Н.Г.ЧЕБОТАРЕВ

СОБРАНИЕ СОЧИНЕНИЙ

АКАДЕМИЯ НАУК СССР

Н. Г. ЧЕБОТАРЕВ

СОБРАНИЕ СОЧИНЕНИЙ

ТОМ ПЕРВЫЙ

ИЗДАТЕЛЬСТВО АКАДЕМИИ НАУК СССР
МОСКВА - ЛЕНИНГРАД
1949

Ответственный редактор
н-корреспондент АН С
Б. Н. ДЕЛОНЕ

ПРЕДИСЛОВИЕ

Николай Григорьевич Чеботарев был одним из крупнейших современных алгебраистов. Работы его о плотностях простых идеалов и о резольвентах принадлежат к числу наиболее выдающихся алгебраических работ последних десятилетий.

Николай Григорьевич родился 15 июня 1894 г. Еще в младших классах гимназии начали обнаруживаться его исключительные математические способности. В 1912 г. Н. Г. поступает в Киевский университет. Эти годы были годами расцвета алгебраической школы Д. А. Граве. Н. Г. посещает семинары Граве, изучает теорию алгебраических чисел, теорию алгебраических функций и многое другое; в эти же годы он делает первую работу — доказывает свою „арифметическую теорему монодромии" о том, что композицией группы инерции образуют всю группу Галуа. На 1915 и 1916 годы Киевский университет в связи с войной эвакуируется в Саратов; туда переезжает и Чеботарев. В Саратове Н. Г. начинает работать над известной задачей Фробениуса о плотностях простых чисел, принадлежащих к данному классу подстановок группы Галуа алгебраического поля, решение которой позже прославило его имя.

В 1916 г. Н. Г. был оставлен при университете для подготовки к профессорскому званию. Вернувшись в Киев, Н. Г. занимается математикой с неослабевающей энергией. Он пишет ряд работ: о поверхностях переноса, о критерии вещественности корней трансцендентных уравнений, о линиях и телах постоянной ширины, об обратной задаче Чирнгаузена и т. д. Одновременно Н. Г. сдает магистерские экзамены и по прочтении двух пробных лекций избирается приват-доцентом Киевского университета.

В 1921 г. Н. Г. переезжает в Одессу. Научная работа Чеботарева, несмотря на большие материальные трудности, становится в Одессе еще более интенсивной, чем в Киеве. Летом 1922 г. он доказывает, наконец, предположение Фробениуса о плотностях.

Эта работа поставила Чеботарева в ряд небольшого числа классиков теории алгебраических чисел. Она стояла в самом центре тогдашних интересов и стала поэтому сразу очень широко известной, тем более что, опираясь на примененный в ней Чеботаревым метод присоединения полей деления круга, немецкому математику Артину удалось доказать одну из основных теорем теории поля классов.

В 1927 г. Н. Г. переходит в Казанский университет. Научное творчество Чеботарева не ослабевает, и уже в 1931 г. появляется вторая его первоклассная работа. Она посвящена теории резольвент, т. е. вопросу о том, на цепь каких простейших вспомогательных уравнений может быть сведено решение данного алгебраического уравнения n-ой степени, каковы числа параметров, от которых зависят коэффициенты этих вспомогательных уравнений. Этой важной задачей занимались крупнейшие математики — Клейн, Гильберт и другие, но получили в ней только частные результаты. Лишь Чеботареву удалось получить в этой области общую теорему.

В 1932 г. состоялся очередной международный конгресс математиков в Цюрихе, который совпал со 100-летием со дня смерти гениального французского алгебраиста Эвариста Галуа. Признание важности алгебраических работ Чеботарева было в то время так велико, что президиум конгресса предложил прочесть обзорный доклад памяти гениального алгебраиста не кому-либо другому, а именно Чеботареву.

В сравнительно недавние годы, во время Отечественной войны, Н. Г. сделал вторую важную работу по теории резольвент, в которой он дал для общего случая границу, больше которой должно быть число параметров хотя бы в одном вспомогательном уравнении цепи.

Чеботарев работал в самых различных областях математики до последних дней жизни. Приехав в Москву на операцию, оказавшуюся для него роковой, Н. Г. за несколько дней до того, как лечь в больницу, выступил с докладом в Московском математическом обществе о своей последней работе. На 11-й день после операции, 2 июля 1947 г., Н. Г. скончался.

Одновременно с Н. Г. в Казани работал крупный геометр П. А. Широков, с которым Н. Г. был тесно связан. Их совместная деятельность подняла значение Казанского университета как математического центра до высоты, которой он не достигал со времен Лобачевского.

В 1929 г. Академия Наук СССР избрала Н. Г. своим членом-корреспондентом, а за работы по теории резольвент Чеботареву была посмертно присуждена Сталинская премия первой степени.

Николай Григорьевич Чеботарев был человеком высоких нравственных качеств, простым в обращении со всеми, без различия их положения, отзывчивым и прямым. Сердечность и обаяние его личности чувствовали все с ним соприкасавшиеся.

В томах I и II помещены все 62 печатные математические работы Н. Г. Чеботарева. Многие из этих работ были опубликованы Н. Г. на немецком языке. Все они были переведены на русский язык учеником Н. Г. Чеботарева, соредактором этого собрания сочинений, профессором Казанского университета В. В. Морозовым.

Б. Делоне

ЗАДАЧА, ОБРАТНАЯ ЗАДАЧЕ ЧИРНГАУЗЕНА

(Вестник чист. и прикл. знания, I, в. 2 (1922), стр. 1—8)

Даны два уравнения одной и той же степени

$$x^n + p_1 x^{n-1} + \cdots + p_{n-1} x + p_n = 0, \tag{1}$$

$$\bar{x}^n + \bar{p}_1 \bar{x}^{n-1} + \cdots + \bar{p}_{n-1} \bar{x} + \bar{p}_n = 0. \tag{2}$$

Требуется узнать, выражается ли рационально корень одного уравнения через корень другого, и если выражается, то найти это выражение. Известно, что в общем эта задача зависит от корня уравнения $n!$-ой степени, который должен быть рационален для того, чтобы задача допускала решение. Таким образом, для кубического уравнения нужно составить и отыскать рациональный корень в уравнении 6-ой степени, для уравнения 4-ой степени — корень уравнения 24-ой степени. Возникает вопрос, нельзя ли упростить эту громоздкую задачу или по крайней мере расчленить ее на несколько более простых приемов.

История вопроса такова. Б. Н. Делоне, занимаясь этой задачей в применении к кубическим уравнениям, подметил, что построенное им уравнение 6-ой степени распадается на два кубических уравнения в том случае, если дискриминанты этих уравнений отличаются лишь квадратным множителем. Вывод свой Б. Н. основывает на существовании особых соотношений (сизигий) между инвариантами бинарных кубических форм. Этот результат не допускает обобщения на уравнения более высоких степеней, так как теория Эрмита о связи преобразования Чирнгаузена с инвариантами бинарных форм переходит для высших степеней в связь с совокупными инвариантами.[1] Между тем задача может быть решена, если применить к ней анализ, основанный на общей теории Галуа. В настоящей статье я и займусь этим анализом, а затем приложу его к общим уравнениям 3-й 4-й степени.

§ 1

Будем предполагать уравнения (1) и (2) неприводимыми. Тогда, если существует рациональное выражение одного корня уравнения (2) через какой-нибудь из корней уравнения (1), например

$$\bar{x}_1 = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_1^2 + \cdots + \alpha_{n-1} x_1^{n-1}, \tag{3}$$

[1] См. Weber. Lhrb. d. Alg., Bd. II, стр. 240.

то, подставляя в это выражение вместо x_1 остальные корни уравнения (1), мы получим все корни уравнения (2)

$$\begin{aligned} \bar{x}_2 &= \alpha_0 + \alpha_1 x_2 + \alpha_2 x^2{}_2 + \cdots + \alpha_{n-1} x_2{}^{n-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \bar{x}_n &= \alpha_0 + \alpha_1 x_n + \alpha_2 x_n{}^2 + \cdots + \alpha_{n-1} x_n{}^{n-1}. \end{aligned} \tag{4}$$

Для определения n коэффициентов $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ мы получили n линейных уравнений с определителем, не равным нулю. Такая формулировка задачи допускает ее решение и в том случае, когда $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ не рациональны, и притом не одно, а $n!$, которые получатся, если мы будем в равенствах (3) и (4) производить над $\bar{x}$ (или над x) всевозможные подстановки. Но коэффициенты $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ можно найти и не умея решать уравнений (1) и (2). Чтобы притти к удобным для этого формулам, будем умножать уравнения (3) и (4) соответственно на $x_1{}^i, x_2{}^i, \ldots, x_n{}^i$ $(i = 0, 1, 2, \ldots, n-1)$ и складывать. Тогда, обозначая через s_k сумму k-тых степеней корней уравнения (1), мы придем к уравнениям

$$\begin{aligned} \bar{s}_1 &= n\alpha_0 + s_1 \alpha_1 + \cdots + s_{n-1} \alpha_{n-1}, \\ \Sigma x \bar{x} &= s_1 \alpha_0 + s_2 \alpha_1 + \cdots + s_n \alpha_{n-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \Sigma x^{n-1} \bar{x} &= s_{n-1} \alpha_0 + s_n \alpha_1 + \cdots + s_{2n-2} \alpha_{n-1}. \end{aligned} \tag{5}$$

Получилась опять система уравнений с не равным нулю определителем. Трудность для вычисления представляют только коэффициенты в левых частях. Чтобы вычислить их, исследуем, к какой группе они принадлежат в области,[1] полученной от соединения областей, образованных корнями уравнений (1) и (2). Группа Галуа этой области должна быть делителем группы, образованной подстановками над корнями

$$x_1, x_2, \ldots, x_n; \bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n. \tag{6}$$

Эти подстановки мы получим, если над $\bar{x}$ станем производить подстановки уравнения (2), а над x совершенно независимо подстановки уравнения (1). Но чтобы найти коэффициенты α, нет надобности находить величины (6): все коэффициенты в левых частях (5) принадлежат к одной и той же группе довольно высокого порядка. Действительно, если станем одновременно производить над x и $\bar{x}$ одну и ту же подстановку, то наши величины не претерпят никаких изменений. В общем случае, когда оба уравнения (1) и (2) без аффекта (или когда мы не знаем их групп), наша группа будет порядка $n!$ и притом изоморфна с группой уравнений (1) и (2). Величины $\Sigma x\bar{x}$, $\Sigma x^2\bar{x}, \ldots,$ $\Sigma x^{n-1}\bar{x}$, как принадлежащие к одной и той же группе (буквенно),

[1] Под словом область мы будем здесь разуметь понятие, соответствующее термину Körper — корпус-поле.

должны рационально выражаться через какую-нибудь одну, например через $\Sigma x\bar{x} = z$. Находить эти выражения придется обычным способом Лагранжа. Величина же z может быть найдена как корень некоторого уравнения $n!$-ой степени, которое мы получим, если составим симметрические функции от величин, сопряженных с z. Для этого нужно производить подстановки только над одной половиной величин (6), например над x. Получатся функции, симметрические относительно x, с коэффициентами, которые будут симметрическими функциями от $\bar{x}$. Чтобы существовало рациональное преобразование (3) — (4), необходимо и достаточно, чтобы функция z была рациональным числом, т. е. чтобы построенное нами уравнение имело рациональный корень. Итак, вся задача сводится в существенных чертах к нахождению рационального корня в численном уравнении.

§ 2

Эта последняя задача представляет большие трудности, так как степень полученного уравнения ($n!$-ая) очень высока. Чтобы облегчить задачу, можно вместо z строить уравнения для функций, принадлежащих к группам более высоких порядков. Тогда степень построенного уравнения будет равна индексу взятой группы относительно симметрической. Дальнейшим шагом в решении задачи будет построение уравнения, корень которого принадлежит к вновь выбранному нами делителю первой группы. Его степень будет равна индексу этого делителя относительно первой группы, так как после нахождения рационального корня в первом уравнении мы имеем право считать функции, принадлежащие к первой группе, известными. Таким путем мы сведем задачу к последовательному решению уравнений более низких степеней. Неудобство этого метода заключается в том, что коэффициенты уравнения, корни которого принадлежат к группам высокого порядка, должны иметь сложное выражение и в общем случае имеют большие численные значения, что затрудняет нахождение рациональных корней.

Задача допускает несравненно более удобный метод решения в том случае, если группа G уравнения (1) (а также группа $\bar{G}$ уравнения (2)) имеет нормальный делитель H (или, соответственно $\bar{H}$). Построим уравнение, корни которого суть функции от x, принадлежащие H (и, соответственно, уравнение с корнями, принадлежащими $\bar{H}$). Группой уравнения будет $\frac{G}{H}$ $\left(\text{соответственно } \frac{\bar{G}}{\bar{H}}\right)$. Отсюда следует, что степень уравнения композиции от них равна индексу (H, G). Пусть далее, следующая группа жорданова ряда будет H_1 (соответственно $\bar{H}_1$). Построим уравнения, корни которых принадлежат H_1, $\bar{H}_1$. Обозначим эти корни через $z, \bar{z}$. Составим функцию $\zeta = \Sigma z\bar{z}$ и затем все функции,

полученные от производства над z подстановок группы $\frac{H}{H_1}$. Основные симметрические функции от этих ζ не должны изменяться от подстановок групп $\frac{H}{H_1}$ и $\frac{\bar{H}}{\bar{H}_1}$ и потому рационально выразятся через найденный нами (рациональный) корень предыдущего уравнения. Для ζ получится уравнение степени (H_1, H). Продолжая в том же роде дальше, мы приведем задачу к последовательному нахождению рациональных корней в уравнениях, степени которых составляют ряд индексов нашей группы G. Получаемые здесь выражения не будут особенно громоздкими; во всяком случае их легче вычислить, чем в предыдущем методе. Впрочем иногда представляется целесообразным комбинировать оба эти метода, в чем мы убедимся на приведенных ниже примерах.

§ 3

Возьмем два кубических уравнения в приведенной форме

$$x^3 + px + q = 0, \tag{7}$$

$$\bar{x}^3 + \bar{p}\bar{x} + \bar{q} = 0. \tag{8}$$

Симметрическая группа 3-ей степени имеет в качестве нормального делителя знакопеременную группу. Корнем z, принадлежащим к знакопеременной группе, будет квадратный корень из дискриминанта

$$\sqrt{D} = \sqrt{-4p^3 - 27q^2}. \tag{9}$$

Поэтому необходимым условием того, чтобы корни уравнений (7) и (8) составляли одну и ту же область, является образование корнями $\sqrt{D}$ и $\sqrt{\bar{D}}$ одной и той же иррациональности, или, что то же, рациональности $\sqrt{D\bar{D}}$. Если это условие соблюдается, составим уравнение, которому удовлетворяют функции

$$\begin{aligned} z_1 &= x_1\bar{x}_1 + x_2\bar{x}_2 + x_3\bar{x}_3, \\ z_2 &= x_1\bar{x}_2 + x_2\bar{x}_3 + x_3\bar{x}_1, \\ z_3 &= x_1\bar{x}_3 + x_2\bar{x}_1 + x_3\bar{x}_2, \end{aligned} \tag{10}$$

получающиеся одна из другой при помощи подстановок знакопеременной группы, производимых над $\bar{x}$ (или x). Пусть это будет

$$z^3 + P_1z^2 + P_2z + P_3 = 0. \tag{11}$$

Станем вычислять P_1, P_2, P_3

$$P_1 = -x_1(\bar{x}_1 + \bar{x}_2 + \bar{x}_3) - x_2(\bar{x}_1 + \bar{x}_2 + \bar{x}_3) - x_3(\bar{x}_1 + \bar{x}_2 + \bar{x}_3) = 0, \tag{12}$$

$$S_2 = \Sigma x_1^2\bar{x}_1^2 + 2\Sigma x_1x_2\bar{x}_1\bar{x}_2 = s_2\bar{s}_2 + 2p\bar{p} = 4p\bar{p} + 2p\bar{p} = 6p\bar{p}, \tag{13}$$

$$P_2 = -\frac{1}{2}S_2 = -3p\bar{p}, \tag{14}$$

$$S_3 = \Sigma x_1^3 \bar{x}_1^3 + 3\,\Sigma (x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1)(\bar{x}_1^2 \bar{x}_2 + \bar{x}_2^2 \bar{x}_3 + \bar{x}_3^2 \bar{x}_1) + \\ + 18\, x_1 x_2 x_3 \bar{x}_1 \bar{x}_2 \bar{x}_3. \qquad (15)$$

Выражения в скобках во втором члене правой части удовлетворяют квадратному уравнению:

$$\zeta_1 = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1, \qquad \zeta_2 = x_1^2 x_3 + x_2^2 x_1 + x_3^2 x_2, \qquad (16)$$

$$\zeta_1 + \zeta_2 = \Sigma x_1^2 x_2 = s_1 s_2 - s_3 = +3q, \qquad (17)$$

$$\zeta_1 \zeta_2 = \Sigma x_1^4 x_2 x_3 + 3 x_1^2 x_2^2 x_3^2 + \Sigma x_1^3 x_2^3 = \\ = -q s_3 + \frac{1}{2} s_3^2 - \frac{1}{2} s_6 + 3q^2 = 6q^2 + \frac{9}{2} q^2 + \frac{1}{2} p s_4 - \frac{3}{2} q^2 = \\ = 9q^2 - \frac{1}{2} p^2 s_2 - \frac{1}{2} pq s_1 = 9q^2 + p^3, \qquad (18)$$

$$\zeta^2 - 3q\zeta + (9q^2 + p^3) = 0, \qquad (19)$$

$$\zeta = \frac{3q \pm \sqrt{9q^2 - 36q^2 - 4p^3}}{2} = \frac{3q \pm \sqrt{D}}{2}, \qquad (20)$$

$$S_3 = s_3 \bar{s}_3 + 18\, q\bar{q} + \frac{3}{4}\,(3q + \sqrt{D})(3\bar{q} \pm \sqrt{\bar{D}}) + \\ + \frac{3}{4}\,(3q - \sqrt{D})(3\bar{q} \mp \sqrt{\bar{D}}) = 9\, q\bar{q} + 18 q\bar{q} + \frac{27}{2} q\bar{q} \pm \\ \pm \frac{3}{2} \sqrt{D\bar{D}} = \frac{81}{2} q\bar{q} \pm \frac{3}{2} \sqrt{D\bar{D}}, \qquad (15a)$$

$$P_3 = -\frac{1}{3} S_3 = \frac{-27 q\bar{q} \mp \sqrt{D\bar{D}}}{2}. \qquad (21)$$

Итак, основное уравнение, в котором мы должны искать рациональный корень, имеет следующий вид:

$$z^3 - 3p\bar{p}z - \frac{27}{2} q\bar{q} \pm \frac{1}{2} \sqrt{D\bar{D}} = 0. \qquad (11a)$$

Какой из двух знаков в последнем члене нужно выбрать, чтобы получить решение? Заранее на этот вопрос ответить трудно, так как, как мы сейчас увидим, он аналогичен вопросу, будут ли две заданные формы proprie или improprie эквивалентны. Ясно только, что если оба уравнения (11a) допускают по решению, то существует нетождественный переход одного корня в другой корень того же уравнения, другими словами, каждое из уравнений (1) и (2) нормально.

Чтобы исследовать общий случай, обратим внимание на то, что верхний знак в уравнении (11a) нужно брать в том случае, если знакопеременная функция $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ имеет тот же знак, что и аналогичная функция для другого уравнения:

$(\bar{x}_1 - \bar{x}_2)(\bar{x}_2 - \bar{x}_3)(\bar{x}_3 - \bar{x}_1)$. Выразим эту последнюю функцию через первую. Вычтем одно из другого равенства

$$\bar{x}_1 = \alpha_0 + \alpha_1 x_1 + \alpha_2 x_1^2, \tag{22}$$

$$\bar{x}_2 = \alpha_0 + \alpha_1 x_2 + \alpha_2 x_2^2. \tag{23}$$

Получим

$$(\bar{x}_1 - \bar{x}_2) = (x_1 - x_2)[\alpha_1 + \alpha_2 (x_1 + x_2)] = (x_1 - x_2)(\alpha_1 - \alpha_2 x_3). \tag{24}$$

Отсюда

$$(\bar{x}_1 - \bar{x}_2)(\bar{x}_2 - \bar{x}_3)(\bar{x}_3 - \bar{x}_1) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) N(\alpha_1 - \alpha_2 x_i). \tag{25}$$

Значит, все зависит от знака $N(\alpha_1 - \alpha_2 x_i)$. Но

$$N(\alpha_1 - \alpha_2 x_i) = \alpha_1^3 + p\alpha_1 \alpha_2^2 + q\alpha_2^3. \tag{26}$$

Знак этого выражения мы, конечно, сможем определить уже после того, как будут вычислены искомые величины α_1 и α_2.

Исследуем еще этот вопрос, рассматривая переход между корнями в форме дробной линейной подстановки, т. е.

$$\bar{x}_1 = \frac{\alpha x_1 + \beta}{\gamma x_1 + \delta}. \tag{27}$$

Тогда

$$\bar{x}_1 - \bar{x}_2 = \frac{\alpha x_1 + \beta}{\gamma x_1 + \delta} - \frac{\alpha x_2 + \beta}{\gamma x_2 + \delta} = \frac{(x_1 - x_2)(\alpha\delta - \beta\gamma)}{(\gamma x_1 + \delta)(\gamma x_2 + \delta)}. \tag{28}$$

Отсюда

$$(\bar{x}_1 - \bar{x}_2)(\bar{x}_2 - \bar{x}_3)(\bar{x}_3 - \bar{x}_1) = \\ = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \frac{(\alpha\delta - \beta\gamma)^3}{[N(\gamma x_i + \delta)]^2}. \tag{29}$$

Итак, верхний знак будет давать решение тогда и только тогда, если для формулы (27) будет иметь место $\alpha\delta - \beta\gamma > 0$. Отсюда вытекает следующая теорема о групповом характере чередования верхнего и нижнего знаков.

Если три кубических уравнения (I), (II) и (III) допускают рациональный переход друг в друга, то при переходе от (I) к (III) нужно взять в уравнении (11а) верхний или нижний знак, судя по тому, будут ли аналогичные знаки при переходе от (I) к (II) и от (II) к (III) одноименны (оба верхние или оба нижние) или разноименны.

Последнее исследование показывает также, что в случае верхнего знака бинарные кубические формы, соответствующие уравнениям (1) и (2), будут proprie эквивалентны, в случае нижнего — improprie эквивалентны.

Для нахождения коэффициентов α_0, α_1, α_2 преобразования необходимо еще знать величину $u = x_1^2 \bar{x}_1 + x_2^2 \bar{x}_2 + x_3^2 \bar{x}_3$. Чтобы выразить

ее через z, воспользуемся способом Лагранжа. Обозначая левую часть уравнения (11а) через

$$f(z) = (z - z_1)(z - z_2)(z - z_3), \tag{30}$$

применим для вычисления u известную формулу Лагранжа

$$u = \frac{\Sigma u_1 (z - z_2)(z - z_3)}{f'(z)} = \frac{Az^2 + Bz + C}{3z^2 - 3p\bar{p}}. \tag{31}$$

Коэффициенты A, B, C имеют значения: $A = 0$, $B = 6q\bar{p} + 3q\bar{p} = 9q\bar{p}$, $C = -6p^2\bar{q} - 3p^2\bar{q} = -9p^2\bar{q}$ и потому u выразится через z следующим образом:

$$u = \frac{9q\bar{p}z - 9p^2\bar{q}}{3z^2 - 3p\bar{p}} = \frac{3(q\bar{p}z - p^2\bar{q})}{z^2 - p\bar{p}}. \tag{31а}$$

Коэффициенты преобразования α_0, α_1, α_2 можно получить из таких формул:

$$\begin{aligned} 0 &= 3\alpha_0 - 2p\alpha_2, \\ z &= -2p\alpha_1 - 3q\alpha_2, \\ u &= -2p\alpha_0 - 3q\alpha_1 + 2p^2\alpha_2. \end{aligned}$$

§ 4

Рассмотрим два уравнения 4-ой степени

$$x^4 + p_2 x^2 + p_3 x + p_4 = 0, \tag{32}$$

$$\bar{x}^4 + \bar{p}_2 \bar{x}^2 + \bar{p}_3 \bar{x} + \bar{p}_4 = 0. \tag{33}$$

Построим уравнение, которому удовлетворяет функция

$$z = x_1 x_2 + x_3 x_4. \tag{34}$$

Эта функция принадлежит к группе 8-го порядка, а потому уравнение будет кубическим. Вместе с тем вся совокупность z_1, z_2, z_3 принадлежит к Vierergruppe, которая является нормальным делителем симметрической. Нужное нам уравнение выписано, например, в „Основах высшей алгебры“ Д. А. Граве. Полагая в нем $p_1 = 0$, получим

$$z^3 - p_2 z^2 - 4p_4 z - p_3^2 + 4p_2 p_4 = 0. \tag{35}$$

Точно так же для уравнения (33)

$$\bar{z}^3 - \bar{p}_2 \bar{z}^2 - 4\bar{p}_4 \bar{z} - \bar{p}_3^2 - 4\bar{p}_2 \bar{p}_3 = 0. \tag{36}$$

Для того чтобы наша задача была возможна, необходимо, чтобы существовал рациональный переход между корнями уравнений (35) и (36). Отыскав его, введем обозначения для следующих величин:

$$\zeta = z_1 \bar{z}_1 + z_2 \bar{z}_2 + z_3 \bar{z}_3, \tag{37}$$

$$u = z_1^2 \bar{z}_1 + z_2^2 \bar{z}_2 + z_3^2 \bar{z}_3, \tag{38}$$

$$\bar{u} = z_1 \bar{z}_1^2 + z_2 \bar{z}_2^2 + z_3 \bar{z}_3^2. \tag{39}$$

Обратимся теперь к уравнениям (32) и (33). Составим уравнение, которому удовлетворяет функция

$$T_1 = x_1\bar{x}_1 + x_2\bar{x}_2 + x_3\bar{x}_3 + x_4\bar{x}_4. \tag{40}$$

Произведем над $\bar{x}$ последовательно подстановки Vierergruppe. Получим величины T_1, T_2, T_3, T_4. Симметрические функции от этих величин не изменяются от подстановок Vierergruppe и потому могут быть выражены через ζ. Значит, через ζ можно выразить коэффициенты уравнения

$$F(T) = (T-T_1)(T-T_2)(T-T_3)(T-T_4) = T^4 + \Pi_1 T^3 + \Pi_2 T^2 + \\ + \Pi_3 T + \Pi_4 = 0. \tag{41}$$

При этом

$$\Pi_1 = 0, \qquad \Pi_2 = -2p_2\bar{p}_2 - 2\zeta,$$

$$\Pi_3 = -8p_3\bar{p}_3, \qquad \Pi_4 = -\frac{1}{3}\zeta^2 - \frac{8}{3}p_2 u - \frac{8}{3}\bar{p}_2 u + \frac{14}{3}p_2\bar{p}_2\zeta +$$

$$+ p_2^2\bar{p}_2^2 + 16p_2^2\bar{p}_4 + 16\bar{p}_2^2 p_4 + \frac{64}{3}p_4\bar{p}_4.$$

Поэтому уравнение (41) будет иметь следующий вид:

$$T^4 - (2p_2\bar{p}_2 + 2\zeta)T^2 - 8p_3\bar{p}_3 T - \frac{1}{3}\zeta^2 - \frac{8}{3}p_2\bar{u} - \frac{8}{3}\bar{p}_2 u +$$

$$+ \frac{14}{3}p_2\bar{p}_2\zeta + p_2^2\bar{p}_2^2 + 16p_2^2\bar{p}_4 + 16\bar{p}_2^2 p_4 + \frac{64}{3}p_4\bar{p}_4 = 0. \tag{41a}$$

Для окончательного решения задачи требуется еще выразить через T величины $\theta = \Sigma x_1^2\bar{x}_1$ и $Z = \Sigma x_1^3\bar{x}_1$. Опять пользуемся формулой Лагранжа

$$\theta = \frac{\Sigma\theta_1(T-T_2)(T-T_3)(T-T_4)}{F'(T)} = \frac{AT^3 + BT^2 + CT + D}{F'(T)}, \tag{42}$$

где $A = 0$, $B = 8p_3\bar{p}_2$, $C = -8p_2^2\bar{p}_3 + 32p_4\bar{p}_3$, $D = 8p_3\bar{u} - 8p_3\bar{p}_2\zeta - \\ - 64p_2p_3\bar{p}_1$.

Итак, θ выражается через T следующим образом:

$$\theta = \frac{8p_3\bar{p}_2T^2 + (-8p_2^2\bar{p}_3 + 32p_4\bar{p}_3)T + (8p_3\bar{u} - 8p_3\bar{p}_2\zeta - 64p_2p_3\bar{p}_4)}{4T^3 - 4(p_2\bar{p}_2 + \zeta)T - 8p_3\bar{p}_3} \tag{42a}$$

Подобным же образом находим выражение для $Z = \Sigma x_1^3\bar{x}_1$

$$Z = \frac{\Sigma Z_1(T-T_2)(T-T_3)(T-T_4)}{F'(T)} = \frac{A_1T^3 + B_1T^2 + C_1T + D_1}{F'(T)}, \tag{43}$$

$$A = 0, \qquad B_1 = -2u - 2p_2\zeta - 4p_2^2\bar{p}_2 + 16p_4\bar{p}_2, \qquad C_1 = -28p_2p_3\bar{p}_3,$$

$$D_1 = -2p_2\zeta^2 - 8p_2\bar{p}_2 u - 10p_2^2\bar{u} + 8p_4\bar{u} + 16p_2^2\bar{p}_2\zeta - 16p_4\bar{p}_2\zeta + \\ + 4p_2^3\bar{p}_2^2 + 6p_3^2\bar{p}_2^2 + 40p_2p_4\bar{p}_2^2 + 64p_2^3\bar{p}_4 + 8p_3^2\bar{p}_4.$$

Итак, выражение для Z таково:

$$Z = \frac{(-2u - 2p_2\zeta - 4p_2^2\bar{p}_2 + 16p_4\bar{p}_2)T^2 - 28p_2p_3\bar{p}_3T + (-2p_2\zeta^2 - \rightarrow}{4T^3 - 4(p_2\bar{p}_2 + \zeta)T - 8p_3\bar{p}_3}$$

$$\frac{-8p_2\bar{p}_2u - 10p_2^2\bar{u} + 8p_4\bar{u} + 16p_2^2\bar{p}_2\zeta - 16p_4\bar{p}_2\zeta + 4p_2^3\bar{p}_2^2 + \rightarrow}{4T^3 - 4(p_2\bar{p}_2 + \zeta)T - 8p_3\bar{p}_3}$$

$$\frac{+6p_3^2\bar{p}_2^2 + 40p_2p_4\bar{p}_2^2 + 64p_2^3\bar{p}_4 + 8p_3^2\bar{p}_4}{4T^3 - 4(p_2\bar{p}_2 + \zeta)T - 8p_3\bar{p}_3}. \qquad (43a)$$

Чтобы получить коэффициенты формул перехода

$$\bar{x} = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3, \qquad (44)$$

необходимо решить следующую систему линейных уравнений:

$$\begin{aligned}
0 &= 4\alpha_0 - 2p_2\alpha_2 - 3p_3\alpha_3,\\
T &= -2p_2\alpha_1 - 3p_3\alpha_2 + (2p_2^2 - 4p_4)\alpha_3,\\
\theta &= -2p_2\alpha_0 - 3p_3\alpha_1 + (2p_2^2 - 4p_4)\alpha_2 + 5p_2p_3\alpha_3,\\
Z &= -3p_3\alpha_0 + (2p_2^2 - 4p_4)\alpha_1 + 5p_2p_3\alpha_2 + (-2p_2^3 + 3p_3^2 + \\
&\qquad + 6p_2p_4)\alpha_3.
\end{aligned} \qquad (45)$$

ОБ ОДНОЙ ТЕОРЕМЕ ГИЛЬБЕРТА

UEBER EIN SATZ VON HILBERT

(Вісті. ВУАН, 1923, стр. 3—7)

В этой работе я доказываю следующую теорему, которую в менее строгой формулировке доказал Гильберт. [1]

Пусть дано нормальное поле Ω, содержащее l — е корни из единицы. Выберем в Ω t целых чисел

$$\alpha_1, \alpha_2, \ldots, \alpha_t$$

так, чтобы произведение

$$\alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdots \alpha_t^{m_t} \quad . \tag{1}$$

представляло l-ю степень некоторого числа из Ω только тогда, когда каждое из чисел $m_1, m_2, \ldots, m_t$ делится на l. Тогда в Ω найдется бесконечное множество таких простых идеалов ρ, что

$$\left\{\frac{\alpha_1}{\rho}\right\} = \zeta^{c_1}, \quad \left\{\frac{\alpha_2}{\rho}\right\} = \zeta^{c_2}, \ldots, \left\{\frac{\alpha_t}{\rho}\right\} = \zeta^{c_t}, \tag{2}$$

где $\zeta = e^{\frac{2\pi i}{l}}$; $c_1, c_2, \ldots, c_t$ — произвольно заданная система чисел из ряда $0, 1, 2, \ldots, l-1$ и $\left\{\frac{\alpha}{\rho}\right\}$ — обобщенный символ вычета, т. е.

$$\left\{\frac{\alpha}{\rho}\right\} = \zeta^c, \quad \text{если} \quad \alpha^{\frac{p^f - 1}{f}} \equiv \zeta^c \pmod{\rho},$$

где f — порядок идеала ρ.

(Нужно заметить, что $p^f - 1$ должно делиться на l, так как поле Ω содержит поле l-х корней из единицы $\omega(\zeta)$ и потому порядок каждого простого идеала из $\omega(\zeta)$, являющегося делителем p, будет делителем f).

Доказательство основывается на выводах моей работы „Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок“, где показано, что всегда существует бесконечное множество таких простых чисел, которые принадлежат к заданному классу подстановок группы данного уравнения. [2]

---

[1] Zahlbericht 5, стр. 426, теорема 152.

[2] Frobenius. Über Bezieh. u. s. w. Sitzber., Berl. Akad. 1896.

Для решения вопроса о существовании простых чисел, принадлежащих данному классу подстановок одновременно в нескольких полях, мы построим нормальное поле, содержащее эти поля, и посмотрим, найдется ли в этом последнем поле подстановка, производящая нужные нам подстановки среди величин заданных полей. При этом будем иметь в виду, что каждому простому числу соответствует класс подстановок и его простым идеальным делителям — подстановки этого класса (цит. выше, конец).

Будем рассматривать в Ω только те простые идеалы, для которых $f = 1$, иными словами — простые идеалы, принадлежащие к единичной подстановке.

Рассмотрим поле $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$, полученное из Ω присоединением величин

$$\beta_1 = \sqrt[l]{\alpha_1}, \quad \beta_2 = \sqrt[l]{\alpha_2}, \ldots, \quad \beta_t = \sqrt[l]{\alpha_t}.$$

Если мы будем считать поле Ω областью рациональности, то группа поля $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$ будет абелевой и состоящей из подстановок, переводящих величины β_i в $\zeta_i\beta_i$, где ζ_i — l-й корень из единицы. Докажем, что порядок этой группы равен l^t. Допустим обратное — пусть порядок этой группы менее l^t. Это значит, что если последовательно присоединять к полю Ω корни уравнений

$$z^l - \alpha_1 = 0, \quad z^l - \alpha_2 = 0, \ldots, z^l - \alpha_t = 0,$$

то после присоединения корней одного из них, последующее уже окажется приводимым. Пусть первое из таких, становящихся приводимыми уравнений будет $z^l - \alpha_v = 0$. Тогда оно распадется в $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$ на множители одной и той же степени, которая может быть только 1-й, так как l — простое число.

Итак

$$\beta_v = \varphi(\beta_1, \beta_2, \ldots, \beta_{v-1}). \tag{3}$$

С другой стороны, порядок поля $\Omega(\beta_1, \beta_2, \ldots, \beta_{v-1})$ должен быть равен l^{v-1}. Обозначим через S_i ту подстановку между величинами $\beta_1, \beta_2, \ldots, \beta_{v-1}$, которая переводит β_i в $\zeta\beta_i$, оставляя неизменными остальные величины $\beta_1, \beta_2, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_{v-1}$. Тогда группа поля $\Omega(\beta_1, \beta_2, \ldots, \beta_{v-1})$ состоит из подстановок типа

$$S_1^{\xi_1} \cdot S_2^{\xi_2} \cdots S_{v-1}^{\xi_{v-1}}.$$

Так как порядок этой группы равен l^{v-1}, то каждый из показателей $\xi_1, \xi_2, \ldots, \xi_{v-1}$ должен пробегать все значения из ряда чисел $0, 1, 2, \ldots, l-1$ совершенно независимо от других. В частности, подстановка S_i сама должна входить в группу поля $\Omega(\beta_1, \beta_2, \ldots, \beta_{v-1})$. Вследствие этого величина $\varphi(\beta_1, \beta_2, \ldots, \beta_{i-1}, \zeta\beta_i, \beta_{i+1}, \ldots, \beta_{v-1})$

ОБ ОДНОЙ ТЕОРЕМЕ ГИЛЬБЕРТА

UEBER EIN SATZ VON HILBERT

(Вісті. ВУАН, 1923, стр. 3—7)

В этой работе я доказываю следующую теорему, которую в менее строгой формулировке доказал Гильберт. [1]

Пусть дано нормальное поле Ω, содержащее l — е корни из единицы. Выберем в Ω t целых чисел

$$\alpha_1, \alpha_2, \ldots, \alpha_t$$

так, чтобы произведение

$$\alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdots \alpha_t^{m_t} \quad . \tag{1}$$

представляло l-ю степень некоторого числа из Ω только тогда, когда каждое из чисел $m_1, m_2, \ldots, m_t$ делится на l. Тогда в Ω найдется бесконечное множество таких простых идеалов ρ, что

$$\left\{\frac{\alpha_1}{\rho}\right\} = \zeta^{c_1}, \quad \left\{\frac{\alpha_2}{\rho}\right\} = \zeta^{c_2}, \ldots, \left\{\frac{\alpha_t}{\rho}\right\} = \zeta^{c_t}, \tag{2}$$

где $\zeta = e^{\frac{2\pi i}{l}}$; $c_1, c_2, \ldots, c_t$ — произвольно заданная система чисел из ряда $0, 1, 2, \ldots, l-1$ и $\left\{\frac{\alpha}{\rho}\right\}$ — обобщенный символ вычета, т. е.

$$\left\{\frac{\alpha}{\rho}\right\} = \zeta^c, \quad \text{если} \quad \alpha^{\frac{p^f - 1}{f}} \equiv \zeta^c \pmod{\rho},$$

где f — порядок идеала ρ.

(Нужно заметить, что $p^f - 1$ должно делиться на l, так как поле Ω содержит поле l-х корней из единицы $\omega(\zeta)$ и потому порядок каждого простого идеала из $\omega(\zeta)$, являющегося делителем p, будет делителем f).

Доказательство основывается на выводах моей работы „Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок“, где показано, что всегда существует бесконечное множество таких простых чисел, которые принадлежат к заданному классу подстановок группы данного уравнения. [2]

---

[1] Zahlbericht 5, стр. 426, теорема 152.

[2] Frobenius. Über Bezieh. u. s. w. Sitzber., Berl. Akad. 1896.

Эти простые числа разлагаются в Ω на простые идеалы первого порядка, так как подстановки S не изменяют величин из Ω. Последние в норме поля $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$ разлагаются на простые идеалы, из которых хотя один принадлежит к S. Обозначим такой идеал через B. Сравнение, характеризующее принадлежность к S, запишется так:

$$\omega^p = \omega/S \pmod{B},$$

где ω — произвольная целая величина из нормы поля $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$. Беря за ω $\beta_1, \beta_2, \ldots, \beta_t$, мы получим

$$\beta_1^p \equiv \zeta^{c_1}\beta_1, \quad \beta_2^p \equiv \zeta^{c_2}\beta_2, \ldots, \beta_t^p \equiv \zeta^{c_t}\beta_t \pmod{B},$$

откуда

$$\beta_1^{p-1} \equiv \zeta^{c_1}, \ \beta_2^{p-1} \equiv \zeta^{c_2}, \ldots, \beta_t^{p-1} \equiv \zeta^{c_t} \pmod{B}.$$

Заметим, что $p-1$ делится на l, так как в нашем случае $f=1$. Следовательно

$$\alpha_1^{\frac{p-1}{l}} \equiv \zeta^{c_1}, \quad \alpha_2^{\frac{p-1}{l}} \equiv \zeta^{c_2}, \ldots, \alpha_t^{\frac{p-1}{l}} \equiv \zeta^{c_t} \pmod{B}. \tag{6}$$

Сравнения эти содержат только величины из Ω и потому сохраняют силу, если за модуль взять в Ω произвольный простой идеал ρ, делящийся на B.

Из сравнения (6) и сравнения $\alpha^{\frac{p-1}{l}} \equiv \left\{\frac{\alpha}{\rho}\right\} \pmod{\rho}$ получаем

$$\left\{\frac{\alpha_1}{\rho}\right\} \equiv \zeta^{c_1}, \quad \left\{\frac{\alpha_2}{\rho}\right\} \equiv \zeta^{c_2}, \ldots, \left\{\frac{\alpha_t}{\rho}\right\} \equiv \zeta^{c_t} \pmod{\rho}.$$

Эти сравнения должны быть равенствами, так как различные l-е корни из единицы не могут быть сравнимы $(\mathrm{mod}\,\rho)$. Последнее утверждение следует из того, что идеал ρ не входит в дискриминант уравнения

$$\zeta^{l-1} + \zeta^{l-2} + \ldots + \zeta + 1 = 0.$$

Следовательно, простой идеал ρ обладает требуемым свойством и теорема доказана.

(Доложено академиком Д. А. Граве 10 ноября 1922 г.).

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ КРОНЕКЕРА — ВЕБЕРА ОТНОСИТЕЛЬНО АБЕЛЕВЫХ ОБЛАСТЕЙ[1]

(Матем. сборн. 31 (1923), стр. 302—308)

В настоящей статье я предлагаю наиболее краткое и элементарное из известных мне доказательств знаменитой теоремы Кронекера — Вебера.

Всякая область с абелевой группой есть область деления круга.

В основу доказательства положены два принципа, уже применявшиеся к циклическим областям Вебером,[2] но не высказанные до сих пор в общей форме. Первый принцип основывается на теореме:

От композиции всех *групп инерции* (Trägheitsgruppen) нормальной области получается полная группа Галуа области.

Этот принцип является в известном смысле обобщением теоремы Минковского, представляя в то же время аналогию свойствам группы монодромии на римановых поверхностях. Ему посвящен § 1.

Второй принцип восходит от Кронекера,[3] который ввел понятие *композиции циклических областей*. Его идея в применении к произвольным областям намечена и использована мной в статье „Задача, обратная задаче Чиргаузена“.[4] Здесь он изложен в § 2.

Кроме того, я пользуюсь гензелевским методом p-адических чисел правда в скрытой форме, а также методом Футера.[5]

§ 1

Дана произвольная нормальная область $K(x)$. Будем рассматривать различные ее подобласти $K(z)$. Поставим себе задачу: найти необходимое и достаточное условие для того, чтобы данное простое число не было *критическим* в области $K(z)$, т. е. чтобы в его разложение на простые идеальные множители внутри $K(z)$ не входили кратные. Пусть z принадлежит к группе g, а разложение p внутри $K(z)$ таково:

$$p = \mathfrak{p}_1^{d_1}.\mathfrak{p}_2^{d_2}. \ldots ,\mathfrak{p}_k^{d_k}. \qquad (1)$$

---

[1] Термином «область» я буду обозначать понятие, обозначаемое также терминами Körper — поле-корпус.

[2] Math. Ann., Bd. 67, 70.

[3] Monatsber. Berl. Akad., 1875.

[4] Журн. чист. и прикл. знания, т. I, в. 2.

[5] Math. Ann., Bd. 75, стр. 190—191.

Обозначая через (g) порядок группы g, а через $g_t^{(i)}$ — группу инерции, соответствующую входящему в ρ_i простому идеалу β_i внутри $K(x)$, мы будем иметь следующие формулы:

$$d_i = \frac{(g_t^{(i)})}{([g, g_t^{(i)}])} \qquad (i = 1, 2, \ldots, k), \tag{2}$$

где через $[g, g_t^{(i)}]$ обозначено пересечение групп g и $g_t^{(i)}$ (см. Bachmann. Zhlth., Bd. V). Из этих формул следует, что $d_i = 1$ тогда и только тогда, когда $g_t^{(i)} = [g, g_t^{(i)}]$, т. е. если $g_t^{(i)}$ является делителем g. Поэтому, для того чтобы p не было критическим числом в $K(z)$, необходимо и достаточно, чтобы все группы инерции, соответствующие идеальным множителям p, входили в группу, к которой принадлежит z.

Сопоставим эти условия для всех критических для $K(z)$ чисел сразу. В силу теоремы Минковского отсутствие критических чисел у $K(z)$ возможно только тогда, если $K(z)$ есть область рациональных чисел, откуда вытекает теорема:

Чтобы алгебраическое число, принадлежащее к нормальной области $K(x)$, было рационально, необходимо и достаточно, чтобы в группу, к которой оно принадлежит, входили все группы инерции области $K(x)$.

Эту теорему можно формулировать так:

От композиции всех групп инерции данной нормальной области получается ее полная группа Галуа.

§ 2

Даны две нормальные области $K(x)$ и $K(\bar{x})$ n-ой степени, группы которых G и $\bar{G}$ изоморфны. Пусть

$$x_1, x_2, \ldots, x_n \tag{3}$$

и

$$\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n \tag{4}$$

будут сопряженные примитивные величины обеих областей, занумерованные так, чтобы группы G и $\bar{G}$ состояли из подстановок, перемещающих одинаковые цифры. Исследуем область, в которой лежат коэффициенты перехода от величин (3) к величинам (4):

$$\begin{aligned}
\bar{x}_1 &= \alpha_0 + \alpha_1 x_1 + \alpha_2 x_1^2 + \cdots + \alpha_{n-1} x_1^{n-1}, \\
\bar{x}_2 &= \alpha_0 + \alpha_1 x_2 + \alpha_2 x_2^2 + \cdots + \alpha_{n-1} x_2^{n-1}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\bar{x}_n &= \alpha_0 + \alpha_1 x_n + \alpha_2 x_n^2 + \cdots + \alpha_{n-1} x_n^{n-1}.
\end{aligned} \tag{5}$$

Для этого умножим уравнения (5) соответственно на $x_1^i, x_2^i, \ldots, x_n^i$ $(i = 0, 1, 2\ldots, n-1)$ и сложим. Получим

$$\begin{aligned}
\bar{s}_1 &= n\cdot\alpha_0 + s_1\cdot\alpha_1 + s_2\cdot\alpha_2 + \ldots + s_{n-1}\cdot\alpha_{n-1},\\
\sum_i x_i\bar{x}_i &= s_1\alpha_0 + s_2\cdot\alpha_1 + s_3\cdot\alpha_2 + \ldots + s_n\cdot\alpha_{n-1},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\sum_i x_i^{n-1}\cdot\bar{x}_i &= s_{n-1}\cdot\alpha_0 + s_n\cdot\alpha_1 + s_{n+1}\cdot\alpha_2 + \ldots + s_{2n-2}\cdot\alpha_{n-1},
\end{aligned} \tag{6}$$

где s и $\bar{s}$ — суммы степеней сопряженных величин, т. е. рациональные числа. Для n неизвестных $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ получается n линейных уравнений с определителем, равным дискриминанту величин x. Значит, коэффициенты перехода $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ рационально выражаются через $\sum_i x_i\cdot\bar{x}_i, \sum_i x_i^2\cdot\bar{x}_i, \ldots, \sum_i x_i^{n-1}\cdot\bar{x}_i$. Эти величины являются элементами области $K(x, \bar{x})$, группа которой изоморфна или с произведением $G\cdot\bar{G}$, или с его гёльдеровским дополнением. Они не изменяются от подстановок типа

$$\begin{pmatrix} x_1, & x_2, \ldots, & x_n \\ x_{\alpha_1}, & x_{\alpha_2}, \ldots, & x_{\alpha_n} \end{pmatrix} \qquad \begin{pmatrix} \bar{x}_1, & \bar{x}_2, \ldots, & \bar{x}_n \\ \bar{x}_{\alpha_1}, & \bar{x}_{\alpha_2}, \ldots, & \bar{x}_{\alpha_n} \end{pmatrix}, \tag{7}$$

где $\begin{pmatrix} x_1, & x_2, \ldots, & x_n \\ x_{\alpha_1}, & x_{\alpha_2}, \ldots, & x_{\alpha_n} \end{pmatrix}$ — подстановки группы G. Эта группа является нормальным делителем $G\cdot\bar{G}$, в силу чего группа нашей *области перехода* изоморфна с делителем ее гёльдеровского дополнения. Сопряженные с $\sum_i x_i^n\cdot\bar{x}_i$ величины мы получим, если, оставляя величины ряда (3) на месте, мы произведем над величинами ряда (4) всевозможные подстановки группы $\bar{G}$ (или наоборот). Поэтому эта группа изоморфна или с G, или с ее делителем. Следующая *теорема* дает ответ на вопрос, когда имеет место тот или другой случай:

Если области $K(x)$ и $K(\bar{x})$ имеют общую область, принадлежащую соответственно в $K(x)$ и $K(\bar{x})$ к подгруппам H и $\bar{H}$ групп G и $\bar{G}$, то группа области перехода изоморфна или с H, или с ее делителем.

Не нарушая общности, можно предположить H нормальным делителем G, так как если в $K(\bar{x})$ входят величины, принадлежащие в $K(x)$ к H, то войдут и величины, принадлежащие к сопряженным с H группам, а также к их пересечению, которое является нормальным делителем G. Рассмотрим функцию Φ от величины $\sum_i x_i^k\bar{x}_i$, принадлежащую к группе, изоморфной с H, подстановки которой мы получим, если, оставляя величины (3) на месте, мы будем над величинами (4) производить подстановки группы $\bar{H}$ (а также наоборот). Величину Φ можно представить в следующем виде:

$$\Phi = X_1(x_1)\cdot\bar{X}_1(\bar{x}_1) + X_2(x_1)\cdot\bar{X}_2(\bar{x}_1) + \ldots,$$

так как величины $x_2, x_3, \ldots, x_n$ рационально выражаются через x_1, а $\bar{x}_2, \bar{x}_3, \ldots \bar{x}_n$ — через $\bar{x}_1$. Наше предположение позволяет написать:

$$\Phi = \frac{1}{h}\left\{X_1(x_1)\sum_{\bar{H}}\bar{X}_1(\bar{x}_i) + X_2(x_1)\cdot\sum_{\bar{H}}\bar{X}_2(\bar{x}_i) + \ldots\right\},$$

где h — порядок групп H и $\bar{H}$. Далее, по той же причине

$$\Phi = \frac{1}{h^2}\left\{\sum_{H}X_1(x_i)\cdot\sum_{\bar{H}}\bar{X}_1(\bar{x}_i) + \sum_{H}X_2(x_i)\cdot\sum_{\bar{H}}\bar{X}_2(\bar{x}_i) + \ldots\right\}.$$

Каждая из сумм внутри выражения рационально выражается через величины z (соответственно $\bar{z}$), принадлежащие к группе H (соответственно $\bar{H}$). Поэтому

$$\Phi = \Psi(z_1, \bar{z}_1).$$

Но, как величина из области перехода, Φ не изменится, если над величинами z_1, $\bar{z}_1$, мы применим подстановку типа (7). Поэтому

$$\Phi = \frac{1}{k}\{\Psi(z_1, \bar{z}_1) + \Psi(z_2, \bar{z}_2) + \cdots + \Psi(z_k, \bar{z}_k)\}, \tag{8}$$

где k — число величин, сопряженных с z_1 (или $\bar{z}_1$). Предположение нашей теоремы дает начало следующим формулам:

$$\bar{z}_1 = \varphi(z_1), \bar{z}_2 = \varphi(z_2), \ldots, \bar{z}_k = \varphi(z_k). \tag{9}$$

Подставляя их в (8), мы придем к выражению для Φ, симметрическому относительно $z_1, z_2, \ldots, z_k$. Это доказывает, что Φ равна рациональной величине, ч. и т. д.

§ 3

Обратимся теперь к теореме Кронекера — Вебера. Как обычно, приведем вопрос к исследованию циклической области $K(x)$ степени $m = l^u$, где l — простое число. Из теоремы § 1 следует, что существует хоть одно простое число, для идеальных множителей которого группа инерции будет совпадать с группой Галуа нашей области. Будем вместе с Вебером называть подобные числа *вполне критическими* (total kritisch). Разберем отдельно случаи, когда вполне критическое простое число отлично от l и совпадает с l.

В первом случае имеет место сравнение

$$p \equiv 1 \pmod{l^u}. \tag{10}$$

Действительно, в этом случае $(p) = (\rho l^u)$, где ρ — простой идеал области $K(x)$. *Область инерции* состоит только из рациональных чисел, а потому всякое целое число области $K(x)$ сравнимо с рациональным числом по модулю ρ. Возьмем число P, делящееся *точно* на первую степень ρ. Пусть s будет одна из первообразных подстановок группы Галуа.

Величина $\frac{sP}{P}$ взаимно проста с ρ, а потому сравнима с некоторым рациональным числом α по модулю ρ, откуда

$$sP \equiv \alpha P \pmod{\rho^2}. \tag{11}$$

Применяя эту подстановку $m = l^u$ раз, мы получим

$$s^m P \equiv \alpha^m \cdot P \pmod{\rho^2}.$$

Отсюда, в силу $s^m = 1$: $P \equiv \alpha^m \cdot P \pmod{\rho^2}$, или

$$\alpha^m \equiv 1 \pmod{p}. \tag{12}$$

С другой стороны, если бы имело место

$$\alpha^d \equiv 1 \pmod{\rho},$$

где $d \cdot d_1 = m$, $d_1 > 1$, то мы имели бы

$$s^d P \equiv P \pmod{\rho^2},$$

откуда

$$s^d P \equiv P + b \cdot P^k \pmod{\rho^{k+1}},$$

где b — целое рациональное число, не делящееся на p. Тогда

$$\begin{aligned} s^{2d} P &\equiv s^d P + b (s^d P)^k \equiv P + 2bP^k \pmod{\rho^{k+1}}, \\ s^{3d} P &\equiv P + 3b \cdot P^k \pmod{\rho^{k+1}}, \\ &\cdots\cdots\cdots\cdots\cdots \\ s^{d_1 d} P &\equiv P + d_1 b P^k \pmod{\rho^{k+1}}. \end{aligned}$$

Но ни d_1, ни b не делятся на p, а потому это сравнение несовместимо с равенством

$$s^{d_1 d} P = s^m P = P.$$

Таким образом, a является первообразным корнем сравнения

$$x^m - 1 \equiv 0 \pmod{p},$$

а потому m должно быть делителем $p - 1$, ч. и т. д. Построим теперь при помощи корня уравнения

$$z^{p-1} + z^{p-2} + \cdots + z + 1 = 0 \tag{13}$$

циклическую область $K(y)$ степени m. Для нее единственным критическим числом будет v, которое в силу этого должно быть вполне критическим.

Покажем, что переход от $K(x)$ к $K(y)$ можно подобрать таким образом, чтобы в области перехода p не было критическим. Для этого особым образом подберем в $K(x)$ и $K(y)$ числа P и $\overline{P}$, делящиеся точно на первые степени простых идеальных множителей p. Возьмем первообразный корень g сравнения

$$x^m - 1 \equiv 0 \pmod{p^k}, \tag{14}$$

где k — сколь угодно большое число, притом так, чтобы

$$g \equiv a \pmod{p} \quad \text{(см. (12).}$$

Составим выражение

$$g^{m-1} \cdot P + g^{m-2} \cdot sP + \cdots + g \cdot s^{m-2}P + s^{m-1}P \tag{15}$$

и возьмем его в качестве P. Оно тоже делится точно на первую степень ρ, так как в силу (11) оно сравнимо по модулю ρ^2 с выражением

$$(g^{m-1} + g^{m-2}a + \cdots + ga^{m-2} + a^{m-1})P \equiv mg^{m-1}P \pmod{\rho^2}.$$

Кроме того,

$$sP \equiv gP \pmod{p^k}. \tag{16}$$

Выбирая различные подстановки (3), мы сможем выбрать для роли g любой корень сравнения (14). Выберем подобным же образом подстановку $\bar{s}$ и число $\bar{P}$ в $K(y)$ так, чтобы имело место

$$\bar{s}\bar{P} \equiv g \cdot \bar{P} \pmod{p^k}. \tag{17}$$

Исследуем по модулю p^k коэффициенты перехода от P к $\bar{P}$

$$\bar{P} = \alpha_0 + \alpha_1 P + \cdots + \alpha_{m-1}P^{m-1}. \tag{18}$$

Рассмотрим норму P

$$N(P) \equiv P \cdot sP \cdots s^{m-1}P \equiv 1 \cdot g \cdots g^{m-1} \cdot P^m \equiv \pm P^m \pmod{p^k}. \tag{19}$$

Но $N(P)$ равна целому рациональному числу, делящемуся точно на первую степень p. Поэтому

$$P^m \equiv ap \pmod{p^k}, \quad (a, p) = 1, \tag{20}$$

и точно так же

$$\bar{P}^m \equiv bp \pmod{p^k}, \quad (b, p) = 1. \tag{21}$$

Отсюда, обозначая через c корень сравнения

$$a \cdot x \equiv b \pmod{p^k}, \tag{22}$$

мы придем к сравнению

$$(\alpha_0 + \alpha_1 P + \cdots + \alpha_{m-1}P^{m-1})^m \equiv cP^m \pmod{p^k}. \tag{23}$$

Взяв $k > m(m-1)$, мы придем к сравнениям

$$\alpha_0 \equiv 0, \quad \alpha_1{}^m \equiv c, \quad \alpha_2 \equiv 0, \ldots, \quad \alpha_{m-1} \equiv 0 \pmod{p^k}. \tag{24}$$

Сравнение $\alpha_1{}^m - c \equiv 0 \pmod{p^k}$ может или разлагаться на линейные множители, и тогда α_1 будет сравнимо по модулю p^k с рациональным числом, или иметь неприводимые по модулю p множители, дискриминант которых не делится на p. Поэтому для уравнения, которому удовлетворяет α_1, число p не будет критическим.

Исследуем теперь коэффициенты перехода от x к y (эти величины выбраны независимо от k).

$$y = \beta_0 + \beta_1 x + \cdots + \beta_{m-1} x^{m-1}.$$

В § 2 доказано, что $\beta_0, \beta_1, \ldots, \beta_{m-1}$ рационально выражаются через

$$\sum_i x_i y_i, \qquad \sum_i x_i^2 y_i, \ldots, \qquad \sum_i x_i^{m-1} y_i. \tag{25}$$

Рассмотрим величину $\sum_i x_i^k y_i$ и выразим в ней x через P, а y — через $\overline{P}$. Подставляя вместо P его выражение (18) и принимая во внимание сравнения (24), мы придем к сравнению

$$\sum_i x_i^k y_i \equiv \varphi(\alpha_1) \pmod{p^k}.$$

Это сравнение показывает, что для величин (25) число p не будет критическим.

Таким образом, величины области $K(x)$ рационально выражаются через корень уравнения (13), т. е. через корень из единицы, и через корень циклического уравнения не выше m-ой степени, область которого имеет одним критическим числом меньше, чем $K(x)$ (новых делителей дискриминант области $K(x, y)$, а тем более области перехода, иметь не может). Избавившись от всех вполне критических чисел, мы придем к приводимым уравнениям m-ой степени, т. е. понизим степень.

§ 4

В случае $p = l$ подобный выбор P невозможен. Я предпочел в этом случае путь постепенного понижения группы инерции.

Предположим, что мы избавились от всех вполне критических простых чисел, кроме l. Образуем для $K(x)$ подобласть l-ой степени. Она входит во все области инерции области $K(x)$, кроме той, что соответствует числу l, потому что степень каждой из них ниже $m = l^u$. Поэтому критическим числом для этой подобласти может служить только l.

Докажем, что существует только одна циклическая область l-ой степени с единственным критическим числом l. Допустим, что существуют две различных области подобного типа, и обозначим их через $K(x)$ и $K(y)$. Если для области $K(x, y)$ группа инерции l-го порядка, то и вся область, в силу теоремы § 1, должна быть l-ой степени, т. е. совпадать и с $K(x)$ и с $K(y)$, и наше утверждение будет доказано. С другой стороны, если бы группа инерции области $K(x, y)$ была l^2-го порядка, т. е. совпадала с полной группой Галуа, то она не была бы циклической, так как в нее входят две существенно различные подгруппы l-го порядка, именно группа, к которой принадлежит $K(x)$, и группа, к которой принадлежит $K(y)$.

Докажем, что при $l>2$ это предположение невозможно. Действительно, пусть область $K(x, y)$ имеет группу инерции l^2-го порядка, все подстановки которой l-го порядка. Тогда $(l)=(\mathfrak{L}^l)$, где $\mathfrak{L}$ — простой идеал области. Рассмотрим величину L, делящуюся точно на первую степень $\mathfrak{L}$. *Область раздвоения* (Verzweigungskörper), область инерции и область рациональных чисел здесь совпадают, в силу чего для каждой подстановки s имеет место сравнение

$$sL\equiv L+a\cdot L^r \qquad (\mathrm{mod}\,\mathfrak{L}^{r+1}), \tag{26}$$

где a — целое рациональное число, не делящееся на l. Так как подстановок всего l^2-1, а различных по модулю l чисел только l, то для некоторых подстановок s и s_1 должно иметь место

$$s_1L\equiv sL \qquad (\mathrm{mod}\,\mathfrak{L}^{r+1}),$$

или

$$\sigma L\equiv L \qquad (\mathrm{mod}\,\mathfrak{L}^{r+1}), \tag{27}$$

где $\sigma=s_1\cdot s^{-1}$. Пусть η_1 и η будут величины, принадлежащие соответственно к группам $[1, s, \ldots, s^{l-1}]$ и $[1, \sigma, \ldots, \sigma^{l-1}]$. Вычислим относительные дифференты области $K(x, y)$ по отношению к областям $K(\eta)$ и $K(\eta_1)$. Всякое целое число в $K(x, y)$ может быть представлено в форме

$$\alpha_0+\alpha_1L+\alpha_2L^2+\cdots \qquad (\mathrm{mod}\,\mathfrak{L}^k),$$

где k — сколь угодно большое число, откуда ясно, что дифферента области содержит $\mathfrak{L}$ в той же степени, что и дифферента числа L. Дифферента по отношению к $K(\eta)$ делится точно на $\mathfrak{L}^{r(l-1)}$, а дифферента по отношению к $K(\eta_1)$ во всяком случае делится на $\mathfrak{L}^{(r+1)(l-1)}$. Отсюда, в силу теоремы о дифферентах (см. Zahlbericht, стр. 209, теорема 41), следует, что дифферента области $K(\eta)$ делится на более высокую степень $\mathfrak{L}$ (или l), чем дифферента области $K(\eta_1)$. Но в случае $l>2$ это невозможно. Действительно, пусть L величина в $K(\eta)$, делящаяся точно на первую степень простого идеала $\mathfrak{c}$ в $K(\eta)$, причем $(\mathfrak{c})=(l^l)$. Далее, пусть

$$sL\equiv L+a\cdot L^r \qquad (\mathrm{mod}\,\mathfrak{c}^{r+1}) \qquad (a\not\equiv 0\,(\mathrm{mod}\,l)). \tag{28}$$

Тогда $\mathfrak{c}$ входит в дифференту в $r(l-1)$-ой степени. С другой стороны, составим уравнение

$$f(x)=x^l+\lambda_1\cdot x^{l-1}+\cdots+\lambda_l=0, \tag{29}$$

которому удовлетворяет L. Дифферента может быть представлена так:

$$\delta=\frac{\partial f(L)}{\partial L}=l\cdot L^{l-1}+(l-1)\lambda_1\cdot L^{l-2}+\cdots+\lambda_{l-1} \tag{30}$$

(см. Zahlbericht, § 12, стр. 200). Во всех λ_i, как рациональных числах $\mathfrak{c}$ входит в степенях, кратных l. Поэтому во всех членах выражения

(30) c входит в разных степенях. В силу этого каждый из членов должен делиться на $c^{r(l-1)}$. Этот факт дает при рассмотрении первого члена начало следующему неравенству: $l+(l-1)\geqslant r(l-1)$, или

$$r\leqslant 2+\frac{1}{l-1}. \tag{31}$$

Отсюда, при $l>2$, $r=2$, т. е. во всякой области рассматриваемого типа c входит в дифференту в $2(l-1)$-ой степени, и одновременное существование двух областей $K(\eta)$ и $K(\eta_1)$ с различными дифферентами невозможно. Наше утверждение доказано.

Обратимся опять к нашей области $K(x)$ l^u-го порядка. Она будет иметь вместе с циклической областью $K(y)$, степени l^u, построенной при помощи корня уравнения

$$z^{l^u+1}-1=0, \tag{32}$$

общую подобласть l-ой степени. Из этого вытекает (см. теорему § 2), что существует область перехода от $K(x)$ к $K(y)$, степень которой равна l^{u+1}. Задача понижения степени области решена. Продолжая рассуждать подобным образом, мы найдем выражение величин первоначальной области через корни из единицы.

Остался неразобранным случай $l=2$. Существуют три различных области второй степени с дискриминантом, равным степени двойки: $K(i)$, $K(\sqrt{-2})$ и $K(\sqrt{2})$; все они являются областями деления круга. Переходя к областям степени 2^u $(u>1)$, заметим, что их подобласти 2-й степени всегда вещественны. Это очевидно, если область $K(x)$ вещественна; в случае мнимой области $K(x)$ подстановка, переводящая комплексные величины $\alpha+i\beta$ области в сопряженные комплексные $\alpha-i\beta$, не изменяя рациональных соотношений между величинами, должна принадлежать к группе области. Эта подстановка — второго порядка, а потому степень принадлежащей к ней подобласти равна 2^{u-1}. Величины этой подобласти, не изменяясь от перемены знака при i, должны быть вещественны. Но $u-1\geqslant 1$, следовательно, подобласть 2-й степени подавно вещественна. Значит, в нашей области подобластью 2-ой степени должна быть $K(\sqrt{2})$. Точно так же циклическая область 2^u-ой степени, являющаяся вещественной подобластью области корней уравнения

$$x^{2^{u+1}}-1=0, \tag{33}$$

имеет тоже $K(\sqrt{2})$ подобластью 2-ой степени. Это позволяет применить к нашему случаю те же рассуждения, что и в случае нечетного l. Таким образом, теорема доказана во всех своих частях.

ОПРЕДЕЛЕНИЕ ПЛОТНОСТИ СОВОКУПНОСТИ ПРОСТЫХ ЧИСЕЛ, ПРИНАДЛЕЖАЩИХ К ЗАДАННОМУ КЛАССУ ПОДСТАНОВОК

(Изв. Российской Академии Наук, 17 (1923), стр. 205—250)

Представлено на заседании Отделения физико-математических наук 7 марта 1923 г.

Задача, решение которой является целью настоящей работы, была поставлена Фробениусом [1]. Она состоит в следующем. Дано неприводимое нормальное уравнение n-ой степени

$$f(x) = 0, \tag{1}$$

Обозначим область, полученную от присоединения к области рациональных чисел его корня, через $\Omega(x)$, а через $\mathfrak{p}$ простой идеал внутри $\Omega(x)$, взаимно простой с дискриминантом уравнения (1). Тогда имеют место сравнения

$$x_1^p \equiv x_{\alpha_1},\ x_2^p \equiv x_{\alpha_2},\ \ldots,\ x_n^p \equiv x_{\alpha_n} \qquad (\mathrm{mod}\ \mathfrak{p}), \tag{2}$$

если через $x_1, x_2, \ldots, x_n$ обозначить сопряженные корни уравнения (1), а

$$S = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \ldots & \alpha_n \end{pmatrix}$$

является подстановкой над $1, 2, 3, \ldots, n$, которая, как известно, входит в группу G уравнения (1) [2,1]. Тогда будем говорить, что простой идеал $\mathfrak{p}$ *принадлежит* к подстановке S, а рациональное простое число p, кратное $\mathfrak{p}$, *принадлежит* к классу подстановок TST^{-1}, где T пробегает все подстановки группы G.

Рассмотрим совокупность всех простых чисел, принадлежащих к этому классу подстановок. Выражение

$$\lim_{=1} \frac{\Sigma p^{-s}}{\lg \frac{1}{s-1}}, \tag{3}$$

где сумма распространяется на все простые числа этой совокупности, носит название *плотности* совокупности. Наша задача заключается в определении величины плотности этой совокупности.

Понятие плотности впервые встречается у Дирихле [3], который доказал, что простые числа *равномерно* распределяются по классам сравнений любого модуля k, взаимно простым с k, т. е. что плот-

ность каждой такой совокупности равна $\frac{1}{\varphi(k)}$. Исследования Куммера связывают этот результат с определением плотности совокупности простых чисел, принадлежащих к каждой из подстановок в области каких-нибудь корней из единицы ([4]; см. также § 11 моей работы). Кронекер [5] нашел величину плотности совокупности простых чисел, принадлежащих к тождественной подстановке в произвольной области.

Вопросом о простых числах, принадлежащих к любому классу подстановок в произвольной области, занялся Фробениус. Скелет его результата был ему известен еще в 1882 г., и в 101 томе Journ. f. Math. он публикует групповую часть этой проблемы.

Однако свой результат в полном объеме он опубликовал лишь после того, как Дедекинд [2] доказал обратную теорему: подстановка, к которой принадлежит какой-нибудь простой идеал, входит в группу области. В своем основном мемуаре Фробениус [1], применяя результат Кронекера последовательно к различным делителям основной области, определяет плотность совокупности простых чисел, принадлежащих к *отделу* данной подстановки, т. е. к совокупности классов, образованных всеми ее первообразными степенями. Фробениусу, однако, не удалось определить плотностей совокупностей простых чисел, принадлежащих к отдельным классам подстановок, о чем он говорит в своей работе в следующих выражениях: „Indem man hier für G der Reihe nach alle cyklischen Untergruppen von H setzt, erhält man eine Reihe von Gleichungen, die aber nicht ausreichen, um schliessen zu können, dass

$$\sum p_\lambda^{-1-w} = \frac{h_\lambda}{h} \lg\left(\frac{1}{w}\right) + \mathfrak{P}_\lambda(w) \tag{16}$$

ist".

И далее: „Wenn es gelänge, die Formel (16) zu beweisen, so würde sich für die Dichtigkeit der Primzahlen P_λ, die der λ^{ten} Classe von Substitutionen entsprechen, der einfache Ausdruck:

$$D_\lambda = \frac{h_\lambda}{h} = \frac{1}{v_\lambda} \tag{18}$$

ergeben, es würde also der Satz gelten:

V. Jeder Classe von Substitutionen der Gruppe H entspreshen unzählig viele rationale Primzahlen. Iher Dichtigkeit ist der Anzahl der verschiedenen Substitutionen der Classe proportional. Oder:

Die Dichtigkeit der Primzahlen, die einer Classe von Substitutionen entsprechen, ist der Dichtigkeit der Classe gleich".

Этому общему результату Фробениуса не было суждено сыграть в науке такой большой роли, какую сыграл результат Гильберта, который был опубликован почти одновременно с фробениусов-

ским и может быть рассматриваем как его частный случай, выраженный в несколько видоизмененной форме. Это—теорема Гильберта о существовании в любой нормальной области, заключающей в себе l-е корни из единицы, бесчисленного множества простых идеалов с наперед заданной вычетностью ([6]; см. также главу VI настоящей работы). Основываясь на этой теореме, Фуртвенглер [7] доказывает для любой области существование соответствующей ей *области классов* (Klassenkörper). Эта же теорема играет большую роль при выводе общего закона взаимности [8].

Дальнейшая литература по этому вопросу невелика. В Arch. d. Math. u. Phys. Bd. 6(3), 1904, помещены три небольшие статьи М. Бауэра, в которых он дает непосредственные приложения фробениусовского результата к констатированию тождественности или независимости двух областей, а также к выводу характеристического свойства областей деления круга. Эти результаты являются частными случаями теоремы, доказываемой в главе V настоящей работы. Кроме этих статей, в Протоколах Харьковского мат. общ. за 1915 год помещена статья Б. Н. Делоне [9], который, пользуясь фробениусовским результатом и законом взаимности Эйзенштейна, доказал (правда, не для всех случаев) теорему Кронекера—Вебера о том, что все абелевы области суть области деления круга.

Моя работа построена по следующему плану:

В § 1 я в существенных чертах воспроизвожу исследование Фробениуса, доделывая все выкладки до конца. В ходе рассуждений я значительно уклоняюсь от Фробениуса главным образом потому, что ограничиваюсь рассмотрением неприводимых уравнений, что дает возможность избежать применения трудных и мало известных теорем из теории групп.

В § 2 я обобщаю найденную Куммером [4] связь между прогрессиями и областями деления круга. Вместо прогрессии, я ввожу в рассмотрение более общее понятие *комплекса.*

В § 3 я обобщаю теорему Дирихле о прогрессиях. Именно, я доказываю существование в любой области бесчисленного множества простых идеалов, нормы которых лежат в наперед заданных допустимых комплексах. *Подобные обобщения делались и другими авторами.* Так, Вебер [10] доказывает даже более общую теорему, но высказывает ее не вполне отчетливо (именно, расплывчато формулировано понятие, соответствующее моим *допустимым комплексам*) и, кроме того, он предполагает существование области классов (Klassenkörper), чего я избегаю, несколько суживая объем результата и вводя понятие комплексов, допустимых в *узком* и в *широком смысле.* При доказательстве приходится обобщать результат Дирихле—Минковского (связь между кратными интегралами и рядами Дирихле). Гильберт [11] делает это же самое обобщение и применяет его к теореме, подобной моей, но только имея в виду комплексы более частного типа.

В § 4 я определяю плотность совокупности простых чисел, принадлежащих к данному классу подстановок. Для этого я присоединяю к нашей области некоторую область деления круга. Тогда, если определяющее эту последнюю уравнение остается по модулю p неприводимым, то теорема 12 показывает, что известные уравнения из распространенной области имеют или не имеют рациональные корни в зависимости от того, к какому из классов отдела принадлежит p. Пользуясь результатом § 3, мы отсюда докажем существование в каждом из классов отдела бесчисленного множества принадлежащих к нему простых чисел. Для того же, чтобы определить величину их плотности, я присоединяю не одну область деления круга, а k, причем k безгранично увеличиваю. Этот прием дает возможность определить искомую плотность. Однако оценить величину остаточного члена мне не удалось.

§ 5 посвящен выводу критерия родственности областей. Он содержит теорему, частные случаи которой рассмотрены в статьях М. Бауэра и Б. Н. Делоне [9].

Наконец, в § 6 я показываю, что теорема Гильберта [6], притом в более общей формулировке, может быть легко выведена из результата § 5.

§ 1. Исследование Фробениуса

Возьмем неприводимое нормальное уравнение

$$f(x) = 0 \tag{1a}$$

и обозначим его корни через $x_1, x_2, \ldots, x_n$. Тогда справедлива

Теорема 1. *Имеют место сравнения*

$$x_1^p \equiv x_{\alpha_1}, x_2^p \equiv x_{\alpha_2}, \ldots, x_n^p \equiv x_{\alpha_n} (\mathrm{mod}\, \mathfrak{p}), \tag{2a}$$

где p — простое число, не входящее в дискриминант уравнения (1), $\mathfrak{p}$ *— его простой идеальный множитель в* $\Omega(x)$, *а*

$$S = \begin{pmatrix} 1, & 2, & 3, \ldots, & n \\ \alpha_1, & \alpha_2, & \alpha_3, \ldots, & \alpha_n \end{pmatrix}$$

подстановка над числами 1, 2, 3, ..., n.

Доказательство — см. [1], стр. 691.

Определение 1. В случае, когда имеют место сравнения (2a), будем говорить, что простой идеал $\mathfrak{p}$ *принадлежит* к подстановке S.

Теорема 2. *Подстановка S входит в группу Галуа G уравнения* (1a).

Доказательство — см. [1], стр. 696.

Теорема 3. *Если $\mathfrak{p}$ принадлежит к S, то простой идеал $\mathfrak{p}/T$, в который $\mathfrak{p}$ переходит посредством подстановки T из G, принадлежит к $T^{-1}ST$.*

Доказательство — см.[1], стр. 70.

Определение 2. Совокупность подстановок $T^{-1}ST$, где T пробегает всю группу G, будем называть *классом* подстановки S.

Так как p является произведением всех различных простых идеалов, сопряженных с $\mathfrak{p}$, то теорема 3 позволяет ввести следующее новое определение:

Определение 3. В случае, если имеют место сравнения (2а), простое число p принадлежит к классу подстановки S.

Теорема 4. *Если z величина из $\Omega(x)$, принадлежащая к группе H, а*

$$F(z) = 0 \tag{4}$$

неприводимое уравнение, которому она удовлетворяет, то сравнение

$$F(z) \equiv 0 \pmod{\mathfrak{p}} \tag{5}$$

имеет рациональные корни тогда и только тогда, когда хоть одна из подстановок S класса, к которому принадлежит p, входит в H, и число этих рациональных корней равно числу входящих в H подстановок в ряду $T_\nu S T_\nu^{-1}$, если T_ν пробегает все значения $T_1 = 1, T_2, T_3, \ldots$ в разложении

$$G = H + T_2 H + T_3 H + \ldots$$

Доказательство — см. [1], § 5, стр. 701.

Определение 4. Под символом $P(s-1)$ будем подразумевать функцию от s, остающуюся конечной при $s = 1$.

Теорема 5 (Кронекера). *Имеет место формула*

$$\sum_{p} \nu_p p^{-s} = \lg \frac{1}{s-1} + P(s-1), \tag{6}$$

где сумма распространяется на все простые числа p, а ν_p обозначает число рациональных корней сравнения (5).

Доказательство — см. [12].

Определение 5. Под *отделом* (Abteilung) мы будем понимать совокупность подстановок $TS^i T^{-1}$, где T пробегает все подстановки группы G, а i — все числа, не превышающие и взаимно простые с порядком f подстановки S.

Определение 6. Совокупность простых чисел, принадлежащих ко всем классам отдела, будем называть совокупностью, принадлежащей к отделу.

Определение 7. Под *плотностью* совокупности простых чисел мы будем разуметь значение выражения

$$\lim_{s=1} \frac{\sum_{p} p^{-s}}{\lg \frac{1}{s-1}},$$

где сумма распространяется на все простые числа этой совокупности. Пусть

$$S_\lambda = (x_{11}, x_{12}, \ldots, x_{1f_\lambda})(x_{21}, x_{22}, \ldots, x_{2f_\lambda}) \ldots (x_{e_\lambda 1}, x_{e_\lambda 2}, \ldots, x_{e_\lambda f_\lambda}). \tag{7}$$
$$(e_\lambda f_\lambda = n)$$

будет подстановка порядка f_λ, входящая в G. Определим плотность совокупности простых чисел, принадлежащих к отделу S_λ.

Введем следующие обозначения:

f_λ — для порядка подстановки S_λ;

n_λ — для числа различных подстановок, входящих в класс S_λ;

k_λ — для числа различных классов, входящих в отдел S_λ:

H_λ — для группы подстановок, входящих в G и перестановочных с S_λ;

$\overline{H_\lambda}$ — для группы таких подстановок T, входящих в G, что подстановки $TS_\lambda T^{-1}$ являются степенями S_λ.

Тогда мы сможем притти к следующей

Главной теореме. *Плотность совокупности простых чисел, принадлежащих к отделу* S_λ, *равна* $k_\lambda \cdot \frac{n_\lambda}{n}$.

Для доказательства изберем индуктивный путь, доказав теорему: A) для тождественной подстановки, B) для случая, когда порядок S_λ есть простое число, и C) для общего случая в предположении, что теорема доказана для тех степеней S_δ подстановки S_λ, порядки которых f_δ суть *настоящие* (echte) делители числа f_λ.

A) Применим формулу (6) к уравнению (1). Так как оно нормально, то сравнение

$$f(x) \equiv 0 \pmod{p} \tag{8}$$

имеет рациональные корни тогда и только тогда, когда имеют место следующие сравнения:

$$x_1^p \equiv x_1,\ x_2^p \equiv x_2,\ \ldots,\ x_n^p \equiv x_n \pmod{p}, \tag{9}$$

а тогда все корни сравнения (8) рациональны, т. е. $\nu_p = n$. Формула (6) принимает вид

$$\sum_{p_0} p_0^{-s} = \frac{1}{n} \lg \frac{1}{s-1} + P(s-1), \tag{10}$$

и таким образом плотность нашей совокупности равна $\frac{1}{n}$.

B) Рассмотрим теперь $\frac{f_\lambda}{q_1}$-ую степень подстановки S_λ

$$S_1 = S_\lambda^{\frac{f_\lambda}{q_1}},$$

где q_1 — какой-нибудь простой делитель f_λ. Образуем величину ξ_1, принадлежащую к группе $(S_1)^i$ (символ $(S_1)^i$ обозначает циклическую группу, состоящую из степеней S_1), и неприводимое уравнение

$$\Phi(\xi_1) = 0, \tag{11}$$

которому она удовлетворяет. Сравнение

$$\Phi(\xi_1) \equiv 0 \pmod{p}$$

имеет, в силу теоремы 4, рациональные корни тогда и только тогда, когда подстановка класса, к которому принадлежит простой модуль p, входит хоть в одну из групп $T_\nu (S_1)^i T_\nu^{-1}$ и их число равно числу таких групп. Это может иметь место в двух случаях: 1) p принадлежит к тождественной подстановке; все $\frac{n}{q_1}$ корней рациональны; это простые числа уже рассмотренного нами типа p_0; 2) или p принадлежит к одной из первообразных подстановок группы $(S_1)^i$, т. е. к одному из классов нашего отдела $T_\nu (S_1)^i T_\nu^{-1}$. Из теоремы 4 следует, что искомое число равно индексу $(\overline{H}_1, (S_1)^i)$. Но так как

$$(\overline{H}_1, (S_1)^i) = (\overline{H}_1, H_1)(H_1, (S_1)^i),$$

то дело сводится к выражению обоих множителей через n, n_1, q_1 и k_1.

С другой стороны,

$$(H_1, (S_1)^i) = (G, (S_1)^i) : (G, H_1),$$

а

$$(G, (S_1)^i) = \frac{n}{q_1}.$$

Если мы теперь введем на время обозначение $(G, H_1) = a$, то из разложения

$$G = H_1 + T_2 H_1 + \cdots + T_a H_1$$

следует, что для того, чтобы две подстановки из G преобразовали S_1 в одну и ту же подстановку, необходимо и достаточно, чтобы они входили в одну и ту же сопряженную систему. Это показывает, что число различных подстановок типа $T_\nu S_1 T_\nu^{-1}$ равно a, т. е. $a = n$. Поэтому

$$(H_1, (S_1)^i) = \frac{n}{q_i n_1}.$$

Чтобы определить величину $(\overline{H}_1, H_1)$, заметим, что все $\varphi(q_1)$ первообразных степеней подстановки S_1 образуют k_1 классов отдела, а поэтому в каждый из этих классов входит по $\frac{\varphi(q_1)}{k_1}$ степеней S_1. Поэтому из разложения

$$\overline{H}_1 = H_1 + T_2 H_1 + \ldots$$

следует, что индекс $(\overline{H}_1, H_1)$ равен $\frac{\varphi(q_1)}{k_1}$. Сопоставляя все полученные результаты, мы видим, что искомое число рациональных корней сравнения $\Phi(\xi_1) \equiv 0 \pmod p$ равно $\frac{n\varphi(q_1)}{q_1 n_1 \cdot k_1}$.

Формула (6) принимает вид

$$\frac{n}{q_1} \sum_{p_0} p_0^{-s} + \frac{n(q_1 - 1)}{q_1 n_1 k_1} \sum_{p_1} p_1^{-s} + P(s-1) = \lg \frac{1}{s-1} + P(s-1),$$

если мы через p_1 будем обозначать простые числа, принадлежащие к нашему отделу. Пользуясь формулой (10), мы приходим к следующему результату:

$$\sum p_{11}^{-s} + \sum p_{12}^{-s} + \ldots + \sum p_{1k_1}^{-s} = k_1 \frac{n_1}{n} \lg \frac{1}{s-1} + P(s-1), \quad (12)$$

где мы совокупность (p_1) разбили на совокупности (p_{11}), (p_{12}), ..., (p_{1k_1}), принадлежащие к различным классам нашего отдела.

C) Теперь мы в состоянии доказать, что плотность совокупности простых чисел, принадлежащих к отделу подстановки S_λ, равна $\frac{k_\lambda n_\lambda}{n}$, если мы будем наше утверждение считать доказанным для тех степеней S_λ, порядок которых f_δ есть настоящий (echter) делитель f_λ $(f_\delta < f_\lambda)$.

Пусть ξ_λ будет величина из $\Omega(x)$, принадлежащая к группе $(S_\lambda)^i$, и пусть

$$\Phi(\xi_\lambda) = 0 \quad (13)$$

будет неприводимое уравнение, которому она удовлетворяет. Степень этого уравнения равна $\frac{n}{f_\lambda}$. Чтобы сравнение

$$\Phi(\xi_\lambda) \equiv 0 \pmod{p} \quad (14)$$

имело рациональные корни, необходимо и достаточно, чтобы p принадлежало к одному из отделов, образованных степенями подстановки S_λ. Рассмотрим простые числа типа p_δ, принадлежащие к отделу S_δ. Порядок S_δ пусть равен f_δ (пока мы не исключаем случая $f_\delta = f_\lambda$). Число рациональных корней сравнения (14) в этом случае равно числу таких подстановок T_ν в разложении

$$G = (S_\lambda)^i + T_2(S_\lambda)^i + \ldots + T_{\frac{n}{f_\lambda}}(S_\lambda)^i, \quad (15)$$

которые преобразуют подстановку S_δ в одну из ее степеней. Но так как группа $(S_\lambda)^i$ ввиду соотношения

$$S_\lambda S_\delta = S_\lambda \cdot S_\lambda{}^i = S_\lambda{}^i S_\lambda = S_\delta S_\lambda$$

является делителем H_δ, то искомое число равно индексу

$$(\overline{H}_\delta, (S_\lambda)^i) = (\overline{H}_\delta, H_\delta) \cdot (H_\delta, (S_\lambda)^i).$$

Далее, мы можем, точно так же как в B), доказать, что $(\overline{H}_\delta, H_\delta)$ равно $\frac{\varphi(f_\delta)}{k_\delta}$. Что касается индекса $(H_\delta, (S_\lambda)^i)$, то он равен

$$(H_\delta, (S_\lambda)^i) = (H_\delta, (S_\delta)^i) : ((S_\lambda)^i, (S_\delta)^i) = (H_\delta, (S_\delta)^i) : \frac{f_\lambda}{f_\delta},$$

Наконец, прием, примененный нами уже в B), дает для индекса $(H_\delta, (S_\delta)^l)$ значение $\frac{n}{f_\delta n_\delta}$, откуда следует, что число рациональных корней сравнения (14) в нашем случае равно

$$\frac{n\varphi(f_\delta)}{f_\lambda n_\delta k_\delta}.$$

Формула (6) для уравнения (13) принимает поэтому следующий вид:

$$\sum_{f_\delta / f_\lambda} \frac{n\varphi(f_\delta)}{f_\lambda n_\delta \cdot k_\delta} \sum_{p_\delta} p_\delta^{-s} = \lg \frac{1}{s-1} + p(s-1). \tag{16}$$

Но для каждого $f_\delta < f_\lambda$ имеет место, в силу нашего предположения, формула

$$\sum_{p_\delta} p_\delta^{-s} = k_\delta \frac{n_\delta}{n} \lg \frac{1}{s-1} + p(s-1) \qquad (f_\delta < f_\lambda). \tag{17}$$

Подставляя эту формулу для всевозможных p_δ в (16), мы получим

$$\sum_{\substack{f_\delta / f_\lambda \\ f_\delta < f_\lambda}} \frac{n\varphi(f_\delta)}{f_\lambda n_\delta k_\delta} k_\delta \frac{n_\delta}{n} \lg \frac{1}{s-1} + \frac{n\varphi(f_\lambda)}{f_\lambda n_\lambda k_\lambda} \sum_{p_\lambda} p_\lambda^{-s} = \lg \frac{1}{s-1} + p(s-1), \tag{18}$$

что может быть преобразовано так:

$$\sum_{p_\lambda} p_\lambda^{-s} = k_\lambda \frac{n_\lambda}{n} \frac{\left\{ f_\lambda - \sum_{\substack{f_\delta / f_\lambda \\ f_\delta < f_\lambda}} \varphi(f_\delta) \right\}}{\varphi(f_\lambda)} \lg \frac{1}{s-1} + p(s-1), \tag{19}$$

откуда мы, в силу известной формулы

$$\sum_{f_\delta / f_\lambda} \varphi(f_\delta) = f_\lambda,$$

получаем

$$\sum_{p_\lambda} p_\lambda^{-s} = k_\lambda \frac{n_\lambda}{n} \lg \frac{1}{s-1} + P(s-1), \tag{20}$$

и мы приходим к искомому результату.

Этот результат принадлежит Фробениусу. Однако ему не удалось доказать, что плотность совокупности простых чисел, принадлежащих к каждому из классов отдела, равна $\frac{n_\lambda}{n}$. Решение этой задачи и является целью настоящего сочинения.

§ 2. Области деления круга

Существует целая категория областей, для которых упомянутая задача решается при помощи известных ранее методов. Это области деления круга. Не ставя вопроса во всей общности, я рассмотрю случай, который играет важную роль для дальнейшего.

Пусть l будет простое число типа $ef+1$, где f — заданное число. не подчиненное никаким дальнейшим ограничениям. Рассмотрим урав, нение

$$x^l - 1 = 0. \tag{21}$$

Далее, пусть ρ будет один из его первообразных корней. Каждый из e-членных гауссовых периодов

$$\begin{aligned}
\eta_0 &= \rho + \rho_f + \rho_{2f} + \ldots + \rho_{(e-1)f}, \\
\eta_1 &= \rho_1 + \rho_{f+1} + \rho_{2f+1} + \ldots + \rho_{(e-1)f+1}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\eta_{f-1} &= \rho_{f-1} + \rho_{2f-1} + \rho_{3f-1} + \ldots + \rho_{ef-1},
\end{aligned} \tag{22}$$

где под ρ_k мы будем разуметь ρ^{g^k}, а g — какой-нибудь первообразный корень сравнения $x^{ef} \equiv 1 \pmod l$, удовлетворяет неприводимому уравнению f-ой степени

$$\varphi_e(y) = 0. \tag{23}$$

Возьмем теперь какое-нибудь простое число p. Возникает вопрос, с какой из сопряженных величин η сравнима степень η_ν^p по модулю p. Пусть $p \equiv g^\alpha \pmod l$. Тогда имеет место следующее сравнение:

$$\begin{aligned}
\eta_\nu^p &= (\rho_\nu + \rho_{f+\nu} + \ldots + \rho_{(e-1)f+\nu})^p \equiv \\
&\equiv \rho_\nu^p + \rho_{f+\nu}^p + \ldots + \rho_{(e-1)f+\nu}^p \equiv \rho_\nu^{g^\alpha} + \rho_{f+\nu}^{g^\alpha} + \ldots + \rho_{(e-1)f+\nu}^{g^\alpha} \equiv \\
&\equiv \rho_{\nu+\alpha} + \rho_{f+\nu+\alpha} + \ldots + \rho_{(e-1)f+\nu+\alpha} \equiv \eta_{\nu+\alpha} \pmod p,
\end{aligned} \tag{24}$$

где значок $\nu+\alpha$ необходимо привести к его наименьшему вычету по модулю f. Следовательно, корни сравнения

$$\varphi_e(y) \equiv 0 \pmod p \tag{25}$$

претерпевают при возвышении их в p-ую степень подстановку $(\nu, \nu+\alpha)$ тогда и только тогда, когда p является членом одной из прогрессий

$$lx + g^\alpha,\ lx + g^{\alpha+f}, \ldots, lx + g^{\alpha+(e-1)f}.$$

Подстановку $(\nu, \nu+\alpha)$ можно рассматривать как α-ую степень подстановки $S = (\nu, \nu+1) = (0, 1, 2, \ldots, f-1)$. Введем следующее

Определение 8. Совокупность прогрессий

$$lx + g^\alpha,\ lx + g^{\alpha+f}, \ldots, lx + g^{\alpha+(e-1)f} \tag{26}$$

назовем *комплексом* индекса α. Про все числа, представляемые одною из прогрессий (26), будем говорить, что они *лежат* в комплексе индекса α.

Тогда результат настоящей главы мы можем выразить в виде следующего предложения:

Главная теорема. *Дано неприводимое уравнение* (23), *которому удовлетворяет система гауссовых периодов* (22). *Тогда возможно таким образом приурочить первообразной подстановке U из его группы Галуа первообразный корень сравнения* $x^{ef} \equiv 1 \pmod l$,

чтобы каждое простое число, принадлежащее к подстановке U^{α}, лежало в комплексе индекса α.

Следует подчеркнуть, что теорема Дирихле (loc. cit.) позволяет нам, таким образом, определить плотность совокупности простых чисел, принадлежащих к каждой заданной подстановке.

§ 3. О распределении норм и простых чисел по различным комплексам

В настоящей главе я намерен доказать теорему, являющуюся в известном смысле обобщением теоремы Дирихле.

Рассмотрим неприводимое уравнение

$$f(x) = 0, \tag{27}$$

которое мы здесь не будем предполагать непременно нормальным. Введем еще в рассмотрение произвольное нечетное число $L = l_1^{\lambda_1} l_2^{\lambda_2} \cdots l_k^{\lambda_k}$ и систему таких чисел $f_1, f_2, \ldots, f_k$, что каждое f_i является делителем

$$\varphi(l_i^{\lambda_i}) \qquad (i = 1, 2, 3, \ldots, k).$$

Обозначив первообразный корень сравнения

$$x^{\varphi(l_i^{\lambda_i})} \equiv 1 \pmod{l_i^{\lambda_i}} \qquad (i = 1, 2, 3, \ldots, k) \tag{28}$$

через g_i, мы можем представить все взаимно простые с l_i классы по модулю $l_i^{\lambda_i}$ в виде системы

$$1, g_i, g_i^2, \ldots, g_i^{\varphi(l_i^{\lambda_i})-1} \qquad (i = 1, 2, 3, \ldots, k).$$

Распределим эти классы по комплексам (*частичным*), называя каждую систему классов

$$g_i^{\alpha_i}, g_i^{\alpha_i+f_i}, \ldots, g_i^{\alpha_i+f_i\left(\frac{\varphi(l_i^{\lambda_i})}{f_i}-1\right)} \qquad (i = 1, 2, 3, \ldots, k)$$

частичным комплексом индекса α_i. Индекс α_i будем считать приведенным по модулю f_i.

Классы сравнений по модулю L могут быть распределены следующим образом по *полным комплексам*:

Определение 9. Дан взаимно простой с L класс A сравнений по модулю L. Если $A \equiv a_i \pmod{l_i^{\lambda_i}}$, а a_i лежит в комплексе индекса α_i $(i = 1, 2, \ldots, k)$, то будем говорить, что A лежит в *полном комплексе* индекса $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Если мы будем умножать числа из комплекса индекса $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ на числа из комплекса индекса $(\beta_1, \beta_2, \ldots, \beta_k)$, то будем получать числа, лежащие в комплексе индекса $(\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_k + \beta_k)$. Стало быть комплексы образуют абелеву группу порядка $f_1 \cdot f_2 \cdots f_k$. В ней роль единицы играет *нулевой комплекс* $(0, 0, \ldots, 0)$.

Вернемся опять к области $\Omega(x)$, образованной при помощи одного из корней уравнения (27). Пусть

$$\omega_1, \omega_2, \ldots, \omega_n$$

будут элементы его фундаментального базиса. Тогда каждое целое число из $\Omega(x)$ может быть представлено так:

$$\mu = c_1\omega_1 + c_2\ \omega_2 + \ldots + c_n\omega_n, \tag{29}$$

где $c_1, c_2, \ldots, c_n$ суть целые рациональные числа, которые называют *координатами* числа μ.

Если возможно подобрать координаты $c_1, c_2, \ldots, c_n$ для числа μ таким образом, чтобы норма $N(\mu)$ лежала в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, то назовем этот комплекс *допустимым* (*в узком смысле*), говоря в то же время про число μ, что оно *лежит* в комплексе индекса $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Для допустимых комплексов можно доказать следующую теорему:

Теорема 6. *Все допустимые комплексы образуют группу, которая является делителем группы всех комплексов.*

Доказательство. Если $N(\mu) \equiv a$ и $N(\nu) \equiv b \pmod{L}$, то имеет место также сравнение $N(\mu\nu) \equiv ab \pmod{L}$. Если теперь a лежит в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, а b—в комплексе $(\beta_1, \beta_2, \ldots, \beta_k)$, то ab лежит в комплексе $(\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_k + \beta_k)$. Далее, нулевой комплекс допустим, так как сравнение

$$N(\mu) \equiv 1 \pmod{L}$$

имеет очевидное решение $\mu = 1$.

Возьмем теперь определенный допустимый комплекс и рассмотрим совокупность всех чисел μ, лежащих в этом комплексе. Назовем эту совокупность совокупностью *решений комплекса*.

Чтобы ввести понятие *числа* решений комплекса, необходимо предварительно условиться в некоторых определениях:

Определение 10. Два целых числа μ и μ' из $\Omega(x)$ будем называть *равными по модулю* L тогда и только тогда, когда их координаты c_i и c_i' удовлетворяют сравнениям

$$c_i \equiv c_i' \pmod{L} \qquad (i = 1, 2, \ldots, n).$$

Из определения фундаментального базиса следует, что эти сравнения необходимы и достаточны для сравнения $\mu \equiv \mu' \pmod{L}$. Это утверждение справедливо и тогда, если мы, вместо фундаментального базиса, положим в основу базис какого-нибудь идеала, взаимно простого с L.

Определение 11. Если для координат c_i числа μ удовлетворяются неравенства

$$0 \leqslant c_i < L \qquad (i = 1, 2, \ldots, n), \tag{30}$$

то число μ мы будем называть *приведенным* по модулю L. Для каждого целого числа μ из $\Omega(x)$ можно подобрать равное ему по модулю L приведенное число μ', и притом только одно.

Очевидно, что каждый допустимый комплекс имеет лишь конечное число приведенных решений. Чтобы определить их число для каждого допустимого комплекса, докажем следующую теорему:

Теорема 7. *Каждый допустимый комплекс имеет одно и то же число приведенных решений.*

Доказательство. Пусть нам задан допустимый комплекс $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ и пусть μ будет одно из его решений. Если числа

$$\eta_1, \eta_2, \ldots, \eta_v \tag{31}$$

обозначают полную систему решений нулевого комплекса, то числа

$$\mu\eta_1, \ \mu\eta_2, \ldots, \mu\eta_v \tag{32}$$

после их приведения по модулю L представят полную систему решений комплекса $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. В самом деле: 1) все числа (32) лежат в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$; 2) все они различны по модулю L; 3) каждое число, лежащее в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, должно быть сравнимо по модулю L с одним из чисел (32).

1) Следует из правила умножения комплексов.

2) Если бы имело место, например, $\mu\eta_i \equiv \mu\eta_j \pmod{L}$, то умножая сравнение на целое алгебраическое число $\frac{N(\mu)}{(\mu)}$ и затем деля на взаимно простое с L целое рациональное число $N(\mu)$, мы получим $\eta_i \equiv \eta_j \pmod{L}$, что стоит в противоречии с определением системы (31).

3) Пусть μ' будет число, лежащее в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Тогда число $\mu' \frac{N(\mu)}{\mu}[N(\mu)]^{\varphi L - 1}$ лежит в нулевом комплексе, так как его норма равна

$$N(\mu')[N(\mu)]^{n-1}[N(\mu)]^{n\varphi L - n} \equiv N(\mu')[N(\mu)]^{-1} \pmod{L}.$$

Поэтому это число должно быть сравнимо с одним из чисел системы (31). Пусть

$$\mu' \frac{N(\mu)}{\mu}[N(\mu)]^{\varphi L - 1} \equiv \eta_i \pmod{L}.$$

Умножая это сравнение на μ, мы придем к сравнению

$$\mu' \equiv \mu\eta_i \pmod{L},$$

что оправдывает утверждение 3). Таким образом, число решений каждого допустимого комплекса равно v, т. е. оно одинаково для всех комплексов, и т. д.

Это число легко определить. В самом деле, обозначим через F число всех допустимых комплексов. Все приведенные решения всех

допустимых комплексов равномерно распределяются по отдельным допустимым комплексам. Но число всех приведенных решений всех допустимых комплексов равно числу взаимно простых с L классов по модулю L внутри $\Omega(x)$, т. е. равно

$$\bar{\varphi}(L) = N(L)\left(1-\frac{1}{N(l_1)}\right)\left(1-\frac{1}{N(l_2)}\right)\cdots\left(1-\frac{1}{N(l_p)}\right), \tag{33}$$

где $l_1, l_2, \ldots, l_p$ представляют собой совокупность всех простых идеальных делителей числа L внутри $\Omega(x)$. Таким образом, число решений каждого допустимого комплекса равно

$$v = \frac{\bar{\varphi}(L)}{F}. \tag{34}$$

То же число решений мы получим, если, вместо фундаментального базиса, положим в основу базис какого-нибудь идеала, взаимно простого с L.

Вспомним теперь, что все целые и делящиеся на идеал $\mathfrak{m}$, взаимно простой с L, числа из $\Omega(x)$ могут быть представлены в форме

$$c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n, \tag{35}$$

где $(\omega_1, \omega_2, \ldots, \omega_n)$ — базис идеала $\mathfrak{m}$, а $c_1, c_2, \ldots, c_n$ пробегают все целые рациональные значения. С другой стороны, все целые и делящиеся на $\mathfrak{m}$ числа из $\Omega(x)$, которые, кроме того, лежат в допустимом комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, могут быть представлены в форме одного из следующих выражений:

$$\omega_i^{(\alpha_1, \ldots, \alpha_k)} + L(c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n), \quad (i = 1,2,\ldots,v) \tag{36}$$

где $\omega_i^{(\alpha_1, \ldots, \alpha_k)}$ $(i = 1,2,\ldots,v)$ обозначает систему приведенных решений комплекса $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, в то время как остальные обозначения имеют то же значение, что и для (35).

Рассмотрим теперь бесконечный ряд

$$\sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s},$$

где сумма распространяется на все делящиеся на $\mathfrak{m}$ и взаимно простые с L главные идеалы. Этот ряд вблизи $s = 1$ может быть представлен так:

$$\sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s} = \frac{\bar{\varphi}(L)}{L^n} \frac{g}{N(\mathfrak{m})} \frac{1}{s-1} + P(s-1), \tag{37}$$

где g имеет следующее независимое от s значение

$$g = \frac{2^{\nu}\pi^n - {}^{\nu}R}{w\sqrt{\pm\Delta}}. \tag{38}$$

В этом выражении ν обозначает сумму числа вещественных корней *и числа пар сопряженных комплексных* корней уравнения (27), R —

регулятор области $\Omega(x)$, w — число корней из единицы внутри $\Omega(x)$, Δ — дискриминант области $\Omega(x)$; $P(s-1)$, как обычно, обозначает функцию, остающуюся вблизи $s=1$ конечной.

Проследим путь получения этой формулы, сообразуясь с обозначениями, принятыми у Вебера [13]. В ней коэффициент при $\frac{1}{s-1}$ равен $\frac{1}{w}$-ой предела выражения $\frac{T}{t}$, при $t=\infty$, где T означает число систем целых значений $c_1, c_2, \ldots, c_n$, подчиненных неравенствам

$$| N(c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n) | \leqslant t, \tag{39}$$

$$\left.\begin{aligned} 0 \leqslant \xi_1(c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n) < 1, \\ 0 \leqslant \xi_2(c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n) < 1, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 \leqslant \xi_{\nu-1}(c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n) < 1, \end{aligned}\right\} \tag{40}$$

где функции $\xi(\mu)$ суть так называемые показатели числа

$$\mu = c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n$$

и определяются при помощи системы следующих ν уравнений:

$$\left.\begin{aligned} \xi_1 l_{11} + \xi_2 l_{21} + \cdots + \xi_{\nu-1} l_{\nu-1,1} + \frac{\delta_1}{n} \lg | N(\mu) | = \lambda_1(\mu), \\ \xi_1 l_{12} + \xi_2 l_{22} + \cdots + \xi_{\nu-1} l_{\nu-1,2} + \frac{\delta_2}{n} \lg | N(\mu) | = \lambda_2(\mu), \\ \cdots\cdots\cdots\cdots, \quad \cdots\cdots\cdots \\ \xi_1 l_{1,\nu} + \xi_2 l_{2,\nu} + \cdots + \xi_{\nu-1} l_{\nu-1,\nu} + \frac{\delta_\nu}{n} \lg | N(\mu) | = \lambda_\nu(\mu), \end{aligned}\right\} \tag{41}$$

из которых только $\nu-1$ независимы. В них δ_i обозначает единицу, если $\Omega(x_i)$, т. е. i-ая сопряженная с $\Omega(x)$ область, вещественна, и 2, если она комплексна. Символы $\lambda_i(\mu)$ выражают величины $\delta_i \lg | \mu_i |$, где μ_i — i-ая сопряженная с μ величина. Наконец, $l_{1i}, l_{2i}, \ldots, l_{\nu-1,i}$ — система логарифмов от основных единиц области $\Omega(x_i)$.

Из формул (41) легко заключить, что функции $\xi(\mu)$ — однородны и нулевого измерения относительно $c_1, c_2, \ldots, c_n$, функция же $N(\mu)$ — однородна и n-го измерения. Поэтому, если в неравенствах (39) и (40) мы сделаем подстановку

$$c_1 = \frac{z_1}{\tau}, c_2 = \frac{z_2}{\tau}, \ldots, c_n = \frac{z_n}{\tau}, t = \tau^{-n}, \tag{42}$$

то они примут вид

$$| N(z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n) | \leqslant 1, \tag{43}$$

$$\left.\begin{aligned} 0 \leqslant \xi_1(z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n) < 1, \\ 0 \leqslant \xi_2(z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n) < 1, \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 \leqslant \xi_{\nu-1}(z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n) < 1 \end{aligned}\right\} \tag{44}$$

и нахождение $\lim_{t=\infty} \frac{T}{t}$ приведется к нахождению интеграла

$$\int\int \dots \int dz_1 \cdot dz_2 \cdots dz_n,$$

распространенного на n-мерное пространство, ограниченное неравенствами (43) и (44), который, как известно, равен

$$\frac{2^{\nu}\pi^n - {}^{\nu}R}{N(\mathfrak{m})\sqrt{\pm\Delta}}.$$

Обратимся теперь к ряду

$$\sum_{\mathfrak{a}}^{(\alpha_1, \dots, \alpha_k)} \frac{1}{N(\mathfrak{a})^s}, \tag{45}$$

в котором сумма распространена на все главные идеалы, делящиеся на $\mathfrak{m}$ и, кроме того, лежащие в допустимом комплексе $(\alpha_1, \alpha_2, \dots, \alpha_k)$. Числа, соответствующие этим главным идеалам, и только эти числа, могут быть представлены при помощи v формул (36). Разобьем сумму (45) на v частичных сумм, относя каждый идеал $\mathfrak{a}$ к той из формул (36), при помощи которой выражается соответствующее ему приведенное число (приведенное в смысле — см. [13], § 193, стр. 708). Конечно, будем все время иметь в виду, что ассоциированные числа лежат в одном и том же комплексе. Поэтому коэффициент при $\frac{1}{s-1}$ в выражении каждой (i-ой) частичной суммы равен

$$\frac{1}{w} \lim_{t=\infty} \frac{T_i}{t}, \tag{46}$$

где T_i — число систем $c_1, c_2, \dots, c_n$, удовлетворяющих неравенствам

$$| N(\omega_i^{(\alpha_1, \dots, \alpha_k)} + Lc_1\omega_1 + Lc_2\omega_2 + \cdots + Lc_n\omega_n) | \leqslant t, \tag{47}$$

$$\left.\begin{aligned} 0 \leqslant \xi_1(\omega_i^{(\alpha_1, \dots, \alpha_k)} + Lc_1\omega_1 + Lc_2\omega_2 + \cdots + Lc_n\omega_n) < 1, \\ 0 \leqslant \xi_2(\omega_i^{(\alpha_1, \dots, \alpha_k)} + Lc_1\omega_1 + Lc_2\omega_2 + \cdots + Lc_n\omega_n) < 1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ 0 \leqslant \xi_{\nu-1}(\omega_i^{(\alpha_1, \dots, \alpha_k)} + Lc_1\omega_1 + Lc_2\omega_2 + \cdots + Lc_n\omega_n) < 1. \end{aligned}\right\} \tag{48}$$

Вводя подстановку

$$c_1 = \frac{z_1}{\tau}, c_2 = \frac{z_2}{\tau}, \dots, c_n = \frac{z_n}{\tau}, t = L^n\tau^{-n}, \tag{49}$$

мы преобразуем неравенства (47) и (48) так:

$$\left| N\left(\frac{\omega_i^{(\alpha_1, \dots, \alpha_k)}}{L}\tau + z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n\right)\right| \leqslant 1, \tag{50}$$

$$\left.\begin{aligned}
0 \leqslant \xi_1 \left(\frac{\omega_i^{(\alpha_1, \ldots, \alpha_k)}}{L} \tau + z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n \right) < 1, \\
0 \leqslant \xi_2 \left(\frac{\omega_i^{(\alpha_1, \ldots, \alpha_k)}}{L} \tau + z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n \right) < 1, \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
0 \leqslant \xi_{\nu-1} \left(\frac{\omega_i^{(\alpha_1, \ldots, \alpha_k)}}{L} \tau + z_1\omega_1 + z_2\omega_2 + \cdots + z_n\omega_n \right) < 1.
\end{aligned}\right\} \quad (51)$$

Как мы видим, неравенства (50) и (51) отличаются от неравенств (43) и (44) только членами

$$\frac{\omega_i^{(\alpha_1, \ldots, \alpha_k)}}{L} \tau,$$

которые при $t = \infty$, т. е. при $\tau = 0$, обращаются в нуль. Теорема 30 в цитированной статье Гильберта ([11], стр. 53) доказывает, что эти члены не влияют ни на величину интеграла

$$\int\int \cdots \int dz_1 dz_2 \cdots dz_n,$$

ни на оценку остаточного члена. С другой стороны, нетрудно убедиться [см. подстановку (49)], что величина (46) равна

$$\frac{1}{wL^n} \int\int \cdots \int dz_1 dz_2 \cdots dz_n,$$

где интеграл имеет прежнее значение. Поэтому каждая из частичных сумм имеет вблизи $s = 1$ выражение

$$\frac{1}{wL^n} \cdot \frac{2^\nu \pi^{n-\nu} R}{N(\mathfrak{m}) \sqrt{\pm \Delta}} \frac{1}{s-1} + P(s-1).$$

Чтобы получить выражение для всей суммы (45), мы должны сложить v подобных сумм. Вспоминая, что

$$v = \frac{\bar{\varphi}(L)}{F},$$

мы получим

$$\sum_{\mathfrak{a}}^{(\alpha_1, \ldots, \alpha_k)} \frac{1}{N(\mathfrak{a})^s} = \frac{\bar{\varphi}(L)}{F} \frac{2^\nu \pi^{n-\nu} R}{L^n w N(\mathfrak{m}) \sqrt{\pm \Delta}} \frac{1}{s-1} + P(s-1). \quad (52)$$

Как мы видим, коэффициент при $\frac{1}{s-1}$ в каждой из этих сумм в F раз меньше, чем в сумме (37).

Выберем теперь в каждом из идеальных классов области $\Omega(x)$ по одному идеалу $\mathfrak{m}$, взаимно простому с L. Если $\mathfrak{m}$ для какого-нибудь класса лежит в допустимом комплексе, то все взаимно простые с L идеалы этого класса должны лежать в допустимых комплексах; если же существуют классы, идеалы которых лежат в недопустимых комплексах, то обозначим через $\bar{K}$ группу тех классов, идеалы которых

будут лежать в допустимых комплексах; группу же всех классов будем обозначать через K. Пусть порядки этих групп будут соответственно $\bar{h}$ и h.

Введем теперь новое определение.

Определение 12. Комплекс, в котором лежит какой-нибудь идеал области $\Omega(x)$, будем называть *допустимым в широком смысле.*

Рассуждения, подобные примененным нами при доказательстве теоремы 6, убеждают нас в том, что все допустимые в широком смысле комплексы образуют абелеву группу, для которой группа допустимых в узком смысле комплексов является делителем. Обозначим первую группу через $\bar{A}$, вторую—через A. Тогда имеет место

Теорема 8. *Гёльдеровские дополнительные группы* $\left(\frac{K}{\bar{K}}\right)$ и $\left(\frac{\bar{A}}{A}\right)$ *однозначно* (holoëdrisch) *изоморфны.*

Доказательство. Разложим группу K на сопряженные системы по подгруппе $\bar{K}$.

$$K = \bar{K} + k_2\bar{K} + k_3\bar{K} + \ldots + k_\eta\bar{K}. \tag{53}$$

Так как классы $k_2, k_3, \ldots, k_\eta$ не входят в $\bar{K}$, то идеалы каждого из них лежат в комплексах, не входящих в A. Пусть $a_2, a_3, \ldots, a_\eta$ будут комплексы, в которых лежат какие-нибудь идеалы соответственно из $k_2, k_3, \ldots, k_\eta$. Рассмотрим систему

$$A, a_2A, a_3A, \ldots, a_\eta A. \tag{54}$$

Каждая из систем a_iA исчерпывает все комплексы, в которых лежат какие бы то ни было взаимно простые с L идеалы из k_i. Действительно, пусть идеал $\mathfrak{m}_i$ из k_i лежит в a_i. В каком комплексе лежит какой-нибудь другой идеал $\mathfrak{n}_i$ из k_i? В силу известной теоремы (см., например, [13], стр. 593, Satz 3) можно найти такой взаимно простой с L идеал $\mathfrak{r}$, чтобы идеал $\mathfrak{m}_i\mathfrak{r}$ был главным. Тогда и идеал $\mathfrak{n}_i\mathfrak{r}$ будет главным. Пусть $\mathfrak{m}_i\mathfrak{r} \sim \mu$ лежит в комплексе b, а $\mathfrak{n}_i\mathfrak{r} \sim \nu$ — в комплексе c. Оба комплекса, согласно определению A, должны входить в A. Но $\mathfrak{n}_i \sim \mathfrak{m}_i\frac{\nu}{\mu}$, а потому $\mathfrak{n}_i$ лежит в комплексе a_icb^{-1}, который входит в систему a_iA.

Каждая из систем a_iA исчерпывает все комплексы, в которых лежат какие бы то ни было взаимно простые с L идеалы из $k_i\bar{K}$. Действительно, пусть идеал $\mathfrak{n}_i$ лежит в классе $k_i\bar{k}$, где $\bar{k}$ — какой-нибудь класс из $\bar{K}$. Выберем в классе $\bar{k}^{-1}$ идеал $\mathfrak{r}$, лежащий в комплексе b, входящем в A. Идеалы $\mathfrak{m}_i$ и $\mathfrak{n}_i\mathfrak{r}$ лежат в классе k_i, т. е. эквивалентны. Предыдущее рассуждение позволяет нам заключить, что идеал $\mathfrak{n}_i\mathfrak{r}$ лежит в комплексе c, входящем в систему a_iA. Значит, идеал $\mathfrak{n}_i$ лежит в комплексе cb^{-1}, который тоже входит в систему a_iA.

С другой стороны, ни одна из систем (54) не можем иметь с какой-

нибудь другой общих элементов. В самом деле, если бы, например, a_iA и a_jA имели общие элементы, то комплекс $a_ia_j^{-1}$, а с ним и система $a_iA\ (a_jA)^{-1}$ входили бы в A, а потому все идеалы из классов системы $k_i\overline{K}(k_j\overline{K})^{-1}$ должны были бы лежать в комплексах из A, т. е. входить в классы группы $\overline{K}$, что противоречит разложению (53).

Таким образом, мы доказали что: 1) системы (54) образуют группу $\overline{A}$, 2) системы (53) и (54) однозначно изоморфны. Это доказывает, что группы

$$\frac{K}{\overline{K}} \text{ и } \frac{A}{\overline{A}}$$

однозначно изоморфны.

Следствие. Порядок группы $\overline{A}$ равен $\overline{F} = F\mathfrak{y}$. Возьмем теперь какой-нибудь допустимый в широком смысле комплекс $(-\alpha_1, -\alpha_2, \ldots, -\alpha_k)$. Идеалы, лежащие в нем, входят в $\overline{h}$ идеальных классов, образующих одну из систем (53). Выберем в каждом из этих классов по одному взаимно простому с L идеалу m_i $(i = 1,2\ldots, \overline{h})$, и пусть каждый идеал m_i лежит в комплексе $(\beta_{1i}, \beta_{2i}, \ldots, \beta_{ki})$. Тогда комплексы $(-\alpha_1 - \beta_{1i}, -\alpha_2 - \beta_{2i}, \ldots, -\alpha_k - \beta_{ki})\ (i = 1, 2, \ldots, \overline{h})$, а с ними и комплексы $(\alpha_1 + \beta_{1i}, \alpha_2 + \beta_{2i}, \ldots, \alpha_k + \beta_{ki})$ будут лежать в A. Поэтому мы можем применить к ним формулу (52), выбирая в роли базиса $(\omega_1, \omega_2, \ldots, \omega_n)$ базис идеала m_i. Таким образом, мы получим

$$\sum_{m_i\mathfrak{a}}^{(\alpha_1+\beta_{1i},\ \ldots,\ \alpha_k+\beta_{ki})} \frac{1}{N(m_i)^s \cdot N(\mathfrak{a})^s} = \tag{55}$$

$$= \frac{1}{F}\frac{\overline{\varphi}(L)}{L^n}\frac{2^{\nu}\pi^{n-\nu}R}{w\sqrt{\pm\Delta}}\frac{1}{s-1} + P(s-1) \qquad (i = 1, 2, \ldots, \overline{h}),$$

где $\mathfrak{a}$ пробегает все идеалы, входящие в противоположный с m_i класс и лежащие в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Умножим формулу (55) на

$$N(m_i)^s = N(m_i) + (s-1)P(s-1)$$

и просуммируем по i. Получим

$$\sum_{\mathfrak{a}}^{(\alpha_1, \alpha_2, \ldots, \alpha_k)} \frac{1}{N(\mathfrak{a})^s} = \frac{\overline{h}}{F}\frac{\overline{\varphi}(L)}{L^n}\frac{2^{\nu}\pi^{n-\nu}R}{w\sqrt{\pm\Delta}}\frac{1}{s-1} + P(s-1), \tag{56}$$

где теперь $\mathfrak{a}$ пробегает идеалы всех классов, противоположных с классами всех m_i. Но это будут вообще все классы, в которые только могут входить идеалы, лежащие в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Преобразуем формулу (56), положив в ней

$$\frac{\overline{h}}{F} = \frac{\overline{h}\mathfrak{y}}{F\mathfrak{y}} = \frac{h}{\overline{F}}.$$

Сравнивая полученную формулу с известной формулой

$$\sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s} = h\frac{\bar{\varphi}(L)}{L^n}\frac{2^{\nu}\pi^{n-\nu}R}{w\sqrt{\pm\Delta}}\frac{1}{s-1} + P(s-1), \tag{57}$$

где $\mathfrak{a}$ пробегает все взаимно простые с L идеалы, мы получим

$$\sum_{\mathfrak{a}}{}^{(\alpha_1,\ldots,\alpha_k)} \frac{1}{N(\mathfrak{a})^s} = \frac{1}{\bar{F}}\sum_{\mathfrak{a}}{}' \frac{1}{N(\mathfrak{a})^s} + P(s-1). \tag{58}$$

Эта формула справедлива для всех допустимых в широком смысле комплексов $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Для группы $\bar{A}$ возможно найти $\bar{F}$ различных систем *характеров*. Выберем одну из таких систем и введем для каждого характера этой системы обозначение $\chi(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Между характерами будет иметь место соотношение

$$\chi(\alpha_1+\beta_1, \ldots, \alpha_k+\beta_k) = \chi(\alpha_1, \ldots, \alpha_k)\,\chi(\beta_1, \ldots, \beta_k). \tag{59}$$

Далее, каждому взаимно простому с L идеалу $\mathfrak{a}$ можно тоже приурочить характер, беря характер комплекса, в котором лежит идеал $\mathfrak{a}$. Для этих характеров введем обозначение $\chi(\mathfrak{a})$. Для них будет иметь место формула

$$\chi(\mathfrak{a})\,\chi(\mathfrak{b}) = \chi(\mathfrak{a}\mathfrak{b}), \tag{60}$$

а потому также

$$\frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}\frac{\chi(\mathfrak{b})}{N(\mathfrak{b})^s} = \frac{\chi(\mathfrak{a}\mathfrak{b})}{N(\mathfrak{a}\mathfrak{b})^s}. \tag{61}$$

Умножим теперь каждую из формул (58) на $\chi(\alpha_1, \alpha_2, \ldots, \alpha_k)$ и сложим их. Если мы выбрали систему *главных* характеров, то придем опять к формуле (57). Если же выбранная система характеров не главная, то, в силу известной формулы

$$\sum_{(\alpha_1, \alpha_2, \ldots, \alpha_k)} \chi(\alpha_1, \alpha_2, \ldots, \alpha_k) = 0, \tag{62}$$

мы придем к формуле

$$\sum_{\mathfrak{a}} \frac{\chi(\alpha_1, \alpha_2, \ldots, \gamma_k)}{N(\mathfrak{a})^s} = P(s-1),$$

или пользуясь вторым обозначением характеров:

$$\sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s} = P(s-1). \tag{63}$$

Эту формулу можно, в силу соотношения (60), преобразовать так:

$$\prod_{\mathfrak{p}} \frac{1}{1-\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}} = P(s-1), \tag{64}$$

где произведение распространяется на все простые идеалы $\mathfrak{p}$ области $\Omega(x)$, отличные от множителей L (ср., например, [13], стр. 725). Прологарифмируем формулу (64) и возьмем от логарифма вещественную часть (для обозначения вещественных частей от выражений введем символ $\Re[\ldots]$). При этом могут встретиться два случая: 1) левая часть (64) имеет при $s=1$ предел, отличный от нуля. Тогда вещественная часть ее логарифма будет тоже типа $P(s-1)$; 2) левая часть (64) стремится при $s=1$ к нулю. Тогда вещественная часть ее логарифма беспредельно растет по абсолютной величине, оставаясь все время отрицательной. Этот результат запишем следующим образом:

$$\Re\left[\sum_{\mathfrak{p}}\frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}+\frac{1}{2}\sum_{\mathfrak{p}}\frac{\chi(\mathfrak{p})^2}{N(\mathfrak{p})^{2s}}+\frac{1}{3}\sum_{\mathfrak{p}}\frac{\chi(\mathfrak{p})^3}{N(\mathfrak{p})^{3s}}+\cdots\right]\leqslant P(s-1).$$

Нетрудно показать [14], что сумма всех сумм, за исключением первой, при $s=1$ стремится к конечной величине. Кроме того, сумма тех членов в первой сумме, которые соответствуют идеалам порядков $\geqslant 2$, тоже остается при $s=1$ конечной, так как для таких идеалов $N(\mathfrak{p})\geqslant p^2$, а число идеалов, имеющих одну и ту же норму, не превышает числа n. Перенося все упомянутые члены внутрь символа $P(s-1)$, мы получим

$$\Re\left[\sum_{p}\frac{\nu_p\,\chi(p)}{p^s}\right]\leqslant P(s-1), \tag{65}$$

где ν_p означает число идеалов 1-го порядка с нормой p, а $\chi(p)$ мы пишем вместо $\chi(\mathfrak{p})$.

