Доклады Академии Наук СССР
1949. Том LXVI, № 3

МАТЕМАТИКА

Е. Л. ЛИТВЕР

О ЧИСЛЕ ИДЕАЛЬНЫХ КЛАССОВ НЕКОТОРЫХ СПЕЦИАЛЬНЫХ ПОЛЕЙ

(Представлено академиком А. Н. Колмогоровым 29 III 1949)

В известной работе Гильберта (1) чисто арифметическим путем выводится формула для числа идеальных классов специального биквадратичного поля Дирихле, найденная впервые Дирихле (2) аналитическим методом. В 1936 г. Lubelski (3) также арифметически получил подобную формулу для некоторых других биквадратичных полей. В 1922 г. Herglotz (4) доказал, что число идеальных классов поля, образованного n квадратными радикалами из рациональных чисел, отличается множителем вида 2^{λ} от произведения чисел классов всех его квадратичных подполей; при этом показатель степени λ им не определяется. Доказательство проводится аналитически, с использованием функционального уравнения Гекке для дзета-функции поля и других трансцендентных средств.

В настоящей статье дается арифметическое доказательство подобной теоремы для более общего случая, а именно, когда к произвольному алгебраическому полю K с одним идеальным классом присоединяются n независимых радикалов степени p (p — простое число) из его чисел

$$\sqrt[p]{\mu_1}, \quad \sqrt[p]{\mu_2}, \ldots, \sqrt[p]{\mu_n}. \tag{1}$$

Обозначим полученное таким образом поле через $K^{(n)}$. Оно содержит всего $p^n - 1$ радикалов степени p, образованных всевозможными произведениями радикалов (1) и их степеней. Поле $K^{(n)}$ имеет всего $\frac{p^n - 1}{p - 1} = m$ различных подполей, каждое из которых образовано одним из этих радикалов. Обозначим эти подполя через K_i, $i = 1, 2, \ldots, m$.

Если α — число поля $K^{(n)}$, то сопряженные с ним числа относительно основного поля K получаются изменением входящих в него радикалов (1) на сопряженные $\omega^t \sqrt[p]{\mu_i}$, где ω — первообразный корень p-й степени из единицы. Обозначим через S_i операцию изменения радикала $\sqrt[p]{\mu_i}$ на $\omega \sqrt[p]{\mu_i}$; тогда все сопряженные с α числа относительно основного поля K получим при помощи последовательного применения операций S_i и их комбинаций. Число всех сопряженных с α чисел будет равно p^n; произведение их дает норму числа α относительно основного поля K.

При помощи только одной операции S_1 получим p сопряженных с α чисел, которые будут всеми сопряженными с α числами относительно поля $K\left(\sqrt[p]{\mu_2}, \ldots, \sqrt[p]{\mu_n}\right) = K^{(n-1)}$, а также сопряженными относительно любого подполя этого поля. При помощи двух операций S_1 и S_2 получим p^2 сопряженных с α чисел, которые будут также всеми сопряженными с α числами относительно подполя $K\left(\sqrt[p]{\mu_3}, \ldots, \sqrt[p]{\mu_n}\right) = K^{(n-2)}$, и т. д. Таким образом при помощи тех же операций S_i можно получить все сопряженные с α числа относительно любого подполя поля $K^{(n)}$. Все сказанное выше относительно числа поля $K^{(n)}$ справедливо и для любого идеала поля $K^{(n)}$.

Обозначим через $\mathfrak{H}$ группу всех идеальных классов поля $K^{(n)}$, а через $\mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_m$ — группы всех идеальных классов его подполей K_i, их порядки обозначим соответственно h и $h_1, h_2, \ldots, h_m$. Идеалы, принадлежащие одному и тому же классу подполя K_i, в поле $K^{(n)}$ будут также принадлежать одному и тому же классу; поэтому каждому идеальному классу подполя K_i можно поставить в соответствие некоторый класс поля $K^{(n)}$, содержащий все его идеалы.

Рассмотрим совокупность всех тех классов подполя K_i, порядок которых не делится на простое число p. Эта совокупность, очевидно, будет группой — некоторой подгруппой группы $\mathfrak{H}_i$. Обозначим ее через $\mathfrak{G}_i$, а порядок ее через g_i.

