamma_k^{(s)})$, $s = 1, \ldots, M$, — образующие A-модуля N, то следует взять $j_s = (\Gamma_1^{(s)} J^{k-1} + \ldots + \Gamma_k^{(s)})/D$.

[17] (с. 72). Такое построение, однако, опирается на теорему I из работы «О теории алгебраических форм», а потому не является конструктивным (см. примечание [3] к цитированной работе). Лишь сравнительно недавно выяснилось, что, привлекая вместо теоремы Кронекера и теоремы I фундаментальную теорему Хохстера и Робертса (*Hochster M., Roberts J.* — Adv. Math., 1974, vol. 13, p. 125–175), можно избежать в этом месте неконструктивных рассуждений: было доказано, что $j_1, \ldots, j_M$ можно выбрать из инвариантов степени не более $R = \deg J_1 + \ldots + \deg J_\varkappa$ (например, взять в качестве $j_1, \ldots, j_M$ базис пространства инвариантов степени $\leqslant R$, который, как известно, может быть найден конструктивно. (см.: *Popov V. L.* — Astérisque, Soc. Math. de France, 1981, vol. 87–88, p. 303–334).

[18] (с. 72). Имеются в виду значения в поле $\mathbb{C}$ комплексных чисел.

[19] (с. 72). В действительности, как видно из доказательства, F, F', F'', ... может быть произвольным множеством функций (а не обязательно последовательностью), обращающихся в нуль там же, где и все $f_1, \ldots, f_m$. В наше время этот результат называется теоремой Гильберта о нулях (или о корнях). Она играет фундаментальную роль в современной коммутативной алгебре и алгебраической геометрии. Эта теорема стимулировала исследования по общей теории идеалов: например, именно она побудила Ласкера ввести общее понятие примарного идеала в кольцах $\mathbb{C}[x_1, \ldots, x_n]$ и $\mathbb{Z}[x_1, \ldots, x_n]$ (см. «Исторический очерк» в книге *Бурбаки Н.* Коммутативная алгебра. — М.: Мир, 1971).

[20] (с. 73). Гильберт понимает под нулем такой набор $(\alpha_1, \ldots, \alpha_n)$ значений переменных, что не все α_i равны нулю и все $f_j(\alpha_1, \ldots, \alpha_n)$ равны нулю.

[21] (с. 74). Сделав предварительно подходящую линейную невырожденную замену переменных, можно с самого начала считать, что все α_i отличны от нуля.

[22] (с. 75). См. примечание [20].

[23] (с. 76). Иначе говоря, если K — поле рациональных функций от переменного t (с коэффициентами из заданного числового поля k), то эта система совместна над K. Доказательство получается с помощью теоремы Кронекера — Капелли. А именно, предположим, что это не так. Тогда ранг r матрицы $A = \begin{pmatrix} c_{11} \ldots c_{1p} \\ \ldots\ldots\ldots \\ c_{q1} \ldots c_{qp} \end{pmatrix}$ меньше ранга s матрицы $B = \begin{pmatrix} c_{11} \ldots c_{1p}\, c_1 \\ \ldots\ldots\ldots\ldots \\ c_{q1} \ldots c_{qp}\, c_q \end{pmatrix}$. Пусть Δ_A и Δ_B — ненулевые миноры

матриц A и B порядков r и s соответственно. Так как они являются многочленами от t с коэффициентами в k, а k — бесконечное поле, то найдется $\alpha \in k$, такое, что $\Delta_A(\alpha) \neq 0$ и $\Delta_B(\alpha) \neq 0$. Это означает, что при подстановке $t = \alpha$ указанная система превращается в несовместную систему над k. Тем самым получено противоречие.

[24] (с. 76). То есть на самом деле F, F', F'', ... — произвольное бесконечное множество форм (не обязательно последовательность).

[25] (с. 76). Коэффициенты этой линейной комбинации являются многочленами от переменных $x_1, \ldots, x_n$ с коэффициентами из основного поля констант.

[26] (с. 76). В действительности это утверждение эквивалентно только что доказанной теореме. Точнее, верно и обратное: если r-я степень каждой из форм F, F', F'', ... лежит в $(f_1, \ldots, f_m)$, то найдется такое натуральное число d, что произведение любых d из этих форм лежит в $(f_1, \ldots, f_m)$ (доказательство легко следует из теоремы Гильберта о базисе, примененной к множеству F, F', F'', ...).

[27] (с. 76). О предпосылках возникновения теоремы Гильберта о нулях см. «Исторический очерк» в книге *Бурбаки Н.* Коммутативная алгебра. — М.: Мир, 1971.

[28] (с. 77). С современных позиций речь идет о применении к равенству $i = a'_1 I_1 + \ldots + a'_\mu I_\mu$ оператора Рейнольдса (см. примечание [47] к работе «О теории алгебраических форм»; в обозначениях этого примечания $\overline{a'_s} = i_s$). Гильберт, не располагавший тогда этим общим средством, пользуется в указанной работе Ω-процессом Кэли.

[29] (с. 77). Таким образом, показано, что алгебра A всех инвариантов является модулем конечного типа (с образующими $j_1, \ldots, j_w$) над подалгеброй B, порожденной $I_1, \ldots, I_\mu$. Известное общее рассуждение, не имеющее отношения к специфике теории инвариантов, показывает тогда, что A цела над B (см., например, *Зарисский О., Самюэль П.* Коммутативная алгебра. Т. 1. — М.; ИЛ, 1963); это рассуждение Гильберт и приводит ниже.

[30] (с. 78). Имеется в виду проективное пространство.

[31] (с. 78). Действительно, степень трансцендентности алгебры инвариантов A равна $\varkappa$, но, с другой стороны, она равна степени трансцендентности алгебры B, порожденной $I_1, \ldots, I_\mu$ (так как A цела над B), и, значит, не превышает μ.

[32] (с. 78). Это утверждение непосредственно следует из описания многообразия нуль-форм, полученного в § 17–19. (В терминах примечания [62] пространство L одномерно, Δ состоит из точек n, $n-2$, $n-4$, ..., $-n$, а соответствующие весовые подпространства одномерны и натянуты соответственно на x_1^n, $x_1^{n-1}x_2$, $x_1^{n-2}x_2^2, \ldots, x_2^n$. Поэтому множество канонических точек является объединением двух линейных подпространств — линейной оболочки множества одночленов $\{x_1^{n-i}x_2^i \mid 0 \leqslant i \leqslant h\}$ и линейной оболочки множества одночленов $\{x_1^{n-i}x_2^i \mid h < i \leqslant n\}$. Эти подпространства переводятся одно в другое преобразованием из SL_2, и ясно, что их «разнесение» с помощью SL_2 — это в точности многообразие всех бинарных форм, имеющих линейный множитель кратности $\geqslant h+1$.)

[33] (с. 78). Пусть p и q — бинарные формы от x_1, x_2 степеней d и e соответственно. Согласно классическому определению, величина $(p,q)_i = \frac{(d-i)!}{d!}\frac{(e-i)!}{e!}\sum_{k=0}^{i}(-1)^k \frac{\partial^i p}{\partial x_1^{i-k}\partial x_2^k}\frac{\partial^i q}{\partial x_1^k \partial x_2^{i-k}}$ называется i-м трансвектантом форм p и q. Отображение $(p,q) \mapsto (p,q)_i$ является GL_2-эквивариантным морфизмом $R_p \times R_q \to R_{p+q-2i}$, где R_s есть GL_2-модуль бинарных форм степени s от x_1, x_2. В этих обозначениях с точностью до множителя $F_i = (f,f)_{2i}$.

[34] (с. 79). Тот факт, что $J_1, \ldots, J_\mu$ — инварианты, имеет место, поскольку F_1, $F_2, \ldots$ — трансвектанты.

[35] (с. 80). См. примечание [35] к работе «О теории алгебраических форм».

[36] (с. 80). Точное описание всех упоминаемых в этом параграфе инвариантов см., например, в книге *Grace J. H., Young A.* The algebra of invariants. — Cambr. Univ. Press, 1903.

[37] (с. 81). Смысл обозначения $(p, q)_i$ см. в примечании [33].

[38] (с. 85). Над подполем, порожденным $J_1, \ldots, J_\varkappa$.

[39] (с. 85). То есть линейно независимых над полем констант.

[40] (с. 85). См. примечание [15].

[41] (с. 85). Первое из следующих ниже неравенств вытекает из алгебраической независимости $J_1, \ldots, J_\varkappa$ и того, что для *любых* многочленов $\Delta_1, \ldots, \Delta_k$ от $J_1, \ldots, J_\varkappa$ сумма $\Delta_1 J^{k-1} + \Delta_2 J^{k-2} + \ldots + \Delta_k$ будет инвариантом. Второе же следует из того, что для *некоторых* многочленов $\Gamma_1, \ldots, \Gamma_k$ от $J_1, \ldots, J_\varkappa$ выражение $(\Gamma_1 J^{k-1} + \ldots + \Gamma_k)/D$ будет инвариантом и в таком виде может быть записан — при соответствующем выборе $\Gamma_1, \ldots, \Gamma_k$ — любой инвариант.

[42] (с. 85). Гильберт использует обозначение $\underset{\sigma=\infty}{L}$, соответствующее современной записи $\lim\limits_{\sigma\to\infty}$.

[43] (с. 90). О «типичном представлении» см., например, *Grace J. H., Young A.*, The algebra of Invariants. — Cambr. Univ. Press, 1903. Речь идет о том, чтобы для общей бинарной базисной формы $f(x_1, x_2) = a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \ldots + a_n x_2^n$ найти такую невырожденную линейную замену переменных $x_1 \mapsto A_{11}x_1 + A_{12}x_2$, $x_2 \mapsto A_{21}x_1 + A_{22}x_2$, где A_{ij} — рациональные функции от $a_0, a_1, \ldots, a_n$, чтобы у получающейся после этой замены бинарной формы $f'(x_1, x_2) = a_0' x_1^n + \binom{n}{1} a_1' x_1^{n-1} x_2 + \ldots + a_n' x_2^n$ все коэффициенты a_i' были рациональными инвариантами формы f. Для нахождения такой замены разработан ряд приемов. Например, если n четно, то за $A_{11}x_1 + A_{12}x_2$ и $A_{21}x_1 + A_{22}x_2$ можно взять (loc. cit.) два коварианта формы f (линейные по x_1, x_2), линейно независимые над полем инвариантов. С современной точки зрения роль рациональных инвариантов a_i' состоит в том, что они позволяют разделять SL_2-орбиты общего положения в пространстве бинарных форм степени n (см. ниже примечание [45]).

[44] (с. 91). См. примечание [39].

[45] (с. 92). На самом деле с определителем, равным 1. Таким образом, смысл предложения, доказанного Клебшем, заключается в том, что SL_2-орбиты общего положения в пространстве бинарных форм степени n разделяются рациональными SL_2-инвариантами. Этот результат следует рассматривать как прототип общей теоремы Розенлихта, указанной в примечании [10].

[46] (с. 92). То есть общее многообразие уровня инвариантов $J_1, \ldots, J_\varkappa$ состоит из k орбит группы SL_2. Это утверждение обобщается на произвольные связные полупростые алгебраические группы G над алгебраически замкнутым полем l, линейно действующие на векторном пространстве V. А именно, пусть $l[V]^G$ — алгебра всех полиномиальных G-инвариантных функций на V и $I_1, \ldots, I_s$ — система ее параметров, т. е. такой набор ее однородных алгебраически независимых элементов, что $l[V]^G$ цела над $l[I_1, \ldots, I_s]$ (такой набор всегда существует по теореме Нётер о нормализации). Будучи конечно порожденными, алгебры $l[V]^G$ и $l[I_1, \ldots, I_s]$ являются алгебрами регулярных функций на некоторых аффинных алгебраических многообразиях; обозначим их соответственно через $V/\!/G$ и X. Пусть $l[V]$ — алгебра полиномиальных функций на V. Вложения $l[V] \supset l[V]^G \supset l[I_1, \ldots, I_s]$ определяют морфизмы $\pi\colon V \to V/\!/G$, $\alpha\colon V \to X$ и $\beta\colon V/\!/G \to X$, причем $\alpha = \beta \circ \pi$. Из того что G — полупростая группа, следует, что поле частных алгебры $l[V]^G$ совпадает с полем $l(V)^G$ рациональных G-инвариантных функций на V (см. примечание [10]). Поэтому слой морфизма β над точкой общего положения в X является конечным множеством, состоящим из r точек, где r — степень поля $l(V)^G$ над подполем, порожденным

$I_1, \ldots, I_s$. Предположим, что стабилизатор точки общего положения в V редуктивен (это условие выполнено в том случае, который рассматривает Гильберт, т. е. когда $G = SL_2$, а V — пространство бинарных форм степени $n \geqslant 2$). Тогда слой морфизма π над точкой общего положения в $V/\!\!/G$ является G-орбитой (см.: *Попов В. Л.* — Изв. АН СССР, сер. мат., 1970, т. 34, № 3, с. 523–531). Отсюда следует, что слой морфизма α над точкой общего положения в X (т. е. общее многообразие уровня инвариантов $I_1, \ldots, I_s$) состоит из r орбит.

[47] (с. 93). А именно, грассманова многообразия 2-мерных линейных подпространств в ν-мерном линейном пространстве, вложенного в соответствующее проективное пространство с помощью плюккеровых координат.

[48] (с. 95). В современных терминах смысл конструкции и основного результата § 12 сводится к следующему. Рассматривается естественное действие группы $G = GL_3(\mathbb{C})$ на пространстве V тернарных форм степени n. Пусть Gf — орбита формы f, $\overline{Gf}$ — замыкание Gf в V (в топологии Зарисского или, что в данном случае одно и то же, в комплексной топологии) и $\varphi\colon G \to \overline{Gf}$ — морфизм, заданный формулой $\varphi(g) = gf$. Пусть, далее, $\mathbb{C}[G]$ и $\mathbb{C}[\overline{Gf}]$ — алгебры регулярных функций на аффинных многообразиях G и $\overline{Gf}$ соответственно. Тогда $\mathbb{C}[G] = \mathbb{C}[\alpha_{11}, \ldots, \alpha_{33}]$, а φ^* осуществляет вложение $\mathbb{C}[\overline{Gf}]$ в $\mathbb{C}[G]$ и $\varphi^*\mathbb{C}[\overline{Gf}] = \mathbb{C}[b_1, \ldots, b_N]$. Основной результат § 12 состоит в том, что функция $\delta \in \mathbb{C}[G]$ цела над алгеброй $\varphi^*\mathbb{C}[\overline{Gf}]$ тогда и только тогда, когда хотя бы один из непостоянных однородных SL_3-инвариантных полиномов на V не обращается в точке f в нуль. В дальнейшем будет доказано, что это, в свою очередь, эквивалентно тому, что SL_3-орбита формы f не содержит в своем замыкании нуля пространства V.

[49] (с. 96). Это следует из того, что, в обозначениях примечания [48], степень трансцендентности алгебры $\mathbb{C}[G]$ равна $\dim G = 9$.

[50] (с. 97). С современной точки зрения смысл этого утверждения и предыдущих рассуждений данного параграфа состоит в следующем. Воспользуемся обозначениями примечания [48]. Поскольку φ^* — вложение, степень трансцендентности r алгебры $\mathbb{C}[b_1, \ldots, b_N]$ равна степени трансцендентности алгебры $\mathbb{C}[\overline{Gf}]$ и, значит, равна $\dim \overline{Gf}$. Но орбита Gf является плотным открытым по Зарисскому подмножеством в $\overline{Gf}$ и потому $r = \dim Gf$. Известно, однако, что $\dim Gf = \dim G - \dim G_f$, где $G_f = \{g \in G \mid gf = f\}$ — стабилизатор формы f. Поскольку G_f — алгебраическая группа, она либо конечна, либо «непрерывна» (т. е. $\dim G_f \geqslant 1$). Следовательно, $r < 9$ в точности тогда, когда G_f «непрерывна».

[51] (с. 98). В силу неприводимости этого предыдущего уравнения.

[52] (с. 98). То есть выяснить, является ли δ целой функцией над $\mathbb{C}[b_1, \ldots, b_N]$.

[53] (с. 99). Если инвариант J имеет степень g, то его вес равен $ng/3$. В самом деле, рассмотрим подстановку $g = \operatorname{diag}(\lambda, \lambda, \lambda)$. Она умножает каждый коэффициент $a_{n_1 n_2 n_3}$ базисной формы на $\lambda^{n_1+n_2+n_3} = \lambda^n$, а значит, переводит J в $\lambda^{ng}J$. Но по определению веса должно быть $\lambda^{ng} = (\det g)^p$, и, поскольку $\det g = \lambda^3$, это дает $p = ng/3$. Таким образом, если $p \leqslant 9n(3n+1)^8$, то $g \leqslant 27(3n+1)^8$.

[54] (с. 99). В современной теории инвариантов такие формы называются неполустабильными (см.: *Mumford D.*, Geometric Invariant Theory. — Ergebn. der Math. und ihrer Grenzg., Bd. 34, Springer-Verlag, 1965; имеется неполный перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974).

[55] (с. 99). Действительно, в этом разделе найдена явная оценка сверху на веса (а потому и на степени) инвариантов $J_1, \ldots, J_\varkappa$. Задача же нахождения базиса в пространстве инвариантов степени не выше заданной может быть решена конструктивно, поскольку сводится к решению соответствующих дифференциальных уравнений, см. примечание [3]. Наконец, выделение из этого базиса системы

$J_1, \ldots, J_\varkappa$ осуществляется указанными в § 1 методами, т. е. тоже конструктивно (см. примечания [7–9]).

[56] (с. 100, 101, 103–105). А точнее, неотрицательным.

[57] (с. 100). Приводимое ниже доказательство использует аналитические соображения — рассмотрение ветвей некоторых алгебраических функций и их продолжений вдоль соответствующих путей на плоскости комплексного переменного. Современное доказательство, использующее лишь методы коммутативной алгебры (и пригодное для любого поля констант нулевой характеристики), см. в гл. 4 книги *Dieudonné J. A., Carrell J. B.*, Invariant Theory. Old and New. — Academic Press, 1971 (имеется перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974).

[58] (с. 103). И Ω.

[59] (с. 103). В действительности верно следующее более общее утверждение: для любой квадратной $(n \times n)$-матрицы $A = (a_{ij})$, коэффициенты a_{ij} которой лежат в поле $k((t))$ формальных степенных рядов (Лорана) от переменной t с коэффициентами в поле k, существуют такие две унимодулярные $(n \times n)$-матрицы B и C с коэффициентами из кольца $k[[t]]$ формальных степенных рядов (Тейлора), что $BAC = \operatorname{diag}(t^{\lambda_1}, \ldots, t^{\lambda_n})$, $\lambda_i \in \mathbb{Z}$. Доказательство основывается на том, что элементарные преобразования строк (столбцов) любой матрицы осуществляются с помощью умножений этой матрицы слева (справа) на матрицу соответствующего элементарного преобразования. Поэтому достаточно показать, что A может быть приведена к виду $\operatorname{diag}(t^{\lambda_1}, \ldots, t^{\lambda_n})$, $\lambda_i \in \mathbb{Z}$, с помощью элементарных преобразований строк и столбцов, матрицы которых имеют лежащие в $k[[t]]$ коэффициенты. Это делается так. Положим $a_{ij} = t^{n_{ij}} b_{ij}$, где $b_{ij} \in k[[t]]$ и $b_{ij} \neq 0$ (это равносильно тому, что $1/b_{ij} \in k[[t]]$). Переставляя местами строки и столбцы, можно добиться того, чтобы $n_{11} = \min\limits_{i,j} n_{ij}$. Заменим теперь i-ю строку $(i = 2, 3, \ldots, n)$ на нее же плюс первая строка, умноженная на $-t^{n_{i1}-n_{11}} b_{i1}/b_{11} \in k[[t]]$. После этого аналогично поступим со столбцами. Наконец, умножая первый столбец полученной матрицы на $1/b_{11} \in k[[t]]$, мы получим матрицу вида $\begin{pmatrix} t^{n_{11}} & 0 \\ 0 & A' \end{pmatrix}$. После этого процедура повторяется с матрицей A' и т. д., и в результате получится матрица вида $\operatorname{diag}(t^{\lambda_1}, \ldots, t^{\lambda_n})$, $\lambda_i \in \mathbb{Z}$.

Матрицу $\operatorname{diag}(t^{\lambda_1}, \ldots, t^{\lambda_n})$ (как точку группы GL_n со значениями в $k((t))$) можно отождествить с гомоморфизмом $t \mapsto \operatorname{diag}(t^{\lambda_1}, \ldots, t^{\lambda_n})$ одномерной мультипликативной группы $\mathbb{G}_m$ в группу GL_n; такой гомоморфизм называется также (полупростой) однопараметрической подгруппой (о. п.) в GL_n. С учетом этого указанный результат допускает важное обобщение на любые редуктивные алгебраические группы G над полем k, принадлежащее Ивахори и Мацумото (*Iwahori N., Matsumoto M.* — Publ. Math. IHES, no. 25, 1965): каждый двойной смежный класс группы $k((t))$-точек группы G по подгруппе $k[[t]]$-точек группы G содержит некоторую о. п. группы G. С помощью этой теоремы Мамфорд (*Mumford D.*, Geometric Invariant Theory. — Ergebn. der Math. und ihrer Grenzg., Bd. 34, Springer-Verlag, 1965; имеется неполный перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974) перенес развитую здесь Гильбертом теорию нуль-форм на случай линейных действий произвольных редуктивных алгебраических групп, а именно, распространил на общий случай понятие «канонической нуль-формы», см. § 17.

[60] (с. 106). Как показано в § 18, в этом определении можно, не ограничивая общности, заменить условие «их сумма отрицательна» на «их сумма равна нулю». В этом случае $\varphi(t) = \operatorname{diag}(t^{\lambda_1}, t^{\lambda_2}, t^{\lambda_3})$ — о. п. группы SL_3 (см. примечание [59]), а условие на коэффициенты $a_{n_1 n_2 n_3}$ равносильно тому, что $\lim\limits_{t \to 0} \varphi(t) f = 0$ (это означает,

что морфизм $\mathbb{A}^1 \setminus \{0\} \to V$, $t \mapsto \varphi(t)f$, продолжается до морфизма $\mathbb{A}^1 \to V$, переводящего нуль в нуль). Последнее равносильно тому, что орбита f относительно группы $\{\varphi(t) \mid t \in \mathbb{C}^*\}$ содержит в своем замыкании нуль.

[61] (с. 106). С учетом примечания [60] этот результат переформулируется так: все непостоянные однородные инварианты группы $G = SL_3$ обращаются в нуль на форме f в точности в том случае, когда найдется такая диагональная о. п. $\varphi\colon \mathbb{G}_m \to SL_3$, $\varphi(t) = \operatorname{diag}(t^{\lambda_1}, t^{\lambda_2}, t^{\lambda_3})$ (см. примечание [59]), и такая форма f', лежащая в G-орбите формы f, что $\lim\limits_{t\to 0}\varphi(t)f' = 0$. Отсюда, между прочим, вытекает следующая важная характеризация нуль-форм: f является нуль-формой в точности в том случае, когда G-орбита этой формы содержит в своем замыкании нуль. (Это утверждение, впрочем, может быть доказано и без использования предыдущих результатов. А именно, достаточность очевидна, а необходимость доказывается следующим образом. Пусть 0 не лежит в замыкании G-орбиты формы f. Тогда найдется полиномиальная функция F, равная 0 на замыкании этой орбиты и 1 на форме 0. Применяя к F оператор Рейнольдса (см. примечание [47] к работе «О теории алгебраических форм»), мы получим инвариант $\overline{F}$ с теми же свойствами. Значит, $1 - \overline{F}$ — ненулевой инвариант, равный нулю на форме 0 и единице на форме f. Поэтому одна из однородных компонент инварианта $1 - \overline{F}$ отлична от нуля на f и, значит, f — не нуль-форма).

Как показал Мамфорд (*Mumford D.*, Geometric Invariant Theory. — Ergebn. der Math. und ihrer Grenzg., Bd. 34, Springer-Verlag, 1965; имеется неполный перевод в кн.: *Дьедонне Ж., Кэррол Дж., Мамфорд Д.* Геометрическая теория инвариантов. — М.: Мир, 1974), эти утверждения переносятся на любые редуктивные алгебраические группы G над алгебраически замкнутым полем k, линейно действующие на конечномерных векторных пространствах V. А именно, точка $v \in V$ называется неполустабильной, если любой непостоянный однородный G-инвариантный многочлен f на V обращается в v в нуль (это — аналог нуль-формы). Пусть $\mathfrak{N}_{G,V}$ — (алгебраическое) многообразие всех неполустабильных точек. Тогда точка $v \in V$ лежит в $\mathfrak{N}_{G,V}$ в том и только том случае, когда существует такая о. п. $\varphi\colon \mathbb{G}_m \to G$, что $\lim\limits_{t\to 0}\varphi(t)v = 0$. Мамфорд доказал эту теорему (называемую сейчас теоремой Гильберта — Мамфорда), опираясь на глубокий результат Ивахори и Мацумото (см. примечание [59]), а в остальном следуя по существу схеме рассуждений Гильберта. В настоящее время известно более простое доказательство при $k = \mathbb{C}$, не использующее результатов о $k((t))$-точках алгебраических групп; оно принадлежит Ричардсону и опирается на разложение Картана группы G (см.: *Винберг Э. Б., Попов В. Л.* Теория инвариантов. — В кн.: Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 55. — М.: ВИНИТИ, 1989, с. 137–314, и *Крафт Х.* Геометрические методы в теории инвариантов. — М.: Мир, 1987; оригинальное доказательство Ричардсона было опубликовано в статье *Birkes D.* — Ann. of Math., 1971, vol. 93, № 3, p. 459–475). В действительности нетривиальная часть теоремы Гильберта — Мамфорда (необходимость) допускает следующее обобщение. Пусть G действует на аффинном алгебраическом многообразии X и $x \in X$ — некоторая точка, а Y — замкнутое G-инвариантное подмножество в замыкании $\overline{Gx}$ орбиты Gx в X. Тогда найдется такая о. п. $\varphi\colon \mathbb{G}_m \to G$, что $\lim\limits_{t\to 0}\varphi(t)x \in Y$. При $k = \mathbb{C}$ доказательство было дано Ричардсоном (см.: *Birkes D.*, loc. cit.; *Винберг Э. Б., Попов В. Л.*, loc. cit.); алгебраическое доказательство над алгебраически замкнутым полем k нулевой характеристики получается комбинацией теоремы Гильберта — Мамфорда и одного из следствий теоремы Луны о слайсе (*Luna D.* — Bull. Soc. Math. France., 1973, vol. 33, p. 81–105).

Теорема Гильберта — Мамфорда позволяет перенести на общую ситуацию действия G на V и понятие канонической нуль-формы. А именно, зафиксируем в G

какой-либо максимальный алгебраический тор T. Точку $u \in V$ назовем канонической, если найдется такая о. п. (см. примечание [59]) $\varphi\colon \mathbb{G}_m \to T$, что $\lim\limits_{t\to 0} \varphi(t)u = 0$ (мы приходим к определению Гильберта, если $G = SL_3$, V — пространство тернарных форм степени n, а T состоит из диагональных матриц). Из теоремы Гильберта — Мамфорда, примененной к действию T на V, следует, что точка $v \in V$ будет канонической в точности тогда, когда замыкание $\overline{Tv}$ орбиты Tv в V содержит нуль (это, впрочем, нетрудно доказать и непосредственно). Поскольку всякий тор в G сопряжен подгруппе группы T, мы получаем обобщение утверждения Гильберта: каждая неполустабильная точка в V содержит в своей G-орбите каноническую точку. Это можно выразить и так: пусть $\mathfrak{N}_{T,V}$ — многообразие неполустабильных точек для действия T на V; тогда $\mathfrak{N}_{T,V}$ — это многообразие канонических точек для действия G на V, а $\mathfrak{N}_{G,V} = G \cdot \mathfrak{N}_{T,V}$. Многообразие $\mathfrak{N}_{T,V}$ устроено совсем просто — оно является объединением конечного числа линейных подпространств в V (см. примечание [62]). Это позволяет исследовать геометрические свойства многообразия $\mathfrak{N}_{G,V}$ (см. примечания [65] и [66]).

[62] (с. 108). Это описание канонических нуль-форм следующим образом переносится на произвольные редуктивные алгебраические группы G, линейно действующие на векторных пространствах V. Сохраним обозначения примечания [61]. Пусть $\mathfrak{X} = \mathrm{Hom}(T, \mathbb{G}_m)$ — группа рациональных характеров тора T в аддитивной записи, а $\Delta \subset \mathfrak{X}$ — система весов тора T на V и V_λ — весовое подпространство веса $\lambda \in \Delta$. Отождествим $\mathfrak{X}$ с решеткой в векторном пространстве $L = \mathfrak{X} \otimes_{\mathbf{Z}} \mathbb{R}$. Для любой ненулевой линейной формы $f \in L^*$ на L положим $\Delta(f) = \{\lambda \in \Delta \mid f(\lambda) > 0\}$ и рассмотрим в V линейное подпространство $V(f) = \bigoplus\limits_{\lambda \in \Delta(f)} V_\lambda$. Оно состоит из канонических точек (см. примечание [61]), а все многообразие $\mathfrak{N}_{T,V}$ канонических точек является объединением всевозможных линейных подпространств $V(f)$, $f \in L^* \setminus \{0\}$ (ясно, что имеется лишь конечное число различных таких подпространств). Геометрические рассмотрения Гильберта из этого параграфа интерпретируются на этом языке так. В качестве T взят тор в SL_3, состоящий из диагональных матриц. Плоскость, которую рассматривает Гильберт, — это L, а целочисленные точки (вершины) координатного треугольника — это веса естественного представления тора T в пространстве тернарных форм порядка n (при этом M — это нуль пространства L). Весовые пространства в этом случае все одномерны и натянуты на одночлены $x_1^{n_1}x_2^{n_2}x_3^{n_3}$, $n_1 + n_2 + n_3 = n$. Рассмотрение таких систем весов λ, что $f(\lambda) > 0$ для фиксированной линейной формы $f \in L^* \setminus \{0\}$ — это то же самое, что рассмотрение вершин координатного треугольника, лежащих строго по одну сторону от некоторой прямой в L, проходящей через M (а именно, от прямой $f^{-1}(0)$). Совершенно аналогично интерпретируются и геометрические построения из § 19.

[63] (с. 108). С точки зрения сказанного в примечании [62] системы весов $\Delta(f_1)$ и $\Delta(f_2)$, где $f_1, f_2 \in L^* \setminus \{0\}$, «существенно различны», если $\Delta(f_1)$ не переводится в $\Delta(f_2)$ преобразованием из группы Вейля.

[64] (с. 108). То есть можно игнорировать такие $f \in L^* \setminus \{0\}$, что $\Delta(f) \subset \Delta(h)$ для некоторой формы $h \in L^* \setminus \{0\}$ (обозначения см. в примечании [62]).

[65] (с. 111). Как следует из сказанного в примечаниях [61] и [62], каждая неприводимая компонента этого многообразия $\mathfrak{N}_{G,V}$ получается «разнесением» с помощью группы G некоторого линейного подпространства, а точнее, имеет (в обозначениях примечания [62]) вид $G \cdot V(f)$ для подходящей линейной функции $f \in L^* \setminus \{0\}$. Можно показать, что множество $G \cdot V(f)$ замкнуто в V (см. *Винберг Э. Б., Попов В. Л.*, loc. cit., *Крафт Х.*, loc. cit. (примечание [61])). Следует отметить, однако, что число неприводимых компонент многообразия $\mathfrak{N}_{G,V}$, вообще говоря, меньше числа неприводимых компонент многообразия $\mathfrak{N}_{T,V}$. Например, для дей-

ствия группы SL_2 в пространстве бинарных форм заданной степени многообразие $\mathfrak{N}_{G,V}$ неприводимо, а многообразие $\mathfrak{N}_{T,V}$ состоит из двух неприводимых компонент, см. примечание [32].

66 (с. 111). Это не вполне очевидно и аккуратное обоснование требует развития некоторой теории. Рассмотрим (в обозначениях примечания [61]) какую-либо неприводимую компоненту $G \cdot V(f)$ многообразия $\mathfrak{N}_{G,V}$ (см. примечание [62]). Пусть $P = \{g \in G \mid gV(f) \subseteq V(f)\}$; это — параболическая подгруппа в G. Рассмотрим однородное векторное алгебраическое расслоение $G *_P V(f)$ над G/P со слоем $V(f)$. Можно доказать, что оно локально тривиально в топологии Зарисского (нужно воспользоваться результатами Серра из работы *Serre J.-P.* — Séminaire C. Chevalley, E. N. S., 1958, p. 1-01–1-37, и тем, что ввиду разложения Брюа G/P содержит открытое подмножество, изоморфное аффинному пространству). Следовательно, $G *_P V(f)$ — рациональное многообразие. Развивая подход Гильберта, Кемпф (*Kempf G. R.* — Ann. of Math., 1978, vol. 108, p. 299–316), Хесселинк (*Hesselink W.H.* — Invent. Math., 1979, vol. 55, p. 141–163), Руссо (*Rousseau G.* — C. R. Acad. Sci. Paris, 1978, vol. 286, A, p. 247–250) и Ф. А. Богомолов (Изв. АН СССР, сер. матем., 1978, т. 42, № 6, с. 1227–1287) независимо пришли к идее исследовать те однопараметрические подгруппы $\mathbb{G}_m \to G$, которые в некотором смысле «наиболее быстро подгоняют» данную неполустабильную точку к нулю. Из их результатов следует, что при соответствующем выборе f естественный морфизм $\varphi: G *_P V(f) \to G \cdot V(f)$ является бирациональным изоморфизмом и поэтому $G \cdot V(f)$ — рациональное многообразие (а φ — разрешение его особенностей). Более того, в $V(f)$ существует такое P-инвариантное открытое подмножество $V(f)^\circ$, что φ осуществляет G-изоморфизм однородного расслоения $G *_P V(f)^\circ$ над G/P со слоем $V(f)^\circ$ и открытого подмножества $G \cdot V(f)^\circ$ в $G \cdot V(f)$. В действительности рассмотрение «оптимальных» однопараметрических подгрупп позволяет доказать, что все многообразие $\mathfrak{N}_{G,V}$ допускает конечную G-инвариантную стратификацию, каждый страт которой является гладким рациональным многообразием вида $G *_Q W^\circ$, где Q — параболическая подгруппа в G, W — конечномерный Q-модуль, а W° — его открытое Q-инвариантное подмножество (см.: *Hesselink W.*, loc. cit; *Kirwan F.* Cohomology of quotients in symplectic and algebraic geometry. — Math. Notes, Princeton Univ. Press, vol. 31, 1984; *Ness L.* Amer. J. Math., vol. 106, 1984, p. 1281–1329, а также *Винберг Э. Б., Попов В. Л.*, loc. cit. (примечание [61])). В действительности вся система стратов целиком определяется только геометрическим взаиморасположением системы весов (с кратностями) группы G в пространстве V и системы корней группы G, что позволяет описать страты с помощью простого конечного алгоритма; см.: *Popov V. L.* Sections in invariant theory. — In: Proc. of the Sophus Lie Memorial Conference, Oslo, 1992, Scandinavian Univ. Press, 1994, p. 315–362.

