

И.Р. Шафаревич

**СОЧИНЕНИЯ
В ТРЕХ ТОМАХ**

Том 3

МАТЕМАТИЧЕСКИЕ РАБОТЫ

Часть 1

МОСКВА, 1996

И. Р. Шафаревич

Ш-30 Сочинения. В 3 т. Т. 3. часть 1 – М.: АОЗТ «Прима В»

Ш **0902050100-011**
966(03)-96 Без объявл.

ББК 66.2(2Р)
Ш30

Математические исследования

ISBN 5-85240-061-0

И.Р.Шафаревич. Собрание сочинений в трех томах. Том третий, часть I.

В третий том собрания сочинений вошли математические работы выдающегося русского математика современности академика РАН Игоря Ростиславовича Шафаревича. Первая часть тома содержит работы по теории чисел, а также, в отделе "Разное", статьи о математике и математиках. Во вторую часть третьего тома входят труды по алгебре и алгебраической геометрии.

Ответственные за выпуск *В.М.Имайкин, С.И.Комаров.*

Компьютерный набор в макропакете *AMS-TeX* выполнен при участии :

Н.Н.Бахтиной, О.В.Никишкиной, Ф.Н.Чемерева.

Настоящее издание математических трудов И.Р. Шафаревича осуществлено при участии Международного Фонда содействия православной культуре свят. блгв. князя Александра Невского.

Том 3
Часть 1

ТЕОРИЯ ЧИСЕЛ
РАЗНОЕ

СОДЕРЖАНИЕ

Математические работы И.Р. Шафаревича.....	vi
Список математических публикаций И.Р. Шафаревича.....	xvii
 ТЕОРИЯ ЧИСЕЛ	
1 О группах Галуа p -адических полей	2
2 О p -расширениях	5
3 Общий закон взаимности (Докл. Акад. Наук СССР)	21
4 Общий закон взаимности (Матем. сб.)	26
5 Новое доказательство теоремы Кронекера–Вебера	72
6 О задаче погружения полей (ДАН)	78
7 О построении полей с заданной группой Галуа порядка l^α	82
8 Об одной теореме существования в теории алгебраических чисел	127
9 О задаче погружения полей (Изв. АН)	138
10 Построение полей алгебраических чисел с заданной разрешимой группой Галуа	178
11 О бирациональной эквивалентности эллиптических кривых	244
12 Показатели эллиптических кривых	250
13 Задача погружения для распадающихся расширений	254
14 Группа главных однородных алгебраических многообразий	258
15 Задача погружения для локальных полей (с С.П. Демушкиным)	261
16 Второе препятствие для задачи погружения полей алгебраических чисел (с С.П. Демушкиным)	285
17 Поля алгебраических чисел	303
18 Расширения с заданными точками ветвления	320
19 О башне полей классов (с Е.С. Голодом)	347
20 О ранге эллиптических кривых (с Дж. Тэйтом)	361

РАЗНОЕ

21 Впечатления от международного математического конгресса в Эдинбурге	368
22 К 150-летию со дня рождения Альфреда Клебша.....	373
23 Математическое мышление и природа.....	380
24 Так сделайте невозможное! (к 80-летию Л.С. Понтрягина)	390
25 Абелева и неабелева математика	397

МАТЕМАТИЧЕСКИЕ РАБОТЫ И.Р.ШАФАРЕВИЧА

Настоящая статья воспроизводит с редакционными изменениями статьи, опубликованные в “Успехах Математических Наук”, т.39, 1984, N 1, и “Трудах математического института Академии Наук” N 208, 1995. .

И.Р.Шафаревич родился в 1923 г. в г. Житомире. Способности к математике у Игоря Ростиславовича проявились очень рано. Учась в школе, он сдает экстерном экзамены в университет, слушает лекции и участвует в работе семинаров. После окончания школы в 1939 г. Игорь Ростиславович за один год завершает обучение в МГУ и в 1940 г. становится аспирантом. С 1944 г. он — преподаватель МГУ, а с 1946 г. — сотрудник Математического института им. В.А.Стеклова. В этом же году Игорь Ростиславович защищает докторскую диссертацию.

Первая работа И.Р.Шафаревича [1] посвящена нахождению критерия нормируемости топологических полей. Она составила предмет его кандидатской диссертации.

С самого начала научной деятельности И.Р.Шафаревича привлекали теория Галуа и теория алгебраических чисел. Его первым значительным достижением в этих областях математики были работы [4], [6], в которых изучались неабелевы p -расширения локальных полей k . Здесь рассматривался случай, когда основное поле $k \supset Q$ не содержит корня степени p из единицы. Если $[k : Q] = n$, то максимальное p -расширение поля k имеет группой Галуа свободную про- p -группу с $n+1$ образующей. Аналогичный результат был получен для неразветвленных p -расширений поля k алгебраических функций с алгебраически замкнутым полем констант характеристики p . Таким образом, в этой ситуации была решена обратная задача теории Галуа для конечных p -групп. Эта работа была удостоена премии Московского математического общества. В [4] введено также важное понятие фундаментального класса в теории полей классов локальных полей. Оно позволяет явно вычислить

возникающее в теории Галуа расширение.

$$1 \rightarrow \text{Gal}(L^{ab}/L) \rightarrow \text{Gal}(L^{ab}/K) \rightarrow \text{Gal}(L/K) \rightarrow 1,$$

где L/K — конечное нормальное расширение, L^{ab} — максимальное абелево расширение поля L . На случай полей алгебраических чисел эта конструкция была перенесена в [5].

К числу крупнейших достижений алгебраической теории чисел относится работа И.Р.Шафаревича “Общий закон взаимности” [7], [8], [9]. В ней были рассмотрены следующие три круга вопросов, относящиеся к полям алгебраических чисел k :

1) Для символа норменного вычета $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$, где α, β — числа из поля алгебраических чисел k и $\mathfrak{p}$ — его простой идеал, дана конструкция, аналогичная определению вычета абелева дифференциала $\alpha d\beta$ в точках римановой поверхности.

2) Задача нахождения общего закона взаимности состоит в явном выражении отношения символов степенных вычетов n -й степени $\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1}$ через числа α, β . Поскольку

$$\left(\frac{\alpha}{\beta}\right)\left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{\mathfrak{p}|n} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right),$$

новая конструкция символа норменного вычета дала возможность получить общий закон взаимности.

3) Основной результат этой статьи позволил более естественно построить теорию полей классов, как локальную, так и глобальную.

Этими результатами была решена проблема нахождения общего закона взаимности, связанная с именами таких математиков, как Гаусс, Якоби, Куммер, Гильберт и др. Эта задача была включена Гильбертом в число его знаменитых проблем (девятая проблема Гильберта).

После работы по общему закону взаимности И.Р.Шафаревич снова обращается к обратной задаче теории Галуа, но теперь уже для полей алгебраических чисел. Его усилия увенчались успехом и в 1954 г. появился большой цикл работ на эту тему. Сначала была опубликована работа [16] о существовании расширений полей алгебраических чисел с заданной группой Галуа порядка l^α . Техника, развитая в этой работе, дала затем возможность получить (в [18]) разрешимость задачи погружения для полупрямых произведений F на G в случае, когда: а) нормальный делитель G имеет порядок l^α ; б) порядок F прост с l , и, наконец, [19], провести построение полей алгебраических чисел с заданной разрешимой группой Галуа. За

цикл работ по решению обратной задачи теории Галуа над полями алгебраических чисел И.Р.Шафаревичу в 1959 г. была присуждена Ленинская премия.

В 1959г. было получено решение задачи погружения для локальных полей [33]. Для этого сначала исследовались первое и второе препятствия в задаче погружения в общем виде. Первое препятствие — это известное ранее условие согласности. Второе препятствие (связанное с выполнимостью условия согласности после первого шага в задаче погружения) было получено в виде набора циклических алгебр, зависящих от некоторого параметра из основного поля. Для локальных полей было доказано, что с помощью этого параметра соответствующий набор циклических алгебр может быть приведен к распадающемуся виду, т.е. что второе препятствие для локальных полей исчезает. Далее в работе 1962 г. [39] было исследовано второе препятствие для задачи погружения полей алгебраических чисел.

К изучению групп Галуа p -расширений И.Р.Шафаревич возвращается в работе [42] 1964 г. Теперь он рассматривает p -расширения поля алгебраических чисел k , имеющие ветвление лишь в фиксированном множестве S простых дивизоров поля k . Пусть $G_S(p)$ — группа Галуа максимального расширения с этими свойствами. Основные результаты, полученные в [42], состоят в оценке минимального числа образующих d и соотношений r группы $G_S(p)$ через число дивизоров в S и инварианты поля k . Если множество S пусто, то $r < d + \rho$, где ρ — число образующих группы единиц поля k . В обзорном докладе на Международном математическом конгрессе в Стокгольме [40] И.Р.Шафаревич обратил внимание на то, что из этого факта вытекает решение известной проблемы башни в теории полей классов, если число соотношений $r = r(G)$ для конечной p -группы G достаточно велико по сравнению с числом ее образующих $d = d(G)$ (при больших d). В работе [43] было показано, что $r > [(d-1)/2]^2$. Это дало решение проблемы башни, более сорока лет не поддававшейся усилиям алгебраистов. На языке групп $G_S(p)$ проблема башни состоит в выяснении, конечна или нет группа $G_S(p)$ (при пустом S) для данного поля k . Полученное решение (и техника его доказательства) имеют много следствий в теории чисел и алгебре. Достаточно упомянуть доказательство существования полей алгебраических чисел, не вложимых в одноклассные, точные оценки роста дискриминанта числового поля в зависимости от его степени, отрицательное решение расширенной проблемы Бернсайда для p -групп с неограниченным показателем степени и аналогичных проблем для колец и алгебр Ли (напомним, что отрицательное решение классической проблемы Бернсайда с ограни-

ченным показателем получено П.С.Новиковым и С.И.Адяном).

Резонанс, вызванной статьей [33], оказался настолько острым, что ее основной результат, вместе с незначительно измененным доказательством, дающим неравенство $r > d^2/4$, вошел почти сразу же в монографическую и учебную литературу. Удивительно, что столь естественный вопрос комбинаторной теории групп, рассматриваемый изолированно вне всякой связи с полями алгебраических чисел, не был решен раньше, хотя со времен И.Шура проявлялся определенный интерес к замкнутым группам, для которых $r(G) = d(G)$. Были известны примеры такого рода для $d = 1, 2, 3$, но понадобился толчок извне, чтобы взглянуть шире на проблему задания конечных p -групп образующими и соотношениями и увидеть, в частности, отсутствие замкнутых p -групп при $d > 3$. Впоследствии были построены примеры конечных p -групп, для которых отношение $r(G)/d(G)^2$ может быть сколько угодно близким к $1/4$. Таким образом, неравенство $r > d^2/4$ асимптотически (при $d \rightarrow \infty$) неумлучшаемо.

Когомологическая интерпретация $d(G) = \dim H^1(G, Z_p)$ и $r(G) = \dim H^2(G, Z_p)$ инвариантов d и r конечной про- p -группы G еще раньше привлекала внимание И.Р.Шафаревича.

В заметке [28], написанной в период экспансии методов гомологической алгебры, было обращено внимание на свойства функции Пуанкаре

$$P_N(t) = \sum_{n \geq 0} \dim H^n(N, k) t^n$$

конечномерной нильпотентной алгебры N над полем k . Хотя гипотеза о рациональности функции $P_N(t)$ не подтвердилась, ее важный частный случай, отвечающий радикалу $N(A)$ групповой алгебры над F_p конечной p -группы G , оказался верным. Аналогичные вопросы о производящих функциях градуированных объектов возникли примерно с 1950 по 1970 г.г. по разным поводам и в разных областях математики.

В середине пятидесятых годов И.Р.Шафаревич начинает заниматься алгебраической геометрией. Современная алгебраическая геометрия находится на стыке большого числа областей математики, переживших за последние 30 лет второе рождение или даже заново родившихся.

Естественно, что первые задачи в алгебраической геометрии, которыми стал заниматься И.Р.Шафаревич, находились на границе теории чисел и геометрии. Они относились к теории эллиптических кривых или, в более старой терминологии, к теории неопределенных уравнений третьей степени.

Первые идеи в этой области были высказаны в докладе на III Всесоюзном математическом съезде [25]. В нем указывалось на аналогию между задачей погружения в теории Галуа полей алгебраических чисел и задачей классификации эллиптических кривых, определенных над полями алгебраических чисел. Объекты, изучаемые в обеих теориях, обладают локальными инвариантами, связанными с пополнениями поля определения, и основной интерес представляют именно “локально тривиальные” объекты. В случае эллиптических кривых это приводит к двум конкретным гипотезам: 1) над заданным полем p -адических чисел имеется лишь конечное число бирационально неизоморфных кубических кривых с заданным абсолютным инвариантом и 2) если над полем алгебраических чисел k задана кубическая кривая C , то над k имеется лишь конечное число бирационально неизоморфных кубических кривых, которые над всеми p -адическими пополнениями поля k изоморфны C .

Эти гипотезы были доказаны в работах 1957 г. [26], [27], причем в более общей ситуации — для эллиптических кривых степени n , а не только для кубических кривых. Здесь же была решена давно стоявшая в теории диофантовых уравнений задача: доказать существование над любым полем алгебраических чисел эллиптических кривых произвольной степени n , бирационально неизоморфных кривым степени $< n$. Все эти результаты явились первыми шагами в новом разделе алгебраической геометрии — теории главных однородных пространств, — возникшем в 50-х годах. В нем изучаются алгебраические многообразия X над незамкнутыми полями k , интересными с точки зрения теории чисел, и такие, что над замыканием $\bar{k}$ поля k X изоморфно некоторой алгебраической группе A . Наиболее интересен случай, когда A — абелево многообразие и, в частности, эллиптическая кривая. Главные однородные пространства образуют группу, которую можно интерпретировать на языке когомологий Галуа как $H^1(G, A(\bar{k}))$, где $G = \text{Gal}(\bar{k}/k)$ и $A(\bar{k})$ — группа точек, определенных над полем $\bar{k}$. Именно язык когомологий Галуа оказался связующим звеном между описанной выше задачей погружения и задачами об эллиптических кривых.

В [32] была построена топологическая двойственность в смысле Понтрягина между группой $H^1(G, A(\bar{k}))$ и группой $A(K)$ для p -адических полей. Построив тем самым локальную теорию главных однородных пространств, И.Р.Шафаревич обратился к глобальной ситуации. Поскольку для глобального (числового или функционального) поля k имеется естественный морфизм локализации

$$\varphi : H^1(G, A(\bar{k})) \rightarrow H^1(\text{Gal}(\bar{k}_p/k_p), A(\bar{k}_p)),$$

где p пробегает все точки поля k , то основной интерес предста-

вляет его ядро, состоящее из локально тривиальных однородных пространств. В честь И.Р.Шафаревича это ядро обозначается в мировой математической литературе через $\Pi(A, k)$. Его вычисление и, в частности, доказательство предполагаемой конечности являются одной из труднейших и интереснейших проблем теории диофантовых уравнений. Первые примеры эллиптических кривых с конечной группой Π были получены лишь во второй половине 80-х годов. Наиболее сильные результаты в этом направлении получены учеником И.Р.Шафаревича В.А.Колывагиным.

В обширной работе [35] И.Р.Шафаревич исследовал случай, когда основное поле k — поле функций на алгебраической кривой над алгебраически замкнутым полем k_0 . Сначала, как и для числового случая, находятся группы $H^1(G_p, A(\overline{k_p}))$ для локальных полей k_p — пополнений поля k . Для них доказывается теорема двойственности с фундаментальной группой $\pi_1(A(k_p))$ проалгебраической (над полем k_0) группы $A(k_p)$. При этом в [35] рассмотрены l -компоненты этих групп с $l \neq \text{char}(k_0)$.

Случай p -компонент разбирался в многочисленных позднейших исследованиях. В глобальной ситуации имеется также отображение φ и в [35] полностью найдена структура его ядра и коядра. Работа [35] оказала большое влияние на последующее развитие арифметики абелевых многообразий и на теорию когомологий алгебраических многообразий. Как показало будущее, в ней, по существу, содержалось вычисление группы этальных когомологий алгебраической поверхности, расслоенной на пучок алгебраических кривых. Редукция этальных когомологий к когомологиям Галуа стала впоследствии стандартным приемом.

Уже в этих работах выявилась характерная и для дальнейших исследований И.Р.Шафаревича особенность: в большинстве своих работ он подходит к геометрии как теоретико-числовик и, наоборот, к теории чисел как геометр. Именно так построен обзорный доклад на Международном математическом конгрессе 1962 г. в Стокгольме [40]. В нем особое место занимают две гипотезы И.Р.Шафаревича об алгебраических кривых X рода $g > 0$, определенных над глобальным полем k . Каждой такой кривой можно сопоставить множество S точек поля k , где она имеет плохую редукцию (в [40] введено также более тонкое понятие дифференты кривой X над k). Вдохновляясь классическими теоремами Эрмита и Минковского, И.Р.Шафаревич предположил, что число, с точностью до изоморфизма над k , кривых X с заданными инвариантами g, k и S конечно. Если же множество S пусто и $k = \mathbb{Q}$, то кривых рода $g > 0$ с такими инвариантами не существует. В функциональном случае последнюю гипотезу можно также сформулировать

для $k = k_0(t)$, если исключить так называемые постоянные кривые. Попытки доказать эти гипотезы привели к существенному продвижению в теории диофантовых уравнений и, в частности, к доказательству гипотезы Морделла о конечности числа рациональных точек на алгебраических кривых рода $g > 1$, определенных над полями алгебраических чисел.

Сравнение числовой и геометрических ситуаций, блестяще использованное И.Р.Шафаревичем уже в его работе по общему закону взаимности, является давней традицией теории чисел и алгебраической геометрии. Она восходит к Кронекеру и Гильберту. В русле этих идей в работе [55] была развита конструкция минимальных моделей и канонического класса для схем размерности два: как обычных двумерных алгебраических многообразий над классическими полями, так и алгебраических кривых над такими естественными кольцами, как кольцо целых чисел. Это единообразное изложение проливает новый свет и на геометрический, и на арифметический случай. По существу, работа [55] впервые открыла возможность серьезного рассмотрения “арифметической поверхности” как геометрического объекта: без нее немыслимы были бы последующие сильные результаты теории чисел, дающие, скажем, полное описание точек конечного порядка эллиптических кривых над полем рациональных чисел. Геометрическому анализу известной проблемы ранга эллиптических кривых посвящена заметка [60], написанная совместно с Дж.Тейтом.

В начале 60-х годов И.Р.Шафаревич собрал и возглавил небольшой коллектив семинара, результатом годичной работы которого явилась монография “Алгебраические поверхности”, изданная в “Трудах Математического института” [49] — первое и долгое время единственное систематическое изложение теории поверхностей, соединившее красоту геометрических методов итальянской школы с мощью новейших аналитических и топологических методов. Вклад И.Р.Шафаревича в теорию алгебраических поверхностей и, более специально, в сборник, значительно превосходит то, что может быть реконструировано по лично написанному тексту. Во всяком случае, глава VII [49] содержит описание класса поверхностей с эллиптическим пучком в терминах главных однородных пространств, не известных классикам, и обнаруживает, что в классической литературе была пропущена целая бесконечная серия таких поверхностей (с кратными слоями). Весь сборник [49], существование которого целиком обязано И.Р.Шафаревичу, оказал большое влияние на исследования алгебраических поверхностей во всем мире (перев. на английский — 1967 г., на немецкий — 1968 г.).

Одним из самых ярких феноменов теории алгебраических поверхностей являются поверхности типа КЗ. Каждая из этих поверхностей обладает единственной невырожденной формой ω типа $(2,0)$. Интеграл этой формы по базисным двумерным циклам удовлетворяет соотношениям, аналогичным соотношениям Римана для римановой поверхности. Двумерный цикл поляризации l дает линейное соотношение на периоды

$$\int_l \omega = 0.$$

Таким образом, поверхность X типа КЗ определяет точку в P_C^{21} с однородными координатами $\int_{\sigma_i} \omega$, (σ_i — базис в $H^2(X, C)$), принадлежащую открытому девятнадцатимерному многообразию Ω , которое оказывается классическим симметрическим пространством. В 1971 г. И.Р.Шафаревич в работе [67] доказал (совместно с И.И.Пятецким–Шапиро), что поверхность X однозначно определяется соответствующей точкой симметрического пространства Ω . Это — аналог знаменитой теоремы Торелли для римановых поверхностей.

В конце 80-х г.г. И.Р.Шафаревич обратил внимание на то, что остается совершенно открытым вопрос об описании рациональных отображений поверхностей типа КЗ, в то время, как теорема Торелли дает полное описание самих поверхностей. Иначе говоря, вопрос стоит в выяснении того, как восстановить категорию поверхностей типа КЗ из категории решеток периодов и морфизмов между ними. Более точно, рациональное отображение поверхностей определяет ортогональный морфизм (изогению) рациональных структур Ходжа, соответствующих трансцендентным циклам, и задача состоит в определении тех изогений, которые отвечают рациональным отображениям исходных поверхностей. Ранг соответствующих Q -пространств может принимать значения от 2 до 21. Для случаев ранга 2 и 3 было показано (совместно с В.В.Никулиным), что отображения поверхностей описываются изогениями рациональных структур Ходжа.

Аналитические методы исследования поверхностей типа КЗ зались непреодолимым препятствием изучения этих поверхностей над полями конечной характеристики. Однако большой цикл работ ([74] – [81], [83]) открыл возможность найти аналог теории периодов и в этом трудном случае. В работе [74] было доказано, что на поверхностях типа КЗ в конечной характеристике отсутствуют векторные поля. Этот результат дал возможность описать деформации поверхностей типа КЗ и построить их многообразие модулей.

Для суперсингулярных поверхностей, у которых все двумерные циклы — алгебраические, можно определить “пространство периодов” и отображение из многообразия модулей в это пространство. В работе [78] получена глобальная теорема Торелли для суперсингулярных поверхностей над полем характеристики два. Кроме того, глобальную теорему Торелли над полем любой конечной характеристики удалось свести к проблеме “невыврождения” суперсингулярных поверхностей. Эта проблема была решена в работе [80] для сильно эллиптических поверхностей. Наконец, в работе [83] получена теорема “невыврождения” как частный случай теории поведения высоты формальной группы Брауэра поверхности при специализации. Тем самым был доказан аналог глобальной теоремы Торелли для суперсингулярных поверхностей типа КЗ.

Помимо работ, объединенных в большие циклы, — также характерная черта научного творчества И.Р.Шафаревича — у него имеется несколько работ по алгебраической геометрии, стоящих особняком. Среди них работа [53], в которой была сделана попытка построить алгебраический аналог теории униформизации для алгебраических многообразий — факторов однородных областей по арифметическим группам. В работе [58] (см. также [82]) изучаются такие группы, как группы автоморфизмов кольца многочленов от $n > 2$ переменных. Хотя ими много занимались, работа И.Р.Шафаревича остается почти единственной, где имеются общие и точные результаты. В случае $n = 2$ дано точное описание группы в терминах разложения в свободное произведение. Полученные факты применены к доказательству того, что у аффинной плоскости нет нетривиальных форм. В случае $n > 3$ получены результаты о структуре алгебр Ли соответствующих групп. Проблема нахождения их “проинтегрированных” версий очень трудна: после работы [58] в ней, по существу, не было прогресса.

К середине 60-х годов в широких кругах математиков пробудился интерес к классификации Э.Картаном простых транзитивных псевдогрупп преобразований. В МИАН СССР некоторое время (1964 – 1966 г.г.) функционировал семинар под руководством И.Р.Шафаревича, на котором обсуждались разные работы по псевдогруппам Ли. Отчасти результатом этой деятельности явились две работы [51], [62], определившие на долгие годы программу классификации простых конечномерных алгебр Ли над алгебраически замкнутым полем характеристики $p > 0$. К тому времени в теории модулярных простых алгебр Ли накопился огромный фактический материал. Казалось, что изобретательности, проявляемой при построении все новых и новых примеров простых алгебр, не будет конца. Важным моментом было появление работы [51], в которой

обращалось внимание на тот факт, что все известные неклассические простые p -алгебры Ли при $p > 5$ укладываются в четыре бесконечные серии алгебр картановского типа W_n, S_n, H_n, K_n — общие, специальные, гамильтоновы и контактные. В работе [51] была высказана гипотеза, что алгебры картановского типа вместе с классическими исчерпывают все простые p -алгебры Ли ($p > 5$). Полученные до сих пор в разных странах результаты прекрасно согласуются с этой гипотезой, причем оказалось, что ограничение $p > 5$ существенно. В работе [62] техника полных картановских продолжений была развита в применении к произвольным алгебрам Ли, не обязательно обладающим p -структурой. Были сконструированы и изучены эталонные примеры простых градуированных алгебр Ли. Фактическими результатами работы [62] положено начало реализации обширной классифицированной программы. Эта работа цитируется практически в каждом исследовании, посвященном модулярным простым алгебрам Ли.

В последние годы внимание И.Р.Шафаревича было привлечено к изучению структуры многообразия неположенных коммутативных алгебр. Наличие в этой задаче непрерывных параметров делает естественным использование методов алгебраической геометрии. Все коммутативные и ассоциативные законы умножения на данном n -мерном векторном пространстве определяют алгебраическое многообразие. В работе [97] автор ограничивается рассмотрением первого нетривиального случая, когда изучаемые алгебры N имеют класс нильпотентности 2 (т.е. $N^3 = 0$). Изучаются неприводимые компоненты в многообразии таких алгебр, найдены их размерности и особые точки. Оказывается, что компоненты определяются рангом r квадрата N^2 алгебры N . Все компоненты можно разделить на два класса — устойчивые и неустойчивые компоненты. Если d — число образующих алгебры, то доказано, что компоненты, соответствующие значениям $2 < r \leq (d-1)(d-2)/6 + 2$, являются устойчивыми, кроме, быть может, случая $d = 5, r = 4$, а компоненты с $r \geq (d^2 - 1)/3$ и $r = 1, 2$ неустойчивы. Так как всегда $r \leq d(d+1)/2$, то интервал возможных значений для r разделяется на три примерно равные части (асимптотически по d), причем часть меньших значений для r соответствует устойчивым компонентам, часть больших значений — неустойчивым, а для средней части ответ остается неизвестным. Каждая алгебра класса два определяет r симметрических матриц, в терминах которых формулируется критерий устойчивости. Для $r = 3$ он тесно связан с известным в теории векторных расслоений на проективной плоскости условием Барта. Все эти конструкции и результаты являются первыми шагами в новой теории классификации коммутативных

алгебр.

И.Р.Шафаревичем написано несколько монографий и учебников (часть из них с соавторами). Уникальной является книга “Теория чисел” [46], созданная на основе многолетних лекционных курсов, читавшихся им в Московском университете. Книга эта вышла двумя изданиями [71], [90] и переведена на все основные языки мира (английский, немецкий – 1966 г., французский – 1967 г., японский – 1971 г.). Огромную популярность завоевали также “Основы алгебраической геометрии” [70] — один из лучших в мировой литературе учебников по алгебраической геометрии. Прозрачность и ясность изложения, обилие неформальных примеров и мотивировок, постепенный переход от простейших ситуаций к более сложным — характерные черты книг И.Р.Шафаревича.

Это в полной мере относится к обзорам [91], [96], написанным Шафаревичем для “Энциклопедии математических наук”, начавшей выходить у нас в 80-е годы стараниями Р.В.Гамкрелидзе. И.Р.Шафаревич с самого начала принял самое активное участие в формировании общих принципов этого издания, по существу, совпадающих с приведенными выше особенностями его книг. Редактируя выпуски по алгебре, теории чисел и алгебраической геометрии, он оказал определяющее влияние на содержание и стиль вошедших в них обзоров. Написанный на едином дыхании обзор основных понятий алгебры [91] сразу же приобрел широкую известность и не только в математических кругах. Почти 80 выпусков этого издания, в появлении которого роль И.Р.Шафаревича весьма велика, дают панораму почти всей современной математики.

Среди учеников И.Р.Шафаревича более трех десятков кандидатов и докторов наук — алгебраистов, геометров, специалистов по теории чисел. С 1960 г. И.Р.Шафаревич заведует отделом алгебры Математического института АН СССР. Он — член редакции математической серии “Известий АН СССР”. С 1970 по 1974 г. И.Р.Шафаревич был президентом Московского математического общества. И.Р.Шафаревич — академик Российской Академии Наук.

Научные заслуги И.Р.Шафаревича получили широкое международное признание. Он является членом Национальной Академии наук США, Американской академии наук и искусств, Лондонского королевского общества, Германской академии естествоиспытателей “Леопольдина”, Национальной Академии Наук Италии “Дей Линчеи”. И.Р.Шафаревич удостоен Ленинской премии, премии Хейнемана Геттингенской академии наук и избран почетным доктором Парижского университета.

**СПИСОК МАТЕМАТИЧЕСКИХ
ПУБЛИКАЦИЙ И.Р. ШАФАРЕВИЧА**

1943

- 1 О нормируемости топологических полей. *Доклады АН СССР*, т. **40**, N 1, 1943, 149–151.

1945

- 2 Об абсолютных группах Галуа относительно-абелевых расширений. В *Рефераты научно-исследовательских работ за 1943–44 г. Отд. физ.-матем. наук АН СССР*. Москва–Ленинград (1945).

1946

- 3 О p -расширениях. В *Рефераты научно-исследовательских работ за 1945 г. Отд. физ.-матем. наук АН СССР*. Москва–Ленинград (1946).

- 4 О группах Галуа p -адических полей. Резюме докторской диссертации. *Доклады АН СССР*, т. **53**, N 1, 1946, 15–16.

- 5 Исследования о конечных расширениях. Резюме докторской диссертации. *Успехи Матем. Наук*, т. **2**, N 2, 1946, 223–226.

1947

- 6 О p -расширениях. *Матем. Сб., Нов. сер.*, т. **20(62)**, N 2, 1947, 351–363.

1948

- 7 Общий закон взаимности. *Успехи Матем. Наук*, т. **3**, N 3, 1948, 165.

1949

- 8 Общий закон взаимности. *Доклады АН СССР*, т. **64**, N 1, 1949, 25–28.

1950

- 9 Общий закон взаимности. *Матем. Сб., Нов. сер.*, т. **26(68)**, N 1, 1950, 113–146.

- 10 Алгебраическая геометрия. *Больш. Сов. Энцикл.*, 2-е изд., т. **2**, 1950, 62–63.

1951

- 11 Новое доказательство теоремы Кронекера–Вебера. *Труды Матем. Инст. им. В.А. Стеклова*, т. **38**, 1951, 382–387.

1952

- 12 Общий закон взаимности и его приложения в теории полей алгебраических чисел. *Труды I Конгр. Венгерских Матем.* 1950, 291–298, 1952.
- 13 Конференция по алгебре и теории чисел. *Успехи Матем. Наук*, т. 7, N 3, 1952, 151–154.
1953
- 14 Комментарии к статье: “О числе решений сравнения степени три”. В Г.Ф. Вороной, *Собрание сочинений*, т.3, стр.205. Киев, Изд. Акад. Наук Укр. ССР, 1953.
- 15 Комментарии к статье: “Замечание о последней теореме Ферма относительно неразрешимости уравнения $x^p + y^p = z^p$ в целых числах x, y, z при нечетном простом числе p ”. В Г.Ф. Вороной, *Собрание сочинений*, т.3, стр.247. Киев, Изд. Акад. Наук Укр. ССР, 1953.
1954
- 16 О построении полей с заданной группой Галуа порядка l^α . *Изв. Акад. Наук СССР, Сер. матем.*, т. 18, 1954, 261–296.
- 17 Об одной теореме существования в теории полей алгебраических чисел. *Изв. Акад. Наук СССР, Сер. матем.*, т. 18, 1954, 327–334.
- 18 О задаче погружения полей. *Изв. Акад. Наук СССР, Сер. матем.*, т. 18, 1954, 389–418.
- 19 Построение полей алгебраических чисел с заданной разрешимой группой Галуа. *Изв. Акад. Наук СССР, Сер. матем.*, т. 18, 1954, 525–578.
- 20 О расширениях полей алгебраических чисел, разрешимых в радикалах. *Доклады АН СССР*, т. 95, N 2, 1954, 227–227.
- 21 О задаче погружения полей. *Доклады АН СССР*, т. 95, N 3, 1954, 459–461.
- 22 О решении уравнений высших степеней (метод Штурма). Москва, Гостехтеориздат, 1954, 24 стр. Немецкий перевод: Berlin, Deutscher Verlag der Wissenschaften, 1956.
- 23 Предисловие к: “Автоморфные функции нескольких комплексных переменных”, К.Л. Зигель, Москва, Гостехтеориздат, Москва–Ленинград, Изд. Иностранной Литературы, 1954, 3–4.
- 24 (с Д.Е. Меньшовым и др.) 16-я Московская Математическая Олимпиада. *Успехи Матем. Наук*, т. 9, N 3, 1954, 257–262.
1956
- 25 Теория Галуа и арифметика полей алгебраических чисел. *Труды 3-го Всесоюзного Математического Съезда*, Москва, 1956.
1957
- 26 О бирациональной эквивалентности эллиптических кривых. *Доклады АН СССР*, т. 114, N 2, 1957, 267–270.
- 27 Показатели эллиптических кривых. *Доклады АН СССР*, т. 111, N 4, 1957, 714–716.

- 28 (с А.И. Кострикиным) Группа гомологий нильпотентных алгебр. *Доклады АН СССР*, т. **115**, N 6, 1957, 1066–1069.
1958
- 29 Задача погружения для распадающихся расширений. *Доклады АН СССР*, т. **120**, N 6, 1958, 1217–1219.
- 30 Дмитрий Константинович Фаддеев (к его 50-летию). *Успехи Матем. Наук*, т. **13**, N 1, 1958, 233–236.
- 31 Аналитические многообразия и алгебраическая геометрия (обзорная статья). *Успехи Матем. Наук*, т. **13**, N 2, 1958.
1959
- 32 Группы главных однородных алгебраических многообразий. *Доклады АН СССР*, т. **124**, N 4, 1959, 42–43.
- 33 (с С.П. Демушкиным) Задача погружения для локальных полей. *Изв. Акад. Наук СССР, Сер. матем.*, т. **23**, N 6, 1959, 823–840.
- 34 Впечатления от Международного Математического Конгресса в Эдинбурге. *Успехи Матем. Наук*, т. **14**, N 2, 1959, 243–246.
1961
- 35 Главные однородные пространства, определенные над полем функций. *Труды Матем. Инст. им. В.А. Стеклова*, т. **64**, 1961, 316–346.
- 36 Борис Николаевич Делоне (к его 70-летию). *Успехи Матем. Наук*, т. **16**, N 3, 1958, 239–241.
1962
- 37 Памяти Франческо Севери. *Вестник Акад. Наук СССР*, т. **2**, 1962, 99–100.
- 38 Contributii Sovietice la teoria lui Galois. *Bucaresti*, 1962, 1–167; *Acad. Republicii Populare Romine*, N 3, 3–36, N 3, 37–93.
- 39 (с С.П. Демушкиным) Второе препятствие для задачи погружения полей алгебраических чисел. *Изв. Акад. Наук СССР, Сер. матем.*, т. **26**, N 6, 1962, 911–924.
1963
- 40 Поля алгебраических чисел. *Proc. Int. Cong. Math. Stockholm 1962*, Inst. Mittag-Leffler, Djursholm, 1963, 163–176.
- 41 Einige Anwendungen der Galoischen Theorie auf Diophantische Gleichungen. *Ber. Dirichlet Tagung*, Berlin, 1963.
1964
- 42 Расширения с заданными точками ветвления. *Publ. Math. Inst. Haut. Etud. Sci. Paris*, vol. **18**, 1964, 295–319.
- 43 (с Е.С. Голодом) О башне полей классов. *Изв. Акад. Наук СССР, Сер. матем.*, т. **28**, N 2, 1964, 261–272.
- 44 Юрий Иванович Манин. *Молодой Коммунист*, N 3, 1964, 61.
- 45 (с С.П. Новиковым и И.И. Пятацким-Шапиро) Фундаментальные направления развития алгебраической топологии и алгебраической геометрии. *Успехи Матем. Наук*, т. **19**, N 6, 1964, 75–82.

- 46 (с З.И. Боровичем) Теория чисел. Москва, Наука, 1964. Немецкий перевод: *Basel-Stuttgart, Birkhäuser Verlag*, 1966; Английский перевод: *New York-London, Academic Press*, 1966; Французский перевод: *Paris, Gauthier-Villars*, 1967; Японский перевод: *Tokyo, Joshioka Shoten*, 1971.
- 47 Конференция по теории чисел. Обервольфах, ФРГ, 6–12 сент. 1964. *Вестник Акад. Наук СССР*, т. 12, 1964, 63–64.
- 48 Лекции по высшей алгебре. Москва, МГУ, 1963, 1–38. 1965
- 49 (с Б.Г. Авербухом и др.) Алгебраические поверхности. *Труды Матем. Инст. им. В.А. Стеклова*, т. 75, 1965, 3–215. Английский перевод: *Providence, Amer. Math. Soc.*, 1967; Немецкий перевод: *Leipzig, Akademische Verlagsgesellschaft*, 1968. Предисловие. Линейчатые поверхности. Поверхности с пучком эллиптических кривых.
- 50 Предисловие к сборнику работ “Комплексные пространства.” Москва, Мир, 1965, 5–10. 1966
- 51 (с А.И. Кострикиным) Псевдогруппы Картана и p -алгебры Ли. *Доклады АН СССР*, т. 168, N 4, 1966, 740–742.
- 52 (с А.И. Кострикиным) Псевдогруппы Картана и p -алгебры Ли. Тезисы. Труды Международного Конгресса Математиков. Секция 2, Москва, Мир, 1966.
- 53 (с И.И. Пятецким-Шапиро) Теория Галуа трансцендентных расширений и униформизация. *Изв. Акад. Наук СССР, Сер. матем.*, т. 30, N 3, 1966, 671–704.
- 54 (с И.И. Пятецким-Шапиро) Теория Галуа трансцендентных расширений и униформизация. В *Современные проблемы теории аналитических функций*. Ереван 1965, 262–264. Москва, Наука, 1966.
- 55 Lectures on minimal models and birational transformations of two-dimensional schemes. *Tata Institute of Fundamental Research, Bombay*, 1966, 175 pp.
- 56 (с А.А. Кирилловым) Вторая летняя школа по топологии. *Успехи Матем. Наук*, т. 21, N 2, 1966, 257–258.
- 57 Über das Klassenkorperproblem. *Berichte Math. Forschungs Inst. Oberwolfach*, Heft 2, 1966, 265. 1967
- 58 On some infinite-dimensional groups. В *Simposio Internazionale di Geometria Algebrica. Roma 1967*, Edizione Cremonese, 208–212.
- 59 (с А.Н. Рудаковым) Неприводимые представления простой трехмерной алгебры Ли над полями конечной характеристики. *Матем. Заметки*, т. 2, N 5, 1967, 439–454.
- 60 (с Дж. Тэйтом) О ранге эллиптических кривых. *Доклады АН СССР*, т. 175, N 4, 1967, 770–773.

1968

- 61 Алгебраическая геометрия. Москва, МГУ, 1968, 250 стр..

1969

- 62 (с А.И. Кострикиным) Градуированные алгебры Ли конечной характеристики. *Изв. Акад. Наук СССР, Сер. матем.*, т. **33**, N 2, 1969, 251–322.

- 63 Дзета-функция. Москва, МГУ, 1969, 148 стр.

- 64 Основы алгебраической геометрии. *Успехи Матем. Наук*, т. **24**, N 6, 1969, 3–184; Немецкий перевод: *Friedrich Vieweg und Sohn*, 1972; Венгерский перевод: *Magyar Tud. Akad. mat. fiz. Tud. Oszt.*, **22**, 1974, 79–184 и **22**, 1975, 283–360.

1970

- 65 Предисловие к: Н. Koch. Galoissche Theorie der 3-Erweiterungen. *Berlin, Deutsche Verlag der Wissenschaften*, Mathematische Monographien, Bd. 1, 1970, 3–4.

- 66 Le Theoreme de Torelli pour les surfaces algebriques de type K3. *Actes Congres Intern. Math. Nice 1970*, **1**, 1971, 413–417.

1971

- 67 (с И.И. Пятецким-Шапиро) Теорема Торелли для алгебраических поверхностей типа K3. *Изв. Акад. Наук СССР, Сер. матем.*, т. **35**, N 3, 1971, 530–572.

- 68 Лекции по высшей алгебре. Москва, МГУ, 1971, 40 стр.

- 69 (с В.И. Арнольдом, И.М. Гельфандом, Б.И. Маниным, Б.Г. Мойшензоном, и С.П. Новиковым) Галина Николаевна Тюрина (некролог). *Успехи Матем. Наук*, т. **26**, N 1, 1971, 207–211.

- 70 Основы алгебраической геометрии. Москва, Наука, 1971, 567 стр.; Немецкий перевод: *Berlin, Deutsche Verlag der Wissenschaften*, 1972; Английский перевод: *Grundlehren der Math. Wissenschaften*, **213**, Berlin, Heidelberg, New York, 1974; Румынский перевод: *Bucharesti, Editura stiintifica enciclopedia*, 1976.

1972

- 71 (с З.И. Боровичем) Теория чисел. Изд. 2-е. Москва, Наука, 1972, 495 стр.

1973

- 72 (с И.И. Пятецким-Шапиро) Арифметика поверхностей типа K3. *Труды Матем. Инст. им. В.А. Стеклова*, т. **132**, 1973, 44–54.

- 73 О некоторых тенденциях развития математики. *Jahrb. Akad. Wiss. Göttingen*, 1973, 31–36; Английский перевод: *Math. Intelligencer*, т. **3**, 1981, 182–184.

1976

- 74 (с А.Н. Рудаковым) Несепарабельные морфизмы алгебраических поверхностей. *Изв. Акад. Наук СССР, Сер. матем.*, т. **40**, N 6, 1976, 1269–1307.

1977

- 75 (с А.Н. Рудаковым) Замечание к работе “Несепарабельные морфизмы алгебраических поверхностей.” *Изв. Акад. Наук СССР, Сер. матем.*, т. **41**, N 2, 1977, 476.

1978

- 76 (с А.Н. Рудаковым) Квазиэллиптические поверхности типа КЗ. *Успехи Матем. Наук*, т. **33**, N 1, 1978, 227–228.
77 (с А.Н. Рудаковым) Векторные поля на эллиптических поверхностях. *Успехи Матем. Наук*, т. **33**, N 6, 1978, 231–232.
78 (с А.Н. Рудаковым) Суперсингулярные поверхности типа КЗ над полями характеристики 2. *Изв. Акад. Наук СССР, Сер. матем.*, т. **42**, N 4, 1978, 848–869.

1981

- 79 (с А.Н. Рудаковым) Поверхности типа КЗ над полями конечной характеристики. В *Итоги Науки и Техники, Сер. Совр. Probl. Матем.*, т. **18**, 1981, 115–207.
80 (с А.Н. Рудаковым) О вырождении поверхностей типа КЗ над полями конечной характеристики. *Изв. Акад. Наук СССР, Сер. матем.*, т. **45**, N 3, 1981, 646–661.
81 (с А.Н. Рудаковым) О вырождении поверхностей типа КЗ. *Доклады АН СССР*, т. **259**, 1981, 1050–1052.

- 82 О некоторых бесконечномерных группах. II. *Изв. Акад. Наук СССР, Сер. матем.*, т. **45**, N 1, 1981, 214–226.

1982

- 83 (с А.Н. Рудаковым и Т. Цинком) Влияние высоты на вырождение алгебраических поверхностей типа КЗ. *Изв. Акад. Наук СССР, Сер. матем.*, т. **46**, N 1, 1982, 117–134.

1983

- 84 (с В.В. Никулиным) Геометрии и группы. Москва, Наука, 1983; Английский перевод: Springer-Verlag, Berlin-Heidelberg- New York-Tokyo, 1987; Японский перевод: Springer-Verlag, 1993.

- 85 Zum 150 Geburtstag von Alfred Clebsch. *Math. Ann.*, т. **266**, 1983, 135–140.

- 86 Предисловие к: Дж. Милн “Этальные когомологии”, Москва, Мир, 1983, 5–6.

1984

- 87 (с А.Н. Паршиным) Арифметика алгебраических многообразий. *Труды Матем. Инст. им. В.А. Стеклова*, т. **168**, 1984, 72–97.

- 88 (с А.Н. Рудаковым) О вырождении поверхностей типа КЗ. *Труды Матем. Инст. им. В.А. Стеклова*, т. **166**, 1984, 222–234.

- 89 Анри Пуанкаре. Мысли о науке (рецензия). *Техника и Наука*, т. **2**, 1984, 42–43.

1985

- 90 (с З.И. Боровичем) Теория чисел. Изд. 3-е. Москва, Наука, 1985, 503 стр.

- 1986
- 91 Основные понятия алгебры. В: *Итоги Науки и Техники, Сер. Совр. Пробл. Матем., Фундаментальные направления*, т. 11, 1986, 288 стр.
- 1988
- 92 Алгебраическая геометрия, т.т. I и II. Изд. 2-е. Москва, Наука, 1988, т. I – 351 стр., т. II – 304 стр.
- 1989
- 93 Так сделайте невозможное! (к 80-летию Л.С. Понтрягина) “*Советская Россия*”, 16 апреля 1989.
- 94 О проблеме Люрота. *Труды Матем. Инст. им. В.А. Стеклова*, т. 183, 1989.
- 95 О факторах одного убывающего центрального ряда. *Матем. Заметки*, т. 45, N 3, 1989, 114–118.
- 96 (с В.А. Исковских) Алгебраические поверхности. В: *Итоги Науки и Техники, Сер. Совр. Пробл. Матем., Фундаментальные направления*, т. 35, 1989, 131–271.
- 1990
- 97 Деформации коммутативных алгебр класса 2. *Алгебра и Анализ*, т. 2, N 6, 1990, 178–194.
- 98 Дмитрий Константинович Фаддеев (к годовщине смерти). *Алгебра и Анализ*, т. 2, N 6, 1990, 3–9.
- 1991
- 99 Abelian and Nonabelian Mathematics. *The Math. Intelligencer*, т. 13, 1991, 67–75.
- 100 Властитель Стекловки (к 100-летию со дня рождения И.М. Виноградова)¹. *Вестник Акад. Наук СССР*, N 9, 1991, 96–100.
- 1994
- 101 Mathematical reasoning versus Nature. *Comment. Math. Univ. Sancti Pauli*, v. 43, N 1, 1994, 109–116.
- 102 On the Arithmetics of Singular K3-surfaces. *International Conference on Algebra and Analysis in Honour of N.G. Chebotarev (1894–1947)*, June 6–11, 1994, Kazan. Proceedings (в печати).
- 1995
- 103 On Some Arithmetic Properties of Algebraic Varieties. *Second Asian Mathematical Conference*, October 17–20, 1995, Nakhon Ratchasima, Thailand. Proceedings (в печати).

¹Без согласия автора название переделано в: “Патриарх советской математики”.

ТЕОРИЯ ЧИСЕЛ

О ГРУППАХ ГАЛУА p -АДИЧЕСКИХ ПОЛЕЙ

ДОКЛ. АКАД. НАУК СССР Т. LIII, no.1 (1946)

В этой заметке решается такой вопрос: пусть R — поле p -адиических чисел, k — нормальное расширение R и K — абелево расширение k , заданное своей группой норм H в k ; как найти группу Галуа K/R (если оно нормально), зная k и H ?

Обозначим группы Галуа: K/R — через $G = \{g, h, \dots\}$, k/R через $F = \{\sigma, \tau, \dots\}$ и K/k — через $\mathfrak{A} = \{\alpha, \beta, \dots\}$.

Пусть $(F: 1) = m$, $(\mathfrak{A}: 1) = n$. По условию $\mathfrak{A}$ — абелев нормальный делитель G с факторгруппой F . Для определения G по $\mathfrak{A}$ и F достаточно задать в $\mathfrak{A}$ автоморфизмы $\alpha \rightarrow \alpha^\sigma$ и систему множителей ([1], стр. 93). При этом, если $\bar{\sigma}, \bar{\tau}$ — система представителей классов G по $\mathfrak{A}$, то

$$\bar{\sigma} \bar{\tau} = \alpha_{\sigma, \tau} \bar{\sigma} \bar{\tau}. \quad (1)$$

Пусть A — нормальная простая алгебра над R степени m с инвариантом $1/m$ ([2], стр. 112). Известно, что A содержит максимальное коммутативное подполе степени m , изоморфное k ([2], стр. 113). Тогда

$$A = (t_\sigma, k, a_{\sigma, \tau}) \quad a_{\sigma, \tau} \in k.$$

Пусть, наконец, $aH \rightarrow \alpha(aH)$ — изоморфизм между k^*/H и $\mathfrak{A}$, установленный при помощи символа Hasse ([3], стр. 149).

Теорема. K/R нормально тогда и только тогда, когда H инвариантно относительно $\sigma \in F$. Если K/R нормально, то автоморфизмы и система множителей в $\mathfrak{A}$ определяются так:

$$\alpha^\sigma(aH) = \alpha(a^\sigma H); \quad (2)$$

$$\alpha_{\sigma, \tau} = \alpha(a_{\sigma, \tau} H). \quad (3)$$

Утверждение (2) легко следует из свойства символа Hasse ([3], стр. 151). Для доказательства (3) рассмотрим, кроме A , еще две

простые алгебры B и C с центрами R и k , степеней mn и n и с инвариантами $1/mn$ и $1/n$:

$$B = (u_g, K/R, b_{g,h}), \quad C = (v_\alpha, K/k, c_{\alpha,\beta}).$$

Известно [4], что при помощи C можно следующим образом вычислить $\alpha_{\sigma,\tau}$:

$$\alpha_{\sigma,\tau} = \alpha(V(v_{\alpha_{\sigma,\tau}})H) = \alpha\left(\prod_{\beta \in \mathfrak{A}} c_{\beta, \alpha_{\sigma,\tau}} H\right). \quad (4)$$

Алгебра B дает возможность из (4) вывести (3). Для этого заметим, что подалгебра B , состоящая из элементов, коммутирующих с k , имеет вид $(u_\alpha, K/k, b_{\alpha,\beta})$. Ее инвариант над k есть $1/n$ [5] и, следовательно, она изоморфна C . Из (4) получаем:

$$\alpha_{\sigma,\tau} = \alpha\left(\prod_{\beta \in \mathfrak{A}} b_{\beta, \alpha_{\sigma,\tau}} H\right). \quad (5)$$

Чтобы и алгебру A связать с B , рассмотрим B^n . С одной стороны, известно [6], что

$$B^n \sim \left(k/R, N_{K/k}(b_{\sigma,\tau}) \prod_{\beta \in \mathfrak{A}} b_{\beta, \sigma\tau} b_{\beta, \sigma\tau}^{-1}\right),$$

а с другой стороны, инвариант B^n есть $1/m$ и, следовательно, $B^n \sim A$, т.е.

$$\alpha_{\sigma,\tau} \sim N_{K/k}(b_{\sigma,\tau}) \prod_{\beta \in \mathfrak{A}} b_{\beta, \sigma\tau} b_{\beta, \sigma\tau}^{-1}. \quad (6)$$

Соединяя (5) и (6), видим, что (3) эквивалентно следующей формуле:

$$N_{K/k}(b_{\sigma,\tau}) \prod_{\beta \in \mathfrak{A}} b_{\beta, \sigma\tau} b_{\beta, \sigma\tau}^{-1} \sim \prod_{\beta \in \mathfrak{A}} b_{\beta, \alpha_{\sigma,\tau}} H. \quad (7)$$

Для ее доказательства перемножим условия ассоциативности для $b_{g,h}$

$$b_{g,h}^\beta b_{\beta,g,h} = b_{\beta,g} b_{\beta g,h}$$

по всем $\beta \in \mathfrak{A}$. В результате получится:

$$N_{K/k}(b_{g,h}) \prod_{\beta \in \mathfrak{A}} b_{\beta,g,h} = \prod_{\beta \in \mathfrak{A}} b_{\beta,g} b_{\beta g,h}.$$

Положим здесь $g = \alpha_{\sigma, \tau}$ и $h = \overline{\sigma\tau}$ и заменим согласно (1) (так как $\alpha_{\sigma, \tau} \in \mathfrak{A}$, то $\prod_{\beta} b_{\beta\alpha_{\sigma, \tau}, \overline{\sigma\tau}} = \prod_{\beta} b_{\beta, \overline{\sigma\tau}}$):

$$N_{K/k}(b_{\alpha_{\sigma, \tau}, \overline{\sigma\tau}}) \prod_{\beta} b_{\beta, \overline{\sigma\tau}} = \prod_{\beta} b_{\beta, \alpha_{\sigma, \tau}} b_{\beta, \overline{\sigma\tau}},$$

т.е.

$$\prod_{\beta} b_{\beta, \alpha_{\sigma, \tau}} H = N_{K/k}(b_{\alpha_{\sigma, \tau}, \overline{\sigma\tau}}) \prod_{\beta} b_{\beta, \overline{\sigma\tau}} b_{\beta, \overline{\sigma\tau}}^{-1} H.$$

В виду того, что все множители вида $N_{K/k}(b) \in H$ можно откинуть, эта формула доказывает (7).

(Поступило в редакцию 18 февраля 1946 г.)

Литература

- [1] Н. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig, 1937.
- [2] M. Deuring, *Algebren*, 1935.
- [3] C. Chevalley, J. reine, angew. Math. **169** (1932), 140.
- [4] F. Nakayama, Math. Ann. **112** (1935), 85.
- [5] G. Köthe, Math. Ann. **107** (1933), 761.
- [6] E. Witt, J. reine, angew. Math. **173** (1936), 191.

О p -РАСШИРЕНИЯХ
МАТ. СБОРН. Т.20 (62) no.2 (1947)

Введение

В этой статье исследуются конечные, нормальные невырождающиеся расширения, степень которых есть степень простого числа p . В дальнейшем они будут называться p -расширениями.

В зависимости от того, расширения какого основного поля мы рассматриваем, работа делится на две части.

В первой части (§§ 1–2) за основное поле берется поле p -адических чисел, не содержащее корня степени p из единицы. Здесь p есть простой идеал, делящий p .

Обозначим основное поле через k и его степень над полем рациональных p -адических чисел – через n_0 . Основной результат тогда можно сформулировать следующим образом:

Теорема 1. p -расширения поля k находятся во взаимно однозначном соответствии с нормальными делителями свободной группы S с $n_0 + 1$ образующими, индекс которых есть степень p . При этом, если полю K соответствует нормальный делитель N , то группа Галуа K изоморфна S/N . Если полям K и K_1 соответствуют нормальные делители N и N_1 , то из $K \supset K_1$ следует, что $N \subset N_1$, и наоборот.

Эту теорему можно рассматривать как обобщение локальной теории полей классов.

Сформулированная теорема дает возможность свести ряд вопросов о p -расширениях k к вопросам теории групп. При помощи теоретико-групповых рассуждений здесь решаются следующие вопросы:

1. О существовании расширения k с данной p -группой Галуа.
2. О числе расширений k с данной p -группой Галуа.
3. О вложимости p -расширения в p -расширение с большей группой Галуа.

Ответы оказываются следующими:

1. Конечная p -группа реализуется в качестве группы Галуа некоторого расширения поля k тогда и только тогда, когда число ее образующих d не больше $n_0 + 1$.

2. Если $d \leq n_0 + 1$, p^n – порядок p -группы и α – число ее автоморфизмов, то число расширений, группа Галуа которых изоморфна этой группе, равно

$$\frac{1}{\alpha} p^{(n_0+1)(n-d)} (p^{(n_0+1)} - 1) (p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1}) .$$

3. Пусть даны две p -группы G и $\bar{G}$, причем G – гомоморфна $\bar{G}$ и гомоморфизм этот фиксирован. Если число образующих G (а следовательно, и $\bar{G}$) не больше $n_0 + 1$, то у любого поля с группой Галуа $\bar{G}$ существует такое расширение с группой Галуа G (над k), что естественный гомоморфизм G на $\bar{G}$ будет совпадать с заданным.

§ 1 посвящен доказательству теоремы 1, а § 2 – выводу следствий.

Во второй части (§ 3) за основное поле берется поле алгебраических функций с алгебраически замкнутым полем констант характеристики $p \neq 0$, при этом исследуются только неразветвленные p -расширения.

Оказывается, что для этого случая имеют место совершенно аналогичные результаты. Единственное изменение заключается в том, что числом образующих свободной группы S , при помощи которой описываются неразветвленные p -расширения, является теперь не $n_0 + 1$, а число γ , определенное для любого поля алгебраических функций характеристики p Hasse и Witt'ом [5].

Эти результаты совпадают в частном случае абелевых полей с результатами Witt'a и Schmid'a [6].

§ 1

Введем следующие обозначения:

k – поле p -адических чисел, не содержащее корня степени p из единицы;

K – p -расширение поля k ;

K^* – мультипликативная группа K ;

$(K^*)^p$ – подгруппа K^* , порожденная p -ми степенями;

K_1 – расширение k , являющееся композитом всех циклических полей степени p ; если K_{i-1} уже определено, то $K_i = (K_{i-1})_1$;

n_0 – степень k над полем рациональных p -адических чисел;

S – свободная группа с $n_0 + 1$ образующими;

$G^{(1)}$ – для любой группы G подгруппа, порожденная коммутаторами и p -ми степенями; если $G^{(i-1)}$ уже определено, то $G^{(i)} = (G^{(i-1)})^{(1)}$;
 $\mathfrak{P}^{(i)} = S/S^{(i)}$.

Докажем теперь теорему 1, сформулированную во введении.

Известно, что если G имеет конечное число образующих, то $(G : G^{(1)}) < \infty$ [1]; но тогда легко доказать индукцией по i , что любое $G^{(i)}$, как подгруппа конечного индекса в группе с конечным числом образующих, имеет тоже конечное число образующих и, следовательно, $(G : G^{(i)}) < \infty$ для любого i .

В частности, $\mathfrak{P}^{(i)}$ – всегда конечная группа.

Из теории полей классов известно, что K_{i+1}/K_i есть конечное расширение и его группа Галуа изоморфна $K_i^*/(K_i^*)^p$. Ясно, что K_i – максимальное из всех тех p -расширений, для группы Галуа которых имеет место соотношение $G^{(i)} = (e)$. Согласно основной теореме теории Галуа, все такие расширения находятся во взаимно однозначном соответствии с нормальными делителями группы Галуа K_i/k , причем это соответствие обладает всеми свойствами, перечисленными в формулировке теоремы 1.

С другой стороны, все нормальные делители S , фактор-группы по которым удовлетворяют условию: $G^{(i)} = (e)$, содержат $S^{(i)}$ и, наоборот, если нормальный делитель содержит $S^{(i)}$, то фактор-группа по нему удовлетворяет этому условию. Следовательно, нормальные делители, для фактор-групп по которым $G^{(i)} = (e)$, находятся во взаимно однозначном соответствии с нормальными делителями $\mathfrak{P}^{(i)}$. Так как для всякой p -группы $G^{(1)} \neq G[1]$, то $G^{(i)} = (e)$ при некотором i .

Следовательно, теорема будет доказана, если мы докажем, что группа Галуа K_i/k изоморфна $\mathfrak{P}^{(i)}$.

Определим сначала число образующих группы Галуа K_i/k . По теореме Burnside'a [1] число образующих p -группы G равно d , если

$$(G : G^{(1)}) = p^d.$$

Но если G – группа Галуа K_i/k , то к $G^{(1)}$ принадлежит K_1 . Следовательно, нам надо найти $[K_1 : k]$. Так как было предположено, что k не содержит корня степени p из единицы, то

$$[K_1 : k] = (k^* : (k^*)^p) = p^{n_0+1} \quad [2].$$

Следовательно, число образующих группы Галуа K_i/k равно n_0+1 . Значит, эта группа изоморфна фактор-группе S по нормальному делителю, который мы обозначим через N_i .

Наше утверждение будет доказано, если мы докажем, что

$$N_i = S^{(i)} .$$

Ясно, что $N_i \supseteq S^{(i)}$, так как для группы Галуа K_i/k имеет место соотношение $G^{(i)} = (e)$. Таким образом, достаточно доказать, что индексы N_i и $S^{(i)}$ равны или, иначе,

$$(S : S^{(i)}) = [K_i : k] . \quad (1)$$

Формула (1) доказывается индукцией по i . Для $i = 1$

$$(S : S^{(1)}) = [K_1 : k] = p^{n_0+1} .$$

Пусть мы уже доказали, что

$$(S : S^{(i)}) = [K_i : k] , \quad (2)$$

$$(S : S^{(i+1)}) = (S : S^{(i)})(S^{(i)} : S^{(i+1)}) . \quad (3)$$

Но так как $S^{(i+1)} = (S^{(i)})^{(1)}$, то

$$(S^{(i)} : S^{(i+1)}) = (S^{(i)} : (S^{(i)})^{(1)}) = p^{d_i} , \quad (4)$$

где d_i — число образующих $S^{(i)}$. По теореме Schreier'а [3]

$$d_i = (S : S^{(i)})(n_0 + 1 - 1) + 1 = (S : S^{(i)})n_0 + 1 . \quad (5)$$

С другой стороны,

$$[K_{i+1} : k] = [K_{i+1} : K_i][K_i : k] . \quad (6)$$

Но так как $K_{i+1} = (K_i)_1$, то

$$[K_{i+1} : K_i] = [(K_i)_1 : K_i] = p^{n_i+1} , \quad (7)$$

где n_i — степень K_i над полем рациональных p -адических чисел.

Так как

$$n_i = [K_i : k]n_0 , \quad (8)$$

то, с одной стороны, ввиду равенств (3), (4) и (5) имеем:

$$(S : S^{(i+1)}) = (S : S^{(i)})p^{(S : S^{(i)})n_0+1} ,$$

а, с другой стороны, ввиду (6), (7) и (8)

$$[K_{i+1} : k] = [K_i : k]p^{[K_i : k]n_0+1} .$$

В силу равенства (2) формула (1) тем самым установлена, а следовательно, доказана теорема 1.

§ 2

В этом параграфе будут выведены некоторые следствия из теоремы 1 предыдущего параграфа.

Следствие 1. p -группа G тогда и только тогда является группой Галуа некоторого расширения поля k , когда число ее образующих не больше, чем $n_0 + 1$,

Доказательство очевидно.

Следствие 2. Пусть $(G : e) = p^n$, d — число образующих G и α — число автоморфизмов G . Если $d \leq n_0 + 1$, то число расширений k , группы Галуа которых изоморфны G , равно

$$\frac{1}{\alpha} p^{(n_0+1)(n-d)} (p^{n_0+1} - 1)(p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1})^*.$$

Ввиду теоремы 1 число расширений, имеющих G своей группой Галуа, равно числу нормальных делителей S , фактор-группы по которым изоморфны G .

Каждому выбору системы $n_0 + 1$ образующих в G соответствует нормальный делитель в S , фактор-группа по которому изоморфна G , и наоборот. Но двум разным системам образующих $s_1, \dots, s_{n_0+1}$ и $t_1, \dots, t_{n_0+1}$ в G могут соответствовать совпадающие нормальные делители. Это имеет место тогда и только тогда, когда между $s_1, \dots, s_{n_0+1}$ и $t_1, \dots, t_{n_0+1}$ существуют одни и те же соотношения, т.е. из

$$f(s_1, \dots, s_{n_0+1}) = e$$

следует

$$f(t_1, \dots, t_{n_0+1}) = e,$$

и наоборот. Последнее же имеет место тогда и только тогда, когда соответствие

$$s_i \rightarrow t_i$$

определяет автоморфизм G .

Таким образом, надо разбить все системы образующих из $n_0 + 1$ элемента в G на системы интранзитивности группы автоморфизмов. Число систем интранзитивности и будет искомым числом. Но автоморфизм определяется своим действием на любую систему образующих, следовательно, число систем образующих во всех

* Аналогичная формула встречается у Witt'a, но совсем в другом случае [4].

системах интранзитивности – одно и то же и равно числу автоморфизмов G . Искомое число равно

$$\frac{1}{\alpha} \varphi_{n_0+1}(G) ,$$

где $\varphi_{n_0+1}(G)$ – число систем образующих из $n_0 + 1$ элемента в G .

По теореме о базисе [1] система элементов $s_1, \dots, s_{n_0+1}$ будет тогда и только тогда системой образующих G , когда совокупность элементов $s_1 G^{(1)}, \dots, s_{n_0+1} G^{(1)}$ будет системой образующих в $G/G^{(1)}$. Поэтому надо сначала определить число $\varphi_{n_0+1}(G/G^{(1)})$.

$G/G^{(1)}$ есть элементарно абелева группа порядка p^d . Нам известно число $\frac{1}{\alpha_1} \varphi_{n_0+1}(G/G^{(1)})$, где α_1 – число автоморфизмов $G/G^{(1)}$. По предыдущему это число равно числу подгрупп порядка p^{n_0+1-d} элементарно абелевой группы порядка p^{n_0+1} , т.е.

$$\frac{1}{\alpha_1} \varphi_{n_0+1}(G/G^{(1)}) = \frac{(p^{n_0+1} - 1)(p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1})}{(p^d - 1)(p^d - p) \dots (p^d - p^{d-1})} \quad [1] .$$

Но

$$\alpha_1 = (p^d - 1)(p^d - p) \dots (p^d - p^{d-1}) \quad [1] ,$$

следовательно

$$\varphi_{n_0+1}(G/G^{(1)}) = (p^{n_0+1} - 1)(p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1}) . \quad (10)$$

Любая система образующих G , состоящая из $n_0 + 1$ элемента, получается из такой же системы образующих $G/G^{(1)}$ рассмотрением любой системы представителей соответствующих классов смежности. Таким образом,

$$\varphi_{n_0+1}(G) = \varphi_{n_0+1}(G/G^{(1)})(G^{(1)} : e)^{n_0+1} . \quad (11)$$

Так как порядок $G^{(1)}$ есть p^{n-d} , то равенства (10) и (11) доказывают формулу (9).

Следствие 3. Пусть G и $\overline{G}$ – две p -группы, причем G гомоморфна $\overline{G}$ при некотором фиксированном гомоморфизме и число образующих G , а следовательно, и $\overline{G}$ не превосходит $n_0 + 1$.

Тогда для всякого расширения $\overline{K}/k$ с группой Галуа $\overline{G}$ существует такое расширение K/k с группой Галуа G , что $K \supset \overline{K}$ и

заданный гомоморфизм G и $\bar{G}$ реализуется, как естественный гомоморфизм группы Галуа поля на группу Галуа подполя.

Доказательство. Пусть G_0 — нормальный делитель G , являющийся ядром гомоморфизма G на $\bar{G}$.

Ввиду теоремы 1 нам надо доказать, что для любого нормального делителя $\bar{N}$ группы S , для которого $S/\bar{N} \simeq \bar{G}$, существует меньший нормальный делитель N , для которого $S/N \simeq G$, причем при этом изоморфизме $\bar{N}$ соответствует G_0 . Так как число образующих G не превосходит $n_0 + 1$, то в S существует такой нормальный делитель N_1 , что $S/N_1 \simeq G$, при этом G_0 соответствует некоторый нормальный делитель S/N_1 и $S/\bar{N}_1 \simeq \bar{G}$.

Выберем теперь столь большое i , чтобы все рассматриваемые подгруппы S содержали $S^{(i)}$. Тогда в $\mathfrak{P}^{(i)}$ всем подгруппам S , о которых шла речь, будут соответствовать подгруппы, которые мы будем отличать от прежних штрихом. Утверждение будет доказано, если мы установим, что в $\mathfrak{P}^{(i)}$ существует автоморфизм, переводящий $\bar{N}'_1$ в $\bar{N}'$. Действительно, этот автоморфизм будет переводить N'_1 в нормальный делитель N' , образ которого в S будет обладать всеми нужными нам свойствами.

Фактор-группы $\mathfrak{P}^{(i)}$ по $\bar{N}'_1$ и $\bar{N}'$ — изоморфны. Поэтому достаточно доказать следующее утверждение:

Два нормальных делителя $\mathfrak{P}^{(i)}$ переводятся друг в друга некоторым автоморфизмом тогда и только тогда, когда фактор-группы по ним изоморфны.

Число нормальных делителей $\mathfrak{P}^{(i)}$ с данной фактор-группой G известно из следствия 2. Подсчитаем теперь число нормальных делителей $\mathfrak{P}^{(i)}$, получающихся из одного с фактор-группой G применением автоморфизмов $\mathfrak{P}^{(i)}$. Эти два числа окажутся равными и, тем самым, наше утверждение будет доказано.

Предварительно исследуем соотношения в группе $\mathfrak{P}^{(i)}$ и ее автоморфизмы.

Пусть $s_1, s_2, \dots, s_{n_0+1}$ — образующие $\mathfrak{P}^{(i)}$, являющиеся образами свободных образующих S . Соотношения между образующими s_i легко описать следующим образом:

Рассмотрим функцию

$$[x, y] = xyx^{-1}y^{p-1} \text{ в } S.$$

Назовем *формой степени 1* любое выражение вида

$$[x_1, y_1]^{a_1} [x_2, y_2]^{a_2} \dots [x_t, y_t]^{a_t}.$$

Если формы степени $k - 1$ уже определены, то *формой степени k* назовем выражение вида:

$$[\xi_1, \eta_1]^{a_1} [\xi_2, \eta_2]^{a_2} \cdots [\xi_i, \eta_i]^{a_i},$$

где ξ_i и η_i — любые формы степени $k - 1$.

Легко видеть, что все соотношения между s_i в $\mathfrak{P}^{(i)}$ имеют вид:

$$f(s_1, \dots, s_{n_0+1}) = e, \quad (12)$$

где f — любая форма степени не меньше i .

Систему образующих $t_1, \dots, t_{n_0+1}$ в $\mathfrak{P}^{(i)}$ будем называть *свободной*, если между t_i существуют такие же соотношения, что и между s_i .

Нам понадобится следующая

Лемма. *Любая система из $n_0 + 1$ образующих в $\mathfrak{P}^{(i)}$ является свободной.*

Действительно, пусть $t_1, \dots, t_{n_0+1}$ — новая система образующих. Если выразить t_i через s_i , то мы увидим, что любая форма степени k относительно t_i является формой степени k относительно s_i . Следовательно, t_i удовлетворяет всем соотношениям вида (12). Это значит, что нормальный делитель S , состоящий из соотношений между t_i , содержит $S^{(i)}$, но он не может быть и больше $S^{(i)}$, так как оба они имеют один и тот же индекс. Значит, они совпадают, что и доказывает лемму.

Следствие леммы. *Переход от s_i к любой системе из $n_0 + 1$ образующих определяет автоморфизм $\mathfrak{P}^{(i)}$.*

Пусть $\mathfrak{N}$ — нормальный делитель $\mathfrak{P}^{(i)}$ с фактор-группой G . Обозначим через $\mathfrak{U}$ группу всех автоморфизмов $\mathfrak{P}^{(i)}$, а через $\mathfrak{P}$ — группу тех из них, которые оставляют $\mathfrak{N}$ на месте. Наконец, через $\mathfrak{C}$ нормальный делитель $\mathfrak{P}$, состоящий из автоморфизмов $\mathfrak{P}^{(i)}$, оставляющих все классы смежности по $\mathfrak{N}$ на месте.

Число нормальных делителей, в которые переходит $\mathfrak{N}$ при применении к нему автоморфизмов $\mathfrak{P}^{(i)}$, равно $(\mathfrak{U} : \mathfrak{P})$. Имеем:

$$(\mathfrak{U} : \mathfrak{P}) = \frac{(\mathfrak{U} : \mathfrak{C})}{(\mathfrak{P} : \mathfrak{C})} = \frac{(\mathfrak{U} : \mathfrak{C})}{\alpha'}, \quad (13)$$

где α' — число тех автоморфизмов G , которые индуцируются автоморфизмами $\mathfrak{P}^{(i)}$. Ясно, что

$$\alpha' \leq \alpha.$$

Найдем теперь $(\mathcal{U} : \mathcal{C})$. Условимся в дальнейшем группу $(\mathfrak{P}^{(i)})^{(1)}$ обозначать, для краткости, через $\overline{\mathfrak{P}}$. Рассмотрим группу $\mathfrak{P}'$ автоморфизмов $\mathfrak{P}^{(i)}$, оставляющих на месте классы смежности по $\mathfrak{N}\overline{\mathfrak{P}}$. Ясно, что

$$(\mathcal{U} : \mathcal{C}) = (\mathcal{U} : \mathfrak{P}')(\mathfrak{P}' : \mathcal{C}) . \quad (14)$$

Ввиду леммы и теоремы Bunside'a о базисе, $\mathfrak{N}\overline{\mathfrak{P}}$ может переходить при автоморфизмах $\mathfrak{P}^{(i)}$ в любую подгруппу того же порядка, лежащую между $\mathfrak{P}^{(i)}$ и $\overline{\mathfrak{P}}$. Число таких подгрупп равно

$$\frac{(p^{n_0+1} - 1)(p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1})}{(p^d - 1)(p^d - p) \dots (p^d - p^{d-1})} . \quad (15)$$

Кроме того, производя опять замену образующих, можно в факторгруппе по любой такой подгруппе вызвать ровно

$$(p^d - 1)(p^d - p) \dots (p^d - p^{d-1}) \quad (16)$$

автоморфизмов. Сравнение чисел (15) и (16) показывает, что

$$(\mathcal{U} : \mathfrak{P}') = (p^{n_0+1} - 1)(p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1}) . \quad (17)$$

Найдем теперь $(\mathfrak{P}' : \mathcal{C})$. Запишем каждый автоморфизм $\mathfrak{P}^{(i)}$ в виде:

$$s_k^\sigma = a_{k,\sigma} \cdot s_k .$$

Этот автоморфизм тогда и только тогда принадлежит $\mathfrak{P}'$, когда все $a_{k,\sigma} \in \mathfrak{N}\overline{\mathfrak{P}}$ тогда и только тогда он принадлежит $\mathcal{C}$, когда все $a_{k,\sigma} \in \mathfrak{N}$.

Рассмотрим группу $\mathfrak{P}$, являющуюся прямым произведением $n_0 + 1$ групп, изоморфных $\mathfrak{P}^{(i)}$. В $\mathfrak{P}$ каждому автоморфизму соответствует определенный элемент, но не всякий элемент $\mathfrak{P}$ соответствует автоморфизму, и те элементы, которые соответствуют автоморфизмам, не образуют подгруппы. Их совокупность обозначим через $\mathcal{L}$. Обозначим нормальный делитель, состоящий из тех элементов $\mathfrak{P}$, каждая компонента которых лежит в $\overline{\mathfrak{P}}$, через $\tilde{B}$. Аналогичный смысл будет иметь $\tilde{\mathfrak{N}}$. Через $(M : e)$ будем обозначать число элементов конечного множества M . Легко видеть, что

$$(\mathfrak{P}' : \mathcal{C}) = \frac{(\mathcal{L} \cap \tilde{\mathfrak{M}}\tilde{\mathfrak{N}} : e)}{(\mathcal{L} \cap \tilde{\mathfrak{M}} : e)} . \quad (18)$$

На основании леммы, система элементов $a_{k,\sigma}$ из $\mathfrak{P}^{(i)}$ тогда и только тогда определяет автоморфизм, когда $a_{k,\sigma}s_k$ являются системой образующих $\mathfrak{P}^{(i)}$. Но, ввиду теоремы о базисе, это будет иметь место тогда и только тогда, когда $a_{k,\sigma}s_k\overline{\mathfrak{P}}$ является системой образующих для $\mathfrak{P}^{(i)}/\overline{\mathfrak{P}}$.

Таким образом, свойство элемента λ из $\mathfrak{P}$ принадлежать $\mathcal{L}$ предопределяется соответствующим ему классом $\lambda\tilde{B}$. Если число классов $\lambda\tilde{B}$ ($\lambda \in \mathcal{L}$), в которых лежат элементы $\tilde{\mathfrak{N}}\tilde{B}$, обозначить через x , то будем иметь:

$$\left. \begin{aligned} (\mathcal{L} \cap \tilde{\mathfrak{N}}\tilde{B} : e) &= x(\tilde{B} : e), \\ (\mathcal{L} \cap \tilde{\mathfrak{N}} : e) &= x(\tilde{B} \cap \tilde{\mathfrak{N}} : e). \end{aligned} \right\} \quad (19)$$

Но

$$\left. \begin{aligned} (\tilde{B} : e) &= (\overline{\mathfrak{P}} : e)^{n_0+1}, \\ (\tilde{B} \cap \tilde{\mathfrak{N}} : e) &= (\overline{\mathfrak{P}} \cap \mathfrak{N} : e)^{n_0+1}. \end{aligned} \right\} \quad (20)$$

Из равенств (18), (19) и (20) получаем:

$$(\mathfrak{P}' : \mathfrak{C}) = (\overline{\mathfrak{P}} : \overline{\mathfrak{P}} \cap \mathfrak{N})^{n_0+1} = (\overline{\mathfrak{P}}\mathfrak{N} : \mathfrak{N})^{n_0+1} = p^{(n_0+1)(n-d)}. \quad (21)$$

Сравнивая равенства (13), (14), (17) и (21), получаем, что искомым нами число нормальных делителей равно

$$\frac{1}{\alpha'} p^{(n_0+1)(n-d)} (p^{n_0+1} - 1)(p^{n_0+1} - p) \dots (p^{n_0+1} - p^{d-1}).$$

Здесь $\alpha' \leq \alpha$. Но, с другой стороны, это число по своему смыслу не больше числа (9). Отсюда получаем, что оба этих числа равны между собой, что и доказывает следствие 3.

В качестве побочного результата получаем, что $\alpha = \alpha'$, т.е. любой автоморфизм любой фактор-группы $\mathfrak{P}^{(i)}$ индуцируется некоторым автоморфизмом $\mathfrak{P}^{(i)}$.

§ 3

В этом параграфе доказывается теорема, во многом аналогичная теореме 1.

В качестве основного поля здесь рассматривается поле k алгебраических функций с алгебраически замкнутым полем констант характеристики $p \neq 0$. В отличие от § 1 исследуются не все p -расширения k , а только неразветвленные. Через γ будем обозначать бирациональный инвариант, который обозначен той же буквой в работе Hasse и Witt'a [5], через S — свободную группу с γ образующими.

Теорема 2. *Неразветвленные p -расширения k находятся во взаимно однозначном соответствии с нормальными делителями группы S , индексы которых – степени p . Это соответствие имеет все те же свойства, которые перечислены в формулировке теоремы 1.*

В дальнейшем будут рассматриваться только неразветвленные p -расширения. Имея в виду эту оговорку, можно сохранить для нашего случая все обозначения § 1 (кроме числа n_0 , которое здесь не имеет смысла).

Почти все рассуждения § 1 проходят и в этом случае, поэтому отметим только несколько мест, в которых необходимы новые рассуждения.

Существование для поля k конечного расширения K_1 , являющегося композитом всех циклических расширений степени p , доказано в нашем случае в работе Hasse и Witt'a [5]. Степень K_1/k обозначается через p^γ .

Как и в § 1, доказательство приводится к доказательству равенства чисел $(S : S^{(i)})$ и $[K_i : k]$.

Рассуждая опять по индукции, мы видим, что утверждение теоремы эквивалентно доказательству формулы:

$$\gamma_i = [K_i : k](\gamma - 1) + 1, \quad (22)$$

где γ_i – число γ , определенное для пол K_i .

Доказательству формулы (22) и посвящен этот параграф.

Докажем более общую формулу:

$$\gamma' = [K : k](\gamma - 1) + 1 \quad (23)$$

для любого расширения K/k (может быть и не нормального), которое может быть получено цепочкой циклических расширений степени p , при этом под γ' подразумевается число γ для поля K .

Достаточно установить формулу (23) для расширений степени p , так как тогда она легко доказывается индукцией по степени K/k . Именно, если $K \supset \bar{K} \supseteq k$ и $K/\bar{K}$ – циклическое расширение степени p , а для K/k формула уже доказана, то

$$\gamma' = [K : \bar{K}](\bar{\gamma} - 1) + 1,$$

но

$$\bar{\gamma} = [\bar{K} : k](\gamma - 1) + 1,$$

следовательно,

$$\gamma' = [K : \bar{K}][\bar{K} : k](\gamma - 1) + 1 = [K : k](\gamma - 1) + 1.$$

Теперь будем доказывать формулу (23) для циклического расширения K/k степени p .

В этом случае $K = k(\theta)$, где

$$\mathcal{P}(\theta) = v, \quad \mathcal{P}(x) = x^p - x, \quad v \in k \quad [7].$$

Все элементы поля K имеют вид:

$$\alpha = a_0 + a_1\theta + \dots + a_{p-1}\theta^{p-1}, \quad a_i \in k.$$

Как известно [5],

$$p^\gamma = (b : \mathcal{P}(a)),$$

где b пробегает аддитивную группу всех элементов k , для которых уравнение $\mathcal{P}(x) = b$ разрешимо в любом p -адическом замыкании k_p поля k (такие элементы в дальнейшем будут называться *неразветвленными*), в то время как a пробегает аддитивную группу всех элементов k . Точно так же

$$p^{\gamma'} = (\beta : \mathcal{P}(\alpha)),$$

где β и α имеют аналогичный смысл для K .

Обозначим через Γ_i аддитивную группу всех неразветвленных элементов из K вида:

$$\beta = b_0 + b_1\theta + \dots + b_{i-1}\theta^{i-1}.$$

В частности, $\Gamma_0 = 0$.

Тогда

$$\begin{aligned} (\beta : \mathcal{P}(\alpha)) &= (\beta : \Gamma_{p-1} + \mathcal{P}(\alpha)) \\ &\times (\Gamma_{p-1} + \mathcal{P}(\alpha) : \Gamma_{p-2} + \mathcal{P}(\alpha)) \dots (\Gamma_1 + \mathcal{P}(\alpha) : \Gamma_0 + \mathcal{P}(\alpha)). \end{aligned}$$

Формула (23) будет доказана, если мы докажем, что

$$(\beta : \Gamma_{p-1} + \mathcal{P}(\alpha)) = p^\gamma, \quad (24)$$

$$(\Gamma_i + \mathcal{P}(\alpha) : \Gamma_{i-1} + \mathcal{P}(\alpha)) = p^{\gamma-1} \text{ при } i = p-1, \dots, 1, \quad (25)$$

так как тогда

$$p^{\gamma'} = (\beta : \mathcal{P}(\alpha)) = p^\gamma (p^{\gamma-1})^{p-1} = p^{p(\gamma-1)+1}.$$

Для доказательства формул (24) и (25) нам потребуется несколько предварительных выкладок.

Во-первых, выясним, каковы должны быть элементы $b_0, b_1, \dots, b_{p-1}$, чтобы элемент $b_0 + b_1\theta + \dots + b_{p-1}\theta^{p-1}$ имел вид $\mathcal{P}(\alpha)$.

Пусть $\alpha = a_0 + a_1\theta + \dots + a_{p-1}\theta^{p-1}$. Найдем $\mathcal{P}(\alpha)$:

$$\mathcal{P}(\alpha) = \mathcal{P}(a_0) + \mathcal{P}(a_1\theta) + \dots + \mathcal{P}(a_{p-1}\theta^{p-1}) .$$

Заменяя всюду θ^p через $\theta + v$ и вычисляя, получим:

$$\left. \begin{aligned} b_{p-1} &= \mathcal{P}(a_{p-1}), \\ b_{p-2} &= \mathcal{P}(a_{p-2}) + a_{p-1}^p c_{p-1}^1 v, \\ &\dots\dots\dots \\ b_{p-k} &= \mathcal{P}(a_{p-k}) + a_{p-k-1}^p c_{p-k-1}^1 v + \dots + a_{p-1}^p c_{p-1}^{k-1} v^{k-1}, \\ &\dots\dots\dots \end{aligned} \right\} \quad (26)$$

В дальнейшем нам понадобится следующая

Лемма. Если элемент $\alpha = a_0 + a_1\theta + \dots + a_i\theta^i$ не разветвлен, то и a_i не разветвлен. Наоборот, для всякого неразветвленного элемента a_i можно подобрать такие $a_0, a_1, \dots, a_{i-1}$, чтобы элемент $a_0 + a_1\theta + \dots + a_i\theta^i$ был не разветвлен.

Предположим, что α не разветвлен. Обозначим автоморфизм K/k , переводящий θ в $\theta + 1$, через σ . Очевидно тогда, что и $\sigma^k \alpha$ не разветвлен.

Докажем, что существуют такие элементы $r_0, \dots, r_i$ простого подполя R_p поля k , что $r_0\alpha + r_1\sigma\alpha + \dots + r_i\sigma^i\alpha = a_i$. Очевидно, что тогда a_i будет тоже неразветвленным элементом.

Подберем r_k так, чтобы удовлетворялись уравнения

$$\begin{aligned} r_0 + r_1 + \dots + r_i &= 0, \\ 0 \cdot r_0 + 1 \cdot r_1 + \dots + i \cdot r_i &= 0, \\ 0^2 \cdot r_0 + 1^2 \cdot r_1 + \dots + i^2 \cdot r_i &= 0, \\ &\dots\dots\dots \\ 0^{i-1} \cdot r_0 + 1^{i-1} \cdot r_1 + \dots + i^{i-1} \cdot r_i &= 0, \\ 0^i \cdot r_0 + 1^i \cdot r_1 + \dots + i^i \cdot r_i &= 0. \end{aligned}$$

Детерминант этой системы есть детерминант Вандермонда, отличный от нуля и, следовательно, она имеет единственное решение.

Докажем, что тогда

$$\theta^k(r_0 + r_1\sigma + \dots + r_i\sigma^i) = \delta_{ik} .$$

Действительно,

$$\begin{aligned}\theta^k(r_0 + r_1\sigma + \dots + r_i\sigma^i) &= r_0\theta^k + r_1(\theta + 1)^k + \dots + r_i(\theta + i)^k \\ &= \theta^k(r_1 + r_2 + \dots + r_i) + \theta^{k-1}c_k^1(0 \cdot r_0 + 1 \cdot r_1 + \dots + ir_i) + \dots \\ &\quad \dots + (0^k \cdot r_0 + 1^k \cdot r_1 + \dots + i^k r_i) = \delta_{ik} \ .\end{aligned}$$

Теперь наше утверждение доказано для любого α , так как

$$(r_0 + r_1\sigma + \dots + r_i\sigma^i)(a_0 + a_1\theta + \dots + a_i\theta^i) = a_i \ .$$

Предположим теперь, что a_i не разветвлен. Тогда для подбора нужных нам элементов $a_{i-1}, a_{i-2}, \dots, a_0$ будем последовательно решать, как показывают соотношения (26), уравнения вида:

$$a_k + \mathcal{P}(a_k^p) = c_k^p$$

для элементов $a_k \in k$ и $a_k^p \in k_p$ при заданных c_k^p . Разрешимость таких уравнений доказана в работе [6].

Теперь можно приступить к доказательству формул (24) и (25).

Введем гомоморфизмы χ_i , определенные в Γ_i :

$$\chi_i(b_0 + b_1\theta + \dots + b_{i-1}\theta^{i-1}) = b_{i-1} \ .$$

Заметим, что $\chi_i(\alpha) = 0$ тогда и только тогда, когда $\alpha \in \Gamma_{i-1}$. Из доказательства леммы следует, что

$$\chi(\alpha) = (r_0 + r_1\sigma + \dots + r_i\sigma^i)\alpha \ . \quad (27)$$

Докажем сначала формулу (24). Имеем:

$$(\beta : \Gamma_{p-2} + \mathcal{P}(\alpha)) = (\chi_p(\beta) : \chi_p(\mathcal{P}(\alpha))) \ .$$

Но ввиду равенства (27)

$$\chi_i(\alpha^p) = (r_0 + r_1\sigma + \dots + r_i\sigma^i)\alpha^p = \chi_i(\alpha)^p \ ,$$

так как r_i принадлежит простому полю R_p . Следовательно,

$$\chi_p(\mathcal{P}(\alpha)) = \mathcal{P}(\chi_p(\alpha)) = \mathcal{P}(\alpha_{p-1}) \ .$$

С другой стороны, из леммы следует, что значение $\chi_p(\beta)$ пробегает всю группу неразветвленных элементов из k . Следовательно,

$$(\beta : \Gamma_{p-1} + \mathcal{P}(\alpha)) = (\beta : \mathcal{P}(\alpha)) = p^\gamma \ .$$

Теперь докажем формулы (25).

Применим гомоморфизм χ_i к группам, стоящим в левой части формулы (25). Тогда, рассуждая, как и в первом случае, получим:

$$(\Gamma_i + \mathcal{P}(\alpha) : \Gamma_{i-1} + \mathcal{P}(\alpha)) = (b : \chi_i(\Gamma_i \cap \mathcal{P}(\alpha))) . \quad ()$$

Теперь надо выяснить, из каких элементов состоит группа $\chi_i(\Gamma_i \cap \mathcal{P}(\alpha))$. Для этого используем уравнения (26), положив в них

$$b_{p-1} = 0, \quad b_{p-2} = 0, \quad \dots, \quad b_{i+1} = 0 .$$

Тогда получим:

$$\mathcal{P}(a_{p-1}) = 0, \text{ т.е. } a_{p-1} = r_{p-1} \in R_p,$$

$$\mathcal{P}(a_{p-2}) + r_{p-1}c_{p-1}^1 v = 0,$$

т.е. если $r_{p-1} \neq 0$, то

$$v = \mathcal{P}\left(-\frac{1}{r_{p-1}c_{p-1}^1}a_{p-2}\right) ,$$

что невозможно, т.е.

$$a_{p-1} = 0, \quad \mathcal{P}(a_{p-2}) = 0 .$$

Продолжая таким образом дальше, получим:

$$a_{p-1} = 0, \quad a_{p-2} = 0, \quad \dots, \quad a_{i+1} = r \in R_p, \quad b_i = \mathcal{P}(a_i) + r(i-1)v .$$

Обратно, если $b_i = \mathcal{P}(a_i)$, то $\mathcal{P}(a_i\theta^i)$ будет элементом вида

$$b_0 + \dots + b_i\theta^i ,$$

и если $b_i = \mathcal{P}(a_i) + rv$, $r \neq 0$, то $\mathcal{P}(a_i\theta^i + \frac{1}{r(i-1)}\theta^{i+1})$ будет элементом такого же вида. Таким образом,

$$\chi_i(\Gamma_i \cap \mathcal{P}(\alpha)) = \mathcal{P}(a) + rv,$$

$$(\Gamma_i + \mathcal{P}(\alpha) : \Gamma_{i-1} + \mathcal{P}(\alpha)) = (b : \mathcal{P}(\alpha) + rv) = p^{\gamma-1}.$$

Доказательство теоремы закончено.

Совершенно очевидно, что все следствия, выведенные из теоремы 1 в § 2, имеют место и в рассматриваемом здесь случае.

(Поступило в редакцию 3 мая 1946 г.)

Литература

- [1] H. Zassenhaus, *Lehrbuch der Gruppentheorie*, Leipzig, 1937.
- [2] C. Chevalley, *La théorie du corp de classes*, Ann. of Math. **41** (1940), no. 2, 394–418.
- [3] O. Schreier, *Die Untergruppen der freien Gruppen*, Abh. Math. Sem. Hamburg **5** (1927), 161–183.
- [4] E. Witt, *Konstruktion von Galoischen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f* , J. für Math. **174** (1935), no. 4, 237–245.
- [5] H. Hasse und E. Witt, *Zyklische unverzweigte Erweiterungskörper vom Prynzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p* , Monatsh. für Math. und Ph. **43** (1936), 477–492.
- [6] E. Witt und L. Schmid, *Unverzweigte Abelsche Körper vom Exponenten p über einem algebraischen Funktionenkörper der Charakteristik p* , J. für Math. **176** (1937), no. 3, 168–173.
- [7] A. Albert, *Modern Higher Algebra*, Chicago, 1937.

ОБЩИЙ ЗАКОН ВЗАИМНОСТИ

ДОКЛ. АКАД. НАУК СССР Т. LXIV no. 1 (1949)

В 1796 году Гаусс доказал первый частный случай закона взаимности – квадратичный закон взаимности. В работах Гаусса, Якоби, Эйзенштейна, Куммера, Гильберта, Такаги, Артина, Хассе и других математиков закон взаимности был выведен в некоторых других частных случаях. Гильберт [2] поставил задачу о нахождении закона взаимности в наиболее общем случае. В настоящей заметке излагается решение этой задачи.

Относительно всех необходимых в дальнейшем определений и результатов читатель отсылается к обзору [1].

Задача заключается в нахождении явной формулы для выражения:

$$\left(\frac{\alpha}{\beta}\right) \left(\frac{\beta}{\alpha}\right)^{-1}, \quad (1)$$

где $\left(\frac{\alpha}{\beta}\right)$ – символ степенного вычета n -й степени, а α и β – два любых отличных от нуля числа произвольного поля алгебраических чисел k , содержащего корень степени n из единицы.

Как показано в работе [1], задача о нахождении в явном виде выражения (1) сводится к нахождению явной формы для символа норменного вычета $\left(\frac{\alpha\beta}{p}\right)$, а эта задача легко сводится к случаю, когда n есть степень простого числа $n = p^m$. В этой же работе показано, что задача решается тривиально, если $(p, p) = 1$. Достаточно, следовательно, вывести явную формулу для $\left(\frac{\alpha\beta}{p}\right)$ при $n = p^m$, $p \equiv 0 \pmod{p}$.

При этом выводе мы будем основываться на давно замеченной аналогии между символом $\left(\frac{\alpha\beta}{p}\right)$ в теории алгебраических чисел и вычетом в точке p , $\text{Res}_p \alpha d\beta$ абелева дифференциала $\alpha d\beta$ в теории алгебраических функций. Мы попытаемся вывести для символа

$\left(\frac{\alpha, \beta}{p}\right)$ формулу, аналогичную той, при помощи которой определяется вычет абелева дифференциала.

Для вычисления вычета дифференциала $\alpha d\beta$ в точке p функции α и β раскладываются в ряды Лорана по степеням локальной униформизирующей в этой точке. Но, как известно, в аналогии между алгебраическими функциями и алгебраическими числами аддитивным формулам в теории алгебраических функций соответствуют мультипликативные формулы в теории алгебраических чисел. Поэтому естественно для определения $\left(\frac{\alpha, \beta}{p}\right)$ представить α и β в виде некоторых произведений. Для этого мы используем функцию $E(\alpha, x)$, введенную в работе [3].

Пусть α — число из неразветвленного p -адического расширения и

$$\alpha = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots$$

его запись с коэффициентами α_i , принадлежащими мультипликативной системе представителей, т.е. системе представителей, состоящей из корней степени $p^f - 1$ из единицы, где f — порядок p в этом поле. Под $\alpha \rightarrow \alpha^P$ мы будем понимать автоморфизм неразветвленного поля, индуцирующий автоморфизм $\alpha \rightarrow \alpha^P$ в поле классов вычетов.

Рассмотрим формальный степенной ряд:

$$L(\alpha, x) = \sum_{n=0}^{\infty} p^{-n} \alpha^{P^n} x^{p^n}.$$

В работе [3] доказывается, что формально рассмотренный степенной ряд

$$E(\alpha, x) = e^{L(\alpha, x)}$$

будет иметь целые p -адические коэффициенты. Следовательно, он сходится для всех x , делящихся на простой делитель p .

Кроме того, функция $E(\alpha, x)$ удовлетворяет функциональному уравнению

$$E(\alpha + \beta, x) = E(\alpha, x)E(\beta, x).$$

Пусть $\bar{k}$ — p -адическое замыкание поля k . Так как $\bar{k}$ содержит корень степени n из единицы, то показатель ветвления e поля $\bar{k}$ делится на $p - 1$:

$$e = (p - 1)e_1.$$

Можно доказать, что если $\varepsilon \equiv 1 \pmod{p}$ в поле $\bar{k}$, то ε может быть представлено в виде

$$\varepsilon = \prod E(\alpha_i, \pi^i) \cdot \zeta^{p^m A}, \quad (2)$$

где π – любое простое число в $\bar{k}$, ζ – корень степени p^m из единицы, а $\zeta^{p^m A}$ – p^m -примарное число из $\bar{k}$, записанное в форме, выведенной в работе [4]. Значок i в произведении пробегает все целые значения $0 < i < e + e_1$, взаимно простые с p . В дальнейшем во всех произведениях будет предполагаться, что индексы i, j и k пробегают эту систему значений.

Не исследуя более подробно единственность записи (2), заметим только, что в ней α_i определены однозначно $(\bmod p^m)$, а $\zeta^{p^m A}$ – с точностью до множителя, равного p^m -й степени единицы поля $\bar{k}$.

Ясно, что любое число из $\bar{k}$ может быть представлено в виде

$$\alpha = \pi^a w \prod E(\alpha_i, \pi^i) \zeta^{p^m A}, \quad (3)$$

где a – целое число, w – корень степени $p^f - 1$ из единицы, а α_i и $\zeta^{p^m A}$ имеют объясненное выше значение.