Теперь вернемся к обозначению $\chi(\alpha_1,\alpha_2,\ldots,\alpha_k)$ и соединим идеалы с одними и теми же характерами. Тогда формула (65) преобразуется так:

$$\Re\left[\sum_{(\alpha_1,\ldots,\alpha_k)}\chi(\alpha_1,\ldots,\alpha_k)\sum_{p_{(\alpha_1,\ldots,\alpha_k)}}\frac{\nu_p}{p^s_{(\alpha_1,\ldots,\alpha_k)}}\right]\leqslant P(s-1). \tag{66}$$

Подобным же образом может быть преобразована и формула (57)

$$\sum_{(\alpha_1,\ldots,\alpha_k)}\sum_{p_{(\alpha_1,\ldots,\alpha_k)}}\frac{\nu_p}{p^s_{(\alpha_1,\ldots,\alpha_k)}}=\lg\frac{1}{s-1}+P(s-1). \tag{67}$$

Складывая формулу (67) со всеми формулами (66), полученными для $\overline{F}-1$ возможных систем не главных характеров, мы, в силу того, что сумма

$$\sum_{\chi}\chi(\alpha_1,\alpha_2,\ldots,\alpha_k),$$

распространенная на все характеры одного и того же комплекса, равна $\overline{F}$, если $(\alpha_1,\alpha_2,\ldots,\alpha_k)$ нулевой комплекс, и равна нулю для всех других комплексов, получим

$$\overline{F}\sum_{p_{(0,\ldots,0)}}\frac{\nu_p}{p^s_{(0,\ldots,0)}}\leqslant\lg\frac{1}{s-1}+P(s-1). \tag{68}$$

В формуле (68) можно, идя другим путем, констатировать *знак равенства.* Но так как доказательство для общего случая довольно громоздко, мы проделаем его только для тех случаев, которые представятся нам необходимыми для дальнейшего.

Этим мы будем заниматься в следующем параграфе. Здесь же отметим, что если в формуле (68) имеет место знак равенства, то он будет иметь место и во всех формулах (66). Действительно, если бы хоть в одной из них имел место знак $<$, то после сложения всех формул (66) и (67) формула (68) получилась бы тоже со знаком $<$.

В случае знака равенства легко получить

$$\sum_{p\,(\alpha_1,\ldots,\alpha_k)} \frac{\nu_p}{p^{s}_{(\alpha_1,\ldots,\alpha_k)}} = \frac{1}{F}\lg\frac{1}{s-1} + P(s-1), \tag{69}$$

где сумма распространяется на все простые числа, лежащие в допустимом в широком смысле комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ (см., например, [3], стр. 357), и мы приходим к следующей

Главной теореме. Если в формуле (68) имеет место *знак равенства,* то совокупность простых чисел первого порядка *равномерно* распределяется по всем допустимым в широком смысле комплексам.

§ 4. О плотностях совокупностей простых чисел, принадлежащих к отдельным классам подстановок

Даны неприводимое нормальное уравнение n-ой степени

$$f(x) = 0 \tag{70}$$

и подстановка f-го порядка

$$S = (x_{11}, x_{12}, \ldots, x_{1f})(x_{21}, x_{22}, \ldots, x_{2f})\ldots(x_{e1}, x_{e2}, \ldots, x_{ef})\ (ef = n), \tag{71}$$

входящая в его группу G. Выберем k простых чисел $l_1, l_2, \ldots, l_k$ вида $fx + 1$, взаимно простых с дискриминантом D уравнения (70) (k — произвольное число, которое мы в дальнейшем будем безгранично увеличивать), и образуем при помощи корней уравнений

$$x^{l_1} - 1 = 0,\ x^{l_2} - 1 = 0, \ldots, x^{l_k} - 1 = 0 \tag{72}$$

k циклических уравнений, каждое степени f (например, при помощи гауссовых периодов). Дискриминанты этих уравнений суть степени простых чисел $l_1, l_2, \ldots, l_k$, а потому области, образованные при помощи их корней, взаимно просты между собой и с $\Omega(x)$ (т. е. не имеют, кроме рациональных чисел, общих элементов). Выберем затем из каждого из наших уравнений по одному корню η_ν ($\nu = 1, 2, \ldots, k$) и по подстановке U_ν, *производящей* группу каждого из наших уравнений. Далее, рассмотрим область $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$. Ее группа однозначно (holoëdrisch) изоморфна с произведением $G\cdot(U_1)^{i_1}\cdot(U_2)^{i_2}\cdots(U_k)^{i_k}$.

Не вводя для подстановок области $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$ новых обозначений, мы будем для них пользоваться символами $S \cdot U_1^{\alpha_1} U_2^{\alpha_2} \cdots U_k^{\alpha_k}$, где подстановка S пробегает группу G, а каждое $\alpha_\nu (\nu = 1, 2, \ldots, k)$ принимает значения $0, 1, 2, \ldots, f-1$. Область $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$ тоже нормальна, и ее порядок равен $n \cdot f^k$.

Рассмотрим теперь совокупность простых чисел, принадлежащих к отделу подстановки S в $\Omega(x)$. Исследуем, как распределяются простые числа этой совокупности по комплексам, образованным областью $\Omega(\eta_1, \eta_2, \ldots, \eta_k)$. Число этих комплексов равно f^k, и каждый комплекс $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ соответствует подстановке $U_1^{\alpha_1} \cdot U_2^{\alpha_2} \cdots U_k^{\alpha_k}$ в том смысле, что простое число принадлежит к этой подстановке тогда и только тогда, когда оно лежит в комплексе $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ (см. § 2 настоящего сочинения, главная теорема).

В основу предстоящего исследования положим следующую классификацию комплексов:

Определение 13. 1) Те комплексы $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, в которых общий наибольший делитель чисел $\alpha_1, \alpha_2, \ldots, \alpha_k, f$ равен единице (другими словами, подстановка $U_1^{\alpha_1} \cdot U_2^{\alpha_2} \cdots U_k^{\alpha_k}$ f-го порядка), назовем *первообразными*.

2) Числа $\alpha_1, \alpha_2, \ldots, \alpha_k, f$ имеют общий наибольший делитель d (подстановка $U_1^{\alpha_1} \cdot U_2^{\alpha_2} \cdots U_k^{\alpha_k}$ порядка $\frac{f}{d}$), причем $1 < d < f$. В этом случае будем называть комплексы $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ *особенными*.

3) *Нулевой* комплекс $(0, 0, \ldots, 0)$.

Чтобы определить число различных первообразных комплексов, заметим, что: 1) число комплексов *порядка* d равно d^k, 2) каждый особенный комплекс $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ порядка f можно, деля его индексы на d, преобразовать в первообразный комплекс порядка $\delta = \frac{f}{d}$. В силу всего этого имеет место формула

$$\sum_{\delta \mid f} \psi(\delta) = f^k, \tag{73}$$

где мы через $\psi(f)$ обозначаем искомое число комплексов, а сумма в левой части распространяется на все делители δ числа f. Так как эта формула справедлива для всех значений f, то, пользуясь обычным дедекиндовским приемом обращения, мы получим для $\psi(f)$ следующее выражение:

$$\psi(f) = \sum_{d \mid f} \mu(d) \left(\frac{f}{d}\right)^k = f^k \left(1 - \frac{1}{q_1^k}\right)\left(1 - \frac{1}{q_2^k}\right) \cdots \left(1 - \frac{1}{q_a^k}\right), \tag{74}$$

где $q_1, q_2, \ldots, q_a$ обозначают систему всех простых делителей числа f.

Если мы возьмем k настолько большим, чтобы k-ая степень наименьшего из всех простых чисел $q_1, q_2, \ldots, q_a$ (назовем его Q) была больше,

чем каждый из биномиальных коэффициентов $C_a^1, C_a^2, \ldots, C_a^{a-1}$, то легко убедиться в справедливости следующего неравенства:

$$\psi(f) > f^k\left(1 - \frac{a}{Q^k}\right). \tag{75}$$

Это неравенство играет в дальнейшем весьма важную роль.

Убедимся в равномерности распределения совокупности простых чисел, принадлежащих к отделу подстановки S, по комплексам. Для этого изберем индуктивный путь. Именно, сначала убедимся в этом для совокупности простых чисел, принадлежащих к тождественной подстановке в $\Omega(x)$. Их общая плотность равна $\frac{1}{n}$. Введем следующее

Определение 14. Систему комплексов

$$(r\alpha_1, r\alpha_2, \ldots, r\alpha_k),$$

где $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ какой-нибудь первообразный комплекс, а r пробегает значения $0, 1, 2, \ldots, f-1$, назовем *лучом* $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Если же r пробегает только взаимно простые с f значения из ряда $0, 1, 2, \ldots, f-1$, то полученную систему комплексов будем называть *первообразной частью* луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Если число (или идеал) лежит в одном из комплексов луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, то будем говорить, что оно *лежит в луче* $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

Из этого определения вытекают следующие очевидные теоремы:

Теорема 9. *Первообразный комплекс не может входить более чем в один луч.*

Теорема 10. *Число всех первообразных частей лучей равно*

$$\frac{\psi(f)}{\varphi(f)} = f^{k-1}\prod_{i=1}^{a}\frac{\left(1 - \frac{1}{q_i^k}\right)}{\left(1 - \frac{1}{q_i}\right)}. \tag{76}$$

Теорема 11. *Чтобы простое число p одновременно принадлежало к тождественной подстановке в $\Omega(x)$ и лежало в первообразной части луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, необходимо и достаточно, чтобы оно в области $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$ принадлежало к отделу подстановки $1 \cdot U_1^{\alpha_1} \cdot U_2^{\alpha_2} \cdots U_k^{\alpha_k}$.*

Существование же подобных простых чисел непосредственно следует из результата Фробениуса. С другой стороны, мы можем рассматривать эти простые числа как нормы идеалов в $\Omega(x)$, а поэтому по крайней мере один из комплексов, лежащих в первообразной части луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, допустим в широком смысле. Стало быть, все эти комплексы допустимы, так как все комплексы луча можно рассматривать как степени какого-нибудь одного первообразного. Поэтому здесь роль $\overline{F}$ играет f^k.

Чтобы констатировать для нашего случая знак равенства в формуле (68), заметим, что плотность совокупности простых чисел, принадлежащих к тождественной подстановке в $\Omega(x)$ и лежащих во всех f^k комплексах, равна $\frac{1}{n}$. С другой стороны, совокупность простых чисел, принадлежащих к тождественной подстановке в $\Omega(x)$ и одновременно лежащих в нулевом комплексе, имеет плотность

$$\frac{1}{nf^k},$$

так как эти и только эти простые числа принадлежат к тождественной подстановке в $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$, а порядок группы этой области равен

$$nf^k.$$

Обе плотности относятся, как $f^k : 1$, т. е. $\overline{F} : 1$, что доказывает, что в формуле (68) должен быть знак равенства. Таким образом, условия достаточные для равномерности распределения наших простых чисел по комплексам, удовлетворены.

Докажем теперь равномерность распределения по комплексам простых чисел, принадлежащих к отделу подстановки (71) f-го порядка, предполагая, что равномерность доказана для тех ее степеней, порядок которых меньше f. Тогда будет достаточно доказать равномерность распределения простых чисел p, удовлетворяющих тому условию, что неприводимое уравнение

$$F(z) = 0, \tag{77}$$

корень которого принадлежит к циклической группе $(S)^i$, рассматриваемое как сравнение по модулю p, имеет рациональные корни. Чтобы провести это доказательство, нужно сперва убедиться в том, что все комплексы для уравнения (77) допустимы. Это следует уже из того, что они допустимы для меньшей совокупности простых чисел, принадлежащих в $\Omega(x)$ к тождественной подстановке. Далее, мы должны доказать, что в формуле (68) для нашего случая имеет место знак равенства. Для этого образуем неприводимое уравнение

$$\Phi(\zeta) = 0, \tag{78}$$

корень которого ζ принадлежит к группе $(S)^i$ в $\Omega(x, \eta_1, \ldots, \eta_k)$. Величину ζ можно рационально выразить через $z, \eta_1, \eta_2, \ldots, \eta_k$, и каждой сопряженной с z величине будет соответствовать f^k сопряженных с ζ величин, которые мы получим, если в выражении ζ через $z, \eta_1, \eta_2, \ldots, \eta_k$ будем над величинами $\eta_1, \eta_2, \ldots, \eta_k$ производить всевозможные подстановки типа соответственно $U_1^{\alpha_1}, U_2^{\alpha_2}, \ldots, U_k^{\alpha_k}$ ($\alpha_\nu = 0, 1, \ldots, f-1$). Если поэтому простое число p лежит в нулевом комплексе, то каждому рациональному корню сравнения

$$F(z) \equiv 0 \pmod{p} \tag{79}$$

должны соответствовать f^k различных корней сравнения

$$\Phi(\zeta) \equiv 0 \pmod{p}. \tag{80}$$

В этом случае величины $\eta_1, \eta_2, \ldots, \eta_k$ сравнимы с рациональными числами, а корни сравнения (80) все различны между собой, если только p не входит в дискриминант уравнения (78). С другой стороны, из групповых соображений следует, что z может быть рационально выражено через ζ, а поэтому каждому рациональному корню сравнения (80) соответствует рациональный корень сравнения (79). Если поэтому мы применим формулу (6) к уравнению (77) и к уравнению (78), то значения ν_p для простых чисел, лежащих в нулевом комплексе, во втором случае в f^k раз больше, чем в первом, а для других простых чисел все ν_p во втором случае равны нулю. Это доказывает, что в нашем случае в формуле (68) имеет место знак равенства. Таким образом, все условия для равномерности распределения рассматриваемых простых чисел выполнены, и мы заключаем отсюда, что плотность совокупности простых чисел, принадлежащих в $\Omega(x)$ к отделу подстановки S_λ f_λ-го порядка и одновременно лежащих в одном из комплексов, равна

$$\frac{1}{f_\lambda^{\,k}} k_\lambda \frac{n_\lambda}{n},$$

а плотность совокупности простых чисел, принадлежащих в $\Omega(x)$ к этому же отделу и лежащих во всех первообразных комплексах, равна

$$\frac{\psi(f_\lambda)}{f_\lambda^{\,k}} k_\lambda \frac{n_\lambda}{n}.$$

Теперь исследуем распределение простых чисел нашего отдела по различным его классам. Для этого образуем неприводимое уравнение

$$\Phi(\xi_\lambda) = 0, \tag{81}$$

корень которого ξ_λ принадлежит к циклической группе $(S_\lambda \cdot U_1^{\alpha_1} \cdot U_2^{\alpha_2} \cdots U_k^{\alpha_k})^i$ в $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$, где $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ — какой-нибудь первообразный комплекс. Тогда мы сможем доказать следующую теорему:

Теорема 12. *Из трех утверждений:*

1°. *Простое число p принадлежит в $\Omega(x)$ к классу подстановки S_λ.*

2°. *Простое число p лежит в одном из комплексов*

$$(r_\mu' \alpha_1, r_\mu' \alpha_2, \cdots, r_\mu' \alpha_k) \qquad \left(\mu = 1, 2, \ldots, t = \frac{\varphi(f_\lambda)}{k_\lambda}\right).$$

Здесь числа $r_1', r_2', \ldots, r_t'$ суть корни соответственно сравнений

$$r_\mu \cdot x \equiv 1 \pmod{f_\lambda} \qquad (\mu = 1, 2, \ldots, t), \tag{82}$$

а числа $r_1, r_2, \ldots, r_t$ *взяты таким образом, чтобы подстановки*

$$S_\lambda^{r_1}, S_\lambda^{r_2}, \ldots, S_\lambda^{r_t}$$

принадлежали к классу подстановки S_λ (*все* r_μ *взаимно просты с* f_λ, *так как порядок подстановки* $S_\lambda^{r_\mu}$ *должен быть равен* f_λ).

3°. *Сравнение*

$$\Phi(\xi_\lambda) \equiv 0 \pmod{p} \tag{83}$$

имеет рациональные корни, — каждое является следствием двух остальных.

А) 3° выводится из 1° и 2° следующим образом. Корни уравнения (81) рационально выражаются через $x, \eta_1, \eta_2, \ldots, \eta_k$. Пусть

$$\xi_\lambda = \varphi(x, \eta_1, \eta_2, \ldots, \eta_k).$$

Возвысим это выражение в p-ую степень и станем рассматривать результат по модулю $\mathfrak{p}$, где $\mathfrak{p}$ один из простых идеальных делителей p в $\Omega(x)$. Тогда мы увидим, что x в нем претерпевает подстановку S_λ, в то время как $\eta_1, \eta_2, \ldots, \eta_k$, в силу 2°, — соответственно подстановки

$$U_1^{r_\mu' \alpha_1}, U_2^{r_\mu' \alpha_2}, \ldots, U_k^{r_\mu' \alpha_k}$$

(последние можно рассматривать по модулю p, так как $\Omega(\eta_i)$ суть области деления круга). Рассмотрим теперь тот корень уравнения (81), который принадлежит к группе $(S_\lambda^{r_\mu} U_1^{\alpha_1} U_2^{\alpha_2} \ldots U_k^{\alpha_k})^i$. Из теоремы Шёнемана следует, что этот корень сравним с собственной p-ой степенью по модулю $\mathfrak{p}$ и, значит, подавно по модулю некоторого простого идеала в $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$, а поэтому, в силу обобщенной теоремы Ферма (см. [13], стр. 618), этот корень сравним по этому модулю с рациональным числом, которое должно быть корнем сравнения (83).

В) Предположим теперь, что удовлетворено условие 3°. Пусть p в $\Omega(x)$ принадлежит к классу какой-нибудь подстановки $\bar{S}$, а в $\Omega(\eta_1, \eta_2, \ldots, \eta_k)$ — к подстановке $U_1^{\beta_1} \cdot U_2^{\beta_2} \ldots U_k^{\beta_k}$ (другими словами, p лежит в комплексе $(\beta_1, \beta_2, \ldots, \beta_k)$). Тогда, как мы убедились, в $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$ оно принадлежит к классу подстановки $\bar{S} \cdot U_1^{\beta_1} \cdot U_2^{\beta_2} \ldots U_k^{\beta_k}$. Но Фробениус доказал ([1], стр. 701), что для существования рационального корня сравнения (83) необходимо и достаточно, чтобы хоть одна из подстановок

$$T\bar{S}T^{-1} \cdot U_1^{\beta_1} \cdot U_2^{\beta_2} \ldots U_k^{\beta_k}$$

входила в группу, к которой принадлежит ξ_λ, т. е. в

$$(S_\lambda \cdot U_1^{\alpha_1} \cdot U_2^{\alpha_2} \ldots U_k^{\alpha_k})^i.$$

Пусть, таким образом,

$$T\bar{S}T^{-1}\cdot U_1^{\beta_1}\cdot U_2^{\beta_2}\cdot\ \ldots\ \cdot U_k^{\beta_k}=S_\lambda^{R}\cdot U_1^{R\alpha_1}\cdot U_2^{R\alpha_2}\ \ldots\ \cdot U_k^{R\alpha_k},$$

где R — одно из чисел ряда $0, 1, 2, \ldots, f_\lambda - 1$. Но так как в S_λ и $\bar{S}$ входят только величины x, а в U_ν — только η_ν и все величины x, $\eta_1, \eta_2, \ldots, \eta_k$ рационально независимы, то должно иметь место

$$T\bar{S}T^{-1}=S_\lambda^{R},\ U_1^{\beta_1}=U_1^{R\alpha_1},\ U_2^{\beta_2}=U_2^{R\alpha_2},\ \ldots,\ U_k^{\beta_k}=U_k^{R\alpha_k}. \quad (84)$$

Из этого следует, что p лежит в луче $(\alpha_1, \alpha_2, \ldots, \alpha_k)$.

C) Если мы еще предположим, что выполнено условие 1°, т. е. что $\bar{S}=S_\lambda$, то тогда в группе G должна находиться такая подстановка T, что $TS_\lambda T^{-1}=S_\lambda^{R}$. Это показывает, что R является одним из чисел ряда $r_1, r_2, \ldots, r_t$. Но ряд $r_1, r_2, \ldots, r_t$ может отличаться от ряда $r_1', r_2', \ldots, r_t'$ только порядком своих членов. В самом деле, возводя соотношение

$$T_iS_\lambda T_i^{-1}=S_\lambda^{r_i}$$

в r_i'-ую степень, мы получим

$$T_iS_\lambda^{r_i'}T_i^{-1}=S_\lambda,$$

или

$$T_i^{-1}S_\lambda T_i=S_\lambda^{r_i'},$$

что показывает, что r_i' находится в ряду $r_1, r_2, \ldots, r_t$. Таким образом, утверждение 2° выполнено.

D) Из 3° и 2°, следует 1°. Действительно, утверждение 2° характеризует следующие сравнения:

$$\beta_i\equiv r_\mu\alpha_i \pmod{f_\lambda}\quad (i=1, 2, \ldots, k),$$

которые вместе с сравнениями

$$\beta_i\equiv R\alpha_i \pmod{f_\lambda}\quad (i=1, 2, \ldots, k)\quad \text{(см. B)}$$

дают:

$$(R-r_\mu)\alpha_i\equiv 0 \pmod{f_\lambda}\qquad (i=1, 2, \ldots, k).$$

Образуем при помощи этих сравнений следующее:

$$(R-r_\mu)(X_1\alpha_1+X_2\alpha_2+\ \ldots\ +X_k\alpha_k)\equiv 0 \pmod{f_\lambda}.$$

Подберем $X_1, X_2, \ldots, X_k$ так, чтобы $X_1\alpha_1+X_2\alpha_2+\ \ldots\ +X_k\alpha_k$ было взаимно просто с f_λ, что возможно в силу первообразности комплекса $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Тогда необходимо, чтобы имело место

$$R\equiv r_\mu \pmod{f_\lambda},$$

откуда $\bar{S}=T^{-1}S_\lambda^{r_\mu}T$, т. е. $\bar{S}$ принадлежит к классу подстановки S_λ. Итак, теорема доказана во всех своих частях.

Теперь докажем равномерность распределения по допустимым комплексам таких простых чисел p, что сравнение (83) имеет рациональные корни. Из предыдущего (см. B) доказательства теоремы (12) ясно, что для этого уравнения могут быть допустимы только f_λ комплексов луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. С другой стороны, они действительно допустимы, так как группа этих комплексов циклическая, а совокупность первообразных комплексов из луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ соответствует отделу $S_\lambda \cdot U_1^{\alpha_1} \cdot U_2^{\alpha_2} \cdot \ldots \cdot U_k^{\alpha_k}$ в $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$. Далее, в формуле (68) имеет место знак равенства. В самом деле, если p лежит в нулевом комплексе, то левая часть сравнения (83) распадается на линейные множители, а потому $\nu_p = n \cdot f_\lambda^{k-1}$ (ведь уравнение (81) nf_λ^{k-1}-ой степени). С другой стороны, эти и только эти простые числа принадлежат к тождественной подстановке в $\Omega(x, \eta_1, \eta_2, \ldots, \eta_k)$, а поэтому плотность их совокупности равна

$$\frac{1}{nf_\lambda^{k}}.$$

Таким образом, обе плотности стоят в отношении $f_\lambda : 1$. Но это число играет здесь роль $\overline{F}$. Таким образом, равномерность распределения наших простых чисел по комплексам может считаться доказанной.

Рассмотрим теперь те из наших простых чисел, которые лежат в первообразной части луча $(\alpha_1, \alpha_2, \ldots, \alpha_k)$. Если какое-нибудь из них принадлежит к классу S_λ в $\Omega(x)$, то в силу D) оно лежит в одном из комплексов

$$(r_\mu \alpha_i) \qquad \begin{pmatrix} \mu = 1, 2, \ldots, t = \dfrac{\varphi(f_\lambda)}{k_\lambda} \\ i = 1, 2, \ldots, k \end{pmatrix}$$

(для краткости мы, вместо $(\alpha_1, \alpha_2, \ldots, \alpha_k)$, вводим обозначение (α_i)). Нетрудно видеть, что ряд $r_1, r_2, \ldots, r_t$ образует группу относительно умножения. Действительно, пусть, например,

$$S_\lambda^{r_i} = T_i S_\lambda T_i^{-1}, \qquad S_\lambda^{r_j} = T_j S_\lambda T_j^{-1};$$

тогда

$$S_\lambda^{r_i r_j} = (S_\lambda^{r_i})^{r_j} = (T_i S_\lambda T_i^{-1})^{r_j} = T_i S_\lambda^{r_j} T_i^{-1} = T_i T_j S_\lambda T_j^{-1} T_i^{-1} = \\ = (T_i T_j) S_\lambda (T_i T_j)^{-1}.$$

Эта группа является делителем группы всех взаимно простых с f_λ классов по модулю f_λ. Обозначив обе группы соответственно через $\mathfrak{r}$ и $\mathfrak{R}$, мы сможем разбить $\mathfrak{R}$ на сопряженные системы по $\mathfrak{r}$

$$\mathfrak{R} = \mathfrak{r} + R_2\mathfrak{r} + R_3\mathfrak{r} + \ldots + R_{k_\lambda}\mathfrak{r}. \tag{85}$$

Таким образом, классы подстановок $S_\lambda, S_\lambda^{R_2}, \ldots, S_\lambda^{R_{k_\lambda}}$ исчерпывают весь отдел S_λ. Приурочим к этим классам значки соответственно

$1, 2, 3, \ldots, k_\lambda$. Вообще около каждого простого числа будем ставить два значка: первый будет обозначать класс, к которому оно принадлежит, второй — комплекс, в котором оно лежнт. Для простых чисел типов

$$p_{\nu,\,\alpha_i},\ p_{\nu,\,r_2\alpha_i},\ \ldots,\ p_{\nu,\,r_l\alpha_l}$$

введем общий символ $p_{\nu,\,r\alpha_i}$.

Каждое простое число, принадлежащее к отделу

$$S_\lambda \cdot U_1^{\alpha_1} \cdot U_2^{\alpha} \ldots U_k^{\alpha_k} \text{ в } \Omega(x, \eta_1, \eta_2, \ldots, \eta_k),$$

должно принадлежать к одному из следующих типов:

$$p_{1,\,r\alpha_i},\ p_{2,\,R_2 r\alpha_i},\ \ldots,\ p_{k_\lambda,\,R_{k_\lambda} r\alpha_i}.$$

Равномерность распределения этих простых чисел по комплексам может быть выражена следующей формулой:

$$\sum_p p_{1,r\alpha_i}^{-s} = \sum_p p_{2,\,R_2 r\alpha_i}^{-s} + P(s-1) = \ldots \sum_p p_{k_\lambda,\,R_{k_\lambda} r\alpha_i}^{-s} + P(s-1) = \\ = \frac{1}{k_\lambda} \sum_{\mu=1}^{k_\lambda} \sum_p p_{\mu,\,R_\mu r\alpha_i}^{-s} + P(s-1). \tag{86}$$

Возьмем в этой формуле в роли (α_i) каждый из комплексов (α_i), $(R_2\alpha_i)$, $\ldots$, $(R_{k_\lambda}\alpha_i)$ и сложим все полученные формулы. При этом заметим, что: 1) все сопряженные системы (85) после их умножения на R_μ могут только изменить порядок своего расположения, 2) при этом ни одна из систем не может остаться не измененной. Поэтому сумма, получаемая в правой части новой формулы, распространяется на все такие простые числа, которые принадлежат к отделу S_λ в $\Omega(x)$ и вместе с тем лежат в $k_\lambda t = \varphi(f_\lambda)$ комплексах $(R_\mu r\alpha_i)$, образующих первообразную часть луча (α_i). Но так как простые числа, принадлежащие к отделу S_λ в $\Omega(x)$, равномерно распределены по всем $f_\lambda^{\,k}$ комплексам, то общая плотность рассматриваемой совокупности простых чисел равна

$$\frac{\varphi(f_\lambda)}{f_\lambda^{\,k}} k_\lambda \frac{n_\lambda}{n},$$

и мы, таким образом, приходим к формуле

$$\sum_{\mu=1}^{k_\lambda} \sum_p p_{1,\,R_\mu\alpha_i}^{-s} = \frac{\varphi(f_\lambda)}{f_\lambda^{\,k}} \frac{n_\lambda}{n} \lg \frac{1}{s-1} + P(s-1), \tag{87}$$

где вся сумма в левой части распространяется на все простые числа, принадлежащие к классу S_λ в $\Omega(x)$ и одновременно лежащие в первообразной части луча (α_i).

Образуем теперь формулы, подобные (87), для всех $\frac{\psi(f_\lambda)}{\varphi(f_\lambda)}$ первообразных частей лучей (см. теорему 10) и сложим их. Этим мы еще можем не исчерпать всех простых чисел, принадлежащих к классу S_λ в $\Omega(x)$, так как еще могут существовать принадлежащие к классу S_λ в $\Omega(x)$ простые числа, лежащие вместе с тем в нулевом или в особенных комплексах. Таким образом, выражение в левой части получаемого уравнения

$$\leqslant \sum_p p_1^{-s} + P(s-1),$$

откуда вытекает неравенство

$$\sum_p p_1^{-s} \geqslant \frac{\psi(f_\lambda)}{f_\lambda^{\,k}} \frac{n_\lambda}{n} \lg \frac{1}{s-1} + P(s-1). \tag{88}$$

Возьмем k настолько большим, чтобы удовлетворялось неравенство (75). Тогда, вместо (88), мы можем написать

$$\sum p_1^{-s} > \left(1 - \frac{a}{Q^k}\right) \frac{n_\lambda}{n} \lg \frac{1}{s-1} + P(s-1). \tag{89}$$

Эта формула дает нам возможность получить искомый результат. Сперва докажем, что

$$\lim_{s=1} \inf \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} \geqslant \frac{n_\lambda}{n}. \tag{90}$$

В самом деле, если бы имело место

$$\lim_{s=1} \inf \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} = \frac{n_\lambda}{n} - \alpha,$$

где $\alpha > 0$, то, взяв

$$k > \frac{\lg n_\lambda - \lg n + \lg a - \lg \alpha}{\lg Q},$$

мы имели бы

$$\frac{n_\lambda}{n} - \alpha < \frac{n_\lambda}{n}\left(1 - \frac{a}{Q^k}\right). \tag{91}$$

С другой стороны, делая неравенство (88) на $\lg \frac{1}{s-1}$ и беря от обеих частей $\lim_{s=1} \inf$, мы получим

$$\frac{n_\lambda}{n} - \alpha \geqslant \left(1 - \frac{a}{Q^k}\right) \frac{n_\lambda}{n}. \tag{92}$$

Несовместимость (91) и (92) доказывает справедливость неравенства (90).

Неравенства, подобные (90), имеют место для каждого из классов нашего отдела. Чтобы *оценить* величину

$$\limsup_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}},$$

перепишем формулу (20) таким образом: (93)

$$\frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} = k_\lambda \frac{n_\lambda}{n} - \left\{ \frac{\sum_p p_2^{-s}}{\lg \frac{1}{s-1}} + \frac{\sum_p p_3^{-s}}{\lg \frac{1}{s-1}} + \ldots + \frac{\sum_p p_{k_\lambda}^{-s}}{\lg \frac{1}{s-1}} \right\} + \frac{P(s-1)}{\lg \frac{1}{s-1}}.$$

Взяв от обеих частей $\limsup_{s=1}$, мы, в силу очевидного неравенства

$$\liminf(\alpha + \beta + \ldots) \geqslant \liminf \alpha + \liminf \beta + \ldots$$

и неравенства (90), примененного ко 2, 3, . . ., k_λ-му классу нашего отдела, получим

$$\limsup_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} \leqslant k_\lambda \frac{n_\lambda}{n} - \overbrace{\left(\frac{n_\lambda}{n} + \frac{n_\lambda}{n} + \ldots + \frac{n_\lambda}{n} \right)}^{k_\lambda - 1 \text{ раз}} = \frac{n_\lambda}{n}. \quad (94)$$

Сопоставим неравенства (90) и (94)

$$\frac{n_\lambda}{n} \leqslant \liminf_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} \leqslant \limsup_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} \leqslant \frac{n_\lambda}{n}. \quad (95)$$

Эти соотношения могут быть справедливы только тогда, когда в них везде будет иметь место знак равенства. Стало быть

$$\liminf_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} = \limsup_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} = \lim_{s=1} \frac{\sum_p p_1^{-s}}{\lg \frac{1}{s-1}} = \frac{n_\lambda}{n}, \quad (96)$$

и искомая плотность найдена.

§ 5. Критерий родственности областей

В этой главе я исследую связь между *степенью родства* нескольких алгебраических областей и разложением определяющих их уравнений, рассматриваемых как сравнения по простым модулям. До сих пор были разобраны два следующих частных случая этой задачи:

1) Если одна область является делителем другой, то принадлежность простого числа к известному классу подстановок во второй

области влечет за собой принадлежность его к вполне определенному классу в первой. В частности, если простое число принадлежит во второй области к тождественной подстановке, то в первой оно тоже принадлежит к тождественной подстановке. Имеет место также обратная теорема, пользуясь которой, Б. Н. Делоне [9] доказал частный случай известной теоремы Кронекера—Вебера о том, что всякая абелева область есть область деления круга.

2) Две области взаимно просты. Тогда, взяв по произволу из обеих областей по классу подстановок, можно найти бесчисленное множество простых чисел, принадлежащих к классам этих подстановок в соответственных областях. Этот случай рассмотрен М. Бауэром (loc. cit.).

Рассмотрим самый общий случай. Возьмем две произвольные области ω_1 и ω_2 и составим их *нормы*, т. е. наименьшие заключающие их нормальные области: Ω_1 и Ω_2. Образуем их наименьшую общую область Ω, которая тоже будет нормальна, и пусть ее группа будет G, а группы, которым принадлежат области, — соответственно G_1 и G_2. Известно, что G_1 и G_2 являются нормальными делителями G. Их гёльдеровские дополнения

$$H_1 = \frac{G}{G_1} \text{ и } H_2 = \frac{G}{G_2}$$

изоморфны с группами Галуа внутри областей соответственно Ω_1 и Ω_2.

Обозначим пересечение областей Ω_1 и Ω_2 через $\overline{\Omega}$. Группа K, к которой оно принадлежит внутри Ω, является наименьшей группой, содержащей группы G_1 и G_2, и потому, в силу нормальности последних, может быть выражена как их символическое произведение

$$K = G_1 G_2.$$

Внутри каждой из областей Ω_1 и Ω_2 оно принадлежит соответственно к группам

$$K_1 = \frac{K}{G_1} \text{ и } K_2 = \frac{K}{G_2}.$$

Индексы (G, K), (H_1, K_1), (H_2, K_2) будут, очевидно, равны одному и тому же числу j.

Разложим теперь группу G на сопряженные системы по K, группу H_1 по K_1, группу H_2 по K_2

$$G = K + KU_1 + KU_2 + \ldots + KU_{j-1}, \tag{97}$$

$$H_1 = K_1 + K_1V_1 + K_1V_2 + \ldots + K_1V_{j-1}, \tag{98}$$

$$H_2 = K_2 + K_2W_1 + K_2W_2 + \ldots + K_2W_{j-1}. \tag{99}$$

Подстановки V_i и W_i выберем так, чтобы они соответствовали системам соответственно G_1U_i и G_2U_i (вспомним определение гёльдеровского дополнения).

Ясно, что если простое число p принадлежит в Ω к классу подстановки, входящей в систему KU_i, то в Ω_1 и Ω_2 оно будет принадлежать к классам подстановок, входящих в системы соответственно K_1V_i и K_2W_i. Докажем, что если две подстановки T_1 и T_2 внутри Ω_1 и Ω_2 будут входить в системы соответственно K_1V_i и K_2W_i, то можно найти соответствующую им подстановку внутри Ω, входящую в систему KU_i. Достаточно доказать это для систем K_1, K_2, K. Чтобы найти подстановку из K, соответствующую подстановкам T_1 из K_1 и T_2 из K_2, достаточно найти подстановку, соответствующую T_1 из K_1 и 1 из K_2, а затем найти подстановку, соответствующую 1 из K_1 и T_2 из K_2. Найдем первое. Для этого достаточно показать, что внутри Ω существует подстановка, оставляющая величины из Ω_2 на месте (т. е. входящая в G_2) и производящая над величинами из Ω_1 любую подстановку группы $K_1 = \frac{K}{G_1}$. Допустим противное, т. е. что подстановки из G_2 производят над величинами из Ω_1 не всевозможные подстановки группы K_1, а только некоторые, которые должны образовать группу $\overline{K_1}$, являющуюся делителем группы K_1.

Рассмотрим величины, принадлежащие внутри Ω к группе $\overline{K_1}$. С одной стороны, они входят в Ω_1, с другой стороны, не изменяясь в Ω от подстановок группы G_2, они входят в Ω_2; значит, они входят в их пересечение $\overline{\Omega}$. Это же невозможно в том случае, если группа $\overline{K_1}$ является *настоящим* делителем группы K_1. Все это позволяет считать нашу теорему доказанной.

Если Ω_2 целиком входит в Ω_1, то $\Omega_1 = \Omega$, $\Omega_2 = \overline{\Omega}$, $K = G_2$, $K_2 = 1$. Здесь для каждой подстановки в G_1 мы, в силу разложений (97), (98), (99), получим вполне определенную подстановку в G_2. В частности, если мы в G_1 выбрали тождественную подстановку, то в G_2 соответствующая подстановка должна быть тоже тождественной.

Если Ω_2 не входит в Ω_1, то G_2 является *настоящим* делителем K, K_2 содержит не тождественные элементы, а потому существуют простые числа, принадлежащие в Ω_1 к тождественной подстановке, а в Ω_2 — к подстановке, отличной от тождественной. Эта теорема противоположная предыдущей; следовательно, справедлива и обратная.

Наконец, если Ω_1 и Ω_2 взаимно просты, т. е. если $\overline{\Omega}$ есть область рациональных чисел, то $K = G$, $K_1 = G_1$, $K_2 = G_2$ $(j = 1)$. В этом случае в обеих областях можно выбрать подстановки совершенно независимо.

Если мы имеем дело с бо́льшим количеством областей, то исследование придется вести следующим образом: сначала надо исследовать, подобно предыдущему, какие-нибудь две из заданных областей; затем взять их общую область вместе с третьей; затем область, заключающую все три области, вместе с четвертой и т. д. В этом случае более симметричного закона подыскать нельзя. Чтобы убедиться в

этом, достаточно рассмотреть области $\Omega(\sqrt{2})$, $\Omega(\sqrt{3})$, $\Omega(\sqrt{6})$. Любые две из этих областей взаимно просты, и потому подстановки в них независимы; когда же мы выбрали в обеих областях по подстановке, то этим мы вполне определили подстановку в третьей области, так как третья область входит делителем в наименьшую область, заключающую в себе обе остальные области.

Для разрешения в каждом отдельном случае вопроса, существуют ли простые числа, одновременно принадлежащие к заданным классам подстановок в нескольких различных областях, достаточно выяснить, существует ли в группе области, образованной из этих областей, подстановка, которая внутри каждой из заданных областей производит соответствующую заданную подстановку. Вспомним, что каждому простому числу соответствует класс подстановок, а каждому простому идеалу — одна определенная подстановка (ср. [1], конец). Этот принцип более общий, так как здесь не играет никакой роли нормальность областей.

§ 6. Теорема Гильберта о существовании простых идеалов с заданной вычетностью

Принцип, высказанный в конце предыдущей главы, позволяет доказать, притом в несколько расширенной формулировке, теорему Гильберта о существовании бесчисленного множества простых идеалов с заданной вычетностью (см. [6], стр. 426, Satz 152).

Дана нормальная область Ω, содержащая в себе l-ые корни из единицы. Пусть α будет целое алгебраическое число из Ω, а $\mathfrak{p}$ простой идеал, не входящий в α. На основании обобщенной теоремы Ферма

$$\alpha^{p^f-1} \equiv 1 \pmod{\mathfrak{p}}, \tag{100}$$

где f — *порядок* идеала $\mathfrak{p}$. Но так как Ω содержит в себе l-ый корень из единицы $\zeta = e^{\frac{2\pi i}{l}}$, то внутри области $\omega(\zeta)$ порядок простого идеального делителя p является делителем f, а потому должно иметь место сравнение

$$p^f \equiv 1 \pmod{l},$$

т. е. $p^f - 1$ должно делиться на l.

Из формулы (100) нетрудно получить

$$\alpha^{\frac{p^f-1}{l}} \equiv \zeta^c \pmod{\mathfrak{p}}, \tag{101}$$

где c — одно из чисел $0, 1, 2, \ldots, l-1$. Условимся в этом случае в обозначении $\zeta^c = \left\{\frac{\alpha}{\mathfrak{p}}\right\}$ (см. [6], стр. 365). Теорема, которую я собираюсь доказать, заключается в следующем.

Даны t целых чисел из Ω

$$\alpha_1, \alpha_2, \ldots, \alpha_t,$$

притом так, что произведение

$$\alpha_1^{m_1} \cdot \alpha_2^{m_2} \ldots \alpha_t^{m_t}$$

может только тогда быть l-ой степенью числа из Ω, *если каждое из чисел* $m_1, m_2, \ldots, m_t$ *делится на* l. *Зададим по произволу t l-ых корней из единицы:* $\zeta^{c_1}, \zeta^{c_2}, \ldots, \zeta^{c_t}$. *Тогда в* Ω *существует бесчисленное множество таких простых идеалов* $\mathfrak{p}$, *для которых одновременно имеют место равенства*

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\} = \zeta^{c_1}, \quad \left\{\frac{\alpha_2}{\mathfrak{p}}\right\} = \zeta^{c_2}, \ \ldots, \ \left\{\frac{\alpha_t}{\mathfrak{p}}\right\} = \zeta^{c_t}. \tag{102}$$

Ограничимся рассмотрением простых идеалов первого порядка, т. е. таких, для которых $f = 1$; иначе говоря, эти идеалы будут в Ω принадлежать к тождественной подстановке.

Присоединим к Ω величины

$$\beta_1 = \sqrt[l]{\alpha_1}, \ \beta_2 = \sqrt[l]{\alpha_2}, \ \ldots, \ \beta_t = \sqrt[l]{\alpha_t}.$$

Считая Ω областью рациональности, мы получим абелеву область, группа которой состоит из подстановок, переводящих величины β_i в $\zeta_i\beta_i$, где ζ_i — какой-нибудь корень из единицы. Докажем, что порядок этой области по отношению к Ω равен l^t. Допустим противное, т. е. что порядок ее ниже. Тогда, если мы станем присоединять к Ω последовательно корни уравнений

$$z^l - \alpha_1 = 0, \quad z^l - \alpha_2 = 0, \ \ldots, \ z^l - \alpha_t = 0, \tag{103}$$

то какое-нибудь из этих уравнений должно будет сделаться приводимым в области, образованной из области Ω посредством присоединения к ней корней предыдущих уравнений. Но в силу нормальности каждого из этих уравнений внутри Ω уравнение должно распасться на множители одной и той же степени, которая благодаря тому, что l простое число, должна быть первой. Пусть первое из таких уравнений будет $z^l - \alpha_\nu = 0$. Тогда мы получим

$$\beta_\nu = \varphi(\beta_1, \beta_2, \ldots, \beta_{\nu-1}). \tag{104}$$

С другой стороны, область $\Omega(\beta_1, \beta_2, \ldots, \beta_{\nu-1})$ должна быть порядка $l^{\nu-1}$ относительно Ω. Обозначим через S_i операцию над $\beta_1, \beta_2, \ldots, \beta_{\nu-1}$, заключающуюся в умножении β_i на ζ и оставляющую величины $\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_{\nu-1}$ без перемены. Группа Галуа области $\Omega(\beta_1, \beta_2, \ldots, \beta_{\nu-1})$ состоит из подстановок типа $S_1^{\xi_1} S_2^{\xi_2} \ldots S_{\nu-1}^{\xi_{\nu-1}}$. Для того чтобы эта группа была порядка $l^{\nu-1}$, необходимо, чтобы показатели $\xi_1, \xi_2, \ldots, \xi_{\nu-1}$ пробегали независимо друг от друга все зна-

чения $0, 1, 2, \ldots, l-1$. В частности, все подстановки S_i $(i = 1, 2, \ldots, \nu-1)$ должны входить в группу области. Таким образом, величина $\varphi(\beta_1, \ldots, \beta_{i-1}, \zeta\beta_i, \beta_{i+1}, \ldots, \beta_{\nu-1})$ будет сопряженной с β_ν, т. е. она должна быть равна $\zeta^c\beta_\nu$, где c — какое-нибудь из чисел $0, 1, 2, \ldots, l-1$. Соотношение (104) можно переписать следующим образом:

$$\beta_\nu = A_0 + A_1\beta_{\nu-1} + A_2\beta_{\nu-1}^2 + \ldots + A_{l-1}\beta_{\nu-1}^{l-1},$$

где $A_0, A_1, A_2, \ldots, A_{l-1}$ — элементы области $\Omega(\beta_1, \beta_2, \ldots, \beta_{\nu-2})$. Тогда

$$\zeta^c\beta_\nu = A_0 + A_1\zeta\beta_{\nu-1} + A_2\zeta^2\beta_{\nu-1}^2 + \ldots + A_{l-1}\zeta^{l-1}\beta_{\nu-1}^{l-1}.$$

Далее,

$$\zeta^{2c}\beta_\nu = A_0 + A_1\zeta^2\beta_{\nu-1} + A_2\zeta^4\beta_{\nu-1}^2 + \ldots + A_{l-1}\zeta^{(l-1)}\beta_{\nu-1}^{l-1},$$

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

$$\zeta^{(l-1)c}\beta_\nu = A_0 + A_1\zeta^{l-1}\beta_{\nu-1} + A_2\zeta^{2(l-1)}\beta_{\nu-1}^2 + \ldots + A_{l-1}\zeta^{(l-1)^2}\beta_{\nu-1}^{l-1}.$$

Из этих равенств легко заключить, что все A, кроме A_c, равны нулю. Продолжая рассуждение подобным же образом применительно к

$$\beta_{\nu-2}, \beta_{\nu-3}, \ldots, \beta_2, \beta_1,$$

мы увидим, что наше соотношение должно иметь вид

$$\beta_\nu = A\beta_1^{c_1}\cdot\beta_2^{c_2}\cdots\beta_{\nu-1}^{c_{\nu-1}},$$

где A — элемент области Ω. Возведем это соотношение в l-ую степень. Получим

$$\alpha_\nu = A^l\cdot\alpha_1^{c_1}\cdot\alpha_2^{c_2}\cdots\alpha_{\nu-1}^{c_{\nu-1}}.$$

Возможность такого соотношения исключена при формулировке теоремы. Поэтому область $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$ должна быть l-го порядка относительно Ω и ее группа должна состоять из подстановок типа

$$S_1^{\xi_1}\cdot S_2^{\xi_2}\cdots S_t^{\xi_t},$$

где каждая подстановка S_i изменяет β_i в $\zeta\beta_i$ и оставляет величины

$$\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_t$$

без перемены, а показатели $\xi_1, \xi_2, \ldots, \xi_t$ пробегают независимо друг от друга все значения $0, 1, 2, \ldots, l-1$. Эти же подстановки должны входить в группу *нормы* области $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$, т. е. наименьшей заключающей ее нормальной области, а потому, в силу результата главы IV, существует бесчисленное множество простых чисел p, принадлежащих к классу подстановки

$$S = S_1^{c_1}\cdot S_2^{c_2}\cdots S_t^{c_t}.$$

Эти простые числа внутри Ω разлагаются на идеальные множители первого порядка, так как подстановка S оставляет величины из Ω без перемены. Внутри же нормы области $\Omega(\beta_1, \beta_2, \ldots, \beta_t)$ каждое такое простое число p разобьется на простые идеалы таким образом, что хоть один из них, например π, будет принадлежать к подстановке S. Применяя характеризующее принадлежность к S сравнение к величинам $\beta_1, \beta_2, \ldots, \beta_t$, мы получим ряд сравнений

$$\beta_1^p \equiv \zeta^{c_1}\beta_1,\ \beta_2^p \equiv \zeta^{c_2}\beta_2,\ \ldots,\ \beta_t^p \equiv \zeta^{c_t}\beta_t \pmod{\pi}. \tag{105}$$

Разделив эти сравнения соответственно на $\beta_1, \beta_2, \ldots, \beta_t$, мы будем иметь

$$\beta_1^{p-1} \equiv \zeta^{c_1},\ \beta_2^{p-1} \equiv \zeta^{c_2},\ \ldots,\ \beta_t^{p-1} \equiv \zeta^{c_t} \pmod{\pi}. \tag{106}$$

Но так как, в силу того что $f = 1$, число $p-1$ делится на l, мы можем переписать сравнения (106) так:

$$\alpha_1^{\frac{p-1}{l}} \equiv \zeta^{c_1},\ \alpha_2^{\frac{p-1}{l}} \equiv \zeta^{c_2},\ \ldots,\ \alpha_t^{\frac{p-1}{l}} \equiv \zeta^{c_t} \pmod{\pi}. \tag{107}$$

В сравнениях (107) фигурируют величины из Ω, а потому эти сравнения будут справедливы и для простого внутри Ω модуля $\mathfrak{p}$, в который π входит множителем.

Далее, из сравнения

$$\alpha^{\frac{p-1}{l}} \equiv \left\{\frac{\alpha}{\mathfrak{p}}\right\} \pmod{\pi}. \tag{108}$$

и сравнений (107) мы получаем

$$\left\{\frac{\alpha_1}{\mathfrak{p}}\right\} \equiv \zeta^{c_1},\ \left\{\frac{\alpha_2}{\mathfrak{p}}\right\} \equiv \zeta^{c_2},\ \ldots,\ \left\{\frac{\alpha_t}{\mathfrak{p}}\right\} \equiv \zeta^{c_t} \pmod{\mathfrak{p}}. \tag{109}$$

Эти сравнения должны быть заменены равенствами, так как различные корни из единицы не могут быть сравнимы по модулю $\mathfrak{p}$, не входящему в дискриминант уравнения $\zeta^{l-1} + \zeta^{l-2} + \ldots + \zeta + 1 = 0$. Значит, идеалы $\mathfrak{p}$ удовлетворяют поставленным требованиям, т. е. теорема доказана.

ЛИТЕРАТУРА

1. Frobenius. Über Beziehungen u. s. w. Sitzungsber. Berl. Akad., 1896, стр. 689.
2. Dedekind, Zur Theorie der Ideale. Gött. Nachr., 1894.
3. Dirichlet. Werke, Bd. I, стр. 307, 313, 1837, Vorlesungen über Zahlentheorie.
4. Kummer. *Über die Divisoren u. s. w. Journ. f. Math.* **30, 35.**
5. Kronecker. Über Irreducibilität von Gleichungen. Monatsber. Berl. Akad., 1880, стр. 156.

6. D. Hilbert. Zahlbericht, стр. 424 — 428.
7. Furtwängler. Allgemeiner Existenzbeweis u. s. w. Math. Ann. **63.**
8. Furtwängler. Allgemeine Reziprozitätsgesetze. Math. Ann. **72**, 74.
9. B. Delaunay. Zur Bestimmung algebraischer Zahlkörper u. s. w. Journ. f. reine und angew. Math. **152**, стр. 120.
10. H. Weber. Über Zahlgruppen u. s. w. Math. Ann. **49.**
11. D. Hilbert. Relativquadratischer Zahlkörper. Math. Ann. **51,** Sätze 30, 31, стр. 53 сл.
12. Landau. Verteilung der Primzahlen in den Idealklassen. Math. Ann. **63**, стр. 150.
13. H. Weber. Lehrbuch d. Alg., Bd. II, XXI Abschnitt, стр. 693 — 735.
14. Lejeune-Dirichlet. Vorles. über Zahlenth., 4-te Aufl., стр. 358.

ОБОБЩЕНИЕ ТЕОРЕМЫ МИНКОВСКОГО С ПРИМЕНЕНИЕМ К ИССЛЕДОВАНИЮ ИДЕАЛЬНЫХ КЛАССОВ ПОЛЯ

(EINE VERALLGEMEINERUNG DES MINKOWSKI' SCHEN SATZES MIT ANWENDUNG AUF DIE BETRACHTUNG DER KÖRPERIDEALKLASSEN)

(Журнал научно-исследовательских кафедр в Одессе, № 4 (1924), стр. 1—4)

Предлагаемое исследование содержит приложение некоторого обобщения знаменитой теоремы Минковского о дискриминанте поля к рассмотрению теоретико-групповой структуры поля классов, позволяющее раскрыть некоторые теоретико-числовые свойства чисел классов. Я ограничиваюсь здесь только рассмотрением полей деления круга, однако примененный метод можно обобщить на случай произвольных полей, что потребует дальнейших исследований в области теории групп.

§ 1

Упомянутое обобщение теоремы Минковского состоит в следующем.

Возьмем нормальное поле Ω и рассмотрим образованные всеми его элементами α поля $\Omega(\alpha)$. [1]

Поставим следующую задачу: найти условия, необходимые и достаточные для того, чтобы данное простое число не было критическим, т. е. чтобы разложение его на простые идеалы поля $\Omega(\alpha)$ не содержало кратных множителей.

Пусть $\mathfrak{G}$ — группа, к которой принадлежит α в поле Ω, и пусть

$$p = \mathfrak{p}_0^{d_0} \cdot \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_{k-1}^{d_{k-1}} \tag{1}$$

— разложение p на простые идеалы в $\Omega(\alpha)$. Обозначим порядок группы $\mathfrak{G}$ через $(\mathfrak{G})$ и группу инерции, соответствующую в поле Ω простому делителю $\mathfrak{P}_i$ идеала $\mathfrak{p}_i$, через $\mathfrak{G}_t^{(i)}$. Тогда

$$d_i = \frac{(\mathfrak{G}_t^{(i)})}{([\mathfrak{G}, \mathfrak{G}_t^{(i)}])} \qquad (i = 0, 1, \ldots, k-1), \tag{2}$$

где символ $[\mathfrak{G}, \mathfrak{G}_t^{(i)}]$ обозначает пересечение $\mathfrak{G}$ и $\mathfrak{G}_t^{(i)}$. [2]

Из формулы (2) следует, что $d_i = 1$ тогда и только тогда, когда $\mathfrak{G}_t^{(i)} = [\mathfrak{G}, \mathfrak{G}_t^{(i)}]$, т. е. если $\mathfrak{G}_t^{(i)}$ есть делитель $\mathfrak{G}$. Следовательно, условие,

---

[1] $\Omega(\alpha)$ обозначает подполе поля Ω, порожденное элементом α (*Ред.*).

[2] См. Bachmann. Zahlentheorie, Bd. V.

необходимое и достаточное для того, чтобы p не было критическим числом в $\Omega(\alpha)$, состоит в том, чтобы все принадлежащие к p группы инерции были делителями группы, к которой принадлежит α.

Сопоставим эти условия для всех простых чисел. При этом мы можем ограничиться простыми делителями дискриминанта поля, так как прочие простые числа, наверное, не будут критическими. Но вследствие теоремы Минковского ни одно простое число не будет критическим в $\Omega(\alpha)$ только тогда, когда α — рациональное. Отсюда следует теорема:

Алгебраическое число α нормального поля Ω будет рациональным тогда и только тогда, когда все группы инерции поля Ω являются делителями группы, к которой принадлежит α.

Или, если перейти к терминам теории групп:

Все подстановки группы Галуа поля Ω получаются посредством композиции всех групп инерции.

В известном смысле эта теорема является обобщением теоремы Минковского, так как последняя только констатирует существование для каждого поля групп инерции, отличных от единичных групп. Указанная структура группы Галуа с давних пор известна в теории алгебраических функций и была причиной возникновения понятия „группы монодромии". [1]

§ 2

Теперь мы можем доказать следующую теорему:

Если поля Ω_1 и Ω_2 являются делителями поля l^m-ых корней из единицы, причем Ω_2 есть делитель Ω_1, то число классов h_1 поля Ω_1 делится на число классов h_2 поля Ω_2.

Теорема эта была впервые высказана Куммером и доказана им для случая $m = 1$; Фуртвенглер доказал ее для общего случая.

Обозначим через n_1 и n_2 порядки Ω_1 и Ω_2 и пусть $\overline{\Omega}_1$ и $\overline{\Omega}_2$ — соответствующие Ω_1 и Ω_2 поля классов. Порядки их равны $n_1 h_1$ и $n_2 h_2$ соответственно. Докажем сначала следующую лемму:

Лемма. $\overline{\Omega}_2$ есть делитель $\overline{\Omega}_1$. Для доказательства рассмотрим наименьшее общее кратное $\overline{\Omega}_2$ и Ω_1. Поле это — относительно-абелево по отношению к Ω_2, так как оно является объединением поля $\overline{\Omega}_2$, относительно-абелева по отношению к Ω_2, и поля Ω_1. Далее мы докажем, что оно не разветвляется относительно Ω_2. Действительно, порядок группы инерции поля $\overline{\Omega}_2$ равен n_2. Когда мы присоединяем к полю $\overline{\Omega}_2$ поле Ω_1, то порядок полученного поля (т. е. Ω') превышает порядок $\overline{\Omega}_2$ не более чем в n_1 / n_2 раз, следовательно и порядок группы инерции поля Ω' превышает порядок группы инерции поля $\overline{\Omega}_2$

[1] Ср. C. Jordan. Traité des substitutions.

не более чем в n_1/n_2 раз, т. е. порядок этот $\leqq n_2 \frac{n_1}{n_2} = n_1$. Однако порядок группы инерции поля Ω_1 равен n_1 и, стало быть, утверждение доказано. Отсюда мы видим, что поле Ω' относительно Ω_1 будет относительно-абелевым и неразветвленным и, значит, будет являться частичным полем классов для Ω_1. Другими словами, Ω' есть делитель $\overline{\Omega}_1$, но $\overline{\Omega}_2$ есть делитель Ω', а значит, и $\overline{\Omega}_1$, что и т. д.

С другой стороны, пересечение $\overline{\Omega}_2$ и Ω_1 может самое большее совпадать с Ω_2. В самом деле, если предположить, что это поле является надполем Ω_2, то как часть Ω_1 оно должно быть абсолютно-абелевым и потому обладать единственной группой инерции.[1] Но теорема § 1 гласит, что эта группа должна быть группой Галуа нашего поля. Тогда порядок ее будет равен порядку поля. Однако поле это есть делитель Ω_2 и потому порядок его группы инерции не более чем n_2 — порядок группы инерции $\overline{\Omega}_2$. Итак, порядок пересечения не превышает n_2, что противоречит предположению, что оно содержит Ω_2 как собственный делитель.

Порядок Ω' равен, следовательно, $n_2 h_2 \frac{n_1}{n_2} = n_1 h_2$. Но поле это есть делитель $\overline{\Omega}_1$, значит, порядок $\overline{\Omega}_1$, т. е. $n_1 h_1$, делится на $n_1 h_2$ и h_1 делится на h_2, что и т. д.[2]

§ 3

Теперь мы подробнее исследуем структуру группы инерции поля классов. Мы имеем $l \sim \lambda^{l^{m-1}(l-1)}$, где $\lambda = 1 - \zeta$ есть простой идеал поля $\Omega(\zeta)$.[3] В поле классов $\Omega\omega$ будет иметь место соотношение $\lambda \sim \Lambda_1 \Lambda_2 \cdots \Lambda_h$, где $\Lambda_1 \Lambda_2, \ldots, \Lambda_h$ — отличные друг от друга простые идеалы в поле $\Omega\omega$. Пусть S_i — одна из подстановок группы поля $\Omega\omega$, переводящих Λ_1 в Λ_i, и пусть простому идеалу Λ_1 соответствует группа инерции T_1. Тогда простому идеалу Λ_i будет соответствовать группа инерции $S_i T_1 S_i^{-1}$. Если $\mathfrak{G}$ есть группа поля $\Omega\omega$, то вследствие теоремы § 1 композиция всех групп $S_i T_1 S_i$ $(i = 1, 2, \ldots, h)$ дает всю группу $\mathfrak{G}$. Иными словами, не существует такого нормального делителя $\mathfrak{G}$, который содержал бы группу T_1.

---

[1] Ибо: 1) оно имеет единственное критическое простое число l; 2) все группы инерции, соответствующие простым идеалам — делителям критического простого числа, сопряжены друг другу; сопряженные же подгруппы абелевой группы совпадают.

[2] В конце этого параграфа следует добавить: «мы предполагаем, что эти поля нормальны». (Исправление внесено Н. Г. Чеботаревым на стр. 13 «Журнала научно-исследовательских кафедр в Одессе», № 8—9, 1924. — *Ред.*).

[3] $\zeta = e^{\frac{2\pi i}{l^m}}$ есть l^m-ый корень из единицы.

Группа T_1 голоэдрически изоморфна с группой инерции поля $\Omega(\zeta)$ Действительно, пусть t_1 — одна из подстановок T_1 и τ_1 — порожденная t_1 подстановка величин $\Omega(\zeta)$. Так как для любой величины α поля $\Omega\omega$ имеет место сравнение

$$t_1 \alpha \equiv \alpha \pmod{\Lambda_1},$$

то для каждой величины β поля $\Omega(\zeta)$ будет выполняться сравнение

$$\tau_1 \beta \equiv \beta \pmod{\Lambda_1},$$

а значит и сравнение

$$\tau_1 \beta \equiv \beta \pmod{\lambda},$$

поскольку λ есть простой идеал поля $\Omega(\zeta)$. При этом подстановке $t_1 t_2$ соответствует подстановка $\tau_1 \tau_2$ и определенный таким образом изоморфизм будет голоэдрическим в силу того, что группы инерции полей $\Omega(\zeta)$ и $\Omega\omega$ имеют одинаковые порядки.

Пусть U — группа порядка u, являющаяся пересечением всех групп $S_i T_1 S_i^{-1} (i = 1, 2, \ldots, l^m)$, и пусть $u' = \frac{l^{m-1}(l-1)}{u} \cdot U$ есть нормальный делитель группы $\mathfrak{G}$. Пусть группе U принадлежит поле $\Omega_1 \omega_1$ порядка hu', группа которого голоэдрически изоморфна с дополнительной группой $\mathfrak{G}/U$. Группы инерции поля $\Omega_1 \omega_1$ голоэдрически изоморфны с дополнительными группами $S_i T_1 S_i^{-1}/U$ и, следовательно, имеют порядок $\frac{l^{m-1}(l-1)}{u} = u'$.

Таким образом, поле $\Omega_1 \omega_1$ не может иметь с полем $\Omega(\zeta)$ пересечение, порядка больше, чем u'. Пусть Ω_1 — делитель $\Omega(\zeta)$, имеющий порядок u' (так как $\Omega(\zeta)$ — циклическое поле, то Ω_1 вполне определяется своим порядком u'). Тогда $\Omega_1 \omega_1$ есть поле классов для Ω_1. Поле, построенное при помощи полей $\Omega_1 \omega_1$ и $\Omega(\zeta)$, будет, следовательно, иметь порядок $\geqslant \frac{hu' l^{m-1}(l-1)}{u'} = hl^{m-1}(l-1)$, т. е. оказывается тождественным с полем $\Omega\omega$. Поэтому поле $\Omega\omega$ можно рассматривать как объединение поля $\Omega(\zeta)$ и поля $\Omega_1 \omega_1$, являющегося полем классов для некоторого делителя Ω_1 поля $\Omega(\zeta)$, имеющего порядок u'.

§ 4

Возьмем теперь некоторое подполе поля $\Omega(\zeta)$, именно поле Ω_1 порядка u. Рассмотрим все его делители и вычислим соответствующие числа классов. По теореме Фуртвенглера (см. § 2), число классов каждого подполя является делителем числа классов Ω_1. Пусть p — делитель числа классов поля Ω_1, не являющийся делителем числа классов ни одного из делителей Ω_1. Докажем справедливость сравнения

$$p \equiv 1 \pmod{u}.$$

Для доказательства рассмотрим частичное поле классов $\Omega_1 \omega_1$ относительного порядка p. Его группы инерции T имеют порядок u. Пересечением их может быть только единичная группа; в противном случае, как мы показали в предыдущем параграфе, нашелся бы делитель поля Ω_1, число классов которого делилось бы на p, что противоречит предположению. Далее, как известно, мы можем представить эти группы как группы перестановок символов, число которых равно индексу $(\mathfrak{G}, T)$. Индекс этот равен $\frac{pu}{u} = p$. С другой стороны, по отношению к циклическому полю Ω_1 поле $\Omega_1 \omega_1$ относительно циклическое и потому его группа $\mathfrak{G}$ разрешима, т. е. является делителем полной метациклической группы порядка $p(p-1)$. Таким образом, $p(p-1)$ делится на pu, а следовательно $p-1$ — на u, что и т. д.

Отсюда, как тривиальный специальный случай, следует хорошо известная теорема:

Если дискриминант квадратичного поля есть простое число, иными словами, когда существует только один род (Geschlecht), *то число классов этого поля нечетное.*

ОБ ОБОСНОВАНИИ ТЕОРИИ ИДЕАЛОВ ПО ЗОЛОТАРЕВУ

(Усп. матем. наук 2 (1947), в. 6, стр. 52—67)

Теория идеалов была почти одновременно обоснована тремя математиками: Дедекиндом [7], Кронекером [8] и Золотаревым [1, 10] Последнее из этих обоснований не получило должного распространения, может быть в силу установившегося о нем мнения, как о не вполне общем. Это мнение справедливо, если мы будем иметь в виду докторскую диссертацию Золотарева. Действительно, развитая в ней теория годится только для простых чисел, не входящих в так называемый индекс поля. У Золотарева имеется еще более поздняя статья [10], в которой теория идеалов развита при самых общих предположениях. Теория Золотарева была еще изложена в диссертации Сохоцкого [4] и в работах И. И. Иванова [2,3]. Кроме того, я изложил ее в 1925 г., и эта статья была перепечатана в американском журнале [5, 9].

Интерес, который представляет теория Золотарева в настоящее время, заключается в том, что в ней впервые была развита теория, получившая в настоящее время название локальной теории идеалов. Последняя оказалась весьма плодотворной в теории полей классов, а также в теории алгебраических функций.

Настоящая статья является дополненной редакцией моей казанской статьи [5].

§ 1. Предварительные сведения

Перечислим без доказательства основные понятия и факты из теории алгебраических чисел, необходимые для дальнейшего.

Будем называть *областью рациональности* поле k, под которым мы будем подразумевать или поле рациональных чисел, или поле рациональных функций от одной переменной с коэффициентами из заданного числового поля. Выделим в поле k кольцо целых элементов (соответственно — или целых чисел, или полиномов). Определяя в нем обычным образом понятия делимости и простых элементов, мы будем иметь теорему об однозначности разложения целых элементов на простые множители. Эта однозначность имеет место с точностью до *единиц* поля k, под которыми в первом случае мы должны разуметь $+1$ и -1, а во втором случае — любые константы.

Обозначим через K поле рациональных функций от корня x неприводимого уравнения

$$f(x) = 0 \tag{1}$$

степени n с коэффициентами из поля k. Тогда всякий элемент поля K может быть представлен в виде полинома степени $\leqslant n-1$ от x с коэффициентами из поля k, и притом единственным образом. При этом всякий элемент y поля K удовлетворяет уравнению степени n с коэффициентами из поля k. Если это уравнение неприводимо, то x, а также любой элемент поля K могут быть рационально выражены через y. В этом случае говорят, что y есть ***примитивный элемент*** поля.

Целым элементом поля K называется элемент, удовлетворяющий *примарному уравнению*, т. е. уравнению, у которого коэффициент при старшей степени есть единица, а остальные коэффициенты суть целые элементы поля k. Из леммы Гаусса следует, что корень примарного уравнения является также корнем неприводимого примарного уравнения. Можно доказать, что совокупность целых элементов поля K составляет *кольцо*, т. е. что сумма, разность и произведение целых элементов являются также целыми элементами.

Имеет место следующий факт: корень уравнения со старшим коэффициентом единица и остальными коэффициентами, которые являются целыми элементами, хотя бы иррациональными, тоже является целым элементом в поле, в которое он входит.

Если n есть степень неприводимого уравнения, которому удовлетворяет примитивный элемент поля K, то в K существует такая система целых элементов $[\omega_1, \omega_2, \ldots, \omega_n]$, что всякий целый элемент поля K выражается в форме

$$c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n,$$

где $c_1, c_2, \ldots, c_n$ — целые элементы поля k. Система $[\omega_1, \omega_2, \ldots, \omega$ носит название *фундаментального базиса поля K*.

Если α, β — целые элементы поля K, то в том случае, если их частное $\alpha : \beta$ тоже является целым элементом, говорят, что α делится на β.

Если α и $1/\alpha$ целые элементы поля K, то α называется *единицей*. Чтобы α было единицей поля K, необходимо и достаточно, чтобы свободный член уравнения, которому удовлетворяет α, был единицей поля k.

Можно было бы по аналогии с рациональным полем развить теорию разложения целых элементов поля K на неразложимые далее множители, определяя последние с точностью до единицы в качестве множителя. Однако полученные таким путем разложения определяются не всегда однозначно. Это и заставило упомянутых авторов создать теорию идеалов или равносильных с ними понятий.

§ 2. Теория локальных колец

В основу определения локального кольца положим простой (т. е. неразложимый на дальнейшие целые множители) целый элемент p поля k. В случае, когда поле k числовое, p есть простое число; если же k есть поле функций, p есть полином, неприводимый в заданном числовом поле. Если последнее алгебраически замкнуто, p есть линейная функция $x - c$.

Под локальным кольцом, соответствующим элементу p, мы будем разуметь совокупность элементов поля k, при представлении которых в виде несократимых дробей знаменатель последних взаимно прост с p. Другими словами, элемент локального кольца, или, как мы в дальнейшем будем говорить, p-целый элемент, характеризуется тем, что, умножая его на некоторый взаимно простой с p элемент, можно превратить его в целый элемент.

Под p-целым элементом поля K мы будем разуметь элемент, удовлетворяющий уравнению, у которого старший коэффициент есть единица, а остальные суть p-целые элементы поля k. Нетрудно доказать, что совокупность p-целых элементов поля K образует кольцо, которое мы и будем называть локальным кольцом.

Для дальнейшего необходимо ввести понятие нормы. Нормой элемента z поля K называется взятый со знаком $(-1)^n$ свободный член уравнения n-ой степени, которому удовлетворяет z (уравнения, получаемого описанным в § 1 методом). Норму также можно определить, как произведение всех (сопряженных) корней этого уравнения.

Норма обладает следующими свойствами:

1) Норма произведения равна произведению норм

$$N(zu) = N(z)\,N(u).$$

2) Если z лежит в k, то

$$N(z) = z^n.$$

3) Норма целого элемента делится на этот элемент. В самом деле, если

$$z^n + a_1 z^{n-1} + \ldots + a_{n-1} z + a_n = 0,$$

то

$$(-1)^n \frac{N(z)}{z} = \frac{a_n}{z} = -(z^{n-1} + a_1 z^{n-2} + \ldots + a_{n-1}).$$

4) Если t произвольный элемент поля k или даже переменная, то

$$N(t - z) = f(t),$$

где $f(z) = 0$ — уравнение, которому удовлетворяет z.

p-целый элемент поля K может быть также определен как элемент, который умножением на взаимно простой с p элемент c поля k может быть преобразован в целый в обычном смысле.

Будем говорить, что z p-делится на u, если частное $z:u$ есть p-целый элемент.

Если $N(z)$ взаимно проста с p, то все целые элементы поля K p-делятся на z. Действительно, тогда достаточно взять в роли взаимно простого с p элемента c норму $N(z)$. Элемент

$$\frac{cu}{z} = \frac{N(z)}{z} u$$

при целом u всегда целый.

Если z p-делится на u, то в $N(z)$ множитель p входит в не меньшей степени, чем в $N(u)$. Действительно, тогда при некотором взаимно простом с p p-целом элементе c поля k элемент $cz:u$ должен быть целым. В силу этого его норма

$$\frac{c^n N(z)}{N(u)}$$

должна быть целым элементом поля k, откуда следует утверждение.

Если два элемента делятся друг на друга, то мы будем называть их p-ассоциированными и с точки зрения p-делимости не будем считать различными.

Нашей ближайшей целью является доказательство однозначности разложения p-целых элементов поля на неразложимые далее p-множители. Для этого нам понадобятся следующие леммы:

Лемма 1. *Если z и u p-делятся на v, то $z \pm u$ тоже p-делится на v.*

Из этой очевидной леммы вытекает следующая:

Лемма 2. *Если z точно p-делится на v^λ* (т. е. *не делится на $v^{\lambda+1}$*), *а u точно p-делится на v^μ, то их сумма точно p-делится* на v^ν, *где ν есть наименьшее из чисел λ, μ ($\lambda \neq \mu$).*

Справедливость этой леммы вытекает из леммы 1.

Будем называть общим наибольшим p-делителем двух элементов z, u поля K элемент d, на который p-делятся оба заданных элемента и который вместе с тем обладает тем свойством, что неопределенное уравнение

$$z\xi + u\eta = d$$

имеет решения в p-целых элементах поля K.

Чтобы убедиться в существовании общего наибольшего делителя для каждой пары p-целых элементов, докажем следующую основную теорему Золотарева.

Теорема Золотарева. *Если из норм всевозможных элементов типа*

$$z + p^\nu u,$$

где u пробегает все целые элементы поля K, в норму элемента z элемент p входит множителем в наименьшей степени, то p^ν p-делится на z.

Доказательство. Пусть уравнение, которому удовлетворяет z, таково:

$$z^n + c_1 p^{\lambda_n - \lambda_1} z^{n-1} + c_2 p^{\lambda_n - \lambda_2} z^{n-2} + \ldots + c_{n-1} p^{\lambda_1} z + c_n p^{\lambda} = 0, \qquad (2)$$

где $c_1, c_2, \ldots, c_n$ — взаимно простые с p элементы поля k. Выберем среди чисел

$$\frac{\lambda - \lambda_1}{1}, \quad \frac{\lambda - \lambda_2}{2}, \quad \frac{\lambda - \lambda_3}{3}, \ldots, \frac{\lambda - \lambda_{n-1}}{n-1}, \quad \frac{\lambda}{n}$$

наибольшее. Пусть это будет

$$\mu = \frac{r}{s},$$

где r и s — взаимно простые целые рациональные числа. Докажем сначала, что

$$u = \frac{c_n p^{\mu}}{z}$$

есть целый элемент. Для этого умножим уравнение (2) на

$$\frac{{c_n}^{n-1} p^{n\mu - \lambda}}{z^n}$$

и перепишем его члены в обратном порядке

$$(c_n p^{\mu})^n + c_{n-1} p^{\lambda_1 + \mu - \lambda} \left(\frac{c_n p^{\mu}}{z}\right)^{n-1} + \ldots +$$

$$+ c_1 {c_n}^{n-1} p^{\lambda_n - 1 + \mu(n-1) - \lambda} \left(\frac{c_n p^{\mu}}{z}\right) + {c_n}^{n-1} p^{\mu n - \lambda} = 0. \qquad (3)$$

Это будет уравнение для u, все коэффициенты которого суть целые элементы, возможно не входящие в k, так как μ может иметь дробное значение. В самом деле, в силу определения μ,

$$\mu \geqslant \frac{\lambda - \lambda_h}{h} \quad (h = 1, 2, \ldots, n),$$

откуда

$$\lambda_h + \mu h - \lambda \geqslant 0 \quad (h = 1, 2, \ldots, n),$$

а потому все показатели при p в коэффициентах уравнения (3) не отрицательны. В силу этого s-ая степень элемента u есть целый элемент поля K. Тогда, в силу нашего предположения, в нормы всевозможных элементов

$$\zeta = z - p^{\nu} u^{si} = z - \frac{{c_n}^{si} p^{ri+\nu}}{z^{si}} \quad (i = 1, 2, 3, \ldots, n)$$

множитель p входит не ниже, чем в λ-ой степени. Но

$$N(\zeta) = N\left(z - \frac{{c_n}^{si} p^{ri+\nu}}{z^{si}}\right) = \frac{N\left(z^{si+1} - {c_n}^{si} p^{ri+\nu}\right)}{[N(z)]^{si}}, \qquad (4)$$

откуда следует, что в

$$N(z^{si+1} - c_n^{si} p^{ri+\nu})$$

множитель p входит по крайней мере в $\lambda(si+1)$-ой степени.

Преобразуем это выражение. Для этого введем в рассмотрение первообразный корень $si+1$-ой степени из единицы

$$\varepsilon = e^{\frac{2\pi i}{si+1}}.$$

Применим тождество

$$x^{si+1} - y^{si+1} = (x-y)(x-\varepsilon y)\cdots(x-\varepsilon^{si} y)$$

к двучлену $z^{si+1} - c_n^{si} p^{ri+\nu}$

$$z^{si+1} - c_n^{si} p^{ri+\nu} = \prod_{j=0}^{si} (z - \varepsilon^j c_n^{\frac{si}{si+1}} p^{\frac{ri+\nu}{si+1}}),$$

откуда

$$N(z^{si+1} - c_n^{si} p^{ri+\nu}) = \prod_{j=0}^{si} N\left(z - \varepsilon^j c_n^{\frac{si}{si+1}} p^{\frac{ri+\nu}{si+1}}\right), \tag{5}$$

где в выражениях норм в правой части с элементами

$$\varepsilon,\ p^{\frac{ri+\nu}{si+1}},\ c_n^{\frac{si}{si+1}}$$

надо поступать, как с рациональными элементами. Применим к каждой из этих норм свойство 4) нормы

$$N\left(z - \varepsilon^j c_n^{\frac{si}{si+1}} p^{\frac{ri+\nu}{si+1}}\right) = \pm f\left(\varepsilon^j c_n^{\frac{si}{si+1}} p^{\frac{ri+\nu}{si+1}}\right) =$$

$$= \pm\left\{\varepsilon^{jn} c_n^{n\frac{si}{si+1}} p^{n\frac{ri+\nu}{si+1}} + \varepsilon^{j(n-1)} c_1 c_n^{(n-1)\frac{si}{si+1}} p^{\lambda_{n-1}+(n-1)\frac{ri+\nu}{si+1}} + \right.$$

$$\left. + \ldots + \varepsilon^j c_{n-1} c_n^{si+1} p^{\lambda_i + \frac{ri+\nu}{si+1}} + c_n p^{\lambda}\right\}, \tag{6}$$

где $f(z) = 0$ — уравнение, которому удовлетворяет z.

Сначала рассмотрим случай

$$\mu = \frac{r}{s} \neq \nu.$$

Каждый член правой части выражения (6) делится на степень p, равную соответственно

$$n\frac{ri+\nu}{si+1},\ \lambda_{n-1} + (n-1)\frac{ri+\nu}{si+1},\ \ldots,\ \lambda_1 + \frac{ri+\nu}{si+1},\ \lambda. \tag{7}$$

Если мы теперь подберем i так, чтобы среди показателей (7) не было равных, то элемент

$$N\left(z - \varepsilon^j c_n^{\frac{si}{si+1}} p^{\frac{ri+\nu}{si+1}}\right)$$

будет делиться на p в степени, показатель которой равен наименьшему из чисел (7). Этого невозможно достичь лишь в том случае, когда хоть одно из уравнений

$$h\frac{ri+\nu}{si+1}+\lambda_h = k\frac{ri+\nu}{si+1}+\lambda_k \qquad (h\neq k)$$

удовлетворяется при всяком i. Преобразуем это уравнение

$$(h-k)(ri+\nu) = (\lambda_k-\lambda_h)(si+1).$$

Оно удовлетворяется тождественно только в случае, если

$$(h-k)r = (\lambda_k-\lambda_h)s, \qquad (h-k)\nu = (\lambda_k-\lambda_h),$$

откуда $\frac{r}{\nu}=\frac{s}{1}$, или $\nu=\frac{r}{s}=\mu$. Этот случай мы разберем отдельно.

Теперь мы можем доказать, что $\mu\leqslant\nu$. Допустим противное, т. е. что $\mu>\nu$. Тогда $r>s\nu$, откуда, прибавляя к обеим частям неравенства по rsi, мы будем иметь

$$r(si+1)>s(ri+\nu), \text{ т. е. } \mu=\frac{r}{s}>\frac{ri+\nu}{si+1}. \qquad (8)$$

С другой стороны, в силу определения μ существует такое значение $i=f$, для которого имеет место

$$\mu=\frac{\lambda-\lambda_f}{f}, \text{ или } \lambda=\lambda_f+\mu f,$$

откуда, в силу (8),

$$\lambda>\lambda_f+f\frac{ri+\nu}{si+1}. \qquad (9)$$

Правая часть этого неравенства равна одному из показателей (7), и, таким образом, из неравенства (9) вытекает, что выражение (6) при любом j делится на p в меньшей степени, чем λ-ая. В силу этого произведение (5) делится на p в меньшей чем $\lambda(si+1)$-ая степени. Таким образом, предположение $\mu>\nu$ приводит нас к противоречию, откуда следует

$$\mu\leqslant\nu.$$

Исключенный нами случай $\mu=\nu$ тоже находится в согласии с полученным неравенством.

Отсюда непосредственно следует, что

$$\frac{c_n p^{\nu}}{z} = p^{\nu-\mu}\,\frac{c_n p^{\mu}}{z}$$

есть целое число поля K, т. е. что p^{ν} p-делится на z, что и т. д.

Примечание. Это трудное доказательство во многих случаях можно было бы заменить весьма простым. Если мы имеем дело с числовыми полями, то это можно сделать в случае $p>n$, который

при каждом n охватывает все простые числа p, кроме конечного числа. Неохваченные простые числа и есть как раз те, из-за которых развитая в диссертации Золотарева теория не может считаться вполне общей. В полях алгебраических функций можно применить простое доказательство, если числовое поле имеет характеристику нуль.

Нетрудно видеть, что найденный по рецепту теоремы Золотарева элемент является общим наибольшим p-делителем элементов z и p^ν. В самом деле, из теоремы Золотарева следует, что при данных z и p^ν можно так подобрать u, чтобы на элемент

$$z + p^\nu u = v$$

p-делится p^ν. Отсюда следует, что на него p-делится и z. Полагая $\xi = 1$, $\eta = u$, мы видим, что элемент v подходит под определение общего наибольшего делителя элементов z и p^ν.

Нетрудно распространить это утверждение на общий наибольший p-делитель двух произвольных целых элементов x, y поля K. Пусть

$$N(y) = yy' = cp^\nu \qquad (c, p) = 1.$$

В силу теоремы Золотарева можно так подобрать u, чтобы

$$xy' + p^\nu u = v$$

был p-делителем элемента p^ν. Вместе с тем из формы этого элемента следует, что он p-делится на y', так что его можно представить в форме $\frac{y'w}{c'}(c', p) = 1$. Тогда y p-делится на w. Сокращая наше равенство на $y' \mid cc'$, мы будем иметь

$$xcc' + yc'u = cw,$$

откуда следует, что элемент w есть общий наибольший p-делитель элементов x и y. Итак,

Теорема 2. *Всякая пара целых элементов поля K имеет общий наибольший p-делитель, входящий в то же поле K.*

§ 3. Разложение элементов на простые множители в локальных кольцах

Предварительно докажем следующие три леммы, аналогичные тем, которые лежат в основе элементарной теории делимости.

Лемма 1. *Если $\alpha\beta$ p-делится на γ, а α p-взаимно просто с γ (т. е. имеет с γ общий наибольший p-делитель 1), то β должно p-делиться на γ.*

Доказательство. Если α и β p-взаимно просты, то можно найти такой элемент $\varepsilon = \alpha + \gamma u$, в норму которого p не входит. Тогда, умножая полученное равенство на целый элемент

$$\frac{c}{\varepsilon}\beta = \varepsilon'\beta \qquad (N(\varepsilon) = \varepsilon\varepsilon' = c),$$

мы получим

$$\beta c = \alpha\beta\varepsilon' + \gamma\varepsilon'\beta u.$$

Но, согласно условию, $\frac{c'\alpha\beta}{\gamma}$ есть при некотором c', взаимно простом с p, целый элемент, в силу чего и

$$\frac{\beta}{\gamma}cc' = \frac{\alpha\beta}{\gamma}\varepsilon c' - \varepsilon'\beta\omega' c'$$

есть целый элемент, т. е. β p-делится на γ.

Лемма 2. *Если α и β p-взаимно просты с γ, то и их произведение $\alpha\beta$ p-взаимно просто с γ.*

Доказательство. В силу определения, существуют такие целые элементы u и v, что нормы элементов

$$\varepsilon = \alpha + \gamma u, \qquad \varepsilon' = \beta + \gamma v$$

не делятся на p. Перемножая эти равенства, получим

$$\varepsilon\varepsilon' = \alpha\beta + \gamma(\beta u + \alpha v + \gamma uv).$$

Здесь

$$N(\varepsilon\varepsilon') = N(\varepsilon)\,N(\varepsilon')$$

не делится на p, откуда и следует, что $\alpha\beta$ p-взаимно просто с γ.

Лемма 3. *Если α p-делится на два p-взаимно простых элемента β и γ, то оно p-делится и на их произведение $\beta\gamma$.*

Доказательство. Если α p-делится на β, то при некотором p-взаимно простом с p элементе c элемент $c\alpha/\beta$ — целый. Но

$$c\alpha = \frac{c\alpha}{\beta}\beta.$$

Это произведение p-делится на γ, а так как β p-взаимно просто с γ, то, в силу леммы 1, элемент $c\alpha/\beta$ должен p-делиться на γ, т. е. при некотором взаимно простом с p элементе c' элемент

$$\frac{c'c\alpha}{\beta\gamma}$$

целый, откуда следует, что α p-делится на $\beta\gamma$.

Назовем p-простым элементом π поля K такой элемент, что всякий целый элемент поля K или p-делится на π, или p-взаимно прост с π. Из этого определения ясно, что p-простой элемент не может быть представлен в виде произведения двух целых элементов, из которых ни один не был бы взаимно прост с p (другими словами, нормы которых не делились бы на p). Обратно, если π есть не простой элемент, то существует элемент π', который и не p-взаимно прост с π и не p-делится на π. Тогда общий наибольший p-делитель элементов π и π' есть p-делитель элемента π и не p-ассоциирован с ним. Их частное есть второй множитель элемента π, и его норма делится на p.

Предварительно разложим элемент p на p-простые в поле K множители и покажем, что их всего конечное число. Будем рассматривать выражения

$$c_1\omega_1 + c_2\omega_2 + \ldots + c_n\omega_n,$$

где $[\omega_1, \omega_2, \ldots, \omega_n]$ есть фундаментальный базис поля K, а $c_1, c_2, \ldots, c_n$ — всевозможные целые элементы поля k. Из этой бесконечной совокупности элементов мы откинем элементы, отличающиеся от других элементов этой совокупности на кратность p. Другими словами, мы не будем считать различными элементы, отличающиеся на кратность p. Будем прибавлять к каждому элементу совокупности такую кратность p, чтобы получался элемент, норма которого делилась бы на возможно меньшую степень p. Тогда, в силу теоремы Золотарева, каждый элемент совокупности есть p-делитель элемента p.

Выберем в этой совокупности элемент, норма которого делится на наименьшую, хотя и положительную степень p. Заметим, что если нормы всех элементов совокупности, кроме p, будут p-взаимно просты с p, то выбранным элементом мы должны считать p. Обозначим через π_1 выбранный таким образом элемент, и пусть его норма точно делится на f_1-ую степень p. Докажем, что π_1 есть p-простой элемент. Пусть u есть произвольный целый элемент поля K. Если существует элемент типа $\pi_1 + uv$, норма которого не делится на p, то u p-взаимно прост с π_1. Если же нормы всех элементов такого рода делятся на p, то каждая из них должна делиться по крайней мере на pf_1 в силу нашего предположения относительно выбора представителей нашей совокупности, а также выбора π_1. Значит, среди всех элементов типа $\pi_1 + uv$ элемент π_1 имеет норму, делящуюся на самую низкую степень p. Но тогда из теоремы Золотарева следует, что u p-делится на π_1. Таким образом, всякий целый элемент поля K или p-взаимно прост с π_1, или p-делится на π_1.

Пусть $\pi_1^{e_1}$ будет наибольшая степень, на которую p-делится p. Целый элемент $cp/\pi_1^{e_1}$ уже не p-делится на π_1 и, следовательно, p-взаимно прост с π_1.

Теперь выберем из элементов нашей совокупности, p-взаимно простых с π_1, тот элемент π_2, в норму которого p входит в наименьшей степени. Докажем, что π_2 есть p-простой элемент. Возьмем произвольный целый элемент u поля K и рассмотрим всевозможные элементы $\pi_2 + \pi_1 uv$. Если среди них нет таких, нормы которых были бы взаимно просты с p, то во всех этих нормах p будет входить не в меньшей степени, чем в $N(\pi_2)$, в силу выбора π_2.

Пусть $\pi_2^{e_2}$ будет наибольшая степень, на которую p-делится элемент p. В силу леммы 3, p должно p-делиться на $\pi_1^{e_1}\pi_2^{e_2}$, так как, в силу леммы 2, элементы $\pi_1^{e_1}$ и $\pi_2^{e_2}$ p-взаимно просты. Элемент

$$\frac{cp}{\pi_1^{e_1}\pi_2^{e}}$$

p-взаимно прост и с π_1 и с π_2.

с π_1. Далее, выбираем среди тех элементов нашей совокупности, которые p-взаимно просты и с π_1 и с π_2, элемент π_3, в норму которого множитель p входит в возможно меньшей степени, и точно так же убеждаемся, что π_3 есть p-простой элемент. Продолжая подобный выбор, мы будем приходить к целым элементам типа

$$\frac{cp}{\pi_1^{e_1}\pi_2^{e_2}\dots\pi_k^{e_k}}. \tag{1}$$

Но норма числителя такого элемента делится точно на p^n, а норма знаменателя по крайней мере на p^k, так что должно иметь место

$$k \leqslant n,$$

и процесс должен на некотором месте закончиться. Но конец процесса на k-ом месте означает, что не существует элементов, которые были бы p-взаимно просты с $\pi_1, \pi_2, \dots, \pi_k$ и в то же время нормы которых делились бы на p. В частности, элемент (1) p-взаимно прост с $\pi_1, \pi_2, \dots, \pi_k$, а потому его норма не делится на p. Но поскольку норма его числителя точно делится на p^n, а норма его знаменателя точно делится на $p^{e_1f_1+\dots+e_kf_k}$, должно иметь место

$$e_1f_1 + e_2f_2 + \dots + e_kf_k = n. \tag{2}$$

Точно так же всякий целый элемент поля K, норма которого делится на p (т. е. не является единицей локального кольца), в силу доказанного, должен делиться по крайней мере на один из p-простых элементов $\pi_1, \pi_2, \dots, \pi_k$. Мы можем разделить его на такие степени элементов $\pi_1, \pi_2, \dots, \pi_k$, чтобы частное было p-целым элементом, норма которого не делилась бы на p. Из этого следует, что $\pi_1, \pi_2, \dots, \pi_k$ являются единственными p-простыми элементами поля K. Вместе с тем мы доказали, что любой целый элемент поля K может быть разложен на p-простые множители, т. е. представлен в форме

$$c\pi_1^{m_1}\pi_2^{m_2}\dots\pi_k^{m_k},$$

где c — единица нашего локального кольца, т. е. p-целый элемент, норма которого не делится на p.

Остается доказать, что всякий целый элемент поля K разлагается на p-простые множители единственным образом. Пусть мы имеем

$$c\pi_1^{m_1}\pi_2^{m_2}\dots\pi_k^{m_k} = c_1\pi_1^{n_1}\pi_2^{n_2}\dots\pi_k^{n_k}.$$

Докажем, что $m_1 = n_1$. Допустим противное, и пусть $m_1 > n_1$. Сокращая равенство на $\pi_1^{n_1}$, мы придем к равенству, левая часть которого делится на π_1, а правая часть, являясь произведением p-взаимно простых с π_1 множителей, в силу леммы 2, сама p-взаимно проста с π_1.

Противоречие доказывает наше утверждение. Продолжая рассуждение для $\pi_2, \pi_3, \ldots, \pi_k$, мы докажем, что

$$m_1 = n_1, \quad m_2 = n_2, \ldots, m_k = n_k, \quad c = c_1,$$

что и т. д.

§ 4. Сопоставление различных локальных колец

Станем рассматривать разложения целых элементов поля K на p-простые множители одновременно по кольцам, соответствующим всевозможным простым элементам p поля k. Возьмем целый элемент z и найдем его разложения, соответствующие тем простым элементам, которые входят множителями в норму $N(z)$ (относительно остальных простых элементов поля k, порождающих локальные кольца, элемент z будет играть роль единицы).

Сопоставим с каждым p-простым элементом π символ (*простой дивизор*) $\mathfrak{p}$, говоря, что z делится на $\mathfrak{p}^k$ тогда и только тогда, если z p-делится на π^k. Нормой простого дивизора $\mathfrak{p}$ будем называть степень элемента p, на которую точно делится норма $N(\pi)$. Произведение нескольких простых дивизоров будем называть просто дивизором (уже не простым).

Если теперь мы напишем произведение всех простых дивизоров, на которые делится (точно) заданный элемент z поля K, для всех локальных колец, соответствующих простым делителям нормы $N(z)$, то полученный дивизор мы будем называть представлением элемента z через дивизоры. Нетрудно видеть, что $N(z)$ равно произведению норм простых дивизоров, входящих в представление элемента z.

Для дальнейшего необходимо доказать три следующие леммы.

Лемма 1. *Если α p-делится на β, то в роли целого элемента с поля k, входящего в выражение целого элемента $c\alpha/\beta$, можно выбрать некоторый делитель нормы $N(\beta)$.*

Доказательство. Пусть $\lambda = \frac{c\alpha}{\beta}$ есть целый элемент. Целым элементом будет и $\mu = \frac{N(\beta)\alpha}{\beta}$. Решаем неопределенное уравнение

$$cX + N(\beta)Y = d$$

(в целых рациональных элементах), где d есть общий наибольший делитель c и $N(\beta)$. Элемент d, с одной стороны, есть делитель $N(\beta)$, с другой стороны, будучи делителем c, он взаимно прост с p. Но целый элемент $\lambda X + \mu Y$ допускает представление

$$\lambda X + \mu Y = \frac{d\alpha}{\beta}.$$

Лемма 2. *Если α p-делится на β, каков бы ни был простой делитель p нормы $N(\beta)$, то α делится на β в обычном смысле.*

Доказательство. Пусть

$$N(\beta) = p_1^{\omega_1} p_2^{\omega_2} \cdot \ldots \cdot p_k^{\omega_k}.$$

Тогда, в силу леммы 1, в поле K будут существовать целые элементы

$$\lambda_1 = \frac{M_1\alpha}{\beta}, \quad \lambda_2 = \frac{M_2\alpha}{\beta}, \quad \ldots, \lambda_k = \frac{M_k\alpha}{\beta},$$

где $M_i\,(i = 1, 2, \cdots, k)$ есть делитель $N(\beta)/p_i^{\omega_i}$ и потому взаимно прост с p_i. Элементы $M_1, M_2, \cdots, M_k$ не имеют общего делителя, а потому неопределенное уравнение

$$M_1X_1 + M_2X_2 + \ldots + M_kX_k = 1$$

имеет решение в целых рациональных элементах. Элемент

$$\lambda_1X_1 + \lambda_2X_2 + \cdots + \lambda_kX_k = \frac{\alpha}{\beta}$$

является целым элементом поля K, что доказывает лемму.

Лемма 3. *Если α и β p-взаимно просты, где p — любой общий простой делитель норм $N(\alpha)$ и $N(\beta)$, то α и β взаимно просты в обычном смысле. Последнее означает, что можно найти такие целые элементы λ и μ поля K, что имеет место*

$$\alpha\lambda + \beta\mu = 1. \tag{1}$$

Доказательство. Пусть $p_1, p_2, \ldots, p_k$ будет совокупность всех простых элементов поля k, входящих одновременно в $N(\alpha)$ и в $N(\beta)$. В силу нашего условия для каждого i имеет место

$$\alpha + \beta u_i = v_i \qquad (i = 1, 2, \ldots, k),$$

где $N(v_i)$ не делится на p_i. Умножая эти равенства на $v_i' = \frac{N(v_i)}{v_i}$ и меняя обозначения, будем иметь

$$\begin{aligned} \alpha\xi_1 + \beta\eta_1 &= N(v_1), \\ \alpha\xi_2 + \beta\eta_2 &= N(v_2), \\ &\ldots\ldots\ldots\ldots \\ \alpha\xi_k + \beta\eta_k &= N(v_k), \end{aligned} \tag{2}$$

где ξ_i и η_i — целые элементы поля K. Присоединим сюда еще равенства

$$\begin{aligned} \alpha\cdot\alpha' &= N(\alpha), \\ \beta\cdot\beta' &= N(\beta), \end{aligned} \tag{3}$$

где α', β' — некоторые целые элементы поля K. Элементы $N(v_1)$, $N(v_2), \ldots, N(v_k)$, $N(\alpha)$, $N(\beta)$ имеют общим наибольшим делителем 1, а потому неопределенное уравнение

$$N(v_1)X_1 + N(v_2)X_2 + \cdots + N(v_k)X_k + N(\alpha)Y_1 + N(\beta)Y_2 = 1$$

имеет решение в целых элементах поля k. Умножим равенства (2) соответственно на $X_1, X_2, \ldots, X_k$, равенства (3) на Y_1, Y_2 и сложим

$$\alpha(\xi_1 X_1 + \xi_2 X_2 + \cdots + \xi_k X_k + \alpha' Y_1) + \beta(\eta_1 X_1 + \eta_2 X_2 + \cdots + \eta_k X_k + \beta' Y_2) = 1. \quad (4)$$

Это равенство является равенством типа (1). Лемма доказана.

Теорема 3. *Элемент α определяется своим дивизором с точностью до единицы поля K как множителя.*

Доказательство. Если двум элементам поля K, которые мы обозначим через α и β, соответствует один и тот же дивизор, то они должны p-делиться друг на друга (т. е. быть p-ассоциированы), причем в роли p может быть взят любой простой делитель элемента

$$N(\alpha) = \pm N(\beta).$$

Отсюда и из леммы 2 следует, что они делятся друг на друга обычным образом, т. е. что их частное есть единица поля K.

Теорема 4 (теорема о независимости). *Если дан дивизор $\mathfrak{a}$, а также целый элемент M поля k, то можно найти такой целый элемент α поля K, делящийся на $\mathfrak{a}$, чтобы норма частного $\alpha : \mathfrak{a}$ была взаимно проста с элементом M.*

Доказательство. Сначала докажем эту теорему для входящего в $\mathfrak{a}$ простого дивизора $\mathfrak{p}$. Пусть π есть p-простой элемент поля K, соответствующий простому дивизору $\mathfrak{p}$, и пусть

$$N(\mathfrak{p}) = p^k, \quad N(\pi) = cp^k, \quad (c, p) = 1.$$

Далее, пусть

$$M = p^m M',$$

где M' взаимно прост с p. Тогда элемент

$$\pi' = M'\pi + p^{k+1}$$

будет удовлетворять условию теоремы, что вытекает из сравнений

$$N(\pi') \equiv N(p^{k+1}) = p^{n(k+1)} \pmod{M'},$$
$$N(\pi') \equiv M'^n cp^k \pmod{p^{k+1}}.$$

Чтобы найти требуемый элемент для всего дивизора $\mathfrak{a}$, нужно составить такие элементы для каждого из его простых делителей, а затем перемножить эти элементы.

§ 5. Связь дивизоров с идеалами

Изложенная теория Золотарева может заменить собой теорию идеалов, созданную Дедекиндом. Более того, оказывается, что обе теории эквивалентны; другими словами, понятия идеала и дивизора хотя определены различным образом, но по существу совпадают. Это было впервые доказано И. И. Ивановым [3]. Я привожу свое, несколько другое доказательство.

Напомним определение идеала.

Идеалом называется такая совокупность целых элементов поля, что:

1) сумма и разность двух элементов идеала входят в идеал,

2) произведение элемента идеала на любой целый элемент поля входит в идеал.

Наряду с идеалами будем рассматривать совокупности целых элементов поля K, делящихся на введенные в предыдущем параграфе дивизоры. Поскольку произведениям элементов поля K соответствуют произведения соответствующих им дивизоров, очевидно, что эти совокупности являются идеалами. Докажем обратное.

Рассмотрим какой-нибудь идеал $\mathfrak{a}$, который пусть будет задан или базисом, или, в более общем случае, системой входящих в него элементов, причем предположим, что не существует другого входящего в $\mathfrak{a}$ идеала, который содержал бы все элементы системы. Пусть эта система состоит из элементов

$$\alpha_1, \alpha_2, \ldots, \alpha_s.$$

Разложим каждый из них на дивизоры, и пусть общий наибольший делитель этих дивизоров будет

$$\begin{aligned} \mathfrak{a} = {} & \mathfrak{p} \cdot \mathfrak{p}' \cdot \mathfrak{p}'' \ldots \\ & \mathfrak{p}_1 \cdot \mathfrak{p}_1' \cdot \mathfrak{p}_1'' \ldots \\ & \mathfrak{p}_2 \cdot \mathfrak{p}_2' \cdot \mathfrak{p}_2'' \ldots \end{aligned} \tag{1}$$

В этом выражении мы расположили в каждой строке простые дивизоры, соответствующие одному и тому же простому элементу p поля K. Ясно, что всякий элемент, входящий в идеал $\mathfrak{a}_1$, делится на дивизор $\mathfrak{a}$. Докажем обратное. Пусть некоторый целый элемент z поля K делится на дивизор $\mathfrak{a}$. Рассмотрим отдельно каждый из простых элементов $p, p_1, \ldots$ поля k, входящих в $N(\mathfrak{a})$. Пусть p соответствует первой строке дивизоров в формуле (1) и пусть

$$\beta = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_s u_s \tag{2}$$

будет элемент из идеала $\mathfrak{a}_1$, точно делящийся на дивизор

$$\mathfrak{p} \cdot \mathfrak{p}' \cdot \mathfrak{p}'' \ldots$$

Если бы такого элемента не существовало, то все элементы, входящие в идеал, получаемый, если в выражении (2) $u_1, u_2, \ldots, u_s$ пробегают всевозможные целые элементы поля K, делились бы на больший дивизор. Но в силу нашего предположения этот идеал совпадает с $\mathfrak{a}_1$. Таким образом, элемент z p-делится на β

$$cz = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_s v_s, \tag{3}$$

где $(c, p) = 1$. Для остальных строк формулы (1) мы тоже получим

аналогичные равенства

$$c_1 z = \alpha_1 v_{11} + \alpha_2 v_{21} + \cdots + \alpha_s v_{s1}, \qquad (3_1)$$

$$c_2 z = \alpha_1 v_{12} + \alpha_2 v_{22} + \ldots + \alpha_s v_{s2}, \qquad (3_2)$$

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

где $(c_1, p_1) = 1$, $(c_2, p_2) = 1$ и т. д.

Элементы p, p_1, $\cdots$ являются единственными простыми делителями элемента D, общего наибольшего делителя норм $N(\alpha_1)$, $N(\alpha_2)$, $\ldots$ $N(\alpha_s)$. Поскольку каждая из этих норм входит в идеал $\mathfrak{a}_1$, это имеет место также относительно D. Входит в идеал $\mathfrak{a}_1$ и произведение Dz, в силу чего имеет место представление

$$Dz = \alpha_1 w_1 + \alpha_2 w_2 + \cdots + \alpha_s w_s. \qquad (4)$$

Элементы D, c, c_1, ... имеют общим наибольшим делителем 1, так как D есть произведение степеней элементов p_i, а каждый p_i взаимно прост с одним из c_i. Отсюда следует, что неопределенное уравнение

$$cx + c_1 x_1 + \cdots + Dy = 1 \qquad (5)$$

имеет решение в целых элементах поля k. Умножая каждое из равенств (3_i) соответственно на x_i, (4) — на y и складывая, мы, в силу (5), будем иметь

$$z = \alpha_1 (v_1 x + v_{11} x_1 + \cdots + w_1 y) + \alpha_2 (v_2 x + v_{21} x_1 + \cdots + w_2 y) + \cdots$$

Это равенство показывает, что элемент z входит в идеал $\mathfrak{a}_1$, что и т. д.

Эквивалентность понятий идеала и дивизора позволяет ввести понятие произведения идеалов при помощи дивизоров, чем достигается бо́льшая простота и естественность теории.

ЛИТЕРАТУРА

1. Е. И. Золотарев. Теория целых комплексных чисел с приложением к интегральному исчислению. СПб., 1874. См. также Полное собр. соч., вып. I, Ленинград, 1931, стр. 161—360.
2. И. И. Иванов. Целые комплексные числа. СПб., 1891.
3. И. И. Иванов. К теории целых комплексных чисел. Прилож. к 72 тому Зап. Имп. Акад. Наук, № 9, стр. 1—14, 1893.
4. Ю. Сохоцкий. Начало общего наибольшего делителя в применении к теории делимости алгебраических чисел. СПб., 1893.
5. Н. Г. Чеботарев. Новое обоснование теории идеалов (по Золотареву). Изв. Каз. ФМО (2), 25 (1925), стр. 1—14.
6. Н. Г. Чеботарев. Основы теории Галуа, т. 2. ГТТИ, Л.—М., 1937.
7. G. Dirihlet. Vorlesungen über Zahlentheorie. Herausgegeben von R. Dedekind. 4-te Aufl., Braunschweig, 1894, Supplement XI.
8. L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Journ. f. reine und angew. Math., 92 (1881).
9. N. Tschebotaröw. On the foundation of the theory of ideals. Amer. Math. Monthly.
10. G. Zolotareff. Sur la theorie des nombres complexes. Journ. de math. pures et appl. (3). 6 (1880), стр. 51—84, 129—166.

К ЗАДАЧЕ НАХОЖДЕНИЯ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ С НАПЕРЕД ЗАДАННОЙ ГРУППОЙ

(Изв. КФМО **1** (1926), стр. 26—32)

Задача нахождения алгебраических уравнений с наперед заданной группой Галуа была разрешена впервые в общем виде Гильбертом для случая симметрических и знакопеременных групп [1]. Его метод представляет собою скорее «Existenzbeweis», так как основывается на теореме, что если какое-нибудь алгебраическое уравнение относительно нескольких переменных неприводимо, то можно для одних из этих переменных подыскать такие значения, чтобы после подстановки уравнение осталось неприводимым относительно остальных переменных, в области, составленной из коэффициентов уравнения найденных значений и еще произвольно заданных величин.

М. Бауэр [2] решил задачу для симметрических групп способом, действительно выполнимым на практике. Именно, он воспользовался теоремой Дедекинда [3] о связи между разложением левой части уравнения на неприводимые по простому модулю множители и цикленным составом подстановок его группы Галуа. Его метод построения был недавно упрощен И. Шуром и О. Перроном [4].

Э. Нётер [5] решила задачу для случая, когда некоторая система функций, зависящих от заданной группы, имеет так называемый *рациональный базис* (о нем будет речь ниже). При этом она тоже пользуется теоремой Гильберта, т. е. ограничивается «Existenzbeweis'ом».

Цель настоящей статьи — показать, что метод Бауэра допускает модификацию, благодаря которой он позволяет получить все возможные уравнения без аффекта (т. е. с симметрической группой), и что этот же метод позволяет решить задачу для группы, допускающей рациональный базис, и даже еще для более общих случаев, причем построение искомых уравнений выполнимо при помощи конечного (т. е. которое сразу может быть указано для каждой группы) числа действий.

Я предпосылаю изложению этого метода доказательство теоремы Дедекинда, проведенное без помощи теории идеалов. Подобное доказательство было также предложено И. Шуром (не могу указать места, где оно напечатано).

§ 1

Теорему Дедекинда можно формулировать так. Если неприводимое уравнение степени n

$$f(x) = x^n + p_1 x^{n-1} + \cdots + p_{n-1} x + p_n = 0 \qquad (1)$$

разлагается по простому модулю p, не входящему в дискриминант уравнения (1), на k неприводимых множителей

$$f(x) \equiv f_1(x) \cdot f_2(x) \cdot \cdots f_k(x) \pmod{p} \qquad (2)$$

степеней соответственно $n_1, n_2, \ldots, n_k$ $(n_1 + n_2 + \ldots + n_k = n)$, то в группе Галуа уравнения (1) содержится подстановка *цикленного типа* $(n_1, n_2, \ldots, n_k)$, т. е. состоящая из циклов порядков $n_1, n_2, \ldots, n_k$.

Доказательство будет состоять из двух частей. Во-первых, мы покажем, что подстановка упомянутого типа содержится в группе Галуа сравнения (2). Во-вторых, будет доказано, что можно так занумеровать корни уравнения (1) и сравнения (2), что группа сравнения (2) будет делителем группы уравнения (1).

1) Предварительно покажем, что корни сравнения (2) можно рассматривать как элементы поля (=область=корпус=Körper). В случае неприводимого сравнения это вытекает из теории мнимостей Галуа. В случае же $k > 1$ заметим, что все полиномы $f_1(x), f_2(x), \cdots, f_k(x)$ различны по модулю p, так как p взаимно просто с дискриминантом уравнения (1). Далее, корни сравнений $f_1(x) \equiv 0$, $f_2(x) \equiv 0, \ldots,$ $f_k(x) \equiv 0 \pmod{p}$ удовлетворяют соответственно сравнениям

$$x^{p^{n_1}} - x \equiv 0, \quad x^{p^{n_2}} - x \equiv 0, \ldots, \quad x^{p^{n_k}} - x \equiv 0 \pmod{p}. \qquad (3)$$

Полином $x^{p^N} - x$, где N — наименьшее кратное чисел $n_1, n_2, \cdots, n_k$, делится на все полиномы $x^{p^{n_i}} - x$ $(i = 1, 2, \ldots, k)$, так как $x^{p^N} - x = (x^{p^N - 1} - 1)x$, $x^{p^{n_i}} - x = (x^{p^{n_i - 1}} - 1)x$ и $p^N - 1$ делится на $p^{n_i} - 1$. Поэтому если мы обозначим через α один из первообразных корней сравнения

$$x^{p^N} - x \equiv 0 \pmod{p}, \qquad (4)$$

то все корни сравнений $f_i(x) \equiv 0 \pmod{p}$ $(i = 1, 2, \ldots, k)$ рационально выразятся через α, т. е. будут элементами поля $K(\alpha)$ мнимостей Галуа, и при действиях над корнями сравнений $f_i(x) \equiv 0 \pmod{p}$ получается поле, являющееся, вообще говоря, частью $K(\alpha)$.

Установив это обстоятельство, мы можем представить все корни сравнения (2) в виде следующей системы:

$$x_1, x_1^p, \ldots, x_1^{p^{n_1 - 1}}; \quad x_2, x_2^p, \ldots, x_2^{p^{n_2 - 1}}; \quad \ldots; \quad x_k, x_k^p, \ldots, x_k^{p^{n_k - 1}}. \qquad (5)$$

Докажем, что группа Галуа сравнения (2) заключает в себе подстановку

$$\left(x_1, x_1^p, \ldots, x_1^{p^{n_1-1}}\right)\left(x_2, x_2^p, \ldots, x_2^{p^{n_2-1}}\right)\ldots\left(x_k, x_k^p, \ldots, x_k^{p^{n_k-1}}\right). \quad (6)$$

Действительно, производство этой подстановки равносильно возведению в p-ую степень каждого из корней. Возьмем любое соотношение между корнями сравнения (2)

$$\Pi(x_1, x_2, \ldots, x_n) \equiv 0 \pmod p \quad (7)$$

и возведем в p-ую степень каждый из корней. Тогда в силу теоремы Шёнемана

$$\Pi(x_1^p, x_2^p, \ldots, x_n^p) \equiv [\Pi(x_1, x_2, \cdots, x_n)]^p \equiv 0 \pmod p, \quad (8)$$

т. е. соотношение не нарушается, ч. и т. д.

2) Постараемся теперь занумеровать корни (1) и (2) так, чтобы группа (2) была делителем группы (1). Чтобы найти группу (1), надо рассмотреть величину

$$\xi = t_1 x_1 + t_2 x_2 + \ldots + t_n x_n,$$

где $t_1, t_2, \ldots, t_n$ — неопределенные переменные, и построить неприводимое уравнение

$$F(\xi) = 0, \quad (9)$$

которому удовлетворяет ξ. Этому уравнению будут также удовлетворять величины типа

$$\xi_i = t_1 x_{\alpha_1} + t_2 x_{\alpha_2} + \cdots + t_n x_{\alpha_n},$$

где

$$\begin{pmatrix} 1, & 2, & 3, \ldots, & n \\ \alpha_1, & \alpha_2, & \alpha_3, \ldots, & \alpha_n \end{pmatrix} \quad (10)$$

некоторые подстановки. Совокупность всех подстановок (10) и составляет группу Галуа [6].

Таким образом, чтобы узнать, принадлежит ли какая-нибудь подстановка типа (10) к группе Галуа уравнения (1), надо образовать соответствующую ей величину $\xi_i = t_1 x_{\alpha_1} + t_2 x_{\alpha_2} + \cdots + t_n x_{\alpha_n}$ и выразить рационально ξ_i через $\xi, t_1, t_2, \ldots, t_n$, что возможно в силу нормальности (9). Пусть $\xi_i = \varphi_i(\xi)$. Тогда если подстановка (10) входит в группу Галуа, то полином $F(\varphi_i(u))$ должен делиться на $F(u)$; в противном случае он не будет делиться.

Обратимся теперь к сравнению (2). Чтобы найти его группу, составим, действуя с теми же числами, сравнение

$$F(\xi) \equiv 0 \pmod p, \quad (11)$$

которому удовлетворяет $\overline{\xi} = t_1 \overline{x_1} + t_2 \overline{x_2} + \ldots + t_n \overline{x_n}$. Это сравнение

будет иметь те же коэффициенты, что и уравнение (9). Но оно может и не быть неприводимым по модулю p.

Пусть $x_i = \psi_i(\xi)\,(i = 1, 2, \ldots, n)$ будут рациональные выражения x через ξ. Как известно, в знаменателях этих выражений может быть только дискриминант уравнения (9), т. е. некоторый полином от переменных $t_1, t_2, \ldots, t_n$, который можно представить в таком виде:

$$\Pi\left((t_1 x_{\alpha_1} + t_2 x_{\alpha_2} + \ldots + t_n x_{\alpha_n}) - (t_1 x_{\beta_1} + t_2 x_{\beta_2} + \ldots + t_n x_{\beta_n})\right)^2.$$

Если бы все его коэффициенты делились на p, то это означало бы, что сравнение (11) имеет кратные корни и что поэтому, прибавляя к его коэффициентам надлежащие кратности p, можно было бы добиться того, чтобы какие-нибудь из его корней были равны между собой, например

$$t_1 \bar{x}_{\alpha_1} + t_2 \bar{x}_{\alpha_2} + \ldots + t_n \bar{x}_{\alpha_n} = t_1 \bar{x}_{\beta_1} + t_2 \bar{x}_{\beta_2} + \ldots + t_n \bar{x}_{\beta_n},$$

что в силу неопределенности переменных влекло бы за собой

$$\bar{x}_{\alpha_1} = \bar{x}_{\beta_1},\ \bar{x}_{\alpha_2} = \bar{x}_{\beta_2},\ \ldots,\ \bar{x}_{\alpha_n} = \bar{x}_{\beta_n},$$

что указывало бы на кратность корней сравнения (2).

Итак, в знаменателях выражений $\psi_i(\xi)$ будут стоять полиномы, имеющие взаимно простые с p коэффициенты. Если в качестве $\bar{\xi}$ взять один из корней сравнения (11), то величины $\psi_i(\bar{\xi})$ будут удовлетворять сравнению (2) (т. е. полиномы $f(\psi_i(\bar{\xi}))$ будут делиться по модулю p на $F(\bar{\xi})$).