Утверждая (без доказательства), что многообразие $G \cdot V(f)$ рационально, Гильберт, по-видимому, подразумевал какое-то соображение, аккуратное оформление которого на современном уровне строгости явилось бы некоторым эквивалентом рассуждений, приведенных выше.

67 (с. 111). Они получаются с помощью тех же рассуждений, что и в примечании [53], если в качестве g взять подстановки $\mathrm{diag}(\lambda, 1, 1)$, $\mathrm{diag}(1, \lambda, 1)$ и $\mathrm{diag}(1, 1, \lambda)$ соответственно для первого, второго и третьего уравнений.

68 (с. 112). Это число может быть явно указано.

69 (с. 113). Речь идет о функциях, введенных в § 12.

70 (с. 113). При условии, что $n \geqslant 3$, а базисная форма, относительно которой строятся все b_i, является формой общего положения; см. § 13 и примечания [10] и [50].

71 (с. 113). Согласно теореме о примитивном элементе.

72 (с. 113). Здесь Гильберт, как и раньше, имеет, по-видимому, в виду упоми-

навшийся в § 2 результат Кронекера. Этот результат, однако, приходится комбинировать с теоремой Гильберта о базисе, доказательство которой неконструктивно; см. примечания [16] и [17] и заключительные абзацы § 2.

[73] (с. 114). См. примечание [72].

В. Л. Попов

О ДИОФАНТОВЫХ УРАВНЕНИЯХ РОДА НУЛЬ

Работа Д. Гильберта и А. Гурвица имеет долгую предысторию. Наиболее простой класс уравнений рода нуль, а именно, уравнения второй степени, определяющие конические сечения на плоскости, был рассмотрен Диофантом Александрийским (II–III вв. от Р. Х.). В своей знаменитой книге «Арифметика» (имеется перевод в кн.: *Диофант Александрийский.* Арифметика и книга о многоугольных числах. Перевод Веселовского И. Н. под ред. Башмаковой И. Г. — М.: Наука, 1974) он показал, что уравнение $F_2(x, y) = 0$, где $F_2(x, y)$ — неприводимый над $\mathbb{Q}$ многочлен второй степени, либо вовсе не имеет рациональных решений, либо, если у него есть одно рациональное решение (x_0, y_0), то оно имеет и бесконечно много таких решений (x, y), причем $x = \varphi(t), y = \psi(t)$, где φ и ψ — рациональные функции с коэффициентами из поля $\mathbb{Q}$. Диофант рассмотрел также уравнения вида $y^2 = F_3(x, y)$ и $y^3 = F_3(x, y)$, где $F_3(x, y)$ — многочлен третьей степени, которые определяют, вообще говоря, кривые рода 1. Для нахождения рациональных решений таких уравнений он ввел новые методы, которые получили в XIX в. название метода касательной и метода секущей (эти методы позволяют строить новые рациональные решения, если известно одно или два таких решения). В XVI–XVII вв. методы Диофанта были восприняты Р. Бомбелли, Ф. Виетом и П. Ферма, в работах которых они получили дальнейшее развитие (большей частью для уравнений степени 3 и 4, и рода 1; более подробно см.: *Башмакова И. Г., Славутин Е. И.* История диофантова анализа от Диофанта до Ферма. — М.: Наука, 1984; *Ферма П.* Исследования по теории чисел и диофантову анализу. — М.: Наука, 1992).

Леонард Эйлер (1707–1783) в своей книге «Vollständige Anleitung zur Algebra» (1770) впервые сформулировал, в чем состоит отличие уравнений второй степени от уравнений степени 3: у первых можно задать сразу «все» рациональные решения, а у вторых это сделать, вообще говоря, нельзя. У уравнения третьей степени можно лишь найти по одному или двум рациональным решениям еще одно новое решение. За всем этим стоит, конечно, различие рода этих кривых. Это понятие было введено Н. Г. Абелем (1802–1829) и затем, другим способом Б. Риманом (1826–1866) в 1856–57 гг. Идеи Абеля и Римана получили дальнейшее развитие в работах А. Клебша. Его мемуар «Über die Anwendung der Abelschen Functionen in der Geometrie» (*Clebsch A.* — J. reine und angew. Math., 1863, Bd. 63, S. 189–243) означал, по мнению И. Р. Шафаревича (*Schafarevich I. R.* — Math. Ann., 1983, Bd. 266, S. 135–140), рождение алгебраической геометрии. В частности, в работах Клебша было введено фундаментальное понятие однозначного преобразования (у Гильберта и Гурвица оно встречается как рациональное однозначно обратимое преобразование) алгебраических кривых и сформулирована основная задача об изучении свойств алгебраических кривых с точностью до таких преобразований. Теперь мы называем эти преобразования бирациональными. Клебш определил род кривой чисто геометрически, через степень и число двойных точек. Он доказал инвариантность рода относительно однозначных преобразований и показал, что над полем $\mathbb{C}$ кривая рода нуль параметризуется рациональными функциями. Ученик Клебша М. Нётер получил эти результаты над полем определения рассматриваемой кривой (как говорили тогда, при помощи одних только рациональных операций). С изложения его работы и начинается исследование Гильберта и Гурвица.

Результаты работы Гильберта и Гурвица можно сформулировать следующим образом. Любая плоская кривая рода 0 и степени (порядка) n бирационально эквивалентна над полем $\mathbb{Q}$ кривой степени $n-2$. Отсюда следует, что при нечетном n кривая рода 0 бирационально эквивалентна прямой, а при четном n — коническому сечению. Из этого вытекает основная теорема: на алгебраической кривой рода 0 и степени n либо совсем нет рациональных точек, либо лежит конечное их число (это те точки, которые «теряются» при бирациональном преобразовании исходной кривой к коническому сечению или прямой), либо существует бесконечное число рациональных точек. В последнем случае координаты почти всех рациональных точек выражаются в виде рациональных функций параметра. При этом, если n нечетно, то возможен только последний случай. Итак, для кривых рода нуль все сводится к тем случаям, которые были рассмотрены Диофантом в его «Арифметике».

И. Г. Башмакова

Соединяя теорему Гильберта — Гурвица с теоремой Минковского — Хассе о квадратичных формах мы получаем алгоритм для описания рациональных точек на алгебраических кривых рода нуль и определенных над любым полем алгебраических чисел. Это обстоятельство (для поля $\mathbb{Q}$) отмечено в работе (см. обсуждение уравнения (13) на стр. 120 с использованием частного случая теоремы Минковского — Хассе, принадлежащего Лежандру). Ни для какого другого класса алгебраических многообразий такой алгоритм не известен и его нахождение, скажем для кривых рода 1 (или кривых рода $\geqslant 1$), представляет собой нерешенную задачу диофантовой геометрии.

Ситуация, рассмотренная Гильбертом и Гурвицем, относится к случаю рациональных многообразий (многообразий бирационально изоморфных проективному пространству) размерности 1. Чтобы обрисовать ситуацию для многообразий размерности $\geqslant 1$ рассмотрим следующие множества неособых алгебраических многообразий размерности n и определенных над полем k характеристики 0:

многообразия, бирационально изоморфные $\mathbb{P}_n$ над k;

многообразия, бирационально изоморфные $\mathbb{P}_n$ над алгебраическим замыканием $\bar{k}$ поля k;

многообразия , для которых имеется конечное рациональное сюръективное отображение $f : \mathbb{P}_n \to X$, определенное над полем k (унирациональные над k многообразия);

многообразия с аналогичным отображением, определенным над $\bar{k}$;

многообразия с обильным антиканоническим классом $-K_X$ (многообразия Фано).

Для случая кривой все эти множества совпадают, причем последнее условие и означает, что род g равен нулю (степень K_X равна $2g-2$). Для более высоких размерностей это уже далеко не так, что приводит к значительно более сложному строению множества рациональных точек. Случай алгебраических поверхностей изучался в 60-е гг. в цикле работ Ю. И. Манина и В. А. Исковских (см.: *Манин Ю. И.* Кубические формы. — М.: Наука, 1972). Резкое различие приведенных выше классов многообразий видно уже на примере неособых кубических поверхностей X. Они являются многообразиями Фано и даже бирационально изоморфны $\mathbb{P}_2$ над $\bar{k}$. Тем не менее над $k = \mathbb{Q}$ не существует (кроме исключительных случаев) таких рациональных отображений $f : \mathbb{P}_2 \to X$, что множество $X(\mathbb{Q})$ описывается параметризацией f. Переход к конечному набору отображений f не спасает положения. Таким образом мы получаем бесконечно много рациональных точек, но далеко не все. Интересно, что операция Диофанта построения новых точек из известных двух, встречающаяся в размерности 1 для многообразий совсем другого типа ($g = 1$, т. е. $K_X = 0$), имеет аналог для кубических поверхностей. Это приводит к наличию неассоциативного группового закона на множестве (некоторых классов)

рациональных точек на таких поверхностях. Соответствующая теория была построена Ю. И. Маниным, на основе идеи И. Р. Шафаревича (см.: *Манин Ю. И.*, loc. cit.; *Манин Ю. И., Цфасман М. А.* — УМН, 1986, т. 41, с. 43–94). Также аналог теоремы Минковского — Хассе не верен в классе кубических поверхностей: наличие рациональной точки над всеми локальными пополнениями основного поля не влечет наличие рациональной точки над основным полем (см.: *Châtelet F.* — L'Ens. Math., 1959, vol. 5, p. 153–170).

В случае кривых X рода g различия между непустыми множествами рациональных точек можно описать асимптотикой числа $N(X, k, H)$ точек $P \in X(k)$, имеющих ограниченную высоту $H(P) \leqslant H$ (относительно дивизора степени 1 на кривой X). Здесь и далее k — конечное расширение поля $\mathbb{Q}$. Имеем (константы везде положительны):

$N(X, k, H) \sim \text{const}\, H^2$, если $g = 0$ (см.: *Schanuel S.* — Bull. Soc. Math. France, 1979, vol. 107, p. 433–449);

$N(X, k, H) \sim \text{const}(\log H)^{r/2}$, если $g = 1$ и X — эллиптическая кривая ранга r (см.: *Neron A.* — Ann. of Math., 1985, vol. 82, p. 249–331);

$N(X, k, H) \sim \text{const}$, если $g > 1$ (см.: *Faltings G.* — Inv. Math., 1983, vol. 73, p. 349–366).

Для размерности $n > 1$ ситуация не очень ясна. Если $X = \mathbb{P}_n$, то Шануэль (*Schanuel S.*, loc. cit.) нашел оценку, аналогичную оценке для $\mathbb{P}_1$, с заменой 2 на $n+1$. Оценка Нерона верна для абелевых многообразий любой размерности. Наконец, В. В. Батырев и Ю. И. Манин предложили ряд гипотез для роста функции $N(X, k, H)$ (см.: *Batyrev V. V., Manin Yu. I.* — Math. Ann., 1990, Bd. 286, S. 27–43; *Manin Yu. I.* — Compos. Math., 1993, vol. 85, p. 37–55). Наиболее доступной оказалась гипотеза о росте для неособых многообразий Фано X: существует такое открытое по Зарисскому подмножество $U \subset X$, что для всех достаточно больших расширений k' основного поля $N(U, k', H) \sim \text{const}\, H(\log H)^{r-1}$, где r — ранг группы Пикара многообразия X (см.: *Manin Yu. I.*, loc. cit.). Здесь рассматривается высота относительно дивизора $-K_X$. Эта гипотеза была доказана для многообразий вида G/P, где P — параболическая подгруппа редуктивной группы G (см.: *Franke J., Manin Yu. I., Tschinkel Yu.* — Inv. Math., 1989, vol. 95, p. 421–435), торических многообразий (см.: *Batyrev V. V., Tschinkel Yu.* — Preprint IHES, Novembre 1995; J. Alg. Geom. (in print)) и ряда других случаев. Недавно, однако, был построен пример неособого многообразия Фано, для которого функция $N(X, k, H)$ растет существенно быстрее, чем утверждается в рассматриваемой гипотезе (см.: *Batyrev V. V., Tschinkel Yu.* — C. R. Acad. Sci., Paris, Ser. I, 1996, vol. 323, p. 41–46). Интересный обзор этого круга вопросов приведен в работе: *Sylverman J. H.* Counting integer and rational points on varieties. — Columbia University Number Theory Seminar, N. Y., 1992. — Asterisque, 1995, vol. 228, p. 223–236.

А. Н. Паршин

О ДИОФАНТОВЫХ УРАВНЕНИЯХ

Результат, доказанный Гильбертом в этой заметке связан с задачей диофантовой геометрии, появившейся много позднее. В 1962 г. И. Р. Шафаревич предположил, что не существует алгебраических кривых над полем $\mathbb{Q}$, имеющих всюду хорошую редукцию (см.: *Шафаревич И. Р.* — Proc. Intern. Congr. Math., Stockholm, 1962, p. 163–176). Справедливость этого была показана независимо В. А. Абрашкиным (см.: *Абрашкин В. А.* — ДАН СССР, 1985, т. 283, с. 1289–1294; Изв. АН СССР, сер. мат., 1987, т. 51, с. 691–736) и Ж.-М. Фонтеном (*Fontaine J.-M.* — Inv. Math., 1985, vol. 81, p. 515–538) с помощью весьма нетривиальной теории конечных групповых схем. Для случая эллиптических кривых элементарное доказательство было

получено самим Шафаревичем (*Шафаревич И. Р.*, loc. cit.). Его удалось обобщить на случай кривых рода 2 (Волынский А. Б., не опубликовано). Были также найдены все эллиптические кривые над $\mathbb{Q}$, имеющие плохую редукцию лишь в 2 (см.: *Шафаревич И. Р.*, loc. cit.; *Ogg A. P.* — J. reine und angew. Math., 1967, Bd. 226, S. 204–215). Эти результаты имеют следующее отношение к теореме Гильберта: наличие нетривиальных решений уравнения $D = \pm 1$ немедленно дает гиперэллиптическую кривую $y^2 = x_0t^n + x_1t^{n-1} + \ldots + x_n$ (относительно переменных y, t), имеющую над $\mathbb{Q}$ хорошую редукцию по всем простым числам, кроме 2. Все вместе эти результаты представляют собой далеко идущие обобщения теоремы Минковского о несуществовании нетривиальных неразветвленных расширений поля $\mathbb{Q}$. Было бы интересно получить такими элементарными соображениями гипотезу Шафаревича хотя бы для какого-то класса алгебраических кривых.

Имеющиеся в конце работы замечания дают примеры рациональных особых кривых, для которых неверен принцип Хассе.

А. Н. Паршин

О НЕПРИВОДИМОСТИ МНОГОЧЛЕНОВ С ЦЕЛОЧИСЛЕННЫМИ КОЭФФИЦИЕНТАМИ

В своем простейшем виде теорема неприводимости Гильберта утверждает, что если $f(x, y)$ неприводимый многочлен от переменных x и y с коэффициентами из поля рациональных чисел $\mathbb{Q}$, то существует бесконечно много значений $x' \in \mathbb{Q}$ переменной x, для которых многочлен $f(x', y)$ неприводим в кольце $\mathbb{Q}[y]$. В наиболее общей постановке задача заключается в следующем. Пусть K — некоторое поле и $f_1(x_1, \ldots, x_r, y_1, \ldots, y_s), \ldots, f_l(x_1, \ldots, x_r, y_1, \ldots, y_s)$ — многочлены с коэффициентами из K, которые неприводимы как многочлены от $r+s$ переменных $x_1, \ldots, x_r, y_1, \ldots, y_s$. Вопрос состоит в том, существуют ли значения $\underline{x'} = (x'_1, \ldots, x'_r)$ переменных $x_1, \ldots, x_r$, в поле K, для которых каждый из многочленов $f_i(\underline{x}, \underline{y}) = f_i(x_1, \ldots, x_r, y_1, \ldots, y_s)$, $1 \leqslant i \leqslant l$, неприводим в кольце $K[\underline{y}] = K[y_1, \ldots, y_s]$. Множество $H_K(f)$ всех таких значений $x' = (x'_1, \ldots, x'_r)$ называется *гильбертовым множеством* системы многочленов $\underline{f} = (f_1, \ldots, f_l)$ в поле K относительно переменных $x_1, \ldots, x_r$. Аналогичным образом определяется гильбертово множество $H_R(f)$ для произвольного подмножества R в поле K. При этом поле K называется *гильбертовым*, если множества $H_K(\underline{f})$ бесконечны для каждой конечной системы $\underline{f} = (f_1, \ldots, f_l)$ неприводимых многочленов $f_1(x_1, \ldots, x_r, y_1, \ldots, y_s), \ldots, f_l(x_1, \ldots, x_r, y_1, \ldots, y_s)$. Нетрудно показать (см. работу Д. Гильберта, а также *Ленг С.* Основы диофантовой геометрии. — М.: Мир, 1986, гл. 9), что вопрос об изучении гильбертовых множеств $H_K(f)$ для случая системы многочленов $\underline{f} = (f_1, \ldots, f_l)$ от нескольких переменных $x_1, \ldots, x_r, y_1, \ldots, y_s$ в определенной степени редуцируется к аналогичному вопросу для одного многочлена $f(x, y)$ с двумя переменными x и y. Ввиду этого все дальнейшее развитие тематики, связанной с теоремой неприводимости Гильберта, касалось, в основном, последнего частного случая.

Первый значительный шаг в направлении усиления результата Гильберта был сделан Дёрге (*Dörge K.* — Math. Ann., 1927, Bd. 96, S. 176–182), установившим, что гильбертово множество $H_{\mathbb{Q}}(f)$ всякого неприводимого многочлена $f \in \mathbb{Z}[x, y]$ с разных точек зрения весьма обширно (например, $H_{\mathbb{Q}}(f)$ содержит «почти все» целые числа, его элементы лежат плотно в $\mathbb{Q}$ как в обычной, так и во всех p-адических топологиях). В 1929 году Зигель (*Siegel C.L.* — Abh. Preuss. Akad. Wiss. Phys. Math. Kl., 1929, Bd. 1, S. 14–67) обнаружил замечательную связь между теоремой неприводимости Гильберта и своей теоремой о конечности числа целых точек на кривой рода $g \geqslant 1$. Шинцель (*Schinzel A.* — Ann. Polon. Math., vol. 1965, № 16,

p. 333–340) установил, что множество $H_{\mathbb{Z}}(f)$ содержит арифметическую прогрессию, зависящую от многочлена $f(x, y)$.

Доказательство теоремы неприводимости, найденное самим Гильбертом, не эффективно в том смысле, что не дает возможности явным образом указать какие-либо элементы множества $H_{\mathbb{Q}}(f)$. Тем же самым недостатком обладает доказательство Зигеля и упомянутые выше результаты Дёрге и Шинцеля. Лишь сравнительно недавно Фриду (*Fried M.* — J. Number Theory, 1974, vol. 6, p. 211–231) и Коэну (*Cohen S. D.* — Proc. London Math. Soc. (3), 1981, vol. 43, № 2, p 227–250) удалось эффективизировать результат А. Шинцеля, указав явные границы для начального члена и разности арифметической прогрессии, лежащей в $H_{\mathbb{Z}}(f)$. Этими же авторами показано, что при $N > c_0(f)$ на отрезке $[1, N]$ имеется не более $c(f)\sqrt{N}$ исключительных целых чисел x', для которых многочлен $f(x', y)$ приводим в $\mathbb{Q}[y]$ (здесь $c_0(f)$, $c(f)$ — эффективно вычислимые постоянные, зависящие лишь от степени и коэффициентов многочлена $f(x, y)$). С. А. Степеновым показано, что для широкого класса многочленов $f \in \mathbb{Z}[x, y]$ множество $H_{\mathbb{Z}}(f)$ содержит не менее $c'x/\log x$ множеств H_p (соответствующих простым числам $p \leqslant x$), каждое из которых является объединением по меньшей мере $c''p$ различных арифметических прогрессий $a + pt$, $0 \leqslant a \leqslant p - 1$ с разностью p (не опубликовано). Здесь c' и c'' — эффективно вычисляемые положительные константы, зависящие лишь от степени n и многочлена $f(x, y)$ по переменному y. Все эти результаты без труда переносятся на конечные расширения K поля рациональных чисел $\mathbb{Q}$.

Первым вопросом, возникающим при попытке распространить указанные выше результаты с поля $\mathbb{Q}$ на другие поля, является вопрос о том, какие из них будут гильбертовыми. Заметим сразу же, что каждое гильбертово поле с необходимостью должно быть бесконечным. С помощью простейших фактов из теории Галуа нетрудно установить, что всякое конечное сепарабельное расширение гильбертова поля K снова является гильбертовым полем. Аналогичный результат справедлив и для чисто несепарабельных расширений гильбертова поля K (см.: *Inaba E.* — Jap. J. Math., 1944, vol. 19, p. 1–25). Кроме того, каждое поле конечного типа над своим простым подполем (степени трансцендентности $\geqslant 1$ в случае положительной характеристики) гильбертово (см.: *Ленг С.*, loc. cit.). Как недавно установил Вейссауер (*Weissauer R.* Hilbertsche Körper. — Thesis Heidelberg, 1980; см. также *Fried M.* — Israel J. of Math., 1985, vol. 51, № 4, p. 347–363) гильбертовость поля K сохраняется и для некоторых бесконечных алгебраических расширений. В частности, им показано, что гильбертовым является всякое поле L, в котором справедлива формула произведения

$$\prod_{\mathfrak{N}} |\alpha|_{\mathfrak{N}} = 1, \quad 0 \neq \alpha \in L,$$

распространенного на все простые дивизоры (классы эквивалентных между собой нормирований) этого поля.

Новый этап в развитии идей Гильберта связан с открытием существования в произвольном гильбертовом поле K (см.: *Gilmore P. C., Robinson A.* — Canad. J. Math., 1995, vol. 7, p. 483–489) *универсальных гильбертовых множеств* (множеств $H \subset K$, содержащихся с точностью до некоторых своих конечных подмножеств в каждом гильбертовом множестве $H_K(f)$ поля K). Явная конструкция универсального гильбертова множества $H \subset K$, где K — конечное расширение поля $\mathbb{Q}$, впервые была осуществлена В. Г. Спринджуком (*Спринджук В. Г.* — Труды МИАН СССР, 1981, т. 158, с. 180–196; J. reine und angew. Math., 1983, Bd. 340, S. 26–52), показавшим, в частности, что если f — произвольный неприводимый многочлен из кольца $\mathbb{Z}[x, y]$ и

$$x_n = [\exp \sqrt{\log \log n}] + n!2^{n^2}, \quad n = 1, 2, \ldots,$$

то многочлен $f(x_n, y)$ неприводим в кольце $\mathbb{Q}[y]$ для всех $n \geqslant n_0(f)$, где константа

$n_0(f)$ эффективно вычислима по коэффициентам и степени многочлена $f(x,y)$ (см. также *Fried M.*, loc. cit.). Более густая универсальная гильбертова последовательность

$$x_n = 2^n p_n, \quad n = 1, 2, \ldots,$$

где p_n — простое число с номером n, была построена затем Ясумото (*Yasumoto M.* — J. Number Theory, 1987, vol. 26, p. 274–285). Метод этой работы, основанной на использовании нестандартной версии (см.: *Robinson A., Roquette P.* — J. Number Theory, 1975, vol. 7, p. 121–176) теоремы Зигеля о целых точках на кривой, не позволяет, однако, эффективным образом определить те исключительные значения x_n, для которых многочлен $f(x_n, y)$ может оказаться приводимым в кольце $\mathbb{Q}[y]$.

С. А. Степанов

Теорема Гильберта о неприводимости имеет интересные применения в теории Галуа и диофантовой геометрии. Одним из наиболее трудных вопросов теории Галуа является построение нормальных расширений поля рациональных чисел $\mathbb{Q}$ с заданной конечной группой Галуа G (обратная задача теории Галуа). Теорема неприводимости дает возможность строить такие расширения, если имеется расширение функционального поля $\mathbb{Q}(x_1, \ldots, x_n)$ с группой Галуа G. С другой стороны, легко построить расширения поля $\mathbb{C}(x_1, \ldots, x_n)$ с заданной конечной группой Галуа G. Для этого нужно учесть, что конечные расширения такого поля отвечают конечным накрытиям аффинного пространства $\mathbb{C}^n$ (или соответствующего проективного пространства), разветвленным над некоторым замкнутым подмногообразием $X \subset \mathbb{C}^n$. Пользуясь явным видом фундаментальной группы $\pi_1(\mathbb{C}^n \setminus X)$, получаем требуемый результат. Основная проблема состоит в том, чтобы «спустить» поле определения построенного накрытия с $\mathbb{C}$ до $\mathbb{Q}$. Это приходится делать для каждой группы G (или какого-то класса групп) своим способом. В настоящее время известен только критерий спуска к полю $\mathbb{R}$. Он состоит в том, что группа должна порождаться элементами порядка 2 (см.: *Debes P., Fried M.* — Acta Arithm., 1990, vol. 56, p. 291–323). В своей работе Гильберт дает решение обратной задачи для $G = S_n$ и $G = A_n$. В дальнейшем этот подход развивался в работах Э. Нётер (*Noether E.* — Math. Ann. 1918, Bd. 78, S. 221–229) и К.-И. Ши (*Shih K.-Y.* — Math. Ann., 1974, Bd. 207, S. 99–120). Последний существенно упростил доказательство Гильберта и добавил к его списку группу $PSL(2, \mathbb{Z}/p)$, где $p \not\equiv \pm 1, \bmod 24$. Расширения, имеющие группой Галуа группу Вейля типа E_6 построил Т. Шиода (*Shioda T.* — Proc. ICM Kyoto–90, vol. 1. — Springer-Verlag, 1991, p. 473–489; Algebra and Analysis, Proc. Intern. Chebotarev conference. — Berlin: de Gruyter, 1996, p. 109–114).

Существенный прогресс в этой области произошел в связи с работами Г. В. Белого (Изв. АН СССР, сер. матем., 1979, т. 43, с. 267–276; J. reine und angew. Math., 1983, Bd. 341, S. 147–156). Он рассмотрел накрытия проективной прямой, разветвленные в трех точках, и выделил класс конечных групп (с двумя образующими), который всегда можно реализовать как группы Галуа таких накрытий, определенных над абелевыми расширениями поля $\mathbb{Q}$, т. е. над круговыми полями. Это дало решение обратной задачи теории Галуа для простых классических групп Шевалле типа A_l, ${}^2A_l$, B_l, C_l, D_l, ${}^2D_l$ (с элементами из конечного поля $\mathbb{F}_q$, $q \neq 2$) над круговыми полями. Впоследствии этот метод был развит и для других классов групп (например, групп Матье) и привел к нетривиальным результатам даже над $\mathbb{Q}$. Так Дж. Томпсон показал, что Монстр (самая большая спорадическая простая группа) может быть реализована как группа Галуа над $\mathbb{Q}$ (*Thompson J. G.* — J. Algebra, 1984, vol. 89, p. 437–499). По поводу других результатов в этом направлении (и истории вопроса) см.: *Чеботарев Н. Г.* Теория Галуа. — М.–Л.: ОНТИ, 1936; *Serre J.-P.* Groupes de Galois sur $\mathbb{Q}$. — Séminaire Bourbaki. Vol. 1987–88,

exp. 689. — Astérisque, 1988, vol. 161, 162, p. 73–85; *Matzat B. H.* Konstruktive Galoistheorie. — Lect. Notes in Math., 1987, vol. 1284. — Springer-Verlag, 1987; *Serre J.-P.* Topics in Galois theory. — Boston–London: 1992; Recent developments in the inverse Galois problem (ed. M. Fried and oth.). — Contemporary Math., vol. 186. — Providence, R. I.: AMS, 1995; *Völklein H.* Groups as Galois groups (an introducrion). — Cambr. Univ. Press, 1996.

По мнению Д. К. Фаддеева (Труды МИАН, 1984, т. 168, с. 49) это «дает веские основания для гипотезы о том, что для поля рациональных чисел и полей алгебраических чисел конечной степени обратная задача должна иметь положительное решение». Заметим, что эта задача решена положительно для разрешимых групп (см.: *Шафаревич И. Р.* — Изв. АН СССР, сер. матем., 1954, т. 18, с. 525–578).

Теорема неприводимости нашла также применения к изучению рациональных точек на алгебраических многообразиях, определенных над полями алгебраических чисел. Основной результат состоит в теоремах специализации, сравнивающих множество рациональных точек на общем слое семейства алгебраических многообразий $f : X \to Y$ с множеством рациональных точек на замкнутых слоях $f^{-1}(y), y \in Y$. Определено отображение специализации (из общего слоя в замкнутый слой) и для гильбертова (и, следовательно, непустого) множества точек $y \in Y$ отображение специализации инъективно (см.: *Ленг С.* Основы диофантовой геометрии. — М., Мир, 1986). С помощью этого метода А. Нерон (*Neron A.* — Bull. Soc. Math. France, 1952, vol. 80, p. 101–166) построил эллиптические кривые C над $\mathbb{Q}$, для которых ранг группы $C(\mathbb{Q})$ не меньше 10, а также абелевы многообразия размерности n над $\mathbb{Q}$, ранг которых не меньше $3n + 6$. Дальнейшие результаты об эллиптических кривых большого ранга над $\mathbb{Q}$ получены в работах: *Fried M.* — Trans. Amer. Math. Soc., 1984, vol. 281, № 2; *Mestre J. F.* — C. R. Acad. Sci. Paris, 1982, vol. 295, 643–644; Compos. Math., 1986, vol. 58, p. 209–232. Отметим еще, что инъективность отображения специализации часто имеет место для гораздо большего множества точек y, чем это следует из теоремы Гильберта. Для некоторых семейств, это верно для всех y, кроме конечного числа (см.: *Sylverman J.* — J. reine und angew. Math., 1983, Bd. 342, S. 197–211; Duke Math. J., 1984, vol. 51, p. 395–403). Эффективные доказательства теоремы неприводимости использовались для получения эффективных оценок некоторых классов рациональных точек на алгебраических кривых произвольного рода (см.: *Спринджук В. Г.* Классические диофантовы уравнения от двух неизвестных. — М.: Наука, 1982). Обзор различных применений теоремы неприводимости дан в докладе: *Debes P.* — Séminaire de Théorie des Nombres. Paris, 1985–86. — Boston–Basel: Birkhäuser, 1987, p. 19–38.

А. Н. Паршин

[1] (с. 146). В современной терминологии $\mathfrak{A}$ — примитивный элемент расширения.

О ТРАНСЦЕНДЕНТНОСТИ ЧИСЕЛ e И π

Трансцендентность числа e была доказана в 1873 г. Эрмитом (C. R. Acad. Sci., 1873, vol. 77, pp. 18–24, 74–79, 226–233, 285), а трансцендентность числа π — в 1882 г. Линдеманом (Math. Ann., 1882, Bd. 20, S. 213–225), т. е. соответственно за 20 и 11 лет до выхода статьи Гильберта. Таким образом, его работа дает лишь вариант (правда, один из самых коротких) доказательства. Между опубликованием работ Эрмита и Гильберта, т. е. между 1873 и 1893 гг. было опубликовано около 10 других доказательств. Публикации продолжались и после 1893 г. Подробный перечень таких работ можно найти в кн.: *Koksma J. F.* Diophantische Approximationen. — Berlin, 1936. Обширная информация содержится и в кн.: *Mahler K.* Lectures on Transcendental Numbers. — Lect. Notes Math., v. 546, 1976.

Более слабые теоремы об иррациональности чисел e и π были доказаны на век раньше, в 1770 г., Ламбертом (его работа воспроизведена в книге *Рудио Ф.* О квадратуре круга. — М., 1936). Впрочем, иррациональность e следует из найденного еще Эйлером разложения в цепную дробь числа $(e-1)/2$.

Общая теорема Линдемана, упоминаемая в конце работы Гильберта, формулируется так следующим образом.

Если $\alpha_1, \ldots, \alpha_n$ — алгебраические числа, отличные от нуля, а $\beta_1, \ldots, \beta_n$ — попарно различные алгебраические числа, то $\alpha_1 e^{\beta_1} + \ldots + \alpha_n e^{\beta_n} \neq 0$.

В этой теореме содержатся в частности, утверждение о трансцендентности числа e ($n = 2, \alpha_1 = \beta_1 = 1, \beta_2 = 0$) и более общее утверждение о трансцендентности чисел e^α при алгебраических $\alpha \neq 0$ ($n = 2, \alpha_1 = 1, \beta_1 = \alpha, \beta_2 = 0$). Отсюда вытекает и трансцендентность и всех отличных от нуля натуральных логарифмов алгебраических чисел и, в частности, числа πi, являющегося одним из логарифмов алгебраического числа -1, а значит и числа π. В общей теореме Линдемана содержится и утверждение о трансцендентности значений в алгебраических точках тригонометрических и обратных тригонометрических функций (за очевидными исключениями).

Доказательство трансцендентности числа π позволило «закрыть» древнюю проблему о квадратуре круга, так как для возможности построения с помощью циркуля и линейки квадрата, имеющего ту же площадь, что и заданный круг, необходимо, чтобы π было алгебраическим числом специального вида.

Во многих работах выводились оценки снизу для мер иррациональности и трансцендентности указанных выше чисел, т. е. неравенства типа

$$|q\theta - p| \geqslant \varphi(q), \qquad p \in \mathbb{Z}, \quad q \in \mathbb{N},$$

$$|P(\theta)| \geqslant \Phi(n, H), \quad P(z) = a_n z^n + \ldots + a_0 \in \mathbb{Z}[z], \quad H = \max_{0 \leqslant j \leqslant n} |a_j| > 0.$$

Первая из таких работ опубликована в 1899 г. Борелем (C. R. Acad. Sci., 1899, vol. 128, p. 596–599).

