

IGOR R. ŠAFAREVIČ

Extensions à points de ramification donnés (en russe)

Publications mathématiques de l'I.H.É.S., tome 18 (1963), p. 71-92

http://www.numdam.org/item?id=PMIHES_1963__18__71_0

© Publications mathématiques de l'I.H.É.S., 1963, tous droits réservés.

L'accès aux archives de la revue « Publications mathématiques de l'I.H.É.S. » (<http://www.ihes.fr/IHES/Publications/Publications.html>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

РАСШИРЕНИЯ С ЗАДАНЫМИ ТОЧКАМИ ВЕТВЛЕНИЯ

И. Р. ШАФАРЕВИЧ

В этой работе исследуются алгебраические расширения K/k поля алгебраических чисел k с заданными точками ветвления. Такая постановка вопроса подсказывается аналогией с теорией римановых поверхностей. Расширения с коммутативной группой Галуа рассматриваются в теории полей классов. Мы рассматриваем расширения, группы Галуа которых являются l -группами, т. е. имеют порядок вида l^{α} , где l —некоторое фиксированное простое число.

Фиксируем конечное множество S простых дивизоров поля k и рассмотрим максимальное l -расширение K_S , разветвленное только в простых дивизорах $p \in S$. Группа Галуа расширения K_S/k обозначается через $\mathfrak{G}_S$. Она является l -группой конечной или топологической. В § 1 определяется минимальное число образующих группы $\mathfrak{G}_S$. Основной целью является определение минимального числа соотношений, связывающих эти образующие. В § 2 выясняется, что этот вопрос связан с условиями разрешимости некоторых задач погружения арифметического характера. В § 4 дается оценка числа соотношений при помощи рассмотрения арифметических инвариантов, введенных в § 3. На основании этой оценки удается в некоторых случаях найти в явном виде группу $\mathfrak{G}_S$.

Если все простые дивизоры множества S не делят l , то доказывается, что разность между числом соотношений и числом образующих группы $\mathfrak{G}_S$ не превосходит числа образующих группы единиц поля k . Во всяком случае, эта разность ограничена, если рассматривать поля ограниченной степени над полем рациональных чисел $\mathbb{R}$.

Очень интересным является вопрос о конечности групп $\mathfrak{G}_S$ (если простые дивизоры из S не делят l). Из теории полей классов следует, что факторы ряда коммутантов групп $\mathfrak{G}_S$ конечны. Таким образом, вопрос о конечности равносильно вопросу об обрыве этого ряда. Если множество пусто, то этот вопрос совпадает с известной проблемой башни полей классов, а в общем случае является ее естественным обобщением. В связи с результатами, о которых было сказано выше, этот вопрос приводит к новым вопросам о конечных l -группах. Эти вопросы обсуждаются в § 6. Во всяком случае, удастся доказать, что длина ряда коммутантов группы $\mathfrak{G}_S$ неограниченно возрастает, если число образующих этой группы стремится к бесконечности. В частности, число этажей башни полей классов поля k неограниченно растет вместе с числом образующих группы

классов поля k , если мы рассматриваем поля ограниченной степени над R .

В заключение я хочу выразить свою благодарность референту, который очень внимательно прочитал рукопись этой работы и сделал ряд полезных замечаний.

§ 1. ЧИСЛО ОБРАЗУЮЩИХ

В этом параграфе мы выведем формулу для минимального числа образующих $d(S)$ группы Галуа $\mathfrak{G}_S$ поля K_S/k —максимального l —расширения поля алгебраических чисел k , разветвленного только в простых дивизорах множества $S = \{p_1, \dots, p_s\}$.

Мы будем считать, что множество S не содержит комплексных бесконечных простых дивизоров. Это не является существенным ограничением, так как всякий комплексный простой дивизор неразветвлен.

Согласно теореме Бернсайда ([1]), $d(S)$ совпадает с минимальным числом образующих группы $\mathfrak{G}_S/\mathfrak{G}_S^{(l)}$, $\mathfrak{G}_S^{(l)} = \mathfrak{G}_S^l(\mathfrak{G}_S, \mathfrak{G}_S)$. К подгруппе $\mathfrak{G}_S^{(l)}$ принадлежит подполе $K_S^{(l)} \subset K_S$, которое является, очевидно, максимальным абелевым расширением периода l поля k , разветвленным только в простых дивизорах $p \in S$. Ввиду этого, определение числа $d(S)$ сводится к вопросу об абелевых расширениях. Этот вопрос может быть решен на основании теории полей классов при помощи стандартных рассуждений.

Мы будем пользоваться теорией полей классов в форме, использующей понятие иделей [2].

Выпишем основные обозначения, которыми мы будем пользоваться (они по возможности согласованы с обозначениями в [2]).

J (или J_k) — группа иделей поля k

a_p — p -компонента идея a

k — группа главных иделей и также мультипликативная группа поля k

$\mathcal{U}_p$ — группа единиц p -адического замыкания k_p поля k

$$\mathcal{U}_S = \{a \mid a_q \in \mathcal{U}_q, a_p = 1 \text{ для } p \in S\}.$$

Если множество S пусто, то $\mathcal{U}_S$ обозначается через $\mathcal{U}$ — это группа единичных иделей.

$$V_S = \{\alpha \in k \mid (\alpha) = a^l, \alpha \in k_p^l \text{ для } p \in S\}$$

(α) — главный дивизор числа α .

Очевидно, что $V_S = \mathcal{U}_S J^l \cap k$.

Если множество S пусто, то V_S обозначается через V — это группа сингулярных чисел [3].

Очевидно, что $V_S \supset k^l$ и V_S/k^l является конечной группой периода l , т. е. конечномерным векторным пространством над полем Z_l из l элементов; положим

$$\sigma(S) = \dim_{Z_l} (V_S/k^l),$$

r — число образующих бесконечного порядка группы единиц поля k :
 $r = r_1 + r_2 - 1$ где r_1 — число вещественных и r_2 — комплексных бесконечных простых дивизоров поля k .

γ — ранг l -компоненты группы классов дивизоров поля k .

ζ — первообразный корень степени l из 1.

Теорема 1. Число образующих $d(S)$ группы $\mathfrak{G}_S$ определяется формулой:

$$d(S) = t(S) + \lambda(S) + \sigma(S) - r - \delta, \quad (1)$$

где $t(S)$ — число тех простых дивизоров $p \in S$, для которых $\zeta \in k_p$,

$$\lambda(S) = \sum_{p|l, p \in S} n(p), \quad n(p) = [k_p : \mathbb{R}_p], \quad p|p$$

и δ полагается равным 0, если $\zeta \notin k$ и 1, если $\zeta \in k$.

Доказательство. Пусть K — абелево расширение поля k и B — соответствующая ему подгруппа группы J . Простой дивизор p тогда и только тогда неразветвлен в K , когда $\mathcal{U}_p \subset B$ ([2] теорема 3 гл. 8). Отсюда легко следует, что полю $K_S^{(1)}$ соответствует подгруппа $\mathcal{U}_S J' k$ и

$$d(S) = \dim_{\mathbb{Z}_l} J / \mathcal{U}_S \cdot J' \cdot k.$$

Положим

$$H_S = J / \mathcal{U}_S \cdot J' \cdot k$$

и если множество S пусто, то обозначим группу H_S через H .

Рассмотрим последовательность групп и гомоморфизмов:

$$(1) \rightarrow V_S / k^l \xrightarrow{f_1} V / k^l \xrightarrow{f_2} \mathcal{U} / \mathcal{U}_S \mathcal{U}' \xrightarrow{f_3} H_S \xrightarrow{f_4} H \rightarrow (1). \quad (2)$$

Гомоморфизмы f_i ($i=1, 2, 3, 4$) определяются следующим образом:

f_1 — естественное отображение группы на факторгруппу

$$H = H_S / (\mathcal{U} \cdot J' \cdot k / \mathcal{U}_S J' k)$$

$$f_2(a) = a \mathcal{U}_S J' k, \quad a \in \mathcal{U}$$

f_4 — естественное вложение, так как очевидно, что $V_S \subset V$.

Для определения гомоморфизма f_3 заметим, что число α принадлежит V_S тогда и только тогда, когда существует такой идеаль a , что $\alpha a^{-1} \in \mathcal{U}$. Положим

$$f_3(\alpha) = \alpha a^{-1} \mathcal{U}_S \mathcal{U}'$$

для любого выбора такого идеала a . От этого выбора $f_3(\alpha)$ не зависит, так как если

$$\alpha a_1^{-1} \in \mathcal{U}, \quad \text{то} \quad \alpha a_1^{-1} = \alpha a^{-1} i, \quad \text{где} \quad i = (a_1/a)^l \in \mathcal{U}^l.$$

Мы проверим сейчас, что последовательность (2) — точна.