Пользуясь представлением (3), мы введем символ (α, β) , определенный для всех не равных нулю α и β из $\bar{k}$, аналогичный вычету в теории алгебраических функций. Значением этого символа будет некоторое p^m -примарное число из $\bar{k}$, определенное с точностью до множителя, являющегося p^m -й степенью. В связи с этим все дальнейшие равенства надо понимать как равенства с точностью до множителя, являющегося p^m -й степенью.

Сначала при помощи формулы:

$$\begin{aligned} & \left(\pi^a w \prod E(\alpha_i, \pi^i) \zeta^{p^m A}, \pi^b w_1 \prod E(\beta_j, \pi^j) \zeta^{p^m B} \right) \\ &= (\pi, \pi)^{ab} \prod_{i,j} (E(\alpha_i, \pi^i), E(\beta_j, \pi^j)) \zeta^{p^m (aB - bA)} \end{aligned} \quad (4)$$

мы сведем определение символа (α, β) для произвольной пары чисел к определению символов

$$(\pi, \pi) \quad \text{и} \quad (E(\alpha_i, \pi^i), E(\beta_j, \pi^j)).$$

Дальнейшая конструкция зависит от того, с каким случаем мы имеем дело: $p \neq 2$ или $p = 2$.

Сначала разберем случай $p \neq 2$. Здесь

$$(\pi, \pi) = 1. \quad (5)$$

Для определения символа

$$(E(\alpha, \pi^i), E(\beta, \pi^j))$$

представим число $E(j\alpha\beta, \pi^{i+j})$ в виде (2):

$$E(j\alpha\beta, \pi^{i+j}) = \prod_k E(\gamma_k, \pi^k) \zeta^{p^m C}.$$

Тогда, по определению:

$$(E(\alpha, \pi^i), E(\beta, \pi^j)) = \zeta^{p^m C}. \quad (6)$$

В случае $p = 2$ нужно несколько модифицировать эти определения.

Для вычисления (π, π) представим число -1 в виде (2)

$$-1 = \prod E(\delta_i, \pi^i) \zeta^{2^m D}.$$

Тогда:

$$(\pi, \pi) = \zeta^{2^m D}. \quad (7)$$

Для вычисления $(E(\alpha, \pi^i), E(\beta, \pi^j))$ представим в виде (2) число:

$$\begin{aligned} E(j\alpha\beta, \pi^{i+j}) \prod_{a,b}^{\infty} E((2^{a-1}i + 2^{b-1}j)\alpha^{2^a}\beta^{2^b}, \pi^{2^a i + 2^b j}) \\ = \prod E(\gamma_k, \pi^k) \zeta^{2^m C}. \end{aligned}$$

Тогда, по определению:

$$(E(\alpha, \pi^i), E(\beta, \pi^j)) = \zeta^{2^m C}. \quad (8)$$

Формулы (4)–(8) определяют символ (α, β) для всех α и β из $\bar{k}$. Следующие свойства этого символа легко следуют из определения:

1) билинейность, т.е.

$$(\alpha_1 \alpha_2, \beta) = (\alpha_1, \beta)(\alpha_2, \beta)$$

и

$$(\alpha, \beta_1 \beta_2) = (\alpha, \beta_1)(\alpha, \beta_2) ;$$

2) кососимметричность, т.е.

$$(\beta, \alpha) = (\alpha, \beta)^{-1} .$$

Как это имеет место и для вычета абелева дифференциала, наиболее глубоким свойством символа (α, β) является его инвариантность. Она устанавливается следующей теоремой.

Теорема 1. Символ (α, β) зависит только от чисел α и β и не зависит от выбора простого числа π , которое фигурирует в разложении (2) и в формулах (4)–(8).

Символ норменного вычета связан очень просто с символом (α, β) . Как показано в работе [4], число A удовлетворяет уравнению

$$A^p - A = a ,$$

где a – целое число из поля инерции $\bar{k}$. Если под $S(a)$ подразумевать след в поле инерции $\bar{k}$ по отношению к полю рациональных p -адических чисел, то связь между символом норменного вычета и символом (α, β) может быть выражена следующим образом.

Теорема 2. Если $(\alpha, \beta) = \varepsilon^{p^m A}$, то $\left(\frac{\alpha, \beta}{p}\right) = \varepsilon^{S(a)}$.

Теорема 2 является простым следствием теоремы 1.

Все приведенные здесь результаты верны для чисел α и β из произвольного дискретно нормированного поля характеристики нуль с совершенным полем классов вычетов. Это дает ответ на вопрос, поставленный в работе [5]

(Поступило в редакцию 13 ноября 1948 г.)

Литература

- [1] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II*, Leipzig, 1930.
- [2] D. Hilbert, *Ges. Abh.* **3**, 310.
- [3] E. Artin und H. Hasse, *Abh. Math. Sem. Hamburg* **6** (1927).
- [4] H. Hasse, *J. reine und angew. Math.* **176** (1936), 174.
- [5] E. Witt, *J. reine und angew. Math.* **176** (1936), 153.

ОБЩИЙ ЗАКОН ВЗАИМНОСТИ

МАТ. СБОРН. Т.26 (68) no.1 (1950)

Введение

В настоящей статье решается задача, связанная с тремя вопросами теории алгебраических чисел: с аналогией между алгебраическими числами и функциями, общим законом взаимности и теорией полей классов.

1. Аналогия между алгебраическими числами и функциями. Идея о глубокой аналогии между полями алгебраических чисел и полями алгебраических функций была подготовлена работами Гаусса (C. Gauss) и Куммера (E. Kummer) и впервые высказана, видимо, Кронекером (L. Kronecker). Было замечено, что простые идеалы в теории алгебраических чисел играют такую же роль, как точки римановой поверхности в полях алгебраических функций, простым делителям дискриминанта соответствуют точки ветвления римановой поверхности и т.д. Возникла задача планомерного перенесения в теорию алгебраических чисел результатов из теории алгебраических функций, доказываемых там аналитическим путем.

Наиболее изученная часть теории алгебраических функций, это — теория абелевых интегралов. Д. Гильберт (D. Hilbert, [8], стр. 365, 483) начал исследовать аналог этой теории в полях алгебраических чисел. В каждом поле алгебраических чисел Ω , содержащем корень степени n из единицы, вводится символ $\left(\frac{\alpha, \beta}{\mathfrak{p}}\right)$, который любым двум числам α и β и простому идеалу $\mathfrak{p}$ поля Ω ставит в соответствие корень степени n из единицы ([3], стр. 53). Для этого символа, называемого *символом норменного вычета*, доказывается соотношение ([3], стр. 54).

$$\prod_{\mathfrak{p}} \left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = 1, \quad (\text{a})$$

в котором α и β — фиксированные числа поля Ω , а $\mathfrak{p}$ пробегает все простые идеалы Ω . Как заметил Гильберт, это соотношение играет

в теории алгебраических чисел ту же роль, какую интегральная теорема Коши играет в теории абелевых интегралов. Теория символа норменного вычета, развитая Гильбертом для случая $n = 2$, была обобщена на произвольное n , благодаря работам Н. Г. Чеботарева, Артина (E. Artin) и Хассе (H. Hasse).

Дальнейшее развитие как теории абелевых интегралов ([10] и [11]), так и теории алгебраических чисел показало, что соотношение (а), точнее говоря, является аналогом не интегральной теоремы Коши, а ее простого следствия — теоремы о том, что сумма вычетов абелева дифференциала $\alpha d\beta$ во всех точках римановой поверхности равна 0. С этой точки зрения символ норменного вычета $\left(\frac{\alpha, \beta}{p}\right)$ аналогичен вычету абелева дифференциала $\alpha d\beta$ в точке p .

Но хотя символ норменного вычета и играет роль вычета, определение его не имеет ничего общего с определением вычета абелевого дифференциала. Более того, хотя символ $\left(\frac{\alpha, \beta}{p}\right)$, как и вычет дифференциала $\alpha d\beta$, зависит только от поведения α и β в точке p , т.е. от разложений α и β в p -адические ряды, но определение символа $\left(\frac{\alpha, \beta}{p}\right)$ существенно зависит от свойств поля Ω в целом, т.е. от свойств всех его простых идеалов.

В этой статье дается конструкция символа $\left(\frac{\alpha, \beta}{p}\right)$, в точности аналогичная определению вычета абелева дифференциала.

При этом оказывается, что разложению алгебраической функции в ряд в окрестности точки римановой поверхности соответствует разложение алгебраического числа в некоторое произведение (§ 1, п. 3). Если над произведениями, в которые разлагаются числа α и β , производить в точности те же действия, какие производятся над разложениями функций в ряды при нахождении вычета, то получается значение символа (α, β) , равного $\left(\frac{\alpha, \beta}{p}\right)$. Все основные свойства вычета абелева дифференциала переносятся в поля алгебраических чисел. При этом, как и в теории алгебраических функций, самым трудным оказывается доказательство независимости символа (α, β) от выбора локальной униформизирующей.

2. Общий закон взаимности. Общий закон взаимности выражает в явной форме отношение символов степенных вычетов n -й степени $\left(\frac{\alpha}{\beta}\right) \left(\frac{\beta}{\alpha}\right)^{-1}$ через числа α и β . В случае, когда α и β рациональны и $n = 2$, закон взаимности был доказан Гауссом, применившим его к теории квадратичных форм. Для α и β , лежащих в поле деления круга на p частей, $n = p$, закон взаимности был доказан Куммером и применен к доказательству теоремы Ферма. Гильберт ([9], стр. 310) поставил задачу о нахождении общего закона взаим-

ности.

Из формулы (а) легко выводится формула ([3], стр. 58):

$$\left(\frac{\alpha}{\beta}\right) \left(\frac{\beta}{\alpha}\right)^{-1} = \prod_{p|n} \left(\frac{\alpha, \beta}{p}\right), \quad (b)$$

которая сводит задачу о нахождении общего закона взаимности к вопросу о нахождении явного выражения символа норменного вычета $\left(\frac{\alpha, \beta}{p}\right)$ через числа α и β .

Даваемая в настоящей статье конструкция символа норменного вычета как раз и дает такое выражение. Эта статья содержит, таким образом, формулировку и доказательство общего закона взаимности.

3. Теория полей классов. Теория полей классов изучает арифметические свойства абелевых расширений полей алгебраических чисел и полей p -адических чисел. Несмотря на очень большое значение основных теорем этой теории, доказательства этих теорем в высшей степени неестественны и мало понятны. Причина этого заключается, видимо, в следующем. Как заметил впервые Хассе ([4], стр. 150), естественным построением теории было бы такое, в котором сначала строилась бы p -адическая теория полей классов, а из нее выводилась бы теория полей классов для полей алгебраических чисел. Но символ норменного вычета $\left(\frac{\alpha, \beta}{p}\right)$, который играет основную роль в p -адической теории полей классов, определялся раньше только через поля алгебраических чисел (или при помощи теории алгебр, что требовало привлечения посторонних методов).

Предлагаемая в настоящей статье конструкция символа норменного вычета дает его чисто p -адическое определение. Она открывает, таким образом, возможность более естественного построения теории полей классов.

Как и в случае полей алгебраических функций, доказательство независимости символа (α, β) от выбора локальной унифицирующей оказывается очень громоздким. Чтобы длинные выкладки не заслонили совсем идею доказательства, в части I этой статьи изложены определения и основные свойства символа (α, β) для произвольного случая и доказана его инвариантность для случая простого нечетного показателя. Следующая часть будет содержать доказательство инвариантности для случая произвольного показателя.

4. Основные определения. Сейчас будут сформулированы основные определения и введены обозначения, которыми мы будем пользоваться на протяжении всей статьи.

Все наши рассуждения будут относиться к некоторому фиксированному полному дискретно нормированному ([2], стр. 304) полю k характеристики 0. Будет также всегда предполагаться, что поле классов вычетов поля k ([2], стр. 304) имеет характеристику $p \neq 0$ и совершенно.

Элементы поля k будут называться числами. Показатель ([2], стр. 304) числа α поля k будет обозначаться через $w(\alpha)$, и будет предполагаться, что он пробегает все целые значения, когда α пробегает все числа поля k . Простое число, т.е. такое число, для которого показатель равен 1, будет обозначаться через π . Всякое число α однозначно представимо в виде

$$\alpha = \xi \pi^a,$$

где a — целое число, а ξ — единица, т.е. $w(\xi) = 0$. При этом $w(\alpha) = a$. Если нам понадобится другое простое число в k , мы обозначим его через τ :

$$\tau = \xi \pi,$$

где ξ — единица.

Известно ([11], стр. 132), что в кольце целых элементов k можно выбрать единственную систему представителей классов по идеалу (π) , замкнутую относительно умножения. Эта система представителей будет называться *мультипликативной* и обозначаться через R .

Всякое число из k может быть однозначно представлено в виде:

$$\alpha = \sum_{i=n}^{\infty} \alpha_i \pi^i,$$

где n — целое число, а $\alpha_i \in R$.

Мы будем обозначать буквой ε и называть *главными единицами* единицы, удовлетворяющие сравнению:

$$\varepsilon \equiv 1 \pmod{(\pi)}.$$

Для характеристики p поля классов вычетов, $w(p) > 0$. Мы обозначим $w(p)$ через e и будем называть *показателем ветвления* поля k . В поле k

$$p = \xi \pi^e.$$

Если $e = 1$, то k называется *неразветвленным полем*. Среди всех подполей k , являющихся неразветвленными полями, существует максимальное. Оно называется *полем инерции* k и будет обозначаться через $\mathfrak{K}$. k имеет над $\mathfrak{K}$ степень e . $\mathfrak{K} \supset R$ и всякое число из

$\Re$ представимо в виде

$$\alpha = \sum_{i=n}^{\infty} \alpha_i p^i,$$

где $\alpha_i \in R$.

Ввиду совершенности поля классов вычетов, соответствие $\alpha \rightarrow \alpha^P$ в поле $\Re$, определенное формулой:

$$\left(\sum_{i=n}^{\infty} \alpha_i p^i \right)^P = \sum_{i=n}^{\infty} \alpha_i^P p^i,$$

где $\alpha_i \in R$, является автоморфизмом. При помощи него вводится функция $\wp(\alpha)$:

$$\wp(\alpha) = \alpha^P - \alpha.$$

Она обладает свойством:

$$\wp(\alpha + \beta) = \wp(\alpha) + \wp(\beta).$$

Всегда будет предполагаться, что поле k содержит первообразный корень степени p^n из единицы. Здесь n — фиксированное на продолжении всей статьи число.

Некоторый, раз навсегда выбранный, первообразный корень степени p^n из единицы будет обозначаться через ζ . Известно, что

$$(\Re(\zeta) : \Re) = p^{n-1}(p-1).$$

Ввиду этого

$$e \equiv 0 \pmod{p^{n-1}(p-1)}.$$

Вводятся обозначения:

$$\frac{e}{p-1} = e_1, \quad \frac{e}{p^{n-1}(p-1)} = \frac{e_1}{p^{n-1}} = e_0.$$

Ясно, что $e + e_1 = pe_1$.

Конечное расширение K/k называется *неразветвленным*, если π остается простым в K . Число из k называется *p^n -примарным* и будет обозначаться через ω , если $k(\sqrt[n]{\omega})/k$ не разветвлено.

В дальнейшем будет употребляться способ обозначений Хассе, согласно которому группа и ее элементы обозначаются одной и той же буквой. Так, например, группа главных единиц будет обозначаться через ε , группа p^n -примарных чисел — через ω и т.д.

Читатель, интересующийся только приложениями к теории алгебраических чисел, может считать, что поле k получается p -адическим замыканием поля алгебраических чисел по простому идеалу $\mathfrak{p}$. В этом случае мультипликативная система представителей R состоит из 0 и корней степени $N(\mathfrak{p}) - 1$ из единицы, где $N(\mathfrak{p})$ — абсолютная норма простого идеала $\mathfrak{p}$.

§ 1. Каноническое разложение

Целью этого параграфа является исследование фактор-группы всех главных единиц поля k по подгруппе p^n -х степеней. Для этого в группе главных единиц выбирается некоторая определенная система образующих и исследуется представление главных единиц через эти образующие.

1. Функция $E(\alpha, x)$. В дальнейшем существенную роль будут играть функции, введенные Артином и Хассе [1]. Сейчас будет дано их определение и указаны некоторые основные свойства. Доказательства можно найти в работе Хассе [5].

В кольце формальных степенных рядов от неизвестной x с коэффициентами из $\mathbb{R}$ рассмотрим ряд

$$L(\alpha, x) = \alpha x + p^{-1} \alpha^p x^p + p^{-2} \alpha^{p^2} x^{p^2} + \dots,$$

где α — целое число из $\mathbb{R}$.

Очевидно, что ряд $L(\alpha, x)$ обладает следующими свойствами:

$$L(\alpha_1 + \alpha_2, x) = L(\alpha_1, x) + L(\alpha_2, x),$$

$$L(a\alpha, x) = aL(\alpha, x),$$

где a — целое рациональное p -адическое число. Отсюда следует, что ряд

$$E(\alpha, x) = e^{L(\alpha, x)}$$

обладает свойствами:

$$E(\alpha_1 + \alpha_2, x) = E(\alpha_1, x)E(\alpha_2, x), \quad (1)$$

$$E(a\alpha, x) = E(\alpha, x)^a. \quad (2)$$

В случае, если $\alpha \in R$, имеет место следующее тождество:

$$E(\alpha, x) = \prod (1 - \alpha^m x^m)^{-\frac{\mu(m)}{m}}, \quad (3)$$

где $\mu(m)$ — функция Мебиуса, а m пробегает все натуральные значения, взаимно простые с p . Это тождество показывает, что при $\alpha \in R$ $E(\alpha, x)$ имеет целые p -адические коэффициенты. Ввиду соотношений (1) и (2) это верно для любого $\alpha \in \mathbb{R}$. Отсюда следует, что $E(\alpha, x)$ сходится, если вместо x подставить любое число из k ,

делящееся на π . Кроме того, равенство (3) показывает, что при $\alpha \in R$

$$E(\alpha, x) \equiv 1 + \alpha x \ (x^2) . \quad (4)$$

Функция $E(1, \xi)$ имеет целые p -адические коэффициенты и ввиду (4) уравнение

$$1 + \eta = E(1, \xi)$$

разрешимо в виде степенного ряда $\xi = Q(\eta)$ по степеням η с целыми p -адическими коэффициентами. При этом

$$\xi \equiv \eta \ (\eta^2) .$$

Применяя это к случаю $1 + \eta = \zeta$, $\eta = \zeta - 1$, увидим, что для $\xi = Q(\zeta - 1)$ будет

$$E(1, \xi) = \zeta, \quad (5)$$

$$\xi \equiv \zeta - 1 \ ((\zeta - 1)^2) . \quad (6)$$

Пусть $\overline{\mathfrak{K}}$ — то дискретно нормированное неразветвленное поле, которое получается из $\mathfrak{K}$ алгебраическим замыканием поля классов вычетов. Для всякого целого α из $\mathfrak{K}$ в $\overline{\mathfrak{K}}$ существует такое целое A , что

$$\wp(A) = \alpha . \quad (7)$$

Введем обозначение

$$E(p^n A, \xi) = E(\alpha) . \quad (8)$$

Это обозначение имеет смысл, так как легко видеть, что различные целые A , удовлетворяющие соотношению (7), дают одно $E(p^n A, \xi)$.

Доказывается, что $E(\alpha)$ принадлежит к полю k и даже $\mathfrak{K}(\zeta)$. Из этого следует, что оно является p^n -примарным, так как $E(\alpha)$ есть p^n -я степень числа $E(A, \xi)$, лежащего в неразветвленном расширении $\overline{\mathfrak{K}}k$ поля k .

Ясно, что $E(\alpha)$ удовлетворяет соотношениям:

$$\begin{aligned} E(\alpha + \beta) &= E(\alpha)E(\beta) , \\ E(a\alpha) &= E(\alpha)^a , \end{aligned}$$

где a — всякое рациональное p -адическое число.

Доказывается, что всякое p^n -примарное число ω из k представимо в виде:

$$\omega = E(\alpha)\lambda^{p^n} ,$$

где α — некоторое целое число из $\mathfrak{R}$, а λ — какое-то число из k .

2. Теорема Гензеля. Гензель (K. Hensel) нашел очень широкое условие, при котором система главных единиц является системой образующих для группы главных единиц. Так как в дальнейшем нам будет нужна не только формулировка теоремы Гензеля, но и некоторые формулы, встречающиеся в ее доказательстве, то здесь будет приведено краткое доказательство. Подробное доказательство содержится в работе Гензеля [7].

Теорема Гензеля. Пусть для каждого i , удовлетворяющего условиям $i \not\equiv 0 \pmod{p}$, $1 \leq i < pe_1$, а также для $i = pe_1$ и для каждого $\alpha \in R$ выбрана главная единица $\varepsilon_i(\alpha)$, удовлетворяющая условию: $\varepsilon_i(\alpha) \equiv 1 + \alpha \pi^i \pmod{\pi^{i+1}}$. Тогда всякая главная единица ε может быть представлена в виде $\varepsilon = \prod_{i,r} \varepsilon_i(\alpha_{i,r})^{p^r}$, где произведение распространено на указанные выше значения i и на все целые неотрицательные r .

Доказательство состоит из трех частей.

А. Пусть дана система главных единиц $\varepsilon_i(\alpha)$, зависящая от натурального индекса i и числа $\alpha \in R$ и удовлетворяющая сравнениям:

$$\varepsilon_i(\alpha) \equiv 1 + \alpha \pi^i \pmod{\pi^{i+1}}. \quad (9)$$

Тогда всякую главную единицу ε можно представить в виде

$$\varepsilon = \prod_{i=1}^{\infty} \varepsilon_i(\alpha_i). \quad (10)$$

Действительно, равенство (10) эквивалентно выполнению сравнений

$$\varepsilon \equiv \prod_{i=1}^n \varepsilon_i(\alpha_i) \pmod{\pi^{n+1}} \quad (11)$$

для любого n . Пусть для $n = r$ сравнение (11) уже доказано. Пусть

$$\varepsilon \left(\prod_{i=1}^r \varepsilon_i(\alpha_i) \right)^{-1} \equiv 1 + \alpha_{r+1} \pi^{r+1} \pmod{\pi^{r+2}}.$$

Тогда

$$\varepsilon \left(\prod_{i=1}^r \varepsilon_i(\alpha_i) \right)^{-1} \equiv \varepsilon_{r+1}(\alpha_{r+1}) \pmod{\pi^{r+2}}$$

или

$$\varepsilon \equiv \prod_{i=1}^{r+1} \varepsilon_i(\alpha_i) (\pi^{r+2}),$$

т.е. сравнение (11) доказано для $n = r + 1$.

В. Пусть $\eta \in R$. Исследуем формулу возведения в p -ю степень единицы $1 + \eta\pi^i + \dots$:

$$(1 + \eta\pi^i + \dots)^p = 1 + p\eta\pi^i + \dots + \eta^p\pi^{pi} + \dots,$$

где точками обозначены члены, делящиеся на большую степень π , чем один из выписанных. Член $p\eta\pi^i$ делится на $e + i$ -ю, а $\eta^p\pi^{pi}$ — на pi -ю степень π . Следовательно, мы имеем три формулы:

$$(1 + \eta\pi^i + \dots)^p \equiv 1 + \eta^p\pi^{pi} (\pi^{pi+1}), \text{ если } i < e_1, \quad (12_1)$$

$$(1 + \eta\pi^i + \dots)^p \equiv 1 + \gamma_e\eta\pi^{e+i} (\pi^{e+i+1}), \text{ если } i > e_1, \quad (12_2)$$

$$(1 + \eta\pi^{e_1} + \dots)^p \equiv 1 + (\eta^p + \gamma_e\eta)\pi^{pe_1} (\pi^{pe_1+1}). \quad (12_3)$$

Здесь $\gamma_e \in R$ и означает коэффициент в формуле

$$p = \gamma_e\pi^e + \gamma_{e+1}\pi^{e+1} + \dots$$

Из формулы (12₂) следует важное для дальнейшего замечание: если $\varepsilon \equiv 1 (\pi^{pe_1+1})$, то ε является p -й степенью некоторой главной единицы.

С. Из (12₂) следует, что если для некоторого $i > pe_1$ заменить в системе $\varepsilon_i(\alpha)$ из A все $\varepsilon_i(\alpha)$ на $\varepsilon_{i-e}(\gamma_e^{-1}\alpha)^p$, то получится система, опять удовлетворяющая условию (9). Аналогично, из (12₁) следует, что если для $i = ph < pe_1$ заменить $\varepsilon_i(\alpha)$ на $\varepsilon_h(\alpha^{p^{-1}})^p$, то получится система, удовлетворяющая условию (9). Возможность извлечения корня p -й степени из $\alpha \in R$ следует из совершенности поля классов вычетов k .

Если произвести все указанные замены, то мы получим, что система $\varepsilon_i(\alpha)^{p^r}$, где i пробегает все значения, меньше pe_1 и не делящиеся на p , а также значение pe_1 , r — все целые неотрицательные числа, а α — все элементы R , будет удовлетворять условию (9). Следовательно, ввиду A всякая главная единица ε может быть представлена в виде

$$\varepsilon = \prod \varepsilon_i(\alpha_{i,r})^{p^r}.$$

Теорема Гензеля доказана.

3. Каноническое разложение. Мы применим теорему Гензеля к доказательству следующей теоремы:

Теорема о каноническом разложении. Всякая главная единица ε может быть представлена в виде $\varepsilon = E(\alpha) \prod E(\alpha_i, \pi^i)$, где α и α_i — целые числа из $\mathfrak{R}$, а i пробегает все значения между 1 и pe_1 , не делящиеся на p .

Доказательство. Покажем, что $E(\alpha_i, \pi^i)$ и $E(\alpha)$ при α_i и $\alpha \in R$ удовлетворяют условиям теоремы Гензеля. Для $E(\alpha_i, \pi^i)$ это очевидно ввиду сравнения (4). Надо доказать, что

$$E(\alpha) \equiv 1 + \beta \pi^{pe_1} (\pi^{pe_1+1}),$$

где $\beta \in R$ и пробегает все R , когда α пробегает все R .

По своему построению $E(\alpha)$ лежит в $\mathfrak{R}(\zeta)$. По формуле (8) $E(\alpha)$ есть p^n -я степень числа $E(A, \xi)$, лежащего в $\mathfrak{R}(\zeta)$. На основании сравнений (4) и (6)

$$E(A, \xi) \equiv 1 + A(\zeta - 1)((\zeta - 1)^2).$$

Будем возводить $E(A, \xi)$ в степень p, p^2, p^3 и т.д. При возведении в степень до p^{n-1} включительно мы можем пользоваться формулой (12₁), так как для поля $\mathfrak{R}(\zeta)$ $e = p^{n-1}(p-1)$, $pe_1 = p^n$. Следовательно,

$$E(A, \xi)^{p^{n-1}} \equiv 1 + A^{p^{n-1}}(\zeta - 1)^{p^{n-1}} ((\zeta - 1)^{p^{n-1}+1}).$$

При возведении этого сравнения в p -ю степень мы обязаны пользоваться уже формулой (12₃):

$$E(A, \xi)^{p^n} \equiv 1 + (A^{p^n} + \gamma_e A^{p^{n-1}})(\zeta - 1)^{p^n} ((\zeta - 1)^{p^n+1}). \quad (13)$$

Теперь вычислим γ_e . Обозначим $\zeta - 1$ через λ . λ удовлетворяет уравнению:

$$(\lambda + 1)^{p^{n-1}(p-1)} + (\lambda + 1)^{p^{n-1}(p-2)} + \dots + (\lambda + 1)^{p^{n-1}} + 1 = 0.$$

Все коэффициенты этого уравнения, кроме первого, делятся на p .

$$\begin{aligned} \lambda^{p^{n-1}(p-1)} + p(1 + a_1 \lambda + \dots) &= 0, \\ p &= -\frac{\lambda^{p^{n-1}(p-1)}}{1 + a_1 \lambda + \dots} = -\lambda^{p^{n-1}(p-1)} + \dots \end{aligned}$$

Следовательно, $\gamma_e = -1$, и равенство (13) принимает вид:

$$E(p^n A, \xi) \equiv 1 + \wp(A)^{p^{n-1}} (\zeta - 1)^{p^n} ((\zeta - 1)^{p^n} + 1) .$$

Пусть в k

$$\zeta - 1 = \gamma_{e_0} \pi^{e_0} + \gamma_{e_0+1} \pi^{e_0+1} + \dots ;$$

когда, ввиду того что $\alpha = \wp(A)$, а $p^n e_0 = p e_1$,

$$E(\alpha) \equiv 1 + \alpha^{p^{n-1}} \gamma_{e_0}^{p^n} \pi^{p e_1} (\pi^{p e_1} + 1) . \quad (14)$$

Так как, когда α пробегает все R , $\alpha^{p^{n-1}} \gamma_{e_0}^{p^n}$ пробегает тоже все R , то применимость теоремы Гензеля доказана. На основании этой теоремы всякая главная единица ε представима в виде

$$\varepsilon = \prod_r E(\alpha_r)^{p^r} \prod_{i,r} E(\alpha_{i,r}, \pi^i)^{p^r} .$$

Но ввиду свойств (1) и (2) функций $E(\alpha, x)$ и аналогичных свойств функции $E(\alpha)$

$$\begin{aligned} \prod_r E(\alpha_{i,r}, \pi^i)^{p^r} &= E\left(\sum_r \alpha_{i,r} p^r, \pi^i\right) , \\ \prod_r E(\alpha_r)^{p^r} &= E\left(\sum_r \alpha_r p^r\right) , \\ \varepsilon &= E\left(\sum_r \alpha_r p^r\right) \prod_i E\left(\sum_r \alpha_{i,r} p^r, \pi^i\right) . \end{aligned}$$

Теорема доказана. В дальнейшем разложение главной единицы на множители $E(\alpha)$ и $E(\alpha_i, \pi^i)$, возможность которого только что доказана, мы будем называть *каноническим разложением*. Если в каком-нибудь произведении будут встречаться индексы i, j или h , мы будем предполагать, что они пробегают систему чисел от 1 до $p e_1$, не делящихся на p .

Заметим, что из приведенных рассуждений следует важный для дальнейшего факт: если $E(\alpha)$ является p -й степенью, то $\alpha \equiv \wp(\beta)(p)$. Действительно, если $E(\alpha) = \varepsilon^p$, то сравнения (14) и (12) показывают, что

$$\begin{aligned} \varepsilon &\equiv 1 + \eta \pi^{e_1} (\pi^{e_1} + 1), \\ \alpha^{p^{n-1}} \gamma_{e_0}^{p^n} &\equiv \eta^p + \gamma_e \eta (p) . \end{aligned}$$

Но, если

$$\begin{aligned}\zeta - 1 &= \gamma_{e_0} \pi^{e_0} + \gamma_{e_0+1} \pi^{e_0+1} + \dots, \\ p &= -(\zeta - 1)^{p^{n-1}(p-1)} + \dots,\end{aligned}$$

то

$$p = -\gamma_{e_0}^{p^{n-1}(p-1)} \pi^{p^{n-1}(p-1)e_0} + \dots,$$

т.е. $\gamma_e \equiv -\gamma_{e_0}^{p^{n-1}(p-1)}(p)$, $\eta^p + \gamma_e \eta \equiv \gamma_{e_0}^p ((\eta \gamma_{e_0}^{-p^{n-1}})^p - (\eta \gamma_{e_0}^{-p^{n-1}}))(p)$.
Следовательно,

$$\alpha^{p^{n-1}} \equiv \wp(\eta \gamma_{e_0}^{-p^{n-1}})(p), \quad \alpha \equiv \wp(\eta^{p^{-(n-1)}} \gamma_{e_0}^{-1})(p).$$

4. Единственность канонического разложения. Исследуем единственность канонического разложения главных единиц.

Лемма 1. Если $E(\alpha) \prod E(\alpha_i, \pi^i) = E(\beta) \prod E(\beta_i, \pi^i)$, то

$$\alpha \equiv \beta + \wp(\eta)(p), \quad \alpha_i \equiv \beta_i(p).$$

Доказательство. Обозначим $\alpha_i - \beta_i$ через γ_i , а $\alpha - \beta$ через γ . Ввиду свойства (1) и аналогичного свойства $E(\alpha)$ имеем:

$$E(\gamma) \prod E(\gamma_i, \pi^i) = 1.$$

Докажем сначала, что все $\gamma_i \equiv 0(p)$. Пусть это не так и γ_j — первое из γ_i , не делящееся на p ,

$$\prod_{i \geq j} E(\gamma_i, \pi^i) = E(\gamma)^{-1} \varepsilon^p.$$

Но это невозможно ввиду сравнений (12₁), (12₂) и (12₃), так как

$$\prod_{i \geq j} E(\gamma_i, \pi^i) = 1 + \gamma_j \pi^j (\pi^{j+1}).$$

Следовательно, все $\gamma_i \equiv 0(p)$. Докажем, что $\gamma \equiv \wp(\eta)(p)$. Ввиду того, что все $\gamma_i \equiv 0(p)$,

$$E(\gamma) = \varepsilon^p,$$

из чего, согласно замечанию, сделанному в п. 3, следует, что $\gamma \equiv \wp(\eta)(p)$. Лемма доказана.

Лемма 2. В любом каноническом разложении

$$\zeta_1 = E(\theta) \prod E(\theta_i, \pi^i) \quad (15)$$

корня степени p из единицы ζ_1 выполняются сравнения:

$$\begin{aligned} \theta &\equiv \wp(\eta) \ (p^{n-1}), \\ \theta_i &\equiv 0 \ (p^{n-1}). \end{aligned}$$

Доказательство. Пусть доказано, что для любого канонического разложения ζ_1 выполняются сравнения:

$$\begin{aligned} \theta &\equiv \wp(\eta) \ (p^r), \\ \theta_i &\equiv 0 \ (p^r) \end{aligned} \quad (16)$$

для некоторого $r \leq n-2$. Докажем, что аналогичные сравнения справедливы и для $r+1$. По определению функции $E(\alpha)$

$$E(\wp(\eta)) = E(p^n \eta, \xi) = E(p^n \sigma) \prod E(p^n \sigma_i, \pi^i), \quad (17)$$

где положено

$$E(\eta, \xi) = E(\sigma) \prod E(\sigma_i, \pi^i).$$

Из соотношений (15) и (17) следует, что ζ_1 имеет следующее каноническое разложение:

$$\zeta_1 = E(\bar{\theta}) \prod E(\bar{\theta}_i, \pi^i),$$

где

$$\begin{aligned} \bar{\theta} &= \theta - \wp(\eta) + p^n \sigma \equiv \theta - \wp(\eta) \ (p^n), \\ \bar{\theta}_i &= \theta_i + p^n \sigma_i \equiv \theta_i \ (p^n), \end{aligned} \quad (18)$$

причем, ввиду (16), имеют место сравнения:

$$\begin{aligned} \bar{\theta} &\equiv 0 \ (p^r) \\ \bar{\theta}_i &\equiv 0 \ (p^r). \end{aligned}$$

Положим

$$\bar{\theta} p^{-r} = \lambda, \quad \bar{\theta}_i p^{-r} = \lambda_i,$$

и пусть

$$\zeta = E(\mu) \prod E(\mu_i, \pi^i)$$

— некоторое каноническое разложение корня степени p^n из единицы ζ . Ввиду (15)

$$\left(E(\lambda) \prod E(\lambda_i, \pi^i) \right)^{p^{r+1}} = 1,$$

следовательно, при некотором целом a

$$E(\lambda) \prod E(\lambda_i, \pi^i) = \zeta^{ap^{n-r-1}} = E(ap^{n-r-1}\mu) \prod E(ap^{n-r-1}\mu_i, \pi^i).$$

Ввиду леммы 1, имеем:

$$\lambda \equiv \wp(\eta_1) + ap^{n-r-1}\mu(p),$$

$$\lambda_i \equiv ap^{n-r-1}\mu_i(p),$$

а так как $n \geq r+2$, то

$$\lambda \equiv \wp(\eta_1)(p),$$

$$\lambda_i \equiv 0(p),$$

т.е.

$$\bar{\theta} - \wp(p^r \eta_1) \equiv 0(p^{r+1}),$$

$$\bar{\theta}_i \equiv 0(p^{r+1}).$$

На основании сравнений (18) отсюда получается, что

$$\theta \equiv \wp(\eta + p^r \eta_1)(p^{r+1}),$$

$$\theta_i \equiv 0(p^{r+1}).$$

Лемма доказана.

Теорема единственности. Если $E(\alpha) \prod E(\alpha_i, \pi^i) = E(\beta) \prod E(\beta_i, \pi^i)$, то $\alpha \equiv \beta + \wp(\eta)(p^n)$, $\alpha_i \equiv \beta_i(p^n)$.

Доказательство. Согласно лемме 1, $\alpha \equiv \beta + \wp(\eta)(p)$, $\alpha_i \equiv \beta_i(p)$. Ввиду соотношения (17)

$$E(\alpha) \prod E(\alpha_i, \pi^i) = E(\bar{\alpha}) \prod E(\bar{\alpha}_i, \pi^i),$$

$$\bar{\alpha} \equiv \alpha - \wp(\eta)(p^n),$$

$$\bar{\alpha}_i \equiv \alpha_i(p^n),$$

$$\bar{\alpha} \equiv \beta(p).$$

(19)

Обозначим $\frac{\bar{\alpha}-\beta}{p}$ через γ , а $\frac{\bar{\alpha}_i-\beta_i}{p}$ — через γ_i .

$$E(p\gamma) \prod E(p\gamma_i, \pi^i) = 1 ,$$

следовательно,

$$\zeta_1 = E(\gamma) \prod E(\gamma_i, \pi^i)$$

есть некоторое каноническое разложение корня степени p из единицы ζ_1 . Согласно лемме 2,

$$\begin{aligned} \gamma &\equiv \wp(\eta_1) (p^{n-1}), \\ \gamma_i &\equiv 0 (p^{n-1}), \end{aligned}$$

т.е.

$$\begin{aligned} \bar{\alpha} &\equiv \beta + \wp(\eta_1 p) (p^n), \\ \bar{\alpha}_i &\equiv \beta_i (p^n). \end{aligned}$$

Ввиду сравнений (19)

$$\begin{aligned} \alpha &\equiv \beta + \wp(\eta + p\eta_1) (p^n), \\ \alpha_i &\equiv \beta_i (p^n). \end{aligned}$$

Теорема доказана.

Заметим, что ввиду соотношения (17) и формулы

$$\left(E(\lambda) \prod E(\lambda_i, \pi^i) \right)^{p^n} = E(p^n \lambda) \prod E(p^n \lambda_i, \pi^i),$$

мы можем в каноническом разложении

$$\varepsilon = E(\alpha) \prod E(\alpha_i, \pi^i)$$

изменить любым образом α_i на слагаемое вида $p^n \beta_i$, а α — на слагаемое вида $\wp(\eta) + p^n \beta$, умножая ε на p^n -ю степень некоторой главной единицы.

§ 2. Символ (λ, μ)

1. Функция $\delta\varepsilon$. В § 1 нами было доказано, что всякая главная единица может быть представлена в виде

$$\varepsilon = E(\alpha) \prod E(\alpha_i, \pi^i),$$

причем, если ε рассматривать с точностью до множителя, являющегося p^n -й степенью, а $\alpha_i \pmod{p^n}$ и α с точностью до слагаемого вида $\wp(\beta) \pmod{p^n}$, то соответствие будет взаимно однозначным.

В дальнейшем нас будут интересовать только равенства с точностью до множителя, являющегося p^n -й степенью. Тот факт, что λ отличается от μ множителем, являющимся p^n -й степенью, мы будем записывать так: $\lambda \approx \mu$.

Каждому ε в его каноническом разложении соответствует первый член $E(\alpha)$, определенный с точностью до p^n -й степени.

Введем функцию, определенную на группе главных единиц:

$$\delta\varepsilon \approx E(\alpha).$$

Ясно, что

$$\delta\varepsilon_1 \varepsilon_2 \approx \delta\varepsilon_1 \delta\varepsilon_2,$$

$$\delta\varepsilon^{p^n} \approx 1.$$

Следовательно, отображение $\varepsilon \rightarrow \delta\varepsilon$ является гомоморфизмом группы $\varepsilon/\varepsilon^{p^n}$ на группу $\omega/(\omega \cap \varepsilon^{p^n})$.

Следует отметить, что член $E(\alpha)$ в каноническом разложении ε зависит не только от ε , но и от выбора простого числа π , при помощи которого мы производим каноническое разложение. Если это надо будет подчеркнуть, мы будем писать $\delta_\pi \varepsilon$ вместо $\delta\varepsilon$.

В случае, если поле классов вычетов поля k конечно, группа $\omega/(\omega \cap \varepsilon^{p^n})$ — циклическая порядка p^n . В самом деле, в этом случае $\mathfrak{K}$ является конечным расширением поля $\mathfrak{K}_0$ рациональных p -адических чисел. Под $S(\alpha)$ будем подразумевать след в $\mathfrak{K}/\mathfrak{K}_0$. Тогда отображение

$$\chi E(\alpha) = \zeta^{S(\alpha)}$$

является изоморфизмом группы $\omega/(\omega \cap \varepsilon^{p^n})$ и циклической группы, порожденной ζ .

Мультипликативность этого отображения следует из свойств следа и функции $E(\alpha)$. То, что на группе $(\omega \cap \varepsilon^{p^n})$ χ обращается в единицу, следует из того, что

$$S(\alpha^P - \alpha) = S(\alpha^P) - S(\alpha) = 0.$$

То, что группа $\omega \cap \varepsilon^{p^n}$ действительно является ядром гомоморфизма, следует из того, что при $S(\alpha) \equiv 0 \pmod{p^n}$; $\alpha \equiv \varphi(\beta) \pmod{p^n}$ ([11], стр. 134). Наконец, то, что χ дает отображение на всю группу, следует из невырожденности конечных полей.

Запись p^n -примарного числа ω в виде $E(\alpha)$ зависит от выбора ζ так же, как и функция χ . Но, как показал Хассе ([5], стр. 182), результирующее отображение

$$\chi\omega = \zeta^{S(\alpha)}$$

от выбора ζ не зависит.

Применив отображение χ , мы можем в случае конечного поля классов вычетов перейти от функции $\delta\varepsilon$ к функции $\chi\delta\varepsilon$, значениями которой являются корни степени p^n из единицы. Однако, большей частью мы будем рассматривать случай произвольного поля классов вычетов и не будем применять отображение χ .

2. Символ (λ, μ) . Всякое число λ поля k может быть записано в виде

$$\lambda = \pi^a w\varepsilon$$

([6], стр. 189), где a — целое число, w — элемент из R , а ε — главная единица. Нас интересует равенство с точностью до p^n -х степеней, и поэтому мы будем отбрасывать множитель w , так как он является p^n -й степенью, и показатель a рассматривать $(\bmod p^n)$.

Все числа мы сможем тогда представить так:

$$\lambda \approx \pi^a E(\alpha) \prod E(\alpha_i, \pi^i). \quad (20)$$

Пусть другое число μ представлено в таком же виде:

$$\mu \approx \pi^b E(\beta) \prod E(\beta_j, \pi^j).$$

Введем в рассмотрение функцию

$$(\lambda, \mu) \approx E(a\beta - b\alpha + \gamma), \quad (21)$$

где

$$E(\gamma) \approx \delta \prod_{i,j} E(i\alpha_i \beta_j, \pi^{i+j}). \quad (22)$$

Функция (λ, μ) есть функция двух переменных на группе λ/λ^{p^n} , значения которой принадлежат группе $\omega/\omega \cap \varepsilon^{p^n}$. Действительно, изменение a , b , α_i или β_j на слагаемые, кратные p^n , не изменит

$a\beta - b\alpha + \gamma \pmod{p^n}$ и, следовательно, не изменит $E(a\beta - b\alpha + \gamma)$ с точностью до p^n -х степеней. Аналогично обстоит дело с изменением α и β на слагаемое вида $\wp(\eta) \pmod{p^n}$.

Символ (λ, μ) обладает следующими четырьмя свойствами, доказательство которых является основной целью настоящей статьи:

I. Билинейность:

$$\begin{aligned}(\lambda_1 \lambda_2, \mu) &\approx (\lambda_1, \mu)(\lambda_2, \mu), \\ (\lambda, \mu_1 \mu_2) &\approx (\lambda, \mu_1)(\lambda, \mu_2).\end{aligned}$$

II. Кососимметричность:

$$(\mu, \lambda) \approx (\lambda, \mu)^{-1}.$$

III. Невырожденность: если в поле классов вычетов не всякий элемент представим в виде $x^p - x$, то

$$\begin{aligned}\text{из } (\lambda, \mu) &\approx 1 \text{ для всех } \mu \text{ следует } \lambda \approx 1, \\ \text{из } (\lambda, \mu) &\approx 1 \text{ для всех } \lambda \text{ следует } \mu \approx 1.\end{aligned}$$

IV. Инвариантность, т.е. независимость значения (λ, μ) от выбора простого числа π , при помощи которого (λ, μ) определяется.

Теорема 1 (билинейность).

$$(\lambda_1 \lambda_2, \mu) \approx (\lambda_1, \mu)(\lambda_2, \mu) \text{ и } (\lambda, \mu_1 \mu_2) \approx (\lambda, \mu_1)(\lambda, \mu_2).$$

Доказательство. Пусть

$$\begin{aligned}\lambda_1 &\approx \pi^{a_1} E(\alpha^{(1)}) \prod E(\alpha^{(1)}_i, \pi^i), \\ \lambda_2 &\approx \pi^{a_2} E(\alpha^{(2)}) \prod E(\alpha^{(2)}_i, \pi^i), \\ \mu &\approx \pi^b E(\beta) \prod E(\beta_j, \pi^j).\end{aligned}$$

Тогда

$$(\lambda_1, \mu) \approx E(a_1 \beta - b \alpha^{(1)} + \gamma^{(1)}),$$

где

$$E(\gamma^{(1)}) \approx \delta \prod_{i,j} E(i \alpha_i^{(1)} \beta_j, \pi^{i+j}),$$

и

$$(\lambda_2, \mu) \approx E(a_2\beta - b\alpha^{(2)} + \gamma^{(2)}) ,$$

где

$$E(\gamma^{(2)}) \approx \delta \prod_{i,j} E(i\alpha_i^{(2)}\beta_j, \pi^{i+j}) ,$$

$$\lambda_1\lambda_2 \approx \pi^{a_1+a_2} E(\alpha^{(1)} + \alpha^{(2)}) \prod E(\alpha_i^{(1)} + \alpha_i^{(2)}, \pi^i),$$

$$(\lambda_1\lambda_2, \mu) \approx E((a_1 + a_2)\beta - b(\alpha^{(1)} + \alpha^{(2)}) + \gamma) ,$$

где

$$E(\gamma) \approx \delta \prod_{i,j} E(i(\alpha_i^{(1)} + \alpha_i^{(2)})\beta_j, \pi^{i+j})$$

$$\approx \delta \prod_{i,j} E(i\alpha_i^{(1)}\beta_j, \pi^{i+j}) \delta \prod_{i,j} E(i\alpha_i^{(2)}\beta_j, \pi^{i+j}) \approx E(\gamma^{(1)})E(\gamma^{(2)}) ;$$

$$(\lambda_1\lambda_2, \mu) \approx E((a_1 + a_2)\beta - b(\alpha^{(1)} + \alpha^{(2)})) E(\gamma)$$

$$\approx E(a_1\beta - b\alpha^{(1)})E(\gamma^{(1)})E(a_2\beta - b\alpha^{(2)})E(\gamma^{(2)})$$

$$\approx E(a_1\beta - b\alpha^{(1)} + \gamma^{(1)})E(a_2\beta - b\alpha^{(2)} + \gamma^{(2)}) \approx (\lambda_1, \mu)(\lambda_2, \mu) .$$

Точно так же доказывается вторая формула.

3. Кососимметричность.

Лемма. Пусть M — некоторая главная единица из поля $k(\sqrt[n]{\pi})$. Тогда $\delta N(M) \approx 1$, где норма берется в поле $k(\sqrt[n]{\pi})/k$.

Доказательство. В поле $k(\sqrt[n]{\pi})$ $\sqrt[n]{\pi}$ является простым числом. Обозначим его через π_n . В этом поле числа e , e_1 и e_0 обозначим через $e^{(n)}$, $e_1^{(n)}$ и $e_0^{(n)}$. Ясно, что $e^{(n)} = p^n e$, $e_1^{(n)} = p^n e_1$, $e_0^{(n)} = p^n e_0 = p e_1$. В частности,

$$\zeta - 1 = \gamma_{e_0} \pi_n^{p e_1} + \gamma_{e_0+1} \pi_n^{p e_1+1} + \dots .$$

Ввиду этого, при $i \not\equiv 0 (p)$

$$\begin{aligned} (1 - \alpha \pi_n^i)^{\sigma-1} &= \frac{1 - \zeta^i \alpha \pi_n^i}{1 - \alpha \pi_n^i} \\ &= 1 - \alpha(\zeta^i - 1) \pi_n^i + \dots \equiv 1 - \alpha \gamma_{e_0} \pi_n^{p e_1+i} (\pi^{p e_1+i+1}) , \end{aligned}$$

где через σ обозначен автоморфизм поля $k(\sqrt[n]{\pi})/k$, переводящий π_n в $\zeta\pi_n$.

Из этого следует, что числа $E(\alpha, \pi_n^i)$ при $i < pe_1$ и $i \not\equiv 0 (p)$ вместе с числами $(1 - \alpha\pi_n^{i-pe_1})^{\sigma-1}$ при $i \not\equiv 0 (p)$ и $pe_1 < i < pe_1^{(n)}$ и с числами $E(\alpha)$ образуют в поле $k(\sqrt[n]{\pi})$ систему, удовлетворяющую условиям теоремы Гензеля.

Из теоремы Гензеля следует, что M может быть представлено в виде

$$M \approx E(\alpha) \prod_{i < pe_1} E(\alpha_i, \pi_n^i) A^{\sigma-1},$$

где A — некоторая главная единица поля $k(\sqrt[n]{\pi})$.

Ввиду очевидного равенства:

$$N(1 - \alpha\pi_n^m) = 1 - \alpha^{p^n} \pi^m$$

при $m \neq 0 (p)$, $\alpha \in R$, и формулы (3) мы получим:

$$N(E(\alpha, \pi_n^i)) = E(\alpha^{p^n}, \pi^i)$$

при $i \not\equiv 0 (p)$. Учитывая, что $E(\alpha)$ лежит не только в $k(\sqrt[n]{\pi})$, но и в k , получим:

$$N(M) = E(p^n \alpha) \prod E(\alpha_i^{p^n}, \pi^i), \\ \delta N(M) \approx 1.$$

Теорема 2 (кососимметричность).

$$(\mu, \lambda) \approx (\lambda, \mu)^{-1}.$$

Доказательство. Согласно соотношениям (21) и (22)

$$(\lambda, \mu)(\mu, \lambda) \approx \delta \prod_{i,j} E((i+j)\alpha_i\beta_j, \pi^{i+j}).$$

Теорема будет доказана, если для любого l мы установим, что

$$\delta E(l \cdot \alpha, \pi^l) \approx 1. \quad (23)$$

Ясно также, что формулу (23) достаточно доказать для $\alpha \in R$. Пусть $l = p^r h$, $h \not\equiv 0 \pmod{p}$. Ввиду (3) достаточно доказать, что

$$\delta(1 - \alpha \pi^{p^r h})^{p^r} \approx 1.$$

На основании леммы это будет доказано, если мы установим, что

$$(1 - \alpha \pi^{p^r h})^{p^r} = N(M)$$

для некоторого $M \in k(\sqrt[p^n]{\pi})$. Что это действительно так, показывает формула:

$$\begin{aligned} (1 - \alpha \pi^{p^r h})^{p^r} &= \prod_{a=1}^{p^r} (1 - \zeta^{ap^{n-r}} \alpha^{p^{-r}} \pi^h)^{p^r} = \prod_{a=1}^{p^r} N(1 - \zeta^a \alpha^{p^{-n}} \pi_n^{p^r h}) \\ &= N\left(\prod_{a=1}^{p^r} N(1 - \zeta^a \alpha^{p^{-n}} \pi_n^{p^r h})\right). \end{aligned}$$

Теорема доказана.

4. Невырожденность.

Теорема 3 (невырожденность). Если в поле классов вычетов поля k не всякий элемент представим в виде $x^p - x$, то из $(\lambda, \mu) \approx 1$ для всех μ следует, что $\lambda \approx 1$, и из $(\lambda, \mu) \approx 1$ для всех λ следует, что $\mu \approx 1$.

Доказательство. Ясно, что второе утверждение теоремы следует из первого ввиду кососимметричности. Пусть

$$\lambda \approx \pi^a E(\alpha) \prod E(\alpha_i, \pi^i).$$

Нам надо доказать, что из $(\lambda, \mu) \approx 1$ для всех μ следует, что А) $a \equiv 0 \pmod{p^n}$, В) $\alpha \equiv \wp(\beta) \pmod{p^n}$, С) $\alpha_i \equiv 0 \pmod{p^n}$.

А) Выберем такое $\beta \in R$, чтобы $\beta \not\equiv \wp(\eta) \pmod{p}$, что возможно ввиду условия, наложенного на поле классов вычетов. $(\lambda, E(\beta)) \approx 1$ дает:

$$E(a\beta) \approx 1, \quad a\beta \equiv \wp(\eta) \pmod{p^n},$$

следовательно, ввиду выбора β , $a \equiv 0 \pmod{p^n}$.

В) Из соотношения $(\lambda, \pi) \approx 1$ получаем:

$$E(-\alpha) \approx 1, \quad E(\alpha) \approx 1,$$

следовательно, $\alpha \equiv \wp(\beta) (p^n)$.

С) Пусть максимальная степень p , на которую делятся все α_i , есть p^r . Мы покажем, что предположение $r < n$ приводит к противоречию.

Пусть j — первый индекс, для которого α_j не делится на p^{r+1} . Введем обозначения:

$$\alpha_i = p^r \bar{\alpha}_i.$$

По предположению $\bar{\alpha}_i \equiv 0 (p)$ при $i < j$, $\bar{\alpha}_j \not\equiv 0 (p)$.

Используем соотношение $(\lambda, \mu) \approx 1$ для $\mu = E(\beta p^{n-r-1}, \pi^{pe_1-j})$. Ясно, что $0 < pe_1 - j < pe_1$ и $pe_1 - j \not\equiv 0 (p)$, следовательно, μ уже представлено в канонической форме,

$$\begin{aligned} (\lambda, \mu) &\approx \delta \prod_i E(p^{n-1} \bar{\alpha}_i \beta, \pi^{pe_1+i-j}) \\ &\approx \delta \prod_{i < j} E(p^{n-1} \bar{\alpha}_i \beta, \pi^{pe_1+i-j}) \delta E(p^{n-1} \bar{\alpha}_j \beta, \pi^{pe_1}) \\ &\quad \times \delta \prod_{i > j} E(p^{n-1} \bar{\alpha}_i \beta, \pi^{pe_1+i-j}) \approx 1. \end{aligned}$$

Мы покажем, что первый и последний множитель этого произведения ≈ 1 , и, следовательно, средний множитель тоже ≈ 1 . Для первого множителя это следует из того, что при $i < j$ $\bar{\alpha}_i \equiv 0 (p)$, и, следовательно, этот множитель — p^n -я степень. Для последнего множителя это следует из того, что при $i > j$

$$E(\bar{\alpha}_i \beta, \pi^{pe_1+i-j}) \equiv 1 (\pi^{pe_1+1}),$$

и, следовательно, согласно сделанному в § 1, п.2 В замечанию, $E(\bar{\alpha}_i \beta \pi^{pe_1+i-j})$ — p -я степень. Таким образом, мы получим, что

$$\delta E(p^{n-1} \bar{\alpha}_j \beta, \pi^{pe_1}) \approx 1. \quad (24)$$

Ввиду только что использованного замечания из § 1 п.2 В и формулы (14)

$$E(\alpha, \pi^{pe_1}) = E(\gamma_{e_0}^{-p} \alpha^{p^{-n+1}}) \varepsilon^p. \quad (25)$$

Следовательно, формула (24) показывает, что

$$E(p^{n-1} \gamma_{e_0}^{-p} (\bar{\alpha}_j \beta)^{p^{-n+1}}) \approx 1,$$

т.е.

$$\gamma_{e_0}^{-p} (\bar{\alpha}_j \beta)^{p^{-n+1}} \equiv \wp(\eta) (p).$$

Ввиду условия, наложенного на поле классов вычетов, и в силу того, что $\bar{\alpha}_j \not\equiv 0 (p)$, можно так подобрать β , чтобы такое соотношение не имело места ни при каком η . Это противоречие доказывает теорему.

§ 3. Инвариантность

При определении символа (λ, μ) мы использовали канонические разложения чисел λ и μ . Но каноническое разложение существенно зависит от того, при помощи какого простого числа π оно строится. Вообще говоря, ниоткуда не следует, что мы получим прежнее значение символа (λ, μ) , если будем вычислять его, пользуясь другим простым числом τ . Инвариантность символа (λ, μ) при переходе к другому простому числу является наиболее глубоким его свойством. В настоящем параграфе инвариантность будет доказана для случая, когда $n = 1$, $p \neq 2$. Ввиду сделанного предположения $n = 1$ значок $\approx$ будет применяться в этом параграфе для равенства с точностью до p -х степеней.

Теорема 4 (инвариантность). В случае $n = 1$, $p \neq 2$ символ (λ, μ) зависит только от чисел λ и μ и не зависит от простого числа π , фигурирующего в его определении.

Для доказательства теоремы достаточно, ввиду билинейности символа (λ, μ) , доказать, что следующие пять формул, верных, если входящий в них символ (λ, μ) вычислять, пользуясь простым числом π , останутся верными, если мы будем пользоваться другим простым числом τ .

$$(E(\alpha), \varepsilon) \approx (\varepsilon, E(\alpha)) \approx 1. \quad (26)$$

$$(\pi, E(\alpha)) \approx (E(\alpha), \pi)^{-1} \approx E(\alpha), \quad (27)$$

$$(\pi, \pi) \approx 1, \quad (28)$$

$$(\pi, E(\alpha, \pi^i)) \approx 1, \quad (I)$$

$$(E(\alpha, \pi^i), E(\beta, \pi^j)) \approx \delta_{\pi} E(i\alpha\beta, \pi^{i+j}). \quad (II)$$

Формула (26) вообще не зависит от выбора π . Докажем инвариантность формулы (27). Пусть τ — другое простое число и $\pi = \tau\varepsilon$. Если вычислять $(\pi, E(\alpha))$, пользуясь простым числом τ , то получится:

$$(\pi, E(\alpha)) = (\tau\varepsilon, E(\alpha)) \approx (\tau, E(\alpha))(\varepsilon, E(\alpha)) \approx \delta_{\tau} E(\alpha) \approx E(\alpha).$$

Наконец, формула (28) является частным случаем формулы:

$$(\lambda, \lambda) \approx 1,$$

верной при любом выборе простого числа и при любом λ ввиду кососимметричности (λ, μ) и нечетности p .

Трудность представляет доказательство инвариантности формул (I) и (II), чему и будет посвящен весь этот параграф.

1. Вспомогательная формула.

Лемма. Имеют место формулы

$$E(\alpha, \pi^{pu}) = E(p\alpha^{P^{-1}}, \pi^u) e^{-p\alpha^{P^{-1}}\pi^u} \approx e^{-p\alpha^{P^{-1}}\pi^u} \quad (29)$$

и

$$e^{\alpha\pi^a} \approx E(\alpha, \pi^a) \text{ при } a > e. \quad (30)$$

Доказательство формулы (29).

$$\begin{aligned} L(\alpha, \pi^{pu}) &= \alpha\pi^{pu} + p^{-1}\alpha^P\pi^{p^2u} + p^{-2}\alpha^{P^2}\pi^{p^3u} + \dots \\ &= pL(\alpha^{P^{-1}}, \pi^u) - p\alpha^{P^{-1}}\pi^u, \end{aligned}$$

соотношение (29) следует из того, что $E(\alpha, x) = e^{L(\alpha, x)}$.

Доказательство формулы (30).

$$E(\alpha, \pi^a) = e^{\alpha\pi^a} \cdot e^{p^{-1}\alpha^P\pi^{pa}} \cdot e^{p^{-2}\alpha^{P^2}\pi^{p^2a}} \cdot \dots$$

Докажем, что при $a > e$, $m \geq 1$ и $p \neq 2$

$$e^{p^{-m}\alpha^{P^m}\pi^{p^ma}} \equiv 1 \pmod{\pi^{pe_1+1}}. \quad (31)$$

Отсюда будет следовать, что все $e^{p^{-m}\alpha^{P^m}\pi^{p^ma}}$ являются p -ми степенями, а следовательно, формула (30) верна.

$$w(p^{-m}\alpha^{P^m}\pi^{p^ma}) = p^ma - me > (p^m - m)e > pe_1 \text{ при } p \neq 2.$$

Но при $w(x) > e_1$ $w(e^x - 1) = w(x)$, что и доказывает формулу (31).

Опираясь на доказанную лемму, мы выведем формулу, обобщающую соотношение

$$(E(\alpha, \pi^i), E(\beta, \pi^j)) \approx \delta E(i\alpha\beta, \pi^{i+j})$$

на случай, когда $E(\alpha, \pi^i)$ или $E(\beta, \pi^j)$ не являются каноническими множителями, т.е. когда i или $j > pe_1$, или $\equiv 0 \pmod{p}$.

Мы докажем, что при любых r и s имеет место формула:

$$\begin{aligned} (E(\alpha, \pi^r), E(\beta, \pi^s)) &\approx \delta E(r\alpha\beta, \pi^{r+s}) \\ &\times \prod_{m=1}^{\infty} E(r\alpha^{P^m}\beta, \pi^{p^mr+s}) E(-s\alpha\beta^{P^m}, \pi^{r+p^ms}). \end{aligned} \quad (32)$$

Здесь, как и всюду в дальнейшем, предполагается, что δ относится ко всей части формулы, стоящей после него.

Доказательство формулы (32). Если r или $s \geq pe_1$, то формула (32) очевидна, так как при этом или $E(\alpha, \pi^r)$ или $E(\beta, \pi^s)$ является p -примарным числом, и, следовательно, левая часть формулы (32) ≈ 1 ввиду соотношения (27), а все члены правой части являются p -ми степенями. Будем теперь предполагать, что r и $s < pe_1$. Если $r \not\equiv 0 (p)$, $s \not\equiv 0 (p)$, то $p^m r + s \not\equiv 0 (p)$ и $r + p^m s \not\equiv 0 (p)$, и формула (32) верна согласно определению символа (λ, μ) .

Нам остается разобрать два случая:

А. Одно из чисел r и s делится на p , а другое нет.

В. r и s оба делятся на p .

Случай А. Ясно, что ввиду кососимметричности достаточно рассмотреть случай $r \not\equiv 0 (p)$, $s = pu$. В этом случае $r + s \not\equiv 0 (p)$ и $r + p^m s \not\equiv 0 (p)$, поэтому формула (32) эквивалентна такой:

$$(E(\alpha, \pi^r), E(\beta, \pi^s)) \approx \delta \prod_{m=1}^{\infty} E(r\alpha^{p^m} \beta, \pi^{p^m r + s}). \quad (33)$$

Ввиду того, что для $s \geq pe_1$ формула (32) верна, мы можем предполагать ее справедливой для $s > pu$ (в том числе и для $s \not\equiv 0 (p)$) и доказывать для $s = pu$. Согласно соотношению (29)

$$\begin{aligned} E(\beta, \pi^{pu}) &\approx e^{-p\beta^{p^{-1}} \pi^u}, \\ (E(\alpha, \pi^r), E(\beta, \pi^{pu})) &\approx \left(E(\alpha, \pi^r), e^{-p\beta^{p^{-1}} \pi^u} \right). \end{aligned} \quad (34)$$

Пусть

$$-p\beta^{p^{-1}} \pi^u = \sum_a \lambda_a \pi^a. \quad (35)$$

При этом все $a \geq e + u > e$, а $\lambda_a \in R$. На основании соотношений (35) и (30)

$$\begin{aligned} e^{-p\beta^{p^{-1}} \pi^u} &\approx \prod_a E(\lambda_a, \pi^a), \\ (E(\alpha, \pi^r), E(\beta, \pi^{pu})) &\approx \prod_a (E(\alpha, \pi^r), E(\lambda_a, \pi^a)). \end{aligned}$$

Так как $pu < pe_1$, то все $a \geq e + u > pu$, и, следовательно, для $s = a$ формула (32) доказана:

$$(E(\alpha, \pi^r), E(\lambda_a, \pi^a)) \approx \delta E(r\alpha\lambda_a, \pi^{r+a}) \\ \times \prod_{m=1}^{\infty} E(r\alpha^{P^m}\lambda_a, \pi^{p^m r+a}) E(-a\alpha\lambda_a^{P^m}, \pi^{r+p^m a}).$$

Но ввиду того, что $r \not\equiv 0 (p)$, $p^m a + r \not\equiv 0 (p)$ при $m \geq 1$ и, следовательно,

$$\delta E(-a\alpha\lambda_a^{P^m}, \pi^{r+p^m a}) \approx 1, \\ (E(\alpha, \pi^r), E(\lambda_a, \pi^a)) \approx \delta \prod_{m=0}^{\infty} E(r\alpha^{P^m}\lambda_a, \pi^{p^m r+a}).$$

Ввиду соотношения (30)

$$E(r\alpha^{P^m}\lambda_a, \pi^{p^m r+a}) \approx e^{r\alpha^{P^m}\lambda_a \pi^{p^m r+a}}$$

и ввиду равенства (35)

$$\sum_a r\alpha^{P^m}\lambda_a \pi^{p^m r+a} = -pr\alpha^{P^m}\beta^{P^{-1}}\pi^{p^m r+u}.$$

Следовательно

$$\prod_{a,m} E(r\alpha^{P^m}\lambda_a, \pi^{p^m r+a}) = \prod_{m=0}^{\infty} e^{-pr\alpha^{P^m}\beta^{P^{-1}}\pi^{p^m r+u}}$$

и ввиду (29)

$$\prod_{a,m} E(r\alpha^{P^m}\lambda_a, \pi^{p^m r+a}) \approx \prod_{m=0}^{\infty} E(r\alpha^{P^{m+1}}\beta, \pi^{p^{m+1}r+pu}) \\ = \prod_{m=1}^{\infty} E(r\alpha^{P^m}\beta, \pi^{p^m r+pu}).$$

Сравнивая с предыдущим, получаем:

$$(E(\alpha, \pi^r), E(\beta, \pi^{pu})) \approx \delta \prod_{m=1}^{\infty} E(r\alpha^{P^m}\beta, \pi^{p^m r+pu}),$$

т.е. формулу (33) для $s = pu$.

Случай В. В этом случае все множители в правой части формулы (32) являются p -ми степенями. Нам надо, следовательно, доказать, что при любых u и v

$$(E(\alpha, \pi^{pu}), E(\beta, \pi^{pv})) \approx 1.$$

Применим соотношение (29)

$$\begin{aligned} E(\alpha, \pi^{pu}) &\approx e^{-p\alpha^{p^{-1}}\pi^u}, \\ E(\beta, \pi^{pv}) &\approx e^{-p\beta^{p^{-1}}\pi^v}, \\ (E(\alpha, \pi^{pu}), E(\beta, \pi^{pv})) &\approx \left(e^{-p\alpha^{p^{-1}}\pi^u}, e^{-p\beta^{p^{-1}}\pi^v} \right). \end{aligned}$$

Ясно, что

$$e^{-p\alpha^{p^{-1}}\pi^u} \equiv e^{-p\beta^{p^{-1}}\pi^v} \equiv 1 \pmod{\pi^{e+1}}.$$

Наша формула будет доказана, если мы докажем, что для любых ε_1 и ε_2 , для которых

$$\begin{aligned} \varepsilon_1 &\equiv \varepsilon_2 \equiv 1 \pmod{\pi^{e+1}}, \\ (\varepsilon_1, \varepsilon_2) &\approx 1. \end{aligned} \tag{36}$$

Действительно, если мы будем представлять ε_1 или ε_2 в каноническом виде,

$$\varepsilon_1 = E(\alpha) \prod E(\alpha_i, \pi^i),$$

то все i , для которых $\alpha_i \not\equiv 0 \pmod{p}$, будут больше, чем e . Следовательно,

$$\begin{aligned} \varepsilon_1 &\approx E(\alpha) \prod_{i>e} E(\alpha_i, \pi^i), \\ \varepsilon_2 &\approx E(\beta) \prod_{j>e} E(\beta_j, \pi^j), \\ (\varepsilon_1, \varepsilon_2) &\approx \delta \prod_{i,j} E(i\alpha_i\beta_j, \pi^{i+j}). \end{aligned}$$

Но $i + j > 2e > pe_1$ и, следовательно, $E(i\alpha_i\beta_j, \pi^{i+j})$ является p -й степенью. Это доказывает (36).

2. Замена переменных. Исследуем теперь разложение числа $E(\alpha, \pi^i)$ в произведение $\prod_r E(\alpha_r, \tau^r)$ при помощи нового простого числа τ . При этом мы не будем предполагать, что $r < pe_1$ и $r \not\equiv 0 (p)$, так что полученное нами разложение не будет, вообще говоря, каноническим.

Пусть $\pi = \varphi(\tau)$, где φ — степенной ряд без свободного члена с коэффициентами из $\mathfrak{R}$. Так как $E(\alpha, \pi^i) = e^{L(\alpha, \pi^i)}$, то нам достаточно выяснить, как ряд $L(\alpha, \varphi(\tau)^i)$ может быть представлен в виде $\sum_r L(\alpha_r, \tau^r)$.

Предварительно введем обозначение:

$$L(1, x) = L(x).$$

Лемма. Имеет место тождество:

$$L(x + y) = L(x) + L(y) + \sum_{r=1}^{\infty} \sum_{i=1}^{p^r-1} A_r^{(i)} L(x^i y^{p^r-i}), \quad (37)$$

где $A_r^{(i)}$ определяются из соотношения:

$$\frac{(x + y)^{p^r} - (x^p + y^p)^{p^{r-1}}}{p^r} = \sum A_r^{(i)} x^i y^{p^r-i}. \quad (38)$$

$A_r^{(i)}$ являются целыми рациональными числами, как это следует из сравнения:

$$(x + y)^{p^r} \equiv (x^p + y^p)^{p^{r-1}} (p^r),$$

которое легко доказывается индукцией по r .

Доказательство леммы. Нам надо доказать, что

$$\sum_{s=0}^{\infty} p^{-s} \sum_{r=1}^{\infty} \sum_{i=1}^{p^r-1} A_r^{(i)} (x^i y^{p^r-i})^{p^s} = L(x + y) - L(x) - L(y). \quad (39)$$

Согласно соотношению (38)

$$\sum_{i=1}^{p^r-1} A_r^{(i)} (x^i y^{p^r-i})^{p^s} = \frac{(x^{p^s} + y^{p^s})^{p^r} - (x^{p^{s+1}} + y^{p^{s+1}})^{p^{r-1}}}{p^r},$$

ПОЭТОМУ

$$\begin{aligned} & \sum_{s=0}^{\infty} p^{-s} \sum_{r=1}^{\infty} \sum_{i=1}^{p^r-1} A_r^{(i)} (x^i y^{p^r-i})^{p^s} \\ &= \sum_{s=0}^{\infty} \sum_{r=1}^{\infty} p^{-(r+s)} \left((x^{p^s} + y^{p^s})^{p^r} - (x^{p^{s+1}} + y^{p^{s+1}})^{p^{r-1}} \right), \quad (40) \end{aligned}$$

$$\begin{aligned} & \sum_{s=0}^{\infty} \sum_{r=1}^{\infty} p^{-(r+s)} (x^{p^s} + y^{p^s})^{p^r} \\ &= \sum_{s=0}^{\infty} p^{-s} \sum_{r=1}^{\infty} p^{-r} (x^{p^s} + y^{p^s})^{p^r} \\ &= \sum_{s=0}^{\infty} p^{-s} (L(x^{p^s} + y^{p^s}) - x^{p^s} - y^{p^s}), \quad (41) \end{aligned}$$

$$\begin{aligned} & \sum_{s=0}^{\infty} \sum_{r=1}^{\infty} p^{-(r+s)} (x^{p^{s+1}} + y^{p^{s+1}})^{p^{r-1}} \\ &= \sum_{s=0}^{\infty} p^{-(s+1)} \sum_{r=1}^{\infty} p^{-(r-1)} (x^{p^{s+1}} + y^{p^{s+1}})^{p^{r-1}} \\ &= \sum_{s=0}^{\infty} p^{-(s+1)} L(x^{p^{s+1}} + y^{p^{s+1}}). \quad (42) \end{aligned}$$

Подставляя (41) и (42) в (40), получим

$$\begin{aligned} & \sum_{s=0}^{\infty} p^{-s} \sum_{r=1}^{\infty} \sum_{i=1}^{p^r-1} A_r^{(i)} (x^i y^{p^r-i})^{p^s} \\ &= L(x+y) - \sum_{s=0}^{\infty} p^{-s} (x^{p^s} + y^{p^s}) = L(x+y) - L(x) - L(y), \end{aligned}$$

т.е. формулу (39). Лемма доказана.

Ясно, что формулу (37) можно распространить на любое число слагаемых, т.е. имеет место соотношение:

$$L\left(\sum x_i\right) = \sum L(x_i) + \sum_{r=1}^{\infty} \sum_{i_1+i_2+\dots+p^r} A_r^{(i_1 i_2 \dots)} L(x_1^{i_1} x_2^{i_2} \dots), \quad (43)$$

где $A_r^{(i_1 i_2 \dots)}$ определяются из формулы:

$$p^{-r} \left(\left(\sum x_i \right)^{p^r} - \left(\sum x_i^p \right)^{p^{r-1}} \right) = \sum_{i_1 + i_2 + \dots = p^r} A_r^{(i_1 i_2 \dots)} x_1^{i_1} x_2^{i_2} \dots$$

Пусть теперь $f(t)$ — степенной ряд от t без свободного члена и с целыми коэффициентами из $\mathbb{R}$:

$$f(t) = \sum_{n=1}^{\infty} \alpha_n t^n.$$

Если каждое число из поля инерции вида

$$\alpha_n = \sum \alpha_n^{(i)} p^i, \quad \alpha_n^{(i)} \in R,$$

записать как сумму элементов из R :

$$\alpha_n = \alpha_n^{(0)} + \underbrace{\alpha_n^{(1)} + \dots + \alpha_n^{(1)}}_{p \text{ раз}} + \underbrace{\alpha_n^{(2)} + \dots + \alpha_n^{(2)}}_{p^2 \text{ раз}} + \dots,$$

то $f(t)$ запишется в виде $\sum x_i$, где каждое x_i будет произведением элемента из R на степень t . Ясно, что

$$\sum x_i = f(t),$$

$$\sum x_i^p = f^P(t),$$

где под $f^P(t)$ подразумевается степенной ряд $\sum \alpha_n^P t^{pn}$. Применяя формулу (43), получим:

$$L(f(t)) = \sum L(\beta_h, t^h),$$

где

$$\sum \beta_h t^h = f(t) + p^{-1} (f(t)^p - f^P(t)) + p^{-2} (f(t)^{p^2} - f^P(t)^p) + \dots$$

или, если ввести обозначения

$$\Lambda_r f(t) = p^{-r} (f(t)^{p^r} - f^P(t)^{p^{r-1}}),$$

$$\sum \beta_h t^h = f + \sum_{r=1}^{\infty} \Lambda_r f. \quad (44)$$

Если $\alpha = \alpha_0 + \alpha_1 p + \dots$, $\alpha_i \in R$, то

$$L(\alpha, x) = L(\alpha_0, x) + pL(\alpha_1, x) + \dots.$$

Применяя к этому соотношению формулу (44), получим:

$$L(\alpha, f(t)) = \sum L(\beta_k, t^k),$$

где

$$\sum \beta_h t^h = \alpha f + \sum_{r=1}^{\infty} \alpha^{P^r} \Lambda_r f.$$

Для записи функции $E(\alpha, f(t))$ введем такое обозначение: если $f(t) = \sum \alpha_n t^n$ — ряд от t без свободного члена с целыми коэффициентами из R , а π — простое число из k , то

$$\mathcal{E}_{\pi}(f(t)) = \prod_n E(\alpha_n, \pi^n).$$

Ясно, что

$$\mathcal{E}_{\pi}(f_1(t) + f_2(t)) = \mathcal{E}_{\pi}(f_1(t)) \mathcal{E}_{\pi}(f_2(t)). \quad (45)$$

Полученную нами формулу замены переменных можно теперь записать так:

$$E(\alpha, \pi^i) = \mathcal{E}_{\tau} \left(\alpha \varphi^i + \sum_{r=1}^{\infty} \alpha^{P^r} \Lambda_r \varphi^i \right), \quad (46)$$

если $\pi = \varphi(\tau)$.

3. Инвариантность формулы (I). Пусть π выражено через τ с коэффициентами из R :

$$\pi = \tau w \psi(\tau), \quad (47)$$

где $w \in R$, а $\psi(\tau)$ — степенной ряд со свободным членом 1. $\psi(\tau)$ является главной единицей, и мы можем поэтому записать $\psi(\tau)$ в виде:

$$\psi(\tau) = \prod_{s=1}^{\infty} E(\beta_s, \tau^s), \quad \beta_s \in R.$$

Это не каноническое разложение, так как s пробегает все целые значения. Такое представление возможно ввиду п. 2 А § 1 и сравнения (4).

$$(\pi, E(\alpha, \pi^i)) = (\tau, E(\alpha, \tau^i w^i \psi(\tau)^i)) (\psi(\tau), E(\alpha, \tau^i w^i \psi(\tau)^i))$$

или, в силу соотношений (46) и (47),

$$\begin{aligned} (\pi, E(\alpha, \pi^i)) &= \left(\tau, \mathcal{E}_\tau \left(\alpha w^i \tau^i \psi^i + \sum \alpha^{P^r} w^{P^r i} \Lambda_r \tau^i \psi^i \right) \right) \\ &\times \left(\mathcal{E}_\tau \left(\sum \beta_s t^s \right), \mathcal{E}_\tau \left(\alpha w^i \tau^i \psi^i + \sum \alpha^{P^r} w^{P^r i} \Lambda_r \tau^i \psi^i \right) \right). \end{aligned} \quad (48)$$

В кольце степенных рядов от t с целыми коэффициентами из $\mathfrak{R}$ введем функцию fDg как билинейную функцию, удовлетворяющую соотношению:

$$\beta t^j D\alpha t^i = i\alpha \beta t^{i+j} + \sum_{m=1}^{\infty} (i\alpha^{P^m} \beta t^{P^m i+j} - j\alpha \beta^{P^m} t^{i+P^m j}).$$

Тогда, ввиду соотношения (32), имеет место формула:

$$(\mathcal{E}_\tau(f(t)), \mathcal{E}_\tau(g(t))) \approx \delta_\tau \mathcal{E}_\tau(gDf). \quad (49)$$

При помощи формулы (49) и соотношения

$$(\tau, \varphi) \approx \delta_\tau \varphi$$

(48) может быть записано в виде

$$(\pi, E(\alpha, \pi^i)) \approx \delta_\tau \mathcal{E}_\tau(\Phi(t)),$$

где

$$\Phi(t) = \rho(t\psi)^i + \sum_{r=1}^{\infty} \rho^{P^r} \Lambda_r (t\psi)^i + \left(\rho(t\psi)^i + \sum \rho^{P^r} \Lambda_r (t\psi)^i \right) D \sum \beta_s t^s,$$

для сокращения положено $\alpha w^i = \rho$.

Кроме функции D , введем в кольцо степенных рядов еще две функции d и ∂ тоже как билинейные функции, обладающие свойствами:

$$\begin{aligned}\beta t^j d \alpha t^i &= i \alpha \beta t^{i+j}, \\ \beta t^j \partial \alpha t^i &= \sum_{m=1}^{\infty} (i \alpha^{P^m} \beta t^{P^m i+j} - j \alpha \beta^{P^m} t^{i+P^m j}).\end{aligned}$$

Ясно, что

$$f D g = f d g + f \partial g. \quad (50)$$

$1 d g$ сокращенно будем записывать как $d g$. Функция $d g$ обладает таким свойством:

$$d f g = f d g + g d f. \quad (51)$$

Степенной ряд f , для которого можно подобрать такой ряд с целыми коэффициентами g , что $f = d g$, мы будем называть *гомологичным* 0 и писать $f \sim 0$. Соотношение (51) показывает, что

$$f d g \sim -g d f. \quad (52)$$

Так как $f \partial g = -g \partial f$, то

$$f D g \sim -g D f. \quad (53)$$

Формула (23) показывает, что если $f \sim 0$, то

$$\delta_\tau \mathcal{E}_\tau(f(t)) \approx 1,$$

следовательно, если мы докажем, что $\Phi \sim 0$, то этим будет доказана инвариантность формулы (I).

Заметим предварительно, что имеет место тождество:

$$f \partial g = f \sum_{m=1}^{\infty} (d g)^{P^m} - g \sum_{m=1}^{\infty} (d f)^{P^m}. \quad (54)$$

Ввиду билинейности обеих частей этой формулы достаточно проверить ее для $f = \beta t^j$, $g = \alpha t^i$, где она очевидна.

Ввиду соотношений (50) и (54)

$$\begin{aligned} \Phi &= \rho(t\psi)^i + \sum \rho^{P^r} \Lambda_r(t\psi)^i + \left(\rho(t\psi)^i + \sum \rho^{P^r} \Lambda_r(t\psi)^i \right) d \sum \beta_s t^s \\ &\quad - \sum \beta_s t^s \cdot \sum_{m=1}^{\infty} \left(d \left(\rho(t\psi)^i + \sum \rho^{P^r} \Lambda_r(t\psi)^i \right) \right)^{P^m} \\ &\quad + \left(\rho(t\psi)^i + \sum \rho^{P^r} \Lambda_r(t\psi)^i \right) \sum_{m=1}^{\infty} \left(d \sum \beta_s t^s \right)^{P^m}. \end{aligned}$$

Мы докажем, что при любом $l = 0, 1, \dots$ сумма всех членов этого выражения, содержащих ρ^{P^l} гомологична 0. Надо отдельно рассмотреть два случая.

А. $l = 0$. Коэффициент при ρ равен:

$$\begin{aligned} (t\psi)^i + (t\psi)^i d \sum \beta_s t^s + (t\psi)^i \sum_{m=1}^{\infty} \left(d \sum \beta_s t^s \right)^{P^m} \\ = (t\psi)^i \left(1 + \sum_{m=0}^{\infty} \left(d \sum \beta_s t^s \right)^{P^m} \right). \end{aligned}$$

Вычислим $\psi^{-1} d\psi$:

$$\psi^{-1} d\psi = d \log \psi = \sum dL(\beta_s, t^s) = \sum_{m=0}^{\infty} \left(d \sum \beta_s t^s \right)^{P^m}. \quad (55)$$

Следовательно, коэффициент при ρ равен:

$$(t\psi)^i (1 + \psi^{-1} d\psi).$$

Но

$$d(t\psi)^i = \psi^i dt^i + t^i d\psi^i = it^i \psi^i + it^i \psi^{i-1} d\psi = it^i \psi^i (1 + \psi^{-1} d\psi).$$

Так как $i \not\equiv 0 (p)$, то

$$(t\psi)^i (1 + \psi^{-1} d\psi) = d \left(\frac{1}{i} (t\psi)^i \right) \sim 0.$$

В. $l \geq 1$. Коэффициент при ρ^{P^l} равен:

$$\Lambda_l(t\psi)^i + \Lambda_l(t\psi)^i d \sum \beta_s t^s + \Lambda_l(t\psi)^i \sum_{m=1}^{\infty} \left(d \sum \beta_s t^s \right)^{P^m} - \sum \beta_s t^s \cdot \left((d(t\psi)^i)^{P^l} + \sum_{m=1}^{l-1} (d\Lambda_m(t\psi)^i)^{P^{l-m}} \right).$$

Первые три члена этого выражения преобразуются, как и в случае А и оказываются равными

$$\Lambda_l(t\psi)^i (1 + \psi^{-1} d\psi).$$

Для преобразования четвертого члена заметим, что для любого f

$$\begin{aligned} dp^{-m} f^{P^m} &= f^{P^m-1} df, \\ dp^{-m} f^{P^{P^m-1}} &= f^{(P^m-1)P} (df)^P, \\ d\Lambda_m f &= f^{P^m-1} df - f^{(P^m-1)P} (df)^P \end{aligned} \quad (56)$$

и, следовательно,

$$\begin{aligned} (df)^{P^l} + \sum_{m=1}^{l-1} (d\Lambda_m f)^{P^{l-m}} &= (df)^{P^l} \\ &+ \sum_{m=1}^{l-1} (f^{(P^m-1)P^{l-m}} (df)^{P^{l-m}} - f^{(P^m-1)P^{l-m+1}} (df)^{P^{l-m+1}}) \\ &= f^{(P^{l-1}-1)P} (df)^P. \end{aligned}$$

Применяя это соотношение к $f = (t\psi)^i$, получим для четвертого члена выражение

$$i(t\psi)^{P^{l-1}i} (1 + (\psi^{-1} d\psi)^P).$$

Таким образом, коэффициент при ρ^{P^l} равен

$$\Lambda_l(t\psi)^i (1 + \psi^{-1} d\psi) - \sum \beta_s t^s \cdot i(t\psi)^{P^{l-1}i} (1 + (\psi^{-1} d\psi)^P). \quad (57)$$

Теперь мы используем то, что $n = 1$, и, следовательно, все эти степенные ряды интересуют нас только $(\bmod p)$. Ввиду тождества

$$df^p g = f^p dg + p f^{p-1} g df \equiv f^p dg \pmod{p}$$

p -е степени степенных рядов играют роль констант и поэтому не влияют на гомологичность 0. В частности, мы можем отбросить в выражении (57) множитель $(t\psi)^{Pp^{l-1}i}$, не изменив гомологичность или негомологичность 0 всего выражения. После этого остается:

$$\psi^{-Pp^{l-1}i} \Lambda_l \psi^i (1 + \psi^{-1} d\psi) - i \sum \beta_s t^s (1 + (\psi^{-1} d\psi)^P). \quad (58)$$

$$\psi^{-Pp^{l-1}i} \Lambda_l \psi^i = p^{-l} ((\psi^p \psi^{-P})^{p^{l-1}i} - 1).$$

Используя формулу (29), получим, что

$$\begin{aligned} \psi^p \psi^{-P} &= e^p \sum \beta_s t^s, \\ \psi^{-Pp^{l-1}i} \Lambda_l \psi^i &= p^{-l} (e^{ip^l \sum \beta_s t^s} - 1). \end{aligned}$$

По предположению $p \neq 2$, и поэтому

$$p^{-l} (e^{ip^l \sum \beta_s t^s} - 1) \equiv i \sum \beta_s t^s \pmod{p^l}.$$

В результате выражение (58) превращается в

$$\begin{aligned} i \sum \beta_s t^s (1 + \psi^{-1} d\psi) - i \sum \beta_s t^s (1 + (\psi^{-1} d\psi)^P) \\ = i \sum \beta_s t^s (\psi^{-1} d\psi - (\psi^{-1} d\psi)^P). \end{aligned} \quad (59)$$

Но

$$\begin{aligned} \psi^{-1} d\psi &= \sum_{m=0}^{\infty} (d \sum \beta_s t^s)^{P^m}, \\ (\psi^{-1} d\psi)^P &= \sum_{m=1}^{\infty} (d \sum \beta_s t^s)^{P^m}, \\ \psi^{-1} d\psi - (\psi^{-1} d\psi)^P &= d \sum \beta_s t^s \end{aligned}$$

и выражение (59) превращается в

$$i \sum \beta_s t^s d \sum \beta_s t^s = d \frac{i}{2} \left(\sum \beta_s t^s \right)^2 \sim 0$$

ввиду того, что $p \neq 2$ и, следовательно, $\frac{i}{2}$ — целое.

4. Преобразование формулы (II). Докажем, что если $\pi = \varphi(\tau)$, то

$$(E(\alpha, \pi^i), E(\beta, \pi^j)) = \delta_\tau \mathcal{E}_\tau (i\alpha\beta\varphi^{i+j-1} d\varphi). \quad (60)$$

Ввиду соотношений (46) и (49)

$$(E(\alpha, \pi^i), E(\beta, \pi^j)) = \delta_\tau \mathcal{E}_\tau (\Phi(t)),$$

где

$$\Phi(t) = \left(\beta\varphi^j + \sum_{r=1}^{\infty} \beta^{P^r} \Lambda_r \varphi^j \right) D \left(\alpha\varphi^i + \sum_{s=1}^{\infty} \alpha^{P^s} \Lambda_s \varphi^i \right).$$

Равенство (60) будет доказано, если мы установим, что

$$\Phi \sim i\alpha\beta\varphi^{i+j-1} d\varphi \pmod{p}.$$

Обозначим φ^i через f , а φ^j через g . Тогда получим:

$$\Phi = \left(\beta g + \sum_{r=1}^{\infty} \beta^{P^r} \Lambda_r g \right) D \left(\alpha f + \sum_{s=1}^{\infty} \alpha^{P^s} \Lambda_s f \right).$$

Ввиду соотношений (50) и (54)

$$\begin{aligned} \Phi &= \left(\beta g + \sum \beta^{P^r} \Lambda_r g \right) d \left(\alpha f + \sum \alpha^{P^s} \Lambda_s f \right) \\ &+ \left(\beta g + \sum \beta^{P^r} \Lambda_r g \right) \sum_{m=1}^{\infty} \left(d \left(\alpha f + \sum \alpha^{P^s} \Lambda_s f \right) \right)^{P^m} \\ &- \left(\alpha f + \sum \alpha^{P^s} \Lambda_s f \right) \sum_{m=1}^{\infty} \left(d \left(\beta g + \sum \beta^{P^r} \Lambda_r g \right) \right)^{P^m} \end{aligned}$$

или, ввиду билинейности функции fdg ,

$$\begin{aligned}\Phi &= \alpha\beta gdf + \sum_{r,s} \beta^{P^r} \Lambda_r g d\alpha^{P^s} \Lambda_s f + \beta g d \sum_s \alpha^{P^s} \Lambda_s f \\ &+ \left(\sum_r \beta^{P^r} \Lambda_r g \right) d\alpha f + \beta g \sum_{m=1}^{\infty} (d\alpha f)^{P^m} + \beta g \sum_{m,s} (d\alpha^{P^s} \Lambda_s f)^{P^m} \\ &+ \left(\sum_r \beta^{P^r} \Lambda_r g \right) \sum_m (d\alpha f)^{P^m} + \sum_{r,s,m} \beta^{P^r} \Lambda_r g (d\alpha^{P^s} \Lambda_s f)^{P^m} \\ &- \alpha f \sum_m (d\beta g)^{P^m} - \alpha f \sum_{m,r} (d\beta^{P^r} \Lambda_r g)^{P^m} \\ &- \left(\sum_s \alpha^{P^s} \Lambda_s f \right) \sum_m (d\beta g)^{P^m} - \sum_{r,s,m} \alpha^{P^s} \Lambda_s f (d\beta^{P^r} \Lambda_r g)^{P^m}.\end{aligned}$$

Мы докажем, что в этом выражении сумма всех членов, за исключением первого $\alpha\beta gdf$, гомологична 0. Именно, мы докажем, что коэффициент при $\alpha^{P^a} \beta^{P^b}$, где или a или $b > 0$, гомологичен 0. Надо отдельно рассмотреть два случая

А. $b = 0$, $a > 0$. Коэффициент при $\alpha^{P^a} \beta$ равен:

$$gd\Lambda_a f + g \left((df)^{P^a} + \sum_{s=1}^{a-1} (d\Lambda_s f)^{P^{a-s}} \right) = g \left((df)^{P^a} + \sum_{s=1}^a (d\Lambda_s f)^{P^{a-s}} \right).$$

На основании соотношений (56) это равно $gf^{P^a-1}df$. Теперь вспомним, что $f = \varphi^i$, $g = \varphi^j$:

$$gf^{P^a-1}df = i\varphi^{P^a i + j - 1}d\varphi.$$

Ввиду того, что $j \not\equiv 0 \pmod{p}$, $P^a i + j \not\equiv 0 \pmod{p}$ и

$$gf^{P^a-1}df = d \left(\frac{i}{P^a i + j} \varphi^{P^a i + j} \right) \sim 0.$$

Аналогично рассматривается случай $a = 0$, $b > 0$.

В. $a > 0$ и $b > 0$. Коэффициент при $\alpha^{P^a} \beta^{P^b}$ равен

$$\begin{aligned}\Lambda_b g d\Lambda_a f + \Lambda_b g \left((df)^{P^a} + \sum_{s=1}^{a-1} (d\Lambda_s f)^{P^{a-s}} \right) \\ - \Lambda_a f \left((dg)^{P^b} + \sum_{r=1}^{b-1} (d\Lambda_r g)^{P^{b-r}} \right).\end{aligned}$$

Применяя тождества (56), получим, что это выражение равно

$$\begin{aligned} \Lambda_b g (f^{p^a-1} df - f^{(p^{a-1}-1)P} (df)^P) + \Lambda_b g \cdot f^{(p^{a-1}-1)P} (df)^P \\ - \Lambda_a f \cdot g^{(p^{b-1}-1)P} (dg)^P = \Lambda_b g \cdot f^{p^a-1} df - \Lambda_a f \cdot g^{(p^{b-1}-1)P} (dg)^P. \end{aligned} \quad (61)$$

Заметим, что имеет место следующее тождество:

$$h^{-1} \Lambda_1 \varphi^h \equiv \varphi^{P(h-1)} \Lambda_1 \varphi \quad (p). \quad (62)$$

Действительно,

$$h^{-1} \frac{\Lambda_1 \varphi^h}{\Lambda_1 \varphi} = h^{-1} \frac{\varphi^{ph} - \varphi^{P^h}}{\varphi^p - \varphi^P} = \varphi^{P(h-1)} h^{-1} \frac{(\varphi^p \varphi^{-P})^h - 1}{(\varphi^p \varphi^{-P}) - 1}.$$

Но, так как $\varphi^p \equiv \varphi^P \quad (p)$, то

$$h^{-1} \frac{(\varphi^p \varphi^{-P})^h - 1}{(\varphi^p \varphi^{-P}) - 1} \equiv 1 \quad (p),$$

что и дает тождество (62).

Если подставить вместо f φ^i , а вместо g φ^j , то, ввиду тождества $\Lambda_a f = p^{-a+1} \Lambda_1 f^{p^{a-1}}$ и на основании тождества (62), выражение (61), будет сравнимо $(\text{mod } p)$ с

$$ij \Lambda_1 \varphi (\varphi^{p^a i + p^b j - p - 1} d\varphi - \varphi^{p^a i + p^b j - 2p} (d\varphi)^P). \quad (63)$$

При этом мы всюду, где можно, заменим φ^P на φ^p . Отбрасывая в (63) $\varphi^{p^a i + p^b j - 2p}$, мы, как указывалось в п. 3, не изменим гомологичности или негомологичности 0 всего выражения. В результате останется

$$ij \Lambda_1 \varphi (\varphi^{p-1} d\varphi - (d\varphi)^P) = ij \Lambda_1 \varphi d\Lambda_1 \varphi.$$

Ввиду того, что $p \neq 2$

$$ij \Lambda_1 \varphi d\Lambda_1 \varphi = d \frac{ij}{2} (\Lambda_1 \varphi)^2 \sim 0.$$

5. Инвариантность формулы (II). Для доказательства инвариантности формулы (II) нам надо, ввиду соотношения (60), показать, что

$$\delta_\pi E(i\alpha\beta, \pi^{i+j}) \approx \delta_\tau \mathcal{E}_\tau(i\alpha\beta \varphi^{i+j-1} d\varphi),$$

где $\pi = \varphi(\tau)$ — выражение простого числа π через простое число τ . Иначе говоря, нам надо доказать, что для любого $m > 1$

$$\delta_\pi E(\alpha, \pi^m) \approx \delta_\tau \mathcal{E}_\tau(\alpha \varphi^{m-1} d\varphi). \quad (64)$$

Для $m > pe_1$ формула (64) очевидна, так как обе ее части являются p -ми степенями. Поэтому мы будем доказывать формулу для фиксированного значения m , считая, что для больших значений m она доказана.

Если $m \neq 0 \pmod{p}$, то формула очевидна, так как левая часть равна 1 по определению, а правая ввиду того, что

$$\alpha \varphi^{m-1} d\varphi = d\left(\frac{\alpha}{m} \varphi^m\right) \sim 0.$$

Нам остается разобрать два случая.