Фельдман Н. И.

Утверждение о трансцендентности $\ln \alpha$ при алгебраических $\alpha \neq 0$ (одна из возможных формулировок теоремы Линдемана) имеет простую геометрическую интерпретацию. Она, очевидно, эквивалентна утверждению о трансцендентности площади сегмента, отсекаемого от гиперболы $y = 1/x$ алгебраической прямой, т. е. прямой, заданной уравнением $ax + by + c = 0$ с алгебраическими коэффициентами a, b, c. Естественно спросить, нельзя ли в этом утверждении заменить гиперболу графиком произвольной рациональной функции $R(x) = P(x)/Q(x)$, где $P(x)$ и $Q(x)$ — многочлены с алгебраическими коэффициентами.

В настоящее время мы знаем полный ответ на этот вопрос. Во-первых, нужно предполагать, что функция $R(x)$ имеет хотя бы один ненулевой вычет в точках комплексной плоскости (т. е. ее первообразная трансцендентна). В противном случае площадь сегмента, конечно, будет алгебраическим числом для любой секущей с алгебраическими коэффициентами. Пример функции $\frac{4-x}{x(x-2)}$ и секущей, проходящей через точки ее графика с абсциссами 3 и 6, показывает, что указанное условие не является достаточным. Вопрос о трансцендентности площади сегмента для функции с двумя ненулевыми вычетами сводится к трансцендентности чисел вида $a \ln \alpha + b \ln \beta$ при алгебраических a, b, α, β.

Седьмая проблема Гильберта утверждает, что при алгебраических α и β отношение $\ln \alpha / \ln \beta$ может быть либо рациональным, либо трансцендентным числом. Иными словами, линейная комбинация $a \ln \alpha + b \ln \beta$ при указанных выше условиях

может равняться нулю лишь в случае, когда $\ln\alpha$, $\ln\beta$ линейно зависимы над полем рациональных чисел. Эквивалентная формулировка гласит, что числа вида a^b при алгебраическом a, отличном от нуля, и алгебраическом иррациональном b, трансцендентны. Эта проблема была независимо решена в 1934 г. А. О. Гельфондом (*Гельфонд А. О.* — ДАН СССР, 1934, т. 2, № 1, с. 1–6) и Т. Шнейдером (*Schneider Th.* — J. reine und angew. Math., 1934, bd. 172, S. 65–69). Несколько раньше, в 1929 г., А. О. Гельфонд решил эту проблему частично, доказав трансцендентность числа $e^\pi = (-1)^{-i}$.

Развивая метод Гельфонда, А. Бейкер (*Baker A.* Transcendental Numner Theory. — Cambr. Univ. Press, 1975) установил следующий результат.

Теорема 1. *Если $\alpha_1,\ldots,\alpha_m$ — ненулевые алгебраические числа, а их логарифмы $\ln\alpha_1,\ldots,\ln\alpha_m$ линейно независимы над полем рациональных чисел, то числа $1,\ln\alpha_1,\ldots,\ln\alpha_m$ линейно независимы над полем всех алгебраических чисел. В частности, любая ненулевая комбинация логарифмов алгебраических чисел с алгебраическими коэффициентами трансцендентна.*

Эта теорема явилась побочным продуктом интенсивной деятельности в теории трансцендентных чисел, связанный с оценками линейных форм от логарифмов алгебраических чисел (*Baker A., Wuestholz G.* — J. reine und angew. Math., 1993, Bd. 442, S. 19–62).

Следствием теоремы 1 является результат о трансцендентности определенных интегралов от рациональных функций, полученный в 1971 г. А. Ван дер Поортеном (*van der Poorten A.* — Proc. Amer. Math. Soc., 1971, v. 29, p. 451–456).

Теорема 2. *Пусть $P(z)$ и $Q(z)$ — взаимно простые многочлены с алгебраическими коэффициентами, $\alpha_1,\ldots,\alpha_n$ — все различные полюса функции $R(z)=P(z)/Q(z)$, а $\nu_1,\ldots,\nu_m$ — соответствующие вычеты. Пусть контур Γ в комплексной плоскости есть либо замкнутый путь в расширенной комплексной плоскости, либо он соединяет две различные алгебраические точки, либо, начинаясь в алгебраической точке, простирается до бесконечности, причем интеграл $\int_\Gamma R(z)\,dz$ существует. Этот интеграл есть алгебраическое число в том и только том случае, когда*

$$\int_\Gamma\left(\sum_{k=1}^{m}\frac{\nu_k}{z-\alpha_k}\right)dz=0.$$

Например, этот результат означает трансцендентность числа

$$\int_0^1\frac{dx}{x^3+1}=\frac{1}{3}\ln 2+\frac{\pi}{3\sqrt{3}}.$$

Кроме того, он дает ответ на вопрос о трансцендентности площадей сегментов, отсекаемых прямыми от графиков рациональных функций. Более того, эта теорема дает ответ и на вопрос о трансцендентности площадей сегментов произвольных рациональных кривых, например, эллипса.

Перейдем теперь от рациональных кривых к произвольным плоским алгебраическим кривым, определенным над полем алгебраических чисел. Исторический интерес представляет здесь рассмотрение так называемых алгебраически неквадрируемых овалов, восходящие к Ньютону. Мы лишь кратко коснемся здесь аналитической стороны дела и его истории, отсылая читателей за подробностями к публикациям В. И. Арнольда (Гюйгенс и Барроу, Ньютон и Гук. — М.: Наука, 1989; Историко-математические исследования, 1989, т. XXXI, с. 7–17). В терминологии упомянутой книги В. И. Арнольда, алгебраический овал (замкнутая выпуклая алгебраическая кривая) называется алгебраически квадрируемым, если площадь его любого сегмента алгебраически зависит от коэффициентов a, b, c уравнения прямой,

отсекающей этот сегмент. Ньютон доказал, что *все гладкие овалы алгебраически неквадрируемы*. Таким образом, имеет смысл ставить вопрос о трансцендентности площади сегмента, отсекаемого от алгебраически неквадрируемого овала алгебраической прямой. В 1691 г. Лейбниц в письме к Гюйгенсу, в частности, писал: «Что касается круга или эллипса, то невозможность их общего квадрирования доказана в достаточной мере, но я еще не видел никакого доказательства неквадрируемости целого круга или какой-то определенной его части...» (письмо цитируется по второй из упомянутых выше работ Арнольда). Если понимать «общую» неквадрируемость как трансцендентность функции, выражающей площадь сегмента, то последующие слова Лейбница, вероятно, следует понимать как вопрос о трансцендентности численных значений площадей соответствующих фигур. Именно такой трактовки , по-видимому, придерживается В. И. Арнольд, указывая в цитируемой книге: «Лейбниц...ставит вопрос о трансцендентности площадей сегментов, отсекаемых от алгебраической кривой, заданной уравнением с рациональными коэффициентами, прямыми с алгебраическими коэффициентами (например, числа π и логарифмов алгебраических чисел). вопрос Лейбница содержит седьмую проблему Гильберта и, кажется, до сих пор не решен».

Ниже мы кратко опишем известные факты, относящиеся к «вопросу Лейбница». Так как случай рациональных кривых уже полностью разобран нами, в дальнейшем будет предполагаться, что рассматриваемые алгебраические кривые не рациональны. Согласно формуле Грина площадь любой компактной области в $\mathbb{R}^2$, ограниченной кусочно гладкими кривыми, равна интегралу $\int_\gamma y\,dx$, где γ — контур, ограничивающий область и проходимый в направлении обхода часовой стрелки. Интеграл от формы $y\,dx$ по любому отрезку с концами в точках с алгебраическими координатами есть алгебраическое число, поэтому, в случае сегмента вопрос сводится к трансцендентности интеграла $\int_\gamma y\,dx$, где путь γ есть дуга действительной алгебраической кривой с концами в точках с алгебраическими координатами. Кроме того, вопрос об арифметических свойствах чисел, выражающих длины дуг с концами в точках с алгебраическими координатами, также сводится к трансцендентности абелевых интегралов.

Рассмотрим сначала эллиптические кривые. В 1937 г. Т. Шнейдер (*Schneider Th.* — Math. Ann., 1937, Bd. 113, S. 1–13) доказал следующую теорему о трансцендентности эллиптических интегралов второго рода.

Теорема 3. *Пусть $R(x,y)$ — рациональная функция, определенная над полем алгебраических чисел, причем $R(x,y)\,dx$ есть дифференциальная форма второго порядка на эллиптической кривой $y^2 = 4x^3 - g_2x - g_3$, не являющаяся дифференциалом никакой рациональной функции. Пусть γ — путь на римановой поверхности этой кривой, соединяющий точки с алгебраическими координатами и не проходящий через полюсы дифференциальной формы. Тогда интеграл $\int_\gamma R(x,y)\,dx$ трансцендентен, за исключением случая, когда путь γ замкнут и гомологичен нулю.*

Приведем некоторые примеры, следующие из теоремы 3. Если (ξ_1,η_1), (ξ,η) — две различные действительные точки на эллипсе $x^2/a^2 + y^2/b^2 = 1$, то длина дуги эллипса, соединяющей эти точки,

$$s = \int_{\xi_1}^{\xi} \sqrt{\frac{a^2 - \varepsilon^2 x^2}{a^2 - x^2}}\,dx, \qquad \varepsilon^2 = 1 - \frac{b^2}{a^2},$$

есть эллиптический интеграл второго рода. Поэтому длина дуги трансцендентна при алгебраических a, b, ξ, ξ_1.

Длина дуги лемнискаты

$$(x^2+y^2)^2 = 2a^2(x^2-y^2), \qquad a>0,$$

задается эллиптическим интегралом первого рода

$$s = a\sqrt{2}\int_{t_1}^{t}\frac{dx}{1-x^4}, \qquad t^2 = \frac{\xi^2-\eta^2}{\xi^2+\eta^2}.$$

Следовательно, при алгебраическом a, длина дуги лемнискаты, соединяющей точки с алгебраическими координатами есть трансцендентное число. В частности, периметр лемнискаты, равный

$$4a\sqrt{2}\int_0^1\frac{dx}{\sqrt{1-x^4}} = a\pi^{-1/2}\Gamma^2(1/4),$$

есть трансцендентное число.

Ответ на вопрос о площадях действительных овалов эллиптических кривых (заданных в канонической форме) также связан с эллиптическим интегралом второго рода $\int_\gamma y\,dx$, вычисляющимися по замкнутому контуру. В частности, если многочлен $4x^3-g_2x-g_3$ имеет три действительных корня, площадь овала, ограниченного соответствующей эллиптической кривой есть трансцендентное число.

Следующая теорема, доказанная в 1984 г. Г. Вюстхольцем (*Wüstholz G.* — J. reine und angew. Math., 1984, Bd. 354, S. 164–174), позволяет доказывать трансцендентность интегралов третьего рода на эллиптических кривых.

Теорема 4. *Пусть $R(x,y)$ — рациональная функция, определенная над полем алгебраических чисел, и γ — замкнутый путь на римановой поверхности кривой $y^2 = 4x^3-g_2x-g_3$, где g_2, g_3 — алгебраические числа. Тогда интеграл $\int_\gamma R(x,y)\,dx$ есть либо нуль, либо трансцендентное число.*

Обобщение этой теоремы на случай алгебраической кривой любого рода (и даже многообразия любой размерности) получено Вюстхольцем (*Wüstholz G.* — Ann. Math., 1989, Bd. 129, S. 471–500, 501–517).

С другими результатами по теории трансцендентных чисел можно познакомиться по книгам: *Шидловский А. Б.* Трансцендентные числа. — М.: Наука, 1987; *Feldman N. I., Nesterenko Yu. V.* Transcendental numbers. — In: Encyclopaedia of Math., Number Theory IV (eds. Parshin A. N., Shafarevich I. R.) — Springer-Verlag, 1997.

[1] (с. 149). Вообще говоря, среди чисел $\beta_1,\dots,\beta_N$ могут быть и равные. Здесь имеется ввиду, что многочлен $(z-p_1)\dots(z-\beta_N)$ имеет рациональные коэффициенты. Последнее утверждение следует из теоремы о симметрических многочленах, поскольку множество $\{\beta-1,\dots,\beta_N\}$ совпадает с совокупностью чисел $\{\alpha_{i_1}+\dots+\alpha_{i_k}\}$, где наборы $(i_1,\dots,i_k)$, $k\geqslant 1$, пробегают все 2^n-1 непустых подмножеств множества $\{1,2,\dots,n\}$.

Ю. В. Нестеренко

О БИКВАДРАТИЧНЫХ ЧИСЛОВЫХ ПОЛЯХ ДИРИХЛЕ

1. Как это часто бывает с математическими работами, они имеют несколько подтекстов. Так и в этой работе Гильберта обнаруживается, как минимум, два. Один из них объявлен в заглавии и в предисловии — дать чисто арифметическое доказательство известной теоремы Дирихле о числе классов биквадратичного поля, которую

тот доказал чисто аналитическими методами, используя дзета-функции полей. Второй подтекст значительно глубже, и мне кажется, он связан с тем, что всякий великий художник, создавая картину, долго подходит к ней, готовится, делает эскизы, наброски. Так и Гильберт в этой работе фактически делает эскиз к своей последней работе по теории алгебраических чисел «О теории относительных абелевых числовых полей». Речь идет о, пожалуй, главной теме Гильберта в алгебраической теории чисел — о законе взаимности.

2. Но прежде чем перейти к обсуждению этой темы объясним, что же сделано Гильбертом в работе относительно теоремы Дирихле. Напомним формулировку этой теоремы. Пусть $K = \mathbb{Q}(\sqrt{m}, \sqrt{-m})$, $m > 0$, и пусть $K_1 = \mathbb{Q}(\sqrt{m})$, $K_2 = \mathbb{Q}(\sqrt{-m})$. Пусть, далее, h — число классов поля K, а h_1, h_2 — числа классов полей K_1 и K_2 соответственно. Тогда

$$h = \begin{cases} h_1 h_2, & \text{если идеал } (2) \text{ ветвится в } K_1, \\ h_1 h_2/2, & \text{в противном случае.} \end{cases}$$

В частности, для простого $m = p$, имеем $h = h_1 h_2/2$, если $p = 1 \mod 4$, и $h = h_1 h_2$, если $p = 3 \mod 4$ или $p = 2$.

Свое арифметическое доказательство Гильберт проводит по следующей схеме, которую мы описываем, в основном, на современном языке.

Пусть H, H_1, H_2 — группы классов полей K, K_1, K_2. Каждому классу $c \in H$ сопоставляется определенная система характеров $\chi_i(c) \in \mu_2 = \langle \pm 1 \rangle$, $i = 1, 2, 3, \ldots, s$, где s — число различных простых делителей дискриминанта d расширения $K/\mathbb{Q}(i)$ (см. конец § 3). Множество классов, которым сопоставляется одна и та же система характеров Гильберт называет родом (Geschlecht). При этом доказывается, что множество классов главного рода (Haupt Geschlecht), соответствующее системе единичных характеров, совпадает с H^2 (см. § 4). Тем самым, множество родов, говоря на языке теории групп, который Гильберт еще не использовал, образует группу, изоморфную H/H^2. Далее Гильберт изучает порядок группы родов. Для этого каждому роду сопоставляется так называемый «ambige Klasse» (амбивалентный класс, т. е. класс идеалов, инвариантный относительно группы Галуа расширения $K/Q(i)$). Получающееся множество классов оказывается в точности 2-кручением в H. Таким образом (см. § 6), Гильберт доказывает, что

$$H/H^2 \cong \operatorname{Tor}_2 H.$$

В § 7 вычисляется порядок подгруппы $\operatorname{Tor}_2 H$, т. е. фактически порядок группы родов, который в случае, когда (2) — квадрат в K_1, равен 2^{s-1}. Поэтому $\#H/H^2 = 2^{s-1}$. Наконец, в последнем параграфе рассматривается гомоморфизм

$$f : H_1 \times H_2 \to H, \quad c_1, c_2 \longmapsto c_1 c_2.$$

Описывается образ этого гомоморфизма, который совпадает с множеством классов идеалов, принадлежащих так называемым родам главного вида (Geschlecht der Hauptart, см. начало § 10), число элементов которого вычисляется непосредственно из определения и равно произведению порядка подгруппы H на 2^π, где π — число распадающихся в $\mathbb{Q}(i)$ простых из разложения числа m на простые в $\mathbb{Q}$, т. е.

$$\#\operatorname{Im} f = 2^\pi \# H^2.$$

Затем вычисляется порядок ядра f , который равен $2^{s-\pi-1}$ (см. § 10) и тем самым в итоге получаем по известной теореме об образе гомоморфизма

$$\#(H_1 \times H_2)/\#\operatorname{Ker} f = \#\operatorname{Im} f \iff h_1 h_2/2^{s-\pi-1} = 2^\pi \# H^2,$$

откуда

$$h_1 h_2 = 2^{s-1} \# H^2 = \#H/H^2 \# H^2 = h.$$

Случай, когда (2) не ветвится в K_1 требует небольшой модификации рассуждений.

3. Как мы уже упомянули, чисто арифметическое доказательство теоремы Дирихле для Гильберта в этой работе не является главной целью. Поэтому мы сделаем лишь краткий обзор литературы по биквадратичным полям перед тем как перейти к закону взаимности. Основной вопрос состоит в арифметическом исследовании множителей в числе классов идеалов поля алгебраических чисел. Такого типа вопрос затрагивал уже Куммер для круговых полей (см.: *Kummer E.* Collected Papers. Vol. 1. — Berlin: Springer-Verlag, 1975, pp. 299–322, 323–344, 363–484, 539–545, 883–885, 887–894, 919–944). Конечно, сюда же принадлежит упомянутая теорема Дирихле, которую обобщил Бахман (*Bachmann P.* — J. reine und angew. Math., 1867, Bd. 67) и далее Амберг (*Amberg E.* Dissert. — Zürich, 1897) и Херглотц (*Herglotz G.* — Math. Zeitschr., 1922, Bd. 12) на любое биквадратичное расширение поля $\mathbb{Q}$. Подробное изложение этих обобщений можно найти в книге Хассе (*Hasse H.* Über die Klassenzahl Abelscher Zahlkörper. — Berlin, 1952). Из более современных работ следует назвать работы Куботы (*Kubota T.* — Nagoya Math. J., 1953, Bd. 6, S. 119–127; Nagoya Math. J. — 1956, Bd. 10, S. 65–85) и Мейера (*Meyer C.* — Symp. Math., vol. XV, 1975, p. 365–387). К этому кругу вопросов относятся также работа: *Lubelski.* — J. reine und angew. Math. 1936, Bd. 174, S. 160–184.

4. Итак, мы приступаем к наиболее интересной части работы, связанной с законом взаимности в гауссовом поле $\mathbb{Q}(i)$. Квадратичные символы в этом поле ввел уже Дирихле :

если $\alpha \in \mathbb{Q}(i)$, π — простое число в $\mathbb{Q}(i)$ и $\pi \neq 1+i$, то

$$\left[\frac{\alpha}{\pi}\right] \overset{\text{def}}{=} \begin{cases} 1, & \text{если } \alpha \text{ — квадратичный вычет по } \bmod \pi, \\ -1, & \text{если } \alpha \text{ — невычет,} \\ 0, & \text{если } \alpha \text{ делится на } \pi. \end{cases}$$

Для $\pi = 1+i$ в этом определении нужно заменить $\bmod \pi$ на $\bmod \pi^5$. Дирихле доказал для этого символа закон взаимности в поле $\mathbb{Q}(i)$ (см.: *Dirichlet G. L.* — J. reine und angew. Math., 1832, Bd. 9, S. 379–389).

Гильберт (см. § 8) доказал квадратичный закон взаимности в более общей, чем у Дирихле, формулировке. Но самое главное, что кроме чисто квадратичного символа Дирихле, Гильберт вводит новый символ

$$\left[\frac{\alpha}{\pi : \delta}\right], \qquad \alpha \in \mathbb{Q}(i), \tag{1}$$

который определяется следующим образом. Пусть δ — целое гауссово число, не делящееся на квадрат целого, и π — какой-либо простой делитель дискриминанта расширения $K/\mathbb{Q}(i)$, где $K = \mathbb{Q}(i, \sqrt{\delta})$. Тогда для числа $\sigma \in \mathbb{Q}(i)$, взаимно простого с π, имеем

$$\left[\frac{\sigma}{\pi : \delta}\right] \overset{\text{def}}{=} \left[\frac{\sigma}{\pi}\right],$$

т. е. это выражение совпадает с символом Дирихле. Для числа $\nu \in \mathrm{Nm}_{K/\mathbb{Q}(i)} K^*$, полагаем

$$\left[\frac{\nu}{\pi : \delta}\right] \overset{\text{def}}{=} 1.$$

Доказывается при этом, что любое число $\alpha \in \mathbb{Q}(i)$ можно представить в в виде $\alpha = \sigma\nu$, где $\mathrm{НОД}(\sigma, \pi) = 1$, а $\nu \in \mathrm{Nm}_{K/\mathbb{Q}(i)} K^*$. Это позволяет определить квадратичный символ Гильберта (1) на всех элементах из $\mathbb{Q}(i)^*$ (см. начало § 3).

Доказанный Гильбертом квадратичный закон взаимности для символов Дирихле применяется далее к проверке следующего равенства

$$\prod_i \left[\frac{\alpha}{\pi_i : \delta}\right] = 1, \tag{2}$$

где $(\alpha) \in \mathrm{Nm}_{K/\mathbb{Q}(i)}c$, c — класс идеалов поля K, а π_i пробегает все ветвящиеся в K простые из $\mathbb{Q}(i)$ (см. конец § 8). Интересно отметить, что последнее свойство, как и сам закон взаимности нигде в доказательстве теоремы Дирихле не применяется, что является еще одним доводом в пользу сказанного в п. 1.

Посмотрим чем же отличается введенный в этой работе Гильбертом символ $\left[\frac{\alpha}{\pi : \delta}\right]$ от его же классического символа норменного вычета $\left(\frac{\alpha, \delta}{\pi}\right)$ (см. «О теории относительных абелевых числовых полей»). Последний символ по определению равен 1 тогда и только тогда, когда α — норма в локальном расширении $K_{(\pi)} = \mathbb{Q}_{(\pi)}(i, \sqrt{\delta})$ над $\mathbb{Q}_{(\pi)}(i)$; в остальных случаях он равен -1. Кроме того, закон взаимности Гильберта для этих символов гласит

$$\prod_{\pi} \left(\frac{\alpha, \delta}{\pi}\right) = 1, \tag{3}$$

где π пробегает все простые в $\mathbb{Q}(i)$, включая и бесконечные. Символ $\left[\frac{\alpha}{\pi : \delta}\right]$ чуть-чуть „недотягивает" до символа норменного вычета $\left(\frac{\alpha, \delta}{\pi}\right)$. Он фактически обладает норменным свойством, которое является основным для символа $\left(\frac{\alpha, \delta}{\pi}\right)$. Кроме того, он удовлетворяет закону взаимности (3) в несколько усеченном виде, т. е. произведение (3) надо рассматривать для символа $\left[\frac{\alpha}{\pi : \delta}\right]$ лишь по ветвящимся простым (а не по всем, как для классического символа). Самое главное его отличие от символа $\left(\frac{\alpha, \delta}{\pi}\right)$ это то, что он определен лишь по модулю простого π.

Таким образом, с этой точки зрения Гильберт сделал эскиз к своей работе «О теории относительно абелевых числовых полей» и судя по всему, именно в этой работе он понял важность норменного свойства символа, а также то, что закон взаимности надо рассматривать не в классическом гауссовом виде, а в виде некоего «большого» произведения символов. И в этом видится основное значение комментируемой работы.

[1] (с. 153). S — автоморфизм квадратичного расширения $K/Q(i)$.

[2] (с. 155). На современном языке эти виды простых называются: распадающиеся, неразветвленные и ветвящиеся.

[3] (с. 159). Разбиение классов идеалов по родам означает следующую операцию на языке групп. Пусть H — группа классов идеалов поля K, и F — множество классов, у которых система характеров состоит из $+1$. Очевидно, что F — подгруппа в H, которая в работе называется главным родом. Род классов идеалов — это класс смежности группы H по подгруппе F и группа родов — это факторгруппа H/F.

[4] (с. 159). Это утверждение означает, что подгруппа главного рода F совпадает с H^2. Таким образом, основное утверждение § 4 означает, что группа классов родов совпадает с факторгруппой H/H^2.

[5] (с. 165). На языке теории групп приведенное рассуждение можно сформулировать в виде следующего утверждения:

Множество амбивалентных классов идеалов совпадает с подгруппой 2-кручения в H, т. е. с $\mathrm{Tor}_2 H$.

[6] (с. 169). Здесь через g обозначен порядок факторгруппы H/H^2, а через f — порядок подгруппы H^2. Очевидно, что $h = gf$, где $h = \#H$.

[7] (с. 169). Это центральное место для понимания того, для чего вводится понятие амбивалентных идеалов. Здесь доказывается (говоря на современном языке)

изоморфизм группы амбивалентных классов $\mathrm{Tor}_2 H$ и группы классов родов H/H^2:

$$\mathrm{Tor}_2 H \to H/H^2, \quad A \longmapsto AH^2.$$

Тогда вычисления в §§ 5 и 6 порядка группы $\mathrm{Tor}_2 H$ дают возможность сосчитать порядок группы родов H/H^2 (см. теорему в конце § 7).

[8] (с. 175). Заметим, что множество родов главного типа — это подгруппа G в группе классов идеалов H, но не в группе родов H/H^2, что может вызывать путаницу.

[9] (с. 175). На языке групп это утверждение эквивалентно следующему. Пусть H' и H'' — группы классов идеалов полей k' и k'' соответственно. Тогда G совпадает с образом гомоморфизма

$$f : H' \times H'' \to H, \quad c', c'' \longmapsto c'c''$$

т. е. $\mathrm{Im}\, f = G$.

[10] (с. 177). На языке теории групп этот результат означает следующее:

$\#\,\mathrm{Ker}\, f$ равен $2^{\pi+\varkappa-1}$, если ∂ — нечетно и число 2 — квадрат в k' или ∂ — четно и 2 не квадрат. Если же ∂ — нечетно и 2 — квадрат в k' или, если ∂ — четно и 2 — не квадрат в k', то $\#\,\mathrm{Ker}\, f = 2^{\pi+\varkappa}$.

[11] (с. 177). Это рассуждение равносильно подсчету:

$$\#H' \times H''/\#\,\mathrm{Ker}\, f = \#\,\mathrm{Im}\, f.$$

С. В. Востоков

К РАБОТАМ ПО ТЕОРИИ ПОЛЕЙ КЛАССОВ

В настоящее издание включены две основополагающие работы Гильберта: «О теории относительно квадратичных числовых полей» (Math. Ann., 1899, Bd. 51, S. 1–127) и «О теории относительно абелевых числовых полей» (Nachr. Ges. Wiss. Göttingen, 1898, 377–399; Acta Math., 1902, Bd. 26, 99–132), посвященные созданию теории полей классов. Работа «О теории относительно абелевых числовых полей», впервые появившаяся в 1898 г. публикуется по варианту 1902 г. с учетом изменений, внесенных в собрание сочинений Гильберта.

Общий исторический комментарий к развитию теории содержится в очерке Г. Хассе «История теории полей классов» (имеется перевод на с. 476–489 настоящего издания). Дальнейшие подробности можно найти в работах: *Вейль Г.* Алгебраическая теория чисел. — М.: ИЛ, 1947; *Вейль А.* Основы теории чисел. — М.: Мир, 1972; *Iyanaga S.* History of the Class Field Theory. — In: The Theory of Numbers (ed. Iyanaga S.). — Amsterdam: North Holland, 1975, p. 479–535; *Frei G.* Heinrich Weber and the Emergence of Class Field Theory. — In: The history of modern mathematics. Vol. 1. — Boston: Acad. Press, 1989, p. 425–450. *Кох Х.*, Алгебраическая теория чисел. — В кн: Теория чисел II. Итоги науки и техники, Современные проблемы математики. Фундаментальные направления. Т. 62. — М.: ВИНИТИ, 1990.

О ТЕОРИИ ОТНОСИТЕЛЬНО АБЕЛЕВЫХ ЧИСЛОВЫХ ПОЛЕЙ

1. В этой работе Гильберт закладывает основы теории полей классов, формулирует и частично доказывает основные факты этой теории, и указывает шаги для достижения поставленной цели. Для непосвященного довольно-таки загадочно звучит название всей теории — теория полей классов, ведь речь идет о теории абелевых расширений полей алгебраических чисел, но все дело в том, что в начале развития

этой теории (см.: *Kronecker L.* — J. reine und angew. Math., Bd. 92, S. 1–122; и в особенности Math. Ann., 1897, Bd. 48, S. 433–473; 1897, Bd. 49, S. 83–100; 1898, Bd. 50, S. 1–26) было не совсем ясно чему соответствуют классы идеалов полей алгебраических чисел, и только в дальнейшем стало понятно, что именно классам идеалов и соответствуют абелевы расширения полей алгебраических чисел. Теперь это название закрепилось за широким спектром теорий абелевых расширений числовых полей, куда включаются и функциональные поля, и локальные поля, и многомерные локальные поля, и многомерные числовые поля, и которые связывают абелевы расширения с арифметическими инвариантами исходного поля (по поводу функциональных полей см.: *Серр Ж.-П.* Алгебраические группы и поля классов. — М.: Мир, 1968; *Katz N. M., Lang S.* — L'Ens. Math., 1981, vol. 27, p. 285–319).

2. Ключ к пониманию всей теории относительно абелевых расширений, как называет теорию полей классов сам Гильберт, лежит, по взгляду Гильберта, в общем законе взаимности. Напомним, что в классическом квадратичном законе взаимности Гаусса речь идет о поведении чисел как квадратичных вычетов и невычетов по простому модулю p. В своей работе Гильберт сделал сначала два замечательных шага. С одной стороны он заменил $\bmod p$ на произвольную степень p, а с другой — заменил квадраты на нормы из квадратичного расширения. Говоря на современном языке, он вложил поле рациональных чисел $\mathbb{Q}$ в его пополнение по p-адической метрике $\mathbb{Q}_p$ (поле p-адических чисел) и задал *символ норменного вычета* $(\ ,\ )$ (в дальнейшем просто с. н. в.) для элементов $\alpha, \beta \in \mathbb{Q}_p^*$ следующим образом:

$$(\alpha,\beta)_p = \begin{cases} 1, & \text{если } \alpha \text{ — } p\text{-адическая норма в } \mathbb{Q}_p(\sqrt{\beta}), \\ -1, & \text{в противном случае.} \end{cases}$$

Следующим выдающимся по значению и элегантным по простоте шагом является формулировка общего закона взаимности в виде бесконечного произведения (Satz 7, § 6)

$$\prod_p (\alpha,\beta)_p = 1$$

(напомним, что квадратичный закон взаимности Гаусса включает кроме основной формулы для нечетных простых еще два дополнения).

При этом для законченности результата (в дальнейшем это пролило свет на многие тонкие арифметические понятия) Гильберт к конечным точкам (конечным простым числам) добавляет бесконечную простую точку p_∞, что соответствует на современном языке рассмотрению архимедова нормирования, при котором поле рациональных чисел переходит в поле вещественных чисел $\mathbb{R}$, и при этом $(\alpha,\beta)_{p_\infty} = 1$, если поле $K = \mathbb{Q}(\sqrt{\beta})$ — вещественное, и $(\alpha,\beta)_{p_\infty} = (\operatorname{sign}\alpha)$, для мнимого поля K.

Этот вид закона взаимности подчеркивает аналогию, которую Гильберт считал основополагающей, между полями алгебраических чисел и полями алгебраических функций. В нашем случае закон взаимности в некотором смысле аналогичен теореме о вычетах для алгебраических функций, причем простые точки с с. н. в. $\neq 1$, соответствуют ветвящимся точкам римановой поверхности. Эта аналогия выглядит еще более удивительной после получения явных формул для локальных символов в ветвящихся точках (см.: *Brückner H.* Eine explizite Formel zum Reziprozitätsgesetz für Primzahlexponenten p. — In: *Hasse H., Roquette P.* Algebraische Zahlentheorie. — Bibliographisches Institut: Manheim, 1966, S. 31–39; Hilbertsymbole zum exponenten p^n und Pfaffsche Formen. — Preprint, Hamburg, 1979; *Востоков С. В.* — Изв. АН СССР, сер. мат., 1978, т. 42, с. 1288–1321), в которые непосредственно входят вычеты функций в особых точках. Для наглядности укажем такую формулу, полученную Куммером в 1858 г. для кругового поля $\mathbb{Q}_p(\zeta)$, $\zeta^p = 1$. Если ξ, η — две главные единицы в $\mathbb{Q}_p(\zeta)$, то

$$(\xi,\eta)_p = \zeta^{\operatorname{res}_x(\log\eta\log\xi)/((1+z)^p-1)},$$

где ряд $z(x)$ получен из разложения ζ в ряд по какой-нибудь униформизующей π поля $\mathbb{Q}_p(\zeta)$, т. е. $\zeta = 1 + z(\pi)$.

Именно формулировка закона взаимности для квадратичного поля с помощью введения с. н. в. дала Гильберту основание считать, что и общий закон взаимности нужно формулировать в терминах с. н. в.

3. Если встать на идельную точку зрения, введенную в обиход Шевалле (*Chevalley C.* Class Field Theory. — Universität Nagoya, 1954), то закон взаимности Гильберта для квадратичного расширения поля k говорит следующее. Пусть $\mathfrak{a} = (\ldots, \alpha_\mathfrak{p}, \ldots)$ — целый идель из группы иделей J_k, где $\alpha_\mathfrak{p}$ — $\mathfrak{p}$-адическая единица для почти всех простых точек $\mathfrak{p}$. Тогда для любого квадратичного расширения $K = k(\sqrt{\beta})$ поля k корректно определен символ $(\mathfrak{a}, K/k) = \prod_\mathfrak{p} (\alpha_\mathfrak{p}, \beta)_\mathfrak{p}$, который является характером на группе иделей (из-за того что в K ветвится лишь конечное число простых $\mathfrak{p}$, и $\alpha_\mathfrak{p}$ — $\mathfrak{p}$-адическая единица для почти всех $\mathfrak{p}$, локальные символы $(\alpha_\mathfrak{p}, \beta)_\mathfrak{p}$ для почти всех $\mathfrak{p}$ равны 1 и произведение определено).

