PUBLICATIONS MATHÉMATIQUES DE L'I.H.É.S.

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>

РАСШИРЕНИЯ С ЗАДАННЫМИ 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 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 равносилен 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, удается 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 $S=\{\mathfrak{p}_1,\dots \mathfrak{p}_s\}$.

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 $\mathfrak{G}_S/\mathfrak{G}_S^{(1)}$, $\mathfrak{G}_S^{(1)}=\mathfrak{G}_S^l(\mathfrak{G}_S, \mathfrak{G}_S)$. К подгруппе $\mathfrak{G}_S^{(1)}$ принадлежит подполе $K_S^{(1)}\subset K_S$, которое является, очевидно, максимальным абелевым расширением периода l поля k, разветвленным только в простых дивизорах $\mathfrak{p}\in S$. 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

$\mathfrak{a}_\mathfrak{p}$—$\mathfrak{p}$-компонента иделя $\mathfrak{a}$

k — группа главных иделей и также мультипликативная группа поля k

$\mathfrak{U}_\mathfrak{p}$ — группа единиц $\mathfrak{p}$-адического замыкания $k_\mathfrak{p}$ поля k

$$\mathfrak{U}_S=\{\mathfrak{a}\,|\,\mathfrak{a}_\mathfrak{q}\in\mathfrak{U}_\mathfrak{q},\ \ \mathfrak{a}_\mathfrak{p}=1 \ \text{ для } \ \mathfrak{p}\in S\}.$$

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

$$V_S=\{\alpha\in k\,|\,(\alpha)=\mathfrak{a}^l,\ \alpha\in k_\mathfrak{p}^l \ \text{ для } \ \mathfrak{p}\in S\}$$

(α)—главный дивизор числа α.

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

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:*

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

где $t(S)$ — *число тех простых дивизоров* $\mathfrak{p}\in S$, *для которых* $\zeta\in k_\mathfrak{p}$,

$$\lambda(S)=\sum_{\mathfrak{p}|l,\,\mathfrak{p}\in S} n(\mathfrak{p}),\quad n(\mathfrak{p})=[k_\mathfrak{p}:R_p],\quad \mathfrak{p}|p$$

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 $\mathfrak{p}$ тогда и только тогда неразветвлен в K, когда $\mathfrak{U}_\mathfrak{p}\subset B$ ([2] теорема 3 гл. 8). Отсюда легко следует, что полю $K_S^{(1)}$ соответствует подгруппа $\mathfrak{U}_S J^l k$ и

$$d(S)=\dim_{Z_l} J/\mathfrak{U}_S.J^l.k.$$

Положим

$$H_S=J/\mathfrak{U}_S.J^l.k$$

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

Рассмотрим последовательность групп и гомоморфизмов:

$$(1)\to V_S/k^l \xrightarrow{f_4} V/k^l \xrightarrow{f_3} \mathfrak{U}/\mathfrak{U}_S\mathfrak{U}^l \xrightarrow{f_2} H_S \xrightarrow{f_1} H\to(1). \tag{2}$$

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

f_1—естественное отображение группы на факторгруппу
$H=H_S/(\mathfrak{U}.J^l.k/\mathfrak{U}_S J^l k)$

$f_2(\mathfrak{a})=\mathfrak{a}\mathfrak{U}_S J^l k$, $\mathfrak{a}\in\mathfrak{U}$

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 идель $\mathfrak{a}$, что $\alpha\mathfrak{a}^{-l}\in\mathfrak{U}$ Положим

$$f_3(\alpha)=\alpha\mathfrak{a}^{-l}\mathfrak{U}_S\mathfrak{U}^l$$

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

$$\alpha\mathfrak{a}_1^{-l}\in\mathfrak{U},\ \text{то}\ \alpha\mathfrak{a}_1^{-l}=\alpha\mathfrak{a}^{-l}\mathfrak{i},\ \text{где}\ \mathfrak{i}=(\mathfrak{a}_1/\mathfrak{a})^l\in\mathfrak{U}^l.$$

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

Действительно, $\operatorname{Im} f_1=H$ и т. к. $H=J/J\mathfrak{U}^l k$, то

$$\operatorname{Ker} f_1=\mathfrak{U}.J^l.k/\mathfrak{U}_S.J^l.k=\operatorname{Im} f_2$$

$$\operatorname{Ker} f_2=\{\mathfrak{i}\mathfrak{U}_S\mathfrak{U}^l\,|\,\mathfrak{i}\in\mathfrak{U},\ \mathfrak{i}=\mathfrak{a}^l b_S\alpha,\ \mathfrak{a}\in J,\ b_S\in\mathfrak{U}_S,\ \alpha\in k\}$$