Введем следующую нумерацию корней $\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$: пусть, если $x_i = \psi_i(\xi)$, то $\bar{x}_i = \psi_i(\bar{\xi})$. Из этих выражений составим функции:

$$\xi_i = t_1 x_{\alpha_1} + t_2 x_{\alpha_2} + \ldots + t_n x_{\alpha_n} = t_1 \psi_{\alpha_1}(\xi) + t_2 \psi_{\alpha_2}(\xi) + \cdots + t_n \psi_{\alpha_n}(\xi) = \varphi_i(\xi),$$

$$\bar{\xi}_i = t_1 \bar{x}_{\alpha_1} + t_2 \bar{x}_{\alpha_2} + \ldots + t_n \bar{x}_{\alpha_n} = t_1 \psi_{\alpha_1}(\bar{\xi}) + t_2 \psi_{\alpha_2}(\bar{\xi}) + \ldots + t_n \psi_{\alpha_n}(\bar{\xi}) = \varphi_i(\bar{\xi}).$$

Пусть $\xi_i = \varphi_i(\xi)\,(i = 1, 2, \ldots, N)$ будет полная система корней уравнения (9) (N — его степень). Тогда $\bar{\xi}_i = \varphi_i(\bar{\xi})\,(i = 1, 2, \cdots, N)$ будут корнями сравнения (11). Других корней сравнение (11) иметь не может, так как сравнения N-ой степени не могут иметь более N корней. Из них корнями неприводимого сравнения, которому удовлетворяет $\bar{\xi}$, будет, вообще говоря, только часть. Но группа уравнения (1) переводит ξ во все величины $\xi_1, \xi_2, \ldots, \xi_N$. Группа же сравнения (2) переводит ξ в другие корни неприводимого сравнения, которому удовлетворяет ξ, т. е. в часть величин ряда $\bar{\xi}_1, \bar{\xi}_2, \ldots, \bar{\xi}_N$. Но так как переход (ξ, ξ_i) вполне определяет собой подстановку между

$x_1, x_2, \ldots, x_n$, то группа Галуа сравнения (2) при нашем способе нумерации корней является делителем группы Галуа уравнения (1), ч. и т. д.

§ 2

Теорема Дедекинда дает возможность строить уравнения, в группу которых входят подстановки заданного цикленного типа.

Пусть нам заданы несколько цикленных типов подстановок и пусть один из этих типов определяется порядками $n_1, n_2, \ldots, n_k$ своих циклов. Возьмем какое-нибудь простое число p (мы наложим на p ограничения, о которых будет речь ниже) и составим k неприводимых по модулю p полиномов степеней $n_1, n_2, \ldots, n_k$. Пусть это будут $f_1(x), f_2(x), \ldots, f_k(x)$ и пусть их произведение равно

$$f_1(x) f_2(x) \ldots f_k(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n. \qquad (1)$$

Если теперь коэффициенты какого-нибудь уравнения

$$F(x) = x^n + A_1 x^{n-1} + \ldots + A_{n-1} x + A_n = 0 \qquad (2)$$

будут удовлетворять сравнениям

$$A_1 \equiv a_1, A_2 \equiv a_2, \ldots, A_n \equiv a_n \pmod{p},$$

то группа уравнения (2) будет, в силу теоремы Дедекинда, содержать в своей группе подстановку, состоящую из циклов $n_1, n_2, \ldots, n_k$-го порядков.

Если задано несколько (m) цикленных типов, то возьмем столько же простых чисел $p^{(1)}, p^{(2)}, \ldots, p^{(m)}$ и найдем для каждого $p^{(i)}$, поступая как при составлении (1), коэффициенты $a_1^{(i)}, a_2^{(i)}, \ldots, a_n^{(i)}$, а затем найдем полином $F(x)$, коэффициенты которого $A_1, A_2, \ldots, A_n$ удовлетворяли бы следующим сравнениям:

$$\begin{aligned}
&A_1 \equiv a_1^{(1)}, \ A_2 \equiv a_2^{(1)}, \ldots, \ A_n \equiv a_n^{(1)} \pmod{p^{(1)}}, \\
&A_1 \equiv a_1^{(2)}, \ A_2 \equiv a_2^{(2)}, \ldots, \ A_n \equiv a_n^{(2)} \pmod{p^{(2)}}, \qquad (3) \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&A_1 \equiv a_1^{(m)}, \ A_2 \equiv a_2^{(m)}, \ldots, \ A_n \equiv a_n^{(m)} \pmod{p^{(m)}}.
\end{aligned}$$

Упомянутое нами ограничение для выбора простых чисел $p^{(i)}$ заключается в следующем. Предположим, что среди показателей $n_1, n_2, \ldots, n_k$ встречается l_i равных одному и тому же числу n_i. Тогда должно существовать по крайней мере l_i различных неприводимых по модулю p полиномов n_i-ой степени. Но число таких полиномов равно

$$\frac{1}{n_i} g(n_i) = \frac{1}{n_i}\left[p^{n_i} - \sum_{d \mid n_i} p^{\frac{n_i}{d}} - \sum_{\substack{d_1 \mid n_i \\ d_2 \mid n_i}} p^{\frac{n_i}{d_1 d_2}} - \ldots\right].$$

Поэтому должно иметь место неравенство

$$l_i \leqslant \frac{1}{n_i}\, g(n_i). \tag{4}$$

Эти неравенства наверное будут удовлетворены, если

$$p \geqslant n, \tag{5}$$

так как очевидно $g(n_i)$ делится на p и потому $g(n_i) \geqslant p$ и, кроме того,

$$l_i n_i \leqslant n.$$

§ 3

Изложенный в § 2 прием дает возможность строить уравнения без аффекта. Для этого нужно взять в качестве заданных подстановок цикл n-го порядка, цикл $(n-1)$-го порядка и транспозицию. В самом деле, группа, содержа цикл n-го порядка, будет транзитивна Содержа транспозицию, она должна быть в силу известной теоремы или симметрической, или импримитивной. Но импримитивная группа не может содержать цикла $(n-1)$-го порядка. Действительно, занумеруем корни так, чтобы этот цикл имел вид: (1) (23... n). Допустим, что группа импримитивна, и пусть 1, $\alpha_2, \alpha_3, \ldots, \alpha_m$ будет ее система импримитивности, в которой находится 1. Согласно определению импримитивности, подстановка (1) (23... n) должна перемещать цифры 1, $\alpha_2, \alpha_3, \ldots, \alpha_m$ между собой, т. е. содержать циклы порядка $< m$. Это противоречие доказывает теорему.

М. Бауэр [2] брал вместо циклов $(n-1)$-го порядка циклы порядка p, где p — простое число, причем $\frac{n}{2} < p < n$, а вместо циклов n-го порядка применял эйзенштейнов критерий неприводимости. Настоящий метод позволяет быть уверенным, что при построении таблиц уравнений без аффекта ни одно уравнение без аффекта не будет пропущено, если достаточно продолжить таблицы. Действительно, Фробениус [7] доказал теорему, обратную теореме Дедекинда:

Если группа Галуа уравнения (1) § 1 содержит подстановку цикленного типа $(n_1, n_2, \ldots, n_k)$, то существует бесчисленное множество таких простых чисел p, что соответствующее сравнение (2) § 1 распадается на неприводимые по модулю p множители степеней $n_1, n_2, \ldots, n_k$.

Таким образом, всякое уравнение без аффекта содержит подстановки трех указанных нами цикленных типов, а потому в силу упомянутой теоремы существует бесчисленное множество простых модулей p, по которым левая часть этого уравнения: 1) остается неприводимой, 2) разлагается на линейную функцию и полином $(n-1)$-ой степени, 3) разлагается на квадратичный полином и $n-2$

линейных функций. Поэтому, продвигаясь в построении уравнений без аффекта, мы рано или поздно придем и к этому уравнению.

§ 4

Задача построения уравнений с наперед заданной (отличной от симметрической) группой встречает ту трудность, что можно построить уравнения, в группу которых входили бы подстановки заданных цикленных типов, но при этом невозможно гарантировать, что в нее не войдут подстановки цикленных типов, не встречающихся в заданной группе. Таким образом, задачу можно формулировать так: пусть $P = p^{(1)} \cdot p^{(2)} \cdots p^{(m)}$ будет произведение выбранных нами простых модулей, и пусть $a_1, a_2, \ldots, a_n$ — представители классов по модулю P, подобранные так, чтобы уравнение

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0 \qquad (1)$$

имело группу, содержащую подстановки заданных цикленных типов. Пусть $z(x_1, x_2, \ldots, x_n)$ будет принадлежащая к заданной группе функция и пусть

$$F(z) = z^k + b_1 z^{k-1} + \cdots + b_{k-1} z + b_k = 0 \qquad (2)$$

будет уравнение, которому удовлетворяет z. Коэффициенты $b_1, b_2, \ldots, b_k$ являются целыми рациональными функциями от $a_1, a_2, \ldots, a_n$. Сравнение

$$F(z) \equiv 0 \qquad (3)$$

по каждому из модулей $p^{(1)}, p^{(2)}, \ldots, p^{(m)}$ и, следовательно, по модулю их произведения P должно иметь рациональный корень. Если мы вместо $a_1, a_2, \ldots, a_n$ возьмем соответственно $A_1 = a_1 + \alpha_1 P$, $A_2 = a_2 + \alpha_2 P, \ldots, A_n = a_n + \alpha_n P$, то $b_1, b_2, \cdots, b_k$ превратятся в $B_1, B_2, \ldots, B_k$, которые являются целыми рациональными функциями от $\alpha_1, \alpha_2, \ldots, \alpha_n$. Сравнение

$$\overline{F}(z) = z^k + B_1 z^{k-1} + \cdots + B_{k-1} z + B_k \equiv 0 \pmod{P} \qquad (4)$$

будет иметь рациональный корень при всех значениях $\alpha_1, \alpha_2, \ldots, \alpha_n$. Мы решили бы главную часть задачи, если бы сумели подобрать $\alpha_1, \alpha_2, \ldots, \alpha_n$ так, чтобы *уравнение* $\overline{F}(z) = 0$ имело рациональный корень.

Могло бы, однако, случиться, что заданная группа имеет подгруппу, содержащую все цикленные типы заданной группы. В этом случае мы представим группу, как транзитивную группу подстановок, порядок которой равен числу переставляемых букв (степени). Для этого достаточно обозначить каждый элемент S группы особой буквой a_s и принять $T = \begin{pmatrix} a_{s_1}, & a_{s_2}, & \ldots, & a_{s_t} \\ a_{s_1 T}, & a_{s_2 T}, & \ldots, & a_{s_t T} \end{pmatrix}$. Вся подгруппа будет при таком

представлении интранзитивна. В то же время мы введем еще один простой модуль $p^{(m+1)}$, чтобы при его помощи ввести Эйзенштейнов критерий неприводимости.

Задача решается очень просто в том случае, когда функции $a_1(x_1, \ldots, x_n)$, $a_2(x_1, \ldots, x_n)$, $\ldots$, $a_n(x_1, \ldots, x_n)$; $z(x_1, \ldots, x_n)$ обладают *рациональным базисом*, т. е. когда существуют такие рациональные функции от них $\zeta_1, \zeta_2, \ldots, \zeta_n$, через которые рационально выражаются все функции $a_1, a_2, \ldots, a_n; z$. Задача нахождения таких функций была решена для случая $n = 1$ Люротом [8]. Кастельнуово решил задачу для случая $n = 2$. Но уже для случая $n = 3$ Энриквес [9] показал на примере, что эта задача не всегда имеет решение.

Итак, рассмотрим случай, когда $\zeta_1, \zeta_2, \ldots, \zeta_n$ найдены. Тогда необходимым и достаточным условием того, что группа уравнения (1) является заданной группой или ее делителем, служит рациональность величин $\zeta_1, \zeta_2, \ldots, \zeta_n$, которые не зависят друг от друга. Вместе с тем, если мы наметим цикленные типы, характеризующие группу, и найдем соответствующие им классы $a_1, a_2, \ldots, a_n$ по модулю P, то сравнение (3) должно будет иметь рациональный корень, который определяет собой класс величины z по модулю P. Если теперь мы подставим значения $a_1, a_2, \ldots, a_n$; z внутри этих классов в выражения $\zeta_i(a_1, a_2, \ldots, a_n; z)$ $(i=1, 2, \ldots, n)$, то получим для последних значения $\zeta_1, \zeta_2, \ldots, \zeta_n$, которые, будучи подставлены в выражения $a_i(\zeta_1, \zeta_2, \ldots, \zeta_n)$; $z(\zeta_1, \zeta_2, \ldots, \zeta_n)$ $(i = 1, 2, \ldots, n)$, дадут для $a_1, a_2, \ldots, a_n$; z значения, лежащие внутри первоначально выбранных классов. Вместе с тем эти значения будут связаны соотношением (2), так что они будут давать решение задачи. Конечно, если в заданной группе будет содержаться подгруппа, заключающая все циклы группы, то нам придется опять перейти к нормальному уравнению и применить критерий неприводимости Эйзенштейна.

Э. Нетер [5] решила задачу для этого же случая, но с применением теоремы Гильберта.

ЛИТЕРАТУРА

1. D. Hilbert. Journ. f. Math. **110**.
2. M. Bauer. Math. Ann. **64**.
3. Dedekind. Zur Theorie der Ideale. Gött. Nachr., 1894.
4. J. Schur u. O. Perron. Sitzber. Bayer. Akad., 1924.
5. E. Noether. Gleichungen mit vorgeschriebener Gruppe. Math. Ann. **78**.
6. Д. А. Граве. Основы алгебры, стр. 554.
7. Frobenius. Über Beziehungen u. s. w. Berl. Akad., 1896, стр. 689.
8. Lüroth. Beweis eines Satzes über rationale Curven. Math. Ann. **9**; Netto. Über einen Lüroth-Gordanschen Satz. Math. Ann. **46**; Castelnuovo. Sulla razionalita delle involutioni piane. Math. Ann. **44**.
9. Enriques. Rend. Linc., t. 21.

ИССЛЕДОВАНИЯ О ПЛОТНОСТЯХ ПРОСТЫХ ЧИСЕЛ. I

(STUDIEN ÜBER PRIMZAHLENDICTIGKEITEN. I)

О ГРАНИЦАХ, МЕЖДУ КОТОРЫМИ НАВЕРНОЕ ЛЕЖАТ ПРОСТЫЕ ЧИСЛА, ПРИНАДЛЕЖАЩИЕ К ЗАДАННОМУ ОТДЕЛУ ПОДСТАНОВОК

(Изв. КФМО **2** (1927), стр. 14—20)

Доказательство знаменитой теоремы Дирихле [1] о том, что существует бесконечное множество простых чисел, содержащихся в данной арифметической прогрессии $mx + a$, $(m, a) = 1$, основано на том факте, что ряд

$$\sum_{p \equiv a \pmod m} \frac{1}{p}$$

расходится. Поэтому оно не дает возможности судить о границах, в которых обеспечивается существование таких простых чисел. Этот пробел был заполнен Кронекером [2] и Мертенсом [3], которые произвели детальную оценку остаточного члена у всех рядов, встречающихся в доказательстве Дирихле.

Теперь задача Дирихле обобщена следующим образом. Пусть задано нормальное алгебраическое числовое поле $\mathfrak{R}$ степени n. Если $\mathfrak{p}$ — простой идеал, не входящий в дискриминант поля $\mathfrak{R}$, то говорят, что $\mathfrak{p}$ *принадлежит* к подстановке S, если для каждого элемента x поля $\mathfrak{R}$ имеет место

$$x^p \equiv x \,|\, S \qquad (\mathrm{mod}\ \mathfrak{p}),$$

где $\mathfrak{p}$ — делитель простого рационального числа p. S входит в группу Галуа $\mathfrak{G}$ поля $\mathfrak{R}$. Говорят также, что p принадлежит к *классу подстановок*, соответствующему подстановке S, т. е. к совокупности подстановок вида TST^{-1}, где T пробегает все подстановки группы $\mathfrak{G}$. Возникает вопрос, принадлежит ли к заданному классу подстановок группы $\mathfrak{G}$ бесконечное множество простых чисел. Кронекер [4] доказал существование такого множества для тождественной подстановки; Фробениус [5] решил этот вопрос для *отдела* подстановок, т. е. для совокупности типа TS^vT^{-1} (T пробегает все подстановки группы $\mathfrak{G}$, v пробегает все числа, простые с порядком S); я полностью решил этот вопрос [6, 7]; Шрайер [8] существенно упростил изложение.

Доказательство этой теоремы основывается на исследовании бесконечного ряда вида

$$\sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}$$

в окрестности $s = 1$. Против этого доказательства можно выдвинуть то же возражение, что и против доказательства Дирихле для арифметических прогрессий. Восполнить этот пробел и является целью настоящей работы. Для этого я ввожу в обычное доказательство небольшую модификацию тем, что, следуя методе Кронекера, рассматриваю *конечные* ряды вида

$$\sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}.$$

В настоящей первой части этой работы я решаю указанную задачу только для отделов подстановок.

§ 1. Уточнение формулы Кронекера

Пусть задано произвольное алгебраическое числовое поле $\Re$. Рассмотрим все его простые идеалы $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_k$, нормы которых не превосходят данного целого положительного числа x. Имеет место равенство

$$\frac{1}{\prod_{\nu=1}^{k}(1 - N\mathfrak{p}_\nu^{-s})} = \sum_{N\mathfrak{a} \leqslant x} N\mathfrak{a}^{-s} + \sum_{N\mathfrak{a} > x} c_{\mathfrak{a}} N\mathfrak{a}^{-s}, \tag{1}$$

где $c_{\mathfrak{a}} = 1$ или 0, смотря по тому, разлагается $\mathfrak{a}$ в произведение степеней простых идеалов с нормой $\leqslant x$ или нет. Соберем теперь все идеалы с одной и той же нормой m и обозначим число их через $f(m)$. При этом мы заменим вторую сумму в правой части суммой с $\sum_{N\mathfrak{a} > x} N\mathfrak{a}^{-s}$, где $c = c(x, s)$ лежит между 0 и 1:

$$\frac{1}{\prod_{p < x}(1 - p^{-s})^{f(p)} \prod_{p^2 \leqslant x}(1 - p^{-2s})^{f(p^2)} \cdots \prod_{p^n < x}(1 - p^{-ns})^{f(p^n)}} =$$

$$= \sum_{m \leqslant x} \frac{f(m)}{m^s} + c \sum_{m > x} \frac{f(m)}{m^s}. \tag{2}$$

Для сумматорной функции

$$S(m) = f(1) + f(2) + \ldots + f(m), \tag{3}$$

которая дает число идеалов с нормой $\leqslant m$, Вебер [9] дал асимптотическое выражение

$$S(m) = ghm + \theta_m Rm^{1-\frac{1}{n}}, \tag{4}$$

где h есть число классов поля $\mathfrak{K}$, g обозначает объем так называемой норменной поверхности (Normfläche), разделенный на число w входящих в поле $\mathfrak{K}$ корней из единицы, $|\theta_m| \leqslant 1$ и R есть величина, определяемая формой норменной поверхности. Если мы введем в правую часть (2) выражение $f(m) = S(m) - S(m-1)$, то ее можно преобразовать следующим образом:

$$\sum_{m \leqslant x} \frac{f(m)}{m^s} + c \sum_{m > x} \frac{f(m)}{m^s} = \sum_{m \leqslant x} \frac{S(m) - S(m-1)}{m^s} + c \sum_{m > x} \frac{S(m) - S(m-1)}{m^s} =$$

$$= \sum_{m \leqslant x} S(m)\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) + \frac{S(x)}{(x+1)^s} - c\,\frac{S(x)}{(x+1)^s} +$$

$$+ c \sum_{m > x} S(m)\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right).$$

Теперь мы используем формулу (4) и введем новую функцию $\theta = \theta(x, s)$ $(|\theta| \leqslant 1)$

$$gh \sum_{m \leqslant x} m\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) + cgh \sum_{m > x}\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) +$$

$$+ R \sum_{m \leqslant x} \theta_m m^{1-\frac{1}{n}}\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) +$$

$$+ cR \sum_{m > x} \theta_m m^{1-\frac{1}{n}}\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) + (1-c)\,\frac{S(x)}{(1+x)^s}.$$

Но так как имеет место

$$\sum_{m \leqslant x} m\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) = \sum_{m \leqslant x} \frac{1}{m^s} - \frac{x}{(x+1)^s} = \int_1^x \frac{dx}{x^s} - c' - \frac{x}{(x+1)^s} =$$

$$= \frac{1}{s-1} - \frac{1}{s-1}\,\frac{1}{x^{s-1}} - c' - \frac{x}{(x+1)^s} \qquad (0 \leqslant c' \leqslant 1),$$

$$\sum_{m > x} m\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) = \sum_{m=x+1}^{\infty} \frac{1}{m^s} + \frac{x}{(m+1)^s} = +c'' + \frac{1}{s-1}\,\frac{1}{x^{s-1}} + \frac{x}{(x+1)^s},$$

$$\sum_{m \leqslant x} m^{1-\frac{1}{n}}\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) < \sum_{m \leqslant x}\left[\frac{1}{m^{s-1+\frac{1}{n}}} - \frac{1}{(m+1)^{s-1+\frac{1}{n}}} + \frac{1}{(m+1)^{s+\frac{1}{n}}}\right] <$$

$$< \frac{s+\frac{1}{n}}{s-1+\frac{1}{n}} \sum_{m \leqslant x}\left[\frac{1}{m^{s-1+\frac{1}{n}}} - \frac{1}{(m+1)^{s-1+\frac{1}{n}}}\right] \leqslant (n+1)\left[1 - \frac{1}{(x+1)^{s-1+\frac{1}{n}}}\right],$$

$(S \leqslant 1)$ (ср. [10])

$$\sum_{m \leqslant x} m^{1-\frac{1}{n}}\left(\frac{1}{m^s} - \frac{1}{(m+1)^s}\right) < \frac{s+\frac{1}{n}}{s-1+\frac{1}{n}} \sum_{m \leqslant x}\left(\frac{1}{m^{s-1+\frac{1}{n}}} - \frac{1}{(m+1)^{s-1+\frac{1}{n}}}\right) \leqslant$$

$$\leqslant (n+1)\,\frac{1}{x^{s-1+\frac{1}{n}}},$$

то выражение

$$\sum_{m \leqslant x} \frac{f(m)}{m^s} + c \sum_{m > x} \frac{f(m)}{m^s}$$

принимает следующий вид:

$$\sum_{m \leqslant x} \frac{f(m)}{m^s} + c \sum_{m > x} \frac{f(m)}{m^s} = \frac{gh}{s-1}\left[1 - \frac{\bar{c}}{x^{s-1}}\right] + \bar{\theta}A, \tag{5}$$

где

$$0 \leqslant \bar{c} \leqslant 1, \qquad -1 \leqslant \bar{\theta} \leqslant 1, \qquad A = 3gh + R(n+2). \tag{6}$$

Оценим в левой части формулы (2) сходящееся при $s = 1$ бесконечное произведение

$$\prod_{p^1 \leqslant x} (1 - p^{-2s})^{-f(p^1)} \cdot \prod_{p^2 \leqslant x} (1 - p^{-3s})^{-f(p^2)} \cdots \prod_{p^n \leqslant x} (1 - p^{-ns})^{-f(p^n)}.$$

Для этого присоединим к соответствующим множителям также и критические простые идеалы первой степени. Это произведение представимо в форме K^{δ}, где

$$K = \prod_{p' \text{ критич}} (1 - p'^{-1})^{-f(p')} \prod_{p^2 \leqslant x} (1 - p^{-2})^{-f(p^2)} \prod_{p^3 \leqslant x} (1 - p^3)^{-f(p^3)} \cdots$$

$$\cdots \prod_{p^n \leqslant x} (1 - p^{-n})^{-f(p^n)},$$

$$0 \leqslant \delta \leqslant 1.$$

Легко указать верхнюю границу для K

$$K < \Delta^n \left(\frac{\pi^2}{6}\right)^{\left[\frac{n}{2}\right]}, \tag{7}$$

где Δ — дискриминант поля $\mathfrak{R}$.

Тогда формула (2) примет вид

$$\prod_{p \leqslant x} (1 - p^{-s})^{-f(p)} = K^{-\delta}\left[\frac{gh}{s-1}\left(1 - \frac{\bar{c}}{x^{s-1}}\right) + \bar{\theta}A\right], \tag{8}$$

причем произведение распространяется на простые числа p, содержащие простые идеалы первой степени, $0 \leqslant \delta \leqslant 1$, $0 \leqslant \bar{c} \leqslant 1$, $-1 \leqslant \bar{\theta} \leqslant 1$

$$A = 3gh + R(n+2). \tag{9}$$

Формула (8) позволит нам определить, какую границу нужно взять для величины x, чтобы существовало не менее V простых чисел, содержащих простые идеалы $\mathfrak{p}$ первой степени с нормой $N(\mathfrak{p}) \leqslant x$.

Имеет место формула

$$\prod_{p < x} (1 - p^{-s})^{-f(p)} < \prod_{p \leqslant x} (1 - p^{-s})^{-n} < \sum_{m=2}^{V} \left(\frac{m}{m-1}\right)^n = V^n.$$

Наше требование будет выполнено, если мы удовлетворим следующему неравенству:

$$\frac{gh}{s-1}\left(1-\frac{1}{x^{s-1}}\right)>A+KV^n. \tag{10}$$

Но это неравенство будет удовлетворено, если мы возьмем $s-1<\frac{gh}{A+KV^n}$ и положим

$$x=\frac{1}{\left(1-\frac{A+KV^n}{gh}(s-1)\right)^{\frac{1}{s-1}}}. \tag{11}$$

Легко убедиться, что функция $x(s)$ обладает одним единственным минимумом в интервале $1<s<1+\frac{gh}{A+KV^n}$, который, очевидно, дает наилучшую оценку для x. Наше требование поэтому удовлетворится, если мы положим

$$x=4^{\frac{A+KV^n}{gh}}$$

Эта формула может быть значительно уточнена, если мы точнее оценим выражение

$$\prod_{k=1}^{V}(1-p_k^{-1})^{-1}.$$

Легко убедиться, что это выражение имеет порядок $\lg V$. Поэтому позволительно вместо V^n взять, например, $(2\lg V)^n$, если только V превосходит некоторую определенную границу. Однако отыскание этой границы лежит вне рамок настоящей работы.

§ 2. Простые числа, принадлежащие к отделам подстановок

Мы докажем теперь существование простых чисел, принадлежащих к *отделам* подстановок. Пусть $\mathfrak{K}$ — нормальное поле n-ой степени и S пусть будет подстановка порядка f его группы Галуа. Мы введем обозначение

$$[s,\ d]=\prod_{p\leqslant x}(1-p^{-s})^{-1}, \tag{12}$$

где произведение распространяется на простые числа, принадлежащие к отделу подстановки $S^{f/d}$ (d/f). Если мы применим формулу (8) ко всем подполям, принадлежащим ко всем $\mathfrak{d}_d$ ($\mathfrak{d}_d$ обозначает циклическую группу, порожденную подстановкой $S^{f/d}$), то получим (ср. [8], стр. 3, последняя формула)

$$\prod_{t/d}[s,\ t]^{\frac{n}{d j_t}}=K_d^{-\delta_k}\left[\frac{g_d h_d}{s-1}\left(1-\frac{c_d}{x^{s-1}}\right)+\theta_d A_d\right], \tag{13}$$

где j_t обозначает число сопряженных с $\mathfrak{d}_t$ подгрупп группы $\mathfrak{G}$.

Возвысим каждое из равенств (13) в степень $\frac{d}{n}\mu\left(\frac{f}{d}\right)$ и перемножим все полученные равенства. Получим

$$[s, f] = \prod_{d|f} K_d^{-\delta_d \frac{d}{n}\mu\left(\frac{f}{d}\right) j_f \left[\frac{g_d h_d}{s-1}\left(1 - \frac{c_d}{x^{s-1}}\right) + \theta_d A_d\right]^{j_f \frac{d}{n}\mu\left(\frac{f}{d}\right)}}. \quad (14)$$

Нам нужно указать такое значение для x, чтобы в интервале $1, \ldots, x$ находилось по меньшей мере V простых чисел, принадлежащих к отделу подстановки S. Для этого мы обозначим через d' (и соотв. d'') те делители d числа f, для которых

$$\mu\left(\frac{f}{d}\right) = 1$$

(и соотв. $= -1$). Тогда нам нужно удовлетворить следующим неравенствам:

$$\frac{g_{d'} h_{d'}}{s-1}\left(1 - \frac{1}{x^{s-1}}\right) - A_{d'} \geqslant \frac{g_{d'} h_{d'}}{s-1}(1-\varepsilon) \text{ для всех } d', \quad (15)$$

$$\frac{g_{d''} h_{d''}}{s-1} + A_{d''} \leqslant \frac{g_{d''} h_{d''}}{s-1}(1+\varepsilon) \text{ для всех } d'', \quad (16)$$

$$QV \leqslant \frac{1}{(s-1)^{j_f \frac{\varphi(f)}{n}}} \frac{(1-\varepsilon)^{\frac{j_f}{n}\Sigma_{d'}}}{(1+\varepsilon)^{\frac{j_f}{n}\Sigma_{d''}}}, \quad (17)$$

причем

$$Q = \prod_{d|f} K_{d'} \frac{(g_{d''} h_{d''})^{\frac{j_f}{n}\Sigma_{d'}}}{(g_{d'} h_{d'})^{\frac{j_f}{n}\Sigma_{d''}}}. \quad (18)$$

Мы можем заменить неравенство (17) более точным

$$QV \leqslant \frac{(1-\varepsilon)^{\frac{j_f}{n} D(f)}}{(s-1)^{\frac{j_f}{n}\varphi(f)}}, \quad (19)$$

где $D(f)$ есть сумма всех делителей f

$$f = \prod_{\nu} q_\nu^{\omega_\nu}, \qquad D(f) = \prod_{\nu} \frac{q_\nu^{\omega_\nu+1} - 1}{q_\nu - 1}. \quad (20)$$

Мы положим

$$1 - \varepsilon = (s-1)^{\varphi(f)/D(f)} (QV)^{n/j_f D(f)} = (s-1)^a W \qquad (a \leqslant 1). \quad (21)$$

Тогда неравенства (15) и (16) примут вид

$$\frac{g_d h_d}{s-1}\left[1 - (s-1)^a W - \frac{1}{x^{s-1}}\right] \geqslant A_d \text{ для всех } d/f, \quad (22)$$

откуда следует

$$x \geqslant \frac{1}{\left(1-\frac{A_d}{g_d h_d}(s-1)-(s-1)^a W\right)^{\frac{1}{s-1}}} \text{ для всех } d/f. \tag{23}$$

Положим

$$\left(\frac{A_d}{g_d h_d}+W\right)(s-1)^a = \frac{1}{2};$$

тогда неравенство

$$x \geqslant 2^{\frac{1}{s-1}} \tag{24}$$

будет точнее, чем неравенство (22). Поэтому, если мы возьмем

$$x = \operatorname{Max}\left\{2\left(\frac{2A_d}{g_d h_d}+2W\right)^{\frac{1}{a}}\right\} \text{ для всех } d/f, \tag{25}$$

то в интервале $1, \ldots, x$ наверное содержится V простых чисел, которые принадлежат к отделу подстановки S.

ЛИТЕРАТУРА

1. Lejeune-Dirichlet. Beweis des Satzes, dass... Werke, I, S. 13.
2. Kronecker. Vorlesungen über Zahlentheorie. Bearb. von K. Hensel. Lpz., 1901, стр. 452—492.
3. Mertens. Über Dirichlet's Beweis des Satzes, dass u. s. w. Sitzber. Wiener Akad. Bd. **106** (1897), Abth IIa, стр. 254—286.
4. Kronecker. Über die Irreducibilität von Gleichungen. Monatsber. Berl. Akad., 1880, стр. 156.
5. Frobenius. Über Beziehungen zwischen den Primidealen eines alg. Körpers und die Substitutionen seiner Gruppe. Sitzber. Berl. Akad., 1896, стр. 689—705.
6. Н. Чеботарев. Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок. Изв. Росс. А. Н., 1923, стр. 205—250 (Собр. соч., т. I, стр. 27—65).
7. N. Tschebotareff. Die Bestimmung der Dichtigkeit u. s. w. Math. Ann. **95**, 1925, стр. 191—228.
8. O. Schreier. Über eine Arbeit von Herrn Tschebotareff. Abh. Math. Sem. Hamb. **5**, 1926, стр. 1—6.
9. Weber. Lehrbuch der Algebra. Bd. 2. Braunschw., 1899, стр. 710—716.
10. Mertens. Über eine zahtentheoretische Function. Sitzber. Wien. Akad. **106**, стр. 779.

ИССЛЕДОВАНИЯ О ПЛОТНОСТЯХ ПРОСТЫХ ЧИСЕЛ. II

(STUDIEN ÜBER PRIMZAHLENDICHTIGKEITEN II).

О ГРАНИЦАХ, МЕЖДУ КОТОРЫМИ НАВЕРНОЕ ЛЕЖАТ ПРОСТЫЕ ЧИСЛА, ПРИНАДЛЕЖАЩИЕ К ЗАДАННОМУ КЛАССУ ПОДСТАНОВОК

(Изв. КФМО **3** (1927), стр 1—17)

В этой части моего исследования я намерен решить для классов подстановок ту же задачу, которую в первой части [1] решил для отделов подстановок. Использованный там метод, состоявший в том, что я просто давал более точные оценки в формуле Кронекера — Фробениуса, здесь отказывается служить вследствие того, что встречающаяся здесь логарифмическая функция многозначна в области комплексного переменного и оценка ее мнимой части представляет большие трудности. Поэтому я вынужден первоначально дифференцировать упомянутую формулу по s. Это как раз тот самый путь, которому следовали Кронекер и Мертенс в своих исследованиях об арифметических прогрессиях (цитированы в I части).

В недавно появившихся работах Артина [2,3] задача о простых числах, принадлежащих к данному классу подстановок, исследована в другом направлении; именно, он доказывает регулярность остаточного члена

$$P_1(s-1) = \sum_{p_1} p_1^{-s} - \frac{n_1}{n} \lg \frac{1}{s-1}$$

в окрестности $s = 1$.

§ 1. Вывод основной формулы

1. Рассмотрим произведение

$$\prod_{N\mathfrak{p} \leqslant x} \{1 - \chi(N\mathfrak{p})\, N\mathfrak{p}^{-s}\}^{-1}, \tag{1.1}$$

распространенное на все простые идеалы с нормой $\leqslant x$. Разлагая каждый его член по степеням $N\mathfrak{p}^{-s}$

$$\{1 - \chi(N\mathfrak{p})\, N\mathfrak{p}^{-s}\}^{-1} = 1 + \chi(N\mathfrak{p})\, N\mathfrak{p}^{-s} + \chi(N\mathfrak{p}^2)\ \ N\mathfrak{p}^{-2s} + \ldots$$

и производя умножение, мы получим

$$\prod_{N\mathfrak{p} \leqslant x} \{1 - \chi(N\mathfrak{p})\, N\mathfrak{p}^{-s}\}^{-1} = \sum_{Nm \leqslant x} \chi(Nm)\, Nm^{-s} + \sum_{Nm > x} c_{\mathfrak{p}}\, \chi(Nm)\, Nm^{-s}, \tag{2.1}$$

где $c_{\mathfrak{p}} = 1$ или $= 0$, смотря по тому, удовлетворяют ли простые идеальные множители $\mathfrak{p}$ идеала $\mathfrak{m}$ неравенству $N\mathfrak{m} \leqslant x$ или нет. Числа $c_{\mathfrak{m}}$, следовательно, независимы от s.

2. Построим логарифмическую производную от (2.1) по s

$$\sum_{N\mathfrak{p} \leqslant x} \frac{\chi(N\mathfrak{p}) \lg(N)}{N\mathfrak{p}^s - \chi(N\mathfrak{p})} =$$

$$= \frac{\sum_{N\mathfrak{m} < x} \chi(N\mathfrak{m}) \lg(N\mathfrak{m}) \cdot N\mathfrak{m}^{-s} + \sum_{N\mathfrak{m} > x} c_{\mathfrak{m}} \chi(N\mathfrak{m}) \lg(N\mathfrak{m}) N\mathfrak{m}^{-s}}{\sum_{N\mathfrak{m} \leqslant x} \chi(N\mathfrak{m}) N\mathfrak{m}^{-s} + \sum_{N\mathfrak{m} > x} c_{\mathfrak{m}} \chi(N\mathfrak{m}) N\mathfrak{m}^{-s}}. \qquad (3.1)$$

3. Пусть характеры $\chi(N\mathfrak{m})$ определены классами вычетов mod L в которых лежат соответствующие нормы $N\mathfrak{m}$. Полагая $N\mathfrak{m} = r + Lm$ $((r, L) = 1)$ и вводя вместо x величину $(L-1) + Lx$, мы преобразуем формулу (3.1) к виду

$$\sum_{v=1}^{n} \sum_{p^v \leqslant L(x+1)} \frac{\chi(p^v) \bar{f}(p^v) \lg p^v}{p^{vs} - \chi(p^v)} =$$

$$= \frac{\sum_{r=1}^{L-1} \chi(r) \left\{ \sum_{m \leqslant x} \frac{f(r+Lm) \lg(r+Lm)}{(r+Lm)^s} + c \sum_{m > x} \frac{f(r+Lm) \lg(r+Lm)}{(r+Lm)^s} \right\}}{\sum_{r=1}^{L-1} \chi(r) \left\{ \sum_{m \leqslant x} \frac{f(r+Lm)}{(r+Lm)^s} + c \sum_{m > x} \frac{f(r+Lm)}{(r+Lm)^s} \right\}}, \qquad (4.1)$$

где $f(m)$ есть число идеалов с абсолютной нормой m, а $\bar{f}(p^v)$ есть число простых идеалов с абсолютной нормой p^v.

Под c мы понимаем здесь и в последующем произвольную величину, лежащую между 0 и 1. Одинаковое обозначение c в различных местах формулы никоим образом не значит, что эти величины равны (ср. с обозначениями Ландау $O(x)$ и $o(x)$). Точно так же θ будет обозначать произвольную величину, расположенную между -1 и $+1$.

§ 2. Преобразование знаменателя правой части основной формулы

4. Сначала преобразуем выражение

$$\sum_{m \leqslant x} f(r+Lm)(r+Lm)^{-s} + c \sum_{m > x} f(r+Lm)(r+Lm)^{-s}. \qquad (1.2)$$

Для этого положим

$$S(r+Lm) = f(r) + f(r+L) + \ldots + f(r+Lm), \qquad (2.2)$$

откуда

$$f(r+Lm) = S(r+Lm) - S(r+L\overline{m-1}). \qquad (3.2)$$

Таким образом, $S(r+Lm)$ есть число идеалов, абсолютная норма которых может быть представлена в виде $r+Lx$, где $0 \leqslant x \leqslant m$.

5. Теперь обратимся к установленному мной прежде неравенству [4]. Число главных идеалов с нормой, равной $r+Lx$ $(x=0,1,\ldots,m)$, равно v (см. [4], стр. 203, формулы (33), (34)), умноженному на число точек сетки, удовлетворяющих неравенствам

$$|N(\omega_i{}^r + Lc_1\omega_1 + Lc_2\omega_2 + \ldots + Lc_n\omega_n)| \leqslant L(m+1), \tag{4.2}$$

$$0 \leqslant \xi_\alpha(\omega_i{}^r + Lc_1\omega_1 + Lc_2\omega_2 + \ldots + Lc_n\omega_n) < 1$$

$$(i=1,2,\ldots,v;\ \alpha=1,2,\ldots,\nu-1) \tag{5.2}$$

([4], стр. 206, формулы (47), (48)). Число это равно

$$gL(m+1) + \theta RL^{1-\frac{1}{n}}(m+1)^{1-\frac{1}{n}}$$

([4], стр. 206 и [1], стр. 16, формула (4)). Его можно представить еще так:

$$gLm + \theta RL^{1-\frac{1}{n}} m^{1-\frac{1}{n}},$$

если взять соответственно большее значение R.

Чтобы получить $S(r+Lm)$, нужно умножить это число еще на число $\bar{h}$ „допустимых классов“ ([4], стр. 208—209). При этом заметим, что для различных идеальных классов слагаемые могут иметь различные значения R. В этом случае мы возьмем за R его максимальное значение. Имеет место

$$v\bar{h} = \frac{\bar{\varphi}(L)}{\bar{F}} \frac{h}{w} = \frac{\bar{\varphi}(L)}{\bar{F}} h,$$

где $\bar{F}$ есть число норменных вычетов $\bmod L$, „допустимых в широком смысле“, $\bar{\varphi}(L)$ есть число всех взаимно простых с L вычетов $\bmod L$ в поле $\mathfrak{R}$.

Таким образом, для $S(r+Lm)$ мы получаем

$$S(r+Lm) = \frac{\bar{\varphi}(L)\,L}{\bar{F}} gh + \theta \frac{\bar{\varphi}(L)}{\bar{F}} RhL^{1-\frac{1}{n}} m^{1-\frac{1}{n}} = \gamma m + \theta\rho m^{1-\frac{1}{n}}, \tag{6.2}$$

где

$$\gamma = \frac{\bar{\varphi}(L)\,L}{\bar{F}} gh, \qquad \rho = \frac{\bar{\varphi}(L)}{\bar{F}} RhL^{1-\frac{1}{n}}. \tag{7.2}$$

6. Рассмотрим первую сумму в (1.2)

$$\sum_{m\leqslant x} \frac{f(r+Lm)}{(r+Lm)^s} = \sum_{m\leqslant x} \frac{S(r+Lm) - S(r+L\overline{m-1})}{(r+Lm)^s} =$$

$$= \sum_{m\leqslant x} S(r+Lm)\left\{\frac{1}{(r+Lm)^s} - \frac{1}{(r+L\overline{m+1})^s}\right\} + \frac{S(r+Lx)}{(r+L\overline{x+1})^s}. \tag{8.2}$$

Из (6.2) следует

$$\sum_{m\leqslant x}\frac{f(r+Lm)}{(r+Lm)^s}=\gamma\sum_{m\leqslant x}m\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L(m+1))^s}\right\}+$$

$$+\theta\rho\sum_{m\leqslant x}m^{1-\frac{1}{n}}\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L(m+1))^s}\right\}+c(\gamma+\theta\rho)\frac{1}{L}. \qquad (9.2)$$

7. Первая сумма равенства (9.2) преобразуется так:

$$\sum_{m\leqslant x}m\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L(m+1))^s}\right\}=\sum_{m=1}^{x}\frac{1}{(r+Lm)^s}-\frac{x}{(r+L(x+1))^s}=$$

$$=\int_1^x\frac{dz}{(r+Lz)^s}+\frac{c}{r+L}-\frac{x}{(r+L(x+1))^s}=$$

$$=\frac{1}{L(s-1)}\left\{\frac{1}{(r+L)^{s-1}}-\frac{1}{(r+Lx)^{s-1}}\right\}+\frac{c}{k+L}-\frac{c}{L}. \qquad (10.2)$$

Но имеют место соотношения

$$1-\frac{1}{(r+L)^{s-1}}=-(s-1)\int_{r+L}^{1}\frac{dz}{z^s}<(s-1)\int_1^{r+L}\frac{dz}{z}=(s-1)\lg(r+L), \qquad (11.2)$$

$$\frac{1}{x^{s-1}}-\frac{1}{(r+Lx)^{s-1}}=\frac{1}{x^{s-1}}\left\{1-\frac{1}{\left(\frac{r}{x}+L\right)^{s-1}}\right\}=$$

$$=\frac{s-1}{x^{s-1}}\int_1^{\frac{r}{x}+L}\frac{dz}{z^s}<\frac{s-1}{x^{s-1}}\lg\left(\frac{r}{x}+L\right)<(s-1)\lg(r+L). \qquad (12.2)$$

Подстановка в (10.2) дает

$$\sum_{m\leqslant x}m\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L(m+1))^s}\right\}=\frac{1}{L(s-1)}\cdot\left(1-\frac{1}{x^{s-1}}\right)+$$

$$+\theta\frac{\lg(r+L)}{L}+\frac{\theta}{(r+L)L}. \qquad (13.2)$$

8. Вторая сумма равенства (9.2) дает

$$\sum_{m\leqslant x}m^{1-\frac{1}{n}}\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+Lm+1)^s}\right\}=$$

$$=\sum_{m\leqslant x}m^{1-\frac{1}{n}}s\int_{r+Lm}^{r+L\overline{m+1}}\frac{dz}{z^{s+1}}<\frac{s}{L^{1-\frac{1}{n}}}\int_{r+L}^{r+L\overline{x+1}}\frac{dz}{z^{s+\frac{1}{n}}}=$$

$$=\frac{1}{L^{1-\frac{1}{n}}}\frac{s}{s+\frac{1}{n}-1}\left\{\frac{1}{(r+L)^{s+\frac{1}{n}-1}}-\frac{1}{(r+L\overline{x+1})^{s+\frac{1}{n}-1}}\right\}<$$

$$<\frac{n}{L^{1-\frac{1}{n}}}\left\{\frac{1}{\sqrt[n]{r+L}}-\frac{1}{\sqrt[n]{r+L\overline{x+1}}}\right\}<\frac{n}{L}. \qquad (14.2)$$

9. Таким образом, выражение (9.2), т. е. первая из сумм в (1.2), принимает вид

$$\frac{\gamma}{L(s-1)}\left(1-\frac{1}{x^{s-1}}\right)+\theta\left\{\gamma\frac{\lg(r+L)}{L}+\frac{\gamma}{(r+L)L}+\frac{\rho n}{L}\right\}+c\frac{\gamma}{L}+\theta\frac{\rho}{L}. \quad (15.2)$$

10. Аналогично преобразуется вторая сумма в (1.2)

$$\sum_{m>x}\frac{f(r+Lm)}{(r+Lm)^s}=\sum_{m>x}\frac{S(r+Lm)-S(r+L\overline{m-1})}{(r+Lm)^s}=$$

$$=\sum_{m>x}S(r+Lm)\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L\overline{m+1})^s}\right\}-\frac{S(r+Lx)}{(r+L\overline{x+1})^s}=$$

$$=\gamma\sum_{m>x}m\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L\overline{m+1})^s}\right\}+$$

$$+\theta\rho\sum_{m>x}m^{1-\frac{1}{n}}\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L\overline{m+1})^s}\right\}-c\frac{\gamma+\theta\rho}{L}. \quad (16.2)$$

11. Первая из сумм (16.2)

$$\sum_{m>x}m\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L\overline{m+1})^s}\right\}=\sum_{m=x+1}^{\infty}\frac{1}{(r+Lm)^s}+\frac{x}{(r+L\overline{x+1})^s}=$$

$$=\int_x^{\infty}\frac{dz}{(r+Lz)^s}-\frac{c}{(r+L\overline{x+1})^s}+\frac{x}{(r+L\overline{x+1})^s}=\frac{1}{L(s-1)}\cdot\frac{1}{(r+Lx)^{s-1}}-$$

$$-\frac{c}{r+Lx}+\frac{c}{L}=\frac{1}{L(s-1)}\frac{1}{x^{s-1}}+\frac{c\lg(r+L)}{L}-\frac{c}{r+Lx}+\frac{c}{L}\ [\text{ср. (11.2),(12.2)}]. \quad (17.2)$$

12. Вторая сумма в (16.2)

$$\sum_{m>x}m^{1-\frac{1}{n}}\left\{\frac{1}{(r+Lm)^s}-\frac{1}{(r+L\overline{m+1})^s}\right\}=$$

$$\leqq\sum_{m>x}m^{1-\frac{1}{n}}s\int_{r+Lm}^{r+L(m+1)}\frac{dz}{z^{s+1}}<\frac{s}{L^{1-\frac{1}{n}}}\int_{r+L(x+1)}^{\infty}\frac{dz}{z^{s+\frac{1}{n}}}=$$

$$=\frac{1}{L^{1-\frac{1}{n}}}\frac{s}{s+\frac{1}{n}-1}\frac{1}{(r+L(x+1))^{s+\frac{1}{n}-1}}<\frac{n}{L}. \quad (18.2)$$

13. Подстановка (17.2) и (18.2) в (16.2) дает

$$\sum_{m>x}\frac{f(r+Lm)}{(r+Lm)^s}=\frac{\gamma}{L(s-1)}\frac{1}{x^{s-1}}+c\frac{\gamma\lg(r+L)}{L}-\frac{c\gamma}{r+L}+$$

$$+\frac{c\gamma}{L}-c\frac{\gamma+\theta\rho}{L}+\theta\frac{\rho n}{L}. \quad (19.2)$$

14. Подстановка (15.2) и (19.2) в (1.2) дает

$$\sum_{m\leqslant x}\frac{f(r+Lm)}{(r+Lm)^s}+c\sum_{m>x}\frac{f(r+Lm)}{(r+Lm)^s}=\frac{\gamma}{L(s-1)}\left(1-\frac{c}{x^{s-1}}\right)+$$
$$+\theta\left\{\gamma\frac{\lg(r+L)}{L}+\frac{\gamma}{L(r+L)}+\frac{\rho n}{L}\right\}+\frac{c\gamma}{L}+\theta\frac{\rho}{L}-$$
$$-c\frac{\gamma\lg(r+L)}{L}+c\frac{\gamma}{r+L}-\frac{c\gamma}{L}+c\frac{\gamma}{L}+\theta\frac{(n+1)\rho}{L}=$$
$$=\frac{\gamma}{L(s-1)}\left(1-\frac{c}{x^{s-1}}\right)+\theta\left\{\frac{2\gamma\lg(r+L)}{L}+\frac{2\gamma}{r+L}+\frac{2\gamma}{L}+\frac{2(n+1)\rho}{L}\right\}=$$
$$=\frac{\gamma}{L(s-1)}\left(1-\frac{c}{x^{s-1}}\right)+\theta Ar, \qquad (20.2)$$

где γ не зависит от r.

§ 3. Оценка знаменателя правой части основной формулы

15. Мы вскоре увидим, что правую часть основной формулы легко оценить, если $\chi(r)$ — главные характеры. В противном же случае возникает некоторая трудность, состоящая в том, что главный член знаменателя исчезает. Чтобы преодолеть эту трудность, мы оценим знаменатель правой части основной формулы.

16. Мы исходим из формулы (2.1), которую на основании (3.1) и (20.2) преобразуем к виду

$$\prod_{p^v<L(x+1)}\{1-\chi(p^v)p^{-vs}\}^{-\overline{f}(p^v)}=$$
$$=\frac{\gamma}{L(s-1)}\sum_r\chi(r)+\theta\frac{\gamma\overline{F}}{L(s-1)}\frac{1}{x^{s-1}}+\theta\sum_r A_r. \qquad (1.3)$$

Те члены левой части, которые соответствуют простым идеалам $\mathfrak{p}$, для которых $N\mathfrak{p}=p^v$, $v>1$, можно представить в виде K^c ([1], стр. 17). Отсюда

$$K^c\prod_{p\leqslant L(x+1)}\{1-\chi(p)p^{-s}\}^{-\overline{f}(p)}=\frac{\gamma}{L(s-1)}\sum_r\chi(r)+$$
$$+\theta\frac{\gamma\overline{F}}{L(s-1)}\frac{1}{x^{s-1}}+\theta\overline{F}A_m, \qquad (2.3)$$

где A_m обозначает максимальную среди величин A_r и $\sum_r\chi(r)=\overline{F}$ или $=0$, смотря по тому, является $\chi(r)$ главным характером или нет.

17. Так как

$$\prod_\chi\{1-\chi(p)p^{-s}\}^{-1}=(1-p^{-s})^{-\overline{F}}\ (\text{если }\chi(p)=1)\ \text{или}=(1-p^{-\delta s})^{-\frac{\overline{F}}{\delta}},$$

где δ — наименьший показатель, для которого $\chi(p^\delta)=1$, то, перемно-

жая формулы (2.3) для всех характеров, мы получим

$$\prod_{p_1 \leqslant L(x+1)} (1-p_1^{-s})^{-\overline{F}\overline{f}(p_1)} \prod_{\substack{p \\ \delta \geqslant 2}} (1-p^{-\delta s})^{-\frac{\overline{F}\overline{f}(p)}{\delta}} =$$

$$= K^{-c\overline{F}} \left\{ \frac{\gamma \overline{F}}{L(s-1)} \left(1 - \frac{c}{x^{s-1}}\right) + \theta \overline{F} A_m \right\} \times \prod_{\chi \neq 1} \left\{ \theta \frac{\gamma \overline{F}}{L(s-1)} \frac{1}{x^{s-1}} + \theta \overline{F} A_m \right\}_{\chi}, \quad (3.3)$$

где все $p_1 \equiv 1 \pmod{L}$.

18. Второе из произведений в левой части (3.3) можно представить так (мы выделяем множители, соответствующие критическим числам):

$$\prod_{p \text{ критич.}} (1-p^{-s})^{-\overline{F}} \prod_{p\ (\delta \geqslant ?)} (1-p^{-\delta s})^{-\frac{\overline{F}\overline{f}(p)}{\delta}} =$$

$$= \Delta^{cn\overline{F}} \zeta(2)^{c\left[\frac{n}{2}\right]\overline{F}} = \Delta^{cn\overline{F}} \left(\frac{\pi^2}{6}\right)^{c\left[\frac{n}{2}\right]\overline{F}}. \quad (4.3)$$

Мы обозначим его через $H^{c\overline{F}}$.

19. Первое же из произведений левой части (3.3) распространено на все те некритические простые числа p_1 первой степени поля $\mathfrak{K}$, для которых

$$p_1 \equiv 1 \pmod{L}.$$

Произведение это мы получим также, если присоединим к $\mathfrak{K}$ некоторое круговое поле. Получившееся поле $\mathfrak{K}^*$ будет относительной степени $\overline{F}$ над $\mathfrak{K}$ (ср. [4], стр. 214—215). Применим к этому полю формулу (2.3), полагая $L = 1$ и принимая во внимание справедливое для простых чисел p_1 соотношение ([4], стр. 215)

$$\overline{f}^*(p_1) = \overline{f}(p_1)\overline{F}. \quad (5.3)$$

Получим

$$\prod_{p_1 \leqslant L(x+1)} (1-p_1^{-s})^{-\overline{F}\overline{f}(p_1)} = K^{*-c} \left\{ \frac{\gamma^*}{s-1} \left(1 - \frac{c}{x^{s-1}}\right) + \theta A^* \right\}. \quad (6.3)$$

Сравнивая правые части (3.3) и (6.3), получим

$$\left\{ \frac{\gamma^*}{s-1} \left(1 - \frac{c}{x^{s-1}}\right) + \theta A^* \right\} \left(\frac{K^*}{K^{\overline{F}} H^{\overline{F}}}\right)^{-c} = \left\{ \frac{\gamma \overline{F}}{L(s-1)} \left(1 - \frac{c}{x^{s-1}}\right) + \theta \overline{F} A_m \right\} \times$$

$$\times \prod_{\chi \neq 1} \left\{ \frac{\theta \gamma \overline{F}}{L(s-1)} \frac{1}{x^{s-1}} + \theta \overline{F} A_m \right\}_{\chi}. \quad (7.3)$$

20. Из формулы (7.3) можно получить искомую нижнюю оценку для основной формулы. Если мы возьмем произвольную систему характеров $\chi_1 \neq 1$, то из (7.3) следует

$$\left\{ \frac{\theta \gamma \overline{F}}{L(s-1)} \frac{1}{x^{s-1}} + \theta \overline{F}_1 A_m \right\}_{\chi_1} =$$

$$= \frac{\left\{\frac{\gamma^*}{s-1}\left(1-\frac{c}{x^{s-1}}\right)+\theta A^*\right\}\left(\frac{K^{\overline{F}}H^{\overline{F}}}{K^*}\right)^c}{\left\{\frac{\gamma^{\overline{F}}}{L(s-1)}\left(1-\frac{c}{x^{s-1}}\right)+\theta\overline{F}A_m\right\}\prod\limits_{\chi\neq 1}\left\{\frac{\theta\gamma^{\overline{F}}}{L(s-1)}\frac{1}{x^{s-1}}+\theta\overline{F}A_m\right\}_\chi} >$$

$$\gamma\neq\chi_1$$

$$> \frac{\gamma^*\left(1-\frac{1}{x^{s-1}}\right)-A^*(s-1)}{K^*\left\{\frac{\gamma^{\overline{F}}}{L}+\overline{F}A_m(s-1)\right\}\left\{\frac{\gamma^{\overline{F}}}{L(s-1)}\frac{1}{x^{s-1}}+A^m\right\}^{\overline{F}-2}}. \qquad (8.3)$$

21. Теперь выберем для s и x такие значения, для которых

$$\frac{1}{x^{s-1}} < \frac{\varepsilon}{2^{\overline{F}}}, \qquad (9.3)$$

$$\frac{1}{(s-1)x^{s-1}} < \frac{A_m L}{\gamma^{\overline{F}}}\frac{\varepsilon}{F}, \qquad (10.3)$$

$$(s-1) < \frac{\gamma^*}{A^*}\frac{\varepsilon}{2^{\overline{F}}}, \qquad (11.3)$$

$$(s-1) < \frac{\gamma}{LA_m}\frac{\varepsilon}{\overline{F}}. \qquad (12.3)$$

Тогда из (8.3) получится

$$\left\{\theta\frac{\gamma^{\overline{F}}}{L(s-1)}\frac{1}{x^{s-1}}+\theta\overline{F}A_m\right\}_{\chi_1} >$$

$$> \frac{\gamma^*}{K^*\frac{\gamma^{\overline{F}}}{L}A_m^{\overline{F}-2}}\frac{\left(1-\frac{\varepsilon}{\overline{F}}\right)}{\left(1+\frac{\varepsilon}{\overline{F}}\right)^{\overline{F}-1}} > R\left(1-\frac{\varepsilon}{\overline{F}}\right)^{\overline{F}} > R(1-\varepsilon) \qquad (13.3)$$

(ср. [4], стр. 217—218), где

$$R = \frac{\gamma^* L}{K^*\gamma^{\overline{F}}A_m^{\overline{F}-2}}. \qquad (14.3)$$

22. ε есть положительное число <1, которое точнее еще не определено. Чтобы определить искомые значения s и x, достаточно взять

$$s-1 < \mathrm{Min}\left\{\frac{\gamma^*}{A^*}\frac{\varepsilon}{2^{\overline{F}}}, \quad \frac{\gamma}{LA_m}\frac{\varepsilon}{\overline{F}}\right\}. \qquad (15.3)$$

Если величина $s-1$ уже определена, то далее положим

$$x > \mathrm{Max}\left\{\left(\frac{2^{\overline{F}}}{\varepsilon}\right)^{\frac{1}{s-1}}, \quad \left(\frac{\gamma^{\overline{F}^2}}{A_m L(s-1)}\right)^{\frac{1}{s-1}}\right\}. \qquad (16.3)$$

§ 4. Преобразование числителя правой части основной формулы

23. Преобразуем теперь выражение

$$\sum_{m\leqslant x}\frac{f(r+Lm)\lg(r+Lm)}{(r+Lm)^s}+c\sum_{m>x}\frac{f(r+Lm)\lg(r+Lm)}{(r+Lm)^s}. \qquad (1.4)$$

24. Подстановка (6.2) в первую сумму дает:

$$\sum_{m\leqslant x}\frac{f(r+Lm)\lg(r+Lm)}{(r+Lm)^s}=\sum_{m\leqslant x}\frac{\lg(r+Lm)}{(r+Lm)^s}\{S(r+Lm)-S(r+L(m-1))\}=$$

$$=\sum_{m\leqslant x}S(r+Lm)\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}+$$

$$+\frac{S(r+Lx)\lg(r+L(x+1))}{(r+L(x+1))^s}=\gamma\sum_{m\leqslant x}m\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\right.$$

$$\left.-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}+\theta\rho\sum_{m\leqslant x}m^{1-\frac{1}{n}}\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\right.$$

$$\left.-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}+\frac{S(r+Lx)\lg(r+L(x+1))}{(r+L(x+1))^s}. \qquad (2.4)$$

25. Первая из сумм (2.4) дает

$$\sum_{m\leqslant x}m\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}=\sum_{m=1}^{x}\frac{\lg(r+Lm)}{(r+Lm)^s}-$$

$$-\frac{x\lg(r+L(x+1))}{(r+L(x+1))^s}=\int_1^x\frac{\lg(r+Lz)\,dz}{(r+Lz)^s}+\frac{c\lg(r+L)}{(r+L)^s}-\frac{x\lg(r+L(x+1))}{(r+L(x+1))^s}= \qquad (3.4)$$

(это следует из того, что

$$\sum_{m=1}^{x}\frac{\lg(r+Lm)}{(r+Lm)^s}>\int_1^{x+1}\frac{\lg(r+Lz)\,dz}{(r+Lz)^s}>\int_1^{x}\frac{\lg(r+Lz)\,dz}{(r+Lz)^s}, \qquad (4.4)$$

$$\sum_{m=2}^{x}\frac{\lg(r+Lm)}{(r+Lm)^s}<\int_1^x\frac{\lg(r+Lz)}{(r+Lz)^s}\,dz, \qquad (5.4)$$

так как $\frac{\lg z}{z^s}$ при $z\geqslant e$ есть монотонно убывающая функция).

$$=\frac{1}{L}\int_{r+L}^{r+Lx}\frac{\lg z\,dz}{z^s}+\frac{c\lg(r+L)}{(r+L)^s}-\frac{x\lg(r+L(x+1))}{(r+L(x+1))^s}=$$

$$=\frac{1}{L}\left[-\frac{1}{(s-1)^2}\frac{1}{z^{s-1}}-\frac{1}{s-1}\frac{\lg z}{z^{s-1}}\right]_{r+L}^{r+Lx}+\frac{c\lg(r+L)}{r+L}-$$

$$-c\frac{\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}=\frac{1}{L(s-1)^2}\left\{\frac{1}{(r+L)^{s-1}}-\frac{1}{(r+Lx)^{s-1}}\right\}+$$

$$+\frac{1}{L(s-1)}\left\{\frac{\lg(r+L)}{(r+L)^{s-1}}-\frac{\lg(r+Lx)}{(r+Lx)^{s-1}}\right\}+\frac{c\lg(r+L)}{r+L}-c\frac{\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}=$$

$$=\frac{1}{L(s-1)^2}\left(1-\frac{1}{x^{s-1}}\right)+\frac{\theta\lg(r+L)}{L(s-1)}+\frac{1}{L(s-1)}\left\{\frac{\lg(r+L)}{(r+L)^{s-1}}-\frac{\lg(r+Lx)}{(r+Lx)^{s-1}}\right\}+$$

$$+c\frac{\lg(r+L)}{r+L}-c\frac{\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}. \qquad (3'.4)$$

26. Для второй суммы (2.4) получаем

$$\sum_{m\leqslant x} m^{1-\frac{1}{n}}\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}=\sum_{m\leqslant x} m^{1-\frac{1}{n}}\int_{r+Lm}^{r+L(m+1)}\frac{s\lg z-1}{z^{s+1}}\,dz<$$

$$<\sum_{m\leqslant x}\frac{1}{L^{1-\frac{1}{n}}}\int_{r+Lm}^{r+L(m+1)}\frac{s\lg z-1}{z^{s+\frac{1}{n}}}\,dz=\frac{1}{L^{1-\frac{1}{n}}}\int_{r+L}^{r+L(x+1)}\frac{s\lg z-1}{z^{s+\frac{1}{n}}}\,dz=$$

$$=\frac{1}{L^{1-\frac{1}{n}}}\frac{s}{s+\frac{1}{n}-1}\int_{r+L}^{r+L(x+1)}\frac{\left(s+\frac{1}{n}-1\right)\lg z-1}{z^{s+\frac{1}{n}}}\,dz+$$

$$+\frac{1}{L^{1-\frac{1}{n}}}\frac{1-\frac{1}{n}}{s+\frac{1}{n}-1}\int_{r+L}^{r+L(x+1)}\frac{dz}{z^{s+\frac{1}{n}}}=$$

$$=\frac{1}{L^{1-\frac{1}{n}}}\frac{s}{s+\frac{1}{n}-1}\times\left\{\frac{\lg(r+L)}{(r+L)^{s+\frac{1}{n}-1}}-\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s+\frac{1}{n}-1}}\right\}+$$

$$+\frac{1}{L^{1-\frac{1}{n}}}\frac{1-\frac{1}{n}}{\left(s+\frac{1}{n}-1\right)^2}\times\left\{\frac{1}{(r+L)^{s+\frac{1}{n}-1}}-\frac{1}{(r+L(x+1))^{s+\frac{1}{n}-1}}\right\}<$$

$$<\frac{n}{L^{1-\frac{1}{n}}}\left\{\frac{\lg(r+L)}{\sqrt[n]{r+L}}+\frac{n-1}{\sqrt[n]{r+L}}\right\}. \tag{6.4}$$

27. Подстановка (3.4) и (6.4) в (2.4) дает

$$\sum_{m\leqslant x}\frac{f(r+Lm)\lg(r+Lm)}{(r+Lm)^s}=\frac{\gamma}{L(s-1)^2}\left(1-\frac{1}{x^{s-1}}\right)+$$

$$+\frac{\theta\gamma}{L(s-1)}\frac{\lg(r+Lx)}{(r+Lx)^{s-1}}+c\gamma\frac{\lg(r+L)}{r+L}-c\gamma\frac{\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}+$$

$$+\theta\frac{n\rho}{L^{1-\frac{1}{n}}}\left\{\frac{\lg(r+L)}{\sqrt[n]{r+L}}+\frac{n-1}{\sqrt[n]{r+L}}\right\}+c\frac{\gamma+\theta\rho}{L}\frac{\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}. \tag{7.4}$$

28. Для второй суммы в (1.4) получаем

$$\sum_{m>x}\frac{f(r+Lm)\lg(r+Lm)}{(r+Lm)^s}=\sum_{m>x}\frac{\lg(r+Lm)}{(r+Lm)^s}\{S(r+Lm)-S(r+L(m-1))\}=$$

$$=\sum_{m=x+1}^{\infty}S(r+Lm)\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}-$$

$$-\frac{S(r+Lx)\lg(r+L(x+1))}{(r+L(x+1))^s}=\gamma\sum m\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}+$$

$$+\rho\sum_{m>x}m^{1-\frac{1}{n}}\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}-c\frac{(\gamma+\theta\rho)\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}.$$

(8.4).

29. Для первой суммы в (8.4) получаем

$$\sum_{m>x} m\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}=\sum_{m>x}\frac{\lg(r+Lm)}{(r+Lm)^s}+$$

$$+\frac{x\lg(r+L(x+1))}{(r+L(x+1))^s}=\int_{x+1}^{\infty}\frac{\lg(r+Lz)}{(r+Lz)^s}\,dz+c\frac{\lg(r+L(x+1))}{(r+L(x+1))^s}+$$

$$+\frac{x\lg(r+L(x+1))}{(r+L(x+1))^s}=\frac{1}{L(s-1)^2}\frac{1}{(r+L(x+1))^{s-1}}+\frac{1}{L(s-1)}\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s-1}}+$$

$$+(x+c)\frac{\lg(r+L(x+1))}{(r+L(x+1))^s}. \tag{9.4}$$

30. Для второй суммы в (8.4) получаем

$$\sum_{m>x} m^{1-\frac{1}{n}}\left\{\frac{\lg(r+Lm)}{(r+Lm)^s}-\frac{\lg(r+L(m+1))}{(r+L(m+1))^s}\right\}=$$

$$=\sum_{m>x} m^{1-\frac{1}{n}}\int_{r+Lm}^{r+L(m+1)}\frac{s\lg z-1}{z^{s+1}}\,dz<\frac{1}{L^{1-\frac{1}{n}}}\int_{r+L(x+1)}^{\infty}\frac{s\lg z-1}{z^{s+\frac{1}{n}}}\,dz=$$

$$=\frac{1}{L^{1-\frac{1}{n}}}\frac{s}{s+\frac{1}{n}-1}\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s+\frac{1}{n}-1}}+\frac{1}{L^{1-\frac{1}{n}}}\frac{1-\frac{1}{n}}{(s+\frac{1}{n}-1)^2}\times$$

$$\times\frac{1}{(r+L(x+1))^{s+\frac{1}{n}-1}}<\frac{n}{L^{1-\frac{1}{n}}}\left\{\frac{\lg(r+L)}{\sqrt[n]{r+L}}+\frac{n-1}{\sqrt[n]{r+L}}\right\}. \tag{10.4}$$

31. Подстановка (9.4) и (10.4) в (8.4) дает

$$\sum_{m>x}\frac{f(r+Lm)\lg(r+Lm)}{(r+Lm)^s}=\frac{\gamma}{L(s-1)^2}\frac{1}{x^{s-1}}+c\frac{\gamma}{L(s-1)}\lg(r+L)+$$

$$+\frac{\gamma}{L(s-1)}\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s-1}}+c\gamma(x+1)\frac{\lg(r+L(x+1))}{(r+L(x+1))^s}+$$

$$+\theta\frac{n\rho}{L^{1-\frac{1}{n}}}\left\{\frac{\lg(r+L)}{\sqrt[n]{r+L}}+\frac{n-1}{\sqrt[n]{r+L}}\right\}-c\frac{(\gamma+\theta\rho)\lg(r+L(x+1))}{L(r+L(x+1))^{s-1}}. \tag{11.4}$$

32. Подстановка (7.4) и (11.4) в (1.4) дает

$$\frac{\gamma}{L(s-1)^s}\left(1-\frac{c}{x^{s-1}}\right)+\frac{\theta\gamma}{L(s-1)}\frac{\lg(r+Lx)}{(r+Lx)^{s-1}}+$$

$$+c\gamma\frac{\lg(r+L)}{r+L}+\frac{\theta\gamma}{L}\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s-1}}+\theta\frac{n\rho}{L^{1-\frac{1}{n}}}\left\{\frac{\lg(r+L)}{\sqrt[n]{r+L}}+\frac{n-1}{\sqrt[n]{r+L}}\right\}+$$

$$+c\frac{\gamma+\theta\rho}{L}\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s-1}}+c\frac{\gamma}{L(s-1)}\lg(r+L)+$$

$$+\frac{c\gamma}{L(s-1)}\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s-1}}+\theta\frac{n\rho}{L^{1-\frac{1}{n}}}\left\{\frac{\lg(r+L)}{\sqrt[n]{r+L}}+\frac{n-1}{\sqrt[n]{r+L}}\right\}-$$

$$-c\frac{(\gamma+\theta\rho)\lg(r+L(x+1))}{L(r+L(x+1))}. \tag{12.4}$$

Положим, что

$$\frac{\lg(r+L(x+1))}{(r+L(x+1))^{s-1}} \leqslant \frac{\lg(r+Lx)}{(r+Lx)^{s-1}}.$$

Это неравенство выполняется, если

$$r+Lx \geqslant e^{\frac{1}{s-1}} \tag{13.4}$$

Кроме того, пусть

$$s-1 \leqslant 1.$$

Тогда (12.4) принимает следующий вид:

$$\frac{\gamma}{L(s-1)^2}\left(1-\frac{c}{x^{s-1}}\right)+\frac{\theta}{s-1}\frac{\lg(r+Lx)}{(r+Lx)^{s-1}}\frac{4\gamma+2\rho}{L}+$$

$$+\frac{\theta}{s-1}\left\{\frac{r}{L}\frac{\lg(r+L)}{r+L}+\frac{\gamma}{L}\lg(r+L)+\frac{2n\rho}{L}\lg(r+L)+\frac{2n(n-1)\rho}{L}\right\}=$$

$$=\frac{\gamma}{L(s-1)^2}\left(1-\frac{c}{x^{s-1}}\right)+\frac{\theta}{s-1}\left(C_r\frac{\lg z_r}{z_r^{s-1}}+D_r\right), \tag{14.4}$$

где

$$z_r=r+Lx,\ C_r=\frac{4\gamma+2\rho}{L},\ D_r=\frac{\gamma}{L}\frac{\lg(r+L)}{r+L}+\frac{\gamma}{L}\lg(r+L)+$$

$$+\frac{2n\rho}{L}\lg(r+L)+\frac{2n(n-1)\rho}{L}. \tag{15.4}$$

§ 5. Оценка основной формулы

33. В силу (20.2) и (14.4) основную формулу можно записать так:

$$\sum_{v=1}^{n}\sum_{p^v\leqslant L(x+1)}\frac{\chi(p^v)\overline{f}(p^v)\lg p^v}{p^{vs}-\chi(p^v)}=$$

$$=\frac{\frac{\gamma}{L}\sum_r\chi(r)+\theta\frac{\gamma\overline{F}}{L}\frac{1}{x^{s-1}}+\theta(s-1)\left\{\overline{F}C_m\frac{\lg z}{z^{s-1}}+\overline{F}D_m\right\}}{(s-1)\left\{\frac{\gamma}{L}\sum_r\chi(r)+\theta\frac{\gamma\overline{F}}{L}\frac{1}{x^{s-1}}+\theta\overline{F}A_m(s-1)\right\}}, \tag{1.5}$$

где

$$z=Lx,\qquad Lx\geqslant e^{\frac{1}{s-1}}.$$

34. Полагая χ главным характером: $\chi(k)=1$, мы получим

$$\sum_{v=1}^{n}\sum_{p^v\leqslant L(x+1)}\frac{\overline{f}(p^v)\lg p^v}{p^{vs}-1}>\frac{1-\frac{1}{x^{s-1}}-\frac{C_mL}{\gamma}\frac{(s-1)\lg z}{z^{s-1}}-\frac{LD_m}{\gamma}(s-1)}{1+\frac{1}{x^{s-1}}+\frac{LA_m}{\gamma}(s-1)}. \tag{2.5}$$

Найдем для s и x значения, удовлетворяющие неравенствам

$$\frac{1}{x^{s-1}} < \frac{\varepsilon}{6}, \tag{3.5}$$

$$\frac{(s-1)\lg z}{z^{s-1}} < \frac{\gamma}{C_m L}\frac{\varepsilon}{6}, \tag{4.5}$$

$$s-1 < \frac{\gamma}{D_m L}\frac{\varepsilon}{6}, \tag{5.5}$$

$$s-1 < \frac{\gamma}{A_m L}\frac{\varepsilon}{6}. \tag{6.5}$$

Эти неравенства не противоречат друг другу и неравенствам (9.3), (10.3), (11.3), (12.3), (13.4). Чтобы удовлетворить им, следует сначала взять достаточно малое значение для $(s-1)$ и затем достаточно большое значение для x. Особого исследования требует только неравенство (4.5). Положим в нем $\zeta = z^{s-1}$ и $\alpha = \frac{6D_m L}{\gamma\varepsilon}$. Тогда

$$\frac{\zeta}{\lg\zeta} > \alpha. \tag{7.5}$$

Левая часть с ростом ζ уменьшается, так как

$$\frac{d}{d\zeta}\left(\frac{\zeta}{\lg\zeta}\right) = \frac{\lg\zeta - 1}{(\lg\zeta)^2} > 0 \qquad \text{при } \zeta > 1. \tag{8.5}$$

Возьмем вместо (7.5) неравенство

$$\frac{\zeta}{\lg\zeta} > \beta \qquad (\beta = \operatorname{Max}\{\alpha, 1\}).$$

Полагая затем $\zeta = \beta^2$, получим $\lg\zeta = 2\lg\beta < \beta$, откуда $\frac{\zeta}{\lg\zeta} > \beta \geqslant \alpha$. Для того чтобы показать, что $\beta > 2\lg\beta$, возьмем

$$f(\beta) = e^{\beta} - \beta^2, \quad f'(\beta) = e^{\beta} - 2\beta, \quad f''(\beta) = e^{\beta} - 2.$$

Из неравенств

$$f''(\beta) > 0 \quad (\text{при } \beta \geqslant 1), \quad f'(1) > 0, \quad f(1) > 0$$

следует

$f(\beta) > 0$ при $\beta \geqslant 1$, т. е. $e^{\beta} - \beta^2 > 0$, $\beta^2 - 2\lg\beta > 0$, ч. и т. д.

В силу (8.5) получаем

$$\frac{\zeta}{\lg\zeta} > \alpha \quad \text{при } \zeta > \operatorname{Max}\{\alpha^2, 1\}. \tag{9.5}$$

Следовательно, (4.5) можно заменить более строгими неравенствами

$$z^{s-1} > \left(\frac{6D_m L}{\gamma\varepsilon}\right)^2, \quad z^{s-1} > 1. \tag{10.5}$$

Если все они удовлетворены, то формула (2.5) принимает вид

$$\sum_{v=1}^{n} \sum_{p^v \leqslant L\,(x+1)} \frac{\overline{f}(p^v) \lg p^v}{p^{vs}-1} > \frac{1}{s-1} \frac{1-\frac{\varepsilon}{2}}{1+\frac{\varepsilon}{2}} > \frac{1-\varepsilon}{s-1}. \tag{11.5}$$

35. В случае не главного характера $\chi(r)$ формула (1.5), в силу (13.3), (3.5), (4.5) и (5.5), преобразуется так:

$$\sum_{v=1}^{n} \sum_{p^v \leqslant L\,(x+1)} \frac{\overline{f}(p^v)\chi(p^v) \lg p^v}{p^{vs}-\chi(p^v)} < \frac{1}{1-s} \frac{\gamma \overline{F}}{LR} \frac{\varepsilon}{1-\varepsilon}. \tag{12.5}$$

36. Правая часть формулы (1.5) может быть оценена и сверху

$$\sum_{v=1}^{n} \sum_{p^v \leqslant L\,(x+1)} \frac{\overline{f}(p^v) \lg p^v}{p^{vs}-1} < \frac{1}{s-1} \frac{1+\frac{\varepsilon}{2}}{1-\frac{\varepsilon}{2}} < \frac{1}{s-1} \frac{1}{1-\varepsilon}. \tag{13.5}$$

§ 6. Простые числа первой степени, лежащие в данной прогрессии

37. Оценим теперь левую часть основной формулы

$$\sum_{v=1}^{n} \sum_{p^v \leqslant L\,(x+1)} \frac{\overline{f}(p^v)\chi(p^v) \lg p^v}{p^{vs}-\chi(p^v)} = \sum_{p \leqslant L\,(x+1)} \frac{\overline{f}(p)\chi(p) \lg p}{p^s-\chi(p)} +$$

$$+ \theta \left[\frac{n}{2}\right] \left\{ \sum_{p=2}^{\infty} \frac{2 \lg p}{p^{2s}-1} + \sum_{p \text{ критич.}} \frac{2 \lg p}{p^2-1} \right\}. \tag{1.6}$$

Вторая сумма не больше чем

$$\sum_{p \text{ критич.}} \frac{2 \lg p}{p-1} + \sum_{p=2}^{\infty} \frac{2 \lg p}{p^2-1} = -2 \frac{\zeta'(2)}{\zeta(2)} + 2\sigma = 2 \left| \frac{\zeta'(2)}{\zeta(2)} \right| + 2\sigma, \tag{2.6}$$

где σ есть число критических простых идеалов первой степени.

38. Для первой суммы в (1.6) имеет место

$$\sum_{p \leqslant L\,(x+1)} \frac{\overline{f}(p)\chi(p) \lg p}{p^s-\chi(p)} = \sum_{p \leqslant L\,(x+1)} \frac{\overline{f}(p)\chi(p) \lg p}{p^s} + \sum_{p \leqslant L\,(x+1)} \frac{\overline{f}(p)\chi(p)^2 \lg p}{p^s(p^s-\chi(p))}. \tag{3.6}$$

Вторая сумма этого выражения может быть представлена так:

$$\sum_{p \leqslant L\,(x+1)} \frac{\overline{f}(p)\chi(p)^2 \lg p}{p^s(p^s-\chi(p))} = \theta \cdot 2n \sum \frac{\lg p}{p^2-1} = \theta \cdot 2n \left\{ \left| \frac{\zeta'(2)}{\zeta(2)} \right| + \sigma \right\}. \tag{4.6}$$

Поэтому формула (12.5) может быть записана в таком виде:

$$\sum_{p \leqslant L\,(x+1)} \frac{\overline{f}(p)\chi(p) \lg p}{p^s} = \frac{\theta}{s-1} \frac{\gamma \overline{F}}{LR} \frac{\varepsilon}{\varepsilon-1} + \theta \cdot 3n \left\{ \left| \frac{\zeta'(2)}{\zeta(2)} \right| + \sigma \right\} \quad \text{при } \chi(r) \neq 1 \tag{5.6}$$

и

$$\sum_{p\leqslant L(x+1)} \frac{\bar{f}(p)\lg p}{p^s} = \frac{1}{s-1} + \frac{\theta}{s-1}\frac{\varepsilon(2-\varepsilon)}{1-\varepsilon} + \theta\cdot 3n\left\{\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \sigma\right\} \text{ при } \chi(r)=1. \tag{6.6}$$

39. Для того чтобы выделить в суммах (5.6) и (6.6) те члены, которые соответствуют простым числам, лежащим в заданной прогрессии $r + Lx$, мы умножаем каждую из формул (5.6) на $\chi^{-1}(r)$, где $\chi(r)$ есть характер, соответствующий этой формуле, затем суммируем по χ и прибавляем еще формулу (6.6). Вследствие

$$\sum_{\chi}\chi(r)\chi^{-1}(t) = \bar{F} \text{ при } r\equiv t(\mathrm{mod}\, L) \text{ и } = 0 \text{ при } r\not\equiv t(\mathrm{mod}\, L) \tag{7.6}$$

мы получим

$$\sum_{\substack{p\leqslant L(x+1)\\ p\equiv r(\mathrm{mod}\, L)}} \frac{\bar{f}(p)\lg p}{p^s} = \frac{1}{\bar{F}(s-1)} + \frac{2\theta\varepsilon}{\bar{F}(s-1)} + \frac{\theta}{s-1}\frac{\gamma(\bar{F}-1)}{LR}\frac{\varepsilon}{1-\varepsilon} + \\ + \theta\frac{3n}{\bar{F}}\left\{\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \sigma\right\}. \tag{8.6}$$

40. Рассмотрим случай *нормального* поля $\mathfrak{R}$. Тогда $\bar{f}(p) = n$ (или $\bar{f}(p) = 0$). Мы хотим знать, в каком интервале $\langle 1, x\rangle$ наверное лежит V простых чисел рассматриваемого типа. Имеем прежде всего

$$\sum_{p\leqslant L(x+1)} \frac{\bar{f}(p)\lg p}{p^s}(p = N\mathfrak{p}, p\equiv r(\mathrm{mod}\, L)) < n\sum_{a=1}^{V}\frac{\lg p_a}{p_a}, \tag{9.6}$$

где сумма в правой части распространяется на V первых простых чисел $2, 3, 5, \ldots$, если в $\langle 1, L(x+1)\rangle$ лежит ровно V простых чисел типа $p = N\mathfrak{p}$, $p\equiv r(\mathrm{mod}\, L)$. Но согласно Мертенсу [5],

$$\sum_{a=1}^{V}\frac{\lg p_a}{p_a} < \lg p_v + 1, \tag{10.6}$$

где p_v есть V-ое простое число. Поэтому, если мы подчиним s и x неравенству

$$\frac{1}{\bar{F}}\frac{1}{s-1} - \frac{2\varepsilon}{\bar{F}(s-1)} - \frac{1}{s-1}\frac{\gamma(\bar{F}-1)}{LR}\frac{\varepsilon}{1-\varepsilon} - \\ - 3n\left\{\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \sigma\right\} > (\lg p_v + 1)n, \tag{11.6}$$

то мы сможем утверждать, что в интервале $\langle 1, L(x+1)\rangle$ лежит не менее V простых чисел вида $p = N\mathfrak{p}$, $p\equiv r(\mathrm{mod}\, L)$.

41. Чтобы удовлетворить неравенству (11.6), достаточно подчинить s и x неравенствам

$$s - 1 \leqslant \frac{1}{2\bar{F}\left\{3n\left|\frac{\zeta'(2)}{\zeta(2)}\right| + n(\lg p_v + 1) + 3n\sigma\right\}}, \tag{12.6}$$

$$\varepsilon \leqslant \frac{1}{8}, \tag{13.6}$$

$$\frac{\varepsilon}{1-\varepsilon} \leqslant \frac{LR}{4\gamma \bar{F}(\bar{F}-1)}. \tag{14.6}$$

Значение ε, полученное из (13.6) и (14.6), нужно подставить в неравенства (15.3), (16.3), (3.5), (5.5), (6.5), (10.5) и подчинить x, s полученным условиям. Если все эти неравенства выполняются, то можно утверждать, что в интервале $\langle 1, L(x+1)\rangle$ наверное содержится V простых чисел типа $p = N\mathfrak{p}$, $p \equiv r \pmod{L}$.

§ 7. Простые числа, принадлежащие к классу подстановок

42. Теперь мы хотим отыскать интервал $\langle 1, x\rangle$, в котором наверное лежат V простых чисел, принадлежащих к подстановке S f-го порядка группы Галуа поля $\mathfrak{K}$. Для этого возьмем некоторое простое число $q \equiv 1 \pmod{f}$, не критическое в поле $\mathfrak{K}$, и присоединим к полю $\mathfrak{K}$ делитель f-ой степени поля q-ых корней из единицы. Пусть r будет примитивный корень сравнения

$$x^{q-1} \equiv 1 \pmod{q}. \tag{1.7}$$

Если простое число p принадлежит к отделу подстановки SU в $\mathfrak{K}^*$ ($\mathfrak{K}^*$ есть поле, полученное указанным присоединением), причем $p \equiv r \pmod{q}$, то можно утверждать, что p принадлежит к классу S в $\mathfrak{K}$. Здесь U обозначает известным образом отнесенную к числу r подстановку присоединенного кругового поля (см. [4], § 2 и теорема 13, стр. 219). Поэтому для решения нашей задачи достаточно найти простые числа, которые принадлежат в $\mathfrak{K}^*$ к отделу подстановки SU и лежат в прогрессии $r + Lx$.

43. Рассмотрим все подполя поля $\mathfrak{K}^*$, принадлежащие к различным подгруппам циклической группы $\mathfrak{Z}$ f-го порядка, порожденной степенями подстановки SU. Здесь $\bar{F}$ равно f ([4], стр. 215). Поэтому формула (8.6) принимает вид

$$\sum_{\alpha \mid a} \frac{n\varphi(\alpha)}{a n_\alpha k_\alpha} \sum_{p_\alpha} \frac{\lg p}{p^s} = \frac{1}{f}\frac{1}{s-1} +$$

$$+ \theta\left\{\frac{2\varepsilon}{f(s-1)} + \frac{1}{s-1}\frac{\gamma_a(f-1)}{qR_a}\frac{\varepsilon}{1-\varepsilon} + 3nf\left(\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \sigma\right)\right\}, \tag{2.7}$$

где a есть делитель f ([4], стр. 198, формула (16)). Умножая эту формулу на $\frac{a}{n}\mu\left(\frac{f}{a}\right)$ и суммируя по всем $a \mid f$, мы, в силу

$$\sum_{a \mid f} \mu(a) = 0 \text{ при } f > 1 \text{ и } = 1 \text{ при } f = 1,$$

$$\sum_{a \mid f} a\mu\left(\frac{f}{a}\right) = \varphi(f),$$

получим

$$\sum_{p\leqslant q\,(x+1)} \frac{\lg p}{p^s} = \frac{k_f n_f}{n_f}\frac{1}{s-1} + \\ + \theta D_f\left\{\frac{2\varepsilon}{f(s-1)} + \frac{1}{s-1}\frac{\gamma_m(f-1)}{q\cdot R}\frac{\varepsilon}{1-\varepsilon} + 3nf\left(\left|\frac{\zeta'(2)}{\zeta(2)}\right| + \sigma\right)\right\}, \qquad (3.7)$$

где сумма слева распространена на те простые числа, принадлежащие к классу S, которые лежат в прогрессии $r + qx$.

44. Чтобы найти интервал $\langle 1, x\rangle$, наверное содержащий V простых чисел, принадлежащих к классу S, достаточно дословно повторить все рассуждения § 6 (№ 40, 41), так как уравнение (3.7) отличается от уравнения (8.6) только другими значениями постоянных.

ЛИТЕРАТУРА

1. Н. Чеботарев. Исследования о плотностях простых чисел. 1. Изв. КФМО 2. 1927, стр. 14—20. Собр. соч., т. I, стр. 95—101.
2. A. Artin. Über eine neue Art von L-Reihen. Abh. Hamb. Sem. 3, стр. 89—108.
3. E. Artin. Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Hamb. Sem. 5, 1927.
4. Н. Чеботарев. Die Bestimmung der Dichtigkeit u. s. w. Math. Ann. 95, стр. 200—211.
5. Mertens. Über Dirichlet's Beweis u. s. w. Sitzber. Wien. 106, 1897, Abth. IIa, стр. 259, формула (4).

p-АДИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО ВТОРОЙ ГЛАВНОЙ ТЕОРЕМЫ ОРЕ

(p-ADISCHER BEWEIS DES ZWEITEN HAUPTZATZES VON HERRN ORE)

(Acta litt. ac sc. univers. Francisco-Josephinae 4 (1928), стр. 56—57).

Совместно с М. Бауэром

(Из переписки Н. Г. Чеботарева и М. Бауэра)

Вторая главная теорема О. Оре [1], дающая возможность разложения любого простого числа на простые идеалы в произвольном алгебраическом числовом поле без знания минимального базиса может быть очень просто доказана с помощью гензелевской теории [2] p-адических чисел. Ход доказательства следующий:

1. Пусть

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{1}$$

$$a_i \text{ цел. рац., } (i = 1, 2, \ldots, n), \quad f(\omega) = 0$$

неприводимое уравнение. Мы хотим разложить рациональное простое число p на простые идеалы в поле $K(\omega)$.

2. Разлагая сначала $f(x)$ на p-адические неприводимые факторы, получаем наивысшие степени простых идеалов. Если $\Phi(x)$ — p-адически неприводимый фактор и

$$\Phi(x) = x^m + c_1 x^{m-1} + \cdots + c_m(p), \tag{2}$$

то

$$p = \mathfrak{p}^g \mathfrak{q}, \qquad (\mathfrak{p}, \mathfrak{q}) = 1, \tag{3}$$

$$f \text{ есть степень } \mathfrak{p}, \quad m = fg. \tag{4}$$

Фактор $\Phi(x)$ можно заменить обыкновенным полиномом, сравнимым с Φ по $(\mathrm{mod}\, p^\alpha)$, где α достаточно велико. Поэтому m можно определить посредством конечного числа операций.

3. Известно, что полином $\Phi(x)$ в поле $(p^f - 1)$-х корней из единицы разлагается на неприводимые факторы g-ой степени. С другой стороны, он не может разлагаться далее ни при каких присоединениях, если p не является критическим в расширенной области рациональности. В самом деле, p содержит g-ую степень простого идеала (в обозначениях Гензеля $\pi^g \sim p$). Поэтому, если мы заключим $K(p)$ в надполе $K(p, \alpha)$, $(\alpha^{p^f-1} - 1 = 0)$, дискриминант которого взаимно прост

с p, то $\Phi(x)$ будет распадаться в неприводимые полиномы точно g-ой степени. Но поле $K(p,\beta)$, $(\beta^{p^m-1}-1=0)$, удовлетворяет этим условиям. Таким образом, чтобы найти g, достаточно определить степень делителей полинома $\Phi(x)$, неприводимых в поле $K(p, \beta)$, где β есть примитивный корень из единицы степени (p^m-1), а это достигается путем конечного числа операций.

Получено
21 июня 1928 года

ЛИТЕРАТУРА

1. O. Ore. Über den Zusammenhang zwischen u. s. w. II. Math. Ann. **97**. стр. 585.
2. K. Hensel. Die Theorie der algebraischen Zahlen. Lpz., 1908.

К ТЕОРИИ ГРУПП ПОЛЯ КЛАССОВ

(ZUR GRUPPENTHEORIE DES KLASSENKÖRPERS)

(Journ. f. reine und ang. Math. 161 (1929), стр. 179—193)

До сих пор определение числа классов[1] поля в общем случае производится только посредством трансцендентного выражения. Даже в простейших случаях аддитивная структура полученных «окончательных выражений» не позволяет сделать какие-либо высказывания о простых множителях числа классов. Мне известна только одна относящаяся сюда теорема, вытекающая из знаменитых гауссовых исследований о genera formarum (здесь я не принимаю во внимание соотношений между числами классов в различных полях):

Если квадратичное поле содержит только одно критическое простое число, то число его классов обязательно нечетное. Если, напротив, существует несколько критических простых чисел, то число классов этого поля четное и степень двойки, содержащаяся в этом числе классов, вполне определяется числом критических простых чисел.

Первое утверждение этой теоремы удивительным образом связано со следующей теоремой из общей теории чисел, которую можно понимать, как обобщение теоремы монодромии [1].

Теорема 1. *В группе Галуа нормального поля не существует правильного делителя, содержащего все группы инерции.*

Эту теорему [2] можно рассматривать так же как усиление теоремы *Минковского* о дискриминанте [3].

В одной из более ранних работ (выше цит., [2]) я приложил эту теорему к полям деления круга и получил в терминах теории сравнений некоторые свойства, которыми обладает каждый множитель числа классов.

В этой работе я намерен предпринять подобное же исследование для общего нормального поля. Разнородность структур групп Галуа таких полей не позволяет получить столь же простые результаты. Группе классов нормального поля я ставлю в соответствие относительную группу его поля классов. При этом я рассматриваю только абсолютные идеальные классы в узком смысле, так что под полем

[1] Под «полем» мы понимаем всюду алгебраическое числовое поле.

классов следует понимать всегда наиболее широкое относительно-абелево неразветвленное относительное поле.

Очевидно, что поле классов абсолютно нормально. Разложим его на частичные поля классов (Teilklassenkörper), каждое из которых абсолютно нормально и не допускает дальнейшего разложения на абсолютно нормальные поля. При этом под «разложением» я понимаю представление поля в виде композита абсолютно нормальных полей. Такие поля мы назовем *элементарными* (абсолютно нормальными) *частичными полями классов*. Каждое так построенное частичное поле классов обладает относительной группой ν-членного типа $\{p^\mu, p^\mu, \ldots, p^\mu\}$, так что ему соответствует множитель числа классов $p^{\mu\nu}$. Такие частичные поля классов, а также соответствующие им множители числа классов мы разобьем на четыре типа и установим особые свойства для каждого из этих типов. Определение этих типов последует ниже (см. § 3, опр. 4).

1. *Собственные множители числа классов* (Eigentliche Klassenzahlfaktoren). Пусть K — нормальное поле и K_p — его собственное элементарное частичное поле классов относительной степени $p^{\mu\nu}$ с относительной группой ν-членного типа $\{p^\mu, p^\mu, \ldots, p^\mu\}$. Тогда группа поля K изоморфна с некоторым делителем голоморфа *абелевой* группы ν-членного типа $\{p^\mu, p^\mu, \ldots, p^\mu\}$.

В частности, если $\mu = 1$, то группа поля K изоморфна с транзитивной группой сравнений по модулю p целочисленных линейных однородных подстановок ν символов.

Если $\mu = \nu = 1$ (что может случиться только для циклического поля K), то имеет место

$$p \equiv 1 \pmod{g},$$

где g есть степень поля K.

2. *Несобственные множители числа классов* (Uneigentliche Klassenzahlfaktoren). Если K_p — поле, определенное в 1, которому соответствует несобственный множитель числа классов, то K содержит нормальное подполе $\overline{K}$, число классов которого тоже содержит множитель p. Соответствующее частичное поле классов $\overline{K}_p$ над $\overline{K}$ порождается присоединением к полю K всего поля K_p. В свою очередь, $\overline{K}$ содержит такое нормальное подполе $\overline{\overline{K}}$, над которым поле $\overline{K}_p$ не разветвляется. Группа поля $\overline{\overline{K}}$ содержится в голоморфе относительной группы поля $\overline{K}_p$ над $\overline{\overline{K}}$. Случай этот аналогичен случаю I, однако не является таким же простым, так как относительная группа поля $\overline{K}_p$ над $\overline{\overline{K}}$ может не быть *абелевой*.

3. *Центральные множители числа классов* (Zentrale Klassenzahlfaktoren). В этом случае как сами множители числа классов, так и их степени, входящие в число классов, определяются структурой группы поля K. Этот тип множителей в циклических полях не встречается.

4. *Родовые множители числа классов* (Geschlechterklassenzahlfaktoren). В этом случае простые множители p числа классов также определяются структурой группы поля K (точнее: они суть делители степени поля K). Их степени, входящие в число классов, зависят от числа критических простых идеалов поля K. Этот тип множителей может встретиться уже в простейших случаях, например в случае квадратичного поля.

Заданное простое число может входить в различные множители одного и того же поля.

Я позволю себе выразить мою сердечную благодарность *Г. Гассе* за многие важные указания относительно формы изложения, а также за некоторые замечания по существу работы, а также *О. Шрейеру* за улучшение хода доказательства теоретико-групповой теоремы 2.

§ 1. Арифметическая теорема монодромии

Рассматривая p-адические разложения чисел данного нормального поля [4], легко убедиться, что теорема 1 является арифметическим аналогом теоремы монодромии, так как алгебраическое число α тогда и только тогда разлагается по д р о б н ы м степеням p, когда p является критическим числом для поля $R(\alpha)$.

Пусть K — нормальное поле. Рассмотрим все его подполя $R(\alpha)$, т. е. поля, полученные присоединением содержащихся в K чисел α к полю рациональных чисел R.

Зададимся таким вопросом: каковы условия, необходимые и достаточные для того, чтобы данное простое число p не было критическим в $R(\alpha)$, т. е. чтобы разложение числа p на простые идеалы поля $R(\alpha)$ не содержало кратных множителей?

Пусть $\mathfrak{H}$ будет группа, к которой принадлежит число α внутри поля K, и $\mathfrak{p}$ — простой идеальный множитель числа p. Группа инерции $\mathfrak{T}$ идеала $\mathfrak{p}$ есть совокупность тех подстановок группы $\mathfrak{G}$ поля K, которые оставляют неизменным modulo $\mathfrak{p}$ функционал $t_1\omega_1 + t_2\omega_2 + \cdots + t_n\omega_n$, где $[\omega_1, \omega_2, \ldots, \omega_n]$ есть минимальный базис поля K. Для того чтобы число p не было критическим в $R(\alpha)$, необходимо и достаточно, чтобы все э л е м е н т ы $t_1(\Omega_1 - \Omega_1^S) + t_2(\Omega_2 - \Omega_2^S) + \cdots + t_m(\Omega_m - \Omega_m^S)$ были взаимно простыми с p, где $[\Omega_1, \Omega_2, \ldots, \Omega_m]$ есть минимальный базис поля $R(\alpha)$ и S пробегает все те подстановки группы поля $R(\alpha)$, которые действительно изменяют функционал $t_1\Omega_1 + t_2\Omega_2 + \cdots + t_m\Omega_m$. Другими словами, выражение $t_1\Omega_1 + t_2\Omega_2 + \cdots + t_m\Omega_m$ должно оставаться абсолютно неизменным при тех подстановках группы $\mathfrak{G}$, которые не изменяют $t_1\Omega_1 + t_2\Omega_2 + \cdots + t_m\Omega_m$ modulo $\mathfrak{p}$; таким образом, подстановки эти должны содержаться в $\mathfrak{H}$. Это значит, что если число p не критическое, то $\mathfrak{H}$ содержит все группы инерции, соответствующие простым идеальным множителям числа p.

Обратно, если все упомянутые группы инерции содержатся в $\mathfrak{H}$, то p не будет критическим в $R(\alpha)$. В самом деле, тогда $t_1\omega_1 + t_2\omega_2 + \cdots + t_n\omega_n \equiv t_1\tilde{\omega}_1 + t_2\tilde{\omega}_2 + \cdots + t_n\tilde{\omega}_n \pmod{\mathfrak{p}}$, где $\tilde{\omega}_1, \tilde{\omega}_2, \ldots, \tilde{\omega}_n$ — числа поля инерции идеала $\mathfrak{p}$. Следовательно, если S не принадлежит к $\mathfrak{T}$, то $t_1\tilde{\omega}_1 + t_2\tilde{\omega}_2 + \cdots + t_n\tilde{\omega}_n$ не остается неизменным modulo $\mathfrak{p}$ при подстановке S, откуда вытекает, что все элементы, а значит и дифферента поля инерции, взаимно просты с $\mathfrak{p}$. A fortiori тоже имеет место и для подполей $R(\alpha)$. Но так как группа $\mathfrak{H}$ должна содержать все группы инерции, сопряженные с $\mathfrak{T}$, то отсюда мы заключаем, что дифферента поля $R(\alpha)$ не содержит никаких идеальных множителей, общих с p, т. е. что число p не будет критическим в $R(\alpha)$, что и т. д.

Таким образом условие, необходимое и достаточное для того, чтобы число p не было критическим в $R(\alpha)$, состоит в том, чтобы все соответствующие p группы инерции являлись делителями той группы $\mathfrak{H}$, к которой принадлежит α в поле K.

Сопоставим эти условия для всех простых чисел. При этом достаточно рассмотреть только простые делители дискриминанта поля K, так как остальные простые числа наверное не будут критическими. Теорема Минковского [3] гласит, что все они тогда и только тогда не будут критическими в $R(\alpha)$, когда α рациональное. Отсюда следует теорема:

Элемент нормального поля будет рациональным тогда и только тогда, если все группы инерции поля K являются делителями группы, к которой принадлежит α.

Принимая во внимание определение группы Галуа, мы получим теорему 1, которую можно формулировать еще так:

Посредством композиции всех групп инерции нормального поля K получаются все подстановки его группы Галуа.

Если считать R не полем рациональных чисел, а произвольным полем, то наши соображения приводят к следующему обобщению теоремы 1:

Теорема 1a. *Композиция всех относительных групп инерции поля K над R порождает группу, к которой принадлежит наибольшее неразветвленное относительно R подполе поля K над R.*

§ 2. Одна теоретико-групповая теорема

Теорема 2. *Пусть $\mathfrak{G}$ — конечная группа и $Q_1, Q_2, \ldots, Q_m$ система элементов группы $\mathfrak{G}$, обладающая следующими свойствами:*

a) *Посредством композиции элементов Q_i получаются все элементы группы $\mathfrak{G}$;*

b) *Если элемент $Q_i (i = 1, 2, \ldots, m)$ входит в эту систему, то в нее входят и все сопряженные с ним элементы.*

Пусть, далее, $\mathfrak{G}'$ будет группа, обладающая следующими свойствами:

1) *группа* $\mathfrak{G}$ *изоморфна с некоторой факторгруппой* $\mathfrak{G}'/\mathfrak{H}$ *группы* $\mathfrak{G}'$;

2) *группа* $\mathfrak{H}$ *содержится в центре группы* $\mathfrak{G}'$;

3) *в* $\mathfrak{G}'$ *найдутся такие элементы* $Q_1', Q_2', \ldots, Q_m'$, *что при отображении* $\mathfrak{G}'/\mathfrak{H} \leftrightarrow \mathfrak{G}$ *классу смежности* $\mathfrak{H}Q_i'$ *соответствует элемент* $Q_i (i = 1, 2, \ldots, m)$;

4) *порядки* Q_i' *и* Q_i *равны*;

5) *все элементы группы* $\mathfrak{H}$ (*а также* $\mathfrak{G}'$) *выражаются через* $Q_1', Q_2', \ldots, Q_m'$.

Тогда $\mathfrak{G}'$ *изоморфна с факторгруппой некоторой определенной конечной группы, зависящей только от* $\mathfrak{G}$ *и выбора элементов* $Q_1, Q_2, \ldots, Q_m$. *В частности, группа* $\mathfrak{G}'$ *также конечна.*

Доказательство. Пусть элементы $\mathfrak{G}$ будут $P_1 = E, P_2, \ldots, P_n$ (n порядок $\mathfrak{G}$); они выражаются через $Q_1, Q_2, \ldots, Q_m$ (не однозначно, но раз навсегда фиксированным образом) так:

$$P_k = \varphi_k(Q_\alpha) \qquad (k = 1, 2, \ldots, n; \quad \alpha = 1, 2, \ldots, m). \tag{12}$$

Пусть система определяющих соотношений группы $\mathfrak{G}$ будет

$$g_\beta(Q_\alpha) = 1 \tag{2.2}$$

или подробнее:

$$Q_1^{\omega_{\beta_1}} \cdot Q_2^{\omega_{\beta_2}} \cdots Q_m^{\omega_{\beta_m}} = 1. \tag{2'.2}$$

В силу изоморфизма $\mathfrak{G} \leftrightarrow \mathfrak{G}'/\mathfrak{H}$ каждое из этих соотношений может быть представлено так:

$$(\mathfrak{H}Q_1')^{\omega_{\beta_1}} \cdot (\mathfrak{H}Q_2')^{\omega_{\beta_2}} \cdots (\mathfrak{H}Q_m')^{\omega_{\beta_m}} = \mathfrak{H},$$

откуда следует, в силу 2):

$$Q_1'^{\omega_{\beta_1}} \cdot Q_2'^{\omega_{\beta_2}} \cdots Q_m'^{\omega_{\beta_m}} = H_\beta, \tag{3.2}$$

где H_β есть элемент группы $\mathfrak{H}$.

Я утверждаю, что композиция элементов H_β дает всю группу $\mathfrak{H}$ Допустим обратное, именно, пусть все H_β содержатся в правильной. подгруппе $\mathfrak{A}$ группы $\mathfrak{H}$. В силу 2), $\mathfrak{A}$ есть нормальный делитель группы $\mathfrak{G}'$. Тогда факторгруппа $\mathfrak{G}'/\mathfrak{A}$ порождается элементами Q_α'' ($\alpha = 1, 2, \ldots, m$), удовлетворяющими соотношениям $g_\beta(Q_\alpha'') = 1$. Это противоречит предположению, так как (2.2) суть определяющие уравнения группы $\mathfrak{G}$.

Пусть группа $\overline{\mathfrak{G}}$ определена соотношениями

$$g_\beta(\overline{Q}_\alpha) = \overline{H}_\beta \tag{4.2}$$

(причем

$$\overline{Q}_\gamma^{m_\alpha} = 1. \tag{4'.2}$$

если

$$\overline{Q}_\alpha^{m_\alpha} = 1), \tag{4''2}$$

$$\varphi_k(\overline{Q}_\alpha)\ \overline{H}_\beta\ \varphi_k^{-1}(\overline{Q}_\alpha) = \overline{H}_\beta, \tag{5.2}$$

$$f_{kl}(\overline{Q}_\alpha)\ \overline{Q}_k f_{kl}^{-1}(\overline{Q}_\alpha) = \overline{Q}_l, \tag{6.2}$$

где

$$f_{kl}(Q_\alpha)\, Q_k\, f_{kl}^{-1}(Q_\alpha) = Q_l. \tag{7.2}$$

Группа $\overline{\mathfrak{G}}$ удовлетворяет всем условиям теоремы: 1) и 3) следуют из (4.2), (5.2), (6.2) и (2.2); 2) следует из (5.2); 4) из (4.'2,) (4,''2) и, наконец, 5) следует из (4.2).

Каждая группа $\mathfrak{G}'$, удовлетворяющая условиям теоремы, изоморфна с некоторой факторгруппой группы $\overline{\mathfrak{G}}$. В самом деле, при отображении $\overline{Q}_\alpha \to Q_\alpha'$ вследствие 1), 2), 3), 4), 5) все условия (4.2), (5.2), (6.2) сохраняют силу.

Следовательно, остается доказать только конечность группы $\overline{\mathfrak{G}}$. Для этого положим

$$\overline{Q}_\alpha \overline{Q}_\beta \overline{Q}_\alpha^{-1} = \overline{Q}_\gamma U_{\alpha\beta}, \tag{8.2}$$

где γ определяется соотношением $Q_\gamma = Q_\alpha Q_\beta Q_\alpha^{-1}$. Так как $\overline{Q}_\alpha^n = 1$ для всех α и элементы $\overline{H}$ перестановочны со всеми $\overline{Q}$, то, возвышая (8.2) в n-ую степень, мы получим

$$U_{\alpha\beta}^n = 1. \tag{9.2}$$

Значит элементы $U_{\alpha\beta}$ имеют конечный порядок, а следовательно порожденная этими элементами группа $\mathfrak{U}$ будет также конечна.

Чтобы доказать конечность числа остальных элементов, обозначим элементы $\overline{Q}_\alpha\mathfrak{U}$ факторгруппы $\overline{\mathfrak{G}}/\mathfrak{U}$ через $S_1, S_2, \ldots, S_m$. В силу (8.2) для всех α, β имеет место

$$S_\alpha S_\beta S_\alpha^{-1} = S_\gamma,$$

а значит и

$$S_\alpha^a S_\beta^b S_\alpha^{-a} = S_\delta^b.$$

Посредством повторного применения этих соотношений каждое произведение степеней S_α может быть преобразовано к такому виду, куда каждое S_i входит как фактор только один раз, конечно с некоторым показателем. Так как элементы S_α порождают факторгруппу $\overline{\mathfrak{G}}/\mathfrak{U}$ и в силу (4'.2) имеют конечный порядок, то группа $\overline{\mathfrak{G}}/\mathfrak{U}$ оказывается конечной, чем и завершается доказательство.

(Здесь в неявной форме использованы идеи В. Дика [5]; способом изложения доказательства я обязан О. Шрейеру).

Легко видеть, что предпосылки теоремы 2, особенно условия 2), 4) и 5) неизбежны при доказательстве конечности группы $\overline{\mathfrak{G}}$. Именно,

если $\mathfrak{H}$ не лежит в центре $\mathfrak{G}'$ и если $\mathfrak{G}$ есть, например, циклическая группа m-го порядка, то метациклическая группа $\mathfrak{G}'$ степени p и порядка mp, где p есть простое число вида $mx+1$, удовлетворяет всем остальным условиям теоремы 2. Чтобы показать это, возьмем в группе $\mathfrak{G}$

$$Q_1,\ Q_2 = Q_1^2; \qquad Q_1' = (x,\ gx+1), \qquad Q_2' = (x,\ g^2x+1) \qquad (\mathrm{mod}\, p),$$

где g есть примитивный корень сравнения $x^m \equiv 1 \pmod p$. Совокупность таких групп, очевидно, бесконечна.

Опуская условие 4), можно взять за $\mathfrak{G}'$ ($\mathfrak{G}$ берется, как выше) произвольную циклическую группу порядка mn, где n — произвольное целое число.

Если же не предполагать справедливость условия 5), то за $\mathfrak{G}'$ ($\mathfrak{G}$—как выше) можно взять прямое произведение $\mathfrak{M} \times \mathfrak{G}$, где $\mathfrak{M}$ совершенно произвольная группа.

В качестве примера возьмем симметрическую группу перестановок из трех элементов. Пусть выбранные порождающие элементы $Q_1 = (23)$, $Q_2 = (31)$, $Q_3 = (12)$ и порождающие подстановки группы $\mathfrak{H}$ $\alpha = Q_1'Q_2'Q_1'Q_3'$, $\beta = Q_2'Q_3'Q_2'Q_1'$, $\gamma = Q_3'Q_1'Q_3'Q_2'$. Имеет место: $\alpha^2 = \beta^2 = \gamma^2 = 1$, $\alpha\beta\gamma = 1$, так что $\mathfrak{H}$ есть абелева группа 4-го порядка и типа $\{2,2\}$. $\mathfrak{G}' = \mathfrak{G} \times \mathfrak{H}$.

Аналогичная задача была решена И. Шуром [6]. Вышеприведенный пример показывает, что наша задача не может рассматриваться как частный случай задачи Шура.

§ 3. Общие сведения о группах инерции полей классов

Пусть K поле, число классов которого делится на простое число p. Если $p = 2$, то классы будем понимать в узком смысле, так что число классов всегда будет равно относительной степени поля классов (понимаемого как наибольшее относительно абелево неразветвленное относительное поле).

Введем два следующих вспомогательных понятия:

Определение 1. *Нормой поля K называется наименьшее нормальное поле, содержащее K.*

Определение 2. *Нормой группы $\mathfrak{H}$, являющейся подгруппой группы $\mathfrak{G}$, называется наименьший нормальный делитель группы $\mathfrak{G}$, содержащий $\mathfrak{H}$.*

Я отмечу две известные теоремы:

Теорема 3. *Каждый элемент нормы поля K может быть выражен через элементы K и сопряженных с K полей (резольвента Галуа).*

Теорема 4. *Каждый элемент нормы группы $\mathfrak{H}$ может быть выражен через элементы $\mathfrak{H}$ и сопряженных с $\mathfrak{H}$ групп.*

Определение 3. *Пусть $\mathfrak{H}$ нормальный делитель группы $\mathfrak{G}'$, $\mathfrak{G} = \mathfrak{G}'/\mathfrak{H}$. Под отображением (Abbildung) некоторой подгруппы $\mathfrak{K}$ группы $\mathfrak{G}'$ на $\mathfrak{G}$ будем понимать совокупность тех смежных классов $\mathfrak{H}S$,*

представителями которых являются элементы $\mathfrak{K}$. *Обозначим его через* $\mathfrak{K}\mathfrak{H}/\mathfrak{H}$.

Теорема 5. *Группа* $\mathfrak{K}$ *гомоморфна группе* $\mathfrak{K}\mathfrak{H}/\mathfrak{H}$. *Отношение порядков групп* $\mathfrak{K}$ *и* $\mathfrak{K}\mathfrak{H}/\mathfrak{H}$ *равно порядку пересечения* $\mathfrak{T}$ *групп* $\mathfrak{K}$ *и* $\mathfrak{H}$.[1]

Доказательство. Пусть разложение $\mathfrak{K}$ по $\mathfrak{T}$ будет

$$\mathfrak{K} = \mathfrak{T} + \mathfrak{T}S_2 + \ldots + \mathfrak{T}S_\nu. \tag{1.3}$$

Группа $\mathfrak{T}$ отображается в единицу группы $\mathfrak{G}$. Если S_i и S_k отображаются в один и тот же элемент группы $\mathfrak{G}$, то $S_i S_k^{-1}$ отображается в 1, т. е. лежит в $\mathfrak{H}$, а следовательно и в $\mathfrak{T}$, что противоречит разложению (1.3).

Теорема 6. *Норма отображения равна отображению нормы.*

Доказательство. 1. Отображение делителя группы есть делитель ее отображения. 2. Если $\mathfrak{K}$ — нормальный делитель группы $\mathfrak{G}'$, то отображение $\mathfrak{K}$ есть нормальный делитель $\mathfrak{G}$. 3. С другой стороны, если $\overline{\mathfrak{K}} = \mathfrak{H} + \mathfrak{H}S_2 + \ldots + \mathfrak{H}S_\nu$ есть нормальный делитель группы $\mathfrak{G}$, то композит $\mathfrak{K}$ групп $\mathfrak{H}, S_2, \ldots, S_\nu$ есть нормальный делитель группы $\mathfrak{G}'$. Отображение $\mathfrak{K}$ совпадает с $\overline{\mathfrak{K}}$ и каждая подгруппа группы $\mathfrak{G}'$, отображение которой есть делитель группы $\overline{\mathfrak{K}}$, в свою очередь будет делителем группы $\mathfrak{K}$. Действительно, она содержит только элементы типа $H_\mu, H_\mu S_2, \ldots, H_\mu S_\nu$, где H принадлежит $\mathfrak{H}$. Поэтому наименьший нормальный делитель группы $\mathfrak{G}'$, содержащий $\mathfrak{K}$, отображается в наименьший нормальный делитель группы $\mathfrak{G}$, содержащий отображение $\mathfrak{K}$, ч. и т. д.

Теорема 7. *Пусть* K' *есть нормальное поле,* $\mathfrak{G}'$ *— его группа и* $\mathfrak{T}$ *— его группа инерции, соответствующая простому идеалу* $\mathfrak{P}$. *Пусть далее* K *— нормальное подполе поля* K', *принадлежащее группе* $\mathfrak{H}$ *и* $\mathfrak{G} = \mathfrak{G}'/\mathfrak{H}$ *— его группа. Если* $\mathfrak{p}$ *есть простой идеал поля* K, *делящийся на* $\mathfrak{P}$, *то группа инерции* $\mathfrak{t}$ *идеала* $\mathfrak{p}$ *равна отображению* $\mathfrak{T}\mathfrak{H}/\mathfrak{H}$ *группы* $\mathfrak{T}$ *на* $\mathfrak{G}$.

Доказательство. Группа инерции $\mathfrak{T}$ есть совокупность подстановок S, не изменяющих величины α поля K' modulo $\mathfrak{P}$

$$\alpha^S \equiv \alpha \pmod{\mathfrak{P}}.$$

Выбрав величину β в поле K, мы получим

$$\beta^S \equiv \beta \pmod{\mathfrak{P}} \text{ и потому } \beta^S \equiv \beta \pmod{\mathfrak{p}}.$$

Следовательно, группа $\mathfrak{T}\mathfrak{H}/\mathfrak{H}$ содержится в $\mathfrak{t}$.

Если K_t' есть поле инерции идеала $\mathfrak{P}$, то простой идеал поля K_t', содержащий $\mathfrak{P}$, не будет критическим в K_t'. То же обстоятельство очевидно имеет место и для поля K_{th}, принадлежащего группе $\mathfrak{T}\mathfrak{H}$ в K' (и следовательно $\mathfrak{T}\mathfrak{H}/\mathfrak{H}$ в K), так как K_{th} есть подполе поля K_t'.

[1] Автор употребляет термин: изоморфный (*Ред.*).

Но отсюда, в силу теоремы 1, следует, что $\mathfrak{T}\mathfrak{H}/\mathfrak{H}$ содержит группу инерции t идеала $\mathfrak{p}$. Следовательно $\mathfrak{T}\mathfrak{H}/\mathfrak{H} = \mathfrak{t}$.

Из теорем 6 и 7 следует

Теорема 8. *Отображение нормы группы инерции поля K' на $\mathfrak{G}$ есть соответствующая норма группы инерции поля K.*

Теорема 9. *Если поле K' относительно неразветвлено над K, то группа $\mathfrak{H}$ взаимно проста с каждой группой инерции поля K'.*

Доказательство. Если K' относительно неразветвлено над K, то порядок каждой группы инерции $\mathfrak{T}$ поля K' равен порядку соответствующей группы инерции поля K, так как порядок группы инерции равен показателю степени, в которой соответствующий простой идеал входит в p. Из теоремы 7 следует, что группа $\mathfrak{T}$ изоморфна с ее отображением на $\mathfrak{G}$. Отсюда, согласно теореме 5, следует, что группы $\mathfrak{T}$ и $\mathfrak{H}$ взаимно просты.

Теоремы 7, 8 и 9 могут быть обобщены на относительные поля, если принять за область рациональности произвольное поле. Если в этом случае под «группой инерции» понимать относительную группу инерции относительно области рациональности и заменить p некоторым простым идеалом области рациональности, то все наши рассуждения останутся неизменными.

Сообразно структурам групп $\mathfrak{G}'$, $\mathfrak{T}'$, $\mathfrak{H}$ мы подразделим частичные поля классов и соответствующие множители чисел классов на четыре типа.

Определение 4. *Пусть $\mathfrak{N}$—наибольшая подгруппа группы $\mathfrak{G}'$, элементы которой перестановочны со всеми элементами $\mathfrak{H}$ и K_n—принадлежащее группе $\mathfrak{N}$ поле.*

I. *Если $\mathfrak{N} = \mathfrak{H}$, то соответствующее элементарное (абсолютно нормальное) частичное поле классов (а равно и множитель числа классов $p^{\mu\nu}$) назовем собственным (eigentlich).*

II. *Если $\mathfrak{N} > \mathfrak{H}$ и группа $\mathfrak{H}$ взаимно проста с композитом $\mathfrak{M}$ всех относительных групп инерции поля K_p относительно K_n, то K_p и $p^{\mu\nu}$ назовем несобственными (uneigentlich).*

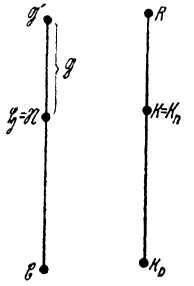
III. *Если $\mathfrak{N} > \mathfrak{H}$ и поле K_p (не обязательно элементарное) обладает относительно K_n некоторой относительной группой инерции $\mathfrak{T}'$, норма которой $\mathfrak{T}$ (относительно $\mathfrak{N}$) не взаимно проста с $\mathfrak{H}$, то назовем поле K_p и множитель $p^{\mu\nu}$ центральными.*

IV. *Если $\mathfrak{N} > \mathfrak{H}$ и $\mathfrak{M}$ не взаимно проста с $\mathfrak{H}$, в то время как каждая норма $\mathfrak{T}$, упомянутая в III, взаимно проста с $\mathfrak{H}$, то $p^{\mu\nu}$ назовем родовым множителем числа классов (Geschlechterklassenzahlfaktor).*

Очевидно, что одно и то же простое число p может входить в различные множители числа классов.

§ 4. Собственные множители числа классов

В случае $\mathfrak{N} = \mathfrak{H}$ каждое преобразование группы $\mathfrak{H}$, произведенное посредством некоторой подстановки группы $\mathfrak{G} \longleftrightarrow \mathfrak{G}' / \mathfrak{H}$, производит действительное перемещение элементов $\mathfrak{H}$.



Фиг. 1 [1]

Таким образом, группа $\mathfrak{G}$ есть делитель *голоморфа*, т. е. группы всех внешних автоморфизмов группы $\mathfrak{H}$. Если $\mathfrak{H}$ есть *абелева* группа ν-членного типа $\{p, p, \ldots, p\}$, то группа $\mathfrak{G}$ изоморфна с некоторой группой целочисленных однородных линейных подстановок ν переменных, взятых по модулю p. Если же $\mu \neq 1$, то группа $\mathfrak{G}$ допускает более сложное представление [7].