На этом языке закон взаимности Гильберта гласит, что для $K = k(\sqrt{\beta})$:

$$(\mathfrak{a}, K/k) = 1 \tag{1}$$

если $\mathfrak{a}$ — главный идель, т. е. идель полученный из элемента поля k. С другой стороны, по определению локального с. н. в. $(\alpha_\mathfrak{p}, \beta)_\mathfrak{p}$ равенство (1) верно, если $\alpha_\mathfrak{p}$ — $\mathfrak{p}$-адическая норма в K для любой простой точки $\mathfrak{p}$, т. е. (1) верно для любого иделя $\mathfrak{a}$ из группы норм $\mathrm{Nm}\, J_K$. Поэтому мы получаем гомоморфизм

$$(\ , K/k): \quad C_k \to \langle \pm 1 \rangle$$

с ядром $\mathrm{Nm}\, C_K$, где C_k — группа классов иделей, т. е. $C_k = J_k/k^*$. С другой стороны, группа Галуа расширения K/k тоже циклическая, порядка 2. Тем самым мы приходим к основополагающему отображению в теории полей классов — отображению взаимности

$$\psi_k: \quad C_k \to \mathrm{Gal}(K/k),$$

ядро которого совпадает с $\mathrm{Nm}\, C_k$. Это как раз то, что фактически сделал Гильберт в своей работе в связи с законом взаимности.

Гильбертовский закон взаимности для простого показателя ℓ был доказан Фуртвенгером (*Furtwänger P.* — I., Math. Ann., 1909, Bd. 67, S. 1–31; II., Math. Ann., 1912, Bd. 72, S. 346–386; III., Math. Ann., 1913, Bd. 74, S. 413–429), а в общем случае Такаги (*Takagi T.* — J. Coll. Sci. Tokyo, 1920, vol. 41 (Art. 9), p. 1–133) и Хассе (*Hasse H.* Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. — Jahresber. der D. Math. Ver., 1926, Bd. 35, S. 1–55; 1927, Bd. 36, S. 233–311; 1930, Bd. 39, S. 1–204).

4. При обобщении с. н. в. с квадратичных расширений на произвольные расширения степени n мы сталкиваемся с очень любопытной трудностью, которая заключается в том, что нет алгебраического свойства, отличающего один корень n-й степени от другого. Если мы рассмотрим расширение Галуа K/k поля алгебраических чисел k и возьмем неветвящийся идеал $\mathfrak{p}$ в k, то в поле K он разложится в произведение попарно различных идеалов поля K относительной степени f, и нетрудно проверить, что $\mathfrak{p}$-адическое число $\alpha_\mathfrak{p} \neq 0$ есть $\mathfrak{p}$-адическая норма в пополнении $K_\mathfrak{p}$ тогда и только тогда, когда локальный порядок $v_\mathfrak{p}(\alpha_\mathfrak{p})$ этого элемента в точке $\mathfrak{p}$ делится на f, и поэтому, выбрав первообразный корень f-й степени из 1, скажем ζ, мы естественно определяем с. н. в. по формуле

$$(\alpha_\mathfrak{p}, K/k) = \zeta^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$$

который является характером, принимающим значение 1 тогда и только тогда, когда $\alpha_\mathfrak{p}$ — норма в $K_\mathfrak{p}/k_\mathfrak{p}$. Однако при этом остается зависимость от произвола в выборе корня ζ. Эта трудность была блестяще преодолена Артиным (*Artin E.* — Abh.

Math. Semin. Univ. Hamburg, 1927, Bd. 5, S. 353–363), который предложил заменить ζ на однозначно определенный элемент группы Галуа $\mathrm{Gal}(K/k)$ — автоморфизм Фробениуса $\left(\frac{k}{\mathfrak{p}}\right)$ и тогда

$$(\alpha_{\mathfrak{p}}, K/k) := \left(\frac{\alpha, K/k}{\mathfrak{p}}\right) = \left(\frac{K/k}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})},$$

что позволяет нам в итоге переформулировать закон взаимности Артина для иделей: с. н. в. $(\ , K/k)$ задает гомоморфное отображение

$$(\ , K/k): \quad C_K \xrightarrow{\text{на}} \mathrm{Gal}^{\mathrm{ab}}(K/k)$$

с ядром $\mathrm{Nm}_{K/k}C_K$, где C_K — группа классов иделей, т. е. фактор-группа всех иделей J_K по главным иделям K^*.

То обстоятельство, что точка $\mathfrak{p}$ может ветвиться (а таких точек в конечном расширении K/k лишь конечное число), и значит, в ветвящихся точках локальный символ не определен, преодолевается на уровне классов иделей. Это связано с тем, что для данного иделя $\alpha \in J_K$ всегда можно подобрать главный идель $a \in k^*$ так, что локальные компоненты произведения $(a\alpha)_{\mathfrak{p}}$ в исключительных точках (в ветвящихся) будут n степенями и поэтому в них по определению можно считать локальный символ $((a\alpha)_{\mathfrak{p}}, K/k)$ тривиальным, что дает нам возможность определить с. н. в. на классах иделей

$$(\bar{\alpha}, K/k) := \prod_{\mathfrak{p}} (\bar{\alpha}_{\mathfrak{p}}, K/k), \qquad \text{где } \bar{\alpha} \in C_k$$

и мы получаем то, что нынче называется *законом взаимности Артина*: с. н. в. задает гомоморфизм

$$(\ , K/k): \quad C_k \xrightarrow{\text{на}} \mathrm{Gal}(K/k)$$

с ядром $\mathrm{Nm}_{K/k}C_K$.

При этом имеют место функториальные свойства. На классическом языке основоположников теории полей классов указанный результат соответствует теореме об изоморфизме. Если поле K и подгруппа H в C_K соответствуют друг другу, в смысле закона взаимности Артина, т. е. $H = \mathrm{Nm}_{K/k}C_k$, то K называется *полем классов* для H, а подгруппа H — *нормальной подгруппой* в C_k. Подробнее см. исторический очерк Хассе в настоящем издании (с. 476–489). Отметим здесь только, что теория полей классов позволяет полностью определить законы разложения простых дивизоров в абелевых расширениях полей алгебраических чисел. Первые примеры законов разложения относились к квадратичным расширениям поля $\mathbb{Q}$ (см. работу Гильберта «О теории относительно квадратичных полей»). Предысторию этого круга вопросов см. в работе: *Башмакова И. Г., Рудаков А. Н.* Алгебра и алгебраическая теория чисел. — В кн.: Математика XIX века (математическая логика, алгебра, теория чисел, теория вероятностей). — М.: Наука, 1978.

5. Сделаем небольшой обзор дальнейшего развития. В окончательном виде теория полей классов для полей алгебраических чисел была развита Фуртвенглером (*Furtwänger P.*, loc. cit.; Math. Ann., 1907, Bd. 63, S. 1–37), Такаги (*Takagi T.*, loc. cit.; J. Coll. Sci.Tokyo, 1922, vol. 44 (Art. 5), p. 1–50), Артиным (*Artin E.* — Abh. Math. Semin. Univ. Hamburg, 1927, Bd. 5, S. 353–363) и Хассе (*Hasse H.*, loc. cit.; J. reine und angew. Math., 1930, Bd. 162, S. 145–154). Подход Шевалле (*Chevalley C.* — Ann. Math., 1940, vol. 41, p. 394–418) позволил связать локальную теорию полей классов, в которой роль арифметических инвариантов, соответствующих абелевым расширениям, играют открытые подгруппы конечного индекса мультипликативной группы, с глобальной теорией. Внедрение когомологических методов дало возможность сделать более прозрачными наиболее трудные места (см.: *Artin E., Tate J.* Class Field Theory. — Harvard, 1961; а также: *Тэйт Дж.* Глобальная теория полей классов. — В кн.: Алгебраическая теория чисел (Под ред. Дж. Касселса,

А. Фрелиха). — М.: Мир, 1969) и сделать изложение теории более учебным (см. также новый подход Хазевинкеля — Нойкирха: *Hazewinkel M.* — Adv. in Math., 1975, vol. 18, p. 148–181; *Neukirch J.* Class Field Theory. — Berlin–New-York: Springer-Verlag, 1986).

Помимо преимуществ изложения когомологический подход к теории полей классов и, вообще, техника когомологий Галуа позволяют находить группы Галуа не только абелевых, но и некоторых неабелевых расширений. Для l-расширений первые глубокие результаты такого рода были получены Шафаревичем для локальных (*Шафаревич И. Р.* — Матем. сб., 1947, т. 20, с. 351–363) и позднее для глобальных полей (*Шафаревич И. Р.* — Public. Math. IHES, 1964, vol. 18, p. 71–95). Дальнейшее их развитие см. в кн.: *Серр Ж.-П.* Когомологии Галуа. — М.: Мир, 1968; *Кох Х.* Теория Галуа p-расширений. — М.: Мир, 1973; *Кох Х.*, Алгебраическая теория чисел. — В кн: Теория чисел II. Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 62. — М.: ВИНИТИ, 1990. Совершенно неожиданное продолжение теория полей классов имела в многомерных локальных полях, возникшее впервые в работах Паршина (*Паршин А. Н.* — УМН, 1975, т. 30, с. 253–254; ДАН СССР, 1978, т. 243, с. 855–858; Труды МИАН СССР, 1985, т. 165, с. 143–170) и Като (*Kato K.* — J. Fac. Sci. Univ. Tokyo, 1979, vol. 26, p. 303–376; 1980, vol. 27, p. 603–683; 1982, vol. 29, p. 31–43). В этих полях вместо мультипликативной группы исходного поля стали рассматривать K-группы Милнора, и гомоморфизм взаимности устанавливал отображение для n-мерного локального поля k в виде

$$\Psi_k : \quad K_n(k) \to \mathrm{Gal}^{\mathrm{ab}}(K/k)$$

(см. также *Фесенко И. Б.* — Изв. РАН, сер. мат., 1993, т. 57, с. 72–91). Подробный обзор этого направления дан в работе: *Raskind W.* Abelian Class Field Theory of Arithmetic Schemes. — In: Proc. Symp. Pure Math., vol. 58, part 1, p. 85–187 — AMS, 1995.

Следует отметить, что в отличие от функциональных полей (для которых имеются вполне прозрачные доказательства закона взаимности А. Вейля), доказательства законов взаимности в полях алгебраических чисел намного более изощренны. Для получения естественных доказательств было бы целесообразно построить разумную категорию когерентных пучков и их когомологий на некоторых компактификациях арифметических кривых. Работы Куботы и Хилла (*Kubota T.* — Japan J. Math., 1987, vol. 13, p. 235–275; *Hill R.* — Mathematica Göttingensis, 1993, Heft 31, S. 1–82; Construction of Symbols on Adelic Matrix Groups. — Preprint MPI94/103; Nagoya Math. J., 1995, vol. 137, p. 77–144) могут быть интерпретированы как шаг в этом направлении.

Теорию полей классов можно переформулировать, как изоморфизм группы характеров группы $C_k = J_k/k^*$ и группы характеров группы Галуа $\mathrm{Gal}(k^{\mathrm{alg}}/k)$, где k^{alg} — алгебраическое замыкание поля k. Ленглендс выдвинул в качестве гипотезы наличие канонического биективного соответствия между множеством некоторых (бесконечномерных) представлений группы $\mathrm{GL}(n, A_k)$ (здесь A_k — кольцо аделей поля k) и множеством неприводимых n-мерных представлений группы Галуа $\mathrm{Gal}(k^{\mathrm{alg}}/k)$ (см., например, кн.: Автоморфные формы, представления и L-функции. — М.: Мир, 1984). Обычная теория полей классов получается, если $n = 1$. Это направление называют иногда неабелевой теорией полей классов. В его рамках получены примеры законов разложения для простых дивизоров в некоторых неабелевых расширениях полей алгебраических чисел (см.: *Shimura G.* — J. reine und angew. Math., 1966, Bd. 221, S. 209–220).

6. После доказательства общего закона взаимности в форме Гильберта (см. цитированные выше работы Фуртвенглера, Такаги и Хассе) стало понятно, что на-

хождение для него явных формул должно сводиться к поиску явных формул для локальных символов

$$(\ ,\ )_{\mathfrak{p}} \quad : \quad k_{\mathfrak{p}}^* \times k_{\mathfrak{p}}^* \to \mu_n,$$

где $k_{\mathfrak{p}}$ — пополнение поля алгебраических чисел k, содержащее группу корней μ_n степени n из 1, по простому идеалу $\mathfrak{p}$. Если при этом идеал $\mathfrak{p}$ взаимно прост с n, то символ вычисляется очень просто и поэтому называется ручным:

$$(\alpha, \beta)_{\mathfrak{p}} = \left[(-1)^{v_{\mathfrak{p}}(\alpha)v_{\mathfrak{p}}(\beta)}\alpha^{v_{\mathfrak{p}}(\beta)}\beta^{-v_{\mathfrak{p}}(\alpha)}\right]^{\frac{N(\mathfrak{p})-1}{n}} \bmod \mathfrak{p}.$$

Иначе дело обстоит в диком случае, когда $\mathfrak{p}$ делит n. В этом случае получение явных формул шло двумя практически непересекающимися путями. Одно направление восходит к классической работе Куммера о круговом законе взаимности в поле $\mathbb{Q}(\zeta)$, где ζ — ℓ-ый корень из 1, ℓ — простое число (см.: *Kummer E.* Über die allgemeinen Reziprozitätsgesetze der Potenzreste. — Königlichen Akademie der Wissenschaften, 1858; J. reine und angew. Math., 1859, Bd. 56, S. 270–279) и далее, проходя через фундаментальную работу Шафаревича (*Шафаревич И. Р.* — Матем. сб., 1950, т. 26(28), с. 113–146) дает окончательный результат в виде некоторой функции от элементов поля, который был получен Брюкнером и Востоковым (loc. cit.). Далее, Востоковым была найдена формула для с. н. в. и в многомерном локальном поле (См.: *Востоков С. В.* — Изв. АН СССР, сер. мат., 1985, т. 49, с. 283–308). Это направление отражает глубокую аналогию полей алгебраических чисел с полями функций.

Второе направление началось с работы Артина и Хассе (*Artin E., Hasse H.* — Abh. Math. Sem. Hamburg, 1928, Bd. 6, S. 146–162) и развивалось от работы Ивасавы (*Iwasawa K.* — J. Math. Soc. Japan, 1968, vol. 20, p. 151–165) к окончательному в этом направлении результату Сена (*Sen S.* — J. reine und angew. Math., 1980, Bd. 313, S. 72–91). Формулы этого вида более тесно связаны с норменным свойством с. н. в., но с другой стороны они дают результат не для всех элементов поля $k_{\mathfrak{p}}$. Приведем для примера формулы Артина — Хассе в поле $\mathbb{Q}_p(\zeta_{p^n})$:

$$(\zeta, \alpha)_{p^n} = \zeta^{\frac{1}{p^n}\operatorname{tr}(\log \alpha)}, \qquad (\zeta - 1, \alpha)_{p^n} = \zeta^{\frac{1}{p^n}\operatorname{tr}(-\frac{\zeta}{\zeta-1}\log \alpha)},$$

где $\operatorname{tr} := \operatorname{tr}_{\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p}$ (см.: *Artin E., Hasse H.*, loc. cit.).

7. Отметим, что в настоящее время само понятие закона взаимности претерпело существенные изменения и отошло довольно далеко от своего первоначального смысла. В это понятие теперь входит как классическое определение закона взаимности в духе Гаусса, Куммера, Эйзенштейна, Гильберта, так и всевозможные спаривания в локальных полях, представленные в явном виде. В этом смысле дальнейшее развитие законы взаимности получили для спариваний одномерных формальных групп, определенных над кольцом целых локального поля (подробные определения см. в работе: *Fröhlich A.* Formal groups. — Lect. Notes in Math., vol. 74, 1968).

Классический символ Гильберта означает на этом языке, что мы рассматриваем мультипликативную формальную группу $\mathbb{G}_m$. Наиболее близкими к $\mathbb{G}_m$ являются группы Любина — Тейта (*Lubin J., Tate J.* — Ann. Math., 1965, vol. 81, p. 380–387), главной особенностью которых является то, что кольцо эндоморфизмов формальной труппы Любина — Тейта изоморфно кольцу, над которым она определена. Первый успех в получении явных формул для групп Любина — Тейта был достигнут Коатсом и Уайлзом (*Coates J., Wiles A.* — Asterisque, 1977, vol. 41–42, s. 7–17), которуе применили эти формулы для доказательства частного случая гипотезы Берча и Суиннертон — Дайера. Более полные результаты были получены Уайлзом (*Wiles A.* — Ann. Math., 1978, vol. 167, p. 235–254) и Колывагиным (*Колывагин В. А.* — Изв. АН СССР, сер. мат., 1979, т. 43, с. 1054–1120). Они получили явные формулы типа формул Артина — Хассе — Ивасава — Сена. Наиболее полные формулы для формальных групп Любина — Тейта в этом направлении были

получены де Шалитом (*de Shalit E.* — Duke Math. J., 1986, vol. 56, p. 163–176). Как и в мультипликативном случае, они имеют ограниченную область определения. В духе первого направления (Шафаревич — Брюкнер — Востоков) окончательный результат для спаривания Гильберта на формальных группах Любина — Тейта был получен в работе Востокова (см.: Изв. АН СССР, сер. мат., 1979, т. 43, с. 985–1014).

Следующий класс групп, для которых имеется полная классификация, а поэтому осмысленна попытка получения явных формул, составляют так называемые группы Хонда (*Honda T.* — J. Math. Soc. Japan, 1970, vol. 22, p. 213–243). В случае спаривания Гильберта со значениями в группе корней p-й степени полные формулы в первом направлении получили Д. Г. Бенуа и С. В. Востоков (см.: Алгебра и Анализ, 1990, т. 2, № 6, с. 69–97; J. reine und angew. Math., 1993, Bd. 437, S. 131–166). Общий результат в этом направлении получил В. А. Абрашкин (Math. Ann., 1997, Bd. 308, S. 5–19; Изв. РАН, сер. мат., 1997, т. 61, № 3, с. 3–56), используя технику полей норм и кристаллических представлений. Используя близкую технику, Бенуа получил также общий результат для такого же спаривания, обобщающий формулы Сена (см.: *Benois D. G.* — J. reine und angew. Math., 1997, Bd. 493).

С. В. Востоков

Еще одна тема, появляющаяся в работе — это теорема о главных идеалах. В теоремах 11^c и 13^c эта теорема формулируется для поля k с числом классов 4, а в теореме 15 дана формулировка для произвольного поля k. Эта теорема утверждает, что все идеалы поля k становятся главными в максимальном абелевом неразветвленном расширении поля k, которое сейчас называют гильбертовым полем классов (Гильберт обозначал его через Kk). Позже Артин (*Artin E.* — Abh. Math. Semin. Univ. Hamburg, 1927, Bd. 5, S. 353–363; 1930, Bd. 7, S. 46–51) показал что группа классов Cl_k поля k канонически изоморфна группе Галуа $G(Kk/k)$, и что для башни полей $L \supseteq K \supseteq k$, где L/k — неразветвленное расширение Галуа и L совпадает с гильбертовым полем классов поля K, естественное отображение групп классов $\mathrm{Cl}_k \to \mathrm{Cl}_K$, индуцированное вложением полей $k \to K$, переходит под действием изоморфизма Артина в теоретико-групповое отображение перемещения

$$\mathrm{Ver} : G(L/k)^{\mathrm{ab}} \longrightarrow G(L/K)^{\mathrm{ab}},$$

где для конечной группы G через G^{ab} обозначается ее факторгруппа по коммутанту. Таким образом, Артин свел теорему о главных идеалах к чисто теоретико-групповому утверждению, что для конечной группы G с коммутантом G^c отображение перемещения $\mathrm{Ver} : G^{\mathrm{ab}} \to (G^c)^{\mathrm{ab}}$ всегда равно 0. Это последнее утверждение было доказано Фуртвенглером (*Furtwängler Ph.* — Abh. Math. Semin. Univ. Hamburg, 1930, Bd. 7, S. 14–36).

Вместе с тем в указанных выше теоремах Гильберт делает ряд предсказаний о том, какие идеалы поля k становятся главными в промежуточных подполях расширения Kk/k и (редкий для него случай) часть этих предсказаний оказалась неверной (интересно отметить, что все предсказания Гильберта полностью выполняются в функциональном случае, т. е. для групп классов дивизоров степени 0 полей алгебраических функций одной переменной над конечным полем констант). В числовом случае оказалось, что, вопреки предсказанию Гильберта, бывают случаи, когда все идеалы поля k становятся главными уже в некотором собственном подполе поля Kk. Это приводит к задаче описания ядра отображения $\mathrm{Cl}_k \to \mathrm{Cl}_{K_0}$ для заданного промежуточного поля K_0, где $Kk \supseteq K_0 \supseteq k$. Этот вопрос исследовали Таусски и Шольц (*Taussky O., Scholz A.* — J. reine und angew. Math., 1934, Bd. 171, S. 19–41) и ряд других авторов. Ивасава (*Iwasawa K.* — J. Math. Pures Appl., 1956, vol. 35, p. 189–192) дал переформулировку этого вопроса на языке когомологий Галуа. Тем не менее до сих пор здесь не только не получено окончательных результатов, но и не сформулировано никаких общих гипотез.

Переформулируя проблему на языке теории групп, мы должны описать ядро отображения $\mathrm{Ver} : G(L_0/k)^{\mathrm{ab}} \to G(L_0/K_0)^{\mathrm{ab}}$, где L_0 — гильбертово поле классов поля K_0. Если L — гильбертово поле классов поля Kk, то $L \supseteq L_0$, поэтому ответ на наш вопрос зависит только от строения группы $G(L/k)$. Отметим, что группа $G(L/k)$ является конечной метабелевой группой. В связи с этим возникает вопрос: всякая ли конечная метабелева группа G может быть реализована таким образом, т. е. как группа Галуа расширения L/k для некоторого поля алгебраических чисел k, где L совпадает с гильбертовым полем классов над гильбертовым полем классов поля k? Последний вопрос является частью более общей задачи об описании группы Галуа максимального неразветвленного расширения заданного поля алгебраических чисел. В настоящее время об этом известно очень немногое. Наиболее важным результатом до сих пор остается теорема Голода — Шафаревича о башне полей классов (см.: *Голод Е. С., Шафаревич И. Р.* — Изв. АН СССР, 1964, т. 28, с. 261–272), утверждающая, что указанная группа Галуа может быть бесконечной (и дающая явные достаточные условия для этого).

Отметим еще, что последнее утверждение теоремы 6 также неверно, т. е. может существовать поле K с нечетным числом классов (в широком смысле), имеющее нетривиальное гильбертово 2-поле классов (в узком смысле) $\overline{K}_2$ такое, что $\overline{K}_2$ имеет нетривиальную 2-группу классов (в широком смысле).

Контрпример может быть получен следующим образом. Пусть k — циклическое расширение степени $s = 2^n$ поля $\mathbb{Q}$, содержащееся в единственном $\mathbb{Z}_2$-расширении поля $\mathbb{Q}$, где $n \geqslant 5$. Хорошо известно, что k имеет тривиальную 2-группу классов как в узком, так и в широком смыслах. Поэтому согласно теории полей классов группа Галуа G_2 максимального абелева расширения $k(2)$ периода 2 поля k содержится в точной последовательности

$$1 \longrightarrow U(k)/U(k)^2 \longrightarrow \prod_v U(k_v)/U(k_v)^2 \longrightarrow G_2 \longrightarrow 1, \tag{2}$$

где $U(k)$ и $U(k_v)$ — группы единиц поля k и его пополнения k_v относительно точки v соответственно, а v пробегает все точки поля k, включая архимедовы.

Отметим, что для архимедовой точки v $U(k_v)/U(k_v)^2 = \mathbb{R}^\times/\mathbb{R}_+^\times \cong \{\pm 1\}$. Положим

$$A_\infty = \prod_{v|\infty} U(k_v)/U(k_v)^2.$$

Поскольку поле k вполне вещественно, единственная архимедова точка ∞ поля $\mathbb{Q}$ вполне распадается в k, т. е. $A_\infty \cong \mathbb{Z}/2\mathbb{Z}[G]$ как модуль Галуа, где $G = G(k/\mathbb{Q})$. Обозначим через IA_∞ ядро норменного отображения $N : A_\infty \to \mathbb{Z}/2\mathbb{Z}$ относительно группы G. Поскольку G — циклическая группа, IA_∞ является циклическим G-модулем. Для каждой архимедовой точки $v|\infty$ поля k существует символ Гильберта

$$(x, y)_v : U(k_v)/U(k_v)^2 \times U(k_v)/U(k_v)^2 \longrightarrow \{\pm 1\}$$

однозначно определенный тем, что $(-1, -1)_v = -1$. Если $x, y \in A_\infty$, $x = \prod_{v|\infty} x_v$, $y = \prod_{v|\infty} y_v$, то положим $(x, y)_\infty = \prod_{v|\infty} (x_v, y_v)_v$. Символ $(x, y)_\infty$ определяет невырожденное произведение $A_\infty \times A_\infty \to \{\pm 1\}$. Относительно этого произведения группа $N(A_\infty) = A_\infty^G$ совпадает с ортогональным дополнением к IA_∞. Положим $JA_\infty = A_\infty/A_\infty^G$. Для любого $x \in k^\times$ через x_v мы будем обозначать образ x в $U(k_v)/U(k)_v^2$. Через x_∞ мы обозначим образ x в A_∞.

Лемма 1. *В поле k существует простой дивизор $\mathfrak{p} = (\alpha)$ такой, что $\alpha_\mathfrak{l} = 1$, где $\mathfrak{l}$ — единственная точка поля k, лежащая над (2), и α_∞ является образующей модуля Галуа IA_∞.*

Доказательство. Из точной последовательности (2) следует, что подгруппы инерции всех архимедовых точек $v|\infty$ поля k и точки $\mathfrak{l}|2$ порождают в G_2 подгруппу, изоморфную $B := A_\infty \times U(K_\mathfrak{l})/U(K_\mathfrak{l})^2$. Легко видеть, что существует конечное расширение k_1 поля k такое, что $k(2) \supset k_1 \supset k$ и подгруппы инерции всех архимедовых точек $v|\infty$ поля k и точки $\mathfrak{l}|2$ снова порождают в $G(k_1/k)$ подгруппу, канонически изоморфную B. Пусть S — конечное множество всех точек, разветвленных в расширении k_1/k. Отметим, что S содержит $\mathfrak{l}$ и все архимедовы точки. Пусть a — некоторая образующая G-модуля IA_∞. Положим $b = a \times 1 \in B$. Тогда b можно рассматриваать как элемент группы $G(k_1/k)$, и согласно теореме плотности Чеботарева в k существует простой дивизор $\mathfrak{p} \notin S$ такой, что определяемый им элемент $\left(\frac{\mathfrak{p}}{k_1/k}\right)$ группы $G(k_1/k)$ совпадает с b^{-1}. Поскольку поле k имеет нечетное число классов, мы можем считать, что дивизор $\mathfrak{p}$ — главный, т. е. $\mathfrak{p} = (\alpha')$ для некоторого $\alpha' \in k$.

Положим $\alpha'_S = \prod_{v \in S} \alpha'_v$. Поскольку α' — главный идель, иделю α'_S соответствует в группе $G(k_1/k)$ элемент $\left(\frac{\mathfrak{p}}{k_1/k}\right)^{-1}$, т. е. элемент b. Это означает, что после умножения на подходящую единицу $u \in U(k)$ элемент $\alpha = u\alpha'$ обладает тем свойством, что $\alpha_S = b$, т. е. $\alpha_\infty = a$ и α является квадратом в $U(k_v)$ для всех неархимедовых точек из S. Лемма доказана.

Лемма 2. *Пусть p — простое нечетное число, делящееся на $\mathfrak{p}$, и $K = k(\sqrt{p})$. Пусть L — нормальное замыкание в $\overline{\mathbb{Q}}$ поля $k(\sqrt{\alpha})$. Тогда $K \subset L$, $[L : K] = 2^{s-1}$, поле K имеет нечетное число классов (в широком смысле) и L содержится в гильбертовом 2-поле классов $\overline{K}_2$ поля K в узком смысле.*

Доказательство. Очевидно, что $L = k(\sqrt{\alpha_1}, \sqrt{\alpha_2}, \ldots, \sqrt{\alpha_s})$, где $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ — все числа, сопряженные с α в k. Поскольку p вполне распадается в $k/\mathbb{Q}$, в каждом из расширений $k(\sqrt{\alpha_i})/k$ разветвлен ровно один простой делитель $\mathfrak{p}_i$ числа p. Следовательно, все эти расширения независимы, и $[L : k] = 2^s$, причем L/k может иметь ветвление только в простых точках, лежащих над p и в архимедовых точках. Из этого же следует, что L — максимальное абелево расширение поля k периода 2 с ветвлением в простых делителях p и архимедовых точках. Поскольку $(\alpha) = \mathfrak{p}$ и $\alpha_\infty \in IA_\infty$, мы имеем $N_{k/\mathbb{Q}}(\alpha) = p$, т. е. $K \subset L$.

Поскольку все простые делители p разветвлены в расширении K/k, мы получаем, что L/K может иметь ветвление только в архимедовых точках, т. е. $L \subset \overline{K}_2$. Более того, используя лемму 1 и спаривание $(x, y)_\infty$, можно показать, что подгруппы инерции архимедовых точек порождают в группе $G(L/k)$ подгруппу $G(L/K)$, которая канонически изоморфна JA_∞ как G-модуль.

Предположим, что K имеет четное число классов, т. е. над K существует нетривиальное неразветвленное абелево 2-расширение E/K. Тогда существует промежуточное подполе $E \supseteq F \subset K$ такое, что $[F : K] = 2$ и F нормально над k. В этом случае $[F : k] = 4$ и F/k является биквадратичным расширением, имеющим ветвление только в простых делителях p и архимедовых точках. Следовательно, $F \subset L$, но группа Галуа $G(L/K)$ порождается подгруппами инерции архимедовых точек. Полученное противоречие показывает, что K имеет нечетное число классов в широком смысле. Лемма доказана.

Отметим, что поля L и $\overline{K}_2$ чисто мнимы, и для них понятия классов в широком и узком смыслах эквивалентны.

Лемма 3. *При $n \geqslant 5$ гильбертово 2-поле классов $\overline{K}_2$ поля K имеет четное число классов. Более того, поле $\overline{K}_2$ имеет бесконечную 2-башню полей классов.*

Доказательство. В доказательстве леммы 2 было отмечено, что группа Галуа $G(L/K)$ канонически изоморфна JA_∞ как G-модуль. Пусть $H = (\sigma - 1)JA_\infty$, где σ — некоторая образующая группы G. Положим $M = L^H$. Тогда $[M : K] = 2$ и любая архимедова точка поля K разветвлена в расширении M/K. Следовательно, расширение L/M не разветвлено, т. е. 2-группа классов поля M имеет не менее $s - 2$ образующих. Итак, если $\mathfrak{G}$ — группа Галуа максимального неразветвленного 2-расширения поля M, то ее минимальное число образующих d удовлетворяет неравенству $d \geqslant s-2$. С другой стороны, если r — минимальное число определяющих соотношений группы $\mathfrak{G}$, то согласно теореме Шафаревича $r - d \leqslant \mathrm{rk}[U(M)/U(M)^2] = 2s$. Согласно теореме Голода — Шафаревича для конечной группы $\mathfrak{G}$ должно выполняться соотношение $r > d^2/4$. Без труда проверяется, что это соотношение не может выполняться при $s \geqslant 32$, т. е. при $n \geqslant 5$, что означает, что при $n \geqslant 5$ группа $\mathfrak{G}$ бесконечна. Лемма доказана.

Поскольку $M \subset \overline{K}_2$, мы получаем, что и поле $\overline{K}_2$ имеет бесконечную 2-башню полей классов, т. е. поле K является искомым контрпримером.

Л. В. Кузьмин

ДОКАЗАТЕЛЬСТВО ПРЕДСТАВИМОСТИ ЦЕЛЫХ ЧИСЕЛ С ПОМОЩЬЮ ФИКСИРОВАННОГО ЧИСЛА n-Х СТЕПЕНЕЙ (ПРОБЛЕМА ВАРИНГА)

Гипотеза, называемая сейчас проблемой Варинга, была высказана им в 1770 г. в следующем виде:

Доказать, что всякое натуральное число является суммой не более четырех квадратов, девяти кубов, девятнадцати биквадратов и т. д.

По-видимому предполагалось, что для любого целого $n \geqslant 2$ существует число $s = s(n)$ с тем свойством, что всякое натуральное число представимо в виде суммы n-х степеней положительных чисел, причем количество слагаемых не превосходит s. Иными словами, для любого натурального N уравнение

$$x_1^n + \ldots + x_s^n = N \tag{1}$$

разрешимо в целых неотрицательных числах. Наименьшее s с этим свойством принято обозначать $g(n)$. В частности, Варинг предположил, что $g(2) = 4$, $g(3) = 9$, $g(4) = 19$.

Теорема о четырех квадратах была доказана в 1770 г. Лагранжем. В последовавшие за тем годы было доказано существование $g(n)$ для $n \leqslant 8$ и $n = 10$ (см. ссылки в работе Гильберта). Одновременно были получены и некоторые оценки для $g(n)$ сверху. В основе доказательств лежала целая серия алгебраических тождеств, доказывавшихся элементарными средствами. Например, тождество Лиувилля, рассматривавшего случай $n = 4$, имеет вид

$$6\left(x_1^2 + x_2^2 + x_3^2 + x_4^2\right)^2 = \sum_{1 \leqslant i < j \leqslant 4} \left[(x_i + x_j)^4 + (x_i - x_j)^4\right].$$

Существование подобного тождества в общем случае предположил в 1908 г. Гурвиц, указавший к тому же, как это тождество позволяет получить решение проблемы Варинга для случая $n = 2m$, в предположении, что гипотеза Варинга справедлива для случая $n = m$.

В 1909 г. Гильберт, с помощью кратных интегралов, доказал общее тождество такого рода (см. теорему 2), а затем с помощью элементарных рассуждений доказал существование функции $g(n)$ для всех $n \geqslant 2$, т. е. решил проблему Варинга.