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

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

Наконец,

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

и

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

Из точности последовательности (2) следует, что

$$\dim_{Z_l} H - \dim_{Z_l} H_S + \dim_{Z_l} \mathfrak{U}/\mathfrak{U}_S \mathfrak{U}^l - \dim_{Z_l} V/k^l + \dim_{Z_l} V_S/k^l = 0. \tag{3}$$

При этом по определению

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

Кроме того,

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

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

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

Отсюда следует, что

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

Наконец

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

Действительно, для $\alpha \in V$ по условию $(\alpha) = \mathfrak{a}^l$ и отображение $\varphi_1 : \alpha \to \mathfrak{a}$ 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:

$$(1) \to E/E^l \xrightarrow{\varphi_2} V/k^l \xrightarrow{\varphi_1} H \to (1),$$

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

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:

$$\mathfrak{G} = \varprojlim G_\alpha. \tag{7}$$

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

$$\mathfrak{G} = \mathfrak{F}/\mathfrak{N}. \tag{8}$$

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 $\mathfrak{F} \to \mathfrak{G}$ определяет изоморфизм групп $\mathfrak{F}/\mathfrak{F}_1$, и $\mathfrak{G}/\mathfrak{G}_1$, где $\mathfrak{F}_1 = \mathfrak{F}^l(\mathfrak{F}, \mathfrak{F})$, $\mathfrak{G}_1 = \mathfrak{G}^l(\mathfrak{G}, \mathfrak{G})$. 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 $\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^l$ — доказательство этого факта дословно повторяет доказательство теоремы Бернсайда. Таким образом, если $r(\mathfrak{G})$ — минимальное число соотношений в группе $\mathfrak{G}$, то

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

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 $\mathrm{Ext}(\mathfrak{G}, Z_l)$ 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

$$\widehat{\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^l} = \mathrm{Hom}(\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^l, Z_l).$$

Очевидно, что последовательность

$$(1) \to \mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^l \to \mathfrak{F}/\mathfrak{N}, \mathfrak{F})\mathfrak{N}^l \to \mathfrak{G} \to (1)$$

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

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

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

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

Таким путем определяется отображение

$$\xi : \widehat{\mathfrak{N}/(\mathfrak{N}, \mathfrak{F})\mathfrak{N}^l} \to \mathrm{E}(\mathfrak{G}), \ \xi(\varphi) = \varphi\Theta. \tag{9}$$

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

Таким образом,

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

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

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

соответствует гомоморфизм

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

и

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

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

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

соответствует гомоморфизм

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

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

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

Если мы положим

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

то получим, что

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

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

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

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

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

определяет элемент

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

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

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

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

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

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

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

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

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

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

и φ определяет вложение $\mathfrak{z}$ в Z_l. 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 $\bar{\bar{K}}$

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

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

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

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

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

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

$$r(\mathfrak{G}) = \operatorname*{Sup}_{\alpha} \dim_{Z_l} E(G_\alpha)/E(G_\alpha)^0,$$

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 $\overline{K}$ 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 $\overline{K}$ и изоморфного вложения его группы Галуа над K в Z_l. Иначе говоря, можно считать, что мы фиксируем поле $\overline{K}$ и элемент группы $\operatorname{Hom}(G(\overline{K}/K), Z_l)$. Этот элемент можно рассматривать и как элемент группы $\operatorname{Hom}(a_K, Z_l)$, где a_K—группа Галуа максимального абелева расширения поля K. Наоборот, каждый элемент χ группы $\hat{a}_K = \operatorname{Hom}(a_K, Z_l)$ определяет некоторое поле — то, которое соответствует подгруппе $\operatorname{Ker}\chi$ группы a_K и гомоморфизм группы Галуа этого поля в Z_l. Таким образом, « расширения », в смысле этой новой структуры, совпадают с элементами группы $\hat{a}_K = \operatorname{Hom}(a_K, Z_l)$. Такая трактовка имеется, например, еще в работе [8]. Нам важно сейчас, что групповая операция переносится, таким образом, с группы $a_K = \operatorname{Hom}(a_K, Z_l)$ на множество расширений поля K с группой изоморфной Z_l или 1. Результат применения этой операции к расширениям $\overline{K}$ и $\overline{\overline{K}}$ мы будем обозначать через $\overline{K} \circ \overline{\overline{K}}$.