Мы исследуем подробнее случай $\mu = 1$. Всегда существует абсолютно нормальное подполе поля K_1', относительная группа которого имеет ν-членный тип $\{p, p, \ldots, p\}$ (это частичное поле классов может, однако, не быть собственным). Если это поле собственное, то мы заключаем, что порядок g группы $\mathfrak{G}$ есть делитель произведения

$$(p^\nu - 1)(p^\nu - p)\ldots(p^\nu - p^{\nu-1}). \tag{1.4}$$

Отсюда вытекают ограничения для p и ν.

В частности, если $\nu = 1$, т. е. поле классов K_p' относительной степени p над K абсолютно нормально, то группа $\mathfrak{G}$ должна быть циклической, причем

$$p \equiv 1 \pmod{g}. \tag{2.4}$$

Следовательно, этот случай встречается только в круговых полях.

Дальнейшее ограничение для p и ν вытекает из того, что упомянутое представление группы $\mathfrak{G}$, как группы сравнений по $\bmod p$, должно быть *нераспадающимся* (unzerfällbar) [2] в поле рациональных вычетов $\bmod p$. Действительно, если эта группа *приводима* (reduzibel),[2] то найдется μ ($\mu < \nu$) линейно независимых $\bmod p$ целочисленных линейных функций

$$y_1 = \alpha_{i1} x_1 + \alpha_{i2} x_2 + \ldots + \alpha_{i\nu} x_\nu \qquad (i = 1, 2, \ldots, \mu),$$

которые подстановками группы $\mathfrak{G}$ переводятся друг в друга. Тогда группа с базисом

$$B_i = A_1^{\alpha_{i1}} A_2^{\alpha_{i2}} \ldots A_\nu^{\alpha_{i\nu}},$$

[1] На всех встречающихся здесь фигурах каждая точка слева означает группу. На каждой соединяющей эти точки линии верхняя точка обозначает надгруппу, нижняя — подгруппу. Соответствующая точка на правой стороне обозначает поле, принадлежащее этой группе.

Это графическое представление я ввел по совету Гассе. Ср. H. Hasse. Höhere Algebra, 2. Berlin, 1927, стр. 103, 122, 123.

[2] Эта терминология заимствована из работы J. Schur. Über die stetige Darstellungen der allgemeinen linearen Gruppe. Sitzber. Berl. Akad., 1928. стр. 100.

где $A_1, A_2, \ldots, A_\nu$ есть базис $\mathfrak{H}$, будет нормальным делителем группы $\mathfrak{G}'$, содержащимся в $\mathfrak{H}$.

Если группа распадается (вполне приводима), то найдется два взаимно простых делителя группы $\mathfrak{H}$, произведение которых воспроизводит всю группу $\mathfrak{H}$ и каждый из которых является нормальным делителем группы $\mathfrak{G}'$. Поля, принадлежащие к этим группам внутри K_p абсолютно нормальны, имеют пересечением поле K и композитом — поле K_p. Существование их опровергается предположением, что K_p есть элементарное абсолютное нормальное поле. [1]

Из определения элементарного поля следует, что (при $\mu = 1$) каждое элементарное поле может быть порождено посредством композиции сопряженных полей относительной степени p над K. Это значит, что группа $\mathfrak{H}$ содержит делитель $\mathfrak{H}_1$, порядка $p^{\nu-1}$, который уже не содержит нормальных делителей группы $\mathfrak{G}'$. Если $\mathfrak{H} = A_1^{x_1} A_2^{x_2} \ldots A_\nu^{x_\nu}$ $(x_i = 0, 1, \ldots, p-1;\ i = 1, 2, \ldots, \nu)$, то каждая подгруппа порядка $p^{\nu-1}$ группы $\mathfrak{H}$ состоит из элементов вида $A_1^{x_1} A_2^{x_2} \ldots A_\nu^{x_\nu}$, где $x_1, x_2, \ldots, x_\nu$ подчинены некоторому сравнению

$$m_1 x_1 + m_2 x_2 + \ldots + m_\nu x_\nu \equiv 0 \pmod{p}. \qquad (3.4)$$

Пересечение группы $\mathfrak{H}_1$ и сопряженных с ней групп состоит из элементов того же вида, где $x_1, x_2, \ldots, x_\nu$ подчинены не более чем g независимым сравнениям типа (3.4). Так как в силу наших предположений эта система сравнений должна допускать только тривиальное решение $x_i \equiv 0 \pmod{p}$ $(i = 1, 2, \ldots, \nu)$, то отсюда вытекает, что

$$\nu \leqslant g.$$

Допустим, что $\nu = g$. Тогда левые части сравнений (3.4), соответствующих всем подстановкам группы $\mathfrak{G}$, должны быть линейно независимы $(\mathrm{mod}\ p)$. Отсюда следует, что пересечение $\mathfrak{h}_1$ $\nu - 1$ сопряженных с $\mathfrak{H}_1$ групп имеет порядок p, так как соответствующие ему $x_1, x_2, \ldots, x_\nu$ удовлетворяют $\nu - 1$ независимым сравнениям типа (3.4). Композит всех сопряженных с $\mathfrak{h}_1$ групп равен $\mathfrak{H}$, так как соответствующие ему $x_1, x_2, \ldots, x_\nu$ свободны от всех условий (3.4). (Заметим, что соответствующие композиту групп $\mathfrak{R}_1$ и $\mathfrak{R}_2$ величины $x_1, x_2, \ldots, x_\nu$

[1] Приводимая группа не должна здесь быть необходимо распадающейся, как это показал мне О. Шрейер на примере группы порядка p^3, определенной соотношениями

$$A^p = B^p = \Theta^p = 1. \qquad \Theta A \Theta^{-1} = A, \qquad \Theta B \Theta^{-1} = AB.$$

(ср. O. Hölder, Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. Math. Ann. 43 (1893), стр. 383, строка 10 сверху). Это свойство обязательно имеет место, если порядок $\mathfrak{G}'/\mathfrak{H}$ взаимно прост с p как это следует из формулы Шура, содержащей в знаменателе порядок $\mathfrak{G}'/\mathfrak{H}$ (J Schur. Neue Begründung der Theorie der Gruppencharaktere. Sitzber Berl Akad, 1905, стр. 415, строка 3 снизу).

удовлетворяют тем и только тем условиям, которые получаются линейной комбинацией из условий, соответствующим группам $\mathfrak{K}_1$ и $\mathfrak{K}_2$.) Таким образом, группа $\mathfrak{H}$ представима через посредство ν-членного базиса $A_1, S_1A_1S_1^{-1}, S_2A_1S_2^{-1}, \ldots, S_{\nu-1}A_1S_{\nu-1}^{-1}$, где A_1 есть производящая подстановка группы $\mathfrak{h}_1$, а $1, S_1, S_2, \ldots, S_{\nu-1}$ суть всевозможные подстановки группы $\mathfrak{G}$. Если мы произведем над системой $A_1, S_1A_1S_1^{-1}, \ldots, S_{\nu-1}A_1S_{\nu-1}^{-1}$ одну из подстановок группы $\mathfrak{G}$, то элементы этой системы претерпят некоторую подстановку, так что группа $\mathfrak{G}$ будет представлена как транзитивная группа подстановок ν символов. Но каждая группа подстановок вполне приводима [8] и притом обладает неприводимой частью первой степени, соответствующей тождественному представлению. Остальные составные части будут также рациональны и, следовательно, представимы посредством целочисленных матриц (ср. [7], теорема 184, стр. 206). Если мы будем рассматривать это представление как группу сравнений $(\mathrm{mod}\, p)$, то она снова породит всю группу $\mathfrak{G}$, исключая только случай $p = 2$, $\nu = 2$ ([7], стр. 209, теорема 187). Поэтому группа $\mathfrak{H}$ распадается на два взаимно простых фактора, каждый из которых является нормальным делителем группы $\mathfrak{G}$, что противоречит нашему предположению. Следовательно,[1]

$$\nu < g. \tag{4.4}$$

Исключение составляет только группа 8-го порядка (Doppelkegelgruppe): $\mathfrak{H} = \{A, B\}$, $AB = BA$, $A^2 = B^2 = 1$; $\mathfrak{G}' = \{A, B, \theta\}$, $\theta^2 = 1$ $\theta A\theta^{-1} = A$, $\theta B\theta^{-1} = BA$. Здесь $p = 2$, $\nu = g = 2$.

Такими представлениями групп полей классов занимался также Шпайзер ([7], стр. 239).

Для специальных типов групп $\mathfrak{G}$ можно дать более точные оценки числа ν.

Одно и то же простое число, при заданном поле K, может, очевидно, соответствовать различным элементарным полям классов, которые могут принадлежать как одному и тому же „типу", так и различным «типам». Кроме того, само разложение поля классов на элементарные поля может быть не однозначным. Таким образом, неравенство (4.4) не может быть рассматриваемо как ограничение для степени, в которой простое число p содержится в числе классов поля K.

Мы пришли к следующим теоремам.

Теорема 10. *Если K_p есть собственное элементарное абсолютно нормальное частичное поле классов над K, относительная группа которого имеет ν-членный тип $\{p, p, \ldots, p\}$, то группа $\mathfrak{G}$ поля K изоморфна некоторой неразложимой группе целочислен-*

[1] См. поправку в конце статьи (*Ред.*).

ных однородных линейных подстановок ν *переменных, рассматриваемой по* mod p.

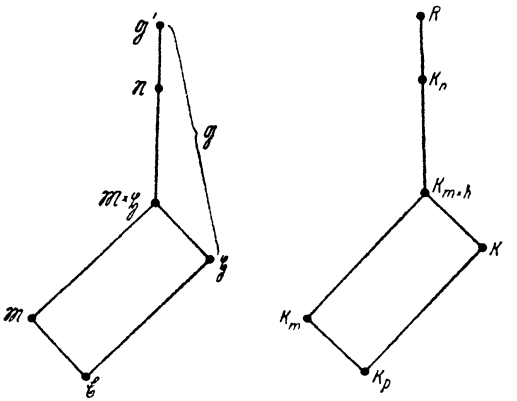
Теорема 11. *Если простое число* p *входит как собственный фактор первой степени в число классов нормального поля* K, *то* K *есть круговое поле, степень которого есть делитель числа* $p-1$.

Замечание. Предыдущие рассуждения можно обобщить, взяв вместо K_p какое-либо неразветвленное над K поле и вместо $\mathfrak{H}$ — его относительную группу *Галуа*. Тогда группа $\mathfrak{G}$ должна быть делителем голоморфа группы $\mathfrak{H}$. В этом случае исследование значительно усложняется, так как мы до сих пор не знаем никакого аналитического способа для представления голоморфа произвольной группы.

§ 5. Несобственные множители числа классов

Рассмотрим теперь случай, когда в группе $\mathfrak{G}'$ содержатся отличные от подстановок $\mathfrak{H}$ подстановки, перестановочные со всеми подстановками группы $\mathfrak{H}$. Подстановки эти образуют группу $\mathfrak{N}$, являющуюся нормальным делителем группы $\mathfrak{G}'$. Факторгруппа $\mathfrak{G}'/\mathfrak{N}$ изоморфна группе внешних автоморфизмов группы $\mathfrak{H}$.

Пусть группе $\mathfrak{N}$ принадлежит поле K_n. Построим все группы инерции поля K_p относительно K_n. Они порождают совместно группу $\mathfrak{M}$, к которой, согласно теореме 1а, принадлежит наибольшее неразветвленное над K_n подполе K_m поля K_p.



Фиг. 2

В нашем случае $\mathfrak{M}$ и $\mathfrak{H}$ взаимно просты, произведение $\mathfrak{M}\times\mathfrak{H}$ есть прямое произведение и содержится в $\mathfrak{N}$. Поле K_p получается посредством композиции полей K_m и K, которые принадлежат в поле K_p к группам $\mathfrak{M}$ и $\mathfrak{H}$ и имеют пересечение $K_{m\times h}$, принадлежащее в K_p к группе $\mathfrak{M}\times\mathfrak{H}$. Относительное поле K_p над $K_{m\times h}$ распадается на два взаимно простых относительных поля над $K_{m\times h}$: 1) $K_h=K$; 2) поле K_m, которое будет абелевым и неразветвленным над $K_{m\times h}$, т. е. полем классов. Следовательно, $p^{\mu\nu}$ будет множителем числа классов наиболее узкого поля $K_{m\times h}$. Соответствующая ему группа $\mathfrak{N}$ изоморфна $\mathfrak{N}/\mathfrak{M}$. В самом деле, каждый элемент группы $\mathfrak{G}'/\mathfrak{M}_1$, перестановочный с каждым элементом группы $\mathfrak{M}\times\mathfrak{H}/\mathfrak{M}$, соответствует некоторому элементу S группы $\mathfrak{G}'$, связанному с каждым элементом H группы $\mathfrak{H}$ соотношением $SHS^{-1}=HM$, где M принадлежит груп-

пе $\mathfrak{M}$. Так как SHS^{-1} содержится в $\mathfrak{H}$ и группа $\mathfrak{M}$ взаимно проста с $\mathfrak{H}$, то необходимо $M=1$, т. е. элементы S и H перестановочны.

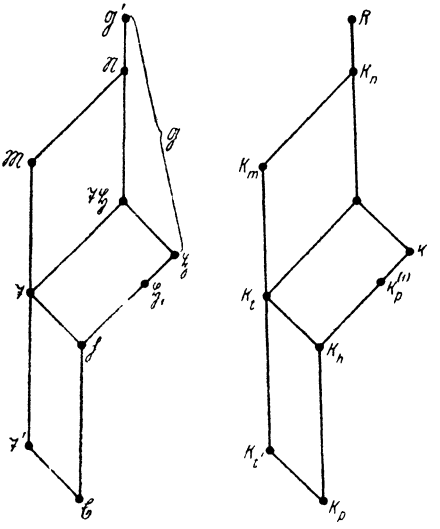
Если $\mathfrak{M}\times\mathfrak{H}$ совпадает с $\mathfrak{N}$, то мы возвращаемся к случаю собственного множителя. Если же это не так, то мы имеем случай несобственного множителя числа классов, причем $\mathfrak{M}=1$. Тогда K_p не разветвляется над K_n. Если при этом группа $\mathfrak{H}$ абелева, то K_p есть поле классов относительно K_n. Во всяком случае, $\mathfrak{G}'/\mathfrak{N}$ содержится в голоморфе группы $\mathfrak{N}$, так как в $\mathfrak{G}'$ нет не принадлежащих $\mathfrak{N}$ подстановок, перестановочных со всеми подстановками группы $\mathfrak{H}$, а тем более и ни одной подстановки, перестановочной со всеми подстановками группы $\mathfrak{N}$.

Здесь вступает в силу «замечание» § 4. Если группа $\mathfrak{N}$ разрешима, то K_p есть башня полей классов (Klassenkörperturm) над K_n [9].

Таким образом, мы приходим к следующей теореме.

Теорема 12. *Если K_p есть несобственное элементарное абсолютно нормальное частичное поле классов над K, то его подполе $K_{m\times h}$ также имеет поле классов K_m, относительная группа которого изоморфна относительной группе K_p над K. Это поле классов будет собственным или несобственным, смотря по тому, совпадают или нет введенные в определении 4 группы $\mathfrak{N}$ и $\mathfrak{M}\times\mathfrak{H}$.*

Поле K_m, принадлежащее группе $\mathfrak{M}$, не разветвлено над K_n. Группа Галуа поля K_n содержится в голоморфе группы $\mathfrak{N}/\mathfrak{M}$.



Фиг. 3

§ 6. Центральные множители числа классов

В этом случае в поле K_p найдется группа инерции $\mathfrak{T}'$ относительно $\mathfrak{N}$, норма которой относительно $\mathfrak{N}$ содержит отличный от 1 делитель $\mathfrak{h}$ группы $\mathfrak{H}$. Если $\mathfrak{h}$ есть наибольший делитель группы $\mathfrak{H}$, содержащийся в $\mathfrak{T}$, то $\mathfrak{h}$ является нормальным делителем как группы $\mathfrak{N}$, так и группы $\mathfrak{T}$. Группа $\mathfrak{h}$ содержится в центре группы $\mathfrak{T}$ и, согласно теореме 9, взаимно проста с $\mathfrak{T}'$. Группы $\mathfrak{H}/\mathfrak{h}$ и $\mathfrak{T}/\mathfrak{h}$ суть нормальные делители группы $\mathfrak{N}/\mathfrak{h}$ и притом взаимно просты, т. е. $\mathfrak{N}/\mathfrak{h}$ содержит прямое произведение $\mathfrak{H}/\mathfrak{h}\times\mathfrak{T}/\mathfrak{h}$. Следовательно, группа $\mathfrak{N}/\mathfrak{h}/\mathfrak{H}/\mathfrak{h}=\mathfrak{N}/\mathfrak{H}$ имеет подгруппу $\mathfrak{T}\mathfrak{H}/\mathfrak{H}$, изоморфную группе $\mathfrak{T}/\mathfrak{h}$, т. е. группа $\mathfrak{T}/\mathfrak{h}$ изоморфна делителю группы $\mathfrak{G}=\mathfrak{G}'/\mathfrak{H}$.

Разложим $\mathfrak{N}$ по $\mathfrak{H}$

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}F_2+\ldots+\mathfrak{H}F_k. \tag{1.6}$$

$K = (\mathfrak{N} : \mathfrak{H})$ есть порядок некоторой подгруппы $\mathfrak{G}$, т. е. зависит только от $\mathfrak{G}$. Каждый элемент одного и того же класса смежности разложения (1.6) переводит $\mathfrak{T}'$ в одну и ту же группу, так как $\mathfrak{H}$ содержится в центре группы $\mathfrak{N}$. Следовательно, число групп, сопряженных с группой инерции $\mathfrak{T}'$ (относительно $\mathfrak{N}$), есть делитель порядка группы $\mathfrak{G}$. С другой стороны, так как в силу теорем 7 и 5 группа $\mathfrak{T}'$ изоморфна с соответствующей группой инерции поля K, которая в свою очередь есть делитель группы $\mathfrak{G}$, то в $\mathfrak{T}'$ можно выбрать некоторое число элементов $Q_1', Q_2', \ldots, Q_\alpha'$, порождающих всю группу $\mathfrak{T}'$, причем α будет зависеть только от $\mathfrak{G}$. Порядки элементов $Q_1' Q_2', \ldots, Q_\alpha'$, очевидно, равны порядкам тех элементов $Q_1, Q_2, \ldots, Q_\alpha$ группы $\mathfrak{G}$, которые при отображении $\mathfrak{T}' \to \mathfrak{T}'\mathfrak{H} / \mathfrak{H} = \mathfrak{T}\mathfrak{H} / \mathfrak{H}$ соответствуют элементам $Q_1', Q_2', \ldots, Q_\alpha'$. Если мы построим систему сопряженных с последними относительно $\mathfrak{N}$ элементов $Q_1', Q_2', \ldots, Q_m'$, то m будет также зависеть только от $\mathfrak{G}$. Композиция же элементов этой системы порождает всю группу $\mathfrak{T}$, так как $\mathfrak{T}$ есть норма группы $\mathfrak{T}'$ относительно $\mathfrak{N}$.

Сопоставляя все эти обстоятельства с условиями теоремы 2 и взаимно относя друг другу

в теореме 2:	$\mathfrak{G}$	$\mathfrak{G}'$	$\mathfrak{H}$	$Q_1, Q_2, \ldots, Q_m$	$Q_1', Q_2', \ldots, Q_m'$
здесь:	$\mathfrak{T}\mathfrak{H} / \mathfrak{H}$	$\mathfrak{T}$	$\mathfrak{h}$	$Q_1, Q_2, \ldots, Q_m$	$Q_1', Q_2', \ldots, Q_m'$

мы видим, что все условия теоремы 2 выполнены. (При этом мы не обращаем внимания на то, что некоторые из элементов Q_i могут совпадать.) Следовательно, все возможные группы $\mathfrak{h}$ полностью определяются структурой группы $\mathfrak{G}$. Число групп, сопряженных с $\mathfrak{h}$ относительно $\mathfrak{G}'$, также зависит только от группы $\mathfrak{G}$, откуда следует, что порядок нормы $\mathfrak{H}_1$ группы $\mathfrak{h}$ относительно $\mathfrak{G}'$ зависит только от $\mathfrak{G}$.

Рассмотрим теперь поле $K_p^{(1)}$, принадлежащее к группе $\mathfrak{H}_1$ внутри K_p. Может случиться, что нормализатор $\mathfrak{N}_1 / \mathfrak{H}_1$ элементов $\mathfrak{H} / \mathfrak{H}_1$ будет больше, чем $\mathfrak{N} / \mathfrak{H}_1$. Тогда $K_p^{(1)}$ может быть центральным частичным полем классов над K. Продолжая таким же образом далее, мы после некоторого, зависящего только от $\mathfrak{G}$, числа a шагов (a не больше, чем число членов *главного ряда* группы $\mathfrak{G}$) придем к полю $K_p^{(a)}$, относительная группа которого $\mathfrak{H} / \mathfrak{H}_a$ имеет нормализатор $\mathfrak{N}_a / \mathfrak{H}_a$, равный $\mathfrak{N}_{a-1} / \mathfrak{H}_a$. Тогда мы утверждаем, что $K_p^{(a)}$ не является центральным частичным полем классов относительно своей группы инерции $\mathfrak{T}'_{a-1} \mathfrak{H}_a / \mathfrak{H}_a$ (см. теорему 7). В самом деле, если относительной группе $\mathfrak{T}'_{a-1}$ по отношению к $K_p^{(a-1)}$ соответствует простой идеал $\mathfrak{P}_{a-1}$ поля $K_p^{(a-1)}$, то содержащему идеал $\mathfrak{P}_{a-1}$ простому идеалу $\mathfrak{P}_a$ поля $K_p^{(a)}$ соответствует относительная группа $\mathfrak{T}_a'$. Так как поле $K_p^{(a-1)}$ не разветвляется над $K_p^{(a)}$, то, в силу теоремы 7, группа $\mathfrak{T}'_a$ изоморфна группе $\mathfrak{T}'_{(a-1)}$ и отнесена ей отображением $\mathfrak{N}_a / \mathfrak{H}_{a-1} \to \mathfrak{N}_a / \mathfrak{H}_a$. Поэтому норма $\mathfrak{T}_a$ группы $\mathfrak{T}'_a$ относительно $\mathfrak{N}_a / \mathfrak{H}_a$

равна отображению $\mathfrak{T}_{a-1}\mathfrak{H}_a/\mathfrak{H}_a$ группы $\mathfrak{T}_{a-1}$ на $\mathfrak{N}_a/\mathfrak{H}_a$, где $\mathfrak{T}_{a-1}$ есть норма $\mathfrak{T}'_{a-1}$ относительно $\mathfrak{N}_{a-1}/\mathfrak{H}_{a-1}=\mathfrak{N}_a/\mathfrak{H}_{a-1}$ (теорема 8). Но так как $\mathfrak{T}_{a-1}$ имеет с $\mathfrak{H}/\mathfrak{H}_{a-1}$ пересечением группу $\mathfrak{h}_{a-1}$, которая содержится в $\mathfrak{H}_a$, то $\mathfrak{T}_{a-1}\mathfrak{H}_a/\mathfrak{H}_a$ и $\mathfrak{H}/\mathfrak{H}_a$ суть взаимно простые группы, ч. и т. д.

Если мы последовательно возьмем в роли $\mathfrak{N}/\mathfrak{H}$ и $\mathfrak{T}\mathfrak{H}/\mathfrak{H}$ все нормальные делители группы $\mathfrak{G}$ и для каждой пары групп ($\mathfrak{T}\mathfrak{H}/\mathfrak{H}$ при этом должна быть делителем $\mathfrak{N}/\mathfrak{H}$) проведем вышеописанное построение, относя элементам $Q_1', Q_2', \ldots, Q_m'$ все возможные комбинации элементов $\mathfrak{T}/\mathfrak{H}$ с повторениями (при условии, чтобы сюда с каждым элементом Q_l' входили все его сопряженные относительно $\mathfrak{N}/\mathfrak{H}$ элементы; верхняя граница числа m зависит только от группы $\mathfrak{G}$), то таким путем мы исчерпаем все возможные группы $\mathfrak{h}$, которые могут соответствовать центральным частичным полям классов для какой-нибудь группы $\mathfrak{T}'$. Отсюда следует

Теорема 13. *Все возможные группы $\mathfrak{H}$, соответствующие центральным множителям числа классов, полностью определяются структурой группы $\mathfrak{G}$.*[1]

При доказательстве мы не пользовались тем, что K_p есть элементарное поле. Поэтому мы можем считать, что K_p есть полное поле классов поля K. Если $\overline{K}$ — наиболее широкое центральное частичное поле классов над K и $\overline{K}^{(a)}$ — наиболее широкое не центральное над K подполе поля $\overline{K}$, то максимальная относительная степень $\overline{K}$ над $\overline{K}^{(a)}$ определяется структурой группы $\mathfrak{G}$ поля K. Это замечание имеет место также и для родовых множителей (§ 7).

Теорема 14. *Центральные множители числа классов не встречаются в циклических полях.*

Доказательство. Пусть $\mathfrak{H}$ лежит в центре $\mathfrak{N}$ и группа $\mathfrak{N}/\mathfrak{H}$ — циклическая. Тогда группа $\mathfrak{N}$ допускает следующее разложение:

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}S+\ldots+\mathfrak{H}S^{m-1},$$

где m — порядок группы $\mathfrak{N}/\mathfrak{H}$. Если $U=H_1S^i$ и $V=H_2S^j$ — два элемента группы $\mathfrak{N}$, то

$$UV=H_1H_2S^{i+j}=VU,$$

т. е. группа $\mathfrak{N}$ — *абелева*. Следовательно, $\mathfrak{T}'=\mathfrak{T}$, что невозможно, так как, по теореме 9, $\mathfrak{T}'$ и $\mathfrak{H}$ взаимно просты, в то время как $\mathfrak{T}$ и $\mathfrak{H}$ не взаимно просты.

§ 7. Родовые множители числа классов

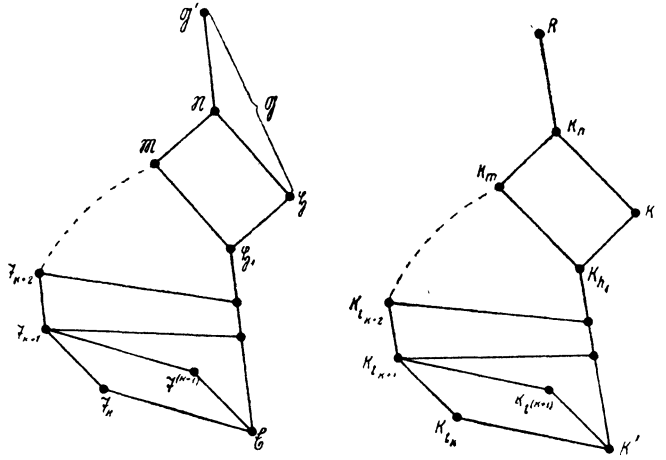
В этом случае не существует такой относительной группы инерции, норма которой (относительно $\mathfrak{N}$) не была бы взаимно простой

[1] Очевидно, что число возможных *абелевых* групп при заданном порядке ограничено.

с $\mathfrak{H}$, композит же $\mathfrak{M}$ всех относительных групп инерции имеет отличное от 1 пересечение $\mathfrak{H}_1$ с группой $\mathfrak{H}$. Так как $\mathfrak{M}$ есть нормальный делитель группы $\mathfrak{G}'$, то и $\mathfrak{H}_1$ есть также нормальный делитель.

Пусть $\mathfrak{T}, \mathfrak{T}', \ldots, \mathfrak{T}^{(a)}$ будут все нормы групп инерции, взятые относительно $\mathfrak{N}$ и расположенные в каком-нибудь порядке. Построим группы $\mathfrak{T}_1, \mathfrak{T}_2, \ldots, \mathfrak{T}_a$, где $\mathfrak{T}_k = \mathfrak{T}\mathfrak{T}' \ldots \mathfrak{T}^{(k)} (k = 1, 2, \ldots, a)$ есть композит групп $\mathfrak{T}, \mathfrak{T}', \ldots, \mathfrak{T}^{(k)}$.

Так как в конце ряда $\mathfrak{T}_0, \mathfrak{T}_1, \ldots$ расположена группа $\mathfrak{M}$, которая, согласно вышесказанному, содержит группу $\mathfrak{H}_1$, то найдется такая $\mathfrak{T}_k$, которая будет взаимно проста с $\mathfrak{H}_1$, в то время как все $\mathfrak{T}_k\mathfrak{T}^{(k+1)}$, $\mathfrak{T}_k\mathfrak{T}^{(k+2)}, \ldots, \mathfrak{T}_k\mathfrak{T}^{(a)}$ уже не будут взаимно просты с $\mathfrak{H}_1$ (при этом, возможно, придется изменить последовательность групп $\mathfrak{T}, \mathfrak{T}', \mathfrak{T}'', \ldots, \mathfrak{T}^{(a)}$).



Фиг. 4

Рассмотрим теперь отображения $\mathfrak{H}_1\mathfrak{T}_k/\mathfrak{T}_k, \mathfrak{T}^{(k+1)}\mathfrak{T}_k/\mathfrak{T}_k, \ldots, \mathfrak{T}^{(a)}\mathfrak{T}_k/\mathfrak{T}_k$ групп $\mathfrak{H}_1, \mathfrak{T}^{(k+1)}, \ldots, \mathfrak{T}^{(a)}$ на $\mathfrak{N}\mathfrak{T}_k$. Так как $\mathfrak{H}_1$ и $\mathfrak{T}_k$ — взаимно просты, то, по теореме 5, порядки групп $\mathfrak{H}_1$ и $\mathfrak{H}_1\mathfrak{T}_k/\mathfrak{T}_k$ равны. Композит же $\mathfrak{T}^{(k+1)}\mathfrak{T}_k/\mathfrak{T}_k \cdot \mathfrak{T}^{(k+2)}\mathfrak{T}_k/\mathfrak{T}_k \ldots \mathfrak{T}^{(a)}\mathfrak{T}_k/\mathfrak{T}_k$ содержит $\mathfrak{H}_i\mathfrak{T}_k/\mathfrak{T}_k$. Следовательно, порядок группы $\mathfrak{H}_1$ есть делитель произведения порядков $\mathfrak{T}^{(k+1)}\mathfrak{T}_k/\mathfrak{T}_k, \mathfrak{T}^{(k+2)}\mathfrak{T}_k/\mathfrak{T}_k, \ldots, \mathfrak{T}^{(a)}\mathfrak{T}_k/\mathfrak{T}_k$, а значит и произведения порядков $\mathfrak{T}^{(k+1)}, \mathfrak{T}^{(k+2)}, \ldots, \mathfrak{T}^{(a)}$.

Докажем, что каждая из групп $\mathfrak{T}^{(i)}$ $(i = k+1, \ldots, a)$ имеет факторгруппу, некоторый делитель которой $\overline{\mathfrak{h}}_i$ будет изоморфен с фактором $\mathfrak{h}_i/\mathfrak{h}_{i-1}$ композиционного ряда группы $\mathfrak{H}$, так что, в частности, $\mathfrak{h}_a = \mathfrak{H}_1$. Для этого заметим, что каждая из групп $\mathfrak{T}^{(i)}\mathfrak{T}_k/\mathfrak{T}_k (i = k+1, \ldots, a)$ содержит делитель группы $\mathfrak{H}_1\mathfrak{T}_k/\mathfrak{T}_k$. Пусть для $i = k+1$ этот делитель будет $\overline{\mathfrak{h}}_{k+1}$. Он будет нормальным делителем группы $\mathfrak{N}/\mathfrak{T}_k$. Далее, группа $\mathfrak{T}^{(k+2)}\mathfrak{T}_{k+1}/\mathfrak{T}_{k+1}$ должна содержать делитель группы $\mathfrak{H}_1\mathfrak{T}_{k+1}/\mathfrak{T}_{k+1}$, изоморфный с делителем $\mathfrak{h}_{k+2}/\mathfrak{h}_{k+1}$ группы $\mathfrak{H}_1/\mathfrak{h}_{k+1}$.

Продолжая так, мы придем наконец к $\mathfrak{H}_1 / \mathfrak{h}_{a-1}$, так как в противном случае группа $\mathfrak{H}_1$ не содержалась бы в $\mathfrak{T}_a = \mathfrak{M}$.

Так как группы $\mathfrak{H}$ и $\mathfrak{T}^{(i)}$ взаимно просты, то отображение $\mathfrak{t}^{(i)} = \mathfrak{T}^{(i)}\mathfrak{H} / \mathfrak{H}$ группы $\mathfrak{T}^{(i)}$ на $\mathfrak{G}$ изоморфно с $\mathfrak{T}^{(i)}$. Но, по теореме 8, $\mathfrak{t}^{(i)}$ есть одна из норм относительных групп инерции поля K по отношению к K_n. Поэтому группу $\mathfrak{H}_1$ можно разложить в цепь факторгрупп, каждый член которой есть группа, изоморфная с одним из делителей некоторой факторгруппы группы $\mathfrak{t}^{(i)}$. Порядок же $\mathfrak{H}_1$ не может быть делителем порядка $\mathfrak{G}$, так как группы $\mathfrak{t}^{(i)}$, соответствующие различным группам $\mathfrak{T}^{(i)}$, могут полностью или частично совпадать. Следовательно, необходимое условие существования родового поля классов состоит в том, чтобы поле K содержало различные критические простые идеалы и чтобы группа $\mathfrak{M}\mathfrak{H} / \mathfrak{H}$, порожденная композицией норм групп инерции $\mathfrak{t}^{(i)}$, порождалась также композицией правильного подмножества $\mathfrak{t}^{(k+1)}, \mathfrak{t}^{(k+2)}, \ldots, \mathfrak{t}^{(a)}$ этих норм. Другими словами, остальные нормы должны быть излишними для построения полной относительной группы K над K_m.

Пусть K' есть некоторое поле классов над K и K_{h_1} — поле, принадлежащее в K' к группе $\mathfrak{H}_1$. K_{h_1} может равным образом быть родовым полем классов над K (даже центральным полем классов), так как соответствующее ему поле K_n может быть другим. По теореме 8, нормы $\mathfrak{T}^{(i)}$ групп инерции не изменяются при отображении на $\mathfrak{N} / \mathfrak{H}_1$. Эти отображения $\mathfrak{T}^{(i)}\mathfrak{H}_1 / \mathfrak{H}_1$ суть делители соответствующих норм $\bar{\mathfrak{T}}^{(i)}\mathfrak{H}_1 / \mathfrak{H}_1$ относительных групп инерции по отношению к новому полю K_n. Если K_{h_1} — центральное над K поле, то по § 6 мы найдем подполе $K_{\bar{h}_1}$, которое не будет центральным над K, в то время как $\frac{K_{h_1}}{K_{\bar{h}_1}}$ будет соответствовать центральному множителю числа классов. Обозначим $K_{\bar{h}_1}$ снова через K_{h_1}. Тогда, как группы $\mathfrak{T}^{(i)}\mathfrak{H}_1 / \mathfrak{H}_1$, так и их композит $\mathfrak{M}\mathfrak{H}_1 / \mathfrak{H}_1$ будут взаимно просты с $\mathfrak{H} / \mathfrak{H}_1$. Предположим, что композит $\bar{\mathfrak{M}}$ групп $\bar{\mathfrak{T}}^{(i)}$ имеет с $\bar{\mathfrak{H}} / \mathfrak{H}_1$ отличное от единицы пересечение $\bar{\mathfrak{H}}_1 / \mathfrak{H}_1$.

Пусть $\bar{\mathfrak{T}}_l = \mathfrak{M}\bar{\mathfrak{T}}^{(1)}\bar{\mathfrak{T}}^{(2)} \ldots \bar{\mathfrak{T}}^{(l)}$ будет группа, которая имеет с $\bar{\mathfrak{H}}_1$ пересечение $\mathfrak{H}_1$, в то время как $\bar{\mathfrak{T}}_{l+1} = \bar{\mathfrak{T}}_l\bar{\mathfrak{T}}^{(l+1)}$ имеет с $\bar{\mathfrak{H}}_1$ пересечение $\mathfrak{H}_2$, которое уже будет правильной надгруппой группы $\mathfrak{H}_1$. Следовательно, $\bar{\mathfrak{T}}_l\bar{\mathfrak{T}}^{(l+1)} / \bar{\mathfrak{T}}_l$ содержит $\bar{\mathfrak{T}}_l\mathfrak{H}_2 / \bar{\mathfrak{T}}_l$. Но так как группа $\bar{\mathfrak{T}}_l\mathfrak{H}_2 / \bar{\mathfrak{T}}_l$ изоморфна с $\mathfrak{H}_2 / \mathfrak{H}_1$, а $\bar{\mathfrak{T}}_l\bar{\mathfrak{T}}^{(l+1)} / \bar{\mathfrak{T}}_l$ — с некоторой факторгруппой группы $\mathfrak{M}\bar{\mathfrak{T}}^{(l+1)} / \mathfrak{M}$, то следовательно группа $\mathfrak{H}_2 / \mathfrak{H}_1$ изоморфна с делителем некоторой факторгруппы группы $\mathfrak{M}\bar{\mathfrak{T}}^{(l+1)} / \mathfrak{M}$. Далее, рассмотрим $\bar{\mathfrak{T}}_{l+1}\bar{\mathfrak{T}}^{(l+2)} / \bar{\mathfrak{T}}_{l+1}$ и $\mathfrak{H}_3 / \mathfrak{H}_2$ и т. д. Отсюда, как и выше, мы заключаем, что группа $\bar{\mathfrak{H}}_1 / \mathfrak{H}_1$ распадается на факторгруппы $\mathfrak{H}_2 / \mathfrak{H}_1, \mathfrak{H}_3 / \mathfrak{H}_2, \ldots, \bar{\mathfrak{H}}_1 / \mathfrak{H}_\nu$, каждая из которых изоморфна какому-нибудь делителю некоторой факторгруппы $\mathfrak{M}\bar{\mathfrak{T}}_l / \mathfrak{M}$. С другой стороны, группа $\mathfrak{M}\bar{\mathfrak{T}}_i / \mathfrak{M}$ изоморфна

с некоторой факторгруппой группы $\mathfrak{T}_i\bar{\mathfrak{T}}_i/\mathfrak{T}_i = \bar{\mathfrak{T}}_i/\mathfrak{T}_i$, где $\mathfrak{T}_i$ есть входящая в $\bar{\mathfrak{T}}_i$ относительная группа инерции по отношению к начальному полю K_n.

Посредством этого способа можно исчерпать все родовые множители числа классов. Но так как все $\bar{\mathfrak{T}}_i$ изоморфны с $\mathfrak{H}\bar{\mathfrak{T}}_i/\mathfrak{H}$, которые можно рассматривать как нормы групп инерции поля K, то отсюда следует

Теорема 15. *Общий родовой множитель числа классов, т. е. произведение порядков групп $\mathfrak{H}_1$, соответствующих родовым полям классов нормального поля K, есть правильный делитель произведения норм всех групп инерции поля K. Каждая из групп $\mathfrak{H}_1$ разлагается на факторгруппы $\mathfrak{h}_i$ так, что каждой из этих факторгрупп можно отнести изоморфный с ней делитель $\mathfrak{t}_i$ некоторой факторгруппы нормы одной из групп инерции, причем различным $\mathfrak{h}_i$ соответствуют различные $\mathfrak{t}_i$.*

В частности, отсюда следует, что каждый простой делитель родового множителя входит в степень поля K. Величина же общего родового множителя зависит также и от числа критических простых идеалов поля K.

Пример. Поле $K(\sqrt{p_1p_2\cdots p_\nu})$, где p_i — простые числа вида $4k+1$, имеет родовой множитель $2^{\nu-1}$. Соответствующее частичное поле классов будет $K(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_\nu})$; группа $\mathfrak{H}$ $(\nu-1)$-членного типа $\{2, 2, \ldots, 2\}$.

Аналогия между числом классов и родом поля алгебраических функций выступает в этом случае особенно ясно. Именно, род может быть определен как половина числа независимых путей, ведущих в некоторую точку *римановой* поверхности, иными словами, как разность между числом точек разветвления и числом, необходимым для построения группы монодромии. В случае гиперэллиптического поля $K(z, \sqrt{(z-a_1)(z-a_2)\cdots(z-a_{2p})})$ существует также аналог поля классов, именно — относительно неразветвленное поле $K(z, \sqrt{(z-a_1)(z-a_2)}, \sqrt{(z-a_3)(z-a_4)}, \ldots, \sqrt{(z-a_{2p-1})(z-a_{2p})})$ относительной степени 2^{p-1}.

Это поле играет важную роль в проблеме обращения.

Получено
8 декабря 1928 г.

ЛИТЕРАТУРА

1. C. Jordan. Traité des substitutions. Paris, 1870, стр. 277—279.
2. N. Tschebotarëw. Eine Verallgemeinerung des Minkowskischen Satzes usw. Журн. н.-и. кафедр Одессы, 1, № 4, 1924.
3. H. Weber. Lehrbuch der Algebra, 2, 1899, стр. 691, теорема 4.
4. K. Hensel. Theorie der algebraischen Zahlen, Lpz., 1908.

5. W. Dyck. Gruppentheoretische Studien. I. Math. Ann. **20**; О. Шмидт. Абстрактная теория групп. Киев, 1915, стр. 49—51.
6. J. Schur. Über die Darstellung der endlichen Gruppen usw. Crelle, 127 и 132, в особенности 132, стр. 85.
7. A. Speiser. Die Theorie der Gruppen von endlicher Ordnung. 2. Aufl., Berlin, 1927, стр. 130—131, теоремы (112), (113).
8. Burnside. Theorie of groups of finite order. 2 ed. Cambridge. 1912, стр. 275; также О. Шмидт. Абстрактная теория групп, стр. 191.
9. H. Hasse. Bericht über neuere usw. Teil I, Klassenkörpertheorie. Jahresbericht d. D. M.-V. **35**, стр. 46—47.

ПОПРАВКА К РАБОТЕ «К ТЕОРИИ ГРУПП ПОЛЯ КЛАССОВ»

(«Berichtigung zur Arbeit: «Zur Gruppentheorie des Klassenkörpers»)

(Там же, **164** (1931),

Из примера, приведенного Г. Гассе, я усмотрел, что высказанное на стр. 132, строки 18—20 утверждение: «Поэтому группа $\mathfrak{H}$ распадается на два взаимно простых фактора, каждый из которых является нормальным делителем группы $\mathfrak{G}'$» — неправильно. В действительности можно утверждать только, что некоторая правильная подгруппа группы $\mathfrak{H}$ распадается на два таких фактора. Именно, если

$$S_i = A_1 S_i^{-1} = A_{i+1} \qquad (i = 1, 2, \ldots, \nu - 1)$$

(здесь A_i — независимы), то группа с базисом

$$B_1 = A_1 A_2 \cdots A_\nu, \qquad B_i = A_i A_{i-1}^{-1} \qquad (i = 2, 3, \ldots, \nu)$$

распадается на две группы $\{B_1\}$ и $\{B_2, \ldots, B_\nu\}$, обладающие требуемым свойством. Формула же (4.4) остается справедливой, так как в нашем случае поле K_p распадается на два абсолютно нормальных поля, т. е. не будет элементарным.

Поступило
1 января 1931 г.

ИССЛЕДОВАНИЯ ОБ ОТНОСИТЕЛЬНО-АБЕЛЕВЫХ ЧИСЛОВЫХ ПОЛЯХ

UNTERSUCHUNGEN ÜBER RELATIV ABELSCHE ZAHLKÖRPER

(Journ. f. reine und ang. Math. **167** (1931), стр. 98—121)

Достигнутые в последнее время успехи в теории относительно-абелевых числовых полей позволяют глубже исследовать структуру их абсолютных групп Галуа. Конечная цель этих исследований может быть формулирована, примерно, следующим образом.

Задача A. Дано поле алгебраических чисел k, группа которого есть $\mathfrak{g}$ и абстрактная группа $\mathfrak{G}$, содержащая такой абелев нормальный делитель $\mathfrak{H}$, что факторгруппа $\mathfrak{G}/\mathfrak{H}$ изоморфна с $\mathfrak{g}$. Найти необходимые и достаточные условия существования для поля k надполя K, группа которого изоморфна с $\mathfrak{G}$.[1]

Задача эта соприкасается, с одной стороны, с проблемой построения поля с заданной (в частности, разрешимой) группой, с другой стороны с вопросами арифметической структуры числовых полей.

Особенно важные результаты для разрешения этой задачи получил A. Шольц [15—19].[2] Его исследования относятся большей частью к двустепенным группам (т. е. группам с абелевой коммутаторгруппой) и идут в двух направлениях. Во-первых, он провел весьма целесообразную классификацию двустепенных групп [15—16]. Для простейшего из их классов, названного им *диспозиционными группами* (Dispositionsgruppe), задача A решается независимо от арифметических свойств основного поля k. В дальнейшем он распространяет понятие диспозиционной группы на произвольные группы [17]. Во-вторых, он устанавливает связь между разрешимостью задачи A и арифметическими свойствами поля k (число классов, распределение основных единиц и т. д.) для других типов двустепенных групп и применяет свои идеи к проблеме башни полей классов [18, 19; 7].

Целью настоящей работы является отыскание наиболее общего класса относительно-абелевых групп,[3] для которого решение задачи A

[1] Слово «изоморфный» я употребляю в смысле «голоэдрически-изоморфный».

[2] Цифры в кв. скобках обозначают нумер цитированной работы в указателе литературы, приведенном в конце статьи.

[3] Под таковой я понимаю группу, содержащую абелев нормальный делитель, если я хочу обратить на последний особое внимание.

не зависит от арифметических свойств основного поля. Группы эти названы мной *шольцевыми группами*, так как они представляют естественное обобщение введенных Шольцем диспозиционных групп. Они соответствуют относительно-абелевым полям, не содержащим никаких относительно-неразветвленных подполей (чисторазветвляющиеся поля, rein verzweigte Körper). Я высказываю предположение, что структура такой группы вполне определяется структурой нормализатора $\mathfrak{N}$ некоторой циклической подгруппы нормального делителя $\mathfrak{H}$ и доказываю это предположение для случая, когда $\mathfrak{N}$ есть прямое произведение нормального делителя $\mathfrak{H}$ и некоторой другой группы.

Далее, я рассматриваю различные типы ведущих идеалов и исследую соответствующие им чисторазветвляющиеся частичные поля классов вместе с их абсолютными группами. Отделить последние возможно только в особых случаях, для которых я вывожу достаточные условия. Чтобы отличать различные типы шольцевых групп, служит некоторый инвариант основного поля, определяемый для каждого простого числа p. Для того чтобы решить задачу A для заданной шольцевой группы, необходимо показать, что существует простое число, для которого этот инвариант принимает заданное значение. Решить эту задачу мне до сих пор не удалось.

Если чисто разветвляющееся частичное поле классов, соответствующее ведущему идеалу, не отделимо, то задача A все-таки может оказаться разрешимой. Это имеет место в том случае, когда $\mathfrak{G}$ есть *дуальная* группа.

Работа эта содержит некоторые методические особенности, представляющие, надеюсь, самостоятельный интерес. К ним принадлежит, например, введение «корпусгруппы» (Körpergruppe), т. е. группы, элементы которой являются относительно-абелевыми полями с некоторым определенным законом композиции. Введение этого понятия позволяет рассматривать также группы не нормальных полей. Если же поле нормально, то соответствующая ему корпусгруппа инвариантна относительно автоморфизмов, соответствующих подстановкам группы Галуа поля k.

Связь между корпусгруппой и обыкновенной группой аналогична геометрическому *закону двойственности*.

Даю обзор содержания работы.

В § 1 я кратко излагаю необходимые для дальнейшего сведения о методе исследования относительно-абелевых групп, открытом Шатле [2]. В нем автоморфизмы абелевых групп сопоставляются с кольцами матриц специального типа. Метод этот позволяет глубоко исследовать природу общих относительно-абелевых групп.

В качестве приложения этого метода я вывожу в § 2 некоторые условия, достаточные для того, чтобы фактор («частное»), соответствующий каждому прямому фактору группы $\mathfrak{H}$, являющемуся нор-

мальным делителем группы $\mathfrak{G}$, был также нормальным делителем $\mathfrak{G}$. Здесь я использую данное И. Шуром доказательство [20] полной приводимости полуприводимых конечных линейных групп. Условия эти полезны в теории чисто разветвляющихся полей.

§ 3 посвящен изложению «закона двойственности». «Координатам» некоторого элемента группы $\mathfrak{H}$ сопоставляются «плоскостные координаты» подгруппы, индекс которой равен порядку этого элемента. Сопоставление это достигается тем, что форма, полярная некоторой, характеристической для группы $\mathfrak{H}$ квадратичной форме, полагается сравнимой с нулем. Если соответствующее представление группы $\mathfrak{G}$ в «дуальном пространстве» подобно первоначальному представлению, то группа $\mathfrak{G}$ обладает следующим свойством: если $\mathfrak{k}$ — делитель $\mathfrak{H}$, являющийся нормальным делителем группы $\mathfrak{G}$, то существует другой делитель того же рода, индекс которого равен порядку $\mathfrak{k}$. С координатами дуального пространства можно сопоставить элементы уже упомянутой корпусгруппы. В частности, если производящие элементы группы $\mathfrak{H}$ одного порядка, то группа дуальна.

В § 4 я ввожу понятие шольцевой группы. Для этих групп характерны следующие «величины»: структура факторгруппы $\mathfrak{G}/\mathfrak{H}$, порядок наибольшей циклической подгруппы $\mathfrak{h}$ группы $\mathfrak{H}$ и структура нормализатора $\mathfrak{N}$ группы $\mathfrak{h}$. Я высказываю предположение, что шольцева группа вполне определяется заданием этих «величин», и доказываю это предположение в случае, когда $\mathfrak{H}$ есть прямой фактор нормализатора $\mathfrak{N}$.

В § 5 я интерпретирую понятие корпусгруппы, используя понятие композиции циклических полей, введенное Кронекером [11]. Затем я вывожу некоторые простейшие свойства чисто разветвляющихся полей.

В § 6 я рассматриваю случай, когда ведущий идеал есть простой идеал $\mathfrak{p}$ основного поля. При этом, если $\mathfrak{p}$ имеет степень 1, то абсолютная группа нормы[1] соответствующего чисто разветвляющегося поля есть диспозиционная группа. Результат этот не зависит от того, какова абсолютная группа классов основного поля (см. § 2, второй критерий). Впрочем, этот случай уже исследован Шольцем.

Если же степень $\mathfrak{p}$ больше 1, то мы получаем чисто разветвляющееся поле, абсолютной группой которого будет шольцева группа. Перестановочность подстановок групп $\mathfrak{N}$ и $\mathfrak{H}$ можно исследовать при помощи простых теоретико-числовых соображений. Характер остальных соотношений между производящими элементами групп $\mathfrak{N}$ и $\mathfrak{H}$ связан со значениями некоторого специального символа типа гильбертовского символа нормменных вычетов. Поэтому решение задачи A требует разрешения некоторой новой проблемы плотностей, что мне не удалось сделать.

[1] Т. е. наименьшего нормального поля, содержащего заданное поле.

В § 7 я исследую случай составного ведущего идеала. Я ввожу «идеальные поля», соответствующие простым идеальным делителям ведущего идеала. Их я представляю себе как надполя абсолютного поля классов поля k. Искомое поле будет тогда некоторым подполем композита («относительного произведения») всех полей, образованных таким образом.

§ 1. Метод Шатле исследования относительно-абелевых групп

Я изложу здесь основы изящной теории Шатле (2),[1] которой в последующем мы будем пользоваться.

1. Пусть $\mathfrak{H}$ — конечная абелева группа; $A_1, A_2, \ldots, A_n$ — ее базис. Базис этот мы предполагаем максимальным, т. е. порядки A_i суть степени простых чисел. Между A_i могут существовать соотношения; пусть производящими соотношениями являются

$$f_i = A_1^{p_{i1}} A_2^{p_{i2}} \ldots A_n^{p_{in}} = E \qquad (i = 1, 2, \ldots, n) \tag{1.1}$$

(т. е. всякое соотношение между A_i есть следствие соотношений (1.1)). Пользуясь терминологией Шатле, мы будем говорить, что матрица $P = (p_{ik})$ представляет модуль (1.1) группы $\mathfrak{H}$ (tableau, associè au module (1.1) de $\mathfrak{H}$).

Если некоторый элемент $B = E$, то

$$B = A_1^{x_1} A_2^{x_2} \ldots A_n^{x_n} = f_1^{y_1} f_2^{y_2} \ldots f_n^{y_n},$$

откуда следует

$$x_k = y_1 p_{1k} + y_2 p_{2k} + \ldots + y_n p_{nk} \qquad (k = 1, 2, \ldots, n),$$

или

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) P,$$

где символ $(x_1, x_2, \ldots, x_n)$ следует рассматривать как однострочную матрицу. Два элемента группы $\mathfrak{H}$ равны тогда и только тогда, если соответствующие им *индексы* $(x_1, x_2, \ldots, x_n)$ и $(z_1, z_2, \ldots, z_n)$ связаны соотношением

$$(x_1, x_2, \ldots, x_n) - (z_1, z_2, \ldots, z_n) = (y_1, y_2, \ldots, y_n) P, \tag{2.1}$$

где $(y_1, y_2, \ldots, y_n)$ есть однострочная целочисленная матрица. Для соотношений типа (2.1) мы введем следующее обозначение:

$$(x_1, x_2, \ldots, x_n) \equiv (z_1, z_2, \ldots, z_n) \pmod{P}. \tag{3.1}$$

2. Под автоморфизмом группы $\mathfrak{H}$ мы понимаем переход к новому базису, для элементов которого остаются справедливыми все соотношения (1.1). Пусть один из таких автоморфизмов будет

$$B_k = \prod_{i=1}^{n} A_i^{t_{ki}} \qquad (k = 1, 2, \ldots n).$$

---

[1] Г. Гассе указал мне, что аналогичная теория была совершенно независимо развита О. Шрейером [19a].

Тогда должны иметь место соотношения

$$f_\lambda(B_k) = \prod_{k=1}^{n} B_k^{p_{\lambda k}} = \prod_{i,\,k=1}^{n} A_i^{p_{\lambda k} t_{ki}} = \prod_{i=1}^{n} A_i^{\sum_{k=1}^{n} p_{\lambda k} t_{ki}} = E \qquad (\lambda = 1, 2, \ldots, n),$$

т. е.

$$\left(\sum_{k=1}^{n} p_{\lambda k} t_{k1}, \sum_{k=1}^{n} p_{\lambda k} t_{k2}, \ldots, \sum_{k=1}^{n} p_{\lambda k} t_{kn} \right) \equiv 0 \pmod{P} \qquad (\lambda = 1, 2, \ldots, n) \quad (4.1)$$

Рассматривая эту строку как строку с нумером λ некоторой квадратной матрицы, мы сможем записать сравнения (4.1) в следующей форме:

$$PT = \Theta P, \qquad (5.1)$$

где $T = (t_{ik})$, а Θ — целочисленная матрица. Свойство это характерно для матрицы T, соответствующей некоторому автоморфизму [по терминологии Шатле, матрица T полуперестановочна (semipermutable) с P]. Если матрицы T_1 и T_2 удовлетворяют уравнению (5.1), то ему удовлетворяют и матрицы $T_1 \pm T_2$, $T_1 T_2$. Говорят, что матрицы, удовлетворяющие уравнению (5.1), образуют конечную *алгебру*.

Если T переводит группу $\mathfrak{H}$ в себя, а не в свою подгруппу, то автоморфизм T называется *собственным* (eigentlich). Чтобы автоморфизм T был собственным, необходимо и достаточно, чтобы подстановка $(y) = (x)T$ была обратимой. Последнее всегда имеет место, если определитель $|T|$ взаимно прост с порядком группы $\mathfrak{H}$ (т. е. с определителем $|P|$). Все собственные автоморфизмы образуют группу.

3. Пусть $\mathfrak{K}$ — подгруппа группы $\mathfrak{H}$ с базисом

$$B_i = \prod_{k=1}^{n} A_k^{q_{ik}} \qquad (i = 1, 2, \ldots, m;\ m \leqslant n). \qquad (6.1)$$

Если $m < n$, то положим $B_{m+1} = B_{m+2} = \ldots = B_n = E$. Пусть производящие соотношения группы $\mathfrak{K}$ будут

$$\varphi_\lambda = \prod_{k=1}^{n} B_k^{r_{\lambda k}} = E \qquad (\lambda = 1, 2, \ldots, n).$$

После подстановки вместо B_k их значений из (6.1) соотношения эти становятся следствиями соотношений (1.1)

$$\prod_{k=1}^{n} B_k^{r_{\lambda k}} = \prod_{k,\,\mu} A_\mu^{r_{\lambda k} q_{k\mu}} = \prod_{\mu,\,k} A_\mu^{e_{\lambda k} p_{k\mu}} \qquad (\lambda = 1, 2, \ldots, n),$$

откуда

$$\sum_{k=1}^{n} r_{\lambda k} q_{k\mu} = \sum_{k=1}^{n} e_{\lambda k} p_{k\mu},$$

или

$$RQ = HP,$$

где R соответствует модулю $\mathfrak{K}$, а H и Q — целочисленные матрицы

С другой стороны, P «делится справа» на R. В самом деле, известно, что всякая подгруппа абелевой группы изоморфна некоторой факторгруппе той же группы. Последняя же может быть построена следующим образом: выбираем снова за производящие элементы $A_1, A_2, \ldots, A_n$, но полагаем, что между ними, кроме соотношений (1.1), имеют место еще некоторые другие, а именно

$$\varphi_i = A_1^{r_{i1}} A_2^{r_{i2}} \ldots A_n^{r_{in}} = E \qquad (i = 1, 2, \ldots, n), \tag{7.1}$$

следствиями которых являются соотношения (1.1), т. е.

$$f_i = \varphi_1^{\lambda_{i1}} \varphi_2^{\lambda_{i2}} \ldots \varphi_n^{\lambda_{in}}, \tag{8.1}$$

или подробнее

$$A_1^{p_{i1}} A_2^{p_{i2}} \ldots A_n^{p_{in}} = (A_1^{r_{11}} \ldots A_n^{r_{1n}})^{\lambda_{i1}} \ldots (A_1^{r_{n1}} \ldots A_n^{r_{nn}})^{\lambda_{in}}.$$

Так как эти соотношения представляют тождества относительно $A_1, A_2, \ldots, A_n$, то

$$p_{ik} = \lambda_{i1} r_{1k} + \lambda_{i2} r_{2k} + \ldots + \lambda_{in} r_{nk} \qquad (i, k = 1, 2, \ldots, n),$$

или

$$p = \Lambda R,$$

где Λ — целочисленная матрица, что и требовалось доказать.

4. Пусть даны два разложения модуля P: $P = QR$ и $P = Q'R'$. Когда они соответствуют одной и той же подгруппе $\mathfrak{R}$ группы $\mathfrak{H}$? С одной стороны, очевидно, что разложение $P = Q\Sigma \cdot \Sigma^{-1} R$, где Σ — произвольная унимодулярная матрица (т. е. матрица с определителем ± 1) соответствует той же подгруппе. Действительно, матрица $Q\Sigma$ соответствует другому базису той же подгруппы $\mathfrak{R}$, а матрица $\Sigma^{-1}R$ определяет те же соотношения, что и R, только лишь в иной форме. С другой стороны, если R и R' соответствуют одной и той же подгруппе $\mathfrak{R}$, то модули R и R' должны совпадать. Иными словами, если $z_1, z_2, \ldots, z_n$ — целые, то должны найтись такие целые $z_1', z_2', \ldots, z_n'$, что

$$(z_1, z_2, \ldots, z_n) R = (z_1', z_2', \ldots, z_n') R'$$

и обратно, каждой целочисленной системе $z_1', z_2', \ldots, z_n'$ должна соответствовать целочисленная система $z_1, z_2, \ldots, z_n$. Это возможно тогда и только тогда, если матрицы $R(R')^{-1}$ и $R'R^{-1} = [R(R')^{-1}]^{-1}$ — целочисленные. Отсюда следует, что $R(R')^{-1} = \Sigma$ — унимодулярная матрица, т. е.

$$R = \Sigma R', \qquad |\Sigma| = \pm 1.$$

§ 2. Нормальные делители. Относительные произведения

1. Пусть теперь $\mathfrak{G}$ — надгруппа группы $\mathfrak{H}$, содержащая $\mathfrak{H}$ как нормальный делитель, и которая, таким образом, может быть рассматриваема как группа автоморфизмов группы $\mathfrak{H}$. Подстановкам группы $\mathfrak{G}$

соответствуют матрицы типа T. Если $\mathfrak{R}$ — подгруппа группы $\mathfrak{H}$ и одновременно нормальный делитель группы $\mathfrak{G}$, и R — матрица модуля $\mathfrak{R}$, то T — полуперестановочна не только с P, но и с R

$$RT = \Theta R. \tag{1.2}$$

2. Предположим, что $\mathfrak{H}$ распадается в ***относительное произведение*** (т. е. в прямое произведение, оба фактора которого являются нормальными делителями группы $\mathfrak{G}$ (ср. [15]), причем одним из факторов является $\mathfrak{R}$:

$$\mathfrak{H} = \mathfrak{R} \cdot \mathfrak{R}_1.$$

Тогда P приводится к виду

$$P = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

причем матрица $\begin{pmatrix} A & 0 \\ 0 & E \end{pmatrix}$, где E — единичная матрица соответствующего порядка, соответствует модулю $\mathfrak{R}$. Если представить T в форме $\begin{pmatrix} M & N \\ R & Q \end{pmatrix}$, то уравнение (1.2) распадется на такие уравнения:

$$AM = XA, \qquad AN = Y, \qquad R = ZA, \qquad Q = U.$$

Воспользовавшись тем, что T определяется с точностью до правого кратного матрицы P, можно привести T к виду

$$\begin{pmatrix} M & N \\ R & Q \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ Z & 0 \end{pmatrix} \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} = \begin{pmatrix} M & N \\ 0 & Q \end{pmatrix}$$

(матрица T полуприводима). Принимая же во внимание второй фактор $\mathfrak{R}_1$, мы сможем представить T во ***вполне приведенной*** форме $\begin{pmatrix} M & 0 \\ 0 & Q \end{pmatrix}$.

Если группа $\mathfrak{R}$ задана как прямой фактор группы $\mathfrak{H}$ и нормальный делитель группы $\mathfrak{G}$, то тем самым $\mathfrak{R}_1$, как известно, однозначно не определяется. Возникает вопрос, нельзя ли в качестве $\mathfrak{R}_1$ выбрать также нормальный делитель группы $\mathfrak{G}$. Мы укажем некоторые необходимые для этого условия.

3. Для того чтобы группа $\mathfrak{R}_1$ была также нормальным делителем группы $\mathfrak{G}$, необходимо и достаточно, чтобы каждый автоморфизм T группы $\mathfrak{G}$ (который мы предполагаем представленным в полуприведенной форме) мог быть приведен к виду $\begin{pmatrix} M & 0 \\ 0 & Q \end{pmatrix}$. Таким образом, дело сводится к задаче изменения B в матрице $P = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$ так, чтобы все матрицы T, образующие полуприведенную группу матриц по модулю P, обратились во вполне приведенные. Задача эта разрешена И. Шуром для обыкновенных конечных групп матриц ([20], стр. 415). Именно, если $T = \begin{pmatrix} M_T & N_T \\ 0 & Q_T \end{pmatrix}$, то И. Шур преобразует группу матриц посред-

ством матрицы вида $\begin{pmatrix} E & F \\ 0 & E \end{pmatrix}$, где достаточно положить $F = \frac{1}{n}\sum_S N_S Q_{S^{-1}}$ (n-порядку группы $\mathfrak{G}/\mathfrak{H}$). Для наших целей необходимо еще, чтобы матрица F была целочисленной. Но так как мы рассматриваем все матрицы по модулю P, то это последнее требование всегда может быть удовлетворено, если определитель $|P| = \text{Пор. } \mathfrak{H}$ взаимно прост с n.

4. Условие, выведенное выше, никоим образом не является необходимым. Чтобы получить другой критерий, представим $\mathfrak{H}$ как аддитивную группу (т. е. положим, например, $x_i = \log A_i$) и будем трактовать $\mathfrak{G}/\mathfrak{H}$ снова как линейную однородную группу подстановок. Рассмотрим линейную форму

$$\xi = u_1 x_1 + u_2 x_2 + \ldots + u_n x_n$$

с неопределенными переменными $u_1, u_2, \ldots, u_n$ и обозначим через ξ^T форму, в которую переводится ξ подстановкой T. Очевидно, что квадратичная форма

$$F = \sum_T (\xi^T)^2 \tag{2.2}$$

инвариантна относительно $\mathfrak{G}/\mathfrak{H}$. Представим F как сумму независимых квадратов и будем рассматривать ее по модулю P. Если F содержит n независимых квадратов и коэффициенты при них взаимно просты с $|P|$, то легко доказать, что группа вполне приводима ([22], стр. 106, фундаментальная теорема 99). Необходимое и достаточное условие для этого состоит в том, чтобы дискриминант D формы F был взаимно прост с $|P|$. Так как дискриминант этот содержит переменные $u_1, u_2, \ldots, u_n$, то можно применить способ Гензеля ([10], гл. 10) и формулировать этот второй критерий так:

Если $p_1, p_2, \ldots, p_k$ — различные простые делители $|P|$, то должно быть:

$$D \not\equiv 0 \,(\text{modd. } p_i, u_1^{p_i} - u_1,\ u_2^{p_i} - u_2, \ldots, u_n^{p_i} - u_n) \qquad (i = 1, 2, \ldots, k).$$

Этот критерий имеет действительное значение только в случае $k = 1$ (т. е. когда порядок группы $\mathfrak{H}$ равен степени простого числа). Он наверное выполняется в случае, если $\mathfrak{G}$ есть общая диспозиционная группа [17], т. е. если все ξ^T независимы по модулю P.

Если форма F содержит только $m < n$ независимых квадратов $y_1^2, y_2^2, \ldots, y_m^2$, то нормальный делитель $\mathfrak{H}_1$ групп $\mathfrak{H}$ и $\mathfrak{G}$, порожденный $y_1, y_2, \ldots, y_m$, всегда распадается в относительное произведение. В этом случае следует рассмотреть $\mathfrak{H}_1$ вместо $\mathfrak{H}$.

5. Пример (предложен О. Шрайером, [25], стр. 187).

$$\text{Пор } A = \text{Пор } B = \text{Пор } \Theta = p, \qquad A^\Theta = A, \qquad B^\Theta = AB = BA,$$

$$\mathfrak{G} = (A, B, \Theta), \qquad \mathfrak{H} = (A, B),$$

$P=\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$. В этом случае можно рассматривать все матрицы не по модулю P, но просто по $\bmod p$. Если элементы A, B соответствуют переменным x и соотв. y, то автоморфизм Θ представляется в следующем виде:

$$\Theta: \qquad x' = x, \qquad y' = x + y.$$

Отсюда следует

$$\Theta^k: \qquad x' = x, \qquad y' = kx + y \qquad (k = 0, 1, 2, \ldots, p-1).$$

$$F = (ux + vy)^2 + (ux + vy)^{2\Theta} + \ldots + (ux + vy)^{2\Theta^{p-1}} =$$

$$= (ux + vy)^2 + (\overline{u + v}x + vy)^2 + \ldots + (\overline{u + pv - v}x + vy)^2 =$$

$$= \left[pu^2 + p(p-1)uv + \frac{p(p-1)(2p-1)}{6}v^2\right]x^2 + 2\left[pu + \frac{p(p-1)}{2}v\right]vxy +$$

$$+ vp^2y^2 \equiv \frac{p(p-1)(2p-1)}{6}v^2x^2 \qquad (\bmod p).$$

Если $p > 3$, то $F \equiv 0 \pmod p$.
Если $p = 3$, то $F \equiv 5x^2 \pmod 3$.
Если $p = 2$, то $F \equiv x^2 \pmod 2$.

Во всех случаях группа $\mathfrak{H}$ не распадается в относительное произведение.

§ 3. Дуальные группы

1. Рассмотренный в § 2 класс относительно-абелевых групп, которые мы назовем *регулярными* группами, допускает важное обобщение, которое и составит содержание этого параграфа.

Определение. Если абелев нормальный делитель $\mathfrak{H}$ группы $\mathfrak{G}$ обладает тем свойством, что в нем каждой подгруппе $\mathfrak{K}$ порядка s можно сопоставить такую подгруппу $\hat{\mathfrak{K}}$ индекса s (причем $\hat{\mathfrak{K}} \longleftrightarrow \mathfrak{H}/\mathfrak{K}$), что: 1. Если $\mathfrak{K}_3$ есть пересечение подгрупп $\mathfrak{K}_1$ и $\mathfrak{K}_2$, то $\hat{\mathfrak{K}}_3$ есть композит $\hat{\mathfrak{K}}_1$ и $\hat{\mathfrak{K}}_2$, и наоборот; 2. Если $\mathfrak{K}$ есть нормальный делитель группы $\mathfrak{G}$, то и $\hat{\mathfrak{K}}$ также; то будем говорить, что группа $\mathfrak{H}$ *дуальна* (относительно $\mathfrak{G}$).

Если мы присоединим сюда еще условие, чтобы подгруппы $\mathfrak{K}$ и $\hat{\mathfrak{K}}$ были взаимно просты в том случае, когда $\mathfrak{K}$ есть прямой фактор группы $\mathfrak{H}$ (т. е. его инварианты либо максимальны, либо равны 1), то получим определение регулярных групп.

2. Геометрические представления послужат нам для установления одного весьма широкого класса дуальных групп. Каждому элементу $A = A_1^{x_1}A_2^{x_2}\ldots A_n^{x_n}$ группы $\mathfrak{H}$ отнесем вектор с координатами $x_1, x_2, \ldots, x_n$. При изменении базиса $[A_1, A_2, \ldots, A_n]$ координаты $x_1, x_2, \ldots, \ldots, x_n$ этого вектора подвергаются некоторому линейному преобразо-

ванию, которое мы будем рассматривать как преобразование координат. Таким образом, каждому элементу группы $\mathfrak{H}$ относится вектор аффинного пространства, причем соответствие это не зависит от выбора системы координат. Точно так же каждой циклической подгруппе группы $\mathfrak{H}$ соответствует прямая и вообще каждой подгруппе — подпространство.

Каждому элементу группы $\mathfrak{H}$ соответствует некоторое отображение нашего пространства. Подгруппам группы $\mathfrak{H}$, являющимся нормальными делителями группы $\mathfrak{G}$, соответствуют подпространства, остающиеся инвариантными при всех таких отображениях.

3. Введем теперь новую систему целых чисел $u_1, u_2, \ldots, u_n$ (так называемые *плоскостные координаты* или *координаты дуального пространства*), связанных с координатами $x_1, x_2, \ldots, x_n$ следующим образом:

$$P^{-1}(x, u) \equiv 0 \pmod 1, \tag{1.3}$$

где $P(x, u)$ есть билинейная форма, $\sum_{i,k} p_{ik} x_i u_k$, соответствующая матрице P (так что $P^{-1}(x, u)$ — форма, соответствующая обратной матрице P^{-1}), и знак $\equiv 0 \pmod 1$ обозначает целочисленность (форма $P^{-1}(x, u)$ не является целочисленной).

Если система чисел $(x_1, x_2, \ldots, x_n)$ пробегает все индексы группы $\mathfrak{H}$, то уравнение (1.3) удовлетворяется тогда и только тогда, если значения всех производных $\frac{\partial P^{-1}(x, u)}{\partial x_i}$ — целые числа. Это означает, что u_i должны удовлетворять следующему условию:

$$(u_1, u_2, \ldots, u_n) = (v_1, v_2, \ldots, v_n) P',$$

где $v_1, v_2, \ldots, v_n$ — целые числа и P' — матрица, полученная из P транспонированием. Системы эти соответствуют единичному элементу абелевой группы $\hat{\mathfrak{H}}$, модуль-матрица которой есть P'. Группа эта изоморфна с $\mathfrak{H}$.

4. Если система чисел $(x_1, x_2, \ldots, x_n)$ пробегает индексы элементов некоторой подгруппы $\mathfrak{K}$ группы $\mathfrak{H}$, то $(u_1, u_2, \ldots, u_n)$ пробегает индексы элементов некоторой подгруппы $\hat{\mathfrak{K}}$ группы $\hat{\mathfrak{H}}$. Докажем, что подгруппа $\hat{\mathfrak{K}}$ изоморфна с $\mathfrak{H}/\mathfrak{K}$. Чтобы избежать длинного счета, возьмем P в диагональной форме:

$$P = \begin{pmatrix} p_1 & 0, \ldots, & 0 \\ 0, & p_1, \ldots, & 0 \\ & \ldots\ldots & \\ 0, & 0, \ldots, & p_n \end{pmatrix}$$

и рассмотрим абелево поле $K = k(\sqrt[p_1]{m_1}, \sqrt[p_2]{m_2}, \ldots, \sqrt[p_n]{m_n})$, группа которого изоморфна с $\mathfrak{H}$, если в k содержится величина $\varepsilon = \exp\left(\frac{1}{p}\right)$

$(p = p_1 p_2 \dots p_n)$.[1] Элементу A_i группы $\mathfrak{H}$ отнесем ту операцию группы поля K, которая переводит $\sqrt[p_i]{m_i}$ в $\varepsilon^{q_i}\sqrt[p_i]{m_i}$ $\left(q_i = \frac{p}{p_i}\right)$, оставляя инвариантными остальные радикалы, и совокупность радикалов рассмотрим как мультипликативную абелеву группу: $B_i \to \sqrt[p_i]{m_i}$. Выделяя систему показателей $u_1, u_2, \dots, u_n$, соответствующую некоторой подгруппе $\hat{\mathfrak{R}}$ этой группы радикалов (или лучше: *корпусгруппы* (Körpergruppe)), мы устанавливаем, что поле, образованное элементами $\hat{\mathfrak{R}}$, принадлежит некоторой подгруппе $\mathfrak{R}$ группы $\mathfrak{H}$. Если произвести над величиной $(\sqrt[p_1]{m_1})^{u_1} \cdot (\sqrt[p_2]{m_2})^{u_2} \dots (\sqrt[p_n]{m_n})^{u_n}$ подстановку $A = A_1^{x_1} A_2^{x_2} \dots A_n^{x_n}$, то величина эта приобретает множитель $\varepsilon^{q_1 x_1 u_1 + q_2 x_2 u_2 + \dots + q_n x_n u_n}$. Значит, A принадлежит к $\mathfrak{R}$ тогда и только тогда, если имеет место

$$q_1 x_1 u_1 + q_2 x_2 u_2 + \dots + q_n x_n u_n \equiv 0 \pmod{p},$$

где система чисел $(u_1, u_2, \dots, u_n)$ пробегает все индексы группы $\hat{\mathfrak{R}}$. Уравнение это может быть записано следующим образом

$$\frac{x_1 u_1}{p_1} + \frac{x_2 u_2}{p_2} + \dots + \frac{x_n u_n}{p_n} \equiv 0 \pmod{1}.$$

Так как

$$P^{-1} = \begin{pmatrix} 1/p_1, 0, \dots, 0 \\ 0, 1/p_2, \dots, 0 \\ \dots\dots\dots \\ 0, 0, \dots, 1/p_n \end{pmatrix},$$

то мы приходим как раз к уравнению (1.3). Таким образом, группа $\hat{\mathfrak{R}}$ изоморфна с группой Галуа поля, образованного элементами $\hat{\mathfrak{R}}$, т. е. с группой $\mathfrak{H}/\mathfrak{R}$.

Так же легко при помощи теории Галуа мы убеждаемся в том, что условие 1 «определения» выполнено.

5. Условие 2 нашего «определения» не всегда выполняется. Чтобы обнаружить это, мы исходим из следующих, легко доказываемых формул, в которых U и V представляют произвольные унимодулярные подстановки

$$P(xU, u) = UP(x, u), \tag{2.3}$$

$$P(x, uV) = PV'(x, u). \tag{3.3}$$

Рассмотрим формулу (5.2)

$$PT = \Theta P. \tag{4.3}$$

[1] Мы вводим следующее обозначение: $\exp(x) = e^{2\pi i x}$.

Она гласит, что каждому автоморфизму T соответствует некоторая другая унимодулярная подстановка Θ, и наоборот. Произведению T_1T_2 соответствует произведение $\Theta_1\Theta_2$, как это следует из формулы

$$PT_1T_2 = \Theta_1 PT_2 = \Theta_1\Theta_2 P.$$

Таким образом, подстановки Θ образуют группу, изоморфную с группой $\mathfrak{G}/\mathfrak{H}$. Полагая в (2.3), (3.3) $U = T$, $V = \Theta'^{-1}$, мы получим

$$P^{-1}(xT, u\Theta'^{-1}) = TP^{-1}\Theta^{-1}(x, u) = P^{-1}(x, u).$$

Это значит, что форма $P(x, u)$ не изменяется, если произвести над x подстановку T и одновременно над u — подстановку Θ'^{-1}.

6. Если T пробегает всю группу $\mathfrak{G}/\mathfrak{H}$, то соответствующая подстановка Θ'^{-1} пробегает некоторую унимодулярную линейную однородную группу, изоморфную с группой $\mathfrak{G}/\mathfrak{H}$. При этом, если P—симметричная матрица (что всегда можно предположить), то Θ'^{-1}, как и T, удовлетворяет уравнению (4.3). В общем случае обе группы не будут унимодулярно-подобны. В случае же, когда это имеет место, мы можем изменить базис группы $\hat{\mathfrak{H}}$ так, чтобы соответствующие друг другу подстановки T и Θ'^{-1} совпали. Тогда $\mathfrak{K}$ и $\hat{\mathfrak{K}}$ являются одновременно нормальными делителями группы $\mathfrak{G}$, т. е. условие 2 «определения» выполняется и группа дуальна.

Заметим, что рассмотренная нами группа автоморфизмов не всегда изоморфна с $\mathfrak{G}/\mathfrak{H}$. Этот случай необходимо имеет место, если группа $\mathfrak{G}$ содержит как нормальный делитель некоторую абелеву надгруппу группы $\mathfrak{H}$. Мы не можем также утверждать здесь, что корпусгруппа изоморфна с группой $\mathfrak{G}$. Понятие корпусгруппы сходно с Круллевским понятием *обобщенной абелевой группы* [11а]. Может случиться, что одной и той же корпусгруппе соответствуют различные группы $\mathfrak{G}$. Однако выводы этого параграфа остаются в силе, если под $\mathfrak{G}/\mathfrak{H}$ понимать группу автоморфизмов группы $\mathfrak{G}$, порожденную подстановками из $\mathfrak{G}$.

7. Пример 1 (см. пример § 2). Пор A = Пор B = Пор $T = p$, $A^T = A$, $B^T = AB = BA$, $\mathfrak{G} = (A, B, T)$, $\mathfrak{H} = (A, B)$.

$$P = \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \Theta = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \Theta'^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

Полагая $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, получим $T^{S^{-1}} = \Theta'^{-1}$. Значит, группа дуальна. Единственный нетривиальный нормальный делитель (A) группы $\mathfrak{G}$ соответствует самому себе, так что группа не регулярна.

Пример 2. Пусть $\mathfrak{H}$ — произвольная абелева группа и $\mathfrak{G}$ — ее полная группа автоморфизмов. Θ'^{-1} есть автоморфизм группы $\mathfrak{H}$ и, значит, содержится в $\mathfrak{G}$. Группа $\mathfrak{G}$ дуальна (ср. [2], стр. 165, строка 1 — 2 сверху).

Пример 3. Пусть все производящие элементы группы $\mathfrak{H}$ — одного порядка. Здесь P — диагональная матрица с одинаковыми элементами, т. е. перестановочна со всякой матрицей. Из формулы (4.3) следует

$$\Theta = T.$$

Представляется весьма вероятным, что все эти группы дуальны.

Пример 4 (сообщен мне в письме А. Шольцем).

$$\text{Пор}\, A = p^2, \quad \text{Пор}\, B = p, \quad A^T = AB = BA, \quad B^T = B, \quad \text{Пор}\, T = p.$$

$$P = \begin{pmatrix} p^2 & 0 \\ 0 & p \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Из (4.3) мы получаем

$$\Theta = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \quad \Theta'^{-1} = \begin{pmatrix} 1 & 0 \\ -p & 1 \end{pmatrix}.$$

Положим $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ и попытаемся удовлетворить уравнению $(\Theta'^{-1})^u = T$. Получим

$$\alpha = 0, \quad -p\beta = \gamma.$$

Значит, матрица U не может быть унимодулярной. С другой стороны, эта группа не может быть дуальной, так как $\mathfrak{G}$ содержит циклический нормальный делитель (A), но циклических нормальных делителей порядка p^2 не существует.

§ 4. Шольцевы группы

1. Шольц [15] рассмотрел один особый тип двустепенных групп названный им диспозиционными группами. Под этим названием он понимает группы $\mathfrak{G}$ с абелевым нормальным делителем $\mathfrak{H}$ и абелевой факторгруппой $\mathfrak{G}/\mathfrak{H}$, в которых $\mathfrak{H}$ есть прямое произведение циклических групп, получающихся, если над одной из них производить подстановки из $\mathfrak{G}$, причем любая из этих групп переводится различными подстановками в одну и ту же сопряженную систему только тогда, если подстановки эти лежат в одном и том же классе смежности $\mathfrak{H}S$. Таким образом, число сопряженных циклических групп максимального порядка равно порядку группы $\mathfrak{G}/\mathfrak{H}$.

Шольц доказал следующие два свойства диспозиционных групп: 1) Диспозиционная группа вполне определена, если известны: группа $\mathfrak{G}/\mathfrak{H}$ и порядок производящего элемента группы $\mathfrak{H}$; 2) Если дано поле алгебраических чисел с группой $\mathfrak{G}/\mathfrak{H}$, то всегда можно найти такое его надполе, группа которого будет $\mathfrak{G}$ (диспозиционное поле).

2. Первую из этих теорем Шольц обобщил (17) на случай, когда $\mathfrak{G}/\mathfrak{H}$ есть произвольная группа, а $\mathfrak{H}$ — прямое произведение произвольных изоморфных групп. Он назвал (в письме) такие группы общими диспозиционными группами.

3. Мы хотим обобщить это понятие в другом направлении. Пусть группа $\mathfrak{G}/\mathfrak{H}$ произвольна, а $\mathfrak{H}$ есть прямое произведение циклических групп: $\mathfrak{H} = \mathfrak{h}_1 \times \mathfrak{h}_2 \times \ldots + \mathfrak{h}_k$, которые подстановками группы $\mathfrak{G}$ переводятся друг в друга. Каждая группа $\mathfrak{h}_i$ имеет нормализатор $\mathfrak{N}_i > \mathfrak{H}$. Число k сопряженных с $\mathfrak{h}_1$ групп равно индексу $(\mathfrak{G} : \mathfrak{N}_1) \cdot (\mathfrak{h}_1)$ переводится подстановкой S в $\mathfrak{h}_i$ тогда и только тогда, если S лежит в i-том классе смежности $\mathfrak{N}_1 S_i$. Наконец, предположим, что пересечение всех $\mathfrak{N}_i$ равно $\mathfrak{H}$. Такие группы мы назовем *шольцевыми группами*.

Да будет мне позволено высказать следующее предположение относительно шольцевых групп.

Предположение. Шольцевая группа вполне определена, если известны факторгруппа $\mathfrak{G}/\mathfrak{H}$ группы $\mathfrak{h}_i$ и группа $\mathfrak{n}_1 = \mathfrak{N}_1 / \mathfrak{h}_2 \times \mathfrak{h}_3 \times \ldots \times \mathfrak{h}_k$.

4. Мне удалось доказать высказанное предположение для того случая, когда $\mathfrak{n}_1$ является прямым произведением, один из факторов которого изоморфен с группой $\mathfrak{h}_1$. Положим $\mathfrak{n}_1 = \mathfrak{h}_1 \times \mathfrak{m}_1$ и пусть порядок группы $\mathfrak{h}_1$ равен m.

Представим $\mathfrak{G}$ как регулярную группу подстановок переменных $x_1, x_2, \ldots$ и построим функцию $u_1 = f(x_1, x_2, \ldots)$, принадлежащую к группе $\mathfrak{m}_1$ $(\mathfrak{h}_2 \times \mathfrak{h}_3 \times \ldots \times \mathfrak{h}_k)$.[1] Применяя к u_1 подстановки циклической группы $\mathfrak{h}_1$, мы получим n функций

$$u_1, u_2 \ldots, u_n,$$

которые, при применении к ним подстановок из $\mathfrak{N}_1$, будут претерпевать только циклические подстановки. Функция

$$v_1 = u_1 + \varepsilon^{-1} u_2 + \ldots + \varepsilon^{-n+1} u_n \left(\varepsilon = \exp\left(\frac{1}{n}\right)\right)$$

при применении к ней подстановок из $\mathfrak{h}_1$ претерпевает только умножения на степени ε и остается инвариантной при подстановках из $\mathfrak{m}_1 \times \mathfrak{h}_2 \times \mathfrak{h}_3 \times \ldots \times \mathfrak{h}_k$. Значит, функция v_1^n не изменяется при всех подстановках из $\mathfrak{N}_1$.

Пусть разложение $\mathfrak{G}$ на классы смежности по $\mathfrak{N}_1$ будет

$$\mathfrak{G} = \mathfrak{N}_1 + \mathfrak{N}_1 S_2 + \ldots + \mathfrak{N}_1 S_k.$$

Применяя к v_1 подстановки $S_1 = E, S_2, \ldots, S_k$, мы получим функции $v_1, v_2, \ldots, v_k$. Их n-е степени $v_1^n, v_2^n, \ldots, v_k^n$ инвариантны относительно $\mathfrak{H}$, а при применении к ним подстановок из $\mathfrak{G}$ подвергаются только подстановкам, образующим представление группы $\mathfrak{G}/\mathfrak{H}$ в виде группы подстановок. Представление это является собственным в силу последнего предположения относительно шольцевых групп.

---

[1] Под этим я понимаю группу, факторгруппа которой относительно $\mathfrak{h}_2 \times \mathfrak{h}_3 \times \ldots \times \mathfrak{h}_k$ равна $\mathfrak{m}_1$. Мы имеем право ввести такое определение, так как эта группа есть делитель $\mathfrak{N}$, а $\mathfrak{N}$ содержит группы $\mathfrak{h}_1$ и $\mathfrak{h}_2 \times \mathfrak{h}_3 \times \ldots \times \mathfrak{h}_k$ в качестве нормальных делителей.

Отсюда следует, что функции v_1 $v_2, \ldots,$ v_k при применении к ним подстановок из $\mathfrak{G}$ испытывают только перестановки и умножения на степени ε. Мы покажем, что в каждом классе смежности разложения

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}T_2 + \ldots + \mathfrak{H}T_n$$

представители T_i могут быть выбраны так, что относительно них функции $v_1, v_2, \ldots, v_k$ будут подвергаться только перестановкам. Пусть U_1 — производящая подстановка группы $\mathfrak{h}_1$, которая переводит v_1 в εv_1 и не изменяет остальные функции v_i. Тогда подстановка $U_\varkappa = S_\varkappa^{-1} U_1 S_\varkappa$ переводит $v_\varkappa$ в $\varepsilon v_\varkappa$ и не изменяет остальные $v_i (\varkappa = 1, 2, \ldots, k)$. Например, если

$$S \to \begin{pmatrix} v_1, & v_2, \ldots, & v_k \\ \varepsilon^{a_1} v_{s_1}, & \varepsilon^{a_2} v_{s_2}, \ldots, & \varepsilon^{a_k} v_{s_k} \end{pmatrix},$$

то

$$U_1^{-a_1} U_2^{-a_2} \ldots U_k^{-a_k} S \to \begin{pmatrix} v_1, & v_2, \ldots, & v_k \\ v_{s_1}, & v_{s_2}, \ldots, & v_{s_k} \end{pmatrix}.$$

Очевидно, что нормированные таким образом подстановки образуют группу, изоморфную с факторгруппой $\mathfrak{G}/\mathfrak{H}$. Полная группа $\mathfrak{G}$ определяется теперь как *моноэиальная группа* ([22], стр. 90), причем ядро ее (Kerngruppe, т. е. максимальная подгруппа, состоящая только из перестановок переменных) изоморфно с $\mathfrak{G}/\mathfrak{H}$, а подстановками группы $\mathfrak{H}$ переменные $v_1, v_2, \ldots, v_k$ независимо друг от друга умножаются на всевозможные комбинации множителей из ряда $1, \varepsilon, \ldots, \varepsilon^{n-1}$. Тем самым группа $\mathfrak{G}$ определена полностью, что и т. д.

§ 5. Общие сведения о чисто разветвляющихся полях

1. Пусть K — относительно-абелево поле над числовым полем k. Будем считать, что оба поля абсолютно нормальны. Пусть $\mathfrak{G}$ есть абсолютная группа поля K и $\mathfrak{H}$ — относительная группа поля K/k. $\mathfrak{H}$ есть абелева группа и является нормальным делителем группы $\mathfrak{G}$. Пусть, затем, K_1 — наибольшее неразветвленное над k подполе поля K; группу его обозначим через $\mathfrak{H}_1$. $\mathfrak{H}_1$ будет нормальным делителем группы $\mathfrak{G}$. Здесь могут встретиться следующие три случая: 1) $\mathfrak{H}_1$ не является прямым фактором группы $\mathfrak{H}$; 2) $\mathfrak{H}_1$ есть прямой фактор группы $\mathfrak{H}$, но нельзя найти такого разложения $\mathfrak{H} = \mathfrak{H}_1 \times \mathfrak{H}_2$, в котором группа $\mathfrak{H}_2$ была бы также нормальным делителем группы $\mathfrak{G}$; 3) можно найти разложение $\mathfrak{H} = \mathfrak{H}_1 \times \mathfrak{H}_2$, в котором группа $\mathfrak{H}_2$ представляет нормальный делитель группы $\mathfrak{G}$.

2. Оставляя в стороне случай 1), спросим себя, когда может встретиться случай 2). Группу $\mathfrak{H}$ можно представить при посредстве некоторого базиса. Тогда группа $\mathfrak{G}/\mathfrak{H}$ допускает представление Γ (возможно, несобственное) в виде линейной однородной группы типа

Шатле, модуль которой будет образован некоторым базисом группы $\mathfrak{H}$. Порядок $\mathfrak{H}$ можно считать равным l^m, где l — простое число. Действительно, K/k всегда можно разложить в относительное произведение абсолютно-нормальных относительных полей, относительные степени которых суть степени простых чисел.

На основании результатов § 2 мы заключаем, что случай 2) может встретиться только тогда, если порядок Г не взаимно прост с порядком $\mathfrak{H}$. Но Г есть факторгруппа группы $\mathfrak{G}/\mathfrak{H}$ и порядок $\mathfrak{H} = l^m$; значит, случай 2) возможен только тогда, если l входит как фактор и в число классов и в степень поля k. Исключив эту возможность, мы придем к случаю 3). Здесь $\mathfrak{H} = \mathfrak{H}_1 \times \mathfrak{H}_2$, причем $\mathfrak{H}_1$ и $\mathfrak{H}_2$ являются нормальными делителями группы $\mathfrak{G}$. Поле K/k разлагается в относительное произведение двух полей, одно из которых относительно неразветвлено над k, в то время как другое не содержит никакого подполя, относительно неразветвленного над k. В последующем мы ограничимся рассмотрением только таких относительных полей.

3. Определение. Если относительно-абелево поле K/k не содержит подполей, относительно неразветвленных над k, то будем говорить, что поле K/k чисто разветвляющееся (rein verzweigt).

Для чисто разветвляющегося поля можно установить простую связь между ведущим идеалом $\mathfrak{f}$ поля K/k и структурой абсолютной группы $\mathfrak{G}$ поля K. Именно, имеет место

Теорема 1. *Пусть K_1 — наибольшее чисто разветвляющееся относительно-абелево надполе поля k, принадлежащее ведущему идеалу $\mathfrak{f}_1$, K — норма K_1 и $\mathfrak{H}_1$ — группа, к которой принадлежит K_1 внутри K. Если $\mathfrak{N}$ — нормализатор группы $\mathfrak{H}_1$ и $\mathfrak{G}_{\mathfrak{f}_1}$ — наибольшая группа, относительно которой идеал $\mathfrak{f}_1$ инвариантен внутри k, то имеет место*

$$\mathfrak{G}_{\mathfrak{f}_1} = \mathfrak{N}/\mathfrak{H}.$$

Доказательство. Если подстановка S группы $\mathfrak{g} = \mathfrak{G}/\mathfrak{H}$ переводит идеал $\mathfrak{f}_1$ в $\mathfrak{f}_1^S$, то поле K_1 той же подстановкой переводится в поле K_1^S, принадлежащее к группе $S^{-1}\mathfrak{H}_1 S$. K_1^S есть наибольшее чисто разветвляющееся поле, принадлежащее ведущему идеалу $\mathfrak{f}_1^S$. Если $\mathfrak{f}_1^S = \mathfrak{f}_1$, т. е. S принадлежит к $\mathfrak{G}_{\mathfrak{f}_1}$, то и $K_1^S = K_1$, откуда следует, что $S^{-1}\mathfrak{H}_1 S = \mathfrak{H}_1$, т. е., что $\mathfrak{H}S$ содержится в нормализаторе $\mathfrak{N}$. Если же $\mathfrak{f}_1^S \neq \mathfrak{f}_1$, то и K_1^S не может совпадать с K_1. В самом деле, если бы K_1^S совпадало с K_1, то K_1 принадлежало, бы как ведущему идеалу $\mathfrak{f}_1$, так и ведущему идеалу $\mathfrak{f}_1^S$, а следовательно, и их общему наибольшему делителю, что противоречит определению ведущего идеала. Теорема доказана.

4. Чтобы более ясно представить последующие рассуждения, рассмотрим не саму группу $\mathfrak{H}$, но изоморфную с ней группу $\hat{\mathfrak{H}}$ дуального

пространства, названную нами в § 3.4 *корпусгруппой*. Способ образования ее уже описан в § 3.4 для случая, когда поле K есть поле радикалов; иначе говоря, когда поле k содержит l^m-ые корни из единицы. Ограничение это легко устранить, если вместо умножения радикалов воспользоваться общим понятием композиции полей, примененным уже Кронекером [11]. Отнесем каждому циклическому полю K_1 циклическую группу $\mathfrak{A}$ того же порядка. Если $K_1 = k(\alpha)$ и $\mathfrak{A} = E + A + \ldots + A^{n-1}$, то каждому элементу из $\mathfrak{A}$ отнесем некоторое расположение сопряженных с α величин. Именно, пусть

$$A^k \to \{\alpha,\ \alpha^{A^k},\ \alpha^{A^{2k}},\ \ldots,\ \alpha^{A^{(n-1)k}}\}.$$

Если теперь $K_2 = k(\beta)$, $\mathfrak{B} = E + B + \ldots + B^{n-1}$, то пусть группа

$$\mathfrak{A}\mathfrak{B} = E + AB + \ldots + A^{n-1}B^{n-1}$$

отнесена полю $K = k(\gamma) = k(\alpha\beta + \alpha^A\beta^B + \ldots + \alpha^{A^{n-1}}\beta^{B^{n-1}})$. Это поле не зависит от выбора величин α и β внутри их полей, если только считать эти величины примитивными. В самом деле, поле это инвариантно внутри K относительно подстановок из $\mathfrak{H}$, переводящих одновременно α в α^{A^k} и β в β^{B^k} ($k = 1, 2, \ldots, n-1$). Группа, образованная этими подстановками, имеет индекс n относительно $\mathfrak{H}$. Теперь, если мы хотим фиксировать в этой группе некоторый элемент, то мы должны поставить вместо γ одну из сопряженных с ней величин, например γ^{AB}

$$AB \to \{\gamma, \gamma^{AB},\ \gamma^{A^2B^2}, \ldots, \gamma^{A^{n-1}B^{n-1}}\}.$$

Точно так же как и в § 3.4, мы можем определить здесь символ A^S, где S обозначает автоморфизм группы $\mathfrak{H}$. Определенная таким образом группа автоморфизмов изоморфна с Г.

§ 6. Случай, когда ведущий идеал — простой

1. Пусть $\mathfrak{f} = \mathfrak{p}$, где $\mathfrak{p}$ — простой идеал поля k, и пусть l — простое число, взаимно простое с $\mathfrak{p}$. Случай этот рассмотрен уже Шольцем ([15], стр. 348—353), и мы здесь в основном будем следовать указанному им пути.

Чтобы над полем k существовало чисто разветвляющееся циклическое поле относительной степени l^m с ведущим идеалом $\mathfrak{p}$ (в этом случае говорят, что $\mathfrak{p}$ *примарно* mod l^m), достаточно, чтобы $\mathfrak{p}$ в поле $k\left(\exp\left(\frac{1}{l^{m+s}}\right), \sqrt[l^m]{\varepsilon_i}, \sqrt[l^m]{\rho_i}\right)$ разлагалось в произведение простых идеалов относительной степени 1 и чтобы имело место сравнение $N(\mathfrak{p}) \equiv 1 \pmod{l^m}$. Здесь $\exp\left(\frac{1}{l^s}\right)$ — наивысший содержащийся в k l-й корень из 1, ε_i — основные единицы и ρ_i — l^m-е степени идеалов поля k.

2. Если k содержит l^m-ый корень из 1, то есть другой критерий примарности простого идеала $\mathfrak{p}$ по mod l^m. В случае $m=1$ он гласит следующее ([24], стр. 16): должен существовать такой идеал $\mathfrak{q}$, что $\mathfrak{p}\mathfrak{q}^l \approx \alpha \equiv 1 \pmod{\lambda^l}$,[1] где $\lambda \equiv 1 - \exp\left(\frac{1}{l}\right)$ (α называется тогда *примарным числом*). В случае $m \neq 1$ условие примарности в терминах сравнений доселе не сформулировано явно (ср. [3] и [8], стр. 47). Замечу только, что числа, удовлетворяющие этому условию, образуют мультипликативную группу. Это обстоятельство будет полезным в случае составного ведущего идеала.

3. Теперь рассмотрим норму относительно-циклического поля K_1 типа, рассмотренного выше. Если мы применим к K_1 подстановку S группы $\mathfrak{g}$, то поле это перейдет в поле K_1^S с ведущим идеалом $\mathfrak{p}^S$. При этом, если подстановка S изменяет идеал $\mathfrak{p}$, то поле K_1^S наверное отлично от поля K_1; если же $\mathfrak{p}^S = \mathfrak{p}$, то только в некоторых специальных случаях можно утверждать, что K_1^S совпадает с K_1. Например, если k содержит l^m-ый корень из единицы и $\mathfrak{p}\mathfrak{q}^l \approx \alpha$, то $K_1^S = K_1$ тогда и только тогда, если между ассоциированными с α числами найдется число, лежащее в поле разложения k_1 идеала $\mathfrak{p}$. Если это не так, то $\frac{\alpha^S}{\alpha} = \varepsilon$ есть степень идеала, норма которого относительно k_1 равна 1. В частности, если $\mathfrak{p} \approx \alpha$, то ε является алгебраической единицей, которая может быть представлена как символическая $(S-1)$-я степень некоторого числа, не являющегося единицей. Этот случай наверное не имеет места, если наперед известно, что поле k допускает отделение чисто разветвляющегося l-поля (см. § 5.2). Тогда справедлива теорема 1.

4. Чтобы исследовать в этом случае структуру абсолютной группы $\mathfrak{G}$ относительного поля, будем различать следующие три подслучая: 1) $\mathfrak{p}$ есть некритический идеал степени 1; 2) $\mathfrak{p}$ есть некритический идеал высшей степени; 3) $\mathfrak{p}$ есть критический идеал.

1) $\mathfrak{p}$ есть некритический идеал степени 1. Для абелевых групп $\mathfrak{G} = \mathfrak{G}/\mathfrak{H}$ случай этот рассмотрен Шольцем ([15], стр. 348—353). Но если группа $\mathfrak{G}$ произвольна, то никаких новых трудностей не возникает.

Каждому сопряженному с $\mathfrak{p}$ простому идеалу соответствует относительно-циклическое поле относительной степени l^m. Так как степень $\mathfrak{p}$ равна 1, то число различных полей этого рода равно порядку группы $\mathfrak{G}/\mathfrak{H}$. Обозначим сопряженные с $\mathfrak{p} = \mathfrak{p}_1$ простые идеалы через $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ ($n = \text{Пор. } \mathfrak{g}$) и будем последовательно присоединять к k соответствующие этим простым идеалам поля $K_1, K_2, \ldots, K_n$. Каждое новое присоединение будет увеличивать относительную степень поля в l^m раз. Действительно, в противном случае существо-

[1] Знак $\approx$ заменяет слово «ассоциирован».

вало бы поле K_{i+1}, пересекающееся с $K_1 K_2 \dots K_i$ вне k, что невозможно, так как относительные дискриминанты $K_1 K_2 \dots K_i$ и K_{i+1} являются произведениями степеней простых идеалов $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_i$ и $\mathfrak{p}_{i+1}$, то есть взаимно просты, в то время как поле K_{i+1} — чисто разветвляющееся.

Отсюда следует, что группа $\mathfrak{H}$ будет n-членного типа $[p^m, p^m, \dots, p^m]$ и что каждый ее базисный элемент может быть переведен в любой другой посредством некоторой подстановки группы $\mathfrak{G}$. Шольц [17] доказал, что подобная группа, которую он назвал *общей диспозиционной группой*, вполне определена, коль скоро заданы $\mathfrak{G}/\mathfrak{H}$ и l^m.

Подчеркнем еще, что в этом случае поля K всегда являются чисто разветвляющимися, какие бы мы ни выбрали чисто разветвляющиеся поля K_1. (Поле K определяется посредством $\mathfrak{p}_1$ только с точностью до неразветвленного «поля—множителя»; если, например, $K_1 = k\left(\sqrt[l^m]{\alpha}\right)$, то можно принять также $K_1 = k\left(\sqrt[l^m]{\alpha\omega}\right)$, где $k\left(\sqrt[l^m]{\omega}\right)$ является неразветвленным полем, т. е. абсолютным полем классов.) Это связано со структурой диспозиционной группы (ср. § 2.4, второй критерий).

5. Теперь мы перейдем к тому случаю, когда $\mathfrak{p}$ является критическим [подслучай 3]. При этом мы воспользуемся понятием корпусгруппы. Пусть $\hat{\mathfrak{H}}$ будет корпусгруппа поля K, $\hat{\mathfrak{h}}$ — циклическая подгруппа, соответствующая циклическому подполю K_1 относительной степени l^m, $\mathfrak{N}$ — нормализатор $\hat{\mathfrak{h}}$ ($\mathfrak{G} > \mathfrak{N} > \hat{\mathfrak{H}}$) и $\mathfrak{N}_1$ — нормализатор производящего элемента группы $\hat{\mathfrak{h}}$. Докажем, что группа инерции идеала $\mathfrak{p}$ содержится в $\mathfrak{N}_1/\hat{\mathfrak{H}}$. Для этого рассмотрим группу классов поля k, соответствующую полю K_1. Так как K_1 — чисто разветвляющееся поле, то каждый из «классов» содержит абсолютные главные идеалы по соответствующему ему делению на классы. Действительно, в противном случае все абсолютные главные идеалы содержались бы в одном правильном делителе группы классов поля K_1. Если мы будем понимать последний как единичный элемент нового деления на классы, то ему соответствует поле, которое должно быть одновременно подполем абсолютного поля классов и поля K_1, что исключено (ср. [15], стр. 351). Таким образом, мы можем рассматривать числа поля k как представителей наших «классов». Умножение числа на единицы или на l^m-е степени идеалов не изменяет «класса» этого числа, так как вследствие примарности $\mathfrak{p}$ имеет место

$$\left(\frac{\varepsilon}{\mathfrak{p}}\right)_{l^m} = 1, \quad \left(\frac{\rho}{\mathfrak{p}}\right)_{l^m} = 1,$$

в то время как все норменные вычеты (и, в частности, все l^m-е степенные вычеты) образуют единичный элемент нашей группы классов ([23], стр. 48—51). Между этими «классами» и подстановками

относительной группы $\hat{\mathfrak{h}}$ поля K_1, согласно артиновскому закону взаимности [1], существует взаимно однозначное соответствие. Именно, если σ — производящая подстановка этой относительной группы, A — любое целое число поля K, то имеет место

$$A^{N(\mathfrak{q})} \equiv A^{\sigma} \pmod{\mathfrak{q}}, \tag{1.6}$$

и σ зависит только от «класса», в котором лежит $\mathfrak{q}$.

Следовательно, если S является подстановкой из $\mathfrak{R}$, то σ^S совпадает с σ тогда и только тогда, если простые идеалы $\mathfrak{q}$ и $\mathfrak{q}^S$ лежат в одном и том же «классе». Если, в частности, $\mathfrak{q} \approx \omega$, $\mathfrak{q}^S \approx \omega^S$ — «главные идеалы», то это свойство может быть формулировано следующим образом:

$$\omega^S / \omega \equiv n(\Omega) \pmod{\mathfrak{p}}, \tag{2.6}$$

где Ω означает некоторое число из поля K_1, а $n(\ldots)$ есть символ относительной нормы. Если S содержится в группе инерции $\mathfrak{f}_p$ идеала $\mathfrak{p}$ (точнее, в $\hat{\mathfrak{f}}_p$), то для каждого целого числа ω поля k имеет место

$$\omega^S / \omega \equiv 1 \equiv n(1) \pmod{\mathfrak{p}},$$

откуда следует, что сравнение (2.6) безусловно удовлетворяется, чем доказывается наше утверждение.

6. Обратное не всегда имеет место. Чтобы исследовать этот вопрос, примем во внимание, что в k можно найти бесчисленное множество простых идеалов, которые являются абсолютными главными идеалами и лежат в произвольно заданных классах сравнений по модулю $\mathfrak{p}$ [9]. Предположим, что $\sigma^S = \sigma$ для всех σ; тогда (2.6) имеет место для каждого целого ω из k. Если при этом всегда $n(\Omega) \equiv 1 \pmod{\mathfrak{p}}$, то S непременно принадлежит группе инерции идеала $\mathfrak{p}$. Это наверное имеет место только тогда, если $p - 1$ не делится на l. В самом деле, если S есть производящая подстановка группы разложения идеала $\mathfrak{p}$ и $N(\mathfrak{p}) \equiv p^f$, то, как известно, имеет место

$$\omega^S \equiv \omega^p \pmod{\mathfrak{p}}. \tag{3.6}$$

Из (2.6) и (3.6) следует

$$\omega^{p-} \equiv n(\Omega) \pmod{\mathfrak{p}}.$$

С другой стороны, $\omega^{l^m} = n(\omega)$. Если (x, y) — решение диофантова уравнения

$$(p-1)x + l^m y = 1,$$

то

$$\omega \equiv n(\Omega^x \omega^y) \pmod{\mathfrak{p}}.$$

Таким образом, каждое число ω из k лежит в «главном классе», что противоречит определению «главного класса». Можно доказать

большее: если $S_{\mathfrak{p}}^d$ есть первая степень подстановки S, перестановочная с σ, то

$$p^d \equiv 1 \pmod{l^m}.$$

Чтобы доказать эту формулу, рассмотрим соответствующую простому идеальному множителю идеала $\mathfrak{p}$ в поле K_1 группу инерции относительно k_1, где k_1 принадлежит к $\mathfrak{N}$. Так как $(p, l) = 1$, то группа $\hat{\mathfrak{h}}$ должна быть изоморфной некоторому делителю факторгруппы $\mathfrak{T}/\mathfrak{B}$ (где $\mathfrak{B}$ — группа разветвления); следовательно, пор. $\mathfrak{T}/\mathfrak{B} \equiv 0 \pmod{l^m}$. Так как $\sigma (= \tau^k)$ можно рассматривать как подстановку группы $\mathfrak{T}/\mathfrak{B}$, а S — как подстановку группы $\mathfrak{N}/\mathfrak{B}$, то по формуле Шпейзера ([21], стр. 177, теорема 1) имеет место

$$S^{-1}\tau S = \tau^p, \quad S^{-1}\sigma S = S^{-1}\tau^k S = \tau^{kp} = \sigma^v, \quad S^{-d}\sigma S^d = \sigma^{pd}.$$

Так как пор. $\sigma = l^m$, то из перестановочности S^a и σ следует

$$\sigma = \sigma^{pd}, \quad \text{т. е. } p^d \equiv 1 \pmod{l^m}, \text{ ч. и т. д.}$$

Наоборот, если $p^d \equiv 1 \pmod{l^m}$ и $\hat{\mathfrak{h}}^S = \hat{\mathfrak{p}}$, то $\sigma^{S^d} = \sigma$, безразлично, является ли идеал $\mathfrak{p}$ критическим, или нет. Действительно, из

$$\omega^{S^d} \equiv \omega^{p^d} \pmod{\mathfrak{p}}$$

следует, что

$$\omega^{S^d} / \omega \equiv \omega^{p^d - 1} \equiv \omega^{kl^m} \equiv n\,(\omega^k) \pmod{\mathfrak{p}},$$

где $k = \dfrac{p^d - 1}{l^m}$, а это значит, что $\dfrac{\omega^{S^a}}{\omega}$ лежит в «главном классе», откуда следует, что подстановка S^d перестановочна с σ.

7. Теперь мы подробнее исследуем случай, когда идеал $\mathfrak{p}$ не является критическим (подслучай 2). В поле K_1 $\mathfrak{p}$ является l^m-ой степенью простого идеала $\mathfrak{P}$: $\mathfrak{p} \approx \mathfrak{P}^{l^m}$. Здесь $\hat{\mathfrak{h}}$ является группой инерции, а $\mathfrak{N}$ — группой разложения идеала $\mathfrak{P}$. (Так как K_1 не является абсолютно нормальным полем, то мы не можем образовать абсолютных групп разложения, а лишь группы разложения относительно поля k_1, которое принадлежит к $\mathfrak{N}$; их поведение точно соответствует π-адическим разложениям, открытым Гензелем, которые применимы и к ненормальным полям). Так как порядок l^m-e группы инерции взаимно прост с p, то мы имеем так называемый регулярный случай ([10], гл. 8). Здесь мы будем следовать обозначениям Оре, так как одна из его работ ([13], стр. 657—660) устанавливает (хотя и не в π-адическом виде) в явной форме связь между π-адическими разложениями и группами разложения.

Прежде всего, мы находим в поле инерции (т. е. в k) число τ, которое является первообразным корнем сравнения

$$x^{p^f-1} \equiv 1 \pmod{\mathfrak{P}^{e\alpha}}, \tag{4.6}$$

где α может быть выбрано произвольно большим ([13], стр. 657, теорема 3). Затем находим в поле K_1 «простое число» π (т. е. число, точно делящееся на первую степень $\mathfrak{P}$), которое удовлетворяет двучленному сравнению

$$x^e + p\tau^a \equiv 0 \pmod{\mathfrak{P}^{e\alpha}} \tag{5.6}$$

при произвольно больших α ([13], стр. 658). Если Z и T — производящие подстановки группы разложения и соотв. группы инерции, так что имеет место

$$\begin{aligned} &\tau^Z \equiv \tau^p \pmod{\mathfrak{P}^{e\alpha}}, \quad \pi^Z \equiv \tau^\lambda \pi \pmod{\mathfrak{P}^2} \quad \left(\lambda = \frac{a(p-1)}{e}\right), \\ &\tau^T \equiv \tau, \qquad\qquad \pi^T \equiv \tau^b \pi \pmod{\mathfrak{P}^{e\alpha}} \quad \left(b = \frac{p^f-1}{e}\right), \end{aligned} \tag{6.6}$$

то группа разложения состоит из произведений

$$Z^i T^j \quad (i = 0, 1, \ldots, f-1; \quad j = 0, 1, \ldots, e-1),$$

причем между Z и T имеют место следующие определяющие соотношения

$$Z^f = T^a, \quad T^e = 1, \quad Z^{-1}TZ = T^p \tag{7.6}$$

([13], стр. 660, теорема 5). При этом $p^f - 1 \equiv a(p-1) \equiv 0 \pmod{e}$.

8. В определяющие соотношения (7.6) нашей группы разложения входит только одна величина, которая не определяется посредством $\mathfrak{G}/\mathfrak{H}$ и p, именно a. Для того чтобы полностью охарактеризовать группу разложения $\mathfrak{N}$, достаточно определить число a сообразно поведению простого числа p по отношению к полю k. Сравнение (5.6) показывает, что число $\pm\tau^a p$ является норменным вычетом некоторого числа из K_1 по модулю любой сколь угодно высокой степени $\mathfrak{p}$. Этот факт может быть записан следующим образом

$$\left(\frac{\pm\tau^a p, K_1}{\mathfrak{p}}\right) = 1, \tag{8.6}$$

где $\left(\frac{\beta, K}{\mathfrak{p}}\right)$ есть введенный Гассе символ норменного вычета ([8], стр. 35, III). В силу его свойства

$$\left(\frac{\alpha\beta, K}{\mathfrak{p}}\right) = \left(\frac{\alpha, K}{\mathfrak{p}}\right)\left(\frac{\beta, K}{\mathfrak{p}}\right) \quad \text{([8], стр. 26, (4)),}$$

мы имеем

$$\left(\frac{\tau, K_1}{\mathfrak{p}}\right)^a = \left(\frac{\pm 1, K_1}{\mathfrak{p}}\right)\left(\frac{p, K_1}{\mathfrak{p}}\right)^{-1}. \tag{9.6}$$

Так как τ является примитивным числом, так что все вычеты по модулю $\mathfrak{p}$ могут быть представлены его степенями, то a вполне определяется из (9.6).

9. Теперь несколько преобразуем формулу (9.6). Положим $\varkappa = \frac{n}{f}$, $p \approx \Pi_1\Pi_2\cdots\Pi_\varkappa R^{-1}$ (R есть l^m-ая степень идеала), $\Pi_1 \approx \pi^e$ (Π_i делится точно на первую степень простого делителя $\mathfrak{p}_i$ числа p и не делится ни на какой другой простой делитель числа p). Тогда имеет место формула ([8], стр. 25):

$$\left(\frac{p, K}{\mathfrak{p}}\right) = \left(\frac{K_1}{\mathfrak{p}_2\mathfrak{p}_3\cdots\mathfrak{p}_\varkappa}\right) = \left(\frac{K_1}{\mathfrak{p}_2}\right)\left(\frac{K_1}{\mathfrak{p}_3}\right)\cdots\left(\frac{K_1}{\mathfrak{p}_\varkappa}\right), \tag{10.6}$$

где $\left(\frac{K_1}{\mathfrak{p}_i}\right)$ есть так называемый символ Артина, который понимается как такая подстановка относительной группы поля K_1/k, которая переводит целое число A поля K_1 по модулю $\mathfrak{p}_i$ в $A^{N(\mathfrak{p}_i)}$ ($i = 2, 3, \ldots, \varkappa$). С другой стороны, легко усмотреть, что двойной знак ± 1 в формуле (9.6) означает, что следует брать -1 для нечетного l и $+1$ для $l = 2$. Но в обоих случаях $\left(\frac{\pm 1, K_1}{\mathfrak{p}}\right) = 1$, так как ± 1 лежит в «главном классе».

10. Выражение (10.6) принимает значительно более простую форму, если K_1 является обобщенным куммеровским полем ([8], стр. 41 и след.), т. е. если основное поле k содержит l^m-ые корни из единицы. В этом случае $\left(\frac{K_1}{\mathfrak{p}_i}\right) = \left(\frac{\Pi_1}{\mathfrak{p}_i}\right) = \left(\frac{\Pi_i}{\mathfrak{p}_i}\right)$ и из формул (9.6) и (10.6) следует

$$\left(\frac{\tau, K_1}{\mathfrak{p}_1}\right)^a = \left(\frac{\Pi_2\Pi_3\cdots\Pi_\varkappa}{\mathfrak{p}_1}\right)^{-1}, \tag{11.6}$$

где $\left(\frac{\alpha}{\mathfrak{p}}\right)$ означает символ Лежандра. Но так как значение символа Лежандра не меняется при прибавлении к «числителю» кратности $\mathfrak{p}_1$, то формула (11.6) может быть представлена в двух следующих видах:

$$\left(\frac{\tau, K_1}{\mathfrak{p}_1}\right)^a = \left(\frac{\Pi_2\Pi_3\cdots\Pi_\varkappa + \Pi_1\Pi_3\cdots\Pi_\varkappa + \cdots + \Pi_1\Pi_2\ldots\Pi_{\varkappa-1}}{\mathfrak{p}_1}\right)^{-1}, \tag{12,6}$$

$$\left(\frac{\tau, K_1}{\mathfrak{p}_1}\right)^a = \left(\frac{(\Pi_2 - \Pi_1)(\Pi_3 - \Pi_1)\cdots(\Pi_\varkappa - \Pi_1)}{\mathfrak{p}_1}\right)^{-1}. \tag{13.6}$$

Формулы эти допускают следующее истолкование. Величины Π_2, $\Pi_3, \ldots, \Pi_\varkappa$ получаются, если мы производим над Π_1 подстановки, являющиеся представителями смежных классов в разложении

$$\mathfrak{G} = \mathfrak{N} + \mathfrak{N}S_2 + \cdots + \mathfrak{N}S_\varkappa.$$

В частности, если мы сможем выбрать Π_1 таким образом, чтобы оно принадлежало к группе $\mathfrak{N}$, то симметрические функции от $\Pi_1, \Pi_2, \ldots, \Pi_\varkappa$

будут рациональными числами. Следовательно, $\Pi_1, \Pi_2, \ldots, \Pi_\varkappa$ будут удовлетворять некоторому уравнению с рациональными коэффициентами

$$F(y) = y^\varkappa + P_1 y^{\varkappa-1} + \cdots + P_{\varkappa-1} y + P_\varkappa = 0.$$

Тогда формулы (12.6), (13.6) мы сможем записать следующим образом:

$$\left(\frac{\tau, K_1}{\mathfrak{p}_1}\right)^a = \left(\frac{P_{n-1}}{\mathfrak{p}_1}\right)^{-1}, \tag{12'.6}$$

$$\left(\frac{\tau, K_1}{\mathfrak{p}_1}\right)^a = \left(\frac{F'(\Pi_1)}{\mathfrak{p}_1}\right)^{-1}. \tag{13'.6}$$

Выражение $F'(\Pi_1)$ есть дифферента числа Π_1.

Заметим, что произвол в выборе примитивного числа τ влияет на значение a. С другой стороны, мы изменяем a, если выбираем другую производящую подстановку T. Таким образом, для нас важно не значение числа a, а только максимальная содержащаяся в нем степень l.

11. Если k и $\mathfrak{p}$ заданы, то мы без труда можем определить число a по одной из формул, приведенных в пункте 10. Для того же, чтобы решить задачу A, важно ответить на следующий вопрос: пусть k и a даны. Имеются ли в k примарные идеалы $\mathfrak{p}$, которым соответствует заданное a. Мне не удалось ответить на этот вопрос. Главная трудность заключается в том, что не удается получить для $\left(\frac{\tau, K_1}{\mathfrak{p}}\right)^a$ такую формулу, чтобы в числителе символа Лежандра стояло число, не зависящее от выбора p. Число $F'(\Pi_1)$ не является дифферентой поля, а дифферентой числа Π_1, $\delta(\Pi_1)$. С другой стороны, очевидно, что значение $\left(\frac{\delta(\alpha)}{\mathfrak{p}}\right)$ изменяется, если мы изменим α и оставим без изменения $\mathfrak{p}$.

12. Резюмируем теперь содержание этого параграфа. Мы рассмотрели здесь относительно циклические поля, ведущий идеал которых состоит только из одного простого идеала и нормы которых чисто разветвляющиеся, и получили следующие результаты.

Если ведущий идеал $\mathfrak{p}$ является простым идеалом первой степени, то группа $\mathfrak{G}$ есть общая диспозиционная группа. Поле K всегда чисто разветвляющееся.