Распространено мнение, что доказательство Гильберта очень громоздко и мало прозрачно. В действительности, оно является естественным развитием всех предшествующих исследований. Собственно доказательство теоремы (леммы 1–5 и последующие рассуждения) совершенно элементарно и, будучи оформлено в виде индуктивного утверждения, оно может быть изложено достаточно компактно. Аналитическая часть необходима только для доказательства упомянутого тождества. Более простое его доказательство (но также, аналитическое) было получено Хаусдорфом (см.: Math. Ann., 1909, Bd. 67, S. 301–305) и опубликовано рядом со статьей Гильберта. Позднее, Стридсберг (см.: Math. Ann., 1914, Bd. 72, S. 145–152) доказал это тождество элементарно.

Функцию $g(n)$ легко оценить снизу. Для этого возьмем $N = 2^n[(3/2)^n] - 1$, где $[x]$ — целая часть числа x. Так как $N < 3^n$, то в представлении (1) числа x_i могут принимать лишь значения $0, 1, 2$. Наименьшее количество слагаемых получим взяв $[(3/2)^n] - 1$ чисел 2^n и $2^n - 1$ чисел 1^n. Таким образом

$$g(n) \geqslant [(3/2)^n] + 2^n - 2. \tag{2}$$

Отметим, что правая часть (2) при $n = 2, 3, 4$ принимает значения $4, 9, 19$ соответственно. Гипотеза о том, что в (2) должен стоять знак равенства получила название идеальной проблемы Варинга.

В 1909 г. Виферих опубликовал доказательство неравенства $g(3) \leqslant 9$. Доказательство, однако, содержало пробел, восполненный в 1912 г. Кемпнером. Тем самым было установлено равенство $g(3) = 9$.

В начале 20-х годов в ряде работ Харди и Литтлвуда был развит новый метод решения проблемы Варинга («круговой метод»). Именно этот метод определил направление дальнейших исследований по проблеме Варинга. Используя средства комплексного анализа и оценки тригонометрических сумм Г. Вейля, Харди и Литтлвуд доказали, что все достаточно большие целые числа представимы в виде суммы не более чем $n2^{n-1}(1 + o(1))$ слагаемых, каждое из которых является n-й степенью натурального числа.

Принято обозначать через $G(n)$ наименьшее число s с тем свойством, что все достаточно большие целые числа представимы в виде суммы не более чем s n-х степеней натуральных чисел. Таким образом результат Харди — Литтлвуда можно представить в виде неравенства

$$G(n) \leqslant n2^{n-1}(1 + o(1))$$

при $n \to \infty$.

В действительности функция $G(n)$ с ростом n увеличивается значительно медленнее чем $g(n)$. В 1934 г. разработав новый аналитический метод, И. М. Виноградов доказал оценку

$$G(n) \leqslant 6n \log n + 10n.$$

Доказательство позволяло вычислить и границу, начиная с которой все целые числа представимы в виде суммы указанного малого количества n-х степеней. Таким образом в принципе задача вычисления $g(n)$ свелась к проверке возможности представления всех целых чисел из ограниченного интервала в виде суммы не более чем $2^n + [(3/2)^n] - 2$ слагаемых, являющихся n-ми степенями натуральных чисел.

В 1936 г. Диксон и независимо Пиллаи, используя очень искусные и достаточно громоздкие вычисления, смогли, опираясь на метод Виноградова, найти при $n > 6$ почти окончательное решение идеальной проблемы Варинга. В частности, было установлено, что в соотношении (2) можно поставить знак равенства, если выполняется соотношение

$$1 - \{(3/2)^n\} \geqslant 2^{-n}([(3/2)^n] + 3).$$

Равенство $g(6) = 73$ было доказано Пиллаи (см.: Proc. Indian Acad. Sci. (A), 1940, vol. 12, p. 30–40). В 1964 г. Чен установил, что $g(5) = 37$ (см.: Scientia Sinica,

1964, vol. 13, № 10, p. 1547–1568). Баласубраманиан (см.: Hardy — Ramanujan J., 1985, vol. 8, p. 1–40) установил, что все натуральные числа, большие чем 10^{700}, представимы суммой 19 биквадратов, а Томас (см.: Trans. Amer. Math. Soc., 1974, vol. 193, p. 427–430) установил, что таким же свойством обладают и все натуральные числа до 10^{310}. Сейчас доказано равенство $g(4) = 19$ (см.: *Ballasubramanian.* — Deshouillers, Dress, C. R. Acad. Sci. Paris, Ser. I Math., 1986, vol. 303, з. 161–163).

Для $n > 6$ к настоящему времени доказано ($\{x\}$-дробная доля действительного числа x), что если

$$1 - \{(3/2)^n\} \geqslant 2^{-n}[(3/2)^n], \tag{3}$$

то

$$g(n) = 2^n + [(3/2)^n] - 2.$$

Неравенство (3) с помощью ЭВМ проверено для всех $n \leqslant 200000$ (см.: *Stemmler.* — Math. Comput., 1964, vol. 18, p. 144–146). Малер (см.: Mathematika, 1957, Bd. 4, S. 122–124) доказал, что множество чисел, не удовлетворяющих (3), конечно. Доказательство этой теоремы, однако, неэффективно, т. е. граница сверху для этих чисел найдена быть не может. В настоящее время известны эффективные оценки

$$1 - \{(3/2)^n\} > e^{-n \cdot 0{,}6238\ldots}, \qquad n > 5000,$$

(см.: *Бейкерс.* — Math. Proc. Camb. Phil. Soc., 1981, vol. 90, p. 13–20)

$$1 - \{(3/2)^n\} > (0{,}5769)^n$$

(см.: *Дубицкас А.* — УМН, 1990, т. 45, № 4, с. 153–154). Они, однако, недостаточны для доказательства (3), поскольку

$$2^{-n}[(3/2)^n] \sim (4/3)^{-n}, \quad \ln 4/3 = 0{,}2875\ldots$$

Диксон и Пиллаи в 1936 г. нашли также значение $g(n)$ и в случае, когда неравенство (3) нарушается. В этом случае, если

$$([(3/2)^n] + 1)([(4/3)^n] + 1) = 2^n + 1,$$

то

$$g(n) = 2^n + [(3/2)^n] + [(4/3)^n] - 2,$$

если же

$$([(3/2)^n] + 1)([(4/3)^n] + 1) > 2^n + 1,$$

то

$$g(n) = 2^n + [(3/2)^n] + [(4/3)^n] - 3,$$

В настоящее время не известны числа, для которых нарушается неравенство (3).

Первоначальная оценка И. М. Виноградова для функции $G(n)$, послужившая основой для вычисления точного значения $g(n)$, впоследствии неоднократно улучшалась. Лучшее при больших n неравенство

$$G(n) < n(2\log n + 4\log\log n + 2\log\log\log n + 13)$$

также принадлежит И. М. Виноградову (см.: Изв. АН СССР, сер. матем., 1959, т. 23, с. 637–692). Эта оценка уже не может быть значительно улучшена в силу легко доказываемого неравенства $G(n) > n$.

При малых n лучшие оценки для $G(n)$ были получены Девенпортом, доказавшим, в частности, равенство $G(4) = 16$ (см.: Ann. of Math., 1939, vol. 40, p. 731–747). Заметим, что точное значение $G(n)$ известно еще только для $n = 2$: $G(2) = g(2) = 4$. Ю. В. Линник (см.: ДАН СССР, 1942, т. 36, с. 179–180) доказал неравенство $G(3) \leqslant 7$. Позднее Ватсон (см.: J. London Math. Soc., 1951, vol. 26, p. 153–156) нашел короткое и элегантное доказательство этой оценки, выполненное в духе предшественников Гильберта, и основанное на асимптотической формуле для количества простых чисел, лежащих в арифметической прогрессии.

Харди и Литтлвуд при $s > (n-2)2^{n-1}+5$ установили асимптотическую формулу для $J(n)$ — числа решений уравнения (1) в целых неотрицательных числах

$$J(N) = \frac{(\Gamma(1+\frac{1}{n}))^s}{\Gamma(s/n)} N^{\frac{s}{n}-1}\sigma(N) + o(N^{\frac{s}{n}-1}),$$

где $\sigma(N)$ — так называемый «особый ряд», $\sigma(N) > C > 0$. С помощью своего метода оценок тригонометрических сумм И. М. Виноградов доказал, что эта формула имеет место уже при $s > 4n^2 \log n(1+o(1))$.

Многочисленные работы посвящены различным обобщениям проблемы Варинга. Еще сам Варинг поставил задачу о представлении натуральных чисел суммами значений фиксированного многочлена $P(x)$, принимающего натуральные значения при натуральных x. Представляемые числа при этом иногда должны будут удовлетворять некоторым условиям. Например, число $P(m) = (m+1)\dots(m+n)$ при любом $m \in Z$ делится на $n!$, так что и числа, представляемые суммами таких величин, должны делиться на $n!$.

Рассматривались представления чисел суммами вида $x_1^{n_1} + \dots + x_k^{n_k}$, где $n_1, \dots, n_k$ — фиксированные натуральные числа, а также суммами вида $\pm x_1^n \pm x_2^n + \dots + x_k^n$. Рассматривались также задачи о совместных представлениях нескольких чисел

$$\left.\begin{aligned} x_1^n + \dots + x_s^n &= N_n \\ x_1^{n-1} + \dots + x_s^{n-1} &= N_{n-1} \\ \dots\dots\dots\dots\dots\dots & \\ x_1 + \dots + x_s &= N_1 \end{aligned}\right\}$$

и задачи, в которых аргументы $x_1, \dots, x_s$ — простые или целые алгебраические числа.

Выше приведен лишь краткий обзор результатов, содержащихся в обширной литературе, посвященной проблеме Варинга. Подробности можно найти в следующих работах: *Вон Р.* Метод Харди — Литтлвуда. — М.: Мир, 1985; *Хуа Ло Кен* Метод тригонометрических сумм и его применение в теории чисел. — М.: Мир, 1964; *Dickson L. E.* History of the theory of numbers. Vol. 2. — N. Y.: Chelsea Publ. Comp., 1971; *Ellison W. J.* — Amer. Math. Monthly, 1971, vol. 78, p. 10–36; *Landau E.* Vorlesungen über Zahlentheorie. — Leipzig, 1927; N. Y.: Chelcia Publ. Comp., 1969.

Ю. В. Нестеренко, *Н. И. Фельдман*

Проблема поставлена в 1770 г. английским математиком Варингом (1734–1798) (*Waring E.* Meditationes algebraicae. — Cambridge, 1770). Она обобщает теорему Лагранжа (доказанную в 1770 г.) о том, что каждое натуральное число есть сумма четырех квадратов целых чисел. Точная формулировка проблемы, короткая история ее решения и само решение изложены в статье Д. Гильберта. В проблеме Варинга, как и в Великой теореме Ферма, ставится вопрос о базисных свойствах n-х степеней целых неотрицательных чисел. В теореме Ферма надо доказать, что сумма двух n-х степеней натуральных чисел не равна n-й степени третьего числа. В проблеме Варинга надо доказать, что любое натуральное число есть сумма ограниченного, может быть даже очень большого числа слагаемых, каждое из которых является n-й степенью целого неотрицательного числа. Решение, данное Гильбертом, очень сложное в идейном и техническом отношении. Кроме чисто арифметических соображений, привлекаются средства анализа для доказательства тождеств теорем 1 и 2. А. Пуанкаре в обзоре научного творчества Гильберта писал, что если когда-нибудь будут поняты основные движущие пружины этого доказательства, то, вероятно, арифметические результаты большого значения посыплются, как из рога изобилия.

Тем не менее, метод Гильберта позволил решить ряд проблем, которые обобщают проблему Варинга. В частности, такой оказалась проблема Гильберта — Камке о представимости целочисленного вектора $(N_1, N_2, \ldots, N_n)$ суммою ограниченного числа целочисленных векторов вида $(x, x^2, \ldots, x^n)$ (поставлена Гильбертом в 1909 г. и решена его учеником Э. Камке в 1921 г. См.: *Kamke E.* Verallgeme inerungen des Waring — Hilbertschen Satzes. — Math. Ann., 1921, Bd. 3, S. 3–38).

В 1920–1922 гг. Г. Харди, Д. Литтлвуд и С. Рамануджан (см.: *Hardy G. H., Littlewood J. E.* Some Problems of «partitio numerorum». Part I: A new solution of Waring's problem. — Nachr. Ges. Wiss. Göttingen, 1920, S. 33–54; Part IV: The singular series in Waring's problem and the value of the number $G(k)$. — Math. Zeitschr., 1922, Bd. 12, S. 161–168) разрабатывают аналитический метод решения аддитивных проблем теории чисел и, в частности, проблемы Варинга, который стал называться круговым. Истоком кругового метода послужил метод производящих функций Эйлера, которым Эйлер решал линейные аддитивные задачи. Если $a_1, \ldots, a_k, N$ — натуральные числа, $A(N)$ — количество решений в целых неотрицательных числах $x_1, \ldots, x_k$ линейного уравнения $a_1x_1 + \ldots + a_kx_k = N$, то при $|z| < 1$ справедливо тождество:

$$\Phi(z) = \sum_{N=0}^{\infty} A(N)z^N = ((1 - z^{a_1}) \ldots (1 - z^{a_n}))^{-1}.$$

Функция $\Phi(z)$ называется производящей функцией чисел $A(N)$. Числа $A(N)$ можно находить либо вычисляя N-ю производную $\Phi(z)$ в точке $z = 0$, либо пользуясь интегральной формулой Коши

$$A(N) = \frac{1}{2\pi i} \int_{|z|=R} \Phi(z) z^{-N-1} dz.$$

Схема решения проблемы Варинга круговым методом такова. Для чисел $A(N)$ решений уравнения Варинга $x_1^n + x_2^n + \ldots + x_k^n = N$ выписывается производящая функция $\Phi(z)$, которая является k-й степенью ряда $f(z)$,

$$f(z) = \sum_{x=0}^{\infty} z^{x^n}; \qquad \Phi(z) = f^k(z)$$

В интегральной формуле для $A(N)$ окружность интегрирования $|z| = R$, $R \to 1 - 0$, разбивается по определенному правилу на большие и малые дуги (отсюда происходит название метода — круговой). Соответственно этому разбиению, $A(N)$ представится суммою двух слагаемых $B(N)$ и $C(N)$, где $B(N)$ — сумма интегралов по большим дугам, $C(N)$ — сумма интегралов по малым дугам. С помощью оригинальных соображений арифметического характера получается асимптотическая формула для $B(N)$, $N \to \infty$, и оценивается сверху $|C(N)|$. Тем самым для $A(N)$ получается асимптотическая формула, из которой уже следует разрешимость уравнения Варинга при $N > N_1$. Круговой метод позволил рассматривать проблему Варинга в гораздо более полной и совершенной постановке, чем только как проблему существования представлений числа N суммою n-х степеней. Харди и Литтлвуд ввели две функции $g(n)$ и $G(n)$: $g(n)$ — наименьшее k, при котором разрешимо уравнение Варинга при любом $N \geqslant 1$; $G(n)$ — наименьшее такое k, что уравнение Варинга разрешимо при $N > N_1(n)$. Ясно, что $G(n) \leqslant g(n)$. Харди и Литтлвуд доказали неравенства $n < G(n) < n2^{n-1}(1 + O(1))$, и при $k > n2^{n-1} + 5$ получили асимптотическую формулу для $A(N)$: $A(N) \sim aN^{k/n-1}$, где $a \geqslant a_1(n, k) > 0$. Харди и Литтлвуд высказали ряд гипотез о функциях $G(n)$ и $g(n)$; в частности, они предположили, что $G(n) \leqslant 4n$, если $n \geqslant 4$, n — четное число; $G(n) \leqslant 2n + 1$, если n — нечетное число; $g(n) = 2^n + (3/2)^n - 2$.

В 1924 г. И. М. Виноградов заменил в круговом методе бесконечные ряды $f(z)$ конечными тригонометрическими суммами (*Виноградов И. М.* Sur un théoreme general de Waring. — Матем. сб., 1924, т. 31, с. 490–507). Это не только значительно упростило метод, но и открыло путь к решению новых проблем аддитивной теории чисел. Теперь формула для $A(N)$ выглядит так:

$$A(N) = \int_0^1 S^k(\alpha) e^{-2\pi i \alpha N} d\alpha; \quad S(\alpha) = \sum_{x^n \leqslant N} e^{2\pi i \alpha x^n}.$$

По схеме кругового метода точки α промежутка интегрирования $[0;1)$ разбиваются на два множества: узкие окрестности рациональных α с малыми знаменателями и оставшиеся точки. В точках первого множества слагаемые суммы $S(\alpha)$ практически не осциллируют, из-за этого $S(\alpha)$ в них велика. На этом множестве получается главный член $B(N)$ асимптотической формулы для $A(N)$. На втором множестве слагаемые $S(\alpha)$ осциллируют, для $|S(\alpha)|$ получаются нетривиальные оценки, и на этом множестве получают остаточный член $C(N)$ асимптотической формулы для $A(N)$. Несколько позднее И. М. Виноградов обнаружил, что таким методом можно решать самые общие тернарные проблемы, т. е. проблемы представимости натуральных чисел N суммой вида $x + y + z = N$, где $x \in X$, $y \in Y$, $z \in Z$. От множеств X, Y требуется их достаточная «густота» и «хорошее» распределение чисел этих множеств в арифметических прогрессиях с «небольшой» разностью. Это нужно для получения главного члена $B(N)$. Множество Z может быть очень «редким», но дробные доли αZ при α из второго множества должны быть «равномерно распределенными». Это нужно для нетривиальной оценки соответствующей тригонометрической суммы по z и оценки остаточного члена $C(N)$. В 1934 г. И. М. Виноградов доказал, что $G(n) < n(6 \log n + 10)$ (см.: *Виноградов И. М.* О верхней границе $G(n)$ в проблеме Варинга. — Изв. АН СССР, 1934, т. 5, № 6, с. 1455–1469). Эту оценку он несколько раз уточнял, и его последний результат (1959 г.) такой: $G(n) < n(2 \log n + 4 \log \log n + 2 \log \log \log n + 13)$ (см.: *Виноградов И. М.* К вопросу о верхней границе для $G(n)$. — Изв. АН СССР, сер. матем., 1959, т. 23, № 5, с. 637–642). Асимптотическая формула для $A(N)$ получена И. М. Виноградовым при $k \geqslant 4n^2 \log n(1 + o(1))$ (см.: *Виноградов И. М.* Избранные труды. — М.: Изд-во АН СССР, 1952). В 1942 г. элементарное решение проблемы Варинга дал Ю. В. Линник; он же доказал, что $G(3) \leqslant 7$ (см.: *Линник Ю. В.* О разложении больших чисел на семь кубов. — Докл. АН СССР, 1942, т. 35, с. 179–180; Элементарное решение проблемы Варинга по методу Шнирельмана. — Матем. сб., 1943, т. 12, с. 225–230). Равенство $G(4) = 16$ доказано Г. Дэвенпортом (см.: *Davenport H.* On Waring's problem for fourth powers. — Ann. Math., 1939, vol. 40, p. 731–747). Гипотеза о величине $g(n)$ доказана при «малых» n, $n \leqslant 100$, и при больших n, $n \geqslant n_1$. Элементарное доказательство оценки $G(n) = O(n \log n)$ дано Б. М. Бредихиным и Т. И. Гришиной. (см.: Элементарная оценка $G(n)$ в проблеме Варинга. — Матем. зам., 1978, т. 24, вып. 1, с. 7–18).

Неожиданное продолжение получила упомянутая выше проблема Гильберта — Камке. Введя для этой проблемы функцию $G_1(n)$, подобную функции $G(n)$, К. К. Марджанишвили в 1937 г. (см.: Об одновременном представлении n чисел суммами 1-х, 2-х, ..., n-х степеней. — Изв. АН СССР, сер. матем., 1937, т. 1, с. 609–631) методом Виноградова доказал неравенство $G_1(n) < n! \, 2^{2n}(n+1)^3$. Неоднократно высказывалась гипотеза, что $G_1(n) = O(n^2 \log n)$. Однако в 1981 г. Г. И. Архипов опроверг это предложение и доказал, что $G_1(n)$ экспоненциально растет: $2^n - 1 < G_1(n) \leqslant 3n^3 2^n - n$ (см.: *Архипов Г. И.* О значении особого ряда в проблеме Гильберта — Камке. — Докл. АН СССР, 1981, т. 259, № 2, с. 265–267; О проблеме Гильберта — Камке. — Изв. АН СССР, сер. матем., 1984, т. 48, № 1, с. 3–52). Позднее результат Архипова был доведен Д. А. Митькиным до асимптотического

равенства $G_1(n) = 2^n + O(2^{n/2})$ (см.: *Митькин Д. А.* Оценка для числа слагаемых в проблеме Гильберта — Камке. — Матем. сб., 1986, т. 129, № 4, с. 549–577). Следствием занятий проблемой Гильберта — Камке явился принципиально новый результат в проблеме Артина о локальном представлении нуля формой, полученной в 1981 г. Г. И. Архиповым и А. А. Карацубой: для нетривиального представления нуля целочисленной формой степени n от k переменных необходимо выполнение неравенства $k > \exp(nR^{-1})$, $R = \log n \log\log n \ldots \underbrace{\log \ldots \log n}_{r} \underbrace{\log \ldots \log^2}_{r+1} n$, где $r \geqslant$ $\geqslant 2$ — произвольное фиксированное число, $n > n_1 > 0$ (см.: *Архипов Г. И., Карацуба А. А.* О локальном представлениим нуля формой. — Изв. АН СССР, сер. матем., 1981, т. 45, № 3, с. 948–961; Об одной задаче теории сравнений. — УМН, 1982, т. 37, вып. 5, с. 161–162). Гипотеза Э. Артина утверждала, что форма нетривиально представляет нуль, если $k > n^2$. Наконец, в 1985 г. А. А. Карацуба дал p-адическое доказательство аналога неравенства Виноградова $G(n) < n(2\log n + 2\log\log n + 12)$ (см.: *Карацуба А. А.* О функции $G(n)$ в проблеме Варинга. — Изв. АН СССР, сер. матем., 1985, т. 49. № 5, с. 935–947). Там же было указано, что примененный p-адический метод позволяет уточнить все результаты об оценке $G(n)$ при малых значениях n. Эти уточнения были получены в последние годы Р. Воном и Т. Вули. Обобщениям проблемы Варинга посвящено большое количество работ (см.: *Вон Р.* Метод Харди — Литтлвуда. — М.: Мир, 1985; *Хуа Ло Кен* Метод тригонометрических сумм и его применения в теории чисел. — М.: Мир, 1964; *Hooley C.* On Waring's problem for two squares and three cubes. — J. reine und angew. Math., 1981, Bd. 328, S. 161–207). Многомерные аналоги содержатся в работах: *Архипов Г. И., Карацуба А. А.* Многомерный аналог проблемы Варинга. — Докл. АН СССР, 1987, т. 295. № 3, с. 521–523; *Архипов Г. И., Карацуба А. А., Чубариков В. Н.* Теория кратных тригонометрических сумм. — М.: Наука, 1987; *Карацуба А. А.* Проблема Гильберта — Камке в аналитической теории чисел. — Матем. зам., 1987, т. 41. № 2. с. 272–284.

А. А. Карацуба

[1] (с. 312). Результат Лиувилля приводился в его лекциях, читавшихся в Collège de France. Он напечатан в книге: *Lebesgue V. A.* Exercices d'Analyse Numérique. — Paris, 1995.

[2] (с. 312). Результат Шура приведен в работе: *Landau E.* — Math. Ann., 1909, Bd. 66, S. 105.

[3] (с. 314). После возведения в степень $2m$.

[4] (с. 318). Точнее, H и K — целые неотрицательные.

Ю. В. Нестеренко, *Н. И. Фельдман*

О ПРЕДСТАВЛЕНИИ ОПРЕДЕЛЕННЫХ ФОРМ В ВИДЕ СУММЫ КВАДРАТОВ ФОРМ. О ТЕРНАРНЫХ ОПРЕДЕЛЕННЫХ ФОРМАХ

В работах Д. Гильберта «О представлении определенных форм в виде суммы квадратов форм» и «О тернарных определенных формах» поставлены и частично изучены следующие две проблемы:

1. Представим ли положительно определенный многочлен от n переменных (т. е. многочлен с вещественными коэффициентами, принимающий неотрицательные значения при всех значениях переменных) в виде суммы квадратов многочленов?

2. Представим ли положительно определенный многочлен от n переменных в виде суммы квадратов рациональных функций (или в виде отношения сумм квадратов многочленов, что одно и то же)?

Очевидно, что из положительного решения первой проблемы следует положительное решение и второй проблемы. Оказалось (это показано Гильбертом в работе «О представлении определенных форм в виде суммы квадратов форм»), что, вообще говоря, первая проблема решается отрицательно. Вторая проблема носит название семнадцатой проблемы Гильберта. В работе «О тернарных определенных формах» Гильберт дает положительное решение этой проблемы для многочленов от двух переменных (или для тернарных форм — это одно и то же).

Семнадцатая проблема Гильберта была решена положительно Э. Артином (*Artin E.* — Abh. Math. Sem. Univ. Hamburg, 1927, vol. 5, p. 100–115) в 1927 г.

Доказательство Артина основано на подробном изучении упорядоченных полей и связи упорядоченности с суммами квадратов.

Рассмотрим сначала обе проблемы для многочленов от небольшого числа переменных. Пусть f — положительно определенный многочлен от одной переменной. Так как его вещественные корни имеют четную кратность, то, группируя сомножители в представлении многочлена f в виде произведения комплексных линейных множителей, получаем разложение $f = F \cdot \bar{F}$ для некоторого комплексного многочлена F. Полагая $F = g + ih$, $g, h \in \mathbb{R}[x]$, находим представление $f = g^2 + h^2$, показывающее, что в этом случае обе проблемы решаются положительно.

Отметим, что одинаковое решение обеих проблем в данном случае является проявлением (несложным в нашей ситуации) следующей замечательной теоремы Касселса — Пфистера. Пусть φ — квадратичная форма над полем k, представляющая некоторый многочлен $f(x) \in k[x]$ над полем $k(x)$. Тогда φ представляет f уже над кольцом $k[x]$. (В нашем случае в качестве формы φ нужно взять сумму квадратов.)

Пусть теперь f — положительно определенный многочлен степени $2n$ от двух переменных. В работе «О представлении определенных форм в виде суммы квадратов форм» Гильберт показал, что тогда обе проблемы решаются положительно в случае $n = 1$ (f является суммой квадратов линейных многочленов) и $n = 2$, а при $n \geqslant 3$ первая проблема решается отрицательно. Одним из простейших примеров, показывающих это, является многочлен $x^4y^2 + y^4 + x^2 - 3x^2y^2$ шестой степени от двух переменных, представимый в виде

$$\left(\frac{x^4y+x^2y^3-2x^2y}{x^2+y^2}\right)^2+\left(\frac{x^3y-xy^3}{x^2+y^2}\right)^2+\left(\frac{x^3-xy^2}{x^2+y^2}\right)^2+\left(\frac{x^2y^2-y^4}{x^2+y^2}\right)^2,$$

но не являющийся суммой квадратов многочленов (см.: *Choi M. D., Lam T. Y.* — Math. Ann., 1977, Bd. 231, S. 1–18).

Если количество переменных больше двух, то первая проблема решается положительно только для многочленов второй степени.

Положительное решение семнадцатой проблемы Гильберта, естественно, привело к вопросу о количестве слагаемых в сумме квадратов, представляющей положительно определенный многочлен от n переменных. Так, например, как показано выше, в случае $n = 1$ достаточно двух квадратов. В 1967 г. Пфистер (*Pfister A.* — Invent. Math., 1967, vol. 4, p. 229–237) доказал следующее уточнение семнадцатой проблемы Гильберта. Каждый положительно определенный многочлен от n переменных представим в виде суммы 2^n квадратов рациональных функций. В частности, произведение двух сумм 2^n квадратов также является суммой 2^n квадратов. Доказательство Пфистера в значительной степени основывалось на результатах, полученных к тому времени в алгебраической теории квадратичных форм, развитию которой, несомненно, способствовали работы Гильберта.

Одним из замечательных результатов алгебраической теории квадратичных форм является теорема Пфистера о том, что произведение сумм $m = 2^n$ квадратов элементов произвольного поля (а не только поля рациональных функций от n переменных

над полем вещественных чисел) также является суммой m квадратов. При малых значениях числа m этот факт хорошо известен; при $m = 2$ утверждение следует из классической формулы $(x_1^2+x_2^2)(y_1^2+y_2^2) = (x_1y_1-x_2y_2)^2+(x_1y_2+x_2y_1)^2$, показывающей, что произведение модулей комплексных чисел равно модулю их произведения. Аналогичные формулы имеют место при $m = 4$ и $m = 8$, только для их получения вместо поля комплексных чисел нужно рассмотреть соответственно классическую алгебру кватернионов и алгебру Кэли.

Результат Пфистера становится более интересным (и удивительным), если вспомнить старую теорему Гурвица (*Hurwitz A.* — Nachr. Ges. Wiss. Göttingen, 1898, S. 309–316), которая утверждает, что при натуральных m, отличных от $1, 2, 4, 8$, многочлен $(x_1^2 + x_2^2 + \ldots + x_m^2)(y_1^2 + y_2^2 + \ldots + y_m^2)$ нельзя представить в виде суммы квадратов m многочленов. Тем не менее по теореме Пфистера при $m = 2^n$ этот многочлен можно представить в виде суммы квадратов m рациональных функций от переменных $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_m$, причем так, что при любых наперед заданных значениях переменных рациональные выражения имеют смысл.

Указанное свойство квадратичной формы, являющейся суммой 2^n квадратов, называется мультипликативностью. Более точно, квадратичная форма над полем k называется мультипликативной, если произведение любых двух значений этой формы над произвольным расширением поля k также является значением этой формы.

Пфистер описал всевозможные мультипликативные квадратичные формы над произвольным полем k. Оказалось, что мультипликативными формами являются так называемые n-формы Пфистера (и только они!), равные тензорному произведению n бинарных форм $X_i^2 - a_iY_i^2$, где $a_i \in k$ $(i = 1, 2, \ldots, n)$. Например, тензорное произведение n форм вида $X_i^2 + Y_i^2$ является суммой 2^n квадратов. В частности, 1-форма Пфистера, т. е. квадратичная форма $X^2 - aY^2$ — это форма норменного отображения для квадратичного расширения $k(\sqrt{a})/k$; 2-форма Пфистера имеет вид $X^2 - aY^2 - bZ^2 + abU^2$ и является формой отображения редуцированной нормы для обобщенной алгебры кватернионов, т. е. четырехмерной алгебры с базисом $1, i, j, k$ и соотношениями $i^2 = a, j^2 = b, ij = -ji, k = ij$; 3-форма Пфистера — это восьмимерная квадратичная форма отображения нормы в алгебре Кэли — Диксона (см.: *Lam T. Y.* Algebraic theory of quadratic forms. — Lecture Notes in Math, Reading, Mass., 1973).

Исторический обзор всего круга вопросов, связанных с семнадцатой проблемой Гильберта, приведен в статье Пфистера (*Pfister A.* Hilbert's seventeenth problem and related problems on definite forms. — In: Proc. Symp. Pure Math., vol. 28, part 2. — Providence, R. I.: AMS, 1976, p. 483–489) и докладе Дж. В. С. Касселса (см.: Труды МИАН, 1973, т. 132, с. 114–117). Связь задачи о суммах квадратов с построением рациональных точек на эллиптических кривых обнаружена в работе: *Cassel J. W. S., Ellison W. J., Pfister A.* — J. Number Theory, 1971, vol. 3, p. 125–149.

Укажем еще, что рассуждение Гильберта для тернарных форм 6-го порядка (в работе 1888 г.) разобрано, с точки зрения функционального анализа, в кн.: *Гельфанд И. М., Виленкин Н. Я.* Некоторые применения гармонического анализа. — М.: Физматгиз, 1961, гл. 2, § 7.

А. С. Меркурьев

ОБ УРАВНЕНИИ ДЕВЯТОЙ СТЕПЕНИ

Основная тема работы связана с задачей о представлении функций нескольких переменных суперпозициями функций меньшего числа переменных, составляющей содержание тринадцатой проблемы Гильберта.

В исследованиях по этой проблеме четко прослеживаются два направления. К первому относятся работы о представимости (или непредставимости) суперпозициями однозначных функций, принадлежащих тем или иным традиционным функциональным классам. Второе направление имеет дело с многозначными функциями (как правило, алгебраическими или алгеброидными), так что появляется определенная свобода в понимании высказывания «функция f в области U представляется суперпозицией F». Вот одна из возможных его интерпретаций: в области U некоторая непрерывная однозначная ветвь функции f совпадает с такой же ветвью функции-суперпозиции F; по существу это возврат к первому направлению. Другая «крайность» — интерпретация того же высказывания как полного совпадения многозначных функций f и F в области U, т. е. совпадение в каждой точке $z \in U$ наборов всех значений функций f и F с учетом их кратностей; в этом случае говорят о «точном» представлении функции f суперпозицией F или о представлении f «полной» суперпозицией F и пишут $f = F$ в U. А вот промежуточный вариант: в каждой точке $z \in U$ каждое из значений функции f (с учетом его кратности!) принадлежит набору $F(z)$ всех значений функции F в той же точке; в этом случае пишут $f \subset F$ в U.