Действительно, $\text{Im } f_1 = H$ и т. к. $H = J / J' k$, то

$$\text{Ker } f_1 = \mathcal{U} \cdot J' \cdot k / \mathcal{U}_S \cdot J' \cdot k = \text{Im } f_2$$

$$\text{Ker } f_2 = \{i \mathcal{U}_S \mathcal{U}' \mid i \in \mathcal{U}, i = a^l b_S \alpha, a \in J, b_S \in \mathcal{U}_S, \alpha \in k\}$$

и т. к. отсюда следует, что $\alpha \in V$, то

$$\text{Ker } f_2 = \text{Im } f_3$$

Наконец,

$$\text{Ker } f_3 = \{\alpha \mid \alpha \in V, \alpha \in J^l \mathcal{U}_S\} = \text{Im } f_4$$

и

$$\text{Ker } f_4 = 1$$

Из точности последовательности (2) следует, что

$$\dim_{Z_l} H - \dim_{Z_l} H_S + \dim_{Z_l} \mathcal{U}/\mathcal{U}_S \mathcal{U}^l - \dim_{Z_l} V/k^l + \dim_{Z_l} V_S/k^l = 0. \quad (3)$$

При этом по определению

$$\dim_{Z_l} H = \gamma, \quad \dim_{Z_l} H_S = d(S), \quad \dim_{Z_l} V_S/k^l = \sigma(S). \quad (4)$$

Кроме того,

$$\dim_{Z_l} \mathcal{U}/\mathcal{U}_S \mathcal{U}^l = \dim_{Z_l} \prod_{p \in S} \mathcal{U}_p/\mathcal{U}_p^l = \sum_{p \in S} \dim_{Z_l} \mathcal{U}_p/\mathcal{U}_p^l.$$

Как известно, (см., например, [4] теорема 11.3).

$$\dim_{Z_l} \mathcal{U}_p/\mathcal{U}_p^l = \begin{cases} 0, & \text{если } p \nmid l, \zeta \notin k_p, \\ 1, & \text{если } p \nmid l, \zeta \in k_p, \\ n(p), & \text{если } p \mid l, \zeta \notin k_p, \\ n(p) + 1, & \text{если } p \mid l, \zeta \in k_p. \end{cases} \quad (5)$$

Отсюда следует, что

$$\sum_{p \in S} \dim_{Z_l} \mathcal{U}_p/\mathcal{U}_p^l = t(S) + \lambda(S).$$

Наконец

$$\dim_{Z_l} V/k^l = \gamma + r + \delta. \quad (6)$$

Действительно, для $\alpha \in V$ по условию $(\alpha) = \alpha^l$ и отображение $\varphi_1: \alpha \rightarrow \alpha$ определяет изоморфизм группы V на группу H_1 , состоящую из элементов периода l в группе классов дивизоров поля k . Очевидно, что $\dim_{Z_l} H_1 = \dim_{Z_l} H$. Мы имеем точную последовательность:

$$(1) \rightarrow E/E^l \xrightarrow{\varphi_1} V/k^l \xrightarrow{\varphi_1} H \rightarrow (1),$$

где E — группа единиц поля k и для $(\epsilon) \in E$, $\varphi_2(\epsilon) = \epsilon k^l$.

Так как $\dim_{Z_l} E/E^l = r + \delta$, то отсюда и следует (6).

Подставляя (4) — (6) в (3), мы получаем, что

$$d(S) = \gamma + t(S) + \lambda(S) - (\gamma + r + \delta) + \sigma(S) = t(S) + \lambda(S) + \sigma(S) - r - \delta.$$

Теорема 1 доказана.

§ 2. ЧИСЛО СООТНОШЕНИЙ И ЗАДАЧА ПОГРУЖЕНИЯ

В этом параграфе мы рассмотрим произвольное поле k и его (конечное или бесконечное) l —расширение K . Таким образом, K/k сепарабельно и нормально, и его группа Галуа $\mathfrak{G}$ является l —группой — конечной или топологической. Мы изложим общий прием для подсчета минимального числа соотношений в группе $\mathfrak{G}$, сводящий эту задачу к некоторой задаче погружения. В частном случае, когда k —поле p —адических чисел, $\zeta \in k$ и K —максимальное p —расширение поля k , аналогичный прием был применен в работе [5]. Рассуждения этого параграфа являются обобщениями рассуждений этой работы.

Пусть $\mathfrak{G}$ —конечная или топологическая нульмерная бикомпактная l —группа. Таким образом, $\mathfrak{G}$ является проективным пределом конечных l —групп:

$$\mathfrak{G} = \varprojlim G_\alpha. \quad (7)$$

Обозначим через $\mathfrak{F}$ свободную топологическую l —группу, гомоморфным образом которой является группа $\mathfrak{G}$:

$$\mathfrak{G} = \mathfrak{F}/\mathfrak{N}. \quad (8)$$

Мы будем предполагать, что минимальная система образующих $\mathfrak{F}$ отображается в минимальную систему образующих $\mathfrak{G}$. Согласно уже цитированной теореме Бернсайда, это означает, что проистекший из представления (8) гомоморфизм $\mathfrak{F} \rightarrow \mathfrak{G}$ определяет изоморфизм групп $\mathfrak{F}/\mathfrak{F}_1$, и $\mathfrak{G}/\mathfrak{G}_1$, где $\mathfrak{F}_1 = \mathfrak{F}'(\mathfrak{F}, \mathfrak{F})$, $\mathfrak{G}_1 = \mathfrak{G}'(\mathfrak{G}, \mathfrak{G})$. Иначе говоря, это значит, что $\mathfrak{N} \subset \mathfrak{F}_1$.

Минимальное число соотношений группы $\mathfrak{G}$ равно минимальному числу образующих нормального делителя $\mathfrak{N}$, как $\mathfrak{F}$ —операторной группы. Это последнее число равно минимальному числу образующих абелевой (не операторной) группы $\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}'$ — доказательство этого факта дословно повторяет доказательство теоремы Бернсайда. Таким образом, если $r(\mathfrak{G})$ — минимальное число соотношений в группе $\mathfrak{G}$, то

$$r(\mathfrak{G}) = \dim_{Z_l} \mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}'.$$

Мы понимаем здесь размерность, как мощность базиса топологического векторного пространства, однако во всех интересных случаях это число будет конечным.

Обозначим через $E(\mathfrak{G})$ группу (которую более подробно обозначают через $\text{Ext}(\mathfrak{G}, Z_l)$ см., например [6] гл. XI) всех расширений группы $\mathfrak{G}$ при помощи Z_l . Конечно, $E(\mathfrak{G}) = H^2(\mathfrak{G}, Z_l)$, но в дальнейшем эта группа будет нам встречаться именно как группа расширений, а не как группа гомологий. Рассмотрим группу

$$\widehat{\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}'} = \text{Hom}(\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}', Z_l).$$

Очевидно, что последовательность

$$(1) \rightarrow \mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^i \rightarrow \mathfrak{F}/\mathfrak{N}, \mathfrak{F})\mathfrak{N}^i \rightarrow \mathfrak{G} \rightarrow (1)$$

определяет некоторое расширение Θ группы $\mathfrak{G}$ при помощи $\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^i$, т. е. элемент

$$\Theta \in \text{Ext}(\mathfrak{G}, \mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^i).$$

Гомоморфизм $\varphi \in \text{Hom}(\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^i, Z_l)$ переводит этот элемент в

$$\varphi\Theta \in E(\mathfrak{G}).$$

Таким путем определяется отображение

$$\xi : \widehat{\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^i} \rightarrow E(\mathfrak{G}), \quad \xi(\varphi) = \varphi\Theta. \quad (9)$$

Легко проверить, что это отображение является изоморфизмом (в терминах групп гомологий это следует из « второй редукционной теоремы » [7]).