А. $m = pe_1$. Согласно соотношению (14), где надо положить $n = 1$,

$$\delta_\pi E(\alpha, \pi^{pe_1}) \approx E(\gamma_{e_0}^{-p} \alpha). \quad (65)$$

Пусть

$$\pi = \varphi(\tau) = \lambda_1 \tau + \dots$$

Подставляя это выражение в

$$\zeta - 1 = \gamma_{e_0} \pi^{e_0} + \dots,$$

получим

$$\zeta - 1 = \gamma_{e_0} \lambda_1^{e_0} \tau^{e_0} + \dots,$$

т.е.

$$\gamma'_{e_0} = \gamma_{e_0} \lambda_1^{e_0}. \quad (66)$$

С другой стороны,

$$[\alpha \varphi^{m-1} d\varphi]_{t=\tau} = \alpha \lambda_1^{pe_1} \tau^{pe_1} + \dots = \alpha \lambda_1^{pe_0} \tau^{pe_1} + \dots,$$

так как $e_0 = e_1$ ввиду того, что $n = 1$. Поэтому

$$\delta_\tau \mathcal{E}_\tau(\alpha \varphi^{m-1} d\varphi) \approx \delta_\tau E(\alpha \lambda_1^{pe_0}, \tau^{pe_1}) \approx E((\gamma'_{e_0})^{-p} \alpha \lambda_1^{pe_0}). \quad (67)$$

Подставляя выражение (66) в соотношение (67) и сравнивая с (65), получаем формулу (64) в нашем случае.

В. $m = pu < pe_1$. Ввиду соотношения (29) имеем:

$$E(\alpha, \pi^{pu}) \approx e^{-p\alpha^{p-1}\pi^u}. \quad (68)$$

Для аналогичного преобразования левой части формулы (64) заметим, что

$$\alpha \varphi^{pu-1} d\varphi - \alpha \varphi^{P(u-1)} (d\varphi)^P = d\alpha u^{-1} \Lambda_1 \varphi^u \sim 0,$$

следовательно,

$$\begin{aligned} \alpha \varphi^{pu-1} d\varphi &\sim \alpha \varphi^{P(u-1)} (d\varphi)^P, \\ \delta_\tau \mathcal{E}_\tau (\alpha \varphi^{pu-1} d\varphi) &\approx \delta_\tau \mathcal{E}_\tau (\alpha \varphi^{P(u-1)} (d\varphi)^P). \end{aligned} \quad (69)$$

По определению $\mathcal{E}_\tau$ и ввиду соотношения (29) имеем:

$$\mathcal{E}_\tau (\alpha \varphi^{P(u-1)} (d\varphi)^P) \approx \left[e^{-p\alpha^{P-1} \varphi^{u-1} d\varphi} \right]_{t=\tau}. \quad (70)$$

Пусть

$$-p\alpha^{P-1} \pi^u = \sum_{v=e+u}^{\infty} \lambda_v \pi^v, \quad (71)$$

где $\lambda_v \in R$, а все $v \geq e+u > pu$, ввиду того, что $u < e_1$. Поскольку $\pi = \varphi(\tau)$, будем иметь:

$$-p\alpha^{P-1} \varphi(\tau)^u = \sum \lambda_v (\varphi(\tau))^v \quad (72)$$

или, умножая на $[\varphi^{-1} d\varphi]_{t=\tau}$,

$$-p\alpha^{P-1} [\varphi^{u-1} d\varphi]_{t=\tau} = \sum \lambda_v [\varphi^{v-1} d\varphi]_{t=\tau}. \quad (73)$$

Из соотношений (69), (70), (73) и (30) следует, что

$$\delta_\tau \mathcal{E}_\tau (\alpha \varphi^{pu-1} d\varphi) \approx \delta_\tau \mathcal{E}_\tau \left(\sum \lambda_v \varphi^{v-1} d\varphi \right), \quad (74)$$

а из (68), (71) и (30), что

$$E(\alpha, \pi^{pu}) \approx \mathcal{E}_\pi \left(\sum \lambda_v t^v \right). \quad (75)$$

Но в формулах (74) и (75) $v > pu$ и, следовательно, для $m = v$ формула доказана, т.е.

$$\delta_\pi \mathcal{E}_\pi (\lambda_v t^v) \approx \delta_\tau \mathcal{E}_\tau (\lambda_v \varphi^{v-1} d\varphi),$$

а ввиду равенства (45)

$$\delta_\pi \mathcal{E}_\pi \left(\sum \lambda_v t^v \right) \approx \delta_\tau \mathcal{E}_\tau \left(\sum \lambda_v \varphi^{v-1} d\varphi \right). \quad (76)$$

Сравнивая соотношения (74), (75) и (76), получаем формулу (64).

§ 4. Закон взаимности

1. Символ норменного вычета. Мы опять предполагаем, как и в § 3, что $n = 1$, $p \neq 2$.

Теорема 5. Если поле k получается замыканием некоторого поля алгебраических чисел по простому идеалу $\mathfrak{p}$, то символ $\chi(\lambda, \mu)$ совпадает с символом норменного вычета $\left(\frac{\lambda, \mu}{\mathfrak{p}}\right)$.

Доказательство. Пусть π — произвольное простое число.

Разберем отдельно четыре случая.

A. $\lambda = \pi$, $\mu = E(\alpha)$. По определению символа $\chi(\lambda, \mu)$

$$\chi(\pi, E(\alpha)) = \chi E(\alpha).$$

С другой стороны, в работе Хассе ([5], стр. 182) доказано, что

$$\chi E(\alpha) = \left(\sqrt[p]{E(\alpha)} \right)^{1-\sigma},$$

где σ — автоморфизм Артина неразветвленного расширения $k\left(\sqrt[p]{E(\alpha)}\right)/k$. Но по определению символа норменного вычета это как раз и значит, что

$$\left(\frac{\pi, E(\alpha)}{\mathfrak{p}} \right) = \chi E(\alpha).$$

B. $\lambda = \pi$, μ — любая главная единица ε . Пусть

$$\varepsilon = E(\alpha) \prod E(\alpha_i, \pi^i); \quad (77)$$

Тогда

$$\chi(\pi, \varepsilon) = \chi E(\alpha).$$

С другой стороны,

$$\left(\frac{\pi, \varepsilon}{\mathfrak{p}} \right) = \left(\frac{\pi, E(\alpha)}{\mathfrak{p}} \right) \prod \left(\frac{\pi, E(\alpha_i, \pi^i)}{\mathfrak{p}} \right). \quad (78)$$

Но ввиду того, что $E(\alpha_i, \pi^i)$ являются нормами из $k(\sqrt[p]{\pi})/k$,

$$\left(\frac{\pi, E(\alpha_i, \pi^i)}{\mathfrak{p}} \right) = 1. \quad (79)$$

Сравнивая соотношения (77), (78) и (79), получаем нужный результат.

С. $\lambda = \varepsilon_1$, $\mu = \varepsilon_2$ — любые главные единицы. Здесь мы существенно пользуемся доказанной в § 3 инвариантностью символа (λ, μ) .

Обозначим простое число $\pi\varepsilon_1$ через τ . Тогда

$$\chi(\varepsilon_1, \varepsilon_2) = \chi(\pi\varepsilon_1, \varepsilon_2)\chi(\pi, \varepsilon_2)^{-1} = \chi(\tau, \varepsilon_2)\chi(\pi, \varepsilon_2)^{-1},$$

$$\left(\frac{\varepsilon_1, \varepsilon_2}{\mathfrak{p}}\right) = \left(\frac{\tau, \varepsilon_2}{\mathfrak{p}}\right) \left(\frac{\pi, \varepsilon_2}{\mathfrak{p}}\right)^{-1}.$$

Ввиду инвариантности символа (λ, μ) мы можем применить результат случая В к простому числу τ так же, как и к π . Мы получим:

$$\chi(\pi, \varepsilon_2) = \left(\frac{\pi, \varepsilon_2}{\mathfrak{p}}\right),$$

$$\chi(\tau, \varepsilon_2) = \left(\frac{\tau, \varepsilon_2}{\mathfrak{p}}\right),$$

что и доказывает теорему в этом случае.

Д. Общий случай. Пусть

$$\lambda \approx \pi^a \varepsilon_1,$$

$$\mu \approx \pi^b \varepsilon_2,$$

$$\chi(\lambda, \mu) = \chi(\pi, \varepsilon_2)^a \chi(\pi, \varepsilon_1)^{-b} \chi(\varepsilon_1, \varepsilon_2),$$

$$\left(\frac{\pi^a \varepsilon_1, \pi^b \varepsilon_2}{\mathfrak{p}}\right) = \left(\frac{\pi, \varepsilon_2}{\mathfrak{p}}\right)^a \left(\frac{\pi, \varepsilon_1}{\mathfrak{p}}\right)^{-b} \left(\frac{\varepsilon_1, \varepsilon_2}{\mathfrak{p}}\right).$$

Но ввиду В и С,

$$\chi(\pi, \varepsilon_1) = \left(\frac{\pi, \varepsilon_1}{\mathfrak{p}}\right),$$

$$\chi(\pi, \varepsilon_2) = \left(\frac{\pi, \varepsilon_2}{\mathfrak{p}}\right),$$

$$\chi(\varepsilon_1, \varepsilon_2) = \left(\frac{\varepsilon_1, \varepsilon_2}{\mathfrak{p}}\right),$$

что и доказывает теорему в общем случае.

Теорема имеет смысл только для случая конечного поля классов вычетов. В случае произвольного поля k можно аналогично доказать совпадение символа (λ, μ) с символом, введенным Виттом (E. Witt, [12], стр. 153) при помощи теории алгебр.

2. Явная форма закона взаимности. Для степенных вычетов степени p выведена ([3], стр. 58) следующая неявная форма закона взаимности:

$$\left(\frac{\lambda}{\mu}\right) \left(\frac{\mu}{\lambda}\right)^{-1} = \prod_{p|\mu} \left(\frac{\lambda, \mu}{p}\right). \quad (80)$$

Применяя теорему 5, получаем следующую теорему:

Теорема 6 (явная форма закона взаимности). Если λ и μ — любые числа поля алгебраических чисел Ω , содержащего корни степени $p \neq 2$ из единицы, то

$$\left(\frac{\lambda}{\mu}\right) \left(\frac{\mu}{\lambda}\right)^{-1} = \prod_{p|\mu} (\lambda, \mu)_p, \quad (81)$$

где через $(\lambda, \mu)_p$ обозначено значение символа $\chi(\lambda, \mu)$ в поле Ω_p .

3. Закон взаимности Куммера. Покажем теперь, что закон взаимности Куммера является частным случаем закона взаимности, выведенного в п.2.

Формулировка закона взаимности Куммера. Пусть Ω — поле корня нечетной простой степени p из единицы, а λ и μ — два целых алгебраических числа, удовлетворяющих условиям:

$$\lambda \equiv \mu \equiv 1 \pmod{p-1}.$$

Представим λ в виде $f(\zeta)$, где $f(1) = 1$ и f — целочисленный многочлен степени не выше p . Положим

$$\left. \frac{d^h \log f(e^v)}{dv^h} \right|_{v=0} = l_h(\lambda).$$

Аналогичный смысл имеют $l_h(\mu)$. Тогда имеет место формула:

$$\left(\frac{\lambda}{\mu}\right) \left(\frac{\mu}{\lambda}\right)^{-1} = \zeta^{l_1(\lambda)l_{p-1}(\mu) - l_2(\lambda)l_{p-2}(\mu) + \dots - l_{p-1}(\lambda)l_1(\mu)}. \quad (82)$$

Доказательство. Ввиду тождества

$$\sum_{h=1}^{p-1} (-1)^h \frac{d^h F(x+1)}{dx^h} \frac{d^{p-h} G(x+1)}{dx^{p-h}} \Big|_{x=0} \equiv \sum (-1)^h \frac{d^h F(e^v)}{dv^h} \frac{d^{p-h} G(e^v)}{dv^{p-h}} \Big|_{v=0} (p),$$

имеющего место для любых функций F и G , $l_h(\lambda)$ можно заменить на $\overline{l}_h(\lambda)$:

$$\overline{l}_h(\lambda) = \frac{d^h \log f(x+1)}{dx^h} \Big|_{x=0}.$$

Обозначим $\zeta - 1$ через π и заметим, что

$$\lambda = f(1 + \pi) = \varphi(\pi),$$

где $\varphi(x)$ — целочисленный многочлен со свободным членом 1. Для вычисления (λ, μ) нам нужно знать коэффициенты α_i в каноническом представлении

$$\lambda = \varphi(\pi) = E(\alpha) \prod_{i=1}^{p-1} E(\alpha_i, \pi^i).$$

Они определяются из тождества: $\log \varphi(x) \equiv \sum_{i=1}^{p-1} \alpha_i x^i (x^p)$, т.е.

$$\alpha_i \equiv \frac{1}{i!} \frac{d^i \log \varphi(x)}{dx^i} \Big|_{x=0} \equiv \frac{1}{i!} \overline{l}_i(\lambda) (p).$$

Следовательно,

$$\lambda \approx E(\alpha) \prod_{i=1}^{p-1} E\left(\frac{1}{i!} \overline{l}_i(\lambda), \pi^i\right), \quad \mu \approx E(\beta) \prod_{j=1}^{p-1} E\left(\frac{1}{j!} \overline{l}_j(\mu), \pi^j\right),$$

$$(\lambda, \mu) \approx \delta \prod_{i,j} E\left(\frac{i}{i!j!} \overline{l}_i(\lambda) \overline{l}_j(\mu), \pi^{i+j}\right).$$

Но если $i + j > p$ или $i + j < p$, то $\delta E\left(\frac{i}{i!j!} \overline{l}_i(\lambda) \overline{l}_j(\mu), \pi^{i+j}\right) \approx 1$. Для $i + j = p$

$$\frac{i}{i!j!} \equiv (-1)^{i-1} (p),$$

следовательно, $\chi(\lambda, \mu) \approx \delta \prod_{i=1}^{p-1} E((-1)^{i-1} \overline{l_i(\lambda)} \overline{l_{p-i}(\mu)}, \pi^p)$, т.е.

$$\chi(\lambda, \mu) = \zeta^{\sum (-1)^{i-1} \overline{l_i(\lambda)} \overline{l_{p-i}(\mu)}}.$$

Если теперь применить закон взаимности, выведенный в п. 2, заметив, что в правой части фигурирует только один простой идеал $\mathfrak{p} = (\zeta - 1)$, то получится формула (82).

(Поступило в редакцию 24 января 1949 г.)

Литература

- [1] E. Artin und H. Hasse, *Die beiden Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln*, Abh. Math. Sem. Hamburg **6** (1928), 146–162.
- [2] Ван-дер-Варден, *Современная алгебра*, ч. I, М.–Л., 1947.
- [3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, II, *Reziprozitätsgesetz*, Leipzig–Berlin, 1930.
- [4] ———, *Die Normenresttheorie relativ-Abescher Zahlkörper als Klassenkörpertheorie im Kleinen*, Journ. für die reine und angew. Math. **162** (1930), 145–168.
- [5] ———, *Die Gruppe der p^n -primären Zahlen für einen Primteiler $\mathfrak{p}$ von p* , Journ. für die reine und angew. Math. **176** (1936), 174–183.
- [6] K. Hensel, *Theorie der algebraischen Zahlen*, Leipzig–Berlin, 1908.
- [7] ———, *Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers*, Journ. für die reine und angew. Math. **136** (1916).
- [8] D. Hilbert, *Gesammelte Abhandlungen*, Bd. I, Berlin, 1932.
- [9] ———, *Gesammelte Abhandlungen*, Bd. III, Berlin, 1935.
- [10] H.L. Schmid, *Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper*, Math. Zeitschr. **40** (1936), 194–209.
- [11] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n* , Journ. für die reine und angew. Math. **176** (1936), 126–140.
- [12] ———, *Schiefkörper über diskret bewerteten Körpern*, Journ. für die reine und angew. Math. **176** (1936), 153–156.

НОВОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ КРОНЕКЕРА–ВЕБЕРА

ТРУДЫ МАТ. ИНСТ. ИМ.

В.А.СТЕКЛОВА Т.XXXVIII (1951)

Теорема Кронекера–Вебера, утверждающая, что всякое абелево расширение поля рациональных чисел содержится в некотором поле деления круга, является центральной теоремой теории абелевых расширений поля рациональных чисел. Эта теорема не только дает классификацию абсолютно абелевых полей, но и определяет законы разложения в них, дает возможность выяснить структуру их дискриминантов и получить явные выражения для числа классов идеалов.

После того как Кронекер [7] в 1853 г. высказал эту теорему, было предложено много ее доказательств, основывающихся на различных принципах [1, 2, 5, 6, 8].

Настоящая статья содержит новое доказательство теоремы Кронекера–Вебера, отличающееся от ранее известных тем, что оно, во-первых, значительно короче их, а во-вторых, в большей мере выясняет суть дела. Именно, оказывается, что теорема Кронекера–Вебера является по существу p -адическим фактом. Если доказать p -адический аналог этой теоремы, то сама теорема получается автоматически путем применения теоремы Минковского о существовании критических простых чисел.

Для удобства читателя мы будем пользоваться только основами теории p -адических полей в изложении Вейля ([4], гл. III, § 10 и 12) и упомянутой выше теоремой Минковского ([4], стр. 166). При этом теорему Минковского мы будем использовать в эквивалентной ей форме, названной Н.Г.Чеботаревым арифметической теоремой монодромии. Согласно этой теореме объединение групп инерции всех критических простых идеалов нормального расширения поля рациональных чисел есть группа Галуа.

Из алгебраических средств будет использована только основная теорема теории Галуа и теорема Лагранжа о циклических полях

([3], гл. VII).

Так как всякое абелево поле есть композит полей, степени которых — степени простых чисел, то мы имеем право ограничиться в дальнейшем рассмотрении полей степени l^n . Обозначим через $K(l^m; p_1, \dots, p_r)$ объединение всех циклических полей K , дискриминанты которых делятся только на простые числа $p_1, \dots, p_r$, а порядок делит l^m . $K(l^m; p_1, \dots, p_r)$ — конечное расширение, так как таких полей K только конечное число. Действительно, если через k обозначить поле корня l^m -й степени из единицы, то $Kk = k(\sqrt[m]{\alpha})$ и в α все простые идеалы, кроме делителей $p_1, \dots, p_r$, входят в степенях, делящихся на l^m . Все числа α с таким свойством получаются из конечного числа их умножением на l^m -ю степень числа, а следовательно, и число полей конечно.

Ввиду того, что всякое абелево поле степени l^n содержится в некотором $K(l^m; p_1, \dots, p_r)$, достаточно доказать, что всякое поле $K(l^m; p_1, \dots, p_r)$ есть подполе поля деления круга. Это и будет сделано, причем сначала мы исследуем аналогичные расширения полей p -адических чисел.

Поле $K(l^m; p_1, \dots, p_r)$ является аналогом поля алгебраических функций, риманова поверхность которого имеет абелеву группу монодромии, заданные точки ветвления и в них порядки ветвления, не превосходящие заданного числа.

Для дальнейшего нам будут нужны следующие три простые леммы.

Лемма 1. Пусть R — поле, характеристика которого не делится на простое число l , $k = R(\zeta)$, где ζ — корень степени l из единицы и s — образующий автоморфизм группы Галуа k , причем $\zeta^s = \zeta^g$. Поле $k(\sqrt[l]{\alpha})$ абелево над R тогда и только тогда, когда $\alpha^s = \alpha^g \alpha_0^l$ при некотором α_0 .

Доказательство. Ввиду нормальности $k(\sqrt[l]{\alpha})$ над R $\alpha^s = \alpha^h \alpha_0^l$. Пусть $\bar{s}$ и σ — автоморфизмы $k(\sqrt[l]{\alpha})$, определенные формулами

$$\begin{aligned}\sqrt[l]{\alpha}^{\bar{s}} &= \sqrt[l]{\alpha}^h \alpha_0; & \xi^{\bar{s}} &= \xi^s \text{ при } \xi \in k, \\ \sqrt[l]{\alpha}^{\sigma} &= \zeta \sqrt[l]{\alpha}; & \xi^{\sigma} &= \xi \text{ при } \xi \in k.\end{aligned}$$

Абелевость $k(\sqrt[l]{\alpha})$ дает $\bar{s}\sigma = \sigma\bar{s}$ или при применении к $k(\sqrt[l]{\alpha})$: $g = h$. Повторяя рассуждение в обратном порядке, доказываем достаточность условия.

Лемма 2. Пусть R — поле характеристики, отличной от 2. Для того, чтобы поле $R(\sqrt{a})$ было подполем циклического поля k 4-й степени, необходимо, чтобы a имело вид $u^2 + v^2$, $u, v \in R$.

Доказательство. Пусть $k = R(\sqrt{a}, \sqrt{x + y\sqrt{a}})$. Из нормальности k следует, что

$$x - y\sqrt{a} = (x + y\sqrt{a})(r + s\sqrt{a})^2.$$

Автоморфизм σ , определенный формулами

$$\sqrt{x + y\sqrt{a}}^\sigma = \sqrt{x + y\sqrt{a}}(r + s\sqrt{a}), \quad \sqrt{a}^\sigma = -\sqrt{a},$$

является образующей группы Галуа k . Условие $\sigma^2 \neq 1$ дает

$$-1 = (r + s\sqrt{a})(r - s\sqrt{a}),$$

или

$$-1 = r^2 - s^2 a,$$

т.е.

$$a = \left(\frac{r}{s}\right)^2 + \left(\frac{1}{s}\right)^2.$$

Лемма 3. Пусть R_p — поле p -адических чисел, ζ и k имеют тот же смысл, что и в лемме 1, и $\lambda = 1 - \zeta$. Для того, чтобы единица $\varepsilon \in k$ и сравнимая с 1 по модулю λ была l -й степенью, необходимо и достаточно, чтобы $\varepsilon \equiv 1 \pmod{\lambda^{l+1}}$.

Доказательство. λ является простым элементом k и $l = \lambda^{l-1}\xi$, где

$$\begin{aligned} \xi &= \frac{(1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{l-1})}{(1 - \zeta)^{l-1}} \\ &= (1 + \zeta)(1 + \zeta + \zeta^2) \cdots (1 + \zeta + \cdots + \zeta^{l-2}) \end{aligned}$$

([4], стр. 86). Заметим, что $\xi \equiv (l - 1)! \equiv -1 \pmod{\lambda}$.

Пусть $\varepsilon = \varepsilon_0^l$, $\varepsilon_0 = 1 + a\lambda + \beta\lambda^2$, где a — целое рациональное, а β — любое из k

$$\varepsilon = \varepsilon_0^l \equiv 1 + la\lambda + a^l\lambda^l \equiv 1 + a(1 + \zeta)\lambda^l \equiv 1 \pmod{\lambda^{l+1}}.$$

Пусть $\varepsilon \equiv 1 \pmod{\lambda^{l+1}}$. Докажем, что для любого $i > l$ существует ε_i такое, что

$$\varepsilon_{i+1} \equiv \varepsilon_i \pmod{\lambda^{i-l+1}}; \quad \varepsilon_i^l \equiv \varepsilon \pmod{\lambda^i}.$$

За ε_{l+1} возьмем 1. Пусть ε_i уже выбрано и

$$\varepsilon \varepsilon_i^{-l} \equiv 1 + a_i \lambda^i (\lambda^{i+1}).$$

Рассмотрим $\eta_i = 1 - a_i \lambda^{i-l+1}$

$$\eta_i^l \equiv 1 - a_i l \lambda^{i-l+1} \equiv 1 + a_i \lambda^i \equiv \varepsilon \varepsilon_i^{-l} (\lambda^{i+1}).$$

Мы можем за ε_{i+1} взять $\varepsilon_i \eta_i$. Если $\lim \varepsilon_i = \varepsilon_0$, то $\varepsilon = \varepsilon_0^l$.

Перейдем теперь к рассмотрению p -адического аналога теоремы Кронекера–Вебера. Мы будем рассматривать абелевы расширения поля p -адических чисел R_p , степень которых есть степень простого числа l . Обозначим через $K(l^m, p)$ композит всех циклических расширений R_p , степень которых есть делитель l^m . Через $Z(l^m, p)$ обозначим в случае $p = l = 2$ поле 2^{m+2} -го корня из единицы, в случае $p = l \neq 2$ подполе l^m -й степени поля l^m -го корня из единицы и при $p \neq l$ максимальное подполе показателя l^m поля p -го корня из единицы. Степень $Z(l^m, p)$ есть 2^{m+1} при $p = l = 2$, l^m при $p = l \neq 2$ и l^h , где $l^h = (l^m, p-1)$ при $p \neq l$.

Локальный аналог теоремы Кронекера–Вебера. Поле $K(l^m, p)$ является композитом неразветвленного поля $W(l^m)$ степени l^m и поля деления круга $Z(l^m, p)$.

Доказательство. Ясно, что $K(l^m, p)$ содержит $W(l^m)$ и $Z(l^m, p)$, а значит и их композит. Достаточно, следовательно, доказать, что степень $K(l^m, p)$ не превосходит степени $W(l^m)Z(l^m, p)$.

Доказательство этого разбивается на три части.

1) $p \neq l$. Степень f простого идеала поля $K(l^m, p)$ совпадает со степенью $W(l^m)$, так как $W(l^m)$ есть поле инерции $K(l^m, p)$ и нам достаточно доказать, что показатель ветвления e не превосходит степени $Z(l^m, p)$, т.е. l^h . Из того, что e является порядком циклической (ввиду $p \neq l$) группы инерции, следует, что e делит l^m . Остается доказать, что оно делит $p-1$.

Пусть σ — автоморфизм, индуцирующий автоморфизм $A \rightarrow A^p$ в поле классов вычетов, τ — образующая группы инерции и Π — простое число $K(l^m, p)$

$$\Pi^\tau \equiv \alpha \Pi (\Pi^2)$$

и порядок α по модулю Π равняется e . Ввиду абелевости поля имеем

$$\Pi^{\sigma\tau} \equiv \alpha \Pi^\sigma \equiv \Pi^{\tau\sigma} \equiv (\alpha \Pi)^\sigma \equiv \alpha^p \Pi^\sigma (\Pi^2),$$

$$\alpha^{p-1} \equiv 1 (\Pi),$$

что и надо было доказать.

2) $p = l \neq 2$. Группа Галуа $W(l^m)Z(l^m, l)$ есть прямое произведение двух циклических групп порядка l^m , т.е. максимальная группа показателя l^m с двумя образующими. Ввиду этого нам достаточно доказать, что группа Галуа поля $K(l^m, l)$ имеет не более двух образующих. Так как число образующих абелевой l -группы равно числу образующих ее максимальной фактор-группы показателя l , то все сводится к тому, чтобы показать, что степень поля $K(l, l)$ не превосходит l^2 .

По лемме 1 эта степень равна индексу $(\alpha : \beta^l)$, где α и β — отличные от 0 числа k и $\alpha^s = \alpha^g \alpha_0^l$. Представим α в виде $\lambda^h \eta$, где η — единица. Ввиду того, что $\lambda^s = \lambda \eta_0$ и $g \not\equiv 1 (l)$, h должно делиться на l . Пусть $\eta \equiv a (\lambda)$, где a — целое рациональное, $\eta \equiv a^l (\lambda)$ и $\eta a^{-l} = \varepsilon \equiv 1 (\lambda)$. Таким образом, $\alpha = \varepsilon \gamma^l$ и при подсчете индекса $(\alpha : \beta^l)$ мы можем считать, что $\alpha \equiv \beta \equiv 1 (\lambda)$. Согласно лемме 3, индекс $(\alpha : \beta^l)$ не превосходит числа тех классов вычетов $(\text{mod } \lambda^{l+1})$, для которых $\alpha^s \equiv \alpha^g (\lambda^{l+1})$.

$\zeta = 1 - \lambda$, по определению s и g , удовлетворяет этому соотношению. Если $\alpha = 1 + a\lambda (\lambda^2)$, то $\alpha \zeta^a = \alpha_1 \equiv 1 (\lambda^2)$ и удовлетворяет тому же соотношению. Предположим, что $\alpha_1 \equiv 1 + a_i \lambda^i (\lambda^{i+1})$. Из того, что $\lambda = 1 - \zeta$, $\zeta^s = \zeta^g$ следует, что $\lambda^s \equiv g\lambda (\lambda^2)$, следовательно

$$\begin{aligned}\alpha_1^s &\equiv 1 + a_i g^i \lambda^i \equiv \alpha_1^g \equiv 1 + a_i g \lambda^i (\lambda^{i+1}), \\ g^{i-1} &\equiv 1 (e), \quad i = l.\end{aligned}$$

Таким образом, $\alpha = \zeta^a (1 + \lambda^l)^b \varepsilon_0^l$, т.е. индекс не превосходит l^2 .

3) $p = l = 2$. Группа Галуа $W(2^m)Z(2^m, 2)$ имеет инварианты $(2, 2^m, 2^m)$, т.е. является максимальной 2-группой с тремя образующими показателя 2^m и одним инвариантом, равным 2. Ввиду этого нам достаточно доказать, что группа Галуа поля $K(2^m, 2)$: а) имеет три образующих и б) по крайней мере один ее инвариант равен 2.

а) Как и в 2), достаточно доказать, что степень $K(2, 2)$ равна 8. Эта степень равна индексу $(a : a^2)$, где a пробегает все отличные от 0 числа $R_2 : a = 2^h c$, где $c \equiv 1 (2)$, причем, по лемме 3, $c = b^2$ тогда и только тогда, когда $c \equiv 1 (8)$. Следовательно,

$$a = 2^n (-1)^m 5^k a_0^2; \quad (a : a_0^2) = 8.$$

б) Если бы все инварианты группы Галуа $K(2^m, 2)$ были бы не меньше 4, то $K(4, 2)$ имело бы группу Галуа с инвариантами $(4, 4, 4)$. Из этого следовало бы, что всякое квадратичное подполе содержится в некотором циклическом 4-й степени. Но это

не так, ввиду леммы 2, для $R_2(\sqrt{-1})$. Действительно, уравнение $-1 = u^2 + v^2$ не разрешимо в R_2 даже (mod 4).

Доказательство локальной теоремы закончено.

Доказательство теоремы Кронекера–Вебера. Поле $K(l^m; p_1, \dots, p_r)$ содержит поля $Z(l^m, p_i)$ $i = 1, \dots, r$, а, следовательно, и их композит $\bar{K}$. Докажем, что оно с этим композитом совпадает. Для этого заметим, что группа Галуа $\bar{K}$ есть прямое произведение групп $Z(l^m, p_i)$, так как пересечение композита всех полей, кроме i -го с i -м, не разветвлено и, следовательно, совпадает с полем рациональных чисел. Показатель ветвления $\bar{e}_i$ простого числа p_i в $\bar{K}$ равен степени $Z(l^m, p_i)$ ([4], стр. 139) и, следовательно, степень $\bar{K}$ равна $\prod_i \bar{e}_i$.

С другой стороны, $K(l^m; p_1, \dots, p_r)$ после p_i -адического замыкания становится, согласно локальной теореме, подполем композита $W(l^m)Z(l^m, p_i)$ и, следовательно, показатель ветвления e_i числа p_i в $K(l^m; p_1, \dots, p_r)$ удовлетворяет неравенству $e_i \leq \bar{e}_i$. Согласно арифметической теореме монодромии, группа Галуа $K(l^m; p_1, \dots, p_r)$ есть объединение групп инерции, а ввиду абелевости поля отсюда следует, что степень его не превосходит $\prod e_i$. Так как $\prod e_i \leq \prod \bar{e}_i$, а $\prod \bar{e}_i$ — степень $\bar{K}$, то $K(l^m; p_1, \dots, p_r) = \bar{K}$. Теорема доказана.

Литература

- [1] Н. Чеботарев, *Доказательство теоремы Кронекера–Вебера относительно абелевых областей*, Матем. сборник **31** (1923).
- [2] Б.Н. Делоне (B. Delaunay), *Zur Bestimmung der Zahlkörper durch Kongruenzen; eine Anwendung auf die Abelschen Gleichungen*, Journ. Math. **152** (1922).
- [3] Ван дер Варден, *Современная алгебра*, М., 1947.
- [4] Вейль, *Алгебраическая теория чисел*, М., 1947.
- [5] R. Fueter, *Abelsche Körper in quadratisch imaginären Zahlkörpern*, Math. Ann. **75** (1914).
- [6] D. Hilbert, *Ges. Abh.*, vol. 1, Berlin, 1932.
- [7] L. Kronecker, *Über die algebraisch auflösbaren Gleichungen*, Ber. K. Akad. Wiss., Berlin, 1853.
- [8] A. Speiser, *Die Zerlegungsgruppe*, Journ. Math. **149** (1920).
- [9] H. Weber, *Theorie der Abelschen Zahlkörper*, Acta Math. **8–9** (1886).

О ЗАДАЧЕ ПОГРУЖЕНИЯ ПОЛЕЙ

ДОКЛ. АКАД. НАУК СССР Т. ХСV, NO.3 (1954)

Пусть дана конечная группа G и ее гомоморфный образ F с фиксированным гомоморфизмом G на F . Задача погружения заключается в разыскании условий, при которых заданное нормальное расширение K/k с группой Галуа F может быть погружено в расширение $\bar{K}/k$ с группой Галуа G , причем так, чтобы предписанный гомоморфизм G на F совпадал с естественным гомоморфизмом группы Галуа поля на группу Галуа подполя.

Расширение F до G называется полупрямым, если соответствующая система множителей ассоциирована с 1. В этом случае G определяется заданием F и ядра $\mathfrak{G}$ гомоморфизма G на F как операторной группы с областью операторов F . Мы будем писать в этом случае $G = F \times \mathfrak{G}$. Шольц [1] показал, что если $\mathfrak{G}$ абелево, а G — полупрямое расширение, то задача погружения всегда разрешима. Имеет место следующее обобщение этого факта на случай нильпотентного нормального делителя $\mathfrak{G}$:

Теорема 1. Если G есть полупрямое расширение F , а нормальный делитель $\mathfrak{G}$ имеет порядок l^α и класс c , и если $l \geq c$, то любое поле алгебраических чисел L/k с группой F погружаемо в поле $K \supset L$ с группой G над k .

Доказательство основано на следующих соображениях. Пусть $(F : 1) = m$. Обозначим через $\mathfrak{G}_{d,F}^{(c,k)}$ фактор-группу свободного произведения md циклических групп порядка l^k с образующими $s_{\sigma,i}$ ($\sigma \in F, i = 1, \dots, d$) по c -му члену убывающего центрального ряда. Правило

$$s_{\sigma,i}^\tau = s_{\sigma\tau,i}, \quad \tau \in F,$$

превращает F в область операторов для $\mathfrak{G}_{d,F}^{(c,k)}$. Любая группа порядка l^α с областью операторов F есть операторно-гомоморфный образ некоторой группы $\mathfrak{G}_{d,F}^{(c,k)}$. Ввиду этого достаточно доказать теорему для случая $\mathfrak{G} = \mathfrak{G}_{d,F}^{(c,k)}$.

Существует такая абелева группа N с областью операторов F , что центр группы $\mathfrak{G} = N \cdot \mathfrak{G}_{d,F}^{(c,k)}$ разлагается в прямое произведение допустимых подгрупп, каждая из которых есть прямое произведение t циклических подгрупп порядка l^k , сопряженных относительно F . Это следует из того, что группа всех автоморфизмов группы $\mathfrak{G}_{d,F}^{(c,k)}$ индуцирует в ее центре представления Ли [2] полной линейной группы по модулю l^k . Ввиду того, что $l \geq c$, представление Ли является прямым слагаемым тензорного представления [3], а будучи ограничено группой F , тензорное представление распадается в прямую сумму регулярных.

Пусть L/k есть поле с группой F . Расширение K/L с группой $\mathfrak{G}_{d,F}^{(c,k)}$, имеющее над k группу $F \times \mathfrak{G}_{d,F}^{(c,k)}$, мы будем строить шольцевым над L относительно l^{k+1} (см. заметку [4], понятиями и результатами которой мы будем дальше пользоваться). Ввиду вышеизложенного поле K может быть построено следующим образом. Пусть уже построено поле K_0/k с группой $F \times \mathfrak{G}_{d,F}^{(c-1,k)}$. Поле K можно найти среди подполей композита полей $\overline{K_i}$, каждое из которых является композитом t сопряженных относительно k полей K_i^σ , $\sigma \in F$. В свою очередь $K_i \supset K_0$, причем K_i нормально над L и имеет над ним совершенно определенную группу Галуа, являющуюся расширением $\mathfrak{G}_{d,F}^{(c-1,k)}$ с центральным нормальным делителем порядка l^k . При этом K_i^σ должны быть независимыми над K_0 .

Условия, при которых K_0 может быть погружено в такие поля $\overline{K_i}$, чтобы их композит был шольцевым, заключаются в том, чтобы для него инварианты $[\chi, X], [X]_\psi$ и $(X)_{l^{k+1}}$, введенные в работе [4], равнялись 1. Этому добиваются так же, как и в этой работе. Именно, доказывается, что для всякого числа d существует такое число $D > d$, что у любого шольцевого поля $\overline{K_0} \supset L \supset k$ с группой $F \times \mathfrak{G}_{D,F}^{(c-1,k)}$ над k существует нормальное над k подполе с группой $F \times \mathfrak{G}_{d,F}^{(c-1,k)}$, все инварианты которого равны 1.

Отсюда индукцией по c (при любом d и заданных k и F) получаем утверждение теоремы.

Аналогичные рассуждения дают следующий результат:

Теорема 2. Если $G = F \times \mathfrak{G}$, порядки F и $\mathfrak{G}$ взаимно просты и $\mathfrak{G}$ нильпотентно, то любое поле алгебраических чисел L/k с группой F погружаемо в поле $K \supset L$ с группой G над k .

Введенные в работе [4] инварианты и в других случаях тесно связаны с задачей о погружении, как это видно на следующем простейшем примере.

Пусть k – поле алгебраических чисел, l – простое число, отличное от 2 и 3, и k содержит корень степени l^2 из 1. Рассмотрим такие три числа $\alpha_1, \alpha_2, \alpha_3$ поля k , что поле $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3})$ имеет степень l^3 и шольцево относительно l^2 . В данном случае требование шольцевости сводится к тому, чтобы α_1, α_2 и α_3 были l -гиперпримарными и удовлетворяли соотношениям

$$\left(\frac{\alpha_i}{p_j}\right) = 1, \quad p_j \mid \alpha_j, \quad i \neq j, \quad i, j = 1, 2, 3.$$

Рассмотрим класс X l -инвариантных чисел поля $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2})$, соответствующий погружению этого поля в поле с некоммутативной группой Галуа порядка l^3 и всеми элементами порядка l и характер χ группы Галуа поля $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3})$, для которого $\alpha_\chi = \alpha_3$. В этом случае определен инвариант $[\chi, X]$, введенный в работе [4] (здесь все $l_i = l$ и $G = \mathfrak{G}_l$ есть элементарная абелева группа порядка l^3). Мы будем его обозначать через $[\alpha_1, \alpha_2, \alpha_3]$. Этот символ обладает следующими свойствами:

$$[\alpha_1 \beta_1, \alpha_2, \alpha_3] = [\alpha_1, \alpha_2, \alpha_3][\beta_1, \alpha_2, \alpha_3],$$

$$[\alpha_i, \alpha_j, \alpha_k] = \pm [\alpha_1, \alpha_2, \alpha_3],$$

где i, j, k есть перестановки чисел 1, 2, 3, а знаки $+$ и $-$ соответствуют четным и нечетным перестановкам.

Обозначим через G фактор-группу свободного произведения трех циклических групп порядка l по третьему члену убывающего центрального ряда. Фактор-группа G по коммутанту изоморфна группе Галуа поля $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3})$, а коммутант абелев (но не содержится в центре). Связь символа $[\alpha_1, \alpha_2, \alpha_3]$ с задачей погружения заключается в следующем:

Теорема 3. *Необходимым и достаточным условием для погружаемости поля $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3})$ в поле с группой Галуа G над k является равенство единице символа $[\alpha_1, \alpha_2, \alpha_3]$.*

Д.К. Фаддеев [5] и позже независимо от него Хассе [6] нашли необходимое условие для погружаемости поля с любой группой F в поле с группой G , являющейся расширением F . Ввиду предположенной нами шольцевости поля $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3})$ для него это условие выполнено. С другой стороны, при заданных α_1 и α_2 можно всегда так подобрать α_3 , чтобы поле $k(\sqrt[l]{\alpha_1}, \sqrt[l]{\alpha_2}, \sqrt[l]{\alpha_3})$ было шольцевым, а символ $[\alpha_1, \alpha_2, \alpha_3]$ имел любое наперед заданное значение. Ввиду теоремы 3 это показывает, что необходимое условие погружаемости, найденное Д.К. Фаддеевым и Хассе, не является достаточным, как это предполагал Хассе [6].

Поступило 21.01.1954

ЛИТЕРАТУРА

1. A. Scholz, Math. Zs. **30** (1929), 332.
2. R. Thrall, Bull. Am. Math. Soc. **47** (1941), 303.
3. R. Brauer, Ann. of Math. **38** (1937), 857.
4. И.Р. Шафаревич, ДАН **95**, **№2** (1954).
5. Б.И. Делоне, Д.К. Фаддеев, Матем. сборн. **15** (**57**) (1944), 243.
6. H. Hasse, Math. Nachr. **40** (1948).

О ПОСТРОЕНИИ ПОЛЕЙ С ЗАДАННОЙ ГРУППОЙ ГАЛУА ПОРЯДКА l^α

ИЗВ. АКАД. НАУК СССР СЕР. МАТ. Т. 18, (1954) 261-296

Резюме. В работе излагается новый метод построения полей с заданной группой Галуа порядка l^α , дающий более широкий класс полей, чем известный ранее метод Шольца-Рейхардта. В частности, этот метод применим и при $l = 2$.

Введение

Существование полей с заданной группой Галуа порядка l^α ($l > 2$) над заданным полем алгебраических чисел было доказано в 1937 году А. Шольцем [9].

Построенное в основном на тех же идеях, но более простое доказательство было предложено Г. Рейхардтом [8].

О решении той же задачи без ограничения $l > 2$ было сообщено Т. Таннака [10]. Кажется, до сих пор не было замечено, что доказательство Таннака содержит ошибку. Указание ошибки в рассуждении и построение противоречащего примера к тому утверждению, на котором Таннака строит свое доказательство, содержится в п.3 §2 настоящей работы.

Класс полей с заданной группой Галуа порядка l^α , который может быть построен методом Шольца-Рейхардта, ограничен в двух отношениях.

Во-первых, накладывается ограничение $l > 2$, так что остается открытым вопрос о существовании полей с заданной группой Галуа порядка 2^α , в то время как этот вопрос представляется интересным, например, с точки зрения теории построений циркулем и линейкой.

Во-вторых, методом Шольца-Рейхардта строятся только расширения над полем рациональных чисел. Правда, из расширения K/R над полем рациональных чисел можно получить расширение Kk/k над любым числовым полем k , которое, если только $K \cap k = R$, имеет ту же группу Галуа. Однако таким образом

строится весьма узкий класс полей. Например, все такие поля инвариантны при всех автоморфизмах k/R .

Легко видеть, что для того, чтобы построить поля с некоторыми очень простыми группами Галуа, необходимо научиться строить поля с группой Галуа порядка l^α , которые не могут быть построены методом Шольца–Рейхардта. Пусть, например, G есть группа порядка l^α , Γ — прямое произведение n групп G_i , изоморфных G , и $\mathfrak{G}$ — группа, имеющая нормальный делитель Γ , причем элементы факторгруппы $\mathfrak{G}/\Gamma$ индуцируют в Γ автоморфизмы, сводящиеся к перестановке G_i . Предположим, что над полем рациональных чисел R существует поле K с группой Галуа $\mathfrak{G}$ и пусть k — подполе, принадлежащее к Γ . Поле K/k является композитом n полей K_i/k , имеющих группу Галуа G , сопряженных между собой и взаимно простых над k . Как было сказано выше, такие поля не могут быть построены методом Шольца–Рейхардта. Аналогичным образом, построение полей с любыми разрешимыми группами Галуа тесно связано с построением достаточно общих полей с группой Галуа порядка l^α .

Настоящая работа содержит метод построения полей с заданной группой Галуа порядка l^α , при котором на конструируемые поля не накладываются ограничения, имеющие место в методе Шольца–Рейхардта. В частности, доказывается, что над любым полем алгебраических чисел существует расширение с заданной группой Галуа порядка 2^a .

При построении используются условия, найденные Шольцем, при которых поле может быть погружено центральным образом в поле с заданной группой Галуа. Поля, удовлетворяющие этим условиям, называются шольцевыми. Основной задачей является нахождение условий, при которых данное шольцево поле погружаемо центральным образом в шольцево же поле с заданной группой Галуа. Для этого строятся инварианты шольцева поля (χ, X) и $(X)_h$, из которых наибольшую роль играют инварианты (χ, X) . Эти инварианты определяются, исходя из арифметических свойств поля. Они представляют собою скалярное произведение элементов одномерной и двумерной групп когомологий, по своим свойствам напоминающее индекс пересечения. Равенство инвариантов единице и является необходимым и достаточным условием погружаемости.

Задача сводится, таким образом, к построению шольцевых полей с инвариантами, равными единице. Это делается в §3, где доказывается, что в шольцевом поле, группа Галуа которого имеет достаточно много образующих, обязательно содержится подполе с нужной группой Галуа и с инвариантами, равными единице. Для этого строится теория гомоморфизмов групп порядка l^α и вводится

понятие их композиции, превращающееся в случае абелевых групп в умножение характеров.

В работе неоднократно используется закон плотностей Чеботарева, так что могло бы показаться, что используются аналитические соображения. Однако, просмотрев соответствующие рассуждения, легко заметить, что можно было бы ограничиться применением теоремы Фробениуса в группах порядка l^α . Как заметил Дейринг [6], в этом случае теорема Фробениуса может быть доказана не аналитически.

Автор глубоко благодарен Д.К. Фаддееву, просмотревшему рукопись этой работы и сделавшему ряд ценных замечаний.

§1. Инварианты центральных расширений

В этом параграфе будут исследованы свойства полей алгебраических чисел, группы Галуа которых имеют порядок, равный степени простого числа. Относительно всех групп, которые будут нам встречаться, мы будем предполагать, что их порядок есть степень одного и того же простого числа l .

1. Алгебраические свойства центральных расширений.

Группа G_1 будет называться центральным расширением группы G , если G является гомоморфным образом G_1 , а ядро гомоморфизма лежит в центре G_1 и имеет показатель l . При этом и самый гомоморфизм включается в понятие расширения, так что два разных гомоморфизма G_1 на G будут давать разные расширения. Если ядро гомоморфизма G_1 на G является циклической группой порядка l , то мы будем называть расширение простым и центральным.

Если k — произвольное поле, Ω — его конечное, нормальное сепарабельное расширение, K — промежуточное подполе $k \subset K \subset \Omega$ и K/k нормально, то группа Галуа Ω/k является расширением группы Галуа K/k . Если это расширение центральное, соответственно простое центральное, то мы и Ω/k будем называть центральным, соответственно простым центральным расширением поля K/k .

Предположим, что k имеет характеристику $\neq l$ и содержит корень степени l из 1, а Ω/k является простым центральным расширением K/k . Тогда Ω/K является циклическим полем степени l и поэтому $\Omega = K(\sqrt[l]{\mu})$ с некоторым $\mu \in K$ (см. [1], стр. 217).

Как известно (см. [8], стр. 3), то обстоятельство, что Ω/k является центральным расширением поля K/k , эквивалентно тому, что μ удовлетворяет соотношению

$$\mu^\sigma \approx \mu, \quad (1)$$

где σ — любой автоморфизм K/k . Здесь, как и всюду дальше, запись

$$\alpha \approx \beta$$

будет обозначать, что $\alpha\beta^{-1}$ есть l -я степень, само же соотношение будет называться l -равенством. Числа μ , обладающие свойством (1), мы будем называть l -инвариантными.

Пусть группа Галуа Ω/k есть G_1 , группа K/k есть G , группа Ω/K есть Z . Так как G_1 есть центральное расширение G , то этим определяется система множителей $a(\sigma, \tau)$ на G со значениями из Z и с единичными автоморфизмами (см. [2], стр. 334). Выбранное нами число μ определяет при помощи соответствия

$$\sqrt[l]{\mu^z} = X(z)\sqrt[l]{\mu}, \quad z \in Z,$$

характер X группы Z . Применяя X к $a(\sigma, \tau)$, мы получим систему множителей

$$X(a(\sigma, \tau)) = \zeta(\sigma, \tau),$$

заданную на G со значениями из группы корней степени l из 1.

Легко проверить, что два l -инвариантных числа определяют одну и ту же систему множителей $\zeta(\sigma, \tau)$ тогда и только тогда, когда их отношение l -равно инвариантному числу (числу из k). Легко видеть, что произведению l -инвариантных чисел соответствует произведение систем множителей. Группу всех классов неассоциированных систем множителей на G со значениями из группы корней l -й степени из 1, мы будем обозначать через $M(G)$. Из вышеизложенного следует, что факторгруппа группы всех l -инвариантных чисел по подгруппе чисел, l -равных инвариантным, изоморфна некоторой подгруппе M' группы $M(G)$:

$$(\mu)/(mC^l) \cong M' \subseteq M(G). \quad (2)$$

Нам будет полезно следующее представление $M(G)$. Пусть $s_1, \dots, s_d$ — некоторая минимальная система образующих G . Она определяет представление G в виде S/N , где S — свободная группа с d образующими, а N — ее нормальный делитель. Обозначим через N' подгруппу N , порожденную коммутаторами элементов N с элементами S и l -ми степенями элементов N .

Лемма 1. $M(G)$ изоморфна группе характеров группы N/N' .

Эта лемма является следствием известной теоремы (см. [2], стр. 335), согласно которой для любой группы G , представленной в виде факторгруппы свободной группы S по нормальному делителю N ,

группа всех классов систем множителей с единичными автоморфизмами и со значениями в произвольной абелевой группе A изоморфна факторгруппе всех гомоморфизмов $N/[S, N]$ в A по подгруппе тех гомоморфизмов, которые индуцируются гомоморфизмами S в A .

Здесь $[S, N]$ означает нормальный делитель S , порожденный коммутаторами элементов S с элементами N .

В рассматриваемом нами случае A есть группа корней степени l из 1. Гомоморфизмы $N/[S, N]$ в A должны поэтому переводить в 1 все l -ые степени элементов N , т.е. совпадают с характерами группы N/N' .

Чтобы вывести из сформулированной выше теоремы нашу лемму, нам остается только показать, что любой характер группы N/N' , индуцируемый характером порядка l группы S , равен 1.

Это эквивалентно тому, что $N \subset S'$, где S' — подгруппа S , порождаемая коммутаторами и l -ми степенями. То же самое условие можно выразить в виде соотношения

$$S/S' \cong G/G',$$

где G' — подгруппа G , порожденная l -ми степенями и коммутаторами (подгруппа Фраттини). Правильность написанного выше соотношения следует из того, что группы, стоящие в обеих частях, изоморфны элементарным абелевым группам порядка l^d . Для S/S' это очевидно. Для G/G' это следует из теоремы о подгруппе Фраттини (см. [2], стр. 402), согласно которой $s_1, \dots, s_d$ будет тогда и только тогда минимальной системой образующих в G , когда она будет таковой в G/G' .

2. Шольцевы поля. Одной из основных задач теории полей, группа Галуа которых есть l -группа, является исследование условий, при которых данное нормальное расширение K/k погружаемо в центральное расширение Ω/k , группа Галуа которого является заданным центральным расширением группы Галуа K/k . Брауэром (см. [5], стр. 56) были найдены для этого необходимые и достаточные условия в терминах распадаения некоторых алгебр. Однако условия Брауэра, как правило, трудно непосредственно использовать. Для случая, когда k есть поле алгебраических чисел, небольшим усилением условий Брауэра можно получить, как заметил Шольц [9], следующие условия, достаточные для того, чтобы K/k было погружаемо в расширение Ω/k , группа Галуа которого есть любое центральное расширение группы Галуа K/k :

1⁰. Простые делители l в k полностью распадаются в K .

2⁰. Вещественные бесконечно удаленные дивизоры k остаются вещественными в K .

3°. Все критические простые дивизоры p_i расширения K/k имеют относительный порядок 1.

4°. Абсолютные нормы критических простых дивизоров удовлетворяют условию: $\mathfrak{N}(p_i)^m \equiv 1(l^h)$ при некотором m , взаимно простом с l , и достаточно большом h (если $(K:k) = l^\alpha$, то достаточно, чтобы было $h > \alpha$).

Заметим, что если k содержит корень степени l из 1, то в условии 4° мы можем положить $m = 1$, так как в этом случае $\mathfrak{N}(p) \equiv 1(l)$.

Будем называть поля, удовлетворяющие условиям 1° — 4°, шольцевыми. У шольцева поля группа M' в (2) совпадает с $M(G)$, т.е.

$$(\mu)/(mC^l) \cong M(G).$$

Ввиду этого, а также ввиду леммы 1, мы будем обозначать одной и той же буквой X :

1) класс l -инвариантных чисел по подгруппе чисел, l -равных инвариантным,

2) элемент $M(G)$ и

3) характер группы N/N' .

Центральные расширения (даже простые) шольцева поля K/k сами, вообще говоря, не являются шольцевыми полями. В самом деле, если даже $K(\sqrt[l]{\mu})/k$ является шольцевым полем, то можно так подобрать число $m \in k$, чтобы поле $K(\sqrt[l]{\mu m})/k$, имеющее над k ту же группу Галуа, что и $K(\sqrt[l]{\mu})$, не было уже шольцевым.

Для доказательства существования поля с заданной группой порядка l^α важно знать, когда у шольцева поля K/k существует шольцево расширение с любой группой, являющейся центральным расширением группы Галуа K/k . Шольц показал, что такое расширение всегда существует, если k есть поле рациональных чисел и $l > 2$. Этот факт является основным в его доказательстве существования расширений поля рациональных чисел с заданной группой нечетного порядка l^α .

Мы введем сейчас необходимые и достаточные условия существования такого расширения. Для этого нам нужно ввести некоторые новые инварианты полей, группы Галуа которых имеют порядок l^α , в предположении, что основное поле содержит корень степени l из 1.

3. Арифметическая структура l -инвариантных чисел.

Исследуем сначала разложение на множители l -инвариантного числа μ поля K . Рассмотрим какой-нибудь его простой делитель $\mathfrak{P}$. Предположим, что $\mathfrak{P}^\sigma$ входит в μ в степени $a(\sigma)$. Из l -инвариантности μ следует, что

$$a(\sigma) \equiv a(1)(l).$$

Таким образом, та часть разложения μ на множители, которая состоит из дивизоров, сопряженных с $\mathfrak{P}$, может быть разложена на произведение всех таких различных дивизоров в одной и той же степени, например, $a(1)$, и на l -ю степень. Первое произведение есть, очевидно, инвариантный дивизор. Поступая аналогично со всеми делителями μ , мы получим, что дивизор (μ) разлагается на l -ю степень и инвариантный дивизор. Так как всякий инвариантный дивизор есть произведение критических простых дивизоров на дивизор из основного поля, то мы получаем для μ разложение:

$$(\mu) \equiv \mathfrak{C}^l \mathfrak{D} m, \quad (3)$$

где m есть дивизор поля k , взаимно простой с дискриминантом K/k , а $\mathfrak{D}$ — инвариантный дивизор, состоящий только из простых делителей дискриминанта K/k , причем ни $\mathfrak{D}$, ни m не содержат l -х степеней. Ясно, что такое разложение однозначно.

Простые дивизоры $\mathfrak{P}$, делящие $\mathfrak{D}$, могут быть также охарактеризованы следующим свойством: порядок образующего автоморфизма группы инерции дивизора $\mathfrak{P}$ в K в l раз меньше, чем порядок любого элемента группы Галуа $K(\sqrt[l]{\mu})/k$, индуцирующего этот автоморфизм. Иными словами, образующая группы инерции $\mathfrak{P}$ в K повышает свой порядок при расширении K до $K(\sqrt[l]{\mu})$. При этом мы говорим об образующей группы инерции $\mathfrak{P}$ в K/k , так как эта группа циклическая, что следует из того, что $(l, \mathfrak{P}) = 1$ ввиду условия 1^0 в определении шольцева поля.

Для доказательства нашего утверждения заметим, что ввиду того же условия, $(l, \mathfrak{P}) = 1$, и группа инерции любого простого делителя $\mathfrak{P}$ в поле $K(\sqrt[l]{\mu})$ циклическая. Порядок этой группы или, что то же самое, ее образующей в l раз больше, чем порядок группы инерции $\mathfrak{P}$ в K , так как порядок ветвления увеличился в l раз при переходе от K к $K(\sqrt[l]{\mu})$. Таким образом, образующая группы инерции увеличивает свой порядок в l раз. Но если σ — любой автоморфизм $K(\sqrt[l]{\mu})/k$, индуцирующий в K образующий автоморфизм группы инерции $\mathfrak{P}$, то он имеет тот же порядок, что и образующий автоморфизм группы инерции простого делителя $\mathfrak{P}$ в $K(\sqrt[l]{\mu})$, так как он отличается от него только множителем, принадлежащим к центру G_1 и имеющим порядок l .

Заметим, что $\mathfrak{D}$ не меняется при умножении на число вида $m\mathfrak{C}^l$ и поэтому является инвариантом класса X . Мы будем поэтому обозначать $\mathfrak{D}$ через $\mathfrak{D}(X)$. Очевидно, что имеет место соотношение:

$$\mathfrak{D}(X_1 X_2) \approx \mathfrak{D}(X_1) \mathfrak{D}(X_2).$$

4. Инварианты (χ, X) . Мы будем называть два дивизора a и b l -взаимно простыми, если любой их общий простой делитель p входит в один из них в степени, делящейся на l . Напомним, что если a и b l -взаимно просты, то символ Лежандра $\left(\frac{a}{b}\right)$ определен.

Мы будем говорить, что дивизор a поля k l -взаимно прост с инвариантным дивизором $\mathfrak{B}$ поля K , если для любого простого дивизора p , входящего в a в степени, не делящейся на l , его простой делитель $\mathfrak{P}$ в K входит в $\mathfrak{B}$ в степени, делящейся на l .

Пусть p — произвольный простой дивизор поля k , l -взаимно простой с μ , и $\mathfrak{P}$ — произвольный простой делитель p в K . Символ Лежандра l -й степени $\left(\frac{\mu}{\mathfrak{P}}\right)$ не зависит от выбора $\mathfrak{P}$ среди делителей p . Действительно, если $\mathfrak{P}^\sigma$ — любой другой делитель, то

$$\left(\frac{\mu}{\mathfrak{P}^\sigma}\right) = \left(\frac{\mu^{\sigma^{-1}}}{\mathfrak{P}}\right) = \left(\frac{\mu}{\mathfrak{P}}\right),$$

так как $\mu^{\sigma^{-1}} \approx \mu$. Ввиду этого мы будем символ $\left(\frac{\mu}{\mathfrak{P}}\right)$ (зависящий на самом деле только от p) обозначать через $\left[\frac{\mu}{p}\right]$. Для p , не l -взаимно простых с μ , $\left[\frac{\mu}{p}\right]$ не определено. Распространив по мультипликативности символ $\left[\frac{\mu}{p}\right]$ на все дивизоры a поля k , l -взаимно простые с $m\mathfrak{D}$, получим символ $\left[\frac{\mu}{a}\right]$. Очевидно, что если a состоит из простых дивизоров, имеющих в K первый порядок, то существует такое $a \in K$, что $a = N_{K/k}(\mathfrak{A})$ и

$$\left[\frac{\mu}{a}\right] = \left(\frac{\mu}{\mathfrak{A}}\right). \quad (4)$$

Пусть α — число поля k , l -взаимно простое с $\mathfrak{D}(X)$ и удовлетворяющее следующим условиям:

- 1) α l -гиперпримарно;
- 2) α тотально-положительно (это условие существенно только при $l = 2$);
- 3) все простые дивизоры, входящие в α в степенях, не кратных l , разлагаются в K на простые множители первого порядка.

Если $(\alpha, m) \neq 1$, то умножим m на такое число $t \in K$, чтобы $(\alpha, mt) = 1$. Тогда для $\mu' = \mu t$ символ $\left[\frac{\mu'}{\alpha}\right]$ определен.

Рассмотрим отношение:

$$\left[\frac{\mu'}{\alpha}\right] \left(\frac{\alpha}{m'}\right)^{-1} \quad \text{с} \quad m' = mt. \quad (5)$$

Очевидно, что это отношение не зависит от выбора вспомогательного числа m . Замена m на m_1 , привела бы к умножению (5) на множитель

$$\left(\frac{mm_1^{-1}}{\alpha}\right)\left(\frac{\alpha}{mm_1^{-1}}\right)^{-1},$$

равный 1, по закону взаимности и ввиду l -гиперпримарности α . Больше того, выражение (5) не зависит от выбора μ внутри класса X l -инвариантных чисел, что доказывается точно так же. Ввиду этого мы будем обозначать отношение (5) через (α, X) .

Рассмотрим некоторый характер χ порядка l группы Галуа K/k . Как известно (см. [11], стр. 45), ему соответствует однозначно с точностью до l -равенства определенное число α_χ из k такое, что:

$$\sqrt[l]{\alpha_\chi} \in K, \quad \sqrt[l]{\alpha_\chi}^\sigma = \chi(\sigma)\sqrt[l]{\alpha_\chi}.$$

Ввиду того, что поле K/k предполагается шольцевым, то если α_χ l -взаимно просто с $\mathfrak{D}(X)$, оно удовлетворяет условиям, наложенным нами на число α , для которого мы только что определили символ (α, X) . Таким образом определен символ (α_χ, X) , который не зависит от выбора числа α_χ , соответствующего χ , и будет поэтому обозначаться через (χ, X) .

Выведем некоторые свойства этого символа. Прежде всего очевидно мультипликативность символа (χ, X) по аргументу χ :

$$(\chi_1\chi_2, X) = (\chi_1, X)(\chi_2, X), \quad (6)$$

так как $\alpha_{\chi_1\chi_2} \approx \alpha_{\chi_1}\alpha_{\chi_2}$, а символ $\left[\frac{\mu}{\alpha}\right]$ мультипликативен по самому своему определению, а также и по аргументу X :

$$(\chi, X_1X_2) = (\chi, X_1)(\chi, X_2), \quad (7)$$

причем в равенствах (6) и (7) символ, стоящий в левой части, определен, если определены оба символа, стоящие в правой части.

Вясним, как связаны символы (χ, X) в различных полях. Пусть K/k есть нормальное подполе шольцева расширения K_1/k , так что его группа Галуа G является факторгруппой группы G_1 поля K_1/k . Тогда всякая система множителей на G является в то же время системой множителей на G_1 , и, следовательно, любой элемент X группы $M(G)$ можно рассматривать как элемент X_1 группы $M(G_1)$. Точно так же любой характер χ порядка l группы G можно рассматривать как характер χ_1 группы G_1 . Мы утверждаем, что при этом

$$(\chi, X) = (\chi_1, X_1). \quad (8)$$

Действительно, в этом случае $\alpha_\chi \approx \alpha_{\chi_1}$. Ввиду условия 3), наложенного на число α ,

$$(\alpha_\chi) = N_{K/k}(\mathfrak{A}_\chi), \quad \mathfrak{A}_\chi \in K,$$

$$(\alpha_{\chi_1}) = N_{K_1/k}(\mathfrak{A}_{\chi_1}), \quad \mathfrak{A}_{\chi_1} \in K_1,$$

причем мы можем считать, что $\mathfrak{A}_\chi$ и $\mathfrak{A}_{\chi_1}$ выбраны так, что

$$\mathfrak{A}_\chi = N_{K_1/K}(\mathfrak{A}_{\chi_1}).$$

Ввиду определения символов (χ, X) и $\left[\frac{\mu}{\mathfrak{A}}\right]$, формулы (4) и известных свойств символа Лежандра, имеем:

$$(\chi_1, X_1) = \left(\frac{\mu}{\mathfrak{A}_{\chi_1}}\right)_{K_1} \left(\frac{\alpha_{\chi_1}}{\mathfrak{m}}\right)_k^{-1} = \left(\frac{\mu}{\mathfrak{A}_\chi}\right)_K \left(\frac{\alpha_\chi}{\mathfrak{m}}\right)^{-1} = (\chi, X).$$

5. Инварианты $(X)_h$. Для того, чтобы изложить конструкцию других инвариантов шольцева поля, определяющих, наряду с инвариантами (χ, X) , его погружаемость в шольцевы центральные расширения, нам понадобится следующая лемма.

Лемма 2. В каждом классе X l -инвариантных чисел шольцева поля K/k содержится l -гиперпримарное число.

Доказательство. Предположим только, что в поле K/k выполнено условие 1^0 , определяющее шольцево поле. Согласно этому условию, любой простой делитель l_i числа l в k полностью распадается в K и поэтому кольцо K_{l_i} , получающееся расширением основного поля k в поле K до его l_i -адического замыкания, есть прямая сумма полей k_{l_i} . В этой прямой сумме автоморфизмы K/k вызывают, как легко видеть, регулярную перестановку компонент. Если мы выделим одну из этих компонент, то любая другая будет определяться тем автоморфизмом σ , который переводит в нее эту выбранную компоненту. Ввиду этого

$$K_{l_i} = \sum k_{l_i}^\sigma,$$

и мы можем отождествить K_{l_i} с кольцом функций, заданных на группе Галуа G поля K/k со значениями в k_{l_i} , причем на функцию $\alpha(\sigma)$ автоморфизм τ действует по правилу

$$\alpha(\sigma)^\tau = \alpha(\sigma\tau).$$

Если l -инвариантному числу μ в кольце K_{l_i} соответствует функция $\mu_i(\sigma)$, то для нее мы будем иметь:

$$\mu_i(\sigma\tau) = \mu_i(\sigma)\gamma_i(\tau)^l \quad (9)$$

при некоторой функции $\gamma_i(\tau)$. Подставляя в (9) $\sigma = 1$, получим:

$$\mu_i(\tau) = \mu_i(1)\gamma_i(\tau)^l.$$

Пусть l^{E_i} — модули l -гиперпримарности, т.е. такие степени l_i , что из

$$\alpha \equiv 1(l_i^{E_i}), \quad \alpha \in k_{l_i},$$

следует $\alpha \approx 1$ в k_{l_i} . Мы можем найти такое число C в K и m в k , что если $C_i(\sigma)$ — функция из K_{l_i} , соответствующая C , то

$$\left. \begin{aligned} C_i(\sigma) &\equiv \gamma_i(\sigma)(l_i^{E_i}), \\ m &\equiv \mu_i(1)(l_i^{E_i}) \quad \text{для всех } l_i \mid l. \end{aligned} \right\} \quad (10)$$

Тогда l -инвариантное число $\mu m^{-1} C^{-1}$ будет лежать в том же классе X , что и μ , и будет l -гиперпримарным ввиду сравнений (10). Лемма доказана.

Заметим, что все l -гиперпримарные числа из одного и того же класса X получаются друг из друга умножением на числа вида mC^l , где m — l -гиперпримарное число.

Перейдем теперь к построению второй серии инвариантов. Пусть k_h есть максимальное расширение k , имеющее абелеву группу показателя l и содержащееся в $k(\zeta_h)$, где ζ_h есть первообразный корень степени l^h из 1. Из элементарных свойств абсолютно абелевых расширений вытекает, что k_h имеет следующее строение. Пусть k содержит корень степени l^r из 1 и не содержит корня степени l^{r+1} из 1. Если $h \leq r$, то $k_h = k$. Если $h > r$ и $l \neq 2$ или $l = 2$, но $r > 1$, то k_h получается присоединением к k корня степени l^{r+1} из единицы и, следовательно, $(k_h : k) = l$. Если $l = 2$ и $r = 1$, то $k_2 = k(\sqrt{-1})$ и $k_h = k(\sqrt{-1}, \sqrt{2})$ при $h > 2$.

Пусть X есть класс l -инвариантных чисел, μ — его l -гиперпримарный представитель и m — делитель μ в разложении (3). Обозначим через $(X)_h$ содержащий m класс смежности по подгруппе, соответствующей, согласно теории полей классов (см. [7]), полю k_h . Класс $(X)_h$ не зависит от выбора μ в X . Действительно, переход к другому представителю сводился бы к умножению m на

l -гиперпримарное число m , которое должно принадлежать к подгруппе, соответствующей k_h . Это следует из того, что поле, соответствующее группе l -гиперпримарных чисел, содержит максимальное абелево поле показателя l , в котором разветвляются только делители l . Так как в k_h это свойство выполняется, то соответствующая ему подгруппа должна содержать, согласно теории полей классов, группу l -гиперпримарных чисел.

Более подробно можно описать $(X)_h$ следующим образом. Обозначим через Λ_h группу рациональных чисел, сравнимых с 1 по модулю l^{r_1} , где $r_1 = r$, если $h \leq r$, $r_1 = r + 1$, если $h > r$ и $l \neq 2$ или $l = 2$, но $r > 1$, $r_1 = 2$, если $l = 2$, $r = 1$, $h = 2$, и $r_1 = 3$, если $l = 2$, $r = 1$, $h > 2$. Заметим, что во всех случаях

$$r_1 \leq \max(h, r). \quad (11)$$

Инвариант $(X)_h$ характеризуется как класс $\mathfrak{N}(m)\Lambda_h$, где $\mathfrak{N}(m)$ означает абсолютную норму m .

Так как поле k содержит поле корня степени l^r из 1, то всегда

$$\mathfrak{N}(m) \equiv 1(l^r).$$

Поэтому $(X)_h$ может принимать только конечное число значений, а именно, при $l \neq 2$ — l значений, а при $l = 2$ — или 2 или 4 значения. Точно так же очевидно, что аналогично (6) и (7) имеют место соотношения:

$$(X_1 X_2)_h = (X_1)_h (X_2)_h, \quad (12)$$

$$(X)_h = (X_1)_h \quad (13)$$

с теми обозначениями, которые были приняты при выводе равенств (7) и (8).

§2. Условия погружаемости для шольцевых расширений

В этом параграфе мы выведем условия, при которых шольцево поле K/k можно погрузить в шольцево поле с заданной группой Галуа, являющейся простым центральным расширением группы K/k . Так как в условие 4⁰, определяющее шольцево поле, входит показатель h , то будем предполагать, что в K/k оно выполнено при некотором h , и требуется погрузить K/k в поле, в котором оно было бы выполнено при том же значении h . Условия при этом будут зависеть от h .

Для некоторого упрощения рассуждений мы предположим, что поле K пересекается с полем $\mathfrak{K}$, являющимся максимальным неразветвленным расширением k с абелевой группой Галуа показателя l , по основному полю k . При этом мы покажем, что K/k можно погрузить в поле, для которого это свойство тоже имеет место.

1. Случай основного поля, содержащего l -й корень из 1. Мы предположим, что основное поле k содержит корень степени l из 1. Тогда для любого шольцева расширения K/k с l -группой Галуа определены инварианты (χ, X) и $(X)_h$, введенные в предшествующем параграфе.

Теорема 1. Для того, чтобы шольцево поле K/k можно было погрузить в шольцево поле с группой Галуа, являющейся простым центральным расширением группы Галуа K/k , соответствующим характеру X , необходимо и достаточно, чтобы инварианты (χ, X) для всех характеров χ и $(X)_h$ поля K были равны 1.

Заметим, что равенство единице этих инвариантов равносильно выполнению условий

$$\left[\frac{\mu}{\alpha_\chi} \right] = \left(\frac{\alpha_\chi}{m} \right), \quad (14)$$

$$\mathfrak{N}(m) \in \Lambda_h \quad (15)$$

для l -инвариантных и l -гиперпримарных чисел μ из класса X и для всех характеров χ . Условие $(\alpha_\chi, m) = 1$ здесь выполнено само собой, так как α_m не содержит делителей дискриминанта K/k .

Докажем необходимость условий (14) и (15). Нам известно, что их достаточно проверить только для одного представителя из класса X l -инвариантных чисел. Но, с другой стороны, в силу условий теоремы, в этом классе существует хотя бы одно число μ , для которого $K(\sqrt[l]{\mu})$ является шольцевым полем. Пусть $\mathfrak{P}$ — критический простой дивизор K/k . Если $(\mathfrak{P}, \mathfrak{D}(X)) = 1$, то из того, что $\mathfrak{P}$ имеет в $K(\sqrt[l]{\mu})$ порядок 1, следует, что

$$\left[\frac{\mu}{p} \right] = \left(\frac{\mu}{\mathfrak{P}} \right) = 1.$$

Так как α_χ состоит из критических простых дивизоров и l -взаимно просто с $\mathfrak{D}(X)$, то

$$\left[\frac{\mu}{\alpha_\chi} \right] = 1. \quad (16)$$

С другой стороны, всякий простой дивизор q/m должен полностью распадаться в K , так как иначе он был бы критическим простым дивизором $K(\sqrt[l]{\mu})$ не первого порядка. Из этого следует, что q полностью распадается в $k(\sqrt[l]{\alpha_\chi})$, т.е.

$$\left(\frac{\alpha_\chi}{q} \right) = 1 \quad \text{для } q/m, \quad \text{т.е.} \quad \left(\frac{\alpha_\chi}{m} \right) = 1. \quad (17)$$

Равенства (16) и (17) показывают, что условия (14) выполняются.

Что касается условий (15), то они тоже выполняются, так как для любого простого дивизора q/m

$$\mathfrak{N}(q) \equiv 1(l^h),$$

т.е.

$$\mathfrak{N}(m) \equiv 1(l^h)$$

и всегда

$$\mathfrak{N}(m) \equiv 1(l^r);$$

это и означает, ввиду (11), что $\mathfrak{N}(m) \in \Lambda_h$.

Докажем теперь достаточность условий (14) и (15). Так как поле K/k — шольцево, то в нем можно найти такое l -инвариантное число μ , что поле $K(\sqrt[l]{\mu})/k$ будет иметь группу Галуа, являющуюся центральным простым расширением группы Галуа K/k , соответствующим характеру X . Не меняя группы Галуа $K(\sqrt[l]{\mu})/k$, мы можем менять μ произвольным образом в его классе X .

Нам нужно, следовательно, доказать, что при выполнении условий (14) и (15) в классе X l -инвариантных чисел можно найти такое число μ , что в поле $K(\sqrt[l]{\mu})$ будут выполняться все четыре свойства, определяющие шольцево поле.

Относительно первого свойства это уже доказано в лемме 2, и мы поэтому будем дальше выбирать в X l -инвариантное l -гиперпримарное число μ_0 .

Выполнения второго условия можно добиться аналогично, но еще проще. Это условие содержательно только для $l = 2$. Пусть $p_{\infty, i}$ — вещественные бесконечно удаленные простые дивизоры k . $K_{p_{\infty, i}}$ является, по условию, прямой суммой полей вещественных чисел $k_{p_{\infty, i}}$. Из рассуждений, аналогичных использованным при доказательстве леммы 2, следует, что числу μ_0 в каждом $K_{p_{\infty, i}}$ соответствует такая вещественная функция $\mu_{0, i}(\sigma)$, что

$$\mu_{0, i}(\sigma\tau) = \mu_{0, i}(\sigma)\beta_i(\tau)^2.$$

Отсюда следует, что все $\mu_{0, i}(\sigma)$ имеют один и тот же знак, совпадающий со знаком $\mu_{0, i}(1)$. Выберем в k такое l -гиперпримарное число m_0 , чтобы знак его компоненты в каждом из $k_{p_{\infty, i}}$ совпадал со знаком соответствующего $\mu_{0, i}(1)$. Тогда $\mu_0 m_0$ будет снова l -гиперпримарным и уже тотально-положительным. Это новое число мы обозначим через μ' . Для него уже выполнены свойства 1⁰ и 2⁰.

Пусть p_i — все критические простые дивизоры K/k , взаимно простые с дивизором $\mathfrak{D}(X)$. Найдем такое l -гиперпримарное тотально-положительное число $m' \in k$, что

$$\left(\frac{m'}{p_i}\right) = \left[\frac{\mu'}{p_i}\right]^{-1}, \quad \text{т.е.} \quad \left(\frac{\mu'm'}{\mathfrak{P}_i}\right) = 1 \quad \text{для всех } p_i.$$

Это условие сводится к конечному числу сравнений по модулям p_i , взаимно простым между собою и с l , а поэтому такое число m' существует. Число $\mu'm'$ обозначим через μ'' и по-прежнему положим

$$(\mu'') = (\mathfrak{C}'')^l \mathfrak{D} m''.$$

Рассмотрим модуль $\mathfrak{F}$, являющийся произведением всех критических простых дивизоров p_i , взаимно простых с $\mathfrak{D}(X)$, всех существенных бесконечно удаленных дивизоров $p_{\infty, i}$ и всех $l_i^{E_i}$ (определение E_i см. в доказательстве леммы 2). Через $S_{\mathfrak{F}}$ обозначим группу l -степеней всех классов $\bmod \mathfrak{F}$, через L/k — поле классов к группе $S_{\mathfrak{F}}$ и через Z_h — поле, получающееся присоединением к k корня степени l^h из 1. Обозначим через σ автоморфизм L/k , являющийся автоморфизмом Артина дивизора m'' . Докажем, что в композите KZ_hL существует автоморфизм $\bar{\sigma}$, индуцирующий в K и Z_h единичный автоморфизм, а в L — автоморфизм σ .

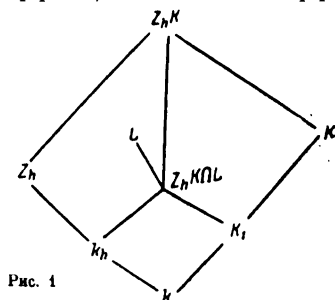


Рис. 1

Действительно, $KZ_h \cap L$ есть поле $K_1 k_h$, где k_h есть поле, участвовавшее в определении инварианта $(X)_h$, а K_1 получается присоединением к k всех $\sqrt[l]{\alpha_X}$, для которых α_X l -взаимно просто с $\mathfrak{D}(X)$ (см. рис. 1). Докажем, что σ индуцирует в $KZ_h \cap L$ единичный автоморфизм. Согласно сказанному выше, σ индуцирует в $KZ_h \cap L$ автоморфизм, являющийся автоморфизмом Артина дивизора m'' в $K_1 k_h$.

В k_h m'' принадлежит к единичному автоморфизму, так как по условию $(X)_h = 1$.

Для всех p_i , взаимно простых с $\mathfrak{D}(X)$, по построению μ'' ,

$$\left[\frac{\mu''}{p_i} \right] = 1, \quad \text{т.е.} \quad \left[\frac{\mu''}{\alpha_X} \right] = 1$$

для α_X , l -взаимно простых с $\mathfrak{D}(X)$. Так как, по условию, $(\chi, X) = 1$, то отсюда следует, что для таких α_X

$$\left(\frac{\alpha_X}{m''} \right) = 1.$$

Это и значит, что m'' принадлежит в K_1 к единичному автоморфизму. Таким образом, m'' принадлежит в K_1 и в k_h , а следовательно, и в $K_1 k_h$ к единичному автоморфизму. Поскольку автоморфизм σ поля L индуцирует в $KZ_h \cap L$ единичный автоморфизм, он может быть продолжен до $KZ_h L$ так, чтобы индуцировать в KZ_h единичный. Это продолжение мы и обозначим через $\bar{\sigma}$.

Согласно закону плотностей Чеботарева (см. [4], стр.148), в k существует простой дивизор q , принадлежащий в $Z_h L K$ к автоморфизму $\bar{\sigma}$. Так как q принадлежит в L к тому же автоморфизму, что и m'' , то q лежит в том же классе по $S_{\mathfrak{F}}$, что и m'' , следовательно, $q = m''(m)i^l$, где m l -гиперпримарно, totally-положительно и сравнимо с 1 по модулю всех p_i . Докажем, что число $\mu = \mu'' m$ удовлетворяет всем четырем нужным нам условиям. Оно l -гиперпримарно и totally-положительно, так как такими были μ'' и m . В поле $\Omega = K(\sqrt[l]{\mu})$ критические простые дивизоры K будут иметь порядок 1, так как у делителей $\mathfrak{D}(X)$ порядок не изменится и только показатель ветвления увеличится в l раз, а для p_i , взаимно простых с $\mathfrak{D}(X)$, это следует из того, что

$$\left(\frac{\mu}{\mathfrak{P}_i} \right) = \left(\frac{\mu'' m}{\mathfrak{P}_i} \right) = \left[\frac{\mu''}{p_i} \right] \left(\frac{m}{p_i} \right) = 1.$$

Расширение Ω/K будет иметь, ввиду того, что

$$(\mu) = (\mu'' m) = (\mathfrak{C}'' i^{-1})^l \mathfrak{D} q,$$

в качестве критических простых дивизоров делители $\mathfrak{D}$, про которые уже доказано, что их порядок 1, и делители q , которые имеют порядок 1, так как, по построению, q принадлежит в K/k к единичному автоморфизму. Наконец, и четвертое условие выполнено. Для критических простых дивизоров K/k это было предположено,

а для q следует из того, что оно, по построению, принадлежит к единичному автоморфизму в Z_h , т.е.

$$\mathfrak{N}(q) \equiv 1(l^h).$$

Теорема доказана.

В случае, когда характер $X \neq 1$, максимальное подполе поля K , имеющее абелеву группу показателя l , не изменится при расширении K до $K(\sqrt[l]{\mu})$, так что и $K(\sqrt[l]{\mu})$ будет пересекаться с неразветвленным полем $\mathfrak{K}$ по k . Если же $X = 1$, то μ l -равно числу α из k . По построению, оно делится на простой дивизор q , взаимно простой со всеми α_χ . Максимальное подполе поля $K(\sqrt[l]{\mu})$, с абелевой группой показателя l получается из такого же подполя поля K присоединением $\sqrt[l]{\alpha}$ и, ввиду сказанного выше, также пересекается с $\mathfrak{K}$ по k .

Заметим, что из доказательства теоремы следует, что мы можем выбрать μ в его классе X так, чтобы дивизор m из разложения (3) был взаимно прост с любым наперед заданным дивизором.

Из теоремы очевидным образом следует, что для того, чтобы шольцево поле K/k можно было погрузить в шольцевы расширения, группы Галуа которых являются простыми центральными расширениями группы Галуа K/k , соответствующими классам $X_1, \dots, X_r$, необходимо и достаточно обращение в 1 инвариантов $(\chi, X_1), \dots, (\chi, X_r)$ для всех χ и всех инвариантов $(X_1)_h, \dots, (X_r)_h$.

Следствие. Обращение в 1 всех инвариантов $(X)_h$ и (χ, X) достаточно также для погружаемости шольцева расширения K/k в шольцево расширение, группа Галуа которого является любым центральным (а не только простым) расширением группы Галуа.

Ввиду того, что поле K/k шольцево, в нем существуют такие l -инвариантные числа $\mu_1, \dots, \mu_m$, что поле $\Omega = K(\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_m})$ имеет нужную нам группу Галуа. Мы можем произвольным образом менять числа $\mu_1, \dots, \mu_m$ в их классах X , не меняя при этом группы Галуа Ω/k . Докажем, что $\mu_1, \dots, \mu_m$ можно выбрать в их классах так, чтобы Ω было шольцевым. Пусть среди $\mu_1, \dots, \mu_m$ числа $\mu_1, \dots, \mu_r$ мультипликативно независимы по модулю подгруппы чисел, l -равных инвариантным, а $\mu_{r+1}, \dots, \mu_m$ l -равны некоторым произведениям $\mu_1, \dots, \mu_r$ и инвариантных чисел $\alpha_{r+1}, \dots, \alpha_m$.

Будем присоединять к K по очереди $\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_r}$.

Число образующих групп Галуа получаемых при этом полей $K(\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_i})$ будет тем же самым числом d , что и у группы Галуа поля K/k . В самом деле, если бы число образующих увеличилось, то увеличилась бы факторгруппа по подгруппе Фраттини,

т.е. в поле $K(\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_i})$ содержалось бы число $\sqrt[l]{\alpha}$, $\alpha \in k$, не содержащееся в K . Мы имели бы тогда:

$$\alpha \approx \mu_1^{x_1} \dots \mu_i^{x_i} \quad \text{в } K \quad \text{и не все } x_i \equiv 0(l),$$

что противоречит выбору $\mu_1, \dots, \mu_r$. Таким образом, при последовательном присоединении $\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_r}$, характеры χ будут оставаться такими же.

На каждом шагу нам надо будет присоединить $\sqrt[l]{\mu_i}$, соответствующее классу X_i , причем μ_i лежит не только в $K(\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_{i-1}})$, но и в K . Ввиду того, что характеры χ остаются теми же, мы получаем из (8) и (13), что

$$(\chi, X_i) = 1, \quad (X_i)_h = 1,$$

а это и значит, что, изменив μ_i на множитель из k , мы сделаем поле $K(\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_i})$ шольцевым.

Теперь нам осталось к шольцеву полю $K(\sqrt[l]{\mu_1}, \dots, \sqrt[l]{\mu_r})$ присоединить, также по очереди, числа $\sqrt[l]{\alpha_{r+1}}, \dots, \sqrt[l]{\alpha_m}$. Так как здесь присоединения будут соответствовать единичному классу, то все инварианты равны 1 и, согласно теореме 1, мы можем $\alpha_{r+1}, \dots, \alpha_m$ выбирать так, чтобы все поле получилось шольцевым.

2. Случай основного поля, не содержащего l -й корень из

1. Предположим, что основное поле k не содержит корня степени l из 1. Пусть K/k — шольцево поле. Присоединим к k и K корень ζ степени l из 1 и обозначим $k(\zeta)$ через $\bar{k}$, а $K(\zeta)$ — через $\bar{K}$. Степень $(\bar{k} : k)$ обозначим через m . Очевидно, что $m \mid l - 1$ и поэтому $(m, l) = 1$.

Заметим, что условия шольцевости для полей K/k и $\bar{K}/\bar{k}$ эквивалентны. Проверим это для всех четырех условий.

Условие 2^0 при этом существенно только при $l = 2$, но в этом случае $\bar{k} = k$, $\bar{K} = K$, так что наше утверждение очевидно.

Для условий 1^0 и 3^0 утверждение доказывается одним и тем же рассуждением. Пусть p — простой дивизор k и $\bar{p}$ — его простой делитель в $\bar{k}$. Докажем, что p тогда и только тогда полностью распадается (соответственно имеет порядок 1) в K , когда p полностью распадается (соответственно имеет порядок 1) в $\bar{K}$. Кольцо K_p является прямой суммой полей $K_{\bar{p}}$, являющихся расширениями k_p степени n_p (порядка r_p), а $\bar{k}_p$ — суммой полей $\bar{k}_{\bar{p}}$ степени m_p (порядка s_p) над k_p . При этом $n_p(r_p)$ есть степень l , а $m_p(s_p)$ делит m , поэтому взаимно просто с l . Кольцо $\bar{K}_p$ является прямой суммой полей $K_{\bar{p}}\bar{k}_{\bar{p}}$, имеющих, ввиду того, что $(n_p, m_p) = 1$, степень

$n_p m_p$ (порядок $r_p s_p$) над k_p и $n_p(r_p)$ над $\bar{k}_p$. Таким образом, $\bar{K}_p$ есть сумма полей степени n_p (порядка r_p) над $\bar{k}_p$. Для того, чтобы p полностью распадался (имел порядок 1) в K , необходимо и достаточно, чтобы $n_p(r_p)$ равнялось 1. Для того же, чтобы $\bar{p}$ полностью распадался (имел порядок 1) в $\bar{K}$, необходимо и достаточно, ввиду доказанного, чтобы также $n_p(s_p)$ равнялось 1.

Нам остается доказать эквивалентность условия 4⁰ для полей K/k и $\bar{K}/\bar{k}$. Если p — делитель дискриминанта K/k в k , $\bar{p}$ — его простой делитель в $\bar{k}$, то $\mathfrak{N}(\bar{p}) = \mathfrak{N}(p)^f$, где f — относительный порядок $\bar{p}$ в $\bar{k}/k$, взаимно простой с l . Отсюда очевидным образом следует наше утверждение.

Таким образом, если K/k — шольцево, то в поле $\bar{K}/\bar{k}$ определены введенные в предшествующем параграфе инварианты (χ, X) и $(X)_h$.

Докажем также, что условие, согласно которому K пересекается по k с максимальным неразветвленным расширением $\mathfrak{K}$ поля k , имеющем абелеву группу показателя l , выполняется тогда и только тогда, когда оно выполняется для $\bar{K}/\bar{k}$. Обозначим соответствующее расширение поля $\bar{k}$ через $\bar{\mathfrak{K}}$ и докажем, что

$$\bar{K} \cap \bar{\mathfrak{K}} = (K \cap \mathfrak{K})\bar{k}.$$

Очевидно, что правая часть содержится в левой и нужно только доказать, что и левая содержится в правой. Для этого заметим, что ввиду того, что $\bar{K} = K\bar{k}$, $K \cap \bar{k} = k$, группа Галуа $\bar{K}/k$ есть прямое произведение группы Галуа K/k , имеющей порядок l^α , и группы Галуа $\bar{k}/k$ порядка m , взаимно простого с l . Отсюда следует, что $\bar{K} \cap \bar{\mathfrak{K}}$ есть композит $\bar{k}$ и подполя $\mathfrak{K}_1$ поля K , причем $\mathfrak{K}_1 \subset \mathfrak{K}$. Ввиду того, что степени $(\mathfrak{K}_1 : k)$ и $(\bar{k} : k)$ взаимно просты, $\mathfrak{K}_1$ должно быть неразветвленным над k . Так как, кроме того, группа Галуа $\mathfrak{K}_1/k$ изоморфна группе Галуа $\mathfrak{K}_1\bar{k}/\bar{k} \subset \bar{\mathfrak{K}}/\bar{k}$, то она абелева и показателя l . Следовательно, $\mathfrak{K}_1 \subseteq \mathfrak{K}$, что и доказывает интересное нас утверждение.

Теорема 2. Для того, чтобы шольцево поле K/k можно было погрузить в шольцево поле с группой Галуа, являющейся простым центральным расширением группы Галуа K/k , соответствующим характеру X , необходимо и достаточно, чтобы инварианты (χ, X) для всех характеров χ и $(X)_h$ поля $\bar{K}/\bar{k}$ были равны 1.

Доказательство в части необходимости прямо сводится к теореме 1. Предположим, что Ω/k является центральным простым шольцевым расширением K/k с нужной нам группой Галуа. Поле

$\bar{\Omega} = \Omega(\zeta)$ является также шольцевым расширением поля $\bar{K}/\bar{k}$, причем с той же группой Галуа. Из теоремы 1 следует тогда, что все инварианты поля $\bar{K}/\bar{k}$ равны 1.

В части достаточности доказательство также сводится к соответствующему утверждению теоремы 1, но более сложным путем. Мы будем пользоваться следующими обозначениями. Через t обозначим образующий автоморфизм поля $\bar{k}/k$, так что $t^m = 1$. Через g обозначим такое число, для которого

$$\zeta^t = \zeta^g, \quad g^m \neq 1 (l^2).$$

Ввиду того, что $\bar{k} \neq k$, мы имеем также

$$g \neq 1 (l).$$

Через s обозначим $t^{m-1} + t^{m-2}g + \dots + tg^{m-2} + g^{m-1}$. Используем следующие соотношения, имеющие место как для чисел, так и для дивизоров поля $\bar{k}$:

из того, что

$$\alpha^s \approx 1, \quad (18)$$

следует, что $\alpha \approx \beta^{t-g}$ при некотором β , и, наоборот, любое такое α удовлетворяет (18);

из того, что

$$\alpha^{t-g} \approx 1, \quad (19)$$

следует, что $\alpha \approx \beta^s$ при некотором β , и, наоборот, любое такое α удовлетворяет (19).

Все соображения, необходимые для доказательства (18) и (19), содержатся у Рейхардта [8].

Обозначим $1 - g^m$ через lx , где $(l, x) = 1$, и определим y из сравнения $xy \equiv 1 (l)$. То, что числа вида β^{t-g} удовлетворяют условию (18), а β^s — условию (19), получается непосредственной подстановкой, если воспользоваться тем, что

$$s(t - g) = t^m - g^m = 1 - g^m \equiv 0 (l).$$

Пусть $\alpha^s = \gamma^l$. Возводя обе части в степень $t - g$, получим

$$\alpha^{lx} = \gamma^{l(t-g)}, \quad \text{т.е.} \quad \alpha^x = \zeta^r \gamma^{t-g}.$$

Возведем обе части этого равенства в степень y . Мы получим:

$$\alpha \approx \zeta^{ry} \gamma^{y(t-g)}.$$

Нам надо доказать, что множитель $\zeta^{ry} \approx 1$. Подставим для этого полученное выражение для α в (18). Так как $\zeta^t = \zeta^g$, то $\zeta^s = \zeta^{mg^{-1}}$. Таким образом,

$$1 \approx \alpha^s \approx \zeta^{rymg^{-1}} \gamma^{y(t-g)s} \approx \zeta^{rymg^{-1}},$$

а так как $mg^{-1} \not\equiv 0(l)$, то и $\zeta^{ry} \approx 1$.

Пусть $\alpha^{t-g} = \gamma^l$. Возводя обе части в степень s , получим, как и раньше,

$$\alpha^{lx} = \gamma^{ls}, \quad \alpha^x = \zeta^r \gamma^{t-g}, \quad \alpha \approx \zeta^{ry} \gamma^{y(t-g)}.$$

Ввиду того, что $\zeta^s = \zeta^{mg^{-1}}$, мы имеем $\zeta^{ry} = \zeta^{rym^{-1}gs}$ и

$$\alpha \approx (\zeta^{rym^{-1}g} \gamma^y)^s.$$

Наконец, мы будем пользоваться также тем, что условие (19) является необходимым для того, чтобы поле $\bar{k}(\sqrt[l]{\alpha})$ было композитом поля $\bar{k}$ и циклического поля степени l над k . Доказательство получается непосредственной проверкой.

Переходя к доказательству, мы построим прежде всего, пользуясь теоремой 1, поле $\bar{K}(\sqrt[l]{\mu})$, являющееся шольцевым расширением $\bar{K}/\bar{k}$ с нужной нам группой Галуа. Далее, мы воспользуемся результатом, полученным Рейхардтом [8]. Он показал, что в $\bar{k}$ существует такое число $\bar{m}$, что l -инвариантное число $\mu_0 = \bar{\mu} \bar{m}$ удовлетворяет соотношению

$$\mu_0^{t-g} \approx 1, \quad (20)$$

а поле $\bar{K}(\sqrt[l]{\mu_0})$ есть прямой композит $\bar{k}$ и некоторого поля Ω , нормального над k и имеющего над ним ту же группу Галуа, что и $\bar{K}(\sqrt[l]{\mu})/\bar{k}$. Наша задача была бы решена, если бы мы могли показать, что Ω является шольцевым расширением k . Это эквивалентно тому, что $\bar{K}(\sqrt[l]{\mu_0})$ является шольцевым расширением $\bar{k}$. Не нарушая свойства (20) числа μ_0 , а также описанных выше свойств поля $\bar{K}(\sqrt[l]{\mu_0})$, мы можем заменить μ_0 числом вида $\mu_0 a^s$, где a — любое число из $\bar{k}$. Теорема будет доказана, если мы покажем, что таким путем мы сможем получить шольцево поле $\bar{K}(\sqrt[l]{\mu_0 a^s})/\bar{k}$.

Начнем с условия 1^0 , определяющего шольцево поле. Пусть l —любой простой делитель l в k . Так как поле $\bar{K}(\sqrt[l]{\mu})$ шольцево, то

$$\bar{\mu} \approx 1 \quad \text{в} \quad \bar{K}_l.$$

Для числа $\mu_0 = \bar{\mu} \bar{m}$ мы получаем отсюда

$$\mu_0 \approx \bar{m} \quad \text{в} \quad \bar{K}_l,$$

а ввиду (20),

$$\overline{m}^{t-g} \approx 1 \quad \text{в} \quad \overline{K}_l.$$

Кольцо K_l разлагается так же, как и в доказательстве леммы 2, в прямую сумму колец:

$$\overline{K}_l = \sum \overline{k}_l^\sigma,$$

где σ пробегает все автоморфизмы K/k . Все компоненты числа $\overline{m}^{t-g}$ в этом разложении равны ему самому. Таким образом,

$$\overline{m}^{t-g} \approx 1 \quad \text{в} \quad \overline{k}_l, \quad \text{т.е.} \quad \overline{m} \approx b_l^s \quad \text{в} \quad \overline{k}_l.$$

Выбирая такое число a_1 из $\overline{k}$, что $a_1 b_l \approx 1$ в k_l , мы получаем l -ги-перпримарное число $\mu_0 a_1^s$. Положим

$$\mu_0 a_1^s = \mu_1 = \overline{\mu} \overline{m}_1. \quad (21)$$

Условие 2^0 в нашем случае всегда выполнено, так как $l \neq 2$. Прежде, чем перейти к рассмотрению условия 3^0 , сделаем следующие замечания. Из разложения

$$(\mu_1) = \mathfrak{C}^l \overline{\mathfrak{D}} \overline{m}_1$$

и из (20) и (21) следует, что

$$\overline{m}_1^{t-g} \approx 1, \quad \text{т.е.} \quad \overline{m}_1 \approx \overline{n}_1^s, \quad \overline{n}_1 \in \overline{k}.$$

Пусть $\overline{p}$ — простой критический дивизор в $\overline{K}/\overline{k}$, взаимно простой с $\mathfrak{D}(X)$. Из того, что $\overline{K}$, по построению, нормально над k , следует, что $\overline{p}^t$ будет критическим в $\overline{K}/\overline{k}$ и взаимно простым с $\mathfrak{D}(X)$. Из (20), (21) и из того, что $\overline{K}(\sqrt[l]{\mu})$ шольцево, следует, что

$$\left(\frac{\overline{m}_1}{\mathfrak{p}^t} \right)_{\overline{k}} = \left(\frac{\overline{m}_1}{\overline{\mathfrak{p}}^t} \right)_{\overline{K}} = \left(\frac{\mu}{\overline{\mathfrak{p}}^t} \right) = \left(\frac{\mu_1^{t^{-1}}}{\overline{\mathfrak{p}}} \right)^g = \left(\frac{\mu_1}{\overline{\mathfrak{p}}} \right) = \left(\frac{\overline{m}_1}{\overline{p}} \right), \quad (22)$$

где $\overline{\mathfrak{p}}$ — простой делитель $\overline{p}$ в $\overline{K}$. Ввиду (22), мы будем обозначать $\left(\frac{\overline{m}_1}{\overline{p}} \right)$ через $\zeta(\mathfrak{p})$, где $\mathfrak{p} = N_{\overline{k}/k}(\overline{p})$.