Остановимся сначала на некоторых результатах, относящихся к первому направлению. В цитируемой Гильбертом работе А. Островского (1920 г.) было установлено, что однозначная аналитическая функция двух вещественных переменных

$$\zeta(u, v) = \sum_{n=1}^{\infty} u^n / n^v, \quad (u, v) \in V = \{|u| < 1, v > 0\},$$

ни в какой области $U \subset V$ не может быть представлена суперпозицией F бесконечно дифференцируемых функций одной переменной и алгебраических функций любого числа переменных (привлекаемые алгебраические функции могут быть многозначными, так что в действительности утверждается невозможность представления $\zeta \subset F$). Дело в том, что функция ζ не может удовлетворять нетривиальному дифференциальному уравнению с постоянными коэффициентами, полиномиальному относительно ζ и ее частных производных, тогда как любая из рассматриваемых функций-суперпозиций непременно удовлетворяет подходящему уравнению этого типа. Следующего успеха пришлось ждать более 30 лет: А. Г. Витушкин (см.: ДАН СССР, 1954, т. 95, № 4, с. 701–704) доказал, что для любых натуральных n, p, k и q, удовлетворяющих условию $n/p > k/q$, существует C^p-гладкая функция n переменных, непредставимая суперпозицией C^q-гладких функций k переменных. Тем больший сюрприз был преподнесен исследованиями А. Н. Колмогорова (см.: ДАН СССР, 1956, т. 108, № 2, с. 179–182; ДАН СССР, 1957, т. 114, № 5, с. 953–956) и В. И. Арнольда (см.: ДАН СССР, 1957, т. 114, № 4, с. 679–681), итогом которых явилась теорема, разрушившая одну из надежд Гильберта: любая непрерывная функция $n \geqslant 2$ переменных оказалась суперпозицией непрерывных функций одной переменной и операции сложения. Обзор дальнейших результатов о суперпозициях однозначных функций см. в статье А. Г. Витушкина (см.: L'Enseignment mathématique, 1977, vol. 23, fasc. 3–4, p. 255–320), его комментариях к тринадцатой проблеме (в кн.: Проблемы Гильберта. М.: Наука, 1969, с. 163–170), в комментариях В. И. Арнольда к работам А. Н. Колмогорова о суперпозициях (в кн.: *Колмогоров А. Н.* Избранные труды. Математика и механика. — М.: Наука, 1985, с. 445–451), а также в статье Лоренца (*Lorentz G. G.* — In: Mathematical developments arising from Hilbert problems. Proc. Symp. Pure Math., vol. 28, part 2. — Providence, R. I.: AMS, 1976, p. 419–430). Заметим, что по-прежнему неизвестно, всякая ли аналитическая функция $n \geqslant 2$ переменных представима суперпозицией C^1-гладких функций меньшего числа переменных (и при $n = 2$ операции сложения).

Второе направление, начатое по существу исследованиями классиков по разрешимости алгебраических уравнений в радикалах, получило дальнейшее развитие

в работах Ф. Клейна, Д. Гильберта, А. Вимана, Н. Г. Чеботарева (см.: Собр. соч. Т. I. — М.–Л., 1949, с. 255–281), В. В. Морозова, Г. Н. Чеботарева, В. И. Арнольда, А. Г. Хованского, В. Я. Лина. Скажем, что алгебраическая функция f от n комплексных переменных $z = (z_1, \ldots, z_n)$ принадлежит классу $\mathrm{AC}(k, U)$ (соответственно классу $\mathrm{TAC}(k, U)$), если в области $U \subset \mathbb{C}^n$ она допускает представление $f \subset F$ (соответственно точное представление $f = F$) суперпозицией F алгебраических функций k переменных и рациональных функций (конечно, рациональная функция любого числа переменных является суперпозицией многочленов от одной переменной и операций сложения и деления). Аналогично, отнесем f к классу $\mathrm{ЦАС}(k, U)$ (соответственно к классу $\mathrm{ТЦАС}(k, U)$), если в U существует представление $f \subset F$ (соответственно точное представление $f = F$) суперпозицией F целых алгебраических функций k переменных и однозначных голоморфных функций любого числа переменных; если при этом в суперпозиции F, представляющей f, участвует лишь s многозначных функций, то отнесем f к классу $\mathrm{ЦАС}(k, U, s)$ (соответственно $\mathrm{ТЦАС}(k, U, s)$). Наконец, если в рассматриваемых суперпозициях F вместо алгебраических допускаются алгеброидные функции, то это отмечается чертой над символом соответствующего класса (например, $\overline{\mathrm{ТЦАС}}(k, U)$). При $U = \mathbb{C}^n$ символ $\mathbb{C}^n$ во всех приведенных выше обозначениях опускается.

О так называемой «универсальной» целой алгебраической функции n переменных f_n, определяемой уравнением

$$f_n^n + z_1 f_n^{n-1} + \ldots + z_{n-1} f_n + z_n = 0, \tag{1}$$

известно, что при $n \leqslant 5$ она принадлежит $\mathrm{AC}(1)$, а при $n = 6, 7, 8, 9$ — классам $\mathrm{AC}(2), \mathrm{AC}(3), \mathrm{AC}(4)$ и $\mathrm{AC}(4)$ соответственно. Тот факт, что $f_9 \in \mathrm{AC}(4)$, и составляет, собственно, основной результат комментируемой работы: Гильберт доказывает, что f_9 представляется суперпозицией, содержащей (кроме рациональных функций) несколько не более чем 5-значных алгебраических функций одной переменной, одну 9-значную и одну 27-значную алгебраические функции от четырех переменных. Виман (*Wiman A.* — Nova Acta R. Soc. Sci. Uppsaliensis, 1927, vol. extra ordin. editum, p. 3–8), упростив метод Гильберта, получил представление f_9 суперпозицией, содержащей (кроме рациональных функций) несколько не более чем 4-значных и одну 5-значную алгебраические функции одной переменной и еще одну 9-значную алгебраическую функцию четырех переменных, а также доказал, что $f_n \in \mathrm{AC}(n-5)$ при $n \geqslant 10$. Наконец, Г. Н. Чеботарев (см.: Уч. зап. Казан. ун-та, 1954, т. 114, № 2, с. 189–193) показал, что $f_n \in \mathrm{AC}(n-6)$ при $n \geqslant 21$ и $f_n \in \mathrm{AC}(n-7)$ при $n \geqslant 121$. Ни при одном $n \geqslant 6$ не известна нижняя граница тех k, для которых $f_n \in \mathrm{AC}(k)$; Гильберт полагал, что при $n \leqslant 9$ приведенные выше результаты являются наилучшими. Не исключено, однако (хотя и совершенно неправдоподобно!), что $f_n \in \mathrm{AC}(1)$ при всех n. Из результатов А. Г. Хованского (см.: Функц. анализ и его прил., 1970, т. 4, вып. 2, с. 74–79) следует, что $f_n \notin \overline{\mathrm{ЦАС}}(1)$ при $n \geqslant 5$. Неизвестно, существует ли целая алгебраическая функция трех (или более) переменных, не входящая в $\overline{\mathrm{ЦАС}}(2)$.

Пусть $k(n)$ (соответственно $\overline{k}(n, U)$) — наименьшее из тех k, для которых $f_n \in \mathrm{ТЦАС}(k)$ (соответственно $f_n \in \overline{\mathrm{ТЦАС}}(k, U)$); очевидно, что $n-1 \geqslant k(n) \geqslant \overline{k}(n, U)$ (коэффициент при f_n^{n-1} в уравнении (1) «убивается» стандартной заменой $f_n = g - z_1/n$). Н. Г. Чеботарев (см.: Изв. АН СССР, сер. мат., 1943, т. 7, с. 123–146; Собр. соч. Т. 1. — М.–Л.: 1949, с. 327–340) пытался доказать, что $k(n) \geqslant [(n-1)/2]$; хотя в дальнейшем выяснилось, что это верно, некоторые из промежуточных утверждений, на которых основывалось доказательство, оказались ошибочными (см.: *Морозов В. В.* — Уч. зап. Казан. ун-та, 1954, т. 114, № 2, с. 173–187). В цитированной работе В. В. Морозов угадал правильный ответ $k(n) = n - 1$, но предложенное им доказательство также ошибочно. Для чисел $n = 2^r, r \geqslant 2$, соотношение $\overline{k}(n, U) =$

$= n-1$ (для любой области $U \ni 0$) было впервые доказано В. И. Арнольдом (см.: Функц. анализ и его прил., 1970, т. 4, вп. 2, с. 1–9), нашедшим когомологическое препятствие (в когомологиях $\bmod 2$ пространства многочленов степени n с простыми корнями) к представлению функции f_n соответствующими суперпозициями. В. А. Васильев в 1987 г. заметил, что непосредственное применение метода Арнольда дает для любого n оценку $k(n) \geqslant n - d(n)$, где $d(n)$ — число единиц в двоичной записи числа n. Кроме того, заменив когомологии $\bmod 2$ когомологиями с подходящими локальными коэффициентами, он доказал (см.: Функц. анализ и его прил., 1988, т. 22, вып. 3, с. 15–24), что $k(n) \geqslant n - D(n)$, где $D(n)$ — минимальное число слагаемых в представлении n в виде суммы степеней произвольного простого числа. Более общим образом, для *произвольной* (не обязательно универсальной) алгебраической функции f минимальное число m, такое, что f разлагается в полную суперпозицию алгебраических функций от $\leqslant m$ переменных, оценивается снизу *родом Шварца* (см.: *Шварц А. С.* — Труды ММО, 1960, т. 10) соответствующего накрытия. Соотношения $k(n) = \overline{k}(n, C^n) = n-1$ для любого $n \neq 4$ впервые были доказаны В. Я. Лином (см.: Функц. анализ и его прил., 1972, т. 6, вып. 3, с. 77–78) на основе предшествовавшего этому изучения эндоморфизмов группы кос Артина и описания голоморфных эндоморфизмов пространства многочленов с простыми корнями (см.: УМН, 1972, т. 27, № 3, с. 192; Функц. анализ и его прил. 1972, т. 6, вып. 1, с. 81–82; см. также: *Лин В. Я.* — В кн.: Алгебра. Топология. Геометрия. Итоги науки и техники. Т. 17. — М.: ВИНИТИ, 1979, с. 159–227). В дальнейшем было найдено «элементарное» доказательство соотношений (см.: *Лин В. Я.* — Функц. анализ и его прил., 1976, т. 10, вып. 1, с. 37–45) $k(n) = \overline{k}(n, U) = n - 1$ для любого $n \geqslant 3$ и любой области $U \ni 0$, основанное, в конечном счете, на том, что если полный прообраз $\varphi^{-1}(w)$ некоторой точки $w \in \mathbb{C}^m$ при голоморфном отображении $\varphi : \mathbb{C}^n \to \to \mathbb{C}^m$ непуст, то $\dim_{\mathbb{C}} \varphi^{-1}(w) \geqslant n-m$. В цитированной работе доказано также, что если $n \geqslant 3$ и $f_n \in \overline{\text{ЦАС}}(k, s)$, то $ks \geqslant n-1$; в частности, не существует представления $f_n \subset F$ суперпозицией F целых алгеброидных функций двух переменных и однозначных голоморфных функций любого числа переменных, содержащей менее чем $(n-1)/2$ многозначных функций. Те же методы позволяют доказать, что если $n > k \geqslant 2$, то при каждом $N \geqslant 2$ в конечномерном пространстве $\mathcal{F}(n, k, N)$ всех алгебраических функций f от k переменных $w = (w_1, \ldots, w_k)$, определяемых уравнениями вида $f^n + p_1(w) f^{n-1} + \ldots + p_n(w) = 0$, где p_i — полиномы от w степени не выше N, функции, допускающие точное представление $f = F$ суперпозициями F целых алгебраических функций, зависящих менее чем от k переменных, и многочленов, лежат в собственном алгебраическом подмножестве $\Sigma \subset \mathcal{F}(n, k, N)$. Стало быть, функция «общего положения» $f \in \mathcal{F}(n, k, N)$ не может быть точно представлена суперпозицией указанного типа.

Наконец, сочетая результаты последней из цитированных выше работ с теоремой Ирла и Кра о голоморфных сечениях «универсальной кривой Тейхмюллера» (см.: *Earle C. J., Kra I.* — Acta math., 1976, Bd. 137, S. 50–79), удается доказать, что если при некотором $n \geqslant 4$ функция f_n допускает представление $f_n \subset F$ суперпозицией F целых алгеброидных функций от $n-2$ переменных и однозначных голоморфных функций любого числа переменных (т. е. если $f_n \in \overline{\text{ЦАС}}(n-2)$), то функция-суперпозиция F непременно имеет лишние по сравнению с f_n точки ветвления.

[1] (с. 358). Здесь речь идет о том, что фундаментальная группа рассматриваемой поверхности должна совпадать с фундаментальной группой проективной плоскости, т. е. с $\mathbb{Z}/2\mathbb{Z}$.

В. Я. Лин

О ВЕЩЕСТВЕННЫХ ВЕТВЯХ АЛГЕБРАИЧЕСКИХ КРИВЫХ. О ФОРМЕ ПОВЕРХНОСТИ ЧЕТВЕРТОГО ПОРЯДКА

В конце XIX столетия, когда Гильберт заинтересовался расположением компонент вещественных плоских алгебраических кривых, топология вещественных алгебраических кривых, да и сама топология как таковая, еще только делала свои первые шаги. Вопрос о том, каким может быть расположение компонент (ветвей) при заданной степени (у Гильберта «порядке») рассматривали и до Гильберта, например, Гарнак и Клейн. Однако до Гильберта не было известно не только ни одного значительного результата в этом направлении, но даже ни одного факта, ни одного примера, затрагивающего существо проблемы. Гильберт проанализировал первый по-настоящему нетривиальный случай — кривые степени 6 — и обнаружил в этом частном случае явление, которое, как мы теперь можем сказать с полной уверенностью, отражает многочисленные общие закономерности. Речь идет о двух гипотезах Гильберта, включенных им в шестнадцатую проблему известного списка проблем: компоненты M-кривой (так называют кривые с максимальным при заданной степени числом компонент; это число равно 11, если степень равна 6) степени 6 не могут располагаться все вне друг друга; среди компонент M-кривой степени 6 должна существовать компонента, внутри которой расположена одна компонента и вне девять или, наоборот, внутри девять и вне одна. Эти гипотезы, а также другие родственные вопросы, поставленные Гильбертом в его шестнадцатой проблеме, до самого последнего времени оставались в центре исследований топологических свойств вещественных алгебраических кривых, поверхностей и многообразий большего числа измерений.

За последующий столетний период в топологии вещественных алгебраических многообразий был накоплен большой фактический материал, найден ряд общих закономерностей, появились совершенно новые средства и расширилась сама область исследований. Познакомиться с нынешним состоянием предмета можно по многим обзорным работам: *Олейник О. А.* — В кн.: «Проблемы Гильберта». — М.: Наука, 1969, с. 182–195; *Гудков Д. А.* — УМН, 1974, т. 29, вып. 4, с. 3–79; *Харламов В. М.* — В кн.: *Петровский И. Г.* Избранные труды. Системы уравнений с частными производными. Алгебраическая геометрия. — М.: Наука, 1986, с. 465–493; *Арнольд В. И., Олейник О. А.* — Вестник МГУ, сер. 1, 1979, № 6, с. 7–17; *Виро О. Я.* — УМН, 1986, т. 41, вып. 3, с. 45–67; *Виро О. Я.* — Алгебра и анализ, 1990, т. 1, № 5, с. 1059–1134.

Здесь мы коснемся лишь тех достижений, которые вплотную примыкают к материалу комментируемых статей Гильберта. Ссылки на оригинальные работы в тех случаях, когда их можно найти в цитированных обзорах, мы не приводим.

1. В настоящее время известно много различных доказательств первой гипотезы Гильберта; некоторые из них достаточно элементарны (см., например: *Харламов В. М.*, loc. cit.; ср. примечание [8] ко второй статье ниже и *Гудков Д. А.* — loc. cit.). Как правило, это специализации некоторых общих теорем. Первое полное доказательство было дано И. Г. Петровским, получившим следующий общий результат (неравенство Петровского): число P четных компонент неособой кривой степени $2k$ (т. е. компонент, лежащих внутри четного числа других компонент) и число N нечетных (прочих) компонент удовлетворяют двойному неравенству

$$-\frac{3}{2}k(k-1) \leqslant P - N \leqslant \frac{3}{2}k(k-1) + 1.$$

Еще раньше на это неравенство обратила внимание В. Рэгсдейл. Она заметила, что не только оно, но и более сильные оценки

$$P \leqslant \frac{3}{2}k(k-1) + 1, \quad N \leqslant \frac{3}{2}k(k-1)$$

выполняются для всех кривых, строящихся методами Гарнака и Гильберта (единственными известными в то время).

Ответ на вопрос, выдвинутый Рэгсдейл (и Петровским, с отличием на 1 для N), верны ли эти более сильные оценки, был найден лишь недавно. И. Штенберг (см.: C. R. Acad. Sci. Paris, 1993, vol. 317, p. 227 — 232) построил контрпримеры к обеим оценкам для всех $k \geqslant 6$. В его первых контрпримерах коэффициент при k^2 равен $\frac{3}{2} + \frac{1}{8}$. Затем Б. Хас и И. Штенберг (см.: *Haas B.* — C. R. Acad. Sci. Paris, 1995) увеличили этот коэффициент до $\frac{3}{2} + \frac{1}{6} + \frac{1}{48}$. Истинное значение этого коэффициента пока неизвестно. Ясно, что он не превосходит $\frac{3}{2} + \frac{1}{4}$.

Неравенство Петровского явилось началом большого ряда дальнейших исследований (см.: *Харламов В. М.*, loc. cit.). Здесь мы лишь упомянем принадлежащее И. Г. Петровскому и О. А. Олейник обобщение неравенства о плоских кривых на гиперповерхности в пространстве произвольной размерности и принадлежащее Олейник обобщение на кривые в трехмерном пространстве, высекаемые на алгебраической поверхности заданной степени алгебраическими поверхностями.

2. Вторая гипотеза Гильберта оказалась неверна: Д. А. Гудков построил M-кривую степени 6, у которой внутри одной компоненты расположены 5 овалов вне друг друга, а снаружи еще 5 овалов вне друг друга. В то же время эта гипотеза в некотором смысле подтвердилась: как показал Гудков, кроме этой схемы расположения и схем, найденных Гарнаком и Гильбертом, других схем M-кривая степени 6 иметь не может. Этот результат послужил основой гипотезы Гудкова: числа P и N для M-кривой степени $2k$ всегда удовлетворяют сравнению

$$P - N \equiv k^2 \mod 8.$$

Доказательство этой гипотезы было дано В. А. Рохлиным. Ему же принадлежат далекие обобщения этого результата (ср. п. 5 настоящих комментариев).

Работе Рохлина предшествовала основополагающая работа В. И. Арнольда, в которой были показаны пути применения современных средств алгебраической и дифференциальной топологии и средств теории чисел в топологии вещественных плоских алгебраических кривых и была продемонстрирована их эффективность. Арнольд в этой работе доказал ослабленное сравнение $P - N \equiv k^2 \bmod 4$ (фактически он доказал, что оно имеет место для кривой с произвольным числом компонент, если множество ее мнимых точек несвязно), получил усиления неравенств Петровского и нашел новые неравенства (например, доказал, что число непустых нечетных овалов кривой степени $2k$ не превосходит $\frac{1}{2}(k-1)(k-2)$). С работ Арнольда и Рохлина началось особенно интенсивное развитие топологии вещественных алгебраических многообразий.

3. Помимо новых методов построения M-кривых и цитированных выше гипотез Гильберт указал и одно, исторически первое, общее ограничение на расположение компонент плоской кривой: M-кривая степени $m > 3$ не может иметь более $m/2-1$ овалов, последовательно вложенных друг в друга. Основано это ограничение на том, что неприводимая кривая степени $m > 1$ и прямая имеют не более m общих точек, т. е. на тривиальном специальном случае теоремы Безу. В настоящее время найдено довольно много ограничений такого происхождения, в которых используются вспомогательные кривые степени 1, 2 и выше.

Эти ограничения весьма специальны и труднообозримы. Эффективным, и, правда, тоже труднообозримым, оказалось применение теоремы Безу в совокупности с появившимися недавно средствами: комплексными ориентациями и арифметикой форм пересечения гомологий разветвленных накрывающих (указанные в следующем пункте результаты Виро и Шустина, касающиеся кривых степени 8, получены именно на этом пути. Другие примеры см. в работе: *Виро О. Я.* — УМН, loc. cit.).

4. В настоящее время классификация схем расположения компонент плоской M-кривой заданной степени m завершена при $m = 6$ и 7 и близка к завершению при $m = 8$.

При $m = 6$ кроме схем расположения компонент, указанных в первой из рассматриваемых статей Гильберта, есть еще одна: внутри одного овала расположены 5 овалов вне друг друга, а снаружи него — еще 5 овалов вне друг друга. Кривые с такой схемой были впервые построены Гудковым; он же доказал, что других M-схем нет (см.: *Гудков Д. А.*, loc. cit.).

Количество M-схем степени 7 равно 14. Они устроены следующим образом: кроме односторонней ветви имеется $2 \leqslant \alpha \leqslant 15$ овалов, расположенных вне друг друга, и внутри одного из них лежат еще $0 \leqslant \beta = 15 - \alpha \leqslant 13$ овалов вне друг друга (см.: *Виро О. Я.* — УМН, loc. cit.).

Количество M-схем степени 8 заключено в пределах между 78 и 91. M-схемы степени 8 делятся на два класса, изображенные на рис. 1.

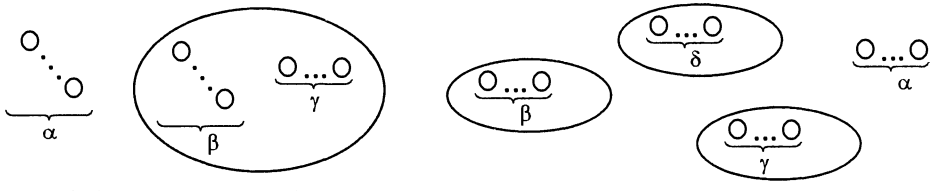


Рис. 1

Для схем первого класса должно выполняться сравнение $\alpha + \gamma \equiv 2 \bmod 4$, а для схем второго класса — сравнение $\alpha \equiv 0 \bmod 4$ (так называемое сравнение Гудкова, см. п. 2 выше). Для схем второго класса в случае $\beta\gamma\delta \neq 0$ числа β, γ, δ должны все быть нечетными. Открытым остается вопрос о реализуемости следующих схем:

$16 ⩡ 1⟨2 ⩡ 1⟨2⟩⟩$, $14 ⩡ 1⟨2 ⩡ 1⟨4⟩⟩$, $4 ⩡ 1⟨2 ⩡ 1⟨14⟩⟩$, $2 ⩡ 1⟨2 ⩡ 1⟨16⟩⟩$,
$13 ⩡ 1⟨2 ⩡ 1⟨5⟩⟩$, $7 ⩡ 1⟨2 ⩡ 1⟨11⟩⟩$, $5 ⩡ 1⟨2 ⩡ 1⟨13⟩⟩$, $1 ⩡ 1⟨1 ⩡ 1⟨18⟩⟩$,
$1 ⩡ 1⟨3 ⩡ 1⟨16⟩⟩$, $1 ⩡ 1⟨4 ⩡ 1⟨15⟩⟩$, $1 ⩡ 1⟨6 ⩡ 1⟨13⟩⟩$, $1 ⩡ 1⟨7 ⩡ 1⟨12⟩⟩$,
$1 ⩡ 1⟨9 ⩡ 1⟨10⟩⟩$

(см.: *Шустин Е. И.* — Изв. АН СССР, сер. матем., 1990, т. 54, №. 5, с. 1069 — 1089).

5. Гильберт в своей шестнадцатой проблеме, формулируя задачи о поверхностях, поставил на первое место вопрос о числе компонент. Во второй из рассматриваемых статей, посвященной поверхностям степени 4, он уже исследует не вопрос о максимальном числе компонент, а вопрос о максимальном ранге, т. е., в современной терминологии, о максимальной сумме чисел Бетти. Как показали результаты последних лет, именно максимальность суммы чисел Бетти служит правильным обобщением на случай поверхностей и многообразий произвольной размерности понятия M-кривой. Во-первых, неравенство Смита

$$\dim H_*(\mathbb{R}A; \mathbb{Z}/2) \leqslant \dim H_*(\mathbb{C}A; \mathbb{Z}/2)$$

между суммой чисел Бетти множества $\mathbb{R}A$ вещественных точек и множества $\mathbb{C}A$ комплексных точек многообразия есть обобщение неравенства Гарнака, оценивающего число компонент вещественной кривой родом комплексификации, увеличенным на единицу. Во-вторых, для широкого запаса классов алгебраических многооб-

разий доказано существование в каждом классе вещественного M-многообразия, т. е. многообразия, для которого неравенство Смита обращается в равенство. Наконец, в-третьих, многие общие теоремы об M-кривых являются специализациями соответствующих теорем об M-многообразиях. Например, сравнение $P - N \equiv k^2 \bmod 8$ для M-кривых (см. п. 2) — это в действительности частный случай сравнения $\chi(\mathbb{R}A) \equiv \sigma(\mathbb{C}A) \bmod 16$ (χ — эйлерова характеристика, σ — сигнатура), имеющего место для всех M-многообразий четной размерности (чтобы получить сравнение для кривой, достаточно воспользоваться сравнением для двулистного разветвленного накрытия плоскости с ветвлением вдоль кривой).

Каково же максимальное число компонент у поверхностей заданной степени в $\mathbb{RP}^3$? Этот вопрос остается открытым для всех степеней, начиная с 5. Для степени 5 известно лишь, что максимальное число компонент находится между 22 и 25 (для M-поверхностей оно равно 21!). Следующий вопрос: какое максимальное значение может принимать первое число Бетти? Он решен для степеней $\leqslant 4$. Ответ для этих степеней: 1, 2, 7 и 20 (те же значения дает число Ходжа $h^{1,1}$ комплексификации рассматриваемых поверхностей).

Для степени 5 известно лишь, что максимальное значение первого числа Бетти равно либо 45, либо 47 (первое число Бетти обязательно нечетно); для M-поверхностей степени 5 оно равно 45. (Заметим, что $h^{1,1} = 45$ для комплексификации поверхности степени 5 и что существуют вещественные поверхности с первым числом Бетти 47 и с комплексификацией того же гомотопического типа, что и у поверхностей степени 5.)

6. Гильберт строит M-поверхность степени 4, применяя метод К. Роона: от плоской кривой степени 6 с уравнением вида $p_3^2 - p_2 p_4 = 0$ (p_r — однородный многочлен степени r от трех переменных) к поверхности степени 4 с уравнением $p_2 t^2 + 2p_3 t + p_4 = 0$, имеющей невырожденную квадратичную особую точку, и затем посредством малого возмущения к неособой поверхности. Как заметил Виро, M-поверхность степени 4 того же топологического (и изотопического) типа, что и у Гильберта, легко получается из построенной Гильбертом же пространственной M-кривой степени 8 (см. первую из рассматриваемых статей Гильберта). Эта кривая лежит на гиперболоиде и высекается на нем поверхностью степени 4. Пусть уравнение гиперболоида есть $H = 0$, а уравнение поверхности есть $F = 0$. Тогда при малом ε уравнение

$$H^2 + \varepsilon F = 0$$

дает поверхность, топологически устроенную как удвоение половины гиперболоида

$$H = 0, \qquad \varepsilon F \leqslant 0,$$

и при подходящем знаке параметра ε из кривой Гильберта получается поверхность Гильберта: двухкомпонентная поверхность, состоящая из сферы и сферы с 10 ручками. Этот прием позволил Виро реализовать все, кроме одного, возможные топологические и изотопические типы поверхностей степени 4 в $\mathbb{RP}^3$.

7. Затронутый Гильбертом вопрос о расположении кривых на гиперболоиде изучался в дальнейшем многими авторами. Изучались и кривые на поверхностях старших степеней (см. цитированные обзоры). Про заузления пространственных кривых до сих пор, насколько мне известно, нет результатов, раскрывающих существо дела.

8. Топологическое строение неособых поверхностей степени 4 трехмерного вещественного проективного пространства и их расположение, с точностью до изотопии, в пространстве исследовались до и после Гильберта. В настоящее время эта проблема решена полностью. Имеется список топологических и изотопических типов, а также найдены их явные реализации. Кроме того, В. В. Никулиным и автором (см., например: *Харламов В. М.*, loc. cit., *Виро О. Я.* — УМН, loc. cit.) найдена классификация этих поверхностей с точностью до более тонкой эквивалентности: с точностью до изотопий в классе неособых поверхностей степени 4 (так называемых жестких изотопий).

Те же проблемы для поверхностей степени $m \neq 4$ решены для $m < 4$ и открыты при всех $m > 4$.

9. Теоремы Гарнака и Гильберта утверждают существование вещественных кривых степени d (плоских в случае Гарнака и лежащих в трехмерном пространстве в случае Гильберта), имеющих максимальный род g при заданной степени и максимальное число вещественных компонент $g+1$ при данном роде. Д. Пеккер (см.: Bull. Sc. Math., 1994, vol. 118, p. 475 — 484) обобщил это утверждение на кривые в проективном пространстве произвольной размерности: для любых целых d и n существует неособая вещественная кривая степени d в вещественном проективном пространстве размерности n, имеющая род $C(d,n)$ ($C(d,n)$ — константа Альфана, т. е. максимальное значение рода при заданных d и n) и $1+C(d,n)$ вещественных компонент.

В. М. Харламов

Примечания к работе **«О вещественных ветвях алгебраических кривых»**

[1] (с. 367). Гильберт пользуется терминами Paarzug и Unpaarzug. Сейчас такая терминология не принята. Вместо термина Zug (ветвь) используется термин «компонента». При этом говорят, что компонента стягивается или соответственно не стягивается в точку либо что она является двусторонней или односторонней. Но мы предпочли более близкий перевод авторских терминов. (Перевод «четная» и «нечетная» невозможен, поскольку в современной терминологии эти слова несут иной смысл.)

[2] (с. 368). Такой набор компонент теперь называют *гнездом*.

[3] (с. 368). Имеется в виду $n > 2$. Здесь, как и во всех остальных местах, где не оговорено противное, кривая предполагается максимальной (имеющей максимальное по Гарнаку число вещественных компонент).

[4] (с. 368). Речь идет о самом внутреннем овале рассматриваемого гнезда из $n/2-1$ компонент.

[5] (с. 368). В каждой степени, начиная с 6, действительно встречаются кривые этого типа с различным расположением компонент. Вместе с тем распределение компонент по кольцевым областям (о которых говорится в статье) далеко не произвольно. Каким же может быть распределение компонент? — этот вопрос до сих пор открыт (решен лишь для степеней $\leqslant 7$ и близок к решению для степени 8).

[6] (с. 368). Имеется в виду $n > 3$. Кривая, как и выше, предполагается максимальной.

[7] (с. 369). Принципиальное отличие способа Гильберта от способа Гарнака заключается в том, что вспомогательная кривая, добавляемая на каждом шаге, имеет степень 2, а не 1, как у Гарнака. Впоследствии появились обобщения этого метода, в которых используются кривые и более высоких степеней (см., например: *Гудков Д. А.* — УМН, 1974, т. 29, вып. 4, с. 3–79). Фактически в заключительной части статьи Гильберта содержится одно такое обобщение: приведено построение M-кривых, в котором вспомогательная кривая является эллиптической, только применяется это построение к кривым не на плоскости (где вспомогательная кривая была бы кривой степени 3), а на гиперболоиде.

[8] (с. 369). Доказательство этого результата, насколько мне известно, так никогда и не было опубликовано (ср. примечание [8] к следующей статье). Сам результат верен (см. цитированный в [7] обзор Д. А. Гудкова).

[9] (с. 370). В настоящее время вопрос, «как, с точностью до изотопии, могут располагаться на проективной плоскости компоненты M-кривой заданной степени m», решен для $m = 6$ и 7 и близок к решению для $m = 8$ (см. комментарии к этой статье).

[10] (с. 370). Гарнак формулирует результат для произвольной кривой, но дает доказательство только для кривых со специальными особенностями. В полном объеме результат доказан Клейном (см.: *Klein F.* — Math. Ann., Bd. 10, S. 398). Следует также отметить, что в этой теореме Гарнака речь идет не о компонентах связности плоской кривой, а о компонентах связности ее нормализации.

[11] (с. 371). На этот результат можно взглянуть с несколько другой точки зрения. Совокупность всех, не обязательно вещественных, кривых данной степени несет естественную структуру алгебраического многообразия. Начиная со степени 3, это многообразие приводимо. Можно поставить задачу: какое максимальное число компонент могут иметь вещественные кривые, отвечающие заданной неприводимой компоненте пространства кривых? Как следует из результата Гильберта, в случае, когда заданная компонента — это совокупность полных пересечений бистепени $(2, n/2)$, где n четно (т. е. совокупность пересечений квадрики с поверхностями степени $n/2$), максимальное число равно роду неособого представителя, увеличенному на 1. В такой формулировке этот результат был перенесен Л. Брюзотти с бистепени $(2, n/2)$ на кривые произвольной бистепени; Виро указал обобщение этого результата на полные пересечения в проективных пространствах старшей размерности (см.: *Виро О. Я.* — УМН, 1986, т. 41, вып. 3, с. 45–67). Обобщение теоремы Гарнака — Гильберта на пространственные кривые, не являющиеся полными пересечениями, получено Д. Пеккером (см. выше комментарии к настоящей статье).

[12] (с. 372). Разумеется, здесь имеются в виду только неплоские кривые.

[13] (с. 372). Этому утверждению, которое, впрочем, дальше не играет никакой роли, противоречат два обстоятельства: во-первых, непарные ветви вообще не могут быть стянуты в точку, а во-вторых, две парные ветви имеют ненулевой коэффициент зацепления (и, следовательно, не могут быть стянуты в точку без пересечения друг с другом), если они реализуют ненулевой класс гомологий гиперболоида, отличный от класса гиперплоского сечения.

[14] (с. 372). Имеется в виду, вероятно, что M-кривая не может иметь никаких (ни вещественных, ни мнимых) особых точек.

[15] (с. 373). Судя по всему, говоря о числе проходов проекции ветви через точку A (соответственно B), Гильберт имеет в виду индекс пересечения этой ветви с прямой на гиперболоиде, проходящей через точку A (соответственно B). В таком случае всякая непарная ветвь (т. е. ветвь, гомологически нетривиальная в $\mathbb{RP}^3$) в проекции проходит нечетное число раз через одну из точек A и B и четное число раз через другую.

В. М. Харламов.

Примечания к работе **«О форме поверхности четвертого порядка»**

[1] (с. 386). В оригинале: «Bei der Untersuchung der Gestalten algebraischer Flächen wird die Kenntnis derjenigen singularitätenfreien Flächen, die topologisch am mannigfaltigsten gestaltet sind, von besonderer Wichtigkeit sein». Скорее всего, Гильберт вкладывал в это предложение тот смысл, который раскрывается в последующих абзацах: поверхность тем разностороннее, чем больше ее ранг (удвоенный ранг равен сумме чисел Бетти, точнее, размерности тотального пространства классов $\mathbb{Z}/2$-гомологий).

[2] (с. 386). В современной терминологии непрерывно связная система — это компонента связности.

[3] (с. 386). Уравнение $F(x, y, z, t) = 0$ определяет поверхность в трехмерном вещественном проективном пространстве. Гильберт рассматривает ее компоненты связности и объясняет, как они соотносятся с компонентами аффинной части поверхности.