Таким образом,

$$r(\mathfrak{G}) = \dim_{Z_l} E(\mathfrak{G}).$$

Воспользуемся представлением (7) группы $\mathfrak{G}$. Каждому гомоморфизму

$$\varphi_{\alpha, \beta} : G_{\alpha} \rightarrow G_{\beta}$$

соответствует гомоморфизм

$$E(\varphi_{\alpha, \beta}) : E(G_{\beta}) \rightarrow E(G_{\alpha})$$

и

$$E(\mathfrak{G}) = \varinjlim E(G_{\alpha}).$$

Каждая группа G_{α} является гомоморфным образом группы $\mathfrak{G}$ и гомоморфизму

$$\varphi_{\alpha} : \mathfrak{G} \rightarrow G_{\alpha}$$

соответствует гомоморфизм

$$\psi_{\alpha} = E(\varphi_{\alpha}) : E(G_{\alpha}) \rightarrow E(\mathfrak{G}).$$

Группа $E(\mathfrak{G})$ является объединением спектра своих подгрупп $\psi_{\alpha} E(G_{\alpha})$ и поэтому

$$r(\mathfrak{G}) = \sup \dim_{Z_l} \psi_{\alpha} E(G_{\alpha}).$$

Если мы положим

$$\text{Ker } \psi_{\alpha} = E(G_{\alpha})^0,$$

то получим, что

$$r(\mathfrak{G}) = \sup \dim_{Z_l} E(G_{\alpha})/E(G_{\alpha})^0.$$

Выясним, каков смысл того, что элемент $\theta \in E(G_{\alpha})$ содержится в $E(G_{\alpha})^0$. Для этого заметим, что если $\mathfrak{N}_{\alpha} = \text{Ker } \varphi_{\alpha}$, то последовательность

$$(1) \rightarrow \mathfrak{N}_{\alpha}/(\mathfrak{N}_{\alpha}, \mathfrak{G})\mathfrak{N}_{\alpha}^i \rightarrow \mathfrak{G}/(\mathfrak{N}_{\alpha}, \mathfrak{G})\mathfrak{N}_{\alpha}^i \rightarrow G_{\alpha} \rightarrow (1)$$

определяет элемент $\Theta \in \text{Ext}(G_{\alpha}, \mathfrak{N}_{\alpha}/(\mathfrak{N}_{\alpha}, \mathfrak{G})\mathfrak{N}_{\alpha}^i)$. Всякий гомоморфизм

$$\varphi \in \widehat{\mathfrak{N}_{\alpha}/(\mathfrak{N}_{\alpha}, \mathfrak{G})\mathfrak{N}_{\alpha}^i} = \text{Hom}(\mathfrak{N}_{\alpha}/(\mathfrak{N}_{\alpha}, \mathfrak{G})\mathfrak{N}_{\alpha}^i, Z_l)$$

определяет элемент

$$\varphi\Theta \in \text{Ext}(G_\alpha, Z_i) = E(G_\alpha).$$

Полученный элемент $\varphi\Theta$ содержится в $E(G_\alpha)^0$. Это легко проверить, или явно строя этот элемент, или используя точную гомологическую последовательность с некоммутативным коэффициентом. Более того, так же просто проверяется, что

$$E(G_\alpha)^0 = \text{Im } \xi, \xi(\varphi) = \varphi\Theta.$$

(это утверждение является непосредственным обобщением утверждения об изоморфном характере отображения ξ в (9), так как в том случае $E(G_\alpha)^0 = 0$, ибо $E(\mathfrak{F}) = 0$).

Рассмотрим подполе K_α поля K , принадлежащее подгруппе G_α группы $\mathfrak{G}$. Если θ —элемент группы $E(G_\alpha)$, содержащийся в $E(G_\alpha)^0$, то по сказанному выше

$$\theta = \xi(\varphi), \varphi \in \mathfrak{N}_\alpha / (\mathfrak{N}_\alpha, \mathfrak{G}) \mathfrak{N}_\alpha^l.$$

Обозначим через $\mathfrak{N}_\theta$ прообраз группы $\text{Ker } \varphi$ при гомоморфизме

$$\mathfrak{N}_\alpha \rightarrow \mathfrak{N}_\alpha / (\mathfrak{N}_\alpha, \mathfrak{G}) \mathfrak{N}_\alpha^l$$

и через K_θ —соответствующее ей подполе поля K . Очевидно, что

$$k \subset K_\alpha \subset K_\theta \subset K.$$

Если G_θ —группа Галуа поля K_θ/k , а $\mathfrak{z}$ —поля K_θ/K_α , то мы имеем точную последовательность

$$(1) \rightarrow \mathfrak{z} \rightarrow G_\theta \rightarrow G_\alpha \rightarrow (1)$$

и φ определяет вложение $\mathfrak{z}$ в Z_i . Таким образом, G_θ определяет элемент группы $E(G_\alpha)$, причем φ переводит этот элемент в θ .

Вообще, пусть $\theta \in E(\bar{G})$, где $\bar{G}$ —группа Галуа некоторого нормального расширения $\bar{K}/k$.

Задачей погружения, соответствующей θ , называется вопрос о существовании такого нормального расширения $\bar{K}$

$$k \subset \bar{K} \subset \bar{\bar{K}}$$

и такого вложения φ группы Галуа $G(K/\bar{K})$ в Z_i , что

$$\theta = \varphi\bar{\theta},$$

где $\bar{\theta}$ —тот элемент из $E(\bar{G})$, который соответствует естественной точной последовательности

$$(1) \rightarrow G(\bar{\bar{K}}/\bar{K}) \rightarrow G(\bar{\bar{K}}/k) \rightarrow \bar{G} \rightarrow (1).$$

Мы будем говорить о K —задаче погружения, если фиксировано расширение K/k и требуется найти $\bar{K}$ как подполе поля K .

Все предшествующие рассуждения приводят к такому результату:

Теорема 2. Если $\mathfrak{G}$ — группа Галуа некоторого l — расширения K поля k , то

$$r(\mathfrak{G}) = \sup_{\alpha} \dim_{Z_l} E(G_{\alpha})/E(G_{\alpha})^0,$$

где G_{α} пробегает все конечные факторгруппы группы $\mathfrak{G}$, а группа $E(G_{\alpha})^0$ — состоит из элементов группы $E(G)$, соответствующая которым K — задача погружения разрешима.

Очевидно, что $\dim_{Z_l} E(G_{\alpha})/E(G_{\alpha})^0$ можно интерпретировать как число условий, которые должны выполняться чтобы задача погружения была разрешима.

§ 3. НЕКОТОРЫЕ АРИФМЕТИЧЕСКИЕ ИНВАРИАНТЫ РАСШИРЕНИЙ

Мы выясним теперь, в чем заключаются условия разрешимости той задачи погружения, которая была сформулирована в предшествующем параграфе в случае, когда k — поле алгебраических чисел.

Рассмотрим всевозможные расширения $\bar{K}$ произвольного поля K , имеющие над K группу Галуа, изоморфную Z_l или 1 . Мы будем включать в термин « расширения » несколько более обильную структуру, чем обычно, рассматривая пару, состоящую из поля $\bar{K}$ и изоморфного вложения его группы Галуа над K в Z_l . Иначе говоря, можно считать, что мы фиксируем поле $\bar{K}$ и элемент группы $\text{Hom}(G(\bar{K}/K), Z_l)$. Этот элемент можно рассматривать и как элемент группы $\text{Hom}(\alpha_K, Z_l)$, где α_K — группа Галуа максимального абелева расширения поля K . Наоборот, каждый элемент χ группы $\hat{\alpha}_K = \text{Hom}(\alpha_K, Z_l)$ определяет некоторое поле — то, которое соответствует подгруппе $\text{Ker } \chi$ группы α_K и гомоморфизм группы Галуа этого поля в Z_l . Таким образом, « расширения », в смысле этой новой структуры, совпадают с элементами группы $\hat{\alpha}_K = \text{Hom}(\alpha_K, Z_l)$. Такая трактовка имеется, например, еще в работе [8]. Нам важно сейчас, что групповая операция переносится, таким образом, с группы $\alpha_K = \text{Hom}(\alpha_K, Z_l)$ на множество расширений поля K с группой изоморфной Z_l или 1 . Результат применения этой операции к расширениям $\bar{K}$ и $\bar{K}$ мы будем обозначать через $\bar{K} \circ \bar{K}$.

Предположим теперь, что поле K нормально над некоторым полем k и имеет над ним группу Галуа G .

Группа Галуа каждого расширения $\bar{K}$ поля K нормального над k , определяет элемент $\xi \in E(G)$. Выясним для случая числовых полей, когда наоборот, для элемента $\xi \in E(G)$ существует соответствующее расширение $\bar{K}$ или, другими словами, когда задача погружения, соответствующая элементу ξ и полю K разрешима. Мы будем дальше называть ее задачей погружения (K, ξ) .

Для любого простого дивизора $\mathfrak{p}$ поля k обозначим через $K_{\mathfrak{p}}$ алгебру $K \otimes_{k_{\mathfrak{p}}} k_{\mathfrak{p}} = \prod_{\mathfrak{p} | \mathfrak{p}} K_{\mathfrak{p}}$. Эта алгебра имеет над полем $k_{\mathfrak{p}}$ группу Галуа G . Имеет место следующий результат:

Задача погружения (K, ξ) разрешима тогда и только тогда, когда для любого простого дивизора p поля k разрешима задача погружения (K_p, ξ) . При этом, если $\zeta \in k$, то из разрешимости задачи погружения для всех p , кроме одного, следует ее разрешимость для этого одного p (см. [9] или [10]).

По поводу разрешимости задачи погружения для алгебр K_p известно следующее:

1. Если алгебра K_p неразветвлена над k_p (т. е. все поля K_p/k_p , $\mathbb{P}|p$ неразветвлены), то задача погружения всегда разрешима, причем даже имеет решение Σ_p , являющееся неразветвленной алгеброй [9].