Из того, что $\overline{K}$ нормально над k , следует, что

$$\overline{\alpha}_x^{t-g} \approx 1, \quad (23)$$

где χ — любой характер порядка l группы Галуа $\overline{K}/k$. (Определение числа $\overline{\alpha_\chi}$ см. в §1, п.4). Отсюда, аналогично выводу (22), следует, что для любого простого дивизора $\overline{q} \in \overline{k}$

$$\left(\frac{\overline{\alpha_\chi}}{\overline{q}^t}\right) = \left(\frac{\overline{\alpha_\chi}}{\overline{q}}\right).$$

Кроме того, из (23) следует, что

$$(\overline{\alpha_\chi}) \approx \mathfrak{A}_\chi^s. \quad (24)$$

Заметим, наконец, что если $\overline{a}$ — любое число из k , то

$$\begin{aligned} \left(\frac{\overline{a}^s}{\overline{p}}\right) &= \prod_{r=0}^{m-1} \left(\frac{\overline{a}^{t^r} g^{m-1-r}}{\overline{p}}\right) = \prod_{r=0}^{m-1} \left(\frac{\overline{a}}{\overline{p}^{t^{-r}}}\right)^{g^{m-1}} \\ &= \left(\frac{\overline{a}}{N_{\overline{k}/k}(\overline{p})}\right)^{g^{m-1}} = \left(\frac{\overline{a}}{\overline{p}}\right)^{g^{-1}}. \end{aligned} \quad (25)$$

Теперь мы можем перейти к рассмотрению условия 3^0 , определяющего шольцево поле. Определим числа $\overline{c_1}$ и $\overline{c_2}$ из $\overline{k}$ так, чтобы имели место соотношения:

$$\left(\frac{\overline{c_1}}{\overline{\alpha_\chi}}\right) = \left(\frac{\overline{\alpha_\chi}}{\overline{n_1}}\right), \quad \left(\frac{\overline{c_2}}{\overline{p_i}}\right)^{g^{-1}} = \zeta(\overline{p_i})^{-1}, \quad (26)$$

где χ пробегает все характеры порядка l группы Галуа $\overline{K}/\overline{k}$, для которых $\overline{\alpha_\chi}$ l -взаимно просто с $\mathfrak{D}(X)$, а $\overline{p_i}$ — все критические простые дивизоры $\overline{K}/\overline{k}$, взаимно простые с $\mathfrak{D}(X)$.

Существование числа $\overline{c_2}$ очевидно, так как это число должно лишь удовлетворять некоторым сравнениям по взаимно простым модулям $\overline{p_i}$, не являющимся l -ми степенями.

Для того, чтобы доказать существование числа $\overline{c_1}$, удовлетворяющего условиям (26), заметим, что эти условия мультипликативны относительно $\overline{\alpha_\chi}$. Выберем из чисел $\overline{\alpha_\chi}$ такие $\overline{\alpha_{\chi_1}}, \dots, \overline{\alpha_{\chi_d}}$, которые мультипликативно независимы по модулю l -х степеней, и всякое $\overline{\alpha_\chi}$ l -равно их произведению. Нам достаточно найти $\overline{c_1}$, при котором (26) выполнялось бы для $\overline{\alpha_{\chi_1}}, \dots, \overline{\alpha_{\chi_d}}$. Заметим, что и дивизоры $(\overline{\alpha_{\chi_1}}), \dots, (\overline{\alpha_{\chi_d}})$ мультипликативно независимы по модулю l -х степеней в группе дивизоров. Действительно, если бы некоторое их произведение было l -й степенью, то это значило бы,

что некоторое $\overline{\alpha}_\chi$ сингулярно и гиперпримарно, т.е. $\overline{K}$ пересекается с неразветвленным полем $\overline{\mathcal{K}}$ по крайней мере по $\overline{k} (\sqrt[l]{\overline{\alpha}_\chi})$ в противоречии со сделанным предложением. Таким образом, дивизоры $(\overline{\alpha}_{\chi_1}), \dots, (\overline{\alpha}_{\chi_d})$ мультипликативно независимы по модулю l -х степеней, и мы можем найти число $\overline{c}_1$, имеющее по ним наперед заданные значения символа Лежандра.

Ввиду (24), число $\overline{c}_1$ определяется значениями символов

$$\left(\frac{\overline{c}_1}{\overline{p}_i^s} \right).$$

Так как

$$\overline{p}_i = \overline{p}_i^{1+t+\dots+t^{m-1}},$$

то все дивизоры $\overline{p}_i$ и $\overline{p}_i^s$ мультипликативно независимы по модулю l -х степеней. Кроме того, все они взаимно просты с l . Поэтому существует l -гиперпримарное число $\overline{c}_0$, для которого выполнены соотношения, аналогичные (26):

$$\left(\frac{\overline{c}_0}{\overline{\alpha}_\chi} \right) = \left(\frac{\overline{\alpha}_\chi}{\overline{n}_1} \right)^{-1}, \quad \left(\frac{\overline{c}_0}{\overline{p}_i} \right)^{g^{-1}} = \zeta(\overline{p}_i)^{-1}. \quad (27)$$

Обозначим через $\mathfrak{F}$ произведение всех $\overline{p}_i$ и модуля l -гиперпримарности, через $\overline{S}_{\mathfrak{F}}$ — группу l -х степеней классов дивизоров $\bmod \mathfrak{F}$, а через $\overline{L}$ — поле классов к группе $\overline{S}_{\mathfrak{F}}$ над $\overline{k}$. Пусть автоморфизм Артина дивизора $\overline{n}\overline{c}_0$ в $\overline{L}$ будет σ_1 . Поле $\overline{K} \cap \overline{L}$ получается из $\overline{k}$ присоединением $\sqrt[l]{\overline{\alpha}_\chi}$ для всех $\overline{\alpha}_\chi$, l -взаимно простых с $\mathfrak{D}(X)$. Ввиду (27),

$$\left(\frac{\overline{\alpha}_\chi}{\overline{n}_1 \overline{c}_0} \right) = \left(\frac{\overline{\alpha}_\chi}{\overline{n}_1} \right) \left(\frac{\overline{\alpha}_\chi}{\overline{c}_0} \right) = \left(\frac{\overline{\alpha}_\chi}{\overline{n}_1} \right) \left(\frac{\overline{c}_0}{\overline{\alpha}_\chi} \right) = 1,$$

так что σ_1 индуцирует в $\overline{K} \cap \overline{L}$ единичный автоморфизм. Из этого следует, что в $\overline{K} \overline{L}$ существует автоморфизм σ , индуцирующий в $\overline{K}$ единичный автоморфизм, а в $\overline{L}$ — автоморфизм σ_1 . Согласно закону плотностей Чеботарева, в $\overline{k}$ существует простой дивизор $\overline{q}_1$, принадлежащий к σ в $\overline{K} \overline{L}$. Так как $\overline{q}_1$ принадлежит в $\overline{L}$ к тому же автоморфизму, что и $\overline{n}_1 \overline{c}_0$, то $\overline{q}_1$ лежит в том же классе по $\overline{S}_{\mathfrak{F}}$, что и $\overline{n}_1 \overline{c}_0$, т.е. $\overline{q}_1 = \overline{n}_1 \overline{c}_0 (\overline{c})^{i^l}$, где $\overline{c}$ l -гиперпримарно и сравнимо с 1 по модулю всех $\overline{p}_i$. Докажем, что для числа $\mu_2 = \mu_1 (\overline{c} \overline{c}_0)$ выполнены условия 1^0 , 2^0 и 3^0 .

Условие 1^0 не нарушилось, так как $\overline{c_0} \overline{c}$, по построению, гиперпримарно. Условие 2^0 в нашем случае всегда выполнено автоматически. В связи с условием 3^0 заметим, что

$$(\mu_2) = \mathfrak{C}_2^t \overline{\mathfrak{D} q_1^s}.$$

Дивизор $\overline{q_1}$ имеет в $\overline{K}$ порядок 1, так как он принадлежит, по построению, к единичному автоморфизму в $\overline{K}$. Наконец, дивизоры $\overline{p_i}$, взаимно простые с $\mathfrak{D}(X)$, имеют порядок 1 в $\overline{K}(\sqrt[\mu]{\mu_2})$, так как, ввиду (21), (25) и (27),

$$\left(\frac{\mu_2}{\mathfrak{p}_i}\right) = \left(\frac{\mu_1}{\mathfrak{p}_i}\right) \left(\frac{(\overline{c_0} \overline{c})}{\mathfrak{p}_i}\right) = \left(\frac{\overline{m_1}}{\mathfrak{p}_i}\right) \left(\frac{\overline{c_0}^s}{\mathfrak{p}_i}\right) \left(\frac{\overline{c}^s}{\mathfrak{p}_i}\right) = 1,$$

а те критические дивизоры $\overline{k}$, которые входят в $\overline{\mathfrak{D}}$, приобретают в $\overline{K}(\sqrt[\mu]{\mu_2})$ в l раз больший показатель ветвления и поэтому остаются первого порядка.

Нам осталось еще рассмотреть свойство 4^0 . Найдем для этого в $\overline{K}$ такое число ξ , что

$$\eta(\xi)^{1-g} \eta(\overline{q_1}) \equiv 1(l^h).$$

Ввиду того, что $g \neq 1(l)$, а $\eta(\overline{q_1}) \equiv 1(l)$, так как $\overline{k}$ содержит корень степени l из единицы, такой набор возможен.

Обозначим через H группу классов дивизоров $\overline{k}$ по модулю, являющемуся общим наименьшим кратным l^h и модуля гиперпримарности, а через $\overline{\mathfrak{K}_1}$ — принадлежащее к ней абелево поле. $\overline{\mathfrak{K}_1}$ имеет в качестве критических простых дивизоров только делители l , а его максимальное неразветвленное подполе, имеющее группу показателя l , совпадает с $\overline{\mathfrak{K}}$.

Так как $\overline{K}$ шольцево, то его критические простые дивизоры отличны от делителей l и поэтому $\overline{K} \cap \overline{\mathfrak{K}_1}$ не разветвлено над $\overline{k}$. Но, по условию, $\overline{\mathfrak{K}} \cap \overline{K} = \overline{k}$, так что $\overline{K} \cap \overline{\mathfrak{K}_1} = \overline{k}$.

Ввиду этого и на основании закона плотностей Чеботарева, мы можем найти в $\overline{k}$ такое число $\overline{x}$, что $\overline{q_1}(\overline{x}) = \overline{q}$, где $\overline{q}$ — простой дивизор, принадлежащий в $\overline{K}$ к единичному автоморфизму, $\overline{x}^{-1} \xi^{t-g} \in H$ и $\overline{x} \equiv 1(\overline{p_i})$ для всех $\overline{p_i}$.

Поле $\overline{K}(\sqrt[\mu]{\mu_2 \overline{x}^s})$ не потеряет свойств 1^0 , 2^0 и 3^0 . Для свойств 2^0 и 3^0 это очевидно, а для свойства 1^0 следует из того, что

$$\overline{x_2}^s H = \xi^{(t-g)s} H = \xi^{lx} H,$$

т.е. $\overline{\kappa}_2^s$ l -гиперпримарно. Но поле $\overline{K}(\sqrt[l]{\mu_2 \overline{\kappa}^s})$ будет обладать также и свойством 4^0 .

Действительно, единственным простым делителем дискриминанта, для которого нам нужно проверить свойство 4^0 , является $\overline{q}$. Для него мы имеем:

$$\eta(\overline{q}) = \eta(\overline{q_1})\eta(\overline{\kappa}) \equiv \eta(\xi^{t-g})\eta(\overline{q_1}) \equiv \eta(\xi)^{1-g}\eta(\overline{q_1}) \equiv 1(l^h),$$

так как $\kappa \equiv \xi^{t-g}(l^h)$. Теорема 2 доказана.

3. Пример. В заключение приведем пример, показывающий, что построенные нами инварианты не всегда равны 1, причем мы ограничимся только инвариантами (χ, X) .

Пусть K_1/k — некоторое шольцево поле и μ — его l -инвариантное число, не лежащее в единичном классе X . Так как дивизор m из разложения (3) взаимно прост с дискриминантом K_1/k , то поле классов к группе, состоящей из l -х степеней классов $\bmod m$, не пересекается с K_1/k . Ввиду этого мы можем найти, на основании закона плотностей Чеботарева, простое l -гиперпримарное (при $l = 2$ totally-положительное) число $\pi \in k$, полностью распадающееся в K_1/k , но инертное в $K_1(\sqrt[l]{\mu})$, для которого $(\frac{\pi}{m}) = 1$.

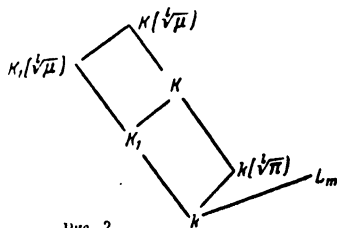


Рис. 2

Если мы обозначим $K_1(\sqrt[l]{\pi})$ через K (см. рис. 2), класс l -инвариантных чисел, в котором лежит μ , — через X , и характер, для которого $\pi = \alpha_X$, — через χ , то

$$(\chi, X) = \left(\frac{\mu}{\mathfrak{P}} \right)_{K_1} \left(\frac{\pi}{m} \right)^{-1} \neq 1, \quad \pi = N_{K_1/k}(\mathfrak{P}).$$

Эти рассуждения при $l = 2$ годятся и для случая, когда k есть поле рациональных чисел R . Простейший конкретный пример этого рода таков.

Пусть $K = R(\sqrt{17}, \sqrt{281})$. K — шольцево, так как

$$17 > 0, \quad 281 > 0, \quad 17 \equiv 281 \equiv 1(8) \quad \left(\frac{281}{17} \right) = 1, \quad \left(\frac{17}{281} \right) = 1.$$

Пусть χ — характер группы Галуа K , для которого $\alpha_\chi = 281$, и X — класс, соответствующий погружению $R(\sqrt{17})$ в циклическое поле 4-й степени. Мы докажем, что $(\chi, X) = -1$.

За представитель μ класса X мы можем взять

$$\mu = 17 + 4(\sqrt{17}) = \sqrt{17}(4 + \sqrt{17}),$$

так как

$$\mu^\sigma = \mu(4 + \sqrt{17})^2.$$

При этом $m = 1$, $\mathfrak{D} = \sqrt{17}$, так как $4 + \sqrt{17}$ является единицей в $R(\sqrt{17})$.

В поле $R(\sqrt{17})$

$$281 = N(37 - 8\sqrt{17}).$$

Очевидно, что

$$\left(\frac{\alpha_\chi}{m}\right) = \left(\frac{281}{1}\right) = 1.$$

Найдем $\left[\frac{\mu}{\alpha_\chi}\right]$. Так как

$$\alpha_\chi = 281 = N(37 - 8\sqrt{17})$$

то,

$$\left[\frac{\mu}{\alpha_\chi}\right] = \left(\frac{\sqrt{17}(4 + \sqrt{17})}{37 - 8\sqrt{17}}\right) = \left(\frac{37 - 8\sqrt{17}}{\sqrt{17}(4 + \sqrt{17})}\right),$$

последнее — по закону взаимности. Так как $4 + \sqrt{17}$ является единицей, то

$$\left(\frac{37 - 8\sqrt{17}}{\sqrt{17}(4 + \sqrt{17})}\right) = \left(\frac{37 - 8\sqrt{17}}{\sqrt{17}}\right) = \left(\frac{37}{17}\right)_R = -1.$$

Таким образом,

$$\left(\frac{\alpha_\chi}{m}\right) = 1, \quad \left[\frac{\mu}{\alpha_\chi}\right] = -1, \quad (\chi, X) = \left[\frac{\mu}{\alpha_\chi}\right] \left(\frac{\alpha_\chi}{m}\right)^{-1} = -1.$$

Хотя инварианты (χ, X) и не равны, вообще говоря, 1, но их значения не могут быть совершенно произвольными. Например, если χ — любой характер группы Галуа шольцева поля $K = k(\sqrt[\alpha]{\alpha}, \sqrt[\beta]{\beta})$,

а X соответствует погружению K в поле с неабелевой группой порядка l^3 и показателя l , то $(\chi, X) = 1$.

В статье Таннака [10], о которой шла речь во введении, утверждается, что если $k \ni \zeta$ и поле K , по нашей терминологии, — шольцево, то его можно погрузить в шольцево поле с наперед заданной группой Галуа, являющейся центральным расширением группы Галуа K/k .

По теореме 1, это возможно только тогда, когда все инварианты (χ, X) и $(X)_h$ равны 1. Построенный пример показывает, что это не всегда так.

Ошибка же в рассуждении Таннака заключается в том, что он сначала умножает l -инвариантное число μ на m так, чтобы все p_i , критические в K/k , имели первый порядок в $K(\sqrt[m]{\mu})$, а потом на такое m' , чтобы все делители $\mu m m'$ имели в K первый порядок, и не замечает, что при втором умножении теряется то, чего удалось добиться при первом.

§3. Существование расширений с заданной группой Галуа порядка l^α .

1. Канонические гомоморфизмы. Рассмотрим ряд нормальных делителей N_c свободной группы S с d образующими, определяемый индуктивно следующим образом: $N_0 = S$, N_{c+1} есть подгруппа N_c , порожденная коммутаторами элементов N_c с элементами S и l -ми степенями элементов N_c . Факторгруппу S/N_c мы будем обозначать через $\mathfrak{G}_d^{(c)}$ или, если это не будет вызывать недоразумений, просто через $\mathfrak{G}_d$. Во всех дальнейших рассуждениях будет играть роль некоторая фиксированная минимальная система образующих $s_1, \dots, s_d$ группы $\mathfrak{G}_d$.

Пусть даны группы $\mathfrak{G}_d$ и $\mathfrak{G}_\delta$ с фиксированными в них минимальными системами образующих $s_1, \dots, s_d$ и $t_1, \dots, t_\delta$. Мы будем предполагать дальше, что $\delta \leq d$. Гомоморфизм $\mathfrak{G}_d$ на $\mathfrak{G}_\delta$ называется каноническим, если при нем $s_1, \dots, s_d$ переходят только в $t_1, \dots, t_\delta$ и единицу группы $\mathfrak{G}_\delta$. Очевидно, что канонический гомоморфизм однозначно определяется отображением множества $s_1, \dots, s_d$ на множество $t_1, \dots, t_\delta, 1$ и всякое такое отображение определяет некоторый канонический гомоморфизм. Канонические гомоморфизмы мы будем обозначать через S, T и т.д. и иногда называть просто гомоморфизмами.

В дальнейшем мы будем рассматривать только такие канонические гомоморфизмы S , при которых в $t_1, \dots, t_{\delta-1}$ переходят $s_1, \dots, s_{\delta-1}$, и только они. Образующие $s_\delta, \dots, s_d$ мы будем называть свободными. Такой гомоморфизм S однозначно определяется множеством тех свободных образующих, которые переходят в t_δ . Это

множество мы будем обозначать через $[S]$. Число элементов $[S]$ будем обозначать через $|S|$. Гомоморфизмы указанного вида мы будем называть гомоморфизмами типа $(s_1, \dots, s_{\delta-1}; t_1, \dots, t_{\delta-1} | t_{\delta})$.

Два гомоморфизма S и T мы будем называть независимыми, если множества $[S]$ и $[T]$ не пересекаются. Тогда существует один единственный гомоморфизм R , для которого

$$[R] = [S] \cup [T].$$

R мы будем называть композитом S и T и обозначать через $S * T$. Операция компонирования гомоморфизмов коммутативна и ассоциативна и применима к любому множеству попарно независимых гомоморфизмов. Очевидно, что при этом

$$|S_1 * \dots * S_m| = |S_1| + \dots + |S_m|.$$

2. Функции гомоморфизмов. В дальнейшем будут рассматриваться и называться коротко функциями гомоморфизмов функции $f(S)$, определенные на множестве всех гомоморфизмов и принимающие значения, являющиеся элементами некоторой абелевой группы порядка g .

Для функций гомоморфизмов одного и того же типа $(s_1, \dots, s_{\delta-1}; t_1, \dots, t_{\delta-1} | t_{\delta})$ определяется степень относительно образующей t_{δ} . Рассмотрим функцию

$$\varphi(S, T) = f(S)f(T)f(S * T)^{-1}, \quad (28)$$

определенную для любой пары независимых гомоморфизмов S и T и симметричную относительно S и T . Степень 0 припишем функции, которая для всех S принимает значение 1. Мы будем говорить, что $f(S)$ имеет степень $\leq n$, если $\varphi(S, T)$ для любого S имеет, как функция от T , степень $\leq n - 1$. Заметим, что не утверждается, что всякая функция имеет некоторую степень. Например, функция, принимающая для всех S одно и то же, отличное от 1, значение, очевидно, не имеет никакой степени.

Определение степени функции можно сформулировать другим эквивалентным образом. Функция $f(S)$ имеет степень $\leq n$, если для любого множества из $n+1$ попарно независимых гомоморфизмов $S_{i_1}, \dots, S_{i_{n+1}}$ удовлетворяется следующее соотношение:

$$\prod_{(j_1, \dots, j_k)} f(S_{j_1} * \dots * S_{j_k})^{(-1)^k} = 1, \quad (29)$$

где $(j_1, \dots, j_k)$ пробегает все непустые подмножества множества $(i_1, \dots, i_{n+1})$.

Докажем эквивалентность обоих определений. Доказательство будем вести по индукции. Покажем предварительно, что для любых попарно независимых $S_{i_1}, \dots, S_{i_{n+1}}$ имеет место тождество

$$\prod_{(r_1, \dots, r_k)} \varphi(S_{i_1}, S_{r_1} * \dots * S_{r_k})^{(-1)^k} = \prod_{(j_1, \dots, j_k)} f(S_{j_1} * \dots * S_{j_k})^{(-1)^k}, \quad (30)$$

где слева $(r_1, \dots, r_k)$ пробегает все непустые подмножества множества $(i_2, \dots, i_{n+1})$, а справа $(j_1, \dots, j_k)$ — непустые подмножества $(i_1, \dots, i_{n+1})$. Для этого в левой части равенства (30) выразим φ через f согласно (28). Мы получим:

$$\begin{aligned} & \prod_{(r_1, \dots, r_k)} f(S_{i_1})^{(-1)^k} \prod_{(r_1, \dots, r_k)} f(S_{r_1} * \dots * S_{r_k})^{(-1)^k} \cdot \\ & \cdot \prod_{(r_1, \dots, r_k)} f(S_{i_1} * S_{r_1} * \dots * S_{r_k})^{(-1)^{k+1}}. \end{aligned} \quad (31)$$

Сравним отдельные множители в (31) и в правой части (30). Первое произведение есть $f(S_{i_1})$, возведенное в степень, равную

$$\sum_{(r_1, \dots, r_k)} (-1)^k = \sum_{k=1}^n (-1)^k C_n^k = -1,$$

т.е. совпадает с множителем $f(S_{i_1})^{-1}$ в правой части (30). Каждый множитель второго и третьего произведений очевидным образом совпадает с определенным множителем в правой части (30). Таким образом, тождество (30) доказано.

Если мы предположим, что $f(S)$ имеет степень $\leq n$ согласно первому определению, то по индуктивному предположению это значит, что левая часть (30) обращается в 1. Тогда и правая часть равна 1, а это и значит, что $f(S)$ имеет степень $\leq n$ согласно второму определению. Если же $f(S)$ имеет степень $\leq n$ согласно второму определению, то правая, а следовательно, и левая часть (30), равна 1. Но, согласно индуктивному предположению, это значит, что $\varphi(S_{i_1}, T)$ имеет при любом S_{i_1} степень $\leq n-1$ относительно T , т.е. что $f(S)$ имеет степень $\leq n$ согласно первому определению.

3. Теорема существования. Докажем теорему, гарантирующую в некоторых случаях существование решений у уравнений $f_i(S) = 1$, где $f_i(S)$ — имеющие определенную степень функции гомоморфизма. При этом мы будем рассматривать канонические гомоморфизмы группы $\mathfrak{G}_d$ с меняющимся числом образующих d на раз навсегда фиксированную группу $\mathfrak{G}_\delta$, причем все гомоморфизмы будут одного и того же типа.

Теорема 3. Для любых натуральных чисел k и n существует зависящее только от них натуральное число $C(k, n)$ со следующим свойством: какие бы k функций гомоморфизмов $f_1(S), \dots, f_k(S)$ степени $\leq n$ ни были заданы на группе $\mathfrak{G}_d$ с $d \geq C(k, n)$, всегда найдется такой гомоморфизм S этой группы, что $f_i(S) = 1$, $i = 1, \dots, k$.

Доказательство ведется индукцией по степени n функций $f_1, \dots, f_k$. Выберем некоторый гомоморфизм T_1 , для которого $|T_1| = 1$, и рассмотрим функции

$$\varphi_i(T_1, T) = f_i(T_1)f_i(T)f_i(T_1 * T)^{-1}, \quad i = 1, \dots, k,$$

как функции от T . Они определены только для гомоморфизмов T , не зависящих от T_1 , или, можно считать, для гомоморфизмов группы $d-1$ образующих, которая получится, если в группе $\mathfrak{G}_d$ перевести в 1 образующую $[T_1]$.

Предположим, что $d \geq C(k, n-1) + 1$, и выделим из числа свободных образующих группы $\mathfrak{G}_d$ подмножество M_1 из $C(k, n-1)$ образующих, не содержащее $[T_1]$. Рассмотрим функции $\varphi_i(T_1, T)$ только на множестве тех гомоморфизмов T , для которых $[T] \subset M_1$, или, что то же самое, на группе с $d + C(k, n-1)$ образующими. Мы можем применить к ним индуктивное предположение и получим, что существует такой гомоморфизм T_2 с $[T_2] \subset M_1$, что

$$\varphi_i(T_1, T_2) = 1,$$

т.е.

$$f_i(T_1 * T_2) = f_i(T_1)f_i(T_2), \quad i = 1, \dots, k.$$

Рассмотрим теперь $3k$ функций:

$$\varphi_i(T_1, T), \quad \varphi_i(T_2, T), \quad \varphi_i(T_1 * T_2, T), \quad i = 1, \dots, k. \quad (32)$$

Эти функции определены на гомоморфизмах T , не зависящих от T_1 и T_2 , или можно считать, на группе с $d-1-C(k, n-1)$ образующими, которая получится, если перевести в 1 все образующие группы $\mathfrak{G}_d$, входящие в $[T_1] \cup M_1$. Предположим, что

$$d \geq 1 + C(k, n-1) + C(3k, n-1),$$

и выделим из числа свободных образующих группы $\mathfrak{G}_d$ подмножество M_2 , не пересекающееся с $[T_1] \cup M_1$ и состоящее из $C(3k, n-1)$ образующих. Рассмотрим функции (32) только на множестве тех гомоморфизмов T , для которых $[T] \subset M_2$, т.е. на группе с

$C(3k, n-1)$ образующими. Мы можем применить к ним индуктивное предположение и получим, что существует такой гомоморфизм T_3 с $[T_3] \subset M_2$, что

$$\varphi_i(T_1, T_3) = 1,$$

$$\varphi_i(T_2, T_3) = 1,$$

$$\varphi_i(T_1 * T_2, T_3) = 1,$$

т.е.

$$f_i(T_1 * T_3) = f_i(T_1)f_i(T_3),$$

$$f_i(T_2 * T_3) = f_i(T_2)f_i(T_3),$$

$$f_i(T_1 * T_2 * T_3) = f_i(T_1)f_i(T_2)f_i(T_3)$$

$$(i = 1, \dots, k).$$

Продолжая этот процесс на r шагов, мы получим, как легко видеть, что, если

$$d \geq 1 + C(k, n-1) + C(3k, n-1) + \dots + C((2^{r-1} - 1)k, n-1),$$

то существуют попарно независимые гомоморфизмы $T_1, \dots, T_r$, для которых имеют место соотношения:

$$f_i(T_{j_1} * \dots * T_{j_s}) = f_i(T_{j_1}) \dots f_i(T_{j_s}) \quad (i = 1, \dots, k), \quad (33)$$

если $(j_1, \dots, j_s)$ — любое подмножество $(1, \dots, r)$. Мы положим $r = g^{k+1}$ и, соответственно,

$$C(k, n) = 1 + C(k, n-1) + C(3k, n-1) + \dots + C((2^{g^{k+1}-1} - 1)k, n-1).$$

Поскольку, согласно предположению теоремы, $d \geq C(k, n)$, гомоморфизмы $T_1, \dots, T_r$ с указанным свойством существуют. Так как мы имеем k функций $f_i(S)$, каждая из которых может принимать g значений, а число гомоморфизмов T в нашем множестве равно g^{k+1} , то существует система гомоморфизмов $T_{j_1}, \dots, T_{j_g}$, для которой выполнены соотношения

$$f_i(T_{j_1}) = f_i(T_{j_2}) = \dots = f_i(T_{j_g}) \quad (i = 1, \dots, k). \quad (34)$$

Положим

$$T_{j_1} * T_{j_2} * \dots * T_{j_g} = S.$$

Ввиду (33) и (34), имеем

$$f_i(S) = f_i(T_{j_1})f_i(T_{j_2}) \dots f_i(T_{j_g}) = f_i(T_{j_1})^g = 1,$$

так как значения функций f_i принадлежат группе порядка g . Таким образом, гомоморфизм S удовлетворяет всем требованиям теоремы.

Заметим, что если группа $\mathfrak{G}_{d_1}^{(c)}$ с $d_1 \leq d$ является гомоморфным образом группы $\mathfrak{G}_d^{(c)}$ при некотором каноническом гомоморфизме, то любая функция гомоморфизма на $\mathfrak{G}_d^{(c)}$ является также функцией гомоморфизма на $\mathfrak{G}_{d_1}^{(c)}$, так как любой канонический гомоморфизм $\mathfrak{G}_{d_1}^{(c)}$ является в то же время каноническим гомоморфизмом $\mathfrak{G}_d^{(c)}$.

Следствие. Если при предположениях теоремы 3 в группе $\mathfrak{G}_d$ указаны m свободных образующих $s_{i_1}, \dots, s_{i_m}$ и $d \geq C(k, n) + m$, то группу $\mathfrak{G}_d$ можно отобразить при помощи канонического гомоморфизма на группу $\mathfrak{G}_{\delta+m}$ с образующими $s'_1, \dots, s'_{\delta+m}$, у которой все функции $f_1, \dots, f_k$ обращаются в единицу на гомоморфизме $s'_1 \rightarrow t_1, \dots, s'_\delta \rightarrow t_\delta, s'_{\delta+1} \rightarrow 1, \dots, s'_{\delta+m} \rightarrow 1$.

Доказательство. Отобразим группу $\mathfrak{G}_d$ на $\mathfrak{G}_{d-m}$, положив

$$s_{i_1} \rightarrow 1, \dots, s_{i_m} \rightarrow 1.$$

К полученной группе $\mathfrak{G}_{d-m}$ можно применить теорему 3 и найти канонический гомоморфизм S , для которого

$$f_1(S) = 1, \dots, f_k(S) = 1.$$

S будет также каноническим гомоморфизмом $\mathfrak{G}_d$. Рассмотрим канонический гомоморфизм $\mathfrak{G}_d$ на группу $\mathfrak{G}_{\delta+m}$ с образующими $s'_1, \dots, s'_\delta, s'_{\delta+1}, \dots, s'_{\delta+m}$, который для всех образующих, кроме $s_{i_1}, \dots, s_{i_m}$ определен так же, как S , а $s_{i_1}, \dots, s_{i_m}$ отображает на $s'_{\delta+1}, \dots, s'_{\delta+m}$. Очевидно, $\mathfrak{G}_{\delta+m}$ будет обладать указанными в формулировке следствия свойствами.

4. Инварианты (χ, X) и $(X)_h$ полей с группой $\mathfrak{G}_d^{(c)}$.

Предположим, что мы имеем шольцево поле K/k , группа Галуа которого есть группа $\mathfrak{G}_d^{(c)}$ с выделенной в ней системой образующих $s_1, \dots, s_d$. Изучим инварианты (χ, X) и $(X)_h$ в этом случае. Прежде всего рассмотрим базис группы характеров порядка l $\chi_1, \dots, \chi_d$, взаимный к системе образующих $s_1, \dots, s_d$, т.е. удовлетворяющий соотношениям

$$\chi_i(s_j) = 1, \quad i \neq j,$$

$$\chi_i(s_i) \neq 1.$$

Числа α_{χ_i} будем сокращенно обозначать через α_i . В дальнейшем будем предполагать, что числа α_i попарно l -взаимно просты.

Заметим, что если представить $\mathfrak{G}_d^{(c)}$ в виде факторгруппы S/N свободной группы с d образующими, как мы это делали в §1, то N будет совпадать с N_c , а N' из леммы 1 — с N_{c+1} . Очевидно, что N/N' есть не что иное, как ядро гомоморфизма $\mathfrak{G}_d^{(c+1)}$ на $\mathfrak{G}_d^{(c)}$, а это есть центр группы $\mathfrak{G}_d^{(c+1)}$.

Таким образом, для исследования характеров X нам нужно знать центр Z группы $\mathfrak{G}_d^{(c+1)}$. Он был исследован в работе А.И. Скопина [9], который показал, что Z разлагается в прямую сумму подгрупп

$$Z = Z_1 + Z_2 + \dots + Z_{c+1}, \quad (35)$$

где Z_ν изоморфно модулю многочленов Ли степени ν от d неизвестных $x_1, \dots, x_d$ над полем вычетов по модулю l^* . При этом неизвестные x_i связаны с образующими s_i соотношениями $s_i = 1 + x_i$. Из этого следует, что гомоморфизм группы $\mathfrak{G}_d^{(c+1)}$, при котором некоторое s_i переходит в 1, индуцирует в модуле многочленов Ли гомоморфизм, при котором соответствующее x_i переходит в 0.

Из конструкции А.И. Скопина следует также, что образующие x_i модуля Z_1 при изоморфном отображении Z_1 на центр $\mathfrak{G}_d^{(c+1)}$ отображаются на $s_i^{l^c}$. Отсюда вытекает, что при расширении группы $\mathfrak{G}_d^{(c)}$, соответствующему характеру X группы Z , аннулирующему подгруппу Z_1 , ни один из элементов вида $s_i^r u$, где $(r, l) = 1$ и u принадлежит подгруппе Фраттини группы $\mathfrak{G}_d^{(c)}$, не повышает своего порядка.

Чтобы показать это, докажем, что в группе S

$$(s_i^r u)^{l^c} \equiv s_i^{r l^c} (N_{c+1}), \quad \text{если } u \in N_1.$$

Проще всего доказать это соотношение индукцией по c . Мы имеем:

$$(s_i^r u)^{l^{c-1}} \equiv s_i^{r l^{c-1}} (N_c),$$

т.е.

$$(s_i^r u)^{l^{c-1}} = s_i^{r l^{c-1}} v, \quad v \in N_c.$$

*Как заметил Н.Коч, в работе А.И.Скопина рассматривается только случай $p \neq 2$. Необходимые в случае $p = 2$ изменения очевидны: см. работу [6] в ч. II.

Возведем обе части в степень l и воспользуемся тем, что элементы N_c коммутируют с элементами S по модулю N_{c+1} .

$$(s_i^r u)^{l^c} \equiv (s_i^{r l^{c-1}} v)^l \equiv s_i^{r l^c} v^l \equiv s_i^{r l^c} (N_{c+1}),$$

так как $v^l \in N_{c+1}$, если $v \in N_c$.

Из доказанного соотношения и следует, что любой элемент вида $s_i^r u$ имеет в $\mathfrak{G}_d^{(c)}$ порядок l^c , а в расширении, соответствующем X , имеет порядок l^{c+1} только при $\chi(s_i^{r l^c}) \neq 1$.

В соответствии с разложением (35) мы можем представить каждый характер X группы Z в виде

$$X = X_1 + X',$$

где X_1 аннулирует все подгруппы Z_i , кроме Z_1 , а X' аннулирует подгруппу Z_1 . Для дивизоров $\mathfrak{D}(X)$, введенных в п. 3 §1, мы имеем при этом:

$$\mathfrak{D}(X) \approx \mathfrak{D}(X_1)\mathfrak{D}(X').$$

Так как было доказано, что $\mathfrak{D}(X)$ содержит те и только те простые дивизоры, образующие автоморфизмы групп инерции которых повышают свой порядок при расширении, соответствующем X , то из сказанного выше следует, что

$$\mathfrak{D}(X') \approx 1, \quad \mathfrak{D}(X) \approx \mathfrak{D}(X_1).$$

Нам остается исследовать подробнее характеры X_1 . Группа Z_1 изоморфна

$$\mathfrak{G}_d^{(1)} = \mathfrak{G}_d^{(c+1)} / \Phi(\mathfrak{G}_d^{(c+1)}),$$

где $\Phi(\mathfrak{G}_d^{(c+1)})$ означает подгруппу Фраттини группы $\mathfrak{G}_d^{(c+1)}$, причем естественный гомоморфизм дается отображением $s \rightarrow s^{l^c}$. В самом деле, отображение

$$x \rightarrow x^{l^c} N_{c+1}$$

является гомоморфизмом, что следует из соотношения

$$(xy)^{l^c} \equiv x^{l^c} y^{l^c} (N_{c+1}),$$

непосредственно доказываемого индукцией по c^* . Мы знаем, что $u \in \Phi(\mathfrak{G}_d^{(c+1)})$ при этом гомоморфизме переходят в 1, а образующие s_i — в образующие Z_1 , что и доказывает наше утверждение.

* Следует заменить N_{c+1} на $N_{c+1}N_c^{(2)}$, где $N_c^{(2)}$ — коммутант группы N_c . См. также работу [6] в ч. II.

Таким образом, характеры X_1 группы Z_1 находятся во взаимно однозначном соответствии с характерами χ порядка l группы $\mathfrak{G}_d^{(c+1)}$. Характер X_1 , соответствующий характеру χ , будем обозначать через $\tilde{\chi}$. Выясним, для каких пар характеров χ_i, χ_j определен инвариант $(\chi_i, \tilde{\chi}_j)$. Для того, чтобы он был определен, необходимо и достаточно, чтобы α_i было l -взаимно просто с $\mathfrak{D}(\tilde{\chi}_j)$. Как мы знаем, α_i не будет l -взаимно просто с $\mathfrak{D}(\tilde{\chi}_j)$, если оно содержит простой делитель p в степени, не делящейся на l , образующая группы инерции которого повышает свой порядок при расширении, соответствующем $\tilde{\chi}_j$. Как легко видеть, ввиду того, что числа $\alpha_1, \dots, \alpha_d$ попарно l -взаимно просты, образующей группы инерции такого дивизора будет автоморфизм σ , для которого $\chi_i(\sigma) \neq 1, \chi_j(\sigma) = 1$ при $i \neq j$. Такой автоморфизм повышает свой порядок при расширении, соответствующем характеру $\tilde{\chi}_j$, только при $i = j$.

Действительно, элемент σ , для которого $\chi_i(\sigma) \neq 1, \chi_j(\sigma) = 1$ при $i \neq j$ имеет вид $s_i^r u$, где $(l, r) = 1$ и u — элемент подгруппы Фраттини. Такой элемент повышает свой порядок при расширении, соответствующем $\tilde{\chi}_j$, только если

$$\tilde{\chi}_j((s_i^r u)^{l^c}) \neq 1.$$

Так как

$$(s_i^r u)^{l^c} = s_i^{rl^c}, \quad \tilde{\chi}_j(s_i^{rl^c}) = \chi_j(s_i^r),$$

то это имеет место только при $i = j$. Таким образом, инварианты (χ_i, X') определены для всех характеров χ_i и X' , а инварианты $(\chi_i, \tilde{\chi}_j)$ тогда и только тогда, когда $i \neq j$.

5. Инварианты (χ, X) и $(X)_h$ как функции гомоморфизмов. Как и в п. 4, мы будем рассматривать шольцево поле K , группа Галуа которого есть группа $\mathfrak{G}_d^{(c)}$ с выделенной в ней системой образующих $s_1, \dots, s_d$, причем числа $\alpha_1, \dots, \alpha_d$ попарно l -взаимно просты. Рассмотрим канонический гомоморфизм группы $\mathfrak{G}_d^{(c)}$ на некоторую группу $\mathfrak{G}_\delta^{(c)}$. Его ядро $\mathfrak{N}$ является нормальным делителем группы $\mathfrak{G}_d^{(c)}$, так что $\mathfrak{N}$ принадлежит нормальное подполе поля K . Это подполе мы будем обозначать через K^S . Очевидно, K^S имеет группу Галуа $\mathfrak{G}_\delta^{(c)}$ с выделенной системой образующих $t_1, \dots, t_\delta$, состоящей из образов образующих $s_1, \dots, s_d$. Числа $\alpha_1, \dots, \alpha_\delta$, соответствующие подполю K^S , получаются перемножением чисел $\alpha_1, \dots, \alpha_d$, причем разные произведения не имеют общих множителей, так что $\alpha_1, \dots, \alpha_\delta$ попарно l -взаимно просты. Это следует из того, что если $[S] = (s_{i_1}, \dots, s_{i_m})$, то числа $\alpha_1, \dots, \alpha_{\delta-1}$,

соответствующие полю K^S , совпадают с такими числами, соответствующими полю K , а число α_δ поля K^S имеет вид $\alpha_{i_1}, \dots, \alpha_{i_m}$, где $\alpha_{i_1}, \dots, \alpha_{i_m}$ — числа, соответствующие полю K . Последнее утверждение можно проверить непосредственно. Именно $\sqrt{\alpha_1}, \dots, \sqrt{\alpha_{\delta-1}}$ и $\sqrt{\alpha_{i_1}}, \dots, \alpha_{i_m}$ — инварианты относительно автоморфизмов поля K , составляющих ядро гомоморфизма S , и соответствуют характеристам $\chi_1, \dots, \chi_d$.

Рассмотрим характеры $\chi_1, \dots, \chi_\delta$ группы $\mathfrak{G}_\delta^{(c)}$ и характеры $\widetilde{\chi}_1, \dots, \widetilde{\chi}_\delta$ и X' центра Z группы $\mathfrak{G}_\delta^{(c+1)}$.

Пусть S есть произвольный канонический гомоморфизм группы $\mathfrak{G}_d^{(c)}$ на $\mathfrak{G}_\delta^{(c)}$. В поле K^S определены инварианты

$$(\chi_i, X'), \quad (\chi_i, \widetilde{\chi}_j) \quad \text{при} \quad i \neq j, \quad (X')_h \quad \text{и} \quad (\widetilde{\chi}_i)_h. \quad (36)$$

При фиксированном поле K каждый из них однозначно определяется гомоморфизмом S и является, таким образом, функцией гомоморфизма. Число инвариантов (36) будем обозначать через k или, если надо будет подчеркнуть зависимость от числа образующих δ группы $\mathfrak{G}_\delta^{(c)}$, — через k_δ . Мы имеем, таким образом, k функций гомоморфизма: $f_1(S), \dots, f_k(S)$. Нашей ближайшей задачей будет исследование их степеней.

Так как в силу (35) каждый характер X является суммой характеров X_ν групп Z_ν , аннулирующих Z_μ при $\mu \neq \nu$, то мы ограничимся рассмотрением только характеров X_ν . Каждый такой характер есть характер модуля многочленов Ли степени ν от d неизвестных $x_1, \dots, x_d$ над полем вычетов по модулю l . Мы будем говорить, что характер имеет степень $\leq n$ относительно образующей x_i , если он аннулирует все одночлены Ли, в которые x_i входит в степени, большей n . Совершенно аналогично тому, как мы это делали для групп $\mathfrak{G}_d^{(c)}$, определим канонические гомоморфизмы для модулей Ли заданной степени от d переменных. Если $\Lambda_\delta^{(\nu)}$ есть модуль Ли многочленов степени ν от переменных $y_1, \dots, y_\delta$, а $\Lambda_d^{(\nu)}$ — от d переменных $x_1, \dots, x_d$ и S — канонический гомоморфизм $\Lambda_d^{(\nu)}$ на $\Lambda_\delta^{(\nu)}$, то каждый характер X_ν модуля $\Lambda_\delta^{(\nu)}$ будет также характером модуля $\Lambda_d^{(\nu)}$. Этот характер мы обозначим через X_ν^S .

Лемма 3. Если характер X_ν модуля $\Lambda_\delta^{(\nu)}$ имеет степень $\leq n$ относительно y_δ и аннулирует все многочлены, зависящие только от $y_1, \dots, y_{\delta-1}$, то

$$\sum_{(i_1, \dots, i_k)} (-1)^k X_\nu^{S_{i_1} * \dots * S_{i_k}} = 0, \quad (37)$$

где $S_{i_1}, \dots, S_{i_k}$ пробегает все непустые подмножества множества $S_1, \dots, S_{n+1}$ из $n+1$ попарно независимых гомоморфизмов одного и того же типа $(x_1, \dots, x_{\delta-1}; y_1, \dots, y_{\delta-1} | y_\delta)$.

Доказательство. Пусть φ есть произвольный многочлен Ли модуля $\Lambda_d^{(\nu)}$. Оператор замены на y_δ всех неизвестных, входящих в $[S_i]$, обозначим через p_i . Оператор замены нулем всех свободных образующих, входящих в $[S_i]$, обозначим через q_i и оператор замены нулем всех свободных образующих, кроме входящих в $[S_1] \cup \dots \cup [S_{n+1}]$, обозначим через q_0 . Тогда условие (37) можно переписать так:

$$X_\nu \left(\sum (-1)^k p_{i_1} \dots p_{i_k} q_{j_1} \dots q_{j_{n+1-k}} q_0 \varphi \right) = 0, \quad (38)$$

где сумма распространена на все разбиения $(i_1 \dots i_k j_1 \dots j_{n+1-k})$ множества $(1, \dots, n+1)$ на две части, из которых первая не пустая.

Заметим, что операторы p_i и p_j коммутируют между собой, так как они действуют на разные образующие. Это же относится и к операторам q_i, q_j и p_i, q_j при $i \neq j$, причем q_0 коммутирует со всеми операторами. Ввиду этого имеем:

$$\begin{aligned} & \sum (-1)^k p_{i_1} \dots p_{i_k} q_{j_1} \dots q_{j_{n+1-k}} q_0 = \\ & = q_0 (q_1 - p_1) \dots (q_{n+1} - p_{n+1}) - q_0 q_1 \dots q_{n+1}. \end{aligned} \quad (39)$$

Применим оператор (39) к произвольному многочлену Ли φ . Если для некоторого i φ не содержит ни одной образующей, входящей в состав $[S_i]$, то $q_i \varphi = p_i \varphi = \varphi$ и поэтому оператор

$$q_0 (q_1 - p_1) \dots (q_{n+1} - p_{n+1}) \quad (40)$$

переводит φ в 0. Если же φ содержит хоть по одной образующей из каждого $[S_i]$, то оператор (40) переводит φ в многочлен, имеющий относительно y_δ степень по крайней мере $n+1$. Наконец, оператор $q_0 q_1 \dots q_{n+1}$ переводит φ в многочлен, зависящий только от $y_1, \dots, y_{\delta-1}$. Таким образом, оператор (39) переводит любой многочлен Ли в сумму многочлена, имеющего степень по крайней мере $n+1$ относительно y_δ , и многочлена, зависящего только от $y_1, \dots, y_{\delta-1}$. На таких многочленах характер X_{n+1} обращается в 0, что и доказывает (38), а следовательно, и (37).

Следствие. В предположениях леммы 3 для любого гомоморфизма S_0 , независимого от $S_1, \dots, S_{n+1}$,

$$\sum_{(i_1 \dots i_k)} (-1)^k X_\nu^{S_0 * S_{i_1} * \dots * S_{i_k}} = 0. \quad (41)$$

Для доказательства достаточно произвести сначала канонический гомоморфизм, который на образующие, входящие в $[S_0]$, действует как S_0 , а все остальные образующие не меняет, и к полученному модулю Ли применить лемму.

В дальнейшем мы будем применять мультипликативную запись, так что формулы (37) и (41) примут вид:

$$\prod_{(i_1 \dots i_k)} (X_\nu^{S_{i_1} * \dots * S_{i_k}})^{(-1)^k} = 1 \quad (42)$$

и

$$\prod_{(i_1 \dots i_k)} (X_\nu^{S_0 * S_{i_1} * \dots * S_{i_k}})^{(-1)^k} = 1 \quad (43)$$

Теорема 4. Если характер X_ν имеет относительно y_δ степень $\leq n$, не аннулирует хотя один многочлен, зависящий от y_δ , и аннулирует все многочлены, зависящие только от $y_1, \dots, y_{\delta-1}$, то инварианты (χ_i, X_ν) и $(X_\nu)_h$ имеют как функции гомоморфизмов типа $(s_1, \dots, s_{\delta-1}; t_1, \dots, t_{\delta-1} | t_\delta)$ группы Галуа $\mathfrak{G}_d^{(c)}$ шольцева поля K , следующие степени:

$$(X_\nu)_h \text{ — степень } \leq n,$$

$$(\chi_i, X_\nu) \text{ при } i \neq \delta \text{ — степень } \leq n,$$

$$(\chi_\delta, X_\nu) \text{ — степень } \leq n + 1.$$

Таким образом, все эти инварианты имеют степень $\leq c + 2$.

Доказательство. Мы воспользуемся вторым из двух данных в п. 2 определений степени и проведем доказательство отдельно для каждого из трех перечисленных в формулировке теоремы случаев.

Обозначим инвариант $(X_\nu)_h$ подполя K^S через $f(S)$ и докажем для него соотношение (29). Характер X_ν , связанный с группой Галуа поля K^S , определяет характер X_ν^S , связанный с группой Галуа поля K , причем, согласно формуле (13) §1,

$$f(S) = (X_\nu)_h = (X_\nu^S)_h.$$

Формула (29) сводится, таким образом, к формуле

$$\prod_{(i_1 \dots i_k)} (X_\nu^{S_{i_1} * \dots * S_{i_k}})^{(-1)^k} = 1.$$

Ввиду формулы (12) §1 мы имеем:

$$\prod_{(i_1 \dots i_k)} (X_\nu^{S_{i_1} \dots S_{i_k}})_h^{(-1)^k} = \left(\prod_{(i_1 \dots i_k)} (X^{S_{i_1} \dots S_{i_k}})^{(-1)^k} \right)_h ;$$

правая же часть этой формулы равна 1 в силу (42).

Обозначим теперь через $f(S)$ инвариант (χ_i, X_ν) подполя K^S поля K , причем напомним, что он определен, если X_ν есть один из характеров X' , т.е. $\nu > 1$, или есть характер $\tilde{\chi}_j$ с $j \neq i$. Характер χ группы Галуа поля K^S является характером χ^S группы Галуа поля K , а характер X_ν , связанный с группой Галуа поля K^S , определяет характер X_ν^S , связанный с группой Галуа поля K . В рассматриваемом случае все характеры χ_i^S совпадают между собой, так как характер χ_i не зависит от образующей t_δ . Мы будем обозначать их все через $\overline{\chi}_i$. Заметим, что инварианты $(\overline{\chi}_i, X_\nu^S)$ определены тогда же, когда определены инварианты (χ_i, X_ν) . Ввиду (7), имеем:

$$f(S) = (\chi_i, X_\nu) = (\overline{\chi}_i, X_\nu^S),$$

и формула (29) сводится в нашем случае к равенству:

$$\prod_{(i_1 \dots i_k)} (\overline{\chi}_i, X_\nu^{S_{i_1} \dots S_{i_k}})^{(-1)^k} = 1.$$

Ввиду (6), мы имеем:

$$\prod_{(i_1 \dots i_k)} (\overline{\chi}_i, X_\nu^{S_{i_1} \dots S_{i_k}})^{(-1)^k} = \left(\overline{\chi}_i, \prod_{(i_1 \dots i_k)} (X_\nu^{S_{i_1} \dots S_{i_k}})^{(-1)^k} \right);$$

правая же часть этой формулы равна 1 в силу (42).

Нам осталось рассмотреть последний случай. Как и в предыдущем случае, имеем:

$$f(S) = (\chi_\delta, X_\nu) = (\chi_\delta^S, X_\nu^S).$$

Левая часть соотношения (29) приводится в данном случае к выражению

$$\prod_{(i_1 \dots i_k)} (\chi_\delta^{S_{i_1} \dots S_{i_k}}, X_\nu^{S_{i_1} \dots S_{i_k}})^{(-1)^k}, \quad (44)$$

где $(S_{i_1}, \dots, S_{i_k})$ пробегает непустые подмножества множества $(S_0, S_1, \dots, S_{n+1})$ из $n+2$ независимых гомоморфизмов. Применим лемму 3 к характеру χ_δ ; мы получим, что

$$\chi_\delta^{S_{i_1} * \dots * S_{i_k}} = \chi_\delta^{S_{i_1}} \dots \chi_\delta^{S_{i_k}}.$$

Заметим, что, как можно непосредственно проверить, инварианты $(\chi_\delta^{S_i}, X_\nu^{S_i})$ определены, если были определены инварианты (χ_δ, X_ν) , так что мы можем записать (44) в виде

$$\prod_{(i_1 \dots i_k)} \prod_{r=1}^k (\chi_\delta^{S_{i_r}}, X_\nu^{S_{i_1} * \dots * S_{i_k}}) (-1)^k.$$

Если в этом произведении собрать все множители, у которых на первом месте стоит $\chi_\delta^{S_j}$, то мы получим выражение:

$$\prod (\chi_\delta^{S_j}, X_\nu^{S_j * S_{i_1} * \dots * S_{i_k}}) (-1)^{k+1},$$

где $S_{i_1}, \dots, S_{i_k}$ пробегает все подмножества множества $S_0, \dots, S_{n+1}$, не содержащие S_j . Мы можем переписать это выражение в виде

$$(\chi_\delta^{S_j}, \prod_{(i_1 \dots i_k)} (X_\nu^{S_{i_1} * \dots * S_{i_k}}) (-1)^k)^{-1},$$

что равно 1 в силу (43). Теорема доказана.

Заметим, что если в предположениях теоремы 4 X аннулирует все многочлены, зависящие от y_δ , то при $i \neq \delta$ (χ_i, X) не имеет степени, а (χ_δ, X) имеет степень 1.

6. Существование расширений с заданной группой порядка l^α .

Теорема 5. Для каждого натурального числа δ существует натуральное число $C(\delta)$ со следующим свойством: в любом шольцевом поле K с группой Галуа $\mathfrak{G}_d^{(c)}$, $d > C(\delta)$, с выделенной системой образующих $s_1, \dots, s_d$ и попарно l -взаимно простыми $\alpha_1, \dots, \alpha_d$, существует подполе K^S с группой Галуа $\mathfrak{G}_\delta^{(c)}$ и всеми инвариантами (χ, X) и $(X)_h$, равными 1.

Доказательство. Выберем в модуле многочленов Ли степени $c+1$ базис, состоящий из одночленов Ли, и рассмотрим базис группы характеров, взаимный к этому базису.

Если в базисный одночлен Ли φ_i входят неизвестные $x_1, \dots, x_d$ в степенях $m_1, \dots, m_d$, то соответствующий базисный характер X_i будет аннулировать все одночлены Ли, в которые переменные входят в других степенях. Если при этом $m_{i_1} \neq 0, \dots, m_{i_r} \neq 0$, а остальные степени $m_j = 0$, то мы будем говорить, что X_i зависит только от $x_{i_1}, \dots, x_{i_r}$. Так как любой характер составляется из базисных, а инварианты (χ, X) и $(X)_h$ мультипликативны, то мы будем добиваться равенства единице только тех инвариантов, в которые входят базисные характеры.

Перепишем все инварианты (χ, X) и $(X)_h$ с базисными характерами χ и X в определенном порядке. Сначала напомним те инварианты, в которые входят характеры X , зависящие только от x_1 и x_2 , и характеры χ_1 и χ_2 . При этом, как легко видеть, если характер χ есть χ_1 , то X зависит от x_2 , а если χ есть χ_2 , то X зависит от x_1 . Число инвариантов этой первой группы обозначим через k_2 . Затем напомним инварианты, в которых χ есть χ_1, χ_2 , или χ_3 , а X зависит только от x_1, x_2, x_3 , причем или χ есть χ_3 , или X зависит от x_3 . Число инвариантов этой группы обозначим через k_3 . Аналогично, через k_i обозначим число инвариантов, в которых есть одно из $\chi_1, \dots, \chi_i$, а X зависит только от $x_1, \dots, x_i$, причем или $\chi = \chi_i$, или X зависит от x_i . Очевидно, что число таких групп будет δ , и каждый инвариант, в который входят только базисные характеры, попадет в одну из этих групп. Пусть $C(k, n)$ — те числа, существование которых установлено в теореме 3. Там число образующих δ группы, на которую отображают группу $\mathfrak{G}_d^{(c)}$ канонические гомоморфизмы, было фиксировано. Так как теперь мы будем его менять, то соответствующее число $C(k, n)$ будем обозначать через $C(k, n, \delta)$. Мы докажем, что число $C(\delta)$, существование которого утверждается теоремой, можно определить формулой:

$$C(\delta) = 1 + C(k_2, c+2, 2) + C(k_3, c+2, 3) + \dots + C(k_\delta, c+2, \delta).$$

Действительно, пусть $f_1^{(2)}(S), \dots, f_{k_2}^{(2)}(S); \dots; f_1^{(\delta)}(S), \dots, f_{k_\delta}^{(\delta)}(S)$ — группы инвариантов, которые мы только что описали, причем мы рассматриваем инварианты как функции гомоморфизмов группы Галуа заданного нам шольцева поля K . Рассмотрим гомоморфизмы типа $(s_1; t_1 | t_2)$. При этих гомоморфизмах инварианты первой группы имеют, согласно теореме 4, степень $\leq c+2$. Применим следствие из теоремы 3; мы получим, что у поля K существует подполе K^{S_1} , группа Галуа которого имеет

$$2 + C(k_3, c+2, 3) + \dots + C(k_\delta, c+2, \delta)$$

образующих и у которого, в свою очередь, существует подполе K^{T_1} , группа Галуа которого имеет две образующих и для которого все k_2 инвариантов первой группы обращаются в единицу.

Будем в дальнейшем рассматривать только поле K^{S_1} и на его группе Галуа — гомоморфизмы типа $(s_1, s_2; t_1, t_2 | t_3)$. При этих гомоморфизмах инварианты первой группы не меняются, т.е. остаются равными 1, а инварианты второй группы имеют, согласно теореме 4, степень $\leq c + 2$. Применяем опять следствие из теоремы 3 и получаем подполя K^{S_2} и K^{T_2} . Группа Галуа поля K^{S_2} имеет $3 + C(k_4, c + 2, 4) + \dots + C(k_\delta, c + 2, \delta)$ образующих. Группа Галуа поля K^{T_2} имеет три образующих. У поля K^{T_2} все инварианты первой и второй групп равны 1. Прделав таким образом δ шагов, мы придем к полю $K^{S_\delta} = K^{T_\delta}$, группа Галуа которого есть группа $\mathfrak{G}_\delta^{(c)}$ и у которого все инварианты равны 1. Теорема доказана.

Теорема 6. Над каждым полем алгебраических чисел существует расширение с наперед заданной группой Галуа порядка l^α .

Доказательство. Так как каждая группа класса c с d образующими является факторгруппой группы $\mathfrak{G}_d^{(c)}$, то нам достаточно доказать существование расширения с группой $\mathfrak{G}_d^{(c)}$. Рассмотрим отдельно два случая.

1. k содержит корень степени l из 1. Мы докажем даже существование шольцева расширения с группой $\mathfrak{G}_d^{(c)}$ и с l -взаимно простыми числами $\alpha_1, \dots, \alpha_d$. Доказательство проведем для любого числа образующих d индукцией по классу c . Нам надо доказать существование поля с указанными свойствами с группой $\mathfrak{G}_\delta^{(c)}$, причем мы можем предполагать построенным поле с теми же свойствами с группой $\mathfrak{G}_d^{(c-1)}$ с любым d . Возьмем $d = C(\delta)$, где $C(\delta)$ — число, существование которого установлено теоремой 5. Пусть K — шольцево поле с группой $\mathfrak{G}_d^{(c-1)}$, существование которого следует из индуктивного предположения. Согласно теореме 5, в нем существует подполе K^S с группой Галуа $\mathfrak{G}_\delta^{(c-1)}$, у которого все инварианты равны 1. Как подполе шольцева поля K , поле K^S — шольцево. Как было отмечено в п. 5 этого параграфа, у поля K^S все числа $\alpha_1, \dots, \alpha_\delta$ попарно l -взаимно просты. Ввиду следствия из теоремы 1, поле K^S может быть погружено в шольцево поле K_1 с группой Галуа $\mathfrak{G}_\delta^{(c)}$. Нам остается только доказать, что у поля K_1 числа $\alpha_1, \dots, \alpha_\delta$ попарно l -взаимно просты. Если $c > 1$, то это очевидно, так как они — те же самые, что и у поля K . Нам нужно, таким образом, рассмотреть только первый шаг индукции. В этом случае $K_1 = k(\sqrt[l]{\alpha_1}, \dots, \sqrt[l]{\alpha_\delta})$, причем, согласно доказательству следствия

из теоремы 1, это поле строится последовательным присоединением $\sqrt[l]{\alpha_i}$ к $k(\sqrt[l]{\alpha_1}, \dots, \sqrt[l]{\alpha_{i-1}})$ на основании теоремы 1. Остается только вспомнить, что при доказательстве теоремы 1 дивизор m (в нашем случае это и есть (α_i)) мог быть сделан взаимно простым с любым наперед заданным дивизором.

2. k не содержит корня степени l из 1. Мы будем пользоваться теми же обозначениями, которые были приняты при доказательстве теоремы 2. Как и в первом случае, мы докажем, что поле K_1 можно построить шольцевым и таким, чтобы у поля $\overline{K_1}$ числа $\overline{\alpha_1}, \dots, \overline{\alpha_\delta}$ были попарно l -взаимно просты. Доказательство снова будем вести индукцией по s и начнем с рассмотрения поля K , обладающего всеми этими свойствами и имеющего группу Галуа $\mathfrak{G}_d^{(c-1)}$ с $d = C(\delta)$. Согласно теореме 5, у поля $\overline{K}$ существует подполе $\overline{K}^S$ с нужными нам свойствами и всеми инвариантами, равными 1. Но легко видеть, что тогда в поле K существует такое подполе $K_0 = K^S$, что $\overline{K_0} = \overline{K}^S$. Ввиду теоремы 2, K_0 может быть погружено в шольцево поле K_1 с группой $\mathfrak{G}_d^{(c)}$. То, что у $\overline{K_1}$ числа $\alpha_1, \dots, \alpha_\delta$ можно выбрать попарно l -взаимно простыми, доказано нами при рассмотрении случая 1. Теорема доказана.

Поступило 13.XI.1953

ЛИТЕРАТУРА

1. Ван дер Ванден, *Современная алгебра, т. I*, Москва, 1947.
2. Курош А. Г., *Теория групп*, Москва, 1953.
3. Скопин А. И., *Факторгруппы одного верхнего центрального ряда*, Доклады Акад. наук СССР **LXXIV**, **3** (1950), 425–428.
4. Чеботарев Н. Г., *Основы теории Галуа, ч. II*, Москва, 1937.
5. Brauer R., *Über die Konstruktion der Schiefkörper, die von endlichem Rang in Bezug auf ein gegebenes Zentrum sind*, J. reine und angew. Math. **Bd. 168** (1932), 44–64.
6. Deuring M., *Neuer Beweis des Bauerschen Satzes*, J. reine und angew. Math. **Bd. 173** (1935), 1–4.
7. Hasse H., *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresbericht D.M.V.; **Bd. 35** (1926); **Bd. 36** (1927); **Erg.-Bd. 6** (1930).
8. Reichardt H., *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. reine und angew. Math. **Bd. 177** (1937), 1–5.
9. Scholz A., *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung*, I, Math. Zeitschrift **Bd. 42** (1936), 161–188.
10. Tannaka T., *Über die Konstruktion der Galoisschen Körper mit vorgegebener p -Gruppe*, Tôhoku Math. Journ. **v. 43** (1937), 252–260.
11. Witt E., *Der Existenzsatz für Abelsche Funktionenkörper*, J. reine und angew. Math. **Bd. 173** (1935), 43–51.

**ОБ ОДНОЙ ТЕОРЕМЕ
СУЩЕСТВОВАНИЯ В ТЕОРИИ
АЛГЕБРАИЧЕСКИХ ЧИСЕЛ**

ИЗВ. АКАД. НАУК СССР, СЕР.

МАТЕМ., 18 (1954), 327-334

В работе доказывается существование алгебраических чисел, для которых символы Лежандра по дивизорам, сопряженным с простыми делителями этих чисел, имеют заданные значения, и которые удовлетворяют некоторым другим условиям.

В некоторых задачах теории Галуа играют роль алгебраические числа, которые связаны теми или иными арифметическими соотношениями со своими сопряженными, например, для которых символы Лежандра по сопряженным с ними числам или по простым делителям сопряженных чисел имеют заданные значения.

Задачу подобного типа впервые рассмотрел Н. Г. Чеботарев [см. [1], стр. 164]. Именно он поставил вопрос о существовании примарных главных дивизоров π в нормальном поле K/k , для которых символ Лежандра $\left(\frac{\pi^{\sum u}}{\pi}\right)$ имеет наперед заданное значение. Здесь сумма в показателе распространена на все отличные от 1 автоморфизмы u поля K/k , символ Лежандра предполагается простой степени l и корни степени l из 1 содержатся в k .

Н. Г. Чеботарев показал [см. [1], стр. 226-234], что если K есть поле гауссовых чисел и $l = 2$, то символ Лежандра $\left(\frac{\pi^u}{\pi}\right)$ для примарного числа π равен 1, и поэтому поставленная им задача не всегда имеет положительное решение. С другой стороны, он показал, что во многих квадратичных полях эта задача разрешима. В дальнейшем мы воспользуемся соображениями, которые применял при этом Н. Г. Чеботарев [см. доказательство формулы (6)].

Задача, которой мы будем заниматься, отличается от задачи Н. В. Чеботарева. Мы исследуем вопрос о существовании алгебраических чисел α , для которых символ Лежандра $\left(\frac{\alpha}{p^u}\right)$ по дивизорам p^u , сопряженным с простыми делителями p числа α , имеет наперед заданное значение. Мы будем также требовать, чтобы α удовлетворяло некоторым другим условиям. Решение этой задачи необходимо для построения полей с разрешимой группой Галуа.

В дальнейшем будут применяться следующие обозначения: K/k — нормальное поле с группой Галуа F , l — такое простое число, что первообразный корень ζ степени l из 1 содержится в K , причем $\zeta^u = \zeta^{g(u)}$, $u \in F$, $q_1, \dots, q_r$ — дивизоры K , взаимно простые друг с другом и с l .

ТЕОРЕМА. Как бы ни были заданы корни степеней l из 1 $\xi_1, \dots, \xi_r$ и функция $\zeta(u)$ на F со значениями в группе корней степени l из 1, удовлетворяющая условию $\zeta(u^{-1}) = \zeta(u)^{g(u)}$, существует бесконечное количество чисел α поля K , удовлетворяющих условиям:

$$\left(\frac{\alpha}{q_i}\right) = \xi_i, \quad i = 1, \dots, r, \quad (1)$$

$$\left(\frac{\alpha}{p^u}\right) = \zeta(u) \quad \text{для всех простых } p|\alpha \text{ и } u \in F, u \neq 1. \quad (2)$$

Условие (2) предполагает, что если $p|\alpha$ и $u \neq 1$, то p^u не делит α .

При $l = 2$ мы должны наложить следующие дополнительные ограничения:

1'. $q_1, \dots, q_r$ взаимно просты с дискриминантом K/k .

2'. Все простые делители двойки в k полностью распадаются в K .

3'. Вещественные бесконечно удаленные простые дивизоры k остаются вещественными в K .

4'. Если u_i — инволютивные автоморфизмы ($u_i^2 = 1$), K_{u_i} — принадлежащие им подполя и $\mathfrak{D}_{u_i}$ — дифференты K/K_{u_i} , то из того, что $\mathfrak{D}_{u_1} \dots \mathfrak{D}_{u_m}$ есть квадрат дивизора K , следует, что

$$\zeta(u_1) \dots \zeta(u_m) = 1.$$

Доказательство распадается на две части, в зависимости от того, нечетно ли l или $l = 2$.

I случай. Пусть $l \neq 2$. Мы докажем, что α можно выбрать в виде произведения двух простых главных дивизоров абсолютно первого порядка. Для этого построим в K последовательность простых l -гиперпримарных главных дивизоров $\pi_1, \dots, \pi_t, \dots$, имеющих абсолютный порядок 1, не делящих l и удовлетворяющих условию:

$$\left(\frac{\pi_t}{q_i}\right) = \xi_i^{\frac{1}{2}}. \quad (3)$$

Показатель $\frac{1}{2}$ имеет здесь смысл виду того, что $l \neq 2$.

Указанные условия мы будем предполагать выполненными для всех членов последовательности, в остальном же строим ее рекуррентно, выбирая π_t при построенных $\pi_1, \dots, \pi_{t-1}$ так, чтобы было выполнено условие:

$$\left(\frac{\pi_t}{\pi_s^u}\right) = \left(\frac{\pi_s}{\pi_s^u}\right)^{-1} \zeta(u), \quad s = 1, 2, \dots, t-1. \quad (4)$$

Условия (3) и (4), наложенные на число π_t , предписывают значения символа Лежандра числа π_t по взаимно простым дивизорам $q_1, \dots, q_r, (\pi_1), \dots, (\pi_{t-1})$ [в условии (3) подразумевается, что $(\pi_t, q_i) = 1$]. Ввиду обобщенной теоремы об арифметической прогрессии, существует простой главный дивизор π_t , удовлетворяющий всем поставленным нами условиям. Таким образом, мы можем продолжить последовательность $\pi_1, \dots, \pi_t$ сколь угодно далеко.

Так как для любого числа π выражения $\left(\frac{\pi}{\pi^u}\right)$ могут принимать лишь конечное число значений (не больше, чем l^n , $n = (K : k)$), то при достаточно большом числе членов в нашей последовательности найдутся два таких числа, скажем, π_s и π_t ($s < t$), что

$$\left(\frac{\pi_s}{\pi_s^u}\right) = \left(\frac{\pi_t}{\pi_t^u}\right) \quad \text{для всех } u \in F, \quad u \neq 1. \quad (5)$$

Докажем, что число $\alpha = \pi_s \pi_t$ удовлетворяет условиям теоремы. Очевидно, что из условия (3) для π_s и π_t следует условие (1) для α . Условие (2) для α имеет теперь вид:

$$\left(\frac{\pi_s \pi_t}{\pi_s^u}\right) = \zeta(u), \quad \left(\frac{\pi_s \pi_t}{\pi_t^u}\right) = \zeta(u).$$

Первое из них выполнено ввиду условия (4), наложенного на π_t . Нам остается доказать, что выполнено и второе условие. Для этого заметим, что

$$\left(\frac{\pi_t}{\pi_s^u}\right) = \left(\frac{\pi^{u^{-1}}}{\pi_s}\right)^{g(u^{-1})} = \left(\frac{\pi_s}{\pi_t^{u^{-1}}}\right)^{g(u^{-1})}$$

и точно так же, ввиду (5),

$$\left(\frac{\pi_s}{\pi_s^u}\right) = \left(\frac{\pi_s^{u^{-1}}}{\pi_s}\right)^{g(u^{-1})} = \left(\frac{\pi_s}{\pi_s^{u^{-1}}}\right)^{g(u^{-1})} = \left(\frac{\pi_t}{\pi_t^{u^{-1}}}\right)^{g(u^{-1})}.$$

Следовательно,

$$\begin{aligned} \left(\frac{\pi_s \pi_t}{\pi_s^u}\right) &= \left(\frac{\pi_s}{\pi_t^{u^{-1}}}\right)^{g(u^{-1})} \left(\frac{\pi_t}{\pi_t^{u^{-1}}}\right)^{g(u^{-1})} \\ &= \left(\frac{\pi_s \pi_t}{\pi_t^{u^{-1}}}\right)^{g(u^{-1})} = \zeta(u^{-1})^{g(u^{-1})} = \zeta(u). \end{aligned}$$

Таким образом, в этом случае теорема доказана.

II случай. Пусть $l = 2$. К сожалению, в этом случае доказательство значительно более громоздко ввиду того, что мы не можем наложить условие (3) (показатель $\frac{1}{2}$ теряет смысл), а поэтому нельзя считать, что α состоит из двух множителей. Мы покажем, однако, что можно найти нужное нам число α , состоящее из трех множителей. Предположим сначала, что u есть инволютивный автоморфизм: $u^2 = 1$. В этом случае можно найти такое простое гиперпримарное число π , что

$$\left(\frac{\pi}{\pi^u}\right) = \zeta(u).$$

В самом деле, пусть K_u есть подполе элементов, инвариантных относительно u , $K = K_u(\sqrt{\Delta_u})$ и $\mathfrak{D}_u$ — дифферента K/K_u . Докажем, что для любого гиперпримарного тотально-положительного ξ имеет место соотношение:

$$\left(\frac{\xi}{\xi^u}\right) = \left(\frac{\xi}{\mathfrak{D}_u}\right), \quad \text{если} \quad (\xi, \xi^u) = 1. \quad (6)$$

Пусть $\xi = \alpha + \beta\sqrt{\Delta_u}$. Так как $\xi + \xi^u = 2\alpha$ и ξ^u гиперпримарно, то

$$\left(\frac{\xi}{\xi^u}\right) = \left(\frac{\xi + \xi^u}{\xi^u}\right) = \left(\frac{2\alpha}{\xi^u}\right) = \left(\frac{\alpha}{\xi^u}\right) = \left(\frac{\xi^u}{\alpha}\right).$$

Может случиться, что α имеет общие множители с двойкой. В случае, если числитель символа Лежандра гиперпримарен, а знаменатель имеет общие множители с двойкой, мы будем вычислять символ Лежандра при помощи соотношения:

$$\left(\frac{\nu}{l}\right) = 1, \quad \text{если} \quad \nu \text{ гиперпримарно, } l \nmid 2.$$

Как легко видеть, закон взаимности при этом сохраняет свою силу.

Мы имеем, далее:

$$\begin{aligned}\left(\frac{\xi^u}{\alpha}\right) &= \left(\frac{\alpha - \beta\sqrt{\Delta_u}}{\alpha}\right) = \left(\frac{-\beta\sqrt{\Delta_u}}{\alpha}\right) \\ &= \left(\frac{-\beta}{\alpha}\right) \left(\frac{\sqrt{\Delta_u}}{\alpha}\right) = \left(\frac{\sqrt{\Delta_u}}{\alpha}\right).\end{aligned}$$

По поводу этих равенств мы должны прежде всего заметить, что α взаимно просто с ξ^u , так как $2\alpha = \xi + \xi^u$ и $(\xi, \xi^u) = 1$. Во вторых, символ $\left(\frac{-\beta}{\alpha}\right)$ в поле K равен, ввиду того, что $\alpha \in K_u$, символу $\left(\frac{\beta^2}{\alpha}\right)$ в поле K_u , т.е. единице. Аналогичным образом имеем:

$$\left(\frac{\sqrt{\Delta_u}}{\alpha}\right) = \left(\frac{\Delta_u}{\alpha}\right),$$

где левый символ вычисляется в K , а правый в K_u .

Ввиду условия $2'$, Δ_u должно быть гиперпримарным и тотально-положительным. Таким образом,

$$\left(\frac{\Delta_u}{\alpha}\right) = \left(\frac{\alpha}{\Delta_u}\right) = \left(\frac{\alpha}{\sqrt{\Delta_u}}\right),$$

где последний символ опять вычисляется в K .

Если $\mathfrak{D}_u$ — дифферента K/K_u , то

$$(\sqrt{\Delta_u}) = \mathfrak{D}_u \mathfrak{C}, \quad \mathfrak{C} \in K_u,$$

$$\left(\frac{\alpha}{\sqrt{\Delta_u}}\right) = \left(\frac{\alpha}{\mathfrak{C}}\right) \left(\frac{\alpha}{\mathfrak{D}_u}\right) = \left(\frac{\alpha}{\mathfrak{D}_u}\right),$$

так как опять

$$\left(\frac{\alpha}{\mathfrak{C}}\right)_K = \left(\frac{\alpha^2}{\mathfrak{C}}\right)_{K_u} = 1.$$

Таким образом,

$$\left(\frac{\xi}{\xi^u}\right) = \left(\frac{\alpha}{\mathfrak{D}_u}\right).$$

Аналогично проверяем, что

$$\left(\frac{\xi}{\mathfrak{D}_u}\right) = \left(\frac{\alpha + \beta\sqrt{\Delta_u}}{\mathfrak{D}_u}\right) = \left(\frac{\alpha}{\mathfrak{D}_u}\right),$$

что и доказывает формулу (6).

Условие 4' и обобщенная теорема об арифметической прогрессии гарантирует нам существование таких простых гиперпримарных totally-положительных π , что

$$\left(\frac{\pi}{\mathfrak{D}_u}\right) = \zeta(u)$$

для любого инволютивного автоморфизма. Ввиду формулы (6), получаем:

$$\left(\frac{\pi}{\pi^u}\right) = \zeta(u)$$

Теперь мы переходим к рассмотрению также и неинволютивных автоморфизмов. Пусть $v^2 \neq 1$, т. е. $v \neq v^{-1}$. Предположим, что мы нашли три простых гиперпримарных и totally-положительных числа π , $\varkappa$ и ρ , удовлетворяющих следующим условиям:

$$\left. \begin{aligned} \left(\frac{\pi}{\varkappa^v}\right) &= 1, & \left(\frac{\pi}{\varkappa^{v^{-1}}}\right) &= \left(\frac{\varkappa}{\varkappa^v}\right) \zeta(v), \\ \left(\frac{\pi}{\rho^v}\right) &= \left(\frac{\rho}{\rho^v}\right) \zeta(v), & \left(\frac{\pi}{\rho^{v^{-1}}}\right) &= 1, \\ \left(\frac{\varkappa}{\rho^v}\right) &= 1, & \left(\frac{\varkappa}{\rho^{v^{-1}}}\right) &= \left(\frac{\rho}{\rho^v}\right) \zeta(v), \\ \left(\frac{\pi}{\pi^v}\right) &= \left(\frac{\varkappa}{\varkappa^v}\right) = \left(\frac{\rho}{\rho^v}\right). \end{aligned} \right\} \quad (7)$$

Докажем, что тогда число $\alpha = \pi \varkappa \rho$ удовлетворяет условиям:

$$\left(\frac{\alpha}{\pi^v}\right) = \left(\frac{\alpha}{\varkappa^v}\right) = \left(\frac{\alpha}{\rho^v}\right) = \zeta(v). \quad (8)$$

В самом деле,

$$\left(\frac{\alpha}{\pi^v}\right) = \left(\frac{\pi \varkappa \rho}{\pi^v}\right) = \left(\frac{\pi}{\pi^v}\right) \left(\frac{\varkappa}{\pi^v}\right) \left(\frac{\rho}{\pi^v}\right).$$

Так как

$$\begin{aligned} \left(\frac{\varkappa}{\pi^v}\right) &= \left(\frac{\varkappa^{v^{-1}}}{\pi}\right) = \left(\frac{\pi}{\varkappa^{v^{-1}}}\right) = \left(\frac{\varkappa}{\varkappa^v}\right) \zeta(v), \\ \left(\frac{\rho}{\pi^v}\right) &= \left(\frac{\rho^{v^{-1}}}{\pi}\right) = \left(\frac{\pi}{\rho^{v^{-1}}}\right) = 1, \\ \left(\frac{\pi}{\pi^v}\right) &= \left(\frac{\varkappa}{\varkappa^v}\right), \end{aligned}$$

то

$$\left(\frac{\alpha}{\pi^v}\right) = \left(\frac{\varkappa}{\varkappa^v}\right) \left(\frac{\varkappa}{\varkappa^v}\right) \zeta(v) = \zeta(v).$$

Точно так же

$$\begin{aligned} \left(\frac{\alpha}{\varkappa^v}\right) &= \left(\frac{\pi}{\pi^v}\right) \left(\frac{\varkappa}{\varkappa^v}\right) \left(\frac{\rho}{\rho^v}\right) = \left(\frac{\varkappa}{\varkappa^v}\right) \left(\frac{\rho}{\rho^v}\right) \zeta(v) = \zeta(v), \\ \left(\frac{\alpha}{\rho^v}\right) &= \left(\frac{\pi}{\rho^v}\right) \left(\frac{\varkappa}{\rho^v}\right) \left(\frac{\rho}{\rho^v}\right) = \left(\frac{\rho}{\rho^v}\right)^2 \zeta(v) = \zeta(v). \end{aligned}$$

Аналогично проверяется, что

$$\left(\frac{\alpha}{\pi^{v-1}}\right) = \zeta(v), \quad \left(\frac{\alpha}{\varkappa^{v-1}}\right) = \zeta(v), \quad \left(\frac{\alpha}{\rho^{v-1}}\right) = \zeta(v). \quad (9)$$

Мы проверим только первое равенство:

$$\left(\frac{\alpha}{\pi^{v-1}}\right) = \left(\frac{\pi}{\pi^{v-1}}\right) \left(\frac{\varkappa}{\pi^{v-1}}\right) \left(\frac{\rho}{\pi^{v-1}}\right).$$

Так как

$$\begin{aligned} \left(\frac{\pi}{\pi^{v-1}}\right) &= \left(\frac{\pi^v}{\pi}\right) = \left(\frac{\pi}{\pi^v}\right) = \left(\frac{\rho}{\rho^v}\right), \\ \left(\frac{\varkappa}{\pi^{v-1}}\right) &= \left(\frac{\varkappa^v}{\pi}\right) = \left(\frac{\pi}{\varkappa^v}\right) = 1, \\ \left(\frac{\rho}{\pi^{v-1}}\right) &= \left(\frac{\rho^v}{\pi}\right) = \left(\frac{\pi}{\rho^v}\right) = \left(\frac{\rho}{\rho^v}\right) \zeta(v), \end{aligned}$$

то

$$\left(\frac{\alpha}{\pi^{v-1}}\right) = \left(\frac{\rho}{\rho^v}\right)^2 \zeta(v) = 1.$$

Разобьем теперь совокупность всех отличных от 1 автоморфизмов K/k на три части. В первую часть, которую мы обозначим через U , соберем все инволютивные автоморфизмы. Неинволютивные автоморфизмы разобьем на две части, относя по произволу из каждой пары взаимно обратных автоморфизмов v и v^{-1} один к одной части, а другой автоморфизм – к другой. Эти части обозначим через V и V^{-1} . Таким образом,

$$F = 1 + U + V + V^{-1}$$

Теперь, как мы это делали при нечетном l , построим последовательность простых гиперпримарных и totally-положительных чисел $\pi_1, \dots, \pi_t, \dots$. Мы будем считать, что все числа π_t удовлетворяют условиям:

$$\begin{aligned} \left(\frac{\pi_t}{q_i} \right) &= \xi_i, \quad i = 1, \dots, r, \\ \left(\frac{\pi_t}{\mathfrak{D}_u} \right) &= \zeta(u), \quad u \in U. \end{aligned}$$

В остальном мы будем строить нашу последовательность рекуррентно по следующему, довольно сложному, правилу. Пусть построены числа $\pi_1, \dots, \pi_{t-1}$. Разобьем их совокупность на две части, которые будем называть первой и второй. Каким именно образом будет производиться разбиение на эти две части, будет указано несколько позже. Теперь выберем π_t так, чтобы, кроме указанных выше условий, оно удовлетворяло еще следующим:

$$\begin{aligned} \left(\frac{\pi_t}{\pi_s^u} \right) &= 1, \quad u \in U, \\ \left(\frac{\pi_t}{\pi_s^v} \right) &= 1, \quad \left(\frac{\pi_t}{\pi_s^{v-1}} \right) = \left(\frac{\pi_s}{\pi_s^v} \right) \zeta(v), \end{aligned}$$

если $v \in V$ и π_s принадлежит первой части, и

$$\left(\frac{\pi_t}{\pi_s^v} \right) = \left(\frac{\pi_s}{\pi_s^v} \right) \zeta(v), \quad \left(\frac{\pi_t}{\pi_s^{v-1}} \right) = 1,$$

если $v \in V$, но π_s принадлежит второй части.

Предположим, что мы определили разбиение на первую и вторую части так, что выполнено следующее условие: каково бы ни было натуральное число N , существует такое M , что при любом разбиении последовательности $\pi_1, \dots, \pi_M$ на N частей хотя бы в одну часть попадут три числа π_r, π_s, π_t ($r < s < t$) со следующим свойством: при разбиении последовательности $\pi_1, \dots, \pi_{t-1}$ на первую и вторую части π_r и π_s попали в разные части, а при разбиении последовательности $\pi_1, \dots, \pi_{s-1}$ π_r попало не в ту часть, в которую оно попало при разбиении последовательности $\pi_1, \dots, \pi_{t-1}$. В этом случае наша задача решена.

Действительно, обозначим через v число элементов множества v и возьмем 2^v за N . В качестве разбиения на N частей возьмем разбиение сообразно значениям $\left(\frac{\pi_i}{\pi_i^v} \right)$, $v \in V$, объединяя в одну часть

все π_i , для которых все $\left(\frac{\pi_i}{\pi_i^v}\right)$, одинаковы. Пусть π_r, π_s, π_t — числа, удовлетворяющие изложенным выше условиям. Если мы примем их за π, κ и ρ , то условия (7) будут выполнены. Действительно, если при разбиении последовательности $\pi_1, \dots, \pi_{t-1}$ на две части π_s принадлежит к первой части, а π_r — ко второй, то условия (7) удовлетворяются, если мы положим $\pi_t = \pi, \pi_s = \kappa, \pi_r = \rho$. Если же π_s принадлежит ко второй части, а π_r — к первой, то надо положить $\pi_t = \pi, \pi_s = \rho, \pi_r = \kappa$.

Нам остается только указать, как производить разбиение на первую и вторую части. Возможность такого разбиения устанавливается следующей, чисто комбинаторной, леммой.

ЛЕММА. Для каждого натурального числа t можно указать такое разбиение чисел $1, 2, \dots, t-1$ на две части — первую и вторую, — чтобы для любого натурального N существовало M со следующими свойствами: при произвольном разбиении чисел $1, 2, \dots, M$ на N частей хотя бы в одной части найдутся такие три числа r, s и t , ($r < s < t$), что при разбиении чисел $1, 2, \dots, t-1$ на две части r и s попадают в разные части, а при разбиении $1, 2, \dots, s-1$ на две части r попадает не в ту часть, в которую оно попадает при разбиении чисел $1, 2, \dots, t-1$.

Решение этой задачи заключается в следующем. При разбиении чисел $1, 2, \dots, t-1$ на две части надо в первую часть относить все числа k , для которых $t-k$ делится на нечетную степень двойки, а остальные — во вторую.

Чтобы доказать, что при этом будет выполняться нужное нам свойство, мы применим теорему Ван дер Вардена об арифметических прогрессиях [см. [2]] для частного случая прогрессий длины три. Согласно утверждению этой теоремы, для любого N существует такое M , что при любом разбиении чисел $1, 2, \dots, M$ на N частей хотя бы в одной части найдутся три числа, образующие арифметическую прогрессию. Чтобы вывести из этого утверждения нужный нам результат, нам остается только проверить, что при указанном разбиении на первую и вторую части любые три числа r, s и t , образующие арифметическую прогрессию, будут удовлетворять нашим условиям. Это почти очевидно.

По предположению, $t-s = s-r$. Пусть $t-s$ делится на нечетную степень двойки. Тогда при разбиении чисел $1, 2, \dots, t-1$ на две части s попадает в первую часть. Так как

$$t-r = (t-s) + (s-r) = 2(t-s),$$

то $t-r$ делится на четную степень двойки, и поэтому r попадает во вторую часть. При разбиении чисел $1, 2, \dots, s-1$ r попадает,

очевидно, в первую часть. Если $t - s$ делится на четную степень двойки, то это рассуждение нужно дословно повторить. Лемма доказана.

Возвращаясь к доказательству теоремы, мы видим, что если положить

$$\pi = \pi_t, \quad \varkappa = \pi_s, \quad \rho = \pi_r, \quad \alpha = \pi \varkappa \rho,$$

то для α будут выполняться условия (8) и (9) для любого $v \in V$, т. е. условия (8) для любого неинволютивного автоморфизма v .

Аналогичные условия

$$\left(\frac{\alpha}{\pi^u}\right) = \left(\frac{\alpha}{\varkappa^u}\right) = \left(\frac{\alpha}{\rho^u}\right) = \zeta(u) \quad (10)$$

будут выполнены также и для любого инволютивного автоморфизма u . В самом деле, по построению,

$$\left(\frac{\pi_i}{\pi_j^u}\right) = 1 \quad \text{при} \quad i \neq j \quad \text{и} \quad \left(\frac{\pi_i}{\mathfrak{D}_u}\right) = \zeta(u),$$

т. е., согласно (6), $\left(\frac{\pi_i}{\pi_i^u}\right) = \zeta(u)$. Таким образом,

$$\left(\frac{\alpha}{\pi^u}\right) = \left(\frac{\pi}{\pi^u}\right) \left(\frac{\varkappa}{\pi^u}\right) \left(\frac{\rho}{\pi^u}\right) = \left(\frac{\pi}{\pi^u}\right) = \zeta(u).$$

Аналогично проверяются два других соотношения (10). Таким образом, для числа α выполнены все условия (2). Но и условия (1) также выполнены, так как, по построению,

$$\left(\frac{\pi}{\mathfrak{q}_i}\right) = \left(\frac{\varkappa}{\mathfrak{q}_i}\right) = \left(\frac{\rho}{\mathfrak{q}_i}\right) = \xi_i \quad \text{и} \quad \left(\frac{\alpha}{\mathfrak{q}_i}\right) = \xi_i^3 = \xi_i.$$

Мы доказали существование одного числа α , удовлетворяющего условиям теоремы. Так как мы можем, однако, при построении выбирать все π_i , а следовательно, и α взаимно простыми с любым наперед заданным модулем, то таких чисел α существует бесконечно много. Теорема доказана.

Заметим, что при построении последовательности простых чисел $\pi_1, \dots, \pi_t, \dots$ имеется большой произвол, которым можно в случае необходимости воспользоваться. Например, если задано какое-либо нормальное поле Ω/K , то мы можем выбрать π_t так, чтобы все они принадлежали в Ω к заданному классу автоморфизмов σ :

$$\left[\frac{\Omega}{\pi_t}\right] = \sigma.$$

При этом нужно только, чтобы существовало бесконечное количество простых примарных чисел π , принадлежащих к классу σ в Ω и удовлетворяющих наложенным нами условиям:

$$\left(\frac{\pi}{q_i}\right) = \xi_i^{\frac{1}{2}} \quad \text{при } l \neq 2 \quad \text{или} \quad \left(\frac{\pi}{q_i}\right) = \xi_i \quad \text{при } l = 2.$$

(Поступило 11.III.1954 г.)

ЛИТЕРАТУРА

1. Чеботарев Н. Г., *Собрание сочинений, т. 1*, М.-Л., 1949.
2. Хинчин А. Я., *Три жемчужины теории чисел*, М.-Л., 1948.

О ЗАДАЧЕ ПОГРУЖЕНИЯ ПОЛЕЙ

ИЗВ. АКАД. НАУК СССР, СЕР. МАТЕМ., 18 (1954), 389-418

В работе исследуется вопрос о погружении нормального поля алгебраических чисел в большее поле в случае, когда относительная группа Галуа имеет порядок l^α , а абсолютная группа является распадающимся расширением.

Введение

Задача погружения полей заключается в следующем. Даны нормальное расширение k/Ω с группой Галуа F и группа G , имеющая нормальный делитель $\mathfrak{G}$ с $G/\mathfrak{G} \cong F$. Требуется узнать, когда существует такое поле $K \supset k$, нормальное над Ω , что его группа Галуа над Ω есть G , а гомоморфизм G на F совпадает с естественным гомоморфизмом группы Галуа поля на группу Галуа подполя.

Простейший случай этой задачи возникает, когда G является распадающимся расширением F при помощи $\mathfrak{G}$. В этом случае G определяется тем, какие автоморфизмы индуцируют элементы F в $\mathfrak{G}$, т. е. заданием $\mathfrak{G}$ как операторной группы с группой операторов F . Наоборот, для любой группы $\mathfrak{G}$ с группой операторов F существует группа G , являющаяся распадающимся расширением F при помощи $\mathfrak{G}$. Это расширение называется полупрямым произведением F на $\mathfrak{G}$. Мы будем обозначать его через $F \cdot \mathfrak{G}$ в отличие от прямого произведения, которое будет для групп A и B обозначаться через $A \times B$.

В настоящей работе рассматривается задача погружения для случая, когда G есть полупрямое произведение $F \cdot \mathfrak{G}$.

Для случая, когда группа $\mathfrak{G}$ коммутативна, задача погружения для полупрямого произведения была полностью решена Шольцем [7], который показал, что в этом случае искомое поле K всегда существует.

Мы рассмотрим в настоящей работе следующий по трудности случай, когда $\mathfrak{G}$ имеет порядок l^α . Доказывается, что здесь, как

и для коммутативной группы $\mathfrak{G}$, задача решается положительно в любом из следующих двух случаев:

- 1) группа $\mathfrak{G}$ имеет класс c и $l > c$;
- 2) порядки групп F и $\mathfrak{G}$ взаимно просты.

Очевидно, что рассмотренный Шольцем случай коммутативной группы $\mathfrak{G}$ содержится в случае 1), так как для абелевой группы $c = 1$.

Как полученные результаты, так и методы их доказательства делают весьма вероятным, что проблема погружения решается положительно для любого полупрямого произведения и любого нильпотентного нормального делителя $\mathfrak{G}$.

В большей части настоящей работы (§2 и 3) предполагается, что читатель знаком с работой [4]. В частности, введенные в этой работе понятия будут использоваться без дальнейших ссылок.

§1. Расширения с нильпотентной диспозиционной группой

1. Нильпотентные диспозиционные группы. Рассмотрим конечную группу G с конечной группой операторов F . Если G есть абелева группа, то, как показал Шольц [7], G является операторно-гомоморфным образом некоторой сравнительно просто построенной абелевой операторной группы, называемой диспозиционной. Мы покажем, что понятие диспозиционной группы можно обобщить на случай, когда G есть произвольная группа порядка l^α .

Обозначим через $\mathfrak{G}_d^{(c)}$ группу с образующими $s_1, \dots, s_d$, на которые наложим соотношения:

- 1) при некотором, раз навсегда фиксированном k

$$s_i^{l^k} = 1, \quad i = 1, \dots, d;$$

- 2) любой коммутатор длины c , составленный из образующих $s_1, \dots, s_d$, равен 1.

Другими словами, $\mathfrak{G}_d^{(c)}$ есть факторгруппа свободного произведения d циклических групп порядка l^k по c -му члену убывающего центрального ряда. Из теоремы Шрейера о подгруппах свободной группы легко вытекает, что $\mathfrak{G}_d^{(c)}$ есть конечная группа. Порядок $\mathfrak{G}_d^{(c)}$ есть некоторая степень l , число образующих — d и класс c .

Пусть F — произвольная конечная группа порядка m . Рассмотрим группу $\mathfrak{G}_{md}^{(c)}$ с md образующими, которые будем обозначать через $s_{u,i}$, $u \in F$, $i = 1, \dots, d$. Отображение, определенное для образующих $s_{u,i}$ условием

$$s_{u,i}^v = s_{uv,i},$$

распространяется на всю группу $\mathfrak{G}_{md}^{(c)}$ и является в ней автоморфизмом, так как все соотношения, наложенные на образующие $s_{u,i}$, в $\mathfrak{G}_{md}^{(c)}$ инвариантны относительно перестановок образующих. Определенные таким образом автоморфизмы образуют группу, изоморфную F^* . Группу $\mathfrak{G}_{md}^{(c)}$ с указанной группой операторов, изоморфной F , обозначим через $\mathfrak{G}_{d,F}^{(c)}$ и будем называть нильпотентной диспозиционной группой. В случае, если $c = 1$, мы получаем абелевы диспозиционные группы Шольца.