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

Группа Галуа каждого расширения $\overline{K}$ 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 $\overline{K}$ 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 $K \otimes k_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} K_\mathfrak{P}$. 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 $\mathfrak{p}$ поля k разрешима задача погружения $(K_\mathfrak{p}, \xi)$. При этом, если $\zeta \in k$, то из разрешимости задачи погружения для всех $\mathfrak{p}$, кроме одного, следует ее разрешимость для этого одного $\mathfrak{p}$ (см. [9] или [10]).

По поводу разрешимости задачи погружения для алгебр $K_\mathfrak{p}$ известно следующее:

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

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

3. Если $\zeta \in k_\mathfrak{p}$, то существует такой элемент χ группы $\mathrm{Hom}(E(G), Z_l)$ 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* $\chi_1, \ldots, \chi_m$ *группы* $\mathrm{Hom}(E(G), Z_l)$, *что* $\xi \in \widetilde{E(G)}$ *тогда и только тогда, когда* $\chi_1(\xi) = 1, \ldots, \chi_m(\xi) = 1$. *Здесь, как и в* § 1, $t(S)$ *обозначает число таких* $\mathfrak{p} \in S$, *что* $\zeta \in k_\mathfrak{p}$, *а* $\delta = 0$, *если* $\zeta \notin k$ *и* $\delta = 1$, *если* $\zeta \in k$. *Если* $\delta = 1$ *и* $S = \varnothing$, *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 $K_0 = K.\bar{k}$ поля мы будем называть тривиальным. Имеет место следующий результат:

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

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

определено неоднозначно, а (согласно утверждению 4) с точностью до замены $\Sigma_\mathfrak{p} \to \Sigma_\mathfrak{p} \circ \Sigma_0$, где $\Sigma_0 = K_\mathfrak{p}.\varkappa$, а $\varkappa/k_\mathfrak{p}$—неразветвленное расширение поля $k_\mathfrak{p}$, группа Галуа которого изоморфна Z_l или 1. Такому расширению соответствует элемент $\varphi_0 \in \hat{k}_\mathfrak{p}$, обладающий свойством $\varphi_0|_{\mathfrak{U}_\mathfrak{p}} = 1$.

Мы видим, что φ определен с точностью до множителя такого типа. Иными словами, однозначно определен характер $\psi \in \mathrm{Hom}(\mathfrak{U}_\mathfrak{p}, Z_l) = \hat{\mathfrak{U}}_\mathfrak{p}$. Мы получили следующий результат.

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

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

$$\mathfrak{U}_S \xrightarrow{\varphi} J/k, \quad \hat{J/k} \xrightarrow{\hat{\varphi}} \hat{\mathfrak{U}}_S.$$

Каждому решению задачи погружения $\bar{K}$ соответствует элемент $\psi \in \hat{\mathfrak{U}}_S$ и можно тогда и только тогда выбрать решение, разветвленное только в простых дивизорах множества S, когда $\psi \in \mathrm{Im}\,\hat{\varphi}$. Очевидно, что элемент $\psi.\mathrm{Im}\,\hat{\varphi}$ группы $\hat{\mathfrak{U}}_S/\mathrm{Im}\,\hat{\varphi} = \mathrm{Coker}\,\hat{\varphi}$ 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* $\psi(\xi) \in \hat{\mathfrak{U}}_S/\mathrm{Im}\,\hat{\varphi} = \mathrm{Coker}\,\hat{\varphi}$, *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* $\mathrm{Coker}\,\hat{\varphi}$.

§ 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*

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

если $S \neq \varnothing$ *или* $\zeta \notin k$ *и*

$$r(S) \leqslant \sigma(S)$$

если $S = \varnothing, \zeta \in k$.

Доказательство. Согласно теореме 2.

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

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

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

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

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

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

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

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

$$\dim_{Z_l} \widetilde{E(G_\alpha)}/E(G_\alpha)^0 \leqslant \dim_{Z_l} \operatorname{Coker} \hat{\varphi}. \tag{13}$$

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

$$\varphi : \mathfrak{U}_S \to J/k.$$

Тот же гомоморфизм является сопряженным к гомоморфизму

$$\varphi_l : \mathfrak{U}_S/\mathfrak{U}_S^l \to J/J^l k,$$

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

$$\dim_{Z_l} \operatorname{Coker} \hat{\varphi}_l = \dim_{Z_l} \operatorname{Ker} \varphi_l. \tag{14}$$

Рассмотрим последовательность

$$(1) \to V_S/k^l \xrightarrow{f} \mathfrak{U}_S/\mathfrak{U}_S^l \xrightarrow{\varphi_l} J/J^l k, \tag{15}$$

в которой гомоморфизм f определен формулой:

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

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

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

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

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

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

Формулы (10) — (16) показывают, что

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

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

$$r(S) \leqslant \sigma(S)$$

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: $l = \mathfrak{l}^e$. 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 $\mathfrak{l}$.