Нетрудно доказать, что индекс группы $\mathfrak{G}_i$ относительно группы $\mathfrak{H}_i$ будет некоторой степенью простого числа p. Действительно, если группы $\mathfrak{G}_i$ и $\mathfrak{H}_i$ совпадают, то этот индекс равен $1 = p^0$; если эти группы не совпадают, то рассмотрим разложение группы $\mathfrak{H}_i$ по подгруппе $\mathfrak{G}_i$. Пусть будет $\mathfrak{G}_i a$ — произвольный элемент дополнительной группы. Если порядок класса a делится на p^l, то порядок класса a^{p^l} не будет делиться на p, и этот класс будет принадлежать подгруппе $\mathfrak{G}_i$. Элемент же дополнительной группы $\mathfrak{G}_i a$ в степени p^l будет давать единицу дополнительной группы $\mathfrak{G}_i$. Следовательно, порядок каждого элемента дополнительной группы будет некоторой степенью простого числа p, а поэтому и порядок дополнительной группы, равный индексу группы $\mathfrak{G}_i$ относительно группы $\mathfrak{H}_i$, будет также некоторой степенью этого простого числа. Обозначим этот индекс через $p^t i$, тогда будем иметь

$$h_i = p^t i g_i, \quad i = 1, 2, \ldots, m. \tag{2}$$

Обозначим теперь идеальные классы поля K_i из подгруппы $\mathfrak{G}_i$ строчными латинскими буквами с индексом i, а соответствующие им классы поля $K^{(n)}$ одноименными заглавными латинскими буквами с тем же индексом.

Рассмотрим совокупность всевозможных произведений вида:

$$A_1 \cdot A_2 \cdots A_m, \tag{3}$$

где A_i пробегают, независимо одно от другого, классы поля $K^{(n)}$, соответствующие всем классам поля K_i из подгруппы $\mathfrak{G}_i$. Эта совокупность, очевидно, образует группу, которую обозначим через $\mathfrak{G}$.

Докажем, что ее порядок g равен произведению порядков подгрупп $\mathfrak{G}_i$. Для этого достаточно доказать, что все произведения (3) будут

различными. Предположим противное, а именно, что имеет место равенство

$$A_1 \cdot A_2 \cdots A_m = B_1 \cdot B_2 \cdots B_m$$

и, по крайней мере, один класс, например a_1, не равен b_1. Если $\mathfrak{A}$ и $\mathfrak{b}_i$ — идеалы поля K_i соответственно из классов a_i и b_i, то из (4) следует

$$\mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdots \mathfrak{A}_m = \alpha \cdot \mathfrak{b}_1 \cdot \mathfrak{b}_2 \cdots \mathfrak{b}_m, \tag{5}$$

где α — некоторое число поля $K^{(n)}$. Перейдем в равенство (5) к норме относительно подполя K_1. Так как $\mathfrak{A}_1$ и $\mathfrak{b}_1$ — идеалы подполя K_1, то

$$N_1(\mathfrak{A}_1) = \mathfrak{A}_1^{p^{n-1}}, \qquad N_1(\mathfrak{b}_1) = \mathfrak{b}_1^{p^{n-1}}.$$

Что касается норм других идеалов, то для них будем иметь

$$N_1(\mathfrak{A}_i) = [N(\mathfrak{A}_i)]^{p^{n-2}}, \qquad N_1(\mathfrak{b}_i) = [N(\mathfrak{b}_i)]^{p^{n-2}},$$

где $N(\mathfrak{A}_i)$ и $N(\mathfrak{b}_i)$ — нормы идеалов относительно основного поля K, а так как последнее имеет только один класс, то эти нормы, являясь идеалами основного поля, будут его числами. $N_1(\alpha)$ будет числом поля K_1.

Таким образом, в подполе K_1 идеалы $\mathfrak{A}_1^{p^{n-1}}$ и $\mathfrak{b}_1^{p^{n-1}}$ будут эквивалентными и будут равны содержащие их классы этого подполя

$$a_1^{p^{n-1}} = b_1^{p^{n-1}}.$$

Умножив это равенство на $b_1^{-p^{n-1}}$, получим

$$(a_1 b_1^{-1})^{p^{n-1}} = 1.$$

Но $a_1 b_1^{-1}$ принадлежит подгруппе $\mathfrak{G}_1$ и, так как порядок ее элементов не делится на p, то $a_1 b_1^{-1} = 1$ и $a_1 = b_1$, что противоречит нашему предположению. Имея в виду формулы (2), можем написать

$$g = g_1 \cdot g_2 \cdots g_m = \frac{h_1 \cdot h_2 \cdots h_m}{p^{t_1 + t_2 + \cdots + t_m}} = \frac{h_1 \cdot h_2 \cdots h_m}{p^t}. \tag{6}$$

Заставим теперь в произведении (3) каждое A_i пробегать независимо одно от другого классы поля $K^{(n)}$, соответствующие в с е м классам поля K_i (а не только из подгруппы $\mathfrak{G}_i$). Полученная совокупность произведений будет также группой, которую обозначим через $\overline{\mathfrak{G}}$. Выше определенная группа $\mathfrak{G}$ будет ее подгруппой.