Обобщением основного результата Шольца об абелевых диспозиционных группах на нильпотентные диспозиционные группы является следующая теорема:

ТЕОРЕМА 1. Любая группа G порядка l^α класса c с группой операторов F является операторно-гомоморфным образом некоторой нильпотентной диспозиционной группы $\mathfrak{G}_{d,F}^{(c)}$.

Доказательство. Пусть группа G имеет d образующих $s_1, \dots, s_d$, и пусть максимальный порядок ее элемента — l^k . Докажем, что G является операторно-гомоморфным образом группы $\mathfrak{G}_{d,F}^{(c)}$. Для этого продолжим отображение

$$\varphi(s_{u,i}) = s_i^u$$

образующих $\mathfrak{G}_{d,F}^{(c)}$ на образующие G по мультипликативности на все элементы $\mathfrak{G}_{d,F}^{(c)}$. Так как все соотношения, имеющие место в $\mathfrak{G}_{d,F}^{(c)}$ между образующими $s_{u,i}$, справедливы для любых элементов G , то φ является гомоморфизмом $\mathfrak{G}_{d,F}^{(c)}$ на G . Нам остается доказать, что этот гомоморфизм операторный, т. е. что имеет место соотношение:

$$\varphi(\sigma^v) = \varphi(\sigma)^v, \quad \sigma \in \mathfrak{G}_{d,F}^{(c)}, \quad v \in F. \quad (1)$$

Ввиду того, что φ является гомоморфизмом, это соотношение достаточно проверить для $\sigma = s_{u,i}$. В этом случае мы имеем:

$$\varphi(s_{u,i}^v) = \varphi(s_{uv,i}) = s_i^{uv},$$

$$\varphi(s_{u,i})^v = (s_i^u)^v = s_i^{uv},$$

чем и доказывается соотношение (1), а тем самым и теорема.

*Мы будем исходить из определения умножения операторов при том порядке следования, который принят в [3], стр. 97.

2. Центральнo-диспозиционные группы. Мы будем называть группу G порядка l^a с группой операторов F центрально-диспозиционной, если ее центр является диспозиционной группой. Таким образом, центр группы G должен иметь следующую структуру: он должен распадаться в прямое произведение допустимых подгрупп, каждая из которых должна являться прямым произведением m сопряженных относительно F циклических подгрупп. Очевидно, что понятия центрально-диспозиционной группы и нильпотентной диспозиционной группы совпадают для абелевых групп, но, как мы увидим дальше, неабелевы нильпотентные диспозиционные группы не являются, вообще говоря, центрально-диспозиционными.

ТЕОРЕМА 2. Любая группа G порядка l^a и класса c с группой операторов F при $l > c$ является операторно-гомоморфным образом некоторой центрально-диспозиционной абелевой группы.

Доказательство. Ввиду теоремы 1, нам достаточно доказать теорему для случая, когда $G = \mathfrak{G}_{d,F}^{(c)}$ и $l < c$. Центр группы $\mathfrak{G}_{d,F}^{(c)}$ в случае $l > c$ определен Трэллом [8]. Из его рассуждений следует, что центр группы $\mathfrak{G}_d^{(c)}$ при $l > c$ изоморфен (аддитивно записанному) модулю многочленов Ли от d неизвестных $x_1, \dots, x_d$ с коэффициентами из кольца классов вычетов по модулю l^k . Известные $x_1, \dots, x_d$ находятся при этом во взаимно однозначном соответствии с образующими $s_1, \dots, s_d$ группы $\mathfrak{G}_d^{(c)}$, и автоморфизм $\mathfrak{G}_d^{(c)}$, сводящийся к перестановке образующих $s_1, \dots, s_d$, индуцирует в центре такую же перестановку неизвестных $x_1, \dots, x_d$.

В случае группы $\mathfrak{G}_{d,F}^{(c)}$ мы имеем модуль многочленов Ли степени c от неизвестных $x_{u,i}$ с коэффициентами из кольца классов вычетов по модулю l^k . Преобразование неизвестных

$$x_{u,i}^v = x_{uv,i} \quad (2)$$

определяет автоморфизм модуля многочленов Ли. Модуль многочленов Ли степени c с группой операторов, определенной формулами (2) и изоморфной F , обозначим через $\Lambda(F)$.

Введем в рассмотрение модуль полилинейных форм от c md -мерных векторов $\xi^{(j)}$, $j = 1, \dots, c$, где $\xi^{(j)}$ есть вектор с координатами $x_{u,i}^{(j)}$, $u \in F$, $i = 1, \dots, d$.

Определим действие элементов F на элементы модуля формулами

$$x_{u,i}^{(j)v} = x_{uv,i}^{(j)}.$$

Этот операторный модуль обозначим через $M(F)$.

Доказательство теоремы 2 непосредственно вытекает из следующих двух предложений:

А) $\Lambda(F)$ является операторным прямым слагаемым $M(F)$, т. е. в $M(F)$ существуют такой F -инвариантный подмодуль $\Lambda'(F)$, операторно-изоморфный $\Lambda(F)$, и такой F -инвариантный подмодуль $N(F)$, что

$$M(F) = \Lambda'(F) + N(F). \quad (3)$$

В) $M(F)$ является диспозиционной группой.

Покажем прежде всего, что из предположений А) и В) следует утверждение теоремы 2. Рассмотрим прямое произведение группы $\mathfrak{G}_{d,F}^{(c)}$ и группы $\mathfrak{N}$, операторно-изоморфной $N(F)$. Центр группы $\mathfrak{G}_{d,F}^{(c)} \times \mathfrak{N}$ операторно-изоморфен $M(F)$ ввиду предположения А) и является, следовательно, диспозиционной группой ввиду предположения В). Таким образом, $\mathfrak{G}_{d,F}^{(c)} \times \mathfrak{N}$ есть центрально-диспозиционная группа, а так как $\mathfrak{G}_{d,F}^{(c)}$ является ее операторно-гомоморфным образом, то из этого следует теорема 2.

Перейдем к доказательству предложений А) и В).

Доказательство предложения А). Мы воспользуемся соображениями, примененными Трэллом [8] к исследованию групп $\mathfrak{G}_d^{(c)}$. Если вместо преобразований (2) рассмотреть любые обратимые линейные преобразования md неизвестных $x_{u,i}$ с коэффициентами из кольца классов вычетов по модулю l^k , то как модуль Λ многочленов Ли, так и модуль M полилинейных форм станет операторным модулем относительно группы $\mathfrak{A}$ всех обратимых линейных преобразований по модулю l^k . Формулы (2) определяют изоморфное отображение F в $\mathfrak{A}$. Таким образом, переход от F к $\mathfrak{A}$ приводит к увеличению группы операторов, так что нам достаточно доказать существование разложения (3) для модулей Λ и M относительно области операторов $\mathfrak{A}$. Ввиду этого мы будем считать, что Λ имеет n образующих (в нашем применении $n = md$) $x_1, \dots, x_n$, а M состоит из форм от n -мерных векторов $x^{(j)}$ с координатами $x_1^{(j)}, \dots, x_n^{(j)}$.

Так как и Λ и M являются модулями над кольцом классов вычетов по модулю l^k , то действие в них операторов из $\mathfrak{A}$ определяет представление $\mathfrak{A}$ по модулю l^k . Представление, определяемое модулем Λ , называется s -м тензорным представлением.

Прежде всего ясно, что Λ является операторно-гомоморфным образом модуля M . Гомоморфизм задается отображением

$$x_{i_1}^{(1)} x_{i_2}^{(2)} \dots x_{i_c}^{(c)} \rightarrow [x_{i_1} x_{i_2} \dots x_{i_c}],$$

где $[x_{i_1} \dots x_{i_c}]$ обозначает произведение $(\dots (x_{i_1} x_{i_2}) \dots x_{i_c})$ в кольце Ли.

Над полем характеристики 0 тензорное представление полной линейной группы вполне приводимо [см. [2], стр. 177], так что представление Ли содержится в нем в виде прямого слагаемого. Как заметил Брауэр [6], формулы, по которым s -тензорное представление полной линейной группы над полем характеристики 0 разлагается в прямую сумму неприводимых, содержат в знаменателях только числа $\leq c$ и, таким образом, могут быть применены для аналогичного разложения над кольцом классов вычетов по модулю l^k , если $l > c$. Ввиду вышесказанного из этого следует, что при $l > c$ s -е представление Ли содержится прямым слагаемым в s -м тензорном представлении, т. е. модуль Λ является прямым слагаемым модуля M , что и доказывает предложение А).

Доказательство предложения В). Базисом модуля M являются одночлены $x_{u_1, i_1}^{(1)} x_{u_2, i_2}^{(2)} \dots x_{u_c, i_c}^{(c)}$, где $u_1, \dots, u_c$ — любые элементы группы F , а $i_1, \dots, i_c$ — любые числа от 1 до d . Пусть $w_2, \dots, w_c$ — любые элементы F . Рассмотрим модуль $T(w_2, \dots, w_c; i_1, \dots, i_c)$, порожденный всеми элементами $x_{v, i_1}^{(1)} x_{w_2 v, i_2}^{(2)} \dots x_{w_c v, i_c}^{(c)}$, где v — любой элемент F . Очевидно, что M есть прямая сумма всех модулей $T(w_2, \dots, w_c; i_1, \dots, i_c)$, причем каждый из этих модулей инвариантен относительно F и является суммой циклических подмодулей, порожденных элементами $x_{v, i_1}^{(1)} x_{w_2 v, i_2}^{(2)} \dots x_{w_c v, i_c}^{(c)}$ и сопряженных относительно F . Это и доказывает предложение В). Теорема доказана.

При помощи рассуждений, использованных при доказательстве теоремы 2, мы выведем еще один результат, который понадобится нам в дальнейшем. Обозначим через Z центр группы $\mathfrak{G}_{d,F}^{(c)}$. Он является прямым произведением циклических групп порядка l^k . Совокупность элементов Z , являющихся l^r -ми степенями элементов Z , обозначим через Z_r . Очевидно, что Z_r является характеристической подгруппой $\mathfrak{G}_{d,F}^{(c)}$. Группу $\mathfrak{G}_{d,F}^{(c)}/Z_r$ обозначим через $\mathfrak{G}_{d,F}^{(c,r)}$ и Z_r/Z_{r+1} — через $Z^{(r)}$. При этом

$$\mathfrak{G}_{d,F}^{(c,0)} = \mathfrak{G}_{d,F}^{(c-1)}, \quad \mathfrak{G}_{d,F}^{(c,k)} = \mathfrak{G}_{d,F}^{(c)}.$$

Следствие. Для любого $r \leq k-1$ существует группа $\mathfrak{G}$ с областью операторов F и со следующими свойствами: $\mathfrak{G}$ содержит такую элементарную допустимую центральную подгруппу A , что

$$1) \mathfrak{G}/A \cong \mathfrak{G}_{d,F}^{(c,r)};$$

2) A есть прямое произведение допустимых подгрупп, каждая из которых является прямым произведением m сопряженных относительно F циклических групп;

1) существует такой гомоморфизм $\mathfrak{G}$ на $\mathfrak{G}_{d,F}^{(c,r+1)}$, что его ядро содержится в A .

Для доказательства надо только заметить, что допустимая подгруппа $Z^{(r)}$ лежит в центре $\mathfrak{G}_{d,F}^{(c,r+1)}$ и операторно-изоморфна модулю многочленов Ли степени s от dm переменных $x_{u,i}$. Применяя теперь предложения А) и В), использованные при доказательстве теоремы 2, мы получаем, что существует такая элементарная абелева группа $\mathfrak{N}$ с группой операторов F , что $A = Z^{(r)} \times \mathfrak{N}$ обладает свойством 2). Следовательно, мы можем принять $\mathfrak{G}_{d,F}^{(c,r+1)} \times \mathfrak{N}$ за $\mathfrak{G}$.

В дальнейшем нам понадобится следующее замечание. Нормальный делитель A можно, очевидно, представить как пересечение таких подгрупп B_i , что $(A : B_i) = I$. Группы $\mathfrak{G}/B_i$ являются простыми центральными расширениями $\mathfrak{G}_{d,F}^{(c,r)}$. Точно так же Z_r можно представить как пересечение таких подгрупп C_i , что $(Z_r : C_i) = I$. Группы $\mathfrak{G}_{d,F}^{(c,r+1)}/C_i$ также являются простыми центральными расширениями $\mathfrak{G}_{d,F}^{(c,r)}$. Очевидно, что системы множителей, соответствующие вторым расширениям, содержатся среди систем множителей, соответствующих первым расширениям. Нам важно отметить, что никаких новых систем множителей первые расширения не дают. Это непосредственно следует из того, что $\mathfrak{G} = \mathfrak{G}_{d,F}^{(c,r+1)} \times \mathfrak{N}$.

3. Поля с центрально-диспозиционной группой Галуа.

Пусть нам задана центрально-диспозиционная группа $\mathfrak{G}$ с группой операторов F , причем, ввиду следствия из теоремы 2, мы можем ограничиться случаем, когда центр $\mathfrak{G}$ есть прямое произведение m циклических групп порядка l , сопряженных относительно F . Обозначим этот центр Z :

$$Z = \{z\} \times \{z^{u_1}\} \times \dots \times \{z^{u_{m-1}}\}. \quad (4)$$

Факторгруппу $\mathfrak{G}$ по подгруппе $Z_1 = \{z^{u_1}\} \times \dots \times \{z^{u_{m-1}}\}$ обозначим через $\mathfrak{G}_1$, а $\mathfrak{G}/Z$ — через $\mathfrak{G}$. Очевидно, что $\mathfrak{G}$ имеет F в качестве группы операторов, но $\mathfrak{G}_1$ не является операторной группой. Полупрямое произведение $\mathfrak{G}$ на F обозначим через $\overline{\mathfrak{G}}$.

Пусть дана цепочка полей $\Omega \subset k \subset \overline{K} \subset K_1$, из которых $\overline{K}/\Omega$, K_1/k и k/Ω нормальны, причем группа Галуа k/Ω есть F , $\overline{K}/\Omega$ — $\overline{G}$, $\overline{K}/k$ — $\mathfrak{G}$, K_1/k — $\mathfrak{G}_1$.

ТЕОРЕМА 3. Если поля K_1^u для всех $u \in F$ независимы над $\overline{K}$, то композит всех K_1^u имеет в качестве группы Галуа над Ω полупрямое произведение $\mathfrak{G}$ на F .

Мы называем здесь расширения $K_1, \dots, K_r$ поля k независимыми над k , если пересечение композита $K_1 \dots K_{i-1} K_{i+1} \dots K_r$ с K_i есть k для любого $i = 1, \dots, r$, так что группа Галуа композита $K_1 \dots K_r$ над k изоморфна прямому произведению групп Галуа K_i/k .

Доказательство. Обозначим композит полей K_1^u через K и вычислим группу Галуа K/Ω . Сначала докажем, что группа Галуа K/k совпадает с $\mathfrak{G}$. Исследуем для этого подробнее группу $\mathfrak{G}$. $\mathfrak{G}$ является расширением $\overline{\mathfrak{G}}$ с центральным нормальным делителем Z и, следовательно, задается своей системой множителей со значениями из Z . Ввиду того что для Z имеет место разложение (4), эта система множителей может быть записана в виде:

$$\alpha'(\sigma, \tau) = z^{\sum^u \alpha_u(\sigma, \tau)u}, \quad \sigma, \tau \in \overline{\mathfrak{G}}.$$

Перейдем к ассоциированной системе множителей, выбрав более удобную систему представителей. Пусть система множителей $\alpha'(\sigma, \tau)$ соответствует такому выбору представителей, при котором из класса σ выбирается представитель $[\sigma]$. Если мы обозначим $\alpha_e(\sigma, \tau)$ просто через $\alpha(\sigma, \tau)$, то группа $\mathfrak{G}_1$ будет центральным расширением $\overline{\mathfrak{G}}$ с системой множителей $z^{\alpha(\sigma, \tau)}$. Рассмотрим представителей $[\sigma^{u^{-1}}]^u$, лежащих, конечно, в тех же классах смежности, что и $[\sigma]$. Рассмотрим одновременно группу $\mathfrak{G}_u = \mathfrak{G}/Z_1^u$. Эта группа будет иметь в качестве центра $\{z^u\}$, причем она будет центральным расширением $\overline{\mathfrak{G}}$ с системой множителей $z^{u\alpha(\sigma^{u^{-1}}, \tau^{u^{-1}})}$ (при указанном выборе представителей $[\sigma^{u^{-1}}]^u$). Из этого следует, что мы можем выбрать представителей в классах смежности $\mathfrak{G}$ по Z так, чтобы вместо $\alpha'(\sigma, \tau)$ получить ассоциированную систему множителей

$$\alpha(\sigma, \tau) = z^{\sum^u u\alpha(\sigma^{u^{-1}}, \tau^{u^{-1}})}.$$

Группа Галуа K/k является, очевидно, расширением $\overline{\mathfrak{G}}$ с ядром гомоморфизма, изоморфным Z , так что для того, чтобы показать, что эта группа изоморфна $\mathfrak{G}$, нам надо только установить, что система множителей у нее та же, что и у $\mathfrak{G}$. Доказательство почти дословно повторяет приведенное выше рассуждение. Факторгруппа группы Галуа K/k по подгруппе $Z_1 = \{z^{u_1}\} \times \dots \times \{z^{u_{m-1}}\}$ изоморфна группе Галуа K_1/k , т. е. $\mathfrak{G}_1$. Центр $\mathfrak{G}_1$ порождается элементом z ,

факторгруппа по центру есть $\overline{\mathfrak{G}}$, и при надлежащем выборе представителей в классах смежности по центру система множителей будет $z^{\alpha(\sigma, \tau)}$. Выбранных нами представителей обозначим через $[\sigma]$. Автоморфизм $[\sigma]$ является некоторым продолжением автоморфизма σ с поля $\overline{K}$ на поле K_1 . Рассмотрим теперь поле K_1^u , принадлежащее к подгруппе Z_1^u , и продолжим автоморфизм σ на это поле. Для этого заметим, что каждое число поля K_1^u представляется в виде α^u , где $\alpha \in K_1$, причем для примитивных элементов поля K_1^u такое представление однозначно. Определим в K_1^u автоморфизм $[\sigma]_u$ по формуле:

$$(\alpha^u)^{[\sigma]_u} = (\alpha^{[\sigma^{u^{-1}}]})^u.$$

Легко видеть, что получается действительно автоморфизм поля K_1^u , продолжающий автоморфизм σ поля K . Группа Галуа K_1^u является расширением $\overline{\mathfrak{G}}$ с ядром гомоморфизма $\{z^u\}$, причем при указанном выборе представителей в классах смежности по $\{z^u\}$ система множителей будет, как легко видеть, $z^{\alpha(\sigma^{u^{-1}}, \tau^{u^{-1}})}^u$. Если для каждого u продолжить указанным образом автоморфизм σ на поле K_1^u , то получится некоторое продолжение этого автоморфизма на поле K , т. е. некоторый фиксированный выбор представителей в классах смежности группы Галуа K/k по Z . Ввиду сказанного, этому выбору представителей соответствует система множителей

$$\sum_u \alpha(\sigma^{u^{-1}}, \tau^{u^{-1}})^u,$$

что и доказывает изоморфизм группы Галуа K/k с $\mathfrak{G}$.

Докажем, что установленный нами изоморфизм между группой Галуа K/k и группой $\mathfrak{G}$ является операторным изоморфизмом относительно группы операторов F . Мы установили изоморфизм между нашими двумя группами, отображив изоморфно друг на друга их центры и некоторые построенные нами системы представителей классов вычетов по центру. Изоморфизм центров очевидным образом является операторным, так как оба центра являются прямыми произведениями групп вида $\{z^u\}$, $u \in F$. Нам остается проверить, что установленное соответствие между представителями классов смежности по центрам выдерживает применение операторов из F . Обозначим представителя построенной нами системы через $\langle \sigma \rangle$. Этот представитель однозначно определяется выбором представителя $[\sigma]$ в классе смежности по центру группы $\mathfrak{G}_1 = \mathfrak{G}/Z_1$ и тем, что при $u \in F$

$$\langle \sigma \rangle Z_1^u = \langle \sigma^{u^{-1}} \rangle^u Z_1^u = ([\sigma^{u^{-1}}] Z_1)^u. \quad (5)$$

Но этим уже однозначно определяется действие операторов из F на представителя $\langle \sigma \rangle$. В самом деле, применяя к (5) автоморфизм $v \in F$, получим:

$$\langle \sigma \rangle^v Z_1^{uv} = \langle \sigma^{u^{-1}} \rangle^{uv} Z_1^{uv}$$

или, обозначая uv через w ,

$$\langle \sigma \rangle^v Z_1^w = \langle \sigma^{vw^{-1}} \rangle^w Z_1^w = (\left[\sigma^{vw^{-1}} \right] Z_1)^w \quad \text{для всех } w \in F,$$

чем элемент $\langle \sigma \rangle^v$ однозначно определен.

Группа Галуа K/Ω является расширением F с ядром гомоморфизма, изоморфным $\mathfrak{G}$, причем, как мы доказали, ядро гомоморфизма даже операторно-изоморфно $\mathfrak{G}$. Нам остается показать, что расширение полупрямое, т. е. что при надлежащем выборе представителей $\bar{u}$ в классе смежности u и по $\mathfrak{G}$ $\bar{u}$ будут образовывать группу.

По условию теоремы, автоморфизмы u поля k могут быть так продолжены до автоморфизмов поля $\bar{K}$, которые мы также будем обозначать через u , что новые автоморфизмы будут по-прежнему образовывать группу. Для того, чтобы указать продолжение автоморфизма v с поля $\bar{K}$ на поле K , достаточно указать его действие на элементы полей K_1^u , так как их композит дает все K . Воспользуемся представлением элементов поля K_1^u в виде α^u , $\alpha \in K_1$, $u \in F$, и положим

$$(\alpha^u)^{\bar{v}} = \alpha^{uv}.$$

Очевидно, что этот автоморфизм действительно продолжает автоморфизм v поля $\bar{K}$, и что

$$\overline{v_1 v_2} = v_1 v_2.$$

Таким образом, теорема 3 доказана.

§2. Условие погружаемости для шольцевых расширений

При построении расширения K/k , имеющего в качестве группы Галуа над k группу $\mathfrak{G}_{d,F}^{(c,k)}$, а в качестве группы Галуа над Ω — полупрямое произведение $F \cdot \mathfrak{G}_{d,F}^{(c,k)}$, мы будем пользоваться, в основном, теми соображениями, которые были изложены в работе [4]. А именно, мы будем строить поле K/k шольцевым, а самую конструкцию вести индукцией по c .

В этом параграфе мы разберем следующий вопрос. Пусть Ω , k и $\bar{K}$ имеют тот же смысл, что и в теореме 3, $K_1 \supset \bar{K}$ и $(K_1 : \bar{K}) = l$,

причем K_1 нормально над k , и K есть композит полей, сопряженных с K_1 над Ω . Мы будем предполагать, что $\overline{K}/k$ шольцево, и выясним, когда можно построить поле K_1 с заданной группой над k так, чтобы K тоже было шольцевым над k . При этом мы будем считать, что простые делители дискриминанта поля $\overline{K}/k$ имеют в k/Ω порядок 1. То, что этого можно добиться и для K/k , очевидно на каждом шаге нижеследующих рассуждений.

Введенные сейчас обозначения мы будем употреблять, не оговаривая этого еще раз.

1. Построение инвариантов $[\chi, X]$. Мы будем предполагать в этом параграфе, что k содержит корни степени l из 1. Пусть $K_1 = \overline{K}(\sqrt[l]{\mu})$, где μ — l -инвариантное число поля $\overline{K}/k$. Обозначим класс l -инвариантных чисел, в котором лежит μ , через X . Рассмотрим любой характер χ порядка l группы Галуа $\overline{K}/k$ и соответствующее ему [см. [4], стр. 268] число α_χ из k . Это число может быть разложено на простые множители следующим образом:

$$(\alpha_\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{\sum \varphi_{\mathfrak{p}}(u)u},$$

где $\mathfrak{p}$ пробегает не сопряженные друг с другом относительно Ω простые дивизоры k , а сумма в показателе распространена на все автоморфизмы u поля k/Ω .

Пусть $\mathfrak{D}$ — тот инвариантный дивизор $\overline{K}/k$, состоящий из критических простых дивизоров, который входит в разложение

$$(\mu) = \mathfrak{C}^l \mathfrak{D}^m \quad (6)$$

[см. [4], стр. 266]. Рассмотрим функцию $g(u)$, определенную тем, что для любого корня степени l из 1

$$\zeta^u = \zeta^{g(u)},$$

и предположим, что для любого $\mathfrak{p} \nmid \mathfrak{D} \sum \varphi_{\mathfrak{p}}(u^{-1})g(u)u$ l -взаимно просто с простым делителем $\mathfrak{P}$ дивизора $\mathfrak{p}$ в $\overline{K}$. Легко проверить, что это условие не зависит от выбора $\mathfrak{P}$ среди делителей $\mathfrak{p}$ в $\overline{K}$. Мы будем поэтому записывать его в виде

$$(\mathfrak{D} \sum \varphi_{\mathfrak{p}}(u^{-1})g(u)u, \mathfrak{p}) \approx 1. \quad (7)$$

Если условие (7) выполнено, то мы определим символ $[\chi, X]$ следующим образом:

$$[\chi, X] = \prod_{\mathfrak{p}} \left[\frac{\mu \sum \varphi_{\mathfrak{p}}(u^{-1})g(u)u}{\mathfrak{p}} \right] \cdot \left(\frac{\alpha_\chi}{\mathfrak{m}} \right)^{-1}. \quad (8)$$

Соотношение (7) гарантирует, что символ, стоящий в правой части равенства (8), определен.

По своему виду условия (7), при которых определен символ $[\chi, X]$, и само определение этого символа зависят не только от χ и X , но и от выбора числа α_χ , соответствующего χ , числа μ в классе X и простых дивизоров $\mathfrak{p}$ среди множества всех сопряженных друг с другом дивизоров. Докажем, что и условия, при которых определен символ $[\chi, X]$, и сам этот символ зависят на самом деле только от χ и X .

а) Независимость от выбора α_χ очевидна, так как если α'_χ — другое число, соответствующее тому же χ , то $\alpha_\chi \approx \alpha'_\chi$, а поэтому $\varphi_{\mathfrak{p}}(u) \equiv \varphi'_{\mathfrak{p}}(u)(l)$ для любых $\mathfrak{p}$ и u .

б) Докажем независимость от выбора μ в классе X . Любое другое l -инвариантное число в классе X получается из μ умножением на l -ю степень числа из $\overline{K}$ и на число из k . Умножение μ на l -ю степень числа из $\overline{K}$ очевидным образом не меняет ни условия (7), ни символа $[\chi, X]$. Пусть мы умножили μ на число $m \in k$, взаимно простое с дискриминантом $\overline{K}/k$. Очевидно, что условие (7) не нарушилось, так как при этом не изменилось $\mathfrak{D}$. Правая же часть формулы (8) умножится на

$$\prod_{\mathfrak{p}} \left(\frac{m^{\sum \varphi_{\mathfrak{p}}(u^{-1})g(u)u}}{\mathfrak{p}} \right) \cdot \left(\frac{\alpha_\chi}{m} \right)^{-1}. \quad (9)$$

Ввиду того, что

$$\left(\frac{m^{\varphi_{\mathfrak{p}}(u^{-1})g(u)u}}{\mathfrak{p}} \right) = \left(\frac{m}{\mathfrak{p}^{\sum \varphi_{\mathfrak{p}}(u^{-1})u^{-1}}} \right),$$

мы имеем:

$$\prod_{\mathfrak{p}} \left(\frac{m^{\sum \varphi_{\mathfrak{p}}(u^{-1})g(u)u}}{\mathfrak{p}} \right) = \prod_{\mathfrak{p}} \left(\frac{m}{\mathfrak{p}^{\sum \varphi_{\mathfrak{p}}(u^{-1})u^{-1}}} \right) = \left(\frac{m}{\alpha_\chi} \right).$$

Так как поле $\overline{K}$ по предположению шольцево, то α_χ гиперпримарно, а поэтому

$$\left(\frac{m}{\alpha_\chi} \right) = \left(\frac{\alpha_\chi}{m} \right),$$

что и показывает, что выражение (9) равно 1.

с) Для доказательства независимости от выбора p предположим, что p^v — любой простой дивизор, сопряженный с p . Тогда

$$p \sum \varphi_p(u)u = p^v \sum \varphi_p(u)v^{-1}u = p^v \sum \varphi_p(vu)u.$$

Таким образом, замена p на p^v приводит к замене функции $\varphi_p(u)$ на $\varphi_p(vu)$. Условие (7) примет тогда вид:

$$\left(\mathfrak{D} \sum \varphi_p(vu^{-1})g(u)u, p^v \right) \approx 1. \quad (10)$$

Чтобы доказать это условие, применим к (7) автоморфизм v . Мы получим:

$$\left(\mathfrak{D} \sum \varphi_p(u^{-1})g(u)uv, p^v \right) \approx 1.$$

Делая в сумме, стоящей в показателе, замену переменной uv на u , получим:

$$\left(\mathfrak{D} \sum \varphi_p(vu^{-1})g(uv^{-1})u, p^v \right) \approx 1.$$

Так как $g(uv^{-1}) \equiv g(u)g(v^{-1})$ (I), то

$$\mathfrak{D} \sum \varphi_p(vu^{-1})g(uv^{-1})u \approx \left(p \sum \varphi_p(vu^{-1})g(u)u \right)^{g(v^{-1})},$$

что и доказывает справедливость соотношения (10).

Таким образом, условие, при котором символ $[\chi, X]$ определен, не зависит от выбора p среди сопряженных. Докажем, что и значение символа $[\chi, X]$ от этого выбора не зависит.

При замене p на p^v множитель

$$\left[\frac{\mu \sum \varphi_p(u^{-1})g(u)u}{p} \right] \quad (11)$$

в правой части (8) заменится на

$$\left[\frac{\mu \sum \varphi_p(vu^{-1})g(u)u}{p^v} \right]. \quad (12)$$

Пользуясь соотношением

$$\left(\frac{\alpha}{b^v} \right) = \left(\frac{\alpha^{g(v^{-1})v^{-1}}}{b} \right),$$

мы получим, что выражение (12) равно

$$\left[\frac{\mu \sum \varphi_p(vu^{-1})g(u)g(v^{-1})uv^{-1}}{p} \right].$$

Если заменить теперь uv^{-1} на u , то мы и получим (11).

Если $k = \Omega$, то символ $[\chi, X]$ превращается в символ (χ, X) , определенный в работе [4]. Очевидно, что символ $[\chi, X]$, как и символ (χ, X) , обладает свойствами:

$$[\chi_1 \chi_2, X] = [\chi_1, X][\chi_2, X], \quad (13)$$

$$[\chi, X_1 X_2] = [\chi, X_1][\chi, X_2], \quad (14)$$

$$[\chi, X] = [\chi', X']. \quad (15)$$

Последнее равенство имеет тот смысл, что, если $\overline{K}$ является подполем нормального над Ω поля $\overline{K}'$, то символ $[\chi, X]$ может быть вычислен в обоих полях и имеет при этом одно и то же значение.

2. Инварианты $[X]_\psi$. Эти инварианты определены только для классов X , содержащих таких l -инвариантных представителей μ , для которых поле $\overline{K}(\sqrt[l]{\mu})$ шольцево. Иными словами, это те классы, для которых все инварианты (χ, X) и $(X)_h$ равны 1. В дальнейшем мы будем предполагать, что представитель μ в классе X выбран так, что поле $\overline{K}(\sqrt[l]{\mu})$ шольцево.

Рассмотрим класс l -инвариантных чисел X и функции $\psi(u)$, заданные на группе F со значениями в группе вычетов по модулю l , удовлетворяющие следующим условиям:

$$1. \psi(1) = 0, \quad \psi(u^{-1}) = -\psi(u)g(u), \quad u \in F,$$

$$2. \mu^{\sum \psi(u)u} \approx \alpha_\psi \in k.$$

Если $l = 2$, то мы наложим еще одно дополнительное условие. Пусть u есть инволютивный автоморфизм $\overline{K}/k : u^2 = 1$, $\overline{K}_u$ — подполе $\overline{K}$, состоящее из чисел, инвариантных относительно u , $\mathfrak{D}_u$ — дифферента $K_u/\overline{K}_u$. Мы потребуем, чтобы функция $\psi(u)$ удовлетворяла соотношению

$$3. \prod_u \mathfrak{D}_u^{\psi(u)} \approx 1 \quad \text{в } \overline{K},$$

где произведение распространено на все инволютивные автоморфизмы из F .

Очевидно, что все эти условия относятся только к функции ψ и классу l -инвариантных чисел X , а не зависят от выбора представителя μ в X . Если выполнены условия 1 и 2, а при $l = 2$ и условие 3, то мы определим символ $[X]_\psi$ следующим образом: выберем в

классе X такого l -гиперпримарного представителя μ , что $\overline{K}(\sqrt[l]{\mu})/k$ будет шольцево и

$$(m, m^u) = 1 \quad \text{для всех} \quad u \neq 1, \quad (16)$$

где m — дивизор из разложения (6), и положим

$$m_\psi = m^{\sum \psi(u)u}, \quad [X]_\psi = \left[\frac{\mu}{m_\psi} \right]. \quad (17)$$

Ввиду условия (16), правая часть (17) действительно определена.

Докажем, что $[X]_\psi$ не зависит от выбора μ в классе X . Очевидно, что при умножении μ на l -ю степень числа из $\overline{K}$ символ $[X]_\psi$ не меняется. Докажем, что он не меняется и при умножении μ на такое число m из k , что поле $\overline{K}(\sqrt[l]{\mu m})$ — шольцево. В доказательстве может встретиться следующее затруднение: если

$$(\mu) = \mathfrak{C}^l \mathfrak{D} m, \quad (\mu') = \mathfrak{C}'^l \mathfrak{D} m',$$

причем m и m' удовлетворяют условию (16), и $\mu' = \mu m$, то из этого не следует, что и m удовлетворяет аналогичному (16) условию:

$$(m, m^u) = 1, \quad u \in F, \quad u \neq 1.$$

Чтобы в дальнейшем не иметь дела с этим затруднением, мы введем такое μ'' , для которого

$$\mu'' = \mu \alpha, \quad \mu' = \mu'' \beta, \quad \mu'' = \mathfrak{C}''^l \mathfrak{D} m'', \quad (18)$$

и будем считать выполненными условия:

$$\begin{aligned} (m'', m''^u) &= 1, & (m'', m^u) &= 1, & (m'', m'^u) &= 1, \\ (\alpha, \alpha^u) &= 1, & (\beta, \beta^u) &= 1. \end{aligned} \quad (19)$$

Для этого достаточно взять простой дивизор абсолютно первого порядка $\mathfrak{p}$, взаимно простой со всеми m^u и m'^u и эквивалентный m . Непосредственная проверка показывает, что условия (18) и (19) выполнены, если положить

$$(\alpha) = \mathfrak{p} m^{-1}, \quad (\beta) = m' \mathfrak{p}^{-1}.$$

Таким образом, нам достаточно доказать, что

$$\left[\frac{\mu}{m_\psi} \right] = \left[\frac{\mu'}{m'_\psi} \right], \quad (20)$$

если

$$\mu = \mu' m, \quad (m, m^u) = (m', m'^u) = (m, m^u) = 1.$$

При этом мы можем считать, что μ , μ' и m l -гиперпримарны. В этом случае

$$m'_\psi = m_\varphi m^{\sum \psi(u)u}$$

и

$$\left[\frac{\mu'}{m'_\psi} \right] = \left[\frac{\mu}{m_\psi} \right] \left(\frac{m}{m_\psi} \right) \left[\frac{\mu}{m^{\sum \psi(u)u}} \right] \left(\frac{m}{m^{\sum \psi(u)u}} \right). \quad (21)$$

Равенство (20) будет доказано, если мы докажем, что произведение второго и третьего сомножителей, а также четвертый сомножитель в правой части (21) равен 1. Действительно,

$$\left[\frac{\mu}{m^{\sum \psi(u)u}} \right] = \left[\frac{\mu^{\sum \psi(u)g(u)u^{-1}}}{m} \right] = \left[\frac{\mu^{-\sum \psi(u^{-1})u^{-1}}}{m} \right] = \left(\frac{\alpha_\psi}{m} \right)^{-1},$$

ввиду условий 1 и 2. Так как m l -гиперпримарно и является вычетом l -й степени по критическим дивизорам, то из закона взаимности следует, что

$$\left[\frac{\mu}{m^{\sum \psi(u)u}} \right] \left(\frac{m}{m_\psi} \right) = \left(\frac{\alpha_\psi}{m} \right)^{-1} \left(\frac{m}{\alpha_\psi} \right) = 1.$$

Доказательство того, что

$$\left[\frac{m}{m^{\sum \psi(u)u}} \right] = 1, \quad (22)$$

различно при $l \neq 2$ и $l = 2$.

При $l \neq 2$ мы имеем:

$$\begin{aligned} \left(\frac{m}{m^{\sum \psi(u)u}} \right) &= \left(\frac{m^{\sum \psi(u)g(u)u^{-1}}}{m} \right) \\ &= \left(\frac{m}{m^{\sum \psi(u)g(u)u^{-1}}} \right) = \left(\frac{m}{m^{\sum \psi(u)u}} \right)^{-1}. \end{aligned}$$

Отсюда мы получаем:

$$\left(\frac{m}{m^{\sum \psi(u)u}} \right)^2 = 1, \quad \text{т. е.} \quad \left(\frac{m}{m^{\sum \psi(u)u}} \right) = 1.$$

При $l = 2$, очевидно, $g(u) = 1$ для всех u . Если u есть неинволютивный автоморфизм, то $u \neq u^{-1}$ и

$$\left(\frac{m}{m^{\psi(u)u+\psi(u^{-1})u^{-1}}}\right) = \left(\left(\frac{m}{m^u}\right)\left(\frac{m}{m^{u^{-1}}}\right)^{-1}\right)^{\psi(u)}. \quad (23)$$

Так как

$$\left(\frac{m}{m^{u^{-1}}}\right) = \left(\frac{m^u}{m}\right) = \left(\frac{m}{m^u}\right),$$

то это выражение равно 1.

Рассмотрим теперь произведение

$$\left(\frac{m}{m^{\sum \psi(u)u}}\right),$$

в котором сумма распространена только на отличные от 1 инволютивные автоморфизмы из F . В работе [5] доказано, что если u — инволютивный автоморфизм поля $\bar{K}$, в котором простые делители двойки и вещественные бесконечно удаленные простые дивизоры полностью распадаются, то для символа Лежандра второй степени имеет место соотношение:

$$\left(\frac{m}{m^u}\right) = \left(\frac{m}{\mathfrak{D}_u}\right),$$

где $\mathfrak{D}_u$ — дифферента $\bar{K}/\bar{K}_u$, а $\bar{K}_u$ — подполе, принадлежащее u . Применяя это соотношение к нашему произведению и учитывая условие 3, получаем:

$$\left(\frac{m}{m^{\sum \psi(u)u}}\right) = \prod \left(\frac{m}{m^u}\right)^{\psi(u)} = \left(\frac{m}{\prod \mathfrak{D}_u^{\psi(u)}}\right) = 1.$$

Это равенство вместе с (23) и дает (22), т. е. доказывает независимость символа $[X]_\psi$ от выбора представителя μ в классе X .

Для символа $[X]_\psi$ имеет место равенство

$$[X]_\psi = [X']_\psi,$$

аналогичное (15), но соотношение, аналогичное (14), не имеет места.

3. Условия погружаемости. Кроме введенных сейчас инвариантов $[\chi, X]$ и $[X]_\psi$, мы рассмотрим еще введенные в работе [4] инварианты $(X)_h$ класса l -инвариантных чисел поля $\overline{K}/k$. При их помощи можно сформулировать следующее необходимое и достаточное условие погружаемости в шольцево поле.

Пусть $\overline{K} \supset k \supset \Omega$, $\overline{K}/k$ — шольцево и имеет группу Галуа степени l^α , $\overline{K}/\Omega$ — нормально, X — класс l -инвариантных чисел в $\overline{K}/k$, K_1 — любое простое центральное расширение $\overline{K}$, соответствующее X , и K — композит всех полей, сопряженных с K_1 над Ω .

ТЕОРЕМА 4. Для того, чтобы существовало поле K_1 , для которого K — шольцево над k , необходимо и достаточно, чтобы все инварианты $(X)_h$, $[X]_\psi$ и $[\chi, X]$ равнялись 1 для всех ψ и χ , для которых они определены.

Доказательство. Необходимость условий теоремы проверяется непосредственно. Равенство единице инварианта $(X)_h$ следует из соответствующего утверждения теоремы 1 работы [4], так как из шольцевости K/k следует шольцевость K_1/k . В формуле (17), определяющей $[X]_\psi$, m_ψ состоит только из простых делителей дивизоров m^u . Ввиду шольцевости K/k ,

$$\left[\frac{\mu^u}{p} \right] = 1, \quad \text{т. е.} \quad \left[\frac{\mu}{p^u} \right] = 1 \quad \text{для всех} \quad u \neq 1, \quad u \in F, \quad p|m,$$

откуда и следует, что $[X]_\psi = 1$.

В формуле (8), определяющей $[\chi, X]$, для любого простого $q|m$, ввиду шольцевости K_1/k ,

$$\left(\frac{\alpha_\chi}{q} \right) = 1, \quad \text{т. е.} \quad \left(\frac{\alpha_\chi}{m} \right) = 1.$$

С другой стороны, ввиду шольцевости K/k и ввиду (7),

$$\left[\frac{\mu \sum \psi_p(u^{-1})g(u)u}{p} \right] = 1, \quad p|\alpha_\chi,$$

откуда и следует, что $[\chi, X] = 1$.

Перейдем теперь к доказательству достаточности условий теоремы. Для этого заметим, что инварианты (χ, X) , определенные в работе [4], содержатся среди инвариантов $[\chi, X]$. В самом деле, для того чтобы инвариант (χ, X) был определен, нужно, чтобы все простые дивизоры, входящие в α_χ в степени, не делящейся на l , были

взаимно просты с $\mathfrak{D}$. Очевидно, что из этого следует выполнение условия (7), т. е. и символ $[\chi, X]$ тоже определен. При этом мы имеем:

$$\begin{aligned} [\chi, X] &= \prod_p \left[\frac{\mu \sum \varphi_p(u^{-1})g(u)u}{p} \right] \cdot \left(\frac{\alpha_\chi}{\mathfrak{m}} \right)^{-1} = \\ &= \prod_p \left[\frac{\mu}{p \sum \varphi_p(u^{-1})u^{-1}} \right] \cdot \left(\frac{\alpha_\chi}{\mathfrak{m}} \right)^{-1} = \left[\frac{\mu}{\alpha_\chi} \right] \left(\frac{\alpha_\chi}{\mathfrak{m}} \right)^{-1} = (\chi, X). \end{aligned}$$

Таким образом, из условий теоремы вытекает равенство единице инвариантов (χ, X) и $(X)_h$. Применяя теперь теорему 1 работы [4], мы видим, что K_1 может быть выбрано шольцевым над k . В дальнейшем мы всегда будем предполагать, что K_1/k шольцево.

Очевидно, что первое, второе и четвертое условия шольцевости, будучи выполнены для поля K_1 , выполняются для его сопряженных K_1^u , а следовательно, и для их композита K . Таким образом, нам остается показать, что если $K_1 = \overline{K}(\sqrt{\mu})$, то μ можно умножить на такое число $m \in k$, что $\overline{K}(\sqrt{\mu m})$ будет по-прежнему шольцевым над k , и для композита полей, сопряженных с $\overline{K}(\sqrt{\mu m})$ относительно Ω , будет выполнено третье условие шольцевости. Умножение μ на m заведомо не будет нарушать шольцевости K_1 , если m будет тотально-положительным (при $l = 2$), будет делиться только на простые дивизоры, полностью распадающиеся в $\overline{K}$, и будет сравнимым с 1 по модулю достаточно высокой степени l . Эту степень мы будем обозначать через l^g .

Мы добьемся шольцевости поля K в два приема. Сначала мы умножим μ на такое число m_1 , чтобы K_1 осталось шольцевым и в K все критические простые дивизоры $\overline{K}$ имели порядок 1. Потом умножим μm_1 на такое число m_2 , чтобы эти свойства не нарушались и, сверх того, все критические простые дивизоры K имели порядок 1.

Пусть $\mathfrak{p}$ — критический простой дивизор $\overline{K}$. Для того, чтобы в поле K , получающемся присоединением к $\overline{K}$ всех $\sqrt[l]{\mu^u}$, простые делители $\mathfrak{p}$ имели порядок 1, необходимо и достаточно, чтобы для любой функции $f_{\mathfrak{p}}(u)$, для которой

$$(\mathfrak{D} \sum f_{\mathfrak{p}}(u)u, \mathfrak{P}) \approx 1, \quad \mathfrak{P} | \mathfrak{p},$$

выполнялось равенство:

$$\left[\frac{\mu \sum f_{\mathfrak{p}}(u)u}{\mathfrak{p}} \right] = 1.$$

Положим

$$\xi_{f_p} = \left[\frac{\mu \sum f_p(u)u}{p} \right]$$

и покажем, что существует тотально-положительное число m_1 , состоящее из простых дивизоров, полностью распадающихся в $\bar{K}$, и сравнимое с 1 по модулю l^g , для которого

$$\left(\frac{m_1 \sum f_p(u)u}{p} \right) = \xi_{f_p}^{-1} \quad (24)$$

при любых p и f_p . Очевидно, что тогда μm_1 будет удовлетворять нужным нам условиям.

Возьмем произвольный первообразный корень ζ степени l из 1 и положим:

$$\left(\frac{m_1}{p^u} \right) = \zeta^{x_{p,u}}, \quad \xi_{f_p}^{-1} = \zeta^{b_{f_p}}. \quad (25)$$

Тогда равенства (24) перепишутся так:

$$\left(\frac{m_1}{p \sum f_p(u)g(u)u^{-1}} \right) = \xi_{f_p}^{-1}$$

или

$$\sum_u f_p(u^{-1})g(u^{-1})x_{p,u} = b_{f_p} \quad \text{для всех } p \text{ и } f_p, \quad (26)$$

причем уравнение рассматривается в поле вычетов $\text{mod } l$. Выясним, когда существует тотально-положительное число m_1 , удовлетворяющее условиям (25), состоящее из простых дивизоров, распадающихся в $\bar{K}$, и сравнимое с 1 по модулю l^g .

Обозначим через $\mathfrak{F}$ произведение всех p^u , l^g и вещественных бесконечно удаленных простых дивизоров, через H — группу l -х степеней классов дивизоров по модулю $\mathfrak{F}$, а через L — поле классов к H . Покажем, что условия (25) и требование, чтобы m_1 было сравнимо с 1 по модулю l^g и тотально-положительно, эквивалентны тому, что дивизор (m_1) принадлежит к определенному автоморфизму в L . Действительно, если числа m_1 и m'_1 удовлетворяют этим условиям, то $(m'_1)H = (m_1)H$, и, наоборот, если дивизор a таков, что $aH = (m_1)H$, то $a = (\alpha)b^l$, причем α удовлетворяет всем нужным нам условиям. Обозначим через σ тот автоморфизм поля L , принадлежность к которому дивизора (m_1) гарантирует выполнение наложенных нами на m_1 условий.

Для того чтобы можно было найти число m_1 , состоящее из простых множителей, полностью распадающихся в $\overline{K}$, и принадлежащее к автоморфизму σ в L , необходимо и достаточно, чтобы в пересечении $\overline{K} \cap L$ σ индуцировал единичный автоморфизм. Очевидно, что $\overline{K} \cap L$ есть поле, получающееся присоединением к k всех $\sqrt[l]{\alpha_\chi}$. Таким образом, нам надо выписать условия, при которых σ индуцирует в каждом из полей $k(\sqrt[l]{\alpha_\chi})$ единичный автоморфизм.

Найдем автоморфизм, который σ индуцирует в $k(\sqrt[l]{\alpha_\chi})$. Для этого возьмем произвольный дивизор α , принадлежащий к σ в L . Мы видели, что $\alpha = (\alpha)^{b^l}$ и, следовательно, (α) принадлежит в L к σ . Автоморфизм, индуцируемый σ в $k(\sqrt[l]{\alpha_\chi})$, сводится к умножению $\sqrt[l]{\alpha_\chi}$ на $(\frac{\alpha_\chi}{\alpha}) = (\frac{\alpha_\chi}{\alpha})$. Так как α_χ l -гиперпримарно и тотально-положительно, то

$$\left(\frac{\alpha_\chi}{\alpha}\right) = \left(\frac{\alpha}{\alpha}\right) = \prod_{p,u} \left(\frac{\alpha}{p^u}\right)^{\varphi_{p,\chi}(u)} = \zeta^{\sum_{p,u} x_{p,u} \varphi_{p,\chi}(u)},$$

если

$$(\alpha_\chi) = \prod_p p^{\sum \varphi_{p,\chi}(u)}.$$

Таким образом, для того чтобы существовало тотально-положительное число m_1 , состоящее из полностью распадающихся в $\overline{K}$ простых дивизоров, сравнимое с 1 по модулю l^g и удовлетворяющее условиям (25), должно иметь место уравнение:

$$\sum_{p,u} x_{p,u} \varphi_{p,\chi}(u) = 0 \quad \text{для всех } \chi. \quad (27)$$

Нам остается доказать, что существуют $x_{p,u}$, удовлетворяющие уравнениям (26) и (27). Мы выпишем условия совместности этой системы уравнений и покажем, что они состоят в равенстве единице инвариантов $[\chi, X]$.

Если система, состоящая из уравнений (26) и (27), не совместна, то существует такая линейная комбинация этих уравнений, в которой все коэффициенты при неизвестных $x_{p,u}$ равны нулю, а свободный член не равен нулю. Пусть

$$\sum_{\chi} c_{\chi} \sum_{p,u} x_{p,u} \varphi_{p,\chi}(u) + \sum_{f,p,p} d_{f,p,p} \sum_u f_p(u^{-1}) g(u^{-1}) x_{p,u} = \sum_{f,p,p} d_{f,p,p} b_{f,p} \quad (28)$$

есть такая линейная комбинация.

Положим

$$\prod_{\chi} \chi^{c_{\chi}} = \chi_0, \quad \sum_{f_p} d_{f_p, p} f_p(u) = F_p(u).$$

Тогда, очевидно,

$$\sum_{\chi} c_{\chi} \varphi_{p, \chi}(u) = \varphi_{p, \chi_0}(u),$$

$$\sum_{f_p} d_{f_p, p} b_{f_p} = b_{F_p}.$$

Принимая во внимание, что в (28) коэффициенты при всех $x_{p, u}$ равны нулю, получаем:

$$\varphi_{p, \chi_0}(u) = -F_p(u^{-1})g(u^{-1}) \quad \text{для всех } p \text{ и } u.$$

Из этого мы заключаем, что, во-первых,

$$(\mathfrak{D} \sum \varphi_{p, \chi_0}(u)g(u)u, p) \approx 1$$

и, во-вторых,

$$\prod_p \left[\frac{\mu \sum \varphi_{p, \chi_0}(u)g(u)u}{p} \right] = \zeta_p^{\sum b_{F_p}}. \quad (29)$$

Для совместности системы (28) необходимо и достаточно, чтобы

$$\sum_{f_p, p} d_{f_p, p} b_{f_p} = \sum b_{F_p} = 0,$$

т. е. чтобы правая часть (29) равнялась 1. Левая же часть этого равенства есть как раз $[\chi_0, X]$, так как, ввиду того что поле K_1 уже предположено шольцевым, $\left(\frac{\alpha_X}{\mathfrak{m}}\right) = 1$. Таким образом, система, состоящая из уравнений (26) и (27), совместна, а следовательно, число m_1 с нужными нам свойствами существует.

Обозначим число μm_1 через μ_1 . Тогда, по доказанному, поле $\overline{K}(\sqrt{\mu_1})$ шольцево, а в композите всех его сопряженных все критические простые дивизоры $\overline{K}$ имеют порядок 1. Нам надо найти такое число m_2 , чтобы для числа $\mu_1 m_2$ вместо μ_1 все эти свойства сохранялись, а в композите сопряженных к полю $\overline{K}(\sqrt{\mu_1 m_2})$ все критические простые дивизоры имели порядок 1.

Мы выберем m_2 так, чтобы оно было тотально-положительным, состояло из простых дивизоров, полностью распадающихся в $\overline{K}$, и удовлетворяло условиям:

$$\left. \begin{aligned} \left(\frac{m_2}{p}\right) &= 1 \quad \text{для всех } p, \text{ критических в } \overline{K}/k, \\ m_2 &\equiv 1 \pmod{p}, \quad (m_2, m_2^u) = 1 \quad u \in F, \quad u \neq 1. \end{aligned} \right\} \quad (30)$$

Так как $\overline{K}/\Omega$ нормально, то вместе с p и p^u будет критическим в $\overline{K}/k$. Из этого следует, что при таком выборе m_2 для $\mu_1 m_2$ будут сохраняться те свойства, выполнения которых для μ_1 мы перед тем добились. Обозначим через K композит сопряженных к $\overline{K}(\sqrt{\mu_1 m_2})$ над Ω . Нам остается подобрать m_2 так, чтобы оно удовлетворяло условиям (30), а в поле K/k все критические простые дивизоры $K/\overline{K}$ имели порядок 1. Критическими дивизорами $K/\overline{K}$, не являющимися критическими в $\overline{K}$, будут только делители $(m_1 m_2)^u$, если

$$(\mu_1) = \mathfrak{C}_1' \mathfrak{D} m_1.$$

Мы предположим, что

$$(m_1, m_1^u) = 1,$$

так как этого, как легко видеть, можно добиться, умножая μ_1 на число m_2 , удовлетворяющее условиям (30).

Для того чтобы делители $m_1 m_2$ имели порядок 1 в K , необходимо и достаточно, чтобы выполнялись условия:

$$\left[\frac{\mu_1 m_2}{q^u}\right] = 1 \quad \text{для всех } q | m_1 m_2.$$

Эти условия естественно распадаются на две части:

$$\left[\frac{\mu_1 m_2}{q^u}\right] = 1, \quad \text{т. е.} \quad \left(\frac{m_2}{q^u}\right) = \left[\frac{\mu_1}{q^u}\right]^{-1} \quad \text{для } q | m_1$$

и

$$\left(\frac{m_2}{r^u}\right) = \left[\frac{\mu_1}{r^u}\right]^{-1} \quad \text{для } r | m_2.$$

Мы будем подбирать m_2 таким, чтобы все делящие его простые дивизоры r удовлетворяли условию:

$$\left[\frac{\mu_1}{r^u}\right] = \zeta(u), \quad (31)$$

где $\zeta(u)$ — некоторая система корней степени l из 1. Само же m_2 должно тогда удовлетворять условиям:

$$\left(\frac{m_2}{q^u}\right) = \left[\frac{\mu_1}{q^u}\right]^{-1}, \quad q|m_1,$$

$$\left(\frac{m_2}{r^u}\right) = \zeta(u)^{-1}, \quad u \in F, \quad u \neq 1, \quad r|m_2. \quad (32)$$

Вопрос о существовании таких чисел был рассмотрен в работе [5]. Для того, чтобы иметь возможность применить доказанную в этой работе теорему, мы будем предполагать, что корни из единицы $\zeta(u)$ удовлетворяют условиям:

$$\zeta(u) = \zeta(u^{-1})^{g(u^{-1})} \quad (33)$$

и в случае $l = 2$ потребуем, чтобы для любых инволютивных автоморфизмов $u_1, \dots, u_r$ из F выполнялось условие:

$$\zeta(u_1) \dots \zeta(u_r) = 1 \quad \text{всякий раз, как} \quad \mathfrak{D}_{u_1} \dots \mathfrak{D}_{u_r} \approx 1. \quad (34)$$

Здесь $\mathfrak{D}_{u_i}$ означает дифференту поля $\overline{K}/\overline{K}_{u_i}$, а $\overline{K}_{u_i}$ — поле, принадлежащее автоморфизму u_i .

Из теоремы работы [5] следует существование бесконечного количества чисел m_2 , удовлетворяющих условиям (32) для любых $\zeta(u)$, удовлетворяющих условиям (33) и (34). Нам остается выяснить, можно ли при этом удовлетворить условиям (30) и (31). Для этого надо отдельно рассмотреть случаи $l \neq 2$ и $l = 2$.

Предположим, что $l \neq 2$. В этом случае число m_2 , согласно доказательству теоремы в работе [5], может быть найдено в виде произведения двух простых чисел $\pi_1 \pi_2$, удовлетворяющих условиям:

$$\left(\frac{\pi_i}{q^u}\right) = \left[\frac{\mu_1}{q^u}\right]^{-\frac{1}{2}}, \quad i = 1, 2,$$

причем мы можем добиться выполнения условий (30) и (31) для m_2 , если докажем существование бесконечного числа простых чисел π , полностью распадающихся в $\overline{K}$ и удовлетворяющих условиям (33) и следующим условиям:

$$\left[\frac{\mu_1}{\pi^u}\right] = \zeta(u); \quad (35)$$

$$\left(\frac{\pi}{p}\right) = 1 \quad \text{для } p, \text{ критических в } \overline{K}/k; \quad (36)$$

$$\pi \equiv 1 \pmod{l^g}; \quad (37)$$

$$(\pi) \neq (\pi^u), \quad u \in F, \quad u \neq 1. \quad (38)$$

Выясним, когда существуют простые числа π , удовлетворяющие всем этим условиям. Как и в первой части доказательства, мы построим модуль $\mathfrak{F}$, состоящий из произведения всех p , q^u , l^g и бесконечно удаленных простых дивизоров, обозначим через H группу l -х степеней классов вычетов по модулю $\mathfrak{F}$ и через L — поле классов к H и построим такой автоморфизм σ в L , что принадлежность дивизора a к σ означает, что $a = (\alpha)b^l$, причем α тотально-положительно и

$$\left(\frac{\alpha}{q^u}\right) = \left[\frac{\mu_1}{q^u}\right]^{-\frac{1}{2}}, \quad \left[\frac{\alpha}{p}\right] = 1, \quad \alpha \equiv 1 \quad (l^g).$$

Условие (35), чтобы простой дивизор τ полностью распадался в $\overline{K}$ и удовлетворял условиям

$$\left(\frac{\mu_1}{\tau^u}\right) = \zeta(u)$$

или

$$\left(\frac{\mu_1^u}{\tau}\right) = \zeta(u^{-1})^{g(u)},$$

эквивалентно тому, чтобы τ принадлежал ко вполне определенному автоморфизму τ поля K' , полученного присоединением к $\overline{K}$ всех $\sqrt[l]{\mu_1^u}$, $u \in F$, $u \neq 1$. Таким образом, нам надо выяснить, когда существует простой дивизор поля k , принадлежащий в L к автоморфизму σ , а в K' — к автоморфизму τ .

Для этого необходимо и достаточно, чтобы σ и τ индуцировали один и тот же автоморфизм в $K' \cap L$. Посмотрим, когда это будет так. Поле $K' \cap L$ получается, очевидно, присоединением к k всех $\sqrt[l]{\alpha_\chi}$ и $\sqrt[l]{\alpha_\varphi}$, где φ — такая функция на группе F со значениями в группе вычетов по модулю l , что

$$\mu^{\sum \varphi(u)u} \approx \alpha_\varphi \in k, \quad \varphi(1) = 0.$$

Таким образом, нам надо выяснить, когда σ и τ индуцируют один и тот же автоморфизм, во-первых, в поле $k(\sqrt[l]{\alpha_\chi})$ и, во-вторых, в поле $k(\sqrt[l]{\alpha_\varphi})$. Очевидно, что в $k(\sqrt[l]{\alpha_\chi})$ и σ , и τ — единичные автоморфизмы. Автоморфизм, который индуцирует σ в $k(\sqrt[l]{\alpha_\varphi})$, может быть найден точно таким же способом, который мы применяли в первой части доказательства. Этот автоморфизм сводится к умножению $\sqrt[l]{\alpha_\varphi}$ на $\left[\frac{\mu_1}{m_\varphi}\right]$, где $m_\varphi = m_1^{\sum \varphi(u)u}$. Аналогично можно найти

и тот автоморфизм, который индуцирует τ в $k(\sqrt{\alpha_\varphi})$. Этот автоморфизм сводится к умножению $\sqrt{\alpha_\varphi}$ на $\prod_u \zeta(u^{-1})^{g(u)\varphi(u)}$. Таким образом, совпадение автоморфизмов σ и τ в $K' \cap L$ эквивалентно выполнению условий:

$$\prod_u \zeta(u^{-1})^{g(u)\varphi(u)} = \left[\frac{\mu_1}{m_\varphi} \right]^{-\frac{1}{2}} \quad \text{для всех } \varphi. \quad (39)$$

Нам остается выяснить, когда существуют корни из единицы $\zeta(u)$, удовлетворяющие условиям (33) и (39).

Возьмем произвольный первообразный корень степени l из 1 и положим:

$$\zeta(u) = \zeta^{x_u}, \quad \left[\frac{\mu_1}{m_\varphi} \right]^{-\frac{1}{2}} = \zeta^{b_\varphi}.$$

Тогда условия (33) и (39) на x_u запишутся в виде уравнений в поле вычетов $(\text{mod } l)$:

$$\begin{aligned} x_u &= x_{u-1}g(u^{-1}), \\ \sum_u x_{u-1}g(u)\varphi(u) &= b_\varphi. \end{aligned} \quad (40)$$

Мы выпишем условия совместности этой системы и покажем, что они заключаются в равенстве единице инвариантов $[X]_\psi$.

Если система (40) не совместна, то существует линейная комбинация входящих в нее уравнений, в которой все коэффициенты при неизвестных x_u равны 0, а свободный член $\neq 0$.

Пусть

$$\sum_u c_u(x_u - x_{u-1}g(u^{-1})) + \sum_\varphi d_\varphi \sum_u x_{u-1}g(u)\varphi(u) = \sum_\varphi d_\varphi b_\varphi \quad (41)$$

есть такая линейная комбинация.

Положим

$$\sum_\varphi d_\varphi \varphi(u) = \psi(u).$$

Тогда, очевидно,

$$\sum_\varphi d_\varphi b_\varphi = b_\psi.$$

Учитывая, что в (41) коэффициенты при всех x_u равны 0, получаем:

$$g(u^{-1})\psi(u^{-1}) = c_{u-1} - c_u g(u^{-1}),$$

откуда легко следует, что

$$\psi(u^{-1}) = -\psi(u)g(u), \quad \psi(1) = 0.$$

Таким образом, функция ψ удовлетворяет условию в определении символа $[X]_\psi$. Отсюда мы заключаем, что

$$\zeta^{b_\psi} = \left[\frac{\mu_1}{m_\psi} \right]^{-\frac{1}{2}} = 1, \quad \text{т. е.} \quad b_\psi = 0,$$

что и означает совместность системы (40).

Аналогичным образом мы поступаем и в случае $l = 2$. Согласно доказательству теоремы в работе [5], число m_2 в этом случае может быть найдено в виде произведения $\pi_1 \pi_2 \pi_3$ трех простых чисел, удовлетворяющих условиям

$$\left(\frac{\pi_i}{q_u} \right) = \left[\frac{\mu_1}{q_u} \right]^{-1} \quad (i = 1, 2, 3),$$

причем мы можем добиться выполнения условий (36) и (37) для m_2 , если докажем существование бесконечного числа простых чисел π , полностью распадающихся в $\bar{K}$ и удовлетворяющих условиям:

$$\left[\frac{\mu_1}{\pi_u} \right] = \zeta(u)$$

и условиям (33), (34), (36), (37) и (38).

Как и в случае $l \neq 2$, для того, чтобы существовали такие числа, необходимо и достаточно, чтобы была совместной следующая система уравнений:

$$\left. \begin{aligned} x_u &= x_{u-1}, \\ x_{u_1} + \dots + x_{u_r} &= 0, \quad \text{если} \quad \mathfrak{D}_{u_1} \dots \mathfrak{D}_{u_r} \approx 1, \\ \sum_u x_{u-1} \varphi(u) &= b_\varphi. \end{aligned} \right\} \quad (42)$$

Предположение о несовместности этой системы опять приводит к наличию линейной комбинации этих уравнений с коэффициентами при x_u , равными нулю, и свободным членом, не равным нулю. Пусть эта линейная комбинация есть

$$\begin{aligned} & \sum_u c_u (x_u - x_{u-1}) + \sum_\varphi d_\varphi \sum_u x_{u-1} \varphi(u) + \\ & + \sum_{(u_1, \dots, u_r)} e_{u_1, \dots, u_r} (x_{u_1} + \dots + x_{u_r}) = \sum d_\varphi b_\varphi, \end{aligned}$$

где третья сумма слева распространена на все совокупности $(u_1, \dots, u_r)$ инволютивных автоморфизмов, для которых

$$\mathfrak{D}_{u_1} \dots \mathfrak{D}_{u_r} \approx 1.$$

Мы полагаем опять

$$\sum_{\varphi} d_{\varphi} \varphi(u) = \psi(u)$$

и получаем, как и при $l \neq 2$,

$$\psi(u^{-1})c_{u^{-1}} - c_u + \sum_{u \in (u_1, \dots, u_r)} e_{u_1, \dots, u_r} = 0.$$

Отсюда мы видим, что при $u \neq u^{-1}$

$$\psi(u^{-1}) \neq -\psi(u),$$

а также, что на множестве инволютивных автоморфизмов

$$\psi(u) = \sum_{(u_1, \dots, u_r)} \epsilon_{u_1, \dots, u_r}(u) \cdot e_{u_1, \dots, u_r}, \quad (43)$$

где $\epsilon_{u_1, \dots, u_r}(u)$ есть характеристическая функция множества $(u_1, \dots, u_r)$. Так как, по определению множеств $(u_1, \dots, u_r)$,

$$\prod_u \mathfrak{D}_u^{\epsilon_{u_1, \dots, u_r}(u)} \approx 1,$$

где произведение распространено на все инволютивные автоморфизмы u , то из (34) следует, что

$$\prod_u \mathfrak{D}_u^{\psi(u)} \approx 1.$$

Таким образом, функция $\psi(u)$ удовлетворяет всем условиям, входящим в определение инварианта $[X]_{\psi}$, а следовательно,

$$\zeta^{b_{\psi}} = \left[\frac{\mu_1}{m_{\psi}} \right] = [X]_{\psi} = 1,$$

что и означает совместность системы (42). Теорема доказана.

Мы применим теорему 4 к выводу условий, при которых шольцево поле K с группой Галуа $F \cdot \mathfrak{G}_{d,F}^{(c,r-1)}$ над Ω может быть погружено в поле K с группой $F \cdot \mathfrak{G}_{d,F}^{(c,r)}$ над Ω . Подполе поля $\bar{K}$, принадлежащее $\mathfrak{G}_{d,F}^{(c,r-1)}$, мы по-прежнему будем обозначать через k .

ТЕОРЕМА 5. Если в поле $\overline{K}$ с группой Галуа $F \cdot \mathfrak{G}_{d,F}^{(c,r-1)}$ над Ω инварианты $[\chi, X]$, $(X)_h$, $[X]_\psi$ равны 1 для всех X , соответствующих расширению $\mathfrak{G}_{d,F}^{(c,r-1)}$ до $\mathfrak{G}_{d,F}^{(c,r)}$, то K можно погрузить в нормальное над Ω шольцево поле K , имеющее над Ω группу Галуа $F \cdot \mathfrak{G}_{d,F}^{(c,r)}$.

Доказательство. Применяя следствие из теоремы 3, мы видим, что операторная группа $A = Z^{(r)} \times \mathfrak{N}$ может быть представлена в виде

$$A = A_1 \times \cdots \times A_m,$$

где каждая группа A_i , в свою очередь, может быть представлена в виде

$$A_i = \prod_{u \in F} Z_i^u,$$

причем Z_i является циклической группой порядка l . Проведем в группе A цепочку подгрупп B_i :

$$B_i = \mathfrak{N}A_{i+1} \dots A_m, \quad B_0 = A, \quad B_m = \mathfrak{N}.$$

Очевидно, что

$$B_{i-1}/B_i \cong A_i/A_i \cap B_i. \quad (44)$$

Мы будем строить цепочку шольцевых полей K_i , содержащих $\overline{K}$ и имеющих группы Галуа $F \cdot \mathfrak{G}_{d,F}^{(c,r)} \times \mathfrak{N}/B_i$ над Ω . Так как K_m имеет группу Галуа $\mathfrak{G}_{d,F}^{(c,r)}$, то его и можно принять за поле K . Пусть поле K_{i-1} уже построено. Обозначим через X_i характер, обращающийся в 1 на всех циклических группах Z_j^u с $j \neq i$ или $u \neq 1$ и отличный от 1 на Z_i . Применим теорему 4 к полю K_{i-1} в качестве $\overline{K}$ и покажем, что K_{i-1} можно погрузить в такое циклическое поле степени l над K_{i-1} и нормальное над k , чтобы группа Галуа этого поля была расширением группы Галуа поля K_{i-1}/k , соответствующим X_i , а композит всех полей, сопряженных с ним над Ω , был шольцевым полем K_i . Для этого нам надо только проверить, что выполняются условия теоремы 4.

Будем различать два случая:

- 1) $c = 1$, $r = 1$ и
- 2) или c , или r отлично от 1.

Докажем, что в обоих случаях все инварианты $[\chi, X_i]$, $(X_i)_h$, $[X_i]_\psi$ равны 1. В случае 1) это очевидно, так как $X_i = 1$. В случае 2) мы воспользуемся тем, что X_i обращается в 1 на всех

A_j , $j < i$, и поэтому соответствует некоторому расширению группы Галуа $\mathfrak{G}_{d,F}^{(c,r-1)}$ поля $\bar{K}$. С другой стороны, факторгруппа по подгруппе Фраттини не изменилась при переходе от группы Галуа поля $\bar{K}$ к группе Галуа поля K_{i-1} , так что характеры χ являются характерами $\mathfrak{G}_{d,F}^{(c,r-1)}$. Ввиду этого, соотношения (15) и их аналоги для инвариантов $(X)_h$ и $[X]_\psi$ показывают, что инварианты $[\chi, X_i]$, $(X_i)_h$, $[X_i]_\psi$ в поле K_{i-1} совпадают с некоторыми инвариантами поля $\bar{K}$. Так как, по предположению, инварианты поля K равны 1, то это верно и для рассматриваемых инвариантов поля K_{i-1} .

Таким образом, доказано, что поле K_{i-1} погружаемо в шольцево поле $\tilde{K}_i$. Соотношение (44) показывает, что в поле $\tilde{K}_i$ содержится подполе K_i с группой Галуа $F \cdot \mathfrak{G}^{(c,r)}/B_i$. Как подполе шольцева поля, поле K_i — шольцево. Теорема доказана.

§3. Конструкция полей, удовлетворяющих условиям задачи погружения

1. Операторные канонические гомоморфизмы. Содержание этого параграфа тесно примыкает к §3 работы [4]. Ввиду этого мы будем опускать доказательства некоторых предложений, если эти доказательства дословно повторяют рассуждения из работы [4], и ограничимся указаниями на соответствующие места этой работы.

Вместо групп $\mathfrak{G}_d^{(c)}$ работы [4] мы будем рассматривать определенные выше операторные нильпотентные диспозиционные группы $\mathfrak{G}_{d,F}^{(c)}$. Так как большей частью c , k и F будут во всех рассуждениях одни и те же, то мы будем обозначать эти группы просто через $\mathfrak{G}_d$.

Во всех дальнейших рассуждениях будет играть роль некоторая фиксированная система образующих $s_{u,i}$ группы $\mathfrak{G}_d$. Все образующие $s_{u,i}$ при одном и том же i и всевозможных $u \in F$ мы будем называть классом образующих. Группа $\mathfrak{G}_d$ имеет, таким образом, d классов образующих.

Пусть даны группы $\mathfrak{G}_d$ и $\mathfrak{G}_\delta$ ($\delta \leq d$) с образующими $s_{u,i}$ ($i = 1, \dots, d$) и $t_{u,i}$ ($i = 1, \dots, \delta$). Гомоморфизм $\mathfrak{G}_d$ на $\mathfrak{G}_\delta$ называется каноническим, если образующие $s_{u,i}$, $u \in F$, $i = 1, \dots, \delta - 1$ переходят при этом гомоморфизме в $t_{u,i}$ при тех же u и i , а остальные образующие $s_{u,i}$ переходят при некоторых i в $t_{u,\delta}$ с тем же самым u , а при других i — в 1. Из определения следует, что всякий канонический гомоморфизм является операторным гомоморфизмом относительно группы F . Мы будем обозначать канонические гомоморфизмы буквами S , T и т. д. Описанный выше гомоморфизм мы будем называть гомоморфизмом типа $(s_{u,1}, \dots, s_{u,\delta-1}; t_{u,1}, \dots, t_{u,\delta-1} | t_{u,\delta})$, а множество образующих группы $\mathfrak{G}_d$, для которых при гомоморфизме

$S \quad s_{u,i} \rightarrow s_{u,\delta}$, будем обозначать через $[S]$. Очевидно, что гомоморфизм S заданного типа однозначно определяется множеством $[S]$. В дальнейшем мы будем рассматривать только канонические гомоморфизмы и поэтому называть их просто гомоморфизмами.

Два гомоморфизма S и T будем называть независимыми, если $[S]$ и $[T]$ не пересекаются. Тогда существует единственный гомоморфизм R , для которого

$$[R] = [S] \cup [T].$$

R мы будем называть композитом S и T и обозначать через $S * T$.

2. Функции гомоморфизмов. Рассмотрим функции $f(S)$, заданные на множестве всех гомоморфизмов и принимающие значения из некоторой конечной абелевой группы порядка ν . Для функций гомоморфизмов одного и того же типа $(s_{u,1}, \dots, s_{u,\delta-1}; t_{u,1}, \dots, t_{u,\delta-1} | t_{u,\delta})$ определяется степень относительно класса образующих $t_{u,\delta}$. Степень 0 имеет функция, тождественно равная 1. Функция $f(S)$ имеет степень $\leq n$, если

$$\varphi(S, T) = f(S)^{-1} f(T)^{-1} f(S * T)$$

имеет для любого S , как функция от T , степень $\leq n - 1$.

Функция $f(S)$ имеет степень $\leq n$ тогда и только тогда, когда для любого множества из $n + 1$ попарно независимых гомоморфизмов $S_1, \dots, S_{n+1}$ выполняется соотношение

$$\prod_{(i_1, \dots, i_k)} f(S_{i_1} * \dots * S_{i_k})^{(-1)^k} = 1, \quad (45)$$

где $(i_1, \dots, i_k)$ пробегает все непустые подмножества множества $(1, \dots, n + 1)$. Доказательство этого факта дословно повторяет доказательство аналогичного утверждения из n^02 §3 работы [4], и мы его опускаем.

ТЕОРЕМА 6. Для любых натуральных чисел k и n существует зависящее только от них число $C(k, n)$ со следующим свойством: какие бы k функций гомоморфизмов $f_1(S), \dots, f_k(S)$ степени $\leq n$ ни были заданы на группе $\mathfrak{G}_d$ с $d \geq C(k, n)$, всегда найдется такой гомоморфизм S , что $f_i(S) = 1, \quad i = 1, \dots, k$.

Следствие. Если при тех же предположениях, что и в теореме 6, в группе $\mathfrak{G}_d$ указаны m классов образующих $s_{u,i_1}, \dots, s_{u,i_m}, i_1, \dots, i_m \geq \delta - 1$ и $d \geq C(k, n + m)$, то группу $\mathfrak{G}_d$ можно отобразить при помощи канонического гомоморфизма на группу $\mathfrak{G}_{\delta+m}$ с образующими $s'_{u,1}, \dots, s'_{u,\delta+m}$, у которой все функции $f_1, \dots, f_k$

обращаются в единицу на гомоморфизме $s'_{u,1} \rightarrow t_{u,1}, \dots, s'_{u,\delta} \rightarrow t_{u,\delta}, s'_{u,\delta+1} \rightarrow 1, \dots, s'_{u,\delta+m} \rightarrow 1$.

Доказательства теоремы 6 и следствия дословно повторяют доказательства теоремы 3 и следствия из нее в n^03 §3 работы [4]. Мы их опускаем.

В дальнейшем мы будем применять теорию канонических гомоморфизмов не к группам $\mathfrak{G}_{d,F}^{(c)}$, а к факторгруппам $\mathfrak{G}_{d,F}^{(c,r)}$ при некотором фиксированном значении r . Легко видеть, что всякий канонический гомоморфизм группы $\mathfrak{G}_{d,F}^{(c)}$ на группу $\mathfrak{G}_{\delta,F}^{(c)}$ определяет некоторый гомоморфизм $\mathfrak{G}_{d,F}^{(c,r)}$ на $\mathfrak{G}_{\delta,F}^{(c,r)}$ при любом $r \leq k$. Эти гомоморфизмы мы также будем называть каноническими и именно с ними мы и будем иметь дело. Группу центральных элементов порядка l в группе $\mathfrak{G}_{\delta,F}^{(c,r)}$, соответственно $\mathfrak{G}_{d,F}^{(c,r)}$, т. е. группу $Z^{(r-1)}$ для этой группы мы будем обозначать через $Z_{\delta}^{(r-1)}$, соответственно $Z_d^{(r-1)}$.

Пусть дана цепочка полей $\Omega \subset k \subset \bar{K}$, причем k/Ω нормально и имеет группу Галуа F , $K/\bar{\Omega}$ также нормально и группа Галуа $\bar{K}/k$ есть $\mathfrak{G}_{d,F}^{(c,r)}$, а $\bar{K}/\Omega$ — полупрямое произведение $\mathfrak{G}_{d,F}^{(c,r)}$ на F . Изучим инварианты $[\chi, X]$ и $[X]_{\psi}$ для тех классов l -инвариантных чисел, которые соответствуют простым центральным расширениям $\mathfrak{G}_{d,F}^{(c,r)}$ до различных факторгрупп группы $\mathfrak{G}_{d,F}^{(c,r+1)}$. Все такие расширения находятся во взаимно однозначном соответствии с характерами порядка l группы $Z_d^{(r)}$. Характер, соответствующий таким образом классу X , мы будем также обозначать через X .

Рассмотрим базис группы характеров порядка l $\chi_{u,i}$ ($i = 1, \dots, d$) взаимный к системе образующих $s_{u,i}$. Числа $\alpha_{\chi_{u,i}} \in k$ будем сокращенно обозначать через $\alpha_{u,i}$. Если перенести операторы из F с группы $\mathfrak{G}_{d,F}^{(c,r)}$ на ее группу характеров при помощи правила:

$$\chi^u(\sigma^u) = \chi(\sigma),$$

то мы будем иметь:

$$\chi_{u,i} = \chi_{1,i}^u, \quad \alpha_{u,i} \approx \alpha_{1,i}^u.$$

Ввиду этого мы обозначим $\alpha_{1,i}$ через α_i и будем считать, что

$$\alpha_{u,i} = \alpha_i^u.$$

Начиная с этого места, мы всегда будем предполагать, что α_i и α_j^u взаимно просты для всех i, j и u . Это условие будет выполнено, если, например, α_i будут делиться только на простые дивизоры порядка 1 над Ω , причем если $p \mid \alpha_i$, то $p^u \nmid \alpha_j$ при всех i, j и u .

Легко проверить, как это сделано в работе [4], стр. 290, что образующим автоморфизмом группы дивизора p , делящего α_i^u , будет автоморфизм σ , удовлетворяющий условиям:

$$\chi_{u,i}(\sigma) \neq 1, \quad \chi_{v,j}(\sigma) = 1 \quad \text{при } v \neq u \text{ или } i \neq j.$$

Такой автоморфизм, очевидно, имеет порядок l^k в факторгруппе группы $\mathfrak{G}_{d,F}^{(c,r)}$ по ее коммутанту. Таким образом, если $c \neq 1$, то образующие автоморфизмы групп инерции делителей α_i^u не повышают своего порядка при переходе от $\mathfrak{G}_{d,F}^{(c,r)}$ к расширению этой группы, соответствующему классу X . Из этого следует, что дивизор $\mathfrak{D}(X)$ l -взаимно прост с α_i^u , а следовательно, все инварианты $[\chi, X]$ определены.

Если $c = 1$, то классы X находятся во взаимно однозначном соответствии с характерами χ . Будем обозначать через $\tilde{\chi}$ класс, соответствующий характеру X . Инвариант $[\chi_{u,i}, \tilde{\chi}_{v,j}]$ всегда определен, за исключением случая, когда $u = v$, $i = j$. Доказательство этих утверждений дословно повторяет доказательство утверждений в n^0 4 §3 работы [4].

Рассмотрим теперь шольцево поле $\bar{K} \supset k \supset \Omega$ с группой Галуа $\mathfrak{G}_{d,F}^{(c,r)}$ над k и $F \cdot \mathfrak{G}_{d,F}^{(c,r)}$ над Ω . Рассмотрим канонический операторный гомоморфизм S $\mathfrak{G}_{d,F}^{(c,r)}$ на $\mathfrak{G}_{\delta,F}^{(c,r)}$ при некотором $\delta \leq d$. Его ядро $\mathfrak{N}$ является нормальным делителем группы $\mathfrak{G}_{d,F}^{(c,r)}$, так что к $\mathfrak{N}$ принадлежит нормальное подполе поля $\bar{K}$, которое мы будем обозначать через $\bar{K}^S$. Поле $\bar{K}^S$ имеет над k группу Галуа $\mathfrak{G}_{\delta,F}^{(c,r)}$, а над $\Omega = F \cdot \mathfrak{G}_{\delta,F}^{(c,r)}$. Кроме того, числа α_i^u , соответствующие полю $\bar{K}^S$, будут l -взаимно просты между собой, как доказано в n^0 5 §3 работы [4]. Каждый из инвариантов $[\chi, X]$, $(X)_h$ и $[X]_\psi$, определенный для поля $\bar{K}^S$, является при фиксированном $\bar{K}$ функцией гомоморфизма S .

Мы можем отождествить X с характером группы $Z^{(r)}$. С другой стороны, группа $Z^{(r)}$ операторно-изоморфна аддитивно записанному модулю многочленов Ли степени s от переменных $x_{u,i}$ ($i = 1, \dots, \delta$). Все переменные $x_{u,i}$ при фиксированном i и любых $u \in F$ мы будем называть классом переменных.

ТЕОРЕМА 7. Если характер X имеет относительно совокупности переменных класса $x_{u,\delta}$ степень $\leq n$, не аннулирует хотя бы одного многочлена, зависящего хотя бы от одной переменной $x_{u,\delta}$, и аннулирует все многочлены, зависящие только от $x_{u,i}$ ($i = 1, \dots, \delta - 1$), то инварианты $[\chi_{u,i}, X]$ и $(X)_\psi$, как функции гомоморфизмов типа $(s_{u,1}, \dots, s_{u,\delta-1}; t_{u,1}, \dots, t_{u,\delta-1} | t_{u,\delta})$ группы Галуа $\mathfrak{G}_{d,F}^{(c,r)}$ шольцева поля $\overline{K}$, имеет следующие степени: $(X)_h$ — степень $\leq n$, $[\chi_{u,i}, X]$ при $i \neq \delta$ — степень $\leq n$, $[\chi_{u,\delta}, X]$ — степень $\leq n + 1$. Таким образом, все эти инварианты имеют степень $\leq c + 1$.

Доказательство этой теоремы дословно повторяет доказательство теоремы 4 из n^0 5 §3 работы [4] (причем нужно доказать и предшествующую ей лемму). Мы его опускаем.

Нам остается исследовать поведение инварианта $[X]_\psi$ как функции гомоморфизма.

При этом мы ограничиваемся случаем, когда в поле $\overline{K}/k$ с группой Галуа $\mathfrak{G}_{d,F}^{(c,r)}$ все инварианты $[\chi, X]$ и $(X)_h$ равны 1.

ТЕОРЕМА 8. Если в поле $\overline{K}$ все инварианты $[\chi, X]$ и $(X)_h$, равны 1, а характер X модуля $Z_d^{(r)}$ имеет степень $\leq n$ относительно совокупности переменных класса $x_{u,\delta}$, не аннулирует хотя бы одного многочлена, зависящего хотя бы от одного из $x_{u,\delta}$, и аннулирует все многочлены, зависящие только от $x_{u,i}$ ($i = 1, \dots, \delta - 1$), то инвариант $[X]_\psi$, как функция гомоморфизмов типа $(s_{u,1}, \dots, s_{u,\delta-1}; t_{u,1}, \dots, t_{u,\delta-1} | t_{u,\delta})$ группы Галуа поля $\overline{K}$, имеет степень $\leq 2n$.

Доказательство. Заметим, прежде всего, что в рассматриваемом нами случае вопрос о том, для каких ψ и X определен инвариант $[X]_\psi$, решается, если известны ψ как функция на группе F , X как система множителей на группе $\mathfrak{G}_{d,F}^{(c,r)}$, и поле k , вне зависимости от свойств поля $\overline{K}$. В самом деле, условия 1 и 3 в определении символа $[X]_\psi$ относятся только к свойствам функции ψ и поля k , а условие 2 эквивалентно такому:

$$X \sum \psi(u)^u = 1. \quad (46)$$

Здесь X^u обозначает образ X при автоморфизме, который u индуцирует в группе характеров группы $Z_d^{(r)}$. Очевидно, что условие (46) не зависит от поля $\overline{K}$.

Пусть X_1 , X_2 и X_3 — три характера, для которых определен инвариант $[X]_\psi$. Докажем, что для них выполняется соотношение:

$$[X_1 X_2 X_3]_\psi [X_1 X_2]_\psi^{-1} [X_1 X_3]_\psi^{-1} [X_2 X_3]_\psi^{-1} [X_1]_\psi [X_2]_\psi [X_3]_\psi = 1, \quad (47)$$

аналогичное частному случаю (45) при $n = 2$.

Соотношение (47) доказывается непосредственной проверкой. Выберем для этого в классах l -инвариантных чисел, соответствующих X_1 , X_2 и X_3 , таких представителей μ_1 , μ_2 и μ_3 , чтобы соответствующие дивизоры $\mathfrak{m}_1$, $\mathfrak{m}_2$ и $\mathfrak{m}_3$ удовлетворяли следующим соотношениям: $(\mathfrak{m}_i, \mathfrak{m}_j^u) = 1$, $i, j = 1, 2, 3$, кроме случая $i = j$, $u = 1$. Пусть $\mathfrak{m}_\psi^{(i)} = \mathfrak{m}_i^{\sum \psi(u)u}$, $i = 1, 2, 3$. Тогда равенство (47) переписывается так:

$$\left[\frac{\mu_1 \mu_2 \mu_3}{\mathfrak{m}_\psi^{(1)} \mathfrak{m}_\psi^{(2)} \mathfrak{m}_\psi^{(3)}} \right] \left[\frac{\mu_1 \mu_2}{\mathfrak{m}_\psi^{(1)} \mathfrak{m}_\psi^{(2)}} \right]^{-1} \left[\frac{\mu_1 \mu_3}{\mathfrak{m}_\psi^{(1)} \mathfrak{m}_\psi^{(3)}} \right]^{-1} \left[\frac{\mu_2 \mu_3}{\mathfrak{m}_\psi^{(2)} \mathfrak{m}_\psi^{(3)}} \right]^{-1} \times \left[\frac{\mu_1}{\mathfrak{m}_\psi^{(1)}} \right] \left[\frac{\mu_2}{\mathfrak{m}_\psi^{(2)}} \right] \left[\frac{\mu_3}{\mathfrak{m}_\psi^{(3)}} \right] = 1. \quad (48)$$

В свою очередь, равенство (48) проверяется непосредственно, если воспользоваться мультипликативностью символа $\left[\frac{\mu}{\mathfrak{a}} \right]$.

Рассмотрим теперь все характеры X , для которых определен инвариант $[X]_\psi$ с фиксированной функцией ψ . Пусть $X_1, \dots, X_m$ — базис этой группы и

$$X = X_1^{c_1} \dots X_m^{c_m} \quad (49)$$

— запись произвольного характера через базисные. При фиксированном поле $\bar{K}$ инвариант $[X]_\psi$ может быть записан в виде $\zeta^{f(c_1, \dots, c_m)}$, где ζ — некоторый корень степени l из 1, $f(c_1, \dots, c_m)$ является функцией от m переменных, причем как аргументы, так и функция пробегает значения из поля классов вычетов по модулю l .

Докажем, что имеет место представление:

$$f(c_1, \dots, c_m) = \sum_{i,k=1}^m a_{i,k} c_i c_k + \sum_{i=1}^m b_i c_i \quad (a_{i,k} = a_{k,i}) \quad \text{при } l \neq 2,$$

$$f(c_1, \dots, c_m) = \sum_{1 \leq i < k \leq m} a_{i,k} c_i c_k + \sum_{i=1}^m b_i c_i \quad \text{при } l = 2. \quad (50)$$

Для этого обозначим через $\bar{c}$ вектор с координатами $(c_1, \dots, c_m)$ из поля классов вычетов по модулю l . Тогда равенство (47) запишется так:

$$f(c + d + e) - f(c + d) - f(c + e) - f(d + e) + f(c) + f(d) + f(e) = 0.$$

Отсюда следует, что симметричная относительно $\mathbf{c}$ и $\mathbf{d}$ функция

$$\varphi(\mathbf{c}, \mathbf{d}) = f(\mathbf{c} + \mathbf{d}) - f(\mathbf{c}) - f(\mathbf{d}) \quad (51)$$

линейна как по аргументу $\mathbf{c}$, так и по аргументу $\mathbf{d}$.

При $l \neq 2$ мы можем записать $\varphi(\mathbf{c}, \mathbf{d})$ в виде:

$$\varphi(\mathbf{c}, \mathbf{d}) = \sum_{i,k=1}^m a_{i,k} c_i d_k \quad (a_{i,k} = a_{k,i}).$$

Если мы положим

$$f_1(c_1, \dots, c_m) = \sum_{i,k=1}^m \frac{1}{2} a_{i,k} c_i c_k, \quad (52)$$

то f_1 будет, как легко проверить, удовлетворять тому же соотношению (51), что и f . Из этого следует, что функция $f(\mathbf{c}) - f_1(\mathbf{c})$ линейна относительно $\mathbf{c}$, т. е.

$$f = f_1 + \sum_{i=1}^m b_i c_i,$$

что вместе с (52) дает в этом случае формулу (50).

При $l = 2$ мы можем записать φ в виде

$$\varphi = \sum_{1 \leq i < k \leq m} a_{i,k} (c_i d_k + d_i c_k) + \sum_{i=1}^m \alpha_i c_i d_i.$$

Положим

$$f_1(c_1, \dots, c_m) = \sum_{1 \leq i < k \leq m} a_{i,k} c_i c_k.$$

Как легко проверить,

$$f_1(\mathbf{c} + \mathbf{d}) - f_1(\mathbf{c}) - f_1(\mathbf{d}) = \sum_{1 \leq i < k \leq m} a_{i,k} (c_i d_k + d_i c_k).$$

Таким образом, если положим $f_2 = f - f_1$, то будем иметь:

$$f_2(\mathbf{c} + \mathbf{d}) - f_2(\mathbf{c}) - f_2(\mathbf{d}) = \sum_{i=1}^m \alpha_i c_i d_i. \quad (53)$$

Положим в равенстве (53) $c = d$. В левой части мы получим:

$$f_2(c + c) - f_2(c) - f_2(c) = 0,$$

а, следовательно,

$$\sum_{i=1}^m \alpha_i c_i^2 = \sum_{i=1}^m \alpha_i c_i = 0.$$

Так как это равенство имеет место для всех c_i , то отсюда следует, что $\alpha_1 = \dots = \alpha_m = 0$. Ввиду этого, функция $f(c) - f_1(\bar{c})$ линейна относительно c , откуда, как и раньше, следует (50).

Рассмотрим теперь любой характер X группы $Z_d^{(r)}$, для которого определен инвариант $[X]_\psi$. При любом каноническом гомоморфизме S ему соответствует характер X^S группы $Z_d^{(r)}$, для которого инвариант $[X^S]_\psi$ также определен. Если записать X^S в виде (49), то c_i будет функцией $c_i(S)$ гомоморфизма S . Ввиду (50), имеем:

$$f(S) = \sum a_{i,k} c_i(S) c_k(S) + \sum b_i c_i(S).$$

С другой стороны, формула (37) работы [4] показывает, что каждая функция $c_i(S)$ имеет степень $\leq n$ относительно S . Утверждение теоремы будет доказано, если мы покажем, что произведение двух функций, имеющих степень $\leq n$, имеет степень $\leq 2n$.

Мы докажем, что вообще, если $f(S)$ и $\varphi(S)$ имеют соответственную степени $\leq n$ и $\leq m$, то $f(S)\varphi(S)$ имеет степень $\leq n + m$. Воспользуемся индукцией по n и m . Нам надо доказать, что

$$f(S * T)\varphi(S * T) - f(S)\varphi(S) - f(T)\varphi(T) \quad (54)$$

имеет как относительно S , так и относительно T степень $\leq n + m - 1$.

Для упрощения записи обозначим выражение $f(S * T) - f(S) - f(T)$ через Δf . Непосредственным приведением подобных членов проверяется следующее тождество:

$$\begin{aligned} \Delta(f\varphi) &= \Delta f \Delta \varphi + f(S) \Delta \varphi + f(T) \Delta \varphi + \varphi(S) \Delta f + \varphi(T) \Delta f + \\ &\quad + f(S) \varphi(T) + \varphi(S) f(T). \end{aligned} \quad (55)$$

Если m или n равно 0, то $f\varphi$ очевидным образом имеет степень, равную $m + n$, так что в этом случае наше утверждение доказано. Рассмотрим теперь случай, когда ни m , ни n не равно 0, и найдем степень $\Delta(f\varphi)$ относительно S (ввиду симметрии S и T

степень относительно T будет такой же). Степень $\Delta f \leq m - 1$, а степень $\Delta \varphi \leq n - 1$. По индуктивному предположению, степень $\Delta f \Delta \varphi \leq m + n - 2$, степень $f(S) \Delta \varphi \leq m + n - 1$, степень $\varphi(T) \Delta f \leq m + n - 1$. Так как мы интересуемся теперь степенью относительно S , то $f(T)$ и $\varphi(T)$ являются постоянными. Очевидно, что при умножении на постоянную степень функции не изменяется. Таким образом степень $f(T) \Delta \varphi \leq n - 1$, степень $\varphi(T) \Delta f \leq m - 1$, степень $f(T) \varphi(S) \leq n$ и степень $f(S) \varphi(T) \Delta f \leq m$. Так как $m \geq 1$ и $n \geq 1$, то $m \leq m + n - 1$ и $n \leq m + n - 1$. Мы доказали, таким образом, что каждое слагаемое в формуле (55) имеет степень $\leq m + n - 1$, а значит, и степень $\Delta(f\varphi) \leq m + n - 1$. Теорема доказана.

Теперь мы можем перейти к доказательству того, что любое поле алгебраических чисел k/Ω с группой Галуа F можно погрузить при $l > c$ в поле K , нормальное над Ω и имеющее над k группу Галуа $\mathfrak{G}_{d,F}^{(c)}$ (как операторную группу).

Доказательство весьма тесно примыкает к содержанию n^0 §3 работы [4].

ТЕОРЕМА 9. Для любого натурального δ существует натуральное число $C(\delta)$ со следующим свойством: в любом шольцевом поле $\overline{K}$, имеющем над k группу Галуа $\mathfrak{G}_{d,F}^{(c,r)}$, над Ω — $F \mathfrak{G}_{d,F}^{(c,r)}$ с $d > C(\delta)$, и попарно l -взаимно простые числа α_i^u , существует подполе $\overline{K}^S$, у которого группа Галуа над k есть $\mathfrak{G}_{\delta,F}^{(c,r)}$, а над Ω — $F \cdot \mathfrak{G}_{\delta,F}^{(c,r)}$ и все инварианты $[\chi, X]$, $(X)_h$ и $[X]_\psi$ равны 1. Здесь $\overline{K}^S$ означает подполе, соответствующее некоторому операторному каноническому гомоморфизму S .

Доказательство. Сначала доказывается существование числа $C_1(\delta)$, которое обладает теми же свойствами, что и число $C(\delta)$ в формулировке теоремы 9, за исключением того, что у поля $\overline{K}^S$ инварианты $[X]_\psi$ не обязаны быть равными 1. Доказательство дословно повторяет доказательство теоремы 5 работы [4]. Мы его опускаем. Затем предполагается, что в поле $\overline{K}$ все инварианты $[\chi, X]$ и $[X]_\psi$ уже равны 1. Тогда это имеет место и для любого его подполя, соответствующего некоторому операторному каноническому гомоморфизму его группы Галуа. Доказывается, что для такого поля существует число $C_2(\delta)$, которое обладает теми же свойствами, что и число $C(\delta)$ в формулировке теоремы 9. Доказательство опять дословно повторяет доказательство теоремы 5 работы [4]. Очевидно, что если взять за $C(\delta)$ число $C_1(C_2(\delta))$, то $C(\delta)$ будет удовлетворять всем требованиям теоремы 9.