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. $\mathfrak{G}_S$ 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: $2 = \mathfrak{l}^e$ и k имеет только один бесконечный вещественный простой дивизор, который мы обозначим через $\mathfrak{p}_\infty$. Примером такого поля является поле рациональных чисел R. Возьмем за S множество, состоящее из двух простых дивизоров: $\mathfrak{l}$ и $\mathfrak{p}_\infty$.

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

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

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

Поэтому $r(S) \neq 0$, т. е.

$$r(S) = 1,$$

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

Для того, чтобы его найти, обозначим через σ изоморфизм поля k в поле вещественных чисел, соответствующий дивизору $\mathfrak{p}_\infty$. 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^σ 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 $\mathfrak{G}_S$: $g, g_1, \ldots, g_{d-1}$. Таким образом, для этой системы образующих выполняется соотношение

$$g^2=1 \tag{17}$$

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*

$$r(S)\leqslant d(S)+r, \tag{18}$$

если $S\neq\varnothing$ *или* $\zeta\in k$ *и*

$$r(S)\leqslant d(S)+1, \tag{18'}$$

если $S=\varnothing$ *и* $\zeta\in k$.

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

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

если $S\neq\varnothing$ или $\zeta\notin k$. 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

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

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

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

$$r(S) = d(S) \ (^1) \tag{19}$$

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*

$$h(\mathfrak{G}_S) \to \infty, \quad \textit{если} \quad d(S) \to \infty,$$

Доказательство. Предположим, что это не так и что для некоторой посделовательности полей k_i и множеств S_i в них $h(\mathfrak{G}_{S_i}) < h$. Мы уже видели, что группы $\mathfrak{G}_S/\mathfrak{G}_S^{(2)}$ конечны. Так же доказывается, что $\mathfrak{G}_S^{(m)}/\mathfrak{G}_S^{(m+1)}$, 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 $h(G) \leqslant h$

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

Тем самым

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

что, однако, при $d(S_i) \to \infty$ 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, $\gamma \to \infty$, то $h(\mathfrak{G}_S) \to \infty$, а это обозначает, что класс раз-

---

(1) Если k—квадратичное мнимое поле, $S = \varnothing$ 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 $m<h(\mathfrak{G}_S)$. 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* 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 $\mathrm{R}(\sqrt{\mathscr{D}})$, где $\mathscr{D}$ свободно от квадратов и делится на все большее число простых чисел (согласно основной теореме о родах). Для произвольного l возьмем t таких простых чисел $p_1, \ldots, p_t$, что $p_i\equiv 1 \pmod{l}$ обозначим через k_i подполе степени l в p_i—круговом поле и через k подполе поля $k_1, \ldots, k_t$, не содержащееся ни в каком композите меньшего числа полей $k_1, \ldots, k_t$ и такое, что $[k:\mathrm{R}]=l$. Для k, как легко видеть, $\gamma\geqslant t-1$. Это следует из того, что все поля k_ik/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* $h(\mathrm{G})\leqslant h$

$$r(\mathrm{G})\geqslant \alpha\, d(\mathrm{G})^2 \tag{20}$$

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

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

$$\mathrm{G}=\mathrm{F}/\mathrm{N}$$

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

Для произвольной группы G положим $\mathrm{G}_{i+1}=(\mathrm{G}_i, \mathrm{G})\mathrm{G}_i^l$, $\mathrm{G}_1=\mathrm{G}$.

Из того, что d—минимальное число образующих следует, что $\mathrm{N}\subset\mathrm{F}_2$. Действительно, если бы это было не так, то гомоморфизм $\mathrm{F}/\mathrm{F}_2\to\mathrm{G}/\mathrm{G}_2$ не был бы изоморфизмом. Значит образы образующих $x_1, \ldots, x_d$ 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 $\mathrm{G}^{h)}=e$ следует, что $\mathrm{N}\supset\mathrm{F}^{h)}$. Положим $c=2^h$. Тогда тем более $\mathrm{NF}_{c+1}\supset\mathrm{F}^{h)}$. Положим

$$\mathrm{F}/\mathrm{F}_{c+1}=\mathfrak{F},\quad \mathrm{NF}_{c+1}/\mathrm{F}_{c+1}=\mathfrak{N}.$$

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

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

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

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

$$[\mathfrak{N}]\geqslant[\mathfrak{F}^{(h)}] \tag{22}$$

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 $\leqslant rd^{k-1}$.