Если $\mathfrak{p}$ есть критический идеал и $\mathfrak{T}/\mathfrak{H}$ — его группа инерции, то $\mathfrak{T}$ содержится в нормализаторе $\mathfrak{N}_1$ производящего элемента корпусгруппы. Если $\mathfrak{N}/\mathfrak{H}$ его группа разложения, то $\mathfrak{N}$ есть нормализатор корпусгруппы поля K_1. Если S — производящая подстановка группы разложения идеала $\mathfrak{p}$, то $\mathfrak{N}_1$ (т. е. нормализатор отдельных элементов и корпусгруппы) есть совокупность подстановок S^d, где показатели d удовлетворяют сравнению $p^d \equiv 1 \pmod{l^m}$.

Если идеал $\mathfrak{p}$ не является критическим, то поле K чисто разветвляющееся, если $\mathfrak{p}$ остается главным идеалом также и в поле разложе-

ния. Структура группы разложения идеала $\mathfrak{p}$ определяется наименьшим корнем d сравнения $p^d \equiv 1 \pmod{l^m}$ и числом a, причем a может быть определено из уравнения

$$\left(\frac{\tau, K_1}{\mathfrak{p}_1}\right)^{-a} = \left(\frac{K_1}{\mathfrak{p}_2}\right)\left(\frac{K_1}{\mathfrak{p}_3}\right)\cdots\left(\frac{K_1}{\mathfrak{p}_\varkappa}\right).$$

Когда структура этой группы разложения $\mathfrak{Z}$ известна, то группа $\mathfrak{G}$ определяется однозначно, если «предположение» § 4 справедливо. Это непременно имеет место в случае, если $\mathfrak{Z}$ есть прямое произведение группы инерции и другой циклической группы, т. е. если

$$p \equiv 1 \pmod{l^m},\ a = 0.$$

13. Мы оставили неисследованным тот случай, когда все сопряженные нормализаторы сопряженных циклических подгрупп группы $\hat{\mathfrak{H}}$ содержат правильную надгруппу $\mathfrak{M}$ группы $\hat{\mathfrak{H}}$. Этот случай требует более подробного исследования. Относящийся сюда простейший подслучай встречается, если K распадается в относительное произведение двух полей, одно из которых есть k (как надполе над k_1, где k_1 принадлежит к $\mathfrak{M}$), другое же есть относительно абелево поле над k_1, относительная группа которого изоморфна с $\mathfrak{H}$. Этот подслучай имеет место тогда и только тогда, если группа $\mathfrak{H}$ есть прямой множитель группы $\mathfrak{M}$.

§ 7. Случай составных ведущих идеалов

1. Мы переходим к исследованию относительно циклических полей степени l^m, в относительные дискриминанты которых входят несколько простых идеалов. В целях упрощения предположим, что ведущий идеал взаимно прост с l. Пусть $\mathfrak{f} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s$. Предположим пока что, что идеалы $\mathfrak{p}_i$ будут первой степени. Присоединим к основному полю k его полное абсолютное l-поле классов $\bar{k}$ (т. е. наиболее широкое относительно неразветвленное абелево надполе, относительная степень которого есть степень l) или же одно из его подполей, так чтобы в новом поле все идеалы $\mathfrak{p}_i$ стали главными [4]. Затем рассмотрим поле $\bar{K}_1 = \bar{k}\left(\sqrt[l^m]{\mathfrak{p}_1}, \sqrt[l^m]{\mathfrak{p}_2}, \ldots, \sqrt[l^m]{\mathfrak{p}_s}\right)$, причем под $\mathfrak{p}_i$ я понимаю здесь просто ассоциированное с $\mathfrak{p}_i$ число поля $\bar{k}$. Одновременно рассмотрим норму $\bar{K}$ этого поля, которую получим, подвергая величины поля K_1 автоморфизмам, состоящим из подстановок группы Галуа $\bar{\mathfrak{G}}$ поля $\bar{K}$. Если k принадлежит в $\bar{k}$ к группе $\mathfrak{K}$, то можно разложить $\bar{\mathfrak{G}}$ следующим образом:

$$\bar{\mathfrak{G}} = \mathfrak{K} + \mathfrak{K}S_2 + \cdots + \mathfrak{K}S_n.$$

Группа $\mathfrak{G}/\mathfrak{K}$ смежных классов $\mathfrak{K}S_i$ изоморфна с первоначальной группой $\mathfrak{G}/\mathfrak{H}$.

Теперь рассмотрим подполе K поля $\bar{K}$, радиканды (Radikanden) которого (состоящие из произведений степеней $\mathfrak{p}_1^{S_i}, \mathfrak{p}_2^{S_i}, \ldots, \mathfrak{p}_s^{S_i}, i = 1, 2, \ldots, n$) ассоциированы с первообразными по модулю l^m числами из k. При этом заметим, что автоморфизмы, лежащие в одном и том же классе смежности разложения (1.7) переводят каждый идеал $\mathfrak{p}_i$ в один и тот же простой идеал, т. е. в число, ассоциированное с $\mathfrak{p}_i$. Каждый из радикандов, образующих поле K, переходит при этом непременно в одно и то же число, если мы выберем числа из $\bar{K}$, соответствующие идеалам $\mathfrak{p}_i$ таким образом, чтобы радиканды поля K являлись числами из k. Последнее всегда может быть достигнуто, так как радиканды поля K образуют мультипликативную абелеву группу, которая в соответствии с этим имеет базис, состоящий из независимых элементов. Если провести указанное нормирование в элементах базиса, то нормируется и вся корпусгруппа. Но легко может случиться, что некоторые из нормированных таким образом величин, ассоциированных с сопряженными друг с другом величинами, не переходят друг в друга при соответствующем автоморфизме, а что одна переходит в другую, умноженную на некоторую единицу поля k. (Если мы примем, что идеалы, о которых идет речь, сами не являются абсолютными главными идеалами поля k, а становятся главными идеалами лишь после умножения на l^m-ые степени идеалов, то вместо единиц здесь могут также появиться l^m-ые степени идеалов.) Однако, если K содержит максимальное чисто разветвляющееся подполе (т. е. если мы имеем случай 3, § 5.1), то этой возможности можно избегнуть.

Рассмотрим теперь группу автоморфизмов поля $\bar{K}$, причем не будем рассматривать как различные автоморфизмы, содержащиеся в одних и тех же смежных классах $\mathfrak{K}S_i$. Поле $\bar{K}$ распадается в относительное произведение полей, из коих каждое порождается простым идеалом $\mathfrak{p}_i$ и всеми с ним сопряженными. Пусть, например, одним из этих полей будет $\bar{k}\left(\sqrt[l^m]{\mathfrak{p}_1}, \sqrt[l^m]{\mathfrak{p}_1^{S_2}}, \ldots, \sqrt[l^m]{\mathfrak{p}_1^{S_n}}\right)$. Его группа будет общей диспозиционной группой, так как все поля $\bar{k}\left(\sqrt[l^m]{\mathfrak{p}_1^{S_i}}\right)$ $(i = 1, 2, \ldots, n)$ имеют различные относительные дискриминанты и, следовательно, взаимно просты над $\bar{k}$.

Для того чтобы получить абсолютную группу Галуа поля K, заметим, что K является подполем поля $\bar{K}$. Его корпусгруппа будет подгруппой корпусгруппы поля $\bar{K}$. Учтем при этом, что эта подгруппа инвариантна относительно автоморфизмов группы $\mathfrak{G}/\mathfrak{H}$, так как каждый элемент поля $\bar{K}$ может принадлежать к K только вместе со всеми своими сопряженными. Группа поля K, таким образом, изоморфна

некоторой факторгруппе произведения диспозиционных групп. Эта группа получается следующим образом: сначала нужно образовать произведение корпусгрупп, о которых идет речь; затем определить его элементы, соответствующие примарным радикандам, т. е. лежащие в K. Автоморфизмы этой подгруппы корпусгруппы, порождаемые группой $\mathfrak{G}/\mathfrak{H}$, образуют абсолютную группу поля K. Это *точно* имеет место (ср. § 3.6), так как мы рассматриваем теперь факторгруппу относительного произведения диспозиционных групп, а каждая диспозиционная группа полностью определяется автоморфизмами своей корпусгруппы.

Вместо того чтобы рассматривать мультипликативную группу радикалов, мы можем непосредственно применить разъясненное в параграфе 5.4 понятие композиции полей, чтобы тем самым избежать присоединения к основному полю корней из единицы. Однако для того чтобы с уверенностью провести эту операцию, было бы необходимо вычислить дискриминанты, а также ведущие идеалы компонируемых полей.

Только что построенное нами поле K должно содержать норму циклического поля с заданным ведущим идеалом $\mathfrak{f}$. Вопрос о том, совпадает ли эта норма с полем K, может быть легко решен по виду ведущего идеала $\mathfrak{f}$.

2. *Пример 1.* Основное поле k есть норма кубического поля без аффекта. $\mathfrak{f} = \mathfrak{p}_1\mathfrak{p}_2$, причем $\mathfrak{p}_1$ — простой идеал первой степени и

$$p = N(\mathfrak{p}_1) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6.$$

Знак ~ 1 должен означать здесь, что левая часть ассоциирована с примарным по модулю l^m числом. Пусть

$$\mathfrak{G} = E + (12)(36)(45) + (135)(246) + (153)(264) + \\ + (14)(23)(56) + (16)(25)(34).$$

Предположим, что все соотношения эквивалентности ($\sim$) между идеалами $\mathfrak{p}_i$ являются следствиями соотношений

$$\mathfrak{p}_1\mathfrak{p}_2 \sim 1, \quad \mathfrak{p}_3\mathfrak{p}_4 \sim 1, \quad \mathfrak{p}_5\mathfrak{p}_6 \sim 1,$$

получаемых из $\mathfrak{p}_1\mathfrak{p}_2 \sim 1$ применением автоморфизмов группы $\mathfrak{G}$. Пусть простому идеалу $\mathfrak{p}_i$ соответствует циклическое поле C_i относительной степени l^m над k. Поле K порождается полями C_1C_2, C_3C_4, C_5C_6. Если представить группу $\mathfrak{G}$ в мономиальной форме, допуская для каждого числа 1, 2, 3, 4, 5, 6 независимо друг от друга умножение на степени $\varepsilon = \exp\left(\frac{1}{l^m}\right)$, то мы увидим, что подстановки $\begin{pmatrix} 1, & 2 \\ \varepsilon\cdot 1, & \varepsilon^{-1}\cdot 2 \end{pmatrix}$, $\begin{pmatrix} 3, & 4 \\ \varepsilon\cdot 3, & \varepsilon^{-1}\cdot 4 \end{pmatrix}$, $\begin{pmatrix} 5, & 6 \\ \varepsilon\cdot 5, & \varepsilon^{-1}\cdot 6 \end{pmatrix}$ не меняют полей C_1C_2, C_3C_4, C_5C_6. Если взять произведения x_1x_2, x_3x_4, x_5x_6 переменных x_1, x_2, x_3, x_4, x_5, x_6 за новые

переменные, то группа $\mathfrak{G}$ будет представлена как мономиальная группа, получающаяся из

$$\mathfrak{G}_3 = E + (12) + (23) + (13) + (123) + (132),$$

если умножить числа 1, 2, 3 независимо друг от друга на степени ε. Таким образом, группа $\mathfrak{G}$ — шольцева.

Пример 2. Сохраняя предположения примера 1, предположим, что кроме соотношений $\mathfrak{p}_1\mathfrak{p}_2 \sim 1$, $\mathfrak{p}_3\mathfrak{p}_4 \sim 1$, $\mathfrak{p}_5\mathfrak{p}_6 \sim 1$ существуют еще соотношения

$$\mathfrak{p}_1\mathfrak{p}_3\mathfrak{p}_5 \sim 1, \quad \mathfrak{p}_2\mathfrak{p}_4\mathfrak{p}_6 \sim 1.$$

Теперь мы должны определить группу, не изменяющую полей

$$C_1C_2,\ C_3C_4,\ C_5C_6,\ C_1C_3C_5,\ C_2C_4C_6.$$

Если мы положим $A_i = \begin{pmatrix} i \\ \varepsilon i \end{pmatrix}$ и будем искать подстановки этой группы в виде $A_1^{x_1}A_2^{x_2}A_3^{x_3}A_4^{x_4}A_5^{x_5}A_6^{x_6}$, то получим для x_i следующие сравнения:

$$x_1 + x_2 \equiv 0, \quad x_3 + x_4 \equiv 0, \quad x_5 + x_6 \equiv 0, \quad x_1 + x_3 + x_5 \equiv 0,$$
$$x_2 + x_4 + x_6 \equiv 0 \pmod{l^m}.$$

При этом, если $(l, 3) = 1$, то решение соответствует следующим независимым подстановкам:

$$A_1A_2^{-1}A_3^{-1}A_4, \quad A_1A_2^{-1}A_5^{-1}A_6.$$

Искомая группа есть факторгруппа полной мономиальной группы относительно группы, порожденной этими подстановками.

Если же $l = 3$, $m = 1$, то мы получаем

$$A_1A_2^{-1}A_3^{-1}A_4, \quad A_1A_2^{-1}A_5^{-1}A_6, \quad A_1A_2A_3A_4^{-1}A_5^{-1}A_6^{-1}.$$

Пример 3. k является циклическим кубическим полем. $\mathfrak{f} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}_3$ где $\mathfrak{p}_1$ и $\mathfrak{q}_3$ — простые идеалы первой степени с различными нормами

$$p = N(\mathfrak{p}_1) = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3, \quad q = N(\mathfrak{q}_1) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3.$$

Согласно определению ведущего идеала, имеем

$$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}_3 \sim 1, \ \mathfrak{p}_2\mathfrak{p}_3\mathfrak{q}_1 \sim 1, \ \mathfrak{p}_3\mathfrak{p}_1\mathfrak{q}_2 \sim 1.$$

Пусть C_i — поле (над z) с ведущим идеалом $\mathfrak{p}_i$, D_i — поле с ведущим идеалом $\mathfrak{q}_i$. Поля C_i (или соотв. D_i) являются сопряженными друг с другом и порождают совместно по одному абсолютно нормальному полю. Введем теперь обозначения: $A_i = \begin{pmatrix} i \\ \varepsilon i \end{pmatrix}$ для первого $B_i = \begin{pmatrix} i \\ \varepsilon i \end{pmatrix}$ для второго из этих абсолютно нормальных полей. Следует различать три случая:

А. p и q примарные по модулю l^m числа. Ищем подстановки вида $A_1^{x_1}A_2^{x_2}A_3^{x_3}B_1^{y_1}B_2^{y_2}B_3^{y_3}$, оставляющие инвариантными поля

$$C_1C_2D_3,\ C_2C_3D_1,\ C_3C_1D_2,\ C_1C_2C_3,\ D_1D_2D_3.$$

Для показателей получаются следующие сравнения:

$$x_1 + x_2 + y_3 \equiv 0, \quad x_2 + x_3 + y_1 \equiv 0, \quad x_3 + x_1 + y_3 \equiv 0,$$
$$x_1 + x_2 + x_3 \equiv 0, \quad y_1 + y_2 + y_3 \equiv 0, \pmod{l^m},$$

которые эквивалентны таким:

$$x_1 \equiv y_1, \; x_2 \equiv y_2, \; x_3 \equiv y_3, \; x_1 + x_2 + x_3 \equiv 0 \pmod{l^m}.$$

Производящими подстановками искомой группы являются:

$$A_1 B_1 A_3^{-1} B_3^{-1}, \quad A_2 B_2 A_3^{-1} B_3^{-1}. \tag{2.7}$$

Группа Галуа поля K есть факторгруппа произведения обеих полных мономиальных групп относительно группы (2.7).

B. Из чисел p и q только одно, например p, примарное. Налицо имеются только следующие производящие поля:

$$C_1 C_2 D_3, \; C_2 C_3 D_1, \; C_3 C_1 D_2, \; C_1 C_2 C_3. \tag{3.7}$$

Соотношения между показателями x_i, y_i таковы:

$$x_1 + x_2 + y_3 \equiv 0, \quad x_2 + x_3 + y_1 \equiv 0, \quad x_3 + x_1 + y_2 \equiv 0,$$
$$x_1 + x_2 + x_3 \equiv 0 \pmod{l^m}.$$

Так же, как и в случае A, они эквивалентны следующим:

$$x_1 \equiv y_1, \; x_2 \equiv y_2, \; x_3 \equiv y_3, \; x_1 + x_2 + x_3 \equiv 0 \pmod{l^m}.$$

Совпадение этого случая со случаем A показывает, что он невозможен. В самом деле: из существования полей (3.7), относительные дискриминанты которых над k состоят только из множителей $\mathfrak{p}_i$, $\mathfrak{q}_i$, следует существование поля $D_1 D_2 D_3$ того же вида.

C. Ни p ни q не являются примарными по модулю l^m. Производящие поля́ по́ля K суть

$$C_1 C_2 D_3, \; C_2 C_3 D_1, \; C_3 C_1 D_2.$$

Соотношения между показателями x_i, y_i следующие:

$$x_1 + x_2 + y_3 \equiv 0, \; x_2 + x_3 + y_1 \equiv 0, \; x_3 + x_1 + y_2 \equiv 0 \pmod{l^m}.$$

Производящими подстановками группы, к которой принадлежит поле K внутри $\overline{K}$, являются подстановки

$$A_1 B_2^{-1} B_3^{-1}, \; A_2 B_3^{-1} B_1^{-1}, \; A_3 B_1^{-1} B_2^{-1}.$$

3. Теперь допустим, что среди простых идеальных множителей ведущего идеала $\mathfrak{f}$ встречаются также простые идеалы более высоких степеней. Пусть $\mathfrak{f}$ один из этих простых идеалов. Тогда мы поступаем подобно тому, как в пункте 1: мы присоединяем к основному полю k его абсолютное поле классов $\overline{k}$. Затем рассмотрим поле $C_1 = \overline{k}\left(\sqrt[l^m]{\mathfrak{p}}\right)$

и его норму C. Группа Галуа поля C (в смысле п. 1) не является диспозиционной группой, но более общей шольцевой группой.

Вид нормализаторов определяется следующим образом: сначала следует определить группу разложения идеала $\mathfrak{p}$ в C_1. При этом следует учитывать, что $\mathfrak{p}$ даже в $\bar{k}$ не может быть простым идеалом. Для случая составного идеала Оре [12] определил *общую группу разложения* как совокупность подстановок, оставляющих этот идеал инвариантным. Теперь заметим, что группа разложения $\mathfrak{Z}$ содержит группу $\mathfrak{R}$ (см. п. 1) как подгруппу, так как $\mathfrak{p}$ является идеалом поля k, принадлежащего к группе $\mathfrak{R}$. Мы разлагаем $\mathfrak{Z}$ по $\mathfrak{R}$

$$\mathfrak{Z} = \mathfrak{R} + \mathfrak{R}U_2 + \ldots + \mathfrak{R}U_n$$

и преобразуем $\hat{\mathfrak{h}}$ (т. е. относительную группу поля C/k) посредством представителей $U_1 = E, U_2, \ldots, U_n$ группы $\mathfrak{Z}$. При этом мы не считаем различными поля, отличающиеся друг от друга в смысле композиции только неразветвленными полями (т. е. имеющие равные относительные дискриминанты). Таким образом, мы можем определить наименьший показатель d, для которого S^d перестановочна с подстановками из $\hat{\mathfrak{h}}$ (ср. § 6. 6).

Труднее в этом случае определить число a ($Z^f = T^a$). Мы можем ожидать, что общие группы разложения и инерции имеют более сложную структуру; кроме того, можно пренебречь неразветвленными «множителями поля» только в том случае, если речь идет лишь о структуре корпусгрупп. Но числа a никоим образом не определяются структурой корпусгрупп.

Получено
17 августа 1931 г.

ЛИТЕРАТУРА

1. E. Artin. Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Hamb. Sem. **5** (1927), стр. 353 — 363.
2. A. Chatelet, Les groupes abeliens finis et les modules des points entiers. Paris—Lille, 1925.
3. Ph. Furtwängler. Über die Reziprozitätsgesetze für ungerade Primzahlpotenzexponenten. Crelle **157** (1927), стр. 15 — 25.
4. Ph. Furtwängler. Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper. Abh. Hamb. Sem. **7** (1929), стр. 14 — 36.
5. H. Hasse. Zwei Existenztheoreme über algebraische Zahlkörper. Math. Ann. **95** (1925). стр. 229 — 238.
6. H. Hasse. Ein weiteres Existenztheorem in der Theorie der algebraischen Zahlkörper. Math. Ztschr. **24** (1925), стр. 149 — 160.
7. H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I. Jahresber. DMV **35** (1926), стр. 1 — 55.
8. H. Hasse. Idem, Teil II. Jahresber. DMV Ergänzungsband VI (1930).
9. E. Hecke. Über die L-Funktionen und der Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper. Gött. Nachr., 1917.

10. K. Hensel. Theorie der algebraischen Zahlen. Lpz., 1908.
11. L. Kronecker. Die Composition Abelscher Gleichungen. Sitzungber. Akad. Berlin, 1882, стр. 1059 — 1064.
11a. W. Krull. Theorie und Anwendung der verallgemeinerten Abelschen Gruppen. Sitzber. Heid. Akad., 1926, I. Abh.
12. O. Ore. Some Theorems on the Connection between Ideals and Groups of a Galois Field. Trans. Amer. Math. Soc. **30** (1927), стр. 610 — 620.
13. O. Ore. Abrisz einer arithmetischen Theorie der Galoisschen Körper I. Math. Ann. **100** (1928), стр. 650 — 673.
14. F. Pollaczek. Über die Einheiten relativ-Abelscher Zahlkörper. Math. Ztschr. **30** (1929), стр. 520 — 551.
15. A. Scholz. Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe. Math. Ztschr. **30** (1929), стр. 332 — 356.
16. A. Scholz. Reduktion der Konstruktion von Körpern mit zweistufiger (metabelscher) Gruppe. Sitzber. Heid. Akad., 1929, 14. Abh.
17. A. Scholz. Ein Beitrag zur Theorie der Zusammensetzung endlicher Gruppen. Math. Ztschr. **32** (1930), стр. 187 — 189.
18. A. Scholz. Zwei Bemerkungen zum Klassenkörperturm. Crelle **161** (1929), стр. 201 — 207.
19. A. Scholz. Über das Verhältnis von Idealklassen und Einheitsgruppe in Abelschen Körpern vom Primzahlpotenzgrad. Sitzber. Heid. Akad, 1930, 3. Abh.
19a. O. Schreier. Über die Erweiterung von Gruppen II. Abh., Hamb. Sem. **4** (1926), стр. 321 — 346.
20. I. Schur. Neue Begründung der Theorie der Gruppencharaktere, Sitzber. Akad. Berlin, 1905, стр. 406 — 432.
21. A. Speiser. Die Zerlegungsgruppe. Crelle **149** (1920), стр. 174 — 188.
22. A. Speiser. Die Theorie der Gruppen von endlicher Ordnung. «Grundlehren», V, Berlin, 1923.
23. T. Takagi. Über eine Theorie des relativ Abel'schen Zahlkörpers. Journ. Coll. Sc. Imp. Univ. Tokyo **41** (1920), Art. 9.
24. T. Takagi. Über das Reziprozitatsgesetz in einem beliebigen algebraischen Zahlkörper. Journ. Coll. Sc. Imp. Univ. Tokyo **44** (1922), Art. 5.
25. N. Tschebotarөw. Zur Gruppentheorie des Klassenkörpers. Crelle **161** (1929), стр. 179 — 193; Собр. соч., т. I, стр. 121 — 140.

ОБ ОДНОМ ОБОБЩЕНИИ ТЕОРЕМЫ КЛИФФОРДА

(UBER EINE VERALLGEMEINERUNG EINES CLIFFORDSCHEN SATZ ES)

(Rendiconti Circ. Mat. di Palermo 55 (1931), стр. 1—11)

Пусть даны поле $\mathfrak{R}$ алгебраических функций одного переменного и соответствующая абсолютная риманова поверхность [1, 2]. Если мы выберем на этой поверхности неограниченную систему точек $P_1, P_2, \ldots P_n \ldots$, то нетеровская „теорема о пробелах“ [3] говорит, что среди систем

$$\begin{array}{l} P_1; \\ P_1, P_2; \\ P_1, P_2, P_3; \\ \ldots\ldots \end{array} \tag{1}$$

найдется ровно p таких, которые не являются системами полюсов какой-либо функции из $\mathfrak{R}$ (пробелы).

Здесь p обозначает жанр поля $\mathfrak{R}$. В случае, когда все точки P_i совпадают, можно высказать некоторые определенные утверждения относительно расположения пробелов в последовательности (1). Для этого употребляется принцип аддитивных модулей [4].

В общем случае, как кажется, до сих пор не известно ни одного правила, по которому можно было бы судить, является ли заданное распределение пробелов в последовательности (1) возможным. Одно из необходимых для этого условий вытекает из известной теоремы Клиффорда [5], говорящей, что между k первыми системами последовательности (1) ($k \leqslant 2p-1$) найдется не менее $\left[\frac{k+1}{2}\right]$ пробелов, причем если число пробелов равно $\left[\frac{k+1}{2}\right]$, то либо $p \leqslant \left[\frac{k+1}{2}\right] + 1$, либо поле $\mathfrak{R}$ гиперэллиптическое.

Настоящая работа имеет целью исследовать, возможно ли дать оценку для жанра поля $\mathfrak{R}$, если в $\mathfrak{R}$ дан класс дивизоров, порядок и измерение которого известны. Я пользуюсь здесь символикой арифметической теории алгебраических функций [1, 2, 4, 6]. Результат гласит: если поле алгебраических функций $\mathfrak{R}$ содержит «специальный» класс дивизоров измерения n и порядка $m = 2n + r - 2$ и если $2n - r - 4 > 0$, то для жанра p поля $\mathfrak{R}$ имеет место неравенство

$$p \leqslant n + 2r + \left[\frac{2r(r+1)}{2n-r-4}\right], \tag{2}$$

причем исключается случай гиперэллиптического поля $\mathfrak{R}$.

При $r = 0$ отсюда получается теорема Клиффорда.

§ 1

Сначала мы докажем, что если класс дивизоров A ([4], стр. 250)— специальный (т. е. является делителем класса дифференциалов W), то его порядок m и измерение n связаны неравенством $m \geqslant 2n-2$.

Допустим обратное. Пусть A — специальный класс измерения $\{A\}=n$ и порядка $m<2n-2$. Выберем $n-1$ произвольных точек (простых дивизоров) $P_1, P_2, \ldots, P_{n-1}$ и найдем в классе A дивизоры $\mathfrak{A}$, делящиеся на дивизор $P_1 \cdot P_2 \cdot \ldots, P_{n-1}$. Покажем, что $P_1, P_2, \ldots, P_{n-1}$ всегда могут быть выбраны так, чтобы существовал только один дивизор требуемого рода.

Лемма 1. *В классе A можно найти такой дивизор $\mathfrak{A}=P_1 \cdot P_2 \cdots P_m$, что всякий из классов $(P_{\alpha_1} \cdot P_{\alpha_2} \cdots P_{\alpha_{m-n-1}})$, где $\alpha_1, \alpha_2, \ldots, \alpha_{m-n+1}$ — одна из комбинаций $m-n+1$ различных чисел ряда $1, 2, \ldots, m$, имеет измерение* 1.

Доказательство. В силу наших предположений относительно A, $\left\{\frac{W}{A}\right\}>0$ и теорема Римана—Роха ([4], стр. 304, формула 11) дает

$$\left\{\frac{W}{A}\right\}=\{A\}+p-1-m, \tag{3}$$

$$m-n+1<p. \tag{4}$$

С другой стороны, условие для того, чтобы измерение $(P_1 \cdot P_2 \cdots P_{m-n+1})$ превышало 1, состоит в существовании постоянных $c_1, c_2, \ldots, c_{m-n+1}$, удовлетворяющих условиям

$$\begin{aligned} &c_1 \Omega_1(P_1)+c_2 \Omega_1(P_2)+\cdots+c_{m-n+1} \Omega_1(P_{m-n+1})=0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &c_1 \Omega_p(P_1)+c_2 \Omega_p(P_2)+\cdots+c_{m-n+1} \Omega_p(P_{m-n+1})=0, \end{aligned} \tag{5}$$

где

$$\Omega_1(P), \Omega_2(P), \ldots, \Omega_p(P)$$

— полная система подинтегральных функций интегралов первого рода ([2], стр. 27). Иными словами, ранг матрицы

$$\left\| \begin{array}{c} \Omega_1(P_1), \Omega_1(P_2), \ldots, \Omega_1(P_{m-n+1}) \\ \Omega_2(P_1), \Omega_2(P_2), \ldots, \Omega_2(P_{m-n+1}) \\ \cdots\cdots\cdots\cdots\cdots \\ \Omega_p(P_1), \Omega_p(P_2), \ldots, \Omega_p(P_{m-n+1}) \end{array} \right\| \tag{6}$$

должен быть менее $m-n+1$. Неравенство (4) позволяет нам предполагать, что возможно выбрать $P_1, P_2, \ldots, P_{m-n+1}$ так, что это условие не будет удовлетворяться. Заметим еще, что $m-n+1 \leqslant n-1$ и потому точки $P_1, P_2, \ldots, P_{m-n+1}$ можно рассматривать как независимые. Для доказательства леммы закрепим точки $P_2, P_3, \ldots, P_{m-n+1}$ и будем перемещать точку P_1 вокруг ее начального положения. Если

при этом ранг матрицы (6) постоянно остается меньше $m-n+1$, то то же будет иметь место для матрицы

$$\left\| \begin{matrix} \Omega_1(P_1), \Omega_1'(P_1), \ldots, \Omega_1^{(q)}(P_1), \\ \cdots\cdots\cdots\cdots \\ \Omega_p(P_1), \Omega_p'(P_1), \ldots, \Omega_p^{(q)}(P_1) \end{matrix} \right\|, \tag{7}$$

где $\Omega^{(q)}(P)$ есть q-тая производная от $\Omega(P)$ и q — сколько угодно большое целое число. Но тогда точка P_1 должна быть «точкой Вейерштрасса» сколь угодно высокого порядка, что невозможно, так как сумма порядков всех точек Вейерштрасса равна $(p-1)p(p+1)$ ([2], стр. 34—40; [4], стр. 496).

Обозначим через $Q^{(i)}$ $(i=1, 2, \ldots, r)$ все дивизоры типа

$$P_1^{(i)} \cdot P_2^{(i)} \ldots P_{m-n+1}^{(i)}, \tag{8}$$

где $P_1^{(i)}, P_2^{(i)}, \ldots, P_{m-n+1}^{(i)}$ — одна из

$$r = \frac{m!}{(n-1)!\,(m-n+1)!} \tag{9}$$

комбинаций из ряда $P_1, P_2, \ldots, P_m$. Предположим, что дивизор $Q^{(1)}$ выбран так, что $\{Q^{(1)}\}=1$. Тогда все главные миноры матрицы (6) не могут обращаться в нули. Пусть $D^{(1)}$ — главный минор, причем

$$|D^{(1)}| = K > 0.$$

Рассмотрим другой дивизор $Q^{(2)}$. Если $\{Q^{(2)}\}=1$, то переходим к рассмотрению следующего дивизора $Q^{(3)}$. Если же, напротив, $\{Q^{(2)}\}>1$, то присоединим к $Q^{(2)}$ еще $(n-1)-(m-n+1)=2n-m-2>0$ точек из $P_1, P_2, \ldots, P_m$ и фиксируем их. Далее, фиксируем все точки из $Q^{(2)}$, за исключением одной, например $P_1^{(2)}$, и будем изменять ее так, чтобы получить $\{Q^{(2)}\}=1$. При этом нефиксированные точки претерпевают некоторые изменения. Покажем, что смещение $P_1^{(2)}$ может быть выбрано настолько малым, что $\{Q^{(1)}\}$ остается равным 1. Для этого заметим следующее. Уравнение $\{Q^{(1)}\}=1$ говорит, что каждая точка $Q^{(1)}$ вполне определена заданием *дополнительного дивизора*, т. е. всех остальных точек $\mathfrak{A}$. Чтобы действительно найти ее, достаточно определить все нули алгебраической функции

$$\lambda_1 + \lambda_2 \frac{\mathfrak{A}_2}{\mathfrak{A}_1} + \ldots + \lambda_{m-1} \frac{\mathfrak{A}_{m-1}}{\mathfrak{A}_1} + \frac{\mathfrak{A}_m}{\mathfrak{A}_1}, \tag{10}$$

где $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_m$ — некоторая система независимых дивизоров класса A и $\mathfrak{A}_1$ взаимно просто с $\frac{\mathfrak{A}}{Q^{(1)}}$. Константы $\lambda_1, \lambda_2, \ldots, \lambda_{m-1}$ нужно выбрать так, чтобы функция (10) обращалась в нуль во всех точках дополнительного дивизора $\frac{\mathfrak{A}}{Q^{(1)}}$. Поскольку описанный процесс — алгебраический, мы заключаем, что точки $Q^{(1)}$ непрерывно зависят от точек дополнительного дивизора.

Теперь подчиним точки дивизора $Q^{(1)}$ условию $\{Q^{(1)}\}=1$ и рассмотрим дополнительный дивизор $R^{(1)}$ порядка $n-1$. Выберем в $R^{(1)}$ некоторую точку и будем перемещать ее, закрепив остальные точки $R^{(1)}$. Вследствие $\{Q^{(1)}\}=1$ все точки $Q^{(1)}$ непрерывно зависят от точек $R^{(1)}$ и потому выбранную точку можно сместить настолько мало, чтобы определитель $D^{(1)}$ не исчезал (для этого достаточно выбрать смещение так, чтобы было $|D^{(1)\prime}-D^{(1)}|<\frac{K}{2}$). Смещением этим распорядимся так, чтобы получить $\{Q^{(2)}\}=1$, где $Q^{(2)}$ — некоторый дивизор $(m-n+1)$-го порядка, содержащийся в $R^{(1)}$. Рассматривая соответствующий $Q^{(2)}$ неисчезающий определитель $D^{(2)}$ и повторяя проведенное рассуждение, придем к некоторому дивизору $R^{(1)}$, поддивизоры $(m-n+1)$-го порядка которого все имеют измерение 1. Переходя затем к новым и новым дивизорам типа $R^{(1)}$, получим, наконец, некоторый дивизор $\mathfrak{A}$ класса A, поддивизоры которого порядка $m-n+1$ будут все измерения 1, что и т. д.

Теперь поставим вопрос о существовании в поле $\mathfrak{R}$ функций, обладающих следующими полюсами:

$$\begin{aligned}
&1)\ P_1;\\
&2)\ P_2 \text{ и, может быть, } P_1;\\
&3)\ P_3 \text{ и, может быть, } P_1,\ P_2;\\
&\quad\ldots\ldots\ldots\ldots\ldots\\
&m)\ P_m \text{ и, может быть, } P_1, P_2, \ldots, P_{m-1};\\
&m+1)\ P_1^2 \text{ и, может быть, } P_2, P_3, \ldots, P_m;\\
&m+2)\ P_2^2 \text{ и, может быть, } P_1, P_2, P_3, \ldots, P_m
\end{aligned} \tag{11}$$

и т. д. до бесконечности.

Теорема Нетера гласит, что в этой бесконечной таблице найдется ровно p систем точек, для которых соответствующие функции не существуют (пробелы). Это число пробелов мы вычислим еще другим образом.

Согласно лемме 1: $\{Q^{(1)}\}=1$, $\{Q^{(1)}R^{(1)}\}=n$, так что разность между порядком и измерением обоих классов одинакова $(=m-n)$. Если ввести обозначения

$$Q^{(1)}=P_1\cdot P_2\cdots P_{m-n+1};\qquad R^{(1)}=P_{m-n+2}\cdots P_m,$$

то получим, что

$$\{Q^{(1)}\}=1,\{Q^{(1)}P_{m-n+2}\}=2,\{Q^{(1)}P_{m-n+2}P_{m-n+3}\}=3,\ldots,\{Q^{(1)}R^{(1)}\}=n.$$

Отсюда же следует, что в таблице (11) $m-n+1$ первых систем дают пробелы, а последующие $n-1$ не дают их. Докажем, что в таблице (11) вообще не существует пробелов. Для этого возьмем класс $(Q^{(1)}P_{m-n+2})$, измерение которого равно 2 и все точки которого собственные, так как, по лемме 1, все подклассы его имеют измерение 1. Точно так же будут собственными все точки классов

$(P_{m-n+3}, \ldots, P_m, P_1, \ldots, P_r)$ $(r = 1, 2, \ldots, m-n+2)$, так как в противном случае один из их подклассов порядка $m-n+1$ имел бы измерение $\geqslant 2$, что исключено в силу леммы 1. Но тогда после прохождения $P_1, P_2, \ldots, P_{m-n+2}$ в ряде $P_1, P_2, \ldots, P_m / P_1, P_2, \ldots, P_{m-n+2}$ уже не может встретиться новых пробелов. В самом деле, существуют функции с собственными полюсами $P_1, P_2, \ldots, P_{m-n+2}$, а равным образом и с собственными полюсами $P_{m-n+3}, \ldots, P_m, P_1, P_2, \ldots, P_r$ $(r = 1, 2, \ldots, m-n+2)$. Произведение их дает функцию с собственными полюсами $P_1, P_2, \ldots, P_m$; $P_1, \ldots, P_r$, т. е. $(m+r)$-тое место $(r = 1, 2, \ldots, m-n+2)$ таблицы (11) не дает пробела.

Далее, чтобы убедиться, что точки $P_1, P_2, \ldots, P_r$ ряда $P_1, \ldots, P_m / P_1, \ldots, P_r$ не дают пробелов, рассмотрим классы $(P_1 . P_2 \ldots P_m)$ и $(P_1 . P_2 \ldots P_r)$. Процесс этот можно продолжить без конца, откуда следует, что только первые $m-n+1$ систем таблицы (11) дают пробелы.

Отсюда, на основании нетеровской теоремы о пробелах, заключаем, что

$$m-n+1 = p.$$

Тогда из теоремы Римана—Роха следует, что

$$\left\{\frac{W}{A}\right\} = 0,$$

т. е. класс A не специальный, что и т. д.

§ 2

Теперь допустим, что

$$m = 2n-2+r \text{ и } r \geqslant 0.$$

Сделаем еще одно предположение.

Предположение. Пусть $Q \cdot P_1 \cdot P_2 \cdots P_n$ — дивизор класса A, причем $\{Q\} = 1$, $\{QP_1\} = 1$ (такой дивизор всегда можно построить). Если выбрать $r+2$ произвольных точки $P_1', P_2', \ldots, P_{r+2}'$ из QP_1, то среди точек $P_2, P_3, \ldots, P_n$ можно найти такую точку P_i, что в классе (QP_1P_i) $(\{QP_1P_i\} = 2)$ все точки $P_1', P_2', \ldots, P'_{r+2}$ будут собственными [т. е. не будут являться общими делителями всех дивизоров из (QP_1P_i)]. В § 3 мы увидим, в каких случаях это предположение несправедливо.

Вышеупомянутую точку P_i обозначим через P_2 и рассмотрим ряды точек

$$P_{n+1}, P_{n+2}, \ldots, P_m;\ P_1, P_2, \ldots, P_n / P_{n+1}, \ldots, P_m;\ P_1, \ldots, P_n/, \ldots \qquad (12)$$

Пробегая точки $P_{n+1}, P_{n+2}, \ldots, P_m, P_1$, мы получим $m-n+1$ пробелов; при прохождении же следующих точек $P_2, P_3, \ldots, P_n$ новых пробелов не получится, так как

$$\{QP_1\} = 1, \{QP_1P_2\} = 2, \ldots, \{QP_1P_2 \cdots P_n\} = n.$$

Присоединим сюда еще $r+2$ точки $P_{n+1}=P_1', P_{n+2}=P_2', \ldots, P_{n+r+2}=P'_{r+2}$. Класс $(P_3\cdots P_n\cdot P_1'\ldots P'_{r+2})$ не может иметь измерение 1, так как порядок его равен $n-2+(r+2)=n+r=m-n+2$. Пусть же P_i' — первая точка, для которой $\{P_3\cdots P_n\cdot P_1'\cdots P_i'\}=2$; тогда присоединение ее к ряду $P_{n+1}, \ldots, P_m; P_1, \ldots, P_n; P_1', \ldots, P'_{i-1}$ не дает пробела. Для доказательства этого достаточно показать существование функции, имеющей полюсами $P_{n+1}, \ldots, P_m; P_1, \ldots, P_n; P_1', \ldots, P_i'$, среди которых P_i' должен быть полюсом второго порядка. Но в силу нашего «предположения» P_i' — собственная точка для класса $(P_{n+1}\cdots P_m\cdot P_1\cdot P_2)$, т. е. существует функция, имеющая полюсами точки $P_{n+1}, \ldots, P_m, P_1, P_2$, причем P_i' действительно является ее полюсом. С другой стороны, вследствие

$$\{P_3\cdots P_n\cdot P_1'\cdots P_i'\}=2, \qquad \{P_3\cdots P_n\cdot P_1'\cdots P'_{i-1}\}=1$$

то же имеет место и для класса $(P_3\cdots P_n\cdot P_1'\cdots P_i')$. Произведение соответствующих функций обладает требуемым свойством.

Таким образом, доказано, что при прохождении точек $P_{n+1}, \ldots, P_m$ ряда $P_{n+1}, \ldots, P_m; P_1, \ldots, P_n/P_{n+1}, \ldots, P_m$ первый «не-пробел» встретится не далее, как на $r+2$-ом месте. Если P_{n+r_1} — этот первый «не-пробел», то вычеркнем точку P_{n+r_1} из ряда $P_{n+1}, \ldots, P_m$ и рассуждаем, как выше. Первый «не-пробел» нового ряда встретится опять не далее как на $r+2$-ом месте. Исчерпав таким образом все точки ряда $P_{n+1}, \ldots, P_m$, мы увидим, что при прохождении точек $P_{n+1}, \ldots, P_m$ ряда $P_{n+1}, \ldots, P_m; P_1, \ldots, P_n/P_{n+1}, \ldots, P_m$ встретится не более $r+1$ пробелов.

Во второй половине второго периода (т. е. при прохождении точек $P_1, P_2, \ldots, P_n$ ряда $P_{n+1}, \ldots, P_m; P_1, \ldots, P_n/P_{n+1}, \ldots, P_n; P_1, \ldots, P_n$) мы не получим ни одного пробела. Это следует из существования функции, для которой точки $P_{n+1}, \ldots, P_m; P_1, \ldots, P_n$ действительно представляют полюсы (мы предполагаем, что класс A — ***примитивный***, т. е. не обладает несобственными точками). Таким же образом мы получаем, что в каждом последующем периоде, и именно в первой его половине, содержится самое большое $r+1$ пробелов.

Выберем наибольшее целое рациональное число k, удовлетворяющее неравенству

$$km+(r+1)\leqslant 2p-1, \tag{13}$$

т. е.

$$k=\left[\frac{2p-r-2}{m}\right]. \tag{14}$$

При прохождении $km+(r+1)$ точек мы получим самое большее $(m-n+1)+(r+1)k$ пробелов, как было показано выше. Но последнее место, на котором могут встретиться пробелы, есть $(2p-1)$-ое ([2], стр. 33). Отсюда, на основании (14), мы заключаем, что после $km+(r+1)$ первых точек ряда (12) уже не может встретиться

пробелов, а так как общее число пробелов, в силу теоремы Нетера, равно p, то мы получаем следующее неравенство:

$$(m-n+1)+(r+1)\geqslant p. \tag{15}$$

Из уравнения (14) следует

$$k\leqslant \frac{2p-r-2}{m}. \tag{16}$$

Подставляя это выражение в (15), получаем

$$m-n+1+\frac{2p-r-2}{m}(r+1)\geqslant p, \tag{17}$$

или, вследствие равенства $m=2n+r-2$,

$$(2n-r-4)p\leqslant (n+r-1)(2n+r-2)-(r+1)(r+2). \tag{18}$$

Мы предположим, что

$$2n-r-4>0, \tag{19}$$

иначе наш метод не даст никакой верхней оценки для p. Теперь из (18) следует

$$p\leqslant n+2r+\left[\frac{2r(r+1)}{2n-r-4}\right]. \tag{20}$$

Это и есть искомая оценка для p.

Полагая $r=0$, получим

$$p\leqslant n. \tag{21}$$

Отсюда следует, что $m\geqslant 2p-2$. Если A — специальный класс, то здесь должен иметь место знак равенства, т. е. A должен совпадать с классом дифференциалов W. Это дополнение к теореме Клиффорда было сделано Бертини [7].

§ 3

Перейдем теперь к вопросу о том, когда не выполняется сделанное выше «предположение». Это означает следующее: если $P_1', P_2', \ldots, P'_{r+2}$ — определенные точки дивизора QP_1, то система всех точек $P_2, \ldots, P_n$ распадается в $r+2$ таких систем, что когда P_i входит в систему с номером α ($\alpha=1, 2, \ldots, r+2$), то P_α' является несобственной точкой для класса (QP_1P_i), т. е.

$$\left\{\frac{QP_1}{P_\alpha'}P_i\right\}=2.$$

Таким образом, если система с номером α содержит k_α точек $P_1^{(\alpha)}, P_2^{(\alpha)}, \ldots, P_{k_\alpha}^{(\alpha)}$, где $\alpha=1, 2, \ldots, r+2$ и $\sum\limits_\alpha k_\alpha=n-1$, и если ввести обозначение

$$S^{(\alpha)}=P_1^{(\alpha)}\cdot P_2^{(\alpha)}\cdots P_{k_\alpha}^{(\alpha)} \qquad (\alpha=1, 2, \ldots, r+2),$$

то класс

$$\left(\frac{QP_1}{P_\alpha'} S^{(\alpha)}\right)$$

имеет измерение $k_\alpha + 1$. Для доказательства обозначим через $R_i^{(\alpha)}$ один из дивизоров класса

$$\left(\frac{QP_1}{P_\alpha'} P_i^{(\alpha)}\right) \qquad (\alpha = 1, 2, \ldots, r+2;\ i = 1, 2, \ldots, k_\alpha + 1).$$

Дивизор этот можно считать взаимно простым с $P_i^{(\alpha)}$, так как, вследствие $\{QP_1\} = 1$, точка $P_i^{(\alpha)}$ есть собственная точка для класса $\left(\frac{QP_1}{P_\alpha'} P_i^{(\alpha)}\right)$. Тогда класс

$$\left(\frac{QP_1}{P_\alpha'} S^{(\alpha)}\right)$$

содержит следующие дивизоры:

$$\frac{QP_1}{P_\alpha'},\ R_1^{(\alpha)} \frac{S^{(\alpha)}}{P_1^{(\alpha)}},\ R_2^{(\alpha)} \frac{S^{(\alpha)}}{P_2^{(\alpha)}}, \ldots, R_{k_\alpha}^{(\alpha)} \frac{S^{(\alpha)}}{P_{k_\alpha}^{(\alpha)}}.$$

Дивизоры эти линейно независимы, ибо из соотношения

$$c_0 \frac{QP_1}{P_\alpha'} + c_1 R_1^{(\alpha)} \frac{S^{(\alpha)}}{P_1^{(\alpha)}} + \cdots + c_{k_\alpha} R_{k_\alpha}^{(\alpha)} \frac{S^{(\alpha)}}{P_{k_\alpha}} = 0$$

следует $c_i = 0$ $(i = 1, 2, \ldots, k_\alpha)$, так как все входящие в него дивизоры делятся на $P_i^{(\alpha)}$, за исключением $R_i^{(\alpha)} \frac{S^{(\alpha)}}{P_i^{(\alpha)}}$. Таким образом,

$$\left\{\frac{QP_1}{P_\alpha'} S^{(\alpha)}\right\} \geqslant k_\alpha + 1.$$

Но так как порядки классов $\left(\frac{QP_1}{P_\alpha'} S^{(\alpha)}\right)$ и $\left(\frac{QP_1}{P_\alpha'} P_i^{(\alpha)}\right)$ разнятся только на $k_\alpha - 1$ ([6], стр. 675—676, Satz 5), то в этом соотношении возможен лишь знак равенства.

Из формул $\left\{\frac{QP_1}{P_\alpha'} S^{(\alpha)}\right\} = k_\alpha + 1$, $\left\{\frac{QP_1}{P_\alpha'}\right\} = 1$ можно заключить, что точки $P_1^{(\alpha)}, P_2^{(\alpha)}, \ldots, P_{k_\alpha}^{(\alpha)}$ вполне определяют дивизор $\frac{QP_1}{P_\alpha'} S^{(\alpha)}$ внутри его класса. Варьируя точки α-ой системы $P_1^{(\alpha)}, P_2^{(\alpha)}, \ldots, P_{k_\alpha}^{(\alpha)}$, притом так, чтобы ни один из рассматриваемых классов измерения 1 не переходил в класс высшего измерения, и закрепив в то же время остальные системы точек, мы увидим, что при этом могут измениться только те точки QP_1, которые остаются неизменными при вариации остальных систем. Иными словами: каждая точка QP_1 как собственная точка может войти только в один класс

$$\left\{\frac{QP_1}{P_\alpha'} S^{(\alpha)}\right\} \qquad (\alpha = 1, 2, \ldots, r+2).$$

Поэтому дивизор QP_1 распадается на $r+2$ дивизора $Q^{(\alpha)}$ порядка l_α ($\alpha = 1, 2, \ldots, r+2$; $\sum l_\alpha = m-n+1$), причем

$$\{Q^{(\alpha)} S^{(\alpha)}\} = k_\alpha + 1 \qquad (\alpha = 1, 2, \ldots, r+2).$$

Вычислим для каждого из этих классов величину $r_\alpha = m_\alpha - 2n_\alpha + 2$. Имеем

$$r_\alpha = (k_\alpha + l_\alpha) - 2(k_\alpha + 1) + 2 = l_\alpha - k_\alpha,$$

$$\sum_\alpha r_\alpha = \sum_\alpha l_\alpha - \sum_\alpha k_\alpha = (m-n+1) - (n-1) = m - 2n + 2 = r.$$

Так как число слагаемых равно $r+2$, то хотя одно из них неположительно. Согласно лемме 1, случай отрицательного r_α невозможен. Если же $r_\alpha = 0$, то «предположение» не может выполняться для класса $(Q^{(\alpha)} S^{(\alpha)})$. Именно, если бы оно выполнялось, то класс $(Q^{(\alpha)} S^{(\alpha)})$ совпадал бы с классом дифференциалов W.[1] Тогда класс A не был бы специальным, что противоречит нашему предположению.

Если «предположение» не выполняется также для класса $(Q^{(\alpha)} S^{(\alpha)})$, то в нем можно найти делитель, для которого $r = 0$. Продолжая таким образом, мы придем, наконец, к классу, порядок которого равен $r + 2 = 2$. Измерение этого класса равно

$$\frac{m - r + 2}{2} = \frac{4}{2} = 2.$$

Это может иметь место только в случае гиперэллиптического поля.

Получено
10 ноября 1929 г.

ЛИТЕРАТУРА

1. Dedekind-Weber. Theorie der alg. Funktionen einer Ver. Journ. f. reine und ang. Math. **92**, 1879, стр. 181—290.
2. H. F. Baker. Abel's Theorem and the allied Theory including the theory of the theta functions. Cambridge, 1897.
3. M. Nöther. Beweis und Erweiterung eines algebraisch-functionen theoretischen Satzes des Herrn Weierstrass. Journ. f. reine und ang. Math. **97**, 1884, стр. 224—229. Ср. также [2], стр. 30—31.
4. K. Hensel u. G. Landsberg. Theorie der alg. Funktionen einer Var. und ihre Anwendung. Leipzig, Teubner, 1902.
5. Clifford. On the Classification of Loci. Phil. Trans. Roy. Soc. of London **169**, 1878, стр. 663—681; Coll. Papers, 329—331; ср. также F. Severi. Vorlesungen über algebraische Geometrie. Leipzig, Teubner, 1921, стр. 131—133.
6. H. Weber. Lehrbuch der Algebra, Bd. 3. Braunschweig, 1908, стр. 623—707.
7. E. Bertini. La geometria delle serie lineari sopra una curva secondo il metodo algebrico. Ann. di Mat., ser. 3. **22**, 1894, стр. 36.

[1] См. выше, § 2, конец.

ДОПОЛНЕНИЕ К СТАТЬЕ «ОБ ОДНОМ ОБОБЩЕНИИ ТЕОРЕМЫ КЛИФФОРДА»

Статья «Об одном обобщении теоремы Клиффорда» содержит некоторые ошибки, замеченные сыном Николая Григорьевича Г. Н. Чеботаревым. Поэтому доказательство было переработано Николаем Григорьевичем. Ниже приводится его редакция, помещенная в монографии «Теория алгебраических функций».

§ 26. Теорема Клиффорда и ее обобщение

Мы уже упоминали, что если дана произвольная последовательность точек

$$P_1,\ P_2,\ P_3,\ \ldots, \tag{1}$$

то мы знаем очень мало о том, на каких местах находятся ее «дефектные» номера. Однако известно, что, идя от начала последовательности, мы будем по порядку номеров чаще встречать дефектные, чем не-дефектные, номера. Это правило, конечно, справедливо до тех пор, пока мы находимся в пределах «специальной» части последовательности.

Формулируем это правило точнее. Рассмотрим последовательность классов

$$(P_1),\ (P_1P_2),\ \ldots,\ (P_1P_2\cdots P_k). \tag{2}$$

Мы знаем, что i есть дефектный номер последовательности (1) тогда и только тогда, если

$$\text{Изм}\ (P_1P_2\cdots P_i) = \text{Изм}\ (P_1P_2\cdots P_{i-1});$$

в противном же случае мы имеем

$$\text{Изм}\ (P_1P_2\cdots P_i) = \text{Изм}\ (P_1P_2\cdots P_{i-1}) + 1.$$

Таким образом, если среди k первых номеров имеется $\varkappa$ дефектных, то, идя вдоль системы классов (2), мы на $\varkappa - 1$ местах не получим роста измерения, так что

$$\text{Изм}\ (P_1P_2\cdots P_k) = k - \varkappa + 1.$$

Теорема Клиффорда состоит в утверждении, что дефектных номеров не меньше, чем не-дефектных:

$$\varkappa \geqslant k - \varkappa. \tag{3}$$

Клиффорд выражал ее, пользуясь числами, выражающими порядок и измерение класса

$$\mathfrak{A} = (P_1P_2\cdots P_k).$$

Эти числа выражаются через k и $\varkappa$ так:

$$\text{Пор}\ \mathfrak{A} = k, \qquad \text{Изм}\ \mathfrak{A} = k - \varkappa + 1,$$

откуда

$$k = \text{Пор}\,\mathfrak{A}, \qquad \varkappa = \text{Пор}\,\mathfrak{A} - \text{Изм}\,\mathfrak{A} + 1.$$

Подставляя в (3), мы получим утверждение Клиффорда в таком виде:

$$2\text{Пор}\,\mathfrak{A} - 2\,\text{Изм}\,\mathfrak{A} + 2 \geqslant \text{Пор}\,\mathfrak{A},$$

т. е.

$$\text{Пор}\,\mathfrak{A} \geqslant 2\,\text{Изм}\,\mathfrak{A} - 2. \tag{4}$$

Но Клиффорд доказал больше: он установил, что в соотношении 4) знак равенства может иметь место только в конце специальной части последовательности (2), т. е. только в том случае, когда

$$\mathfrak{A} = \mathfrak{W}, \qquad \text{Изм}\,\mathfrak{A} = \rho, \qquad \text{Пор}\,\mathfrak{A} = 2\rho - 2.$$

Другими словами, если мы имеем специальный класс $\mathfrak{A}$, у которого порядок и измерение связаны соотношением

$$\text{Пор}\,\mathfrak{A} = 2\,\text{Изм}\,\mathfrak{A} - 2, \tag{5}$$

то $\mathfrak{A}$ есть класс дифференциалов $\mathfrak{W}$, откуда

$$\rho = \text{Изм}\,\mathfrak{A}.$$

Утверждение Клиффорда дает возможность получить верхнюю границу для жанра ρ поля $k(x, y)$, если в нем известен класс $\mathfrak{A}$ дивизоров, удовлетворяющий соотношению (5). При этом не требуется, чтобы класс был специальным: в самом деле, если класс $\mathfrak{A}$ не-специален, то ограничение для жанра вытекает сразу из теоремы Римана — Роха

$$\rho = \text{Пор}\,\mathfrak{A} - \text{Изм}\,\mathfrak{A} + 1; \tag{6}$$

при существовании соотношения (5) это приводит к значению

$$\rho = \text{Изм}\,\mathfrak{A} - 1.$$

Второе утверждение Клиффорда допускает исключение: если $k(x, y)$ есть гиперэллиптическое поле, причем

$$\text{Изм}\,(P_1 P_2) = 2,$$

то, беря в роли (1) такую последовательность:

$$P_1, P_2;\ P_1, P_2;\ P_1, P_2; \ldots,$$

мы получим следующие значения для измерений построенных с ее помощью классов (2):

$$1,2;\ 2,3;\ 3,4; \ldots,$$

так что равенство (5) будет выполняться на каждом четном месте. В дальнейшем мы увидим, что это исключение теоремы Клиффорда единственное, и во всех остальных случаях теорема Клиффорда справедлива.

Теорему Клиффорда можно обобщить, задавшись следующей проблемой. Даны измерение и порядок некоторого класса $\mathfrak{A}$ в поле $k(x, y)$. В каком случае мы можем определить жанр поля $k(x, y)$ или, по крайней мере, указать для него верхнюю границу?

Если класс $\mathfrak{A}$ не-специален, то жанр поля $k(x, y)$ сразу определится из формулы (6). В случае же специального класса надо попрежнему исключить гиперэллиптическое поле. Тогда, введя обозначения

$$\text{Изм}\,\mathfrak{A} = n, \quad \text{Пор}\,\mathfrak{A} = m, \quad r = m - 2n + 2,$$

мы, при условии выполнения неравенства

$$2n - r - 4 > 0, \tag{7}$$

получим для жанра ρ следующее ограничение:

$$\rho \leqslant n + 2r + \left[\frac{2r(r+1)}{2n - r - 4}\right], \tag{8}$$

где, как в теории чисел, под символом $[a]$ мы будем разуметь наименьшее целое число, не превышающее a (entier).

Если $r = 0$, мы получим отсюда теорему Клиффорда:

Теорема 47 (Клиффорда). *Между измерением и порядком специального класса $\mathfrak{A}$ существует неравенство*

$$\text{Пор}\,\mathfrak{A} \geqslant 2 \cdot \text{Изм}\,\mathfrak{A} - 2. \tag{9}$$

Доказательство. Допустим противное: пусть класс $\mathfrak{A}$ имеет измерение n и порядок m, причем

$$m < 2n - 2. \tag{10}$$

Не нарушая общности, предположим, что класс $\mathfrak{A}$ собственный; в противном случае мы сократили бы его на общий дивизор, что уменьшило бы его порядок и оставило бы неизменным его измерение, так что неравенство (10) не нарушалось бы.

Возьмем произвольную не-вейерштрассову точку P и закрепим в классе $\mathfrak{A}$ $(n-1)$-ую степень простого дивизора P. Тогда в классе $\mathfrak{A}$ определится по крайней мере один дивизор вида

$$P^{n-1}P_1P_2\cdots P_{m-n+1}.$$

В силу (10), мы имеем

$$n - 2 \geqslant m - n + 1,$$

так что, закрепляя в классе $\mathfrak{A}$ точки $P_1, P_2, \ldots, P_{m-n+1}$, мы получим класс

$$(P^{n-1}),$$

измерение которого подчинено неравенству

$$\text{Изм}\,(P^{n-1}) \geqslant n - (m - n + 1) \geqslant n - (n - 2) = 2,$$

так что в поле $k(x, y)$ существует элемент, в представлении которого через дивизоры знаменатель состоит из дивизора P^{n-1}. Это, однако, противоречит тому, что P не есть точка Вейерштрасса. В самом деле, мы предположили, что класс $\mathfrak{A}$ специален, откуда

$$\text{Изм}\,\mathfrak{A} \leqslant \text{Изм}\,\mathfrak{W},$$

т. е.

$$n \leqslant \rho,$$

так что

$$\text{Изм}\,(P^{\rho-1}) \geqslant 2.$$

Получившееся противоречие доказывает теорему.

В дальнейшем нам понадобится следующая простая

Лемма. *Если*

$$\text{Изм}\,\mathfrak{A} = n,$$

то мы можем найти в классе $\mathfrak{A}$ *такой дивизор*

$$Q \cdot P_1 P_2 \cdots P_{n-1}, \tag{11}$$

чтобы имело место

$$\text{Изм}\,(Q) = 1.$$

Доказательство. Выберем в качестве P_1 простой дивизор, не входящий в общий делитель класса $\mathfrak{A}$. Тогда, находя в классе $\mathfrak{A}$ все дивизоры, делящиеся на P_1, и сокращая их на P_1 («закрепив» P_1), мы придем к классу $\mathfrak{A}_1$ измерения $n-1$. Закрепим в нем точку P_2, которой соответствует простой дивизор, не входящий в общий делитель класса $\mathfrak{A}_1$. Получим класс $\mathfrak{A}_2$ измерения $n-2$. Продолжая процесс мы, наконец, придем к классу $\mathfrak{A}_{n-1}$ измерения 1. Если он порождается дивизором Q, то в классе $\mathfrak{A}$ лежит дивизор (11), ч. и т. д.

Теорема 48. *Пусть измерение* n *и порядок* m *специального класса* $\mathfrak{A}$ *поля* $k(x, y)$ *связаны соотношением*

$$m = 2n - 2 + r, \qquad r \geqslant 0, \tag{12}$$

причем

$$2n - r - 4 > 0. \tag{13}$$

Кроме того, пусть класс $\mathfrak{A}$ *содержит такой дивизор*

$$A = P_1 P_2 \cdots P_{n-2} P_{n-1} Q, \tag{14}$$

что класс $(P_1 Q)$ *имеет измерение* 2 *и является собственным. Тогда жанр* ρ *поля* $k(x, y)$ *удовлетворяет неравенству*

$$\rho \leqslant n + 2r + \left[\frac{3r(r+1)}{2n-r-4}\right]. \tag{15}$$

Доказательство. В силу предыдущей леммы, в классе $\mathfrak{A}$ можно найти такой дивизор (14), что $\text{Изм}\,(Q) = 1$. Тогда

$$\text{Изм}\,(P_1 Q) = 2, \text{Изм}\,(P_1 P_2 Q) = 3, \ldots, \text{Изм}\,(P_1 P_2 \ldots P_{n-1} Q) = n. \tag{16}$$

В силу нашего предположения класс $(P_1 Q)$ собственный. Кроме того, из рассуждения при доказательстве предыдущей леммы следует, что каждую из точек $P_1, P_2, \ldots, P_{n-1}$ можно выбирать произвольно, избегая лишь конечного числа значений. Выберем эти точки так, чтобы

$$\text{Изм}\,(P_1 P_2 \ldots P_{n-1}) = 1. \tag{17}$$

Для этого достаточно выбрать P_1 произвольно; P_2— так, чтобы P_2 не был общим делителем класса $\left(\frac{\mathfrak{W}}{P_1}\right)$; P_3--так, чтобы P_3 не был общим делителем класса $\left(\frac{\mathfrak{W}}{P_1 P_2}\right)$, и т. д. Тогда

$$\text{Изм}\left(\frac{\mathfrak{W}}{P_1 P_2 \ldots P_{n-1}}\right) = \rho - n + 1,$$

и теорема Римана — Роха дает

$$\text{Изм}\,(P_1 P_2 \ldots P_{n-1}) = \text{Пор}\,(P_1 P_2 \ldots P_{n-1}) - \rho + 1 + \text{Изм}\left(\frac{\mathfrak{W}}{P_1 P_2 \ldots P_{n-1}}\right) =$$
$$= (n-1) - \rho + 1 + (\rho - n + 1) = 1.$$

Введем обозначение

$$Q = P_1' P_2' \ldots P_{m-n+1}'$$

и применим теорему Нетера к последовательности точек, состоящей из периодически повторяющейся последовательности

$$P_1', P_2', \ldots, P'_{m-n+1}; P_1, P_2, \ldots, P_{n-1}.$$

На отрезке

$$P_1', P_2', \ldots, P_{m-n+1}'$$

первого периода мы, в силу

$$\text{Изм}\,(Q) = 1,$$

получим $m - n + 1$ пробелов. На остальной части первого периода мы, в силу (16), не получим ни одного пробела.

Рассмотрим отрезок

$$P_1', P_2', \ldots, P_{m-n+1}', P_1$$

второго периода. На отрезке

$$P_2, \ldots, P_{n-1}, P_1', \ldots, P'_{m-n+1}, P_1 \tag{18}$$

в силу

$\text{Изм}\,(P_2) = 1$, $\text{Изм}\,(P_2 \ldots P_{n-1} P_1' \ldots P'_{m-n+1} P_1) = \text{Изм}\,\mathfrak{A} = n$

встречается ровно $n - 1$ не-пробелов. В силу (17), эти не-пробелы не встречаются на первых $n - 2$ местах. Пусть дивизор

$$P_2 \ldots P_{n-1} P_1' \ldots P_\alpha' \qquad (\alpha = 1, 2, \ldots, m - n + 2) \tag{19}$$

дает не-пробел. Это значит, что в поле $k(x, y)$ существует элемент, представляемый дивизором со знаменателем (19), причем P_α не сокращается с числителем. С другой стороны, в силу того, что класс

(QP_1) собственный, в поле $k(x, y)$ существует элемент, представляемый дивизором со знаменателем QP_1, причем ни один из простых дивизоров знаменателя не сокращается с числителем. Беря произведение обоих элементов, мы убедимся, что отрезку

$$P_1', \ldots, P'_{m-n+1}, P_1, P_2, \ldots, P_{n-1}, P_1', \ldots, P_\alpha'$$

соответствует не-пробел. Таким образом, на отрезке

$$P_1', \ldots, P'_{m-n+1}, P_1$$

второго периода встречается по крайней мере $n-1$ не-пробелов и, следовательно,

$$\leqslant (m-n+2)-(n-1)=r+1$$

пробелов.

Отрезок

$$P_2, \ldots, P_{n-1}$$

второго периода, в силу (16) и того, что класс $\mathfrak{A}$ собственный, не дает пробелов. Таким образом, в рассматриваемой периодической последовательности точек первый период дает $m-n+1$ пробелов, а каждый из последующих периодов не более $r+1$ пробелов.

Пусть в нашей последовательности все пробелы закончатся после k полных периодов, так что k-тый период пусть содержит хотя бы один пробел, а $(k+1)$-тый вовсе не содержит пробелов. Из теоремы Нетера следует

$$(m-n+1)+(k-1)(r+1)\geqslant \rho. \tag{20}$$

Кроме того, поскольку пробелы могут встречаться не далее чем на $(2\rho-1)$-м месте и в то же время в начале k-го периода непременно встретится хотя бы один пробел, мы имеем

$$(k-1)m+1\leqslant 2\rho-1. \tag{21}$$

Подставляя в (20) значения $k-1$

$$k-1\leqslant \frac{2\rho-2}{m},$$

получим

$$m(m-n+1)+(2\rho-2)(r+1)\geqslant m\rho,$$

откуда, подставляя

$$m=2n+(r-2),$$

будем иметь

$$\rho\leqslant \frac{(2n+r-2)(n+r-1)-2r-2}{2n-(r+4)},$$

или

$$\rho\leqslant n+2r+\frac{3r(r+1)}{2n-r-4},$$

откуда и вытекает формула (15).

Особо отметим случай $r = 0$, в котором неравенство (15) принимает вид

$$\rho \leqslant n.$$

Отсюда следует

$$m = 2n - 2 \geqslant 2\rho - 2$$

Если при этом класс $\mathfrak{A}$ специален, то он должен совпадать с $\mathfrak{W}$. Итак,

Следствие. Если измерение и порядок специального класса $\mathfrak{A}$ связаны соотношением

$$\text{Пор}\,\mathfrak{A} = 2 \cdot \text{Изм}\,\mathfrak{A} - 2,$$

и если $\mathfrak{A}$ содержит собственный класс порядка $m - n + 1$ и измерения 2, то $\mathfrak{A}$ есть класс дифференциалов.

Примечание. В ходе доказательства мы предположим, что $\mathfrak{A}$ есть собственный класс. Это предположение не ведет к существенным ограничениям, так как в противном случае, сокращая класс $\mathfrak{A}$ на общий делитель, мы придем к собственному классу $\mathfrak{A}'$, тоже специальному, у которого измерение останется тем же, а порядок и, следовательно, число r уменьшится. Ограничение для ρ, наложенное при помощи формулы (15) для класса $\mathfrak{A}'$, более жестко, чем то, которое мы получили бы, применяя формулу (15) непосредственно к классу $\mathfrak{A}$.

Перейдем к исследованию случаев, когда сделанное нами предположение не выполняется. В этих случаях, выбирая совершенно произвольно точки $P_1, P_2, \ldots, P_{n-1}$ и определяя в классе $\mathfrak{A}$ дивизор $QP_1P_2 \ldots P_{n-1}$, мы получим классы

$$(QP_i) \qquad (i = 1, 2, \ldots, n-1), \tag{22}$$

ни один из которых не является собственным.

Пусть класс (QP_1) имеет делителем точку P_1'. Она не может быть общим делителем всех классов (22), так как в противном случае она была бы общим делителем всех дивизоров линейных семейств

$$(QP_i)\frac{P_1P_2 \ldots P_{n-1}}{P_i} \qquad (i = 1, 2, \ldots, n-1). \tag{23}$$

Но линейными комбинациями этих дивизоров исчерпываются все дивизоры класса $\mathfrak{A}$. В самом деле, пусть в классе (QP_i) содержится дивизор R_i, не делящийся на $P_i\,(i = 1, 2, \ldots, n-1)$. Тогда в семействах (23) можно выделить n дивизоров

$$QP_1 \ldots P_{n-1}, R_1\frac{P_n \ldots P_{n-1}}{P_1}, R_2\frac{P_1 \ldots P_{n-1}}{P_2}, \ldots, R_{n-1}\frac{P_1 \ldots P_{n-1}}{P_{n-1}}, \tag{24}$$

лежащих в классе $\mathfrak{A}$. Они линейно независимы, так как, предположив между ними линейную зависимость

$$A_0 QP_1 \ldots P_{n-1} + \sum_{i=1}^{n-1} A_i R_i \frac{P_1 \ldots P_{n-1}}{P_i} = 0,$$

мы из делимости всех слагаемых, кроме $R_i \frac{P_1 \dots P_{n-1}}{P_i}$, на P_i заключаем, что

$$A_i = 0 \qquad (i = 1, 2, \dots, n-1).$$

Если бы P_1' был общим делителем всех классов (QP_i), то и Q и все R_i и, значит, все дивизоры (24) делились бы на P_1'. Следовательно, P_1' был бы общим делителем класса $\mathfrak{A}$.

Пусть $A_1, A_2, \dots, A_n$ представляет собой систему линейно независимых дивизоров класса $\mathfrak{A}$ и пусть их частным соответствуют элементы поля $k(x, y)$:

$$\frac{A_2}{A_1} \approx z_2, \frac{A_3}{A_1} \approx z_3, \dots \frac{A_n}{A_1} \approx z_n.$$

Специализируем A_1, A_2, A_3 так, чтобы они делились на простые дивизоры $P_3, \dots, P_{n-1}$, выбранные так, чтобы при их закреплении в классе $\mathfrak{A}$ получался класс измерения 3. Сократив семейство (A_1, A_2, A_3) на $P_3, \dots, P_{n-1}$, получим класс измерения 3. Соответствующее ему поле $k(z_2, z_3)$ порождается элементами z_2, z_3, которые пусть связаны уравнением

$$g(z_2, z_3) = 0. \tag{25}$$

Выберем точку P_1, на которую пусть не делится A_1 и которая пусть не соответствует особой точке кривой (25). Пусть ζ_2, ζ_3 будут значения элементов z_2, z_3 в точке P_1. Имеем

$$z_2 - \zeta_2 \approx \frac{A_2 - \zeta_2 A_1}{A_1}, \qquad z_3 - \zeta_3 \approx \frac{A_3 - \zeta_3 A_1}{A_1}.$$

Очевидно, что семейство $(A_2 - \zeta_2 A_1, A_3 - \zeta_3 A_1)$ по сокращении приводится к классу измерения 2, который получается из класса $\mathfrak{A}$ после закрепления точек $P_1, P_3, \dots, P_{n-1}$. В силу нашего предположения его общий наибольший делитель содержит простые дивизоры, отличные от $P_1, P_3, \dots, P_{n-1}$ и, в силу доказанного относительно точек P_1 и P_2, отличные от простых дивизоров, входящих одновременно в A_1, A_2, A_3. Допустим, что

$$k(z_2, z_3) = k(x, y).$$

$z_2 - \zeta_2$ и $z_3 - \zeta_3$ имеют общими делителями, кроме P_1, еще другие дивизоры. Но тогда, в силу теоремы 54 (см. ниже), точка (ζ_2, ζ_3) есть особая точка кривой (25), что мы исключили. Таким образом, $k(z_2, z_3)$ есть истинное подполе поля $k(x, y)$.

Более того: оказывается, что все поле $k(z_2, z_3, \dots, z_n)$ является истинным подполем поля $k(x, y)$. Для строгого доказательства этого факта понадобилось бы применение довольно тонких соображений теории Галуа, а потому мы ограничимся приведением интуитивного геометрического доказательства. Будем считать $z_2, z_3, \dots, z_n$ координатами $(n-1)$-мерного пространства. Считая их функциями от x, y,

которые связаны алгебраическим уравнением, мы получим в этом пространстве кривую L. Предполагая, что

$$k(z_2, z_3, \ldots, z_n) = k(x, y),$$

мы должны считать кривую L *простой*. Это означает, что различным точкам поля $k(x, y)$ будут соответствовать в общем случае (т. е. за исключением особых точек) различные точки кривой L. Закрепив на L $n-1$ обыкновенных точек $P_1, P_2, \ldots, P_{n-1}$, мы определим проходящее через них $(n-2)$-мерное плоское многообразие, пересекающее кривую L в дальнейших точках $P_1', P_2', \ldots, P_{m-n+1}'$. Выражаясь языком, к которому мы привыкли, элемент

$$\lambda_1 + \lambda_2 z_2 + \ldots + \lambda_n z_n,$$

где $\lambda_1, \lambda_2, \ldots, \lambda_n$ подобраны (с точностью до постоянного множителя так, чтобы он обращался в нуль в точках $P_1, P_2, \ldots, P_{n-1}$, будет обращаться в нуль еще в точках $P_1', P_2', \ldots, P_{m-n+1}'$.

Если мы предоставим точке P_2 свободно двигаться вдоль кривой L, то наше плоское многообразие опишет пучок многообразий, точки пересечения которых с L опишут двумерное семейство дивизоров класса $\mathfrak{A}$ с закрепленными точками $P_1, P_3, \ldots, P_{n-1}$. Согласно предположению, кроме точек $P_1, P_3, \ldots, P_{n-1}$, в этом семействе остаются неподвижными еще некоторые точки. Это означает, что пучок наших плоских многообразий пересекает кривую L, кроме точек $P_1, P_3, \ldots, P_{n-1}$, еще в нескольких неподвижных точках, одна из которых пусть будет P_1'. Поскольку они неподвижны, они должны лежать на всех наших плоских многообразиях, пересечение которых образует $(n-3)$-мерное плоское многообразие, однозначно определяемое точкам $P_1, P_3, \ldots, P_{n-1}$. Будем называть такие многообразия *гиперпрямыми*.

Для большей наглядности дальнейшего доказательства предварительно проведем его для случая $n = 4$, который соответствует трехмерному пространству. Здесь роль $(n-2)$-мерных плоских многообразий играют плоскости, проходящие через точки P_1, P_2, P_3, а роль гиперпрямых — прямые $P_1 P_3$. Дано, что прямая $P_1 P_3$, где P_1 и P_3 — произвольные точки кривой L, всегда проходит еще через одну точку кривой L, которую мы будем обозначать через P_1'. Если мы закрепим точку P_1 и заставим точку P_3 пробегать кривую L, то получим конус $K(P_1) = K_1$, каждая образующая которого, кроме вершины P_1, должна пересекать кривую L еще по крайней мере в двух точках. Докажем, что тогда кривая L лежит в неподвижной плоскости. Доказательство было бы гораздо проще провести в том случае, если бы точки P_1, P_3, P_1' пробегали три различные кривые L_1, L_3, L_1'. Чтобы притти к этому случаю, возьмем в качестве L_1 и L_3 произвольные малые отрезки кривой L, не имеющие общих точек, а в качестве L_1' — отрезок, который пробегает точка P_1' пересечения прямой $P_1 P_3$

с кривой L, когда P_1 пробегает L_1, а $P_3 - L_3$. При этом выберем L_1 и L_3 настолько малыми, чтобы L_1' не имела общих точек ни с L_1, ни с L_3. Фиксируем точку P_1 и заставим P_3 пробегать кривую L_3. Прямые P_1P_3 опишут конус K_1, на котором будет лежать часть L_{11}' кривой L_1'. Переместим точку P_1 в положение P_{12} на кривой L_1. Получим другой конус K_2, пересекающийся с L_1' по отрезку L_{12}'. Перемещение сделаем настолько малым, чтобы отрезки L_{11}' и L_{12}' имели общую часть, которую мы обозначим через L_{13}'. Конусы K_1 и K_2, если они различны, пересекаются по кривой L_3 и, кроме того, как алгебраические поверхности, могут иметь общими лишь конечное число образующих, которые в свою очередь могут пересекаться с L_{13}' лишь в конечном числе точек. Но, поскольку L_{13}' целиком лежит на обоих конусах, последние должны совпадать (точнее выражаясь, должны быть частями одного общего конуса). С другой стороны, единственным типом конуса, имеющего неопределенную вершину, является плоскость. Поскольку вершины совпадающих конусов K_1 и K_2 различны, оба они представляют собой плоскость. Беря на кривой L всевозможные отрезки, мы убедимся, что вся кривая лежит на неподвижной плоскости.

Проведем аналогичное доказательство для $(n-1)$-мерного пространства. Выделим на кривой L достаточно малые и не имеющие общих частей отрезки L_1 и L_3. Заставляя точку P_1 пробегать отрезок L_1, а точки $P_3, \ldots, P_{n-1}$ — независимо друг от друга отрезок L_3, и проводя через $P_1, P_3, \ldots, P_{n-1}$ гиперпрямые, мы, согласно условию, каждый раз будем получать по крайней мере еще одно пересечение гиперпрямой с кривой L; обозначим одно из них через P_1', и пусть оно описывает на кривой L отрезок L_1'. Отрезки L_1 и L_3 пусть будут настолько малы, чтобы L_1' не имел общих частей ни с L_1, ни с L_3. Фиксируем точку P_1. Тогда наши гиперпрямые опишут неплоское $(n-2)$-мерное многообразие (гиперконус) K_1, а точка P_1' — лежащий на L_1' отрезок L_{11}'. Сдвигая точку P_1 в положение P_{12}, мы точно таким же образом получим гиперконус K_2 и отрезок L_{12}'. Сдвиг P_1 и P_{12} будем предполагать настолько малым, чтобы отрезки L_{11}' и L_{12}' имели общую часть. Гиперконусы K_1 и K_2, если они различны, могут иметь пересечением только направляющую L_3 и конечное число образующих гиперпрямых, которые отсекут на L_1' конечное число точек. Так как, с другой стороны, они должны отсекать на L_1' общую часть отрезков L_{11}' и L_{12}', то гиперконусы K_1 и K_2 дожны иметь общую $(n-2)$-мерную часть. Но, поскольку они имеют разные вершины P_1 и P_{12}, они должны содержать наименьшее плоское многообразие, проведенное через P_1 и P_{12}. Произведя достаточное число сдвигов вершины P_1, мы придем к $(n-2)$-мерному плоскому многообразию, проходящему через каждый из получаемых гиперконусов. Но тогда каждый из них совпадет с этим плоским многообразием. Таким образом, отрезки кривой L лежат на $(n-2)$-мерном плоском многообразии, ч. и т. д. Анали-

тически это выражается так: элементы $z_2, z_3, \ldots, z_n$ связаны линейным соотношением

$$c_1 + c_2 z_2 + c_3 z_3 + \ldots + c_n z_n = 0 \tag{26}$$

с постоянными $c_1, c_2, \ldots, c_n$.

Проведенное рассуждение справедливо и для комплексных значений $z_2, z_3, \ldots, z_n$, поскольку условие их вещественности нигде не было использовано.

Соотношение (26) показывает, что не все дивизоры $A_1, A_2, \ldots, A_n$ линейно независимы, т. е. что измерение класса $\mathfrak{A}$ меньше n. Так как это противоречит нашему предположению, то наше предположение, что поле $k(z_2, z_3, \ldots, z_n)$ совпадает с $k(x, y)$, неверно: $k(z_2, z_3, \ldots, z_n)$ есть истинное подполе поля $k(x, y)$.

Представим через дивизоры элементы $z_2, z_3, \ldots, z_n$ внутри поля $k(z_2, z_3, \ldots, z_n)$. Ниже (в § 35) мы убедимся, что простой дивизор поля $k(z_2, z_3, \ldots, z_n)$ представляется как произведение одного и того же числа k простых дивизоров поля $k(x, y)$. Таким образом, классу $\mathfrak{A}$ в поле $k(z_2, z_3, \ldots, z_n)$ будет соответствовать класс $\mathfrak{A}'$, измерение которого останется тем же, а порядок уменьшится в k раз

$$n' = n, \qquad m' = \frac{m}{k}.$$

При этом, в силу доказанного, класс $\mathfrak{A}'$ будет удовлетворять сделанному нами предположению, так как иначе образованное элементами $z_2, z_3, \ldots, z_n$ поле не могло бы совпадать с $k(z_2, z_3, \ldots, z_n)$.

Число r' для класса $\mathfrak{A}'$ равно

$$r' = m' - 2n' + 2 = \frac{m - 2k(n-1)}{k}.$$

Но так как $k \geqslant 2$, то если мы учтем предположение (13), то получим

$$r' \leqslant \frac{m - 4n + 4}{k} = \frac{2n - 2 + r - 4n + 4}{k} = \frac{-2n + r + 2}{k} < -\frac{2}{k} < 0,$$

откуда, в силу теоремы Клиффорда, следует, что класс $\mathfrak{A}'$ не-специален. Применяя к нему теорему Риманна — Роха, получим для жанра ρ' поля $k(z_2, z_3, \ldots, z_n)$ величину

$$\rho' = \text{Пор}\,\mathfrak{A}' - \text{Изм}\,\mathfrak{A}' + 1 = \frac{m - k(n-1)}{k} \leqslant \frac{m - 2(n-1)}{k} = \frac{r}{k}.$$

В частности, если принять $r = 0$, как это сделано у Клиффорда, то

$$\rho' = 0,$$

т. е. поле $k(z_2, z_3, \ldots, z_n)$ уникурсально. Отсюда также следует

$$k = 2.$$

Обращаясь опять к § 35, мы выведем отсюда, что относительный порядок поля $k(x, y)$ над $k(z_2, z_3, \ldots, z_n)$ равен 2. Но так как поле

$k(z_2, z_3, \ldots, z_n)$ уникурсально, то отсюда следует, что $k(x, y)$ есть гиперэллиптическое поле. В этом состоит известное дополнение к теореме Клиффорда (например см. F. Severi. Vorlesungen über algebraische Geometrie. Übersetzt von D-r E. Löffler, Lpz.—B., 1921, стр. 133).

Изложение обобщения теоремы Клиффорда, опубликованное в моей статье «Über eine Verallgemeinerung eines Cliffordschen Satzes». Rendic. Circ. Mat. Pal. **55** (1931), содержит погрешности. Одна из основных идей изложенного здесь доказательства геометрической теоремы принадлежит А. Н. Нордену, сообщившему мне ее устно.

О КВАДРИРУЕМЫХ ЛУНОЧКАХ. I

(ÜBER QUADRIERBARE KREISBOGENZWEIECKE)

(Math. Ztschr. **39** (1934), стр. **161 — 175**)

Посвящается проф. Михаэлю Бауэру к 60-летию со дня рождения, 20 сентября 1934 г.

Э. Ландау [1] свел проблему квадрируемых луночек к решению уравнения

$$\left(\frac{\sin m\theta}{\sin n\theta}\right)^2 = \frac{m}{n}, \tag{1}$$

где m и n — взаимно простые целые рациональные числа. Он показал, что в случае $m = p$ (p — простое число) уравнение это разрешимо в квадратных радикалах только тогда, если p есть так называемое гауссово простое число, т. е. имеет вид $2^k + 1$. Недавно Л. Чакалов [2] существенно обобщил результат Ландау и показал, что условие это недостаточно, установив неразрешимость уравнения (1) в квадратных радикалах в случае $m = 17$, $n = 1$. В другой работе [3] при помощи весьма остроумного метода он исследовал несколько более общих случаев уравнения (1), пытаясь доказать предположение Клаузена [4] о том, что уравнение (1) решается в квадратных радикалах только в следующих случаях:

$$\begin{array}{lllll} m=2 & m=3 & m=3 & m=5 & m=5 \\ n=1 & n=1 & n=2 & n=1 & n=3. \end{array}$$

В настоящей работе я решаю задачу для случая $m - n \equiv 0 \pmod 2$. При этом я пользуюсь двумя критериями, которые были впервые применены М. Бауэром [5, 6] для исследования групп Галуа уравнений.

§ 1. Общие алгебраические критерии

1. Первый критерий Бауэра может быть формулирован следующим образом:

Лемма 1. *Если корень уравнения*

$$f(x) = 0 \tag{2}$$

допускает разложение в p-адический ряд

$$x = \varepsilon + ap^{\circ}, \tag{3}$$

где $\rho = \frac{\varkappa}{\lambda}$, $(\varkappa, \lambda) = 1$, *то порядок группы этого уравнения делится на* λ.

Доказательство. Из теоремы Орэ [7] следует, что в этом случае поле, образованное корнем уравнения (2), содержит простой идеальный множитель $\mathfrak{P}$ числа p, порядок которого e делится на λ. Отсюда мы заключаем, что в нормальном поле $K(x_1, x_2, \ldots, x_n)$, где $x_1, x_2, \ldots, x_n$ суть все корни уравнения (2), порядок группы инерции, соответствующий простому идеальному множителю $\mathfrak{P}$, делится на λ [8]. Но так как группа инерции является делителем группы Галуа, то лемма доказана.

Следствие. *Если уравнение* (1) *решается в квадратных радикалах, то соответствующие ему числа должны содержать в знаменателе только степени двойки.*

2. Второй критерий Бауэра можно вывести из следующей знаменитой теоремы Дедекинда, если распространить ее на критически простые числа.

Лемма 2. *Если левая часть уравнения* (2), *рассматриваемая по модулю произвольного простого числа* p, *разлагается на неприводимые по модулю* p *полиномы степеней* $n_1, n_2, \ldots, n_k$, *то порядок его группы Галуа* $\mathfrak{G}$ *делится на каждое из чисел* $n_1, n_2, \ldots, n_k$.

Доказательство. Из той же самой теоремы Орэ следует, что в этом случае существует простой идеальный множитель $\mathfrak{P}$ числа p степень которого f делится на степень n_i любого неприводимого по модулю p множителя $f(x)$. Отсюда мы заключаем, что в нормальном поле $K(x_1, x_2, \ldots, x_n)$, где $x_1, x_2, \ldots, x_n$ представляют все корни уравнения (2), $\mathfrak{P}$ разлагается на простые идеалы, степень которых F делится на f, а значит, и на n_i [8, стр. 499]. Но так как степень F равна индексу $(\mathfrak{Z} : \mathfrak{T})$, где $\mathfrak{Z}$ — группа разложения и $\mathfrak{T}$ — группа инерции этого простого идеального множителя, то отсюда следует, что порядок $\mathfrak{Z}$ и, значит, тем более порядок группы Галуа уравнения (2), делится на n_i, что и т. д.

Следствие. *Для того чтобы уравнение* (2) *решалось в квадратных радикалах, необходимо, чтобы его левая часть по каждому простому модулю* p *распадалась на неприводимые множители, степени которых есть степени числа 2.*

§ 2. Значение показателя ρ для уравнения луночки

1. Как показал Чакалов, уравнение (1) подстановкой $e^{i\theta} = x$, $y = x^2$ преобразуется в уравнение

$$\left(\frac{y^m - 1}{y - 1}\right)^2 - \frac{m}{n}\, y^{m-n} \left(\frac{y^n - 1}{y - 1}\right)^2 = 0. \qquad (4)$$

Если $m-n$ — четное число, то это уравнение распадается в следующие уравнения:

$$\frac{y^m-1}{y-1}-\sqrt{\frac{m}{n}}\,y^{\frac{m-n}{2}}\frac{y^n-1}{y-1}=0,$$
$$\frac{y^m-1}{y-1}+\sqrt{\frac{m}{n}}\,y^{\frac{m-n}{2}}\frac{y^n-1}{y-1}=0. \qquad (5)$$

Если же $m-n$ — нечетное, то сделаем сначала в уравнении (4) подстановку $y=x^2$ и положим $m_1=2m$, $n_1=2n$, $\sqrt{\frac{m_1}{n_1}}=\sqrt{\frac{m}{n}}$. Тогда уравнение (4) распадается на уравнения того же самого типа (5). Однако в этом случае числа m_1 и n_1 не являются взаимно простыми, а имеют наибольшим общим делителем число 2.

Мы ограничимся рассмотрением только одного из уравнений (5) и запишем его в форме

$$y^m-1-\sqrt{\frac{m}{n}}\cdot y^{\frac{m-n}{2}}(y^n-1)=0, \qquad (6)$$

добавив к его корням тривиальный корень $y=1$.

В последующем мы будем рассматривать уравнение (6) как сравнение по модулям простых множителей чисел m, n, $m-n$ и 2.

2. Пусть p — нечетный простой множитель числа m, так что $m=p^km_1$, $(m_1, p)=1$. Если мы рассмотрим уравнение (6) по модулю $\sqrt{p}$, то получим сравнение

$$(y^m-1)=y^{p^k m_1}-1\equiv(y^{m_1}-1)^{p^k}\equiv 0 \pmod{\sqrt{p}}.$$

Взяв за первое приближение к решению этого сравнения число ε, удовлетворяющее *уравнению* $(y^{m_1}-1)^{p^k}=0$, мы получим для ε следующие значения:

I. Иррациональный корень из единицы степени m_1; число таких корней равно $(m_1-1)p^k$, если m_1 — нечетное, и $(m_1-2)p^k$, если m_1 — четное.

II. p^k — кратный корень $+1$; здесь учитывается также тривиальный корень $+1$.

III. p^k — кратный корень -1; здесь учитывается также тривиальный корень -1.

Подставив затем в уравнение (6)

$$y=\varepsilon+ap^\rho,$$

где a — взаимно простое с p число, выпишем в полученном разложении только те члены, которые могут быть «наинизшими», т. е. порядки которых относительно p для некоторых значений ρ могут быть ниже, чем порядки всех других членов. При этом заметим, что биномиальные

коэффициенты $\binom{m}{s}$ $(s \leqslant p^k)$ делятся точно на p^{k-l}, если s делится точно на p^l. Таким образом, получаем

$$\binom{m}{1}\varepsilon^{m-1}ap^{\circ} + \ldots + \binom{m}{p}\varepsilon^{m-p}a^{p}p^{p\rho} + \ldots + \binom{m}{p^2}\varepsilon^{m-p^2}a^{p^2}p^{p^2\rho} + \ldots +$$

$$+ \binom{m}{p^k}\varepsilon^{m-p^k}a^{p^k}p^{p^k\rho} -$$

$$- \sqrt{\frac{m}{n}}\left\{(\varepsilon^n - 1) + \binom{n}{1}\varepsilon^{n-1}ap^{\circ} + \ldots\right\} \equiv 0 \pmod{\sqrt{p}}.$$

Будем различать два случая:

I ε — иррациональное число. Тогда, в силу $(m, n) = 1$ или $= 2$, $\varepsilon^n - 1 \neq 0$, так что порядки членов разложения будут

$$\boxed{k + \rho,\ k - 1 + p\rho,\ k - 2 + p^2\rho, \ldots, 1 + p^{k-1}\rho,\ p^k\rho,\ k\,/\,2.}$$

Значения ρ равны либо

$$\rho = \frac{1}{p^{\lambda+1} - p^{\lambda}} \qquad \left(\frac{k}{2} < \lambda \leqslant k\right), \tag{7}$$

либо

$$\rho = \frac{2\lambda - k}{2p^{\lambda}} \qquad \left(\frac{k}{2} < \lambda \leqslant k\right) \text{ (фиг. 1).} \tag{8}$$

II. $\varepsilon = 1$ (или $\varepsilon = -1$, если m и n — четные). Тогда порядки членов разложения будут

$$\boxed{k + \rho,\ k - 1 + p\rho,\ k - 2 + p^2\rho, \ldots, 1 + p^{k-1}\rho,\ p^k,\ \frac{k}{2} + \rho.}$$

Значения ρ равны либо

$$\rho = \frac{1}{p^{\lambda+1} - p^{\lambda}}, \tag{9}$$

либо

$$\rho = \frac{2\lambda - k}{2(p^{\lambda} - 1)} \qquad \text{(фиг. 2).} \tag{10}$$

3. Пусть теперь простое число q делит n, так что $n = q^{k_1}n_1$, $(n_1, q) = 1$. Положим в уравнении (6) $y = bq^{\circ}$, где b — взаимно простое с q число:

$$(b^m q^{m\rho} - 1) - \sqrt{\frac{m}{n}} \cdot (b^n q^{n\rho} - 1)\, b^{\frac{m-n}{2}} q^{\frac{m-n}{2}\rho} = 0.$$

Порядки членов этого уравнения суть

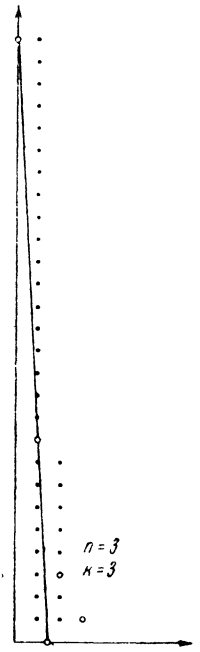
$$\boxed{m\rho,\ 0,\ -\frac{k_1}{2} + \frac{m+n}{2}\rho,\ -\frac{k_1}{2} + \frac{m-n}{2}\rho.}$$

Значения ρ будут

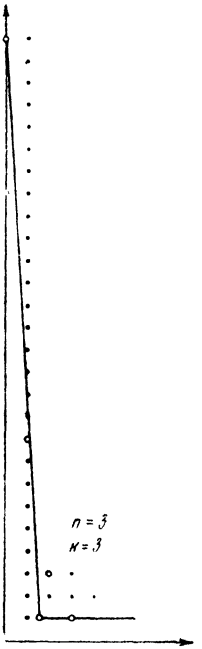
$$\rho = \pm \frac{k_1}{m-n}, \tag{11}$$

$$\rho = 0 \qquad \text{(фиг. 3)}. \tag{12}$$

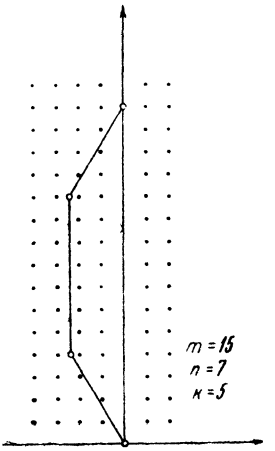
Если мы возьмем $\rho = 0$, то b будет корнем сравнения $(x^n - 1) \equiv 0 \pmod{\sqrt{q}}$, так что можно положить $y = \varepsilon + aq^\circ$ $(\varepsilon^n = 1)$ и повторить все рассуждения $n^\circ 2$. Таким образом, получаем:



Фиг. 1



Фиг. 2



Фиг. 3

I. Для $\varepsilon \neq \pm 1$

$$\rho = \frac{1}{q^{\lambda+1} - q^\lambda}, \tag{13}$$

$$\rho = \frac{2\lambda - k_1}{2q^\lambda}. \tag{14}$$

II. Для $\varepsilon = \pm 1$

$$\rho = \frac{1}{q^{\lambda+1} - q^\lambda}, \tag{15}$$

$$\rho = \frac{2\lambda - k_1}{2(q^\lambda - 1)}. \tag{16}$$

4. Пусть r — нечетный множитель числа $m-n$, так что $m-n = 2r^{k_1}s$, $(s, r) = 1$. Тогда

$$\sqrt{\frac{m}{n}} = \sqrt{1 + \frac{2r^{k_1}s}{n}} = 1 + \frac{r^{k_1}s}{n} - \frac{r^{2k_1}s^2}{2n^2} + \ldots$$

Подставляя это выражение в уравнение (6), получим

$$\left(y^{\frac{m+n}{2}}-1\right)\left(y^{\frac{m-n}{2}}+1\right)+\frac{r^{k_2 s}}{n}\,y^{\frac{m-n}{2}}(y^n-1)+\ldots=0.$$

Рассмотрим это уравнение по модулю r; тогда

$$\left(y^{\frac{m+n}{2}}-1\right)(y^{r^{k_2 s}}+1)\equiv 0 \pmod r,$$

Первый множитель $y^{\frac{m+n}{2}}-1$ левой части не имеет по модулю r кратных корней. Следовательно, к этому множителю можно применить второй критерий. Чтобы определить степень неприводимого по модулю r множителя бинома $y^{\frac{m+n}{2}}-1$, заметим, что, по лемме 2, полином $y^{\frac{m+n}{2}}-1$ содержит множитель степени f тогда и только тогда, если он имеет с полиномом $y^{r^f-1}-1$ общий делитель. С другой стороны, два полинома $y^\lambda-1$ и $y^\mu-1$ имеют наибольший общий делитель $y^\delta-1$, где δ есть общий наибольший делитель чисел λ и μ. Вследствие этого мы должны разложить $\frac{m+n}{2}$ на простые множители и для каждого такого простого множителя π исследовать, к какому показателю принадлежит r по модулю π. Затем мы рассмотрим r по модулю произведения двух, трех и т. д. множителей числа $\frac{m+n}{2}$.

Второй множитель $y^{r^{k_2 s}}+1$ можно представить по модулю r следующим образом:

$$(y^{r^{k_2 s}}+1)\equiv(y^s+1)^{r^{k_2}} \pmod r.$$

Следовательно, можно положить $y=\varepsilon+ar^\rho$, где ε есть корень уравнения $\varepsilon^s+1=0$. Тогда получим

$$\left(\varepsilon^{\frac{m+n}{2}}+1+\frac{m+n}{2}\varepsilon^{\frac{m+n}{2}-1}ar^\rho+\ldots\right)\left(\binom{r^{k_2 s}}{1}\varepsilon^{r^{k_2 s}-1}ar^\rho+\ldots+\right.$$
$$\left.+\binom{r^{k_2 s}}{r}\varepsilon^{r^{k_2 s}-r}a^r r^{r\rho}+\ldots+\binom{r^{k_2 s}}{r^{k_2}}\varepsilon^{r^{k_2 s}-r^{k_2}}a^{r^{k_2}}r^{r^{k_2}\rho}+\ldots\right)+$$
$$+\frac{r^{k_2 s}}{n}\left(\varepsilon^{r^{k_2}}+\binom{r^{k_2 s}}{1}\varepsilon^{r^{k_2 s}-1}ar^\rho+\ldots\right)\left(\varepsilon^n-1+\binom{n}{1}\varepsilon^{n-1}ar^\rho+\ldots\right)=0.$$

Порядки «наинизших» членов суть

$$\boxed{k_2+\rho,\ k_2-1+r\rho,\ \ldots,\ r^{k_2}\rho,\ \{k_2\},\ k_2+\rho.}$$

Порядок k_2 встретится тогда и только тогда, если $\varepsilon^n - 1 \neq 0$, т. е. если $\varepsilon \neq -1$. Коэффициент при $r^{k_2+\rho}$ равен

$$\left(\varepsilon^{\frac{m+n}{2}} + 1\right)\varepsilon^{\frac{m-n}{2}-1} sa + \frac{s}{n}\varepsilon^{\frac{m-n}{2}} n\varepsilon^{n-1} a =$$

$$= \varepsilon^{\frac{m-n}{2}-1} sa\left\{\varepsilon^{\frac{m+n}{2}} + 1 + \varepsilon^n\right\} = \varepsilon^{\frac{m-n}{2}-1} sa\{-\varepsilon^n + 1 + \varepsilon^n\} = \varepsilon^{\frac{m-n}{2}-1} sa,$$

т. е. не делится на r.

I. $\varepsilon^n - 1 \neq 0$. Значения ρ будут

$$\rho = \frac{1}{r^{\lambda-1}(r-1)}, \tag{17}$$

$$\rho = \frac{1}{r}. \tag{18}$$

II. $\varepsilon^n - 1 = 0$. Тогда значения ρ равны

$$\rho = \frac{1}{r^{\lambda-1}(r-1)} \qquad (\lambda = 2, 3, \ldots, k_2), \tag{19}$$

$$\rho = \frac{1}{r-1}. \tag{20}$$

5. Теперь мы перейдем к исследованию уравнения (6) по модулю 2. Здесь нужно различать два случая:

A. m и n — нечетные. Тогда 2 не является критическим простым числом в поле $K\left(\sqrt{\frac{m}{n}}\right)$. Мы имеем

$$y^m - 1 - \sqrt{\frac{m}{n}}\, y^{\frac{m-n}{2}}(y^n - 1) \equiv \left(y^{\frac{m+n}{2}} - 1\right)\left(y^{\frac{m-n}{2}} - 1\right) \pmod 2.$$

Одно из чисел $\frac{m+n}{2}$, $\frac{m-n}{2}$ в силу $\frac{m+n}{2} + \frac{m-n}{2} = m$ должно быть четным, другое — нечетным. Предположим, что $\frac{m+n}{2}$ — нечетное. Чтобы определить степень неприводимого по модулю 2 делителя бинома $x^{\frac{m+n}{2}} - 1$, нужно узнать, к какому показателю принадлежит число 2 по модулю π, где π — простой делитель числа $\frac{m+n}{2}$.

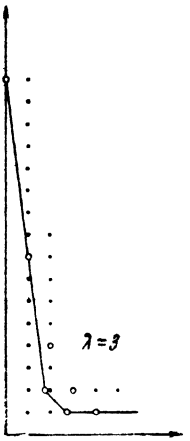
B. m и n — четные. Так как $\frac{m-n}{2}$ должно быть нечетным, то одно из чисел m, n делится точно на 2, другое — на высшую степень числа 2, скажем, на $2^{\lambda+1}$ $(\lambda > 0)$. Пусть, например, $m = 2^{\lambda+1} m_1$, $n = 2n_1$, где m_1, n_1 — нечетные числа. Тогда

$$(y^{m_1} - 1)^{2^{\lambda+1}} \equiv 0 \pmod 2,$$

так что в разложении $y = \varepsilon + a \cdot 2^{\rho}$ величина ε есть m_1-й корень из единицы. Порядки членов разложения левой части уравнения (6) будут

$$\lambda+1+\rho, \lambda+2\rho, \ldots, \lambda-1+2^2\rho, \ldots, 1+2^{\lambda}\rho, \ldots, 2^{\lambda+1}\rho, \ldots,$$
$$\left\{\frac{\lambda}{2}\right\}, \frac{\lambda}{2}+1+\rho, \frac{\lambda}{2}+2\rho.$$

Порядок $\lambda/2$ существует только тогда, если $\varepsilon^n - 1 \neq 0$.



Фиг. 4

I. $\varepsilon^n - 1 \neq 0$. Значения ρ будут:

$$\rho = \frac{1}{2^{\mu-1}}, \tag{21}$$

$$\rho = \frac{\mu - \frac{\lambda}{2}}{2^{\mu}}. \tag{22}$$

II. $\varepsilon^n - 1 = 0$. Значения ρ будут:

$$\rho = \frac{1}{2^{\mu-1}}, \tag{23}$$

$$\rho = \frac{\mu - \frac{\lambda}{2}}{2(2^{\mu}-1)} \quad \text{(фиг. 4)}. \tag{24}$$

§ 3. Исследование уравнения (6) при нечетных m, n

1. Предположим, что уравнение (6) имеет делитель степени u

$$g(y) = 0, \tag{25}$$

неприводимый в поле $K\left(\sqrt{\frac{m}{n}}\right)$. Исследуем, при каких условиях это уравнение решается в квадратных радикалах. Из леммы 1 следует, что для этого необходимо, чтобы корням его по каждому простому модулю p соответствовали числа ρ, содержащие в знаменателях только степени двойки. Если для какого-либо из его корней $\rho = \frac{r}{s}$, $(r, s) = 1$, то корню этому соответствует s сопряженных корней, которые, как мы будем говорить, образуют s-членный корневой цикл первого рода. Если s есть степень двойки, то соответствующий корневой цикл назовем *благоприятным*.

Точно так же из леммы 2 мы заключаем следующее. Если $g(y)$ имеет делитель степени f, неприводимый по модулю p, то будем говорить, что его корни образуют f-членный корневой цикл второго рода. Тогда имеет место

Теорема 1. *Для того чтобы уравнение* (25) *решалось в квадратных радикалах, необходимо, чтобы его корни по каждому*

простому модулю образовывали только благоприятные циклы. При этом должно быть

$$u = 2^{\alpha} + 2^{\alpha'} + \ldots, \tag{26}$$

где $2^{\alpha}, 2^{\alpha'}, \ldots$ *обозначают порядки корневых циклов. Каждому простому модулю должно соответствовать разложение числа и типа (26).*

2. Пусть m и n — нечетные и p — простой множитель числа m, так что $m = p^k m_1$, $(m_1, p) = 1$. Циклы уравнения (6) по модулю p имеют, в силу (7), (8), (9) и (10), порядки

$$p^{\lambda}\frac{p-1}{2},\ p^{\lambda},\ p^{\lambda}\frac{p-1}{2},\ \frac{p^{\lambda}-1}{(p^{\lambda}-1,\ 2\lambda-k)}$$

(мы принимаем во внимание, что простое число p является критическим в поле $K\left(\sqrt{\frac{m}{n}}\right)$, так что порядок $p^{1/2}$ встречается в области рациональности). Из этих порядков только последний может быть степенью числа 2, так что только один соответствующий ему корневой цикл может быть благоприятным. Исследуем, когда он в действительности благоприятен. Тогда число $\frac{2\lambda-k}{2(p^{\lambda}-1)}$ $\left(\frac{k}{2} < \lambda \leqslant k\right)$ после сокращения должно содержать в знаменателе только степень числа 2. Рассмотрим два случая:

I. λ содержит нечетный простой множитель t: $\lambda = t\lambda_1$. Тогда

$$\frac{2\lambda-k}{2(p^{\lambda}-1)} = \frac{2\lambda-k}{2(p^{\lambda_1}-1)(p^{\lambda_1(t-1)}+p^{\lambda_1(t-2)}+\ldots+p^{\lambda_1}+1)}.$$

Число $p^{\lambda_1(t-1)}+p^{\lambda_1(t-2)}+\ldots+p^{\lambda_1}+1$ — нечетно и, при $p>2$, больше, чем $t+2\lambda$, а значит тем более больше, чем $2\lambda-k$. Вследствие этого этот нечетный множитель не сократится с числителем, так что этот случай не благоприятен.

II. λ есть степень числа 2: $\lambda = 2^{\alpha}$. Число $\frac{2\lambda-k}{2(p^{\lambda}-1)}$ можно представить следующим образом:

$$\frac{2\lambda-k}{2(p^{2^{\alpha}}-1)} = \frac{2\lambda-k}{2(p^{2^{\alpha-1}}+1)(p^{2^{\alpha-2}}+1)\ldots(p^2+1)(p+1)(p-1)}. \tag{27}$$

Знаменатель состоит из $\alpha+1$ множителей, которые также могут содержать нечетные множители. Если по меньшей мере два из этих множителей не содержат нечетных простых множителей, то

$$p^{2^{\beta}}+1 = 2^{\xi},\ p^{2^{\gamma}}\pm 1 = 2^{\eta} \qquad (\beta>\gamma,\ \xi>\eta)$$

(знак минус встречается только в случае $\gamma = 0$). Отсюда следует, что $p^{2^{\beta}}+1$ делится на $p^{2^{\gamma}}\pm 1$. Но так как $p^{2^{\beta}}-1 = (p^{2^{\gamma}})^{2^{\beta-\gamma}}-1$

делится на $p^{2^\gamma} \pm 1$, то $2 = (p^{2^\beta} + 1) - (p^{2^\beta} - 1)$ также делится на $p^{2^\gamma} \pm 1$. Это может быть только в случае

$$p^{2^\gamma} - 1 = 2, \quad p = 3, \quad \gamma = 0.$$

Если $p = 3$, то

$$(3^{2^\alpha} - 1)(3^{2^{\alpha-1}} + 1)(3^{2^{\alpha-2}} + 1) \ldots (3^2 + 1)(3 + 1)(3 - 1),$$

в силу

$$(3^{2^s} + 1) \equiv (9^s + 1) \equiv 2 \pmod 4,$$

делится точно на $2^{\alpha+2}$. Частное $\frac{3^{2^\alpha} - 1}{2^{\alpha+2}}$ как нечетный множитель знаменателя должно быть множителем числа $2\lambda - k$, откуда следует

$$\frac{3^{2^\alpha} - 1}{2^{\alpha+2}} \leqslant 2\lambda - k,$$

или, в силу $2\lambda - k \leqslant \lambda = 2^\alpha$,

$$3^{2^\alpha} \leqslant 2^{2^\alpha + 2}; \tag{28}$$

откуда следует:

$$2^\alpha \leqslant 2\alpha + 2, \text{ т. е. } \alpha \leqslant 2.$$

Но значение $\alpha = 2$ не удовлетворяет неравенству (28):

$$3^{2^2} > 2^{2 \cdot 2 + 2} + 1.$$

Вследствие этого допустимы только значения $\alpha = 0$, $\alpha = 1$. Если $\alpha = 0$, то $\lambda = 1$, $k = 1$. Если $\alpha = 1$, то $\lambda = 2$, $k \leqslant 3$. Значит, мы имеем здесь две возможности:

$$\text{A) } p^k = 27, \ \rho = \frac{1}{16}; \quad \text{B) } p^k = 9, \ \rho = \frac{1}{8}.$$

Если все множители знаменателя в (27) (возможно, кроме одного) делятся на нечетные простые множители, которые все также содержатся в числителе, то $2\lambda - k$ должно содержать по меньшей мере α нечетных множителей. Каждый из этих множителей равен по меньшей мере 3, так что

$$2\lambda - k \geqslant 3^\alpha.$$

Так как, с другой стороны, в силу $k \geqslant \lambda$ имеет место неравенство $2\lambda - k \leqslant \lambda = 2^\alpha$, то мы приходим к неравенству

$$2^\alpha \geqslant 3^\alpha,$$

которое возможно только в случае $\alpha = 0$.

III. $\lambda = 1$, $k = 1$. Тогда $\rho = \frac{1}{2(p-1)}$ должно иметь в знаменателе только степень числа 2. Отсюда следует, что p есть так называемое гауссово простое число, т. е. имеет форму $2^s + 1$.

6. Теперь зададимся вопросом о степени u неприводимого уравнения (25). Так как благоприятные корневые циклы имеют для ρ значения (10), т. е. соответствуют значению $\varepsilon = 1$, в то время как сравнение

$$y^m - 1 \equiv 0 \pmod{p}$$

содержит p^k-кратный корень $y = 1$ и уравнение (6) имеет тривиальный корень $y = 1$, то u не может быть больше чем $p^k - 1$. Если, с другой стороны, $k = 1$, то ρ имеет значение $\frac{1}{2(p-1)}$, так что степень неприводимого уравнения, которому удовлетворяет корень, соответствующий этому значению ρ, по меньшей мере равна $p - 1$, так как производящее число области рациональности $\sqrt{\frac{m}{n}}$ имеет относительно p порядок $^1/_2$. Итак, $u = p - 1$.

Если $p = 3$, $k = 2$, то $\rho = \frac{1}{p^k - 1}$. Но так как простое число 3 не является критическим, то здесь тоже $u \geqslant p^k - 1$. Вследствие этого в этих случаях

$$u = p^k - 1. \tag{29}$$

Если же $p = 3$, $k = 3$, то из фиг. 2 видно, что соответствующие значению $\varepsilon = 1$ корни образуют один 8-членный цикл и два 9-членных цикла. Следовательно, в благоприятном случае

$$u = 8. \tag{30}$$

Формула (29) показывает, что m не может содержать двух различных простых множителей. В самом деле, если $m = p^k p_1^{k_1} \ldots$, то

$$u = p^k - 1 = p_1^{k_1} - 1,$$

откуда следует: $p = p_1$. Если же m делится на 27, то $u = 8$. Если p_1 — другой простой множитель m, то $8 = p_1^{k_1} - 1$, т. е. $p_1^{k_1} = 9$; значит, p_1 не отличается от $p = 3$. Итак, во всех случаях мы имеем

$$m = p^k. \tag{31}$$

4. Теперь рассмотрим разложение корней по степеням q, где q — простой множитель числа n. Принадлежащие сюда корневые циклы подобны p-корневым циклам; но, кроме того, имеется два $\frac{m-n}{2}$-членных q-корневых цикла. Мы будем различать здесь два случая:

I. Если $m - n$ не является степенью числа 2, то $\frac{m-n}{2}$-членные циклы не благоприятны. Значит благоприятные циклы соответствуют значению $\rho = \frac{2\lambda - k_1}{2(q^\lambda - 1)}$; вследствие этого $u = q^{k_1} - 1$, т. е. $p = q$, что

невозможно, так как m и n взаимно просты. Если $p^k = 27$, $u = 8$, то $q^{k_1} = 9$, т. е. m и n опять-таки не взаимно просты.

II. $m - n = 2^s$. Корням уравнения (25) соответствуют либо A) значения $\rho = \pm \frac{k}{m-n}$, либо B) как значения $\rho = \frac{2\lambda - k_1}{2(q^\lambda - 1)}$, так и значения $\rho = \pm \frac{k}{m-n}$.

A. В первом случае либо $u = m - n$, либо $u = \frac{m-n}{2}$. Если $m \neq 27$, то либо $n = 1$, либо $m - 1 = \frac{m-n}{2}$, что, в силу $n \geqslant 1$, невозможно. Если же $m = 27$, то или $n = m - u = 19$, или $n = m - 2u = 11$.

1) $n = 1$, $k = 1$, $p = 1 + 2^s$. Уравнение (6) распадается по модулю 2 следующим образом:

$$(y^{\frac{p+1}{2}} - 1)(y^{\frac{p-1}{2}} - 1) \equiv 0 \pmod 2.$$

Так как здесь $u = m - 1$, то в благоприятном случае должны быть благоприятными все корневые циклы. Мы рассмотрим множитель $\varphi(y) = y^{\frac{p+1}{2}} - 1$. Он не имеет по модулю 2 кратных корней, так как полином

$$\varphi'(y) = \frac{p+1}{2} y^{\frac{p-1}{2}} \equiv y^{\frac{p-1}{2}} \pmod 2$$

в случае $p \equiv 1 \pmod 4$ взаимно прост с $\varphi(y)$. Известно,[1] что каждый неприводимый по модулю числа 2 полином k-й степени является делителем полинома $y^{2^k} - y$ и никакого другого полинома типа $y^{2^{k_1}} - y$ $(k_1 < k)$. Если бы все неприводимые по модулю 2 делители полинома $\varphi(y)$ были степени 2^w, то наименьший полином типа $y^{2^l} - y$, который делился бы на $\varphi(y)$, имел бы показатель l вида 2^t. Но полином $y^{2^l} - y = y(y^{2^l - 1} - 1)$ тогда и только тогда делится на полином $\varphi(y) = y^{2^{s-1}+1} - 1$ $\left(\frac{p+1}{2} = 2^{s-1} + 1\right)$, если $2^l - 1$ делится на $2^{s-1} + 1$. Теперь, $2^{2(s-1)} - 1$ делится на $2^{s-1} + 1$. С другой стороны, l не может быть меньше, чем $2s - 2$, так как в этом случае можно было бы положить $l = \varepsilon(s-1) + r$, $\varepsilon = 0$ или $= 1$, $r < s - 1$. Тогда имело бы место

$$2^l - 1 = 2^{\varepsilon(s-1)+r} - 1 \equiv \pm 2^r - 1 \pmod{2^{s-1} + 1},$$

что исключает делимость $2^l - 1$ на $2^{s-1} - 1$, так как $2^r \mp 1$ меньше, чем $2^{s-1} + 1$.

[1] Ср., например, [8], стр. 99 (56).

Итак, $l = 2s - 2$. Наше условие требует, чтобы $l = 2^t$. С другой стороны, $p = 2^s + 1$ может быть простым числом только тогда, если s имеет вид 2^α. Значит,

$$2^t = 2 \cdot 2^\alpha - 2,$$

т. е.

$$2^{t-1} = 2^\alpha - 1.$$

Это уравнение может иметь место только при $t - 1 = 0$. Тогда мы получаем

$$\alpha = 1, \qquad s = 2^\alpha = 2, \qquad p = 2^2 + 1 = 5.$$

К этому также можно добавить случай $p = 3$, в котором $2s - 2 = 0$. Все остальные случаи $m = p$, $n = 1$ не благоприятны.

2) $m = 9$, $n = 1$. Уравнение

$$\frac{x^9 - 1}{x - 1} \mp 3x^4 \frac{x - 1}{x - 1} = 0,$$

т. е.

$$x^8 + x^7 + x^6 + x^5 + (1 \pm 3)x^4 + x^3 + x^2 + x + 1 = 0 \qquad (32)$$

является возвратным и посредством преобразования $x + \frac{1}{x} = z$ превращается в уравнение

$$z^4 + z^3 - 3z^2 - 2z + (1 \pm 3) = 0. \qquad (33)$$

Если z_1, z_2, z_3, z_4 — корни этого уравнения, то величина $u = z_1 z_2 + z_3 z_4$ удовлетворяет кубическому уравнению

$$u^3 + 3u^2 + (-6 \mp 12)u - 17 \mp 39 = 0, \qquad (34)$$

которое имеет рациональные корни тогда и только тогда, если уравнение (33) [а следовательно, и (32)] решается в квадратных радикалах. Если в уравнении (34) мы возьмем верхний знак, то это уравнение имеет рациональный корень $u = -4$. Отсюда легко вытекает, что уравнение (33) допускает следующее разложение:

$$(z^2 - \varepsilon z - 2)(z^2 - \varepsilon^2 z - 2) = 0,$$

где $\varepsilon = e^{\frac{2\pi i}{3}}$. Значит, этот случай благоприятен, т. е. уравнение (32) при верхнем знаке решается в квадратных радикалах. Но этому решению не соответствует никакой луночки, так как все корни $z = x + \frac{1}{x} = 2\cos\theta$ уравнения (33) мнимы.

При нижнем знаке уравнение (34) не имеет рациональных корней.

3) $m = 27$, $n = 19$. Здесь мы имеем

$$(y^{23} - 1)(y^4 - 1) \equiv 0 \pmod 2.$$

Чтобы узнать, на какие неприводимые по модулю 2 множители распадается полином $y^{23} - 1$ по модулю 2, мы должны найти наименьший

показатель f, при котором $y^{2^f}-y$ делится на $y^{23}-1$. Для этого необходимо и достаточно, чтобы имело место

$$2^f \equiv 1 \pmod{23}.$$

Легко находим: $f=11$. Отсюда мы заключаем, что в этом случае корневые циклы 2-го рода по модулю 2 имеют степени 1, 1, 1, 1, 1, 11, 11. Степень $u=8$ не может быть составлена из этих степеней.

4) $m=27$, $n=11$. Корневые циклы по модулю 3 имеют степени 9, 9, 8, 1, а по модулю 11—степени 8, 10, 8, 1. Уравнение (25) в благоприятном случае должно иметь степень $u=8$. Тогда его корни соответствуют по модулю 11 одному из 8-членных циклов, для которого значение ρ или положительно, или отрицательно. Но уравнение (6)— возвратное; в случае, если корни его множителя $g(y)$ по модулю 11 имеют положительное значение ρ, то корни полинома $y^8 g\left(\frac{1}{y}\right)$, который во всяком случае входит множителем в уравнение (6), имеют отрицательное значение ρ и, значит, этот полином взаимно прост с $g(y)$. Отсюда следует, что уравнение (6) содержит два множителя восьмой степени с коэффициентами из $K\left(\sqrt{\frac{27}{11}}\right)$. Но это противоречит тому факту, что корневые циклы уравнения (6) по модулю 3 имеют степени 9, 9, 8, 1. Значит, случай $m=27$, $n=11$ не благоприятен.