2. Если $\zeta \notin k_p$, то задача погружения всегда разрешима. Напомним, что мы считаем G , как и в §§ 1-2, l —группой. Для $p \nmid l$ это следует из того, что при сделанных предположениях K_p неразветвлено. При $p|l$ утверждение доказано в [11].

3. Если $\zeta \in k_p$, то существует такой элемент χ группы $\text{Hom}(E(G), Z_l)$ что равенство $\chi(\xi) = 1$ необходимо и достаточно для разрешимости задачи погружения ([12] и [4]).

Предположим, теперь, что K/k разветвлено только в простых дивизорах фиксированного множества S . Обозначим через $\widetilde{E(G)}$ подгруппу тех элементов группы $E(G)$, соответствующие которым задачи погружения разрешимы. Из сформулированных результатов вытекает:

Теорема 3. *Существуют такие $m = t(S) - \delta$ элементов $\chi_1, \dots, \chi_m$ группы $\text{Hom}(E(G), Z_l)$, что $\xi \in \widetilde{E(G)}$ тогда и только тогда, когда $\chi_1(\xi) = 1, \dots, \chi_m(\xi) = 1$. Здесь, как и в § 1, $t(S)$ обозначает число таких $p \in S$, что $\zeta \in k_p$, а $\delta = 0$, если $\zeta \notin k$ и $\delta = 1$, если $\zeta \in k$. Если $\delta = 1$ и $S = \emptyset$, надо положить $m = 0$.*

Выясним теперь, когда решение задачи погружения можно выбрать в виде расширения $\bar{K}/k$, разветвленного только в простых дивизорах множества S .

Для этого напомним, как выражаются все решения задачи погружения через одно из них. Обозначим через $\bar{k}$ произвольное расширение поля k с группой Галуа, изоморфной Z_l или 1 . Расширение $K_0 = K \cdot \bar{k}$ поля мы будем называть тривиальным. Имеет место следующий результат:

4. Если $\bar{K}$ —одно решение задачи погружения, то любое другое решение имеет вид $\bar{K} = \bar{K}_0 K_0$, где K_0 —тривиальное расширение ([9] и [10]).

Пусть p такой простой дивизор поля k , что алгебра K_p неразветвлена. Тогда задача погружения (K_p, ξ) имеет неразветвленное решение (утверждение 1). Обозначим его через Σ_p . Пусть $\bar{K}$ —некоторое решение задачи погружения (K, ξ) . Тогда $\bar{K}_p = \Sigma_p \circ K_0$ где $K_0 = K_p \cdot \bar{k}_p$ —тривиальное расширение, а $\bar{k}_p/k_p$ —расширение с группой Галуа, изоморфной Z_l или 1 (утверждение 4). Как всякое расширение поля k_p , $\bar{k}_p$ соответствует элементу φ группы $\text{Hom}(a_{K_p}, Z_l)$. Согласно локальной теории полей классов $\text{Hom}(a_{K_p}, Z_l) = \text{Hom}(k_p, Z_l) = \hat{k}_p$. Поэтому, мы можем считать, что $\varphi \in \hat{k}_p$. С другой стороны, само неразветвленное расширение

определено неоднозначно, а (согласно утверждению 4) с точностью до замены $\Sigma_p \rightarrow \Sigma_p \circ \Sigma_0$, где $\Sigma_0 = K_p \cdot \kappa$, а κ/k_p — неразветвленное расширение поля k_p , группа Галуа которого изоморфна Z_i или 1. Такому расширению соответствует элемент $\varphi_0 \in \hat{K}_p$, обладающий свойством $\varphi_0|_{U_p} = 1$.

Мы видим, что φ определен с точностью до множителя такого типа. Иными словами, однозначно определен характер $\psi \in \text{Hom}(U_p, Z_i) = \hat{U}_p$. Мы получили следующий результат.

Лемма. *Каждому решению $\bar{K}$ задачи погружения (K, ξ) и неразветвленному в K простому дивизору p поля k соответствует элемент ψ группы $\hat{U}_p$. Равенство $\psi = 1$ необходимо и достаточно для того, чтобы p было неразветвлено и в $\bar{K}$.*

Пусть K разветвлено только в простых дивизорах множества S , $p \notin S$ и $\bar{K}$ — некоторое решение задачи погружения. Ему соответствует элемент $\psi \in \hat{U}_p$, который мы обозначим через ψ_p . Так как $\bar{K}$ имеет только конечное число точек ветвления, то $\psi_p = 1$ для почти всех p . Набор всех ψ_p можно, следовательно, рассматривать как элемент ψ группы $\prod_{p \notin S} \hat{U}_p = \hat{U}_S$. Любое другое решение той же задачи погружения имеет вид $\bar{K} \circ K_0$, где $K_0 = K \cdot \bar{k}$, а $\bar{k}/k$ — циклическое расширение поля k , т. е. соответствует, согласно теории полей классов элементу группы $\text{Hom}(J/k, Z_i) = \hat{J}/k$. Если $\bar{\psi} \in \hat{J}/k$, то соответствующие $\bar{\psi}_p \in \hat{U}_p$ получаются, очевидно, из вложения $U_p \rightarrow J/k$. Мы имеем, таким образом, стандартные гомоморфизмы.

$$U_S \xrightarrow{\circ} J/k, \quad \hat{J}/k \xrightarrow{\hat{\circ}} \hat{U}_S.$$

Каждому решению задачи погружения $\bar{K}$ соответствует элемент $\psi \in \hat{U}_S$ и можно тогда и только тогда выбрать решение, разветвленное только в простых дивизорах множества S , когда $\psi \in \text{Im } \hat{\phi}$. Очевидно, что элемент $\psi \cdot \text{Im } \hat{\phi}$ группы $\hat{U}_S / \text{Im } \hat{\phi} = \text{Coker } \hat{\phi}$ зависит только от задачи погружения (K, ξ) и не от выбранного решения $\bar{K}$.

Таким образом, имеет место следующий результат.

Теорема 4. *Каждому элементу ξ группы $\widetilde{E(G)}$ соответствует элемент $\psi(\xi) \in \hat{U}_S / \text{Im } \hat{\phi} = \text{Coker } \hat{\phi}$, который равен 1 тогда и только тогда, когда существует решение задачи погружения, разветвленное только в простых дивизорах множества S . Функция ψ определяет вложение группы $\widetilde{E(G)} / (E)^0$ в $\text{Coker } \hat{\phi}$.*

§ 4. ЧИСЛО СООТНОШЕНИЙ

Мы будем опять пользоваться обозначениями, введенными в § 1.

Теорема 5. *Для минимального числа соотношений $r(S)$ в группе $\mathfrak{G}_S$ выполнено неравенство*

$$r(S) \leq t(S) + \sigma(S) - \delta,$$

если $S \neq \emptyset$ или $\zeta \notin k$ и

$$r(S) \leq \sigma(S)$$

если $S = \emptyset$, $\zeta \in k$.

Доказательство. Согласно теореме 2.

$$r(S) = \sup_{\alpha} \dim_{Z_l} E(G_{\alpha})/E(G_{\alpha})^0.$$

Рассмотрим группу $\widetilde{E(G_{\alpha})}$, введенную в § 3.

Так как

$$E(G_{\alpha})^0 \subset \widetilde{E(G_{\alpha})} \subset E(G_{\alpha}),$$

то

$$\dim_{Z_l} E(G_{\alpha})/E(G_{\alpha})^0 = \dim_{Z_l} E(G_{\alpha})/\widetilde{E(G_{\alpha})} + \dim_{Z_l} \widetilde{E(G_{\alpha})}/E(G_{\alpha})^0. \quad (11)$$

Согласно теореме 3 существует $t(S) - \delta$ гомоморфизмов группы $E(G_{\alpha})$ в Z_l , пересечение ядер которых совпадает с $\widetilde{E(G_{\alpha})}$. Отсюда следует, что

$$\dim_{Z_l} E(G_{\alpha})/\widetilde{E(G_{\alpha})} \leq t(S) - \delta, \quad (12)$$

если $S \neq \emptyset$ или $\zeta \notin k$. Если $S = \emptyset$, $\zeta \in k$, то

$$E(G_{\alpha}) = \widetilde{E(G_{\alpha})}. \quad (12')$$

Из теоремы 4 следует, что существует вложение группы $\widetilde{E(G_{\alpha})}/E(G_{\alpha})^0$ в $\text{Coker } \hat{\varphi}$. Поэтому

$$\dim_{Z_l} \widetilde{E(G_{\alpha})}/E(G_{\alpha})^0 \leq \dim_{Z_l} \text{Coker } \hat{\varphi}. \quad (13)$$