ТЕОРЕМА 10. Пусть задано произвольное нормальное поле алгебраических чисел k/Ω с группой Галуа F и F — операторная группа $\mathfrak{G}$ порядка l^α и класса c , причем $l > c$. Существует поле K , содержащее k , нормальное над Ω и имеющее над k группу Галуа $\mathfrak{G}$, а над Ω — $F \cdot \mathfrak{G}$.

Доказательство. Рассмотрим отдельно два случая:

1. k содержит корень степени l из 1. В этом случае мы можем применить все предшествующие рассуждения. Мы докажем даже, что поле $\bar{K}$ можно построить шольцевым и таким, чтобы соответствующие ему числа α_i^u были попарно l -взаимно просты.

Так как каждая группа $\mathfrak{G}$ является операторно гомоморфным образом некоторой группы $\mathfrak{G}_{d,F}^{(c)}$, то достаточно рассмотреть случай $\mathfrak{G} = \mathfrak{G}_{d,F}^{(c)}$. Мы рассмотрим более общий случай $\mathfrak{G} = \mathfrak{G}_{d,F}^{(c,r)}$. Доказательство будем вести индукцией по c , а при фиксированном c — индукцией по r . Так как $\mathfrak{G}_{d,F}^{(c,0)} = \mathfrak{G}_{d,F}^{(c-1)}$, а $\mathfrak{G}_{d,F}^{(c,k)} = \mathfrak{G}_{d,F}^{(c+1)}$, то достаточно рассмотреть только индукцию по r при фиксированном c .

Пусть нам надо построить поле K с группой Галуа $F \cdot \mathfrak{G}_{d,F}^{(c,r)}$ над Ω . Мы можем считать построенным поле $\bar{K}$ с группой $\mathfrak{G}_{d,F}^{(c,r-1)}$ с любым d . Возьмем за d число $C(\delta)$, существование которого установлено теоремой 9. Пусть $\bar{K}$ — поле с группой Галуа $F \cdot \mathfrak{G}_{\delta,F}^{(c,r-1)}$, над Ω , существование которого следует из индуктивного предположения. Согласно теореме 9, в нем существует подполе $\bar{K}^S$ с группой Галуа $F \cdot \mathfrak{G}_{\delta,F}^{(c,r-1)}$, над Ω и всеми инвариантами $[\chi, X]$, $(X)_h$ и $[X]_\psi$, равными 1. Как подполе шольцева поля $\bar{K}$, поле $\bar{K}^S$ — шольцево и все соответствующие ему числа α_i^u будут l -взаимно просты.

Из теоремы 5 настоящей работы следует, что поле $\bar{K}^S$ можно погрузить в шольцево поле K с группой Галуа $F \cdot \mathfrak{G}_{\delta,F}^{(c,r)}$ над Ω . Дословным повторением рассуждений, использованных при доказательстве теоремы 6 работы [4], доказывается, что у поля K числа α_i^u попарно l -взаимно просты.

2. k не содержит корня степени l из единицы. Пусть в результате присоединения к k этого корня получается поле $\bar{k}$ с группой Галуа $\bar{F}$ над Ω . Группа F имеет нормальный делитель H , являющийся группой Галуа $\bar{k}/k$. Рассмотрим $\mathfrak{G}$ как операторную группу с группой операторов $\bar{F}$, считая, что элементам H соответствует единичный оператор, а любому $\bar{u} \in \bar{F}$ соответствует тот же оператор, что и $u \in F$, если $u = \bar{u}H$. Ввиду того что в $\bar{k}$ содержится

корень степени l из 1, мы можем применить результат, полученный в случае 1, и построить поле $\overline{K}$ с группой $\overline{F} \cdot \mathfrak{G}$ над Ω . В группе $\overline{F} \cdot \mathfrak{G}$ H является нормальным делителем. К нему принадлежит нормальное подполе $K \supset k$, которое, очевидно, имеет над Ω группу Галуа $\overline{F} \cdot \mathfrak{G}/H \cong F \cdot \mathfrak{G}$. Теорема доказана.

Заметим в заключение, что ограничение $l > c$, накладывавшееся все время, использовалось нами только раз — при доказательстве теоремы 2. Это ограничение было существенно в том месте, где мы доказали, что представление Ли является прямым слагаемым тензорного представления. Как известно [см. [1], стр. 211], если $(m, l) = 1$, то любое представление группы F порядка m в поле характеристики l вполне приводимо. Отсюда следует, что представление Ли, являющееся фактором тензорного представления, содержится в нем в качестве прямого слагаемого. Таким образом, все предшествующие рассуждения сохраняют силу, если заменить ограничение $l > c$ ограничением $(m, l) = 1$. Мы получаем следующий результат:

ТЕОРЕМА 11. Пусть k/Ω — нормальное поле алгебраических чисел с группой Галуа F порядка m и G — любая группа, имеющая такой нормальный делитель $\mathfrak{G}$ порядка l^a , что $G/\mathfrak{G} \cong F$, $(m, l) = 1$. Существует поле $K \supset k$, нормальное над Ω и имеющее над ним группу Галуа G .

В формулировку теоремы не включено требование, чтобы G было полупрямым произведением F и $\mathfrak{G}$, так как, ввиду условия $(m, l) = 1$, это следует из теоремы Шура [см. [3], стр. 386].

ЛИТЕРАТУРА

1. Ван дер Варден, *Современная алгебра*, т.2, М., 1947.
2. Вейль Г., *Классические группы, их инварианты и представления*, М., 1947.
3. Курош А. Г., *Теория групп*, М., 1953.
4. Шафаревич И. Р., О построении полей с заданной группой Галуа порядка l^a , *Известия Ак. наук СССР, сер. матем.* **18** (1954), 261–296.
5. Шафаревич И. Р., Об одной теореме существования в теории алгебраических чисел, *Известия Ак. наук СССР, сер. матем.* **18** (1954), 327–334.
6. Brauer R., On algebras which are connected with the semisimple continuous groups, *Ann. Math.* **38** (1937), 857–872.
7. Scholtz A., Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe, *Math. Zeitschr.* **30** (1929), 332–356.
8. Thrall R. M., A note on a theorem by Witt, *Bull. Amer. Math. Soc.* **47** (1941), 303–308.

Поступило 10.V.1954

**ПОСТРОЕНИЕ ПОЛЕЙ
АЛГЕБРАИЧЕСКИХ ЧИСЕЛ С ЗАДАННОЙ
РАЗРЕШИМОЙ ГРУППОЙ ГАЛУА**

ИЗВ. АКАД. НАУК СССР, СЕР.

МАТЕМ., Т.18 (1954), 525-578

В работе доказывается, что над любым полем алгебраических чисел существует бесконечное число расширений с наперед заданной разрешимой группой Галуа.

Введение

В настоящей работе излагается метод построения расширений заданного поля алгебраических чисел, имеющих наперед заданную разрешимую группу Галуа. В частности, дается доказательство существования таких расширений.

Основным аппаратом, которым мы пользуемся, являются введенные в работе [6] инварианты полей, группа Галуа которых имеет порядок l^α , и развитая в той же работе теория композиции гомоморфизмов групп порядка l^α и функций гомоморфизмов. Эти соображения, относящиеся к полям с группой Галуа порядка l^α , оказываются применимыми здесь, так как задача построения полей с заданной разрешимой группой Галуа тесно связана с некоторыми вопросами теории полей с группой Галуа порядка l^α . Эта связь дается теоретико-групповой теоремой, доказанной независимо Д. К. Фаддеевым (см. [4] и [5]) и Гашютцем (Gaschütz) [1]. Если высказать теорему Фаддеева-Гашютца как теорему не об абстрактных группах, а о группах Галуа, то она получит следующую формулировку (см. Kochendörffer [2]). Пусть задана группа $\mathfrak{G}$ с абелевым нормальным делителем A порядка l^α и $\Omega \subset L \subset k \subset K \subset K^*$ есть последовательность полей со следующими свойствами: k/Ω нормально и имеет группу Галуа $G \cong \mathfrak{G}/A$, L принадлежит в k к силовой

l -подгруппе H группы G , K/L нормально и группа Галуа его изоморфна силовой подгруппе $\mathfrak{H}$ группы $\mathfrak{G}$, причем поля, сопряженные с K/Ω , независимы над k и их композит есть K^* . Тогда у поля K^*/k имеется подполе с группой Галуа, изоморфной $\mathfrak{G}$. В силу этой теоремы, при построенном поле k/Ω с группой Галуа G , построение поля с группой Галуа $\mathfrak{G}$ над Ω сводится к построению содержащего k поля K/L с заданной группой Галуа $\mathfrak{H}$ порядка l^α , но такого, что поля, сопряженные к K/Ω , независимы над k . При этом для построения поля с заданной разрешимой группой Галуа этот прием надо применять несколько раз и добиться того, чтобы на каждом шаге конструкция указанного поля с группой Галуа порядка l^α действительно была выполнима. Эта задача и решается в настоящей статье.

Мы предполагаем все рассматриваемые поля k/Ω шольцевыми относительно некоторого модуля M (определение см. в §1). Это гарантирует нам то, что в поле k/L (L принадлежит к силовой l -подгруппе группы Галуа k/Ω) любая система множителей, состоящая из корней степени l из единицы, распадается, а поэтому поле K с указанными выше свойствами можно построить, проводя убывающий центральный ряд в группе $\mathfrak{H}$ через нормальный делитель A .

Основная трудность заключается в том, что теперь нам необходимо, чтобы и вновь построенное поле K^* было шольцевым. Вводятся некоторые инварианты поля k/Ω , обращение которых в 1 является необходимым и достаточным условием того, что поле K^* может быть построено шольцевым. Наконец, того, чтобы инварианты поля k/Ω обратились в 1, можно добиться следующим образом. За G берется некоторая “приведенная свободная” группа, причем каждая разрешимая группа является факторгруппой некоторой “приведенной свободной”. Вместо того, чтобы строить поле k с группой G , мы строим поле $\tilde{k}$ с группой $\tilde{G}$, которая является “приведенной свободной” того же типа, что и G , но с гораздо большим числом образующих. Путем применения развитой в работе [6] теории композиции гомоморфизмов удастся показать, что в $\tilde{k}$ содержится подполе k с группой Галуа G и всеми инвариантами, равными 1.

Предполагается, что читателю известны работы [6], [7] и [8]. Краткое изложение полученных здесь результатов было опубликовано раньше (см. [9]). Сравнительно с изложенным в [9] в настоящей работе удалось добиться некоторых упрощений. Наиболее существенное из них заключается в следующем. Как известно (см. Оге [3]), в любой разрешимой группе имеется полудополненный нильпотентный нормальный делитель. Ввиду этого, любая разрешимая группа является факторгруппой некоторого полупря-

мого произведения групп порядков l^α . Проведение набросанного выше построения для таких групп заметно проще, чем для любых разрешимых. Мысль о том, что результат Оре, о котором сейчас было сказано, может быть применен к построению полей с разрешимой группой Галуа, была сообщена мне Д. К. Фаддеевым, с любезного разрешения которого я ею здесь воспользовался.

В этой работе не раз встречаются ссылки на результаты Д. К. Фаддеева. Однако я обязан ему гораздо больше, чем могут отразить ссылки на его работы. За многократные обсуждения и советы, поданные мне Дмитрием Константиновичем, я рад высказать ему здесь глубокую благодарность.

§1. Инварианты относительно-абелевых полей

1. Формулировка задачи. Мы дадим сейчас определение одного класса полей, который интересен тем, что для него задача погружения имеет положительное решение в ряде наиболее важных случаев.

Пусть Ω есть поле алгебраических чисел, k/Ω – нормальное расширение и M – натуральное число, делящееся на все простые делители степени k/Ω . Расширение k/Ω будет называться шольцевым относительно M , если выполнены следующие условия:

1⁰. Все простые дивизоры k , критические в k/Ω , имеют относительный порядок 1 над Ω .

2⁰. Для любого простого критического дивизора $\mathfrak{P}$ поля k/Ω

$$\mathfrak{N}(\mathfrak{P}) \equiv 1 \pmod{M},$$

где $\mathfrak{N}(\mathfrak{P})$ означает абсолютную норму $\mathfrak{P}$.

3⁰. Все простые делители M и Ω полностью распадаются в k .

4⁰. Все вещественные бесконечно удаленные простые дивизоры Ω распадаются в k только на вещественные.

Если λ есть простой делитель M , то максимальную степень λ , делящую M , мы будем обозначать в дальнейшем через M_λ .

Если $l|M$, $k \ni \zeta$, где ζ есть корень степени l из 1, и $(k : \Omega)$ и M являются степенями l , то понятие шольцевости совпадает с тем, которое введено для полей степени l^α в работе [6].

Если дано число M и его простой делитель l , то нормальное расширение k/Ω , содержащее корень ζ степени l из 1, будет называться шольцевым относительно M и l , если $k/\Omega(\zeta)$ шольцево относительно M и для любого не делящего l простого делителя p дискриминанта поля k/Ω

$$\mathfrak{N}(p) \equiv 1 \pmod{l}. \quad (1)$$

Очевидно, что если $\Omega \ni \zeta$, то понятие шольцевости относительно M и шольцевости относительно M и l совпадают. В общем случае эти понятия связываются следующими двумя утверждениями.

ЛЕММА 1. Если k/Ω – шольцево относительно M и $l|M$, то $k(\zeta)/\Omega$ – шольцево относительно M и l .

Проверим сначала все требования шольцевости относительно M для поля $k(\zeta)/\Omega(\zeta)$.

1) Пусть $\overline{\mathfrak{P}}$ – критический простой дивизор $k(\zeta)/\Omega(\zeta)$, $\mathfrak{P}$ – его делитель в k , $\overline{\mathfrak{p}}$ – в $\Omega(\zeta)$, а $\mathfrak{p}$ – в Ω . Очевидно, что $\mathfrak{P}$ или критический в k/Ω или делитель l , так как $k(\zeta) = k \cdot \Omega(\zeta)$. Второй случай встретиться не может. В самом деле, если $\overline{\mathfrak{P}}|l$, то $\mathfrak{p}$ полностью распадается в k и получающаяся $\mathfrak{p}$ -адическим замыканием алгебра $k_{\mathfrak{p}}$ является прямой суммой полей $\Omega_{\mathfrak{p}}$. Алгебра $\Omega(\zeta)_{\mathfrak{p}}$ есть прямая сумма полей $\Omega(\zeta)_{\overline{\mathfrak{p}}}$, а поэтому алгебра $k(\zeta)_{\mathfrak{p}} = k_{\mathfrak{p}} = \Omega(\zeta)_{\mathfrak{p}}$ является также прямой суммой полей $\Omega_{\overline{\mathfrak{p}}}$. Из этого следует, что порядок и показатель ветвления для $\overline{\mathfrak{P}}$ в $k(\zeta)/\Omega$ – те же, что для $\overline{\mathfrak{p}}$ в $\Omega(\zeta)$. Из мультипликативности этих чисел при последовательных расширениях и из того, что они равны 1 в k/Ω следует, что они равны 1 и в $k(\zeta)/\Omega(\zeta)$. Таким образом, $(\overline{\mathfrak{P}}, l) = 1$, а простые делители l и $\Omega(\zeta)$ полностью распадаются в $k(\zeta)$.

Мы видим, что $\mathfrak{P}$ – критический в k/Ω . Так как он имеет там порядок 1, то любое число из k сравнимо с числом из $\Omega \pmod{\mathfrak{P}}$. Из этого следует, что любое число из $k(\zeta)$ сравнимо с числом из $\Omega(\zeta) \pmod{\overline{\mathfrak{P}}}$, а это и значит, что порядок $\overline{\mathfrak{P}}$ равен 1.

2) Из предыдущего рассуждения следует, что если $\overline{\mathfrak{P}}$ – критический в $k(\zeta)/\Omega(\zeta)$, то его кратное $\mathfrak{P}$ – критическое в k/Ω . Так как

$$\mathfrak{n}(\overline{\mathfrak{P}}) = \mathfrak{n}(\mathfrak{P}), \quad \mathfrak{n}(\mathfrak{P}) \equiv 1 \pmod{M},$$

то

$$\mathfrak{n}(\overline{\mathfrak{P}}) \equiv 1 \pmod{M}.$$

3) Для простых делителей l свойство 3^0 уже доказано. Если $\lambda|M$, $\lambda \neq l$, то для простых делителей λ доказательство дословно повторяет доказательство свойства 3^0 .

Наконец, свойство 4^0 для $k(\zeta)/\Omega(\zeta)$ тривиально, так как при $l = 2$ $\zeta \in \Omega$, а при $l > 2$ $\Omega(\zeta)$ чисто мнимо.

Для проверки сравнения (1) заметим, что простые делители дискриминанта $k(\zeta)/\Omega$, взаимно простые с l , являются, как нами доказано, простыми делителями дискриминанта k/Ω , для них же сравнение (1) следует из условий 1^0 и 2^0 в определении шольцева поля, так как $l|M$.

Обращение леммы 1, вообще говоря, неверно, однако имеет место следующее, несколько более слабое утверждение.

ЛЕММА 2. Если k/Ω — шольцево относительно M , k' — нормальное расширение k и $(k' : k)$ является степенью l , где l — простой делитель M , то из шольцевости $k'(\zeta)/\Omega$ относительно M и l следует шольцевость k'/Ω относительно M .

Проверим для k'/Ω все требования шольцевости относительно M .

1) Обозначим $k'(\zeta)$ через $\bar{k}'$, $k(\zeta)$ через $\bar{k}$, $\Omega(\zeta)$ через $\bar{\Omega}$. Пусть $\bar{\mathfrak{P}}'$ — простой дивизор $\bar{k}'$. Обозначим делящиеся на него простые дивизоры в k' через $\mathfrak{P}'$, в $\bar{k}$ — через $\bar{\mathfrak{P}}$, в k — через $\mathfrak{P}$, в $\bar{\Omega}$ — через $\bar{\mathfrak{p}}$, в Ω — через $\mathfrak{p}$. Поле классов вычетов дивизора $\mathfrak{p}$ в Ω будем обозначать через $\Omega[\mathfrak{p}]$.

Пусть $\mathfrak{P}'$ — критический дивизор k'/Ω . Ввиду условия (1),

$$\bar{k}[\bar{\mathfrak{P}}] = k[\mathfrak{P}].$$

С другой стороны,

$$\bar{k}'[\bar{\mathfrak{P}}'] = \bar{k}[\bar{\mathfrak{P}}]k'[\mathfrak{P}'] = k'[\mathfrak{P}'],$$

так как

$$\bar{k}[\bar{\mathfrak{P}}] = k[\mathfrak{P}] \subset k'[\mathfrak{P}'].$$

По условию,

$$\bar{k}'[\bar{\mathfrak{P}}'] = \bar{k}[\bar{\mathfrak{P}}].$$

Отсюда следует, что

$$k'[\mathfrak{P}'] = k[\mathfrak{P}].$$

Так как, по условию,

$$k[\mathfrak{P}] = \Omega[\mathfrak{p}],$$

то

$$k'[\mathfrak{P}'] = \Omega[\mathfrak{p}],$$

что и означает, что $\mathfrak{P}'$ имеет в k'/Ω порядок 1.

2) Как мы доказали,

$$\bar{k}'[\bar{\mathfrak{P}}'] = k'[\mathfrak{P}'] = k[\mathfrak{P}].$$

Из этого следует, что

$$\mathfrak{n}(\bar{\mathfrak{P}}') = \mathfrak{n}(\mathfrak{P}').$$

Таким образом,

$$\mathfrak{N}(\mathfrak{P}') = \mathfrak{N}(\overline{\mathfrak{P}'}') \equiv 1 \quad (M).$$

3) Пусть теперь $\overline{\mathfrak{M}'}$ — делитель M в $\overline{k'}$. По условию, мы имеем:

$$k_{\mathfrak{M}} = \Omega_{\tau}, \quad \overline{k'_{\mathfrak{M}'}} = \overline{k_{\mathfrak{M}}}.$$

Из соотношений

$$\overline{k'_{\mathfrak{M}'}} = \overline{k_{\mathfrak{M}}} k'_{\mathfrak{M}'} = \overline{\Omega_{\tau}} k'_{\mathfrak{M}'}, \quad \overline{k_{\mathfrak{M}}} = \overline{\Omega_{\tau}} k_{\mathfrak{M}} = \overline{\Omega_{\tau}}$$

мы выводим:

$$\overline{k_{\mathfrak{M}}} = \overline{k_{\mathfrak{M}}} k'_{\mathfrak{M}'}. \quad (2)$$

Так как по условию $(k' : k)$, а следовательно, и $(k'_{\mathfrak{M}'} : k_{\mathfrak{M}})$ есть степень l , а $(\overline{k} : k)$ (а значит, и $(\overline{k_{\mathfrak{M}}} : k_{\mathfrak{M}})$) делит $l-1$ и поэтому взаимно просто с l , то мы можем заключить из (2), что $k'_{\mathfrak{M}'} = k_{\mathfrak{M}} = \Omega_{\tau}$, что и означает, что простые делители M полностью распадаются в k'/Ω .

Наконец, условие 4^0 очевидно, так как при $l = 2$ $\zeta \in \Omega$, а при $l > 2$ k'/k имеет нечетную степень, а поэтому чисто вещественно.

Лемма доказана.

Перейдем к рассмотрению цепочки полей, которая соответствует, согласно теории Галуа, цепочке групп, исследуемой в теореме Фаддеева-Гашютца.

Рассмотрим пять полей алгебраических чисел

$$\Omega \subset L \subset k \subset K \subset K^*, \quad (3)$$

обладающих следующими свойствами: k/Ω есть нормальное расширение с группой Галуа G , L принадлежит силовской l -подгруппе H , K/L нормально и является простым центральным расширением k/L , K/Ω не нормально и поля, сопряженные с K относительно Ω , независимы над k ; их композит есть K^* .

В этом и следующем параграфах будет разобрана следующая задача: найти условия, которым должно удовлетворять шольцево относительно M и l поле k/Ω для того, чтобы существовало поле K , группа Галуа которого является заданным простым центральным расширением группы Галуа k/L и такое, чтобы поле K^*/Ω было шольцевым относительно M и l . Ответ будет дан в терминах некоторых инвариантов поля k/Ω , к определению которых мы сейчас и переходим. В дальнейшем мы будем все время считать поле k/Ω шольцевым относительно M и l . Будем, таким образом, предполагать, что k содержит корень ζ степени l из 1 и положим

$$\zeta^{\sigma} = \zeta^{g(\sigma)}, \quad \sigma \in G.$$

Очевидно, что

$$g(\sigma\tau) \equiv g(\sigma)g(\tau) \quad (l). \quad (4)$$

2. Инварианты $[\chi, X]$. Возьмем произвольный характер χ порядка l группы H и такое соответствующее ему число α_χ из L , что

$$\sqrt[l]{\alpha_\chi} \in k, \quad \sqrt[l]{\alpha_\chi}^h = \chi(h)\sqrt[l]{\alpha_\chi}, \quad h \in H.$$

Рассмотрим разложение α_χ на простые множители в k . В первых, мы имеем:

$$(\alpha_\chi) = a_\chi b^l,$$

где a_χ и b – простые дивизоры из L , причем a_χ состоит только из критических простых дивизоров k/L . Так как α_χ определяется характером χ однозначно с точностью до l -равенства, то a_χ зависит только от χ , а не от выбора соответствующего ему α_χ .

Если p есть простой делитель a_χ в L , то, ввиду условия 1^0 в определении шольцева поля,

$$p = \mathfrak{p}^{\sum h},$$

где $\mathfrak{p}$ – простой дивизор из k , а сумма в показателе распространена на все $h \in H$. Если $\sigma \in G$ и $\tau \in G$, то, как легко видеть,

$$\mathfrak{p}^{\sigma \sum h} = \mathfrak{p}^{\tau \sum h}$$

тогда и только тогда, когда классы по двойному модулю $\mathfrak{z}_{\mathfrak{p}} \sigma H$ и $\mathfrak{z}_{\mathfrak{p}} \tau H$ совпадают. Здесь $\mathfrak{z}_{\mathfrak{p}}$ означает группу разложения $\mathfrak{p}$.

Таким образом, разложение α_χ на простые множители в k имеет вид:

$$(\alpha_\chi) = b^l \prod_{\mathfrak{p}} \mathfrak{p}^{\sum \varphi_{\mathfrak{p}, \chi}(\mathfrak{S}) \sigma \sum h}.$$

Здесь $\mathfrak{p}$ пробегает все не сопряженные между собой критические дивизоры k/L , $\mathfrak{S}$ – классы смежности G по двойному модулю $(\mathfrak{z}_{\mathfrak{p}}, H)$ и σ – произвольный представитель $\mathfrak{S}$.

Рассмотрим класс X l -инвариантных чисел поля k/L . Пусть $\mathfrak{D}(X)$ – дивизор, соответствующий классу X (определение его см. в [6], стр. 266), и μ – произвольный представитель X . Предположим, что для любого критического дивизора $\mathfrak{p}$

$$(\mathfrak{D}(X))^{\sum \varphi_{\mathfrak{p}, \chi}^*(\mathfrak{T}) \tau, \mathfrak{p}} \approx 1. \quad (5)$$

Здесь $\varphi_{\mathfrak{p}, \chi}^*(\mathfrak{T})$ означает функцию на классах смежности по двойному модулю $(H, \mathfrak{z}_{\mathfrak{p}})$, определенную соотношением

$$\varphi_{\mathfrak{p}, \chi}^*(\mathfrak{T}) \equiv \varphi_{\mathfrak{p}, \chi}(\mathfrak{T}^{-1})g(\tau) \quad (l),$$

а τ , как и раньше, — произвольный представитель $\mathfrak{T}$.

Заметим, что функция $g(\tau)$ удовлетворяет условиям:

$$g(z\tau) = g(\tau z) = g(\tau h) = g(h\tau) = g(\tau), \quad h \in H, \quad z \in \mathfrak{Z}_{\mathfrak{P}}, \quad (6)$$

так что $\varphi^*(\mathfrak{T})$ действительно является функцией на классах смежности по модулю $(H, \mathfrak{Z}_{\mathfrak{P}})$.

Для доказательства условий (6) нам достаточно показать, что

$$g(h) \equiv 1 \pmod{l}, \quad h \in H, \quad (7)$$

$$g(z) \equiv 1 \pmod{l}, \quad z \in \mathfrak{Z}_{\mathfrak{P}}. \quad (8)$$

Так как порядок H есть степень l , то (7) следует из (4) и из того, что

$$g(h)^{l-1} \equiv 1 \pmod{l}.$$

Очевидно, что автоморфизмы $z \in \mathfrak{Z}_{\mathfrak{P}}$ индуцируют в поле $\Omega(\zeta)/\Omega$ автоморфизмы группы разложения простого дивизора этого поля, делящегося на $\mathfrak{P}$. Ввиду условия (1) и предположений шольцевости относительно M и l поля k/Ω , дивизор $\mathfrak{p}$ из Ω полностью распадается в $\Omega(\zeta)$, так что группа разложения его простого делителя в этом поле равна 1. Отсюда следует, что $\zeta^z = \zeta$ при $z \in \mathfrak{Z}_{\mathfrak{P}}$, т. е. условие (8).

Для того, чтобы условие (5) имело определенный смысл, нам надо показать, что выполнение его не зависит от выбора представителей τ в классах $\mathfrak{T}$ по модулю $(H, \mathfrak{Z}_{\mathfrak{P}})$.

Очевидно, что

$$\mathfrak{D}(X)^{\tau} = \mathfrak{D}(X)^{h\tau}$$

при $h \in H$, так как $\mathfrak{D}(X)$ — дивизор, инвариантный относительно h . Обозначим через $[\mathfrak{D}(X)]_{\mathfrak{P}}$ ту степень $\mathfrak{P}$, которая входит в $\mathfrak{D}(X)$. Из очевидных равенств

$$\begin{aligned} [\mathfrak{D}(X)^{\tau z}]_{\mathfrak{P}} &= ([\mathfrak{D}(X)^{\tau}]_{\mathfrak{P}})^z = [\mathfrak{D}(X)^{\tau}]_{\mathfrak{P}}, \\ \mathfrak{P}^z &= \mathfrak{P}, \quad z \in \mathfrak{Z}_{\mathfrak{P}}, \end{aligned} \quad (9)$$

мы получаем:

$$[\mathfrak{D}(X)^{\tau z}]_{\mathfrak{P}} = [\mathfrak{D}(X)^{\tau}]_{\mathfrak{P}},$$

что и доказывает наше утверждение.

Если условие (5) выполнено, то мы определяем смысл $[\chi, X]$, полагая

$$[\chi, X] = \prod_{\mathfrak{P}} \left(\frac{\mu^{\sum \varphi_{\mathfrak{P}, \chi}^*(\mathfrak{T})\tau}}{\mathfrak{P}} \right)_k \left(\frac{\alpha_{\chi}}{\mathfrak{m}} \right)_L^{-1}, \quad (10)$$

где $\mathfrak{P}$ пробегает все не сопряженные между собой критические простые дивизоры k/Ω , а m есть дивизор из разложения

$$\mu = \mathfrak{C}^l \mathfrak{D}(X)m \quad (11)$$

(см. [6], стр. 266). Если условие (5) не выполнено, то символ $[\chi, X]$ не определен.

Перейдем к доказательству того, что символ $[\chi, X]$ не зависит от выбора:

- а) представителей τ в классах $\mathfrak{T}$,
- б) дивизора $\mathfrak{P}$ среди совокупности сопряженных друг с другом дивизоров и
- с) μ в классе X .

Для доказательства утверждения а) покажем сначала, что если $z \in \mathfrak{Z}_{\mathfrak{P}}$, то для любого A , для которого

$$(A^{1-z}, \mathfrak{P}) \approx 1,$$

имеем:

$$\left(\frac{A^{1-z}}{\mathfrak{P}} \right) = 1, \quad z \in \mathfrak{Z}_{\mathfrak{P}}. \quad (12)$$

Очевидно, что класс вычетов $A^{1-z} \bmod \mathfrak{P}$ имеет в мультипликативной группе классов вычетов $\bmod \mathfrak{P}$ порядок, делящий порядок $e_{\mathfrak{P}}$ группы разложения $\mathfrak{P}$. Так как порядок группы классов вычетов есть $\mathfrak{N}(\mathfrak{P}) - 1$, то условие (12) следует из соотношения

$$\mathfrak{N}(\mathfrak{P}) \equiv 1 \pmod{e_{\mathfrak{P}}}. \quad (13)$$

Действительно, из (13) ввиду сказанного выше следует, что индекс подгруппы, порожденной классом $A^{1-z} \bmod \mathfrak{P}$ в группе классов вычетов, делится на l , а значит, этот класс является l -й степенью некоторого другого класса, что эквивалентно (12).

Для доказательства (13) мы воспользуемся произволом в выборе числа M , относительно которого мы предполагали поле k/Ω шольцевым. Мы потребуем, чтобы любой простой делитель l степени $(k : \Omega)$ входил в M в степени, по крайней мере на единицу большей, чем та, в которой он входит в показатель (общий наибольший делитель порядков элементов) группы G . При этом условии соотношение (13) будет, очевидно, выполняться, так как, с одной стороны, ввиду того, что $(\mathfrak{P}, l) = 1$,

$$\mathfrak{N}(\mathfrak{P}) \equiv 1 \pmod{e_{\mathfrak{P}}},$$

а с другой — $\mathfrak{N}(\mathfrak{P}) - 1$ делится на l в степени, по крайней мере на единицу большей, чем $e_{\mathfrak{P}}$, что следует из введенного нами условия и того, что $e_{\mathfrak{P}}$ является порядком циклической (ввиду шольцевости k) группы $\mathfrak{Z}_{\mathfrak{P}}$.

Теперь утверждение а) доказывается совсем просто. Нам надо доказать, что выражение (10) не изменится, если какое-нибудь τ заменить другим представителем $h\tau z$, $h \in H$, $z \in \mathfrak{Z}_{\mathfrak{P}}$, того же класса смежности по двойному модулю $(H, \mathfrak{Z}_{\mathfrak{P}})$. Но инвариантность относительно умножения на h следует из l -инвариантности μ в k/L , а относительно z — из (12).

Переходим к доказательству утверждения б). Пусть $\mathfrak{P}^{\theta}$ — дивизор, сопряженный с $\mathfrak{P}$. Тогда

$$\mathfrak{P}^{\sigma} = \mathfrak{P}^{\theta\theta^{-1}\sigma} \quad \text{и} \quad (\alpha_{\chi}) = \mathfrak{b}^l \prod \mathfrak{P}^{\theta \sum \varphi_{\mathfrak{P}, \chi}(\mathfrak{S})\theta^{-1} \sum h}.$$

При этом когда σ пробегает полную систему представителей классов смежности по модулю $(\mathfrak{Z}_{\mathfrak{P}}, H)$, $\theta^{-1}\sigma$ пробегает также полную систему представителей классов смежности по модулю $(\theta^{-1}\mathfrak{Z}_{\mathfrak{P}}\theta, H) = (\mathfrak{Z}_{\mathfrak{P}^{\theta}}, H)$, так как из

$$G = \sum \mathfrak{Z}_{\mathfrak{P}}\sigma_i H$$

следует:

$$G = \sum \theta^{-1}\mathfrak{Z}_{\mathfrak{P}}\theta\theta^{-1}\sigma_i H.$$

Если $\mathfrak{S} = \mathfrak{Z}_{\mathfrak{P}}\sigma H$, то $\theta^{-1}\mathfrak{Z}_{\mathfrak{P}}\theta\theta^{-1}\sigma_i H$ мы будем обозначать через $\theta^{-1}\mathfrak{S}$. Таким образом,

$$(\alpha_{\chi}) = \mathfrak{b}^l \prod \mathfrak{P}^{\theta \sum \varphi_{\mathfrak{P}^{\theta}, \chi}(\mathfrak{R})\rho \sum h},$$

где $\mathfrak{R}$ пробегает все классы по модулю $(\mathfrak{Z}_{\mathfrak{P}}\theta, H)$, ρ — представитель $\mathfrak{R}$ и

$$\varphi_{\mathfrak{P}^{\theta}, \chi}(\mathfrak{R}) = \varphi_{\mathfrak{P}, \chi}(\theta\mathfrak{R}).$$

Теперь очевидно, что

$$(\mathfrak{D}(X)^{\sum \varphi_{\mathfrak{P}^{\theta}, \chi}^{*}(\mathfrak{U})v}, \mathfrak{P}^{\theta}) = (\mathfrak{D}(X)^{\sum \varphi_{\mathfrak{P}, \chi}^{*}(\mathfrak{U}^{\theta^{-1}})v\theta^{-1}\theta}, \mathfrak{P}^{\theta})^{\theta(\theta^{-1})},$$

где $\mathfrak{U}$ пробегает классы смежности по модулю $(H, \mathfrak{Z}_{\mathfrak{P}^{\theta}})$, $v \in \mathfrak{U}$. Если положить

$$\mathfrak{U}\theta^{-1} = \mathfrak{T}, \quad v\theta^{-1} = \tau,$$

то $\mathfrak{I}$ будет пробегать классы по модулю $(H, \mathfrak{Z}_{\mathfrak{P}})$, и $\tau \in \mathfrak{I}$. Следовательно,

$$(\mathfrak{D}(X)^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{U})v}, \mathfrak{P}^{\theta}) = (\mathfrak{D}(X)^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}, \mathfrak{P})^{\theta g(\theta^{-1})}.$$

Таким образом, выполнение условия (5), при котором определен символ $[\chi, X]$, не зависит от выбора $\mathfrak{P}$ среди сопряженных дивизоров.

Аналогично преобразуется и самый символ:

$$\left(\frac{\mu^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{U})v}}{\mathfrak{P}^{\theta}} \right) = \left(\frac{\mu^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau\theta}}{\mathfrak{P}^{\theta}} \right)^{g(\theta^{-1})} = \left(\frac{\mu^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}}{\mathfrak{P}} \right),$$

что и доказывает его независимость от выбора $\mathfrak{P}$ среди сопряженных дивизоров.

Нам остается доказать утверждение с). Очевидно, что достаточно проверить инвариантность выражения для $[\chi, X]$ при умножении μ на l -ю степень и на число $m \in L$, взаимно простое с дискриминантом k/L . Первое очевидно; при втором $\mathfrak{D}(X)$ не меняется и поэтому инвариантность условия (5) очевидна. Рассмотрим самый символ $[\chi, X]$:

$$\begin{aligned} & \prod_{\mathfrak{P}} \left(\frac{(\mu m)^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}}{\mathfrak{P}} \right) \left(\frac{\alpha_{\chi}}{m} \right)^{-1} = \\ & = \prod_{\mathfrak{P}} \left(\frac{\mu^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}}{\mathfrak{P}} \right) \left(\frac{\alpha_{\chi}}{m} \right)^{-1} \prod_{\mathfrak{P}} \left(\frac{m^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}}{\mathfrak{P}} \right) \left(\frac{\alpha_{\chi}}{m} \right)^{-1}. \end{aligned}$$

Нам надо, таким образом, доказать, что

$$\prod_{\mathfrak{P}} \left(\frac{m^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}}{\mathfrak{P}} \right)_k \left(\frac{\alpha_{\chi}}{m} \right)_L^{-1} = 1. \quad (14)$$

Действительно,

$$\begin{aligned} & \prod_{\mathfrak{P}} \left(\frac{m^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau}}{\mathfrak{P}} \right)_k = \prod_{\mathfrak{P}} \left(\frac{m}{\mathfrak{P}^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{T})\tau^{-1}g(\tau^{-1})}} \right)_k = \\ & = \prod_{\mathfrak{P}} \left(\frac{m}{\mathfrak{P}^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{S})\sigma}} \right)_k = \prod_{\mathfrak{P}} \left(\frac{m}{\mathfrak{P}^{\sum \varphi_{\mathfrak{P},x}^{\bullet}(\mathfrak{S})\sigma \sum h}} \right)_L = \left(\frac{m}{\alpha_{\chi}} \right)_L. \quad (15) \end{aligned}$$

Теперь (14) следует из (15) и из закона взаимности, так как α_X l -гиперпримарно ввиду условия 3^0 в определении шольцева поля.

Инварианты $[\chi, X]$ обладают свойствами:

$$[\chi_1 \chi_2, X] = [\chi_1, X][\chi_2, X], \quad (16)$$

$$[\chi, X_1 X_2] = [\chi, X_1][\chi, X_2], \quad (17)$$

$$[\chi_1, X_1] = [\chi, X], \quad (18)$$

причем в (16) и (17) предполагается, что оба символа в правой части определены, и утверждается, что тогда определена и левая часть. В (18) предполагается, что $k \subset k_1$, причем степень $(k_1 : k)$ есть степень l . Характер χ и класс X рассматриваются в k , а χ_1 и X_1 — характер и класс, соответствующие им в k_1 .

Заметим, что если k/Ω шольцево, то k/L тоже шольцево, причем если определен инвариант (χ, X) (см. [6], стр. 248), то определен и инвариант $[\chi, X]$, и они совпадают.

3. Инварианты $(X)_M$. Обозначим через L_M максимальное расширение L , имеющее абелеву группу показателя l и содержащееся в $L(\zeta_M)$, где ζ_M есть первообразный корень степени M из 1. Выберем в классе X такого представителя μ , чтобы в поле $k(\sqrt[l]{\mu})/\Omega$ все простые делители M в $\Omega(\zeta)$ полностью распадались. Для случая делителя M , являющегося в то же время делителем l , существование такого представителя доказано в работе [6], стр. 269. Если $q|M$, $(q, l) = 1$, $q \in L$, то, ввиду шольцевости k/Ω относительно M , q не разветвлено и имеет порядок 1 в k/Ω . Для того, чтобы q обладало этими же свойствами в $k(\sqrt[l]{\mu})/\Omega$, необходимо и достаточно выполнения условия

$$\left[\frac{\mu}{q} \right] = 1. \quad (19)$$

Очевидно, что найдя число m , удовлетворяющее условию

$$\left(\frac{m}{q} \right) = \left[\frac{\mu}{q} \right]^{-1}, \quad (20)$$

мы добьемся выполнения условия (19) для μm . Очевидно также, что условия (20) для различных $q|M$, $(q, l) = 1$, а также соответствующие условия для $q|l$ совместны.

Инвариант $(X)_M$ мы определим как класс $m\Lambda_M$ по подгруппе Λ_M , соответствующей полю L_M/L в смысле теории полей классов, к которому принадлежит дивизор m из разложения (11) выбранного таким образом представителя μ класса X .

Покажем, что $(X)_M$ не зависит от выбора μ в X , если только этот выбор подчинен указанным выше условиям. Действительно, другой представитель должен иметь вид μt , где t l -гиперпримарно и

$$\left(\frac{t}{q}\right) = 1 \quad \text{для } q|M, \quad (q, l) = 1.$$

Таким образом, t лежит в группе $S_{\mathfrak{F}}$, состоящей из l -х степеней лучевых классов по модулю $\mathfrak{F}$, являющемуся произведением модуля l -гиперпримарности и всех q , которые делят M , но не делят l . Поле, соответствующее $S_{\mathfrak{F}}$, является максимальным расширением поля L , имеющим абелеву группу показателя l и дискриминант, состоящий только из делителей M . Так как L_M также обладает всеми этими свойствами, за исключением максимальнойности, то оно содержится в этом поле и, следовательно, $\Lambda_M \supset S_{\mathfrak{F}}$, и из $t \in S_{\mathfrak{F}}$ следует, что $t \in \Lambda_M$.

Инвариант $(X)_M$ обладает свойствами

$$\begin{aligned} (X_1 X_2)_M &= (X_1)_M (X_2)_M, \\ (X_1)_M &= (X)_M, \end{aligned}$$

аналогичными (17) и (18).

Очевидно, что из $(X)_M = 1$ следует $(X)_{M_1} = 1$ при $M_1|M$. Точно так же очевидно, что $(X)_M$ может принимать только конечное число значений – заведомо не больше, чем M .

4. Инварианты $[X]_{\psi}$. Эти инварианты определены только для таких классов X l -инвариантных чисел поля k/L , для которых все инварианты $[\chi, X]$, которые определены, равны 1, а также $(X)_M = 1$.

В §2 будет доказано, что в каждом таком классе можно выбрать такого представителя μ , что в поле K^* , получающемся присоединением к k всех $\sqrt[l]{\mu^\sigma}$, все критические простые дивизоры k распадутся на дивизоры 1-го порядка. Это эквивалентно выполнению соотношений

$$\left(\frac{\mu^{\sum f_{\mathfrak{P}}(S)\sigma}}{\mathfrak{P}}\right) = 1 \quad (21)$$

для всех критических простых дивизоров $\mathfrak{P}$ поля k/Ω и всех функций $f_{\mathfrak{P}}(S)$ на правых классах смежности G по H , для которых

$$(\mathfrak{D}(X)^{\sum f_{\mathfrak{P}}(S)\sigma}, \mathfrak{P}) \approx 1.$$

Пока теорема 1 из §2 еще не доказана, мы будем считать, что инвариант $[X]_\psi$ определен для тех классов X , для которых существует представитель μ , удовлетворяющий условиям (21).

В дальнейшем мы всегда будем предполагать, что выбор представителя μ в X произведен именно таким образом.

Рассмотрим функцию $\psi(\mathfrak{S})$ на классах смежности $\mathfrak{S}$ группы G по двойному модулю (H, H) со значениями в поле классов вычетов $\text{mod } l$, обладающую следующими свойствами:

$$1^0. \psi(1) \equiv 0, \quad \psi^*(\mathfrak{S}) \equiv -\psi(\mathfrak{S}) \pmod{l}.$$

$$2^0. \mu \sum \psi(S)^\sigma \approx m_\psi \in L \quad \text{при} \quad \mu \in X.$$

Здесь S пробегает все правые классы смежности G по H , σ — любой представитель S , а $\psi(S)$ означает $\psi(\mathfrak{S})$, где $\mathfrak{S}$ — класс по двойному модулю (H, H) , содержащий S .

3⁰. Если $m_\psi = \mathfrak{d}m_\psi$ есть разложение m_ψ на множитель $\mathfrak{d}$, состоящий только из простых делителей дискриминанта k/L , и m_ψ , взаимно простой с дискриминантом, то

$$\mathfrak{d} = (\alpha_\chi) \prod_{\mathfrak{P}} \mathfrak{P}^{\sum f_{\mathfrak{P}}(S)^\sigma \sum h}, \quad (\mathfrak{D}(X)^{\sum f_{\mathfrak{P}}^*(\mathfrak{T})^\tau}, \mathfrak{P}) \approx 1, \quad (22)$$

где χ — один из характеров порядка l группы H .

Заметим, что путем умножения m_ψ на $\alpha_\chi^{-1} = (\sqrt[l]{\alpha_\chi})^{-l}$ мы можем добиться того, чтобы α_χ в формуле (22) не участвовало. Тогда $\mathfrak{d}$ будет определено однозначно с точностью до такого множителя α_χ , что инвариант $[\chi, X]$ определен.

При $l = 2$ мы наложим еще одно дополнительное условие. Пусть $\mathfrak{S}$ — инволютивный класс по двойному модулю, т. е. класс, совпадающий со своим обратным: $\mathfrak{S} = \mathfrak{S}^{-1}$. Каждому такому классу мы поставим в соответствие дивизор $\mathfrak{C}_\mathfrak{S}$ поля L по следующему правилу.

Пусть σ — представитель класса $\mathfrak{S}$, удовлетворяющий условию

$$\sigma^2 \in H. \quad (23)$$

Существование такого представителя следует из условия $\mathfrak{S}^{-1} = \mathfrak{S}$, как это доказано в приложении.

Обозначим через LL^σ композит полей L и L^σ , принадлежащий к подгруппе $H \cap H^\sigma$, а через Λ_σ — подполе, принадлежащее подгруппе $\{\sigma, H \cap H^\sigma\}$, порожденной σ и $H \cap H^\sigma$. Ввиду условия (22),

$$\{\sigma, H \cap H^\sigma\} = H \cap H^\sigma + \sigma H \cap H^\sigma$$

и, ввиду (23),

$$(LL^\sigma : \Lambda_\sigma) = 2.$$

Обозначив через $\mathfrak{D}_\sigma$ дифференту поля LL^σ/Λ_σ , мы положим

$$\mathfrak{C}_\mathfrak{S} = N_{LL^\sigma/L}(\mathfrak{D}_\sigma).$$

Условие, которое мы наложим на функцию ψ , записывается теперь в следующем виде:

$$4^0. \prod_{\mathfrak{S}} \mathfrak{C}_\mathfrak{S}^{\psi(\mathfrak{S})} \approx (\alpha_\chi) \text{ в } L, [\chi, X] \text{ определено,}$$

где произведение распространено на все инволютивные классы $\mathfrak{S}$ по двойному модулю (H, H) .

Очевидно, что все эти условия зависят только от функции ψ и класса X , а не от выбора μ в X . Если выполнены условия 1^0 , 2^0 и 3^0 , а при $l = 2$ и 4^0 , то мы определим символ $[X]_\psi$ следующим образом: выберем в X такого представителя μ , для которого

$$(m, m^\sigma) = 1 \quad \text{при} \quad \sigma \notin H \quad (24)$$

и положим

$$[X]_\psi = \left[\frac{\mu}{m_\psi} \right], \quad (25)$$

где $m_\psi = m^{\sum \psi(s)\sigma}$, а m — дивизор из разложения (11). Символ $\left[\frac{A}{b} \right]$ определен в работе [6], стр. 267.

Ввиду условия $\psi(1) \equiv 0$ (1) и условия (24), правая часть (25) действительно определена.

Докажем теперь, что символ $[X]_\psi$ не зависит от выбора представителя μ в классе X . Напомним, что при этом речь идет о выборе представителя, удовлетворяющего сформулированным в начале этого пункта условиям.

Положим

$$\mu' = \mu t, \quad m' = m(m), \quad m \in L,$$

причем t состоит из простых дивизоров L , имеющих в L/Ω порядок 1 и полностью распадающихся в k .

Дословным повторением рассуждений на стр. 400 работы [8] проверяется, что мы можем считать при этом выполненными следующие условия:

$$(m, m^\sigma) = 1, \quad (m, m^\sigma) = 1, \quad (m', m'^\sigma) = 1, \quad \sigma \notin H,$$

причем μ , m и μ' l -гиперпримарны.

Нам надо доказать, что

$$\left[\frac{\mu}{m_\psi} \right] = \left[\frac{\mu'}{m'_\psi} \right], \quad (26)$$

где

$$m'_\psi = m_\psi m^{\sum \psi(S)\sigma}.$$

Заметим, что $m^{\sum \psi(S)\sigma}$ есть число из L . Действительно, в приложении доказано, что если S пробегает все правые классы смежности по H , содержащиеся в одном двустороннем классе по (H, H) , а σ есть любой представитель S , то $\alpha^{\sum \sigma} \in L$, если $\alpha \in L$. Из того, что ψ постоянно на классах по двойному модулю (F, H) , следует, что $m^{\sum \psi(S)\sigma}$ есть произведение такого рода чисел и, следовательно, принадлежит L .

Переходя к доказательству (25), заметим, что

$$\left[\frac{\mu'}{m'_\psi} \right] = \left[\frac{\mu}{m_\psi} \right] \left(\frac{m}{m_\psi} \right) \left[\frac{\mu}{m^{\sum \psi(S)\sigma}} \right] \left(\frac{m}{m^{\sum \psi(S)\sigma}} \right). \quad (27)$$

Равенство (26) будет доказано, если мы покажем, что произведение второго и третьего множителей, а также четвертый множитель в правой части (27) равны 1.

В самом деле,

$$\left[\frac{\mu}{m^{\sum \psi(S)\sigma}} \right] = \left[\frac{\mu^{\sum \psi(S)\sigma^{-1}g(\sigma^{-1})}}{m} \right],$$

где σ^{-1} пробегает представителей левых классов смежности S^{-1} группы G по H . Так как из $S \in \mathfrak{S}$ следует, что $S^{-1} \in \mathfrak{S}^{-1}$, то, ввиду условий 1⁰ и 2⁰, мы имеем:

$$\left[\frac{\mu^{\sum \psi(S)\sigma^{-1}g(\sigma^{-1})}}{m} \right] = \left[\frac{\mu^{\sum \psi^*(S)\sigma}}{m} \right] = \left(\frac{m_{\psi^*}}{m} \right)^{-1}. \quad (28)$$

т. е.

$$\left(\frac{m}{m_\psi} \right) \left[\frac{\mu}{m^{\sum \psi(S)\sigma}} \right] = \left(\frac{m}{m_\psi} \right) \left(\frac{m_\psi}{m} \right)^{-1}. \quad (29)$$

Мы докажем, что

$$\left(\frac{m}{m_\psi} \right) = \left(\frac{m}{m_\psi} \right) \quad (30)$$

и тогда из (29), ввиду закона взаимности, будет следовать, что

$$\left(\frac{m}{m_\psi}\right) \left[\frac{\mu}{m \sum \psi(S)\sigma}\right] = 1.$$

Для доказательства (30) заметим, что

$$(m_\psi) = \mathfrak{d} m_\psi,$$

где $\mathfrak{d}$ удовлетворяет условию (22). Ввиду этого условия

$$\left(\frac{m}{\mathfrak{d}}\right)_L \prod_{\mathfrak{P}} \left(\frac{m}{\mathfrak{P} \sum f_{\mathfrak{P}(S)\sigma}\right)_k = \prod_k \left(\frac{m \sum f_{\mathfrak{P}(T)\tau}^*}{\mathfrak{P}}\right), \quad (30')$$

где

$$(\mathfrak{d} \sum f_{\mathfrak{P}(T)\tau}^*, \mathfrak{P}) \approx 1. \quad (31)$$

Так как μ уже удовлетворяет условию (21), то из (22) следует, что

$$\left(\frac{\mu \sum f_{\mathfrak{P}(T)\tau}^*}{\mathfrak{P}}\right) = 1,$$

а так как это же должно иметь место для μm вместо μ , то

$$\left(\frac{m \sum f_{\mathfrak{P}(T)\tau}^*}{\mathfrak{P}}\right) = 1.$$

Отсюда и из (30) следует, что

$$\left(\frac{m}{m_\psi}\right) = \left(\frac{m}{m_\psi}\right) \left(\frac{m}{\mathfrak{d}}\right)^{-1} = \left(\frac{m}{m_\psi}\right).$$

Доказательство того, что

$$\left(\frac{m}{m \sum \psi(S)\sigma}\right) = 1, \quad (32)$$

различно при $l \neq 2$ и при $l = 2$.

При $l \neq 2$ мы имеем:

$$\left(\frac{m}{m \sum \psi(S)\sigma}\right) = \left(\frac{m \sum \psi(S)\sigma^{-1}g(\sigma^{-1})}{m}\right),$$

ввиду того, что $\psi(S)$ постоянно на классах по двойному модулю (H, H) и на основании формулы (104) приложения. В силу условия 1^0 , имеем, как и при доказательстве (29):

$$\left(\frac{m \sum \psi(S) \sigma^{-1} g(\sigma^{-1})}{m} \right) = \left(\frac{m \sum \psi(S) \sigma}{m} \right)^{-1}.$$

Ввиду l -гиперпримарности m , отсюда следует:

$$\left(\frac{m}{m \sum \psi(S) \sigma} \right)^2 = 1,$$

что эквивалентно (32) при $l \neq 2$.

При $l = 2$ рассмотрим сначала неинволютивный класс $\mathfrak{S}$. Тогда, ввиду условия 1^0 и на основании формулы (104) приложения,

$$\begin{aligned} \left(\frac{m}{m \sum \psi(S) \sigma + \psi(S^{-1}) \sigma^{-1}} \right) &= \left(\frac{m}{m \sum \sigma} \right)^{\psi(\mathfrak{S})} \left(\frac{m}{m \sum \sigma^{-1}} \right)^{\psi(\mathfrak{S}^{-1})} = \\ &= \left(\frac{m}{m \sum \sigma} \right)^{\psi(\mathfrak{S}) + \psi(\mathfrak{S}^{-1})} = 1, \end{aligned}$$

где S пробегает все правые классы по H , содержащиеся в $\mathfrak{S}$.

Рассмотрим выражение

$$\left(\frac{m}{m \sum \psi(S) \sigma} \right),$$

в котором сумма распространена только на отличные от 1 классы S , содержащиеся в инволютивных двусторонних классах $\mathfrak{S}$. Имеем:

$$\left(\frac{m}{m \sum \psi(S) \sigma} \right) = \prod_{\mathfrak{S}} \left(\frac{m}{m \sum} \right)^{\psi(\mathfrak{S})},$$

где произведение распространено на все инволютивные классы $\mathfrak{S}$, а σ пробегает представителей правых классов смежности по H , содержащихся в $\mathfrak{S}$.

В приложении доказано (формула (126)), что

$$\left(\frac{m}{m \mathfrak{S}} \right) = \left(\frac{m}{\mathfrak{C}_{\mathfrak{S}}} \right),$$

поэтому мы имеем:

$$\left(\frac{m}{m^{\sum \psi(s)\sigma}}\right) = \left(\frac{m}{\prod_{\mathfrak{S}} \mathfrak{c}_{\mathfrak{S}}^{\psi(\mathfrak{S})}}\right) = \left(\frac{m}{\alpha_{\chi}}\right) = 1,$$

ввиду условия 4^0 и соотношения (21).

Тем самым независимость символа $[X]_{\psi}$ от выбора представителя μ в классе X доказана.

Для символа $[X]_{\psi}$ имеет место равенство

$$[X]_{\psi}^* = [X_1]_{\psi},$$

аналогичное (18), но равенство, аналогичное (17), не имеет места.

§2. Условия погружаемости для шольцевых расширений

В этом параграфе мы изложим решение задачи, сформулированной в п. 1 предшествующего параграфа. Согласно этой формулировке, нам заданы в цепочке (3) поля Ω , L и k , а также группа Галуа K/L как простое центральное расширение группы Галуа H поля k/L . Ввиду шольцевости поля k/Ω , а значит, и k/L , этому расширению группы H соответствует класс l -инвариантных чисел поля k/L , который мы будем обозначать через X .

ТЕОРЕМА 1. Для того, чтобы поле k/L можно было погрузить в поле K , соответствующее классу X и такое, что K^*/Ω шольцево, необходимо и достаточно, чтобы инварианты $(X)_M$, $[\chi, X]$ и $[X]_{\psi}$ равнялись 1 для всех χ и X , для которых они определены.

Доказательство. Необходимость равенства инвариантов единице проверяется непосредственно. Равенство единице инварианта $(X)_M$ следует из того, что в классе X существует такое число μ , что в $k(\sqrt{\mu})$ все простые делители M в $\Omega(\zeta)$ полностью распадаются, в то время как для любого простого делителя $\mathfrak{p}$ дивизора $\mathfrak{m}$ выполнено соотношение $\mathfrak{N}(\mathfrak{p}) \equiv 1 \pmod{M}$. В формуле (10), определяющей $[\chi, X]$, для любого простого $\mathfrak{q}|\mathfrak{m}$, ввиду шольцевости K/L ,

$$\left(\frac{\alpha_{\chi}}{\mathfrak{q}}\right) = 1, \quad \text{т. е.} \quad \left(\frac{\alpha_{\chi}}{\mathfrak{m}}\right) = 1.$$

С другой стороны, ввиду шольцевости K^*/L и ввиду (5),

$$\left(\frac{\mu^{\sum \varphi_{\mathfrak{P}}^*(T)\tau}}{\mathfrak{P}}\right) = 1,$$

откуда следует, что $[\chi, X] = 1$.

Из шольцевости K^*/L следует, что

$$\left[\frac{\mu^{\sum \sigma^{-1}}}{p} \right] = \left[\frac{\mu}{p^{\sum \sigma}} \right] = 1, \quad p|m,$$

если сумма распространена на представителей σ всех правых классов смежности G по H , содержащихся в одном, отличном от 1, классе по (H, H) . Ввиду того, что m_ψ состоит из множителей $p^{\sum \sigma}$, $p|m$, отсюда следует, что $[X]_\psi = 1$.

Перейдем теперь к доказательству достаточности. Для этого заметим, что из равенства единице инвариантов $(X)_{M_l}$ и $[\chi, X]$ следует равенство единице инвариантов (χ, X) работы [6] для поля k/L . Применяя теорему 1 работы [6], мы найдем, что в классе $[X]$ можно выбрать такого представителя μ_0 , что поле $k(\sqrt[l]{\mu_0})/L$ будет шольцевым относительно M_l .

Покажем сначала, что в X можно выбрать такого представителя μ_1 , что $k(\sqrt[l]{\mu_1})/L$ будет по-прежнему шольцевым, а в $k(\sqrt[l]{\mu_1})/\Omega$ будет выполнено третье условие шольцевости. Для этого найдем такое число $m_0 \in L$, чтобы оно состояло из простых дивизоров 1-го порядка, полностью распадающихся в k , было l -гиперпримарно, а при $l = 2$ тотально положительно, и удовлетворяло условиям:

$$\begin{aligned} \Re(q) &\equiv 1 \pmod{M_l}, & q|m_0, \\ \left(\frac{m_0}{\tau} \right) &= \left[\frac{\mu_0}{\tau} \right]^{-1}, & \left(\frac{m_0}{p} \right) = 1 \end{aligned} \quad (33)$$

для всех простых делителей τ числа M/M_l в L и простых делителей дискриминанта p поля k/L . Такой выбор возможен ввиду того, что τ взаимно просто с l и дискриминантом k/L . Очевидно, что при $\mu_1 = \mu_0 m_0$ $k(\sqrt[l]{\mu_1})/L$ будет по-прежнему шольцевым относительно M_l , а все простые делители M/M_l в $\Omega(\zeta)$ будут полностью распадаться в $k(\sqrt[l]{\mu_1})$, ввиду (33).

Теперь докажем, что в X существует такой представитель μ_2 , что в поле $k(\sqrt[l]{\mu_2})/\Omega$ выполнены второе и третье условия шольцевости относительно M и l , а $k(\sqrt[l]{\mu_2})/L$ по-прежнему шольцево. Для этого положим

$$\mu_1 = \mathfrak{C}_l^l \mathfrak{D}(X) m_1$$

и обозначим через $\mathfrak{F}$ произведение модуля l -гиперпримарности в L , всех критических простых дивизоров k/L и M , а через $S_{\mathfrak{F}}$ – главное соединение по модулю $\mathfrak{F}$. Найдем в классе $m_1 S_{\mathfrak{F}}$ простой дивизор q

1-го порядка над Ω , полностью распадающийся в k и удовлетворяющий условию

$$\Re(q) \equiv 1 \quad (M). \quad (34)$$

Такой дивизор q действительно существует. Чтобы показать это, обозначим произведение всех критических простых дивизоров k/L , модуля гиперпримарности и M_l через $\mathfrak{F}'$, так что

$$\mathfrak{F} = \mathfrak{F}' M / M_l.$$

Обозначим через Σ' поле классов $k S_{\mathfrak{F}'}$, а через Σ'' — $k S_{M/M_l}$. Очевидно, что

$$\Sigma = \Sigma' \Sigma''.$$

Нам надо найти простой дивизор q 1-го порядка над Ω , который лежал бы в классах $m_1 S_{\mathfrak{F}'}$ и $m_1 S_{M/M_l}$, полностью распадался в k и удовлетворял условию (34). Иначе говоря, он должен принадлежать к тому же автоморфизму, что и m_1 в полях Σ' и Σ'' и к единичному автоморфизму в полях k и $L(\zeta_M)$. Чтобы доказать существование такого простого дивизора, достаточно показать, что все указанные автоморфизмы могут быть продолжены до одного автоморфизма поля $\Sigma' \cdot \Sigma'' \cdot k \cdot L(\zeta_M)$.

То, что в поле $\Sigma' \cdot k \cdot L(\zeta_{M_l})$ существует автоморфизм, индуцирующий в Σ' , k и $L(\zeta_{M_l})$ указанные автоморфизмы, следует из того, что m_1 состоит из простых дивизоров, полностью распадающихся в k , а инвариант $(X)_{M_l}$ равен 1. Доказательство приведено на стр. 273 работы [6].

Рассмотрим теперь поле $\Sigma'' L(\zeta_{M/M_l})$. Очевидно, что $\Sigma'' \times \cap L(\zeta_{M/M_l})$ есть поле L_{M/M_l} , участвующее в определении инварианта $(X)_{M/M_l}$. Так как $(X)_{M/M_l} = 1$, то m_1 принадлежит в L_{M/M_l} к единичному автоморфизму. Из этого следует существование нужного нам автоморфизма.

Представим теперь $\Sigma' \Sigma'' k L(\zeta_M)$ как композит полей $\Sigma' \cdot k \cdot L(\zeta_{M_l})$ и $\Sigma'' \cdot L(\zeta_{M/M_l})$. Эти поля имеют взаимно простые дискриминанты и поэтому их пересечение, совпадающее с пересечением Σ' и Σ'' , есть максимальное абелево неразветвленное расширение с показателем $l = \Sigma_0/L$. Построенные нами автоморфизмы индуцируют в Σ_0/L один и тот же автоморфизм — тот, к которому принадлежит m_1 . Поэтому и во всем поле $\Sigma' \Sigma'' k L(\zeta_M)$ существует автоморфизм с нужными нам свойствами.

Если q — простой дивизор 1-го порядка над Ω , принадлежащий к этому автоморфизму, то

$$q = m_1(m_1)c^l.$$

Положив $\mu_2 = \mu_1 t_1$, мы получим, как легко видеть, число с нужными нам свойствами.

Наконец, докажем, что в X существует такой представитель μ_3 , что в $k(\sqrt[l]{\mu_3})/\Omega$ выполняются первое, второе и третье условия шольцевости. Так как $k(\sqrt[l]{\mu_2})/L$ уже шольцево, то нам надо, не нарушая этого, а также второго и третьего условий шольцевости относительно M и l для $k(\sqrt[l]{\mu_2})/\Omega$, добиться того, чтобы критические простые дивизоры L , не являющиеся критическими в $k(\sqrt[l]{\mu_2})/L$, там распадались. Для этого найдем l -гиперпримарное и тотально-положительное число m_2 , состоящее из простых дивизоров 1-го порядка, полностью распадающихся в k , и удовлетворяющих условиям:

$$\begin{aligned} \left(\frac{m_2}{p}\right) &= 1 \quad \text{для } p, \text{ критических в } k/L; \\ \left(\frac{m_2}{\tau}\right) &= 1, \quad \tau | M/M_1; \\ \Re(q) &\equiv 1 \pmod{M}, \quad q | m_2; \\ \left(\frac{m_2}{p'}\right) &= \left[\frac{\mu_2}{p'}\right]^{-1}, \quad p' - \text{критическое в } L, \text{ но не в } k/L. \end{aligned}$$

Так как дивизоры p' в последнем условии взаимно просты со всеми дивизорами q , τ и M из предшествующих условий и с дискриминантом k/L , то все условия совместны. Очевидно, что $\mu_3 = \mu_2 m_2$ обладает нужными нам свойствами.

Легко видеть, что четвертое условие шольцевости выполняется в $k(\sqrt[l]{\mu})/\Omega$, если оно выполняется в k/Ω и $k(\sqrt[l]{\mu})/L$ (его нужно проверять только при $l = 2$). Таким образом, положив $\mu' = \mu_3$, мы можем сказать, что поле $K = k(\sqrt[l]{\mu'})/\Omega$ — шольцево относительно M и l . Посмотрим, какие из условий шольцевости выполнены тогда в K^* . Очевидно, что третье и четвертое условия выполнены, а второе также выполнено, если выполнено первое. Таким образом, нам надо, не нарушая второго, третьего и четвертого условий шольцевости $k(\sqrt[l]{\mu'})/\Omega$, умножить μ' на такое число $m' \in L$, чтобы для $K = k(\sqrt[l]{\mu' m'})/\Omega$ выполнялось и первое условие шольцевости. При этом условие 1⁰ мы разобьем теперь на два:

А. Требование, чтобы критические дивизоры k распадались в K^* на дивизоры первого порядка и

В. Требование, чтобы простые критические дивизоры K^* , взаимно простые с дискриминантом k/Ω , имели относительно Ω порядок 1.

Рассмотрим сначала требование А. Умножение μ' на число m' заведомо не нарушит второго, третьего и четвертого условий шольцевости $k(\sqrt[m']{\mu'})/\Omega$ относительно M и l , если m' будет простым главным дивизором 1-го порядка в L/Ω , полностью распадающимся в k , тотально-положительным, гиперпримарным и удовлетворяющим условиям:

$$\left(\frac{m'}{\tau}\right) = 1, \quad \tau | M/M_l, \\ \mathfrak{N}(m') \equiv 1 \pmod{M}.$$

Все эти условия мы будем дальше называть условиями (*).

Пусть $\mathfrak{P}$ – критический дивизор k/Ω . Для того, чтобы в K^* , получающемся присоединением к k всех $\sqrt[m']{\mu^\sigma}$, простые делители $\mathfrak{P}$ имели порядок 1, необходимо и достаточно, чтобы для любой функции $f_{\mathfrak{P}}(T)$ на правых классах смежности T группы G по H , для которой

$$(\mathfrak{D}(X)^{\sum f_{\mathfrak{P}}(T)\tau}, \mathfrak{P}) \approx 1, \quad (35)$$

выполнялось равенство

$$\left(\frac{\mu^{\sum f_{\mathfrak{P}}(T)\tau}}{\mathfrak{P}}\right) = 1. \quad (36)$$

Положим

$$\xi_{f_{\mathfrak{P}}} = \left(\frac{\mu'^{\sum f_{\mathfrak{P}}(T)\tau}}{\mathfrak{P}}\right)$$

и покажем, что существует число m' , удовлетворяющее условиям (*) и такое, что

$$\left(\frac{m'^{\sum f_{\mathfrak{P}}(T)\tau}}{\mathfrak{P}}\right) = \xi_{f_{\mathfrak{P}}}^{-1} \quad (37)$$

для любого $\mathfrak{P}$ и любого $f_{\mathfrak{P}}$, удовлетворяющего (35). Очевидно, что тогда $\mu'm'$ будет удовлетворять требованию А.

Ввиду равенств

$$\left(\frac{m'}{\mathfrak{P}^{\sigma h}}\right) = \left(\frac{m'}{\mathfrak{P}^{\sigma}}\right), \quad \left(\frac{m'}{\mathfrak{P}^{z\sigma}}\right) = \left(\frac{m'}{\mathfrak{P}^{\sigma}}\right), \quad h \in H, \quad z \in \mathfrak{Z}_{\mathfrak{P}},$$

мы можем обозначить $\left(\frac{m'}{\mathfrak{P}^{\sigma}}\right)$ через $\zeta^{x_{\mathfrak{P}}, \mathfrak{S}}$, где $\mathfrak{S}$ – класс смежности по двойному модулю $(\mathfrak{Z}_{\mathfrak{P}}, H)$, содержащий σ . Кроме того, введем обозначение:

$$\xi_{f_{\mathfrak{P}}}^{-1} = \zeta^{b_{f_{\mathfrak{P}}}}.$$

условие (37) переписывается тогда в виде

$$\sum_S f_{\mathfrak{P}}^*(S) x_{\mathfrak{P}, \mathfrak{S}} \equiv b_{f_{\mathfrak{P}}} \pmod{l}, \quad (38)$$

причем сумма в (38) распространена на все левые классы смежности S группы G по H , а $\mathfrak{S}$ есть класс смежности по модулю $(\mathfrak{f}_{\mathfrak{P}}, H)$, содержащий S .

Выясним, когда существует число m' , удовлетворяющее условиям (*) и соотношениям:

$$\left(\frac{m'}{\mathfrak{P}^{\sigma}} \right)_k = \left(\frac{m'}{N_{k/L} \mathfrak{P}^{\sigma}} \right)_L = \zeta^{x_{\mathfrak{P}, \mathfrak{S}}} \quad (39)$$

при заданных $x_{\mathfrak{P}, \mathfrak{S}} \pmod{l}$.

Для этого обозначим через $\mathfrak{F}$ произведение всех дивизоров L , критических в k/L или L/Ω , модуля гиперпримарности, M_1 и вещественных бесконечно удаленных дивизоров, через $S_{\mathfrak{F}}$ — группу соединений классов дивизоров по модулю $\mathfrak{F}$, а через $\Sigma_{\mathfrak{F}}$ — поле классов к $S_{\mathfrak{F}}$. Повторяя дословно рассуждения на стр. 404 работы [8], мы получим, что условия (*) и (39) эквивалентны требованию, чтобы дивизор (m_1) принадлежал к определенному автоморфизму в $\Sigma_{\mathfrak{F}}$ и к единичным автоморфизмам в $L(\zeta_{M/M_1})$, k/L и полю классов Σ' к группе соединений по модулю, являющемуся произведением всех простых делителей M/M_1 . Так как дискриминанты $\Sigma_{\mathfrak{F}} \cdot k$ и $\Sigma' L(\zeta_{M/M_1})$ взаимно просты, то совместность условий (*) и (39) эквивалентна утверждению, что в $\Sigma_{\mathfrak{F}} \cap k$ указанный выше автоморфизм поля $\Sigma_{\mathfrak{F}}$ индуцирует единичный автоморфизм.

Повторяя опять соответствующие рассуждения на стр. 404 работы [8], мы видим, что $\Sigma_{\mathfrak{F}} \cap k$ получается присоединением к L всех $\sqrt[\alpha]{\alpha}$ и что автоморфизм поля $\Sigma_{\mathfrak{F}}$, о котором идет речь, сводится в $L(\sqrt[\alpha]{\alpha})$ к умножению $\sqrt[\alpha]{\alpha}$ на

$$\zeta^{\sum_{\mathfrak{P}, \mathfrak{S}} x_{\mathfrak{P}, \mathfrak{S}} \varphi_{\mathfrak{P}, \chi}(\mathfrak{S})},$$

если

$$(\alpha_{\chi}) = \prod_{\mathfrak{P}} \mathfrak{P}^{\sum \varphi_{\mathfrak{P}, \chi}(S) \sigma \sum h}$$

есть разложение α на простые множители в k .

Таким образом, совместность условий (*) и (39) эквивалентна совместности системы, состоящей из уравнения (38) и

$$\sum_{\mathfrak{P}, \mathfrak{S}} x_{\mathfrak{P}, \mathfrak{S}} \varphi_{\mathfrak{P}, \chi}(\mathfrak{S}) \equiv 0 \pmod{l}. \quad (40)$$

Мы выпишем условия совместности этой системы и покажем, что они совпадают с равенством единице инвариантов $[\chi, X]$.

Если система, состоящая из уравнений (38) и (40), не совместна, то существует такая линейная комбинация этих сравнений, в которой коэффициенты при всех неизвестных равны нулю, а свободный член отличен от нуля.

Пусть

$$\sum_{\chi} c_{\chi} \sum_{\mathfrak{P}, \mathfrak{S}} x_{\mathfrak{P}, \mathfrak{S}} \varphi_{\mathfrak{P}, \chi}(\mathfrak{S}) + \sum_{\mathfrak{P}, f_{\mathfrak{P}}} d_{\mathfrak{P}, f_{\mathfrak{P}}} \sum_S f_{\mathfrak{P}}^*(S) x_{\mathfrak{P}, \mathfrak{S}} \equiv \sum_{\mathfrak{P}, f_{\mathfrak{P}}} d_{\mathfrak{P}, f_{\mathfrak{P}}} b_{f_{\mathfrak{P}}} \quad (l) \quad (41)$$

является такой линейной комбинацией. Положим

$$\prod_{\chi} \chi^{c_{\chi}} = \chi_0, \quad \sum_{f_{\mathfrak{P}}} d_{\mathfrak{P}, f_{\mathfrak{P}}} f(T) = F_{\mathfrak{P}}(T).$$

Тогда, очевидно,

$$\begin{aligned} \sum_{\chi} c_{\chi} \varphi_{\mathfrak{P}, \chi}(\mathfrak{S}) &\equiv \varphi_{\mathfrak{P}, \chi_0}(\mathfrak{S}) \quad (l), \\ \sum_{f_{\mathfrak{P}}} d_{\mathfrak{P}, f_{\mathfrak{P}}} b_{f_{\mathfrak{P}}} &\equiv b_{f_{\mathfrak{P}}} \quad (l). \end{aligned}$$

Принимая во внимание, что в (41) коэффициенты при всех $x_{\mathfrak{P}, \chi}$ равны нулю, получаем:

$$\varphi_{\mathfrak{P}, \chi_0}(\mathfrak{S}) \equiv - \sum_{S \in \mathfrak{S}} F_{\mathfrak{P}}^*(S) \quad (l)$$

или

$$\varphi_{\mathfrak{P}, \chi_0}^*(\mathfrak{T}) \equiv - \sum_{T \in \mathfrak{T}} F_{\mathfrak{P}}(T) \quad (l) \quad (42)$$

для всех $\mathfrak{P}$ и $\mathfrak{T}$.

Так как все $f_{\mathfrak{P}}$, а значит, и $F_{\mathfrak{P}}$, удовлетворяют условию (35), то из (42) мы заключаем, что

$$(\mathfrak{D}(X)^{\sum \varphi_{\mathfrak{P}, \chi_0}^*(T)^{\tau}}, \mathfrak{P}) \approx 1. \quad (43)$$

Кроме того, из (42) следует, что

$$\prod_{\mathfrak{P}} \left(\frac{\mu'^{\sum \varphi_{\mathfrak{P}, \chi_0}^*(T)\tau}}{\mathfrak{P}} \right) = \zeta^{\sum_{\mathfrak{P}} b_{F\mathfrak{P}}}. \quad (44)$$

Для совместности нашей системы необходимо и достаточно, чтобы

$$\sum d_{\mathfrak{P}, f\mathfrak{P}} b_{f\mathfrak{P}} \equiv b_{f\mathfrak{P}} \equiv 0 \quad (l).$$

т. е. чтобы правая часть равнялась 1. Левая же часть равенства есть как раз $[\chi_0, X]$, так как ввиду того, что поле $k(\sqrt[l]{\mu'})$ по предположению уже шольцево,

$$\left(\frac{\alpha_{\chi_0}}{\mathfrak{m}} \right) = 1.$$

При этом символ $[\chi_0, X]$ действительно определен ввиду (43). Таким образом, система, состоящая из уравнений (38) и (40), совместна, а следовательно, число $\bar{\mu} = \mu' m'$, удовлетворяющее требованию А, существует.

Взяв за исходное число $\bar{\mu}$, мы должны теперь найти такое $\bar{m} \in L$, чтобы число $\mu = \bar{\mu} \bar{m}$ по-прежнему удовлетворяло требованию А, но сверх того, и требованию В.

Мы выберем $\bar{m}$ l -гиперпримарным и (при $l = 2$) тотально-положительным и удовлетворяющим условиям

$$\left(\frac{\bar{m}}{\mathfrak{P}^{\sum f^*(s)\sigma}} \right) = 1, \quad (45)$$

если $\mathfrak{P}$ – критическое в k/Ω ,

$$(\mathfrak{D}(X)^{\sum f(T)\tau}, \mathfrak{P}) \approx 1$$

и

$$\left(\frac{\bar{m}}{\tau} \right) = 1, \quad \tau | M/M_l, \\ \mathfrak{N}(\mathfrak{q}) \equiv 1 \quad (M) \quad \mathfrak{q} | m.$$

Мы положим

$$\left(\frac{\bar{m}}{\mathfrak{P}^\sigma} \right) = \zeta^{y_{\mathfrak{P}, \mathfrak{S}}}, \quad (46)$$

где $\mathfrak{S}$ есть класс смежности по двойному модулю $(3\mathfrak{p}, H)$. Тогда условие (45) эквивалентно (46) и тому, что

$$\sum f^*(S)y_{\mathfrak{p}, \mathfrak{S}} \equiv 0 \quad (I), \quad \text{если} \quad (\mathfrak{D}(X)^{\sum f(T)\tau}, \mathfrak{P}) \approx 1. \quad (47)$$

Все эти условия мы будем в дальнейшем называть условиями (**). Очевидно, что если они выполняются для $\overline{m}$, то $\overline{\mu m}$ будут по-прежнему удовлетворять требованию А.

Посмотрим, когда $\overline{\mu m}$ удовлетворяет требованию В. Простыми критическими дивизорами K^* , не являющимися критическими в k , будут при $K = k(\sqrt[4]{\mu m})$ простые делители $(\overline{m}m)^\sigma$, если

$$\overline{\mu} = \mathfrak{C}' \mathfrak{D}(X) \overline{m}.$$

Мы предположим, что

$$(\overline{m}, \overline{m}^\sigma) = 1 \quad \text{при} \quad \sigma \notin H,$$

так как этого можно добиться, умножая $\overline{\mu}$ на число, удовлетворяющее условиям (**). Для того, чтобы $\overline{\mu m}$ удовлетворяло условию В, необходимо и достаточно, чтобы выполнялось условие

$$\left(\frac{\overline{\mu m}}{\Omega^\sigma} \right) = 1, \quad (48)$$

где символ Лежандра вычисляется в k , Ω – любой простой делитель $\overline{m}m$ и $\sigma \notin H$.

Условия естественно разбиваются на две группы:

$$\left(\frac{\overline{\mu m}}{\mathfrak{B}^\sigma} \right) = 1, \quad \text{т. е.} \quad \left(\frac{\overline{m}}{\mathfrak{B}^\sigma} \right) = \left(\frac{\overline{\mu}}{\mathfrak{B}^\sigma} \right)^{-1} \quad \text{для} \quad \mathfrak{B} | \overline{m}$$

и

$$\left(\frac{\overline{m}}{\Omega^\sigma} \right) = \left(\frac{\overline{\mu}}{\Omega^\sigma} \right)^{-1} \quad \text{для} \quad \Omega | \overline{m}.$$

Мы будем подбирать $\overline{m}$ таким, чтобы все делящие его простые дивизоры удовлетворяли условию:

$$\left(\frac{\overline{\mu}}{\Omega^\sigma} \right) = \zeta(\sigma),$$

где $\zeta(\sigma)$ – некоторая система корней степени l из 1. Само же $\overline{m}$ должно удовлетворять условиям:

$$\left(\frac{\overline{m}}{\mathfrak{B}^\sigma}\right) = \left(\frac{\overline{\mu}}{\mathfrak{B}^\sigma}\right)^{-1}, \quad \mathfrak{B}|\overline{m}, \quad (49)$$

$$\left(\frac{\overline{m}}{\Omega^\sigma}\right) = \zeta(\sigma)^{-1}, \quad \sigma \notin H, \quad \Omega|\overline{m}. \quad (50)$$

Систему корней из 1 $\zeta(\sigma)$ мы будем считать постоянной на левых классах смежности S группы G по H и обозначать $\zeta(\sigma)$ через $\zeta(S)$, если $\sigma \in S$. Если же $\mathfrak{S}$ является классом смежности G по модулю (H, H) , то под $\zeta(\mathfrak{S})$ мы будем понимать

$$\zeta(S_1) \dots \zeta(S_r),$$

где $S_1, \dots, S_r$ – различные левые классы смежности G по H , содержащиеся в $\mathfrak{S}$. Мы будем предполагать, что определенные таким образом корни из 1 $\zeta(\mathfrak{S})$ удовлетворяют следующим условиям:

$$\zeta(\mathfrak{S})^{\mathfrak{g}(\mathfrak{S})} = \zeta(\mathfrak{S}^{-1}), \quad (51)$$

а в случае $l = 2$ потребуем, чтобы для любых инволютивных классов $\mathfrak{S}_1, \dots, \mathfrak{S}_u$ выполнялось условие

$$\zeta(\mathfrak{S}_1) \dots \zeta(\mathfrak{S}_u) = 1 \quad (52)$$

всякий раз, как

$$\mathfrak{C}_{\mathfrak{S}_1} \dots \mathfrak{C}_{\mathfrak{S}_u} \approx (\alpha_\chi) \quad \text{в } L.$$

В приложении к этой работе доказано существование бесконечного количества чисел $\overline{m}$, удовлетворяющих условиям (50) для любых корней из 1 $\zeta(S)$, удовлетворяющих условиям (51) и (52). Нам остается выяснить, можно ли добиться, чтобы m удовлетворяло также условиям (**). Для этого надо рассмотреть отдельно случаи $l \neq 2$ и $l = 2$.

Предположим, что $l \neq 2$. В этом случае число $\overline{m}$, согласно доказательству теоремы в приложении, может быть найдено в виде произведения двух простых чисел, удовлетворяющих условиям:

$$\left(\frac{\varkappa_i}{\mathfrak{B}^\sigma}\right)_k = \left(\frac{\varkappa_i}{N_{k/L}\mathfrak{B}^\sigma}\right)_L = \left(\frac{\overline{\mu}}{\mathfrak{B}^\sigma}\right)^{-\frac{1}{2}}, \quad \mathfrak{B}|\overline{m}, \quad i = 1, 2, \quad (53)$$

причем мы можем добиться выполнения условий (**) для m , если докажем существование бесконечного количества простых чисел первого порядка κ , удовлетворяющих условиям (**), (53) и соотношению

$$\left(\frac{\bar{\mu}}{\bar{\Omega}^\sigma}\right)_\kappa = \zeta(S). \quad (54)$$

Выясним, когда существуют простые числа, удовлетворяющие всем этим условиям.

Сначала мы предположим, что $y_{\mathfrak{F}, \sigma}$ в условиях (46) и (47) заданы и посмотрим, когда существует κ , удовлетворяющее (46) и (47), остальным условиям (**), а также (53) и (54). Для этого обозначим через $\mathfrak{F}$ произведение $N_{k/L} \mathfrak{P}$ для всех критических в k/Ω дивизоров $\mathfrak{P}$, всех $N_{k/L} \mathfrak{B}^\sigma$ для $\mathfrak{B}|\mathfrak{m}$, простых делителей $\mathfrak{B}$ числа M/M_1 , модуля гиперпримарности и вещественных бесконечно удаленных простых дивизоров L , через $S_{\mathfrak{F}}$ — группу соединений классов дивизоров по модулю $\mathfrak{F}$, а через $\Sigma_{\mathfrak{F}}$ — поле классов к $S_{\mathfrak{F}}$. Дословно повторяя рассуждения на стр. 404 работы [8], мы получим, что (46) и другие условия (**), а также равенство

$$\left(\frac{\bar{m}}{\bar{\mathfrak{B}}^\sigma}\right) = \left(\frac{\bar{\mu}}{\bar{\mathfrak{B}}^\sigma}\right)^{-\frac{1}{2}} \quad (55)$$

эквивалентны тому, что дивизор $(\bar{m})$ принадлежит ко вполне определенному автоморфизму s в $\Sigma_{\mathfrak{F}}$ и к единичному автоморфизму в поле $L(\zeta_M)$, а условия

$$\left(\frac{\bar{\mu}}{\bar{\Omega}^\sigma}\right) = \zeta(S), \quad \Omega|\kappa, \quad \sigma \notin H,$$

т. е.

$$\left(\frac{\bar{\mu}^\tau}{\bar{\Omega}}\right) = \zeta(T^{-1})^{g(\tau)},$$

где S — левый, а T — правый классы смежности G по H , эквивалентны тому, что (κ) принадлежит ко вполне определенному автоморфизму t в поле K^* , получающемуся присоединением к k всех $\sqrt[\nu]{\mu}^\sigma$, $\sigma \in H$.

Как и в первой части доказательства, мы видим, что эти условия совместны тогда и только тогда, когда в $K^* \cap \Sigma_{\mathfrak{F}}$ автоморфизмы s и t совпадают.

Поле $K^* \cap \Sigma_{\mathfrak{F}}$ получается присоединением к L всех $\sqrt[\nu]{\alpha_\chi}$ и $\sqrt[\nu]{m_\Phi}$, где $\Phi(T)$ — такая функция на правых классах смежности T группы G по H , что

$$\mu^{\Sigma\Phi(T)\tau} \approx m_\Phi \in L, \quad \Phi(1) = 0. \quad (56)$$

Заметим, что из того, что $m_\Phi \in L$, т. е. $m_\Phi^h = m_\Phi$, ввиду того, что m делится на простые дивизоры 1-го порядка, следует, что тождественно

$$(\sum \Phi(T)\tau)h \equiv \sum \Phi(T)\tau \quad (l).$$

Это показывает, что $\varphi(T)$ постоянно на классах смежности по модулю (H, H) .

Нам надо теперь выяснить, когда s и t совпадают, во-первых, в $L(\sqrt[m_\Phi]{m_\Phi})$ и, во-вторых, в $L(\sqrt[\alpha_\chi]{\alpha_\chi})$. Повторяя рассуждения на стр. 404 работы [8], мы видим, что в $L(\sqrt[\alpha_\chi]{\alpha_\chi})$ t индуцирует единичный автоморфизм, а s индуцирует автоморфизм, сводящийся к умножению $\sqrt[\alpha_\chi]{\alpha_\chi}$ на

$$\zeta^{\sum_{\mathfrak{P}, \mathfrak{S}} \varphi_{\mathfrak{P}, \chi}(\mathfrak{S}) y_{\mathfrak{P}, \mathfrak{S}}},$$

если

$$(\alpha_\chi) = \prod_{\mathfrak{P}} \mathfrak{P}^{\sum \varphi_{\mathfrak{P}, \chi}(\mathfrak{S}) \sigma \sum h}.$$

В поле $L(\sqrt[m_\Phi]{m_\Phi})$ s индуцирует автоморфизм, сводящийся к умножению $\sqrt[m_\Phi]{m_\Phi}$ на

$$\left[\frac{\bar{\mu}}{m_\Phi} \right]^{-\frac{1}{2}} \prod_{\mathfrak{P}} \zeta^{\sum_{\mathfrak{S}} F_{\mathfrak{P}, \Phi}(\mathfrak{S}) y_{\mathfrak{P}, \mathfrak{S}}},$$

если

$$\mathfrak{d}_\Phi = \prod_{\mathfrak{P}} \mathfrak{P}^{\sum_{\mathfrak{S}} F_{\mathfrak{P}, \Phi}(\mathfrak{S}) \sigma \sum h}, \quad m_\Phi = \mathfrak{d}_\Phi m_\Phi.$$

Автоморфизм t индуцирует в поле $(\sqrt[m_\Phi]{m_\Phi})$ автоморфизм, сводящийся к умножению $\sqrt[m_\Phi]{m_\Phi}$ на

$$\prod_T \zeta^{(T^{-1})^{g(T^{-1})\Phi(T)}},$$

где произведение распространено на все правые классы смежности группы G по H .

Обозначим $\left[\frac{\bar{\mu}}{m_\Phi} \right]^{-\frac{1}{2}}$ через ζ^{a_Φ} , $\prod_T \zeta^{(T^{-1})^{g(T^{-1})\Phi(T)}}$ – через ζ^{b_Φ} . Тогда речь будет идти о совместности системы сравнений:

$$\sum f_{\mathfrak{P}}(S) y_{\mathfrak{P}, \mathfrak{S}} \equiv 0 \quad (l), \quad (57)$$

если $f_{\mathfrak{P}}(S)$ удовлетворяет (35),

$$\sum \varphi_{\mathfrak{P},\chi}(\mathfrak{S})y_{\mathfrak{P},\mathfrak{S}} \equiv 0 \quad (I), \quad (58)$$

$$\sum F_{\mathfrak{P},\Phi}(\mathfrak{S})y_{\mathfrak{P},\mathfrak{S}} + a_{\Phi} \equiv b_{\Phi} \quad (I), \quad (59)$$

Если бы эта система была не совместна, то существовала бы линейная комбинация этих сравнений, у которой все коэффициенты при $y_{\mathfrak{P},\mathfrak{S}}$ равны 0, а свободный член $\neq 0$. Заметим, что линейная комбинация различных сравнений (57) есть снова одно из сравнений, только с другим $f_{\mathfrak{P}}(S)$, и то же самое относится к каждой из групп сравнений (58) и (59). Таким образом, если бы наша система была не совместна, то существовали бы такие $f_{\mathfrak{P}}$, χ и Φ , что в сравнении

$$\sum f_{\mathfrak{P}}(S)y_{\mathfrak{P},\mathfrak{S}} + \sum \varphi_{\mathfrak{P},\chi}(\mathfrak{S})y_{\mathfrak{P},\mathfrak{S}} + \sum F_{\mathfrak{P},\Phi}(\mathfrak{S})y_{\mathfrak{P},\mathfrak{S}} + a_{\Phi} \equiv b_{\Phi} \quad (I)$$

все коэффициенты при $y_{\mathfrak{P},\mathfrak{S}}$ равны 0, а свободный член $b_{\Phi} - a_{\Phi}$ отличен от 0. Из сделанного предположения следует, что

$$\sum F_{\mathfrak{P},\Phi}(\mathfrak{S}) \equiv - \sum_{S \in \mathfrak{S}} f_{\mathfrak{P}}(S) - \varphi_{\mathfrak{P},\chi}(\mathfrak{S}) \quad (I),$$

т. е.

$$\mathfrak{d}_{\Phi} = (\alpha_{\chi})^{-1} \prod_{\mathfrak{P}} \mathfrak{P}^{-\sum_{S \in \mathfrak{S}} f_{\mathfrak{P}}(S) \sigma_{\mathfrak{P}} h}, \quad (60)$$

где $\sum_{S \in \mathfrak{S}} f_{\mathfrak{P}}(S)$ удовлетворяет условию (35). Условие же совместности нашей системы записывается теперь в виде $a_{\Phi} \equiv b_{\Phi} \quad (I)$, т. е.

$$\prod \zeta(T^{-1})^{g(T^{-1})\Phi(T)} = \left[\frac{\bar{\mu}}{\mathfrak{m}_{\Phi}} \right]^{-\frac{1}{2}} \quad (61)$$

для всякого Φ , которое постоянно на классах смежности по модулю (H, H) , удовлетворяет условию (56) и для которого дивизор $\mathfrak{d}_{\Phi}$ в разложении $\mathfrak{m}_{\Phi}$ имеет вид (22).

Нам остается выяснить, когда существуют корни из 1 $\zeta(S)$, удовлетворяющие условиям (51), (52) и (61).

Положим

$$\zeta(S) = \zeta^{x_S}, \quad \left[\frac{\bar{\mu}}{\mathfrak{m}_{\Phi}} \right]^{-\frac{1}{2}} = \zeta^{b_{\Phi}'};$$

тогда условия на x_S запишутся в виде сравнений:

$$\begin{aligned} g(\mathfrak{S}) \sum_{S \in \mathfrak{S}} x_S &\equiv \sum_{S' \in \mathfrak{S}^{-1}} x_{S'} \quad (l), \\ \sum_T x_{T^{-1}} \Phi(T) g(T^{-1}) &\equiv b_\Phi \quad (l). \end{aligned} \quad (62)$$

Найдем условия совместности этой системы. Если система не совместна, то существует линейная комбинация входящих в нее сравнений, в которой все коэффициенты при неизвестных x_S равны 0, а свободный член $\neq 0$. Пусть

$$\begin{aligned} \sum_{\mathfrak{S}} C_{\mathfrak{S}} g(\mathfrak{S}) \left(\sum_{S \in \mathfrak{S}} x_S - \sum_{S' \in \mathfrak{S}^{-1}} x_{S'} \right) + \\ \sum_{\Phi} d_{\Phi} \sum_T x_{T^{-1}} \Phi(T) g(T^{-1}) \equiv \sum_{\Phi} d_{\Phi} b_{\Phi} \quad (l) \end{aligned} \quad (63)$$

является такой комбинацией. Положим

$$\sum_{\Phi} d_{\Phi} \Phi(T) = \psi(T).$$

Тогда, очевидно,

$$\sum_{\Phi} d_{\Phi} b_{\Phi} \equiv b_{\psi} \quad (l).$$

Учитывая, что в (63) коэффициенты при всех x_S равны 0, получаем:

$$g(T) \psi(T^{-1}) \equiv C_{\mathfrak{T}^{-1}} - C_{\mathfrak{T}} g(T) \quad (l),$$

т.е.

$$\psi(T) \equiv g(\mathfrak{T}) C_{\mathfrak{T}} - C_{\mathfrak{T}^{-1}} \quad (l). \quad (64)$$

Мы уже видели, что $\psi(T)$ постоянно на классах смежности по модулю (H, H) . Из (64) это следует еще раз, причем, если положить

$$\psi(\mathfrak{S}) = \psi(S), \quad S \in \mathfrak{S},$$

то из (64) следует, что

$$g(\mathfrak{S}) \psi(\mathfrak{S}^{-1}) \equiv -\psi(\mathfrak{S}) \quad (l).$$

Вместе с (60) это показывает, что $\psi(\mathfrak{S})$ удовлетворяет всем условиям, встречающимся в определении символа $[X]_\psi$. Отсюда мы заключаем, что

$$\zeta^{b_\psi} = \left[\frac{\bar{\mu}}{m_\Phi} \right]^{-\frac{1}{2}} = 1,$$

т. е. $b_\psi \equiv 0 \pmod{l}$, откуда и следует совместность системы (62).

Аналогичным образом мы поступаем и в случае $l = 2$. Согласно доказательству теоремы, данному в приложении, число $\bar{m}$ может быть в этом случае найдено в виде произведения $\kappa_1 \kappa_2 \kappa_3$ трех простых чисел, удовлетворяющих условиям:

$$\left(\frac{\kappa_i}{\mathfrak{B}_\sigma} \right) = \left(\frac{\bar{\mu}}{\mathfrak{B}_\sigma} \right), \quad \sigma \notin H, \quad i = 1, 2, 3, \quad (65)$$

причем мы можем добиться выполнения условий (**) и (48) для $\bar{m}$, если докажем существование бесконечного числа простых чисел κ , удовлетворяющих условиям (**), (54) и (65).

Как и в случае $l \neq 2$, для того, чтобы существовали такие числа, необходимо и достаточно, чтобы была совместна следующая система:

$$\sum_{S \in \mathfrak{S}} x_S \equiv \sum_{S' \in \mathfrak{S}^{-1}} x_{S'} \pmod{l}, \quad (66)$$

$$\sum_{S \in \mathfrak{S}_1 + \dots + \mathfrak{S}_u} x_S \equiv 0 \pmod{l}, \text{ если } \mathfrak{C}_{\mathfrak{S}_1} \dots \mathfrak{C}_{\mathfrak{S}_u} \approx (\alpha_\chi) \text{ и } [\chi, X] \text{ определено,}$$

$$\sum_T x_{T^{-1}} \Phi(T) \equiv b_\Phi \pmod{l}$$

для каждой функции Φ , удовлетворяющей условию (56).