В. В этом случае q должен подчиняться условиям § 2. 3, так что мы имеем только следующие подслучаи:

1) $m=p=1+2^{2^\alpha}$, $n=q=1+2^{2^\beta}$. Здесь $2^{2^\alpha}=2^{2^\beta}+2^s$, откуда следует

$$s=2^\beta,\ 2^{2^\alpha}=2^{2^\beta+1},\ 2^\alpha=1+2^\beta,\ \beta=0,\ \alpha=1,\ p=5,\ q=3.$$

Этот случай упоминает уже Клаузен (loc. cit.).

2) $m=9$, $n=9$, $9-q=2^s$. Здесь $q=5$, т. е. $m=9$, $n=5$. Уравнение (6) распадается по модулю 2 следующим образом:

$$(y^7-1)(y^2-1)\equiv 0 \pmod 2.$$

Полином y^7-1 распадается по модулю 2 на не приводимые по модулю 2 полиномы степеней 1, 3, 3, что противоречит тому факту, что здесь $u=9-1=8$.

3) $m=p$, $n=9$, $2^{2^\alpha}+1=2^3+1+2^s$, $s=3$, $\alpha=2$, $p=17$.

Отсюда следует: $m=17$, $n=9$. Уравнение (6) распадается по модулю 2 следующим образом:

$$(y^{13}-1)(y^4-1)\equiv 0 \pmod 2.$$

Так как 2 принадлежит по модулю 13 к показателю 12, то это уравнение по модулю 2 распадается на не приводимые по модулю 2 мно-

жители степеней 12, 1, 1, 1, 1, 1. Это противоречит тому, что здесь $u = 17 - 1 = 16$.

4) $m = 27$, $n = q$. Здесь $27 = 2^{2^\beta} + 1 + 2^s$, $2^s + 2^{2^\beta} = 26$.

Отсюда следует, в силу $26 \equiv 2 \pmod 4$, что или $s = 1$, или $2^\beta = 1$. Оба случая невозможны, так как число $26 - 2 = 24$ не является степенью 2.

5) $m = p$, $n = 27$. Здесь $2^{2^\alpha} + 1 = 2^s + 27$, $2^{2^\alpha} - 2^s = 26$, $s = 1$, $2^{2^\alpha} = 28$, что снова невозможно.

В случае B, n может состоять из различных простых множителей. Это дает нам следующие подслучаи:

6) $m = p$, $n = q^{k_1} \cdot q_1 \cdot q_2 \ldots$. В этом случае $u = p - 1$, т. е. уравнение (25) охватывает все корневые циклы, которые по модулям q, q_1, $q_2, \ldots$ не все благоприятны. Значит, этот случай не благоприятен.

7) $m = 3^k$, $n = q^{k_1} \cdot q_1 \cdot q_2 \ldots$ В этом случае $m < n$ (наименьшее значение n есть $5 \cdot 7 = 35$), что противоречит нашим условиям.

Поступило
20 февраля 1933 года

ЛИТЕРАТУРА

1. E. Landau. Über quadrierbare Kreisbogenzweiecke. Sitzber. Berl. Math. Ges. **2** (1903) стр. 1 — 6.
2. L. Tschakaloff. Beitrag zum Problem der quadrierbaren Kreisbogenzweiecke. Math. Ztschr. **30** (1929), стр. 552 — 559.
3. L. Tschakaloff. Anwendung der Theorie der algebraischen Zahlen usw. C. R. du Premier Congrès des Pays Slaves, Warszawa, 1930, стр. 134 — 139.
4. Clausen. Vier neue mondförmige Flächen, deren Inhalt usw. Journ. f. Math. **21** (1840), стр. 375 — 376.
5. M. Bauer. Zur allgemeinen Theorie der algebraischen Grössen. Journ. f. Math. **132** (1907), стр. 21 — 32.
6. M. Bauer. Ganzzahlige Gleichungen ohne Affekt. Math. Ann. **64** (1907).
7. Ö. Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. Math. Ann. **99** (1928), стр. 99 — 100, Satz 1.
8. P. Bachmann. Zahlentheorie. Bd. 5, Lpz., 1905, стр. 494, 495.

ЗАМЕТКИ ПО АЛГЕБРЕ И ТЕОРИИ ЧИСЕЛ

(Уч. зап. КГУ, **94**, кн. 7, стр. 3—16)

I. О «теореме главных идеалов» в промежуточных полях

Ф. Фуртвенглер (Ph. Furtwängler) доказал «теорему главных идеалов» (Hauptidealsatz) для полного поля классов (Klassenkörper). [1]. Э. Артин (E. Artin) поставил вопрос о том, какие идеалы первоначального поля k обращаются в главные внутри частичного поля классов [2]. Повидимому, эта задача не допускает простого решения и зависит не только от группы поля k, но также от его арифметических свойств [3].

В настоящей заметке я предлагаю существенно новую групповую интерпретацию этой проблемы. Г. Гассе (H. Hasse) указал мне на эту проблему и сделал по поводу настоящей заметки ряд ценных указаний, за что я выражаю ему мою сердечную признательность.

§ 1. Постановка вопроса. В дальнейшем я буду пользоваться обозначениями цитированной статьи Фуртвенглера [1], если только не будет оговорено противное.

Пусть k будет первоначальное алгебраическое поле, $H = [c_1, c_2, \ldots, c_n]$ — его группа идеальных классов, H_1 — подгруппа группы H. Пусть K_1 будет (частичное) поле классов, соответствующее группе H_1, и K_2 — полное поле классов поля K_1. Тогда относительное поле K_2/k — нормально. Пусть G будет его группа и $\mathfrak{H}$ та ее подгруппа, к которой принадлежит K_1, $G/\mathfrak{H}$ — изоморфна с группой H/H_1.

Пусть $\overline{K}$ будет полное поле классов поля k. Очевидно, что $\overline{K}$ содержится в K_2. Пусть $\overline{K}$ принадлежит внутри K_2 к группе L. Так как все рассматриваемые относительные поля не разветвлены (т. е. их относительные дискриминанты равны единице), то L является коммутантом группы G. В самом деле, принадлежащее к L поле $\overline{K}/k$ является наибольшим абелевым делителем поля $\frac{K_2}{k}$, а потому L есть наименьший делитель группы G такого рода, что дополнительная группа G/L абелева. Группа G/L изоморфна с полной группой идеальных классов H.

Пусть P будет простой идеал поля k, лежащий в идеальном классе c_1 и P_1, $\overline{P}$ и P_2 — его простые идеальные множители соответст-

венно внутри K_1, $\overline{K}$ и K_2. Если P_2 принадлежит внутри $\frac{K_2}{k}$ к подстановке X группы G, то, как известно, имеет место

$$A_2^{N(P)} \equiv A_2^X \pmod{P_2}, \tag{1}$$

где A_2 — произвольное взаимно простое с P целое число поля K_2. Если мы в качестве A_2 возьмем число $\overline{A}$ из $\overline{K}$, то получим

$$\overline{A}^{N(P)} \equiv \overline{A}^X \pmod{P}. \tag{2}$$

Но так как P лежит в идеальном классе c_1, то, в силу артиновского закона взаимности [4] (который мы в дальнейшем будем для краткости обозначать буквами А. З. В.), следует, что подстановка X соответствует идеальному классу c_1 при изоморфном сопоставлении элементов групп $\frac{G}{L}$ и H. Если записать группу G в виде

$$G = S_1^{a_1} \cdot S_2^{a_2} \ldots S_n^{a_n} L \qquad (S_i \longleftrightarrow c_i), \tag{3}$$

где $a_1, a_2, \ldots, a_n$ пробегают независимо друг от друга значения от 0 до $h_1 - 1$, $h_2 - 1, \ldots, h_n - 1$, где $h_1, h_2, \ldots, h_n$ — порядки элементов $S_1, S_2, \ldots, S_n$, то из наших рассуждений вытекает, что X лежит в смежном классе $S_1 L$, и потому можно принять $X = S_1$, и мы будем иметь

$$A_2^{N(P)} \equiv A_2^{S_1} \pmod{P_2}. \tag{4}$$

Таким образом, если e_k есть порядок элемента $c_k H_1$ [т. е. наименьший показатель, для которого $c_k^{e_k}$ содержится в H_1; введем обозначение $e_k = \text{Пор}(c_k H_1)$], то из закона разложения [5] следует

$$N(P_1) = [N(P)]^{e_1}. \tag{5}$$

Возвышая обе части сравнения (4) в e_1-ю степень, мы получим

$$A_2^{N(P)} \equiv A_2^{S_1^{e_1}} \pmod{P_2}, \tag{6}$$

а для чисел A_1 из K_1 даже

$$A_1^{N(P_1)} \equiv A_1^{S_1^{e_1}} \pmod{P_1}. \tag{6'}$$

Отсюда следует, что P_1 лежит внутри K_1 в идеальном классе, соответствующем подстановке $S_1^{e_1}$. Но так как, в силу закона разложения, имеет место

$$\mathfrak{p} = P_1 \cdot P_2^{\sigma_2} \ldots P_k^{\sigma_k} = P_1^{G/\mathfrak{H}f_1}, \tag{7}$$

где

$$f_1 = 1 + S_1 + \ldots + S_1^{e_1 - 1},$$
$$G = \mathfrak{H}f_1 + \mathfrak{H}f_1\sigma_2 + \ldots + \mathfrak{H}f_1\sigma_k,$$

где G/Gf_1 обозначает сумму представителей смежных классов разложения G по $\mathfrak{H}f_1$, то G лежит внутри K_1 в идеальном классе, соответствующем подстановке

$$\tau_1 = S_1^{e_1 \frac{G}{\mathfrak{H}f}}. \tag{8}$$

Способ записи и рассуждения заимствованы из [1].)

Принимая во внимание, что группу $G/\mathfrak{H}$ можно записать так:

$$\frac{G}{\mathfrak{H}} = f_1 \cdot f_2 \cdots f_k, \tag{9}$$

и что возведение (символическое) S_1 в степень f_1 равносильно возведению S_1 в e_1-ю степень в обыкновенном смысле:

$$S_1^{f_1} = S_1^{1+S_1+S_1^2+\cdots+S_1^{e_1-1}} = S_1 \cdot S_1^{S_1} \cdot S_1^{S_1^2} \cdots S_1^{S_1^{e_1-1}} =$$

$$= S_1 \cdot S_1 \cdots S_1 = S_1^{e_1}$$

(под S^T мы разумеем $T^{-1}ST$, так что $S^S = S$), мы можем даже переписать равенство (8) так:

$$\tau_1 = S^{G/\mathfrak{H}}, \tag{8'}$$

если только мы условимся под показателем $G/\mathfrak{H}$ разуметь выражение (9), причем порядок возведения в степени $f_1, f_2, \ldots, f_n$ не безразличен. Именно, надо всегда начинать с возведения в степень той f_1, которая соответствует циклической группе, содержащей S_1.

В общем случае, если какой-нибудь идеальный класс внутри k соответствует элементу X группы $G/\mathfrak{H}$, то, чтобы найти тот идеальный класс, в который превращается наш идеальный класс внутри K_1, надо разложить $G/\mathfrak{H}$ (абелева группа) в прямое произведение типа (9) таким образом, чтобы один из циклических множителей содержал элемент X (из теории абелевых групп известно, что это всегда можно выполнить). Чтобы получить ту подгруппу группы классов поля K_1, которая производится идеалами поля k, надо символически возвести каждый элемент X группы G в символическую степень $G/\mathfrak{H}$, в первую очередь возвышая X в степень того циклического множителя, который содержит X. Это возведение сразу переводит X в элемент группы $\mathfrak{H}$, с которой, в силу А. З. В., сопоставляется группа идеальных классов поля K. Порядок остальных символических возведений в степени безразличен ввиду того, что $X^{f_1} = H$ есть элемент группы $\mathfrak{H}$, а также коммутативности группы $G/\mathfrak{H}$, из которой следует

$$S_1 S_2 = H_1 S_2 S_1,$$

где S_1, S_2 входят в G, а H_1 — в $\mathfrak{H}$. Отсюда

$$H^{S_1 S_2} = H^{H_1 S_2 S_1} = H^{S_2 S_1}.$$

Это равенство влечет за собой перестановочность всех f_i в показателе:

$$H^{f_i f_j} = H^{f_j f_i}.$$

Итак, классам поля K_1, производимым идеалами поля k, соответствуют (на основании А. З. В.) те подстановки группы $\mathfrak{H}$, которые выражаются как произведения *символических норм* элементов группы G, т. е.

$$X^{G/\mathfrak{H}}. \tag{10}$$

Из них делаются главными внутри K_1 те идеальные классы, которым соответствуют подстановки X группы G $\left(\text{вернее, } \frac{G}{\mathfrak{H}}\right)$, удовлетворяющие равенству

$$X^{G/\mathfrak{H}} = 1. \tag{11}$$

§ 2. Свойства символических норм. Пусть $A_1, A_2, \ldots, A_r$ будут элементы базиса абелевой группы $\mathfrak{H}$. Элементы группы $\frac{G}{\mathfrak{H}}$ можно рассматривать как автоморфизмы группы $\mathfrak{H}$. Пусть S — какой-нибудь из таких автоморфизмов, т. е. элемент из G, который будем считать единичным, если он содержится в $\mathfrak{H}$ (тогда преобразование с его помощью будет оставлять элементы группы $\mathfrak{H}$ инвариантными). Пусть m-я степень S впервые дает элемент из $\mathfrak{H}$; пусть $m = m_1 p$, где p — простое число. Тогда элемент $s = S^{m_1}$ имеет относительный порядок p. Рассмотрим сначала автоморфизм s. Вводя обозначение

$$f = 1 + s + s^2 + \ldots + s^{p-1},$$

рассмотрим символические степени

$$A_1^f, A_2^f, \ldots, A_r^f,$$

производящие группу, которую мы будем обозначать так: $\mathfrak{H}^f$.

Пусть $\mathrm{Ord}(A_i) = e_i$ и пусть $e_i = e_i' p$ в случае, если e_i делится на p, и $e_i = e_i'$ в противоположном случае. Введем обозначения

$$B_i = A_i^{e_i'} \qquad (i = 1, 2, \ldots, r).$$

Подгруппа $[B_1, B_2, \ldots, B_r]$ есть абелева группа порядка p^r и типа $[1, 1, \ldots, 1]$ (т. е. все ее элементы имеют порядок p). Автоморфизм s производит над ее элементами однородную линейную подстановку по модулю p.

Это дает представление s в виде однородной линейной подстановки по модулю p. Из $s^p = 1$ следует, что все характеристические числа матрицы, соответствующей этой подстановке, удовлетворяют сравнению

$$x^p \equiv 1 \pmod{p},$$

откуда $x \equiv 1 \pmod{p}$. Поэтому при помощи линейного преобразования над $B_1, B_2, \ldots, B_r$ с рациональными (целыми) коэффициентами мы

можем привести эту матрицу к виду

$$R=\left\|\begin{matrix} R_1, 0, \ldots, 0 \\ 0, R_2, \ldots, 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0, 0, \ldots, R_t \end{matrix}\right\|, \tag{12}$$

где матрицы $R_1, R_2, \ldots, R_t$ имеют вид

$$R_k=\left\|\begin{matrix} 1, \lambda, 0, \ldots, 0 \\ 0, 1, \lambda, \ldots, 0 \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0, 0, 0, \ldots, 1 \end{matrix}\right\| \qquad (k=1, 2, \ldots, t) \tag{13}$$

и порядки $u_k \leqslant p$. Рассмотрим два случая.

I. $u<p$. Пусть элементы $B_1, B_2, \ldots, B_u$ нашей подгруппы претерпевают под влиянием автоморфизма s подстановку R_1 вида (13). Это означает, что под влиянием автоморфизма s эту подстановку претерпят показатели $x_1, x_2, \ldots, x_u$ элемента $C=B_1^{x_1}B_2^{x_2}\ldots B_u^{x_u}$. Тогда показатели элемента

$$C^f=C\cdot C^s\cdots C^{s^{p-1}}$$

могут быть представлены в виде

$$(x_1, x_2, \ldots, x_u)(E+R_1+R_1^2+\ldots+R_1^{p-1}).$$

Докажем, что все элементы матрицы $E+R_1+R_2^2+\ldots+R_1^{p-1}$ делятся на p. В самом деле, легко проверить путем индукции справедливость формулы

$$R_1^m=\left\|\begin{matrix} 1, \binom{m}{1}\lambda, \binom{m}{2}\lambda^2, \ldots \\ 0, \quad 1, \quad \binom{m}{1}\lambda, \ldots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0, \quad 0, \quad 0, \ldots \quad 1 \end{matrix}\right\| \qquad (m=1, 2, \ldots, p-1), \tag{14}$$

где $\binom{m}{k}=C_m^k$ биномиальные коэффициенты. Из этой формулы мы получаем

$$E+R_1+R_1^2+\ldots+R_1^{p-1}=$$

$$=\left\|\begin{matrix} p, \lambda\sum_{m=1}^{p-1}\binom{m}{1}, \lambda^2\sum_{m=1}^{p-1}\binom{m}{2}, \ldots, \lambda^{u-1}\sum_{m=1}^{p-1}\binom{m}{u-1} \\ 0, \quad p, \quad \lambda\sum_{m=1}^{p-1}\binom{m}{1}, \ldots, \lambda^{u-2}\sum_{m=1}^{p-1}\binom{m}{u-2} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0, \quad 0, \quad 0, \quad \ldots, \quad p \end{matrix}\right\|, \tag{15}$$

если принять обозначение $\binom{m}{k} = 0$ при $k > m$. Но сумма

$$\sum_{m=1}^{p-1} \binom{m}{a}$$

равна коэффициенту при x^a в разложении суммы

$$1 + (1+x) + (1+x)^2 + \ldots + (1+x)^{p-1} = \frac{(1+x)^p - 1}{x},$$

по степеням x. Отсюда следует:

$$\sum_{m=1}^{p-1} \binom{m}{a} = \binom{p}{a+1}. \tag{16}$$

Но $\binom{p}{a+1}$, в силу $a \leqslant u - 1 < p - 1$, делится на p, откуда мы заключаем, что C^f в этом случае равно единице. Из этого следует, что группа $\mathfrak{H}^f$ содержится в группе $\mathfrak{H}^p$, т. е. группе, элементы которой состоят из p-тых степеней элементов группы $\mathfrak{H}$.

II. Некоторые из матриц R_k суть матрицы порядка p. Это означает, что элементы $B_1, B_1^s, \ldots, B_1^{s^{p-1}}$ независимы друг от друга и могут быть выбраны в качестве элементов базиса. В самом деле,

$$\begin{aligned}
B_1^s &= B_1 \cdot B_2^{\lambda}, \\
B_1^{s^2} &= B_1 \cdot B_2^{2\lambda} \cdot B_3^{\lambda^2}, \\
B_1^{s^3} &= B_1 \cdot B_2^{3\lambda} \cdot B_3^{3\lambda^2} \cdot B_4^{\lambda^3}, \\
&\cdots\cdots\cdots\cdots \\
B_1^{s^{p-1}} &= B_1 \cdot B_2^{(p-1)\lambda} \cdot B_3^{\frac{(p-1)(p-2)}{2}\lambda^2} \cdots B_{p-1}^{(p-1)\lambda^{p-2}} \cdot B_p^{\lambda^{p-1}}.
\end{aligned} \tag{17}$$

Так как $\lambda \not\equiv 0 \pmod{p}$, то при помощи этих формул можно последовательно выразить $B_1, B_2, \ldots, B_p$ через $B_1, B_1^s, \ldots B_1^{s^{p-1}}$.

Будем обозначать $B_1, B_1^s, \ldots, B_1^{s^{p-1}}$ через $C, C_1, \ldots, C_{p-1}$. Тогда

$$C_i^f = C_i \cdot C_i^s \cdot C_i^{s^2} \cdots C_i^{s^{p-1}} = B_1 \cdot B_1^s \cdot B_1^{s^2} \cdots B_1^{s^{p-1}},$$

т. е.

$$C_0^s = C_1^s = \cdots = C_{p-1}^s.$$

Таким образом, в этом случае каждым p членам базиса группы $\mathfrak{H}$ соответствует только один элемент в группе $\mathfrak{H}^f$ того же порядка, так что здесь хотя порядки отдельных элементов группы могут все и не уменьшаться, но порядок всей группы уменьшится по крайней мере в p^{p-1} раз.

Перейдем к рассмотрению более общего случая, когда (относительный) порядок автоморфизма S есть произвольное составное число

$m = p_1 p_2 \cdots p_v$ (его множители могут быть и равными). Для этого рассмотрим сначала автоморфизм $s = S^{\frac{m}{p_1}}$,

$$f_1 = 1 + S + \ldots + S^{p_1 - 1}.$$

В силу только что доказанного, группа $\mathfrak{H}^{f_1}$ или является делителем $\mathfrak{H}^p$, или (случай II) содержит только один элемент базиса, не входящий в $\mathfrak{H}^p$. Кроме того, очевидно, что элементы группы $\mathfrak{H}^{f_1}$ инвариантны по отношению к автоморфизму $s = S^{\frac{m}{p_1}}$, в силу чего по отношению к группе $\mathfrak{H}^{f_1}$ автоморфизм S имеет (относительный) порядок m/p_1. Проделывая этот процесс с автоморфизмом $S^{m/p_1 p_2}$, мы убедимся, что элементы базиса группы $\mathfrak{H}^{f_1 f_2}$ содержатся в группе $\mathfrak{H}^{p_1 p_2}$, за исключением самое большее или одного элемента, являющегося элементом базиса первоначальной группы $\mathfrak{H}$, или двух элементов, из которых один входит в группу $\mathfrak{H}^{p_1}$, а другой в группу $\mathfrak{H}^{p_2}$. Продолжая процесс, мы получим аналогичный результат для общего автоморфизма S.

Обратим внимание на то, что в том случае, если некоторые из простых чисел $p_1, p_2, \ldots, p_v$ совпадают, символический показатель в символической норме будет иметь тот же вид, что и $f_1 f_2 \cdots f_v$. Разъясним дело на примере. Пусть S имеет (относительный) порядок p^2. Показатель в символической норме имеет вид

$$1 + S + S^2 + \ldots + S^{p^2 - 1}, \tag{18}$$

у нас же получится выражение

$$(1 + S^p + S^{2p} + \ldots + S^{(p-\lambda)p})(1 + S + S^2 + \ldots + S^{n-1}). \tag{19}$$

Но нетрудно доказать, что оба выражения (18) и (19) даже алгебраически равны друг другу. Аналогично доказывается общее утверждение.

Если $\mathfrak{H}$ совпадает с коммутантом группы G, что соответствует случаю полного поля классов, то Фуртвенглер [1] доказал, что в этом случае символическая норма группы $\mathfrak{H}$ есть единичная группа. В общем случае эта символическая норма зависит от индивидуальных особенностей *двустепенной группы* G, в рассмотрение которых я не вхожу в настоящей заметке.

II. К гильбертовой теореме неприводимости для многих переменных

Предполагая, что теорема Гильберта доказана для случая одной переменной, докажем ее для случая многих переменных.

Пусть нам задано абсолютно неприводимое уравнение

$$f(x_1, x_2, \ldots, x_m; y_1, y_2, \ldots, y_n) = 0. \tag{1}$$

Требуется доказать, что можно придать переменным $x_1, x_2, \ldots, x_m$ такие рациональные значения, чтобы получаемое после их подстановки в (1) уравнение было неприводимо относительно $y_1, y_2, \ldots, y_n$ в любом наперед заданном конечном алгебраическом поле K.

Что касается абсолютной неприводимости, то ее не всегда можно достичь. В виде примера рассмотрим уравнение

$$y_1^2 - x_1^3 y_2^2 = 0, \tag{2}$$

которое абсолютно неприводимо относительно переменных x_1, y_1, y_2, но всегда абсолютно приводимо относительно y_1, y_2, если мы придадим x_1 какое бы то ни было рациональное значение.

Будем считать левую часть уравнения (1) полиномом относительно $y_1, y_2, \ldots, y_n$, а переменные $x_1, x_2, \ldots, x_m$ будем считать параметрами включенными в коэффициенты полинома. Если этот полином абсолютно приводим, то между его коэффициентами имеют место некоторые соотношения, которые мы будем называть уравнениями (R). Нетрудно понять, как получить эти соотношения. Для этого приравняем полином $f(y_1, y_2, \ldots, y_n)$ произведению двух полиномов той же степени относительно каждой из переменных $y_1, y_2, \ldots, y_n$ с неопределенными коэффициентами:

$$f(y_1, y_2, \ldots, y_n) = \varphi(y_1, y_2, \ldots, y_n)\,\psi(y_1, y_2, \ldots, y_n). \tag{3}$$

Пусть $u_1, u_2, \ldots$ будут коэффициенты полинома φ и $v_1, v_2, \ldots$ — полинома ψ. Приравнивая коэффициенты при различных степенях переменных $y_1, y_2, \ldots, y_n$ в тождестве (3), мы получим систему соотношений между коэффициентами u_i и v_i

$$g_i(u_1, u_2, \ldots; v_1, v_2, \ldots) = 0. \tag{4}$$

Эта система имеет всегда тривиальное решение, соответствующее случаю, когда один из полиномов φ, ψ равен постоянной величине. Чтобы получить остальные решения, исключим из системы (4) неизвестные u_i и v_i. Получится система соотношений между коэффициентами полинома f, которую мы и назовем системой уравнений (R). Так как, в силу нашего предположения, в коэффициенты полинома f входят переменные $x_1, x_2, \ldots, x_m$, то уравнения (R) являются уравнениями, связывающими эти переменные.

Рассмотрим отдельно два случая:

I. Уравнения (R) не все являются тождествами относительно переменных $x_1, x_2, \ldots, x_m$. В этом случае всегда можно найти такую систему значений для переменных, чтобы не все уравнения (R) удовлетворялись. Такая система значений делает полином f абсолютно неприводимым относительно переменных

$$y_1, y_2, \ldots, y_n.$$

II. Уравнения (R) являются тождествами относительно переменных $x_1 x_2, \ldots, x_m$. Так как эти уравнения являются условиями совместимости уравнений (4), то в этом случае уравнения (4) непременно имеют решения, отличные от тривиального. Рассматривая поле $K[x_1, x_2, \ldots, x_n]$ (получаемое присоединением к полю K переменных $x_1, x_2, \ldots x_m$) как область рациональности, мы получим решения u_i и v_i системы (4) в некотором алгебраическом относительно $K[x_1, x_2, \ldots, x_m]$ поле (это следует из того, что число возможных разложений полинома f — конечное, с точностью до постоянной величины; последнюю нетрудно нормировать, например потребовав, чтобы свободный член полинома φ равнялся единице) $K[x_1, x_2, \ldots, x_m; u_i, v_j]$, которое мы будем называть *полем разложимости* полинома f. Выберем в этом поле примитивную величину z, через которую и через величины $x_1, x_2, \ldots, x_m$ должны рационально выражаться величины u_i, v_j. Величина z является непременно *иррациональной функцией* от $x_1, x_2, \ldots, x_m$. В самом деле, в противном случае величины u_i, v_j рационально бы выражались через $x_1, x_2, \ldots, x_m$, а это означало бы, что полином f разлагался бы на множители, коэффициенты которых были бы рациональными функциями от $x_1, x_2, \ldots, x_m$; другими словами, полином $f(x_1, x_2, \ldots x_m; y_1, y_2, \ldots, y_n)$ был бы приводимым относительно переменных $x_1, x_2, \ldots, x_m; y_1, y_2, \ldots, y_n$, что противоречит предположению.

Лемма Гаусса стирает здесь грань между рациональностью и целой рациональностью коэффициентов.

Пусть

$$F(z; x_1, x_2, \ldots, x_m) = 0 \tag{5}$$

абсолютно неприводимый полином, корнем которого является z. Из иррациональности z следует, что степень полинома F относительно z должна быть выше первой.

Станем рассматривать одно из неизвестных в уравнении (5), например x_m, как параметр, который мы включим в коэффициенты уравнения (5). Здесь опять мы должны рассмотреть два случая. Если уравнение (5) абсолютно неприводимо относительно переменных $z; x_1, x_2, \ldots, x_{m-1}$, то, поступая, как в I, мы найдем для x_m такое численное значение, при котором F останется абсолютно неприводимым относительно остальных переменных. В противном случае, поступая, как в II, обозначим через ξ примитивную величину поля разложимости полинома F и через

$$h(\xi; x_m) = 0 \tag{6}$$

абсолютно неприводимое уравнение, корнем которого является ξ. Опять мы убедимся, что уравнение (6) выше первой степени относительно ξ. Поэтому в силу теоремы Гильберта для одной переменной

можно придать переменной x_m такое значение, чтобы уравнение (6) осталось неприводимым относительно ξ внутри заданного поля K. Пусть K_2 будет поле, образованное корнем уравнения (6). Тогда (5) имеет корнями или иррациональные функции от $x_1, x_2, \ldots, x_{m-1}$ (если уравнение (5) не имеет линейного множителя), или рациональные функции, коэффициенты которых принадлежат к полю K_2. Эти коэффициенты воспроизводят *все* поле K_2, так как ξ, в силу нашего условия, рационально выражается через эти коэффициенты. Но так как коэффициенты уравнения (5) принадлежат полю K, то, беря в качестве коэффициентов одной из этих рациональных функций сопряженные по отношению к K величины, мы получим другие корни уравнения (5). Если мы придадим переменным $x_1, x_2, \ldots, x_{m-1}$ какие-нибудь рациональные значения, то получаемые при этом значения корней уравнения (5) только тогда могут лежать в поле K, если они совпадают друг с другом, а это может случиться только тогда, если дискриминант уравнения (5) обращается в нуль. Но этот дискриминант есть полином $D(x_1, x_2, \ldots, x_{m-1})$, не обращающийся тождественно в нуль, так как уравнение (5) неприводимо. Если мы в связи с этим наложим на выбираемое значение x_m дополнительное условие, чтобы его подстановка не обращала D тождественно в нуль (это всегда возможно, так как этим мы исключаем лишь конечное число значений x_m), и после этого выберем систему значений $x_1, x_2, \ldots, x_{m-1}$, не обращающих D в нуль, то корень z уравнения (6) не будет лежать в поле K. Отсюда вытекает, что при этих значениях $x_1, x_2, \ldots, x_m$ полином f останется неприводимым в поле K, что и т. д.

Возвращаясь к случаю, когда уравнение (5) осталось абсолютно неприводимым (или, во всяком случае, не имело линейных относительно z множителей), мы продолжим наше рассуждение относительно переменной x_{m-1}, а затем x_{m-2}, и т. д.

III. К одной теореме Минковского

Г. Минковский доказал теорему:

Дано n вещественных линейных функций

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_1, \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n + b_2, \\ &\cdots\cdots\cdots\cdots\cdots \\ y_n &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n + b_n \end{aligned} \tag{1}$$

от n переменных $x_1 x_2, \ldots, x_n$ с определителем D. Существуют целочисленные значения $x_1, x_2, x_3, \ldots, x_n$ такого рода, что для них

$$| y_1 \cdot y_2 \cdots y_n | \leqslant \frac{D}{2^n} \tag{2}$$

для случая $n=2$ [6] Р. Ремак доказал ее справедливость для $n=3$ [7]. Эти доказательства имеют геометрический характер и довольно сложны. Я намерен здесь предложить два простых результата, относящихся к этой теореме для произвольного n. Они далеко не доказывают теоремы Минковского, но, имея весьма простые чисто арифметические доказательства, может быть, представят некоторый интерес.

§ 1

I. Теорема Минковского справедлива, если предположить, что отношения чисел a_{ij} в каждой строке системы (1) рациональны.

Доказательство. Предварительно примем во внимание, что если теорема доказана для каких-нибудь функций $y_1, y_2, \ldots, y_n$, то она справедлива также для функций $c_1y_1, c_2y_2, \ldots, c_ny_n$, где $c_1, c_2, \ldots, c_n$ — совершенно произвольные вещественные числа. Исходя из этого, мы можем предположить, что все коэффициенты a_{ij} суть целые рациональные числа.

Пусть a_n будет наименьшее по абсолютной величине из чисел $a_{11}, a_{12}, \ldots, a_{1n}$ (этого можно добиться, изменяя нумерацию переменных $x_1, x_2, \ldots, x_n$). Найдем целые числа $q_2, q_3, \ldots, q_n$ такого рода, чтобы

$$|r_2| = |a_{12} - q_2a_{11}| < \tfrac{1}{2}|a_{11}|, |r_3| = |a_{13} - q_3a_{11}| < \tfrac{1}{2}|a_{11}|, \ldots,$$
$$|r_n| = |a_{1n} - q_na_{11}| < \tfrac{1}{2}|a_{11}|. \qquad (3)$$

Тогда

$$y_1 = a_{11}x_1 + (q_2a_{11} + r_2)x_2 + \ldots + (q_na_{11} + r_n)x_n + b_1 =$$
$$= a_{11}(x_1 + q_2x_2 + \ldots + q_nx_n) + r_2x_2 + \ldots + r_nx_n + b_1.$$

Сделаем в системе (1) замену переменных

$$z_1 = x_1 + q_2x_2 + \ldots + q_nx_n, z_2 = x_2, \ldots, z_n = x_n,$$

которая обратима в целых числах. Тогда коэффициенты функции y_1 уменьшатся по абсолютному значению. Продолжая процесс, мы приведем y_1 к виду c_1u_1. Применяя эти преобразования к y_2, затем к y_3 и т. д., мы в конце концов приведем систему (1) к виду

$$\begin{aligned} y_1 &= c_{11}u_1 + b_1, \\ y_2 &= c_{21}u_1 + c_{22}u_2 + b_2, \\ &\ldots\ldots\ldots\ldots \\ y_n &= c_{n1}u_1 + c_{n2}u_2 + \ldots + c_{nn}u_n + b_n, \end{aligned} \qquad (4)$$

где $|D| = |c_{11}c_{22}\ldots c_{nn}|$. Переменные $x_1, x_2, \ldots, x_n$ и $u_1, u_2, \ldots, u_n$ принимают целые значения одновременно.

Найдем для u_1 такое целое значение, чтобы имело место

$$|y_1| \leqslant \tfrac{1}{2}|c_{11}|.$$

Подставляя значение u_1 в остальные функции y_1, подберем u_2 так, чтобы

$$|y_2|<\frac{1}{2}|c_{22}|.$$

Продолжая процесс, получим систему таких целых значений $u_1, u_2, \ldots, u_n$, чтобы имело место

$$|y_1|\leqslant\frac{1}{2}|c_{11}|, |y_2|\leqslant\frac{1}{2}|c_{22}|, \ldots, |y_n|\leqslant\frac{1}{2}|c_{nn}|, \tag{5}$$

откуда

$$|y_1y_2\ldots y_n|\leqslant\frac{1}{2^n}|c_{11}c_{22}\cdots c_{nn}|=\frac{1}{2^n}|D|,$$

что и т. д.

§ 2

II. В общем случае произведение $|y_1, y_2, \ldots, y_n|$ может быть при целых значениях $x_1, x_2, \ldots, x_n$ сделано меньше λ, где λ — число, сколь угодно близкое к $\frac{D}{(\sqrt{2})^n}$.

Доказательство. Если мы будем придавать $x_1, x_2, \ldots, x_n$ всевозможные целочисленные значения, то произведение $|y_1y_2\cdots y_n|$ будет принимать некоторое множество значений. Пусть L — нижний предел (может быть, недостижимый) этого множества.[1] Достаточно доказать, что

$$L\leqslant\frac{1}{2^{\frac{n}{2}}}|D|. \tag{6}$$

Допустим противное. Выберем систему целых значений $x_1, x_2, \ldots, x_n$, для которых значения $y_1, y_2, \ldots, y_n$ удовлетворяют неравенствам

$$L\leqslant|y_1y_2\cdots y_n|<L+\varepsilon, \tag{7}$$

где ε — сколь угодно малое положительное число.

С другой стороны, если $\xi_1, \xi_2, \ldots, \xi_n$ — система произвольных целых значений, то

$$y_i(x_1+\xi_1, x_2+\xi_2, \ldots, x_n+\xi_n)=(a_{i1}x_1+\ldots+a_{in}x_n+b_i)+$$
$$+(a_{i1}\xi_1+\ldots+a_{in}\xi_n)=y_i+\eta_i,$$

где η_i — значение однородной части функции $y_i(x_1, \ldots, x_n)$, соответствующее значениям $x_i=\xi_i$. Согласно определению L, будем иметь

$$|(y_1+\eta_1)(y_2+\eta_2)\cdots(y_n+\eta_n)|\geqslant L. \tag{8}$$

[1] Идея рассмотрения нижнего предела принадлежит Н. Н. Мейману.

Деля (8) на (7), получим

$$\left|\left(1+\frac{\eta_1}{y_1}\right)\left(1+\frac{\eta_2}{y_2}\right)\cdots\left(1+\frac{\eta_n}{y_n}\right)\right|>\frac{L}{L+\varepsilon}. \tag{9}$$

В силу произвольности $\xi_1, \xi_2, \ldots \xi_n$ берем в их роли $-\xi_1, -\xi_2, \ldots, -\xi_n$, и тогда получим вместо $\eta_1, \eta_2, \ldots, \eta_n$ величины $-\eta_1, -\eta_2, \ldots, -\eta_n$. Для них тоже имеет место неравенство (9):

$$\left|\left(1-\frac{\eta_1}{y_1}\right)\left(1-\frac{\eta_1}{y_2}\right)\cdots\left(1-\frac{\eta_n}{y_n}\right)\right|>\frac{L}{L+\varepsilon}. \tag{10}$$

Перемножая (9) и (10), получим

$$\left|\left(1-\frac{\eta_1^2}{y_1^2}\right)\left(1-\frac{\eta_2^2}{y_2^2}\right)\cdots\left(1-\frac{\eta_n^2}{y_n^2}\right)\right|>\frac{L^2}{(L+\varepsilon)^2}. \tag{11}$$

Введем обозначение

$$L:\frac{1}{2^{\frac{n}{2}}}|D|=a^n, \tag{12}$$

так что, в силу нашего предположения, имеет место

$$a>1. \tag{13}$$

В силу теоремы Минковского об однородных линейных функциях, можно найти для $\xi_1, \xi_2, \ldots, \xi_n$ такие целые значения, чтобы

$$|\eta_1|\leqslant\frac{|y_1|}{a}\sqrt{2}, |\eta_2|\leqslant\frac{|y_2|}{a}\sqrt{2}, \ldots, |\eta_n|\leqslant\frac{|y_n|}{a}\sqrt{2}. \tag{14}$$

В самом деле, произведение правых частей здесь равно

$$\frac{|y_1\cdot y_2\cdots y_n|}{a_n}2^{\frac{n}{2}}\geqslant\frac{L}{a^n}\cdot 2^{\frac{n}{2}}=|D|.$$

Выберем из этих систем $\eta_1, \eta_2, \ldots, \eta_n$, удовлетворяющих неравенствам (14), такую, что система $2\eta_1, 2\eta_2, \ldots, 2\eta_n$ уже не будет удовлетворять (14). Тогда по крайней мере для одного из η_i (пусть это будет η_1) имеет место

$$\eta_1\geqslant\frac{|y_1|}{a\sqrt{2}}. \tag{15}$$

Из (14) следует, что в силу (13),

$$-1\leqslant 1-\frac{\eta_i^2}{y_i^2}\leqslant 1 \qquad (i=2,3,\ldots,n). \tag{16}$$

Кроме того, из (14) и (15) следует

$$1-\frac{2}{a^2}\leqslant 1-\frac{\eta_1^2}{y_1^2}\leqslant 1-\frac{1}{2a^2}. \tag{17}$$

Если $1-\frac{\eta_1^2}{y_1^2}>0$, то $\left|1-\frac{\eta_1^2}{y_1^2}\right|\leqslant 1-\frac{1}{2a^2}$, откуда, подставляя в (11) и пользуясь (16), получим

$$1-\frac{1}{2a^2}>\frac{L^2}{(L+\varepsilon)^2}. \tag{18}$$

Если $1-\frac{\eta_1^2}{y_1^2}<0$ $\left(\text{в этом случае непременно } 1-\frac{2}{a^2}<0\right)$, то

$$\left|1-\frac{\eta_1^2}{y_1^2}\right|\leqslant\frac{2}{a^2}-1,$$

откуда, подставляя в (11) и пользуясь (16), получим

$$\frac{2}{a^2}-1>\frac{L^2}{(L+\varepsilon)^2}. \tag{19}$$

Но ни одно из неравенств (18), (19) невозможно, так как их левые части суть постоянные величины, меньшие единицы, а правые могут быть сколь угодно близки к единице. Противоречие доказывает недопустимость нашего предположения, что и т. д.

ЛИТЕРАТУРА

1. Ph. Furtwängler. Beweis des Hauptidealsatzes für die Klassenkörper algebraischer Zahlkörper. Abh. Hamb. Sem. **7**, 1929, стр. 14—36.
2. E. Artin. Idealklassen in Oberkörper und allgemeines Reziprozitätsgesetz. Abh. Hamb. Sem. **7**, 1929, стр. 46—51.
3. O. Taussky. Über eine Verschärfung des Hauptidealsatzes für algebraische Zahlkörper. Journ. f. Math. **168**, 1932, стр. 193—210.
4. E. Artin. Beweis des allgemeinen Reziprozitätsgesetzes. Abh. Hamb. Sem. **5**, 1927, стр. 353—363.
5. H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I. Jahresber. DMV **35**, 1926, стр. 19, теорема 4.
6. H. Minkowski. Geometrie des Zahlen. Lpz. 1896.
7. R. Remak. Verallgemeinerung eines Minkowski'schen Satzes. Math. Ztschr. **17**, 1923, стр. 1—34, **18**, 1923, стр. 173—200.

КРАТКОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ О ДИСКРИМИНАНТЕ

(KURZER BEWEIS DES DISKRIMINANTENSATZES)

(Acta Arithmetica **1** (1935), стр. 78—82)

Цель настоящей заметки — дать новое доказательство теоремы о дискриминанте, которая, как известно, представляет особые трудности при изложении арифметической теории идеалов. Это доказательство при относительной краткости имеет еще ту особенность, что оно требует довольно мало знаний из теории идеалов (например, понятие нормы идеала, как числа классов сравнений, не является необходимым). Напротив, элементы теории Галуа и первая теорема Силова предполагаются известными.

Формулируем доказываемую теорему о дискриминанте следующим образом.

Пусть k — алгебраическое числовое поле, $\mathfrak{R}$ — его кольцо (sein Ring), которое должно содержать все целые рациональные числа и $[\omega_1, \omega_2, \ldots, \omega_n]$ — базис $\mathfrak{R}$. Дискриминант

$$\Delta = \begin{vmatrix} S(\omega_1\omega_1), & S(\omega_1\omega_2), & \ldots, & S(\omega_1\omega_n) \\ S(\omega_2\omega_1), & S(\omega_2\omega_2), & \ldots, & S(\omega_2\omega_n) \\ \ldots & & & \\ S(\omega_n\omega_1), & S(\omega_n\omega_2), & \ldots, & S(\omega_n\omega_n) \end{vmatrix} = \begin{vmatrix} \omega_1, & \omega_2, & \ldots, & \omega_n \\ \omega_1', & \omega_2', & \ldots, & \omega_n' \\ & & & \\ \omega_1^{(n-1)}, & \omega_2^{(n-1)}, & \ldots, & \omega_n^{(n-1)} \end{vmatrix}^2$$

делится на рациональное простое число p тогда и только тогда, если p есть критическое число относительно $\mathfrak{R}$, т. е. если в $\mathfrak{R}$ существует такое число, которое в $\mathfrak{R}$ не делится на p, в то время как некоторая его степень делится на p в $\mathfrak{R}$. Здесь $\omega, \omega', \ldots, \omega^{(n-1)}$ обозначают алгебраически сопряженные с ω величины, а $S(\omega) = \omega + \omega' + \ldots + \omega^{(n-1)}$ — след числа ω.

Пусть p — критическое число и $\alpha = x_1\omega_1 + \ldots + x_n\omega_n$ — число из $\mathfrak{R}$, степень α^l которого делится на p, в то время как не все $x_i \equiv 0 \pmod{p}$. Сопряженные числа $(\alpha')^l, (\alpha'')^l, \ldots, (\alpha^{(n-1)})^l$ делятся на p, однако не обязательно в $\mathfrak{R}$, но в сопряженных с $\mathfrak{R}$ кольцах $\mathfrak{R}', \mathfrak{R}'', \ldots, \mathfrak{R}^{(n-1)}$, следовательно, также и в нормальном поле K, которое заключает в себе все поля, сопряженные с k.

Если Ω_{ij} — алгебраические дополнения элементов $\omega_i^{(j)}$ в определителе

$$\delta = \begin{vmatrix} \omega_1, & \omega_2, & \dots, & \omega_n \\ \omega_1', & \omega_2', & \dots, & \omega_n' \\ \dots & \dots & \dots & \dots \\ \omega_1^{(n-1)}, & \omega_2^{(n-1)}, & \dots, & \omega_n^{(n-1)} \end{vmatrix}, \tag{1}$$

то

$$\sum_j \Omega_{ij}\,\alpha^{(j)} = \sum_j \Omega_{ij} \sum_\mu \omega_\mu^{(j)} x_\mu = \sum_\mu x_\mu \sum_j \Omega_{ij}\omega_\mu^{(j)} = \\ = x_i\delta \qquad (i = 1, 2, \dots, n).$$

Если $p^h \geqslant l$, то в поле K делятся на p величины

$$\left\{\sum_j \Omega_{ij}\alpha^{(j)}\right\}^{p^h} \equiv \sum_j \Omega_{ij}^{p^h} (\alpha^{(j)})^{p^h} \pmod p$$

и так как не все $x_i \equiv 0 \pmod p$, то $\delta^{p^h} \equiv 0 \pmod p$. Но $\Delta = \delta^2$ есть целое рациональное число; следовательно, $\Delta \equiv 0 \pmod p$, что и т. д.

Теперь предположим, что Δ делится на p. Число δ лежит в поле K. Из $\delta^2 \equiv 0 \pmod p$ мы заключаем, что δ делится на произведение $\mathfrak{Q} = \mathfrak{P}_1 \dots \mathfrak{P}_m$ всех различных простых идеалов $\mathfrak{P}_i$, которые в поле K делят число p. Идеал $\mathfrak{Q}$ инвариантен относительно всех подстановок группы Галуа $\mathfrak{G}$ поля K. Простые идеалы $\mathfrak{P}_i$ являются сопряженными между собой, т. е. они переходят друг в друга при помощи подстановок из группы $\mathfrak{G}$. Докажем следующие три леммы:

1. *Если δ делится на $\mathfrak{Q}$, то систему сравнений*

$$\omega_1^{(i)}\xi_1 + \omega_2^{(i)}\xi_2 + \dots + \omega_n^{(i)}\xi_n \equiv 0 \pmod{\mathfrak{Q}} \qquad (i = 1, 2, \dots, n-1) \tag{2}$$

можно решить в целых числах поля K, которые не все делятся на $\mathfrak{Q}$.[1]

Пусть

$$\begin{vmatrix} \omega_\alpha^{(i)}, & \dots, & \omega_\beta^{(i)} \\ \dots & \dots & \dots \\ \omega_\alpha^{(j)}, & \dots, & \omega_\beta^{(j)} \end{vmatrix}$$

такой минор определителя (1), который не делится на $\mathfrak{Q}$, в то время как все миноры высшего порядка определителя (1) делятся на $\mathfrak{Q}$. Введем обозначения

$$\begin{vmatrix} u_\alpha, & \dots, & u_\beta, & u_\gamma \\ \omega_\alpha^{(i)}, & \dots, & \omega_\beta^{(i)}, & \omega_\gamma^{(i)} \\ \dots & \dots & \dots & \dots \\ \omega_\alpha^{(j)}, & \dots, & \omega_\beta^{(j)}, & \omega_\gamma^{(j)} \end{vmatrix} = A_\alpha u_\alpha + \dots + A_\beta u_\beta + A_\gamma u_\gamma.$$

Тогда система чисел $\xi_\alpha = A_\alpha, \dots, \xi_\beta = A_\beta, \xi_\gamma = A_\gamma$ (остальные $\xi = 0$) является искомым решением, для которого $\xi_\gamma \not\equiv 0 \pmod{\mathfrak{Q}}$.

[1] См. E. Landau. Vorlesungen über Zahlentheorie, Bd. 3. Leipzig, 1927, S. 129. Satz 822.

Покажем, что систему (2) можно удовлетворить целыми рациональными числами, которые не все делятся на p. Для этого докажем лемму:

II. *Если* $[\xi_1, \xi_2, \ldots, \xi_n]$ *— решение системы* (2), *то решением ее будет также* $[\xi_1 T, \xi_2 T, \ldots, \xi_n T]$, *где* T *— любая подстановка группы* $\mathfrak{G}$.

Рассмотрим сравнения (2) как соотношения между величинами поля K и применим к ним подстановку T ($\mathfrak{Q}$ инвариантен относительно T), при этом формы $\omega_1^{(i)} u_1 + \ldots + \omega_n^{(i)} u_n$ перейдут друг в друга и система (2) останется той же самой.

III. *Если система*

$$\omega_\alpha^{(i)} \xi_\alpha + \ldots + \omega_\beta^{(i)} \xi_\beta \equiv 0 \pmod{\mathfrak{Q}} \qquad (i = 1, 2, \ldots, n-1) \tag{3}$$

имеет решение $[\xi_\alpha, \ldots, \xi_\beta]$, *в котором* ξ_α *не делится на* D, *то она имеет также решение* $[\eta_\alpha, \ldots, \eta_\beta]$, *в котором* η_α *взаимно просто с* p.

Пусть $\Pi_1, \Pi_2, \ldots, \Pi_m$ — целые числа поля K, которые делятся соответственно на $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$ и ни на какие другие идеальные множители числа p. Если, например, ξ_α делится на $\mathfrak{P}_{h+1}, \ldots, \mathfrak{P}_m$, но не делится на $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$, и мы положим $\tau_\nu = \Pi_2 \Pi_3 \cdots \Pi_h \xi_\nu$ ($\tau_\nu = \xi_\nu$ для $h = 1$), то в решении $[\tau_\alpha, \ldots, \tau_\beta]$ системы (3) τ_α делится на $\mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_m$, но не делится на $\mathfrak{P}_1$. Если $S_2, S_3, \ldots, S_m$ — подстановки группы $\mathfrak{G}$, которые переводят $\mathfrak{P}_1$ соответственно в $\mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_m$, то число $\tau_\alpha + \tau_\alpha S_2 + \ldots + \tau_\alpha S_m$ взаимно просто с $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m$, а следовательно, и с p. С другой стороны, в силу леммы II, система $[\tau_\alpha S_i, \ldots, \tau_\beta S_i]$ ($i = 2, 3, \ldots, m$), а значит, и система $[\tau_\alpha + \tau_\alpha S_2 + \ldots + \tau_\alpha S_m, \ldots; \tau_\beta + \tau_\beta S_2 + \ldots + \tau_\beta S_m]$ являются решениями системы (3). Последнее решение удовлетворяет нашему условию.

Пусть

$$\omega_1^{(i)} \xi_1 + \omega_2^{(i)} \xi_2 + \ldots + \omega_r^{(i)} \xi_r \equiv 0 \pmod{\mathfrak{Q}} \qquad (i = 0, 1, \ldots, n-1) \tag{4}$$

— система, имеющая решение, в котором $\xi_1 \not\equiv 0 \pmod{\mathfrak{Q}}$, причем r имеет возможно меньшее значение. В силу леммы III, мы можем предположить, что ξ_1 в решении $[\xi_1, \xi_2, \ldots, \xi_r]$ системы (4) взаимно простое с p. Для $r > 1$ система

$$\omega_2^{(i)} \xi_2 + \ldots \omega_r^{(i)} \xi_r \equiv 0 \pmod{\mathfrak{Q}} \qquad (i = 0, 1, \ldots, n-1) \tag{5}$$

не имеет решения, в котором одно или больше чисел $\xi_\nu \not\equiv 0 \pmod{\mathfrak{Q}}$. Действительно, в противном случае мы могли бы, изменив нумерацию неизвестных, представить систему (5) в форме (4) с меньшим значением r. Если теперь мы умножим ξ_ν на $\frac{N(\xi_1)}{\xi_1}$, то получим решение $[\eta_1, \eta_2, \ldots, \eta_n]$, в котором $\eta_1 = N(\xi_1)$ — есть целое рациональное число, взаимно простое с p. Это решение единственное в том смысле, что каждое другое решение $[\eta_1, \eta_2^*, \ldots, \eta_r^*]$ удовлетворяет сравнениям $\eta_\nu^* \equiv \eta_\nu \pmod{\mathfrak{Q}}$. В самом деле, в противном случае $[\eta_2^* - \eta_2, \ldots$

$\ldots, \eta_r^* - \eta_r]$ было бы решением системы (5), что вследствие нашего предположения невозможно.

В частности $\eta_\nu T \equiv \eta_\nu \pmod{\mathfrak{Q}}$ $(\nu = 1, 2, \ldots, r)$ (см. II), где T — любая подстановка из $\mathfrak{G}$. Пусть теперь $\mathfrak{H} = 1 + S_2 + \ldots + S_\pi$ есть принадлежащая p силовская подгруппа группы $\mathfrak{G}$, т. е. подгруппа порядка $\pi = p^s$ (s может равняться нулю), индекс которой $a = (\mathfrak{G} : \mathfrak{H})$ взаимно прост с p (первая теорема Силова). Существует показатель f, для которого

$$\eta_\nu^{p^f} \equiv \eta_\nu \pmod{\mathfrak{P}_i} \qquad (i = 1, 2, \ldots, m)$$

и, следовательно,

$$\eta_\nu^{p^f} \equiv \eta_\nu \pmod{\mathfrak{Q}}$$

(обобщенная теорема Ферма). Возьмем такое целое рациональное число q, чтобы $l = qf - s$ было положительным. Тогда

$$(\eta_\nu \cdot \eta_\nu S_2 \cdots \eta_\nu S_\pi)^{p^l} \equiv \eta_\nu^{p^s p^{qf-s}} \equiv \eta_\nu \pmod{\mathfrak{Q}}.$$

Левая часть этого сравнения инвариантна относительно $\mathfrak{H}$. Следовательно,

$$\eta_\nu \equiv \tau_\nu \pmod{\mathfrak{Q}},$$

причем τ_ν инвариантно относительно $\mathfrak{H}$.

Разложим теперь группу $\mathfrak{G}$ по подгруппе $\mathfrak{H}$:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}T_2 + \ldots + \mathfrak{H}T_a \qquad (a, p) = 1.$$

В сравнении

$$a\tau_\nu \equiv \tau_\nu + \tau_\nu T_2 + \ldots + \tau_\nu T_a \pmod{\mathfrak{Q}}$$

правая часть инвариантна относительно всех подстановок из $\mathfrak{G}$ и следовательно, есть целое рациональное число. Поэтому мы можем решение $[a\eta_1, a\eta_2, \ldots, a\eta_r]$ системы (4) заменить решением $[a\eta_1, x_2, \ldots, x_r]$, в котором $a\eta_1, x_2, \ldots, x_r$ целые рациональные числа, причем $(a\eta_1, p) = 1$.[1]

Пусть $\mathfrak{Q}^l$ делится на p. Число

$$\alpha = a\eta_1\omega_1 + x_2\omega_2 + \ldots + x_r\omega_r$$

делится на $\mathfrak{Q}$; следовательно, α^l делится на p. С другой стороны, α в кольце $\mathfrak{R}$ не делится на p, так как иначе число $\frac{\alpha}{p} = \frac{a\eta_1\omega_1 + \cdots + x_2\omega_r}{p}$ содержалось бы в $\mathfrak{R}$ и имело бы дробную первую координату $\frac{a\eta_1}{p}$, что противоречит предположению, что $[\omega_1, \ldots, \omega_n]$ есть базис $\mathfrak{R}$. Тем самым показано, что p является критическим числом, что и т. д.

Поступило
26 октября 1934 г.

[1] Это доказательство заимствовано у Д. Гильберта. См. Ges. Abh., Bd. I Berlin 1932, стр. 135.

ЗАДАЧА ИЗ ТЕОРИИ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

(Сборник памяти академика Д. А. Граве, 1940, стр. 283—290)

(EINE AUFGABE AUS DER ALGEBRAISCHEN ZAHLENTHEORIE)

(Acta Arithm. 2 (1937), стр. 221—229)

В одной из моих прежних работ [1] я привел вопрос о существовании некоторых относительно абелевых числовых полей к проблеме существования l-примарных простых идеалов $\mathfrak{p}$ внутри заданного нормального алгебраического числового поля k, для которых символ степенного вычета

$$\left\{\frac{\Pi_2\,\Pi_3\cdots\Pi_k}{\mathfrak{p}}\right\} \tag{1}$$

имел бы заданное значение. Здесь

$$\mathfrak{p}=\mathfrak{p}_1,\ \mathfrak{p}_2,\ \ldots,\ \mathfrak{p}_k$$

означают сопряженные с $\mathfrak{p}$ простые идеалы, а

$$\Pi_i=\mathfrak{p}_i\mathfrak{q}_i^l \qquad (i=1,2,\ldots,k)$$

— сопряженные друг с другом целые числа поля k, причем

$$(\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_k,\ \mathfrak{q}_i)=1 \qquad (i=1,2,\ldots,k).$$

В силу примарности идеала $\mathfrak{p}$ значение символа (1) не зависит от выбора идеалов $\mathfrak{q}_i$.

Эта задача казалась мне неразрешимой средствами современных методов аналитической теории чисел, так как я не мог привести ее к задаче Фробениуса о существовании простых идеалов, принадлежащих к различным подстановкам группы поля. В настоящее время мне удалось решить эту задачу для случая $l=2$ для мнимых квадратичных полей $k(\sqrt{-m})$, где m — целое нечетное, лишенное квадратов число, представимое в форме x^2+y^2.

§ 1

В дальнейшем нам понадобятся формулы, выражающие лежандровы символы в иррациональных алгебраических числовых полях через символы в поле рациональных чисел. Эти формулы были получены Ф. Фуртвенглером [2] для относительно нормальных полей и Т. Такаги [3] — для общего случая.

Будем обозначать через $\{\cdots\}$ символ l-го степенного вычета в поле K, через $(\cdots)$ — в его делителе k и через $N(\cdots)$ — относительную норму чисел и идеалов поля K по отношению к k. Тогда имеет место равенство

$$\left\{\frac{\alpha}{\mathfrak{B}}\right\}=\left(\frac{\alpha}{N(\mathfrak{B})}\right), \tag{2}$$

где α — число из k, а $\mathfrak{B}$ — идеал из K. Далее, имеет место равенство

$$\left\{\frac{A}{\mathfrak{c}}\right\}=\left(\frac{N(A)}{\mathfrak{c}}\right), \tag{3}$$

где A — число из K и $\mathfrak{c}$ — идеал из k.

§ 2

Пусть k — поле рациональных чисел и K — мнимое квадратичное поле:

$$K=k(\sqrt{-m}),$$

где m — целое, положительное, нечетное и лишенное квадратов число. Далее, предположим, что m представимо в форме суммы двух квадратов:

$$m=\xi^2+\eta^2.$$

Это означает, что каждый простой множитель q_i числа m

$$m=q_1q_2\cdots q_s \tag{4}$$

удовлетворяет сравнению

$$q_i\equiv 1 \pmod 4 \quad (i=1, 2, \ldots, s). \tag{5}$$

Базис поля K может быть представлен в форме

$$[1, \sqrt{-m}].$$

Условие: число

$$p=N(a+b\sqrt{-m})=a^2+mb^2 \tag{6}$$

должно быть нечетным простым числом,— требует выполнения одной из следующих двух систем сравнений:

$$a\equiv 1 \pmod 2, \qquad b\equiv 0 \pmod 2 \tag{7}$$

или

$$a\equiv 0 \pmod 2, \qquad b\equiv 1 \pmod 2. \tag{8}$$

В первом случае искомый символ $\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}$ может быть

преобразован так:

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=\left\{\frac{2a}{a+b\sqrt{-m}}\right\}=\left(\frac{2a}{a^2+mb^2}\right)= \tag{9}$$
$$=\left(\frac{2}{a^2+mb^2}\right)\left(\frac{m}{a}\right)=(-1)^{\frac{p-1}{4}}\left(\frac{a}{m}\right).$$

Символ Якоби $\left(\frac{a}{m}\right)$, в силу (4), может быть представлен так:

$$\left(\frac{a}{m}\right)=\left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_s}\right).$$

Каждый из символов $\left(\frac{a}{q_i}\right)$ имеет значение $+1$ тогда и только тогда, если сравнение

$$\xi^2\equiv a \pmod{q_i} \tag{10}$$

имеет рациональные решения. Но так как

$$p\equiv a^2 \pmod{q_i}, \tag{11}$$

то $\left(\frac{a}{q_i}\right)=+1$ тогда и только тогда, если p есть *биквадратичный вычет* по модулю q_i. Необходимость этого условия очевидна. С другой стороны, если

$$p\equiv\xi_1^4 \pmod{q_i},$$

то, в силу (6), или

$$a\equiv\xi_1^2 \pmod{q_i},$$

или

$$a\equiv-\xi_1^2 \pmod{q_i}.$$

Оба значения a, в силу

$$q_i\equiv 1 \pmod 4, \tag{12}$$

являются квадратичными вычетами по модулю q_i. Это означает, что символ $\left(\frac{a}{q_i}\right)$ имеет значение $+1$. Если нам предоставлено выбрать по произволу класс сравнений по модулю q_i, в котором должно лежать p, лишь с тем ограничением, что p должно быть квадратичным вычетом по модулю q_i, то мы имеем в своем распоряжении $\frac{p-1}{4}$ биквадратичных вычетов и $\frac{p-1}{4}$ невычетов. Для первых имеет место $\left(\frac{a}{q_i}\right)=+1$, для вторых $\left(\frac{a}{q_i}\right)=-1$.

Обращаясь к случаю (8) и полагая

$$a=2^\lambda a_1, \qquad (a_1, 2)=1,$$

будем иметь

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=\left(\frac{2a}{a^2+mb^2}\right)=\left(\frac{2}{a^2+mb^2}\right)^{\lambda+1}\left(\frac{m}{a_1}\right)=$$
$$=(-1)^{\frac{p-1}{4}(\lambda+1)}\left(\frac{a_1}{m}\right)=(-1)^{\frac{p-1}{4}(\lambda+1)}(-1)^{\frac{m-1}{4}\lambda}\left(\frac{a}{m}\right). \tag{13}$$

Подвергнем простое число p дальнейшему ограничению

$$p\equiv m \pmod 8. \tag{14}$$

Тогда оба выражения (9) и (13) приобретают одну и ту же форму

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=(-1)^{\frac{m-1}{4}}\left(\frac{a}{m}\right), \tag{15}$$

так что теперь мы можем не различать случаев (7) и (8). Таким образом, мы видим, что значение нашего символа

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}$$

вполне определится, если мы будем знать класс сравнений по модулю $8m$, в котором лежит p.

§ 3

Особого рассмотрения требует случай, когда K есть гауссово поле: $K=k(i)$. Тогда мы можем нормировать число $a+bi$ при помощи единиц ± 1, $\pm i$ таким образом, чтобы было

$$a>0, \qquad a\equiv 1 \pmod 2, \qquad b\equiv 0 \pmod 2,$$

и искомый символ может быть преобразован так:

$$\left\{\frac{a-bi}{a+bi}\right\}=\left\{\frac{2a}{a+bi}\right\}=\left(\frac{2a}{a^2+b^2}\right)= \tag{16}$$
$$=\left(\frac{2}{a^2+b^2}\right)\left(\frac{a}{a^2+b^2}\right)=(-1)^{\frac{p-1}{4}}.$$

Условие примарности

$$\left\{\frac{i}{a+bi}\right\}=1$$

требует, чтобы значения символов

$$\left\{\frac{a-bi}{a+bi}\right\}, \quad \left\{\frac{b+ai}{b-ai}\right\}$$

были равны друг другу. Отсюда следует

$$\left\{\frac{a-bi}{a+bi}\right\}=\left\{\frac{b+ai}{b-ai}\right\}=\left\{\frac{2b}{b-ai}\right\}=\left(\frac{2b}{a^2+b^2}\right). \tag{17}$$

Стало быть, в силу (16), мы будем иметь

$$\left(\frac{4ab}{a^2+b^2}\right)=\left(\frac{2a}{a^2+b^2}\right)\left(\frac{2b}{a^2+b^2}\right)=1,$$

откуда получаем

$$1=\left(\frac{4ab}{a^2+b^2}\right)=\left(\frac{2(a+b)^2-2(a^2+b^2)}{a^2+b^2}\right)=\left(\frac{2}{a^2+b^2}\right).$$

Это условие можно также написать так:

$$p\equiv 1 \pmod 8. \tag{18}$$

Если это условие выполняется, то значение искомого символа $\left\{\frac{a-bi}{a+bi}\right\}$, в силу (16), равно $+1$. Таким образом, наша задача допускает решение в *отрицательном смысле*.

§ 4

Вернемся опять к общему случаю § 2. Чтобы найти главные простые идеалы $(a+b\sqrt{-m})$, удовлетворяющие условию

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=\varepsilon, \tag{19}$$

достаточно найти рациональные простые числа $p=N(a+b\sqrt{-m})$, подчиненные следующим условиям:

1) p должны разлагаться внутри $K(\sqrt{-m})$ на два различных простых идеала.

2) p должны быть примарными, т. е. иметь форму $4k+1$. Более того, они должны удовлетворять условию

$$p\equiv m \pmod 8.$$

3) p должны быть квадратичными вычетами по модулям $q_i\,(i=1, 2, \ldots, s)$:

$$\left(\frac{p}{q_i}\right)=+1 \qquad (i=1, 2, \ldots, s).$$

4) Обозначая через ε_i $+1$, или -1 в зависимости от того, есть ли p биквадратичный вычет или невычет по модулю q_i (допуская, что условие 3) уже выполнено), потребуем, чтобы имело место

$$\varepsilon_1\varepsilon_2\ldots\varepsilon_s=(-1)^{\frac{m-1}{4}}\varepsilon, \tag{20}$$

где ε — заданная величина, равная $+1$ или -1.

Условие 1) может быть следующим образом видоизменено на основании свойств *поля классов*. В силу определения поля классов [4], простое число p является нормой главного идеала первой степени поля K тогда и только тогда, если p является нормой идеала

первой степени поля $\mathfrak{K}$, где $\mathfrak{K}$ означает поле классов поля K. Поэтому условие 1) равносильно следующему условию:

1') p должны принадлежать к тождественной подстановке внутри поля $\mathfrak{K}$.

Условия 2), 3), 4) также могут быть формулированы подобным же образом. Для этого мы введем в рассмотрение поле K_1 $8m$-ых корней из единицы. Тогда условия 2), 3), 4) равносильны следующему условию:

2') p должны принадлежать внутри поля K_1 к определенному классу подстановок.

Вопрос о существовании бесчисленного множества простых чисел, принадлежащих внутри двух различных полей $\mathfrak{K}$ и K_1 к заданным классам подстановок, имеет утвердительный или отрицательный ответ в зависимости от того, вызывают ли обе заданные внутри обоих полей подстановки одну и ту же или разные подстановки среди величин пересечения K_2 полей $\mathfrak{K}$ и K_1 [5].

K_1, а потому и K_2 являются абсолютно абелевыми полями. С другой стороны, наибольшее абсолютно абелево частичное поле классов квадратичного поля $K = k(\sqrt{-m})$ есть поле $k(i, \sqrt{-q_1}, \sqrt{-q_2}, \ldots, \sqrt{-q_s})$ [6]. Это поле действительно содержится в K_1, а потому

$$K_2 = k(i, \sqrt{-q_2}, \ldots, \sqrt{-q_s}). \tag{21}$$

Тождественной подстановке в $\mathfrak{K}$, очевидно, соответствует подстановка в K. Таким образом, остается лишь доказать, что подстановка в K_2, вызванная подстановкой из K_1, определенной условиями 2), 3), 4), есть также тождественная подстановка. Условия того, чтобы p внутри K_2 разлагалось на простые идеалы первой степени, состоит в выполнении сравнений

$$\left(\frac{-1}{p}\right) = +1, \quad \left(\frac{q_1}{p}\right) = +1, \quad \left(\frac{q_2}{p}\right) = +1, \ldots, \left(\frac{q_s}{p}\right) = +1. \tag{22}$$

Эти условия, за исключением первого, совпадают, в силу лежандрова закона взаимности, с условием (3), а первое из этих условий содержится в условии 2). Таким образом, существование искомых простых чисел доказано.

§ 5

Я позволю себе остановиться на тех трудностях, которые связаны с решением нашей задачи в других случаях. Рассмотрим все типы мнимых квадратичных полей и проведем для каждого из этих типов рассуждения, подобные тем, которые мы применили при выводе формул (9) и (13).

I. $K = k(\sqrt{-m})$, $m \equiv 1 \pmod 4$. Базисом является

$$[1, \sqrt{-m}].$$

Формулы (9) и (13) сохраняются в силе

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=(-1)^{\frac{p-1}{4}}\left(\frac{a}{m}\right) \quad [a\equiv 1 \pmod 2,\ b\equiv 0 \pmod 2]; \tag{23}$$

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=(-1)^{\frac{p-1}{4}(\lambda+1)}(-1)^{\frac{m-1}{4}\lambda}\left(\frac{a}{m}\right) \tag{24}$$

$$[b\equiv 1 \pmod 2, \qquad a=2^{\lambda}a_1, \qquad (a_1,2)=1].$$

Но здесь мы должны допустить, что m содержит также простые множители вида $4k+3$. Пусть q_1 будет один из таких множителей. Тогда

$$\left(\frac{a}{q_1}\right)=-\left(\frac{-a}{q_1}\right),$$

так что здесь нормирование $a>0$ существенно. С другой стороны, сравнение

$$\xi^4\equiv p \pmod{q_1}$$

при $q_1\equiv 3 \pmod 4$ всегда имеет два и только два рациональных решения. Мы не имеем способа различать, имеет ли при этом сравнение

$$\xi^2\equiv a \pmod{q_1}, \qquad a>0$$

рациональные решения или нет.

Формулу (23) можно записать следующим образом:

$$\left\{\frac{a-b\sqrt{-m}}{a+b\sqrt{-m}}\right\}=(-1)^{\frac{p-1}{4}}\prod_{i=1}^{s}(-1)^{\frac{a-1}{2}\frac{q_i-1}{2}}\left(\frac{a}{q_1}\right). \tag{25}$$

Здесь каждый множитель

$$(-1)^{\frac{a-1}{2}\frac{q_i-1}{2}}\left(\frac{a}{q_i}\right) \qquad (i=2,3,\ldots,s)$$

не зависит от выбора знака при a. Но зато он зависит от поведения числа a по модулю 4, каковое нельзя охарактеризовать никаким свойством сравнения для числа p.

II. $K=k(\sqrt{-m})$, $m\equiv 3 \pmod 4$. Базисом является

$$\left[1, \frac{1+\sqrt{-m}}{2}\right].$$

Поэтому целые нечетные числа поля K могут быть представлены или в виде

$$\frac{a}{2}+\frac{b}{2}\sqrt{-m}, \tag{26}$$

где

$$a\equiv 1 \pmod 2, \qquad b\equiv 1 \pmod 2,$$

или в виде

$$a + b\sqrt{-m},$$

где либо

$$a \equiv 1 \pmod 2, \qquad b \equiv 0 \pmod 2, \tag{27}$$

либо

$$a \equiv 0 \pmod 2, \qquad b \equiv 1 \pmod 2. \tag{28}$$

В случае (26) имеем

$$\left\{\frac{\frac{a}{2} - \frac{b}{2}\sqrt{-m}}{\frac{a}{2} + \frac{b}{2}\sqrt{-m}}\right\} = \left\{\frac{a}{\frac{a}{2} + \frac{b}{2}\sqrt{-m}}\right\} = \left(\frac{a}{\frac{a^2 + mb^2}{4}}\right) = \left(\frac{\frac{a^2 + mb^2}{4}}{a}\right) =$$

$$= \left(\frac{a^2 + mb^2}{a}\right) = \left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}}\left(\frac{a}{m}\right) =$$

$$= \prod_{i=1}^{s} (-1)^{\frac{a-1}{2}\frac{q_i - 1}{2}}\left(\frac{a}{q_i}\right).$$

Здесь сохраняют свою силу все замечания к случаю I.
Аналогично в случае (27) получим

$$\left\{\frac{a - b\sqrt{-m}}{a + b\sqrt{-m}}\right\} = \left\{\frac{2a}{a + b\sqrt{-m}}\right\} = \left(\frac{2a}{a^2 + mb^2}\right) = \left(\frac{2}{a^2 + mb^2}\right)\left(\frac{m}{a}\right) =$$

$$= (-1)^{\frac{p-1}{4}}(-1)^{\frac{a-1}{2}}\left(\frac{a}{m}\right) = (-1)^{\frac{p-1}{4}} \prod_{i=1}^{s} (-1)^{\frac{a-1}{2}\frac{q_i - 1}{2}}\left(\frac{a}{q_i}\right).$$

В случае (28) число p не примарно.

III. Случай $K = k(\sqrt{-3})$ отличается от случая II тем, что поле $k(\sqrt{-3})$ содержит нетривиальные единицы

$$\varepsilon = \frac{-1 + \sqrt{-3}}{2}, \qquad \varepsilon^2 = \frac{-1 - \sqrt{-3}}{2}.$$

Можно было бы ожидать, что здесь условие примарности наложит на простые числа новые ограничения. Это, однако, не имеет места, так как

$$\left\{\frac{\varepsilon}{\omega}\right\} = \left\{\frac{\varepsilon^2}{\omega}\right\}^2 = +1,$$

где ω означает простое число поля $k(\sqrt{-3})$.

IV. Случай $K = k(\sqrt{-2m})$, $m \equiv 1 \pmod 2$. Базисом является

$$[1, \sqrt{-2m}].$$

Имеем

$$a \equiv 1 \pmod 2, \qquad b \equiv 0 \pmod 2,$$

так как условие примарности

$$\left\{\frac{-1}{a+b\sqrt{-2m}}\right\}=\left(\frac{-1}{a^2+2mb^2}\right)=1$$

требует соблюдения сравнения

$$a^2+2mb^2\equiv 1 \pmod 4.$$

Отсюда следует

$$p=a^2+2mb^2\equiv 1 \pmod 8.$$

Имеем

$$\left\{\frac{a-b\sqrt{-2m}}{a+b\sqrt{-2m}}\right\}=\left(\frac{2a}{a^2+2mb^2}\right)=\left(\frac{a^2+2mb^2}{a}\right)=\left(\frac{2}{a}\right)\left(\frac{m}{a}\right)=$$

$$=(-1)^{\frac{a^2-1}{8}}(-1)^{\frac{a-1}{2}\frac{m-1}{2}}\left(\frac{a}{m}\right).$$

Чтобы решить нашу задачу для всех этих случаев, необходимо определить плотность простых чисел вида

$$a+b\sqrt{-m},$$

которые удовлетворяли бы условиям

$$a>0, \qquad a\equiv 1 \pmod 4.$$

Для этой цели может оказаться полезным следующий обобщенный L-ряд:

$$L(s)=\sum_{a,b}\frac{a+b\sqrt{-m}}{(a^2+mb^2)^s},$$

где a пробегает все (положительные и отрицательные) целые числа вида $4k+1$, а b — все (или соответственно все четные) целые числа в зависимости от типа поля $k(\sqrt{-m})$. Я надеюсь исследовать этот вопрос в дальнейшей работе.

ЛИТЕРАТУРА

1 N. Tschebotarö w. Untersuchungen über relativ Abelsche Zahlkörper. Journ. f. reine und ang. Math. **167**, 1932, стр. 98—121; Собр. соч., т. I, стр. 141—171.

2. Ph. Furtwängler. Über die Reziprozitätsgesetze zwischen l-ten Potenzresten in algebraischen Zahlkörpern, wenn l eine ungerade Primzahl bedeutet. Math. Ann. **58**, 1904, стр. 24.

3. T. Takagi. Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper. Journ. of Coll. of Sc. Imp. Univ. Tôkjo **44**, 1922, стр. 10.

4. H. Hasse. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I: Klassenkörpertheorie. Jber. D. M.-V. **35**. 1926, стр. 4, Definition 1°.

5. N. Tschebotareff. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, die zu einer gegebenen Substitutionsklasse gehören. Math. Ann. **95**, 1925, стр. 213. Собр. соч., т. I, стр. 27—65.

6. N. Tschebotarö w. Zur Gruppentheorie des Klassenkörpers. Journ. f. reine und ang. Math. **161**, 1929, стр. 193, Beispiel. Собр. соч., т. I, стр. 121—140.

О ВЫРАЖЕНИИ АБЕЛЕВЫХ ИНТЕГРАЛОВ ЧЕРЕЗ ЭЛЕМЕНТАРНЫЕ ФУНКЦИИ

(Усп. матем. наук 2 (1947), в. 2, стр. 3 — 20)

В моей статье не предполагается предложить принципиально новые результаты. Моя цель — дать новые выводы старых результатов Лиувилля, Абеля и Чебышева, выводы которых, в силу своей трудности, не получили всеобщего распространения, на что следовало бы рассчитывать в силу важности результатов. Мои выводы основаны на теории римановых поверхностей и вообще на современной теории алгебраических функций, которая была создана позднее, чем работы упомянутых авторов.

§ 1. Форма представления абелевых интегралов через элементарные функции

I. Будем рассматривать интегралы вида

$$\int u\,dx, \tag{1}$$

где u — рациональная функция двух переменных x, y, связанных алгебраическим соотношением

$$f(x, y) = 0. \tag{2}$$

Будем называть совокупность рациональных функций от x, y полем $k(x, y)$. Интегралы же типа (1) носят название абелевых интегралов.

Предположим, что интеграл (1) выражается через элементарные функции. Точнее, пусть его можно представить как алгебраическую (вообще говоря, иррациональную) функцию от x, $\log w_1$, $\log w_2$, ..., $\log w_k$, где w_1, w_2, ..., w_k являются алгебраическими функциями от x:

$$\int u\,dx = \Phi(x, \log w_1, \log w_2, \ldots, \log w_k). \tag{3}$$

Оказывается, что в этом случае функцией Φ может быть функция весьма частного вида, как это было в свое время показано Лиувиллем.

Если интеграл (1) выражается в логарифмах, то это выражение может быть представлено в форме

$$w_0 + a_1 \log w_1 + \ldots + a_k \log w_k, \tag{4}$$

где $w_0, w_1, \ldots, w_k$ — некоторые алгебраические функции от x, не обязательно входящие в поле $k(x, y)$, а $a_1, a_2, \ldots, a_k$ — константы.

Доказательство. Предположим, что $x, \log w_1, \log w_2, \ldots, \log w_k$ не связаны никаким рациональным сооотношением типа

$$\psi(x, \log w_1, \ldots, \log w_k) = 0, \tag{5}$$

где ψ — полином. В противном случае мы бы могли исключить из выражения (3) одну из функций $\log w_\nu$. Дифференцируем равенство (3) по x

$$u = \frac{\partial \Phi}{\partial x} + \frac{\partial \Phi}{\partial \log w_1}\frac{w_1'}{w_1} + \cdots + \frac{\partial \Phi}{\partial \log w_k}\frac{w_k'}{w_k}. \tag{6}$$

Получается соотношение типа (5). В силу нашего условия, оно должно быть тождеством относительно $\log w_1, \log w_2, \ldots, \log w_k$, а потому производная от него по $\log w_\nu$ должна быть равна нулю:

$$\frac{\partial^2 \Phi}{\partial x\, \partial \log w_\nu} + \frac{\partial^2 \Phi}{\partial \log w_1\, \partial \log w_\nu}\frac{w_1'}{w_1} + \cdots + \frac{\partial^2 \Phi}{\partial \log w_k\, \partial \log w_\nu}\frac{w_k'}{w_k} = 0$$
$$(\nu = 1, 2, \ldots, k),$$

но это выражение есть полная производная по x от функции $\dfrac{\partial \Phi}{\partial \log w_\nu}$, которая, в силу этого, равна постоянной

$$\frac{\partial \Phi}{\partial \log w_\nu} = a_\nu \qquad (\nu = 1, 2, \ldots, k). \tag{7}$$

При этом соотношения (7) являются тождествами относительно $\log w_\nu$ и, следовательно, относительно x: в противном случае они опять приводили бы к соотношениям типа (5).

Отсюда следует, что в выражение Φ аргументы $\log w_\nu$ входят линейно с постоянными коэффициентами a_ν, т. е. что Φ имеет форму (4).

II. Можно нормировать выражения (4) так, чтобы $w_0, w_1, \ldots, w_k$ были функциями из поля $k(x, y)$.

Доказательство. Пусть $x, w_0, w_1, \ldots, w_k, y$ порождают поле $k(x, z)$. Пусть

$$F(x, y; z) = 0 \tag{8}$$

будет неприводимое в поле $k(x, y)$ уравнение, которому удовлетворяет z, и пусть $z_1, z_2, \ldots, z_h$ будут его корни, соответствующие определенным значениям x, y (здесь удобно представить себе их расположенными на разных листах римановой поверхности). Пусть y выражается через x, z так:

$$y = \varphi(x, z).$$

В силу неприводимости уравнения (8) в поле $k(x, y)$ полином $\varphi(x, z) - y$, как функция z, делится на $F(x, y; z)$, а потому

$$y = \varphi(x, z_1) = \varphi(x, z_2) = \cdots = \varphi(x, z_h).$$

Таким образом, наряду с

$$\int u\,dx = w_0 + a_1 \log w_1 + \cdots + a_k \log w_k, \tag{9}$$

мы будем также иметь

$$\int u\,dx = w_0^{(\mu)} + a_1 \log w_1^{(\mu)} + \cdots + a_k \log w_k^{(\mu)} \qquad (\mu = 1, 2, \ldots, h), \tag{10}$$

где под $w_\nu^{(\mu)}$ мы разумеем функцию, сопряженную с w_ν: если

$$w_\nu = \psi_\nu(x, z),$$

то

$$w_\nu^{(\mu)} = \psi_\nu(x, z^{(\mu)}) \qquad (\mu = 1, 2, \ldots, h).$$

Суммируя равенства (10), получим

$$\int u\,dx = \frac{1}{h}\sum_{\mu=1}^{h} w_0^{(\mu)} + \frac{a_1}{h}\log\prod_{\mu=1}^{h} w_1^{(\mu)} + \cdots + \frac{a_k}{h}\log\prod_{\mu=1}^{h} w_k^{(\mu)}.$$

Но сумма $\sum_{\mu=1}^{h} w_0^{(\mu)}$ и произведения $\prod_{\mu=1}^{h} w_\nu^{(\mu)}$ как симметрические функции от корней уравнения (8) являются элементами поля $k(x, y)$, и таким образом полученное равенство дает искомое представление интеграла через элементы поля $k(x, y)$, ч. и т. д.

III. Можно нормировать выражение (4) так, чтобы коэффициенты $a_1, a_2, \ldots, a_k$ не были связаны линейными соотношениями

$$a_1 m_1 + a_2 m_2 + \cdots a_k m_k = 0 \tag{11}$$

с целыми рациональными $m_1, m_2, \ldots, m_k$.

Доказательство. Пусть имеет место (11), причем, например, $m_1 \neq 0$. Тогда выражение (4) может быть представлено так:

$$w_0 + \frac{a_2}{m_1}\log\frac{w_2^{m_1}}{w_1^{m_2}} + \cdots + \frac{a_k}{m_1}\log\frac{w_k^{m_1}}{w_1^{m_k}}.$$

Вводя для элементов $\frac{w_\nu^{m_1}}{w_1^{m_\nu}}$ новые символы, мы уменьшим на единицу число членов в выражении (4). Продолжая процесс, мы в конце концов придем к выражению типа (4), для которого соотношений (11) уже не будет существовать.

IV. Если интеграл (1) представлен в нормированной форме (4), то всякая точка, обращающая в нуль или в бесконечность одну (или несколько) из функций $w_1, w_2, \ldots, w_k$, является логарифмической точкой интеграла (1).

Доказательство. Пусть, например, w_1 обращается в нуль в точке P. Выберем в качестве x новый элемент поля $k(x, y)$, обраща-

ющийся в нуль в точке P, но более ни в одной другой точке, в которой обращается в нуль элемент w_1. Произведя в (9) замену переменных и затем переходя к сопряженным относительно x значениям элементов поля $k(x, y)$ и суммируя получаемые таким образом из (10) равенства, будем иметь

$$\sum_{\mu=1}^{n} \int u^{(\mu)}\, dx = \sum_{\mu=1}^{n} w_0^{(\mu)} + a_1 \log \prod_{\mu=1}^{n} w_1^{(\mu)} + \cdots + a_k \log \prod_{\mu=1}^{n} w_k^{(\mu)}. \quad (12)$$

В силу сделанного относительно x предположения, $\prod_{\mu=1}^{n} w_1^{(\mu)}$ представляется в форме

$$x^{m_1} \cdot \varphi(x), \quad \varphi(0) \neq 0, \quad \varphi(0) \neq \infty,$$

где m_1 — целое положительное число. Аналогично представляются и остальные выражения $\prod_{\mu=1}^{n} w_\nu^{(\mu)}$, но только m_ν при $\nu \geqslant 2$ может принимать нулевые и отрицательные значения. Отсюда следует, что (12) можно представить в таком виде:

$$\sum_{\mu=1}^{n} \int u^{(\mu)}\, dx = \sum_{\mu=1}^{n} w_0^{(\mu)} + (a_1 m_1 + a_2 m_2 + \cdots + a_k m_k) \log x + \\ + \sum_{\nu=1}^{k} a_\nu \log \varphi_\nu(x). \quad (13)$$

Коэффициент при $\log x$ в правой части, в силу III, отличен от нуля, так что правая часть равенства (13) имеет в точке $x = 0$ логарифмическую бесконечность. С другой стороны, если бы $\int u\, dx$ не имел логарифмической бесконечности в точке $x = 0$, то ни один из интегралов $\int u^{(\mu)}\, dx$ тоже не имел бы ее, так как все эти интегралы на всей римановой поверхности пробегают одну и ту же совокупность значений. Отсюда в качестве простых следствий вытекает:

V. Интеграл 1-го рода не может быть выражен через элементарные функции.

В самом деле, из IV следует, что его выражение через элементарные функции не может содержать логарифмов и потому должно быть равно функции поля $k(x, y)$. Но функция $k(x, y)$, если она не есть константа, всегда в каких-нибудь точках обращается в бесконечность, в то время как интеграл первого рода таковых не имеет.

VI. Если интеграл второго рода может быть выражен через элементарные функции, то он равен функции поля $k(x, y)$.

§ 2. О биномиальных дифференциалах

Биномиальными дифференциалами называются дифференциалы вида

$$x^m (x^n + 1)^p \, dx, \tag{1}$$

где m, n, p — какие-нибудь рациональные числа. Вопрос об их интегрировании через элементарные функции впервые был окончательно решен Чебышевым [5].

Предварительно заметим, что подстановка

$$x = z^\alpha, \tag{2}$$

где α — общий знаменатель чисел m и n, приводит дифференциал (1) к такому же виду, но где m, n будут целыми числами.

Известно, что интегрирование дифференциала (1) при помощи элементарных функций возможно в трех следующих случаях:

I. p есть целое число. В самом деле, тогда (1) есть рациональная функция.

II. $\frac{m+1}{n}$ есть целое число. В самом деле, тогда подстановка

$$x^n + 1 = z, \qquad x = (z - 1)^{\frac{1}{n}}$$

приведет дифференциал (1) к виду

$$\frac{1}{n} z^p (z - 1)^{\frac{m+1}{n} - 1} \, dz,$$

и после подстановки (2) мы придем к случаю I.

III. $\frac{m+1}{n} + p$ есть целое число. В самом деле, дифференциал (1) можно представить в таком виде:

$$x^{m+np} (1 + x^{-n})^p \, dx. \tag{3}$$

Поступая с этим дифференциалом, как в случае II, мы точно так же придем к случаю I.

Чебышев [5] показал, что интегрирование этого дифференциала при помощи элементарных функций возможно только в этих трех случаях. Для удобства дальнейших рассуждений произведем подстановку

$$x = z^{\frac{1}{n}}:$$

$$\int x^m (x^n + 1)^p \, dx = \frac{1}{n} \int z^{\frac{m+1}{n} - 1} (z + 1)^p \, dz$$

и, вводя обозначения

$$\frac{m+1}{n} - 1 = -r, \qquad p = -s,$$

рассмотрим интеграл

$$\int x^{-r}(x+1)^{-s}\,dx, \tag{4}$$

в котором, как мы предположим, ни r, ни s, ни $r+s$ не являются целыми числами (т. е. не подходят под случай I, II, III).

Из легко проверяемых дифференцированием рекуррентных формул

$$x^{-r+1}(x+1)^{-s+1} = (-r+1)\int x^{-r}(x+1)^{-s}\,dx + \\ +(-r-s+2)\int x^{-r+1}(x+1)^{-s}\,dx, \tag{5}$$

$$x^{-r+1}(x+1)^{-s+1} = -(-s+1)\int x^{-r}(x+1)^{-s}\,dx + \\ +(-r-s+2)\int x^{-r}(x+1)^{-s+1}\,dx \tag{6}$$

мы заключаем, что нахождение интеграла (4) приводится к нахождению таких же интегралов, у которых r или s увеличены (или уменьшены) на единицу. Путем достаточного числа таких редукций мы можем выразить заданный интеграл через алгебраические функции и интеграл типа (4), у которого

$$0<r<1, \qquad 0<s<1.$$

Если при этом

$$r+s>1,$$

то интеграл (4) является интегралом 1-го рода, так как остается конечным при $x=0$, $x=-1$, $x=\infty$. В силу V, он не может быть выражен в конечном виде.

Если

$$r+s<1,$$

то интеграл (4) остается конечным в точках $x=0$ и $x=-1$. При этом вблизи $x=0$ при надлежаще подобранной константе интегрирования он разлагается так:

$$\int x^{-r}(x+1)^{-s}\,dx = \frac{1}{1-r}x^{1-r} - \frac{s}{2-r}x^{2-r} + \ldots, \tag{7}$$

т. е. обращается в нуль с той же скоростью, что и x^{1-r}.

Вблизи точки $x=\infty$ интеграл (4) разлагается так:

$$\int x^{-r}(x+1)^{-s}\,dx = \frac{1}{1-r-s}x^{1-r-s} + \frac{s}{r+s}x^{-r-s} + \ldots, \tag{8}$$

т. е. обращается в бесконечность с той же скоростью, что и x^{1-r-s}.

Допустим, что (4) выражается через элементарные функции. Тогда, в силу VI, как интеграл 2-го рода, он равен алгебраической функции от x. Точно так же произведение

$$x^{r+s-1}\int x^{-r}(x+1)^{-s}\,dx. \tag{9}$$

Но это произведение, в силу (8), при $x = \infty$ остается конечным, при $x = 0$, в силу (7), стремится к нулю, как

$$x^{1-r}x^{r+s-1} = x^s,$$

а при $x = -1$ остается конечным. Таким образом, выражение (9) остается конечным во всех точках римановой поверхности, что, в силу обобщенной теоремы Лиувилля, невозможно. Таким образом, интеграл (4) при сделанных предположениях не может быть выражен в конечном виде, и мы приходим к

Теореме 1 (Чебышева). *Интеграл*

$$\int x^m (x^n + 1)^p \, dx$$

с рациональными показателями m, n, p выражается через элементарные функции тогда и только тогда, когда одно из чисел

$$p, \quad \frac{m+1}{n}, \quad p + \frac{m+1}{n}$$

— целое.

§ 3. О псевдогиперэллиптических интегралах

Выведем результат Абеля [4], касающийся псевдогиперэллиптических интегралов, т. е. интегралов вида

$$\int \frac{(x^\rho + b_1 x^{\rho-1} + \cdots + b_\rho)\, dx}{\sqrt{x^{2\rho+2} + a_1 x^{2\rho+1} + \cdots + a_{2\rho+2}}}, \tag{1}$$

выражаемых через элементарные функции. Абель привел нахождение псевдогиперэллиптических интегралов к вопросу о периодичности разложения радикала

$$\sqrt{R(x)} = \sqrt{x^{2+2\rho} + a_1 x^{2\rho+1} + \cdots + a_{2\rho+2}}$$

в непрерывную дробь. Это не может считаться решением вопроса, так как если после получения сколь угодно большого числа звеньев непрерывной дроби периодичность не обнаруживается, то это не гарантирует, что она не обнаружится на последующих звеньях. Окончательно этот вопрос был решен Золотаревым [2], который, опираясь на созданную им теорию «целых комплексных чисел», привел вопрос к изучению арифметической природы коэффициентов. Впрочем, Золотарев ограничился случаем вещественных коэффициентов. Подробное изложение вопроса содержится в диссертации Пташицкого [3], а результат Абеля весьма просто изложен в статье Долбни [1].

Интеграл (1) как функция от верхнего предела имеет логарифмические бесконечности в обеих точках P_1, P_2, в которых x обращается в бесконечность, и более не имеет особых точек. Отсюда следует,

что в его предполагаемом представлении через элементарные функции алгебраичес кий член отсутствует. Далее, если считать представление

$$\int \frac{b(x)\,dx}{\sqrt{R(x)}} = a_1 \log w_1 + a_2 \log w_2 + \cdots + a_k \log w_k \qquad (2)$$

нормированным, то, в силу IV, каждый член $a_\nu \log w_\nu$ может иметь нули и бесконечности только в точках P_1, P_2, а потому w_ν при представлении через дивизоры выражается так:

$$w_\nu \approx \frac{P_1^{m_\nu}}{P_2^{m_\nu}},$$

где m_ν (положительное или отрицательное) — целое число. Отсюда следует существование показателя m, при котором

$$P_1^m \sim P_2^m. \qquad (3)$$

Будем считать m возможно меньшим положительным показателем такого рода. С точки зрения трансцендентной теории алгебраических функций, это вполне решает вопрос, так как, в силу теоремы Абеля, соотношение (3) равносильно сравнению

$$m \int_{P_1}^{P_2} du_\nu(P) = m u_\nu(P_2) - m u_\nu(P_1) \equiv 0 \qquad (\nu = 1, 2, \ldots, \rho), \qquad (4)$$

где $u_\nu(P)$ — система интегралов 1-го рода, а знак сравнения обозначает, что левая часть (4) равна целочисленной линейной комбинации периодов интеграла $u_\nu(P)$. Это сравнение показывает, что интегралы

$$\int_{P_1}^{P_2} du_\nu(P) \qquad (\nu = 1, 2, \ldots, \rho)$$

должны быть рациональными комбинациями периодов. Конечно, установить сравнение (4) для практического примера представляет собой весьма трудную задачу.

Из того, что m есть наименьший положительный показатель, при котором имеет место (3), следует, что все m_ν делятся на m

$$m_\nu = m q_\nu \qquad (\nu = 1, 2, \ldots, k).$$

Вводя обозначение

$$\frac{P_1^m}{P_2^m} = \varphi(x, \sqrt{R(x)}) = \varphi,$$

мы будем иметь:

$$w_\nu = \varphi^{q_\nu} \qquad (\nu = 1, 2, \ldots, k).$$

Подставляя в равенство (2), получим

$$\int \frac{b(x)\,dx}{\sqrt{R(x)}} = (a_1 q_1 + a_2 q_2 + \cdots + a_k q_k) \log \varphi(x, \sqrt{R(x)}).$$

Обозначим коэффициент $a_1q_1 + a_2q_2 + \cdots + a_kq_k$ через a, а функцию φ представим в форме

$$\varphi(x, \sqrt{R(x)}) = p(x) + q(x)\sqrt{R(x)}, \tag{5}$$

где $p(x)$, $q(x)$ — рациональные функции. Тогда

$$\int \frac{b(x)\,dx}{\sqrt{R(x)}} = a \log(p + q\sqrt{R}).$$

Меняя знак при $\sqrt{R}$ (т. е. переходя к другому листу римановой поверхности), получим

$$-\int \frac{b(x)\,dx}{\sqrt{R(x)}} = a \log(p - q\sqrt{R}).$$

Беря полуразность обоих выражений, будем иметь

$$\int \frac{b(x)\,dx}{\sqrt{R(x)}} = \frac{a}{2} \log \frac{p + q\sqrt{R}}{p - q\sqrt{R}}. \tag{6}$$

Уничтожая дроби в числителе и знаменателе выражения под знаком логарифма, мы можем считать $p(x)$ и $q(x)$ полиномами, и притом взаимно простыми.

Обратно, если имеет место (3), то при заданном полиноме $R(x)$ мы можем подобрать полином ρ-й степени $b(x)$ так, чтобы имело место (6). В самом деле, из представления функции φ через дивизоры следует, что она есть целая относительно x функция, т. е. корень квадратного уравнения

$$\varphi^2 - 2p\varphi + (p^2 - q^2R) = 0, \tag{7}$$

коэффициенты которого должны быть полиномами. Итак, $2p$ и $p^2 - q^2R$ — полиномы. Отсюда p и q^2R — полиномы. Но так как, по предположению, R не имеет кратных корней, то и q есть полином. При этом, в силу сопряженности точек P_1 и P_2, уравнению (7) удовлетворяют функции, представляемые через дивизоры так:

$$\varphi \approx \frac{P_1{}^m}{P_2{}^m}, \qquad \varphi' \approx \frac{P_2{}^m}{P_1{}^m},$$

откуда следует

$$\varphi\varphi' = \text{const}.$$

Нормируя при $p(x)$ и $q(x)$ числовой множитель, мы можем получить $\varphi\varphi' = 1$, т. е.

$$p^2(x) - q^2(x)R(x) = 1. \tag{8}$$

Дифференцируем правую часть формулы (6)

$$\frac{d}{dx}\left(\log \frac{p + q\sqrt{R}}{p - q\sqrt{R}}\right) = \frac{2(pq' - p'q)R + pqR'}{2\sqrt{R}}. \tag{9}$$

С другой стороны, дифференцируя (8)

$$2pp' - q(2q'R + qR') = 0, \tag{10}$$

мы видим, что pp' делится на q. Но так как p и q взаимно просты, то p' делится на q:

$$p' = qr. \tag{11}$$

Преобразуя (9) при помощи (8), (10) и (11), будем иметь

$$\frac{d}{dx}\left(\log\frac{p+q\sqrt{R}}{p-q\sqrt{R}}\right) = \frac{p'}{q\sqrt{R}} = \frac{r}{\sqrt{R}}.$$

Но из (8) видно, что степень $p(x)$ превышает степень $q(x)$ на $\rho+1$ единиц, в силу чего $r(x)$ есть полином ρ-й степени. Поэтому можно подобрать полином $b(x)$ так, чтобы имело место (6).

Итак, задача привелась к решению в полиномах неопределенного уравнения (8), аналогичного уравнению Пелля в теории чисел. Покажем, что уравнение (8) имеет решение тогда и только тогда, если $\sqrt{R(x)}$ разлагается в периодическую непрерывную дробь (к сожалению, в теории полиномов это случается не всегда). В дальнейшем будем предполагать известной арифметическую теорию непрерывных дробей. По аналогии с ней, мы можем разлагать в непрерывные дроби и аналитические функции, допускающие разложения вблизи точки $x = \infty$. Будем называть *степенью* функции $f(x)$ и обозначать символом $\delta f(x)$ показатель наивысшей степени ее разложения по убывающим степеням x. Имеет место

$$\delta\{f(x)+g(x)\} \leqslant \operatorname{Max}\{\delta f(x), \delta g(x)\},$$
$$\delta\{f(x)\,g(x)\} = \delta f(x) + \delta g(x).$$

Далее, под *целой частью* $[f(x)]$ функции $f(x)$ мы будем разуметь сумму ее членов разложения, имеющих неотрицательные степени. $[f(x)]$ вполне определяется равенством

$$\delta\{f(x) - [f(x)]\} < 0. \tag{12}$$

Разложение функции $f(x)$ в непрерывную дробь производится так. Определяют целую часть (полином) функции $f(x)$, а затем определяют функцию $f_1(x)$ равенством

$$f(x) = a_1 + \frac{1}{f_1(x)}.$$

Ясно, что $\delta f_1(x) > 0$. Затем определяют целую часть a_2 функции $f_1(x)$ и функцию $f_2(x)$ равенством

$$f_1(x) = a_2 + \frac{1}{f_2(x)}.$$

Продолжая процесс, мы получим для $f(x)$ выражение

$$f(x) = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{f_n(x)}}} \tag{13}$$

для любого n. Здесь $a_1, a_2, \ldots, a_n$ — полиномы, а $\delta f_n(x) > 0$. Такое выражение называется *непрерывной дробью*, полиномы $a_1, a_2, \ldots, a_n$ — ее *звеньями*, а функции $f_n(x)$ — *полными частными*.

Отрезок непрерывной дроби

$$\frac{P_n}{Q_n} = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}, \tag{14}$$

приведенный к виду несократимой дроби $\frac{P_n}{Q_n}$, носит название ее n-й *подходящей дроби*. Ее числители и знаменатели могут быть определяемы соотношениями

$$P_n = P_{n-1}\, a_n + P_{n-2}\,, \qquad Q_n = Q_{n-1}\, a_n + Q_{n-2}\,. \tag{15}$$

Имеет место

$$P_n Q_{n-1} - Q_n P_{n-1} = (-1)^n. \tag{16}$$

Из (15) видно, что

$$\delta P_n > \delta P_{n-1}\,, \qquad \delta Q_n > \delta Q_{n-1}\,, \tag{17}$$

поскольку a_n — полиномы не ниже 1-й степени (только a_1 может быть константой и даже нулем). Очевидно также, что

$$\delta P_n \geqslant n - 2, \qquad \delta Q_n \geqslant n - 1. \tag{18}$$

Вычислим степень разности $f(x) - \frac{P_n}{Q_n}$. Вычисляя конечную непрерывную дробь (13) [с последним звеном $f_n(x)$] по правилу (15), будем иметь:

$$f(x) = \frac{P_n f_n(x) + P_{n-1}}{Q_n f_n(x) + Q_{n-1}}\,.$$

Отсюда

$$f(x) - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^n f_n(x)}{Q_{n-1}\,(Q_n f_n(x) + Q_{n-1})}\,,$$

а также

$$f(x) - \frac{P_n}{Q_n} = \frac{(-1)^{n-1}}{Q_n\,(Q_n f_n(x) + Q_{n-1})}\,.$$

Отсюда следует, в силу (18),

$$\delta\left\{ f(x) - \frac{P_n}{Q_n} \right\} \leqslant -(2n-1), \tag{19}$$

а также

$$\delta\left\{f(x)-\frac{P_n}{Q_n}\right\}\leqslant\delta\left\{f(x)-\frac{P_{n-1}}{Q_{n-1}}\right\}-2. \tag{20}$$

Справедливо и обратное: если для какой-нибудь рациональной дроби $\frac{P}{Q}$ имеет место

$$\delta Q=m-1,\qquad \delta\left\{f(x)-\frac{P}{Q}\right\}\leqslant-(2m-1), \tag{21}$$

то $\frac{P}{Q}$ есть подходящая дробь разложения функции $f(x)$.

Чтобы доказать это, разложим $\frac{P}{Q}$ в непрерывную дробь:

$$\frac{P}{Q}=a_1+\frac{1}{a_2+}\cdots+\frac{1}{a_n}$$

и определим $f_n(x)$ при помощи равенства

$$f(x)=a_1+\frac{1}{a_2+}\cdots+\frac{1}{a_n+}\frac{1}{f_n(x)}, \tag{22}$$

т. е.

$$f(x)=\frac{Pf_n(x)+P_{n-1}}{Qf_n(x)+Q_{n-1}},\qquad f_n(x)=\frac{Q_{n-1}\left\{\frac{P_{n-1}}{Q_{n-1}}-f(x)\right\}}{Q\left\{f(x)-\frac{P}{Q}\right\}}. \tag{23}$$

Но

$$\frac{P_{n-1}}{Q_{n-1}}-f(x)=\left(\frac{P}{Q}-f(x)\right)-\frac{(-1)^n}{Q_{n-1}Q},$$

откуда, в силу (21) и

$$\delta\left(\frac{1}{Q_{n-1}Q}\right)\geqslant-(m-1)-(m-2)=-(2m-3),$$

мы будем иметь

$$\delta\left\{\frac{P_{n-1}}{Q_{n-1}}-f(x)\right\}=-\delta Q_{n-1}-\delta Q,$$

так что второе равенство (23) даст нам

$$\delta f_n(x)\geqslant\delta Q_{n-1}+(-\delta Q_{n-1}-\delta Q)-\delta Q+(2m-1)=1.$$

Из равенства же (13), $\delta f_n(x)\geqslant 1$, и того, что a_ν — полиномы, мы постепенно заключаем, что

$$\left[a_n+\frac{1}{f_n(x)}\right]=a_n,\qquad \left[a_{n-1}+\frac{1}{a_n+}\frac{1}{f_n(x)}\right]=a_{n-1}\qquad \text{и т. д.},$$

а это показывает, что (22) есть разложение $f(x)$ в непрерывную дробь, а $\frac{P}{Q}$ — n-я подходящая.

Приложим этот результат к решению p, q уравнения (8). Перепишем его так:

$$p - q\sqrt{R(x)} = \frac{1}{p + q\sqrt{R(x)}}. \tag{24}$$

Не может быть, чтобы степени $p - q\sqrt{R(x)}$ и $p + q\sqrt{R(x)}$ были одинаковы, так как тогда они равны нулю и степень их суммы, т. е. $2p$, тоже не превышала бы нуля. Нормируем знак при $\sqrt{R(x)}$ так, чтобы

$$\delta(p - q\sqrt{R(x)}) < 0, \qquad \delta(p + q\sqrt{R(x)}) > 0.$$

Представим (24) так:

$$\frac{p}{q} - \sqrt{R(x)} = \frac{1}{q(p + q\sqrt{R(x)})}.$$

Если $\delta q = m - 1$, то $\delta p = (m-1) + (\rho + 1) = m + \rho$.

Из $\quad \delta 2p \leqslant \operatorname{Max}\{\delta(p + q\sqrt{R}), \quad \delta(p - q\sqrt{R})\} = \delta(p + q\sqrt{R})$

следует

$$\delta(p + q\sqrt{R}) \geqslant \delta p = m + \rho,$$

откуда

$$\delta\left(\frac{p}{q} - \sqrt{R(x)}\right) \leqslant -(m-1) - (m+\rho) \leqslant -(2m-1),$$

так что из доказанного мы заключаем, что $\frac{p}{q}$ есть подходящая дробь разложения $\sqrt{R(x)}$ в непрерывную дробь. Пусть

$$\frac{p}{q} = a_1 + \frac{1}{a_2 + \ddots + \frac{1}{a_n}}, \qquad \sqrt{R(x)} = a_1 + \frac{1}{a_2 + \ddots + \frac{1}{a_n + \frac{1}{f_n(x)}}}. \tag{25}$$

Представим $f_n(x)$ в форме $\frac{\alpha}{\gamma} + \frac{\beta}{\gamma}\sqrt{R}$, где α, β, γ — полиномы от x. Из второго равенства (25) имеем

$$\sqrt{R(x)} = \frac{pf_n(x) + P_{n-1}}{qf_n(x) + Q_{n-1}},$$

откуда

$$q\frac{\alpha}{\gamma}\sqrt{R(x)} + q\frac{\beta}{\gamma}R(x) + Q_{n-1}\sqrt{R(x)} = p\frac{\alpha}{\gamma} + p\frac{\beta}{\gamma}\sqrt{R(x)} + P_{n-1}.$$

Если $\sqrt{R(x)}$ есть иррациональная функция, то это равенство должно быть тождеством относительно $\sqrt{R(x)}$, так что

$$\begin{cases} q\frac{\alpha}{\gamma} + Q_{n-1} = p\frac{\beta}{\gamma}, \\ p\frac{\alpha}{\gamma} + P_{n-1} = q\frac{\beta}{\gamma}R(x). \end{cases} \tag{26}$$

Умножая первое из равенств на p, второе на $-q$ и складывая, получим

$$(-1)^n = \frac{\beta}{\gamma}(p^2 - q^2 R(x)),$$

так что тождество (8) равносильно тождеству

$$\frac{\beta}{\gamma} = (-1)^n.$$

При этом, если выполняется (8), то из равенств (26) вытекает, что, в силу взаимной простоты p и q, дробь $\frac{\alpha}{\gamma}$ равна полиному

$$\frac{\alpha}{\gamma} = b, \qquad f_n(x) = \frac{\alpha}{\gamma} + \frac{\beta}{\gamma}\sqrt{R(x)} = b + (-1)^n \sqrt{R(x)}.$$

Подставляя в (25) выражение для $f_n(x)$, где $\sqrt{R(x)}$ предположим опять разложенным в непрерывную дробь, мы убедимся, что разложение $\sqrt{R(x)}$ в случае четного n имеет период

$$[a_1, (a_2, a_3, \ldots, a_n, b + a_1)], \tag{27}$$

а в случае нечетного n имеет период

$$[a_1, (a_2, \ldots, a_n, b - a_1, -a_2, \ldots, -a_n, -b + a_1)]. \tag{28}$$

Итак, чтобы неопределенное уравнение (8) имело решение в полиномах, необходимо и достаточно, чтобы $\sqrt{R(x)}$ разлагался в периодическую непрерывную дробь одного из типов (27) и (28); другими словами, чтобы период начинался со 2-го звена.

Докажем, что всякое периодическое разложение $\sqrt{R(x)}$ имеет именно эту форму. Для этого мы убедимся, что:

1) все f_n имеют форму $\frac{\alpha_n + \sqrt{R}}{\gamma_n}$, где α_n и γ_n — полиномы, причем γ_n есть делитель $\alpha_n^2 - R$;

2) сопряженные с f_n функции f_n' имеют степень < 0, начиная с $n = 1$.

Чтобы доказать 1), обратим внимание, что f_1 удовлетворяет 1): из

$$\sqrt{R} = a_1 + \frac{1}{f_1}$$

мы имеем

$$f_1 = \frac{1}{\sqrt{R} - a_1} = \frac{a_1 + \sqrt{R}}{R - a_1^2}.$$

Пусть $f_{n-1} = a_n + \frac{1}{f_n}$ удовлетворяет 1). Тогда

$$f_n = \frac{1}{f_{n-1} - a_{n-1}} = \frac{1}{\frac{\sqrt{R} + \alpha_{n-1} - a_n \gamma_{n-1}}{\gamma_{n-1}}} = \frac{\gamma_{n-1}(\sqrt{R} - \alpha_{n-1} + a_n \gamma_{n-1})}{R - (\alpha_{n-1} - a_n \gamma_{n-1})^2}.$$

При этом, из нашего предположения следует, что $R-\alpha_{n-1}^2$ и потому $R-(\alpha_{n-1}-a_n\gamma_{n-1})^2$ делится на γ_{n-1}. Сокращая выражение для f_n на γ_{n-1}, мы получим выражение, удовлетворяющее 1). Индукция установлена.

Для доказательства 2) для $n=1$ имеем

$$f_1'=\frac{1}{-\sqrt{R}-a_1}, \text{ откуда } \delta f_1'<0.$$

Предположим, что $\delta f'_{n-1}<0$. Тогда $f'_{n-1}=a_n+\frac{1}{f_n'}$, откуда

$$f_n'=\frac{1}{f'_{n-1}-a_n}.$$

Но $\delta(f'_{n-1}-a_n)=\delta a_n>0$, откуда $\delta f_n'<0$. Индукция установлена.

Равенства

$$f'_{n-1}-a_n=\frac{1}{f_n'}, \quad \delta f'_{n-1}<0$$

показывают, что a_n вполне определяется как целая часть от $\frac{1}{f_n'}$.

Таким образом, если непрерывная дробь — периодическая, начиная с $n=n_0$, т. е. если $f_{n_0}=f_{n_0+p}$, то и $f_{n_0-1}=f_{n_0+p-1}$ и т. д., вплоть до $f_1=f_{p+1}$, $f_p\neq f$, так как $f=\sqrt{R}$ уже не удовлетворяет свойству 2).

Пусть

$$f_{p+1}=f_1=\frac{1}{\sqrt{R}-a_1}.$$

Тогда

$$f'_p=\frac{1}{f'_{p+1}}+a_{p+1}=-\sqrt{R}-a_1+a_{p+1}.$$

Из $\delta f_p'<0$ следует, что $-a_1+a_{p+1}=[\sqrt{R}]=a_1$, откуда $a_{p+1}=2a$. Таким образом, в дробях (27) и (28) соответственно $b=a_1$ и $b=-a_1$.

Сопоставляя все наши выводы, мы приходим к следующему результату Абеля:

Теорема 2 (Абеля). *Чтобы для данного полинома $R(x)$ степени $2\rho+2$ существовал такой полином $b(x)$ степени ρ, что интеграл*

$$\int\frac{b(x)}{\sqrt{R(x)}}dx$$

выражается в элементарных функциях, необходимо и достаточно, чтобы $\sqrt{R(x)}$ разлагался в периодическую непрерывную дробь.

§ 4. О результате Золотарева

В своей докторской диссертации Золотарев [2] предложил прием, позволяющий всегда при помощи конечного числа действий определить, является ли интеграл

$$\int \frac{x+A}{\sqrt{R(x)}}\,dx, \tag{1}$$

где $R(x)$ — заданный полином 4-й степени, псевдоэллиптическим. Откладывая упрощенный вывод полного результата Золотарева до следующей статьи, я ограничусь приведением алгоритма, который дает критерий для узнавания, является ли интеграл (1) псевдоэллиптическим, не доказывая, что после конечного числа действий мы не преминенно придем к одному из этих критериев.

Обратимся к данному формулой (4) § 3 критерию псевдоэллиптичности интеграла (1). В случае $\rho = 1$ он имеет вид

$$m\,u(P_1) - m\,u(P_2) \equiv 0, \tag{2}$$

где $u(P)$ — единственный в этом случае интеграл 1-го рода.

Пусть

$$R(x) = (x-x_1)(x-x_2)(x-x_3)(x-x_4).$$

Подвергнем x дробной линейной подстановке, переводящей x_1, x_2, x_3, x_4 соответственно в x_1', x_2', x_3', x_4'. Точки x_1', x_2', x_3', x_4' нельзя задать вполне произвольно, поскольку между ними имеет место соотношение

$$\frac{(x_1-x_2)(x_3-x_4)}{(x_1-x_3)(x_2-x_4)} = \frac{(x_1'-x_2')(x_3'-x_4')}{(x_1'-x_3')(x_2'-x_4')}. \tag{3}$$

Полагая

$$x_3 = x, \qquad x_4 = x+dx, \qquad x_3' = x', \qquad x_4' = x'+dx',$$

будем из (3) иметь

$$\frac{(x_1-x_2)\,dx}{(x-x_1)(x-x_2)} = \frac{(x_1'-x_2')\,dx'}{(x'-x_1')(x'-x_2')}$$

и точно так же $$\frac{(x_3-x_4)\,dx}{(x-x_3)(x-x_4)} = \frac{(x_3'-x_4')\,dx'}{(x'-x_3')(x'-x_4')}.$$

Перемножая эти равенства и извлекая корень, получим

$$\frac{\sqrt{(x_1-x_2)(x_3-x_4)}\,dx}{\sqrt{(x-x_1)(x-x_2)(x-x_3)(x-x_4)}} = \frac{\sqrt{(x_1'-x_2')(x_3'-x_4')}\,dx'}{\sqrt{(x'-x_1')(x'-x_2')(x'-x_3')(x'-x_4')}}. \tag{4}$$

Это формула линейного преобразования эллиптических интегралов.

Положим

$$x_1' = 1, \qquad x_2' = 0, \qquad x_3' = \infty, \qquad x_4' = \frac{1}{k^2}.$$

Из формулы (3) получим

$$k^2 = \frac{(x_1 - x_2)(x_3 - x_4)}{(x_1 - x_3)(x_2 - x_4)}, \tag{5}$$

а формула (4) дает

$$\frac{dx'}{\sqrt{x'(1-x')(1-k^2x')}} = \frac{\sqrt{(x_1 - x_2)(x_3 - x_4)}\,dx}{k\sqrt{R(x)}}. \tag{6}$$

После подстановки $x' = y^2$ и использования формулы (5) получим

$$\frac{dy}{\sqrt{(1-y^2)(1-k^2y^2)}} = \frac{\sqrt{(x_1 - x_3)(x_4 - x_2)}\,dx}{2\sqrt{R(x)}}. \tag{7}$$

Обозначая это общее отношение через du, будем иметь

$$y = \operatorname{sn} u,$$

откуда

$$x' = \operatorname{sn}^2 u, \qquad 1 - x' = \operatorname{cn}^2 u, \qquad 1 - k^2x' = \operatorname{dn}^2 u.$$

Найдем значение x' в точках P_1 и P_2, в которых $x = \infty$. Для этого положим в формуле (3)

$$x'_1 = 1, \qquad x_2' = 0, \qquad x'_3 = \infty, \qquad x_4' = x', \qquad x_4 = \infty:$$

$$x' = \frac{x_1 - x_3}{x_1 - x_2},$$

откуда

$$\operatorname{sn} u(P_i) = \pm\sqrt{\frac{x_1 - x_3}{x_1 - x_2}}, \quad \operatorname{cn} u(P_i) = \pm\sqrt{\frac{x_2 - x_3}{x_1 - x_2}}, \tag{8}$$

$$\operatorname{dn} u(P_i) = \pm\sqrt{\frac{x_2 - x_3}{x_2 - x_4}} \qquad (i = 1, 2).$$

Заметим, что, в силу (4), $u(P_1)$ и $u(P_2)$ имеют разные знаки

$$u(P_1) \equiv -u(P_2),$$

так что критерий (2) устанавливает соизмеримость с периодами аргумента u, которому соответствуют значения sn, cn, dn, данные в формулах (8). Чтобы узнать, имеет ли место эта соизмеримость, мы можем вычислять по формулам сложения

$$\operatorname{sn} 2u, \operatorname{cn} 3u, \ldots$$

Если она имеет место, то на некотором шаге нашего процесса мы должны получить

$$\operatorname{sn} mu = 0.$$

Золотарев предпочитает удваивать аргумент, пользуясь формулой удвоения

$$\operatorname{sn} 2u = \frac{2\operatorname{sn} u \operatorname{cn} u \operatorname{dn} u}{1 - k^2 \operatorname{sn}^4 u}. \tag{9}$$

Удобнее пользоваться ею так: введем обозначение

$$\operatorname{sn}^2 2^k u = \lambda(2^k u). \tag{10}$$

Полагая в формуле (9) $2^k u$ вместо u, возводя ее в квадрат и вводя обозначения (10), будем иметь

$$\lambda(2^{k+1}u) = \frac{4\lambda(2^k u)[1-\lambda(2^k u)][1-k^2\lambda(2^k u)]}{[1-k^2\lambda^2(2^k u)]^2}. \tag{11}$$

Далее, полагая

$$k^2 = \frac{\mu}{\nu}, \qquad \lambda(2^k u) = \frac{a_k}{b_k},$$

мы из формулы (11) получим

$$\begin{aligned} a_{k+1} &= 4\nu a_k b_k (b_k - a_k)(\nu b_k - \mu a_k), \\ b_{k+1} &= (\nu b_k^2 - \mu a_k^2)^2. \end{aligned} \tag{12}$$

Будем различать два случая периодичности:

I. Период m есть нечетное число. Тогда, полагая

$$s = \varphi(m),$$

где $\varphi(m)$ — функция Эйлера, мы получим

$$2^s \equiv 1 \pmod{m},$$

откуда

$$\lambda(2_s u) = \lambda(u),$$

$$\frac{a_s}{b_s} = \frac{a_0}{b_0}.$$

Это показывает, что период последовательности $\frac{a_k}{b_k}$ — чистый, т. е. начинается с первого же члена. Для нас важно установить, когда этот случай невозможен. Пусть для некоторого $k \geqslant 1$ в числителе или знаменателе дроби $\frac{a_k}{b_k}$ появится простой идеальный множитель, взаимно простой с $2\mu\nu$. Тогда из формул (12) следует, что во всех дальнейших членах

$$\frac{a_{k+1}}{b_{k+1}}, \quad \frac{a_{k+2}}{b_{k+2}}, \ldots$$

этот идеал будет непременно входить в числитель, так что чистая периодичность наверное не будет иметь места.