A. доказывается по индукции. Для $k=1$ утверждение следует из того, что $\mathfrak{N}\subset\mathfrak{F}_2$, т. к. $N\subset F_2$. 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

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

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 систему $S_1, \ldots, S_r$. Пусть оно доказано для k. Очевидно тогда, что для $k+1$ системой операторных образующих будут коммутаторы

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

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

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

$$({}^{(k)}\mathfrak{N}:{}^{(k+1)}\mathfrak{N})\leqslant l^{crd^{k-1}}. \tag{23}$$

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

$$[\mathfrak{N}]\leqslant l^{cr(1+d+\ldots+d^{c-2})}. \tag{24}$$

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

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

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

$$\xi_{i_1}=x_{i_1}\ (\textit{при}\ m=1)$$

$$\xi_{i_1\ldots i_{2m}}=(\xi_{i_1\ldots i_m},\ \xi_{i_{m+1}\ldots i_{2m}}).$$

Таким образом,

$$\xi_{i_1i_2}=(x_{i_1},\ x_{i_2}),\ \xi_{i_1i_2i_3i_4}=((x_{i_1},\ x_{i_2}),\ (x_{i_3},\ x_{i_4}))\qquad \text{и т. д.}$$

Мы докажем, что элементы $\xi_{i_1\ldots i_c}$ содержатся в $\mathfrak{F}^{(h)}$ и что все $\binom{d}{c}$ таких элементов, соответствующие всем $\binom{d}{c}$ последовательностям $1\leqslant i_1<i_2<\ldots<i_c\leqslant d$, 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 $y_1,\ldots,y_d$ с целыми коэффициентами: $Z\{y_1,\ldots,y_d\}$ и рассмотрим отображение μ группы F в $Z\{y_1,\ldots,y_d\}$:

$$\mu x_i=1+y_i,\qquad \mu x_i^{-1}=1-y_i+y_i^2-y_3^3+\ldots$$

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

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

С другой стороны легко проверить, что

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

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

$$\eta_{i_1}=y_{i_1}$$

$$\eta i_1\ldots i_{2m}=[\eta_{i_1\ldots i_m},\ \eta i_{m+1}\ldots i_{2m}],$$

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

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

$$\prod\xi_{i_1\ldots i_c}^{a_{i_1\ldots i_c}}\equiv 1\ (\mathfrak{F}_{c+1}),$$

то существовала бы зависимость с теми же коэффициентами

$$\Sigma a_{i_1 \dots i_c} \eta_{i_1 \dots i_c} \equiv 0 \pmod{l} \tag{26}$$

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

Такая зависимость невозможна, т. к. все формы $\eta_{i_1 \dots i_c}$ 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 $\eta_{j_1 \dots j_c}$ 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

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

т. е.

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

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

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

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

$$r(G)=d(G). \tag{28}$$

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

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

легко выводится точная последовательность

$$0\to H'(G, T)/lH'(G, T)\to H^2(G, Z_l)\to H^2(G, T)_l\to 0,$$

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

$$Z_{l^n},\ n \geqslant 1$$

группы обобщенных кватернионов

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

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

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

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

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

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:

$$bab^{-1} = a^{1+l^m},\quad b^{l^n} = a^{l^k}, \tag{31}$$
$$m \leqslant k \leqslant n.$$

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

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

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.

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

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

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

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

$$p_1 \equiv \mathrm{X}_1^l \ (\mathrm{mod}\ p_2)$$
$$p_2 \equiv \mathrm{X}_2^l \ (\mathrm{mod}\ p_1)$$

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 $\mathrm{R}(\sqrt{-4\,027})$ и $\mathrm{R}(\sqrt{-3\,299})$. 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 Ак. 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 центральногор ряда*, Доклады Ак. 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 маскимального 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. Taussky, Die Hauptideale der kubischen Klassenkörper imaginärquadratischer 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 multiplicator. *Publ. Math. Debrecen*, t. 4 (1956), p. 190-194.

Manuscrit reçu le 6 mars 1963.