[4] (с. 386). Под овалоидом (Ovale) подразумевается компонента, гомеоморфная сфере.

[5] (с. 388). Под узловой точкой (Knotenpunkt) подразумевается точка, в которой поверхность подобна невырожденному непустому квадратичному конусу, т. е. точка, в окрестности которой поверхность имеет в подходящих локальных координатах уравнение $w^2 = uv$.

[6] (с. 388). Гильберт проектирует поверхность из ее узловой точки на xy-плоскость. Эта проекция является двулистным накрытием той части плоскости, в которой $D > 0$. При этой проекции прообраз бесконечно удаленной прямой плоскости имеет две компоненты связности и состоит из двух овалов. Прообраз окружности $x^2 + y^2 - 1 = 0$ состоит из овала и раздутой узловой точки. Таким образом, поверхность гомеоморфна несвязной сумме сферы (простой овалоид в тексте) и сферы с десятью ручками, одна из которых ущемлена.

[7] (с. 389). Во время рассматриваемого изменения коэффициентов.

[8] (с. 389). В этих диссертациях проделана большая работа в направлении к доказательству этой теоремы. Кан разработала некоторую подготовительную технику деформации и возмущения особых кривых. С помощью этой техники Лёбенштайн предприняла исследование расположения овалов кривых степени 6. Основной результат диссертации Лёбенштайн: если кривая степени 6 с 11 овалами, расположенными вне друг друга, существует, то такую кривую можно получить малым возмущением квадрата уравнения кривой степени 3, имеющей простую двойную точку. Существует ли такое возмущение? — этот вопрос цитированные диссертации оставляют открытым. В доказательстве сформулированного частичного результата имеются пробелы.

В. М. Харламов.

О ПОВЕРХНОСТЯХ ПОСТОЯННОЙ ГАУССОВОЙ КРИВИЗНЫ

Как известно, появление в 1868 г. работы Э. Бельтрами (*Beltrami E.* Saggio di interpretazione della geometria non-euclidea — Giornale di Matem., Napoli, 1868, vol. 6, p. 284–312; имеется перевод в сб.: Об основаниях геометрии. — М.: Физматгиз, 1956, с. 180–212, 517) сыграло важную роль в широком признании неевклидовой геометрии Лобачевского. Действительно, чисто теоретическая система пространственных отношений, созданная Лобачевским и столь сильно отличавшаяся от привычной евклидовой, что многим она казалась абсурдной, получила здесь, можно сказать, наглядную реализацию с помощью геодезических линий на поверхности постоянной отрицательной кривизны в обычном трехмерном евклидовом пространстве. Это, казалось, убедительно говорило об отсутствии противоречия в новой геометрии, и потому следовало ожидать, что она найдет применения как внутри самой математики (начало этому положил уже Лобачевский, вычислив сотни определенных интегралов с ее помощью), так и при исследовании физической реальности (в этом Лобачевский был глубоко убежден, хотя естественная реализация прямых световыми лучами позволила ему на основании астрономических данных лишь установить, что если отклонения от евклидовой геометрии и имеются, то даже при очень больших размерах фигур они ничтожно малы: например, для треугольников, вмещающихся в пределы солнечной системы, отклонение суммы углов от 180° не превосходят нескольких миллионных долей секунды). Нельзя не отметить, что Э. Бельтрами в упомянутой работе сослался на полученный ранее результат Ф. Миндинга, опубликованный в 1840 г. (*Minding F.* Beiträge zur Theorie der kürzesten Linien auf krummen Flächen. — J. reine und angew. Math., 1840, Bd. 20, S. 323–327; имеется перевод в сб.: Об основаниях геометрии. — М.: Физматгиз, 1956, с. 176–179),

в период его работы в Берлинском университете, т. е. еще при жизни Н. И. Лобачевского (1792–1856). Миндинг вывел формулы тригонометрии геодезических треугольников на поверхностях постоянной отрицательной кривизны. Эти формулы совпадали с формулами геометрии Лобачевского, но записаны были с помощью гиперболических функций, тогда как Лобачевский применял введенную им функцию $\Pi(x)$ — угол параллельности для отрезка x — и дальше пользовался обычными тригонометрическими функциями. Поэтому при поверхностном взгляде совпадение формул не было очевидно. Миндинг, по-видимому, не знал работ Лобачевского, не интересовался ими, хотя одна из них на французском языке появилась в том же журнале в 1837 г. (*Lobatschefskij N. I.* Géométrie imaginaire. — J. reine und angew. Math., 1837, Bd. 17, S. 295–320; имеется перевод в кн: Полное собр. соч. Н. И. Лобачевского. Т. 3. — М.–Л.: ГИТТЛ, 1951, с. 139–170). Лобачевский же по случайным причинам 20-й том журнала Крелля не брал из библиотеки для просмотра (см.: *Каримуллин А. Г., Лаптев Б. Л.* Что читал Н. И. Лобачевский. — Казань: Изд-во Казанск. ун-та, 1979, с. 18–20). Таким образом, сопоставление этих двух результатов при жизни Лобачевского не состоялось. Оно произошло через 28 лет благодаря Бельтрами (*Beltrami E.*, loc. cit.). Но блестящая убедительная реализация Бельтрами неожиданно натолкнулась на роковое препятствие. Ни на одной из известных или полученных в последующие годы поверхностей такого рода не удавалось реализовать всю плоскость Лобачевского, всегда появлялись особенности.

Правда, через несколько лет, а именно в 1871 г., уже была открыта на другом пути интерпретация, не имеющая этого недостатка, а именно проективная интерпретация Кэли — Клейна (см.: *Klein F.* Über die sogenannte nich-euklideische Geometrie. — Math. Ann., 1971, Bd. 4, S. 573–625; имеется перевод в сб.: Об основаниях геометрии. — М.: Физматгиз, 1956, с. 253–303, 519), а затем, позднее, в 1882 г. конформная интерпретация А. Пуанкаре, использованная им при изучении автоморфных функций (см.: *Poincaré H.* Théorie des groupes fuchsiens. — Acta Math., 1882, p.1–62 (§ 2, p. 6–8); имеется перевод в сб.: Об основаниях геометрии. — М.: Физматгиз, 1956, с. 304–306, 519), так что вопрос об относительной непротиворечивости системы Лобачевского был решен во всей полноте, а также была новым примером подтверждена возможность ее плодотворных применений внутри математики.

Но удастся ли найти поверхность без особенностей, на которой по методу Бельтрами можно реализовать всю плоскость Лобачевского, оставалось неизвестным. Этот вопрос интересовал многих математиков. Гильберт включил его в число нерешенных актуальных проблем математики, названных им в его известном докладе 1900 г. на втором Международном конгрессе математиков в Париже (см.: *Hilbert D.* Mathematische Probleme. — Nachr. Ges. Wiss. Göttingen, 1900, S. 253–297; имеется перевод в т. 2 настоящего издания). Однако уже в следующем году Гильберт опубликовал найденное им решение (см.: Über Flächen von konstanter Gaußscher Krümmung. — Trans. Amer. Math. Soc., 1901, vol. 2, p. 87–99).

Гильберт дал доказательство невозможности существования аналитической поверхности такого типа, не имеющей особенностей. Через два года статья была включена как дополнение („Anhang V") во 2-е издание его книги «Основания геометрии» (*Hilbert D.* Grundlagen der Geometrie, 1903 г.) и затем публиковалась без изменения в последующих изданиях: 3-м (1909 г.), 4-м (1913 г.), 5-м (1922 г.) и 6-м (1928 г.). Но в 7-м издании (1930 г.) (имеется перевод этого издания: *Гильберт Д.* Основания геометрии. — М.–Л.: ГИТТЛ, 1948, с. 304–314) Гильберт несколько изменил доказательство, придав ему (после формулы (3)) более аналитический характер, что сократило эту дальнейшую часть почти в 3 раза. В примечании к формуле (3) он отметил, что теперь дальнейшее изложение является переработкой доказательства Хольмгрена (см.: *Holmgren E.* Sur les surfaces à courbure constante négative. — C. R. Acad. de Paris, 1902, vol. 134, p. 740–743), примыкающей к изложению В. Бляш-

ке в его книге «Дифференциальная геометрия» (*Blaschke W.* Elementare Differential Geometrie. I. — Berlin: 1921, § 80; имеется перевод 3-го изд. 1930 г.: *Бляшке В.* Дифференциальная геометрия. — М.–Л.: ОНТИ, 1935, § 96, с. 225–229). Однако прежнее доказательство, сохраняемое Гильбертом на протяжении 29 лет, представляет геометрический интерес благодаря тщательному анализу возможного поведения геодезических линий на изучаемой поверхности. Поэтому оно приводится в приложении к настоящему изданию как „Фрагмент первого варианта работы «О поверхностях постоянной отрицательной кривизны»".

В примечании к формуле (3) Гильберт упомянул работу Л. Бибербаха (*Bieberbach L.* Hilberts Satz über Flächen konstanter negativer Krümmung. — Acta Math., 1926, Bd. 48, S. 26–33), который усовершенствовал его доказательство. Бибербах использовал понятие накрывающей поверхности, полученной с помощью ортогональной полугеодезической сети. Установив регулярность асимптотической сети, он, исходя из уравнения (3) и теоремы о Curvatura integra $\iint K\,df$, показал, что, с одной стороны, площадь рассмотренного им четырехугольного куска поверхности не может быть более 2π, а с другой стороны, она может расти неограниченно.

Он отметил серьезный дефект работы Либманна (*Liebmann H.* Hilberts Beweise der Sätze über Fächen fester Gauszschen Krümmungsmaszes. — Math. Zeitschr. 1925, Bd. 22, S. 26–33), улучшавшего доказательство Гильберта, но ошибочно допустившего, что если семейство линий на плоскости таково, что через каждую точку проходит только одна линия семейства, то каждая изогональная траектория пересекает каждую линию семейства.

Проблема, решенная Гильбертом в рассматриваемой работе 1901 г., представляет собой частный случай проблемы погружения риманова пространства V_n в евклидово пространство E^N.

В первоначальной общей постановке проблема погружения в евклидово пространство была впервые сформулирована Л. Шлёфли (*Schläfli L.* Nota alla Memoria del sig. Beltrami. Sugli spazii della curvatura costante. — Annali di Mat. (2), 1871–1873, vol. 2, p. 170–173), и им были выписаны основные уравнения

$$\partial_i \bar{r}\,\partial_j \bar{r} = g_{ij} \quad (i,j = 1,\ldots,n),$$

где $\bar{r}$ — радиус-вектор точки n-поверхности в E^N. При $N = n(n+1)/2$ число неизвестных функций и число уравнений совпадают. Шлёфли сделал отсюда на первый взгляд справедливый вывод, что в этом случае для аналитических метрик локальное погружение возможно и дело сводится к интегрированию системы уравнений в частных производных.

Разработка метода решения этой трудной задачи была осуществлена в 1926–1931 гг. в работах М. Жане (*Janet M.* Sur la possibilité de plonger un espace Riemannien donné dans un espace Euclidien. — Ann. Soc. Polon. Math., 1926, vol. 5), Э. Картана (*Cartan E.* Sur la possibilité de plonger un espace Riemannien dans un espace Euclidien. — Ann. Soc. Polon. Math., 1927, vol. 6, p. 1–7) и Ц. Бурстина (*Burstin C.* Ein Beitrag zum Problem der Einbettung der Riemannischen Räumen. — Матем. сб., 1931, т. 38, № 3/4, с. 74–85).

В дальнейшем проблема погружения получила как обобщение, так и многочисленные специализации. Так, вмещающее пространство может быть псевдоевклидовым или пространством постоянной кривизны, или вообще некоторым римановым пространством. Можно рассматривать для метрик того или иного типа погружения не только локальные, но и в целом, или погружение отдельных бесконечных областей. Можно допустить то или иное изменение степени гладкости погружения, ту или иную топологическую структуру (о состоянии этой обширной области исследований дают представление обзорные статьи и работы Э. Г. Позняка и Д. Д. Соколова (Изометрические погружения римановых пространств в евклидовы. — В кн.: Алгебра. Топология. Геометрия. Итоги науки и техники. Т. 15. — М.: ВИНИТИ, 1977, с. 173–211), Ю. А. Аминова (Проблема вложений: геометрические и топологиче-

ские аспекты. — В кн.: Проблемы геометрии. Итоги науки и техники. Т. 13. — М.: ВИНИТИ, 1982, с. 119–156), а также Э. Г. Позняка и Е. В. Шикина (Поверхности отрицательной кривизны. — В кн.: Алгебра. Топология. Геометрия. Итоги науки и техники. Т. 12. — М.: ВИНИТИ, 1974, с. 171–207).

Если обратиться к истории проблемы погружения пространств H^n постоянной отрицательной кривизны в евклидово пространство E^N (Гильберт показал, что для аналитических поверхностей при $n = 2$ и $N = 3$ вложение в целом при условии C^2-гладкости невозможно), то следует отметить, что еще в 1886 г. Ф. Шур (*Schur F.* Über die Deformation der Räume konstanter Riemannschen Krümmungsmaszes. — Math. Ann., 1986, Bd. 27, S. 170) установил возможность локального аналитического погружения пространства H^n в E^N при $N = 2n-1$. Таким образом, в частности, плоскость Лобачевского ($n = 2$) локально погружается в E^3 (примером может служить результат Миндинга 1840 г. (*Minding F.*, loc. cit.), т. е. она имеет локальный класс $N - n = 1$, но глобально (результат Гильберта) в E^3 она не погружается.

В 1938 г. А. Е. Либер (О классе римановых пространств постоянной отрицательной кривизны. — Учен. зап. Сарат. гос. ун-та. Сер. физ.-мат., 1938, т. 1 (14), № 2, с. 105–122) установил, что локально H^n ($n > 2$) не может быть погружено в виде аналитической поверхности в E^{2n-2}, т. е. локальный класс метрики H^n равен $n-1$.

Отметим, что снижение требований на гладкость поверхности, а именно отыскание решений в классе гладкости C^1, как показывают результаты работ Нэша (Nash J. F., 1954) и Кейпера (Kuiper N. H., 1955), приводит к значительному снижению размерности вмещающего пространства; так, V^n может быть тогда глобально погружено в E^{2n-1} (т. е., в частности, H^2 в E^3), однако при этом теряется обычная связь между внешними и внутренними свойствами поверхности.

В итоге исследований Д. Блануши (*Blanuša D.* Über die Einbettung hyperbolischer Räume in euklidische Räume. — Monatsh. Math., 1955, Bd. 59, № 3, S. 217–229) и Э. Р. Розендорна (Реализация метрики $ds^2 = du^2 + f^2(u)dv^2$ в пятимерном евклидовом пространстве. — Докл. АН Арм. ССР, 1960, т. 30, № 4, с. 197–199) установлено, что H^2 может быть глобально регулярно погружено в E^6, а с самопересечением — в E^5; однако вопрос о погружении в E^4 остался открытым.

Интересны результаты о погружении частей плоскости Лобачевского: Н. В. Ефимов (Непогружаемость полуплоскости Лобачевского. — Вестник МГУ. Сер. мат. мех., 1975, т. 2, с. 83–86) показал, что полуплоскость Лобачевского не может быть погружена в E^3 в виде поверхности гладкости C^4. С. И. Воробьева снизила класс гладкости до C^2 (см.: *Воробьева Л. И.* Невозможность C^2 изометрического погружения в E^3 полуплоскости Лобачевского. — Вестник МГУ. Сер. мат. мех., 1976, т. 5, с. 42–46). Отсюда непосредственно следует невозможность погружения в E^3 области плоскости Лобачевского, ограниченной двумя полупрямыми, выходящими из одной точки, а также лежащей между двумя различными прямыми на плоскости Лобачевского или вообще области, содержащей две прямые.

Важным обобщением теоремы Д. Гильберта является замечательный результат Н. В. Ефимова: полные метрики отрицательной кривизны K ($K \leqslant a < 0$), где a — произвольное число, не могут быть регулярно реализованы в целом в евклидовом пространстве (см.: *Ефимов Н. В.* Возникновение особенностей на поверхностях отрицательной кривизны. — Матем. сб., 1964, т. 64, № 2, с. 286–320)[1)].

[1)] Изложение доказательства Н. Е. Ефимова см. также в работе: *Клотц-Милнор Т.* — УМН, 1986, т. 41, № 5, с. 3–50. О дальнейших результатах в этом направлении см.: *Розендорн Э. Р.* — УМН, 1986, т. 41, № 5, с. 51–55; сб. Исследования по метрической теории поверхностей. — М.: Мир, 1980; Геометрия–III (Теория поверхностей). — Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. Т. 48. — М.: ВИНИТИ, 1989. — *Прим. ред.*

Примечания к работе **«О поверхностях постоянной гауссовой кривизны»**

[1] (с. 390). Имеется в виду конечная часть пространства.

[2] (с. 392). См. фрагмент этого доказательства в приложении к т. 1 настоящего издания.

[3] (с. 394). То есть это топологическая модель проективной плоскости.

[4] (с. 396). Имеется в виду натуральный логарифм.

[5] (с. 396). Правую часть можно представить в виде $-\mathrm{sh}(2\rho)/2$.

Примечания к приложению **„Фрагмент первого варианта работы «О поверхностях постоянной гауссовой кривизны»“**

[1] (с. 469). Более ранней является статья Хаццидакиса: *Hazzidakis J. N.* Über die Fläche mit konstanten Krümmumgsmasz. — J. reine und angew. Math., 1880, Bd. 88.

[2] (с. 475). Ее называют геодезической окружностью.

[3] (с. 475). Имеется в виду сама статья «О поверхностях постоянной гауссовой кривизны» (с. 390).

Б. Л. Лаптев

К РАБОТАМ ПО ОСНОВАНИЯМ МАТЕМАТИКИ

Безусловно, ярчайшей индивидуальной особенностью Гильберта как математика было то, что не ограничиваясь огромным личным вкладом в развитие самых разнообразных разделов математической науки, которую он, судя по всему, считал, — имея к тому серьезные основания, — „своей“, он остро ощущал свою почти что кровную связь с ней и нес на себе бремя ответственности за общее состояние ее дел. Отсюда его неусыпный интерес к ее будущему (вспомним хотя бы его знаменитый, — во многом предопределивший развитие математики в XX столетии, — доклад «Математические проблемы»[1)] на Парижском математическом конгрессе 1900 г.); отсюда же его безустальное внимание к проблемам оснований математики — этого фундамента, от прочности и надежности которого зависит не только ее настоящее, но и будущее; отсюда и такая, — ныне практически уже не встречающаяся, — эмоциональность текстов, посвященных этим вопросам.

Кроме работ, вошедших в настоящее издание, у Гильберта по данной проблематике имеется ряд других журнальных публикаций (включая и текст известного доклада[2)], прочитанного в 1927 г. на математическом семинаре Гамбургского университета), но самые фундаментальные его сочинения по основаниям математики — это, во-первых, ставшая ныне уже классической двухтомная монография «Основания математики»[3)], написанная им совместно с П. Бернайсом и, во-вторых, классический труд «Основания геометрии»[4)], выдержавший десять немецких изданий

[1)] *Hilbert D.* Mathematische Probleme. — Nachr. Ges. Wiss. Göttingen, 1900, S. 253–297. Имеется перевод в т. 2 наст. изд.

[2)] *Hilbert D.* Die Grundlagen der Mathematik. — Abh. Math. Sem. Univ. Hamburg, 1928, Bd. 6, S. 65–85; имеется перевод в кн.: *Гильберт Д.* Основания геометрии. — М.–Л.: ГИТТЛ, 1948, с. 365–388.

[3)] *Hilbert D., Bernays P.* Grundlagen der Mathematik. Bd 1, 2. — Heidelberg & New York: Springer-Verlag, 1934, 1939; 2 Aufl. Bd 1, 2. — 1968, 1970.

[4)] *Hilbert D.* Grundlagen der Geometrie. — Stuttgart: Teubner, 1899; 10 Aufl. — 1968.

и переведенный на многие языки Большую известность получил также, написанный им совместно с В. Аккерманом, один из первых в мире учебников по математической логике[1], выдержавший четыре немецких издания и тоже переведенный на ряд языков. Все эти три книги издавались на русском языке[2], причем перевод «Оснований математики» является пока единственным переводом их на другой язык. Что же касается «Оснований геометрии», то при их переводе эпиграф «Так все человеческое познание начинается с созерцания, переходит от него к понятиям и заканчивается идеями»[3], взятый Гильбертом из «Критики чистого разума» Канта, был снят[4] явным образом из-за того, что он „противоречил бы" параллельной формуле из «Философских тетрадей» Ленина: «От живого созерцания к абстрактному мышлению и от него к практике — таков диалектический путь познания».

Говоря о главных концептуальных достижениях Гильберта в области оснований математики и оставляя в стороне многие конкретные детали, — пусть даже и важные, но для автора такого масштаба выглядящие почти что техническими, — следует особо отметить два из них — это: а) создание Гильбертом *современной версии аксиоматического метода* и б) создание им, — в развитие предыдущего пункта, — *теории доказательств*, часто называемой ныне *метаматематикой*. Каждого из этих достижений любому другому хватило бы для того, чтобы навсегда остаться в истории науки.

Отдельные относящиеся к этому кругу вопросов идеи Гильберта многими не вполне отчетливо осознаются и по сей день, и чтобы облегчить читателю знакомство с комментируемыми работами, а в какой-то мере и восполнить отсутствие ряда других, не вошедших в данное издание, я попытаюсь — в несколько осовремененном виде — изложить суть упомянутых достижений. Это целесообразно сделать еще и потому, что сам Гильберт пользовался иногда архаичной, в ту пору еще не устоявшейся терминологией и порой выражал свои мысли несколько туманно (в том числе и по независящим от него причинам: в те времена еще не сформировались некоторые из действительно требовавшихся ему понятий, — например, точное понятие *алгорифма*, которое было выработано в математике лишь в 1936 г.).

Необходимо отдать себе полный отчет в том, что занятия Гильберта проблематикой оснований начались вскоре после создания Кантором его знаменитого *учения о множествах*[5] (Mengenlehre), в момент практически единодушного упоения свершившимся „прорывом в бесконечность". Учение Кантора фактически положило начало первой сознательно продуманной „архитектурной программе для математики", позволявшей по детально продуманному плану единообразным способом „возводить" математику на едином и, — надеялись! — прочном фундаменте. Быть

---

[1] *Hilbert D., Ackermann W.* Grundzüge der theoretischen Logik. — Heidelberg & New York: Springer-Verlag, 1928; 4 Aufl. — 1959.

[2] Первая из них переведена (в двух книгах) автором данного комментария с 2-го нем. изд.: *Гильберт Д., Бернайс П.* Основания математики. Логические исчисления и формализация арифметики. — М.: Наука, 1979 (2-е изд. 1982); *Гильберт Д., Бернайс П.* Основания математики. Теория доказательств. — М.: Наука, 1982; вторая — И. С. Градштейном с 7-го нем. изд.: *Гильберт Д.* Основания геометрии. — М.–Л.: ГИТТЛ, 1948; третья — А. А. Ерофеевым с 2-го нем. изд.: *Гильберт Д., Аккерман В.* Основы теоретической логики. — М.: ИЛ, 1947.

[3] В подлинике: «So fängt denn alle menschliche Erkenntnis mit Anschaungen an, geht von da zu Begriffen und endigt mit Ideen» (*Kant* „Kritik der reinen Vernunft", Elementarlehre 2. T. 2. Abt.).

[4] Так идеалисту Канту повезло гораздо меньше, чем „материалисту" Кантору, о котором речь впереди: его учение о множествах, восходящее к основоположнику объективного *идеализма* Платону, в свое время было объявлено *материалистическим*, а значит «подлинно научным и единственно правильным», и за его критику можно было попасть в большую немилость.

[5] Позже стали часто говорить о *теории* множеств, хотя, конечно же, учение и теория — это не одно и то же: последняя предполагает бóльшую степень научности, знания; между тем как в учении серьезный упор делается на веру.

может, исторически это была первая попытка восстановить достигнутую пифагорейцами, а затем с ходом развития утраченную гармонию в математике, и через нее вновь попытаться постичь Божественную гармонию мира.

Основная идея канторовской программы заключалась в том, чтобы „надстраивать" математику над теорией множеств таким образом, чтобы *все без исключения* математические понятия определялись в теоретико-множественных терминах. При последовательной реализации этого подхода, в которой деятельное участие принял также Дедекинд, *любой* математический объект в конечном счете оказывался *множеством*, удовлетворяющим некоторому характеризующему его условию, и в итоге в математике устанавливалось поразительное единообразие в структуре ее объектов, открывающее на будущее заманчивые перспективы. Идея Кантора настолько захватила Гильберта, что даже потом, уже гораздо позже, в далеко не лучшие для теории множеств времена он все еще оценивал его программу как «рай, который создал нам Кантор» (см. доклад «О бесконечном», с. 439 наст. изд.).

Начиналась реформа математики, уточнялись ее понятия и методы. Рано или поздно этот процесс должен был затронуть и один из фундаментальнейших методов математики — *аксиоматический*. Этот метод еще в III в. до Р. Х. был использован Евклидом в его «Началах» для изложения основ геометрии, и с тех пор он до конца XIX в. не претерпел никаких принципиальных изменений. Вместе с тем, изложение Евклида изобиловало многими несовершенствами: основные объекты геометрии (точки, прямые, плоскости) имели у него какие-то странные, совершенно нематематического характера „определения" типа «линия — это длина без ширины», исходя из которых вообще ничего доказать нельзя; имелись аксиомы, которые с учетом этих определений должны были выглядеть *очевидными*, но для этого, во-первых, приходилось опираться на какие-то скрытые, подразумеваемые толкования определений, а во-вторых, степень очевидности этих аксиом в результате все равно оказывалась неодинаковой (вспомним хотя бы историю с так называемым V постулатом Евклида); и т. д. и т. п.

В 1898–99 гг. учебном году Гильберт прочел в Гёттингене курс лекций по геометрии. В этом курсе он поступил решительно вразрез с традицией, далеко опередив свое время; поступил почти так, как если бы у него уже имелся изрядный опыт общения с компьютером. Изложим суть дела так, как оно обстояло у Гильберта фактически, игнорируя ту словесную форму, в которую оно было облечено „по педагогическим соображениям".

Фактически Гильбертом была построена некая *формальная теория*, и для того, чтобы иметь возможность говорить о ее объектах, он сначала разработал особый *формализованный язык* с точной синтаксической структурой. В этом языке имелись: 1) переменные для «вещей» трех различных типов и 2) некоторое количество знаков для «отношений» между этими вещами. Затем, исходя из переменных и знаков для отношений, по точно сформулированным *синтаксическим правилам* этого языка конструировались выражения определенного, алгорифмически распознаваемого типа, которые получали у Гильберта статус «высказываний». Некоторые из них он объявил «аксиомами» (эти последние легко распознавались по их внешнему виду). Исходя из аксиом, предлагалось по правилам формальной логики[1)], — чисто *механически*, для чего указывался алгорифм, — выводить новые выражения этого языка, которые в данном случае снова оказывались высказываниями. Они-то и объявлялись Гильбертом «теоремами» этой формальной теории. (В порядке сюрприза для „нетренированного" читателя, заметим, что вопрос об *истинности* теорем и аксиом фактически Гильбертом даже не ставился: речь у него шла просто о *выводимости* теорем из аксиом.)

И конечно же эти „теоремы" были теоремами геометрии! Сказанное надо по-

---

[1)] Здесь, конечно, подразумевалась традиционная аристотелевская логика, верность которой, несмотря на критику Брауэра, Гильберт сохранил на всю свою жизнь.

нимать следующим образом: если вместо упоминавшихся выше переменных для «вещей» в высказывания подставлять соответственно геометрические точки, прямые и плоскости в какой-нибудь их точной интерпретации, а вместо знаков для «отношений» надлежащим образом подставлять геометрические отношения *инцидентности, между* и т. д. (в той же самой интерпретации), то аксиомы построенной Гильбертом формальной теории перейдут в аксиомы евклидовых «Начал», а ее теоремы — в теоремы евклидовой геометрии. Таким образом, евклидова геометрия оказывается „моделью" гильбертовой формальной системы. (Аккуратнее сказать — *одной* из ее моделей.)

Такой подход к геометрии позволяет решить сразу несколько задач: 1) отпадает надобность в „изначальных" евклидовых определениях точек, прямых и плоскостей; 2) в этой аксиоматике исчезают подразумеваемые представления: в ней можно использовать лишь те „сведения" о точках и т. п., которые явно формулируются в аксиомах; 3) появляется возможность в точных терминах обсуждать вопросы: 3.1) о независимости тех или иных аксиом геометрии, 3.2) о непротиворечивости этой системы аксиом[1)] и так далее. Наконец, появляется возможность интересоваться вопросом о том, нет ли у этой системы аксиом каких-нибудь других моделей. В своей прощальной речи «Познание природы и логика», произнесенной в связи с уходом на пенсию, Гильберт с нескрываемым удовольствием говорит об одной модели подобного рода из области генетики: «Так просто и так точно! И вместе с тем все это выглядит таким чудом, что об этом ранее, пожалуй, никто не смог бы даже помыслить в самых смелых своих мечтах» (см. с. 458–459 наст. изд.). Очень красивую «электротехническую» модель упоминает Г. Вейль в своей статье «Давид Гильберт и его математические труды» (имеется перевод в т. 2 наст. изд.; см. раздел «Аксиоматика»).

Следует особо подчеркнуть, что занимаясь выводом теорем в формальной системе, о которой у нас идет речь, человек *может* (другое дело, что он *не должен* этого делать!) вести себя чисто *механически*, не интересуясь *смыслом* того, что́ у него при этом получается. Несколько пофантазировав, мы можем представить себе ситуацию, в которой он даже будет *вынужден* делать это в силу каких-нибудь посторонних причин. В самом деле, грамматические категории формализованного языка, с которым он имеет дело, алгорифмически проверяемы, а правила, применяемые в процессе логического вывода, носят чисто механический характер, и значит, вся эта работа может быть поручена не только человеку, но и какому-нибудь автоматическому устройству — например, компьютеру. Во времена Гильберта вопрос этот еще не мог стать в повестку дня, но любопытно, что кратко обрисованная здесь концепция фактически предвосхитила не только весь структурализм XX века, но и всю идеологию машинной математики: компьютер *не должен* понимать ничего; идеально *общепонятным* может быть лишь то, что вообще не требует никакого понимания!

И это не единственный случай предвосхищения в истории оснований математики. В качестве особо впечатляющих примеров я упомяну лишь два: 1) произведенное (причем одновременно и независимо друг от друга четырьмя математиками сразу[2)] — А. Чёрчем, С. К. Клини, А. М. Тьюрингом и Э. Л. Постом) в 1936 г., — когда никаких компьютеров еще не было и в помине, — уточнение общего понятия *алгорифма*, этого математического эквивалента понятия *компьютерной программы*, ныне далеко шагнувшего за пределы не только математики, но и Computer Science, и 2) основополагающую работу С. К. Клини[3)], давшую вместе с работой

[1)] Данный вопрос в известном смысле решается в § 9 гл. 2 «Основания геометрии»: более точно, он сводится здесь к вопросу о непротиворечивости теории вещественных чисел.

[2)] Библиографию см., напр., в кн.: *Марков А. А., Нагорный Н. М.* Теория алгорифмов. 2-е изд. — М.: Фазис, 1996.

[3)] *Kleene S. C.* On the interpretation of intuitionistic number theory. — J. Symbolic Logic, 1945, vol. 10,

его ученика Д. Нельсона[1] исчерпывающее теоретическое обоснование возможности синтеза компьютерных программ по их спецификациям за несколько десятилетий до возникновения самой этой проблемы. Это ли не ярчайшие примеры той «предустановленной гармонии», о которой с таким энтузиазмом и вдохновением говорил в упомянутой выше речи Гильберт!

Перейдем теперь к вопросу о *теории доказательств*. Как известно, на рубеже XIX и XX столетий основания теории множеств были потрясены неожиданно разразившимся кризисом: в ней были обнаружены самые что ни на есть контрадикторные *противоречия*, которые то ли из эвфемизма, то ли из ужаса перед ними стали называть „удобными", анестезирующими словами «парадокс» и «антиномия». Шокирующий, невыносимый (по выражению Гильберта) смысл этого открытия заключался в том, что в математике, „надстроенной" по рецепту Кантора над теорией множеств, после обнаружения *хотя бы одного* такого „парадокса" становились — по правилам логики — *доказуемыми* (а стало быть, и истинными?!) *все* высказывания — в том числе, например, и равенство $0 = 1$. «И на учение Кантора с самых различных сторон посыпались ожесточеннейшие нападки» — говорит, вспоминая уже в 1925 г. события того времени, Гильберт (см. доклад «О бесконечном», с. 438 наст. изд.). Безусловно, этим открытием был потрясен и он сам. Говоря о «противоречии, найденном Цермело и Расселом»[2], Гильберт отмечает, что оно «...оказало на математический мир прямо-таки катастрофическое воздействие». И далее с чувством большой тревоги, — едва ли не отчаяния, — он восклицает: «Перед лицом этих парадоксов надо согласиться, что положение, в котором мы пребываем сейчас, на длительное время невыносимо. Подумайте: в математике, — этом образце надежности и истинности, — понятия и умозаключения, как их всякий изучает, преподает и применяет, приводят к нелепостям[3]. Где же тогда искать надежность и истинность, если даже само математическое мышление дает осечку?» (см. доклад «О бесконечном», там же).

Впечатление отчаяния усиливается еще больше, когда внезапно начинаешь понимать, что последняя фраза цитаты — это ведь фактически слова из заупокойной мессы, «Реквиема» (конец „Tuba mirum"):

Quid sum miser tunc dicturus?
Quem patronum rogaturus
Cum vix justus sit securus?[4]

Гильберт, безусловно д о л ж е н б ы л выступить в защиту «рая, созданного для него Кантором», и он сделал это с присущей ему энергией и изобретательностью!

---

p. 109–124.

[1] *Nelson D.* Recursive functions and intuitionistic number theory. — Trans. Amer. Math. Soc., 1947, vol. 61, p. 307–368.