Остается вычислить $\dim_{Z_l} \text{Coker } \hat{\varphi}$. Гомоморфизм $\hat{\varphi}$ является сопряженным в смысле спаривания со значениями в Z_l к гомоморфизму

$$\varphi : \mathcal{U}_S \rightarrow J/k.$$

Тот же гомоморфизм является сопряженным к гомоморфизму

$$\varphi_l : \mathcal{U}_S/\mathcal{U}_S^l \rightarrow J/J^l k,$$

так что $\hat{\varphi} = \hat{\varphi}_l$. Но, φ_l и $\hat{\varphi}_l$ являются уже гомоморфизмами векторных пространств над Z_l . Из обычных соображений двойственности следует, что

$$\dim_{Z_l} \text{Coker } \hat{\varphi}_l = \dim_{Z_l} \text{Ker } \varphi_l. \quad (14)$$

Рассмотрим последовательность

$$(1) \rightarrow V_S/k^l \xrightarrow{i} \mathcal{U}_S/\mathcal{U}_S^l \xrightarrow{\varphi_l} J/J^l k, \quad (15)$$

в которой гомоморфизм f определен формулой:

$$f(\alpha) = i\mathcal{U}_S^l, \quad \text{где } \alpha = i\alpha^l, i \in \mathcal{U}_S, \alpha \in J.$$

Существование такого разложения для $\alpha \in V_S$ следует из того, что $V_S = \mathcal{U}_S J^l \cap k$. Легко проверить, что $f(\alpha)$ не зависит от выбора идеала α в этом разложении.

Проверим, что последовательность (15) — точная. Если $i \in \mathcal{U}_S$ и $\varphi_i(i) = 1$, то $i \in \mathcal{U}_S \cap J^l k$, т. е. $i = a^l \alpha$, $a \in J$, $\alpha \in k$.

Отсюда следует, что $\alpha \in V_S$ и $i = f(\alpha)$. Если же $f(\alpha) = 1$, то в равенстве $\alpha = i a^l$ идеаль $i \in \mathcal{U}_S^l$, т. е. $\alpha \in J^l$, а значит, $\alpha \in k^l$.

Из того, что последовательность (15) точная, мы получаем, что

$$\dim_{Z_l} \text{Ker } \varphi_l = \dim_{Z_l} V_S / k^l = \sigma(S). \quad (16)$$

Формулы (10) — (16) показывают, что

$$r(S) \leq t(S) - \delta + \sigma(S),$$

если $S \neq \emptyset$ или $\zeta \notin k$ и

$$r(S) \leq \sigma(S)$$

если $S = \emptyset$, $\zeta \in k$.

Теорема доказана.

Рассмотрим некоторые частные случаи.

1. Предположим, что $\zeta \in k$, число классов дивизоров поля k не делится на $l \neq 2$ и l делится в k только на один простой дивизор: $l = l^e$. Примером такого поля является поле деления круга на l^n частей $R(\zeta_n)$, если l — регулярное простое число. За S возьмем множество, состоящее из одного простого дивизора l .

В этом случае $t(S) = 1$, $\delta = 1$. Покажем, что $\sigma(S) = 0$. Действительно, если $\alpha \in V_S$, то $k(\sqrt[l]{\alpha})$ неразветвлено над k , что возможно, ввиду условия, наложенного на число классов поля k только при $\alpha \in k^l$.

Таким образом, в этом случае теорема 5 показывает, что

$$r(S) = 0,$$

т. е. $\mathcal{G}_S$ является свободной группой. Для числа ее образующих $d(S)$ мы имеем согласно теореме 1.

$$d(S) = [k : R] - r.$$

2. Предположим, что $l = 2$, число классов дивизоров поля k нечетно, 2 делится в k только на один простой дивизор: $2 = l^e$ и k имеет только один бесконечный вещественный простой дивизор, который мы обозначим через p_∞ . Примером такого поля является поле рациональных чисел R . Возьмем за S множество, состоящее из двух простых дивизоров: l и p_∞ .

В этом случае $t(S) = 2$, $\delta = 1$ и так же, как и в случае 1 $\sigma(S) = 0$. Из теоремы 5 теперь следует, что

$$r(S) \leq 1.$$

С другой стороны, простое рассмотрение максимального абелева подполя поля K_S показывает, что уже группа $\mathcal{G}_S / (\mathcal{G}_S, \mathcal{G}_S)$ не является свободной абелевой группой.

Поэтому $r(S) \neq 0$, т. е.

$$r(S) = 1,$$

т. е. группа $\mathcal{G}_S$ определяется единственным соотношением.

Для того, чтобы его найти, обозначим через σ изоморфизм поля k в поле вещественных чисел, соответствующий дивизору p_∞ . Обозначим той же буквой σ изоморфизм поля всех алгебраических чисел в поле всех комплексных чисел $\mathbf{C}$, продолжающий этот изоморфизм поля k . Наконец, через τ обозначим автоморфизм поля $\mathbf{C}$, переводящий любое число в комплексно сопряженное. Так как поле K_S нормально, то поле K_S^g инвариантно относительно τ . Таким образом, $g = \sigma^{-1}\tau\sigma$ является автоморфизмом поля K_S . Так как $\tau^2 = 1$, то и $g^2 = 1$.

Из теоремы Бернсайда легко следует, что элемент g может быть включен в некоторую систему образующих группы $\mathfrak{G}_S : g, g_1, \dots, g_{d-1}$. Таким образом, для этой системы образующих выполняется соотношение

$$g^2 = 1 \quad (17)$$

Легко проверить, что это соотношение может быть включено в минимальную систему соотношений. Точнее, если $\mathfrak{G}_S = \mathfrak{F}/\mathfrak{N}$ — есть представление $\mathfrak{G}_S$ в виде факторгруппы свободной группы с d образующими, то $g^2 \in \mathfrak{N}$, $g^2 \notin (\mathfrak{N}, \mathfrak{F})\mathfrak{N}^2$. Это следует из того, что $g^2 \notin \mathfrak{N}(\mathfrak{F}, \mathfrak{F})$, т. к. $g^2 = e$ является, как легко видеть, определяющим соотношением группы $\mathfrak{G}_S/(\mathfrak{G}_S, \mathfrak{G}_S)$. Из того, что $r(S) = 1$ мы можем заключить теперь, что группа $\mathfrak{G}_S$ определяется единственным соотношением (17). Для числа ее образующих $d(S)$ мы имеем, согласно теореме 1:

$$d(S) = [k : R] + 1 - r.$$

Таким образом, группа $\mathfrak{G}_S$ является 2-адическим пополнением свободного произведения группы Z_2 и свободной группы с $[k : R] - r$ образующими. В частности, при $k = R$

$$\mathfrak{G}_S = \overline{Z_2 * Z}$$

Этот результат был получен раньше другим путем Г. Н. Маркшайтисом [13].

3. Предположим, что все простые дивизоры из множества S взаимно просты с l . Мы будем обозначать это так: $(S, l) = 1$.

Теорема 6. Если $(S, l) = 1$, то

$$r(S) \leq d(S) + r, \quad (18)$$

если $S \neq \emptyset$ или $\zeta \in k$ и

$$r(S) \leq d(S) + 1, \quad (18')$$

если $S = \emptyset$ и $\zeta \in k$.

Действительно, тогда в формуле (1) $\lambda(S) = 0$ и

$$r(S) - d(S) \leq t(S) + \sigma(S) - \delta - (t(S) + \sigma(S) - r - \delta) = r,$$

если $S \neq \emptyset$ или $\zeta \in k$. Формула (18') доказывается аналогично.

Таким образом, для всех полей заданной степени над R и любых множеств S в них, для которых $(S, l) = 1$ разность $r(S) - d(S)$ ограничена сверху.

В частности, если поле k совпадает с R или является квадратичным мнимым полем, то из теоремы 6 следует, что

$$r(S) \leq d(S),$$

за исключением случая $S = \emptyset, l = 2$.

С другой стороны, из теории полей классов следует, т. к. $(S, l) = 1$, что группа $\mathfrak{G}_S/(\mathfrak{G}_S, \mathfrak{G}_S)$ конечна. Отсюда вытекает, что

$$r(S) = d(S) \quad (1)$$
(19)

т. к. в противном случае абелева группа $\mathfrak{G}_S/(\mathfrak{G}_S, \mathfrak{G}_S)$ определялась бы меньшим числом соотношений, чем ее число образующих и, следовательно, не могла бы быть конечной.

Для любой группы G построим убывающий ряд коммутантов

$$G^{(i)} : G^{(1)} = G, G^{(m+1)} = (G^{(m)}, G^{(m)}).$$

Обозначим через $h(G)$ класс разрешимости группы G , т. е. наименьшее значение m , для которого $G^{(m+1)} = e$ (если все $G^{(m)} \neq e$, то $h(G) = \infty$). Из теоремы 6 и теоретико-групповой леммы, доказательство которой мы отложим до следующего параграфа, следует.