II. Период m есть четное число: $m = 2^{\mu_0} m'$, где m' — нечетное число. Тогда, полагая

$$s = \varphi(m'),$$

откуда

$$2^s \equiv 1 \pmod{m'},$$

мы будем иметь

$$\lambda(2^{s+\mu_0}u) = \lambda(2^{\mu_0}u),$$

т. е. период будет иметь s членов и начинаться с (μ_0+1)-го члена.

Для этого случая Золотарев вывел критерий; если он не соблюдается, то мы будем иметь или случай I, или непсевдоэллиптический случай. Выведем этот критерий. В этом случае полиномы $p(x)$ и $q(x)$ — четной степени. Представим уравнение (8) § 3 так:

$$(p+1)(p-1) = q^2R.$$

Могут встретиться два случая: 1) один из полиномов $p+1$, $p-1$ делится на R; 2) $p+1$ и $p-1$ делятся на квадратичные множители полинома R.

1. Пусть $p+1$ делится на R. Так как $p+1$ и $p-1$ взаимно просты, то

$$p+1 = u^2R, \qquad p-1 = v^2,$$

где

$$uv = q.$$

Отсюда

$$2 = u^2R - v^2.$$

Нормируя при u, v численные множители, мы видим, что уравнение (8) § 3 удовлетворяется при более низких степенях полиномов, чем p, q, чего мы не будем предполагать.

2. Пусть

$$R = R_1R_2,$$

причем

$$R_1 = (x-x_1)(x-x_2), \qquad R_2 = (x-x_3)(x-x_4),$$

и пусть

$$p+1 = u^2R_1, \qquad p-1 = v^2R_2. \tag{13}$$

Отсюда

$$2 = u^2R_1 - v^2R_2.$$

Полагая

$$x = x_1, x_2, x_3, x_4,$$

получим

$$\left.\begin{aligned} -v^2(x_1)(x_1-x_3)(x_1-x_4) &= 2; & -v^2(x_2)(x_2-x_3)(x_2-x_4) &= 2;\\ u^2(x_3)(x_3-x_1)(x_3-x_2) &= 2; & u^2(x_4)(x_4-x_1)(x_4-x_2) &= 2. \end{aligned}\right\} \tag{14}$$

Вместе с тем учтем, что $p(x)$ и $q(x)$ находятся при помощи алгоритма непрерывных дробей, а потому их коэффициенты рационально выражаются через коэффициенты полинома $R(x)$. Далее, из формул (13) следует, что коэффициенты полиномов $u(x)$, $v(x)$ лишь общим множителем отличаются от рациональных функций от x_1, x_2, x_3, x_4, в силу чего произведения и частные пар выражений $u(x_i)$, $v(x_i)$ рационально выражаются через x_1, x_2, x_3, x_4. Имея это в виду и попарно перемножая и деля формулы (14) друг на друга, мы убедимся, что

$$\sqrt{(x_1-x_4)(x_2-x_3)}, \qquad \sqrt{(x_1-x_3)(x_2-x_4)}$$

рационально выражаются через x_1, x_2, x_3, x_4. Если это условие не соблюдается, т. е. если из трех величин

$$\sqrt{(x_1-x_2)(x_3-x_4)}, \qquad \sqrt{(x_1-x_4)(x_2-x_3)}, \qquad \sqrt{(x_1-x_3)(x_2-x_4)}$$

ни одна или одна рационально выражается через x_1, x_2, x_3, x_4, то случай II наверное не имеет места. Отсюда следует, что дополнительный модуль

$$k'^2 = 1 - k^2 = \frac{(x_1-x_4)(x_2-x_3)}{(x_1-x_3)(x_2-x_4)}$$

является квадратом рациональной функции от x_1, x_2, x_3, x_4.

Если это условие удовлетворяется, Золотарев применяет к интегралу преобразование Ландена, которое, как известно, преобразует дополнительный модуль в величину

$$\frac{2\sqrt{k'}}{1+k'}.$$

Далее, Золотарев показывает, что после нескольких преобразований Ландена мы придем к величине дополнительного модуля, которая уже не выражается рационально через x_1, x_2, x_3, x_4. Это служит признаком, что мы имеем или случай I, или неприводоэллиптический интеграл. Для различения двух последних случаев мы имели уже критерий. Золотарев показывает, что после нескольких указанных нами преобразований мы или обнаружим периодичность процесса, или придем к a_k, делящемуся на простой идеал, не входящий в $2\mu\nu$, что исключит возможность периодичности.

Все свое исследование Золотарев проводил в предположении, что коэффициенты полинома $R(x)$ вещественны. Это ограничение существенно только для преобразования Ландена.

ЛИТЕРАТУРА

1. И. П. Долбня. Новое доказательство теоремы Абеля, относящееся к интегрированию дифференциалов вида $\frac{\rho dx}{\sqrt{R}}$; ρ и R — целые функции. Собр. прот. зас. секции физ.-мат. наук Об-ва естеств. при Каз. ун-те, **6**, 1880, стр. 307—324.
2. Е. И. Золотарев. Теория целых комплексных чисел с приложением к интегральному исчислению. Докт. дисс., СПб., 1874. См. также Полное собр. соч., в. 1. Л., 1931, стр. 161—360.
3. И. Л. Пташицкий. Об интегрировании в конечном виде эллиптических дифференциалов, СПб., 1888.
4. N. H. Abel. Sur l'intégration de la formule différentielle $\frac{\rho dx}{\sqrt{R}}$, R et ρ étant des fonctions entières. Journ. f. reine u. ang. Math. **1**, 1926, стр. 185—221; Oeuvres complètes. 1, Kristiania (1881), стр. 104—144.
5. P. Tschebycheff. Sur l'intégration des différentielles irrationelles. Journ. de math. pures et appl. (1) **18**, 1853, стр. 87—111. Oeuvres, I, St.-Pétersbourg, 1899, стр. 147—168.

ОБ ОДНОЙ АЛГЕБРАИЧЕСКОЙ ПРОБЛЕМЕ ГИЛЬБЕРТА. I

(ÜBER EIN ALGEBRAISCHES PROBLEM VON HERRN HILBERT. I)

(Math. Ann. **104** (1931), стр. 459—471)

Д. Гильберт посвятил недавно изящную работу [1] одному вопросу, поставленному ранее им самим [2].

Пусть дано алгебраическое уравнение n-й степени

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_{n-1} x + p_n = 0 \qquad (1)$$

с неограниченно переменными коэффициентами $p_1, p_2, \ldots, p_n$. Требуется найти такое уравнение (резольвенту) n-й степени

$$\varphi(y) = y^n + \Pi_1 y^{n-1} + \ldots + \Pi_{n-1} y + \Pi_n = 0, \qquad (2)$$

чтобы каждый из корней $x_1, x_2, \ldots, x_n$ уравнения (1) при подходящем выборе значений $\Pi_1, \Pi_2, \ldots, \Pi_n$ рационально выражался через корни уравнения (2) (или с помощью заданной рациональной функции Φ корней $x_1, x_2, \ldots, x_n$, принадлежащей данной подгруппе группы Галуа уравнения (1), например с помощью $\sqrt{D}$, где D — дискриминант уравнения (1)) и функции $\Pi_1, \Pi_2, \ldots, \Pi_n$ зависели от возможно меньшего числа k параметров. При этом $p_1, p_2, \ldots, p_n$ следует считать принадлежащими к области рациональности.

С помощью весьма искусных методов Гильберт нашел для k следующие значения:

$$n = 5\ 6\ 7\ 8\ 9,$$
$$k \leqslant 1\ 2\ 3\ 4\ 4.$$

В этой работе я намереваюсь дать общее решение этой проблемы. Для этого я пользуюсь теорией непрерывных групп преобразований (в последующем обозначаемых кратко н. г. п.). Именно, я ищу решение проблемы «одевания» конечных групп, т. е. отыскания н. г. п. с возможно меньшим числом параметров, содержащей данную группу как делитель [3].

Если мы «оденем» группу Галуа $\mathfrak{G}$ уравнения (1) посредством н. г. п. Γ, то оказывается, что искомое число k равно измерению наименьшего пространства, в котором можно представить Γ так, чтобы подстановкам $\mathfrak{G}$ соответствовали нетривиальные (т. е. отличные от тождественного преобразования) преобразования этого представления.

Как пример рассмотрим уравнение пятой степени. Пусть $\mathfrak{G}$ — его знакопеременная группа. Она, как известно, изоморфна с группой икосаэдра. Но группа икосаэдра есть группа наибольшего порядка, которую можно представить как группу дробных линейных преобразований. С другой стороны, каждая н. г. п. одномерного пространства изоморфна некоторому делителю группы дробных линейных преобразований. Это значит, во-первых, что можно найти резольвенту пятой степени, коэффициенты которой зависят только от одного параметра. Это обстоятельство хорошо известно [4], и именно оно навело меня на мысль об указанной зависимости для уравнений произвольной степени.

Во-вторых, мы заключаем, что никакое общее уравнение высшей степени не может быть приведено к однопараметрической резольвенте.

В § 1 я исследую вопрос одевания конечных групп посредством н. г. п. В основном этот вопрос может быть сведен к проблеме итераций [5, 6]. Я показываю, что всякая группа преобразований конечного порядка может быть одета с помощью некоторого итерационного процесса. В частности, если итерируемые преобразования линейны (что имеет место, например, для группы подстановок), то можно найти линейную итерационную функцию, так что получение ее не представляет никаких трудностей.

В § 2 я привожу задачу представления н. г. п. в пространстве возможно меньшего числа измерений к задаче отыскания определенных систем импримитивности. Задача эта полностью решена С. Ли и Ф. Энгелем [7]. Решение требует применения только алгебраических операций.

В § 3 я решаю поставленную проблему резольвент. Для этого я одеваю группу Галуа уравнения (1) посредством н. г. п. и затем нахожу описанное в § 2 подпространство. Важно заметить, что все эти задачи решаются посредством только алгебраических операций. Но чтобы доказать, что этим способом мы получаем все возможные решения проблемы, необходимы некоторые условия относительно голоморфности рассматриваемых функций.

§ 1. Одевание конечных групп посредством н. г. п.

Пусть дана конечная группа $\mathfrak{G}$. Требуется найти такую н. г. п. Γ с возможно меньшим числом параметров, которая содержала бы $\mathfrak{G}$ как делитель. Это значит, что некоторые преобразования группы Γ, соответствующие определенным системам значений $A_1, \cdot A_2, \cdots, A_s$ параметров этой группы (мы будем говорить: точкам $A_1 \cdot A_2 \cdots A_s$ *параметрического пространства*), образуют группу порядка m, изоморфную группе $\mathfrak{G}$.

В основном задача эта решена Бернсайдом [3] и Ле-Вавассером [8]. Избранный мной путь отличается тем, что я беру за основу не

абстрактные элементы, но определенные функциональные преобразования. Если, например, дана группа подстановок $\mathfrak{G}$, то я рассматриваю ее подстановки $\begin{pmatrix} x_1, & x_2, & \ldots, & x_n \\ x_{\alpha_1}, & x_{\alpha_2}, & \ldots, & x_{\alpha_n} \end{pmatrix}$ как некоторые линейные преобразования переменных $x_1, x_2, \ldots, x_n$.

Рассмотрим сначала случай, когда группа $\mathfrak{G}$ циклическая. Пусть дано преобразование

$$\begin{aligned} x_1' &= f_1(x_1, x_2, \ldots, x_n), \\ x_2' &= f_2(x_1, x_2, \ldots, x_n), \\ &\ldots\ldots\ldots\ldots \\ x_n' &= f_n(x_1, x_2, \ldots, x_n). \end{aligned} \tag{1}$$

Требуется найти такую однопараметрическую н. г. п., чтобы преобразования ее при нулевом значении параметра t обращались в тождественное преобразование $x_i' = x_i$ $(i = 1, 2, \ldots, n)$, а при $t = 1$ — в преобразование (1). Иными словами, мы ищем систему функций $f_1(x_1, x_2, \ldots, x_n, t), f_2(x_1, x_2, \ldots, x_n, t), \ldots, f_n(x_1, x_2, \ldots, x_n, t)$, удовлетворяющую следующим условиям:

$$\begin{aligned} &\text{A. } f_\mu(x_1, x_2, \ldots, x_n, 0) = x_\mu, \\ &\text{B. } f_\mu(x_1, x_2, \ldots, x_n, 1) = f_\mu(x_1, x_2, \ldots, x_n), \\ &\text{C. } f_\mu(f_1(x, t), f_2(x, t), \ldots, f_n(x, t), u) = \\ &= f_\mu(x_1, x_2, \ldots, x_n, t + u) \qquad (\mu = 1, 2, \ldots, n). \end{aligned}$$

При этом мы предполагаем, что функции (1) — аналитические.

Сначала будем искать *неподвижную точку* преобразования (1), т. е. такую систему значений $x_1, x_2, \ldots, x_n$, для которой

$$x_1 = f_1(x_1, x_2, \ldots, x_n), \quad x_2 = f_2(x_1, x_2, \ldots, x_n), \ldots,$$
$$x_n = f_n(x_1, x_2, \ldots, x_n).$$

При этом мы оставим вне рассмотрения случай, когда преобразования (1) не имеют неподвижной точки. В частности, если функции f_μ рациональны, то мы непременно будем иметь неподвижную точку, может быть, соответствующую бесконечным значениям x_i. Если, например, $x_i = \infty$, то мы введем вместо x_i переменное $z_i = \frac{1}{x_i}$.

Не нарушая общности выводов, мы можем всегда считать, что неподвижной будет точка $x_1 = x_2 = \ldots = x_n = 0$. Функции (1) развернем в степенные ряды

$$\begin{aligned} x_1' &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n + b_{111}x_1^2 + \ldots \\ x_2' &= a_{21}x_1 + a_{22}x_2 + a_{2n}x_n + b_{211}x_1^2 + \ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n' &= a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n + b_{n11}x_1^2 + \ldots. \end{aligned} \tag{1'}$$

Мы ограничимся преобразованиями, для которых точка $x_1 = x_2 = \ldots = x_n = 0$ также является неподвижной точкой. Если преобра-

зование (1′) имеет конечный (m-й) порядок, т. е. его m-я итерация дает тождественное преобразование, то определитель матрицы (a_{ik}) (мы будем говорить: матрицы, отнесенной преобразованию (1′)) не равен нулю. Действительно, матрица, отнесенная m-й итерации, очевидно, будет $(a_{ik})^m$. С другой стороны, она равна

$$I = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Кроме того, известно, что характеристическая матрица $(a_{ik}) - \lambda I$ матрицы конечного порядка (т. е. матрицы, для которой существует такое целое число m, что $(a_{ik})^m = I$) имеет только простые элементарные делители и потому посредством некоторого линейного преобразования может быть приведена в диагональную форму. Поэтому мы можем подходяще выбранным преобразованием переменных $x_1, x_2, \dots, x_n$ привести преобразование (1′) к виду

$$\begin{aligned} x_1' &= \varepsilon_1 x_1 + \dots + b_{111} x_1^2 + \dots, \\ x_2' &= \varepsilon_2 x_2 + \dots + b_{211} x_1^2 + \dots, \\ &\dots\dots\dots\dots\dots\dots \\ x_n' &= \varepsilon_n x_n + \dots + b_{n11} x_1^2 + \dots, \end{aligned} \tag{1″}$$

где $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n$ представляют некоторые корни m-й степени из единицы.

Чтобы действительно получить преобразования н. г. п., введем еще одну замену переменных. Пусть k-я итерация преобразования (1″) будет

$$x_1' = f_1^{(k)}(x_1, x_2, \dots, x_n),\ x_2' = f_2^{(k)}(x_1, x_2, \dots, x_n), \dots, \\ x_n' = f_n^{(k)}(x_1, x_2, \dots, x_n). \tag{2}$$

Рассмотрим переменные

$$\begin{aligned} z_1 &= x_1 + \varepsilon_1^{-1} f_1^{(1)} + \varepsilon_1^{-2} f_1^{(2)} + \dots + \varepsilon_1^{-m+1} f_1^{(m-1)} = \\ &= \Phi_1(x_1, x_2 \dots, x_n), \\ z_2 &= x_2 + \varepsilon_2^{-1} f_2^{(1)} + \varepsilon_2^{-2} f_2^{(2)} + \dots + \varepsilon_2^{-m+1} f_2^{(m-1)} = \\ &= \Phi_2(x_1, x_2, \dots, x_n), \\ z_n &= x_n + \varepsilon_n^{-1} f_n^{(1)} + \varepsilon_n^{-2} f_n^{(2)} + \dots + \varepsilon_n^{-m+1} f_n^{(m-1)} = \\ &= \Phi_n(x_1, x_2, \dots, x_n). \end{aligned} \tag{3}$$

Легко видеть, что разложения функций (2) в ряды начинаются так:

$$f_i^{(k)}(x_1, x_2, \dots, x_n) = \varepsilon_i^k x_i + \dots$$

Следовательно, разложения функции (3) будут

$$z_1 = m x_1 + \dots,\ z_2 = m x_2 + \dots,\ \dots,\ z_n = m x_n + \dots$$

Отсюда вытекает, что, обратно, в окрестности точки $x_1 = x_2 = \ldots = x_n = 0$ переменные $x_1, x_2, \ldots, x_n$ представляют голоморфные функции от $z_1, z_2, \ldots, z_n$.

Производя преобразование (1) над функциями (3), мы получим функции $z_1', z_2', \ldots, z_n'$, связанные с $z_1, z_2, \ldots, z_n$ следующим образом:

$$z_1' = \varepsilon z_1 = g_1(z),\ z_2' = \varepsilon_2 z_2 = g_2(z), \ldots, z_n' = \varepsilon_n z_n = g_n(z). \quad (4)$$

Пусть $\varepsilon_k = e^{\frac{2\pi i a_k}{m}}$. Очевидно, что преобразование

$$z_k' = \varepsilon^{\frac{2\pi i a_k}{m} t} z_k = g_k(z_1, z_2, \ldots, z_n, t) \quad (k = 1, 2, \ldots n) \quad (5)$$

удовлетворяет условиям A, B, C. Но условия эти определяют одночленную н. г. п., содержащую как делитель циклическую группу, образованную степенями преобразования (4).

Чтобы возратиться к исходным переменным, следует разрешить относительно $x_1', x_2', \ldots, x_n'$ систему уравнений

$$\Phi_k(x_1', x_2', \ldots, x_n') = e^{\frac{2\pi i a_k}{m} t} \Phi_k(x_1, x_2, \ldots, x_n) \quad (k = 1, 2, \ldots, n). \quad (6)$$

Как мы видели, это всегда возможно.

Теперь перейдем к случаю, когда группа $\mathfrak{G}$ не циклическая. Выберем в $\mathfrak{G}$ систему производящих подстановок $A_1, A_2, \ldots, A_s$, т. е. таких подстановок, что каждый элемент $\mathfrak{G}$ может быть представлен в виде

$$A_i A_k A_l \ldots$$

Затем найдем соответствующие подстановкам $A_1, A_2, \ldots, A_s$ однопараметрические н. г. п. и их инфинитезимальные операторы $X_1(f)$, $X_2(f), \ldots, X_s(f)$. Теперь, чтобы найти наименьшую н. г. п., содержащую эти операторы, образуем всевозможные операторы $X_i(f)$, $(X_i, X_j)f$, $(X_i, (X_j, X_l))f$ и т. д. и выделим среди них линейно независимые (с постоянными коэффициентами). В нашем случае число их всегда конечно, так как все рассматриваемые группы линейны, т. е. являются делителями n^2-членной однородной линейной н. г. п.

§ 2. Одна задача из теории н. г. п.

Пусть дана н. г. п.

$$\Gamma: \quad x_i' = f_i(x_j, a_l) \quad (i, j = 1, 2, \ldots, n;\ l = 1, 2, \ldots, r). \quad (1)$$

Требуется найти систему из возможно меньшего числа k функций

$$u_1(x_1, x_2 \ldots, x_n),\ u_2(x_1, x_2, \ldots, x_n), \ldots, u_k(x_1, x_2, \ldots, x_n), \quad (2)$$

обладающих тем свойством, что функции

$$u_i(f_1, f_2, \ldots, f_n)$$

зависят только от $u_1, u_2, \ldots, u_k$; $a_1, a_2, \ldots, a_r$. При этом каждому преобразованию той конечной группы $\mathfrak{G}$, из которой посредством одевания ее получена группа Г, должно соответствовать отличное от тождественного преобразование функций $u_1, u_2, \ldots, u_k$.

Очевидно, что многообразия

$$u_1 = C_1, \; u_2 = C_2, \ldots, \; u_k = C_k$$

представляют систему импримитивности группы Г. Обратно, каждой системе импримитивности группы Г соответствует некоторая система функций (2). Но мы в состоянии определить все системы импримитивности группы Г.

Проблема эта была полностью разрешена Ли и Энгелем [7]. Формулировку полученного ими результата приводим дословно:

«Теорема 92. Если в пространстве $x_1, x_2, \ldots, x_s$ дана r-членная транзитивная группа G_r, то все возможные для этой группы инвариантные разбиения пространства найдутся следующим образом.

Сначала нужно найти ту $r-s$-членную подгруппу группы G_{r-s}, которая оставляет инвариантной какую-либо точку P, не лежащую ни на одном инвариантном относительно G_r многообразии. Затем разыскать все те подгруппы группы G_r, которые содержат G_{r-s}. Если G_{r-s+h} — одна из этих подгрупп, то произвести над P все преобразования группы G_{r-s+h}, при этом P займет ∞^h различных положений, образующих некоторое h-мерное многообразие M; если произвести затем над M все преобразования G_r, то M займет ∞^{s-h} различных положений, определяющих одно из инвариантных относительно G_r разбиений пространства. Рассматривая таким образом все подгруппы G_r, содержащие G_{r-s}, получим все инвариантные относительно G_r разбиения».

Так как все подгруппы некоторой н. г. п. можно найти при помощи алгебраических действий (там же, стр. 208 и последующие, §56), то $u_1, u_2, \ldots, u_k$ будут алгебраическими функциями переменных $x_1, x_2, \ldots, x_n$ по крайней мере в том случае, когда группа Г транзитивна. Если же группа Г интранзитивна, то мы читаем далее в книге Ли и Энгеля следующее:

«Теорема 92 показывает, что для *транзитивной* группы все инвариантные разбиения можно найти без интеграции, если конечные уравнения группы известны. То же самое имеет место и для интранзитивных групп, но, чтобы убедиться в этом, нужны довольно длинные рассуждения, излагать которые здесь было бы нецелесообразно»

Чтобы разъяснить второе условие, определим наибольший делитель Γ_1 группы Г, оставляющий неизменной каждую из функций u_i. Для того чтобы удовлетворить второму условию, мы требуем, чтобы Γ_1 не содержало преобразований группы.

В частности, если $\mathfrak{G}$ — простая группа (что, например, имеет

место, если $\mathfrak{G}$ — знакопеременная группа и $n>4$), то условие это не создает никаких новых затруднений. Именно, при отображении $(x_1, x_2, \ldots, x_n)$ на $(u_1, u_2, \ldots, u_n)$ группа $\mathfrak{G}$ отображается в одну из своих факторгрупп, которой может быть либо единичная группа, либо сама группа $\mathfrak{G}$. В первом случае Γ_1 содержит всю группу $\mathfrak{G}$. Это значит, что Γ_1 может быть взята вместо Γ; т. е. что мы одели $\mathfrak{G}$ не посредством н. г. п. с наименьшим возможным числом параметров.

Если, напротив, группа $\mathfrak{G}$ — не простая, например если она содержит нормальный делитель $\mathfrak{H}$, то можно расчленить основную проблему, решая ее отдельно для $\mathfrak{H}$ и для $\mathfrak{G}/\mathfrak{H}$.

§ 3. Проблема резольвент

Возвратимся теперь к основной проблеме. Рассмотрим корни $x_1, x_2, \ldots, x_n$ уравнения

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_{n-1} x + p_n = 0 \qquad (1)$$

как независимые переменные. Если коэффициенты уравнения

$$\varphi(y) = y^n + \Pi_1 y^{n-1} + \ldots + \Pi_{n-1} y + \Pi_n = 0 \qquad (2)$$

зависят от k параметров, то то же имеет место и для корней $y_1, y_2, \ldots, y_n$. Чтобы выразить, что y_1 рационально выражается через $x_1, p_1, p_2, \ldots, p_n$; Ф, мы полагаем, что:

1) y_1 есть рациональная функция от $x_1, x_2, \ldots, x_n$, принадлежащая к той подгруппе группы $\mathfrak{G}$, которая не изменяет x_1;

2) когда выражение $y_1(x_1, x_2, \ldots, x_n)$ подвергается всем подстановкам группы $\mathfrak{G}$, то получаются все корни $y_1, y_2, \ldots, y_n$.

Теорема Лагранжа гласит, что x_1 и y_1 взаимно рационально выражаются друг через друга с помощью коэффициентов $p_1, p_2, \ldots, p_n$; Ф. Задачу можно обобщить, если отбросить требование рациональности функции.

Удобнее рассматривать вместо y_1 функцию

$$u_1 = t_1 y_1 + t_2 y_2 + \ldots, + t_n y_n, \qquad (3)$$

где $t_1, t_2, \ldots, t_n$ представляют рациональные числа, которые должны быть выбраны так, чтобы сопряженные с u_1 функции $u_1, u_2, \ldots, u_m$ (т. е. функции, получаемые из u_1 посредством подстановок группы $\mathfrak{G}$) были все отличны друг от друга. Тогда u_1 принадлежит к тождественной подстановке. С другой стороны, как $y_1, y_2, \ldots, y_n$, так и функции $u_1, u_2, \ldots u_m$ зависят только от k существенных параметров, иными словами, система $u_1, u_2, \ldots, u_m$ содержит только k функционально независимых функций.

Пусть A — производящее преобразование s-го порядка группы $\mathfrak{G}$, производящее над переменными $x_1, x_2, \ldots, x_n$ подстановку S и над

$u_1, u_2, \ldots, u_m$ — подстановку Σ. Отнесем каждому циклу подстановок S и Σ новую систему функций

$$\begin{aligned}
&\bar{z}_1 = \bar{x}_1 + \bar{x}_2 + \cdots + \bar{x}_s,\\
&\bar{z}_2 = \bar{x}_1 + \varepsilon\bar{x}_2 + \cdots + \varepsilon^{s-1}\bar{x}_s,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\bar{z}_s = \bar{x}_1 + \varepsilon^{s-1}\bar{x}_2 + \cdots + \varepsilon^{(s-1)^2}\bar{x}_s;\\
&\bar{v}_1 = \bar{u}_1 + \bar{u}_2 + \cdots + \bar{u}_s,\\
&\bar{v}_2 = \bar{u}_1 + \varepsilon\bar{u}_2 + \cdots + \varepsilon^{s-1}\bar{u}_s,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&\bar{v}_s = \bar{u}_1 + \varepsilon^{s-1}\bar{u}_2 + \cdots + \varepsilon^{(s-1)^2}\bar{u}_s,
\end{aligned}$$

где $\varepsilon = e^{\frac{2\pi i}{s}}$, а циклы, о которых идет речь, имеют вид $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_s)$ и, соответственно, $(\bar{u}_1, \bar{u}_2, \ldots, \bar{u}_s)$. Таким образом, мы получаем две системы функций $(z_1, z_2, \ldots, z_n)$ и $(v_1, v_2, \ldots, v_m)$. A производит следующее преобразование этих функций:

$$v_1' = \varepsilon^{\alpha_1} v_1,\ v_2' = \varepsilon^{\alpha_2} v_2, \ldots,\ v_m' = \varepsilon^{\alpha_m} v_m, \tag{4}$$

$$z_1' = \varepsilon^{\beta_1} z_1,\ z_2' = \varepsilon^{\beta_2} z_2, \ldots,\ z_n' = \varepsilon^{\beta_n} z_n, \tag{5}$$

где $\alpha_1, \alpha_2, \ldots, \alpha_m$; $\beta_1, \beta_2, \ldots, \beta_n$ — некоторые целые рациональные числа. Нетрудно видеть, что $u_1, u_2, \ldots, u_m$ линейно выражаются через $v_1, v_2, \ldots, v_m$, а $x_1, x_2, \ldots, x_n$ — через $z_1, z_2, \ldots, z_n$. Следовательно, система $(v_1, v_2, \ldots, v_m)$ содержит ровно k, а система $(z_1, z_2, \ldots, z_n)$ — ровно n функционально независимых функций. Пусть $v_1, v_2, \ldots, v_k$ — функционально независимы. Дополним систему $(v_1, v_2, \ldots, v_k)$ с помощью некоторых $n-k$ переменных системы $z_1, z_2, \ldots, z_n$ так, чтобы дополненная система $(v_1, v_2, \ldots, v_k; z_{k+1}, \ldots, z_n)$ содержала ровно n функционально независимых функций.

Возьмем в качестве однопараметрической н. г. п., одевающей группу $(1, A, A^2, \ldots, A^{s-1})$, следующую группу

$$v_1' = e^{\frac{2\pi i\alpha_1}{s}t} v_1,\ v_2' = e^{\frac{2\pi i\alpha_2}{s}t} v_2, \ldots, v_k' = e^{\frac{2\pi i\alpha_k}{s}t} v_k, \tag{6}$$

$$z'_{k+1} = e^{\frac{2\pi i\beta_k+1}{s}t} z'_{k+1},\ z_{k+2} = e^{\frac{2\pi i\beta_k+2}{s}t} z_{k+2}, \ldots, z_n' = e^{\frac{2\pi i\beta_n}{s}t} z_n, \tag{7}$$

где t — параметр этой группы. Из (4), (5) следует, что преобразование (6), (7) обращается в A при $t = 1$.

Из этих уравнений можно найти $x_1', x_2', \ldots, x_n'$ в виде функций от $x_1, x_2, \ldots, x_n$, определяющих искомую однопараметрическую н. г. п. Поступая таким же образом со всеми производящими преобразованиями группы $\mathfrak{G}$, мы получим н. г. п. Γ, одевающую всю группу $\mathfrak{G}$. Система $u_1, u_2, \ldots, u_k$, очевидно, представляет систему импримитивно-

сти группы Г. Преобразования $\mathfrak{G}$ осуществляют над $u_1, u_2, \ldots, u_m$ подстановки, которые образуют группу, изоморфную с $\mathfrak{G}$, что и т. д.

Обратно, предположим, что н. г. п. Г, одевающая группу Галуа уравнения (1), имеет систему импримитивности

$$u_1 = C_1,\ u_2 = C_2, \ldots, u_k = C_k. \tag{8}$$

При этом ни одна подстановка из $\mathfrak{G}$ не должна оставлять инвариантными все функции $u_1, u_2, \ldots, u_k$. Из § 2 мы заключаем, что все возможные системы импримитивности могут быть получены алгебраическими операциями и потому можно считать $u_1, u_2, \ldots, u_k$ алгебраическими функциями переменных $x_1, x_2, \ldots, x_n$.

Согласно нашему определению системы импримитивности, функции $u_1, u_2, \ldots, u_k$ должны оставаться инвариантными относительно некоторой подгруппы Γ_1 группы Г, факторгруппа которой Γ_2 содержит группу, изоморфную $\mathfrak{G}$. Переменные $u_1, u_2, \ldots, u_k$ порождают некоторую н. г. п. Γ_3, которая, по терминологии О. Шрейера [9], «локально изоморфна» с Γ_2.[1]

Докажем, что Γ_3 содержит группу, изоморфную либо с $\mathfrak{G}$, либо, по крайней мере, с ее факторгруппой относительно центра. Для этого повторим глубокие рассуждения О. Шрейера (см. [9], стр. 20). Пусть θ — подгруппа Γ_2, переходящая в тождественное преобразование при отображении Γ_2 на $(u_1, u_2, \ldots, u_k)$. Так как Γ_2 и Γ_3 — «локально изоморфны», т. е. имеют одинаковое число параметров, то θ должна быть дискретной группой. Выберем в θ преобразование A и рассмотрим выражение $X^{-1}AX$, где X — преобразование, непрерывно изменяющееся от 1 и до произвольного преобразования из Γ_2. Так как преобразование $X^{-1}AX$ непрерывно зависит от X, в то время как преобразования θ дискретны, то при этом $X^{-1}AX$ должно оставаться неизменным. Это показывает, что θ лежит в центре Γ_2, что и т. д. В частности, если $\mathfrak{G}$ — группа без центра, то $\theta = 1$.[1]

Докажем теперь следующее: если $u_1, u_2, \ldots, u_k$ — некоторая определенная система ветвей рассматриваемых многозначных функций, то всякая другая ветвь u_i' каждой из этих функций представляет функцию от $u_1, u_2, \ldots, u_k$.

Пусть полная система интранзитивности группы Г будет

$$\Psi_1 = C_1,\ \Psi_2 = C_2, \ldots, \Psi_l = C_l. \tag{9}$$

Мы можем предполагать, что $\Psi_1, \Psi_2, \ldots, \Psi_l$ суть рациональные функции от $x_1, x_2, \ldots, x_n$. С помощью теории исключения можно получить из (9) связное частичное многообразие T, на котором группа Г будет транзитивной.

Пусть $u_i, u_i', \ldots, u_i^{(p-1)}$ — полная система значений (ветвей) функции u_i в точке $(x_1, x_2, \ldots, x_n)$ и пусть $(x_1, x_2, \ldots, x_n)$ описывает на T

[1] Этот абзац добавлен при корректуре в декабре 1930 г.

произвольный замкнутый путь. Вследствие полноты системы интранзитивности (9) группа Γ является транзитивной группой на T. Поэтому каждый путь U на T можно аппроксимировать при помощи замкнутого полигона, каждая сторона которого является отрезком некоторой траектории группы Γ, т. е. соответствует некоторой последовательности преобразований группы Γ.

Производя над u_i шаг за шагом преобразования этой последовательности и считая наш полигон выбранным достаточно близким к U, мы получим в конце концов ту ветвь u_i, которая соответствует обходу замкнутого пути U. Но так как u_i, в силу определения системы импримитивности, переводится преобразованиями Γ в функции от $u_1, u_2, \ldots, u_n$, то значит $u_i^{(j)}$ будет функцией от $u_1, u_2, \ldots, u_n$ $(j = 0, 1, \ldots$ $\ldots, p-1)$.

Положим

$$\xi = t_1 u_1 + t_2 u_2 + \ldots + t_k u_k,$$

причем рациональные числа $t_1, t_2, \ldots, t_k$ подберем так, чтобы как все ветви $\xi, \xi', \ldots, \xi^{(p-1)}$ на T, так и все ветви функций $\xi^A, \xi^B, \ldots$, полученных из ξ преобразованиями $A, B, \ldots$ ($A, B, \ldots$ пробегают все преобразования $\mathfrak{G}$), были отличны друг от друга. Полином

$$\varphi(t) = (t-\xi)(t-\xi')\cdots(t-\xi^{(p-1)}) \tag{10}$$

представляет на T однозначную функцию переменных $x_1, x_2, \ldots, x_n, t$ и одновременно функцию $u_1, u_2, \ldots, u_k, t$. Если произвести над $\xi, \xi', \ldots, \xi^{(p-1)}$ какое-либо преобразование группы $\mathfrak{G}$, отличное от тождественного, то полученный полином должен быть отличен от исходного. Следовательно, можно приписать переменной t такое значение t_1, что функция

$$\varphi(t_1) = v(x_1, x_2, \ldots, x_n)$$

будет отлична от всех функций $v^A, v^B, \ldots$, где $A, B, \ldots$ пробегают все преобразования группы $\mathfrak{G}$.

Уравнения многообразия T можно представить следующим образом:

$$\begin{aligned} &\Psi_1(x_1, x_2, \ldots, x_n, C_1, C_2, \ldots, C_l) = 0,\\ &\Psi_2(x_1, x_2, \ldots, x_n, C_1, C_2, \ldots, C_l) = 0,\\ &\qquad\qquad\cdots\cdots\cdots\cdots\cdots\\ &\Psi_l(x_1, x_2, \ldots, x_n, C_1, C_2, \ldots, C_l) = 0. \end{aligned} \tag{11}$$

Пусть v удовлетворяет уравнению

$$F(v, x_1, x_2, \ldots, x_n) = 0, \tag{12}$$

где F — рациональная функция от $v, x_1, x_2, \ldots, x_n$. Исключая посредством уравнений (11) переменные $x_1, x_2, \ldots, x_l$ из (12), мы получим уравнение

$$\overline{F}(v, x_{l+1}, \ldots, x_n, C_1, C_2, \ldots, C_l) = 0. \tag{13}$$

Это уравнение должно удовлетворяться такой функцией v переменных $x_{l+1}, \ldots, x_n$, которая на T совпадает с v, т. е. однозначна на T. Но так как в уравнении (13) на переменные $x_{l+1}, \ldots, x_n$ не налагается никаких ограничений, то $\bar{v}$ будет повсюду однозначной, т. е. рациональной функцией переменных $x_{l+1}, \ldots, x_n$:

$$\bar{v} = \bar{v}(x_{l+1}, \ldots, x_n, C_1, C_2, \ldots, C_l). \tag{14}$$

В этом выражении $C_1, C_2, \ldots, C_l$ могут входить и иррационально. Если рассматривать $C_1, C_2, \ldots, C_l$ как функции от $x_1, x_2, \ldots, x_n$, определенные уравнениями (11), то мы должны возвратиться к первоначальной функции v. Если в выражении (14) произвести все преобразования $A, B, \ldots$ группы $\mathfrak{G}$, то получится только k функционально независимых функций. Но так как вследствие определения системы интранзитивности, функции $C_1, C_2, \ldots, C_l$, определенные уравнениями (11), инвариантны относительно преобразований группы $\mathfrak{G}$, то между $\bar{v}, \bar{v}^A, \bar{v}^B, \ldots$ существуют $m - k$ независимых соотношений типа

$$\Phi(\bar{v}(x_{l+1}, \ldots, x_n, C_1, \ldots, C_l), \bar{v}^A(x_{l+1}, \ldots, x_n, C_1, \ldots, C_l),$$
$$\bar{v}^B(x_{l+1}, \ldots, x_n, C_1, \ldots, C_l), \ldots) = 0.$$

Соотношения эти сохраняют силу, если вместо $C_1, C_2, \ldots, C_l$ подставить какие-либо числовые значения. Таким образом, мы получаем рациональную функцию $\bar{v}(x_{l+1}, x_{l+2}, \ldots, x_n)$, сопряженные с которой функции $\bar{v}^A, \bar{v}^B, \ldots$ отличны друг от друга и образуют систему k функционально независимых функций. Отсюда, между прочим, следует, что в $\mathfrak{G}$ не существует такой отличной от 1 подстановки, которая не изменяла бы переменных $x_{l+1}, \ldots, x_n$. В частности, если $\mathfrak{G}$ — знакопеременная группа, то $l \leqslant 2$.

Поле $R(x_1, \ldots, x_n; C_1, \ldots, C_l)$ можно представить как поле $\mathfrak{R}(x_1, \ldots, x_n, \theta)$, где θ имеет форму $t_1 C_1 + t_2 C_2 + \cdots + t_l C_l$. θ удовлетворяет уравнению, коэффициенты которого суть рациональные функции от $x_1, \ldots, x_n$ и инвариантны относительно Г. Поэтому число параметров в этом уравнении $\leqslant l$. Мы назовем его «побочной резольвентой». В частности, если $\mathfrak{G}$ — знакопеременная группа, то побочная резольвента, самое большее, однопараметрическая. В самом деле, здесь $l \leqslant 2$, а если положить $x_1 + \cdots + x_n = 0$ (чего можно достигнуть рациональными операциями), то число параметров уменьшится еще на единицу [10]).

Чтобы получить уравнение, корни которого рационально выражаются через корни уравнения (1) и наоборот, мы построим такую функцию от $\bar{v}$, которая принадлежит той же подгруппе $\mathfrak{H}$ группы $\mathfrak{G}$, что и x_1. Для этого достаточно рассмотреть полином

$$\psi(z) = (z - \bar{v})(z - \bar{v}^A)(z - \bar{v}^B)\ldots,$$

где $1, A, B, \ldots$ представляют все преобразования группы $\mathfrak{G}/\mathfrak{H}$, и придать переменному z подходящее рациональное значение z_1. Тогда,

по теореме Лагранжа, $\psi(z_1)$ рационально выражается через x_1 и наоборот. С другой стороны, коэффициенты уравнения n-й степени ($n = (\mathfrak{G} : \mathfrak{H})$), которому удовлетворяет $\psi(z_1)$ и сопряженные с ней величины, зависят только от k параметров, так как они являются функциями $v, v^A, v^B, \ldots$, где $1, A, B, \ldots$ представляют все преобразования группы $\mathfrak{G} : \mathfrak{H}$.

Неразрешенным остается вопрос, все ли возможные одевания конечной группы изоморфны между собой. Поэтому нелегко ответить на конкретный вопрос: не имеет ли уравнение с заданной группой k-параметрическую резольвенту? Действительно, если одно полученное нами одевание дает отрицательный ответ, то мы не можем быть уверены, что всякое другое одевание также даст отрицательный ответ. Я надеюсь исследовать этот вопрос в последующих работах. Одевания абстрактных групп, построенные Ле-Вавассером и Бернсайдом (см. выше), дают вполне определенные решения. Чтобы дать исчерпывающий ответ на поставленный вопрос, мы должны поступать так: сначала испытаем, не содержит ли какая-либо из k-мерных н. г. п. (число их, как известно, конечно) делитель конечного порядка, изоморфный с $\mathfrak{G}$. Это достигается следующим образом: представим эту н. г. п., как группу однородных линейных преобразований, скажем, s переменных. Согласно теореме Жордана, существует только конечное число таких конечных групп, которые будут факторгруппами относительно центра для групп, представимых в виде групп однородных линейных преобразований s переменных. Структура же центра $\mathfrak{G}$ для нас не интересна, так как центр есть абелева группа и потому имеет однопараметрическую резольвенту. Теперь мы в состоянии сравнить эти факторгруппы с факторгруппой $\mathfrak{G}$ относительно ее центра. Конечно, этот путь практически очень сложен.

Гильберт поставил также вопрос о последовательности резольвент. Вопрос этот аналогичен вопросу о натуральных иррациональностях в теории Галуа. Я исследую этот вопрос в последующих работах.

Получено
16 июня 1930 г.

ЛИТЕРАТУРА

1. D. Hilbert. Über die Gleichung neunten Grades. Math. Ann. **97**, 1926, стр. 243—250.
2. D. Hilbert. Mathematische Probleme. Gött. Nachr., 1900, № 13, стр. 280.
3. W. Burnside. On the Continuous Group, that is defined by any gived Group of Finite Order. Proc. Lond. Math. Soc. **29**, 1898, стр. 207—224, 546—565.
4. H. Weber. Lehrbuch der Algebra. I. 1 Aufl., Braunschweig, 1898, стр. 675.
5. L. Leau. Etude sur les équations fonctionnelles... Toul. Ann. **11**, 1897.
6. P. Fatou. Sur l'itération analytique et les substitutions permutables. Journ. de math. (9) **2**, 1923, стр. 343; (9) **3**, 1924, стр. 1.
7. Lie-Engel. Theorie der Transformationsgruppen 1. Leipzig, 1888, стр. 522, Theorem 92.
8. R. Le-Vavasseur. Quelques considérations sur les groupes d'ordre fini et les groupes finis continus. Lyon-Paris, 1904.
9. O. Schreier. Abstrakte kontinuierliche Gruppen. Abh. Hamb. Sem. **4**, 1925, стр. 15—32.

ОБ ОДНОЙ АЛГЕБРАИЧЕСКОЙ ПРОБЛЕМЕ ГИЛЬБЕРТА. II

(ÜBER EIN ALGEBRAISCHEN PROBLEM VON HERRN HILBERT. II)

(Math. Ann. **105**, (1931), стр. 240—255)

В ранее появившейся работе под таким же названием [1] я указал на связь между гильбертовской проблемой резольвент [2] и так называемым одеванием конечных групп посредством н. г. п. (непрерывных групп преобразований). Теперь я в состоянии формулировать эту связь более точно:

Для того чтобы алгебраическое уравнение с группой Галуа $\mathfrak{G}$ *обладало* k*-параметрической резольвентой, необходимо и достаточно, чтобы среди тех абстрактных н. г. п., которые содержат в качестве делителя изоморфную с* $\mathfrak{G}$ *группу, нашлась хотя одна группа* Γ, *имеющая представление в* k*-мерном пространстве* (*короче: которая была бы «*k*-группой»*).

Для этого я доказываю следующее. Если Γ — некоторое представление k-группы в пространстве $X(x_1, x_2, \ldots, x_n)$, то можно так расширить это пространство, т. е. ввести такую систему переменных, ковариантную относительно Γ с системой $(x_1, x_2, \ldots, x_n)$, что в расширенном пространстве представления группы Γ найдутся k функций, образующих систему импримитивности группы Γ (§ 1, теорема 3).

В § 2 я даю способ получения всех неизоморфных о. г.[1] (одевающих групп) для простых конечных групп. При этом я могу рассматривать только линейные о. г. для всех линейных однородных представлений Γ (теорема 5). Представления, о которых идет речь, вообще только «локально изоморфны». (Это важное понятие введено О. Шрейером [3].) Поэтому они могут содержать не $\mathfrak{G}$, но некоторую группу $\mathfrak{G}'$, факторгруппа которой относительно центра изоморфна $\mathfrak{G}$. Группы $\mathfrak{G}'$ этого рода являются, по терминологии И. Шура [4], «группами представлений» группы $\mathfrak{G}$. Как доказал Шур, каждая группа имеет только конечное число групп представлений. Таким образом, для того чтобы решить вопрос о представимости хотя одной о. г. группы $\mathfrak{G}$ в k-мерном пространстве, необходимо рассмотреть линейные одевания не только группы $\mathfrak{G}$, но и всех ее групп представлений.

---

[1] Как стало теперь обычным, я употребляю слово «изоморфный» в смысле «однозначно изоморфный». Вместо «многозначно изоморфный» я говорю «гомоморфный».

В § 3 я доказываю, что уравнение (1) тогда и только тогда обладает k-параметрической резольвентой, если его группа Галуа $\mathfrak{G}$ допускает в качестве о. г. некоторую k-группу. При этом не исключено, что, кроме некоторой k-параметрической резольвенты придется разрешать еще некоторую побочную резольвенту, коэффициенты которой будут инвариантами н. г. п. Г. В частности, если $\mathfrak{G}$ — знакопеременная группа, то эта побочная резольвента может быть только однопараметрической (теорема 7). При этом я опираюсь на тот факт, что все системы импримитивности некоторой н. г. п. находятся алгебраическими операциями. Этот результат получен С. Ли и Ф. Энгелем [5] для случая транзитивных н. г. п. и легко может быть обобщен на случай интранзитивных н. г. п. Чтобы использовать эти системы импримитивности, я должен ввести, кроме корней $x_1, x_2, \ldots, x_n$ уравнения (1), еще некоторые ковариантные величины как координаты пространства представления группы Г. Тогда к цели приводит преобразование (9) § 3.

Проблема наша весьма тесно связана с клейновской «проблемой форм». Для этой последней Ф. Клейн получил некоторые общие предложения и подробно рассмотрел случай уравнений пятой, шестой и седьмой степеней [6]. Существенный прогресс в задаче Клейна был достигнут Виманом [7], который показал, что знакопеременная группа подстановок из шести элементов может быть представлена как группа колинеаций двух переменных. Сложность геометрических соображений, используемых этими авторами, воспрепятствовала мне обстоятельно разобрать их работы.

Поставленный Гильбертом вопрос о последовательности резольвент я надеюсь разрешить в дальнейших работах. Решение его зависит от решения проблемы резольвент для того случая, когда коэффициенты уравнения (1) связаны некоторыми соотношениями. Тогда возможно, что коэффициенты эти зависят от k параметров, но о. г. группы $\mathfrak{G}$ не является k-группой (ср. замечание 2 в конце § 3).

В заключение я позволю себе выразить мою сердечную благодарность Э. Картану и П. А. Широкову за их интерес к этой работе и некоторые важные указания.

§ 1. Теоретико-групповые теоремы

Теорема 1. *Пусть даны две изоморфные н. г. п.*

$$\Gamma \text{ в пространстве } X(x_1, x_2, \ldots, x_m)$$

$$\Gamma_1 \text{ в пространстве } Y(y_1, y_2, \ldots, y_m).$$

Возможно расширить пространство $(x_1, x_2, \ldots, x_m)$ *до такого пространства*

$$\bar{X}\begin{pmatrix} x_1, x_2, \ldots, x_m \\ x_1', x_2', \ldots, x_m' \\ \ldots\ldots\ldots\ldots \\ x_1^{(s-1)}, x_2^{(s-1)}, \ldots, x_m^{(s-1)} \end{pmatrix},$$

что в последнем найдется система таких функций

$$y_i = \theta_i(x_1, \ldots, x_m; x_1', \ldots, x_m'; \ldots; x_1^{(s-1)}, \ldots, x_m^{(s-1)}) \quad (i = 1, 2, \ldots, m),$$

которые будут подвергаться преобразованиям группы Γ, *если над каждой из систем* $x_1^{(i)}, x_2^{(i)}, \ldots, x_m^{(i)}$ $(i = 0, 1, 2, \ldots, s-1)$ *параллельно производить соответствующие преобразования группы* Γ.

(Для этой теоремы, которую я высказал в качестве предположения на Математическом съезде в Харькове в 1930 г., Э. Картан тотчас же набросал геометрическое доказательство.)

Доказательство. Расширим обе группы Γ и Γ_1 таким образом, чтобы:

1. Пространства, соответствующие расширенным группам $\bar{\Gamma}$ и $\bar{\Gamma}_1$, были одного измерения.

2. Матрицы $\| \xi_{ij} \|$, элементы которых представляют коэффициенты инфинитезимальных преобразований групп $\bar{\Gamma}$ и $\bar{\Gamma}_1$, были ранга r, если Γ и Γ_1 (а значит, и $\bar{\Gamma}$, $\bar{\Gamma}_1$) r-членные группы.

Это всегда возможно [8]. Тогда группы $\bar{\Gamma}$ и $\bar{\Gamma}_1$ подобны ([8], стр. 254—259). Это означает, что координаты пространства Y можно представить как функции от координат пространства $\bar{X}$, что и т. д.

Теорема 2. *Теорема 1 остается справедливой и тогда, когда* Γ_1 *изоморфна некоторой факторгруппе группы* Γ.

Доказательство. На основании теоремы 1 достаточно доказать теорему для случая, когда Γ_1 является факторгруппой группы Γ. Итак, пусть $\Gamma_1 = \frac{\Gamma}{\Gamma_2}$, где Γ_2 — некоторый нормальный делитель Γ. Расширим пространство группы Γ так, чтобы матрица $\| \xi_{ij} \|$ группы $\bar{\Gamma}$ имела ранг r, а матрица $\| \xi_{ij}' \|$ группы $\bar{\Gamma}_2$ — ранг r_2, причем мы предполагаем, что группа $\bar{\Gamma}$ r-членна, а $\bar{\Gamma}_2$ — r_2-членна. Для этого достаточно повторить пространство группы Γ r раз ([8], стр. 95—96). Если k — размерность пространства $\bar{X}$, то группа $\bar{\Gamma}$ имеет ровно $k - r$, а группа $\bar{\Gamma}_2$ — ровно $k - r_2$ независимых инвариантов ([8], стр. 174). Точно так же убеждаемся в том, что всякая r'-членная группа, промежуточная между $\bar{\Gamma}$ и Γ_2, имеет ровно $k - r'$ независимых инвариантов.

Пусть полная система независимых инвариантов группы $\bar{\Gamma}_2$ будет

$$z_1, z_2, \ldots, z_\mu \quad (\mu = k - r_2). \tag{1}$$

Если мы будем производить над $z_1, z_2, \ldots, z_\mu$ преобразования группы $\bar{\Gamma}$, то получим снова инварианты группы $\bar{\Gamma}_2$, так как $\bar{\Gamma}_2$ является

нормальным делителем группы $\bar{\Gamma}$. Полученные преобразованные величины будут функциями от $z_1, z_2, \ldots, z_\mu$ в силу того, что система (1) представляет полную систему инвариантов $\bar{\Gamma}_2$. Таким образом, мы получаем некоторое представление ϑ группы $\bar{\Gamma}$, в котором преобразования $\bar{\Gamma}_2$ представлены тождественным преобразованием.

Допустим, что в $\bar{\Gamma}$ существуют другие преобразования, представленные в ϑ тождественным преобразованием. Они образуют r'-членную группу $\bar{\Gamma}'$, промежуточную между $\bar{\Gamma}$ и $\bar{\Gamma}_2$. Тогда функции $z_1, z_2, \ldots, z_\mu$ все должны быть инвариантами $\bar{\Gamma}'$, что противоречит тому факту, что $\bar{\Gamma}'$ имеет $k - r' < k - r_2$ независимых инвариантов. Следовательно, ϑ есть изоморфное представление группы $\bar{\Gamma}_1$, и теорема доказана.

Теорема 3. *Если н. г. п.* Γ *имеет представление в* k*-мерном пространстве, то некоторое расширение* $\bar{\Gamma}$ *группы* Γ *имеет систему импримитивности, представляющую* k*-мерное семейство многообразий.*

Доказательство. Пусть Γ представлена как н. г. п. в пространстве $(z_1, z_2, \ldots, z_k)$. Построим такое расширение $\bar{\Gamma}$ группы Γ в пространстве $\bar{X}$, чтобы z_i могли быть представлены как функции координат пространства $\bar{X}$, что, по теореме 1, всегда возможно. Эти функции и образуют искомую систему импримитивности, что и требовалось доказать.

Поставим теперь вопрос, является ли данная н. г. п. Γ k-группой? Если c_{ijs} $(i, j, s = 1, \ldots, r)$ — структурные постоянные группы Γ, то вопрос сводится к определению операторов

$$X_i(f) = \sum_{j=1}^{k} \xi_{ij} \frac{\partial f}{\partial x_j} \qquad (i = 1, 2, \ldots, r), \tag{2}$$

удовлетворяющих соотношениям

$$(X_i, X_k) = \sum_{s=1}^{r} c_{iks} X_s. \tag{3}$$

Таким образом, мы приходим к интегрированию дифференциальных уравнений

$$\sum_{j=1}^{k} \left(\xi_{ij} \frac{\partial \xi_{kt}}{\partial x_j} - \xi_{kj} \frac{\partial \xi_{it}}{\partial x_j} \right) = \sum_{j=1}^{r} c_{iks}\, \xi_{st} \tag{4}$$

$$(i, k = 1, 2, \ldots, r;\ t = 1, 2, \ldots, k).$$

Если система эта интегрируема и полученные операторы $X_i(f)$ линейно независимы (с постоянными коэффициентами), то получается истинное представление группы Γ. Если же, напротив, $X_i(f)$ связаны соотношениями, то получится представление некоторой факторгруппы группы Γ. Наконец, если система (4) не имеет решений, то задача невозможна.

К сожалению, этот практически наиболее удобный путь для решения нашей задачи не дает никаких указаний на возможность алгебраического выполнения описанных процессов. Но для этого служит следующий способ. Возьмем какое-либо представление группы Г, например ее параметрическую группу (если группа Г не имеет центра, то можно взять однородную линейную группу, т. е. такую, которую наверное можно найти алгебраически; во всяком случае, можно найти алгебраическое представление группы Г). Затем ищем соответствующую систему импримитивности для некоторого «повторения» группы Г, что всегда возможно согласно выше цитированной книге Ли — Энгеля.

§ 2. Проблема одевания

Определение. Н. г. п. Г назовем одевающей группой конечной группы $\mathfrak{G}$, если

1) Г содержит как делитель изоморфную с $\mathfrak{G}$ группу;

2) Г не содержит нетривиальных непрерывных подгрупп, обладающих свойством 1;

3) Г не имеет нетривиальных непрерывных факторгрупп, обладающих свойством 1.

Мы будем называть одевающую группу кратко: о. г. Нам нужно показать, что всякая простая группа имеет только конечное число неизоморфных о. г., являющихся в то же время k-группами. Сначала заметим, что всякая о. г. Г простой группы $\mathfrak{G}$ должна быть простой н. г. п. Допустим, что Г имеет нетривиальный нормальный делитель Γ_1. Тогда пересечение $\mathfrak{G}_1$ групп Г и $\mathfrak{G}$ будет нормальным делителем группы $\mathfrak{G}$. Поскольку группа $\mathfrak{G}$ — простая, то $\mathfrak{G}_1$ либо совпадает с Г, либо является единичной группой. В первом случае $\mathfrak{G}$ содержится в Γ_1, что противоречит условию 2 определения. Во втором случае «отображение» $\frac{\mathfrak{G}\Gamma_1}{\Gamma_1}$ группы $\mathfrak{G}$ в $\frac{\Gamma}{\Gamma_1}$ есть группа, изоморфная с $\mathfrak{G}$ [9] и содержащаяся в $\frac{\Gamma}{\Gamma_1}$, что противоречит условию 3 определения.

Таким образом, группа Г не может иметь центра и потому может быть представлена как однородная линейная группа ([9], стр. 217, 223). Представление это Γ_1 будет, по терминологии О. Шрейера [3], только «локально-изоморфно» с $\mathfrak{G}$. Шрейер показал, что в этом случае обе н. г. п. Г и Γ_1 будут факторгруппами одной и той же н. г. п. T, т. е. $\Gamma \longleftrightarrow \frac{T}{D}$, $\Gamma_1 \longleftrightarrow \frac{T}{D_1}$, где D и D_1 — «вполне разрывные» группы, которые содержатся в центре T (выше цит. стр. 20, Satz 8 и стр. 30, Satz 11). Если $\mathfrak{G}$ содержится в Г, то группа T содержит группу $\mathfrak{G}_1$ (может быть, бесконечную), факторгруппа которой $\frac{\mathfrak{G}_1}{D}$ изоморфна с $\mathfrak{G}$. При этом коммутаторгруппа $\mathfrak{R}$ группы $\mathfrak{G}_1$ конечна и также содержится

в T ([4], стр. 38, III). Шур назвал такие группы «группами представления» группы $\mathfrak{G}$. Они характеризуются следующими свойствами:

1. $\mathfrak{R}$ содержит подгруппу $\mathfrak{M}$, состоящую из инвариантных элементов $\mathfrak{R}$, причем $\frac{\mathfrak{R}}{\mathfrak{M}}$ изоморфна группе $\mathfrak{G}$.

2. Коммутатор $\mathfrak{R}$ содержит все элементы $\mathfrak{M}$.

3. Не существует группы $\mathfrak{G}$, порядок которой превышает порядок $\mathfrak{R}$ и которая обладает свойствами 1 и 2 (там же, стр. 47).

Шур дал также метод для нахождения всех групп представления группы $\mathfrak{G}$. При этом он доказал, что если $\mathfrak{G}$ совпадает со своей коммутаторгруппой, что наверное имеет место, если группа $\mathfrak{G}$ простая, то существует только одна группа представления группы $\mathfrak{G}$ (там же, стр. 38, IV).

Пример. Знакопеременная группа подстановок шести элементов может быть представлена как группа дробных линейных подстановок двух переменных. Но ее нельзя представить как однородную линейную группу от трех переменных. Это возможно только для ее группы представления, порядок которой равен $3 \cdot 360 = 1080$ ([7], Anm. 9).

Теперь мы установим некоторые специальные типы о. г. группы $\mathfrak{G}$. Рассмотрим все линейные однородные представления группы $\mathfrak{G}$. Число их, как известно, конечно [10].[1] Пусть $\mathfrak{G}_1$ — одно из этих представлений и $A, B, \ldots, L$ — какие-либо подстановки переменных $x_1, \ldots, x_n$, порождающие группу $\mathfrak{G}_1$. Переменные $x_1, x_2, \ldots, x_n$ можно линейно преобразовать к переменным $y_1, y_2, \ldots, y_n$ так, чтобы подстановка A приняла вид

$$y_1' = e^{2\pi i k_1} y_1,\ y_2' = e^{2\pi i k_2} y_2,\ \ldots,\ y_n' = e^{2\pi i k_n} y_n, \tag{5}$$

где $k_1, k_2, \ldots, k_n$ — некоторые рациональные дроби.

Выберем в качестве производящего преобразования одночленной одевающей н. г. п. следующее преобразование:

$$y_1' = e^{2\pi i (k_1 + M_1) t} y_1,\ y_2' = e^{2\pi i (k_2 + M_2) t} y_2,\ \ldots,\ y_n' = e^{2\pi i (k_n + M_n) t} y_n, \tag{6}$$

где $M_1, M_2, \ldots, M_n$ — произвольные целые числа. Затем возвратимся к исходным переменным $x_1, x_2, \ldots, x_n$. Полученная одночленная н. г. п. содержит подстановку A и ее степени, т. е. является о. г. той циклической подгруппы группы $\mathfrak{G}_1$, которая порождена подстановкой A.

Таким же образом оденем каждую из подстановок $B, \ldots, L$. Комбинируя полученные о. г., мы найдем некоторую н. г. п., содержащую $\mathfrak{G}_1$ как делитель. Группа эта будет конечной н. г. п., так как она является делителем полной линейной однородной группы в n переменных. Если мы изменим целые числа $M_1, M_2, \ldots, M_n$ для каждой из подстановок $A, B, \ldots, L$ и произведем над одночленными

[1] Степень представления предполагается заданной.

о. г. подстановок $B, \ldots, L$ все преобразования, коммутативные с A, то можно получить другую одевающую группу. Но так как число неизоморфных подгрупп полной линейной однородной группы для ограниченного n конечно, то мы можем получить только конечное число о. г. Следует заметить, что выбор производящих подстановок $A, B, \ldots, L$ не имеет значения, так как при другом их выборе получится та же система о. г., ибо имеет место

Теорема 4. *Всякая линейная о. г. конечной линейной циклической группы всегда может быть посредством линейного преобразования приведена к форме* (6).

Этот результат непосредственно следует из следующей теоремы И. Шура [11]:

«IX. Каждая матрица $F(t)$, непрерывная относительно вещественного переменного t, удовлетворяющая уравнению

$$F(t)F(u) = F(t+u)$$

и имеющая период 2π, вполне приводима. Ее неприводимые составные части имеют форму $e^{\nu it}$ ($\nu = 0, \pm 1, \pm 2, \ldots$)».

Описанным способом мы получим для каждого представления группы $\mathfrak{G}$ конечное число различных о. г. Пусть полная система полученных о. г. будет

$$\Gamma_1, \Gamma_2, \ldots, \Gamma_s. \tag{7}$$

Имеет место

Теорема 5. *Система* (7) *исчерпывает все возможные о. г. группы* $\mathfrak{G}$.

Доказательство. Рассмотрим произвольную о. г. Γ группы $\mathfrak{G}$, полагая, что она приведена к виду линейной однородной н. г. п. Γ содержит как делитель некоторую изоморфную с $\mathfrak{G}$ конечную линейную однородную группу. Группу эту назовем также $\mathfrak{G}$. Подвергнем переменные ее пространства представления такому линейному преобразованию, чтобы группа $\mathfrak{G}$ приняла вполне приведенную форму.

Рассмотрим сначала случай, когда группа Γ распадается. Возьмем одну из неприводимых частей этого представления. Пусть $y_1, \ldots, y_n$ — переменные, ей соответствующие. Полагая все переменные, кроме $y_1, y_2, \ldots, y_n$, равными нулю, мы получим некоторую, гомоморфную с Γ, н. г. п. $\bar{\Gamma}$ в пространстве $y_1, y_2, \ldots, y_n$. В самом деле, каждому преобразованию группы Γ будет соответствовать некоторое определенное преобразование группы $\bar{\Gamma}$: $S \longleftrightarrow \bar{S}$. Гомоморфизм этот должен быть изоморфизмом, так как группа Γ проста как о. г. простой группы $\mathfrak{G}$.

Н. г. п. $\bar{\Gamma}$ содержит как делитель некоторую однородную линейную группу $\bar{\mathfrak{G}}$, гомоморфную с $\mathfrak{G}$. Так как группа $\mathfrak{G}$ простая, то гомоморфизм этот является изоморфизмом. Рассматривая то преобразование группы $\bar{\mathfrak{G}}$, которое соответствует, скажем, преобразованию A

группы $\mathfrak{G}$, мы заключаем, на основании теоремы 4, что оно может быть приведено в форму (6). То же самое относится и к преобразованиям $B, \ldots, L$. Отсюда следует, что $\bar{\Gamma}$ содержит все преобразования, порождающие одну из групп (7). Преобразования эти должны порождать всю группу $\bar{\Gamma}$, так как иначе в группе $\bar{\Gamma}$ существовал бы нетривиальный делитель, изоморфный одной из одевающих группу $\mathfrak{G}$ групп системы (7). Так как $\bar{\Gamma} \leftrightarrow \Gamma$ является о. г. группы $\mathfrak{G}$, то это противоречит условию 2 определения о. г.

Если группа Γ не распадается, то можно найти верхнюю границу для n, так как, по исследованиям Картана, число простых k-групп конечно (Thèse, стр. 71, 147).

Теорема 6. *Если н. г. п.* Γ_1 *является* k*-группой и имеет факторгруппу* Γ, *то группа* Γ, *если она проста, также является* k*-группой.*

Доказательство. Производная группа Γ_2 группы Γ_1 как делитель Γ_1 будет k-группой. Так как факторгруппа $\frac{\Gamma_1}{\Gamma_2}$ абелева, то Γ_2 также содержит Γ как факторгруппу. То же самое имеет место для группы Γ_3, производной от Γ_2, и т. д. Продолжая это рассуждение, мы приходим, наконец, к некоторой группе $\bar{\Gamma}$, которая

1) имеет факторгруппу Γ,

2) является k-группой,

3) совпадает со своей производной группой.

Но В. Киллинг [12][1] получил такой результат:

«Если r-членная группа совпадает со своей собственной главной подгруппой (т. е. производной группой) и при этом не распадается, то можно выбрать r ее независимых инфинитезимальных преобразований $X_1, \ldots, X_r$ так, чтобы первые r_1 преобразований $X_1, \ldots, X_{r_1}$ образовывали простую группу, в то время как преобразования $X_{r_1+1}, \ldots, X_r$ образовывали бы группу ранга нуль, являющуюся инвариантной подгруппой для данной r-членной группы».

Если $\bar{\Gamma}$ распадается в прямое произведение нескольких групп, то хотя один из неразложимых факторов, скажем $\bar{\bar{\Gamma}}$, должен содержать как факторгруппу группу Γ. С другой стороны, так как $\bar{\Gamma}$ содержит как делитель некоторую группу, изоморфную $\bar{\bar{\Gamma}}$, то группа $\bar{\bar{\Gamma}}$ есть k-группа и из цитированной теоремы Киллинга следует, что $\bar{\bar{\Gamma}}$ содержит простой делитель, изоморфный группе Γ, что и т. д.

§ 3. Проблема резольвент

Теорема 7. *Если группа Галуа* $\mathfrak{G}$ *уравнения*

$$f(x) = x^n + p_1 x^{n-1} + \cdots + p_{n-1} x + p_n = 0 \qquad (1)$$

[1] Указанием на последнюю работу я обязан Э. Картану, который своими критическими замечаниями также существенно способствовал доказательству теоремы 5.

не имеет центра и, рассматриваемая как абстрактная группа, допускает одевающую группу Γ, *представимую как н. г. п. в* k*-мерном пространстве, то уравнение* (1) *имеет* k*-параметрическую резольвенту.*

Доказательство. Пусть

$$x_1, x_2, \ldots, x_n$$

— корни уравнения (1), которые мы рассматриваем как независимые переменные. Пусть, кроме того, задана н. г. п. $\bar{\Gamma}$, содержащая как делитель группу $\bar{\mathfrak{G}}$, изоморфную группе Галуа уравнения (1). Группа $\bar{\Gamma}$ представима в k-мерном пространстве $(z_1, z_2, \ldots, z_k)$.

Мы можем считать, что группа $\bar{\Gamma}$ не имеет центра. Действительно, если $\bar{\Gamma}_1$ — центр $\bar{\Gamma}$, то группы $\bar{\Gamma}_1$ и $\bar{\mathfrak{G}}$ взаимно просты, откуда следует, что, вместо Γ, мы можем рассмотреть факторгруппу $\frac{\bar{\Gamma}}{\bar{\Gamma}_1}$. Если последняя имеет центр, то мы повторяем снова ту же редукцию, и т. д.

Таким образом, $\bar{\Gamma}$ представима как линейная однородная группа преобразований ([8], стр. 217, 223). В этом представлении группа $\mathfrak{G}$ также будет представлена как однородная линейная группа в некотором пространстве $(y_1, y_2, \ldots, y_m)$. Группу подстановок $\mathfrak{G}$ мы рассматриваем как однородную линейную группу в пространстве $(x_1, x_2, \ldots, x_n)$.

Мы можем считать, что уравнение (1) нормально (уравнение Галуа). Этого всегда можно добиться, если вместо x_1 взять величину $t_1 x_1 + \cdots + t_n x_n$. Тогда группа подстановок $\mathfrak{G}$ является регулярным представлением группы $\bar{\mathfrak{G}}$, в которое каждое возможное представление $\bar{\mathfrak{G}}$ входит столько раз, какова степень этого представления [13].

Пространства $(x_1, x_2, \ldots, x_n)$ и $(y_1, y_2, \ldots, y_m)$ мы можем подвергнуть линейным преобразованиям так, чтобы в преобразованных пространствах рассматриваемые подстановки наших групп распались на неприводимые части, причем эквивалентные неприводимые части имели бы одну и ту же форму.

Теперь можно столько раз повторить (расширить) пространство $(x_1, x_2, \ldots, x_n)$ и так дополнить пространство $(y_1, y_2, \ldots, y_m)$, чтобы в полученных пространствах рассматриваемые группы совпали. Отсюда следует, что координаты пространства $(y_1, y_2, \ldots, y_m)$ можно представить как линейные функции от координат расширенного пространства $(x_1, x_2, \ldots, x_n)$. Соответствующее линейное преобразование переводит линейную н. г. п. расширенного пространства $(x_1, x_2, \ldots, x_n)$ в некоторую линейную группу в пространстве $(y_1, y_2, \ldots, y_m)$. Группе Γ должна соответствовать некоторая подгруппа Γ этой н. г. п. Но так как связь между расширенным пространством $(x_1, x_2, \ldots, x_n)$ и пространством $(y_1, y_2, \ldots, y_m)$ не является обратимой, то вообще $\bar{\Gamma}$ будет изоморфна некоторой факторгруппе группы Γ.

Заметим, что группа $\overline{\Gamma}$ представима в k-мерном пространстве $(z_1, z_2, \ldots, z_k)$ и потому из теоремы 3 следует, что величины $(z_1, z_2, \ldots, z_k)$ могут быть представлены как функции координат расширенного пространства $(y_1, y_2, \ldots, y_m)$. Отсюда мы заключаем, что величины $(z_1, z_2, \ldots, z_k)$ могут быть представлены как функции координат расширенного пространства $(x_1, x_2, \ldots, x_n)$. Следовательно, система $z_1, z_2, \ldots, z_k$ представляет систему импримитивности расширенной группы Г. На основании исследований Ли и Энгеля можно выбрать в качестве представителей этой системы импримитивности рациональные функции от x_i и корней некоторой «побочной резольвенты» ([1], § 2).

Мы хотим специализировать «расширенные» величины. Пусть $(u_1, u_2, \ldots, u_n)$ — одно из «повторений» пространства $(x_1, x_2, \ldots, x_n)$. Заменим переменные $u_1, u_2, \ldots, u_n$ новыми переменными: $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$, которые связаны с $u_1, u_2, \ldots, u_n$ и $x_1, x_2, \ldots, x_n$ следующими соотношениями:

$$\begin{aligned} u_1 &= \alpha_0 + \alpha_1 x_1 + \alpha_2 x_1^2 + \cdots + \alpha_{n-1} x_1^{n-1}, \\ u_2 &= \alpha_0 + \alpha_1 x_2 + \alpha_2 x_2^2 + \cdots + \alpha_{n-1} x_2^{n-1}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_n &= \alpha_0 + \alpha_1 x_n + \alpha_2 x_n^2 + \cdots + \alpha_{n-1} x_n^{n-1}. \end{aligned} \tag{2}$$

Величины $z_1, z_2, \ldots, z_k$ представляют функции от $x_1, x_2, \ldots, x_n$; $u_1, u_2, \ldots, u_n$; $v_1, v_2, \ldots$ и обладают как таковые следующими свойствами:

1. Если над переменными

$$\begin{matrix} x_1, & x_2, & \ldots, & x_n, \\ u_1, & u_2, & \ldots, & u_n, \\ v_1, & v_2, & \ldots, & v_n, \\ \cdots & \cdots & \cdots & \cdots \end{matrix}$$

параллельно производить преобразования группы Г, то каждая из величин $z_1, z_2, \ldots, z_k$ переходит в некоторую функцию от $z_1, z_2, \ldots, z_k$.

2. Если над переменными

$$\begin{matrix} x_1, & x_2, & \ldots, & x_n, \\ u_1, & u_2, & \ldots, & u_n, \\ v_1, & v_2, & \ldots, & v_n, \\ \cdots & \cdots & \cdots & \cdots \end{matrix}$$

параллельно производить преобразования S группы $\mathfrak{G}$ (т. е некоторые подстановки), то функция

$$Z = t_1 z_1 + t_2 z_2 + \cdots + t_k z_k$$

при неопределенных t претерпевает действительное изменение. Иными словами, если S пробегает все подстановки группы $\mathfrak{G}$, то все величины

$$Z^S - Z \tag{3}$$

отличны от нуля.

Будем рассматривать $z_1, z_2, \ldots, z_k$ как функции от $x_1, x_2, \ldots, x_n$; $\alpha_0, \alpha_1 \ldots, \alpha_{n-1}; \ldots$ Обращаясь к формулам (2), легко видеть, что если над $x_1, \ldots, x_n$; $u_1, \ldots, u_n$; $v_1, \ldots$ параллельно производить подстановки группы $\mathfrak{G}$, то величины $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$; $\beta_0, \beta_1, \ldots$ остаются инвариантными. С другой стороны, величины (3) все отличны от нуля при неопределенных $t_1, \ldots, t_k$; $\alpha_0, \ldots, \alpha_{n-1}; \beta_0, \ldots$ и, следовательно, можно придать $t_1, \ldots, t_k; \alpha_0, \ldots, \alpha_{n-1}; \beta_0, \ldots$ такие рациональные числовые значения, чтобы величины (3) оставались отличными от нуля. Отсюда следует, что величина Z является рациональной функцией от $x_1, x_2, \ldots, x_n$, принадлежащей к единичной группе. Значит, каждый из корней $x_1, x_2, \ldots, x_n$ уравнения (1) рационально выражается через Z, коэффициенты уравнения (1) и величину Φ (ср. [1]). Но Z зависит только от k переменных величин $z_1, \ldots, z_k$. Таким образом, величины $Z, Z^S, \ldots$ удовлетворяют уравнению

$$Z^n + \Pi_1 Z^{n-1} + \cdots + \Pi_{n-1} Z + \Pi_n = 0, \qquad (3')$$

которое и можно рассматривать как k-параметрическую резольвенту, что и т. д.

Замечание 1. Функция $Z(x_1, \ldots, x_n)$ никоим образом не является функцией, остающейся функцией от $z_1, z_2, \ldots, z_n$, когда над величинами $x_1, x_2, \ldots, x_n$ производятся преобразования группы Г. Чтобы убедиться в этом, заметим, что величины $\alpha_0, \ldots, \alpha_{n-1}$; $\beta_0, \beta_1, \ldots$ остаются инвариантными при преобразованиях группы $\mathfrak{G}$, но не при преобразованиях группы Г.

Иррациональность θ зависит от инвариантов расширенной н. г. п. Г. Но функции $z_1, \ldots, z_k$ можно выбрать так, чтобы они после подстановки постоянных значений $\alpha, \beta, \ldots$ зависели только от инвариантов первоначальной н. г. п. Г. Для этого рассмотрим вместо $x, u, v, \ldots$ как независимые переменные величины $x, \alpha, \beta, \ldots$ Заметим при этом, что переменные $\alpha, \beta, \ldots$ инвариантны относительно преобразований группы $\mathfrak{G}$ (но не группы Г). Полную систему инвариантов расширенной н. г. п. Г можно представить следующим образом:

$$\Psi_i(x_1, x_2, \ldots, x_n) = u_i \qquad (i = 1, 2, \ldots, p), \qquad (4)$$

$$\Psi_{p+i}(\gamma_1, \gamma_2, \ldots, \gamma_t) = v_i \qquad (i = 1, 2, \ldots, q), \qquad (5)$$

$$\Psi_{p+q+i}(x_{p+i}, \ldots, x_n; \gamma_{q+1}, \ldots, \gamma_t) = w_i \quad (i = 1, 2, \ldots, r-p-q). \qquad (6)$$

Здесь величины $\alpha, \beta, \ldots$ обозначены через $\gamma_1, \gamma_2, \ldots, \gamma_t$ $(t = n(s-1))$, p есть число инвариантов первоначальной н. г. п. Г, r — число инвариантов расширенной н. г. п. Г.

Воспользовавшись соотношениями (4) и (5), исключим из функций $z_i(x_1, \ldots, x_n; \gamma_1, \ldots, \gamma_t)$ переменные $x_1, \ldots, x_p$; $\gamma_1, \ldots, \gamma_q$. Получим

$$z_i(x_{p+1}, \ldots, x_n; \gamma_{q+1}, \ldots, \gamma_t; u_1, \ldots, u_p; v_1, \ldots, v_q) \quad (i = 1, 2, \ldots, k). \qquad (7)$$

Если положить здесь $u_i = \text{конст.}$, $v_i = \text{конст.}$ и рассматривать преобразования группы Γ в «укороченной» форме, то функции эти сохраняют свое основное свойство переводиться преобразованиями Γ в функционально-эквивалентные системы. С другой стороны, если положить в этих функциях $u_i = \text{конст.}$, $v_i = \text{конст.}$, $\gamma_{q+1} = \text{конст.}$, ..., $\gamma_t = \text{конст.}$, то они обращаются в однозначные, т. е. рациональные функции переменных $x_{p+1}, \ldots, x_n$, переходящие в функционально-эквивалентные системы, когда над $x_{p+1}, \ldots, x_n$ производятся преобразования группы $\mathfrak{G}$. Действительно, если

$$F(x_1, x_2, \ldots, x_n; \gamma_1, \ldots, \gamma_t; z) = 0$$

— уравнение, которому удовлетворяют величины z_i, то они, очевидно, удовлетворяют и уравнению

$$\prod_S F(x_1^S, x_2^S, \ldots, x_n^S; \gamma_1^S, \ldots, \gamma_t^S; z) = 0,$$

которое мы получим, рассматривая $x_1, \ldots, x_p; \gamma_1, \ldots, \gamma_q$ как алгебраические функции переменных $x_{p+1}, \ldots, x_n; \gamma_{q+1}, \ldots, \gamma_t$, определенные уравнениями (4) и (5), и обозначая через S подстановки группы Галуа образованного ими поля. Тогда, если рассматривать $u_1, \ldots, u_p; v_1, \ldots, v_q$ как величины, принадлежащие некоторому алгебраически-замкнутому полю коэффициентов, то z представляется как однозначная, т. е. рациональная, функция от $x_{p+1}, \ldots, x_n$.

Подстановка $v_i = \text{конст.}$, $\gamma_{q+1} = \text{конст.}$, ..., $\gamma_t = \text{конст.}$, очевидно, не налагает на $x_1, x_2, \ldots, x_n$ никаких ограничений. Если же мы полагаем $u_1 = \text{конст.}$, то x_i перестают быть независимыми функциями. Отсюда следует, что функции (7) зависят только от иррациональных функций переменных u_i, и, возможно, от числовых иррациональностей.

Вместо этой подстановки мы можем придать в (7) величинам γ_i подходяще выбранные постоянные значения и получить этим приемом те же самые функции. Если мы хотим построить функцию Z, исходя из (7), то коэффициенты соответствующей побочной резольвенты $R(\theta) = 0$ будут зависеть только от p параметров $u_1, \ldots, u_p$. Таким образом, здесь можно взять, например, $\theta = t_1 u_1 + \cdots + t_p u_p$, где $t_1, \ldots, t_p$ — подходяще выбранные рациональные числа.

Если уравнение (1) не нормальное, то число параметров побочной резольвенты $R(\theta) = 0$ может быть еще снижено. Именно, пусть это уравнение

$$X^s + P_1 X^{s-1} + \cdots + P_{s-1} X + P_s = 0 \qquad (1')$$

($s < n$). Тогда

$$x_1 = t_1 X_1 + t_2 X_2 + \cdots + t_s X_s. \qquad (8)$$

Здесь уже нельзя рассматривать x_i как независимые переменные, ибо они связаны $n - s$ линейными соотношениями. x_i мы всегда можем

заменить линейными комбинациями величин $y_1, y_2, \ldots, y_n$ таким образом, чтобы при применении к x_i подстановки (8) $y_1, \ldots, y_s$ переходили соответственно в $x_1, x_2, \ldots, x_s$, а $y_{s+1}, \ldots, y_n$ исчезали.

Теперь мы можем представить систему инвариантов группы Г следующим образом:

$$u_1(y_1, \ldots, y_s; y_{s+1}, \ldots, y_n),\ u_2(y_2, \ldots, y_s; y_{s+1}, \ldots, y_n), \ldots,$$
$$u_h(y_h, \ldots, y_s; y_{s+1}, \ldots, y_n),\ u_{h+1}(y_{s+1}, \ldots, y_n), \ldots, u_p(y_{s+1}, \ldots, y_n).$$

После подстановки (8) среди этих функций только h первых не становятся постоянными, так что коэффициенты $R(\theta) = 0$ зависят самое большее от h параметров.

С другой стороны, в силу уравнений

$$u_i(X_i, \ldots, X_s; 0, 0, \ldots, 0) = u_i \qquad (8')$$

величину $\xi = t_1 z_1 + \cdots + t_k z_k$ возможно представить как однозначную функцию от $X_{h+1}, \ldots, X_s$.[1] Отсюда следует, что степень транзитивности группы перестановок $\mathfrak{G}$ величин X_i не менее, чем h. Например, если $\mathfrak{G}$ — знакопеременная группа перестановок величин X_i, то $h \leqslant 2$. Ибо, если бы было $h \geqslant 3$, то ξ оставалась бы инвариантной относительно перестановки (X_1, X_2, X_3), что противоречит тому обстоятельству, что ξ изменяется от каждой перестановки группы $\mathfrak{G}$.

Число параметров в уравнении $R(\theta) = 0$ можно уменьшить еще на единицу. Именно, заметим, что по самому способу построения о. г. след от x_1 является инвариантом группы Г. Но след X_1, а значит, и x_1, можно рациональными операциями сделать равным нулю. Поэтому у группы Г остается только один инвариант и в уравнении $R(\theta)=0$ — один существенный параметр.

Теорема 8. *Если уравнение* (1) *имеет k-параметрическую резольвенту, то одевающая группа его группы Галуа* $\mathfrak{G}$, *построенная в* [1], *допускает представление в k-мерном пространстве. Представление это может быть несобственным, но должно содержать в качестве делителя группу, изоморфную* $\mathfrak{G}$.

Доказательство. Пусть

$$Z_1, Z_2, \ldots, Z_n \qquad (8'')$$

— корни k-параметрической резольвенты уравнения (1), которое мы предполагаем нормальным. Величины (8″) являются функциями от $x_1, x_2, \ldots, x_n$, принадлежащими единичной группе. Если производить над $x_1, x_2, \ldots, x_n$ подстановки группы $\mathfrak{G}$, то $Z_1, Z_2, \ldots, Z_n$ будут подвергаться некоторым подстановкам, образующим группу $\overline{\mathfrak{G}}$, изоморфную с $\mathfrak{G}$ и которая отличается от $\mathfrak{G}$ только другим обозначением переменных.

[1] (Примечание при корректуре). Так как она однозначна на многообразии (8′).

Возьмем за независимые переменные $Z_1, Z_2, \ldots, Z_n$ и оденем $\mathfrak{G}$ посредством н. г. п. Γ так, как было описано в [1]:

$$Z'_1 + \varepsilon_j Z'_2 + \cdots + \varepsilon_j^{n-1} Z'_n = e^{\varkappa i l}(Z_1 + \varepsilon_j Z_2 + \cdots + \varepsilon_j^{n-1} Z_n)$$

$$(j = 0, 1, \ldots, n-1;\ \varepsilon_j = e^{\frac{2\pi i j}{m}}). \qquad (9)$$

Затем используем тот факт, что величины $(8'')$ являются корнями k-параметрической резольвенты, т. е. между ними только k функционально независимы. Будем рассматривать $x_1, x_2, \ldots, x_n$ как координаты точки некоторого пространства R, считая точки $(x_1, \ldots, x_n)$ и $(x_1', \ldots, x_n')$ совпадающими, если

$$Z_i(x_1, \ldots, x_n) = Z_i(x_1', \ldots, x_n') \qquad (i = 1, 2, \ldots, n).$$

Пространство это, очевидно, имеет k измерений. Преобразования (9) определяют в R некоторую н. г. п., которая «локально изоморфна» с Γ и содержит как делитель группу, изоморфную $\mathfrak{G}$, так как, например, Z_1 принадлежит к единичной подгруппе группы $\mathfrak{G}$. Теорема доказана.

Замечание 2. При доказательстве этой теоремы существенно, что каждая система значений параметров этой н. г. п. однозначно определяет точку, в которую переходит заданная точка R. Поэтому наша группа подпадает под шрайеровское топологическое определение [3] и здесь применима вся теория Шрайера. Если же это условие не выполнено, то мы можем столкнуться, например, с тем обстоятельством, что нециклическая группа монодромии алгебраической функции одного переменного может допускать в качестве о. г. одночленную н. г. п.

Пример: одночленная н. г. п., определенная уравнениями

$$x + y + z = C_1,$$
$$x^2 + y^2 + z^2 = C_2,$$
$$x^3 + y^3 + z^3 = C_3,$$

содержит как делитель симметрическую группу подстановок трех элементов, которая даже не будет абелевой.

Теоремы 7 и 8 позволяют нам разрешить проблему резольвент в каждом отдельном случае посредством конечного числа действий. Для этого следует одеть группу $\mathfrak{G}$ данного уравнения способом, описанным в § 2. Затем отыскать все взаимно простые с $\mathfrak{G}$ нормальные делители н. г. п. Γ, одевающей группу $\mathfrak{G}$, и построить соответствующие им факторгруппы. Наконец, нужно исследовать, в каком пространстве наименьшего числа измерений представима каждая из этих факторгрупп. Для этого нужно достаточно расширить эти факторгруппы и найти их системы импримитивности, что, в силу теоремы 7, делает возможным и действительное построение резольвенты. Теорема 8 гласит, что так исчерпываются все возможные способы построения резольвент.

Поступило
20 ноября 1930 г.

ЛИТЕРАТУРА

1. N. Tschebotarö w. Über ein algebraisches Problem von Herrn Hilbert. I. Math. Ann. **104**, 1931. Собр. соч., т. I, 255—266.
2. D. Hilbert. Mathematische Probleme. Gött. Nachr., 1900, № 13, стр. 280.
3. O. Schreier. Abstrakte kontinuierliche Gruppen. Abh. Hamb. Sem. **4**, 1925, стр. 15—32.
4. J. Schur. Über die Darstellung usw. Journ. f. Math. **127**, 1904, стр. 20—50.
5. Lie-Engel. Theorie der Transformationsgruppen I. Lpz., 1888, стр. 522, Satz 92.
6. F. Klein. Gesammelte math. Abhandlungen, 2. Berlin, 1922, стр. 255—504; ср. также R. Fricke. Lehrbuch der Algebra, 2. Braunschweig, 1926.
7. Wiman. Math. Ann. **47**.
8. L. Bianchi. Lezioni sulla teoria dei gruppi continui di trasformazioni. Pisa, 1918, стр. 95—96.
9. N. Tschebotarö w. Zur Gruppentheorie des Klassenkörpers. Journ. f. Math. **161**, 1929, стр. 184, Definition 3. Собр. соч., т. I, стр. 121—140.
10. A. Speiser. Die Theorie der Gruppen von endlicher Ordnung. 1 Aufl., Berlin, 1923, стр. 119, Satz 113.
11. J. Schur. Über die stetigen Darstellungen der allgemeinen linèaren Gruppe. Sitzber. Berl. Akad., 1928, стр. 109, Satz IX.
12. W. Killing. Die Zusammensetzung usw. III. Math. Ann. **34**, стр. 57; E. E. Levi. Sulla struttura dei gruppi finiti e continui. Atti Torino **40**, 1905, стр. 424.
13. A. Speiser. Die Theorie der Gruppen von endlicher Ordnung. Berlin, 1923, стр. 119, Satz 113.

О КЛЕЙН-ГИЛЬБЕРТОВСКОЙ ПРОБЛЕМЕ РЕЗОЛЬВЕНТ

(ÜBER DAS KLEIN — HILBERTSCHE RESOLVENTENPROBLEM)

(Изв. КФМО 6 (1932 — 1933), стр. 5—22)

Несколько раньше я опубликовал две статьи [1], в которых изложил свои результаты, относящиеся к одной алгебраической проблеме, поставленной Ф. Клейном под названием «проблемы форм» [2] и впоследствии значительно обобщенной Д. Гильбертом [3]. Но так как мои работы были написаны in statu nascendi, так что при редактировании их мне самому не все было ясно, а теперь я в состоянии преодолеть некоторые встречавшиеся там затруднения, то я считаю целесообразным дать новое систематическое изложение своих результатов. При этом я большей частью ограничиваюсь простейшим случаем, когда группа Галуа проста, хотя некоторые из моих теорем легко распространяются и на более общие случаи. Однако рассматриваемый случай почти только один является существенным для этой теории. Эта статья не предполагает предварительного знакомства с моими прежними работами.

Я подчеркиваю теперь различие двух проблем, из которых первая проблема, в основном поставленная Клейном, может рассматриваться как частный случай второй проблемы, поставленной Гильбертом.

1. Проблема Клейна. Дано алгебраическое уравнение

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0, \qquad (1)$$

коэффициенты которого мы предполагаем неограниченно переменными. Требуется найти такое преобразование Чирнгаузена этого уравнения, чтобы коэффициенты преобразованного уравнения зависели от возможно меньшего числа переменных параметров.

Коэффициенты искомого преобразования могут содержать числовые иррациональности и некоторую функцию $\Phi(x_1, x_2, \ldots, x_n)$ от корней $x_1, x_2, \ldots, x_n$ уравнения (1), принадлежащую заданной группе подстановок $\mathfrak{G}$.

Проблему эту можно формулировать в терминах теории полей следующим образом.

Ia. Дано поле k, содержащее $n+1$ переменную $a_1, a_2, \ldots, a_n$; Φ, которые связаны алгебраическим соотношением

$$F(a_1, a_2, \ldots, a_n; \Phi) = 0.$$

Кроме того, задано алгебраическое расширение K этого поля, производящие величины которого $x_1, x_2, \ldots, x_n$ связаны с производящими величинами поля k следующим образом:

$$\begin{gathered} x_1 + x_2 + \ldots + x_n = -a_1, \\ x_1x_2 + \ldots + x_{n-1}x_n = a_2, \\ \cdots\cdots\cdots\cdots\cdots \\ x_1x_2\ldots x_{n-1} + \ldots + x_2x_3\ldots x_n = (-1)^{n-1}a_{n-1}, \\ x_1x_2\ldots x_n = (-1)^n a_n, \\ \Phi = \Phi(x_1, x_2, \ldots, x_n), \end{gathered} \tag{2}$$

где $\Phi(x_1, x_2, \ldots, x_n)$ есть рациональная функция, принадлежащая заданной группе подстановок $\mathfrak{G}$. При этом предполагается, что уравнение (1) после подстановки (2) удовлетворяется тождественно. Требуется найти такое подполе $\mathfrak{R}$ поля K, что:

1) композит полей $\mathfrak{R}$ и k есть поле K,

2) степень трансцендентности s поля $\mathfrak{R}$ была бы возможно меньше.

Число s мы назовем *истинной степенью трансцендентности* расширения K/k.

Последняя формулировка проблемы резольвент Клейна допускает следующее естественное обобщение:

Ib. Дано произвольное поле k степени трансцендентности n и его алгебраическое расширение K/k. Требуется найти такое подполе $\mathfrak{R}$ поля K возможно меньшей степени трансцендентности s, чтобы поля $\mathfrak{R}$ и k производили все поле K.

II. Проблема резольвент Гильберта. Дано алгебраическое расширение K/k поля k, имеющее степень трансцендентности n. Требуется найти наименьшее целое число s, обладающее следующими свойствами:

1) существует последовательность алгебраически-трансцендентных расширений $K_1/k, K_2/K_1, \ldots, K_m/K_{m-1}$, истинная степень трансцендентности каждого из которых равна s;

2) поле K_m содержит поле K.

В этой работе я полностью решаю только проблему I—Ia.

Представляется весьма вероятным, что проблема II не является тривиальным обобщением проблемы I, т. е. что в некоторых случаях решение проблемы II дает меньшее значение для s, чем решение проблемы I.

Содержание

§ 1. Теория представлений непрерывных групп преобразований

Основой наших исследований будет рассмотрение непрерывных групп преобразований (короче: н. г. п.) вида

$$x_i' = f_i(x_1, x_2, \ldots, x_n; a_1, a_2, \ldots, a_r) \qquad (1.1)$$
$$(i = 1, 2, \ldots, n).$$

Две н. г. п. называются *локально изоморфными* (по Ли: gleich zusammengesetz), если инфинитезимальные операторы $X_1, X_2, \ldots, X_r$ обеих групп могут быть выбраны так, что структурные постоянные c_{ij}^{ν} в соотношениях

$$(X_i, X_j) = \sum_{\nu=1}^{r} c_{ij}^{\nu} X_\nu \qquad (i, j = 1, 2, \ldots, r)$$

будут одинаковы для обеих групп.

Две н. г. п. Γ и $\overline{\Gamma}$ называются *подобными*, если существует такое преобразование S, которое каждое преобразование A группы Γ переводит в некоторое преобразование $\overline{A}$ группы $\overline{\Gamma}$: $S^{-1}AS = \overline{A}$ или $S^{-1}\Gamma S = \overline{\Gamma}$. Подробнее: если

$$\Gamma: \quad x' = f(x, a),$$
$$\overline{\Gamma}: \quad y' = \overline{f}(y, a),$$

то существует обратимое преобразование

$$S: \quad x = \varphi(y), \qquad y = \varphi^{-1}(x),$$

такое, что

$$\varphi^{-1}[f(\varphi(y), a)] = \overline{f}(y, a)$$

или

$$f(\varphi(y), a) = \varphi(\overline{f}(y, a)).$$

Для простоты мы предполагаем, что параметр a один и тот же в обеих группах. Вообще же, для того чтобы перевести группу Γ в $\overline{\Gamma}$, следует вместе с переменной x преобразовать также и параметр a. Но группы, которые переводятся друг в друга преобразованием параметра, мы будем рассматривать как просто совпадающие.

Таким образом, для того чтобы перейти от группы Γ к группе $\overline{\Gamma}$, следует заменить в определяющих группу уравнениях переменные x переменными y с помощью преобразования S.

Рассмотрим также случай, когда преобразование S необратимо, т. е. когда система функций φ_i содержит меньше, чем n, функционально независимых. В этом случае мы говорим, что представление $\overline{\Gamma}$ *содержит* представление Γ, или символически: $\overline{\Gamma} \supset \Gamma$. Очевидно, что понятие это транзитивно, т. е. имеет место

Теорема 1. *Если* $\Gamma_1 \supset \Gamma$, $\Gamma_2 \supset \Gamma_1$, *то* $\Gamma_2 \supset \Gamma$.

Пусть Γ является параметрической группой какой-либо н. г. п. $\mathfrak{G}$, а Γ_1 — произвольное представление группы $\mathfrak{G}$. Тогда имеет место

Теорема 2. *Параметрическая группа некоторой н. г. п. содержит все существующие представления этой группы.*

Доказательство. Пусть (1.1) будут уравнения н. г. п. Γ_1, а

$$a_i = \varphi_i(a, b) \qquad (i = 1, 2, \ldots, r) \tag{1.2}$$

— уравнения ее параметрической группы Γ. Тогда

$$f_i(f(x, a), b) = f_i(x, \varphi(a, b)) \qquad (i = 1, 2, \ldots, n). \tag{1.3}$$

Придадим переменным x_i произвольные постоянные значения $x_i^{(0)}$. Уравнения (1.3) показывают, что если мы будем подвергать параметры a_i преобразованиям $a_i = \varphi_i(a, b)$ группы Γ, то переменные $x_i' = f_i(x^{(0)}, a)$ будут претерпевать преобразования $x_i'' = f_i(x', b)$ группы Γ, что и т. д.

Характерным для параметрической группы является ее свойство быть *просто транзитивной*. Это значит, что в ней найдется одно и только одно преобразование, переводящее одну из двух произвольно заданных точек в другую. Аналитически свойство это выражается тем, что порядок группы и размерность ее пространства представления совпадают и что ее инфинитезимальные операторы не связаны никаким линейным соотношением типа

$$\varphi_1(x_1, x_2, \ldots, x_n) X_1(f) + \varphi_2(x_1, x_2, \ldots, x_n) X_2(f) + \ldots + \varphi_n(x_1, x_2, \ldots, x_n) X_n(f) = 0.$$

Теорему 2 можно доказать, основываясь только на простой транзитивности параметрической группы. Действительно, пусть $X_1, X_2, \ldots, X_r$ и $Y_1, Y_2, \ldots, Y_r$ будут системы инфинитезимальных операторов двух локально изоморфных групп и первая из них просто транзитивна. Тогда система

$$X_i(f) + Y_i(f) = 0 \qquad (i = 1, 2, \ldots, r) \tag{1.4}$$

имеет ровно $(n + r) - r = n$ независимых интегралов $\Phi_1, \Phi_2, \ldots, \Phi_n$, где n — размерность пространства представления $(y_1, y_2, \ldots, y_n)$ первой группы. В силу транзитивности первой группы, система (1.4) не имеет решений, зависящих только от x_i, и, значит, якобиан

$$\frac{d(\Phi_1, \Phi_2, \ldots, \Phi_n)}{d(y_1, y_2, \ldots, y_n)}$$

не исчезает тождественно. Следовательно, система конечных уравнений

$$\Phi_1 = c_1, \quad \Phi_2 = c_2, \ldots, \Phi_n = c_n$$

разрешима относительно $y_1, y_2, \ldots, y_n$, и легко убедиться, что полученные при этом уравнения

$$y_1 - \varphi_1(x_1, x_2, \ldots, x_n) = 0,$$
$$y_2 - \varphi_2(x_1, x_2, \ldots, x_n) = 0, \ldots, y_n - \varphi_n(x_1, x_2, \ldots, x_n) = 0 \qquad (1.5)$$

определяют искомое преобразование [4].

Отсюда непосредственно следует, что две изоморфные просто транзитивные н. г. п. подобны.

Пусть Γ и Γ_1 — два представления некоторой н. г. п., причем $\Gamma \supset \Gamma_1$. Последнее всегда выполняется, если группа Γ просто транзитивна. Если преобразование (1.5) переводит Γ в Γ_1, то уравнения

$$\varphi_1(x_1, x_2, \ldots, x_r) = c_i \qquad (i = 1, 2, \ldots, r) \qquad (1.6)$$

определяют одну из систем импримитивности группы Γ вследствие того, что всякое преобразование группы Γ переводит переменные y_i в функции от одних только y_i. Обратно, если уравнения (1.6) представляют систему импримитивности группы Γ, то каждое преобразование группы Γ переводит уравнения (1.6) в уравнения типа $\varphi_i(x_1, x_2, \ldots, x_n) = c_i'$, причем константы c_i являются функциями от c_i' и параметров a группы Γ:

$$c_i = \psi_i(c', a) \qquad (i = 1, 2, \ldots, n).$$

Другими словами, имеют место соотношения

$$\varphi_i(f(x, a)) = \psi_i(\varphi(x), a) \qquad (i = 1, 2, \ldots, n).$$

Отсюда следует, что уравнения

$$y_i = \psi_i(y_i, a) \qquad (i = 1, 2, \ldots, n)$$

определяют некоторую изоморфную (или гомоморфную) с Γ н. г. п. Γ_1, которая получается из Γ посредством преобразования

$$y_i = \varphi_i(x_1, x_2, \ldots, x_n).$$

Группа эта транзитивна тогда и только тогда, если функции $\varphi_i(x)$ — функционально независимы. Вычеркивая из системы $\varphi_i(x)$ те функции, которые зависят от других, мы получим транзитивное представление (*укороченную группу*). Обратно, имея транзитивное представление, можно получить из него некоторое интранзитивное представление, если дополнить систему переменных $y_i = \varphi_i(x_1, x_2, \ldots, x_n)$ некоторой новой системой переменных, инвариантных относительно преобразований группы Γ. Если над полученной таким образом системой переменных производить самые общие преобразования, то получится наиболее общее представление, принадлежащее нашей системе импримитивности. Сказанное позволяет нам рассматривать только транзитивные представления.

Если представление Γ содержит другое представление Γ_1 той же группы и это последнее не подобно представлению Γ, то переменные представления Γ_1, выраженные как функции от переменных представления Γ, определяют левые части уравнений некоторой системы импри-

мативности группы Г. С другой стороны, Ли ([4], стр. 522, теорема 92) нашел следующий наиболее общий способ построения систем импримитивности транзитивной группы. Следует построить *стационарную группу* (Stabilitätsgruppe) H_p произвольной точки P пространства представления Г, т. е. совокупность всех тех преобразований группы Г, которые оставляют неподвижной точку P. Затем взять произвольную, лежащую между Г и H_p группу Σ (наличие такой группы необходимо и достаточно для того, чтобы группа Г была импримитивна) и определить то многообразие, которое получится, если подвергать точку P всем преобразованиям группы Σ. Число степеней свободы этой системы импримитивности (т. е. число функционально независимых среди левых частей уравнений системы импримитивности; иными словами, размерность пространства представления укороченной группы Г) равно *индексу* группы Σ относительно Г, т. е. разности порядков этих групп. Представление Γ_1 будет правильным (treu), т. е. изоморфным с Г тогда и только тогда, если Σ не содержит никаких нормальных делителей группы Г, кроме единичной группы.

Если группа Г просто транзитивна, то стационарная группа H совпадает с единичной группой, так что каждой подгруппе группы Г соответствует содержащееся в Г представление, и наоборот. Представление это примитивно тогда и только тогда, если соответствующая ему подгруппа *максимальна*, т. е. не содержится ни в какой подгруппе группы Г, отличной от Г. Если Γ_1 и Γ_2 — два представления одной и той же группы, то $\Gamma_1 \supset \Gamma_2$ тогда и только тогда если для соответствующих им подгрупп Σ_1, Σ_2 параметрической группы имеет место

$$\Sigma_1 \leqslant S^{-1}\Sigma_2 S,$$

где S есть подходящее подобранное преобразование параметрической группы, а знак $\leqslant$ означает, что левая часть является делителем правой части.

Мы приходим, таким образом, к следующей теореме:

Теорема 3. *Н. г. п.* Г *тогда и только тогда имеет представление в s-мерном пространстве* (*мы будем говорить короче: является s-группой*), *если она имеет подгруппу индекса s, не содержащую никакого нормального делителя группы* Г, *кроме единичной группы.*

Представляется вероятным, что всякое представление можно получить чисто алгебраическими операциями из конечных уравнений параметрической группы. Мы покажем сначала, что инфинитезимальные операторы такого представления можно получить алгебраически, а затем докажем, что при известных ограничениях, налагаемых на структуру группы, то же самое возможно и для ее конечных уравнений.

Чтобы доказать первую часть этого утверждения, достаточно показать, что все подгруппы данной транзитивной н. г. п. можно определить алгебраически. Ли ([4], стр. 208—210, § 5) дал следующий способ

этого определения. Пусть $X_1, X_2, \ldots, X_r$ будут инфинитезимальные операторы н. г. п. Г. Ищем такие их линейные комбинации

$$Y_i = g_{i1}X + g_{i2}X_2 + \ldots + g_{ir}X_r \qquad (i = 1, 2, \ldots, m), \tag{1.7}$$

которые удовлетворяют соотношениям

$$(Y_i, Y_j) = \sum_{\nu=1}^{m} \gamma_{ij}^{\nu} Y_\nu \qquad (i, j = 1, 2, \ldots, m). \tag{1.8}$$

Подставляя в последние Y_i из (1.7) и пользуясь формулами

$$(X_i, X_j) = \sum_{\nu=1}^{r} c_{ij}^{\nu} X_\nu \qquad (i, j = 1, 2, \ldots, r),$$

получим

$$(Y_i, Y_j) = \sum_{\lambda, \mu=1}^{r} g_{i\lambda} g_{j\mu} (X_\lambda, X_\mu) = \sum_{\lambda, \mu, \nu} g_{i\lambda} g_{j\mu} c_{\lambda\mu}^{\nu} X_\nu.$$

С другой стороны,

$$\sum_{\nu} \gamma_{ij}^{\nu} Y_\nu = \sum_{\nu, \mu} \gamma_{ij}^{\nu} g_{\nu\mu} X_\mu.$$

Приравнивая коэффициенты при X_ν в обеих частях равенства (1.8), получим

$$\sum_{\lambda, \mu} g_{i\lambda} g_{j\mu} c_{\lambda\mu}^{\nu} = \sum_{\mu} \gamma_{ij}^{\mu} g_{\mu\nu}.$$

Исключая из этой системы постоянные γ_{ij}^{μ} мы получим для определения $g_{\mu\nu}$ систему алгебраических уравнений. Подставляя решение этой системы в (1.7), найдем искомые инфинитезимальные операторы $Y_1, Y_2, \ldots, Y_m$.

Прежде чем переходить к определению конечных уравнений подгруппы, мы докажем одну весьма важную теорему, полученную Э. Картаном [5], которая позволяет рассматривать множество всех представлений некоторой н. г. п. как множество в известном смысле «архимедово».

Теорема 4. *Если* Γ *и* Γ_1 *— два произвольных представления некоторой н. г. п., то найдется такой показатель* m, *что* $\Gamma^m \supset \Gamma_1$.

Под степенью Γ^m представления

$$\Gamma: \qquad x_i' = f_i(x_1, x_2, \ldots, x_n; a_1, a_2, \ldots, a_r) \qquad (i = 1, 2, \ldots, m)$$

мы понимаем представление в nm-мерном пространстве

$$\begin{array}{l} x_1, x_2, \ldots, x_n, \\ x_1', x_2', \ldots, x_n', \\ \ldots\ldots\ldots \\ x_1^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}, \end{array}$$

любое преобразование которого индуцирует в каждом пространстве $x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}$ преобразования представления Γ с теми же значениями параметров $a_1, a_2, \ldots, a_r$ («расширение группы» — по Ли).

Доказательство. Пусть

$$X_i(f) = \sum_{\nu} \xi_{i\nu}(x) \frac{\partial f}{\partial x_\nu} \qquad (i = 1, 2, \ldots, r)$$

— инфинитезимальные операторы представления Г. Выберем m настолько большим, чтобы ранг матрицы

$$\begin{gathered}
\xi_{11}(x), \xi_{12}(x), \ldots, \xi_{1n}(x); \xi_{11}(x'), \ldots; \ldots, \xi_{1n}(x^{(m-1)}), \\
\xi_{21}(x), \xi_{22}(x), \ldots, \xi_{2n}(x); \xi_{21}(x'), \ldots; \ldots, \xi_{2n}(x^{(m-1)}), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\xi_{r1}(x), \xi_{r2}(x), \ldots, \xi_{rn}(x); \xi_{r1}(x'), \ldots; \ldots, \xi_{rn}(x^{(m-1)})
\end{gathered}$$

был равен r. Это всегда возможно, так как вследствие независимости операторов $X_1, X_2, \ldots, X_r$ между строчками этой матрицы не существует линейных соотношений с постоянными коэффициентами. Затем найдем решения системы

$$\begin{gathered}
Y_1(f) + X_1(f) + X_1'(f) + \cdots + X_1^{(m-1)}(f) = 0, \\
Y_2(f) + X_2(f) + X_2'(f) + \cdots + X_2^{(m-1)}(f) = 0, \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
Y_r(f) + X_r(f) + X_r'(f) + \cdots + X_r^{(m-1)}(f) = 0,
\end{gathered}$$

где $X_j^{(i)}(f) = \sum_{\nu=1}^{n} \xi_{j\nu}(x^{(i)}) \frac{\partial f}{\partial x^{(i)}}$, а $Y_i(f)$ есть оператор, соответствующий оператору $X_i(f)$ в представлении Γ_1, заданном в пространстве $(y_1, y_2, \ldots, y_s)$. Очевидно, что система эта полная и, значит, имеет $s + mn - r$ независимых интегралов. Между этими интегралами найдется ровно $mn - r$ таких, которые зависят только от переменных $x_j^{(i)}$ $(i = 0, 1, \ldots, m-1; j = 1, 2, \ldots, n)$. Остальные же интегралы можно, следовательно, привести к виду

$$\begin{gathered}
y_1 - \theta_1(x_1, x_2, \ldots, x_n^{(m-1)}), \; y_2 - \theta_2(x_1, x_2, \ldots, x_n^{(m-1)}), \ldots, \\
y_s - \theta_s(x_1, x_2, \ldots, x_n^{(m-1)}).
\end{gathered}$$

Тогда формулы

$$\begin{gathered}
y_1 = \theta_1(x_1, x_2, \ldots, x_n^{(m-1)}), \; y_2 = \theta_2(x_1, x_2, \ldots, x_n^{(m-1)}), \ldots, \\
y_s = \theta_s(x_1, x_2, \ldots, x^{(m-1)})
\end{gathered}$$

дадут искомое преобразование, переводящее представление Γ^m в представление Γ_1.

Замечание. Мы нигде не предполагаем, что представление Γ_1 правильное. Таким образом, можно утверждать, что достаточно высокая степень любого представления данной н. г. п. $\mathfrak{G}$ содержит также представления факторгрупп группы $\mathfrak{G}$.

Переходим к доказательству нашего утверждения о возможности алгебраического нахождения конечных уравнений представления. При

этом мы предположим, что группа $\mathfrak{G}$ *полупроста*. Это значит, что $\mathfrak{G}$ не содержит отличных от единичной группы разрешимых нормальных делителей. Тогда ее присоединенная группа E является правильным представлением. В силу теоремы 4, достаточно высокая степень группы E содержит параметргруппу, и потому мы можем вместо параметргруппы рассматривать такую степень группы E. Чтобы алгебраически получить какую-либо максимальную подгруппу группы $\mathfrak{G}$, мы предположим, следуя В. Киллингу [6], что искомая подгруппа содержит такое преобразование, отличные от нуля характеристические корни которого все — простые. Картан [7] считает весьма правдоподобным, что это предположение не содержит никаких действительных ограничений. Известно, что инфинитезимальные операторы группы E можно нормировать таким образом, чтобы некоторые из них — $Y_1, Y_2, \ldots, Y_l$ (l называется *рангом* группы $\mathfrak{G}$) — были перестановочны между собой, в то время как остальные $X_1, X_2, \ldots, X_{r-l}$ были бы связаны с Y_i соотношениями

$$(X_i, e_i Y_i + e_2 Y_2 + \cdots + e_l Y_l) = (e_1 \omega_i^{(1)} + e_2 \omega_i^{(2)} + \cdots + e_l \omega_i^{(l)}) X_i,$$

где $\omega_i^{(j)}$ представляют отличные от нуля характеристические корни оператора Y_j.

Киллинг ([6], стр. 242) показал, что всякая подгруппа $\mathfrak{H}$ группы $\mathfrak{G}$, содержащая, например Y_1, порождается входящими в нее операторами X_i, Y_j. Если, кроме того, группа $\mathfrak{H}$ максимальна, то она содержит все операторы $Y_1, Y_2, \ldots, Y_l$. Можно взять за Y_1 такую линейную комбинацию $Y_1, Y_2, \ldots, Y_l$, чтобы соответствующие ей характеристические корни были просты, а отношения их рациональны (для этого достаточно взять в качестве Y_1 какой-либо из операторов $(X_\alpha, X_{\alpha'})$, где $X_\alpha, X_{\alpha'}$ — операторы, соответствующие корням ω_α и $-\omega_\alpha$ ([7], стр. 42). Более того, всю порожденную операторами Y_i абелеву группу можно построить из операторов такого рода. С другой стороны, очевидно, что вся группа $\mathfrak{G}$ порождается посредством операторов, отличные от нуля характеристические корни которых просты. Каждый из таких операторов, взятый за Y_1, можно описанным выше образом заменить посредством нескольких операторов типа $(X_\alpha, X_{\alpha'})$, для каждого из которых отличные от нуля характеристические корни просты и находятся в рациональных отношениях. Таким образом, за операторы, порождающие группу $\mathfrak{G}$, можно взять независимые операторы этого типа $Z_1, Z_2, \ldots, Z_u$. Теперь, чтобы найти конечные уравнения группы $\mathfrak{H}$, достаточно найти инварианты m-ой степени группы E. Таковыми будут решения системы

$$Z_i + Z_i' + \cdots + Z_i^{(m-1)} = 0 \qquad (i = 1, 2, \ldots, u), \tag{1.9}$$

где пространство $(x_1, x_2, \ldots, x_r)$ есть пространство представления присоединенной группы, а пространства $(x_1^{(i)}, x_2^{(i)}, \ldots, x_r^{(i)})$ $(i = 0, 1, \ldots, m-1)$ в совокупности содержат параметргруппу. Решения

каждого отдельного уравнения системы (1.9) суть интегралы одной из систем линейных однородных дифференциальных уравнений

$$\frac{dx_1}{\sum_\nu c^1_{i\nu} x_\nu} = \frac{dx_2}{\sum_\nu c^2_{i\nu} x_\nu} = \cdots = \frac{dx_r^{(m-1)}}{\sum_\nu c_{i\nu}{}^r x_\nu^{(m-1)}} = dt \qquad (1.10)$$

$$(i = 1, 2, \ldots, u).$$

Каждая из этих систем имеет простые элементарные делители, и потому интегралы ее могут быть записаны в виде

$$z_1 = c_1 e^{\omega_1 t},\ z_2 = c_2 e^{\omega_2 t},\ \ldots,\ z_r^{(m-1)} = c_r^{(m-1)} e^{\omega_r t},$$

где z_i представляют некоторые линейные функции от x_i. Так как отношения величин ω_i рациональны, то отсюда посредством исключения t получаются алгебраические интегралы. Для получения же решений всей системы нужно построить такие функции, которые можно представить как функции от интегралов каждой из систем (1.10) для $i = 1, 2, \ldots, u$, а это есть чисто алгебраическая задача. Таким образом доказана

Теорема 5. *Каждая полупростая s-группа имеет в s-мерном пространстве алгебраическое представление* ([7], стр. 133).

Киллинг и Картан ([7], стр. 151) определили все типы простых групп и вычислили для каждой из них индекс s наибольшей подгруппы. Результаты их представляются в таком виде.

1° *Унимодулярные линейные однородные группы* от n переменных (тип A); $r = n^2 - 1$, $s = n - 1$.

2° *Ортогональные группы* от n переменных (тип B при нечетном n и тип D при четном n); $r = \frac{n(n-1)}{2}$, $s = n - 1$,

3° *Комплексгруппы* от n переменных (n — четное), т. е. линейные однородные группы, которые оставляют инвариантным выражение Пфаффа

$$(x_1\,dx_2 - x_2\,dx_1) + (x_3\,dx_4 - x_4\,dx_3) + \cdots + (x_{n-1}\,dx_n - x_n\,dx_{n-1})$$

(тип C); $r = \frac{n(n+1)}{2}$, $s = n - 1$.

4° Тип E:

1) группа G_{78}; $r = 78$, $s = 16$;

2) группа G_{133}; $r = 133$, $s = 27$;

3) группа G_{248}; $r = 248$, $s = 57$.

5° Тип F: G_{52}; $r = 52$, $s = 15$.

6° Тип G: G_{14}; $r = 14$, $s = 5$.

§ 2. Конечные и непрерывные группы

Связь между конечными и непрерывными группами изучалась уже с давних пор, когда была поставлена следующая задача, приведшая к весьма замечательным результатам [8, 9]: определить все конечные подгруппы данной непрерывной группы.

Мы займемся следующим обращением этой задачи: определить все н. г. п., изоморфные с заданной конечной группой.

Так как при этой формулировке задачи мы вынуждены рассматривать бесконечное множество неинтересных для нас решений (например, каждая надгруппа любого решения будет тоже решением), то уточним нашу проблему, назвав ее проблемой отыскания *одевающих групп* [1] (короче — о. г.), причем определим это понятие следующим образом:

Н. г. п. Γ называется о. г. конечной группы $\mathfrak{G}$, если:

1° Γ содержит делитель, изоморфный с $\mathfrak{G}$,

2° ни одна из правильных непрерывных подгрупп группы Γ не обладает свойством 1°,

3° ни одна из правильных непрерывных факторгрупп группы Γ не обладает свойством 1°.

В большинстве случаев, когда нам придется искать о. г. для конечной группы $\mathfrak{G}$, эта последняя будет простой группой. Тогда справедлива

Теорема 6. *Каждая о. г. простой группы* $\mathfrak{G}$ *также проста.*

Доказательство. Предположим, что о. г. Γ группы $\mathfrak{G}$ содержит правильный непрерывный нормальный делитель Γ_1. Подгруппа G группы Γ, изоморфная с $\mathfrak{G}$, имеет с Γ_1 пересечение G_1. Так как каждая сопряженная с группой G_1 группа $S^{-1}G_1S$ содержится в группе $S^{-1}\Gamma_1 S=\Gamma_1$, то G_1 является нормальным делителем группы G. Последняя проста, и потому либо $G=G_1$, либо $G_1=1$. В первом случае мы приходим к противоречию с условием 2°. Во втором случае среди элементов $U\Gamma_1$ факторгруппы Γ/Γ_1 (U пробегает элементы группы Γ) содержатся все элементы $S\Gamma_1$, где S пробегает всю совокупность элементов группы G. Элементы $S\Gamma_1$ все отличны друг от друга и, следовательно, образуют группу, изоморфную с G, что противоречит условию 3°.

Когда мы ищем о. г. данной конечной группы $\mathfrak{G}$, то естественно определить для каждой о. г. одно из ее представлений, например представление в виде линейной однородной группы. Но здесь возникает некоторое затруднение, так как все представления одной и той же н. г. п. только локально изоморфны между собой. Поэтому вполне может случится, что из двух представлений одно будет содержать группу $\mathfrak{G}$, а другое нет. Вследствие этого мы должны несколько углубиться в развитую О. Шрейером [10] теорию локально изоморфных н. г. п.

Если рассматривать элементы каждой н. г. п. как точки соответствующего «группового пространства», то локальный изоморфизм двух н. г. п. означает взаимное соответствие окрестностей единичных

[1] В прежних работах я употреблял название «Einkleidungsgruppe» (здесь автор пользуется термином «Einbettungsgruppe» — *Ред.*)

элементов этих групп. Это однозначное соответствие можно неограниченно продолжить аналитически, так как окрестности любых соответствующих друг другу точек, лежащих внутри уже отображенных друг на друга окрестностей, также могут быть взаимно отображены друг на друга. Однако отсюда можно заключить, что обе группы изоморфны (в целом) только тогда, если каждое из соответствующих им групповых пространств *односвязно*, т. е. если в любом из них каждый замкнутый путь может быть непрерывно стянут в точку. Если же групповое пространство не односвязно, то, как доказал Шрейер (выше цит.), ему можно сопоставить некоторое односвязное *накрывающее пространство*. Соответствующая этому пространству группа (называемая *накрывающей группой*) обладает тем свойством, что каждая локально изоморфная с ней группа изоморфна с ее факторгруппой относительно некоторого нормального делителя Δ, элементы которого дискретны (это значит, что для каждого элемента из Δ можно найти такую его окрестность внутри группового пространства, которая не содержит других элементов из Δ).

Теорема 7 (Шрейера). *Если две н. г. п.* Γ *и* Γ_1 *локально изоморфны и если группа* Γ_1 *изоморфна группе* Γ/Δ, *то* Δ *лежит в центре группы* Γ.