[2] Впоследствии за ним установилось название „парадокса Рассела". Трагической жертвой этого парадокса стал знаменитый Г. Фреге, в 1-м томе трактата которого (*Frege F. L. G.* Grundgesetze der Arithmetik. Begriffsschriftlich abgeleited. Bd. 1, 2. — Jena: Pohle, 1893, 1903) этот парадокс и был обнаружен в 1902 г. Б. Расселом. Подробнее см. об этом, напр., в книге *Марков А. А., Нагорный Н. М.*, op. cit., с. XII–XIII.

[3] В подлиннике — Ungereimtheit. Буквально: несрифмованность, отсутствие рифмы — т. е. нелепость, вздор, бессмыслица, чепуха, ахинея...Читатель почти успокоен: нелепый человек часто мил; ахинея, чепуха — такие, в общем, пустячки... Увы, ни одно из этих слов, — в том числе и Ungereimtheit, — не адекватно ситуации. Несколькими строками выше Гильберт употребляет „настоящее" слово — Widerspruch (противоречие)! Но, конечно же, соображения стиля мешают ему употребить это слово дважды...

[4] В переводе с латинского:

Что тогда скажу я, несчастный?
К кому обращусь за покровительством,
Когда и праведник едва спасется?

Одним из самых уязвимых мест канторовской концепции являлось понимание *экзистенциальных математических высказываний*, то есть высказываний о *существовании* математических объектов. Что́ имеется здесь в виду, когда про один из них утверждается, что он *существует*? Такой объект, как об этом уже говорилось, всегда представляет собой некоторое *множество*, и так как никакого *определения* множества мы в учении Кантора не находим (обычно это понятие разъясняется в нем лишь „на примерах"), то ответить на поставленный вопрос особенно нелегко.

И вот Гильберт предлагает искусный выход из положения, выход, который легче всего понять на каком-нибудь простом примере. Мы в качестве такого примера возьмем „чистую" теорию чисел — арифметику Пеано, это «чистейшее, — по словам Гильберта, — и наивнейшее дитя человеческого духа» (см. доклад «О бесконечном», с. 434 наст. изд.). Натуральный ряд по Кантору определяется как множество, описываемое аксиомами Пеано, и Гильберт предлагает *существование* натурального ряда понимать как *непротиворечивость* этих описывающих его аксиом. Именно ее и требуется теперь установить.

Записывая аксиомы Пеано на специальном формализованном *логико-арифметическом языке* и подключая к ним аксиомы формальной логики в виде *исчисления предикатов*, Гильберт получает формальную систему, в которой „доказательство", то есть «вывод» из аксиом, есть наглядный, синтаксический, — *конструктивный*, как теперь говорят, — объект, допускающий кодирование „нуликами и единичками". Эти выводы суть объекты, алгорифмически распознаваемые. Задача сводится теперь к тому, чтобы показать, что *хоть что-то*, — например, равенство $0 = 1$ — *невыводимо* в этой системе, то есть не является заключительной формулой никакого вывода. Гильберт уверен, что сделать это легко: он даже *ограничивает* — правда, несколько туманно и никогда не сделает этого в четкой форме — круг средств, которые он считает допустимыми и надежными (имеется в виду его «финитная установка»; см. доклад «О бесконечном», с. 439–442 наст. изд.).

То же самое Гильберт предлагает проделать и с остальными математическими теориями (в том числе и с теорией множеств!): сначала аксиоматизировать их, потом доказать их непротиворечивость и уж затем развивать эти теории. (Именно в этом порядке! Вскоре, правда, эпигоны гильбертовой программы второй этап станут „отодвигать" на второй же план — может быть потому, что с ним, — а особенно в случае аксиоматической теории множеств[1], — дело оказалось совсем не таким уж простым.) Гильберт надеялся устроить *полные* и *непротиворечивые* аксиоматики всех основных математических теорий и таким способом «...разделаться с проблемами оснований как таковыми раз и навсегда»[2] В этом должна была заключаться третья, как мне представляется, „архитектурная программа для математики". (Второй из этих программ — весьма необычной *интуиционистской* программы Л. Э. Я. Брауэра[3] — мы здесь за недостатком места коснуться не имеем возможности; остается, стало быть, в стороне и ожесточенная научная полемика между Гильбертом и Брауэром, к сожалению, со временем осложнившая и личные отношения этих двух великих математиков и мыслителей. Смотри об этом, например, раздел «Аксиоматика» в уже упоминавшейся статье Г. Вейля, где он пишет: «...Л. Э. Я. Брауэр своим интуиционизмом открыл нам глаза и заставил увидеть, насколько далеко общепринятая математика выходит за рамки таких утверждений, которые могут претендовать на реальный смысл и истинность, основанную на очевидности. Мне жаль, что в своей оппозиции Брауэру Гильберт никогда открыто

---

[1] Здесь наибольшее распространение получила знаменитая ZF — система Цермело — Френкеля.

[2] См. упоминавшийся выше доклад Гильберта «Die Grundlagen der Mathematik».

[3] Краткую ее характеризацию можно, например, найти, в книге *Марков А. А., Нагорный Н. М.*, op. cit., с. XVIII–XX.

не признал, насколько он, равно как и другие математики, в долгу перед Брауэром за это открытие.

Гильберт не хотел приносить тяжелые жертвы, которых требовала точка зрения Брауэра. Он увидел, по крайней мере в общих чертах, тот путь, который позволит избежать жестокого увечья. В то же время он был обеспокоен признаками колебания в среде математиков, ряд которых открыто встал на сторону Брауэра.».

Колебания, о которых пишет Вейль, это ведь и его колебания — колебания любимейшего ученика, причинившего боль недавно ушедшему учителю[1]. Его слова о «тяжелых жертвах», о «жестоких увечьях» — в сущности повторенные им слова Гильберта, слова, несправедливость которых он отчетливо сознает, — звучат как покаянная жертва. Но жертва эта мучительна: ведь он понимает, что их прочтет и Брауэр...).

Мы теперь знаем, что реализация этой программы Гильберта столкнулась с серьезными трудностями. И более того, отчетливо понимаем, что она неизбежно должна была столкнуться с ними, поскольку была нацелена на реабилитацию мероприятия, фактически безнадежного. О громадной и загадочной суггестивной мощи, которую несет в себе канторовская идея, мне уже приходилось писать ранее (*Марков А. А.*, *Нагорный Н. М.*, op. cit., с. XXV), и мне кажется, что слова коржавинской «Наивности» о тех,

. . . в ком дух железный,
Кто преградил сомненьям путь,
В чьем сердце страх увидеть бездну
Сильней, чем страх в нее шагнуть,

очень удачно передают сложившуюся здесь ситуацию. Даже задача установления непротиворечивости „чистой" арифметики была впервые решена учеником Гильберта Г. Генценом только в 1936 г. и то — лишь средствами, не укладывающимися в финитную установку Гильберта. К настоящему времени известны три ее решения, принадлежащие Генцену, два решения К. Шютте, а также решения В. Аккермана, Л. Кальмара, П. Лоренцена, П. С. Новикова, И. Н. Хлодовского и автора данного комментария[2]. Степень совместимости приводимых авторами доказательств с финитной установкой Гильберта анализируется далеко не всегда, а отдельные авторы демонстративно считают этот вопрос «проблемой субъективной природы». Последнее из перечисленных здесь доказательств, не укладываясь в рамки финитной установки, обладает, тем не менее, той особенностью, что в нем выдержан принцип некоего „логического консенсуса": оно одинаково приемлемо и для теоретико-множественно настроенного математика, и для интуициониста, и для конструктивиста марковского направления. Что же касается проблемы установления непротиворечивости анализа, от решения которой зависит, по мнению Бернайса[3], «окончательный приговор судьбе теории доказательств», то она не решена до сих пор, не говоря уж о проблеме непротиворечивости аксиоматической теории множеств, интерес к которой сейчас, — в связи с многочисленными „результатами о независимости", — носит, пожалуй, скорее спортивный, чем математический характер[4]. К обсуждению этой проблемы мы еще вернемся.

Тяжелый удар по теории доказательств был нанесен той же осенью 1930 г. и в том же Кёнигсберге, где Гильберт 8 сентября произносил свою уже упоминавшую-

---

[1] Статья опубликована в 1944 г., через год после кончины Гильберта.

[2] Библиографию можно найти, напр., в моей работе «К вопросу о непротиворечивости классической формальной арифметики». Сообщения по прикладной математике. — М.: ВЦ РАН, 1985; или в кн.: *Мендельсон Э.* Введение в математическую логику. 3-е изд. — М.: Наука, 1984.

[3] Смотри, напр., его предисловие к книге: *Гильберт Д., Бернайс П.* Основания математики. Теория доказательств. — М.: Наука, 1982, с. 13.

[4] Детальное критическое обсуждение данной ситуации можно найти, напр., в *Марков А. А., Нагорный Н. М.*, op. cit., с. XV–XVI.

ся выше прощальную речь, знаменитым и теперь уже общеизвестным результатом К. Гёделя[1] о *неполноте*, — и даже *непополнимости*, — арифметики, о непротиворечивости которой мы только что говорили. Фактически Гёделем была доказана не только невозможность полной непротиворечивой ее аксиоматизации, но и — в определенном точном смысле слова — невозможность доказать ее непротиворечивость, средствами, формализуемыми в ней самой. Гильберт впервые услышал о работе Гёделя от Бернайса, и он был «слегка рассержен». В предисловии к 1-му тому монографии «Основания математики», рукопись которой из-за этого результата пришлось „ремонтировать", притом в крайне тяжелых условиях (с приходом к власти Гитлера Бернайс вынужден был эмигрировать), Гильберт пишет: «...я хотел бы подчеркнуть, что возникшее на определенное время мнение, будто из некоторых недавних результатов Гёделя следует неосуществимость моей теории доказательств, является заблуждением. Этот результат на самом деле лишь показывает, что для более глубоких доказательств непротиворечивости финитная точка зрения должна быть использована некоторым более сильным образом, чем это оказалось необходимым при рассмотрении элементарных формализмов». Здесь уже явственно слышны раскаты грома. И близится публикация Г. Генцена...

Странная и, по существу, гротескная ситуация сложилась с теорией ZF, естественным образом рассматриваемой на базе традиционной аристотелевской логики. Это, как уже отмечалось, — наиболее популярный вариант *аксиоматической теории множеств*. Однако, в настоящий момент, несмотря на крайнюю заинтересованность специалистов, непротиворечивость этой теории *не установлена*. Если однажды вдруг окажется, что ZF противоречива, то в ней можно будет доказать *что угодно* (и значит, она будет ненужна). При условии же, что она окажется непротиворечивой, в ней, — вследствие знаменитых ныне результатов Гёделя (1939 г.), П. Дж. Коэна (1962–63 гг.), П. Вопенки (1962–64 гг.), а затем и других авторов, — будут недоказуемы: ни аксиома выбора, ни ее отрицание; ни континуум-гипотеза[2], ни ее отрицание; и т. д. и т. п. Количество таких „дыр" в ZF уже сейчас можно было бы значительно увеличить и никто не сомневается, что наряду со старыми в дальнейшем обнаружатся новые. Возникает естественный вопрос: какой прок от *такой* теории множеств?

Таким образом, на первый взгляд и сама теория доказательств, и ее создатель потерпели фиаско. И тем не менее, сказать так было бы глубоко неверно: неудачи гениев иногда бывают столь же плодотворны, как и их взлеты. Безусловно, математическую логику создал не Гильберт, и не ему принадлежат самые трудные и самые знаменитые теоремы этой науки. И однако Отцом математической логики — и с полным на то правом! — считается именно он. Гильбертом были сформулированы важные задачи — пусть иногда (вспомним его 10-ю проблему) даже не совсем удачно — и благодаря именно его авторитету к ним было привлечено внимание искусных мастеров. Под его влиянием возникли выдающиеся результаты Гёделя, обнаружившие границы и тщету структуралистского мышления. Не без его воздействия возникла и *точная* теория алгорифмов (а на ее базе и четвертая „архитектурная программа для математики" — *конструктивизм Маркова*). Но он же своей поистине фанатической преданностью аристотелевской логике (особенно закону исключенного третьего) стоял на пути прогресса в логике почти полстолетия, и здесь влияние его

---

[1] *Gödel K.* Über formal unentscheidbare Sätze der «Principia Mathematica» und verwandter Systeme. I — Monatshefte für Mathematik und Physik, 1931, Bd. 38, S. 173–198. Рукопись статьи была представлена в редакцию журнала 17-го ноября 1930 г.

[2] Конечно, речь здесь идет о „казенной" недоказуемости, — т. е. о невозможности соответствующих *выводов*, — и если это обстоятельство четко иметь в виду, то станет ясно, что мнения типа того, что «такими-то и такими-то авторами получено *решение* континуум-проблемы», необоснованно. Результаты такого рода показывают разве лишь то, что *подлинное* решение *подлинной* континуум-проблемы является невероятно трудным делом, и на „казенном" пути, — т. е. в виде *вывода*, — оно получено быть не может.

мощного авторитета ощущается и по сей день. Им была создана крупная — и поистине новаторская! — концепция: «Математика без апелляции к Смыслу». Такая идея могла придти в голову только гению, характер, природу и „последействие" которого нам, возможно, еще предстоит полностью ощутить и понять.

Н. М. Нагорный [1)]

ОБ ОСНОВАНИЯХ ЛОГИКИ И АРИФМЕТИКИ

[1] (с. 399). Доклад Гильберта на III Международном математическом конгрессе (Гейдельберг, 1904 г.) опубликован в трудах этого конгресса, а также в седьмом (1930 г.) издании «Оснований геометрии» (добавление VII). См.: *Гильберт Д.* Основания геометрии. Перевод И. С. Градштейна. — ГИТТЛ: М.–Л., 1948, с. 322–337. Перевод И. С. Градштейна был учтен при подготовке настоящего издания. Публикация этого доклада в «Основаниях геометрии» снабжена примечанием: «Хотя этот доклад по своему содержанию и был перекрыт моими более поздними исследованиями по основаниям математики, мне все же показалось полезным снова поместить его здесь, особенно потому, что я в этом докладе впервые изложил многие концепции и методы исследования, как, например, требование непротиворечивости, самостоятельное рассмотрение множества как некоторой вещи, тенденцию к финитной установке, совместное исследование логики и арифметики».

[2] (с. 399). В «Основаниях геометрии» Гильберт свел проблему непротиворечивости геометрии к доказательству непротиворечивости арифметики вещественных чисел.

[3] (с. 400). Речь идет о неограниченном принципе свертывания, т. е. определении множества как объема произвольного «мыслимого» понятия, или же как совокупности элементов, обладающих произвольным выразимым в языке ZF свойством F:

$$\exists y \quad \forall x \quad (x \in y \equiv F(x)),$$

где y — определяемое множество, элементы которого обладают свойством F (см.: *Френкель А., Бар-Хиллел И.* Основания теории множеств. — М.: Мир, 1966, с. 171–174).

[4] (с. 400). См.: *Dedekind R.* Was sind und was sollen die Zahlen. Braunschweig, 1888. (Имеется перевод: *Дедекинд Р.* Что такое числа и для чего они служат. — Известия Физ.-мат. о-ва Казанского университета, 1906, т. 15, с. 25–104.)

[5] (с. 401). Первый параграф упомянутого в предыдущем примечании сочинения Дедекинд начинает так:

«I. Условимся на будущее время понимать под *вещью* всякий объект нашего сознания. Для того, чтобы было удобней вести речь о «вещах», мы будем означать их какими-либо знаками, например, буквами, и будем просто говорить о вещи a или об a, разумея под a в действительности, конечно, означаемый буквой a объект, но не самую букву.» *Dedekind R.* Was sind und was sollen die Zahlen. — Braunschweig, 1888, S. 11.

[6] (с. 401). Воспитанник Гёттингенского университета Х. Б. Карри (1900–1981) защитил в 1930 г. докторскую диссертацию, предметом которой является теория комбинаторов. Исходными объектами теории служат константы и переменные, новые объекты строятся из исходных и полученных ранее посредством операции аппликации: если a и b — объекты, то (ab) считается объектом. Одной из наиболее примечательных особенностей комбинаторных теорий является бестиповость, или

[1)] Комментарий подготовлен в рамках гранта № 97-06-80211 РФФИ.

равноправие переменных. Так, если f — функциональная, x — предметная переменные, то каждая из них есть объект: из них посредством аппликации получаются объекты

$$(xf),\quad (xx),\quad (fx),\quad (ff),\quad ((fx)f),\quad ((xf)f),\quad ((ff)x)$$

и т. д.

Обычно в числе самых ранних работ, относящихся к комбинаторным теориям, называют статью нашего соотечественника М. И. Шейнфинкеля, опубликованную в 1924 г. (Math. Ann., 1924, Bd. 92, S. 305–316) Бёманом на основании его записи доклада, который Шейнфинкель прочел на семинаре Гильберта 7 декабря 1920 г. (см., например, *Клини С. К.* Введение в метаматематику. — М.: ИЛ, 1957, с. 286). Теория «вещей» Гильберта, очевидно, является более ранним источником подобных теорий.

[7] (с. 402). $x^{(\lambda)}$ и $x^{(\iota)}$ — это кванторы, соответственно, существования и общности (в современных обозначениях $\exists x$ и $\forall x$, x) — предметная переменная, «пробегающая» множество всех мыслимых вещей и их комбинаций.

[8] (с. 402). Иными словами, равенство 2 означает: «Для всяких мыслимых вещей x и y, если $x = y$ и x обладает свойством w, то y обладает свойством w. Иногда подобную аксиому называют принципом Лейбница (см.: *Клини С. К.* Математическая логика. — М.: Мир, 1973, с. 194).

[9] (с. 403). Мыслимая вещь $б$ (бесконечное множество), например, множество натуральных чисел, или же порядковых чисел: c — «следующий за», аналог прибавления единицы, c' — «предшественник», например, на множестве натуральных чисел $c'(n+1)$ есть n. Эти обозначения расходятся с общепринятым в дальнейшем, в том числе и самим Гильбертом, обозначением c'. Сейчас говорят об арифметической размерности $n-1$.

[10] (с. 403). В комбинаторных теориях аппликацию можно истолковывать как принадлежность элемента множеству, считать (ab) означающим, что $b \in a$. (См.: *Барендрегт Х.* Ламбда-исчисление. Его синтаксис и семантика. — М.: Мир, 1985, с. 43, 101.)

[11] (с. 406). «Произвольные» Гильберта — это предметные переменные, пробегающие некоторое множество «мыслимых» вещей.

[12] (с. 406). Таким образом, «множество» оказывается частным случаем «мыслимой вещи», а излагаемая здесь теория «мыслимых вещей» Гильберта более широкой, чем теория множеств. Здесь видно явное стремленье Гильберта найти основание математики, более надежное, чем теория множеств, дискредитированная парадоксами.

[13] (с. 407). В статье «О бесконечном» Гильберт использует иную терминологию, вместо «несуществующих вещей» он говорит об «идеальных элементах».

[14] (с. 408). См. с. 111–113, гл. III книги: *Гильберт Д.* Основания геометрии. — М.–Л.: ГИТТЛ, 1948.

З. А. Кузичева

АКСИОМАТИЧЕСКОЕ МЫШЛЕНИЕ

Этот доклад Гильберта существенно проясняет его взгляды на роль аксиоматического метода не только для обоснования математики в целом, но и для конкретных математических и физических теорий (см. *Демидов С. С.*, в сб. «Методологический анализ оснований математики». — М.: Наука, 1988, с. 104–107).

[1] (с. 412). См. доклад «Математические проблемы» (6-ая проблема) и комментарии к работам по физике в т. 2 настоящего издания.

[2] (с. 413). Работы Гильберта по теории излучения (1912–1914 гг.) собраны в его собрании сочинений (см. Ges. Abh., Bd. 3, S. 217–257. — Springer-Verlag: Berlin, 1935).

[3] (с. 415). См. комментарии к работам по теории инвариантов.

[4] (с. 416). См. комментарии к работам «О вещественных ветвях алгебраических кривых» и «О форме поверхности четвертого порядка».

ЛОГИЧЕСКИЕ ОСНОВАНИЯ МАТЕМАТИКИ

В серии докладов, с которыми Гильберт выступил в 20-е годы, разъяснялась его позиция в решении проблемы обоснования математики. Эта проблема возникла в связи с появлением трудностей, в том числе парадоксов, в теории множеств. Основным инструментом обоснования математики Гильберт считал формальный аксиоматический метод, впервые продемонстрированный им в «Основаниях геометрии». Методы обоснования классической математики, предложенные им, стали называть «программой Гильберта», а возглавляемую им школу — формализмом, или «формалистическим направлением» в основаниях математики, в противоположность подходу Брауэра, названному «интуиционистским», или «интуиционизмом». Программа Гильберта, таким образом, состояла в том, чтобы аксиоматизировать важнейшие разделы классической логики, доказать непротиворечивость этих аксиоматизированных (формальных) систем и тем самым спасти классическую математику, включая канторовскую теорию множеств.

Позиция Гильберта подверглась резкой критике, можно даже сказать нападкам, со стороны Брауэра и его последователей. Подробно позиции Брауэра и Гильберта описаны в кн.: *Клини С.* Введение в метаматематику. — М.: ИЛ, 1957, ч. I, гл. III, §§ 13, 14; *Френкель А., Бар-Хиллел И.* Основания теории множеств. — М.: Мир, 1966, гл. IV, V.

В процессе попыток реализации своей программы Гильберт получает интересные чисто математические результаты. К их числу можно отнести рассмотрение рекурсивных функций некоторых частных типов.

Истоки этой теории можно усмотреть в практике использования рекуррентных формул, примером которых могут быть формулы для последовательности чисел Фибоначчи

$$\left.\begin{aligned} \Phi(0) &= 0 \\ \Phi(1) &= 1 \\ \Phi(n+2) &= \Phi(n) + \Phi(n+1). \end{aligned}\right\}$$

Первые определения, которые теперь принято называть рекурсивными, были опубликованы в XIX в. при построении вариантов систем аксиом натуральных чисел. Наиболее ранним является строгое построение арифметики в трудах братьев Г. и Р. Грассманов. В современной символике предложенное ими определение сложения и умножения можно записать в виде

$$\begin{aligned} a+0 &= a & \qquad a\cdot 0 &= 0 \\ a+1 &= a' & \qquad a\cdot 1 &= a \\ a+b' &= (a+b)' & \qquad a\cdot n' &= an+a. \end{aligned}$$

(см.: *Grassman H.* Ausdehnungslehre. — Leip., 1844; Lehrbuch der Arithmetik. — Berlin, 1861; *Grassman R.* Zahlenlehre oder Arithmetik. — Stettin., 1872.)

В 1889 г. опубликована широко известная теперь система аксиом Пеано. Несколько раньше опубликованы аксиомы Дедекинда. Оба автора приводят рекурсивное определение сложения и умножения. Современный термин «рекурсия» при этом

не используется. Пеано молчаливо предполагает, что законность такого определения следует из аксиомы полной индукции; Дедекинд доказывает их как теоремы:

$$m+1=m' \qquad m\cdot 1=m$$
$$m+n'=(m+n)' \qquad m\cdot n'=mn+m$$

(см.: *Dedekind R.* Was sind und was sollen die Zahlen. — Braunschweig, 1888. Имеется перевод: *Дедекинд Р.* Что такое числа и для чего они служат. — Известия Физ.-мат. о-ва Казанского университета, 1906, т. 15, с. 25–104).

В настоящем докладе Гильберт употребляет термины «рекурсия» и «определение посредством рекурсии» как уже известные слушателям. В исторических замечаниях к изложению теории рекурсивных функций последующие авторы (см., например: *Петер Р.* Рекурсивные функции. — М.: ИЛ., 1954, § 21) называют Гильберта в числе основателей этой теории. Нигде не удалось найти упоминания о том, когда же и у кого впервые появляется термин «рекурсия». Так что установление этого факта представляет интересную историко-математическую проблему.

Здесь Гильберт приводит схемы рекурсивного определения функции, перечисляющей некоторую последовательность действительных чисел. Он определяет также функцию, называемую теперь характеристической функцией множества, и приводит схему определения такой функции.

Термин «примитивная рекурсия» Гильберт не употребляет в этом докладе, не ставит вопроса и о классификации (или градации) таких функций. Однако позднее, в 1925 г., он ставит глубокую проблему о скорости роста некоторой рекурсивной функции. (См.: *Hilbert D.* Über das Unendliche. — Math. Ann., 1925, Bd. 95, S. 185–186. Мы используем в изложении обозначения Клини. См.: *Клини С. К.*. loc. cit., с. 246.)

Пусть $\varphi_0(b,a)=a+b$, $\varphi_1(b,a)=a\cdot b$, $\varphi_2(b,a)=a$. Продолжим эту последовательность при помощи «обычных» рекурсий вида $\varphi_{n'}(0,a)=a$, $\varphi_{n'}(b',a)=\varphi_n(\varphi_{n'}(b,a),a)$, $n\geqslant 2$. Тогда $\varphi_3(b,a)=a^{a^{a^{\cdot^{\cdot^{\cdot}}}}}\}^{b\text{ раз}}$. Рассматриваем далее $\varphi_n(b,a)$ как функцию $\varphi(n,b,a)$ от трех переменных n,b,a.

Определим теперь функцию α:

$$\alpha(n,a)=\begin{cases}0, & \text{если } n=0,\\ 1, & \text{если } n=1,\\ a & \text{в остальных случаях.}\end{cases}$$

Тогда $\varphi(n,b,a)$ определяется следующей схемой:

$$\varphi(0,b,a)=a+b,\quad \varphi(n',0,a)=\alpha(n,a),\quad \varphi(n',b',a)=\varphi(n,\varphi(n',b,a),a).$$

Положим теперь

$$\varphi(a)=\varphi(a,a,a).$$

Гильберт поставил вопрос: является ли $\varphi(a)$ примитивно рекурсивной, или, более общо: имеются ли рекурсии, не сводимые к «обычной» (т. е. примитивной) рекурсии.

Аккерман В. показал, что $\varphi(a)$ с увеличением a возрастает быстрее, чем любая примитивно рекурсивная функция. Доказательство Аккермана опубликовано в Math. Ann., 1928, Bd. 99, S. 118–133. Гильберт упоминает это доказательство в подстрочном примечании на с. 185 статьи «Über das Unendliche».

На дальнейшее развитие теории рекурсивных функций оказало влияние появление известной статьи Гёделя (см.: Monatshefte f. Math. und Phys., 1931, Bd. 38, S. 173–198), а также осознание адекватности отождествления рекурсивности с вычислимостью (см.: *Church A.* — Amer. journ. Math. Soc., 1936, v. 58, p. 345–363; *Cleene S. C.* Duke math. journ., 1936, v. 2, p. 340–353; *Turing A.* Proc. Lond. Math. Soc. Ser. 2, 1936–37, v. 42, p. 230–265).

[1] (с. 418). Цермело Э. (1871–1953). См.: *Zermelo E.*, Math. Ann., 1904, Bd. 59, S. 514–516; Math. Ann., 1908, Bd. 65, S. 107–128.

[2] (с. 420). Это, пожалуй, наиболее понятное описание «финитного».

[3] (с. 423). Гильберт предлагает здесь вывод в виде последовательности перестроить в такой, который теперь принято называть выводом в виде дерева. В «Основаниях математики» Гильберта и Бернайса (1934 г.) этот способ назван «разложением фигуры доказательства на нити вывода». См.: *Гильберт Д., Бернайс П.* Основания математики. Теория доказательств. § 6, b), 1; § 8, d), 2. — М.: Наука, 1982.

[4] (с. 424). μ-символ впоследствии сделался общеупотребительным в теории рекурсивных функций: μ-оператор, или оператор минимизации, определяется следующим образом: $\mu_y(f(x_1,\ldots,x_n,y)=0)$ означает наименьшее значение y, для которого $f(x_1,\ldots,x_n,y)=0$. Это неограниченный μ-оператор. Ограниченный μ-оператор

$$\mu_{y<z}(f(x_1,\ldots,x_n,y)) = \begin{cases} \text{такому наименьшему } y, \text{ что } y<z \text{ и} \\ f(x_1,\ldots,x_n,y)=0, \text{ если такое } y \text{ существует;} \\ z \text{ в противном случае.} \end{cases}$$

[5] (с. 424). В соответствии с точкой зрения Брауэра функция определена, если известно, какая из двух возможностей $f(a)=0$ или $f(a)\neq 0$ имеет место. В случае конечного множества, которому принадлежат значения аргумента, вопрос решается перебором; в случае бесконечного — перебор может не дать результата, если за какое-то разумное число шагов не получен ответ на вопрос о том, какое же равенство имеет место в точке a, не достигнутой в этом переборе. См. также примечание [9].

[6] (с. 426). См.: *Вейль Г.* Континуум. — В кн.:*Вейль Г.* Математическое мышление. — М.: Наука, 1989, § 6; Порочный круг в современном обосновании анализа. — В кн.: *Вейль Г.* Избранные труды. Математика, теоретическая физика. — М.: Наука, 1984, с. 94–99.

[7] (с. 426). Определение функции $\varphi(a)$ может служить примером определения, неприемлемого для Брауэра.

[8] (с. 427). См. с. 491.

[9] (с. 429). $\nu(f)$ — это характеристическая функция множества.

З. А. Кузичева

О БЕСКОНЕЧНОМ

[1] (с. 431). Публикуемый текст является сокращенным (самим Гильбертом) вариантом работы «Über das Unendliche» — Math. Ann., 1926, Bd. 95, S. 161–190.

[2] (с. 441). В настоящее время известно, что числа вида 2^n-1 с $n=132049$ и $n=216091$ являются простыми.

ПРОБЛЕМЫ ОБОСНОВАНИЯ МАТЕМАТИКИ

[1] (с. 449). Данная статья была также опубликована в книге: *Гильберт Д.* Основания геометрии. Перевод И. С. Градштейна. — М.: ГИТТЛ, 1948, добавление X. Этот перевод был учтен при подготовке настоящего издания.

[2] (с. 450). См.: *Zermelo E.* — Math. Ann., 1908, Bd. 65, S. 261–281.

[3] (с. 450). Речь, по-видимому, идет о непредикативных определениях. Определение называется непредикативным, если определяемый объект входит в ту совокупность, через которую он определяется. О способах устранения непредикативных

определений см., например: *Френкель А., Бар-Хиллел И.* Основания теории множеств. — М.: Мир, 1966, гл. III.

[4] (с. 450). А. Френкель, начиная с 1921 г., публиковал работы, посвященные основаниям теории множеств (*Fraenkel A.* — Math. Ann., 1921, Bd. 86, S. 230–231; *Jahresb D. M. V.* — 1924, Bd. 33, S. 97–103; Math. Zeitschr., 1925, Bd. 22, S. 250–273). Первая из них содержала уточнение аксиоматики Цермело. Теперь такого рода системы аксиом теории множеств называют системами типа Цермело — Френкеля и обозначают ZF.

[5] (с. 452). Для устранения известных в то время (но не *всех вообще*) теоретико-множественных парадоксов Б. Рассел (1872–1970) и А. Уайтхед (1861–1947) построили так называемую разветвленную теорию типов. См.: *Russell B, Whitehead A.* Principia Mathematica. — London, 1910–1913, vol. 1–3.

[6] (с. 452). См. примечание [8] к статье «Логические основания математики».

[7] (с. 453). См. примечание [4] к работе «Об основаниях логики и арифметики».

[8] (с. 455). См. *Schröder E.* Vorlesungen über die Algebra der Logik (exakte Logik). Bd. 3: Algebra und Logik der Relative, Part 1. — Leipzig, 1895; *Löwenheim L.* — Math. Ann., 1915, Bd. 76, S. 447–470; *Behmann H.* — Math. Ann., 1922, Bd. 86, S. 163–229.

З. А. Кузичева

ПОЗНАНИЕ ПРИРОДЫ И ЛОГИКА

[1] (с. 457). Торжественная речь на съезде Общества германских естествоиспытателей и врачей (Кёнигсберг, 8 сентября 1930 г.), произнесенная по случаю присвоения Гильберту городским советом Кёнигсберга почетного гражданства.

[2] (с. 464). В греческой мифологии (Гомер, «Одиссея», IX, 83–104) лотофаги (поедатели лотоса) — это мирное племя, питавшееся плодами лотоса. Спутники Одиссея, отведав у лотофагов сладко-медвяный лотос, позабыли обо всем и, утратив желание вернуться на родину, захотели навсегда остаться в стране лотофагов. Одиссею пришлось силой вернуть их на корабли и привязать к корабельным скамьям (см., например: Мифы народов мира. Т. 2. — М.: СЭ, 1988, с. 72.)

[3] (с. 464). Близкие высказывания Л. Н. Толстого см., например, в его произведении «Так что же нам делать?» — М.: Худож. лит., собр. соч. в 22 т., 1983, т. 16, с. 341.

[4] (с. 465). Карл Густав Якоб Якоби (1804–1851). Имеется в виду речь, произнесенная им в 1834 г., в которой он сказал: «Господин Фурье придерживается, правда, мнения, что главной целью математики является общественная польза и объяснение законов природы; но как философ он должен был бы знать, что единственная цель науки заключается в том, чтобы возвысить честь человеческого разума, и что, таким образом, какой-нибудь вопрос о числах ничуть не менее важен, чем любой вопрос о системе мира» (см.: *Клейн Ф.* Лекции о развитии математики в XIX в. — М.: Наука, 1989, с. 131).

[5] (с. 465). Огюст Конт (1798–1857). Французский философ, один из основоположников позитивизма.

Н. М. Нагорный

ДАВИД ГИЛЬБЕРТ

ИЗБРАННЫЕ ТРУДЫ.
ТОМ I
ТЕОРИЯ ИНВАРИАНТОВ. ТЕОРИЯ ЧИСЕЛ. АЛГЕБРА. ГЕОМЕТРИЯ. ОСНОВАНИЯ МАТЕМАТИКИ

Научное издание

Редакторы *В. И. Авербух, Ю. Н. Торхов, Г. М. Цукерман*
Корректоры *О. А. Васильева, Е. А. Коноваленко, И. Н. Мельникова*
Оригинал-макет *К. Е. Панкратьев, Ю. Н. Торхов*

Формат 70 × 100/16. Гарнитура литературная.
Усл. печ. л. 47,5. Бумага офсетная № 1. Подписано к печати 16.2.1998.
Тираж 1000 экз. Заказ 3343

Издательство «Факториал», 117449, Москва, а/я 331; ЛР № 063537 от 22.07.19[illegible]

Оригинал-макет подготовлен с использованием макропакета AMS-TEX
Отпечатано во 2-й типографии издательства «Наука».
121099, Москва Г-99, Шубинский пер., 6