Составим прямое произведение абстрактных групп $\mathfrak{H}_i'$, изоморфных группам $\mathfrak{H}_i$. Порядок его будет равен $h_1 \cdot h_2 \cdots h_m$.

Очевидно, это прямое произведение будет гомоморфно группе $\overline{\mathfrak{G}}$ и порядок последней $\bar{g}$ будет делителем порядка прямого произведения, равного

$$h_1 \cdot h_2 \cdots h_m = p^t \cdot g_1 \cdot g_2 \cdots g_m = p^t \cdot g.$$

Так как группа $\overline{\mathfrak{G}}$ имеет подгруппу $\mathfrak{G}$ порядка g, то ее порядок $\bar{g}$ будет отличаться от g множителем вида p^v.

Докажем теперь, что любой класс поля $K^{(n)}$ в степени p^{n-1} будет принадлежать группе $\overline{\mathfrak{G}}$. Для этого достаточно доказать, что любой идеал $\mathfrak{A}$ поля $K^{(n)}$ в степени p^{n-1} эквивалентен произведению идеалов из подполей K_i.

Поле $K^{(n)}$ имеет всего $p+1$ различных подполей вида $K^{(n-1)} = K\left(\sqrt[p]{\mu_1^t \mu_2^r}, K^{(n-2)}\right)$, где $K^{(n-2)} = K\left(\sqrt[p]{\mu_3}, \ldots, \sqrt[p]{\mu_n}\right)$. Норма идеала $\mathfrak{A}$ относительно каждого из подполей $K^{(n-1)}$, равная произведению всех p сопряженных с $\mathfrak{A}$ идеалов относительно этого поля, будет его идеалом. Заметим, что все эти сопряженные с $\mathfrak{A}$ идеалы относительно полей $K^{(n-1)}$ будут сопряженными, и притом всеми сопряженными, и относительно поля $K^{(n-2)}$. Перемножим все эти $p+1$ норм. В этом произведении $p+1$ раз встретится идеал $\mathfrak{A}$ и, кроме него, будут все p^2-1 других сопряженных с ним идеалов относительно поля $K^{(n-2)}$. Таким образом, в результате перемножения норм, с одной стороны, будем иметь произведение $\mathfrak{A}^p$ на норму идеала $\mathfrak{A}$ относительно поля $K^{(n-2)}$, а с другой стороны, будем иметь произведение $p+1$ идеалов из подполей $K^{(n-1)}$. Норма идеала $\mathfrak{A}$ относительно поля $K^{(n-2)}$ будет идеалом этого поля, который можно считать и идеалом любого поля $K^{(n-1)}$. Из всего этого следует, что идеал $\mathfrak{A}^p$ эквивалентен произведению идеалов из подполей $K^{(n-1)}$. Повторив эти рассуждения $n-1$ раз, получим, что идеал $\mathfrak{A}^{p^{n-1}}$ эквивалентен произведению идеалов из подполей K_i. Итак, p^{n-1} степень любого класса из группы $\mathfrak{H}$ всех классов поля $K^{(n)}$ попадает в подгруппу $\overline{\mathfrak{G}}$.

Докажем, что индекс группы $\overline{\mathfrak{G}}$ относительно группы $\mathfrak{H}$ будет некоторой степенью простого числа p. Если группы $\overline{\mathfrak{G}}$ и $\mathfrak{H}$ совпадают, то индекс равен $1 = p^0$. Если эти группы не совпадают, то разложим группу $\mathfrak{H}$ по подгруппе $\overline{\mathfrak{G}}$. Так как все классы группы $\mathfrak{H}$ в степени p^{n-1} принадлежат подгруппе $\overline{\mathfrak{G}}$, то порядок всех элементов дополнительной группы будет некоторой степенью простого числа p, а следовательно, и порядок дополнительной группы, равный индексу группы $\overline{\mathfrak{G}}$ относительно группы $\mathfrak{H}$, будет также некоторой степенью простого числа p.

Сопоставляя это с ранее доказанным относительно порядков групп $\mathfrak{G}$ и $\overline{\mathfrak{G}}$, убеждаемся в справедливости теоремы:

Теорема. *Число идеальных классов поля, образованного присоединением к произвольному алгебраическому полю с одним идеальным классом n радикалов степени p (p — простое число) из его чисел, отличается множителем вида p^λ от произведения чисел идеальных классов всех его подполей, каждое из которых образовано одним радикалом.*

Поступило
19 III 1949

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] D. Hilbert, Math. Ann., 45, (1894). [2] G. Legeune Dirichlet, Recherches sur les formes quadratiques à coefficients et à indéterminées complexes, Werke, 1, 625, 1889. [3] S. Lubelski, J. f. Math., 174, 160 (1936). [4] G. Herglotz, Math. Z., 12, 255 (1922).