Предположение о несовместности этой системы приводит опять к наличию линейной комбинации входящих в нее уравнений, в которой коэффициенты при всех x_S равны 0, а свободный член $\neq 0$. Пусть эта линейная комбинация есть

$$\begin{aligned} & \sum_{\mathfrak{S}} C_{\mathfrak{S}} \left(\sum_{S \in \mathfrak{S}} x_S - \sum_{S' \in \mathfrak{S}^{-1}} x_{S'} \right) + \sum_{\Phi} d_{\Phi} \sum_T x_S \Phi(S^{-1}) + \\ & + \sum_{(\mathfrak{S}_1, \dots, \mathfrak{S}_u)} e_{\mathfrak{S}_1, \dots, \mathfrak{S}_u} \sum_{S \in \mathfrak{S}_1 + \dots + \mathfrak{S}_u} x_S \equiv \sum_{\Phi} d_{\Phi} b_{\Phi} \pmod{l}, \end{aligned}$$

где внешняя сумма в третьем слагаемом распространена на все совокупности $(\mathfrak{S}_1, \dots, \mathfrak{S}_u)$ инволютивных классов по модулю (H, H) , для которых

$$\mathfrak{C}_{\mathfrak{S}_1} \dots \mathfrak{C}_{\mathfrak{S}_u} \approx (\alpha_\chi) \quad \text{и} \quad [\chi, X] \quad \text{определено.} \quad (67)$$

Мы полагаем опять

$$\sum_{\Phi} d_{\Phi} \Phi(T) = \psi(T)$$

и получаем, как и при $l \neq 2$,

$$\psi(\mathfrak{S}^{-1}) \equiv C_{\mathfrak{S}^{-1}} + C_{\mathfrak{S}} + \sum_{(\mathfrak{S}_1, \dots, \mathfrak{S}_u)} e_{\mathfrak{S}_1, \dots, \mathfrak{S}_u} \varepsilon_{\mathfrak{S}_1, \dots, \mathfrak{S}_u}(\mathfrak{S}) \quad (2), \quad (68)$$

где $e_{\mathfrak{S}_1, \dots, \mathfrak{S}_u}(\mathfrak{S})$ есть характеристическая функция множества $\mathfrak{S}_1, \dots, \mathfrak{S}_u$ инволютивных автоморфизмов, если для этого множества выполнено условие (67), и 0 - в противном случае. Отсюда мы заключаем, что

$$\psi(\mathfrak{S}^{-1}) \equiv \psi(\mathfrak{S}) \quad (2).$$

Так как, по определению,

$$\prod_{\mathfrak{S}} \mathfrak{C}_{\mathfrak{S}}^{e_{\mathfrak{S}_1, \dots, \mathfrak{S}_u}(\mathfrak{S})} \approx (\alpha_\chi), \quad [\chi, X] \quad \text{определено,}$$

где произведение распространено на все инволютивные автоморфизмы, то из (68) следует, что

$$\prod_{\mathfrak{S}} \mathfrak{C}_{\mathfrak{S}}^{\psi(\mathfrak{S})} \approx (\alpha_\chi), \quad [\chi, X] \quad \text{определено.}$$

Таким образом, функция $\psi(\mathfrak{S})$ удовлетворяет всем условиям, входящим в определение $[X]_\psi$, а следовательно,

$$(-1)^{b_\psi} = \left[\frac{\bar{\mu}}{\mathfrak{m}_\psi} \right] = [X]_\psi = 1,$$

что и означает совместность системы (66). Теорема доказана.

§3. Общее условие погружаемости для шольцевых полей

В дальнейшем нам понадобится обобщение теоремы 1 на более общий случай, когда поле K/L в цепочке (3) является центральным, но не простым центральным расширением поля k/L . Для этого нам необходимо ввести в рассмотрение еще одну серию инвариантов поля k .

Обозначим группу Галуа поля K/L через $\mathfrak{G}$, а поля K/k – через $\mathfrak{Z}$. Очевидно, $\mathfrak{G}/\mathfrak{Z} \cong G$ и $\mathfrak{Z}$ лежит в центре $\mathfrak{G}$. В дальнейшем мы будем предполагать, что $\mathfrak{Z}$ имеет показатель l . Любой характер X группы $\mathfrak{Z}$ определяет некоторый класс l -инвариантных чисел X в k . Очевидно, что эти классы образуют группу, являющуюся гомоморфным образом группы характеров $\mathcal{X}$ группы $\mathfrak{Z}$. Выберем в $\mathcal{X}$ некоторый фиксированный базис $X_1, \dots, X_r$, с которым в дальнейшем всегда будем иметь дело. Мы будем всегда предполагать, что инварианты $[\chi, X_i]$, $(X_i)_M$ и $[X_i]_\psi$ для $i = 1, \dots, r$ равны 1.

Пусть $\varphi_1(S), \dots, \varphi_s(S)$ – функции на правых классах смежности G по H , постоянные на классах смежности G по модулю (H, H) . Под A^φ мы будем подразумевать $A^{\sum \varphi(S)\sigma}$, где S в показателе пробегает все правые классы смежности группы G по H , а $\sigma \in S$. Ввиду того, что φ постоянно на классах смежности по модулю (H, H) , из $\alpha \in L$ следует $\alpha^\varphi \in L$ и из l -инвариантности μ в k/L следует l -инвариантность μ^φ . Поэтому X^φ есть определенный класс l -инвариантных чисел, если X – тоже класс l -инвариантных чисел.

Предположим, что функции $\varphi_1, \dots, \varphi_{s-1}$ таковы, что

$$X_1^{\varphi_1} \dots X_{s-1}^{\varphi_{s-1}} = 1, \quad (69)$$

$$X_s^{\varphi_1^*} = \dots = X_s^{\varphi_{s-1}^*} = 1. \quad (70)$$

Выберем в классах $X_1, \dots, X_{s-1}$ l -гиперпримарных представителей $\mu_1, \dots, \mu_{s-1}$. Ввиду (69), мы имеем:

$$\mu_1^{\varphi_1} \dots \mu_{s-1}^{\varphi_{s-1}} \approx m_{\varphi_1, \dots, \varphi_{s-1}} \in L. \quad (71)$$

Положим

$$[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}} = [m_{\varphi_1, \dots, \varphi_{s-1}}, X_s],$$

где символ $[\alpha, X]$ определяется формулами (4') и (10) с заменой α_χ на α .

Докажем, что символ $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$ не зависит от выбора l -гиперпримарных представителей $\mu_1, \dots, \mu_{s-1}$ в классах

$X_1, \dots, X_{s-1}$. Переход к другой системе представителей $\mu_1 m_1, \dots, \mu_{s-1} m_{s-1}, m_i \in L$, приводит к умножению $m_{\varphi_1, \dots, \varphi_{s-1}}$ на $m_1^{\varphi_1}, \dots, m_{s-1}^{\varphi_{s-1}}$. Ввиду очевидной мультипликативности символа $[\alpha, X]$ по α , символ $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$ умножится тогда на

$$[m_1^{\varphi_1} \dots m_{s-1}^{\varphi_{s-1}}, X_s].$$

На основании очевидного тождества

$$[\alpha^\varphi, X] = [\alpha, X^{\varphi^*}]$$

мы имеем:

$$\begin{aligned} [m_1^{\varphi_1} \dots m_{s-1}^{\varphi_{s-1}}, X_s] &= [m_1^{\varphi_1}, X_s] \dots [m_{s-1}^{\varphi_{s-1}}, X_s] = \\ &= [m_1, X_s^{\varphi_1^*}] \dots [m_{s-1}, X_s^{\varphi_{s-1}^*}]. \end{aligned} \quad (72)$$

Ввиду (70),

$$X_s^{\varphi_i^*} = 1, \quad i = 1, \dots, s-1,$$

а ввиду l -гиперпримарности m_i , отсюда следует

$$[m_i, X_s^{\varphi_i^*}] = 1.$$

В комбинации с (72) это и дает независимость символа

$$[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$$

от выбора $\mu_i \in X_i$.

Заметим, что формулой (71) $m_{\varphi_1, \dots, \varphi_{s-1}}$ определяется в L неоднозначно с точностью до l -равенства, но однозначно с точностью до множителя α_χ . Ввиду того что, по предположению, $[\chi, X_s] = 1$, символ $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$ не меняется при умножении $m_{\varphi_1, \dots, \varphi_{s-1}}$ на α_χ .

ТЕОРЕМА 2. Для того, чтобы шольцево поле K с инвариантами $[\chi, X]$, $(X)_M$ и $[X]_\psi$, равными 1, можно было погрузить в такое поле K^* с группой Галуа $\mathfrak{G}$ над L , что K^*/Ω – шольцево, необходимо и достаточно, чтобы все инварианты $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$, $s = 2, \dots, r$, обращались в 1.

Доказательство. Для доказательства необходимости предположим, что поле k погружаемо в поле K с нужным нам свойством.

Это значит, что в классах $X_1, \dots, X_r$ можно выбрать таких представителей $\mu_1, \dots, \mu_r$, что поле, получающееся присоединением к k всех $\sqrt[\sigma]{\mu_i^\sigma}$, $i = 1, \dots, r$, $\sigma \in G$, — шольцево. Тем более шольцево поле K_s , получающееся присоединением к k всех $\sqrt[\sigma]{\mu_i^\sigma}$, $i = 1, \dots, s$. Очевидно, что K_s получается присоединением к K_{s-1} всех $\sqrt[\sigma]{\mu_s^\sigma}$, $\sigma \in G$.

Ввиду теоремы 1, для шольцевости K_s необходимо, чтобы $[\chi, X_s] = 1$ в K_{s-1} . Число $m_{\varphi_1, \dots, \varphi_{s-1}}$ является таким числом из L , что $\sqrt[m_{\varphi_1, \dots, \varphi_{s-1}}]{m} \in K_{s-1}$, т. е. одним из чисел α_χ . Таким образом, $[m_{\varphi_1, \dots, \varphi_{s-1}}, X_s]$ должно равняться 1, чем теорема 2 и доказана в части необходимости.

Достаточность условий теоремы 2 мы докажем, показав, что при выполнении этих условий поле k при любом $s \leq r$ может быть погружено в поле K_s , для которого K_s^* — шольцево. Теорема 2 вытекает из этого утверждения ввиду того, что $K_r = K$. Само утверждение мы будем доказывать индукцией по s . Мы можем таким образом считать, что в классах $X_1, \dots, X_{s-1}$ выбраны такие числа $\mu_1, \dots, \mu_{s-1}$, что поле K_{s-1}^* , получающееся присоединением к k всех $\sqrt[\sigma]{\mu_i^\sigma}$, $i = 1, \dots, s-1$, $\sigma \in G$, — шольцево. При этом мы будем считать, что соответствующие им дивизоры $m_i \neq 1$ и удовлетворяют условиям:

$$(m_i, m_j^\sigma) = 1 \quad \text{при} \quad i \neq j, \quad \sigma \notin H. \quad (73)$$

Ввиду теоремы 1, для того, чтобы существовало поле K_s с нужными нам свойствами, необходимо и достаточно, чтобы в K_{s-1}^* все инварианты $[\chi, X_s]$, $(X_s)_M$ и $[X_s]_\psi$ равнялись 1. Так как X_s содержит l -инвариантные числа из k , то инварианты $(X_s)_M$ и $[X_s]_\psi$ можно вычислить в поле k , где они, по предположению, равны 1. По той же причине инварианты $[\chi, X_s]$ равны 1 для характеров χ группы Галуа поля k/L .

Все числа α_χ для любых характеров χ группы Галуа поля K_{s-1}^*/L получаются из чисел α_χ , соответствующих характерам группы Галуа k/L , умножением на числа $m_{\varphi_1, \dots, \varphi_{s-1}}$, где $\varphi_1, \dots, \varphi_{s-1}$ — функции, удовлетворяющие условиям (69).

Действительно, нам надо найти такие числа $m \in L$, что $\sqrt[m]{m} \in K_{s-1}$. Так как тем более $m \in k$, то $m \approx \mu_1^{\varphi_1} \dots \mu_{s-1}^{\varphi_{s-1}}$ в k .

Рассматривая дивизоры m_i , мы видим, что ввиду (73) можно считать, что

$$m_1^{\varphi_1} \in L, \dots, m_{s-1}^{\varphi_{s-1}} \in L.$$

Из этого следует, как и на стр. 549, что $\varphi_1, \dots, \varphi_{s-1}$ постоянны на классах смежности G по модулю (H, H) и $m \approx m_{\varphi_1, \dots, \varphi_{s-1}}$ в k , а тем самым $m \approx m_{\varphi_1, \dots, \varphi_{s-1}} \alpha_\chi$ в L .

Таким образом, нам надо добиться того, чтобы выполнялись равенства

$$[m_{\varphi_1, \dots, \varphi_{s-1}}, X_s] = 1 \quad (74)$$

для всех $\varphi_1, \dots, \varphi_{s-1}$, удовлетворяющих условиям (69).

Мы можем добиваться выполнения равенств (74), умножая каждое μ_i на $m_i \in L$, $i = 1, \dots, s-1$, если при этом не нарушается шольцевость поля K_{s-1}^* . При таком умножении $[m_{\varphi_1, \dots, \varphi_{s-1}}, X_s]$ умножится на $[m_1^{\varphi_1} \dots m_{s-1}^{\varphi_{s-1}}, X_s]$. Следовательно, нам надо подобрать m_i так, чтобы выполнялись равенства:

$$[m_1^{\varphi_1} \dots m_{s-1}^{\varphi_{s-1}}, X_s] = [m_{\varphi_1, \dots, \varphi_{s-1}}, X_s]^{-1}$$

или

$$[m_1, X_s^{\varphi_1^*}] \dots [m_{s-1}, X_s^{\varphi_{s-1}^*}] = [m_{\varphi_1, \dots, \varphi_{s-1}}, X_s]^{-1}. \quad (75)$$

Обозначим $[m_i, X_s^{\varphi_i^*}]$ через $\zeta_i(\varphi_i)$, а $[m_{\varphi_1, \dots, \varphi_{s-1}}, X_s]$ — через $\eta(\varphi_1, \dots, \varphi_{s-1})$. Соотношение (75) на m_i переписывается тогда так:

$$[m_i, X_s^{\varphi_i^*}] = \zeta_i(\varphi_i)^{-1}, \quad (76)$$

где

$$\zeta_1(\varphi_1) \dots \zeta_{s-1}(\varphi_{s-1}) = \eta(\varphi_1, \dots, \varphi_{s-1}). \quad (77)$$

При этом, очевидно,

$$\zeta_i(\varphi_i + \varphi'_i) = \zeta_i(\varphi_i)\zeta_i(\varphi'_i), \quad (77')$$

$$\eta(\varphi_1 + \varphi'_1, \dots, \varphi_{s-1} + \varphi'_{s-1}) = \eta(\varphi_1, \dots, \varphi_{s-1})\eta(\varphi'_1, \dots, \varphi'_{s-1}). \quad (77'')$$

Посмотрим, какие условия надо наложить на m_i , чтобы замена μ_i на $\mu_i m_i$ не нарушила шольцевости поля K_{s-1}^* . Обозначим через $\mathfrak{P}$ произвольный простой делитель дискриминанта $k/\Omega(\zeta)$, через Ω_i — произвольный простой делитель m_i , через $\mathfrak{B}_i$ — произвольный простой делитель m_i . Следующие условия заведомо гарантируют нам, что умножение μ_i на m_i не нарушит шольцевости K_{s-1}^* :

$$\left(\frac{m_i}{\mathfrak{P}}\right) = 1, \quad \left(\frac{m_i}{\Omega_j^\sigma}\right) = 1, \quad \left(\frac{\mu_i}{\Omega_j^\sigma}\right) = 1, \quad \left(\frac{m_i}{\mathfrak{B}_j^\sigma}\right) = 1. \quad (78)$$

$$\Re(\Omega_i) \equiv 1 \pmod{M}, \quad \left(\frac{m_i}{\Re}\right) = 1, \quad \Re \nmid M. \quad (79)$$

Для того, чтобы удовлетворялось условие (71), положим

$$\left(\frac{\mu_s^{\varphi_i}}{\Omega_i}\right) = 1, \quad \left(\frac{m_i}{m_s^{\varphi_i}} \Omega_i\right) = \zeta_i(\varphi_i). \quad (80)$$

Среди условий (77) содержатся условия:

$$\left(\frac{m_i}{\Omega_i^\sigma}\right) = 1, \quad \Omega_i | m_i.$$

Для того, чтобы удовлетворить им, нам нужно применить теорему, доказанную в приложении. Согласно доказательству этой теоремы, мы должны искать m в виде $\kappa_i \kappa_i'$ при $l \neq 2$ и $\kappa_i \kappa_i' \kappa_i''$ при $l = 2$, где $\kappa_i, \kappa_i', \kappa_i''$ — простые главные дивизоры. Выпишем условия, которым должны удовлетворять κ_i, κ_i' и κ_i'' для того, чтобы для m_i удовлетворялись условия (76) и (78). При этом мы запишем условия лишь для κ_i , подразумевая, что они же должны выполняться и для κ_i' , а при $l = 2$ — и для κ_i'' :

$$\left(\frac{\kappa_i}{\mathfrak{P}}\right) = 1, \quad (81)$$

$$\left(\frac{\kappa_i}{\Omega_j^\sigma}\right) = 1, \quad i \neq j, \quad (82)$$

$$\left(\frac{\mu_j}{\Omega_i^\sigma}\right) = 1, \quad \left(\frac{\kappa_i}{\mathfrak{B}_j^\sigma}\right) = 1, \quad (83)$$

$$\left(\frac{\mu_s^{\varphi_i}}{\Omega_i}\right) = 1, \quad \left(\frac{\kappa_i}{m_s^{\varphi_i}}\right) = \zeta_i(\varphi_i)^\varepsilon, \quad (84)$$

$$\kappa_i \equiv 1 \pmod{M}, \quad (85)$$

где $\varepsilon = \frac{1}{2}$ при $l \neq 2$ и $\varepsilon = 1$ при $l = 2$. Числа κ_i мы будем подбирать последовательно при $i = 1, \dots, s-1$, добиваясь для любого κ_i выполнения условий (83) для $i = t$ и сразу для всех $j = 1, \dots, s-1$, условий (82) — для $i = t, j < t$ и $i < t, j = t$, а условий (81) — для $i = t$.

Заметим, что условия (81), (82), (83) и (84) совместны, так как они равносильны тому, что κ_i принадлежит к единичному автоморфизму в некотором поле Σ . Для того чтобы выяснить совместность этих условий с условием (84), надо найти пересечение Σ с тем полем Σ' , принадлежность в котором к определенному автоморфизму

эквивалентна выполнению (84). Очевидно, что дискриминант Σ' состоит только из делителей m_s . Отсюда легко следует, что пересечение Σ с Σ' есть композит полей $L(\sqrt[s]{m_{\varphi^*}})$, где $\mu_s^{\varphi^*} \approx m_{\varphi^*} \in L$ для тех функций φ , для которых это равенство имеет место. Таким образом, все условия (78), (79) и (80) совместны, если

$$\zeta_i(\varphi) = 1 \quad (85')$$

для любого φ , для которого

$$\mu_s^{\varphi^*} \approx m_{\varphi^*} \in L.$$

Теперь нам остается только доказать, что существуют функции $\zeta_i(\varphi)$, удовлетворяющие условиям (69) и (70). Для этого рассмотрим прямое произведение $\Phi^{(s-1)}$ $s-1$ экземпляра группы Φ функций $\varphi(S)$, постоянных на классах смежности G по (H, H) и определенных $\bmod l$. Формула (77'') показывает, что $\eta(\varphi_1, \dots, \varphi_{s-1})$ является характером подгруппы Φ_0 группы $\Phi^{(s-1)}$, состоящей из тех наборов $(\varphi_1, \dots, \varphi_{s-1})$ функций, для которых

$$X_1^{\varphi_1} \dots X_{s-1}^{\varphi_{s-1}} = 1.$$

С другой стороны, $\zeta_1(\varphi_1) \dots \zeta_{s-1}(\varphi_{s-1})$, где $\zeta_i(\varphi_i)$ удовлетворяет (77') – это самый общий характер на $\Phi^{(s-1)}$. Условия (85') означают, что этот характер должен обращаться в 1 на подгруппе Φ_1 группы $\Phi^{(s-1)}$, состоящей из тех наборов функций $(\varphi_1, \dots, \varphi_{s-1})$, для которых

$$X_s^{\varphi_1} = \dots = X_s^{\varphi_{s-1}} = 1.$$

Наша задача заключается, таким образом, в том, чтобы доказать существование такого характера группы $\Phi^{(s-1)}$, который совпадает на Φ_0 с $\eta(\varphi_1, \dots, \varphi_{s-1})$, а на Φ_1 – с единичным характером. Очевидно, что для существования такого характера необходимо, чтобы характер η совпадал с единичным характером на $\Phi_0 \cap \Phi_1$. Но как раз это и утверждается равенством единице инварианта $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$. Теорема доказана.

Заметим, что для инвариантов $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$ имеют место соотношения:

$$\begin{aligned} & [X_1 X'_1, \dots, X_{s-1} X'_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}} = \\ & = [X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}} [X'_1, \dots, X'_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}, \end{aligned} \quad (86)$$

$$\begin{aligned} & [X_1, \dots, X_{s-1}; X_s X'_s]_{\varphi_1, \dots, \varphi_{s-1}} = \\ & = [X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}} [X_1, \dots, X_{s-1}; X'_s]_{\varphi_1, \dots, \varphi_{s-1}} \end{aligned} \quad (87)$$

и соотношение, аналогичное (18) для инвариантов $[\chi, X]$.

§4. Построение полей с разрешимой группой Галуа

1. Канонические гомоморфизмы. Рассмотрим произвольную конечную группу F порядка m и свободную группу S_d с md образующими, которые мы будем обозначать через $s_{u,i}$, $u \in F$, $i = 1, \dots, d$. В S_d рассмотрим ряд нормальных делителей N_c , определяемых следующим образом: $N_0 = S_d$, N_{c+1} есть подгруппа N_c , порожденная l^k -ми степенями элементов S_d и коммутаторами элементов S_d с элементами N_c . Здесь простое число l и показатель k раз навсегда фиксированы. S_d/N_c мы будем обозначать через $\mathfrak{G}_d^{(c)}$. Очевидно, что эта факторгруппа зависит от c , d , l , k и m , но так как l , k и группа F будут во всех наших рассуждениях одни и те же, то обозначение отражает только c и d . Каждому $v \in F$ соответствует перестановка образующих $s_{u,i}$ по правилу:

$$s_{u,i}^v = s_{uv,i}, \quad i = 1, \dots, d, \quad u \in F. \quad (88)$$

Такая перестановка определяет автоморфизм S_d , причем эти автоморфизмы образуют группу, изоморфную F . Так как N_c , как легко видеть, — характеристическая подгруппа S_d , то и в $\mathfrak{G}_d^{(c)}$ мы получаем группу автоморфизмов, изоморфную F . Элементы $x \in \mathfrak{G}_d^{(c)}$, которые принадлежат к центру $\mathfrak{G}_d^{(c)}$ и удовлетворяют уравнению $x^{l^k-r} = 1$, образуют нормальный делитель $\mathfrak{G}_d^{(c)}$. Факторгруппу $\mathfrak{G}_d^{(c)}$ по этому нормальному делителю обозначим $\mathfrak{G}_d^{(c,r)}$. Очевидно, что

$$\mathfrak{G}_d^{(c,0)} = \mathfrak{G}_d^{(c-1)}, \quad \mathfrak{G}_d^{(c,k)} = \mathfrak{G}_d^{(c)}$$

и что $\mathfrak{G}_d^{(c,r)}$ гомоморфно $\mathfrak{G}_d^{(c,r-1)}$. Ядро этого гомоморфизма обозначим через Z_r .

Ясно, что определенные нами группы $\mathfrak{G}_d^{(c,r)}$ являются факторгруппами групп $\mathfrak{G}_d^{(c)}$ по нормальным делителям, допустимым относительно операторов из F , определенных формулой (88). Таким образом, все эти группы являются операторными группами с областью операторов F .

Рассмотрим в F некоторую фиксированную силовскую l -подгруппу $\mathfrak{h}$. Определим в $\mathfrak{G}_d^{(c,r)}$ ряд подгрупп $Z_{r,s}$ по следующему правилу: $Z_{r,0} = Z_{r-1}$, $Z_{r,s} = [\mathfrak{h}, Z_{r,s-1}]$ — подгруппа, порожденная элементами z^{1-h} , где $z \in Z_{r,s-1}$, $h \in \mathfrak{h}$. $\mathfrak{G}_d^{(c,r)}/Z_{r,s}$ обозначим через $\mathfrak{G}_d^{(c,r,s)}$. Очевидно, что при некотором m , зависящем только от группы F ,

$$\mathfrak{G}_d^{(c,r,m)} = \mathfrak{G}_d^{(c,r)}.$$

Пусть в цепочке полей $\Omega \subset L \subset k \subset K$ группа Галуа поля K/Ω есть $F \cdot \mathfrak{G}_d^{(c,r)}$, где F – группа Галуа k/Ω , $\mathfrak{G}_d^{(c,r)}$ – группа Галуа K/k . Рассмотрим поле $\bar{K} \supset K$ такое, что группа Галуа K/k есть $\mathfrak{G}_d^{(c,r+1,s)}$, а $\bar{K}/L \cong \mathfrak{h} \cdot \mathfrak{G}_d^{(c,r+1,s)}$. Если поля, сопряженные с $\bar{K}/\Omega$, независимы над k , то их композит мы будем обозначать через $\bar{K}^*$.

Группа Галуа поля $\bar{K}^*/\Omega$ имеет следующее строение (что легко получить, повторяя рассуждения на стр. 395 работы [8]).

Обозначим $Z_r/Z_{r+1,s}$, через $\mathfrak{A}$, $Z_r/Z_{r+1,s}^u$, $u \in F$, – через $\mathfrak{A}^u$. Существует естественный изоморфизм $\mathfrak{A}$ на $\mathfrak{A}^u$. Действие его на $\alpha \in \mathfrak{A}$ будем обозначать через α^u . При этом различные u , принадлежащие к одному правому классу смежности A группы F по $\mathfrak{h}$, оказывают на α одно и то же действие. Ввиду этого, мы будем обозначать α^u через α^U и $\mathfrak{A}^u$ через $\mathfrak{A}^U$. Пусть $a(\sigma, \tau)$ – система множителей на $\mathfrak{G}_d^{(c,r)}$, соответствующая расширению $\mathfrak{G}_d^{(c,r+1,s)}$. Рассмотрим расширение $\mathfrak{G}_d^{(c,r+1,s)*}$ группы $\mathfrak{G}_d^{(c,r)}$ с нормальным делителем, являющимся прямым произведением всех $\mathfrak{A}^u$, и системой множителей

$$A(\sigma, \tau) = (\dots, \alpha(\sigma^{u^{-1}}, \tau^{u^{-1}})^U, \dots).$$

Элементы из F определяют естественным образом автоморфизмы в группе $\mathfrak{G}_d^{(c,r+1,s)*}$, которую мы будем теперь рассматривать как F -операторную группу. Группа Галуа поля $\bar{K}^*/\Omega$ есть полупрямое произведение $F \cdot \mathfrak{G}_d^{(c,r+1,s)*}$.

Мы будем в дальнейшем рассматривать операторные канонические гомоморфизмы групп $\mathfrak{G}_d^{(c)}$ на $\mathfrak{G}_\delta^{(c)}$, определенные в работе [8]. Легко видеть, что эти гомоморфизмы определяют гомоморфизмы $\mathfrak{G}_d^{(c,r)}$ на $\mathfrak{G}_\delta^{(c,r)}$ и $\mathfrak{G}_d^{(c,r,s)*}$ на $\mathfrak{G}_\delta^{(c,r,s)*}$. При этом, очевидно, эти гомоморфизмы являются F -операторными. К таким гомоморфизмам применимы понятия композиции гомоморфизмов, функций гомоморфизма и их степеней, введенные в работах [6] и [8].

Мы будем применять эти понятия к теории полей при помощи следующих соображений. Пусть дана цепочка полей $\Omega \subset L \subset k \subset K$, где k/Ω нормально с группой Галуа F , L принадлежит к силовой подгруппе $\mathfrak{h}$, а K/k имеет в качестве группы Галуа одну из групп $\mathfrak{G}_d^{(c)}$, $\mathfrak{G}_d^{(c,r)}$, $\mathfrak{G}_d^{(c,r,s)*}$. При этом K/Ω нормально и имеет группу Галуа $F \cdot \mathfrak{G}_d^{(c)}$, соответственно, $F \cdot \mathfrak{G}_d^{(c,r)}$ и $F \cdot \mathfrak{G}_d^{(c,r,s)*}$. Предположим, что K/Ω – шольцево относительно M и l . Каждому гомоморфизму S группы Галуа K/k соответствует подполе $K(S)$, также шольцево относительно M и l . В этом поле определены инварианты $[\chi, X]$ и $(X)_M$, инварианты $[X]_\psi$, если $[\chi, X] = (X)_M = 1$, и инварианты $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$, если $[\chi, X] = (X)_M = [X]_\psi = 1$,

так что каждый из этих инвариантов является функцией гомоморфизма S .

2. Степени инвариантов как функций гомоморфизмов. В работах [6] и [8] значительные трудности вызывало то обстоятельство, что инварианты $[\chi, X]$ и $[X]_\psi$ поля k определены не для всех χ и X и поля k , и тем самым, один такой инвариант, рассмотренный как функция гомоморфизма, определен не для всех гомоморфизмов. В нашем, более общем случае эти трудности еще возрастают. Они, однако, могут быть обойдены при помощи следующего предложения.

ЛЕММА 3. Для любого шольцева относительно M и l поля k , для всех его подполей и для всех χ и X можно определить символ $\{\chi, X\}$, совпадающий с $[\chi, X]$ каждый раз, как этот символ определен, и удовлетворяющий условиям:

$$\{\chi_1 \chi_2, X\} = \{\chi_1, X\} \{\chi_2, X\}, \quad (89)$$

$$\{\chi, X_1 X_2\} = \{\chi, X_1\} \{\chi, X_2\}, \quad (90)$$

$$\{\chi_1, X_1\} = \{\chi, X\}, \quad (91)$$

аналогичным (16), (17) и (18).

Доказательство. Нам достаточно определить символ $\{\chi, X\}$, удовлетворяющий условиям (89) и (90) для любых χ и X в самом поле k . Тогда в любом подполе мы определим этот символ при помощи соотношения (91), причем все условия леммы 3 будут, как легко проверить, выполнены.

Задача о доопределении символа $[\chi, X]$ до символа $\{\chi, X\}$ есть, по существу, задача о продолжении функции $\varphi(a, b)$, заданной на некоторых парах векторов из пространств A и B до билинейной функции, заданной на любых парах векторов. В общем случае легко выяснить, когда такое продолжение возможно. Для этого рассмотрим кронекеровское произведение $A \circ B$ пространств A и B и поставим паре векторов a, b в соответствие вектор $a \circ b \in A \circ B$. Билинейность функции $\varphi(a, b)$ эквивалентна тому, что функция

$$f(a \circ b) = \varphi(a, b),$$

заданная в $A \circ B$, может быть линейно продолжена на все $A \circ B$. Таким образом, для того, чтобы функцию $\varphi(a, b)$ можно было билинейно распространить на все $a \in A, b \in B$, необходимо и достаточно, чтобы выполнялось условие: если $\varphi(a_1, b_1)$, $\varphi(a_2, b_2)$ и $\varphi(a_3, b_3)$ определены и

$$a_1 \circ b_1 + a_2 \circ b_2 \equiv a_3 \circ b_3,$$

то

$$\varphi(a_1, b_1) + \varphi(a_2, b_2) = \varphi(a_3, b_3), \quad (92)$$

причем $\equiv$ означает равенство векторов в $A \circ B$.

Перейдем к заданной нами функции $[\chi, X]$, помня, что мы должны заменить аддитивную запись мультипликативной. Выберем в группе классов X базис $X_1, \dots, X_t$, а в каждом классе X_i — произвольного представителя μ_i . Положим

$$\mu_X \approx \mu_{X_1}^{r_1} \cdots \mu_{X_t}^{r_t},$$

если

$$X = X_1^{r_1} \cdots X_t^{r_t}.$$

Очевидно, что $X \rightarrow \mu_X$ является изоморфизмом группы X в группу $k^\times/k^{\times l}$. Возьмем произвольный простой дивизор $\mathfrak{P}$ и определим функцию

$$\alpha_{\mathfrak{P}}(\chi, X) \approx \mu_X^{\sum \varphi_{\mathfrak{P}, \chi}^{(i)}(X)}$$

в обозначениях, принятых в §1. Очевидно, что

$$\alpha_{\mathfrak{P}}(\chi_1 \chi_2, X) \approx \alpha_{\mathfrak{P}}(\chi_1, X) \alpha_{\mathfrak{P}}(\chi_2, X),$$

$$\alpha_{\mathfrak{P}}(\chi, X_1 X_2) \approx \alpha_{\mathfrak{P}}(\chi, X_1) \alpha_{\mathfrak{P}}(\chi, X_2),$$

откуда следует, что отображение $\chi \circ X \rightarrow \alpha_{\mathfrak{P}}(\chi, X)$ определяет гомоморфизм кронекеровского произведения группы характеров χ и группы классов X в группу $k^\times/k^{\times l}$. В частности, если

$$(\chi_1 \circ X_1)(\chi_2 \circ X_2) \equiv (\chi_3 \circ X_3),$$

то

$$\alpha_{\mathfrak{P}}(\chi_1, X_1) \alpha_{\mathfrak{P}}(\chi_2, X_2) \approx \alpha_{\mathfrak{P}}(\chi_3, X_3). \quad (93)$$

Так как

$$[\chi, X] = \prod_{\mathfrak{P}} \left(\frac{\alpha_{\mathfrak{P}}(\chi, X)}{\mathfrak{P}} \right) \quad (94)$$

и определено только тогда, когда все символы $\left(\frac{\alpha_{\mathfrak{P}}(\chi, X)}{\mathfrak{P}} \right)$ определены, то из (94) следует выполнение условия (92) для функции $[\chi, X]$. Тем самым лемма доказана.

В точности те же рассуждения применимы к инвариантам $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$ и показывают, что можно определить в поле k и всех его подполях для любых $X_1, \dots, X_{s-1}; X_s$ инвариант

$\{X_1, \dots, X_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}}$, совпадающий с $[X_1, \dots, X_{s-1}; X_s]_{\varphi_1, \dots, \varphi_{s-1}}$, когда этот последний инвариант определен, и обладающий свойствами:

$$\begin{aligned} & \{X_1, X'_1, \dots, X_{s-1} X'_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}} = \\ & = \{X_1, \dots, X_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}} \{X'_1, \dots, X'_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}}, \quad (95) \end{aligned}$$

$$\begin{aligned} & \{X_1, \dots, X_{s-1}; X_s X'_s\}_{\varphi_1, \dots, \varphi_{s-1}} = \\ & = \{X_1, \dots, X_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}} \{X_1, \dots, X_{s-1}; X'_s\}_{\varphi_1, \dots, \varphi_{s-1}}, \quad (96) \end{aligned}$$

$$\{X'_1, \dots, X'_{s-1}; X'_s\}_{\varphi_1, \dots, \varphi_{s-1}} = \{X_1, \dots, X_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}}, \quad (97)$$

аналогичными (89), (90) и (91).

Ввиду соотношения (95), мы можем разложить любой инвариант

$$\{X_1, \dots, X_{s-1}; X_s\}_{\varphi_1, \dots, \varphi_{s-1}}$$

в произведение инвариантов

$$\{1, \dots, X_i, \dots, 1; X_s\}_{\varphi_1, \dots, \varphi_{s-1}}.$$

В дальнейшем мы будем пользоваться обозначениями

$$\{1, \dots, X_i, \dots, 1; X_s\}_{\varphi_1, \dots, \varphi_{s-1}} = \{X_i, X_s\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$$

и ограничимся, на основании сказанного выше, рассмотрением инвариантов $\{X, X'\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$.

ЛЕММА 4. Пусть задано шольцево относительно M и l поле k , в котором $[\chi, X] = (X)_M = 1$ для всех χ и X . В поле k и во всех его подполях можно определить для любого X символ $\{X\}_\psi$, совпадающий с $[X]_\psi$ всякий раз, как этот символ определен, и удовлетворяющий условиям:

$$\{X X' X''\}_\psi \{X' X''\}_\psi^{-1} \{X X''\}_\psi^{-1} \{X X'\}_\psi^{-1} \{X\}_\psi \{X'\}_\psi \{X''\}_\psi = 1, \quad (98)$$

$$\{X_1\}_\psi = \{X\}_\psi, \quad (99)$$

из которых (99) аналогично (91). При этом предполагается, что функция ψ удовлетворяет условию 1^0 в определении символа $[X]_\psi$.

Доказательство. Выберем в группе классов X базис $X_1, \dots, X_t$, а в каждом классе X_i — произвольного представителя μ_{X_i} . Этот выбор произведем так, что если

$$\mu_{X_i} = \mathfrak{C}_i^l \mathfrak{D}_i \mathfrak{m}_i,$$

то

$$(m_i, m_j^\sigma) = 1, \quad \sigma \notin H. \quad (100)$$

Положим

$$\mu_X \approx \mu_{X_1}^{r_1} \cdots \mu_{X_t}^{r_t},$$

если

$$X = X_1^{r_1} \cdots X_t^{r_t}.$$

Дивизор m из разложения (11) для μ_X обозначим через m_X . Очевидно, что

$$\mu_{XX'} \approx \mu_X \mu_{X'}, \quad m_{XX'} \approx m_X m_{X'}. \quad (101)$$

Положим

$$\{X\}_\psi = \left[\frac{\mu_X}{m_X^\psi} \right].$$

Таким образом определенный инвариант $\{X\}_\psi$ совпадает с $[X]_\psi$, когда $[X]_\psi$ определено, т. е. когда выполнены условия 2^0 и 3^0 , а при $l = 2$ и условие 4^0 в определении $[X]_\psi$, так как в этом случае $\{X\}_\psi$ отличается от $[X]_\psi$ только другим выбором представителя μ_X в классе X , а как мы доказали в §1, $[X]_\psi$ не зависит от этого выбора.

Для символа $\{X\}_\psi$ выполнено также условие (98). В самом деле, левая часть (98) равна

$$\begin{aligned} & \left[\frac{\mu_{XX'X''}}{m_{XX'X''}^\psi} \right] \left[\frac{\mu_{X'X''}}{m_{X'X''}^\psi} \right]^{-1} \left[\frac{\mu_{XX''}}{m_{XX''}^\psi} \right]^{-1} \left[\frac{\mu_{XX'}}{m_{XX'}^\psi} \right]^{-1} \\ & \times \left[\frac{\mu_X}{m_X^\psi} \right] \left[\frac{\mu_{X'}}{m_{X'}^\psi} \right] \left[\frac{\mu_{X''}}{m_{X''}^\psi} \right]. \end{aligned}$$

Используя соотношения (100) и (101), а также мультипликативность символа $\left[\frac{\mu}{a} \right]$, мы получаем, путем разложения на множители, что это выражение равно 1.

Соотношение (99) мы, как и при доказательстве леммы 3, принимаем за определение символа $\{X\}_\psi$ в подполях поля k и получаем таким образом символ $\{X\}_\psi$, удовлетворяющий всем требованиям, сформулированным в условиях леммы.

Рассмотрим произвольную l -группу G класса c с заданной системой образующих $s_1, \dots, s_d$. Пусть $G = S_d/N$ есть представление G в виде факторгруппы свободной группы S_d , соответствующее этому выбору образующих. Обозначим через N' подгруппу N , порожденную коммутаторами элементов N с элементами S_d и l -ми степенями

элементов N . Классы X систем множителей на G со значениями в группе корней степени l из 1 находятся во взаимно однозначном соответствии с характерами группы N/N' (см. [6], лемма 1). С другой стороны, группа S_d/N' имеет класс $\leq c+1$ и поэтому все ее элементы и, в частности, элементы N/N' представляются коммутаторными формами (см. [10]) степени $\leq c+1$ от образующих $s_1, \dots, s_d$. Ввиду этого, N/N' является гомоморфным образом модуля форм Ли степени $\leq c+1$ от d переменных $x_1, \dots, x_d$. Переменные $x_1, \dots, x_d$ находятся во взаимно однозначном соответствии с образующими $s_1, \dots, s_d$. Если в G задана группа автоморфизмов, состоящих в перестановках образующих, то те же перестановки $x_1, \dots, x_d$ определяют в модуле Ли группу автоморфизмов, относительно которой указанный гомоморфизм является операторным. Ввиду указанных свойств мы будем рассматривать классы X как характеры модуля Ли.

Вернемся к цепочке полей $\Omega \subset L \subset k \subset K$, рассматривавшейся в предыдущем пункте, где группа Галуа K/k есть одна из групп $\mathfrak{S}_d^{(c)}$, $\mathfrak{S}_d^{(c,r)}$, $\mathfrak{S}_d^{(c,r,s)*}$ и K/Ω – шольцево. Определим в K символы $\{\chi, X\}$, $\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$ и $\{X\}_\psi$ согласно леммам 3 и 4. Как было указано, будучи рассмотрены для подполей $K(S)$, они являются функциями гомоморфизмов.

ТЕОРЕМА 3. Если характеры X , X' и X'' имеют относительно совокупности переменных $x_{u,\delta}$ степени $< n$, n' и n'' , X и хотя бы один из X' и X'' не аннулирует хотя бы одного многочлена Ли, зависящего хотя бы от одного $x_{u,\delta}$, и X , X' и X'' аннулируют все многочлены, зависящие только от $x_{u,i}$, $i < \delta - 1$, а $\chi(s_{u,i}) = 1$, $i \leq \delta - 1$, то инварианты $\{\chi, X\}$, $(X)_M$, $\{X\}_\psi$ и $\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$ имеют, как функции гомоморфизмов типа $(s_{u,1}, \dots, s_{u,\delta-1}; t_{u,1}, \dots, t_{u,\delta-1} | t_{u,\delta})$ шольцева относительно M и l поля K , следующие степени:

$$(X)_M - \text{степень} \leq n,$$

$$\{\chi, X\} - \text{степень} \begin{cases} \leq n, & \text{если } \chi(s_{u,\delta}) = 1 \text{ для всех } u, \\ \leq n+1, & \text{если } \chi(s_{u,\delta}) \neq 1 \text{ для некоторого } u, \end{cases}$$

$$\{X\}_\psi - \text{степень} \leq 2n,$$

$$\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)} - \text{степень} \leq n' + n''.$$

Доказательство этой теоремы в части, касающейся инвариантов $(X)_M$ и $\{\chi, X\}$, дословно совпадает с доказательством теоремы 4 работы [6], а в части, касающейся инвариантов $\{X\}_\psi$, также дословно совпадает с доказательством теоремы 7 работы [8]. Нам

остается, таким образом, доказать утверждение теоремы 3, относящееся к степени инварианта $\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$.

Наши рассуждения будут весьма близки к тем, которые использованы при доказательстве теоремы 7 работы [8].

Выберем в группе характеров X базис $X_1, \dots, X_t$ и запишем X' и X'' через этот базис:

$$X' = X_1^{c'_1} \dots X_t^{c'_t}, \quad X'' = X_1^{c''_1} \dots X_t^{c''_t}.$$

При фиксированном поле K инвариант $\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$ может быть записан в виде:

$$\zeta^{f(c'_1, \dots, c'_t; c''_1, \dots, c''_t)} = \zeta^{f(c', c'')},$$

где c' и c'' – векторы с координатами $(c'_1, \dots, c'_t)$, $(c''_1, \dots, c''_t)$ в t -мерном пространстве над полем классов вычетов $\text{mod } l$.

Соотношения

$$\begin{aligned} \{X'_1 X'_2, X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)} &= \{X'_1, X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)} \{X'_2, X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}, \\ \{X', X''_1 X''_2\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)} &= \{X', X''_1\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)} \{X', X''_2\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)} \end{aligned}$$

дают нам:

$$\begin{aligned} f(c'_1 + c'_2, c'') &\equiv f(c'_1, c'') + f(c'_2, c'') \pmod{l}, \\ f(c', c''_1 + c''_2) &\equiv f(c', c''_1) + f(c', c''_2) \pmod{l}, \end{aligned}$$

т. е. показывает, что функция $f(c', c'')$ билинейна. Из этого следует, что имеет место представление

$$f(c', c'') \equiv \sum_{i,k} a_{i,k} c'_i c''_k \pmod{l}.$$

Если рассматривать инвариант $\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$ как функцию канонического гомоморфизма S поля K , то и $c'_i(S)$, и $c''_k(S)$ будут функциями гомоморфизма, причем

$$f(S) \equiv \sum a_{i,k} c'_i(S) c''_k(S) \pmod{l}.$$

Соотношения (37) работы [6] показывают, что $c'_i(S)$ имеют степень $\leq n'$, а $c''_i(S)$ – степень $\leq n''$ относительно S . С другой стороны, в работе [8] доказано (стр. 416), что степень произведения двух функций не превосходит суммы их степеней. Ввиду этого, степень $f(S) \leq n' + n''$, что и доказывает теорему.

3. Построение поля с заданной разрешимой группой Галуа. В этом пункте мы будем пользоваться следующими обозначениями. Если в цепочке полей $\Omega \subset L \subset k \subset K$ поле K/k имеет группу Галуа $\mathfrak{G}_d^{(c)}$, $\mathfrak{G}_d^{(c,r)}$ или $\mathfrak{G}_d^{(c,r,s)*}$, то мы будем обозначать его, соответственно, через $K_d^{(c)}$, $K_d^{(c,r)}$, $K_d^{(c,r,s)*}$.

ТЕОРЕМА 4. Для любых натуральных чисел δ , r и s существует натуральное число $c_1(\delta, r, s)$ со следующим свойством: в любом шольцевом относительно M и l поле $K_d^{(c,r,s)*}/\Omega$ с группой Галуа $F \cdot \mathfrak{G}_d^{(c,r,s)*}$ и $d > c_1(\delta, r, s)$ существует подполе $K_\delta^{(c,r,s)*} = K_d^{(c,r,s)*}(S)$ с группой Галуа $F \cdot \mathfrak{G}_\delta^{(c,r,s)*}$ и всеми инвариантами $\{\chi, X\}$, $(X)_M$, $\{X\}_\psi$ и $\{X', X''\}_{\varphi_1, \dots, \varphi_{s-1}}^{(i)}$, равными 1.

Доказательство этой теоремы дословно повторяет доказательство теоремы 5 работы [6], если только заменить в нем ссылку на теорему 4 работы [6] ссылкой на теорему 3 настоящей работы.

ЛЕММА 5. Для любых чисел δ , r и s существует число $c(\delta, r, s)$ со следующим свойством: в любом шольцевом относительно M и l поле $K_d^{(c,r)}/\Omega$ с группой Галуа $F \cdot \mathfrak{G}_d^{(c,r)}$ над Ω и $d > c(\delta, r, s)$ существует подполе $K_\delta^{(c,r)} = K_d^{(c,r)}(S)$ с группой Галуа $F \cdot \mathfrak{G}_\delta^{(c,r)}$ над Ω , погружаемое в шольцево поле $K_\delta^{(c,r+1,s)*}$ с группой Галуа $F \cdot \mathfrak{G}_\delta^{(c,r+1,s)*}$ над Ω .

Мы докажем лемму индукцией по s . Пусть для любого δ найдено число $c(\delta, r, s-1)$. Докажем, что можно положить

$$c(\delta, r, s) = c(c_1(\delta, r, s), r, s-1),$$

где число $c_1(\delta, r, s)$ определено в теореме 4. Действительно, пусть $d > c(\delta, r, s)$ и $K_d^{(c,r)} \supset k$ — заданное нам шольцево поле с группой Галуа $F \cdot \mathfrak{G}_d^{(c,r)}$ над Ω . По предположению индукции, в поле $K_d^{(c,r)}$ существует подполе

$$K_{d_1}^{(c,r)} = K_d^{(c,r)}(S_1),$$

погружаемое в шольцево поле $K_{d_1}^{(c,r+1,s-1)*}$ с группой Галуа $F \cdot \mathfrak{G}_{d_1}^{(c,r+1,s-1)*}$ над Ω и $d_1 > c_1(\delta, r, s)$. Ввиду теоремы 4, в $K_{d_1}^{(c,r+1,s-1)*}$ существует подполе

$$K_\delta^{(c,r+1,s-1)*} = K_{d_1}^{(c,r+1,s-1)*}(S)$$

со всеми инвариантами, равными 1. Применяя теорему 2, мы видим, что $K_\delta^{(c,r+1,s-1)*}$ погружаемо в шольцево поле K^* , причем, очевидно, $K_\delta^{(c,r+1,s)} \subset K^*$ по определению поля K . Таким образом, $K_\delta^{(c,r+1,s)*}$ – шольцево, и лемма доказана.

Для некоторого натурального m

$$\mathfrak{G}_\delta^{(c,r+1,m)} = \mathfrak{G}_\delta^{(c,r+1)}.$$

Мы будем обозначать $\mathfrak{G}_\delta^{(c,r+1,m)*}$ через $\mathfrak{G}_\delta^{(c,r+1)*}$. Из леммы 5 очевидным образом вытекает

Следствие. Для любых δ, c и r существует число $c(\delta, c, r)$ со следующим свойством: в любом шольцевом поле $K_d^{(c,r)}$ с $d > c(\delta, c, r)$ существует подполе $K_\delta^{(c,r)} = K_d^{(c,r)}(S)$, погружаемое в шольцево поле $K_\delta^{(c,r+1)*} \supset k$ с группой Галуа $F \cdot \mathfrak{G}_\delta^{(c,r+1)*}$ над Ω .

Для доказательства достаточно положить в лемме 5 $s = m$.

ТЕОРЕМА 5. Любое шольцево относительно M и l поле k/Ω с группой Галуа F погружаемо в шольцево относительно M и l поле $K \supset k$ с группой Галуа G над k и $F \cdot G$ над Ω при любой F -операторной группе G порядка l^α . При этом M должно делиться на l в степени хотя бы на 1 большей, чем произведение показателей G и силовой l подгруппы группы F .

Доказательство. Так как любая F -операторная группа является операторно-гомоморфным образом группы $\mathfrak{G}_d^{(c)}$, имеющей тот же показатель, то нам достаточно доказать теорему для случая $G = \mathfrak{G}_d^{(c)}$. Мы докажем ее для более общего случая $G = \mathfrak{G}_\delta^{(c,r)}$. Так как

$$\mathfrak{G}_\delta^{(c,k)} = \mathfrak{G}_\delta^{(c)}, \quad \mathfrak{G}_\delta^{(c,0)} = \mathfrak{G}_\delta^{(c-1)},$$

то мы можем доказывать теорему индукцией по r при фиксированном и произвольном δ .

Пусть для групп $\mathfrak{G}_\delta^{(c,r-1)}$ теорема доказана. Тогда поле k погружаемо в шольцево поле $K_d^{(c,r-1)}$ с группой Галуа $F \cdot \mathfrak{G}_d^{(c,r-1)}$ над Ω и любым d . Возьмем, в частности, $d > c(\delta, r-1)$, где $c(\delta, r-1)$ – то число, существование которого доказано в следствии из леммы 5. Согласно этому следствию,

$$K_d^{(c,r-1)} \supset K_\delta^{(c,r-1)} = K_d^{(c,r-1)}(S),$$

причем $K_\delta^{(c,r-1)} \supset k$ и погружаемо в шольцево поле $K_\delta^{(c,r)*}$. Поля

$$\Omega \subset L \subset K_\delta^{(c,r-1)} \subset K_\delta^{(c,r,m)} \subset K_\delta^{(c,r)*}$$

образуют цепочку полей, к которым применима теорема Фаддеева-Гашютца. Согласно этой теореме, между $K_\delta^{(c,r-1)}$ и $K_\delta^{(c,r)*}$ содержится поле $K_\delta^{(c,r)}$ с группой Галуа $F \cdot \mathfrak{G}_\delta^{(c,r)}$ над Ω . Ввиду того, что $K_\delta^{(c,r)}$ является подполем шольцева поля $K_\delta^{(c,r)*}$, оно само шольцево. Теорема доказана.

Заметим, что ограничение на M в формулировке теоремы 5 мы должны были наложить, так как пользовались им при выводе свойств символа $[\chi, X]$ на стр. 532 и при применении теоремы Шольца, на основании которой для шольцевых полей степени l^α и центральных расширений задача погружения всегда разрешима.

ТЕОРЕМА 6. Утверждение теоремы 5 сохраняет силу при замене требования шольцевости относительно M и l требованием шольцевости относительно l .

Доказательство. Если Ω содержит корень ζ степени l из 1, то понятия шольцевости относительно M и l и шольцевости относительно M совпадают. Если Ω не содержит корня степени l из 1, то обозначим $k(\zeta)$ через $\bar{k}$, его группу – через $\bar{F}$, естественный гомоморфизм $\bar{F}$ на F – через $\varphi(\bar{u}) = u$, и ядро этого гомоморфизма – через C . Рассмотрим полупрямое произведение $\bar{F} \cdot G$, определив действие операторов из $\bar{F}$ на G формулой

$$\sigma^{\bar{u}} = \sigma^{\varphi(\bar{u})}, \quad \sigma \in G, \quad \bar{u} \in \bar{F}, \quad \varphi(\bar{u}) \in F.$$

Согласно лемме 1, поле $\bar{k}$ – шольцево относительно M и l , а ввиду теоремы 5 оно погружаемо в шольцево относительно M и l поле $\bar{K}$ с группой Галуа $\bar{F} \cdot G$ над Ω . В поле $\bar{K}$ подгруппе C его группы Галуа соответствует подполе K с группой Галуа $F \cdot G$ над Ω . Очевидно, что $K \supset k$ и дает решение интересующей нас задачи погружения. Так как $K(\zeta) = \bar{K}$ – шольцево относительно M и l , то на основании леммы 2 мы заключаем, что K – шольцево относительно M . Теорема доказана.

Следствие. Теорема 6 имеет место для любого нильпотентного нормального делителя G . При этом ограничение на M должно накладываться для каждой силовой подгруппы G .

Доказательство очевидно.

ТЕОРЕМА 7. Над любым полем алгебраических чисел существует расширение с любой наперед заданной разрешимой группой Галуа.

Доказательство. Пусть G – заданная нам разрешимая группа. Как доказал Оре [3], максимальный нильпотентный нормальный

делитель N группы G полудополнен, т. е. существует такая истинная подгруппа $G_1 \subset G$, что $G = G_1 \cdot N$. Из этого следует, что G есть гомоморфный образ полупрямого произведения $G_1 \cdot N$. Применим подобное же рассуждение к G_1 и будем продолжать до тех пор, пока не дойдем до единичной подгруппы. В результате мы получим группу $\tilde{G}$, гомоморфным образом которой является G и которая обладает рядом нормальных делителей:

$$\tilde{G} \supset N_1 \supset N_2 \supset \dots \supset N_r = (I)$$

со следующим свойством: $\tilde{G}/N_i$ является полупрямым произведением подгруппы F_i , изоморфной $\tilde{G}/N_{i-1}$, и нильпотентного нормального делителя N_{i-1}/N_i . Возьмем за M число, содержащее любой простой делитель l порядка $\tilde{G}$ в степени большей, чем он входит в произведение показателей силовских l -подгрупп групп N_{i-1}/N_i . Применяя r раз следствие из теоремы 6, мы получим поле $\tilde{K}/\Omega$ с группой Галуа $\tilde{G}$. Так как G является гомоморфным образом $\tilde{G}$, то в $\tilde{K}$ содержится подполе K/Ω с группой Галуа G .

Теорема доказана.

Заметим, что при доказательстве теоремы 7 можно добиться, чтобы дискриминанты всех рассматриваемых полей были взаимно просты с любым наперед заданным дивизором $\mathfrak{M}$. Из этого следует, что число расширений поля Ω , имеющих заданную разрешимую группу Галуа, бесконечно.

Приложение

Мы докажем здесь теорему существования, обобщающую на случай ненормальных полей основной результат работы [7].

Пусть k/Ω — нормальное поле алгебраических чисел с группой Галуа G . Мы будем предполагать, что k содержит корень ζ простой степени l из 1 и положим

$$\zeta^\sigma = \zeta^{g(\sigma)}, \quad \sigma \in G.$$

Пусть H — подгруппа G , порядок которой есть степень l , и L — принадлежащее к ней подполе k . Очевидно, что

$$g(\sigma_1\sigma_2) \equiv g(\sigma_1)g(\sigma_2), \quad g(h) \equiv 1 \quad (l), \quad h \in H,$$

и поэтому $g(\sigma)$ постоянно на правых и левых классах смежности G по H , а также на классах G по двойному модулю (H, H) . Мы будем писать $g(S)$, где S — один из этих классов, вместо $g(\sigma)$, $\sigma \in S$.

Пусть задана функция $\zeta(S)$ на множестве левых классов смежности S группы G по H со значениями в группе корней степени l из 1. Если $\mathfrak{S}$ – класс смежности G по модулю (H, H) , состоящий из классов $S_1, \dots, S_r$, то положим

$$\zeta(\mathfrak{S}) = \zeta(S_1) \cdots \zeta(S_r).$$

Мы предположим, что функция $\zeta(S)$ такова, что для любого класса $\mathfrak{S}$ по модулю (H, H)

$$1. \zeta(\mathfrak{S}) = \zeta(\mathfrak{S}^{-1})^{\mathfrak{g}(\mathfrak{S})}.$$

В случае, если $l = 2$, мы наложим некоторые дополнительные ограничения.

Пусть $\mathfrak{S}$ – инволютивный класс, т. е. $\mathfrak{S} = \mathfrak{S}^{-1}$. Докажем, что в $\mathfrak{S}$ существует такой представитель σ , что $\sigma^2 \in H$. В самом деле, если σ – любой представитель $\mathfrak{S}$, то из инволютивности следует, что

$$\sigma_1^{-1} = h_1 \sigma_1 h_2, \quad h_1, h_2 \in H.$$

Отсюда мы получаем:

$$(\sigma_1 h_1)(\sigma_1 h_1) h_1^{-1} h_2 = 1,$$

т. е.

$$(\sigma_1 h_1)^2 = h_2^{-1} h_1 \in H.$$

Таким образом, нам достаточно принять $\sigma_1 h_1$ за σ .

Очевидно, что σ лежит в нормализаторе подгруппы $H \cap H^\sigma$. С другой стороны, из

$$\sigma^2 \in H, \quad \sigma^2 = \sigma^{-1} \sigma^2 \sigma \in \sigma^{-1} H \sigma = H^\sigma$$

следует, что $\sigma^2 \in H \cap H^\sigma$. Ввиду этого, подгруппа $\{\sigma, H \cap H^\sigma\}$, порожденная σ и $H \cap H^\sigma$, содержит $H \cap H^\sigma$ как нормальный делитель индекса 2. Обозначим через LL^σ композит полей L и L^σ , принадлежащий подгруппе $H \cap H^\sigma$, а через Λ_σ – подполе, принадлежащее $\{\sigma, H \cap H^\sigma\}$. Очевидно, что

$$LL^\sigma \supset \Lambda_\sigma, \quad (LL^\sigma : \Lambda_\sigma) = 2.$$

Обозначим через $\mathfrak{D}_\sigma$ дифференту поля $LL^\sigma / \Lambda_\sigma$ и положим

$$\mathfrak{C}_\mathfrak{S} = N_{LL^\sigma / L}(\mathfrak{D}_\sigma).$$

Нетрудно доказать, что $\mathfrak{C}_\mathfrak{S}$ не зависит от выбора σ и $\mathfrak{S}$.

Теперь мы можем сформулировать дополнительные условия, накладываемые при $l = 2$:

1'. Все простые делители двойки полностью распадаются в k/Ω .

2'. Вещественные бесконечно удаленные простые дивизоры Ω распадаются на вещественные в k .

3'. Для любых инволютивных классов $\mathfrak{S}_1, \dots, \mathfrak{S}_r$, для которых $\mathfrak{C}_{\mathfrak{S}_1} \cdots \mathfrak{C}_{\mathfrak{S}_r} \approx \alpha_\chi$ в L

$$\zeta(\mathfrak{S}_1) \cdots \zeta(\mathfrak{S}_r) = 1.$$

Здесь α_χ – такое число из L , что $\sqrt{\alpha_\chi} \in k$.

ТЕОРЕМА. Пусть задано поле k/Ω и функция $\zeta(S)$, удовлетворяющие условию 1, а при $l = 2$ – условиям 1', 2' и 3', не критические и не сопряженные друг с другом в k/L простые дивизоры 1-го порядка $\mathfrak{Q}_1, \dots, \mathfrak{Q}_m$ поля L/Ω и корни степени l из 1 $\xi_1, \dots, \xi_m$. Существует бесконечно много чисел $\alpha \in L$, удовлетворяющих условиям:

$$\left(\frac{\alpha}{\mathfrak{Q}_i} \right) = \xi_i, \quad i = 1, \dots, m, \quad (102)$$

$$\left(\frac{\alpha}{\mathfrak{P}^\sigma} \right) = \zeta(S) \quad \text{для всех } \mathfrak{P}|\alpha, \quad \sigma \in G, \quad \sigma \notin H. \quad (103)$$

Условие (103) предполагает, что если $\mathfrak{P}|\alpha$ и $\sigma \notin H$, то $(\mathfrak{P}^\sigma, \alpha) = 1$.

При доказательстве мы будем пользоваться следующими обозначениями. Пусть $\mathfrak{T}$ – класс смежности G по модулю (H, H) и $\mathfrak{T} = T_1 + \dots + T_r$, где T_i – правые классы смежности G по (H, H) . Если α есть число из L , то под $\alpha^\mathfrak{T}$ мы будем понимать $\alpha^{\tau_1} \cdots \alpha^{\tau_r}$, где $\tau_i \in T_i$. Аналогичный смысл имеет $\mathfrak{a}^\mathfrak{T}$, где $\mathfrak{a}$ – дивизор из L .

Нам понадобится следующая лемма.

ЛЕММА. Если α и $\mathfrak{b}$ – число и дивизор из L , то $\alpha^\mathfrak{T}$ и $\mathfrak{b}^\mathfrak{T}$ также лежат в L . При этом

$$\left(\frac{\alpha}{\mathfrak{b}^\mathfrak{T}} \right) = \left(\frac{\alpha^{\mathfrak{T}^{-1}}}{\mathfrak{b}} \right)^{g(\mathfrak{T})}. \quad (104)$$

Доказательство. Из того, что $\mathfrak{T}$ есть класс смежности по двойному модулю (H, H) , следует, что $T_i = T_1 h_i$, $h_i \in H$, где h_i – представители классов смежности H по $H \cap H^{\tau_1}$. Ввиду этого,

$$\alpha^\mathfrak{T} = \alpha^{\tau_1(h_1 + \dots + h_r)}$$

и, соответственно,

$$\mathfrak{b}^{\mathfrak{T}} = \mathfrak{b}^{\tau_1(h_1 + \dots + h_r)}.$$

Число α^{τ_1} и дивизор $\mathfrak{b}^{\tau_1}$ принадлежат полю LL^{τ_1} . Изоморфизмы расширения LL^{τ_1}/L индуцируются, как легко видеть, автоморфизмами $h_1, \dots, h_r$ поля k/L . Таким образом, мы имеем:

$$\alpha^{\mathfrak{T}} = N_{LL^{\tau_1}/L}(\alpha^{\tau_1}), \quad \mathfrak{b}^{\mathfrak{T}} = N_{LL^{\tau_1}/L}(\mathfrak{b}^{\tau_1}),$$

откуда и следует, что $\alpha^{\mathfrak{T}}$ и $\mathfrak{b}^{\mathfrak{T}}$ принадлежат L .

Применим эти соображения к символу Лежандра $\left(\frac{\alpha}{\mathfrak{b}^{\mathfrak{T}}}\right)$. Мы имеем:

$$\left(\frac{\alpha}{\mathfrak{b}^{\mathfrak{T}}}\right)_L = \left(\frac{\alpha}{N_{LL^{\tau_1}/L}(\mathfrak{b}^{\tau_1})}\right)_L = \left(\frac{\alpha}{\mathfrak{b}^{\tau_1}}\right)_{LL^{\tau_1}}. \quad (105)$$

Применим теперь к α , $\mathfrak{b}^{\tau_1}$ и LL^{τ_1} автоморфизм τ_1^{-1} . Мы получим:

$$\left(\frac{\alpha^{\tau_1^{-1}}}{\mathfrak{b}}\right)_{LL^{\tau_1^{-1}}} = \left(\frac{\alpha}{\mathfrak{b}^{\tau_1}}\right)_{LL^{\tau_1}}^{g(\tau_1^{-1})} \quad \text{или} \quad \left(\frac{\alpha}{\mathfrak{b}^{\tau_1}}\right)_{LL^{\tau_1}} = \left(\frac{\alpha^{\tau_1^{-1}}}{\mathfrak{b}}\right)_{LL^{\tau_1^{-1}}}^{g(\mathfrak{T})}. \quad (106)$$

Наконец, аналогично (105), имеем:

$$\left(\frac{\alpha^{\tau_1^{-1}}}{\mathfrak{b}}\right)_{LL^{\tau_1^{-1}}} = \left(\frac{N_{LL^{\tau_1^{-1}}/L}(\alpha^{\tau_1^{-1}})}{\mathfrak{b}}\right)_L = \left(\frac{\alpha^{\mathfrak{T}^{-1}}}{\mathfrak{b}}\right)_L. \quad (107)$$

Соединяя (105), (106) и (107), получаем:

$$\left(\frac{\alpha}{\mathfrak{b}^{\mathfrak{T}}}\right)_L = \left(\frac{\alpha^{\mathfrak{T}^{-1}}}{\mathfrak{b}}\right)_L^{g(\mathfrak{T})}.$$

Лемма доказана.¹

¹ Аналогично доказывается более общее соотношение:

$$\left(\frac{\alpha}{\mathfrak{b}^{\mathfrak{T}}}\right)_{L_1} = \left(\frac{\alpha^{\mathfrak{T}^{-1}}}{\mathfrak{b}}\right)_{L_2}^{g(\mathfrak{T})},$$

где α есть число из поля L_1 , принадлежащего подгруппе H_1 , $\mathfrak{b}$ – дивизор из поля L_2 , принадлежащего подгруппе H_2 , $\zeta \in L_1 \cap L_2$, и $\mathfrak{T}$ – класс смежности G по двойному модулю (H_1, H_2) .

Доказательство теоремы. Рассмотрим сначала случай $l \neq 2$. Построим, как и в работе [7], последовательность простых l -гиперпримарных главных дивизоров $\pi_i \in L$, имеющих порядок 1 в L/Ω , полностью распадающихся в k/L , взаимно простых с l и удовлетворяющих условиям:

$$\left(\frac{\pi_i}{\Omega_i} \right) = \xi_i, \quad i = 1, \dots, m. \quad (108)$$

Эти условия должны быть выполнены для всех членов последовательности, в остальном же она строится рекуррентно, причем при построенных $\pi_1, \dots, \pi_{t-1}$ число π_t строится так, чтобы выполнялись условия:

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma} \right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma} \right)^{-1} \zeta(S), \quad s = 1, \dots, t-1, \quad \sigma \notin H, \quad (109)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_i^\sigma} \right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma} \right)^{-1} \zeta(S), \quad s = 1, \dots, t-1, \quad \sigma \notin H, \quad (110)$$

где $\mathfrak{P}_s$ – фиксированный простой делитель π_s в k .

Докажем, что такой выбор π_t возможен. Обозначим через f произведение модуля гиперпримарности, всех $N_{k/L}(\mathfrak{P}_s^\sigma)$ и $N_{k/L}(\Omega_i)$, через S_f – группу классов по модулю f в L , состоящую из l -х степеней главных дивизоров, а через Σ_f – поле классов к S_f . То, что простой дивизор $\mathfrak{p} \in L$ является главным ($\mathfrak{p} = (\pi)$, где π l -гиперпримарно) и удовлетворяет условиям (108) и (109), эквивалентно тому, что $\mathfrak{p}$ принадлежит в Σ_f ко вполне определенному автоморфизму σ . То, что $\mathfrak{p}$ полностью распадается в k/L и удовлетворяет условию (110), эквивалентно тому, что $\mathfrak{p}$ принадлежит ко вполне определенному автоморфизму τ в поле k' , получающемся присоединением к k всех $\sqrt[l]{\pi_i^\sigma}$, $i = 1, \dots, t-1$, $\sigma \notin H$. Для того, чтобы существовал простой дивизор $\mathfrak{p}$, удовлетворяющий всем этим условиям, необходимо и достаточно, в силу закона плотностей Чеботарева, чтобы в композите $\Sigma_f \cdot k'/L$ существовал автоморфизм, индуцирующий в Σ_f σ , а в k' – τ . Для этого, в свою очередь, необходимо и достаточно, чтобы в поле $\Sigma_f \cap k'$ σ и π индуцировали один и тот же автоморфизм.

Выясним, каково поле $\Sigma_f \cap k'$. Так как дискриминант k/L и все π_i^σ ($i = 1, \dots, t-1$) взаимно просты с Ω_i , то и дискриминант k' взаимно прост с Ω_i , а поэтому в дискриминант $\Sigma_f \cap k'$ дивизоры Ω_i не входят. Точно так же критические простые дивизоры k/L не входят в дискриминант $\Sigma_f \cap k'$, который состоит, таким образом, только из простых делителей π_i^σ и l . Обозначим через k_0 максимальное

абелево подполе поля k , дискриминант которого содержит только простые делители l , а группа Галуа k_0 над максимальным неразветвленным подполем имеет показатель l . Очевидно, что $\Sigma_f \cap k'$ содержит k_0 .

С другой стороны, $\Sigma_f \cap k'$ абелево над L и имеет над k_0 группу Галуа показателя l , т. е. получается присоединением к k_0 радикалов $\sqrt[l]{\eta_i}$, $\eta_i \in k_0$.

Пусть η – любое такое число поля k_0 , что $\sqrt[l]{\eta} \in \Sigma_f \cap k'$. Тогда тем более

$$\sqrt[l]{\eta} \in k', \quad \eta \in k.$$

Ввиду этого мы имеем для η представление

$$\eta = \prod_i \pi_i^{\sum f_i(T)\tau} \cdot \beta^l, \quad (111)$$

где $f_i(T)$ – функции на правых классах смежности G по H , а $\beta \in k$. Обозначим через H_0 подгруппу группы G , к которой принадлежит k_0 . Очевидно, что $H_0 \subset H$. Ввиду того, что $\eta \in k_0$, $\eta^{h_0} = \eta$ при $h_0 \in H_0$. Подставим в это соотношение выражение (111) для η . Так как π_i являются дивизорами 1-го порядка, то в получающемся равенстве показатели при π_i^T в левой и правой частях должны быть сравнимы $\text{mod } l$. Мы получаем, что

$$\begin{aligned} \left(\sum f_i(T)\tau \right) h_0 &\equiv \sum f_i(T)\tau \pmod{l}, \\ f_i(Th_0) &\equiv f_i(T) \pmod{l} \quad \text{при } h_0 \in H_0. \end{aligned}$$

Таким образом, $f_i(T)$ можно считать постоянными на классах смежности по двойному модулю (H, H_0) . Из этого, однако, следует, что

$$\pi_i^{\sum f_i(T)\tau} \in k_0,$$

а так как и $\eta \in k_0$, то и $\beta^l \in k_0$. Очевидно, что

$$\sqrt[l]{\pi_i^{\sum f_i(T)\tau}} \in \Sigma_f \cap k',$$

а так как и $\sqrt[l]{\eta} \in \Sigma_f \cap k'$, то и $\beta \in \Sigma_f \cap k'$. Мы видим, что

$$k_0(\beta) = \Sigma_f \cap k', \quad \beta^l \in k_0.$$

Предшествующие рассуждения показывают, что дискриминант $k_0(\beta)/L$ может делиться только на делителей l . Легко видеть, что

группа Галуа $k_0(\beta)$ над его максимальным неразветвленным подполем имеет показатель l , а над L она абелева. Таким образом, $k_0(\beta)$ обладает всеми теми свойствами, при помощи которых мы определили k_0 , а ввиду максимальности k_0 должно с ним совпадать, так что $\beta \in k_0$. Следовательно, $\Sigma_f \cap k'$ содержится в поле, получающемся присоединением к k_0 всех

$$\sqrt[l]{\pi_i^{\sum f_i(T)\tau}},$$

где $f_i(T)$ постоянны на классах смежности G по модулю (H, H_0) . Предположим, что

$$k_0(\sqrt[l]{\eta}) \subset \Sigma_f \cap k'.$$

Как мы показали,

$$\eta = \prod_i \pi_i^{\sum f_i(T)\tau}.$$

Из абелевости $\Sigma_f \cap k'/L$ следует, что $\eta^h = \eta$, $h \in H$. Рассуждая как и раньше, мы видим, что $f_i(T)$ должны быть постоянны на классах смежности G по модулю (H, H) . Но и наоборот, очевидно, что все числа

$$\pi_i^{\sum f_i(T)\tau} \in L,$$

так что

$$\sqrt[l]{\pi_i^{\sum f_i(T)\tau}} \subset \Sigma_f \cap k',$$

если $f_i(T)$ постоянно на классах смежности по модулю (H, H) . Таким образом, мы доказали, что $\Sigma_f \cap k'$ является композитом полей k_0 и $L(\sqrt[l]{\pi_i^{\mathfrak{S}}})$, где $\mathfrak{S}$ – классы смежности G по модулю (H, H) .

Найдем теперь автоморфизмы, которые индуцируют σ и τ в каждом из этих полей. В k_0 и σ , и τ индуцируют, как легко проверить, единичный автоморфизм. Возьмем какое-либо поле $L(\sqrt[l]{\pi_i^{\mathfrak{S}}})$ и простой дивизор $\mathfrak{p}$, принадлежащий к автоморфизму σ в Σ_f . По построению это значит, что $\mathfrak{p}$ – главный ($\mathfrak{p} = (\pi)$) и

$$\left(\frac{\pi}{\mathfrak{P}_s^\sigma} \right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma} \right)^{-1} \zeta(S) \quad \text{для любого } s = 1, \dots, t-1.$$

Из этого следует, что

$$\left(\frac{\pi_i^{\mathfrak{S}}}{\pi} \right) = \left(\frac{\pi}{\pi_i^{\mathfrak{S}}} \right) = \left(\frac{\pi_i}{\pi_i^{\mathfrak{S}}} \right)^{-1} \zeta(\mathfrak{S}).$$

Таким образом, π принадлежит в $L(\sqrt[l]{\pi_i^{\mathfrak{S}}})$ к автоморфизму, сводящемуся к умножению $\sqrt[l]{\pi_i^{\mathfrak{S}}}$ на

$$\left(\frac{\pi_i}{\pi_i^{\mathfrak{S}}}\right)^{-1} \zeta(\mathfrak{S}),$$

а следовательно, именно этот автоморфизм и индуцирует σ в этом поле.

Рассмотрим теперь простой дивизор $\mathfrak{p}$, принадлежащий к τ в k' . Очевидно, что тогда $\mathfrak{p} = N_{k/L}(\mathfrak{P})$, причем

$$\left(\frac{\pi_i^{\sigma}}{\mathfrak{P}_i}\right) = \left(\frac{\pi_i^{\sigma}}{\mathfrak{P}_i}\right)^{-1} \zeta(S^{-1})^{g(\sigma)}.$$

Рассуждая аналогично предыдущему, мы видим, что τ сводится в $L(\sqrt[l]{\pi_i^{\mathfrak{S}}})$ к умножению $\sqrt[l]{\pi_i^{\mathfrak{S}}}$ на

$$\left(\frac{\pi_i^{\mathfrak{S}}}{\pi_i}\right) \zeta(\mathfrak{S}^{-1})^{g(\mathfrak{S})}.$$

Ввиду l -гиперпримарности π_i , мы имеем:

$$\left(\frac{\pi_i^{\mathfrak{S}}}{\pi_i}\right) = \left(\frac{\pi_i}{\pi_i^{\mathfrak{S}}}\right),$$

а ввиду условия 1^0 , наложенного на $\zeta(S)$,

$$\zeta(\mathfrak{S}^{-1})^{g(\mathfrak{S})} = \zeta(\mathfrak{S}).$$

Таким образом, σ и τ сводятся к умножению $\sqrt[l]{\pi_i^{\mathfrak{S}}}$ на одно и то же число, и, значит, совпадают в $\Sigma_f \cap k'$. Этим доказана возможность выбора π_i на каждом шаге так, чтобы удовлетворялись условия (108), (109) и (110).

Теперь мы рассуждаем в точности так, как в работе [7]. В последовательности $\pi_1, \pi_2, \dots$ должны существовать два таких числа π_i и π_j , что

$$\left(\frac{\pi_i}{\mathfrak{P}_i^{\sigma}}\right) = \left(\frac{\pi_j}{\mathfrak{P}_j^{\sigma}}\right)$$

для любого $\sigma \in G$, $\sigma \notin H$. Непосредственная проверка показывает, что число $\alpha = \pi_i \pi_j$ удовлетворяет условиям теоремы.

Рассмотрим случай $l = 2$. Очевидно, что теперь $g(\sigma) = 1$. Разобьем все отличные от единицы классы по двойному модулю (H, H) на три группы. К первой мы отнесем все инволютивные классы. Неинволютивные классы разобьем на две части, отнеся по произволу из каждой пары взаимно обратных классов $\mathfrak{S}$ и $\mathfrak{S}^{-1}$ один к одной части, а другой – к другой части. Эти три части мы обозначим через U , V и V^{-1} и будем в дальнейшем рассматривать их не только как множества классов $\mathfrak{S}$, но и как множества содержащихся в них автоморфизмов.

Как и при нечетном l , построим последовательность простых главных дивизоров $\pi_1, \dots, \pi_t, \dots$ поля L , l -гиперпримарных, totally-положительных, полностью распадающихся в k/L и удовлетворяющих условиям:

$$\left(\frac{\pi_t}{\Omega_i}\right) = \xi_i, \quad i = 1, \dots, m, \quad \left(\frac{\pi_t}{\mathfrak{C}_{\mathfrak{S}}}\right) = \zeta(\mathfrak{S}), \quad \mathfrak{S} \in U. \quad (112)$$

В остальном мы строим последовательность рекуррентно по следующему правилу. Пусть $\pi_1, \dots, \pi_{t-1}$ построены. Разобьем их совокупность на две части – первую и вторую – способом, который будет указан позже. Первую и вторую части будем обозначать через Π_1 и Π_2 . Выберем π_t так, чтобы оно удовлетворяло условиям: если $\pi_s \in \Pi_1$, $\sigma \in U$, то

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma}\right) = 1, \quad (113)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_t^\sigma}\right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma}\right) \zeta(S); \quad (114)$$

если $\pi_s \in \Pi_2$, $\sigma \in U$, то

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma}\right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma}\right) \zeta(S), \quad (115)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_t^\sigma}\right) = 1; \quad (116)$$

если $\pi_s \in \Pi_1$, $\sigma \in V$, то

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma}\right) = 1, \quad (117)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_t^\sigma}\right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma}\right) \zeta(S); \quad (118)$$

если $\pi_s \in \Pi_2$, $\sigma \in V$, то

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma} \right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma} \right) \zeta(S), \quad (119)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_t^\sigma} \right) = 1; \quad (120)$$

если $\pi_s \in \Pi_1$, $\sigma \in V^{-1}$, то

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma} \right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma} \right) \zeta(S), \quad (121)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_t^\sigma} \right) = 1; \quad (122)$$

если $\pi_s \in \Pi_2$, $\sigma \in V^{-1}$, то

$$\left(\frac{\pi_t}{\mathfrak{P}_s^\sigma} \right) = 1, \quad (123)$$

$$\left(\frac{\pi_s}{\mathfrak{P}_t^\sigma} \right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma} \right) \zeta(S). \quad (124)$$

Здесь $\mathfrak{P}_s$ означает простой делитель π_s в k , выбранный для каждого s произвольно, но раз навсегда.

Как и в первой части доказательства (при $l \neq 2$), нам надо проверить, что такой выбор действительно возможен. Эта проверка проводится точно так же, как и в первой части.

Обозначим через f произведение простых дивизоров L , критических в k/L или в L/Ω , модуля l -гиперпримарности, всех $N_{k/L}(\mathfrak{P}_s^\sigma)$ и $N_{k/L}(\Omega_i)$ и построим, как и в первой части доказательства, поля Σ_f и k' . Пусть каждому простому дивизору τ в L , критическому в k/L или в L/Ω , отнесен корень степени 2 из 1 $(-1)^{x_\tau}$. То, что простой дивизор $p \in L$ является главным ($p = (\pi)$, где π 2-гиперпримарно), удовлетворяет условиям (113), (115), (117), (119), (121), (123) и

$$\left(\frac{\pi}{\tau} \right) = (-1)^{x_\tau}, \quad (125)$$

эквивалентно тому, что p принадлежит в Σ_f ко вполне определенному автоморфизму ω_1 . Точно так же то, что p полностью распадается в k и удовлетворяет условиям (116), (118), (120), (122),

(124) и (126), эквивалентно тому, что p принадлежит в k' ко вполне определенному автоморфизму ω_2 . Наша задача сводится теперь к тому, чтобы показать, что при некотором выборе x_τ автоморфизмы ω_1 и ω_2 будут индуцировать в $\Sigma_f \cap k'$ один и тот же автоморфизм и будут выполнены условия:

$$\sum f(\tau)x_\tau \equiv b(\mathfrak{S}) \quad (2), \quad \text{если} \quad \mathfrak{C}_\mathfrak{S} \approx \prod_\tau p^{f(\tau)}, \quad \zeta(\mathfrak{S}) = (-1)^{b(\mathfrak{S})}.$$

Рассуждая, как и в первой части доказательства, мы видим, что $\Sigma_f \cap k'$ есть композит полей k_0 , $L(\sqrt{\alpha_\chi})$ и $L(\sqrt{\pi_s^\mathfrak{S}})$, где α_χ – такие числа из L , что $\sqrt{\alpha_\chi} \in k$, а $\mathfrak{S}$ – любые классы смежности по модулю (H, H) . Легко видеть, что в k_0 ω_1 и ω_2 индуцируют один и тот же автоморфизм, а именно – единичный. Рассмотрим поле $L(\sqrt[l]{\pi_s^\mathfrak{S}})$, где $\pi_s \in \Pi_1$, а $\mathfrak{S} \in U$. Рассуждая, как и в случае $l \neq 2$, мы видим, что ω_1 индуцирует в этом поле единичный автоморфизм, а ω_2 – автоморфизм, сводящийся к умножению $\sqrt[l]{\pi_s^\mathfrak{S}}$ на

$$\left(\frac{\pi_s}{\pi_s^\mathfrak{S}} \right) \zeta(\mathfrak{S}).$$

Нам надо, таким образом, доказать, что

$$\left(\frac{\pi_s}{\pi_s^\mathfrak{S}} \right) = \zeta(\mathfrak{S}).$$

Так как, по условию,

$$\left(\frac{\pi_s}{\mathfrak{C}_\mathfrak{S}} \right) = \zeta(\mathfrak{S}),$$

то достаточно доказать, что

$$\left(\frac{\pi_s}{\pi_s^\mathfrak{S}} \right) = \left(\frac{\pi_s}{\mathfrak{C}_\mathfrak{S}} \right).$$

Мы докажем, что

$$\left(\frac{\alpha}{\alpha^\mathfrak{S}} \right) = \left(\frac{\alpha}{\mathfrak{C}_\mathfrak{S}} \right), \quad \mathfrak{S} \in U, \quad (126)$$

для любого 2-гиперпримарного числа α .

Ввиду формулы (105), мы имеем:

$$\left(\frac{\alpha}{\alpha^{\mathfrak{S}}}\right)_L = \left(\frac{\alpha}{\alpha^{\tau_1}}\right)_{LL^{\tau_1}}.$$

Выберем в качестве τ_1 того представителя $\mathfrak{S}$, квадрат которого содержится в H . В поле $LL^{\tau_1}/\Lambda_{\tau_1}$ τ_1 индуцирует автоморфизм второго порядка. Мы можем применить к этому полю формулу (6) работы [7] и тогда получим:

$$\left(\frac{\alpha}{\alpha^{\tau_1}}\right)_{LL^{\tau_1}} = \left(\frac{\alpha}{\mathfrak{D}_{\tau_1}}\right)_{LL^{\tau_1}} = \left(\frac{\alpha}{N_{LL^{\tau_1}/L}(\mathfrak{D}_{\tau_1})}\right)_L = \left(\frac{\alpha}{\mathfrak{C}_{\mathfrak{S}}}\right)_L.$$

Случай поля $k(\sqrt{\pi_s^{\mathfrak{S}}})$, где $\pi_s \in \Pi_2$, а $\mathfrak{S} \in U$, рассматривается совершенно аналогично.

Рассмотрим поле $k(\sqrt{\pi_s^{\mathfrak{S}}})$, где $\pi_s \in \Pi_1$, а $\mathfrak{S} \in V$. Равенства (117) показывают, что ω_1 индуцирует в этом поле единичный автоморфизм. Возьмем любой простой дивизор $\mathfrak{p}$, принадлежащий к ω_2 в k' . Равенства (122) показывают, что

$$\left(\frac{\pi_s}{\mathfrak{P}^{\sigma}}\right)_k = 1, \quad \text{если } \sigma \in V^{-1}, \quad \pi_s \in \Pi_1, \quad N_{k/L}(\mathfrak{P}) = \mathfrak{p},$$

т. е.

$$\left(\frac{\pi_s^{\sigma}}{\mathfrak{P}}\right)_k = 1, \quad \text{если } \sigma \in V, \quad \pi_s \in \Pi_1.$$

Из этих равенств мы видим, что

$$\left(\frac{\pi_s^{\mathfrak{S}}}{\mathfrak{P}}\right)_k = \left(\frac{\pi_s^{\mathfrak{S}}}{\mathfrak{p}}\right)_L = 1,$$

так как, ввиду леммы, $\pi_s^{\mathfrak{S}} \in L$. Таким образом, ω_2 также индуцирует в $k(\sqrt{\pi_s^{\mathfrak{S}}})$ единичный автоморфизм.

Рассмотрим поле $k(\sqrt{\pi_s^{\mathfrak{S}}})$, где $\pi_s \in \Pi_2$, а $\mathfrak{S} \in V$. Равенства (119) показывают, что ω_1 индуцирует в этом поле автоморфизм, сводящийся к умножению $\sqrt{\pi_s^{\mathfrak{S}}}$ на

$$\left(\frac{\pi_s}{\pi_s^{\mathfrak{S}}}\right) \zeta(\mathfrak{S}).$$

Равенства (124) показывают, что при $\sigma^{-1} \in V^{-1}$, т. е. $\sigma \in V$

$$\left(\frac{\pi_s^{\mathfrak{S}}}{\mathfrak{p}} \right) = \left(\frac{\pi_s^{\mathfrak{S}}}{\pi_s} \right) \zeta(\mathfrak{S}^{-1}),$$

если $\mathfrak{p}$ принадлежит к ω_2 в k' . Таким образом, ω_2 индуцирует в $L(\sqrt{\pi_s^{\mathfrak{S}}})$ автоморфизм, сводящийся к умножению $\sqrt{\pi_s^{\mathfrak{S}}}$ на

$$\left(\frac{\pi_s^{\mathfrak{S}}}{\pi_s} \right) \zeta(\mathfrak{S}^{-1}).$$

Так как

$$\left(\frac{\pi_s}{\pi_s^{\mathfrak{S}}} \right) = \left(\frac{\pi_s^{\mathfrak{S}}}{\pi_s} \right),$$

ввиду 2-гиперпримарности π_s , а $\zeta(\mathfrak{S}) = \zeta(\mathfrak{S}^{-1})$ по условию, то ω_1 и ω_2 совпадают в $L(\sqrt{\pi_s^{\mathfrak{S}}})$. Исследование случая, когда $\mathfrak{S} \in V^{-1}$, проводится совершенно аналогично.

Рассмотрим, наконец, поле $L(\sqrt{\alpha_\chi})$. Автоморфизм, который ω_1 индуцирует в этом поле, сводится к умножению $\sqrt{\alpha_\chi}$ на

$$(-1)^{\sum \varphi_\chi(\mathfrak{r})x_\mathfrak{r}}, \quad \text{если} \quad \alpha_\chi \approx \prod \mathfrak{r}^{\varphi_\chi(\mathfrak{r})},$$

а ω_2 индуцирует в нем единичный автоморфизм. Таким образом, нам надо подобрать $x_\mathfrak{r}$ так, чтобы удовлетворялись сравнения:

$$\begin{aligned} \sum f_\mathfrak{S}(\mathfrak{r})x_\mathfrak{r} &\equiv b(\mathfrak{S}) \pmod{2}, \quad \text{если} \quad \mathfrak{C}_\mathfrak{S} = \prod \mathfrak{r}^{f_\mathfrak{S}(\mathfrak{r})}, \\ \mathfrak{S} &\in U, \quad \zeta(\mathfrak{S}) = (-1)^{b(\mathfrak{S})}, \\ \sum \varphi_\chi(\mathfrak{r})x_\mathfrak{r} &\equiv 0 \pmod{2}, \quad \text{если} \quad (\alpha_\chi) = \prod \mathfrak{r}^{\varphi_\chi(\mathfrak{r})}. \end{aligned}$$

Если бы эта система была не совместна, то существовала бы линейная комбинация левых частей с коэффициентами при всех $x_\mathfrak{r}$, равными нулю и со свободным членом, отличным от 0.

Пусть

$$\sum_{\mathfrak{S} \in U} c(\mathfrak{S}) \sum_{\mathfrak{r}} f_\mathfrak{S}(\mathfrak{r})x_\mathfrak{r} + \sum_{\chi} d_\chi \sum \varphi_\chi(\mathfrak{r})x_\mathfrak{r} \equiv \sum_{\mathfrak{S}} c(\mathfrak{S})b(\mathfrak{S}) \pmod{2}, \quad (127)$$

есть такая линейная комбинация. Обозначим $\prod \chi^{d_x}$ через χ_0 . Принимая во внимание, что в (127) все коэффициенты при x_r равны 0, получаем:

$$\varphi_{\chi_0}(\tau) \equiv \sum_{\mathfrak{S} \in U} c(\mathfrak{S}) f_{\mathfrak{S}}(\tau) \quad (2)$$

или

$$(\alpha_{\chi_0}) \approx \prod_{\mathfrak{S} \in U} \mathfrak{c}_{\mathfrak{S}}^{c(\mathfrak{S})}.$$

Но в этом случае, по условию теоремы,

$$\prod_{\mathfrak{S}} \zeta(\mathfrak{S})^{c(\mathfrak{S})} = 1, \quad \text{т. е.} \quad \sum_{\mathfrak{S}} b(\mathfrak{S}) c(\mathfrak{S}) \equiv 0 \quad (2),$$

что показывает, что и свободный член в (127) обращается в 0.

Таким образом, выбор нужного нам числа π_i на каждом шаге возможен, как бы мы при этом ни разбивали множество $\pi_1, \dots, \pi_{t-1}$ на подмножества Π_1 и Π_2 . Мы будем производить это разбиение так, чтобы для любого числа n существовало $C(n)$ со следующим свойством: как бы мы ни разбили множество $\pi_1, \dots, \pi_{C(n)}$ на n подмножеств, хотя бы в одном из них найдутся три числа π_r, π_s и π_t ($r < s < t$) таких, что при разбиении $\pi_1, \dots, \pi_{t-1}$ на Π_1 и Π_2 π_r и π_s попадут в различные части, а при разбиении $\pi_1, \dots, \pi_{s-1}$ на Π_1 и Π_2 π_r попадет не в ту часть, в которую оно попало при разбиении $\pi_1, \dots, \pi_{t-1}$. Возможность производить разбиение на каждом шаге указанным образом доказана в лемме, содержащейся в работе [7].

Мы будем разбивать $\pi_1, \dots, \pi_{C(n)}$ на подмножества, относя к одному подмножеству все π_i с одинаковыми значениями $\left(\frac{\pi_i}{\mathfrak{P}_i^\sigma}\right)$, $\sigma \notin H$. Таким образом, $n = 2^{(G:H)-1}$. Ввиду указанного свойства разбиения на Π_1 и Π_2 , мы найдем три числа π_r, π_s и π_t , удовлетворяющих условиям:

$$\left(\frac{\pi_r}{\mathfrak{P}_r^\sigma}\right) = \left(\frac{\pi_s}{\mathfrak{P}_s^\sigma}\right) = \left(\frac{\pi_t}{\mathfrak{P}_t^\sigma}\right).$$

Непосредственная проверка, полностью аналогичная проведенной в работе [7], показывает, что тогда число $\alpha = \pi_1 \pi_2 \pi_3$ удовлетворяет условиям теоремы. Теорема доказана.

Заметим, что, как видно из доказательства теоремы, мы можем π_i выбрать принадлежащими к заданному автоморфизму в любом расширении K/L поля k , если этот автоморфизм индуцирует в k

единичный автоморфизм и существуют простые главные дивизоры, принадлежащие в K к этому автоморфизму и удовлетворяющие условиям (108) и (112).

Поступило 4.IX.1954

ЛИТЕРАТУРА

1. Gaschütz W., *Zur Erweiterungstheorie der endlichen Gruppen*, J. reine und angew. Math. **190** (1952), 93–107.
2. Kochendörffer R., *Zwei Reduktionssätze zum Einbettungsproblem für Abelsche Algebren*, Math. Nachr., 10 Nr. 1–2 (1953), 75–84.
3. Ore O., *Contributions to the theory of groups of finite order*, Duke Math. J., 5 N 2 (1939), 431–460.
4. Фаддеев Д. К., *К теории гомологий в группах*, Изв. Ак. наук СССР, сер. матем. **16** (1952), 17–22.
5. Фаддеев Д. К., *Об одной теореме теории гомологий в группах*, Доклады Ак. наук СССР, 92 4 (1953), 703–705.
6. Шафаревич И. Р., *О построении полей с заданной группой Галуа порядка l^α* , Изв. Ак. наук СССР, сер. матем. **18** (1954), 261–296.
7. Шафаревич И. Р., *Об одной теореме существования в теории алгебраических чисел*, Изв. Ак. наук СССР, сер. матем. **18** (1954), 327–334.
8. Шафаревич И. Р., *О задаче погружения полей*, Изв. Ак. наук СССР, сер. матем. **18** (1954), 389–418.
9. Шафаревич И. Р., *О разрешимых в радикалах расширениях полей алгебраических чисел*, Доклады Ак. наук СССР, 95 2 (1954), 225–227.
10. Zassenhaus H., *Lehrbuch der Gruppentheorie*, Leipzig, 1937.

О БИРАЦИОНАЛЬНОЙ ЭКВИВАЛЕНТНОСТИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

ДОКЛ. АКАД. НАУК СССР ТОМ 114, no.2 (1957)

1. Рассмотрим эллиптические кривые (кривые рода I) над произвольным полем k , про которое мы будем только предполагать, что его характеристика отлична от 2 и 3. Классификация таких кривых с точки зрения бирациональной эквивалентности хорошо известна в случае алгебраически замкнутого поля k [1]. В этом случае каждая эллиптическая кривая γ бирационально эквивалентна кривой ω , имеющей вейерштрассову нормальную форму

$$y^2 = x^3 + ax + b; \quad a, b \in k. \quad (1)$$

В свою очередь две кривые, имеющие вейерштрассову форму, тогда и только тогда бирационально эквивалентны, когда их абсолютные инварианты j , определяемые формулой

$$j = \frac{4a^3}{4a^3 + 27b^2},$$

совпадают.

Если поле k не алгебраически замкнуто, то эллиптическая кривая, заданная над k , может быть приведена к вейерштрассовой форме в некотором конечном расширении поля k , причем ее абсолютный инвариант будет лежать в k [2].

Так как среди кривых с заданным абсолютным инвариантом есть и такие, которые имеют вейерштрассову форму над k , то мы получим все эллиптические кривые над k с заданным значением абсолютного инварианта, взяв кривую ω с уравнением (1) и рассмотрев все эллиптические кривые над k , бирационально эквивалентные ей над конечными расширениями поля k .

2. Рассмотрим некоторое конечное нормальное расширение K/k поля k и исследуем эллиптические кривые γ , заданные над k и бирационально эквивалентные ω над K . Обозначим через M общую

точку γ над k , а через $k(M)$ и $K(M)$ — поля рациональных функций на γ с коэффициентами из k и K , соответственно. По условию поле $K(M)$ изоморфно $K(x, y)$, где (x, y) — общая точка ω .

Любой автоморфизм σ поля K/k можно продолжить до автоморфизма $\varphi_\gamma(\sigma)$ поля $K(M)$, положив $M^\sigma = M$, а ввиду изоморфизма $K(M)$ с $K(x, y)$ перенести на $K(x, y)$. Очевидно, что

$$\varphi_\gamma(\sigma\tau) = \varphi_\gamma(\sigma)\varphi_\gamma(\tau). \quad (2)$$

Наоборот, если задан такой изоморфизм $\sigma \rightarrow \varphi(\sigma)$ группы Галуа K/k в группу автоморфизмов поля $K(x, y)$, что $\sigma = \varphi(\sigma)$ на K , то подполе функций из $K(x, y)$, инвариантных относительно всех $\varphi(\sigma)$, определяет некоторую эллиптическую кривую над k , бирационально эквивалентную ω над K . Нетрудно проверить, что две кривые γ_1 и γ_2 рассматриваемого типа будут тогда и только тогда бирационально эквивалентны над k , когда

$$\varphi_{\gamma_1}(\sigma) = t\varphi_{\gamma_2}(\sigma)t^{-1}, \quad (3)$$

где t — некоторый автоморфизм поля $K(x, y)$, не меняющий элементов поля K .