Теорема 7. *Для полей фиксированной степени над R и для таких множеств S , что $(S, l) = 1$ мы имеем*

$$h(\mathfrak{G}_S) \rightarrow \infty, \text{ если } d(S) \rightarrow \infty,$$

Доказательство. Предположим, что это не так и что для некоторой последовательности полей k_i и множеств S_i в них $h(\mathfrak{G}_{S_i}) < h$. Мы уже видели, что группы $\mathfrak{G}_{S_i}/\mathfrak{G}_{S_i}^{(2)}$ конечны. Так же доказывается, что $\mathfrak{G}_{S_i}^{(m)}/\mathfrak{G}_{S_i}^{(m+1)}$, а следовательно (если $h(\mathfrak{G}_{S_i}) < h$) и $\mathfrak{G}_{S_i}$ конечна. В следующем параграфе будет доказано существование такой константы $\alpha > 0$, что для всех конечных l -групп G , для которых $h(G) \leq h$

$$r(G) > \alpha d(G)^2.$$

Тем самым

$$r(S_i) > \alpha d(S_i)^2,$$

что, однако, при $d(S_i) \rightarrow \infty$ противоречит неравенству (18).

Мы можем, в частности, выбрать множество S пустым. Тогда $d(S) = \gamma$ и поле K_S — максимальное неразветвленное l -расширение поля k . Если, для полей k заданной степени над $R, \gamma \rightarrow \infty$, то $h(\mathfrak{G}_S) \rightarrow \infty$, а это обозначает, что класс раз-

(1) Если k — квадратичное мнимое поле, $S = \emptyset$ и $l = 2$, то из предшествующих рассуждений следует, что $r(S) = d(S) + 1$ или $r(S) = d(S)$. Оба случая действительно могут встретиться. Первый из них имеет место при $k = R(\sqrt{-21})$ ($\mathfrak{G}_S = Z_2 \times Z_2$), а второй при $k = R(\sqrt{-65})$ ($\mathfrak{G}_S$ — группа, заданная соотношениями (31) с $l = 2, n = 2, k = m = 1$).

решимости максимального разрешимого неразветвленного расширения поля k стремится к бесконечности. Иными словами, если мы обозначим через k_{m+1} гильбертово поле классов над k_m , $k_1 = k$ то $k_{m+1} \neq k_m$ для всех $m < h(\mathbb{G}_S)$. Последовательность полей k_m называется башней полей классов, отдельные поля — ее этажами, а число различных полей — числом этажей. Мы доказали, таким образом.

Следствие. Если для последовательности полей ограниченной степени над $\mathbb{R}$, число образующих группы классов дивизоров неограниченно возрастает, то число этажей башни полей классов над этими полями также неограниченно возрастает.

Заметим, что примеры полей ограниченной степени, для которых γ сколь угодно велико, строятся очень легко. Например, при $l = 2$ такими полями будут поля $\mathbb{R}(\sqrt{\mathcal{D}})$, где $\mathcal{D}$ свободно от квадратов и делится на все большее число простых чисел (согласно основной теореме о родах). Для произвольного l возьмем t таких простых чисел $p_1, \dots, p_t$, что $p_i \equiv 1 \pmod{l}$ обозначим через k_i подполе степени l в p_i — круговом поле и через k подполе поля $k_1, \dots, k_t$, не содержащееся ни в каком композите меньшего числа полей $k_1, \dots, k_t$ и такое, что $[k : \mathbb{R}] = l$. Для k , как легко видеть, $\gamma \geq t - 1$. Это следует из того, что все поля k_i/k неразветвлены.

§ 5. ГРУППОВАЯ ЛЕММА

Лемма. Для любого целого числа h существует такая константа $\alpha > 0$, что для всех конечных l -групп G , для которых $h(G) \leq h$

$$r(G) \geq \alpha d(G)^2 \quad (20)$$

для всех достаточно больших $d(G)$ (т. е. для $d(G) > \mathcal{D}$, где $\mathcal{D}$ зависит только от h).

Доказательство. Пусть G — группа, удовлетворяющая условиям леммы. Положим $d(G) = d$, $r(G) = r$. Пусть F свободная l -группа с d образующими и

$$G = F/N$$

представление G в виде факторгруппы F . По условию N имеет r операторных образующих $\sigma_1, \dots, \sigma_r$, если рассматривать N как F — операторную группу.

Для произвольной группы G положим $G_{i+1} = (G_i, G)G_i^l$, $G_1 = G$.

Из того, что d — минимальное число образующих следует, что $N \subset F_2$. Действительно, если бы это было не так, то гомоморфизм $F/F_2 \rightarrow G/G_2$ не был бы изоморфизмом. Значит образы образующих $x_1, \dots, x_d$ группы F в группе G не были бы независимы по модулю G_2 , а тогда из теоремы Бернсайда следовало бы, что в группе G можно найти систему образующих, состоящую менее чем из d элементов. Из того, что $G^{(h)} = e$ следует, что $N \supset F^{(h)}$. Положим $c = 2^h$. Тогда тем более $NF_{c+1} \supset F^{(h)}$. Положим

$$F/F_{c+1} = \mathfrak{F}, \quad NF_{c+1}/F_{c+1} = \mathfrak{N}.$$

Длина l —центрального ряда группы $\mathfrak{F}$ равна c , т. е. $\mathfrak{F}_{c+1} = e$. При этом

$$\mathfrak{N} \supset \mathfrak{F}^{(h)} \quad (21)$$

и по-прежнему $\mathfrak{N}$ обладает системой из r операторных образующих (как $\mathfrak{F}$ —операторная группа), которые мы обозначим через $S_1, \dots, S_r$.

Группа $\mathfrak{F}_{c+1}$ имеет период l^c . Действительно, т. к. $\mathfrak{F}_m^l \subset \mathfrak{F}_{m+1}$, то $\mathfrak{F}_m^{l^r} \subset \mathfrak{F}_{m+r}$, в частности $\mathfrak{F}^{l^c} = \mathfrak{F}_1^{l^c} \subset \mathfrak{F}_{c+1} = e$.

Доказательство соотношения (20) основывается на том, что оценивается с одной стороны порядок $[\mathfrak{N}]$ группы $\mathfrak{N}$, а с другой — порядок $[\mathfrak{F}^{(h)}]$ группы $\mathfrak{F}^{(h)}$ и потом используется неравенство

$$[\mathfrak{N}] \geq [\mathfrak{F}^{(h)}] \quad (22)$$

следующее из (21).

1. Оценка $[\mathfrak{N}]$. Определим ряд подгрупп ${}^{(k)}\mathfrak{N}$ группы $\mathfrak{N}$:

$${}^{(1)}\mathfrak{N} = \mathfrak{N}, \quad {}^{(k+1)}\mathfrak{N} = ({}^{(k)}\mathfrak{N}, \mathfrak{F}).$$

Мы докажем следующие свойства групп

A. ${}^{(k)}\mathfrak{N} \subset \mathfrak{F}_{k+1}$.

B. ${}^{(k)}\mathfrak{N}/{}^{(k+1)}\mathfrak{N}$ —абелева группа, число образующих которой $\leq rd^{k-1}$.

A. доказывается по индукции. Для $k=1$ утверждение следует из того, что $\mathfrak{N} \subset \mathfrak{F}_2$, т. к. $\mathfrak{N} \subset \mathfrak{F}_2$. Если уже доказано, что ${}^{(k)}\mathfrak{N} \subset \mathfrak{F}_{k+1}$, то

$${}^{(k+1)}\mathfrak{N} = ({}^{(k)}\mathfrak{N}, \mathfrak{F}) \subset (\mathfrak{F}_{k+1}, \mathfrak{F}) \subset \mathfrak{F}_{k+2}.$$

Для доказательства свойства B. проверим сначала, что коммутаторы

$$S_{i, j_1, \dots, j_{k-1}} = (S_i, x_{j_1}, \dots, x_{j_{k-1}}), \quad i = 1, \dots, r; \quad j_s = 1, \dots, d$$

составляют систему операторных образующих группы ${}^{(k)}\mathfrak{N}$, если ее рассматривать как $\mathfrak{F}$ —операторную группу. Это свойство опять проверяется по индукции. Действительно, для $k=1$ оно содержится в определении системы $S_1, \dots, S_r$. Пусть оно доказано для k . Очевидно тогда, что для $k+1$ системой операторных образующих будут коммутаторы

$$(S_{i, j_1, \dots, j_{k-1}}, x_{j_k}),$$

а это и есть элементы $S_{i, j_1, \dots, j_k}$.