Доказательство. Пусть U — произвольное преобразование группы Γ. Будем непрерывно изменять значения параметров группы Γ таким образом, чтобы соответствующее им преобразование непрерывно изменялось от тождественного преобразования I до U. Так как Δ есть нормальный делитель группы Γ, то все преобразования $U^{-1}DU$ (где D принадлежит к Δ) содержатся в Δ. С другой стороны, $I^{-1}DI = D$. При непрерывном изменении параметров преобразования U преобразование $U^{-1}DU$ изменяется также непрерывно и потому остается в некоторой окрестности преобразования D, не содержащей никаких других преобразований из Δ. Следовательно, $U^{-1}DU = D$, и теорема доказана.

Пусть Γ_1 есть о. г. конечной группы $\mathfrak{G}$ и Γ — накрывающая группа группы Γ_1. Γ может не содержать никакой изоморфной с $\mathfrak{G}$ подгруппы, так как при отображении Γ на Γ_1 в изоморфную с группой $\mathfrak{G}$ подгруппу G_1 может переходить такая группа G, только некоторая факторгруппа которой G/H изоморфна с $\mathfrak{G}$. Здесь H является делителем Δ и, следовательно, содержится в центре группы G.

В частности, если группа $\mathfrak{G}$ проста, то коммутаторгруппа G' группы G также содержит в качестве факторгруппы группу, изоморфную с $\mathfrak{G}$, и содержится в Γ как делитель. Докажем, что G' совпадает со своей коммутаторгруппой G''. Так как факторгруппа G/Δ изоморфна с группой $\mathfrak{G}$, т. е. проста и, следовательно, совпадает со своей коммутаторгруппой, то каждый элемент s группы G/Δ можно представить в виде $\prod_{i,j} s_i s_j s_i^{-1} s_j^{-1}$. Отсюда следует, что всякий элемент S группы G

может быть представлен в форме

$$D\prod_{i,j} S_i S_j S_i^{-1} S_j^{-1}, \tag{2.1}$$

где D — элемент группы Δ. Для того чтобы доказать, что всякий элемент G' содержится в G'', достаточно показать это для элементов вида $S_1 S_2 S_1^{-1} S_2^{-1}$. Если

$$S_1 = D_1 \prod_{i,j} S_{1i} S_{1j} S_{1i}^{-1} S_{1j}^{-1},$$

$$S_2 = D_2 \prod_{i,j} S_{2i} S_{2j} S_{2i}^{-1} S_{2j}^{-1},$$

то

$$S_1 S_2 S_1^{-1} S_2^{-1} = \left(D_1 \prod_{i,j} S_{1i} S_{ij} S_{1i}^{-1} S_{1j}^{-1}\right)\left(D_2 \prod_{i,j} S_{2i} S_{2j} S_{2i}^{-1} S_{2j}^{-1}\right)$$

$$\left(D_1 \prod_{i,j} S_{1i} S_{1j} S_{1i}^{-1} S_{1j}^{-1}\right)^{-1}\left(D_2 \prod_{i,j} S_{2i} S_{2j} S_{2i}^{-1} S_{2j}^{-1}\right)^{-1}$$

или, так как элементы D_1, D_2 перестановочны со всеми S,

$$S_1 S_2 S_1^{-1} S_2^{-1} = \left(\prod_{i,j} S_{1i} S_{1j} S_{1i}^{-1} S_{1j}^{-1}\right)\left(\prod_{i,j} S_{2i} S_{2j} S_{2i}^{-1} S_{2j}^{-1}\right)$$

$$\prod_{i,j} (S_{1i} S_{1j} S_{1i}^{-1} S_{1j}^{-1})^{-1}\left(\prod_{i,j} S_{2i} S_{2j} S_{2i}^{-1} S_{2j}^{-1}\right)^{-1}.$$

Отсюда непосредственно следует, что $S_1 S_2 S_1^{-1} S_2^{-1}$ содержится в G'', что и требовалось.

Таким образом доказано, что накрывающая группа группы Γ_1, и значит всякая н. г. п., изоморфная с Γ_1, имеет делитель G', факторгруппа которого относительно центра изоморфна с группой $\mathfrak{G}$ и коммутаторгруппа которой совпадает с самой группой G'.

Такие группы можно считать частным случаем рассмотренных И. Шуром [11] групп представления $\mathfrak{R}$ группы $\mathfrak{G}$, которые он характеризовал такими свойствами:

«1. $\mathfrak{R}$ содержит подгруппу $\mathfrak{M}$, состоящую из инвариантных элементов группы $\mathfrak{R}$, причем факторгруппа $\mathfrak{R}/\mathfrak{M}$ изоморфна с группой G;

2. Коммутаторгруппа $\mathfrak{R}$ содержит все элементы группы $\mathfrak{M}$;

3. Не существует такой группы, которая обладала бы свойствами 1 и 2 и порядок которой превышал бы порядок группы $\mathfrak{R}$».

И. Шур показывает, что всякая группа $\mathfrak{G}$ имеет только конечное число неизоморфных групп представления и дает метод для построения всех групп представления. При этом он доказывает, что если группа $\mathfrak{G}$ совпадает со своей коммутаторгруппой, что наверное имеет место, если группа $\mathfrak{G}$ простая, то существует только одна группа представления группы $\mathfrak{G}$ ([11], стр. 38, IV).

Пример. Знакопеременная группа шестой степени может быть представлена как группа дробных линейных подстановок от двух

переменных. Однако ее нельзя представить как однородную линейную группу от трех переменных. Последнее имеет место впервые для ее группы представления, порядок которой равен 3.360 [12].

Для того чтобы построить о. г. некоторой конечной группы, заметим, что всякое представление Г любой простой н. г. п. может быть представлено в виде линейной однородной группы. При этом изоморфная с группой $\mathfrak{G}$ подгруппа этой группы будет представлена в виде конечной линейной однородной группы. Предположим, что группа $\mathfrak{G}$ — приводима, именно, что ее матрицы посредством линейного преобразования T приводятся к виду $S = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$. Отсюда еще не следует приводимость группы $T^{-1}\Gamma T$. Однако если взять какой-либо инфинитезимальный оператор X группы $T^{-1}\Gamma T$, содержащий подстановку S, то X (рассматриваемый как матрица) будет перестановочен с S. Если бы все характеристические корни матрицы S были простыми, то одно и то же линейное преобразование приводило бы матрицы X и S одновременно к диагональной форме. Значит, X имеет вид $\begin{pmatrix} M & 0 \\ 0 & N \end{pmatrix}$. С другой стороны, если S пробегает систему производящих подстановок группы $\mathfrak{G}$ (т. е. таких, композиция которых дает всю группу $\mathfrak{G}$), то система соответствующих им инфинитезимальных операторов X_i не может содержаться ни в какой правильной подгруппе группы $T^{-1}\Gamma T$. Действительно, в противном случае, в силу условия 2 определения о. г., группа Г не была бы о. г. группы $\mathfrak{G}$. Иначе говоря, операторы X_i и порожденные ими операторы (X_i, X_j) представляют полную систему инфинитезимальных операторов группы $T^{-1}\Gamma T$. Отсюда видно, что группа Г может быть неприводимой только тогда, если каждая система производящих подстановок группы $\mathfrak{G}$ содержит подстановки с кратными характеристическими корнями. Это обстоятельство необходимо имеет место, если некоторые неприводимые части группы $\mathfrak{G}$ подобны друг другу. Весьма вероятно, что характеристические корни могут быть кратными только в этом случае.

Общая задача одевания группы $\mathfrak{G}$ может быть сформулирована так. Пусть $I, A, B, \ldots$ — совокупность линейных подстановок, соответствующих элементам группы $\mathfrak{G}$. Введем обозначение

$$X^A = A^{-1}XA$$

и пусть $X_1, X_2, \ldots, X_r$ будут искомые инфинитезимальные операторы о. г. Г (которую мы считаем линейной однородной группой). Тогда для каждого A должны иметь место уравнения

$$X_i^A = \sum_{\nu=1}^{r} a_{i\nu}^A X_\nu \qquad (i = 1, 2, \ldots, r),$$

где a_{iv}^{A} — неизвестные постоянные. Соответствие $A \to (a_{iv}^{A})$ дает новое линейное однородное представление группы $\mathfrak{G}$. Мы назовем его представлением, «приводимым в узком смысле», если существуют такие линейные комбинации $Y_1, Y_2, \ldots, Y_n$ операторов X_i, которые:

1) образуют подгруппу группы Γ (т. е. (Y_i, Y_j) линейно выражаются через Y_i),

2) подвергаются посредством преобразований A только линейным подстановкам.

Очевидно, что н. г. п. Γ, соответствующая представлению, приводимому в узком смысле, не является о. г. группы $\mathfrak{G}$, так как она обладает правильной непрерывной подгруппой, содержащей делителем изоморфную с $\mathfrak{G}$ группу. Таким образом, наша задача сводится к отысканию неприводимых в узком смысле систем $X_1, X_2, \ldots, X_r$.

Решить эту общую задачу очень трудно. Я даже не могу сказать до сих пор, соответствует ли каждой конечной группе конечное или бесконечное число о. г. Но если мы поставим себе задачу определения для данной простой конечной группы $\mathfrak{G}$ только тех о. г., которые имеют представление в пространстве возможно меньшего числа s измерений, то эту задачу можно решить сравнительно легко. Для этого следует найти все неприводимые представления как группы $\mathfrak{G}$, так и ее групп представления. Затем, выбрав правильное представление $\mathfrak{g}$ возможно меньшего числа измерений f, следует определить, является ли $\mathfrak{g}$ комплексным или вещественным. В первом случае полная унимодулярная линейная однородная группа f-той степени и будет искомой о. г., если локально изоморфная с ней группа дробных линейных подстановок от $(f-1)$ переменных действительно содержит делитель, изоморфный с $\mathfrak{G}$. Последнее имеет место тогда, когда $\mathfrak{g}$ является представлением группы $\mathfrak{G}$, а не ее группы представления. Если же группа $\mathfrak{g}$ вещественна, то она приводится к вещественной ортогональной группе ([9], стр. 107, теорема 100) и, следовательно, будет делителем ортогональной группы f-той степени, которая является $(f-2)$-группой. Этот способ с точностью до конечного числа исключений является наиболее общим способом построения о. г., имеющих представления в пространстве возможно меньшего числа измерений. Действительно, за конечным числом исключений, каждая простая н. г. п. может быть представлена либо как полная унимодулярная линейная однородная группа, либо как комплексгруппа, либо, наконец, как полная ортогональная группа. Но второй случай не представляет для нас интереса, так как переход от полной унимодулярной линейной группы к комплексгруппе не дает снижения числа измерений наименьшего пространства представления. Изоморфная с $\mathfrak{G}$ подгруппа входит в эти представления либо как линейная однородная, либо как ортогональная группа. Она будет неприводимой, за исключением того случая, когда наименьшему значению f соответствует группа представления, так что ее одевающая группа не содержит изоморфных

с $\mathfrak{G}$ подгрупп. Значение f, соответствующее самой группе $\mathfrak{G}$, будет в этом случае больше, чем сумма двух (или большего числа) значений f, соответствующих группам представления. Таким образом, смотря по тому, является ли комплексным или вещественным представление, соответствующее наименьшему значению f, будет либо $s = f - 1$, либо $s = f - 2$.

В частности, если $\mathfrak{G}$ есть знакопеременная группа от n переменных и $n \geqslant 8$, то, как доказал А. Виман [13], как группа $\mathfrak{G}$, так и ее группа представления не могут быть представлены как линейные однородные группы менее чем $(n-1)$-й степени. С другой стороны представление группы $\mathfrak{G}$ как знакопеременной группы подстановок от n переменных распадается в тождественное представление и вещественное неприводимое представление $(n-1)$-й степени. Таким образом, здесь $s = n-3$.

Следует еще решить вопрос: не существует ли такой н. г. п. Γ_1, которая была бы представима в пространстве меньшего числа измерений, чем данная простая н. г. п. Γ, изоморфная с одной из факторгрупп группы Γ_1. Такой случай невозможен. Действительно, Е. Э. Леви [14] показал, что каждая н. г. п. Γ_1, имеющая простую факторгруппу Γ, содержит подгруппу, изоморфную с Γ. Поэтому, если группа Γ_1 представима в s-мерном пространстве, то то же справедливо, очевидно, и для ее подгрупп и, значит, для факторгруппы Γ.

§ 3. Решение проблемы резольвент Клейна

Формулированная во введении задача 1 разрешается следующей теоремой:

Теорема 8. *Если группа Галуа $\mathfrak{G}$ уравнения*

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = 0 \qquad (3.1)$$

простая и, рассматриваемая как абстрактная группа, является делителем некоторой н. г. п. Γ и если Γ есть s-группа, то уравнение (3.1) *имеет s-параметрическую резольвенту.*

Замечание. Нет сомнения, что эта теорема справедлива для всякой конечной группы $\mathfrak{G}$. Я считаю группу $\mathfrak{G}$ простой только потому, что в настоящее время возможность рационального выполнения всех необходимых операций представляется непосредственно очевидной только для простых групп.

Сначала мы докажем следующую теорему:

Теорема 9. *Уравнение* (3.1) *имеет s-параметрическую резольвенту тогда и только тогда, если таковую имеет его резольвента Галуа*

$$F(\xi) = \xi^m + A_1 \xi^{m-1} + \ldots + A_{m-1} \xi + A_m = 0. \qquad (3.2)$$

Доказательство. Пусть уравнение (3.1) имеет s-параметрическую резольвенту

$$f_1(y) = 0, \tag{3.3}$$

коэффициенты которой суть рациональные функции от $a_1, a_2, \ldots, a_n; \Phi$, где Φ есть некоторая функция корней $x_1, x_2, \ldots, x_n$ уравнения (3.1), принадлежащая к группе $\mathfrak{G}$. Пусть, кроме того, дано нормальное уравнение (3.2) с неограниченно переменными коэффициентами, группа которого $\mathfrak{G}$ — просто транзитивна. Обозначим через $\overline{\Phi}$ функцию от корней уравнения (3.2), принадлежащую к группе $\mathfrak{G}$. Для построения s-параметрической резольвенты уравнения (3.2) выберем функцию $x(\xi)$, принадлежащую к той же группе $\mathfrak{H}$, что и корень x_1 уравнения (3.1) внутри поля $K(x_1, x_2, \ldots, x_n)$. Коэффициенты уравнения n-й степени, которому удовлетворяет $x(\xi)$, будем рассматривать как частные значения коэффициентов a_i уравнения (3.1). Таким же образом выразим Φ через A_i, $\overline{\Phi}$. Тогда коэффициенты как резольвенты (3.3), так и формулы перехода от (3.1) к (3.3) выразятся через A_i, $\overline{\Phi}$. Теперь построим резольвенту Галуа для уравнения (3.2)

$$F_1(\eta) = 0. \tag{3.4}$$

Ее можно рассматривать как s-параметрическую резольвенту уравнения (3.2), так как любой корень ξ уравнения (3.2) рационально выражается через корни уравнения (3.1), которые, в свою очередь, рационально выражаются через корни уравнения (3.3) и величины $a_1, a_2, \ldots, a_n; \Phi$, т. е. через один из корней уравнения (3.4) и величины $A_1, A_2, \ldots, A_m; \overline{\Phi}$.

Обратно, если уравнение (3.2) имеет s-параметрическую резольвенту (3.4) и корень x_1 уравнения (3.1) принадлежит к группе $\mathfrak{H}$, то коэффициенты $A_1, A_2, \ldots, A_m; \overline{\Phi}$ уравнения (3.2) рационально выражаются через коэффициенты $a_1, a_2, \ldots, a_n; \Phi$ уравнения (3.1). В этом случае корни уравнения (3.3) принадлежат к группе $\mathfrak{H}$ внутри поля $K(\eta)$, где η — один из корней уравнения (3.4), и, следовательно, уравнение (3.3) может рассматриваться как s-параметрическая резольвента уравнения (3.1), что и т. д.

Переходим к доказательству теоремы 8. Пусть корни уравнения (3.1), которые мы рассматриваем как независимые переменные, будут

$$x_1, x_2, \ldots, x_n.$$

Кроме того, пусть дана н. г. п. $\overline{\Gamma}$, содержащая делителем группу $\overline{\mathfrak{G}}$, изоморфную с группой Галуа $\mathfrak{G}$ уравнения (3.1) (т. е. с той группой, к которой принадлежит присоединенная нами к полю коэффициентов функция $\Phi(x_1, x_2, \ldots, x_n)$). Группа $\overline{\Gamma}$ пусть является s-группой, именно, имеющей представление в пространстве $(z_1, z_2, \ldots, z_s)$.

Мы можем считать группу $\overline{\Gamma}$ простой. Действительно, если группа

$\bar{\Gamma}$ имеет правильный нормальный делитель $\bar{\Gamma}_1$, то либо $\bar{\Gamma}_1$, либо $\bar{\Gamma}/\bar{\Gamma}_1$ имеет делителем группу, изоморфную с группой $\mathfrak{G}$. При этом, в силу теоремы Е. Э. Леви [14], группы эти являются s-группами. Продолжая этот процесс, мы придем, наконец, к простой о. г. группы $\mathfrak{G}$, которая также будет s-группой.

Обозначим через Γ то представление нашей s-группы либо как полной унимодулярной линейной однородной группы, либо как полной ортогональной группы, m-ая степень которого содержит представление $\bar{\Gamma}$ (в первом случае $m=1$). В обоих случаях легко убедиться, что координаты $z_1, z_2, \ldots, z_s$ пространства представления группы $\bar{\Gamma}$ рационально выражаются через координаты соответствующего пространства группы Γ^m.

Будем рассматривать группу подстановок $\mathfrak{G}$ как линейную однородную группу от переменных $x_1, x_2, \ldots, x_n$ и подвергнем эти переменные такому линейному преобразованию, чтобы группа $\mathfrak{G}$ перешла во вполне приведенную форму. Затем рассмотрим те составные части этого представления, которые являются делителями представления Γ^m. Иными словами, ищем такие линейные функции $y_1, y_2, \ldots, y_u$ от переменных $x_1, x_2, \ldots, x_n$, которые будут подвергаться подстановкам, соответствующим выше упомянутым неприводимым составным частям группы $\mathfrak{G}$, если подвергать переменные $x_1, x_2, \ldots, x_n$ подстановкам группы $\mathfrak{G}$. Если уравнение (3.1) нормально, то представление $\mathfrak{G}$ регулярно и, значит, содержит в качестве составных частей все неприводимые линейные представления этой группы, притом каждое столько раз, какова его степень ([9], стр. 119, прим. 14). Если эти неприводимые представления входят как делители в Γ^m в кратностях, высших, чем в $\mathfrak{G}$, то добавим к системе $x_1, x_2, \ldots, x_n$ еще дальнейшие параллельные системы от n переменных и число этих систем обозначим снова через m

$$\begin{aligned} &y_1, \quad y_2, \ldots, y_u, \\ &y_1^{(1)}, \quad y_2^{(1)}, \ldots, y_u^{(1)}, \\ &\ldots\ldots\ldots\ldots \\ &y_1^{(m-1)}, y_2^{(m-1)}, \ldots, y_u^{(m-1)}. \end{aligned} \tag{3.5}$$

Переменные (3.5) мы можем рассматривать как координаты пространства представления группы Γ^m. Подвергая переменные $x_1, x_2, \ldots, x_n$ подстановкам группы Галуа уравнения (3.1) и подвергая все системы переменных (3.5) тем же самым подстановкам, мы получим содержащийся в этом представлении изоморфный с группой $\mathfrak{G}$ делитель. Так как $\Gamma^m \supset \bar{\Gamma}$, то мы можем найти такие рациональные функции

$$z_1, z_2, \ldots, z_s \tag{3.6}$$

от переменных (3.5), которые преобразованиями Γ^m, а значит, и подстановками $\mathfrak{G}^m$ будут переводиться в функции от $z_1, z_2, \ldots, z_s$.

Первая из систем (3.5) состоит из определенных однородных линейных функций от корней $x_1, x_2, \ldots, x_n$ уравнения (3.1). Другие из систем (3.5) мы будем считать такими же функциями от новых переменных $x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}$, так что получим следующую новую систему переменных

$$\begin{aligned} &x_1, x_2, \ldots, x_n, \\ &x_1^{(1)}, x_2^{(1)}, \ldots, x_n^{(1)}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &x_1^{(m-1)}, x_2^{(m-1)}, \ldots, x_n^{(m-1)}. \end{aligned} \tag{3.7}$$

Преобразуем переменные (3.7) следующим образом:

$$\begin{aligned} x_1^{(i)} &= \alpha_0^{(i)} + \alpha_1^{(i)} x_1 + \ldots + \alpha_{n-1}^{(i)} x_1^{n-1}, \\ x_2^{(i)} &= \alpha_0^{(i)} + \alpha_1^{(i)} x_2 + \ldots + \alpha_{n-1}^{(i)} x_2^{n-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n^{(i)} &= \alpha_0^{(i)} + \alpha_1^{(i)} x_n + \ldots + \alpha_{n-1}^{(i)} x_n^{n-1} \end{aligned} \qquad (i=1, 2, \ldots, m-1) \tag{3.8}$$

и примем за новые переменные величины

$$x_1, x_2, \ldots, x_n; \ \alpha_0^{(i)}, \alpha_1^{(i)}, \ldots, \alpha_{n-1}^{(i)} \qquad (i = 1, 2, \ldots, m-1). \tag{3.9}$$

Очевидно, что переход от (3.7) к (3.9) осуществляется обратимым преобразованием. Если теперь производить над системой (3.9) подстановки группы $\mathfrak{G}^m$, то переменные $\alpha_0^{(i)}, \alpha_1^{(i)}, \ldots, \alpha_{n-1}^{(i)}$ $(i = 1, 2, \ldots, m-1)$ не изменяются.

Подставляя в выражение (3.6) вместо $y_j^{(i)}$ их значения, вычисленные с помощью формул (3.8), мы получим систему s функций

$$\bar{Z}_1, \bar{Z}_2, \ldots, \bar{Z}_s \tag{3.10}$$

от переменных (3.9), причем функции эти будут переходить в свои собственные функции, если производить над переменными $x_1, x_2, \ldots, x_n$ подстановки группы $\mathfrak{G}$, оставляя инвариантными величины $\alpha_j^{(i)}$. Поэтому, если в одной из функций (3.10), например $\bar{Z}$, придать величинам $\alpha_j^{(i)}$ какие-либо рациональные числовые значения и затем подвергнуть переменные $x_1, x_2, \ldots, x_n$ подстановкам группы $\mathfrak{G}$, то получится система функций

$$\bar{Z}, \bar{Z}^{S_2}, \bar{Z}^{S_3}, \ldots, \bar{Z}^{S_n}, \tag{3.11}$$

функционально зависимых от $\bar{Z}_1, \bar{Z}_2, \ldots, \bar{Z}_s$, т. е. содержащих только s переменных параметров. Элементарные симметрические функции от величин (3.11) рационально выражаются через $a_1, a_2, \ldots, a_n$; Ф и содержат также только s переменных параметров (иначе говоря, содержат только s функционально независимых величин). Чтобы убедиться в том, что таким образом мы приходим к s-параметрической резольвенте уравнения (3.1), достаточно показать, что при подходящем

выборе функций $\bar{Z}$ и значений $\alpha_j^{(i)}$ величины (3.11) отличны друг от друга.

Допустим, что это не так. Тогда в группе $\mathfrak{G}$ существует такая подстановка S, что все разности $\bar{Z}_i^S - \bar{Z}_i$ исчезают при всех значениях $\alpha_j^{(i)}$. Более того: каждая из функций Z_i^U, где U — произвольное преобразование н. г. п. $\bar{\Gamma}^m$, удовлетворяет уравнению

$$Z_i^{US} - Z_i^U = 0.$$

Применяя к этому уравнению преобразование U^{-1}, получим

$$Z_i^{USU^{-1}} - Z_i = 0.$$

Но S не может быть перестановочным со всеми преобразованиями группы $\bar{\Gamma}^m$. Следовательно, совокупность преобразований USU^{-1} представляет такое непрерывное семейство преобразований, которое содержит S и еще отличные от S преобразования. Композит этого семейства (т. е. совокупность преобразований, полученных композицией преобразований вида USU^{-1}) представляет, следовательно, непрерывную группу, оставляющую инвариантной все функции $Z_1, Z_2, \ldots, Z_s$. Это противоречит предположению о том, что представление группы $\bar{\Gamma}^m$ в пространстве (3.6) правильное. Если же одна из разностей $Z_i^S - Z_i$ не обращается в нуль тождественно, то возможно выбрать такие рациональные значения величин $\alpha_j^{(i)}$, чтобы все величины (3.11) были отличны друг от друга и представляли, следовательно, все корни s-параметрической резольвенты уравнения (3.1).

Рассуждения эти должны быть несколько изменены в том случае, когда не сама группа $\mathfrak{G}$, но одна из ее групп представления, например $\mathfrak{R}$, является делителем той линейной однородной н. г. п. $\bar{\Gamma}$, степень которой $\bar{\Gamma}^m$ содержит s-мерное представление. Тогда мы решаем проблему резольвент для группы $\mathfrak{G}$, построив уравнение

$$F(\xi) = 0, \tag{3.12}$$

группа которого есть $\mathfrak{R}$ и корни рационально выражаются через корни уравнения (3.1). Для этого достаточно рассмотреть уравнение

$$f(\zeta^d) = 0,$$

где d — порядок группы $\mathfrak{H}\left(\mathfrak{G} \approx \frac{\mathfrak{R}}{\mathfrak{H}}\right)$, и построить такое подполе поля $K(\zeta)$, группа которого изоморфна с $\mathfrak{G}$. Дальнейшие рассуждения можно повторить без изменения, так как о. г. группы $\mathfrak{G}$ проста, хотя $\mathfrak{G}$ и не является простой. Корни построенной таким образом резольвенты принадлежат в поле $K(\xi)$ не к единичной группе, а к группе $\mathfrak{H}$. Но к той же группе принадлежат и корни уравнения (3.1). Следовательно, они рационально выражаются через корни резольвенты и величины $a_1, a_2, \ldots, a_n$; Ф, что и т. д.

§ 4. Обращение основной теоремы

Теорема 8, которая, вследствие своего значения для всей теории, названа основной теоремой, допускает следующее обращение:

Теорема 10. *Если уравнение* (3.1) *имеет s параметрическую резольвенту, то его группа* $\mathfrak{G}$ *имеет в качестве о. г. некоторую s-группу.*

Доказательство. Пусть корни s-параметрической резольвенты уравнения (3.1), которое мы считаем нормальным, будут

$$Z_1, Z_2, \ldots, Z_n. \tag{4.1}$$

Величины (4.1) являются такими функциями от корней $x_1, x_2, \ldots, x_n$ уравнения (3.1), каждая из которых принадлежит к единичной группе. Если производить над $x_1, x_2, \ldots, x_n$ подстановки группы $\mathfrak{G}$, то величины (4.1) будут подвергаться известным подстановкам, которые образуют группу $\overline{\mathfrak{G}}$, изоморфную с $\mathfrak{G}$. Группы $\mathfrak{G}$ и $\overline{\mathfrak{G}}$ отличаются друг от друга только различным обозначением переменных.

Рассмотрим сперва величины (4.1) как независимые переменные и оденем группу $\overline{\mathfrak{G}}$ с помощью произвольной н. г. п. Г. Можно воспользоваться для этого, скажем, линейной однородной группой от переменных (4.1). Еще лучше, если посредством линейного преобразования величин Z_i представить группу $\overline{\mathfrak{G}}$ во вполне приведенной форме и затем одеть одну из ее неприводимых частей посредством линейной н. г. п.

Затем мы используем тот факт, что величины (4.1) представляют корни s-параметрической резольвенты, т. е., что между ними существует ровно s функционально независимых. Будем считать $x_1, x_2, \ldots, x_n$ координатами точки специального пространства $\mathfrak{R}$, в котором мы будем считать две точки $(x_1, x_2, \ldots, x_n)$ и $(x_1', x_2', \ldots, x_n')$ совпадающими, если

$$Z_i(x_1, x_2, \ldots, x_n) = Z(x_1', x_2', \ldots, x_n) \qquad (i = 1, 2, \ldots, n). \tag{4.2}$$

Очевидно, что пространство $\mathfrak{R}$ — s-мерно.

Пусть теперь преобразования н. г. п. Г будут

$$Z_i' = f_i(Z_1, Z_2, \ldots, Z_n; a_1, a_2, \ldots, a_r) \qquad (i = 1, 2, \quad, n). \tag{4.3}$$

Если мы подставим сюда вместо Z_i и Z_i' функции $Z_i(x_1, x_2, \ldots, x_n)$, $Z_i(x_1', x_2', \ldots, x_n')$, то полученные уравнения определяют преобразование «индуцированной в пространстве $\mathfrak{R}$» н. г. п. Г, которая будет содержать делителем группу $\mathfrak{G}$. В самом деле, функции $Z_i(x_1, x_2, \ldots, x_n)$ принадлежат к единичной группе и потому те подстановки над переменными $x_1, x_2, \ldots, x_n$, которые входят в группу $\mathfrak{G}$, производят действительно подстановки над функциями Z_i и, значит, согласно определению $\mathfrak{R}$, соответствуют нетождественным преобразованиям пространства $\mathfrak{R}$. Теорема доказана.

Замечание. Для доказательства теоремы 10 является существенным то, что каждая система значений параметров н. г. п. Г однозначно определяет ту точку, в которую переходит заданная точка пространства $\mathfrak{R}$. В силу этого группа Г подпадает под шрейеровское ([10], прим. 16) топологическое определение, так что к ней применима вся теория Шрейера. Если же это условие не выполняется, то можно, например, столкнуться с таким явлением, что нециклическая группа монодромии некоторой алгебраической функции имеет в качестве о. г. одночленную н. г. п. Например: одночленная н. г. п. пространства (x, y, z), определенная уравнениями

$$x+y+z=c_1t,$$
$$x^2+y^2+z^2=c_2t$$
$$x^3+y^3+z^3=c_3t,$$

содержит делителем симметрическую группу подстановок третьей степени, которая даже не является абелевой.

Теорема 10 совместно с выше цитированными исследованиями А. Вимана ([13], прим. 21) делает весьма правдоподобным предположение о том, что при $n \geqslant 8$

$$n-s \leqslant 3.$$

Для проблемы же Гильберта, как недавно показал А. Виман [15], имеет место

$$n-s \geqslant 5.$$

ЛИТЕРАТУРА

1. N. Tschebotarëw. Über ein algebraisches Problem von Herrn Hilbert. I. Math. Ann. **104**, 1931, стр. 459—471; II. Math. Ann. **105**, 1931, стр. 240—255. Собр. соч., т. I, стр. 255—266, 267—281.
2. F. Klein. Gesammelte Math. Abhandlungen, Bd. 2, Berlin, 1922, стр. 255—504.
3. D. Hilbert. Mathematische Probleme. Gött. Nachr., 1900, стр. 253—297; D. Hilbert. Über die Gleichung neunten Grades. Math. Ann. **97**, 1926, стр. 243—250.
4. S. Lie. Theorie der Transformationsgruppen. Bd, I, Lpz., 1888 (или 2-te Aufl., Lpz., 1930, стр. 337).
5. E. Cartan. Sur la structure des groupes infinis. C. R. **135**, 1902, стр. 851—854.
6. W. Killing. Bestimmung der grössten Untergruppen von endlichen Transformationsgruppen. Math. Ann. **30**, 1890, стр. 343.
7. E. Cartan. Sur la structure des groupes de transformations finis et continus. Paris, 1894 (также Paris, 1933), стр. 148.
8. C. Jordan. Mémoire sur les équations différentielles linéaires à intègrale algébrique. Journ. f. Math. **84**, 1888, стр. 89—215.
9. A. Speiser. Die Theorie der Gruppen von endlicher Ordnung. Berlin, 1923 (также 2 Aufl. Berlin, 1927), стр. 160.
10. O. Schreier. Die Verwandschaft stetiger Gruppen im Grossen. Hamb. Abh. **5**, 1926, стр. 233—244.

11. J. Schur. Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen. Journ. f. Math. **127**, 1904, стр. 47.
12. A. Wiman. Übe eine einfache Gruppe von 360 ebenen Collineationen. Math. Ann. **47**, 1896, стр. 531–556.
13. A. Wiman. Über die Darstellung der symmetrischen und alternierenden Vertäuschungsgruppen... Math. Ann. **52**, 1989, стр. 243—270.
14. E. E. Levi. Sulla struttura dei gruppi finiti e continui. Atti Acc. di Torino **40**, 1905, стр. 423—437.
15. A. Wiman. Über die Anwendung der Tschirnhausentransformation auf die Reduktion algebraischer Gleichungen. Nova Acta R. Soc. Sc. Uppsaliensis, Vol. extra ord. ed., 1927.

ПРОБЛЕМА РЕЗОЛЬВЕНТ И КРИТИЧЕСКИЕ МНОГООБРАЗИЯ

(Изв. АН СССР, серия матем. 7 (1943), стр. 123—146)

Работа посвящена проблеме резольвент, т. е. проблеме нахождения по заданному уравнению, коэффициенты которого зависят от нескольких независимых параметров, резольвенты, число параметров в коэффициентах которой было бы возможно меньшим. Автор приводит проблему к исследованию критических многообразий в пространстве параметров уравнений.

Настоящая статья посвящена проблеме резольвент, поставленной Ф. Клейном [3] и значительно подвинутой Д. Гильбертом [1,2]. Она состоит в нахождении такого рационального преобразования алгебраического уравнения, содержащего переменные параметры, чтобы преобразованное уравнение содержало возможно меньше независимых параметров. В то время как Клейн считал коэффициенты преобразования рациональными или содержащими наперед заданные иррациональности, Гильберт предполагал их зависящими от корней вспомогательных уравнений, в свою очередь допускающих резольвенты с небольшим числом параметров.

Методы, при помощи которых делались попытки решить проблемы Клейна и Гильберта, тоже существенно различны. Проблема Клейна была приведена к задаче одевания группы Галуа заданного уравнения группой Ли, представляемой в пространстве возможно меньшего числа измерений. Я [5] показал, что уравнение n-ой степени с неограниченно переменными коэффициентами и знакопеременной группой Галуа не может быть преобразовано к резольвенте, зависящей менее чем от $n-3$ параметров. Тем самым было обнаружено, что решение проблемы Клейна существенно отличается от решения проблемы Гильберта.

Для проблемы Гильберта сам Гильберт предложил частный прием, дающий для $n=5, 6, 7, 8, 9$ значений числа параметров в резольвентах, приводимые в следующей таблице:

n	5	6	7	8	9
s	1	2	3	4	4

Виман [7] показал, что при $n \geqslant 9$ существуют резольвенты с числом параметров $s \leqslant n-5$. При этом остается невыясненным, являются ли эти значения s наименьшими из возможных.

В настоящей статье предлагается новый принцип изучения резольвент. Этот принцип основан на рассмотрении высших критических многообразий в пространствах, образованных параметрами, от которых зависят коэффициенты заданного уравнения. Я называю высшим критическим многообразием совокупность точек в пространстве параметров, в которых несколько корней уравнения совпадают. Для каждого уравнения можно определить все типы высших критических многообразий. Если для данного уравнения найдена цепь из s критических многообразий, из которых каждое содержится в предыдущем как часть, то при бирациональном преобразовании уравнения эта цепь переходит в такую же цепь, у которой каждое многообразие имеет меньшее измерение, чем предыдущее. Это показывает, что уравнение не может иметь резольвенты менее чем с s параметрами. Это дает для значения s нижнюю границу (в то время как Гильберт и Виман дают верхнюю границу), если мы ограничимся рациональными резольвентами. Изучение иррациональных резольвент, требующее детального исследования критических многообразий для относительных полей, я откладываю до следующей статьи.

Применение этого метода к уравнениям с неограниченно переменными коэффициентами и с знакопеременной группой Галуа дает для нижней границы числа s значения

$$s = \left[\frac{n-1}{2}\right],$$

которые весьма близки к значениям, найденным Гильбертом:

n	5	6	7	8	9
s	2	2	3	3	4

Однако сопоставление обоих значений s для $n = 5$ показывает, что применение иррациональных резольвент имеет существенное значение.

Вопрос о том, будет ли найденная нижняя граница для s также и верхней границей, связан с вопросом о фактическом построении резольвент при помощи критических многообразий. В настоящее время я располагаю некоторыми соображениями, делающими весьма вероятным положительный ответ на этот вопрос. Однако они недостаточны для того, чтобы делать какое-либо категорическое заключение.

§ 1. Высшие критические многообразия

Дано уравнение

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n = 0, \tag{1}$$

коэффициенты которого пусть будут полиномами от некоторого числа независимых переменных

$$u_1, u_2, \ldots, u_m$$

с коэффициентами из поля всех комплексных чисел. Будем представлять себе эти переменные комплексными координатами точек пространства U, которое мы будем считать или m-мерным в комплексном смысле, или $2m$-мерным в вещественном смысле. Если для какой-нибудь точки P пространства U дискриминант D уравнения 1) не обращается в нуль, то корни

$$x_1, x_2, \ldots, x_n$$

уравнения (1) определяются в окрестности точки P как аналитические функции от m переменных u_i, которые могут быть продолжены на все пространство U. Однако такое продолжение не всегда однозначно, если мы будем производить его по двум различным путям. Более того, если уравнение (1) неприводимо в области рациональных функций от $u_1, u_2, \ldots, u_m$, то в пространстве U можно найти замкнутый путь такого рода, что при продолжении вдоль него любой из корней $x_1, x_2, \ldots x_n$ переходит в любой другой из этих корней. В самом деле, если бы при продолжении по всем замкнутым путям корень x_1 переходил только в

$$x_1, x_2, \ldots, x_k \qquad (k < n),$$

то все элементарные симметрические функции от этих корней были бы однозначными во всем пространстве U. Отсюда следовало бы, что они рациональны относительно каждой из переменных $u_1, u_2, \ldots u_m$, взятых в отдельности и, следовательно, от этих переменных в совокупности. Таким образом, уравнение (1) имело бы множитель степени $k < n$ с коэффициентами, рационально зависящими от $u_1, u_2, \ldots, u_m$.

Совокупность подстановок, получаемых в результате продолжения корней по всевозможным замкнутым путям пространства U, носит название *группы монодромии* G уравнения (1). Не трудно убедиться, что она совпадает с группой Галуа этого уравнения, если в качестве области рациональности взять совокупность рациональных функций от $u_1, u_2, \ldots u_m$ с любыми комплексными коэффициентами.

Всякий замкнутый путь в пространстве U может быть стянут в точку. Отсюда следует, что в U существуют бесконечно малые замкнутые пути, при обходе которых корни претерпевают нетождественные подстановки, и притом совокупность последних имеет композитом всю группу G. Ясно, что перемещаемые на бесконечно малом замкнутом пути корни должны быть бесконечно близки, так что такие пути лежат в окрестностях точек многообразия

$$D(u_1, u_2, \ldots, u_m) = 0 \tag{2}$$

где D — дискриминант уравнения (1).

Чтобы определить многообразия точек, в окрестностях которых существуют замкнутые пути, при обходе по которым корни претерпевают

подстановки заданного цикленного типа (точнее, заданного класса элементов группы G), рассмотрим произведение

$$\prod_{S \mid G} (t_1 x_{\alpha_1} + t_2 x_{\alpha_2} + \ldots + t_n x_{\alpha_n}) = \Phi(t_1, t_2, \ldots, t_n), \tag{3}$$

где $t_1, t_2, \ldots, t_n$ — независимые переменные, подстановка

$$S = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

а произведение распространено на все подстановки S группы G. Коэффициенты формы (3), очевидно, суть рациональные функции от переменных $u_1, u_2, \ldots u_m$.

Запишем подстановку S в циклах

$$S = (1, 2, \ldots, \mu_1)\ (\mu_1 + 1, \ldots, \mu_2) \ldots, (\mu_{k-1} + 1, \ldots, n).$$

Будем говорить, что точка P пространства U лежит в многообразии, соответствующем подстановке S, если в P имеют место совпадения:

$$\left.\begin{aligned} x_1 = x_2 = \ldots = x_{\mu_1}, \\ x_{\mu_1+1} = \ldots = x_{\mu_2}, \\ \ldots\ldots\ldots \\ x_{\mu_{k-1}+1} = \ldots = x_n. \end{aligned}\right\} \tag{4}$$

Если многообразие, соответствующее подстановке T (будем обозначать его через U_T), составляет часть многообразия U_S

$$U_T \subset U_S,$$

то будем говорить, что подстановка T *выше* подстановки S:

$$T > S. \tag{5}$$

Для того чтобы имело место (5), необходимо и достаточно, чтобы каждая совокупность корней, составляющих цикл в подстановке S, целиком входила в один и тот же цикл подстановки T.

В дальнейшем под $U_{(S)}$ мы будем разуметь многообразие точек из U, соответствующих одной из подстановок класса, в котором содержится S. Будем говорить, что класс (T) выше класса (S), если в (T) содержится подстановка, которая выше, чем какая-нибудь подстановка из (S).

Будем обозначать через Φ_S форму (3), в которой мы подчиним переменные $t_1, t_2, \ldots, t_n$ соотношениям

$$\left.\begin{aligned} t_1 + t_2 + \ldots + t_{\mu_1} = 0, \\ t_{\mu_1+1} + \ldots + t_{\mu_2} = 0, \\ \ldots\ldots\ldots \\ t_{\mu_{k-1}+1} + \ldots + t_n = 0. \end{aligned}\right\} \tag{6}$$

Имеет место

Теорема 1. *Чтобы точка P лежала на многообразии $U_{(S)}$, необходимо и достаточно, чтобы для этой точки все коэффициенты формы Φ_S обращались в нуль.*

Доказательство. 1°. Условие необходимо. В самом деле, если для точки P имеют место совпадения (4), то линейная форма

$$t_1x_1 + t_2x_2 + \ldots + t_nx_n$$

при условиях (6) обращается в нуль, так как

$$\left.\begin{aligned}
&t_1x_1 + t_2x_2 + \cdots + t_nx_n = \\
&= t_1x_1 + \cdots + t_{\mu_1-1}x_{\mu_1-1} - (t_1 + \cdots + t_{\mu_1-1})\,x_{\mu_1} + \\
&+ t_{\mu_1+1}x_{\mu_1+1} + \cdots + t_{\mu_2-1}x_{\mu_2-1} - (t_{\mu_1+1} + \cdots + t_{\mu_2-1})\,x_{\mu_2} + \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&+ t_{\mu_{n-1}+1}x_{\mu_{k-1}+1} + \cdots + t_{n-1}x_{n-1} - (t_{\mu_{k-1}+1} + \cdots + t_{n-1})\,x_n = \\
&= t_1(x_1 - x_{\mu_1}) + \cdots + t_{\mu_1-1}(x_{\mu_1-1} - x_{\mu_1}) + \\
&+ t_{\mu_1+1}(x_{\mu_1+1} - x_{\mu_2}) + \cdots + t_{\mu_2-1}(x_{\mu_2-1} - x_{\mu_2}) + \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
&+ t_{\mu_{k-1}+1}(x_{\mu_{k-1}+1} - x_n) + \cdots + t_{n-1}(x_{n-1} - x_n).
\end{aligned}\right\} \quad (7)$$

Если же для точки P имеют место совпадения, соответствующие какой-нибудь другой подстановке класса (S), то обратится в нуль какой-нибудь другой множитель выражения (3). Таким образом

$$\Phi_S = 0.$$

2° Условие достаточно. В самом деле, если в точке P имеет место

$$\Phi_S = 0,$$

то при условиях (6) равен нулю по крайней мере один из множителей выражения (3). Представив его в форме, подобной (7), мы убедимся, что имеют место совпадения, подобные (4). Именно, если обращается в нуль множитель

$$t_1x_{\alpha_1} + t_2x_{\alpha_2} + \ldots + t_nx_{\alpha_n} = 0,$$

где

$$T = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix} \subset G,$$

то таблица совпадений будет иметь вид

$$\begin{aligned}
x_{\alpha_1} &= x_{\alpha_2} = \ldots = x_{\alpha_{\mu_1}}, \\
x_{\alpha_{\mu_1+1}} &= \ldots = x_{\alpha_{\mu_2}}, \\
&\ldots\ldots\ldots \\
x_{\alpha_{\mu_{k-1}+1}} &= \ldots = x_{\alpha_n},
\end{aligned}$$

т. е. будет соответствовать подстановке

$$\begin{pmatrix}\alpha_1\alpha_2\ldots\alpha_n\\ 1\ 2\qquad n\end{pmatrix}(1,2,\ldots,\mu_1)(\mu_1+1,\ldots,\mu_2)\ldots$$
$$\ldots(\mu_{k-1}+1,\ldots,n)\begin{pmatrix}1\ 2\ldots n\\ \alpha_1\alpha_2\ldots\alpha_n\end{pmatrix}=T^{-1}ST,$$

откуда следует, что точка P принадлежит многообразию $U_{(S)}$, что и требовалось доказать.

В кольце полиномов от $u_1, u_2, \ldots, u_m$, рационально выражающихся через коэффициенты уравнения (1), каждому многообразию $U_{(S)}$ соответствует полиномиальный идеал, представляющий совокупность полиномов, обращающихся в нуль на многообразии $U_{(S)}$. Обозначим такой идеал через $A_{(S)}$. Чтобы узнать, принадлежит ли заданный полином

$$h(u_1, u_2, \ldots, u_m),$$

выражающийся через коэффициенты уравнения (1), идеалу $A_{(S)}$, выразим h через корни $x_1, x_2, \ldots, x_n$ уравнения (1), приравняем друг другу некоторые из них сообразно с таблицей совпадений (4) и посмотрим, обратится ли после этого полином в нуль.

Если переменные $u_1, u_2, \ldots, u_m$ входят в коэффициенты уравнения (1) линейно, то $A_{(S)}$ будет простым идеалом. В самом деле, без нарушения общности можно предположить, что тогда отдельные переменные $u_1, u_2, \ldots, u_m$ рационально (и даже линейно) выражаются через коэффициенты $a_1, a_2, \ldots, a_n$. Тогда, если произведение полиномов gh принадлежит $A_{(S)}$, выразим в g и h все переменные $u_1, u_2, \ldots, u_m$ через корни $x_1, x_2, \ldots, x_n$ и приравняем некоторые из них друг другу сообразно с таблицей совпадений (4). Если при этом произведение gh обратится в нуль, то должен обратится в нуль по крайней мере один из его множителей, а это и доказывает простоту идеала $A_{(S)}$.

Заметим, что если мы вместо подстановки S возьмем любую другую подстановку $T^{-1}ST$ того же класса ($T \subset G$), то получим тот же идеал $A_{(S)}$. Это следует из того, что таблица совпадений для подстановки $T^{-1}ST$ получается из таблицы совпадений (4), если к ней применить подстановку T. С другой стороны, всякая рациональная функция от $x_1, x_2, \ldots, x_n$, рационально выражающаяся через $u_1, u_2, \ldots, u_m$, не изменяется, если к ней применить подстановку T.

§ 2. Группы инерции

Совокупность подстановок между корнями уравнения (1), образуемых при всевозможных бесконечно малых обходах, взятых в окрестности какой-нибудь точки P пространства U, мы будем, по аналогии с теорией алгебраических (вернее, p-адических) чисел, называть *группой инерции* точки P. Зададимся целью определить группу инерции для точки P, лежащей на многообразии $U_{(S)}$. С одной стороны, ясно, что корни,

переходящие друг в друга при обходах в окрестности точки P, должны в точке P совпадать. Отсюда следует, что всякая подстановка группы инерции не выше одной из подстановок класса (S). Обратное справедливо только при некоторых оговорках. Для облегчения исследования сначала предположим, что переменные $u_1, u_2, \ldots, u_m$ входят в коэффициенты $a_1, a_2, \ldots, a_n$ линейно. Это, в частности, будет иметь место, если мы в качестве U станем рассматривать пространство коэффициентов $a_1, a_2, \ldots, a_n$.

В нашем случае уравнение (1) можно переписать в форме

$$f_0(x) + f_1(x)(u_1 - p_1) + f_2(x)(u_2 - p_2) + \ldots + f_m(x)(u_m - p_m) = 0, \quad (8)$$

где $p_1, p_2, \ldots, p_m$ — координаты точки P. Полиномы $f_0(x), f_1(x), \ldots, f_m(x)$ не имеют общих множителей, так как корни всякого их общего множителя были бы корнями уравнения (1) и вместе с тем не зависели бы от $u_1, u_2, \ldots, u_m$, что противоречит неприводимости уравнения (1).

Предположим, что точка P лежит на $U_{(S)}$, но не лежит ни на одном из более высоких критических многообразий. Тогда полином $f_0(x)$ будет иметь постоянные корни, совпадения которых точно соответствуют таблице (4). Обозначая их через $b_1, b_2, \ldots, b_n$, мы, таким образом, будем иметь

$$\begin{aligned} b_1 &= b_2 = \ldots = b_{\mu_1}, \\ b_{\mu_1+1} &= \ldots = b_{\mu_2}, \\ &\ldots\ldots\ldots\ldots \\ b_{\mu_{k-1}+1} &= \ldots = b_n, \end{aligned} \quad (9)$$

причем ни одно из значений

$$b_1, \ b_{\mu_1+1}, \ldots, \ b_{\mu_{k-1}+1}$$

не совпадает ни с одним другим. В силу взаимной простоты полиномов $f_0(x), f_1(x), \ldots, f_m(k)$ можно подобрать константы $c_1, c_2, \ldots, c_m$ так, чтобы полином

$$g(x) = c_1 f_1(x) + c_2 f_2(x) + \ldots + c_m f_m(x)$$

был взаимно прост с $f_0(x)$, т. е. не обращался в нуль ни при одном из значений (9). Произведем над $u_1, u_2, \ldots, u_m$ линейное преобразование

$$\begin{aligned} u_1 - p_1 &= c_1 v_1, \\ u_2 - p_2 &= c_2 v_1 + v_2, \\ &\ldots\ldots\ldots\ldots \\ u_m - p_m &= c_m v_1 + v_m. \end{aligned}$$

Тогда уравнение (8) перепишется так:

$$f_0(x) + g(x) v_1 + f_2(x) v_2 + \ldots + f_m(x) v_m = 0. \quad (10)$$

Переменные $v_1, v_2, \ldots, v_m$ в точке P обращаются в нуль. Полагая

$$v_2 = v_3 = \ldots = v_m = 0, \tag{11}$$

получим

$$v_1 = -\frac{f_0(x)}{g(x)} = -\frac{(x-b_1)^{\mu_1}(x-b_{\mu_1+1})^{\mu_2-\mu_1}\cdots(x-b_{\mu_{k-1}+1})^{n-\mu_{k-1}}}{g(x)} \tag{12}$$

где знаменатель $g(x)$ взаимно прост с числителем, т. е. не обращается в нуль при $v_1 = 0$. Если в этом уравнении мы положим

$$v_1 = \rho e^{i\theta}, \tag{13}$$

где $\rho > 0$ — весьма малое число, а θ заставим пробегать значения от 0 до 2π, то из теоремы о непрерывности корней алгебраических уравнений будет следовать, что μ_1 из корней уравнения (12) будут весьма близки к b_1, μ_2—μ_1 — к b_2 и т. д. При этом, при полном обходе значений θ от 0 до 2π корни каждой из этих категорий будут циклически переходить друг в друга, и, таким образом, все корни претерпят подстановку того же цикленного типа, что и подстановка S.

Вместе с тем равенства (12) и (13) определяют в пространстве U весьма малую окружность вокруг точки P. Таким образом, мы доказали следующую теорему:

Теорема 2. *Группа инерции точки P содержит подстановку, циклы которой соответствуют строкам в таблице совпадения корней, имеющего место для точки P.*

Исследуем, каковы типы низших подстановок, входящих в группу инерции точки P. Если в точке P пересекаются несколько более низких, чем $U_{(S)}$, критических многообразий, например многообразие $U_{(S_1)}$, то в любой окрестности точки P содержится бесчисленное множество точек, для которых $U_{(S_1)}$ есть наивысшее из критических многообразий, на которых они лежат. Из этого, в силу теоремы 2, следует, что в любой окрестности точки P существуют пути, при обходе по которым корни $x_1, x_2, \ldots, x_n$ претерпевают подстановку, подобную подстановке S_1. Отсюда мы имеем:

Лемма 1. *Группа инерции точки P содержит подстановки всех цикленных типов, соответствующих таблицам совпадений тех критических многообразий, на которых лежит P.*

Справедливо также обратное утверждение. Для доказательства нам будут необходимы следующие леммы:

Лемма 2. *В каждой цепи содержащихся одно в другом критических многообразий*

$$U_{(S_1)} \supset U_{(S_2)} \supset \ldots \supset U_{(S_r)}$$

измерение каждого последующего по крайней мере на единицу меньше, чем измерение предыдущего.

Доказательство. Это следует из того, что, как мы убедились из § 1, идеал, соответствующий каждому критическому многообразию, есть простой идеал. В самом деле, существует теорема (см. Ван-дер-Варден [6], стр. 63), согласно которой два простых идеала, из которых один содержится в другом, только тогда имеют одинаковое измерение, если они совпадают.

Следствие. Самое низшее, т. е. не содержащееся как часть в другом, критическое многообразие имеет комплексное измерение $\leqslant m-1$.

Будем рассматривать теперь пространство U как $2m$-мерное вещественное пространство. Из только что доказанного вытекает, что низшие критические многообразия имеют измерение $\leqslant 2m-2$. Пусть какая-нибудь точка пространства U, принадлежащая к одному из высших (может быть, не к самому высшему) критических многообразий $U_{(S)}$ и вместе с тем не принадлежащая ни к одному из более высоких критических многообразий,[1] имеет в своей окрестности замкнутую кривую C, при обходе по которой корни $x_1, x_2, \ldots, x_n$ претерпевают подстановку S. Проведем через C двумерное многообразие A (натянем пленку), которое пусть не пересекается ни с P, ни с одним из более высоких, чем самое низшее, критических многообразий. Этого всегда можно достигнуть путем малых деформаций многообразия A, так как, в силу леммы 2, всякое высшее критическое многообразие имеет вещественное измерение $\leqslant 2m-4$. С другой стороны, если S не есть тождественная подстановка, то A обязательно пересекает низшее критическое многообразие. В самом деле, в противном случае, разбив A на сколь угодно малые площадки, мы могли бы рассматривать контур каждой из этих площадок как замкнутую кривую, находящуюся в окрестности некритической точки. Следовательно, при обходе по каждому из этих контуров корни претерпевают тождественную подстановку. Но так как обход по C равносилен совокупности обходов по этим контурам, произведенных в определенном порядке, то обход по C тоже производил бы среди корней тождественную подстановку, что противоречит предположению.

Мы можем предположить многообразие A алгебраическим. Тогда при помощи малой деформации число его пересечений с критическими многообразиями можно сделать конечным. Пусть точки этих пересечений будут $P_1, P_2, \ldots, P_k$ и пусть обходам вокруг них (по кривым, лежащим на A) соответствуют низшие подстановки $S_1, S_2, \ldots, S_k$. Очевидно, их можно занумеровать в таком порядке, чтобы имело место

$$S_1 \cdot S_2 \cdots S_k = S.$$

[1] Последнее условие не играет роли при доказательстве и поэтому в случае нужды может быть отброшено.

Отсюда следует

Лемма 3. *Все подстановки группы инерции точки P суть произведения низших подстановок, соответствующих точкам низшего критического многообразия, находящимся в окрестности точки P.*

Из хода доказательства этой леммы как побочное следствие вытекает

Лемма 4. *Вещественное измерение низшего критического многообразия в точности равно $2m-2$.*

Действительно, если бы это измерение было меньше $2m-2$, то многообразие A после малой деформации не имело бы пересечений с критическими многообразиями.

Вообще, теперь мы можем уточнить лемму 2. Многообразие $U_{(S_1)}$ является пересечением или двух различных низших многообразий, или двух полей одного и того же многообразия $U_{(S_1)}$. В самом деле, в силу леммы 3, высшая соответствующая ему подстановка есть произведение низших подстановок, а соответствующие двум низшим подстановкам многообразия в пересечении образуют высшее критическое многообразие, измерение которого, таким образом, равно $2m-4$. Продолжая рассуждение, получим следующую лемму:

Лемма 5. *В цепи содержащихся одно в другом последовательных критических многообразий*

$$U_{(S_1)} \supset U_{(S_2)} \supset \ldots \supset U_{(S_k)}$$

вещественное измерение каждого равно соответственно

$$2m-2,\ 2m-4,\ \ldots,\ 2m-2k.$$

Пусть в группе инерции точки P содержится подстановка S, может быть не самая высшая для точки P. Из леммы 3 следует, что ее можно представить в виде произведения низших подстановок

$$S = S_1 \cdot S_2 \cdots S_k.$$

Это означает, что точка P лежит на пересечении низших критических многообразий. В силу леммы 5, их пересечение образует критическое многообразие измерения $2m-2k$. Поэтому в окрестности точки P лежит ∞^{2m-2k} точек многообразия $U_{(S)}$, из которых только самое большее $\infty^{2m-2k-2}$ [1] принадлежит к высшим критическим многообразиям. Таким образом, в окрестности точки P находятся точки, для которых $U_{(S)}$ есть высшее многообразие, на котором они лежат. Сопоставляя с теоремой 2, мы приходим к следующей теореме:

Теорема 3. *Группа инерции точки P тогда и только тогда*

---

[1] Когда речь идет об алгебраических многообразиях, употребление старинного обозначения ∞^{ν} придает изложению бо́льшую ясность и в то же время не может привести ни к каким недоразумениям.

содержит подстановку S, если в ее окрестности находятся точки, для которых $U_{(S)}$ есть наивысшее критическое многообразие.

Перейдем к рассмотрению более общих случаев. Пусть коэффициенты $a_1, a_2, \ldots, a_n$ уравнения (1) — произвольные полиномы от $u_1, u_2, \ldots, u_m$. Построим пространство A коэффициентов $a_1, a_2, \ldots, a_n$, которые мы будем считать независимыми переменными. Для такого пространства мы умеем найти и критические многообразия и группы инерции. Каждой точке пространства U соответствует одна точка пространства A, и замкнутому пути в пространстве U соответствует замкнутый путь в пространстве A. Обратно, каждой точке пространства A соответствует несколько точек пространства U, причем некоторые из них могут быть кратными, в силу чего замкнутому пути в пространстве A может соответствовать разомкнутый путь в пространстве U. Другими словами, замкнутому пути в пространстве U может соответствовать несколько раз повторенный замкнутый путь в пространстве A.

Точка пространства U является критической только тогда, если ей соответствует критическая точка пространства A. Однако может случиться, что критической точке пространства A соответствуют обыкновенные точки пространства U. Это имеет место в том случае, если для производства замкнутого пути в окрестности некоторой точки пространства U мы должны обойти одну из соответствующих точек пространства A число раз, кратное порядкам каждой из подстановок. Таким образом, числа содержащихся друг в друге критических многообразий в пространстве U не превышают этих чисел в пространстве A. Оставляя детальный анализ взаимоотношений между пространствами U и A до другого случая, замечу, что в пространстве U критическим многообразиям могут соответствовать и не простые полиномиальные идеалы.

Если параметры $u_1, u_2, \ldots, u_m$ коэффициентов уравнения (1) подчинены алгебраической зависимости

$$g(u_1, u_2, \ldots, u_m) = 0, \tag{14}$$

то мы должны выделить в пространстве U алгебраическую поверхность, определяемую уравнением (14), которую мы и будем считать параметрическим пространством U_1 уравнения (1). В пространстве U_1 допустимыми замкнутыми путями должны считаться только те, все точки которых лежат на поверхности (14), и группы инерции критических точек должны быть определяемы только для таких путей. Заметим, что в такого рода пространствах U_1 не имеет места теорема монодромии: может существовать функция на U_1, однозначная относительно всех бесконечно малых замкнутых путей, но не однозначная в целом. Классическая (двумерная) теория римановых поверхностей дает примеры таких функций.

В некоторых случаях переменные $u_1, u_2, \ldots, u_m$ независимы, но вместе с тем задана группа Галуа G уравнения (1). Тогда параметрическое пространство уравнения (1) строится следующим образом. Составляется функция от корней уравнения (1), принадлежащая к группе G. Обозначим ее через u_{m+1}. Пусть в поле рациональных функций от $u_1, u_2, \ldots, u_m$ она удовлетворяет неприводимому уравнению

$$g(u_1, u_2, \ldots, u_m, u_{m+1}) = 0. \tag{15}$$

Определим параметрическое пространство U как поверхность (15) в $(m+1)$-мерном пространстве с координатами $u_1, u_2, \ldots, u_m, u_{m+1}$.

Заметим, что если мы будем определять замкнутый путь в пространстве U' с координатами $u_1, u_2, \ldots, u_m$ (проекция пространства U), то в пространстве U он будет замкнутым только тогда, если при его обходе функция u_{m+1} будет возвращаться к своему исходному значению; другими словами, если подстановка S, совершаемая корнями уравнения (1) при обходе этого пути, содержится в G. В противном случае замкнутый обход в U можно представить в виде k-кратного обхода в U', где k — наименьший показатель, при котором

$$S^k \subset G.$$

§ 3. Проблема резольвент в различных формулировках

Пусть даны два алгебраических уравнения

$$f(x) = 0, \tag{16}$$

$$g(y) = 0 \tag{17}$$

одной и той же степени n и с изоморфными группами Галуа $G, \bar{G}$. Будем считать для них областью рациональности композит полей, образованных коэффициентами, а также функциями от корней уравнений (16), (17), принадлежащими к группам $G, \bar{G}$. Имеет место

Теорема 4. *Чтобы корни уравнений* (16), (17) *находились в рациональной зависимости*

$$y_i = \alpha_0 + \alpha_1 x_i + \ldots + \alpha_{n-1} x_i^{n-1} \qquad (i = 1, 2, \ldots, n), \tag{18}$$

необходимо и достаточно, чтобы уравнение

$$F(u) = 0, \tag{19}$$

корнем которого является величина

$$u = \sum_{k=0}^{n-1} t_k (x_1^k y_1 + x_2^k y_2 + \ldots + x_n^k y_n), \tag{20}$$

где $t_1, t_2, \ldots, t_n$ — неопределенные переменные (которые мы включим в область рациональности), имело по крайней мере один рациональный корень.

Доказательство. Если имеют место зависимости (18), где α_0, $\alpha_1, \ldots, \alpha_{n-1}$ — рациональные величины, то, подставляя (18) в (20), получим для каждой из величин

$$u_k = x_1^k y_1 + x_2^k y_2 + \ldots + x_n^k y_n \qquad (k = 0, 1, 2, \ldots, n-1) \quad (21)$$

выражение

$$u_k = \alpha_0 s_k + \alpha_1 s_{k+1} + \ldots + \alpha_{n-1} s_{n+k-1}, \qquad (22)$$

где s_m — сумма m-ых степеней корней уравнения (16), т. е. рациональная величина. Из формулы (22) следует, что в этом случае u_k, а значит и u, суть рациональные величины.

Теперь предположим, что условия теоремы выполнены. Чтобы составить уравнение (19), которому удовлетворяет u, условимся обозначать через S и $\bar{S}$ формально одинаковые подстановки, производимые соответственно над корнями $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$. Производя над выражением (20) подстановку S, или, что то же, подстановку $\bar{S}^{-1}$ (так как выражение (20) инвариантно относительно подстановок $S\bar{S}$), мы переведем u в выражение u^S. Заставляя S пробегать группу G, получим величины, элементарно симметрические функции от которых симметричны относительно каждой из систем $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$, в силу чего величины

$$u^S = \sum_k t_k u_k^S$$

являются корнями уравнения (19), коэффициенты которого рациональны.

Группа Галуа поля, образованного всеми корнями x_i, y_i, есть подгруппа прямого произведения $G \times \bar{G}$. В этом поле величина u принадлежит или к группе, составленной из произведений $S\bar{S}$ (будем обозначать ее через $G\bar{G}$), или к ее надгруппе. Однако если уравнения (16) и (17) не имеют кратных корней, то не существует подстановок, отличных от $S\bar{S}$, которые оставляли бы инвариантной величину u, т. е., иначе говоря, все величины u_k. В самом деле, пусть существует такая подстановка $S_1\bar{S}_2$ $(S_1 \neq S_2)$. Умножая ее на $(S_1\bar{S}_1)^{-1}$, получим подстановку

$$\bar{S}_2\bar{S}_1^{-1} = \bar{S}_3 \neq 1,$$

относительно которой все величины u_k будут инвариантны. Полагая

$$\bar{S}_3 = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix},$$

придем к равенствам

$$u_k - u_k^{\bar{S}_3} = x_1^k (y_1 - y_{\alpha_1}) + x_2^k (y_2 - y_{\alpha_2}) + \cdots + x_n^k (y_n - y_{\alpha_n}) = 0,$$
$$(k = 0, 1, \ldots, n-1).$$

Рассматривая их как систему однородных линейных уравнений относительно $y_k - y_{\alpha_k}$ с неравным нулю определителем [вандермондов определитель от корней уравнения (16)], мы получим

$$y_k - y_{\alpha_k} = 0 \qquad (k = 1, 2, \ldots, n),$$

что находится в противоречии с тем, что уравнение (17) не имеет кратных корней.

Отсюда следует, что величина

$$u = \sum_k t_k u_k$$

принадлежит группе $G\bar{G}$. Если уравнение (19) имеет рациональный корень, то это означает, что группа Галуа поля, образованного корнями $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$, есть одна из групп, сопряженных с $G\bar{G}$. Меняя нумерацию корней $y_1, y_2, \ldots, y_n$, мы добьемся ее совпадения с $G\bar{G}$. Тогда все величины u_k будут рациональны. Решая относительно $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ систему уравнений (22), мы получим для $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ рациональные выражения. Тогда формулы (18) будут удовлетворять требованиям теоремы, что и требовалось доказать.

Примечание. Если уравнение (17) не имеет кратных корней, то формулы (18) обратимы. Это следует, например, из теоремы 47 моих „Основ теории Галуа“ [4].

Будем называть *преобразуемыми* уравнения (16), (17) в том случае, если между их корнями имеет место рациональная зависимость типа [18].

Проблема резольвент, поставленная в различных формулировках Клейном [3] и Гильбертом [1, 2], может быть поставлена в следующем виде, более общем и вместе с тем более просто формулируемом

Дано уравнение, коэффициенты которого зависят от $m (\leqslant n)$ параметров. Требуется найти преобразуемое в него уравнение, коэффициенты которого зависели бы от возможно меньшего числа параметров (которое мы обозначим через s).

Коэффициенты (или параметры) уравнений (16) и (17) могут и не зависеть рационально друг от друга. Задача состоит в установлении между ними таких алгебраических зависимостей, чтобы при этом соблюдались два условия:

1) Преобразование (18) должно быть обратимым. Мы видели, что это условие всегда соблюдается, если уравнения (16) и (17) не имеют кратных корней.

2) Уравнение (19) должно иметь корень, рационально зависящий от коэффициентов уравнений (16) и (17), а также от функций от их корней, принадлежащих соответственно к группам G и $\bar{G}$.

Сравним приведенную формулировку проблемы резольвент с формулировками, предложенными Клейном и Гильбертом.

Проблема Клейна. По данному уравнению (16) найти такое уравнение (17), зависящее от возможно меньшего числа s параметров,

чтобы между их корнями имели место зависимости типа (18), коэффициенты которых $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ должны рационально зависеть от коэффициентов уравнения (16).

Как обобщение проблемы Клейна рассматривается допущение зависимости $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ еще от некоторых наперед заданных иррациональностей.

Проблема Клейна является более частной, т. е. налагающей больше требований, по сравнению с проблемой Гильберта.

Проблема Гильберта. По данному уравнению (16) найти такое уравнение (17) (будем называть его резольвентой), зависящее от возможно меньшего числа s параметров, чтобы коэффициенты $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ зависимостей (18) между их корнями определялись при помощи вспомогательного уравнения, которое в свою очередь должно иметь резольвенту с $\leqslant s$ параметрами, причем коэффициенты зависимостей между корнями последних опять должны зависеть от корней уравнения, допускающего резольвенту с $\leqslant s$ параметрами, и т. д. Число получаемых при этом вспомогательных уравнений должно быть конечно.

Докажем, что проблема Гильберта является частной по сравнению с формулированной нами проблемой. Достаточно ограничиться случаем, когда G есть простая группа. В самом деле, если G имеет нормальный делитель H, то мы предварительно должны решить проблему Гильберта для вспомогательного уравнения, группа Галуа которого изоморфна с факторгруппой G/H. Затем, считая это уравнение вспомогательным и присоединяя его корни к области рациональности, понизим группу Галуа заданного уравнения до H. Таким образом, число s в проблеме Гильберта для уравнений с группой Галуа G равно наибольшему из чисел s в проблеме Гильберта для уравнений с группами Галуа H и G/H.

Предположим, что уравнение (16) с простой группой Галуа G имеет s-параметрическую резольвенту (17) в смысле Гильберта. Докажем, что (17) будет также резольвентой и в нашем смысле. Допустим противное: пусть уравнение (19) не имеет рационального корня, если считать областью рациональности композит полей коэффициентов уравнений (16) и (17). В этой области рациональности поле, образованное корнями уравнений (16) и (17), имеет группой Галуа некоторую подгруппу прямого произведения $G \times \overline{G}$, которая, таким образом, не содержится ни в группе $G\overline{G}$, образованной подстановками типа $S\overline{S}$, ни в одной из сопряженных с $G\overline{G}$ групп.

Прежде всего докажем, что группа уравнения (16) не снизится, если к области рациональности присоединить коэффициенты уравнения (17). Действительно, в противном случае это поле содержало бы натуральную иррациональность, принадлежащую к настоящей подгруппе G. Ее пересечение со всеми сопряженными подгруппами есть единичная группа, в силу чего эта иррациональность будет корнем уравнения,

группа Галуа которого изоморфна с G. Таким образом, поле корней этого уравнения, которое должно быть рассматриваемо как вспомогательное (поле, образованное величинами $\alpha_0, \alpha_1 \ldots, \alpha_{n-1}$, должно его содержать), содержит в себе корни исходного уравнения (16). Это означает, что резольвента для вспомогательного уравнения будет иметь не меньше параметров, чем резольвента (17), и новое вспомогательное уравнение опять будет содержать ту же иррациональность и т. д., так что процесс никогда не кончится.

Меняя ролями уравнения (16) и (17), мы докажем, что в области рациональности, образованной коэффициентами уравнений (16) и (17), группы Галуа обоих этих уравнений изоморфны с G.

Если поля K_1, K_2, образованные соответственно корнями уравнений (16) и (17), взаимно просты, т. е. имеют пересечением композит полей коэффициентов, то группа композита $K_1 \times K_2$ изоморфна с $G \times \overline{G}$. Так как кроме G и $\overline{G}$ эта группа не имеет других нормальных делителей, то группа $G\overline{G}$, к которой принадлежит корень уравнения (19), не есть нормальный делитель группы $G \times \overline{G}$ и, более того, имеет с сопряженными подгруппами единичную группу в качестве пересечения. В силу этого группа уравнения (19) изоморфна с $G \times \overline{G}$. Отсюда следует, что корни уравнений (16) и (17) содержатся в поле корней уравнения (19), так что последнее, будучи вспомогательным уравнением, имеет не более простое решение, чем каждое из уравнений (16) и (17).

Пересечение полей K_1 и K_2 есть нормальное поле, и потому внутри каждого из полей K_1, K_2 принадлежит соответственно к нормальным делителям групп G, $\overline{G}$. В силу простоты последних групп это пересечение, если оно не есть композит полей коэффициентов, должно совпадать с каждым из полей K_1, K_2.

Отсюда еще не всегда следует существование рациональной зависимости типа (18) между корнями уравнений (16) и (17). Именно, она не имеет места тогда и только тогда, когда G допускает несколько различных (т. е. не переходящих друг в друга путем изменения порядка цифр) представлений в виде транзитивной группы подстановок из n цифр, т. е. если G имеет внешние автоморфизмы. Например, это имеет место, когда G — знакопеременная группа из 6 цифр. Однако и в этом случае наше утверждение остается в силе. Именно, если уравнения (16) и (17) таковы, что образованные их корнями поля K_1 и K_2 совпадают, то можно преобразовать резольвенту (17) так, чтобы после этого между корнями уравнений (16) и (17) установились рациональные зависимости типа (18). Для этого надо составить уравнение n-ой степени, корень которого, будучи элементом поля K_2, принадлежал бы к той же группе внутри поля K_1, к которой принадлежит корень уравнения (16). Построенное таким образом уравнение, являясь преобразуемым в уравнение (16), в то же время остается s-параметрическим.

Вопрос об условиях, при которых обе проблемы эквивалентны, требует специального исследования.

§ 4. Условия, необходимые для существования резольвенты

В настоящей статье мы ограничимся случаем, когда область рациональности резольвенты (17) совпадает с областью рациональности уравнения (16). Пусть коэффициенты уравнения (16) рационально зависят от параметров $u_1, u_2, \ldots, u_m$ и пусть s параметров резольвенты (17) $v_1, v_2, \ldots, v_s$ приведены с $u_1, u_2, \ldots, u_m$ в такое соответствие, что являются их целыми рациональными функциями. Тогда каждому замкнутому пути пространства

$$U(u_1, u_2, \ldots, u_m)$$

будет соответствовать вполне определенный замкнутый путь пространства

$$V(v_1, v_2, \ldots, v_s).$$

Если при этом первый из путей находится в окрестности какой-нибудь одной точки (т. е. бесконечно мал), то и второй путь находится в окрестности определенной точки.

Если при обходе по замкнутому пути C в окрестности точки P корни уравнения (16) претерпевают подстановку S, то при обходе по соответствующему пути $\bar{C}$ пространства V корни уравнения (17) претерпевают подстановку $\bar{S}$, отличающуюся от S только другими переставляемыми объектами. В самом деле, пусть рациональный корень уравнения (19) имеет вид

$$\sum_k t_k u_k,$$

где

$$u_k = x_1^k y_1 + x_2^k y_2 + \cdots + x_n^k y_n, \qquad (k = 0, 1, \ldots, n-1).$$

Если бы при обходе пути C корни $x_1, x_2, \ldots, x_n$ претерпевали подстановку

$$S = \begin{pmatrix} x_1 & x_2 \ldots x_n \\ x_{\alpha_1} & x_{\alpha_2} \ldots x_{\alpha_n} \end{pmatrix},$$

и при обходе пути $\bar{C}$ корни $y_1, y_2, \ldots, y_n$ претерпевали бы подстановку

$$\bar{S}_1 = \begin{pmatrix} y_1 & y_2 \ldots y_n \\ y_{\beta_1} & y_{\beta_2} \ldots y_{\beta_n} \end{pmatrix},$$

то в силу однозначности функций u_k должно быть

$$x_{\alpha_1}^k y_{\beta_1} + x_{\alpha_2}^k y_{\beta_2} + \cdots + x_{\alpha_n}^k y_{\beta_n} = x_1^k y_1 + x_2^k y_2 + \cdots + x_n^k y_n$$
$$(k = 0, 1, \ldots, n-1),$$

откуда

$$x_1^k(y_1 - y_{\gamma_1}) + x_2^k(y_2 - y_{\gamma_2}) + \cdots + x_n^k(y_k - y_{\gamma_n}) = 0, \qquad (23)$$
$$(k = 0, 1, \ldots, n-1),$$

где

$$\begin{pmatrix} \alpha_1 & \alpha_2 \ldots \alpha_n \\ \beta_1 & \beta_2 \ldots \beta_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ \gamma_1 & \gamma_2 & \cdots & \gamma_n \end{pmatrix},$$

откуда

$$S_1 = \begin{pmatrix} 1 & 2 \ldots & n \\ \beta_1 & \beta_2 \ldots & \beta_n \end{pmatrix} = \begin{pmatrix} 1 & 2 \ldots & n \\ \alpha_1 & \alpha_2 \ldots & \alpha_n \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 \ldots \alpha_n \\ \beta_1 & \beta_2 \ldots \beta_n \end{pmatrix} = S \begin{pmatrix} 1 & 2 & \ldots n \\ \gamma_1 & \gamma_2 & \cdots \gamma_n \end{pmatrix},$$

т. е.

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \gamma_1 & \gamma_2 & \cdots & \gamma_n \end{pmatrix} = S^{-1} \cdot S_1.$$

Но так как путь C проходит по не критическим точкам пространства U, то определитель системы однородных линейных уравнений (23) на пути C нигде не обращается в нуль, откуда мы получаем

$$y_1 = y_{\gamma_1}, \quad y_2 = y_{\gamma_2}, \ldots, y_n = y_{\gamma_n}. \qquad (24)$$

С другой стороны, зависимости (18) между корнями уравнений (16) и (17) предполагаются обратимыми, в силу чего на пути $\overline{C}$ корни уравнения (17) также не делаются кратными. Поэтому из равенств (24) мы имеем

$$\gamma_1 = 1, \quad \gamma_2 = 2, \ldots, \gamma_n = n,$$

откуда

$$S_1 = S.$$

Мы приходим к теореме:

Теорема 5. *Если параметры уравнения* (17) *— целые рациональные функции от параметров уравнения* (16) *и оба эти уравнения преобразуемы друг в друга, то соответственные точки пространств, образуемых параметрами уравнения* (17), *имеют группы инерции, содержащие как подгруппы группы, изоморфные с группами инерции точек пространства параметров уравнения* (16).

Рассмотрим случай, когда параметры $u_1, u_2, \ldots, u_m$ входят в коэффициенты уравнения (16) линейно. Пусть уравнение (17) становится преобразуемым по отношению к уравнению (16), если мы положим вместо параметров $v_1, v_2, \ldots, v_s$ полиномы: $v_1 = \varphi_1(u_1, u_2, \ldots, u_m), \ldots, v_s = \varphi_s(u_1, u_2, \ldots, u_m)$. Из теоремы 5 следует, что точкам критических многообразий пространства U соответствуют точки критических многообразий пространства V. Если мы условимся считать допустимыми замкнутыми путями в пространстве V только те, которым соответствуют замкнутые пути в пространстве U, то в силу теоремы 5 группы инерции соответствующих точек изоморфны.

Пусть пространство U содержит цепь из содержащихся друг в друге критических многообразий

$$U_{(s_1)} \supset U_{(s_2)} \supset \cdots \supset U_{(s_q)}.$$

Этим многообразиям пусть в пространстве V соответствуют многообразия

$$V_1 \supset V_2 \supset \cdots \supset V_a.$$

Докажем, что эти многообразия имеют различные измерения. С одной стороны, ни одна пара соседних многообразий V_i, V_{i+1} не может совпадать. В самом деле, пусть P будет точка пространства U, принадлежащая многообразию $U_{(s_{i+1})}$, но не принадлежащая никакому более высокому многообразию. В силу теоремы 3 в ее окрестности содержатся точки P' многообразия $U_{(s_i)}$, не принадлежащие многообразию $U_{(s_{i+1})}$ и, следовательно, группы инерции которых не совпадают с группой инерции точки P (порядок последней выше). Пусть в пространстве V точкам P, P' соответствуют точки Q, Q'. При нашем условии относительно допустимых замкнутых путей из теоремы 5 следует, что группы инерции точек Q и Q' различны. Обе они лежат на многообразии V_i, но вместе с тем точка Q лежит на многообразии V_{i+1}, а точка Q' нет.

С другой стороны, многообразиям V_i соответствуют простые идеалы B_i. В самом деле, чтобы узнать, лежит ли полином $g(v_1, v_2, \ldots, v_s)$ в идеале B_i, надо выразить переменные $v_1, v_2, \ldots, v_s$ через $u_1, u_2, \ldots, u_m$, которые, в свою очередь, выражаются через корни $x_1, x_2, \ldots, x_n$ уравнения (16). После этого мы должны приравнять друг другу эти корни сообразно с таблицей совпадений, соответствующей подстановке S_i. Полином g лежит в идеале B_i тогда и только тогда, если он после указанных операций обратится в нуль. Из этого критерия следует, что произведение gh лежит в B_i. Таким образом, B_i есть простой идеал.

Из этого следует, что все измерения многообразий $V_1, V_2, \ldots, V_q$ различны, и так как измерение многообразия V_q не меньше нуля, то V_1 имеет измерение $\geqslant q-1$. Но так как V_1 есть критическое многообразие, а V содержит не-критические точки, то измерение пространства V не меньше, чем q, и мы приходим к теореме:

Теорема 6. *Если уравнение типа* (16) *с параметрами, линейно входящими в коэффициенты, содержит цепь из q критических многообразий, из которых каждое последующее содержится в предыдущем, то всякая рациональная резольвента содержит не менее q параметров.*

Эта теорема дает возможность установить нижнюю границу для числа параметров резольвенты.

В виде примера рассмотрим самые общие уравнения (т. е. с независимыми переменными в качестве коэффициентов) со знакопере-

менной группой Галуа. В этом случае U есть поверхность, определяемая в $(n+1)$-мерном пространстве $a_1, a_2, \ldots, a_n, z$ при помощи уравнения

$$z^2 - D(a_1, a_2, \ldots, a_n) = 0,$$

где D — дискриминант уравнения (16). Не трудно убедиться, что каждому типу четных подстановок в пространстве U соответствует критическое многообразие. В самом деле, мы всегда имеем возможность сконструировать уравнение (может быть, приводимое), у которого группа Галуа состоит из степеней любой четной подстановки S. Это уравнение будет частным видом уравнения (16), поскольку у последнего коэффициенты суть независимые переменные. С другой стороны, построенное таким образом уравнение непременно будет иметь в своем параметрическом пространстве (которое получается из U придаванием некоторым из коэффициентов частных значений) критическое многообразие U_S.

Например, если

$$S = (1, 2, \ldots, \mu_1)(\mu_1 + 1, \ldots, \mu_2)\ldots(\mu_{k-1} + 1, \ldots, n),$$

то в качестве такого частного уравнения можно взять

$$(x^{\mu_1} - w_1)\ (x^{\mu_2 - \mu_1} - w_2)\ldots(x^{n - \mu_{k-1}} - w_k) = 0,$$

где $w_1, w_2, \ldots, w_k$ — независимые переменные.

Таким образом, в нашем случае мы получим нижнюю границу для возможного числа параметров резольвенты уравнения (16), если подсчитаем максимальное число звеньев во всевозможных цепях из четных подстановок n-ой степени, в которых последующий член выше предыдущего. Одной из таких цепей может служить

$$S_1 < S_2 < \ldots < S_{\left[\frac{n-1}{2}\right]},$$

где

$$S_1 = (123), \quad S_2 = (12345), \quad \ldots, \quad S_i = (123\ldots 2i+1);$$

$$i = 1, 2, \ldots, \left[\frac{n-1}{2}\right].$$

Эта цепь состоит из $\left[\frac{n-1}{2}\right]$ звеньев.

Докажем, что в знакопеременной группе n-ой степени не содержится цепей большей длины, чем $\left[\frac{n-1}{2}\right]$. В самом деле, отмечая в каждой подстановке число содержащихся в ней циклов, включая в это число и одночленные циклы (инвариантные цифры), заметим, что для четной подстановки это число имеет ту же четность, что n. С другой стороны, если, например,

$$T_1 < T_2$$

то подстановка T_2 непременно должна содержать меньшее число циклов, чем T_1. В силу одинаковой четности эти числа должны отличаться, по крайней мере, на 2. Поэтому числа циклов в подстановках цепи

$$T_k > T_{k-1} > \ldots > T_2 > T_1$$

не могут быть меньше, чем соответственно числа

$$1, 3, 5, \ldots, 2k-1.$$

Но T_1 не может быть ни тождественной подстановкой, ни транспозицией, в силу чего

$$2k-1 \leqslant n-2,$$

откуда

$$k \leqslant \left[\frac{n-1}{2}\right].$$

Таким образом, искомая нижняя граница для числа параметров равна

$$s = \left[\frac{n-1}{2}\right]. \tag{25}$$

Сопоставим эти значения с теми, которые были получены Гильбертом [2] для $5 \leqslant n \leqslant 9$:

	5	6	7	8	9
s [по формуле (25)]	2	2	3	3	4
s (по Гильберту)	1	2	3	4	4

Это сопоставление показывает, что при $n=5$ введение иррациональных резольвент на самом деле снижает число параметров. В случаях $n=6, 7, 9$ числа s, определенные с разных концов, повидимому дают для числа параметров точные значения. Наконец, случай $n=8$ требует дополнительного исследования.

В заключение упомянем о двух основных вопросах, стоящих на очереди при решении рассматриваемой проблемы:

1) *Вопрос об иррациональных резольвентах.* Мы только что видели, что введение иррациональностей в область коэффициентов уравнения может существенным образом понизить число параметров в резольвенте. Эти иррациональности должны быть введены так, чтобы критические многообразия не все оставались неприводимыми. При этом пространства U и V будут находиться в алгебраической, но не в рациональной зависимости. Пусть координаты $v_1, v_2, \ldots, v_s$ пространства V определяются из уравнений

$$\varphi^i(u_1, u_2, \ldots, u_m, v_s) = 0 \quad (i = 1, 2, \ldots, s).$$

Считая областью рациональности совокупность рациональных функций от $u_1, u_2, \ldots, u_m$, найдем примитивный элемент

$$\xi = c_1 v_1 + c_2 v_2 + \ldots + c_s v_s$$

поля, образованного элементами $u_1, \ldots, u_m; v_1, \ldots, v_s$. Пусть

$$F(u_1, u_2, \ldots, u_m, \xi) = 0. \tag{26}$$

Назовем пространством W поверхность, образованную координатами $u_1, u_2, \ldots u_m, \xi$, которые подчинены уравнению (26). Координаты пространств U и V рационально выражаются через координаты пространства W. Группами инерции обоих уравнений (16), (17) мы будем считать совокупности подстановок, испытываемых их корнями при обходах бесконечно малых замкнутых путей в пространстве W Последним в пространствах U, V могут соответствовать или простые, или повторенные по нескольку раз замкнутые пути. Задача состоит в построении такого пространства W, чтобы благодаря повторению замкнутых путей в U и V группы инерции, соответствующие различным критическим многообразиям, пришли к совпадению.

2) *Вопрос о верхней границе для числа параметров в резольвенте.* Если дано пространство U параметров уравнения (16), в котором критические многообразия образуют цепи длины $\leqslant s$, то возникает вопрос о возможности построения s-параметрической резольвенты. Если U_S — высшее критическое многообразие пространства U, то в пространстве V ему должно соответствовать критическое многообразие нулевого измерения. Это указывает путь к фактическому построению резольвент. Вопрос требует дальнейших исследований.

Поступило
24 / II 1943 года

ЛИТЕРАТУРА

1. D. Hilbert. Mathematische Probleme. Problem 13. Gött. Nachr., 1900, стр. 253—297; Ges. Abh. 3, стр. 290—329.
2. D. Hilbert. Ueber die Gleichung neunten Grades. Math. Ann. 97, 1927, стр. 243—250; Ges. Abh. 2, стр. 393—400.
3. F. Klein. Ges. math. Abh. 2, стр. 255—504.
4. Н. Чеботарев. Основы теории Галуа, I. ОНТИ. 1934.
5. N. Tschebotaröw. Ueber das Klein-Hilbertsche Resolventenproblem. Изв. Каз. физ.-мат. общ. (3), 7, 1934, стр. 5—22. Собр. соч., т. I, стр. 282—304.
6. B. L. van der Waerden. Moderne Algebra. 2. Springer, 1931.
7. A. Wiman. Ueber die Anwendung der Tschirnhausen—Transformation auf die Reduktion algebraischer Gleichungen. Nova Acta R. Soc. Sc. Upsal., vol. e. o. e. 1927, стр. 3—8.

ПРОБЛЕМА РЕЗОЛЬВЕНТ

(Юб. сборн. АН СССР, 1947, стр. 80—95)

В истории математики известно немало случаев, когда та или иная проблема привлекала внимание ученых из эстетических или теоретических побуждений, и только по истечении многих лет и даже веков обнаруживалось ее практическое значение. Кроме общеизвестного примера теории вероятностей, можно назвать цикл задач на построение при помощи циркуля и линейки. Нас может удивить, с какой настойчивостью древние греки решали делосскую задачу о нахождении стороны куба с удвоенным объемом, стремясь дать теоретическое решение при помощи циркуля и линейки для задачи, которую на практике можно было бы решить точнее, поскольку циркуль — инструмент, всегда приводящий к неточностям.

У греков этот интерес к теоретическим решениям, возможно, был связан с их пренебрежительным отношением к практическим задачам. Но как нам ни чужд образ мыслей древних греков, он сыграл в истории науки большую положительную роль. Не говоря уже о развитой ими строгости логической мысли, давшей возможность впоследствии поднять на огромную высоту уровень точных наук, самая постановка теоретически точных задач позволила четко расклассифицировать задачи, увидеть, какая из них решается какими средствами.

В XIX в. возникли доказательства невозможности решения определенных задач определенными средствами: деления круга на три части циркулем и линейкой, представления некоторых интегралов через элементарные функции и т. п. Этот круг задач в свою очередь оказался полезным для практики: он дал возможность экономить труд при решении так называемых серийных задач, на которых в дальнейшем остановимся подробнее.

Вернемся к задачам на построение циркулем и линейкой. Невозможность решения некоторых из них была доказана при помощи теории алгебраического решения уравнений, созданной молодым гениальным математиком Эваристом Галуа [1]. Незадолго до появления его работ Абель [7] доказал невозможность решения в радикалах уравнений выше 4-й степени. Галуа же дал способ узнавать относительно каждого данного уравнения, решается ли оно в радикалах, или нет. Для этого он сопоставил с каждым уравнением *группу*

(получившую в последнее время название группы Галуа), т. е. совокупность подстановок, которые можно производить над его корнями без нарушения существующих между ними рациональных соотношений. Оказалось, что вопрос о возможности решить заданное уравнение в радикалах вполне определяется структурой его группы Галуа. Не будем описывать тех свойств, которые присущи *разрешимым группам*, т. е. группам, которым соответствуют разрешимые в радикалах уравнения.

Теория Галуа дала возможность также ответить на вопрос, возможно ли выполнить всякую заданную задачу на построение при помощи циркуля и линейки. Для этого нужно построить уравнение, от которого зависит искомая для задачи величина, и найти группу этого уравнения. Чтобы решение было возможно, необходимо и достаточно, чтобы число подстановок, содержащихся в группе, было степенью двойки. Идя таким путем, Гаусс еще до Галуа дал «теоретически» «точное» построение правильного 17-угольника [4]. Таким же путем была доказана невозможность деления угла на три равные части, а а также построения стороны куба с удвоенным объемом при помощи циркуля и линейки.

Введенное Галуа понятие группы играет в современной математике роль, далеко выходящую за пределы задачи решения уравнений в радикалах. Наряду с конечными группами подстановок, операции которых состоят в перестановке некоторого конечного числа предметов, были введены непрерывные группы, теорию которых создал Ли [5]. Их операции состоят из определенного типа перемещений точек в пространстве. Для лучшего уяснения этого понятия возьмем гидродинамическую аналогию. Представим себе пространство заполненным жидкостью (или газом), находящейся в непрерывном движении. Запомним положение каждой ее частицы в какой-нибудь определенный момент времени t_0. В каждый момент времени t положение каждой частицы будет другим. Будем говорить, что расположение частиц в момент t переводится из их расположения в момент t_0 преобразованием нашей непрерывной группы, которое внутри группы определяется для каждого момента t. При этом движение жидкости должно быть установившимся. Это значит, что, совершая подряд два любых преобразования из одной и той же группы, мы опять придем к преобразованию той же группы.

Переменная t, значения которой определяют преобразования внутри группы, называется *параметром* группы. Наша аналогия предусматривает случай группы с одним параметром; обыкновенно же рассматриваются группы с несколькими параметрами. Так, одна из наиболее простых групп, преобразования которой определяются перемещениями в пространстве твердого тела, есть группа с шестью параметрами, поскольку положение твердого тела в пространстве определяется шестью величинами.

Вернемся к вопросу о решении уравнений в радикалах. Казалось бы, что этот вопрос потерял всякое практическое значение, поскольку известно, что не всякое уравнение решается в радикалах, а узнать, решается ли оно, — далеко не легкая задача. Гораздо проще применить один из хорошо разработанных в настоящее время способов численного решения уравнений, позволяющих находить корни уравнений любой степени с любой точностью. Все это совершенно справедливо до тех пор, пока мы имеем дело с одним уравнением или пока нам изредка приходится решать разрозненные уравнения. Но современная наука и техника столкнулись с необходимостью решать громадное число уравнений более или менее однородного типа, но с различными числовыми значениями входящих в него параметров. Лучшим примером этому может служить астрономия. Для вычисления элементов орбит по нескольким наблюдениям астрономам приходится решать уравнения нескольких определенных типов. Так, для вычисления орбит комет (с параболическими орбитами) по трем наблюдениям нужно решать кубические уравнения. Для вычисления орбит планет нужно решать определенного типа уравнения 8-й степени с входящими в выражение коэффициентов данными наблюдений в качестве параметров. При громадном числе комет и планет (астероидов) астрономам приходится вычислять корни очень большого числа уравнений одинакового типа. Очевидно, что составление таблиц для такого рода уравнений значительно сократит их труд. Для кубических уравнений астрономы и пользуются особыми таблицами Баркера. Для уравнений же высших степеней составление таблиц тормозится большим числом входящих в коэффициенты параметров.

Очень просто составить таблицы каких-нибудь функций от одного аргумента; подавляющее большинство существующих таблиц принадлежит именно к этому типу. Таблицы функций от двух аргументов очень неудобны для пользования. Это знает всякий, пользовавшийся большими таблицами умножения.

А вот другой пример. Астрономы (равно как и другие вычислители) весьма заинтересованы в том, чтобы по данным $\log a$ и $\log b$ быстро и просто находить значение $\log(a+b)$. Но таблица от двух аргументов, дающая эти значения, была бы очень неудобна для пользования. Вычислители вменяют в большую заслугу Гауссу изобретение принципа, в силу которого эта задача решается при помощи таблицы от одного аргумента.

Этот принцип крайне прост [2, 3]: таблица содержит значения величин $\log\left(1+\frac{b}{a}\right)$ по данным значениям $\log a - \log b = \log \frac{a}{b}$.

Для нахождения значений функций от двух и даже большего числа аргументов очень полезны методы номографии. Но, чем больше аргументов, тем сложнее номограмма, тем труднее пользование ею и тем менее надежен результат. Таким образом, задача максимального

уменьшения числа параметров, входящих в коэффициенты уравнения, приобретает большую важность.

Если бы всякое уравнение решалось в радикалах, то упомянутая задача получила бы идеально простое решение. В самом деле, каждый радикал есть функция только одного аргумента (если значения последнего комплексны, то получится функция от двух аргументов; но, представив аргумент в тригонометрической форме, мы приведем радикал к функциям от одного аргумента). Если известно выражение корней уравнения через радикалы, то для вычисления этих корней достаточно иметь набор таблиц радикалов соответствующих степеней и производить над получаемыми из них данными вычисления в пределах четырех арифметических действий.

К сожалению, таких радикальных выражений в природе не существует. Но их значение для „серийных задач" наводит на такую мысль: какой смысл искать выражения корней уравнения в радикалах, т. е. в форме выражений через функции одного аргумента весьма частного вида, когда мы имеем гораздо больше шансов на успех, если станем отыскивать выражения для корней в форме многократно повторяемых функций одного аргумента, не задаваясь заранее видом этих последних?

Такое обобщение задачи вначале имело успех. Оказалось, что уравнения 5-й степени, которые, как известно, не решаются в радикалах, тем не менее допускают представление своих корней через функции от одного аргумента. Это в принципе было известно очень давно. Чтобы разъяснить это, станем на несколько другую точку зрения. Если

$$f(x) = 0 \tag{1}$$

заданное уравнение, а

$$y = \varphi(x) \tag{2}$$

любая рациональная функция с рациональными коэффициентами, то y удовлетворяет уравнению

$$F(y) = 0 \tag{3}$$

той же степени. Это преобразование уравнения носит название *преобразования Чирнгаузена*. Если нам удастся подобрать функцию (2) так, чтобы соответствующее ей уравнение (3) содержало в коэффициентах всего один параметр, то задача будет решена. В самом деле, из равенства (2) определенным образом можно получить рациональное выражение корней x через корни y

$$x = \psi(y). \tag{4}$$

С другой стороны, корень y уравнения (3) зависит только от одного параметра, входящего в коэффициенты. Из (4) следует, что x выражается рационально через функцию одного параметра.

Давно известно, что можно подобрать преобразование (2) так, чтобы самое общее уравнение 5-й степени

$$f(x) = x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 = 0 \tag{5}$$

преобразовывалось в уравнение так называемого бринг-жерраровского вида

$$F(y) = y^5 + py + q = 0. \tag{6}$$

При этом коэффициенты функции (2) могут быть не рациональными, а быть корнями уравнений 2, 3 и 4-й степеней. Но поскольку все такие уравнения решаются в радикалах, они, следовательно, тоже выражаются через функции от одного аргумента. С другой стороны, в коэффициенты уравнения (6) входят два параметра p, q; но подстановка

$$y = \sqrt[5]{q}\cdot z$$

приводит уравнение (6) к виду

$$z^5 + \frac{p}{\sqrt[5]{q^4}}z + 1 = 0;$$

в последнем уравнении выражение $\frac{p}{\sqrt[5]{q^4}}$ является единственным параметром.

Можно дать более простое приведение уравнения (5) к однопараметрическому виду, если не ограничивать себя бринг-жерраровской формой. Именно, можно добиться того, чтобы в коэффициенты функции (2) входили только квадратные радикалы. Это сделал впервые Гальфен [8], пользуясь уравнениями деления аргумента эллиптической функции на 5. В алгебраической форме эти же результаты были получены Клейном [11, 15]; его уравнение (3) имеет вид

$$y^5 + 15y^4 - 10\gamma v^2 + 3\gamma^2 = 0, \tag{7}$$

где γ — параметр.

Этот результат Клейна связан с очень интересными соображениями из области теории групп, конечных и непрерывных. Группа Галуа уравнения (5) общего вида есть совокупность всех подстановок его пяти корней; таких подстановок всего $1\cdot2\cdot3\cdot4\cdot5 = 120$. Если же мы присоединим к области рациональности (т. е. условно будем считать рациональным) квадратный корень из так называемого дискриминанта уравнения (5), то группа Галуа понизится: в ней останутся только четные подстановки, всего числом 60. Эта группа — наименьшая из неразрешимых групп; она изоморфна (т. е. одинакова по структуре) группе вращений самого сложного правильного многогранника — *икосаэдра*. Представим себе икосаэдр вписанным в шар и будем

считать вращением икосаэдра такой поворот шара вокруг центра, при котором каждая вершина икосаэдра попадет в положение какой-нибудь другой из его вершин (или останется на месте). Подсчитаем число различных вращений, учитывая, что икосаэдр имеет 12 вершин, составляющих шесть пар, каждая из которых лежит на одном и том же диаметре шара, и что вокруг каждой вершины расположено пять треугольных граней. Можно придать какой-нибудь определенной оси одно из шести положений; выбрав определенное положение оси, можно поменять местами обе находящиеся на ней вершины; наконец, фиксируя обе вершины, можно вращать вокруг них фигуру, придавая ей пять различных положений. Всего получится $6 \cdot 2 \cdot 5 = 60$ различных вращений.

Группа икосаэдра есть наибольшая из конечных групп вращений шара, поскольку икосаэдр — самый сложный из правильных многогранников. Другими словами, группа икосаэдра — наибольшая из конечных подгрупп группы всевозможных вращений шара. Последняя является непрерывной группой и зависит от трех параметров. Она изоморфна группе всевозможных дробных линейных преобразований

$$y = \frac{ax + b}{cx + d}. \tag{8}$$

Группа же дробных линейных преобразований является наибольшей группой из существующих в пространстве одного измерения групп. Этот факт делал весьма вероятной следующую гипотезу.

Если уравнение (1) можно преобразовать в уравнение (3), в коэффициенты которого входит k параметров, то его группа Галуа изоморфна конечной подгруппе некоторой непрерывной группы преобразований точек k-мерного пространства. Справедливо и обратное.

Эта гипотеза в неявном виде содержится в работах Клейна и других математиков, работавших над *проблемой резольвент*, или, как она называлась в ранней стадии своего развития, *проблемой форм*. В явном виде мне удалось доказать ее в 1931 г. [12] и привести в более совершенную форму в 1933 г. [13].

Однако результаты, полученные таким образом для проблемы Клейна, были весьма неутешительны. Дело в том, что Виман [16] доказал, что знакопеременная группа степени $n \geqslant 8$ не может быть представлена как однородная линейная группа менее чем от $n - 1$ переменных. С другой стороны, Картан в своей диссертации высказал предположение, что все подгруппы максимального числа параметров у простых непрерывных групп (о которых только и должна итти здесь речь) регулярны, т. е. принадлежат к типу подгрупп, допускающих простое перечисление геометрическим методом, который был открыт Киллингом и усовершенствован Картаном. Известны все типы простых непрерывных групп: кроме пяти исключительных групп, они состоят из однородных линейных групп, ортогональных и так назы-

ваемых симплициальных групп от n переменных. Из них только ортогональные группы содержат подгруппы с числом параметров на $n-2$ меньшим, чем самые группы; у групп остальных типов они на $n-1$ меньше. Из этого следует, что ортогональные группы могут быть представлены в пространстве не меньшего числа измерений, чем $n-2$. Таким образом, знакопеременная группа из $n \geqslant 8$ цифр является подгруппой непрерывной группы, представляемой в пространстве числа измерений не меньшего, чем $n-3$. Из этого, в силу приведенного результата, следует, что уравнение n-ой степени общего вида, группа Галуа которого после присоединения к области рациональности квадратного корня из дискриминанта является знакопеременной группой, имеет резольвенту не менее чем с $n-3$ параметрами. При этом коэффициенты преобразования могут содержать иррациональности; но их резольвенты не могут содержать более n—3 параметров.

Можно было бы еще надеяться, что гипотеза Картана не верна. Тогда можно было бы уменьшить число параметров в резольвенте более чем на три параметра. Однако в 1938 г. мне удалось доказать правильность гипотезы Картана [14]. Таким образом, в приведенной постановке Клейна польза от решения проблемы резольвент имеет очень ограниченный характер.

Вместе с тем Гильберт предложил другую, расширенную формулировку проблемы резольвент. Она состоит в том, что задается число S параметров, которые должна содержать резольвента. При этом коэффициенты уравнения (2) могут не быть рациональными, но уравнения с рациональными коэффициентами, которым они удовлетворяют, тоже допускают резольвенты, содержащие не более S параметров. Коэффициенты преобразования корней этих уравнений в корни резольвент, если они иррациональны, являются корнями уравнений, резольвенты которых опять содержат не более S параметров, и т. д. Этот процесс должен содержать конечное число шагов. Ищется наименьшее значение S, удовлетворяющее этим условиям.

Гильберт опубликовал свою формулировку проблемы резольвент в 1900 г. как одну из своих знаменитых 23 задач, которые на много лет определили направление работы математиков [9]. Из них 13-я задача посвящена проблеме резольвент. Собственно говоря, Гильберт формулировал более частную задачу: доказать, что для общего уравнения 7-й степени не существует резольвенты с двумя параметрами. В 1926 г. он доказал [10], что для общего уравнения 9-й степени существует резольвента с четырьмя параметрами. Виман [17] получили более общий результат: общее уравнение степени $n \geqslant 10$ имеет резольвенту с $\leqslant (n-5)$ параметрами. Другие значения числа параметров в проблеме Гильберта указывают, что проблема резольвент в формулировке Гильберта существенно отличается от проблемы Клейна.

При решении своей проблемы Гильберт (и точно так же Виман) пользовался частными свойствами форм определенных степеней, а поэтому его методы не могут быть распространены на уравнения высших степеней. Кроме того, он не задавался целью доказать, что найденные им значения для S являются наименьшими из возможных.

Таким образом, для решения проблемы резольвент Гильберта недоставало общего принципа. Этот принцип невозможно было извлечь из сложной формулировки Гильберта. Мне удалось найти его в 1943 г. [6], поставив более общую проблему резольвент. Для разъяснения сущности этой проблемы пришлось ввести понятие *группы монодромии* уравнения, в коэффициенты которого входит некоторое число, скажем, m, параметров. Пусть эти параметры будут комплексными числами; будем считать их вещественные и мнимые части декартовыми координатами $2m$ мерного пространства, каждая точка которого будет, таким образом, соответствовать системе численных значений параметров. Поэтому каждой точке пространства будет соответствовать n корней нашего уравнения. Если мы будем непрерывно двигать точку, то корни тоже будут непрерывно менять значения. Пусть теперь точка описала в пространстве некоторый замкнутый путь. Поскольку она вернулась в исходное положение, корни *в своей совокупности* вернутся на свои старые места. Это, однако, не означает, что *каждый* из корней вернется в свое старое положение. В общем случае корни претерпят подстановку. Совокупность подстановок, испытываемых корнями при пробеге точкой всевозможных замкнутых путей в пространстве, носит название группы монодромии уравнения. Можно показать, что группа монодромии есть группа Галуа уравнения, если в качестве области рациональности взять поле рациональных функций от параметров. Если уравнение неприводимо, то его группа монодромии транзитивна. Это значит, что, задав любые два корня, соответствующие заданной точке пространства, можно найти такой замкнутый путь, проходящий через эту точку, при обходе которого один заданный корень переместится в другой.

В теории аналитических функций доказана так называемая *теорема монодромии*, обычно приводимая для одной независимой переменной (т. е. для плоскости); но ее без труда можно распространить на любое число независимых переменных. Она состоит в том, что если вообще существуют замкнутые пути, вдоль которых корни уравнения перемещаются, то существуют точки, в любой окрестности которых содержатся замкнутые пути, вдоль которых корни испытывают перемещения. Такого рода точки называются *критическими*. По аналогии с теорией алгебраических чисел, будем называть группой инерции критической точки совокупность подстановок, которые испытывают корни уравнения при обходе точки по всевозможным замкнутым путям, расположенным в окрестности критической точки. Тогда теорему монодромии можно высказать в следующей расширенной формулировке:

Наименьшая группа подстановок, содержащая как подгруппы все группы инерции, соответствующие всевозможным критическим точкам $2m$-мерного пространства, есть группа монодромии.

В силу непрерывности корней уравнения как функций точки пространства при обходе точкой бесконечно малых замкнутых путей корни могут перемещаться только тогда, когда они бесконечно близки. Отсюда следует, что в критических точках некоторые из корней уравнения должны сливаться. Таким образом, мы получим все многообразие критических точек, если приравняем нулю дискриминант уравнения как функцию параметров

$$D(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0. \tag{9}$$

Не исключена возможность, что некоторые из точек, лежащих на многообразии (9), не будут критическими.

Для наших целей необходимо более тонкое различение критических точек. Если в какой-нибудь критической точке сольется только два корня уравнения, то единственным возможным перемещением корней при обходе вблизи этой критической точки будет транспозиция, т. е. перемещение двух близких корней. Это будет наиболее простая из возможных критических точек. Если же в критической точке сольются три корня или две различные пары корней, то при обходе вблизи нее станут возможными различные типы подстановок между корнями. Чем больше корней сливается в критической точке, тем сложнее сама критическая точка, а также соответствующая ей группа инерции. Для решения проблемы резольвент необходимо знать число различных типов критических точек, входящих в критическое многообразие. Для различения этих типов нами был предложен следующий прием. Пусть корни уравнения будут $x_1, x_2, \ldots, x_n$. Составим выражение

$$\prod_S (t_1 x_{\lambda_1} + t_2 x_{\lambda_2} + \ldots + t_n x_{\lambda_n}),$$

в котором будем считать $t_1, t_2, \ldots, t_n$ независимыми переменными, а произведение распространим на все подстановки

$$S = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \lambda_1 & \lambda_2 & \lambda_3 & \ldots & \lambda_n \end{pmatrix}$$

руппы монодромии уравнения. Получится форма (однородный полином) от $t_1, t_2, \ldots, t_n$, коэффициенты которой, как не меняющиеся от подстановок группы монодромии, рационально выражаются через коэффициенты уравнения и, следовательно, через параметры $\alpha_1, \alpha_2, \ldots, \alpha_m$. Обозначим эту форму через

$$\Phi(t_1, t_2, \ldots, t_n). \tag{10}$$

Подставим в нее значения параметров $\alpha_1, \alpha_2, \ldots, \alpha_m$, соответствующие

испытуемой критической точке. Чтобы в ней имели место следующие совпадения корней

$$\begin{aligned} x_1 &= x_2 = \ldots = x_{\mu_1}, \\ x_{\mu_1+1} &= \ldots = x_{\mu_2}, \\ &\ldots\ldots\ldots\ldots \\ x_{\mu_{k-1}+1} &= \ldots = x_n. \end{aligned} \tag{11}$$

необходимо и достаточно, чтобы форма (10) обращалась в нуль, если положить

$$\begin{aligned} t_1 + t_2 + \ldots + t_{\mu_1} &= 0 \\ t_{\mu_1+1} + \ldots + t_{\mu_2} &= 0, \\ &\ldots\ldots\ldots\ldots \\ t_{\mu_{k-1}+1} + \ldots + t_n &= 0. \end{aligned} \tag{12}$$

При этом мы не можем различать равенств (11) от равенств, получаемых из (11) применением к $x_1, x_2, \ldots, x_n$ любой подстановки группы монодромии. Таким образом, если ввести обозначение

$$S = (x_1, x_2, \ldots, x_{\mu_1})(x_{\mu_1+1}, \ldots, x_{\mu_2}) \cdots (x_{\mu_{k-1}+1}, \ldots, x_n),$$

то в случае выполнения равенств (11) мы будем говорить, что наша критическая точка соответствует подстановке S или более высокой подстановке, если, кроме (11), в ней имеются и другие слияния корней. Ограничимся случаем, когда параметры $\alpha_1, \alpha_2, \ldots, \alpha_m$ входят в коэффициенты уравнения линейно. Тогда, если критическая точка соответствует подстановке S, то в ее группу инерции входит подстановка S (или подобные ей), а также более низкие подстановки, т. е. подстановки, которым соответствуют равенства, являющиеся частью равенств (11).

Таким образом, чтобы узнать, соответствует ли данная критическая точка подстановке S (или более высокой), надо к форме Φ применить равенства (12) (например, выражая $t_{\mu_1}, t_{\mu_2}, \ldots, t_n$ через остальные переменные) и проверить, все ли коэффициенты полученной таким образом формы Φ_S обращаются в этой точке в нуль.

Чтобы выяснить, на какие категории подразделяются критические точки в данном уравнении, расположим входящие в нее подстановки по высоте

$$S_1 \subset S_2 \subset \ldots \subset S_q.$$

При этом может случиться, что такой цепочкой не исчерпаются все подстановки группы монодромии. Тогда надо составить всевозможные цепочки.

Приравняем нулю коэффициенты формы Φ_{S_1}; получим многообразие из самых низших критических точек (относительно данной цепочки), а также из высших, соответствующих подстановкам $S_2, \ldots, S_q$. Затем приравняем нулю коэффициенты формы Φ_{S_2}. Может случиться, что

мы не получим новых соотношений между параметрами; это будет означать, что все точки, соответствующие S_1, соответствуют более высокой подстановке S_2 или еще выше. Продолжая делать то же относительно форм $\Phi_{S_2}, \ldots, \Phi_{S_q}$, мы получим ряд критических многообразий, из которых каждое последующее будет содержаться в предыдущем. Каждое из последующих критических многообразий определяется, как это можно доказать, одним дополнительным уравнением между комплексными значениями параметров, т. е. двумя уравнениями между их вещественными и мнимыми частями. Из этого следует, что последовательные критические многообразия, соответствующие подстановкам одной цепочки, имеют соответственно измерения $2m-2$, $2m-4, \ldots$, $2m-2q_1$, где $q_1 \leqslant q$.

Теперь можно формулировать проблему резольвент в более общем и, как нам кажется, в более естественном виде. Пусть даны два уравнения одной и той же степени и пусть коэффициенты второго из них суть функции коэффициентов первого. Тогда замкнутому пути в пространстве, соответствующем первому уравнению, будет соответствовать замкнутый путь в пространстве, соответствующем второму уравнению. Таким образом, подстановки групп монодромии обоих уравнений мы приведем в соответствие, носящее характер изоморфизма: произведению двух подстановок одной группы соответствует произведение подстановок соответствующих множителей второй группы. В частности, критической точке соответствует критическая точка, причем, ввиду соответствия замкнутых путей в их окрестностях, будут подобны их группы инерции, в силу чего обе критические точки должны быть одной и той же высоты. Другими словами, в обоих пространствах устанавливаются цепочки равной длины подстановок и критических многообразий, и тогда критической точке, соответствующей определенному номеру подстановки, в другом пространстве соответствует критическая точка, соответствующая подстановке с тем же номером. При этом учтем, что пространства для обоих уравнений могут быть различных измерений. Однако из того, что в первом уравнении существует q_1 различных категорий критических точек, следует, что во втором уравнении их должно быть также q_1. Поэтому, если мы обозначим через m_2 число параметров в коэффициентах второго уравнения, то

$$2m_2 - 2q_1 \geqslant 0,$$

откуда

$$m_2 \geqslant q_1. \tag{13}$$

Итак, под резольвентой заданного уравнения мы будем разуметь уравнение, коэффициенты которого можно поставить в зависимость от коэффициентов заданного уравнения так, чтобы отдельные корни одного из уравнений были однозначными аналитическими функциями отдельных корней другого уравнения, т. е. чтобы при обходе замкнутых путей в пространствах этих уравнений корни уравнений, при надлежащей

нумерации, испытывали те же подстановки. При этом может случиться, что замкнутым путям в одном пространстве будут соответствовать разомкнутые пути в другом.

Этим не исчерпываются требования, которые мы налагаем на резольвенту: резольвента должна еще содержать в своих коэффициентах возможно меньшее число параметров. Из наших рассуждений относительно критических многообразий вытекает, что число параметров в коэффициентах резольвенты не может быть меньше, чем максимальная длина цепочки подстановок в группе монодромии уравнения, причем, конечно, мы должны выкинуть из цепочки те подстановки, которым не соответствуют критические многообразия, так что это число в наших обозначениях есть q_1, а не q. Можно ли действительно построить резольвенту с q_1 параметрами для *всякого* заданного уравнения, до настоящего времени не удалось решить. Кроме того, до сих пор не выяснен вопрос, что изменится в полученных результатах, если освободиться от требования, чтобы параметры входили в коэффициенты линейно.

Рассмотрим, в виде примера, общее уравнение n-ой степени, в котором будем полагать старший коэффициент равным единице, а остальные считать независимыми переменными. Его группа монодромии есть симметрическая группа; но, присоединив к области рациональности квадратный корень из дискриминанта этого уравнения, мы снизим его группу монодромии до знакопеременной группы, которая, как известно, проста. В знакопеременной группе содержатся следующие цепочки подстановок:

$$(1\,2\,3) \subset (1\,2\,3\,4\,5) \subset (1\,2\,3\,4\,5\,6\,7) \subset \ldots \subset \left(1\ 2\ 3 \ldots 2\left[\frac{n}{2}\right] - (-1)^n\right),$$

где $2\left[\frac{n}{2}\right] - (-1)^n$ есть самое большое нечетное число, не превышающее n. Длина этой цепочки равна

$$\left[\frac{n}{2}\right] - \frac{1 + (-1)^n}{2} = \left[\frac{n-1}{2}\right]. \tag{14}$$

С другой стороны, в знакопеременной группе не содержится цепочек, длина которых превышает число (14). В самом деле, отмечая в каждой подстановке число содержащихся в ней циклов, включая в это число и одночленные циклы (т. е. инвариантные цифры), заметим, что для четной подстановки число имеет ту же четность, что и n. С другой стороны, если, например,

$$S_i \subset S_{i+1},$$

то подстановка S_{i+1} непременно содержит меньшее число циклов, чем S_i. В силу одинаковой четности эти числа должны отличаться по крайней мере на 2. Поэтому числа циклов в подстановках цепочки

$$S_k \supset S_{k-1} \supset \ldots \supset S_2 \supset S_1$$

не могут быть меньше, чем соответственно числа

$$1, 3, 5, \ldots, 2k-1.$$

Но S_1 не может быть ни тождественной подстановкой, ни транспозицией, в силу чего

$$2k-1 \leqslant n-2,$$

откуда

$$k \leqslant \left[\frac{n-1}{2}\right].$$

Таким образом, искомая нижняя граница для числа параметров резольвенты равна

$$S = \left[\frac{n-1}{2}\right]. \tag{15}$$

Сопоставим эти значения с теми, которые были получены Гильбертом для $5 \leqslant$ и $\leqslant 9$:

n	5	6	7	8	9
S [по формуле (15)]	2	2	3	3	4
S (по Гильберту)	1	2	3	4	4

Это сопоставление показывает, что при $n = 5$ введение иррациональных резольвент в самом деле снижает число параметров. Случай же $n = 8$ требует дополнительного исследования. Не исключена возможность, что примененный Гильбертом частный прием нахождения резольвенты не дает минимального числа параметров.

Предложенный способ нахождения числа параметров для резольвент дает перспективу к нахождению решения проблемы резольвент для произвольного n, причем не только для уравнений общего типа, но также всякого конкретно заданного уравнения, у которого коэффициенты являются определенными функциями от параметров.

ЛИТЕРАТУРА

1. Галуа, Сочинения. ОНТИ, 1936.
2. Гаусс. Пятизначные логарифмические таблицы. ГТТИ, 1933.
3. Пржевальский. Пятизначные таблицы логарифмов.
4 Чеботарев. Основы теории Галуа. ОНТИ, 1937.
5. Чеботарев. Теория групп Ли. ОНТИ, 1940.
6. Чеботарев. Проблема резольвент и критические многообразия Изв. АН СССР, серия матем. 1943, т. 7, стр. 123—126; Собр. соч., т. I, стр. 305—326.
7. Abel. Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré. Journ. f. reine u. angew. Math. **1**, 1826; Oeuvres complètes. Christiania. 1881, стр. 66—94.
8. Halphen. Traitè des fonctions elliptiques. T. 3.
9. Hilbert. Mathematische Probleme. Gött. Nachr. 1900, стр. 253—297; Ges. Abh. **3**, 1935, Berlin, стр. 290—329.
10. Hilbert. Ueber die Gleichung neunten Grades. Math. Ann. **97**, 1927, стр. 243—250; Ges. Abh. **2**, 1933, Berlin, стр. 393—400.

11. Klein. Ges. Math. Abh. **2**, 1922, Berlin, стр. 255—504.
12. Tschebotarëw. Ueber ein algebraisches Problem von Herrn Hilbert. I. Math. Ann. **104**, 1931, стр. 459—471; II, **105**, стр. 240—255; Собр. соч., т. I, стр. 255—281.
13. Tschebotarëw. Ueber das Klein-Hilbertsche Resolventenproblem. Bull. Soc. Math. de Kasan. **6**, 1933, N. 3, стр. 5—22; Собр. соч., т. I, стр. 282—304.
14. Tschebotarëw. Ueber irreguläre Darstellungen von halbeinfachen Lieschen Gruppen. Comp. Math. **6**, 1938, стр. 103—117.
15. Weber. Lehrbuch der Algebra, 2. Braunschweig, 1899, стр. 489.
16. Wiman. Ueber die Darstellung der symmetrischen und alternierenden Vertauschungsgruppen usw. Math. Ann. **52**, 1899, стр. 243—270.
17. Wiman. Ueber die Anwendung der Tschirnhausen-Transformation auf die Reduktion algebraischer Gleichungen. Nova Acta R. Sos. Sc. Uppsaliensis, vol. extra ordin. editum, 1927, стр. 3—8.

ИМЕННОЙ УКАЗАТЕЛЬ ПЕРВОГО ТОМА

СОДЕРЖАНИЕ

Печатается по постановлению
Редакционно-издательского совета
Академии Наук СССР

*

Редактор издательства *А. А. Ерофеев*
Технический редактор *А. А. Киселева*
Корректор *В. Е. Посельский*

*

РИСО АН СССР № 3530. А-08745. Издат. № 2057
Тип. заказ № 2310. Подп. к печ. 24/IX 1949 г.
Формат бум. 70×108$^{1}/_{16}$. Печ. л. 21,5+1 вкл.
Уч.-издат. 22. Тираж 2000.
Цена в переплете 22 руб.

2-я тип. Издательства Академии Наук СССР
Москва, Шубинский пер., д. 10