Теперь ясно, что элементы $S_{i, j_1, \dots, j_k} {}^{(k+1)}\mathfrak{N}$ составляют систему образующих группы ${}^{(k)}\mathfrak{N}/{}^{(k+1)}\mathfrak{N}$. Это частный случай известного факта: элементы $t_1, \dots, t_m$ нормального делителя $\mathfrak{H}$ некоторой l —группы $\mathfrak{F}$ тогда и только тогда порождают $\mathfrak{H}$ как l —операторную группу, когда $t_1(\mathfrak{H}, \mathfrak{F}), \dots, t_m(\mathfrak{H}, \mathfrak{F})$ порождают $\mathfrak{H}/(\mathfrak{H}, \mathfrak{F})$ (обобщение теоремы Бернсайда). Так как число элементов $S_{i, j_1, \dots, j_{k-1}}$ равно rd^{k-1} , то этим свойство B доказано.

Из того, что период группы $\mathfrak{F}$ равен l^c следует, что период группы ${}^{(k)}\mathfrak{N}$ не больше. Из B тогда вытекает, что

$$({}^{(k)}\mathfrak{N} : {}^{(k+1)}\mathfrak{N}) \leq l^{cd^{k-1}}. \quad (23)$$

Из А следует (при $k=c$), что ${}^{(c)}\mathfrak{N} = e$. Поэтому

$$[\mathfrak{N}] = \prod_{k=1}^{c-1} ({}^{(k)}\mathfrak{N} : {}^{(k+1)}\mathfrak{N}).$$

Отсюда и из (23) вытекает неравенство

$$[\mathfrak{N}] \leq l^{cr(1+d+\dots+d^{c-2})}. \quad (24)$$

П. Оценка $[\mathfrak{F}^{(h)}]$. Мы докажем, что

$$[\mathfrak{F}^{(h)}] \geq l^{\binom{d}{c}}. \quad (25)$$

Для этого рассмотрим любую систему индексов $1 \leq i_1 < i_2 < \dots < i_m \leq d$ ($m = 2^p$, $p \leq h$) и составим коммутатор $\xi_{i_1 \dots i_m}$, положив по индукции

$$\begin{aligned} \xi_{i_1} &= x_{i_1} \quad (\text{при } m=1) \\ \xi_{i_1 \dots i_{2m}} &= (\xi_{i_1 \dots i_m}, \xi_{i_{m+1} \dots i_{2m}}). \end{aligned}$$

Таким образом,

$$\xi_{i_1 i_2} = (x_{i_1}, x_{i_2}), \quad \xi_{i_1 i_2 i_3 i_4} = ((x_{i_1}, x_{i_2}), (x_{i_3}, x_{i_4})) \quad \text{и т. д.}$$

Мы докажем, что элементы $\xi_{i_1 \dots i_c}$ содержатся в $\mathfrak{F}^{(h)}$ и что все $\binom{d}{c}$ таких элементов, соответствующие всем $\binom{d}{c}$ последовательностям $1 \leq i_1 < i_2 < \dots < i_c \leq d$, независимы в этой группе. Отсюда, очевидно, следует (25).

Для доказательства воспользуемся представлением Магнуса коммутаторов в свободном кольце Ли [14]. Рассмотрим кольцо некоммутативных степенных рядов от d переменных $y_1, \dots, y_d$ с целыми коэффициентами: $Z\{y_1, \dots, y_d\}$ и рассмотрим отображение μ группы F в $Z\{y_1, \dots, y_d\}$:

$$\mu x_i = 1 + y_i, \quad \mu x_i^{-1} = 1 - y_i + y_i^2 - y_i^3 + \dots$$

Нетрудно доказать, что у элементов $\mu \xi$, $\xi \in \mathfrak{F}_c$ все коэффициенты при членах степени k , $0 < k \leq c$ относительно $y_1 \dots y_d$ делятся на l (см., например, работу [15]). Поэтому

$$\mu \mathfrak{F}_{c+1} \equiv 1 \pmod{l, (y_1, \dots, y_d)^{c+1}}.$$

С другой стороны легко проверить, что

$$\mu \xi_{i_1 \dots i_c} \equiv 1 + \eta_{i_1 \dots i_c} ((y_1, \dots, y_d)^{c+1}),$$

где коммутаторы $\eta_{i_1 \dots i_m}$, $m = 2^p$ определяются теми же формулами

$$\begin{aligned} \eta_{i_1} &= y_{i_1} \\ \eta_{i_1 \dots i_{2m}} &= [\eta_{i_1 \dots i_m}, \eta_{i_{m+1} \dots i_{2m}}], \end{aligned}$$

что и $\xi_{i_1 \dots i_m}$, но только в кольце $Z\{y_1, \dots, y_d\}$.

Таким образом, если бы существовала зависимость между элементами $\xi_{i_1 \dots i_c}$ по модулю $\mathfrak{F}_{c+1}$:

$$\prod \xi_{i_1 \dots i_c}^{a_{i_1 \dots i_c}} \equiv 1 \pmod{\mathfrak{F}_{c+1}},$$

то существовала бы зависимость с теми же коэффициентами

$$\sum a_{i_1 \dots i_c} \eta_{i_1} \dots \eta_{i_c} \equiv 0 \pmod{l} \quad (26)$$

между однородными многочленами $\eta_{i_1} \dots \eta_{i_c}$ степени c от переменных $y_1, \dots, y_d$.

Такая зависимость невозможна, т. к. все формы $\eta_{i_1} \dots \eta_{i_c}$ зависят от разных систем переменных. Точнее говоря, полагая в тождестве (26) все $y_i = 0$ кроме $y_{j_1}, \dots, y_{j_c}$, мы обратим в 0 все члены кроме $\eta_{j_1} \dots \eta_{j_c}$ и получим, что $a_{j_1 \dots j_c} \equiv 0 \pmod{l}$.

Таким образом, неравенство (25) доказано. Соединяя его с неравенством (24) и (22), мы получим, что

$$\sum_{k=0}^{c-2} c r d^k \geq \binom{d}{c} = \frac{d(d-1) \dots (d-c+1)}{c!},$$

т. е.

$$r \geq \frac{d(d-1) \dots (d-c+1)}{c(c!)(1+d+\dots+d^{c-2})}.$$

Очевидно, что для любого $\alpha < \frac{1}{c(c!)}$ выражение в правой части $> \alpha d^2$ при достаточно больших d . Этим лемма доказана. Мы видим, что за α можно взять любое число, удовлетворяющее неравенству

$$\alpha < \frac{1}{2^h(2^h)!}$$

§ 6. НЕКОТОРЫЕ ЗАМЕЧАНИЯ

В настоящее время неизвестно, будут ли группы $\mathfrak{G}_S$ конечны или нет, если $(S, l) = 1$. В случае, когда множество S пусто, этот вопрос совпадает с так называемой проблемой l —башни полей классов. Если бы группы $\mathfrak{G}_S$ были конечны, то согласно теореме 6 § 4 существовала бы последовательность конечных l —групп G с неограниченно растущим числом образующих $d(G_i)$, для которых разность $r(G_i) - d(G_i)$ была бы ограничена. В связи с этим мы приходим к следующему вопросу

1. Определим функцию $\rho(d)$ условием:

$$\rho(d) = \min_{d(G)=d} r(G),$$

где $r(G)$ —минимальное число соотношений конечной l —группы G , а минимум берется по всем конечным l —группам G , минимальное число образующих которых равно d . Верно ли, что

$$\rho(d) - d \rightarrow \infty \text{ при } d \rightarrow \infty? \quad (27)$$

Простейшие известные l —группы обладают очень большим числом соотношений $r(G)$ сравнительно с числом образующих d .

Так, для коммутативной группы

$$r(G) = \frac{d(d+1)}{2}$$

Для групп F/F_m (в обозначениях § 5) или силовских l подгрупп симметрических групп число $r(G)$ еще больше. Если бы утверждение (27) выполнялось, то из этого следовало бы, что для любого поля алгебраических чисел, у которых число образующих группы классов достаточно велико сравнительно со степенью над R , башня полей классов не обрывается ⁽¹⁾.

В связи с соотношением (19) § 4, которое имеет место, когда поле k совпадает с R или является квадратичным мнимым полем, интересно исследовать конечные l -группы G , для которых

$$r(G) = d(G). \quad (28)$$

Группы подобного рода рассматривал И. Шур [16] в связи с изучением мультипликаторов, т. е. групп $H^2(G, T)$, где $T = R/Z$ — группа всех корней из 1. Связь с условием (28) заключается в следующем. Из точной последовательности

$$(1) \rightarrow Z_l \rightarrow T \xrightarrow{l} T \rightarrow (1)$$

легко выводится точная последовательность

$$0 \rightarrow H^1(G, T)/lH^1(G, T) \rightarrow H^2(G, Z_l) \rightarrow H^2(G, T)_l \rightarrow 0,$$

где $H^2(G, T)_l$ — группа элементов периода l в $H^2(G, T)$.

Легко видеть, что $\dim_{Z_l} H^2(G, T)_l$ совпадает с числом образующих $m(G)$ мультипликатора $H^2(G, T)$, а

$$\dim_{Z_l} H^1(G, T)/lH^1(G, T) = d(G).$$

Таким образом,

$$r(G) - d(G) = m(G),$$

т. к.

$$r(G) = \dim_{Z_l} H^2(G, Z_l).$$

В частности, группы, удовлетворяющие условию (28) совпадают с группами, мультипликатор которых равен 0. Шур называет такие группы замкнутыми.

В работе [16] Шур приводит несколько серий замкнутых групп. Эти серии имеют одну или две образующие (они выписаны ниже). В работе [17] ⁽²⁾ приведен пример замкнутой группы с тремя образующими. В связи с этим возникает следующий вопрос:

II. Существуют ли замкнутые группы со сколь угодно большим числом обра-

⁽¹⁾ Другое доказательство этого утверждения о связи между гипотезой (27) и проблемой башни полей классов, опирающееся на результаты работы [23] см в [22].

⁽²⁾ На эту работу внимание автора обратил J.-P. Serre.

зующих? В частности, существуют ли замкнутые группы более, чем с тремя образующими?

Замкнутыми группами являются, конечно, циклические группы

$$Z_l^n, n \geq 1$$

группы обобщенных кватернионов

$$G = \{a, b\}$$

$$b^2 = a^{2^{n-1}}, b^{-1}ab = a^{-1}, n \geq 2$$

и группы

$$G = \{a, b\}$$

$$b^2 = a^{2^{n-1}}, b^{-1}ab = a^{-1+2^{n-1}}, n > 2$$

(последняя группа определяется этими соотношениями только как 2—группа, т. е. как факторгруппа свободной 2—группы, т. к. из соотношений следует, что $a^{2^n(1-2^{n-2})} = 1$ откуда только в 2—группе следует, что $a^{2^n} = 1$. Эту группу можно определить двумя соотношениями и как дискретную группу, см [24] ⁽¹⁾).

Чтобы найти примеры замкнутых l —групп с $d(G) = 2$ и $l > 2$ запишем соотношения в виде

$$\begin{aligned} a^{l^m}(a, b)^{\alpha}(a, b, b)^{\beta}(a, b, a)^{\gamma} \dots &= 1 \\ b^{l^n}(a, b)^{\alpha'}(a, b, b)^{\beta'}(a, b, a)^{\gamma'} \dots &= 1 \end{aligned} \quad (29)$$

Предположим, что одно из чисел α или α' , например α не делится на l . Тогда согласно теореме, доказанной С. П. Демушкиным [18], можно путем замены образующих привести первое соотношение к виду

$$a^{l^m}(a, b) = 1 \quad (30)$$

В группе, определенной соотношением (30), всякий элемент можно записать в виде $a^x b^y$. В частности, в таком виде можно записать и второе из соотношений. После очевидных преобразований мы сможем записать систему соотношений в виде:

$$\begin{aligned} b a b^{-1} &= a^{1+l^m}, \quad b^{l^n} = a^{l^k}, \\ m &\leq k \leq n. \end{aligned} \quad (31)$$

Различные тройки (m, n, k) , связанные условием $m \leq n \leq k$, дают разные группы, т. к. для группы, определенной соотношением (31),

$$(G, G) \cong Z_{l^k}, \quad G/(G, G) \cong Z_{l^m} \times Z_{l^n}.$$

Известны и некоторые другие (см: например, работу [19] ⁽²⁾) примеры замкнутых групп. Интересно было бы знать, каковы замкнутые группы с двумя образующими, другими словами.

⁽¹⁾ Эту работу автору указал J. Browkin.

⁽²⁾ Эту работу указал автору А. И. Кострикин.

III. Когда будет конечной l —группа, определенная соотношениями (29), если $\alpha \equiv \alpha' \equiv 0 \pmod{l}$?

Заметим, что ситуация последнего вопроса может реализоваться в группах $\mathfrak{G}_S$. Согласно работе Фрöлиха [20] так будет обстоять дело, если $k = \mathbb{R}$, $l > 2$, $S = \{p_1, p_2\}$

$$p_1 - 1 = lm_1, \quad p_2 - 1 = lm_2, \quad (l, m_1 m_2) = 1,$$

причем p_1 и p_2 являются вычетами степени l друг относительно друга, т. е. сравнения

$$p_1 \equiv X_1^l \pmod{p_2}$$

$$p_2 \equiv X_2^l \pmod{p_1}$$

разрешимы. Например, $l = 3$, $p_1 = 79$, $p_2 = 97$. По-видимому, это простейший случай, в котором неизвестно, конечно ли поле K_S .

В случае, когда множество S пусто, т. е. в случае башни l —полей классов, известно очень мало примеров, в которых удалось бы установить конечность башни. Во всех этих случаях при $l > 2$ группы оказываются одного из типов, задаваемых формулами (31). Конечность, очевидно, всегда имеет место, когда группа классов дивизоров поля k циклическая. Кроме этого случая Шольц и Таусская в работе [19] доказали конечность башни 3-полей классов для полей $\mathbb{R}(\sqrt{-4027})$ и $\mathbb{R}(\sqrt{-3299})$. Группы $\mathfrak{G}_S$ (S —пустое множество) задаются в этом случае соотношениями (31) с $m=n=k=1$ в первом случае и $m=k=1$, $n=2$ во втором.

ЛИТЕРАТУРА

- [1] H. ZASSENHAUS, *Lehrbuch der Gruppentheorie*, Leipzig, 1937.
- [2] E. ARTIN and J. TATE, *Class field theory*, Princeton, 1961.
- [3] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. *Jahresber. Deutsch. Math. Ver.*, t. 35 (1926).
- [4] C. CHEVALLEY, *Class field theory*, Nagoya, 1954.
- [5] Д. К. Фаддеев и А. И. Скопин, К доказательству одной теоремы Кавада Доклады АН СССР, t. 127, № 3 (1959), стр. 529-530.
- [6] H. CARTAN and S. EILENBERG, *Homological Algebra*, Princeton, 1956.
- [7] S. MAC LANE, Cohomology theory in abstract groups III. *Ann. of Math.*, t. 50 (1949), p. 736-761.
- [8] C. CHEVALLEY, La théorie du corps de classes. *Ann. of Math.*, t. 41 (1940), p. 391-418.
- [9] A. SCHOLTZ, Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung. I. *Math. Zeitschrift*, t. 42 (1936), p. 161-188.
- [10] H. REICHARDT, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. reine und angew. Math.*, t. 177 (1937), p. 1-5.
- [11] И. Р. Шафаревич, О p -расширениях, Матем. сб., t. 20 (62), № 2 (1947).
- [12] R. BRAUER, Über die Konstruktion der Schiefkörper, die von endlichem Rang in Bezug auf gegebenes Zentrum sind. *J. reine und angew. Math.*, t. 168 (1932), p. 44-64.
- [13] Г. Н. Маркшайтис, О p -расширениях с одним критическим простым числом. Известия АН. Наук СССР, серия матем., t. 27, № 2 (1963).
- [14] W. MAGNUS, Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring, *Math. Ann.*, t. 111 (1935), p. 259-284.
- [15] А. И. Скопин, Факторгруппы одного верхнего центрального ряда, Доклады АН. Наук СССР, t. LXXIV, 13 (1950), стр. 425-428.
- [16] J. SCHUR, Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen, *J. reine und angew. Math.*, t. 132 (1907), p. 85-137.
- [17] J. MENNICKE, Einige Gruppen mit drei Erzeugenden und drei Relationen, *Archiv der Math.*, t. 10 (1959), p. 409.
- [18] С. П. Демушкин, Группа максимального расширения локального поля, Известия Акад. Наук СССР, серия матем., t. 25, № 3 (1961), стр. 329-346.
- [19] I. D. MACDONALD, On a class of finitely presented groups. *Canadian Journ. of Math.*, t. XIV (1962), p. 602-614.
- [20] A. FRÖLICH, On fields of class two. *Proc. Lond. Math. Soc.*, t. IV (1954), p. 235-256.
- [21] A. SCHOLTZ und O. TAUSKY, Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper, *J. reine und angew. Math.*, t. 171 (1934), p. 19-42.
- [22] J.-P. SERRE, *Leçons sur la cohomologie galoisienne*, Collège de France, 1963.
- [23] K. IWASAWA, A note on the group of units of an algebraic number field. *Journ. de Math. pures et appl.*, (9), t. 35 (1956), p. 189-192.
- [24] B. NEUMANN, On some finite groups with trivial multiplier. *Publ. Math. Debrecen*, t. 4 (1956), p. 190-194.

Manuscript reçu le 6 mars 1963.