Аutomорфизм $s_\gamma(\sigma)$ поля $K(x, y)$, определяемый из равенства

$$\varphi_\gamma(\sigma) = s_\gamma\sigma\varphi_\omega(\sigma),$$

очевидно, не меняет элементов поля K , т.е. является автоморфизмом $K(x, y)/K$. Для того, чтобы удовлетворялось соотношение (2), необходимо и достаточно, чтобы $s_\gamma(\sigma)$ удовлетворяли условиям

$$s_\gamma(\sigma\tau) = s_\gamma(\sigma)s_\gamma(\tau)^{\varphi_\omega(\sigma)},$$

где,

$$s_\gamma(\tau)^{\varphi_\omega(\sigma)} = \varphi_\omega(\sigma)s_\gamma(\tau)\varphi_\omega(\sigma)^{-1},$$

а условие (3) переписывается в виде

$$s_{\gamma_1}(\sigma) = ts_{\gamma_2}(\sigma)t^{-\varphi_\omega(\sigma)}.$$

Аutomорфизмы s поля $K(x, y)/K$ хорошо известны [3]. Они имеют вид

$$s(x, y) = \varepsilon(x, y) + P, \quad (4)$$

где P есть некоторая точка на ω с координатами из K , а сложение понимается в смысле сложения точек на ω . Если $j \neq 0, 1$, то

$$\varepsilon(x, y) = (x, \pm y),$$

а если $j = 0$ или 1 , то ε может быть одним из шести или четырех автоморфизмов, не меняющих бесконечно удаленной точки ω . Записав автоморфизмы $s_\gamma(\sigma)$ в виде (4), мы приходим к следующему результату:

Теорема 1. Каждая эллиптическая кривая γ над k , бирационально эквивалентная над K кривой ω с уравнением (1), определяет систему автоморфизмов $\varepsilon_\gamma(\sigma)$ поля $K(x, y)$ и точек $P_\gamma(\sigma)$ кривой ω над K . Выполняются соотношения

$$\begin{aligned}\varepsilon_\gamma(\sigma\tau) &= \varepsilon_\gamma(\sigma)\varepsilon_\gamma(\tau)^\sigma, \\ P_\gamma(\sigma\tau) &= P_\gamma(\sigma)\varepsilon_\gamma(\tau)^\sigma + P_\gamma(\tau)^\sigma.\end{aligned}\tag{5}$$

Любая система автоморфизмов и точек, удовлетворяющая этим условиям, определяется некоторой кривой γ . Кривые γ_1 и γ_2 тогда и только тогда бирационально эквивалентны над k , когда существует такой автоморфизм ε и такая точка P на ω , что

$$\begin{aligned}\varepsilon_{\gamma_1}(\sigma) &= \varepsilon_{\gamma_2}(\sigma)\varepsilon^{1-\sigma}, \\ P_{\gamma_1}(\sigma) &= \varepsilon^{-\sigma}(P_{\gamma_2}(\sigma) + \varepsilon_{\gamma_2}(\sigma)P - P^\sigma).\end{aligned}\tag{6}$$

3. В изучаемом нами множестве кривых может быть несколько кривых, имеющих вейерштрассову форму. Любую из них мы могли бы взять за ω . Можно показать, что кривая γ тогда и только тогда может быть над k приведена к вейерштрассовой форме, когда γ бирационально эквивалентна над k кривой γ' , для которой $P_{\gamma'}(\sigma) = O$ (нулю группы точек над ω). Таким образом, в совокупности всех кривых с одной системой автоморфизмов $\varepsilon_\gamma(\sigma)$ есть с точностью до бирациональной эквивалентности одна кривая, имеющая вейерштрассову форму над k . Если бы мы приняли ее за ω , то всем кривым, которым в первом описании соответствовала система автоморфизмов $\varepsilon_\gamma(\sigma)$, соответствовала бы, как можно показать, единичная система автоморфизмов. Ввиду этого мы ограничимся рассмотрением кривых, для которых $\varepsilon_\gamma(\sigma) = 1$. Равенства (5) и при $\varepsilon = 1$ (6) переходят тогда в определения скрещенного гомоморфизма и главного скрещенного гомоморфизма [4].

Если для кривой γ $\varepsilon_\gamma(\sigma) = 1$, то кривая ω является ее якобиевым многообразием [5].

Действительно, ввиду того, что $K(x, y) = K(M)$,

$$(x, y) = \Phi(M),$$

где Φ — бирациональное отображение γ на ω над K . Для дивизора $\mathfrak{A} = \mathfrak{P}_1^{a_1} \dots \mathfrak{P}_r^{a_r}$ на γ положим

$$\Phi(\mathfrak{A}) = a_1\Phi(\mathfrak{P}_1) + \dots + a_r\Phi(\mathfrak{P}_r).$$

Как известно, если $d(\mathfrak{A}) = d(\mathfrak{B}) = 0$, то $\mathfrak{A} \sim \mathfrak{B}$ на γ тогда и только тогда, когда $\Phi(\mathfrak{A}) = \Phi(\mathfrak{B})$. Нам остается только проверить,

что если $d(\mathcal{A}) = 0$ и $\mathcal{A}$ определено над некоторым полем $k' \supset k$, то и $\Phi(\mathcal{A})$ определено над k' . Это легко следует из (4): если σ — изоморфизм K/k' , то

$$(\Phi(\mathcal{A}))^\sigma = \Phi^\sigma(\mathcal{A}^\sigma) = \Phi(\mathcal{A}^\sigma) + (\Sigma a_r)P_\sigma = \Phi(\mathcal{A}) + d(\mathcal{A})P_\sigma = \Phi(\mathcal{A}).$$

Таким образом, множество эллиптических кривых над k , имеющих ω своим якобиевым многообразием и бирационально эквивалентных ω над K , отображается на множество скрещенных гомоморфизмов группы Галуа G поля K/k в группу точек $\mathcal{A}_K$ на ω с координатами из K . Формулы (6) показывают, что две кривые рассматриваемого типа бирационально эквивалентны над k только если: или 1) соответствующие им скрещенные гомоморфизмы отличаются на главный скрещенный гомоморфизм, или 2) один из них получается из другого применением автоморфизма ε кривой ω , рассматриваемой как алгебраическая группа. Если мы включим в понятие эллиптической кривой с заданным якобиевым многообразием ω и каноническую функцию Φ , отображающую группу классов дивизоров нулевой степени на γ на кривую ω , то преобразования второго типа с $\varepsilon \neq 1$ отпадут, и бирациональные (в новом смысле) классы кривых γ будут находиться во взаимно-однозначном соответствии с элементами одномерной группы гомологий [4] $H^1(G, \mathcal{A}_K)$. Групповая операция, определенная на $H^1(G, \mathcal{A}_K)$, естественно переносится на эти классы. Все кривые с якобиевым многообразием ω получатся, если рассмотреть объединение всех полей K и соответственно индуктивный предел группы $H^1(G, \mathcal{A}_K)$. Таким образом, мы приходим к следующему результату:

Теорема 2. Бирациональные классы эллиптических кривых над k с заданным якобиевым многообразием ω образуют группу, изоморфную $H^1(\mathfrak{G}, \mathcal{A}_{\tilde{k}})$, где $\mathfrak{G}$ — группа Галуа сепарабельного алгебраического замыкания $\tilde{k}$ поля k , а $\mathcal{A}_{\tilde{k}}$ — группа точек на ω с координатами из $\tilde{k}$. При этом скрещенные гомоморфизмы считаются непрерывными, $\mathfrak{G}$ топологизирована по Круллю [6], $\mathcal{A}_{\tilde{k}}$ дискретна.

Как объединение групп гомологий конечных групп, группа $H^1(\mathfrak{G}, \mathcal{A}_{\tilde{k}})$ периодична. Можно показать, что порядок эллиптической кривой γ в этой группе делится на наименьший порядок класса дивизоров на γ .

4. Если k есть поле алгебраических чисел, то по теореме Морделя–Вейля [7] группа $\mathcal{A}_K$ имеет конечное число образующих. Тем самым это верно и для $H^1(G, \mathcal{A}_K)$; но так как эта группа периодична, то она конечна. Вместе с теоремами 1 и 2 это приводит нас к следующему результату:

Теорема 3. *Имеется только конечное число бирационально неэквивалентных кривых над полем алгебраических чисел k , которые имеют заданное значение абсолютного инварианта j и простой дивизор первой степени в заданном конечном расширении K/k .*

Ввиду теоремы Лютца [8] то же верно, когда k является полем p -адических чисел. Но так как над полем p -адических чисел имеется только конечное число расширений заданной степени, то имеет место более сильное утверждение:

Теорема 4. *Все эллиптические кривые заданной степени и с заданным значением абсолютного инварианта j распадаются на конечное число бирациональных классов над полем p -адических чисел k .*

Аналогичная теорема не верна для рациональных чисел, даже если ограничиться кривыми с заданным якобиевым многообразием. Действительно, кривые с уравнением (в однородных координатах)

$$a_0 x_0^3 + a_1 x_1^3 + a_2 x_2^3 = 0$$

имеют якобиевым многообразием кривую

$$a_0 a_1 a_2 x_0^3 + x_1^3 + x_2^3 = 0.$$

Следовательно, при $a_i = p^i$ ($i = 0, 1, 2$) и произвольном простом p мы получаем бесконечно много кривых с общим якобиевым многообразием и бирационально неэквивалентных между собой, так как они не эквивалентны даже в поле p -адических чисел.

5. В работе [9] Вейль определяет группу главных однородных алгебраических пространств с заданной абелевой группой операторов. Так как каждая эллиптическая кривая является однородным пространством относительно своего якобиевого многообразия, то результат Вейля применим к нашему случаю. Можно показать, что определенная им группа изоморфна той, которая описывается теоремой 2. Те же соображения, которыми мы пользовались при выводе этой теоремы, применимы и к случаю, рассмотренному Вейлем, так что имеет место следующая теорема.

Теорема 5. *Группа главных однородных алгебраических многообразий над k с заданной коммутативной абелевой группой G изоморфна одномерной группе гомологий $H^1(\mathfrak{G}, \mathfrak{A}_{\tilde{k}})$, где $\mathfrak{G}$ — группа Галуа сепарабельного алгебраического замыкания $\tilde{k}/k$; $\mathfrak{A}_{\tilde{k}}$ — группа точек на ω с координатами из $\tilde{k}$.*

Поступило 12.XI.1956

ЛИТЕРАТУРА

1. Р.Уокер, *Алгебраические кривые*, ИЛ, (1951).
2. M.Deuring, Math. Zs. **47** (1941), 4756.
3. H.Hasse, J. f. Math **175** No **2** (1936).
4. А.Г.Курош, *Теория групп*, М., 1953.
5. W.L.Chow, Am. J. Math **76** No **2** (1954).
6. W.Krull, Math. Ann. **100** (1928), 687.
7. A.Weil, Bull. Sci. Math., 2 ser. **54** (1930), 182.
8. E.Lutz, J. f. Math. **177**, No **4** (1937).
9. A.Weil, Am. J. Math. **77** No **3** (1955).

ПОКАЗАТЕЛИ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

ДОКЛ. АКАД. НАУК СССР ТОМ 114, no.4 (1957)

Алгебраической кривой γ , определенной над полем k , можно, кроме рода g , сопоставить еще несколько целочисленных инвариантов: наименьшую положительную степень f дивизора на γ ; наименьшую степень d кривой, бирационально эквивалентной γ над k ; наименьшую степень ν простого дивизора на γ . Связи между этими инвариантами мало изучены в случае произвольных кривых, но для эллиптических кривых ($g = 1$) все они выражаются через один, а именно, как легко следует из теоремы Римана-Роха, для эллиптической кривой $\nu = f$, $d = f$ при $f > 2$; $d = 4$ при $f = 2$ и $d = 3$ при $f = 1$. Инвариант f мы будем называть *показателем* кривой γ .

Для кривой рода g $f|2g - 2$, и поэтому при $g \neq 1$ показатель может принимать только конечное число значений. Для эллиптических кривых, как уже отмечалось (см., например, [1, 2]), неизвестно, какие значения может принимать показатель. В этой заметке будет доказано, что над полем рациональных чисел R существуют эллиптические кривые γ со сколь угодно большим показателем, причем даже может быть произвольным образом предписана якобиева кривая ω кривой γ .

Для доказательства мы используем группу $H(\omega)$, которую образуют классы бирационально эквивалентных над k кривых с заданной якобиевой кривой ω . Эта группа была впервые определена А. Вейлем [3]. Далее мы будем пользоваться той конструкцией группы $H(\omega)$, которая дана в моей работе [4]. Как показано в этой работе, показатель кривой γ кратен порядку γ как элемента группы $H(\omega)$. Там же показано, что подгруппа $H(K, \omega)$ группы $H(\omega)$, состоящая из всех кривых из $H(\omega)$, имеющих простой дивизор первой степени в заданном нормальном расширении K поля R , изоморфна группе $H^1(G, \mathfrak{A}_K)$, где G — группа Галуа K/R ; $\mathfrak{A}_K$ — группа точек на ω с координатами из K , а $H^1(G, \mathfrak{A}_K)$ — группа скрещенных гомоморфизмов G в $\mathfrak{A}_K$.

Если p — простой дивизор K ; p — делящее его простое число; G_p — группа разложения p , а K_p и R_p — соответствующие локальные

поля, то имеется естественный гомоморфизм вложения:

$$\varphi_p: H^1(G, \mathcal{A}_K) \rightarrow H^1(G_p, \mathcal{A}_{K_p}). \quad (1)$$

Сначала мы рассмотрим группу $H^1(G_p, \mathcal{A}_{K_p})$.

Пусть уравнение ω имеет вид

$$y^2 = x^3 + ax + b, \quad \Delta = 4a^3 + 27b^2 \neq 0,$$

причем a и b можно считать целыми числами. Обозначим через H_p подгруппу тех элементов группы H , порядки которых взаимно просты с p .

При изучении группы $H^1(G_p, \mathcal{A}_{K_p})_p$ можно предположить, что поле K_p не имеет высшего ветвления, так как в противном случае можно было бы перейти к некоторому его подполю. Обозначим через $\mathcal{A}_{K_p}^r$ подгруппу $\mathcal{A}_{K_p}$, рассмотренную Лютц [5] и состоящую из точек (x, y) на ω , для которых $x p^{2(r-1)}$ и $y p^{3(r-1)}$ нецелые. Легко доказать, что при $r \geq 1$ группа $\mathcal{A}_{K_p}^r / \mathcal{A}_{K_p}^{r+1}$ является p -группой. Из этого легко вывести, что группа $H^1(G_p, \mathcal{A}_{K_p})_p$ изоморфна группе $H^1(G_p, \mathcal{A}'_{K_p} / \mathcal{A}''_{K_p})_p$.

Предположим, что сверх того $p \nmid \Delta$. Тогда, как показано в [5], группа $\mathcal{A}_{K_p} / \mathcal{A}_{K_p}^1$ изоморфна $\mathcal{A}_{\mathcal{K}_p}$, где $\mathcal{K}_p$ — поле классов вычетов K_p по p , а $\mathcal{A}_{\mathcal{K}_p}$ — группа точек на кривой ω , рассмотренной по модулю p . Обозначим через F_p группу инерции $\mathfrak{p}$ в K_p . Тогда G_p / F_p является группой Галуа поля $\mathcal{K}_p$, и G_p является группой операторов для $\mathcal{A}_{\mathcal{K}_p}$, причем F_p действует тривиально. Как было сказано,

$$H^1(G_p, \mathcal{A}_{K_p})_p \cong H^1(G_p, \mathcal{A}_{\mathcal{K}_p})_p.$$

Рассмотрим гомоморфизм ограничения

$$H^1(G_p, \mathcal{A}_{\mathcal{K}_p})_p \rightarrow H^1(F_p, \mathcal{A}_{\mathcal{K}_p})_p. \quad (2)$$

Ядро этого отображения состоит из гомоморфизмов, обращающихся в 0 на F_p и, следовательно, являющихся гомоморфизмами G_p / F_p в $\mathcal{A}_{\mathcal{K}_p}$. Так как для кривых над конечным полем, как известно [6], $f = 1$, то

$$H^1(G_p / F_p, \mathcal{A}_{\mathcal{K}_p}) = 0,$$

и поэтому гомоморфизм (2) является мономорфизмом. Легко видеть, что образ этого гомоморфизма совпадает с группой $\text{Hom}_{G_p / F_p}(F_p, \mathcal{A}_{\mathcal{K}_p})$ операторных G_p / F_p -гомоморфизмов F_p в $\mathcal{A}_{\mathcal{K}_p}$. Мы приходим к следующему результату:

Теорема 1. Если $p \nmid \Delta$ и поле K_p не имеет высшего ветвления, то

$$H^1(G_p, \mathfrak{A}_{K_p})_p \cong \text{Hom}_{G_p/F_p}(F_p, \mathfrak{A}_{K_p}).$$

Теперь мы построим поле K , в котором имеется скрещенный гомоморфизм $f \in H^1(G, \mathfrak{A}_K)$ заданного порядка m . Для этого рассмотрим все алгебраические точки P на ω , для которых $mP = 0$. Они образуют группу $\mathfrak{A}_m$, являющуюся суммой двух циклических групп порядка m . Через T_m обозначим поле, получающееся присоединением к R координат $P \in \mathfrak{A}_m$. Это поле нормально. Группу Галуа его обозначим через $\overline{G}$. Очевидно, что для $\sigma \in \overline{G}$, $P \in \mathfrak{A}_m$ и $P^\sigma \in \mathfrak{A}_m$, и σ определяет автоморфизм группы $\mathfrak{A}_m$. Рассмотрим группу G , содержащую нормальный делитель A , изоморфный $\mathfrak{A}_m$, и являющуюся полупрямым произведением $\overline{G}$ и A с автоморфизмами

$$\alpha^\sigma = \varphi^{-1}(\varphi(\alpha)^\sigma), \quad \alpha \in A, \quad (3)$$

где φ — некоторый фиксированный изоморфизм A на $\mathfrak{A}_m$.

Построим поле K , содержащее T_m , нормальное над R и имеющее над ним группу Галуа G . Существование такого поля следует из результатов Шольца [7] и Делоне и Фаддеева [8]. Строя поле K любым из этих методов, можно добиться, чтобы любой простой дивизор $\mathfrak{p}$ поля T_m имел в K показатель ветвления m . Мы выберем $\mathfrak{p}$ взаимно простым с дискриминантом T_m/R , m , Δ и 2.

Определим отображение f группы G в $\mathfrak{A}_K$ так:

$$f(\sigma\alpha) = \varphi(\alpha), \quad \sigma \in \overline{G}, \quad \alpha \in A.$$

Из (3) легко вывести, что f является скрещенным гомоморфизмом, т.е. $f \in H^1(G, \mathfrak{A}_K)$. Очевидно, что $mf = 0$. Мы покажем, что f имеет в $H^1(G, \mathfrak{A}_K)$ порядок, точно равный m . Для этого достаточно доказать, что его образ $\varphi_p f$ при гомоморфизме φ_p , определенном (1), имеет порядок m . В силу теоремы 1 это будет доказано, если мы докажем, что $\varphi_p f$ как операторный гомоморфизм F_p в $\mathfrak{A}_{K_p}$ имеет порядок m . Последнее утверждение следует из того, что по выбору $\mathfrak{p}$ группа F_p — циклическая порядка m , и f отображает ее образующую на элемент P из $\mathfrak{A}_m$, который имеет порядок m , а так как $\mathfrak{p}$ не критично в T_m , то и образ P в $\mathfrak{A}_{K_p}$ имеет тот же порядок.

Мы пришли к окончательному результату:

Теорема 2. В группе эллиптических кривых, имеющих над полем рациональных чисел заданную яковиевскую кривую, существуют элементы любого порядка.

Следствие. Среди эллиптических кривых, имеющих над полем рациональных чисел заданную яковиевую кривую, существуют кривые, показатель которых делится на любое наперед заданное число.

Все доказательства со значительными упрощениями сохраняются и для поля рациональных функций над полем комплексных чисел. Сам факт был в этом случае отмечен без подробных доказательств Энриквесом [9].

Заметим, что для поля p -адических чисел аналогичная теорема не верна. Действительно, теорема 1 показывает, что если дискриминант ω не делится на p , то показатели кривых, имеющих ω своей яковиевой кривой, могут делиться только на p и на простые делители числа точек на ω в поле вычетов по модулю p .

Поступило 20.XII.1956

ЛИТЕРАТУРА

1. H.Hasse, *Zahlentheorie*, Berlin, 1949.
2. A.Weil, Arch. d. Math. 5, No 1-3 (1954), 197.
3. A.Weil, Am. j. Math. 77, No 3 (1955), 493.
4. И.П.Шафаревич, ДАН 114, No 2 (1957).
5. E.Lutz, J. f. reine u. angew. Math. 177, No 4 (1937), 238.
6. F.K.Schmidt, Math. Zs. 33, No 1 (1931), 1.
7. A.Scholtz, Math. Zs. 30 (1929), 332.
8. Б.Н.Делоне, Д.К.Фаддеев, Матем. сборн. 15 (57) (1944), 243.
9. F.Enriques, Math. Ann. 51 (1899), 134.

**ЗАДАЧА ПОГРУЖЕНИЯ ДЛЯ
РАСПАДАЮЩИХСЯ РАСШИРЕНИЙ**
ДОКЛ. АКАД. НАУК СССР Т.120, №6 (1958)

Задача погружения предполагает заданными нормальное расширение k/Ω с группой Галуа F , группу G и эпиморфизм $\phi : G \rightarrow F$. Требуется найти условия, при которых существует нормальное расширение K/Ω с группой Галуа G такое, что $K \supset k$, и эпиморфизм ϕ совпадает с естественным гомоморфизмом группы Галуа поля на группу Галуа подполя.

Группа G называется **распадающимся расширением своего образа F при гомоморфизме ϕ** , если она содержит подгруппу, которая при ϕ изоморфно отображается на F . Таких подгрупп может быть несколько. В дальнейшем мы будем считать выбранной одну из них и будем обозначать ее через F . Если ядро ϕ есть N , то $G = F \cdot N$. Мы будем говорить, что G есть **распадающееся расширение группы F с ядром N** .

Настоящая заметка имеет своей целью сообщение следующего результата*:

Теорема 1. *Задача погружения разрешима для любого поля алгебраических чисел k , если G — распадающееся расширение с нильпотентным ядром.*

Эта теорема содержит в качестве частных случаев ряд результатов, полученных раньше в задаче погружения и в задаче построения полей с заданной группой Галуа.

Если $F = 1$, то теорема 1 доказывает существование расширения с произвольной нильпотентной группой Галуа N , которое было доказано, если порядок N нечетен, Шольцем [1] и Рейхартом [2], а для произвольной группы N — автором [3]. В случае, когда ядро N

* Доказательство дано в работе: В.В. Ишханов, Изв. Акад. Наук СССР, Сер. Матем. 40(1976), 3-25. См. также: В.В. Ишханов, Б.Б. Лурье и Д.К. Фаддеев, Задача погружения в теории Галуа, Москва, "Наука", 1990.

абелево, теорема 1 была доказана Шольцем [4] и более прямым методом — Делоне и Фаддеевым [5]. В случаях, когда группа N есть p -группа класса $c \leq p$ или порядки групп G и N взаимно просты, теорема 1 была доказана автором [6]. Так как всякая разрешимая группа $\mathfrak{G}$ является фактор-группой группы G , получающейся цепочкой распадающихся расширений с нильпотентными ядрами [7], то из теоремы 1 вытекает существование поля алгебраических чисел с произвольной разрешимой группой Галуа. Этот факт был раньше доказан автором [8] на основании решения некоторой более искусственной задачи погружения.

Доказательство теоремы 1 основывается на соображениях, близких к тем, которые использовались в работах автора [3], [6], [8]. Основным отличием является то, что понятие шольцева поля, использовавшееся в этих работах, заменяется теперь понятием относительно-шольцева поля. Очевидно, что можно ограничиться случаем, когда N — группа порядка l^a , где l — простое число. Рассмотрим сначала случай, когда и G является l -группой. Подполе поля K , принадлежащее подгруппе F , обозначим через L .

Поле K будем называть **относительно-шольцевым** (относительно k), если для него выполнены следующие условия:

1. От каждого простого делителя дискриминанта поля k/Ω отщепляется в L простой множитель 1-го порядка в 1-й степени.
2. Простые делители дискриминанта K/k распадаются в K на простые дивизоры 1-го порядка, а в k/Ω не являются критическими и имеют порядок 1.
3. Абсолютные нормы простых делителей дискриминанта K/k удовлетворяют условиям

$$\Re(p) \equiv 1(l^h),$$

где h достаточно велико.

4. Простые делители l полностью распадаются в K/k .

5. Вещественные бесконечно удаленные дивизоры k остаются вещественными в K .

Связь этого понятия с задачей погружения основывается на следующей теореме. Пусть Z — нормальный делитель порядка l в N . Обозначим через $\bar{N}$, $\bar{G}$ и $\bar{K}$ группы N/Z , G/Z и поле, имеющее группу Галуа $\bar{G}$. Гомоморфизм $\phi : G \rightarrow \bar{G}$ отображает F изоморфно. Отождествляя ϕF с F , мы можем написать, что $\bar{G} = \bar{N} \cdot F$. Подполе $\bar{K}$, принадлежащее $\bar{N}$, обозначаем через k .

Теорема 2. Задача погружения, определяемая полем $\bar{K}$ и гомоморфизмом $\phi : \bar{G} \rightarrow G$, разрешима, если поле $\bar{K}$ относительно-шольцево (относительно k).

Пусть теперь порядок G произволен. Обозначим через H силовскую l -подгруппу G . Пусть A — минимальный абелев нормальный делитель G , лежащий в N . Положим $G/A = \overline{G}$, $H/A = \overline{H}$, $N/A = \overline{N}$, и обозначим через ϕ гомоморфизм G на $\overline{G}$. Поле с группой Галуа $\overline{G}$ над полем κ обозначим через $\overline{K}/\kappa$, а его подполя, принадлежащие $\overline{H}$ и $\overline{N}$, — через Ω и k . Применяя редукционную теорему Фаддеева [9] и Кохендёрфера [10], можно получить из теоремы 2 следующий результат.

Теорема 3. *Задача погружения, определяемая полем $\overline{K}/\kappa$ и гомоморфизмом $\phi: G \rightarrow \overline{G}$, разрешима, если поле $\overline{K}/\Omega$ относительно-но-шольцево (относительно k).*

Поле K , являющееся решением задачи погружения, которая сформулирована в теореме 3, не будет, вообще говоря, относительно-но-шольцевым. Условия того, чтобы его можно было выбрать относительно-шольцевым, могут быть найдены аналогично тому, как это делалось в работах [3], [6], [8]. Они заключаются в равенстве единице некоторых инвариантов $\chi_i(\overline{K})$ поля $\overline{K}$, значения которых являются корнями l -й степени из 1.

Предположим, что группа N имеет d образующих $s_1, \dots, s_d$, а группа F — порядок m . Рассмотрим приведенную свободную группу класса $\mathfrak{R}_d^c$ с md образующими $\sigma_{f,i}$, $i = 1, \dots, d$, $f \in F$, фактор-группой которой является N . Определив перестановку f с $\sigma_{f,i}$ правилами

$$f_1^{-1} \sigma_{f,i} f_1 = \sigma_{ff_1,i},$$

мы получим группу $F \cdot \mathfrak{R}_d^c$, которую обозначим через $\mathfrak{G}_d^c$. Отображение

$$f \rightarrow f, \quad \sigma_{f,i} \rightarrow s_i^f$$

определяет гомоморфизм $\mathfrak{G}_d^c$ на G , изоморфно отображающий F на F . Из этого следует, что из разрешимости задачи погружения, определенной полем k и гомоморфизмом $\mathfrak{G}_d^c \rightarrow F$, следует разрешимость исходной задачи погружения.

Предположим, что для любого d доказано существование поля $K_d^{c-1} \supset k$, имеющего группу Галуа $\mathfrak{G}_d^{c-1}$. Для возможности погружения этого поля в поле K_d^c необходимо, чтобы инварианты $\chi^i(K_d^{c-1})$, о которых было сказано выше, равнялись 1. Применяя аппарат, развитый в работах [3], [6], [8], можно получить следующее утверждение.

Теорема 4. Для каждого натурального числа δ существует такое число $d(\delta)$, что в любом поле K_d^{c-1} , содержащем k и относительно-шольцевом, существует подполе $\overline{K}_\delta^{c-1}$, также содержащее k , инварианты которого $\chi_i(\overline{K}_\delta^{c-1})$ равны 1.

Такое поле $\overline{K}_\delta^{c-1}$ можно, следовательно, погрузить в относительно-шольцево (над k) поле K_δ^c . Последовательное применение этого процесса и дает доказательство теоремы 1.

(Поступило 11 февраля 1958 г.)

ЛИТЕРАТУРА

1. A.Scholz, Math.Zs. **161** (1936), 42.
2. H.Reichardt, J.Reine u. Angew. Math. **1** (1937), 177.
3. И.Р.Шафаревич, Изв.АН СССР, сер.матем. **216** (1954), 18.
4. A.Scholz, Math.Zs. **332** (1929), 30.
5. Б.Н.Делоне, Д.К.Фаддеев, Матем.сборн. **243** (1943), 15(57).
6. И.Р.Шафаревич, Изв.АН СССР, сер.матем. **389** (1954), 18.
7. O.Ore, Duke Math.J. **431** (1939), 5.
8. И.Р.Шафаревич, Изв.АН СССР, сер.матем. **525** (1954), 18.
9. Д.К.Фаддеев, ДАН **703** (1953), 92.
10. R.Kochendörffer, Math.Nachr. **75** (1953), 10.

ГРУППА ГЛАВНЫХ ОДНОРОДНЫХ АЛГЕБРАИЧЕСКИХ МНОГООБРАЗИЙ

ДОКЛ. АКАД. НАУК СССР ТОМ 124, no.1 (1959)

В заметке исследуется группа $\mathfrak{H}(\alpha, k)$ главных однородных алгебраических многообразий, на которых действует абелево многообразие α , причем все многообразия рассматриваются над фиксированным полем k . Определение этой группы содержится в работе Вейля [1]. В случае, когда α — эллиптическая кривая, группа $\mathfrak{H}(\alpha, k)$ совпадает с группой эллиптических кривых, имеющих α своей якобиевой кривой.

Введем следующие обозначения: α_K — группа точек на α , рациональных над расширением K/k . $G(K/k)$ — группа Галуа K/k . Предполагается, что K/k — нормальное сепарабельное алгебраическое (может быть, бесконечное) расширение. κ — сепарабельное алгебраическое замыкание k . $\mathfrak{G} = G(\kappa/k)$, $\alpha = \alpha_\kappa$.

Если n — натуральное число, A — абелева группа, то A_n — подгруппа элементов периода n в A , $A^{(n)} = A/nA$. Число n будет дальше предполагаться взаимно простым с характеристикой k (любым, если k без характеристики). k_n — наименьшее расширение k , над которым все точки из α_n рациональны, $\mathfrak{R}$ — соответствующий нормальный делитель $\mathfrak{G}$, $F = \mathfrak{G}/\mathfrak{R} = G(k_n/k)$. K^* — мультипликативная группа поля K .

1. Произвольное поле k . Как известно [2], $\mathfrak{H}(\alpha, k) \cong H^1(\mathfrak{G}, \alpha)$. Из точной последовательности

$$0 \rightarrow \alpha_n \rightarrow \alpha \xrightarrow{\nu} \alpha \rightarrow 0,$$

в которой ν есть гомоморфизм умножения на n , легко получается точная последовательность

$$0 \rightarrow \alpha_k^{(n)} \rightarrow H^1(\mathfrak{G}, \alpha_n) \rightarrow H^1(\mathfrak{G}, \alpha)_n \rightarrow 0.$$

Таким образом, для определения группы $H^1(\mathfrak{G}, \alpha)_n$ достаточно найти группу $H^1(\mathfrak{G}, \alpha_n)$.

Рассмотрим конечные сепарабельные расширения K/k_n , которые нормальны над k и для которых группа $G(K/k)$ имеет следующее строение:

I. $G(K/k_n)$ изоморфна подгруппе группы a_n .

Мы фиксируем некоторый мономорфизм

$$i: G(K/k_n) \rightarrow a_n.$$

II. i является F -операторным гомоморфизмом.

Очевидно, что a_n и $G(K/k_n)$ являются F -операторными группами.

III. Если $\xi \in H^2(F, G(K/k_n))$ — класс когомологий, определяемый согласно теории Шрейера расширением $G(K/k)/G(K/k_n) = F$, то $i\xi = 0$.

Мы фиксируем коцикл $\xi_0 \in \xi$ и коцепь η , для которой

$$\delta\eta = \xi_0.$$

Множество троек (K, i, η) образует абелеву группу относительно естественной групповой операции. Эту группу мы обозначим через $\mathcal{A}_n$.

Теорема 1. Группы $H^1(\mathcal{G}, a_n)$ и $\mathcal{A}_n$ изоморфны.

2. Поле алгебраических чисел k . В этом случае доказано существование бесконечного числа полей K/k_n , удовлетворяющих условиям I — III даже с $\xi = 0$ (см. [3, 4]). Так как $\alpha_k^{(n)}$ по теореме Морделла–Вейля конечна, то отсюда легко следует:

Теорема 2. Группа $H^1(\mathcal{G}, a)_n$ содержит бесконечно много элементов порядка p .

Этот результат был получен мною раньше [5] из более частных соображений.

Обозначим через $\mathfrak{h}(\alpha, k)_n$ подгруппу группы $\mathfrak{H}(\alpha, k)_n$, состоящую из однородных пространств, содержащих рациональную точку в любом p -адическом замыкании k_p поля k .

Простым следствием из теоремы 1 является:

Теорема 3. Группа $\mathfrak{h}(\alpha, k)_n$ конечна.

Тот факт, что группа $\mathfrak{h}(\alpha, k)_n$ может быть нетривиальной, впервые обнаружил Зелмер [6] для $n = 3$ в случае, когда α — эллиптическая кривая. Для случая эллиптических кривых теорема 3 имеет следующий смысл.

Объединим в один класс все эллиптические кривые заданной степени над k , бирационально эквивалентные над k , а в один род —

все кривые, бирационально эквивалентные над любым k_p . Тогда любой род состоит из конечного числа классов.

Как мне сообщили Ленг и Тэйт, они независимо доказали теорему 2.

3. Поле p -адических чисел k . Мы ограничимся случаем, когда α — эллиптическая кривая. Как показал Д.К.Фаддеев [7], над произвольным полем существует скалярное произведение $\alpha_k \otimes H^1(G, \alpha_K) \rightarrow B_k$, где $G = G(K/k)$ и B_k — группа Брауера поля k . Над полем p -адических чисел группа Брауера изоморфна группе W всех корней из 1, и мы получаем скалярное произведение

$$\varphi : \quad \alpha_k \otimes \mathfrak{H}(\alpha, k) \rightarrow W.$$

Теорема 4. Скалярное произведение φ невырождено, так что группы α_k и $\mathfrak{H}(\alpha, k)$ являются группами характеров друг для друга.

Как сообщил мне Тэйт [8], он независимо доказал теорему 4 и получил ее обобщение на случай, когда α — произвольное абелево многообразие.

Поступило 13.IX.1958

ЛИТЕРАТУРА

1. A.Weil, Am. J. Math. **77** No 3 (1955).
2. И.Р.Шафаревич, ДАН **114** No 2 (1957).
3. A.Scholtz, Math. Zs. **30** (1929), 332.
4. Б.Н.Делоне, Д.К.Фаддеев, Матем. сборн. **15** (57) (1944), 243.
5. И.Р.Шафаревич, ДАН **114** No 4 (1957).
6. E.Selmer, Acta Math. **85** No 3-4 (1951).
7. Д.К.Фаддеев, Вестн. ЛГУ No 7 (1957), 45.
8. J.Tate, Séminaire Bourbaki Décembre (1957).

**ЗАДАЧА ПОГРУЖЕНИЯ
ДЛЯ ЛОКАЛЬНЫХ ПОЛЕЙ
(С С. П. ДЕМУШКИНЫМ)**

ИЗВ. АКАД. НАУК СССР, СЕР.

МАТЕМ., Т. 23 (1959), 823-840

В работе исследуется задача погружения конечного расширения в большее расширение с заданной абсолютной группой Галуа. Доказывается, что в случае локальных полей условие согласности Д. К. Фаддеева необходимо и достаточно для разрешимости задачи погружения.

Введение

В работе исследуются условия, при которых заданное нормальное конечное расширение k/Ω с группой Галуа F может быть погружено в большее расширение K/Ω с группой Галуа G , заданное эпиморфное отображение которой $\varphi : G \rightarrow F$ должно реализоваться в качестве гомоморфизма группы Галуа поля на группу Галуа подполя. Мы рассматриваем только тот случай, когда ядро A эпиморфизма φ абелево и, следовательно, K/k должно иметь абелеву группу Галуа A .

Вопрос заключается в разыскании инвариантов поля k , группы G и эпиморфизма φ , от которых зависит разрешимость задачи погружения. Мы называем такие инварианты препятствиями. Ряд условий, необходимых для разрешимости задачи погружения, был найден Д. К. Фаддеевым [3] и переоткрыт Н. Hasse [4]. Мы называем эти условия первым препятствием. Определение первого препятствия приведено в §1. Оно состоит из набора элементов групп $H^2(F_x, k^*)$, где $x \in \text{Hom}(A, k^*)$, а F_x — стационарная подгруппа x (если рассматривать $\text{Hom}(A, k^*)$ как F -операторную группу). Если первое препятствие исчезает, то поле k/Ω называется согласным с рассматриваемой задачей погружения. В общем случае согласности не достаточно для разрешимости задачи погружения.

Дальше мы пользуемся редукционной теоремой Kochendörffer'a [5], согласно которой исследование задачи погружения сводится к случаю, когда G есть p -группа. Мы можем поэтому предполагать, что A содержит нормальный делитель A_1 группы G такой, что $(A : A_1) = p$. Тогда A/A_1 лежит в центре G/A_1 . Если поле k/Ω согласно с исходной задачей погружения, то задача погружения того же поля в поле с группой Галуа G/A_1 , как легко видеть, разрешима. Ее решение есть поле $k(\sqrt[p]{\mu})$, где число μ определяется однозначно с точностью до замены $\mu \rightarrow \mu t$, $t \in \Omega$. Мы выясняем, когда это поле $k(\sqrt[p]{\mu})$ может быть выбрано так, чтобы оно было согласно с задачей погружения его в поле с группой G .

Основной результат заключается в том, что в этом случае первое препятствие состоит из набора циклических алгебр $(a_{x_1}, b_{x_1})_{k_{x_1}}$ индекса p , где $x_1 \in \text{Hom}(A_1, k^*)$. Здесь k_{x_1} – подполе, принадлежащее стационарной подгруппе F_{x_1} гомоморфизма x_1 , $a_{x_1} \in k_{x_1}$, определяется тем, что $k_{x_1}(\sqrt[p]{a_{x_1}}) = k_x$, k_x – подполе, принадлежащее стационарной подгруппе F_x гомоморфизма x , который продолжает x_1 с A_1 на A , а b_{x_1} – элемент k_{x_1} , определенный заданием μ . При замене μ на μt все b_{x_1} умножаются на t . Эти результаты получаются как следствие выводимых нами более общих свойств первого препятствия.

Полученные сведения мы применяем к случаю локальных полей (конечных расширений поля p -адических чисел). Используя основные свойства групп когомологий локальных полей, мы приходим к основному результату этой работы: для локальных полей тривиальность первого препятствия (т. е. выполнение условий Д. К. Фаддеева – Н. Hasse) не только необходима, но и достаточна для разрешимости задачи погружения. Отсюда следует, что для случая поля алгебраических чисел k/Ω условие Д. К. Фаддеева – Н. Hasse разрешимости задачи погружения эквивалентно разрешимости всех соответствующих p -адических задач погружения для полей k_p/Ω_p и для всех простых дивизоров p .

§1. Первое препятствие в задаче погружения

Задача, которой мы будем заниматься, формулируется следующим образом. Задана конечная группа G , ее эпиморфное отображение $\varphi : G \rightarrow F$ и нормальное сепарабельное расширение k_0/Ω с группой Галуа F . Требуется найти условия, которым должны удовлетворять k_0 , G и φ для того, чтобы существовало поле $K \supset k_0$, нормальное над Ω , группа Галуа которого была бы изоморфна группе G , а гомоморфизм φ совпадал бы при этом с естественным гомоморфизмом группы Галуа поля K на группу Галуа подполя k_0 .

Эта задача называется задачей погружения. Мы будем называть ее задачей погружения

$$(k_0/\Omega, G, \varphi).$$

Задача погружения интересна именно в той постановке, какую мы дали, но естественная формулировка результатов получается, если в качестве решений K задачи погружения допускать и регулярные алгебры. Регулярной (см. [4]) называется полупростая коммутативная алгебра K , в которой задана группа автоморфизмов G , причем соответствующее представление G в векторном пространстве K/Ω эквивалентно регулярному. С другой стороны, при индукции нам придется ставить задачи погружения над решениями некоторых других задач погружения, в качестве решения которых могут получиться регулярные алгебры. Поэтому с самого начала мы будем считать, что задача погружения ставится над некоторой регулярной алгеброй k . Здесь важно отметить, что все регулярные алгебры, которые встретятся в наших рассуждениях, всегда будут расширениями нормального над Ω поля k_0 , над которым ставится наша первоначальная задача; они будут содержать поле k_0 в качестве подалгебры. Поле k_0 мы будем называть ядром регулярных алгебр. Таким образом, мы будем рассматривать задачу погружения $(k/\Omega, G, \varphi)$, где k – регулярная алгебра, содержащая нормальное над Ω поле k_0 , а в качестве решений допускаются регулярные алгебры K .

Обозначим через A ядро гомоморфизма φ . Мы имеем тогда точную последовательность

$$1 \rightarrow A \xrightarrow{i} G \xrightarrow{\varphi} F \rightarrow 1. \quad (1)$$

Будем называть задачу погружения $(k/\Omega, G, \varphi)$ задачей погружения, связанной с последовательностью (1).

Дальше мы будем заниматься задачей погружения исключительно в предположении, что выполнены следующие условия:

- 1) группа A абелева;
- 2) характеристика алгебры k взаимно проста с порядком группы A ;
- 3) поле Ω содержит бесконечное число элементов;
- 4) ядро k_0 алгебры k содержит все корни степени m из единицы, где m есть период A (общее наименьшее кратное порядков всех элементов). Кроме того, мы предполагаем, что ядро k_0 в алгебре k принадлежит подгруппе $\mathfrak{A}_0$, для которой $\varphi^{-1}(\mathfrak{A}_0)$ абелева. Это условие оправдывается тем, что мы рассматриваем задачу погружения с абелевой группой A , а все встречающиеся далее регулярные алгебры получаются расширением поля k_0 .

Р. Брауер [1] решил задачу погружения в одном случае, который будет играть далее основную роль. Для формулировки результата Брауер'а заметим, что вложение i группы A в G вследствие абелевости A определяет в A структуру F -операторной группы. Мы будем дальше считать, что в A определена эта F -операторная структура. Кроме того, точная последовательность (1) определяет, согласно теории Schreier'а, класс когомологий $a \in H^2(F, A)$, который мы будем называть фундаментальным классом этой точной последовательности.

Определение 1. F -операторная группа A называется k -элементарной, если имеется F -операторный мономорфизм

$$x: A \rightarrow k_0^*$$

этой группы в мультипликативную группу ядра k_0 алгебры k .

Очевидно, что k -элементарная группа всегда циклическая. Если корни степени m из единицы лежат в Ω , то условие k -элементарности совпадает с требованием, чтобы A была тривиальной операторной группой.

Мы будем называть задачу погружения $(k/\Omega, G, \varphi)$ элементарной, если в точной последовательности (1) группа A является k -элементарной F -операторной группой.

ТЕОРЕМА BRAUER'А. Элементарная задача погружения $(k/\Omega, G, \varphi)$ разрешима тогда и только тогда, когда класс когомологий $x^*(a)$, в который гомоморфизм $x^*: H^2(F, A) \rightarrow H^2(F, k^*)$, индуцированный гомоморфизмом x , переводит фундаментальный класс a точной последовательности (1), распадается в k^* .

Иными словами, фундаментальный класс a должен лежать в ядре гомоморфизма

$$x^*: H^2(F, A) \rightarrow H^2(F, k^*),$$

определенного гомоморфизмом x .

Во множестве всех задач погружения введем частичную упорядоченность. Для этого рассмотрим две следующие операции над задачами погружения.

I. Расширение основного поля. Если $(k/\Omega, G, \varphi)$ — некоторая задача погружения и k' — произвольное подполе алгебры k , то, положив $G' = \varphi^{-1}(F')$, где F' — группа Галуа k/k' , и взяв за φ' ограничение φ на G' , мы получим задачу погружения $(k/k', G', \varphi')$.

II. Замена группы G ее фактор-группой по нормальному делителю, содержащемуся внутри A . Пусть $A' \subset A$ – нормальный делитель группы G . Положим

$$G' = G/A', \quad \varphi' = \varphi\psi'^{-1},$$

где $\psi' : G \rightarrow G'$ – естественное отображение на фактор-группу. Очевидно, что вместе с задачей $(k/\Omega, G, \varphi)$ задача $(k/\Omega, G', \varphi')$ также является задачей погружения.

Определение 2. Задача погружения $(k/k', G', \varphi')$ называется сопутствующей задаче погружения $(k/\Omega, G, \varphi)$, если она может быть получена из последней последовательным применением некоторого числа операций I и II.

Легко проверить, что отношение “сопутствования” действительно определяет частичную упорядоченность во множестве задач погружения.

Из разрешимости данной задачи погружения $(k/\Omega, G, \varphi)$ следует разрешимость всех ее сопутствующих задач погружения. Это достаточно проверить для задач погружения, получающихся применением операций I или II. Если K/Ω – решение задачи погружения $(k/\Omega, G, \varphi)$, то K/k' – будет решением задачи $(k/k', G', \varphi')$, полученной из предыдущей при помощи операции I, и если алгебра $\bar{K} \subset K$ принадлежит нормальному делителю A' , то $\bar{K}/\Omega$ будет решением задачи $(k/\Omega, G', \varphi')$, полученной из первоначальной применением операции II.

Ввиду этого, всякое условие, необходимое для разрешимости некоторой задачи погружения, сопутствующей данной задаче $(k/\Omega, G, \varphi)$, будет необходимым условием для разрешимости задачи $(k/\Omega, G, \varphi)$.

Мы выпишем сейчас необходимые и достаточные условия (известные ввиду теоремы Brauer'a) для разрешимости элементарных задач погружения, сопутствующих задаче $(k/\Omega, G, \varphi)$, и получим, таким образом, некоторые необходимые условия для разрешимости задачи $(k/\Omega, G, \varphi)$.

Пусть $x : A \rightarrow k_0^*$ – произвольный гомоморфизм группы $A = \text{Ker } \varphi$ в мультипликативную группу ядра k_0 алгебры k . Обозначим через F_x подгруппу, состоящую из тех элементов $f \in F$, для которых

$$x(a^f) = x(a)^f, \quad a \in A.$$

Так как $x(a) \in k_0$, то при $f \in \mathfrak{A}_0$ будет

$$x(a)^f = x(a).$$

С другой стороны, мы предположили, что $\varphi^{-1}(\mathfrak{A}_0)$ – абелева группа, поэтому $a^f = a$ для $f \in \mathfrak{A}_0$. Отсюда вытекает, что $F_x \supset \mathfrak{A}_0$ и, следовательно, принадлежащая F_x подалгебра k_x содержится в ядре k_0 , т. е. является полем.

Положим

$$A_x = \text{Ker}(x), \quad \overline{G}_x = \varphi^{-1}(F_x), \quad G_x = \overline{G}_x/A_x$$

и обозначим через φ_x естественный гомоморфизм G_x на F_x . Очевидно, что задача погружения $(k/k_x, G_x, \varphi_x)$ сопутствует задаче $(k/\Omega, G, \varphi)$. При этом ядро гомоморфизма φ_x – группа A/A_x – является элементарной F_x -операторной группой. Действительно,

$$x: \quad A/A_x \rightarrow k_0^*$$

является F_x -мономорфизмом. Поэтому задача погружения $(k/k_x, G_x, \varphi_x)$ элементарна.

Легко показать, что любая элементарная задача погружения, сопутствующая задаче $(k/\Omega, G, \varphi)$, сопутствует обязательно и одной из задач вида $(k/k_x, G_x, \varphi_x)$. Поэтому условия разрешимости для задач $(k/k_x, G_x, \varphi_x)$ будут одновременно условиями разрешимости для всех элементарных задач, сопутствующих задаче $(k/\Omega, G, \varphi)$. Условия же разрешимости задач $(k/k_x, G_x, \varphi_x)$ следуют из теоремы Брауэра. Они заключаются в том, что классы когомологий

$$\rho a \in H^2(F_x, A)$$

гомоморфизмом

$$x^*: \quad H^2(F_x, A) \rightarrow H^2(F_x, k^*)$$

должны переводиться в единицу. Здесь через ρ обозначен оператор ограничения классов когомологий с F на F_x , а через a – фундаментальный класс точной последовательности (1). Классы $x^*\rho a$ будем обозначать через C_x .

Определение 3. Классы когомологий

$$C_x = x^*\rho a \in H^2(F_x, k^*), \quad x \in \text{Hom}(A, k_0^*),$$

называются первым препятствием для задачи погружения $(k/\Omega, G, \varphi)$. Если первое препятствие исчезает, то говорят, что поле k/Ω согласно с задачей погружения $(k/\Omega, G, \varphi)$.

§2. Второе препятствие

В этом параграфе мы будем рассматривать случай, когда группа G есть p -группа. Как показывают результаты Kochendörffer'a [5], задачу погружения достаточно решить в этом случае. Если G — p -группа, то в A будет содержаться подгруппа A_1 , являющаяся нормальным делителем в G и имеющая в A индекс p . Положим $G/A_1 = F^1$ и пусть ψ будет естественным гомоморфизмом F^1 на F . Очевидно, что задача погружения $(k/\Omega, F^1, \psi)$ сопутствует исходной задаче погружения $(k/\Omega, G, \varphi)$.

По предположению, корни степени p из единицы содержатся в ядре k_0 алгебры k , а так как $(k : \Omega)$ есть степень p , то они содержатся в Ω . Группа A/A_1 есть нормальный делитель порядка p в p -группе F^1 и, следовательно, лежит в ее центре. Отсюда следует, что задача $(k/\Omega, F^1, \psi)$ — элементарная. Если мы предположим, что алгебра k/Ω согласна с задачей погружения $(k/\Omega, G, \varphi)$, то задача погружения $(k/\Omega, F^1, \psi)$ будет разрешима. Обозначим через k^1 одно из решений последней задачи. Предположим сначала, что исходная задача погружения разрешима и K — ее решение. Подалгебра k^1 алгебры K , принадлежащая A_1 , с одной стороны, является решением задачи $(k/\Omega, F^1, \psi)$; с другой стороны, погружение k^1 в K есть решение некоторой новой задачи погружения, а именно той, которая связана с точной последовательностью

$$1 \rightarrow A_1 \rightarrow G \xrightarrow{\varphi_1} F^1 \rightarrow 1. \quad (2)$$

В частности, решение k^1 будет согласно с этой новой задачей погружения.

Ввиду этого мы исследуем в настоящем параграфе вопрос: когда решение задачи погружения $(k/\Omega, F^1, \psi)$ — поле k^1 — можно выбрать так, чтобы оно было согласно с задачей погружения, связанной с точной последовательностью (2)? Получающиеся условия необходимы для разрешимости исходной задачи погружения $(k/\Omega, G, \varphi)$. Мы будем называть их вторым препятствием. Мы не вычисляем в общем виде второго препятствия, но выводим некоторые его свойства, которые дадут нам возможность доказать, что для локального поля Ω оно исчезает.

Дальше мы исследуем такую, несколько более общую, ситуацию. Дана задача погружения $(k/\Omega, G, \varphi)$, соответствующая точной последовательности (1), и в группе A — подгруппа A_1 индекса p , являющаяся нормальным делителем G и такая, что задача $(k/\Omega, F^1, \psi)$, соответствующая точной последовательности

$$1 \rightarrow A/A_1 \rightarrow F^1 \rightarrow F \rightarrow 1,$$

элементарна, центральна и разрешима. Пусть k^1 – одно из ее решений. Исследуем связь между первым препятствием для задачи погружения $(k/\Omega, G, \varphi)$ и первым препятствием для задачи погружения $(k^1/\Omega, G, \varphi_1)$, соответствующей точной последовательности (2).

Пусть $x_1 \in \text{Hom}(A_1, k_0^*)$ и x – продолжение x_1 на A . Обозначим через G_x и G_{x_1} централизаторы x и x_1 в G . Очевидно, что

$$G \supset G_{x_1} \supset G_x \supset A \supset A_1.$$

Соответствующая цепочка алгебр будет:

$$\Omega \subset k_{x_1}^1 \subset k_x \subset k \subset k^1.$$

В силу сделанного ранее замечания, $k_{x_1}^1$ и k_x будут полями.

Положим

$$\begin{aligned} G_x/A &= F_x, & G_{x_1}/A &= F_{x_1}, \\ G_x/A_1 &= F^1, & G_{x_1}/A_1 &= F_{x_1}^1. \end{aligned}$$

Первое препятствие для задачи погружения $(k/\Omega, G, \varphi)$ имеет вид

$$C_x = x^* \rho a,$$

а для задачи $(k^1/\Omega, G, \varphi_1)$ –

$$C_{x_1} = x_1^* \rho_1 a_1,$$

где a и a_1 – фундаментальные классы последовательностей (1) и (2), ρ – гомоморфизм ограничения с F на F_x , ρ_1 – гомоморфизм ограничения с F^1 на $F_{x_1}^1$.

Теорема 1. $C_{x_1} \otimes k_x \sim C_x$.

Доказательство. Как известно,

$$C_{x_1} \otimes k_x \sim (k^1/k_{x_1}, r x_1 \rho_1 a_1),$$

где r – гомоморфизм ограничения с $F_{x_1}^1$ на F_x^1 .

С другой стороны,

$$C_x \sim (k^1/k_x, \lambda x \rho a),$$

где λ – гомоморфизм подъема с F_x на F_x^1 . Следовательно, теорема 1 утверждает, что

$$r x_1^* \rho_1 a_1 = \lambda x^* \rho a.$$

Очевидно, что $rx_1^* = x_1^*r$. Гомоморфизм $r\rho_1$ обозначим через r_1 — это ограничение с F^1 на F_x^1 . Нам надо доказать, что

$$x_1^*r_1a_1 = \lambda x^*\rho a.$$

Коцикл, стоящий слева, принадлежит к $H^2(F_x^1, x_1(A_1))$, а коцикл, стоящий справа, — к $H^2(F_x^1, x(A))$.

Рассматриваются эти коциклы в $H^2(F_x^1, k^{1*})$. Мы докажем, что они совпадают уже в $H^2(F_x^1, x(A))$. Для этого достаточно применить лемму 1, которая будет доказана в следующем параграфе, к случаю, когда в качестве a берется $\rho_{F_x}^F a$. Тогда, очевидно,

$$(\rho_{F_x}^F a)_1 = \rho_{F_x}^{F^1} a_1,$$

и лемма 1 дает:

$$i^* \rho_{F_x^1}^{F^1} a_1 = \lambda_{F_x}^{F^1} \rho_{F_x}^F a.$$

Применяя к последнему равенству x^* , будем иметь:

$$x_1^* \rho_{F_x^1}^{F^1} a_1 = \lambda_{F_x}^{F^1} x^* \rho_{F_x}^F a$$

(x перестановочен с $\lambda_{F_x}^{F^1}$).

Теорема 1 доказана.

Теорема 1 показывает, что при выполнении условия согласности для задачи погружения $(k/\Omega, G, \varphi)$, т. е. при $C_x \sim 1$, первое препятствие после первого шага C_{x_1} будет разлагаться полем k_x , так как

$$C_{x_1} \otimes k_x \sim C_x \sim 1.$$

Это означает, что алгебра C_{x_1} будет циклической алгеброй. Чтобы убедиться в этом, достаточно показать, что $(k_x : k_{x_1}^1) = p$ или 1. Для доказательства последнего утверждения рассмотрим функцию, определенную на F_{x_1} :

$$f(\sigma) = \frac{x(\bar{z}^\sigma)}{x(\bar{z})^\sigma},$$

где z — образующий элемент A/A_1 , $\bar{z}$ — его представитель в A . Функция f не зависит ни от выбора представителя $\bar{z}$ в A , ни от выбора продолжения x_1 на A . Равенство $f(\sigma) = 1$ означает, что $\sigma \in F_x$. Кроме того, прямое вычисление показывает, что

$$f(\sigma\tau) = f(\sigma)^\tau f(\tau),$$

т. е. f является коциклом. Ясно также, что значения f – корни степени p из единицы, так как

$$f(\sigma)^p = \frac{x((\bar{z}^p)^\sigma)}{x(\bar{z}^p)^\sigma} = \frac{x_1((\bar{z}^p)^\sigma)}{x_1(\bar{z}^p)^\sigma} = 1.$$

Поэтому будет выполняться равенство

$$f(\sigma\tau) = f(\sigma)f(\tau).$$

Отсюда, в частности, получается, что F_x – нормальный делитель F_{x_1} , так как

$$f(\tau\sigma_x\tau^{-1}) = f(\tau)f(\sigma_x)f(\tau^{-1}) = f(\sigma_x) = 1$$

при $\sigma_x \in F_x$.

Докажем, что $(F_{x_1} : F_x) = p$ или 1. Достаточно рассмотреть случай $(F_{x_1} : F_x) \neq 1$ и показать, что

$$(F_{x_1} : F_x) = p.$$

Пусть σ – такой элемент F_{x_1} , что $f(\sigma) = \zeta_p$. Тогда $\sigma \notin F_x$, $\sigma^p \in F_x$ и

$$F_{x_1} = \sum_{i=0}^{p-1} F_x \sigma^i,$$

т. е.

$$(F_{x_1} : F_x) = p.$$

Коцикл f постоянен на классах смежности F_{x_1} и F_x , следовательно, он получается поднятием с F_{x_1}/F_x на F_{x_1} некоторого коцикла. Обозначим его снова через f .

Рассмотрим коцикл f в $k_{x_1}^*$. Как одномерный коцикл он распадается, т. е. в k_x существует такое число α_{x_1} , зависящее только от x_1 , что

$$f(\sigma) = \alpha_{x_1}^{\sigma-1}.$$

Если последнее равенство возвести в степень p , то получим:

$$(\alpha_{x_1}^p)^{\sigma-1} = f(\sigma)^p = 1,$$

т. е. $\alpha_{x_1}^p = \alpha_{x_1}^1 \in k_{x_1}^1$. Отсюда получаем, что

$$k_x = k_{x_1}^1 \left(\sqrt[p]{\alpha_{x_1}} \right).$$

Таким образом, если $C_x \sim 1$, то $C_{x_1} \sim (a_{x_1}, b_{x_1})$ и является циклической алгеброй.

Перейдем к формулировке теоремы 2.

Пусть у нас имеются три точные последовательности:

$$1 \rightarrow A \rightarrow G \rightarrow F \rightarrow 1 \quad (\text{с классом } a),$$

$$1 \rightarrow A \rightarrow \overline{G} \rightarrow F \rightarrow 1 \quad (\text{с классом } b),$$

$$1 \rightarrow A \rightarrow \tilde{G} \rightarrow F \rightarrow 1 \quad (\text{с классом } a \cdot b).$$

Пусть A_1 – нормальный делитель группы G , содержащийся внутри A . Тогда A_1 будет нормальным делителем и в $\overline{G}$, и в $\tilde{G}$. Следовательно, можно поставить задачи погружения

$$(k/\Omega, F^1, \psi), \quad (k/\Omega, \overline{F}^1, \overline{\psi}), \quad (k/\Omega, \tilde{F}^1, \tilde{\psi}),$$

где

$$F^1 = G/A_1, \quad \overline{F}^1 = \overline{G}/A_1, \quad \tilde{F}^1 = \tilde{G}/A_1.$$

Предположим, что задачи $(k/\Omega, F^1, \psi)$ и $(k/\Omega, \overline{F}^1, \overline{\psi})$ разрешимы, и пусть k^1 и $\overline{k}^1$ – некоторые их решения. Рассмотрим тогда алгебру $K = k^1 \otimes_k \overline{k}^1$. Группу алгебры K над Ω обозначим через Γ . Это будет прямое произведение групп F^1 и $\overline{F}^1$ с объединенной фактор-группой F . Она будет также расширением прямого произведения $A/A_1 \times \overline{A}/A_1$ с помощью группы F с коциклом $aA_1 \times \overline{bA_1}$. В группе $A/A_1 \times \overline{A}/A_1$ выделим подгруппу $\tilde{A}$, состоящую из элементов $(a, \overline{a}^{-1})$. Пусть алгебра $\tilde{k}^1$ по определению принадлежит в K подгруппе $\tilde{A}$. Алгебра $\tilde{k}^1$ имеет над Ω группу $\Gamma/\tilde{A}$, которая изоморфна группе $\tilde{F}^1$. Следовательно, $\tilde{k}^1$ будет решением задачи погружения $(k/\Omega, \tilde{F}^1, \tilde{\psi})$.

Пусть $x_1 \in \text{Hom}(A_1, k_0^*)$. Рассмотрим соответствующие характеру x_1 первые препятствия для задач погружения

$$(k^1/\Omega, G, \varphi_1), \quad (\overline{k}^1/\Omega, \overline{G}, \overline{\varphi}_1), \quad (\tilde{k}^1/\Omega, \tilde{G}, \tilde{\varphi}_1),$$

где φ_1 , $\overline{\varphi}_1$ и $\tilde{\varphi}_1$ – естественные гомоморфизмы G , $\overline{G}$ и $\tilde{G}$ на F^1 , $\overline{F}^1$ и $\tilde{F}^1$.

Они имеют вид:

$$C_{x_1} = (k^1/k_{x_1}^1, F_{x_1}^1, x_1 \rho a_1),$$

$$\overline{C}_{x_1} = (\overline{k}^1/\overline{k}_{x_1}^1, \overline{F}_{x_1}^1, x_1 \overline{\rho} b_1),$$

$$\tilde{C}_{x_1} = (\tilde{k}^1/\tilde{k}_{x_1}^1, \tilde{F}_{x_1}^1, x_1 \tilde{\rho}(ab)_1),$$

где ρ , $\bar{\rho}$ и $\tilde{\rho}$ – ограничения соответственно с F^1 на $F_{x_1}^1$, с $\bar{F}^1$ на $\bar{F}_{x_1}^1$ и с $\tilde{F}^1$ на $\tilde{F}_{x_1}^1$. Но, как легко видеть, поля $k_{x_1}^1$, $\bar{k}_{x_1}^1$ и $\tilde{k}_{x_1}^1$ совпадают (мы их обозначим через $k_{x_1}^1$). Поэтому алгебры C_{x_1} , $\bar{C}_{x_1}$ и $\tilde{C}_{x_1}$ определены над одним и тем же полем.

Пусть Γ_{x_1} – подгруппа Γ , к которой принадлежат $k_{x_1}^1$ в K .

Теорема 2. $C_{x_1} \otimes \bar{C}_{x_1} \sim \tilde{C}_{x_1}$.

Доказательство. Как известно,

$$\begin{aligned} C_{x_1} &\sim (K/k_{x_1}^1, \Gamma_{x_1}, \lambda x_1 \rho a_1), \\ \bar{C}_{x_1} &\sim (K/k_{x_1}^1, \Gamma_{x_1}, \bar{\lambda} x_1 \bar{\rho} b_1), \\ \tilde{C}_{x_1} &\sim (K/k_{x_1}^1, \Gamma_{x_1}, \tilde{\lambda} x_1 \tilde{\rho}(ab)_1), \end{aligned}$$

где λ – подъем с $F_{x_1}^1$ на Γ_{x_1} , $\bar{\lambda}$ – подъем с $\bar{F}_{x_1}^1$ на Γ_{x_1} , $\tilde{\lambda}$ – подъем с $\tilde{F}_{x_1}^1$ на Γ_{x_1} .

Теорема 2 утверждает, следовательно, что классы, в которых лежат коциклы $\lambda x_1 \rho a_1 \cdot \bar{\lambda} x_1 \bar{\rho} b_1$ и $\tilde{\lambda} x_1 \tilde{\rho}(ab)_1$, совпадают. Но, очевидно, x_1 коммутирует со всеми подъемами λ , $\bar{\lambda}$ и $\tilde{\lambda}$, поэтому достаточно показать, что совпадают классы $\lambda \rho a_1 \cdot \bar{\lambda} \bar{\rho} b_1$ и $\tilde{\lambda} \tilde{\rho}(ab)_1$.

Для того, чтобы еще больше упростить последнее утверждение, рассмотрим коммутативные диаграммы:

$$\begin{array}{ccccc} F^1 & \xleftarrow{\Pi} & \Gamma & \bar{F}^1 & \xleftarrow{\bar{\Pi}} & \Gamma & \tilde{F}^1 & \xleftarrow{\tilde{\Pi}} & \Gamma \\ i \uparrow & & \uparrow I & \bar{i} \uparrow & & \uparrow I & \tilde{i} \uparrow & & \uparrow I \\ F_{x_1}^1 & \xleftarrow{\pi} & \Gamma_{x_1} & \bar{F}_{x_1}^1 & \xleftarrow{\bar{\pi}} & \Gamma_{x_1}^1 & \tilde{F}_{x_1}^1 & \xleftarrow{\tilde{\pi}} & \Gamma_{x_1} \end{array}$$

Здесь гомоморфизмы, обозначенные буквами π и Π , – проекции, а гомоморфизмы, обозначенные буквами i и I , – вложения.

Тогда коммутативными будут и соответствующие диаграммы для групп когомологий (мы их пишем только для размерности 2):

$$\begin{array}{ccc} H^2(F^1, A_1) & \xrightarrow{\Lambda} & H^2(\Gamma, A_1) \\ \rho \downarrow & & \downarrow \mathbf{P} \\ H^2(F_{x_1}^1, A_1) & \xrightarrow{\lambda} & H^2(\Gamma_{x_1}, A_1) \end{array}$$

$$\begin{array}{ccc}
H^2(\bar{F}^1, A_1) & \xrightarrow{\bar{\Lambda}} & H^2(\Gamma, A_1) & H^2(\tilde{F}^1, A_1) & \xrightarrow{\tilde{\Lambda}} & H^2(\Gamma, A_1) \\
\bar{\rho} \downarrow & & \downarrow \mathbf{P} & \bar{\rho} \downarrow & & \downarrow \mathbf{P} \\
H^2(\bar{F}_{x_1}^1, A_1) & \xrightarrow{\bar{\lambda}} & H^2(\Gamma_{x_1}, A_1) & H^2(\tilde{F}_{x_1}^1, A_1) & \xrightarrow{\tilde{\lambda}} & H^2(\Gamma_{x_1}, A_1)
\end{array}$$

Отсюда мы получаем, что

$$\lambda \rho = \mathbf{P} \Lambda,$$

$$\bar{\lambda} \bar{\rho} = \mathbf{P} \bar{\Lambda},$$

$$\tilde{\lambda} \tilde{\rho} = \mathbf{P} \tilde{\Lambda}.$$

Равенство, которое нам нужно доказать, сводится к следующему:

$$\mathbf{P} \Lambda a_1 \cdot \mathbf{P} \bar{\Lambda} b_1 = \mathbf{P} \tilde{\Lambda} (ab)_1,$$

или

$$\Lambda a_1 \cdot \bar{\Lambda} b_1 = \tilde{\Lambda} (ab)_1.$$

Но последнее равенство следует из леммы 2, которая будет доказана в следующем параграфе.

Применим теорему 2 к случаю, когда $b = 1$. Решение k^1 задачи $(k/\Omega, F^1, \psi)$ имеет вид

$$k^1 = k(\sqrt[p]{\mu_0}).$$

Группа $\bar{F}^1$ будет прямым произведением F и A/A_1 , поэтому решением задачи $(k/\Omega, \bar{F}^1, \bar{\psi})$ будет

$$\bar{k}^1 = k(\sqrt[p]{m}), \quad m \in \Omega.$$

По самому построению,

$$\tilde{k}^1 = k(\sqrt[p]{\mu_0 m})$$

и поэтому является решением задачи $(k/\Omega, F^1, \psi)$.

Теорема 2 дает в таком случае для $x_1 \in \text{Hom}(A_1, k_0^*)$:

$$C_{x_1}(\mu_0) \otimes \bar{C}_{x_1}(m) \sim \tilde{C}_{x_1}(\mu_0 m).$$

Так как в рассматриваемом случае $ab = a$ и $\tilde{G} = G$, то

$$\tilde{C}_{x_1}(\mu_0 m) = C_{x_1}(\mu_0 m)$$

и теорема 2 показывает, что при переходе от решения $k(\sqrt[p]{\mu_0})$ задачи $(k/\Omega, F^1, \psi)$ к решению $k(\sqrt[p]{\mu_0 m})$ алгебра $C_{x_1}(\mu_0)$ умножается на некоторую алгебру $\overline{C}_{x_1}(m)$.

Прямое вычисление показывает, что

$$\overline{C}_{x_1}(m) \sim (a_{x_1}, m).$$

Из только что сделанного замечания и из замечания к теореме 1 получаем следующее утверждение.

Теорема 3. Если для задачи погружения $(k/\Omega, G, \varphi)$ выполняется условие согласности, то после первого шага (построения поля $k^1 = k(\sqrt[p]{\mu_0})$) первое препятствие для задачи $(k^1/\Omega, G, \varphi_1)$ будет набором циклических алгебр вида

$$(a_{x_1}, b_{x_1})_{k_{x_1}}, \quad x_1 \in \text{Hom}(A_1, k_0^*),$$

причем при переходе от решения $k^1 = k(\sqrt[p]{\mu_0})$ к решению $k(\sqrt[p]{\mu_0 m})$ все они умножаются на циклические алгебры $(a_{x_1}, m)_{k_{x_1}}$.

Таким образом, второе препятствие заключается в невозможности выбрать такое $m \in \Omega$, что

$$(a_{x_1}, m) \sim (a_{x_1}, b_{x_1})^{-1}$$

для всех $x_1 \in \text{Hom}(A_1, k_0^*)$.

Задача погружения распадается, следовательно, на две задачи:

1) можно ли для данного $x_1 \in \text{Hom}(A_1, k_0^*)$ найти $m_{x_1} \in \Omega$ такое, что $(a_{x_1}, m_{x_1}) \sim (a_{x_1}, b_{x_1})^{-1}$?

2) Если для каждого x_1 можно найти такое $m_{x_1} \in \Omega$, то каковы условия того, что выбор можно сделать согласованно?

Остановимся на некоторых нужных нам свойствах гомоморфизма переноса t , который определяется так (см. [2]): если $f \in \text{Hom}_H(A, B)$ H – подгруппа G , A и B – G -модули и $G = \sum_i H s_i$ – разложение G на смежные классы по H , то

$$(tf)(a) = \sum_i f(a^{s_i^{-1}})^{s_i}.$$

При таком определении tf будет уже G -гомоморфизмом A в B . Если классы когомологий понимать как гомоморфизмы членов резольвенты в соответствующий модуль, то гомоморфизм переноса становится определенным для классов когомологий.

Гомоморфизм переноса обладает свойствами:

1. Инварианты алгебр C_{x_1} и tC_{x_1} совпадают (в локальном случае).
2. $tC_{x_1} = C_{tx_1}$.

Утверждение 1 следует из теории алгебр над локальными полями.

Доказательство утверждения 2. Класс когомологий a_1 есть некоторый F^1 -гомоморфизм второго члена X_2 резольвенты для F^1 в A_1 : $a_1 \in \text{Hom}_{F^1}(X_2, A_1)$; ρa_1 — это тот же самый гомоморфизм, только понимаемый как $F_{x_1}^1$ -гомоморфизм. К последнему коциклу применяем x_1 . Тогда

$$x_1 \rho a_1 \in \text{Hom}_{F_{x_1}^1}(X_2, k_0^*).$$

Пусть ξ — некоторый элемент из X_2 . Тогда

$$(t(x_1 \rho a_1))(\xi) = \prod_i [(x_1 \rho a_1)(\xi^{s_i^{-1}})]^{s_i}.$$

Но $a_1 \in \text{Hom}_{F^1}(X_2, A_1)$, поэтому

$$\begin{aligned} (t(x_1 \rho a_1))(\xi) &= \prod_i [x_1(a_1(\xi)^{s_i^{-1}})]^{s_i} = \prod_i x_1^{s_i}(a_1(\xi)) = \\ &= \left(\prod_i x_1^{s_i}\right)(a_1(\xi)) = (tx_1)(a_1(\xi)), \end{aligned}$$

т. е.

$$tC_{x_1} = C_{tx_1}.$$

§3. Две леммы

В этом параграфе доказываются две групповые леммы, которые мы использовали при доказательстве теорем 1 и 2.

Пусть группа G получается из точной последовательности

$$1 \rightarrow A \rightarrow G \rightarrow F \rightarrow 1$$

с коциклом a и A_1 – нормальный делитель G , лежащий внутри A . Тогда группу G мы можем рассматривать как расширение A_1 . Это приводит к точной последовательности

$$1 \rightarrow A_1 \rightarrow G \rightarrow F^1 \rightarrow 1,$$

фундаментальный коцикл которой мы обозначаем через a_1 .

Пусть у нас имеются три точные последовательности:

$$1 \rightarrow A \rightarrow G \rightarrow F \rightarrow 1 \quad (\text{с фундаментальным коциклом } a), \quad (1)$$

$$1 \rightarrow A \rightarrow \bar{G} \rightarrow F \rightarrow 1 \quad (\text{с фундаментальным коциклом } b), \quad (\bar{I})$$

$$1 \rightarrow A \rightarrow \tilde{G} \rightarrow F \rightarrow 1 \quad (\text{с фундаментальным коциклом } a \cdot b).$$

Если G_1 и G_2 имеют нормальные делители A_1 и A_2 и $\varepsilon : G_1/A_1 \rightarrow G_2/A_2 = E$ – изоморфизм, то элементы $(g_1, g_2) \in G_1 \times G_2$, для которых

$$g_2 A_2 = \varepsilon(g_1 A_1)$$

образуют подгруппу G' , называемую прямым произведением G_1 и G_2 с объединенной фактор-группой E . Мы эту подгруппу обозначаем через $G_1 \times^E G_2$. Эта группа содержит подгруппу, изоморфную $A_1 \times A_2$, и

$$G'/A_1 \times A_2 \cong E.$$

Группы A_1 и A_2 – нормальные делители G' и

$$G'/A_1 \cong G_1, \quad G'/A_2 \cong G_2.$$

Если $\nu : A_1 \rightarrow A_2 = A$ – изоморфизм, то элементы $(a_1, a_2) \in A_1 \times A_2$, для которых $a_2 \nu(a_1) = 1$ образуют нормальный делитель группы G' , который мы обозначим через U . Фактор-группа G'/U обозначается через $G_1 \times_{A'}^E G_2$.

Пусть $\Gamma = F^1 \times^F \bar{F}^1$ и $i : A_1 \rightarrow A$ – вложение для первоначальных нормальных делителей группы G .

Тогда имеют место следующие утверждения.

Лемма 1. $i^* a_1 = \lambda_{F^1}^F a.$

Лемма 2. $\lambda_{F^1}^\Gamma a_1 \cdot \lambda_{\bar{F}^1}^\Gamma b_1 = \lambda_{\bar{F}^1}^\Gamma (ab)_1.$

Здесь λ обозначает гомоморфизм подъема. Мы докажем эти соотношения между двумерными классами когомологий, интерпретируя их как соотношения между соответствующими расширениями групп. Это удобно, так как переход от a к a_1 определяется теоретико-групповым образом. Но для этого нам нужно напомнить теоретико-групповую характеристику умножения классов когомологий и оператора подъема λ (они хорошо известны).

1⁰. **Умножение.** Если a и b – фундаментальные коциклы последовательностей (1) и $(\bar{1})$, то $(a \cdot b)$ – фундаментальный класс последовательности

$$1 \rightarrow A \rightarrow G \times_A {}^F\overline{G} \rightarrow F \rightarrow 1.$$

2⁰. **Подъем.** Если a – фундаментальный класс последовательности (1) и

$$\Phi \rightarrow F \quad (2)$$

– эпиморфизм с ядром N , причем N действует на A тривиально, то $\lambda_F^\Phi a$ – фундаментальный класс последовательности

$$1 \rightarrow A \rightarrow G \times {}^F\Phi \xrightarrow{P} \Phi \rightarrow 1.$$

Обратно, если задан эпиморфизм (2), ядро которого N действует на A тривиально, а в последовательности

$$1 \rightarrow A \rightarrow \mathfrak{G} \xrightarrow{P} \Phi \rightarrow 1$$

$P^{-1}(N) = A \times N'$, где $N' \cong N$ и N' является нормальным делителем $\mathfrak{G}$, то фундаментальный класс $\mathfrak{A}$ этой последовательности представляется в виде

$$\mathfrak{A} = \lambda_F^\Phi a,$$

где a – фундаментальный класс последовательности

$$1 \rightarrow A \rightarrow \mathfrak{G}/N' \rightarrow F \rightarrow 1.$$

Доказательство леммы 1. Класс a_1 является фундаментальным классом последовательности

$$1 \rightarrow A_1 \rightarrow G \rightarrow F^1 \rightarrow 1.$$

При вложении A_1 в A группа G переходит в группу $\mathfrak{G}$, которая получается простым расширением ее нормального делителя A_1 до A . В группе $\mathfrak{G}$ будут, таким образом, содержаться два нормальных делителя, изоморфных A , причем пересечение их есть A_1 . Для того чтобы их различать, мы второй из них, до которого A_1 расширяется формальным образом, обозначим через $\bar{A}$. Так как $A \cap \bar{A} = A_1$, то $\bar{A}_1 = A_1$.

Рассмотрим в $\mathfrak{G}$ подгруппу, образованную элементами вида $a \cdot \bar{a}^{-1}$. Эту подгруппу мы обозначим через D и отображение $a \rightarrow a \cdot \bar{a}^{-1}$ будем записывать в виде:

$$d(a) = a\bar{a}^{-1}.$$

Это будет гомоморфизм с ядром A_1 . Таким образом, $d : A/A_1 \rightarrow D$ есть изоморфизм. Подгруппа D , как легко видеть, будет в $\mathfrak{G}$ нормальным делителем, даже прямым множителем, изоморфным A/A_1 . Подгруппа A не пересекается с D , поэтому в $\mathfrak{G}$ содержится нормальный делитель $A \times D$. При проекции p группы $\mathfrak{G}$ на F^1 этот нормальный делитель переходит в

$$p(A \times D) = p(D) = A/A_1,$$

причем p есть изоморфизм D с A/A_1 . Таким образом,

$$p^{-1}(A/A_1) = A \times D$$

и

$$D \cong A/A_1.$$

Согласно 2^0 , коцикл $i^* a_1$ постоянен на классах смежности $\mathfrak{G}/D$ и получается поднятием на F^1 фундаментального коцикла последовательности

$$1 \rightarrow A \rightarrow \mathfrak{G}/D \rightarrow F \rightarrow 1.$$

Но $\mathfrak{G}/D$ изоморфно G , поэтому окончательно имеем:

$$i^* a_1 = \lambda_F^{F^1} a.$$

Лемма 1 доказана.

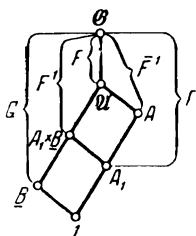


Рис.1

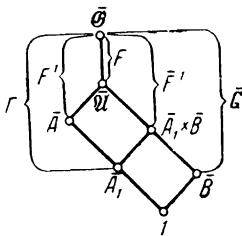


Рис.2

Доказательство леммы 2. Согласно 2^0 , $\lambda_{F^1}^\Gamma a_1$ является фундаментальным классом последовательности

$$1 \rightarrow A_1 \rightarrow \mathfrak{G} \rightarrow \Gamma \rightarrow 1,$$

где $\mathfrak{G} = G \times^{F^1} \Gamma$. Нормальный делитель A/A_1 группы F^1 обозначим через B , аналогично $\overline{A}/\overline{A}_1$ — через $\underline{B}$. Тогда $\Gamma \supset B \times \underline{B}$ и

$$\Gamma/\underline{B} \cong F^1, \quad \Gamma/B \cong \overline{F}^1, \quad \Gamma/B \times \underline{B} \cong F.$$

По определению прямого произведения с объединенной фактор-группой, $\mathfrak{G}$ содержит подгруппу, изоморфную $A_1 \times \underline{B}$.

В группе $\mathfrak{G}$ содержится подгруппа, порожденная элементами (a, aA_1) . Эта подгруппа изоморфна A , и мы обозначим ее снова через A . Обозначим $A \times \underline{B} \subset \mathfrak{G}$ через $\mathfrak{A}$. Тогда

$$\mathfrak{G}/A \times \underline{B} = F.$$

Иначе говоря, мы видим, что

$$\mathfrak{G} = G \times {}^F \overline{F^1}.$$

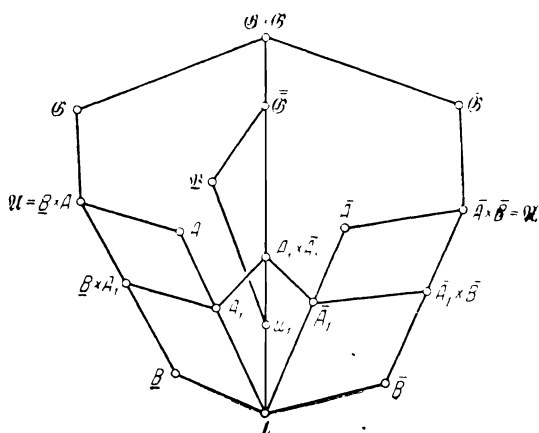


Рис.3

Обозначая аналогичные объекты для b чертой наверху, получим:

$$\overline{\mathfrak{G}} = \overline{G} \times {}^F \overline{F^1}.$$

Для того, чтобы получить $\lambda_{F^1}^\Gamma a_1 \cdot \lambda_{F^1}^\Gamma b_1$, мы должны, согласно 1⁰, рассмотреть прямое произведение $\mathfrak{G} \times \overline{\mathfrak{G}}$.

Положим $\mathfrak{G} \times {}^\Gamma \overline{\mathfrak{G}} = \overline{\overline{\mathfrak{G}}}$. Для того, чтобы получить эту группу, нам надо рассмотреть те элементы $(g, \overline{h}) \in \mathfrak{G} \times \overline{\mathfrak{G}}$, для которых $\varepsilon(gA_1) = \overline{hA}$, где ε – изоморфизм:

$$\varepsilon: \mathfrak{G}/A_1 \rightarrow \overline{\overline{\mathfrak{G}}}/\overline{A_1} = \Gamma.$$

Заметим, что

$$\varepsilon B = \varepsilon A/A_1 = \overline{B}, \quad \varepsilon \underline{B} = \overline{B}.$$

В группе $\underline{B} \times A \times \overline{A} \times \overline{B} \subset \mathfrak{G} \times \overline{\mathfrak{G}}$ рассмотрим подгруппу, состоящую из элементов вида

$$\underline{a^{-1}A_1} \times a \times \bar{a}^{-1} \times aA_1.$$

Эту подгруппу обозначим через $\mathfrak{B}$. Очевидно, что $\mathfrak{B} \subset \overline{\mathfrak{G}}$, так как

$$\varepsilon(\underline{a^{-1}A_1} \times aA_1) = \overline{a^{-1}A_1} \times \overline{aA_1}.$$

В заключение обозначим через U_1 подгруппу элементов вида

$$(a_1, \bar{a}_1^{-1}) \in A_1 \times \overline{A_1} \subset \overline{\mathfrak{G}}.$$

По определению,

$$\overline{\mathfrak{G}}/U_1 = \mathfrak{G} \times_{A_1} \overline{\mathfrak{G}}.$$

Ясно, что $U_1 \subset \mathfrak{B}$ и $\mathfrak{B}/U_1 \cong A/A_1$. Подгруппу $\mathfrak{B}/U_1$ группы $\overline{\mathfrak{G}}/U_1$ обозначим через $\tilde{B}$.

Рассмотрим гомоморфизм

$$\pi: \overline{\mathfrak{G}} \rightarrow \overline{\mathfrak{G}}/U_1.$$

Непосредственная проверка показывает, что гомоморфизм π действует на A изоморфно и что $\tilde{B}$ является нормальным делителем $\pi\overline{\mathfrak{G}}$.

Так как $\lambda_{F^1}^\Gamma a_1 \cdot \lambda_{\overline{F^1}}^\Gamma b_1$ является фундаментальным классом последовательности

$$1 \rightarrow A_1 \rightarrow \pi\overline{\mathfrak{G}} \rightarrow \Gamma \rightarrow 1,$$

то из сказанного выше следует, что коцикл $\lambda_{F^1}^\Gamma a_1 \cdot \lambda_{\overline{F^1}}^\Gamma b_1$ постоянен на классах смежности $\Gamma/\tilde{B}$ (здесь $\tilde{B}$ отождествляется со своим образом в $\pi\overline{\mathfrak{G}}/\pi A_1 \cong \Gamma$). В группе Γ подгруппа $\tilde{B}$ состоит из элементов $b_1 \times b_2 \in B \times \overline{B}$, для которых $b_1 b_2 = 1$. Таким образом, $\Gamma/\tilde{B} \cong \overline{F^1}$ и мы видим, что

$$\lambda_{F^1}^\Gamma a_1 \cdot \lambda_{\overline{F^1}}^\Gamma b_1 = \lambda_{\overline{F^1}}^\Gamma c,$$

где c — некоторый класс из $H^2(\tilde{F}^1, A_1)$. Чтобы найти этот класс, нам надо, согласно 2^0 , рассмотреть $\pi\overline{\mathfrak{G}}/\tilde{B} = \hat{G}$. Класс c будет фундаментальным классом последовательности

$$1 \rightarrow A_1 \rightarrow \hat{G} \rightarrow \tilde{F}^1 \rightarrow 1.$$

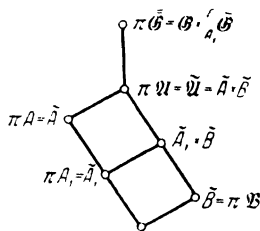


Рис.4

Так как $\tilde{B} = \pi\mathfrak{B}$, то $\hat{G} = \pi\overline{\mathfrak{G}}/\pi\mathfrak{B} \cong \overline{\mathfrak{G}}/\mathfrak{B}$, и нам достаточно доказать, что

$$\hat{G} \cong \overline{\mathfrak{G}}/\mathfrak{B} \cong \tilde{G}.$$

Для этого заметим, что

$$\mathfrak{G}/\underline{B} \cong G, \quad \overline{\mathfrak{G}}/\overline{B} \cong \overline{G}$$

и, следовательно, существует изоморфизм

$$\eta: \mathfrak{G} \times \overline{\mathfrak{G}}/\underline{B} \times \overline{B} \rightarrow G \times \overline{G}.$$

Непосредственная проверка показывает, что

$$\overline{\mathfrak{G}} \cong G \times {}^F\overline{G}, \quad \eta \cong U, \quad \eta\mathfrak{B} \cong U,$$

где $U \subset A \times \overline{A} \subset G \times \overline{G}$ есть подгруппа, состоящая из элементов вида $(a, \bar{a}^{-1})$. Таким образом,

$$\hat{G} \cong \overline{\mathfrak{G}}/\mathfrak{B} \cong \eta\overline{\mathfrak{G}}/\eta\mathfrak{B} \cong G \times {}^F\overline{G}/U = G \times_A {}^F\overline{G} = \tilde{G},$$

что и требовалось доказать.

§4. Задача погружения над локальным полем

Предположим теперь, что поле Ω локальное. В этом случае имеет место

Теорема 4. При выполнении условия согласности задача погружения $(k/\Omega, G, \varphi)$ будет разрешима.

Доказательство. Как уже отмечалось, теорему достаточно доказать для случая, когда G есть p -группа. Тогда внутри A будет содержаться нормальный делитель A_1 группы G и $(A : A_1) = p$. Задача погружения, соответствующая точной последовательности

$$1 \rightarrow A/A_1 \rightarrow F^1 \rightarrow F \rightarrow 1,$$

будет сопутствующей к исходной задаче и, следовательно, должна быть разрешима.

Пусть одним из ее решений будет $k^1 = k(\sqrt[p]{\mu_0})$, где $\mu_0 \in k$. Элемент μ_0 определяется с точностью до множителя m из основного поля Ω . Задача заключается в таком выборе множителя m , чтобы алгебра $k(\sqrt[p]{\mu_0 m})$, тоже являющаяся решением задачи погружения $(k/\Omega, F^1, \psi)$, была согласна с группой G . Покажем, что выбор такого множителя m возможен. Для этого заметим, что так как tC_{x_1} имеет такой же инвариант, что и C_{x_1} , то достаточно рассматривать только алгебры tC_{x_1} . Но $tC_{x_1} = C_{tx_1}$, и характер tx_1 инвариантен относительно всей группы F^1 . Поэтому достаточно рассматривать только препятствия для характеров $x_1 \in \text{Hom}_{F^1}(A_1, k_0^*)$.

Обозначим через x продолжение характера x_1 на всю группу A .

В силу теоремы 3, алгебра $C_{x_1}(\mu_0)$ имеет вид (a_{x_1}, b_{x_1}) и при переходе от решения $k(\sqrt[p]{\mu_0})$ задачи $(k/\Omega, F^1, \psi)$ к решению $k(\sqrt[p]{\mu_0 m})$ умножается на (a_{x_1}, m) .

Пусть $x_1, x_2, \dots, x_n$ — все F^1 -инвариантные характеры группы A_1 . Множитель m нам нужно выбрать так, чтобы алгебра (a_{x_i}, m) принимала наперед заданное значение $C_{x_i}^{-1}(\mu_0)$. Выражение (a_{x_i}, m) является характером при фиксированном m , и система уравнений

$$(a_{x_i}, m) = C_{x_i}^{-1}(\mu_0)$$

будет разрешима, если из любого соотношения

$$\prod_i (a_{x_i}, m)^{\beta_i} = 1$$

(при всех m) следует, что

$$\prod_i (C_{x_i}^{-1}(\mu_0))^{\beta_i} = 1.$$

Покажем, что это действительно так. Равенство

$$\prod_i (a_{x_i}, m)^{\beta_i} = 1$$

означает, что $\prod_i a_i^{\beta_i}$ — p -я степень в Ω , т. е.

$$\prod_i a_{x_i}^{\beta_i} \in \Omega.$$

Это в свою очередь означает, что

$$\prod_i f_i^{\beta_i} = 1,$$

где f_i — коцикл, построенный по формуле

$$f_i(\sigma) = \frac{x'_i(\bar{z}^\sigma)}{x'_i(z)^\sigma}$$

(x'_i — продолжение x_i на A). Отсюда следует, что

$$(C_{\prod_i x_i^{\beta_i}}(\mu_0))^{-1} \sim 1.$$

Остается заметить, что для F^1 -инвариантных характеров x_1 и x_2

$$C_{x_1 x_2}(\mu_0) \sim C_{x_1}(\mu_0) \otimes C_{x_2}(\mu_0).$$

Из $C_{\prod_i x_i^{\beta_i}}(\mu_0)^{-1} \sim 1$ получаем:

$$\prod_i (C_{x_i}^{-1}(\mu_0))^{\beta_i} \sim 1.$$

Доказательство теоремы закончено.

Замечание 1. Условие согласности для задачи погружения $(k/\Omega, G, \varphi)$ заключается в том, что все алгебры $C_x = x\rho a$, где ρ — ограничение с F на F_x , распадаются. Но, как мы видели, tC_x и C_x имеют один и тот же инвариант в локальном случае, $tC_x = C_{tx}$

и tx уже инвариантно относительно всей группы F . Поэтому в локальном случае условие согласности достаточно проверять только для характеров $x \in \text{Hom}_F(A, k_0^*)$.

Остановимся на вопросе о том, когда решение задачи погружения $(k/\Omega, G, \varphi)$ (k – локальное поле) будет полем. В случае, когда G – p -группа, этот вопрос решает

Предложение. Если число образующих группы G равно числу образующих группы F , то любое решение задачи погружения $(k/\Omega, G, \varphi)$ будет полем.

Для доказательства утверждения предложения нужно решать задачу погружения последовательными центральными шагами степени p (сделать это можно, так как G – p -группа). Тогда в случае равенства числа образующих G и F при каждом шаге число образующих не будет увеличиваться. Достаточно, следовательно, проверить утверждение только для случая, когда $(G : F) = p$. Решение такой задачи $K = k(\sqrt[p]{\mu})$ будет полем тогда и только тогда, когда $\mu \neq \mu'^p$, $\mu' \in k$.

Если $\mu = \mu'^p$ в k , то G будет прямым произведением F и A (это легко проверяется). Отсюда получается доказательство предложения.

ЛИТЕРАТУРА

1. Brauer R., *Über die Konstruktion der Schiefkörper, die von endlichem Rang in Bezug auf ein gegebenes Zentrum sind*, J. f. die reine und angew. Mathem. **168** H.1 (1932), 44–64.
2. Cartan H. und Eilenderg S., *Homological algebra*, Princeton Univ. Press, 1956.
3. Делоне Б. Н., Фаддеев Д. К., *Исследования по геометрии теории Галуа*, Матем. сборн. **15** (57) :2 (1944), 243–276.
4. Hasse H., *Existenz und Mannigfaltigkeit Abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers*, Mathem. Nachrichten **B. 1**, H. 1 (1948), 40–61.
5. Kochendörffer R., *Zwei Reduktionssätze zum Einbettungsproblem für Abelsche Algebren*, Mathem. Nachrichten **B. 10**, H. 1-2 (1953), 75–84.

Поступило 18.VI.1959

**ВТОРОЕ ПРЕПЯТСТВИЕ ДЛЯ ЗАДАЧИ
ПОГРУЖЕНИЯ ПОЛЕЙ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ
(С С. П. ДЕМУШКИНЫМ)**

ИЗВ. АКАД. НАУК СССР СЕР. МАТЕМ., 26 (1962), 911-924

В работе исследуется задача погружения полей алгебраических чисел в поля с большей группой Галуа. Вычисляется второе препятствие к разрешимости задачи погружения.

Рассматривается задача погружения нормального над Ω поля k с группой F в большее поле K с группой G над Ω , причем поле K должно быть таким, чтобы естественный гомоморфизм

$$G = \mathfrak{G}(K/\Omega) \rightarrow \mathfrak{G}(k/\Omega) = F$$

группы Галуа поля на группу Галуа подполя совпадал с предписанным гомоморфизмом $\varphi : G \rightarrow F$. Такую задачу погружения будем записывать в виде $(k/\Omega, G, \varphi)$. Как и в работе [1], будем считать, что ядро A гомоморфизма $\varphi : G \rightarrow F$ есть абелева группа, и что корни степени m (период группы A) из единицы содержатся в k . Кроме того, так как задача погружения редуцируется к задаче погружения с p -группами (см. [3]), то мы всюду будем предполагать, что G — p -группа.

Некоторые необходимые условия для разрешимости задачи погружения, условия согласности, были открыты Д. К. Фаддеевым [4].

В удобной для нас форме они приведены в работе [1]. Мы эти условия называем первым препятствием. Далее всюду предполагается, что первое препятствие для задачи $(k/\Omega, G, \varphi)$ исчезает.

Задачу погружения мы решаем последовательными шагами. В A выбираем F -инвариантный ряд

$$A \supset A_1 \supset \dots \supset A_i \supset \dots \supset 1$$

$\varphi [A_i : A_{i+1}] = p$ (так как G — p -группа, то такой ряд выбрать можно). Затем решаем задачу $(k/\Omega, G/A_1, \bar{\varphi})$, которая разрешима, так как является сопутствующей для задачи $(k/\Omega, G, \varphi)$. Пусть k^1 — решение задачи $(k/\Omega, G/A_1, \varphi)$. Спрашивается, когда поле k^1 можно выбрать так, что для задачи $(k^1/\Omega, G, \varphi_1)$ первое препятствие исчезает? Инварианты, которые дают ответ на этот вопрос, мы называем вторым препятствием для задачи погружения. В неявном виде второе препятствие дано в работе [1]. В настоящей работе второе препятствие находится для случая, когда k — поле алгебраических чисел.

§1. Задача согласования циклических алгебр; построение инвариантов

Так как все результаты, о которых будет идти речь в дальнейшем, относятся к случаю, когда погружаемое поле k является полем алгебраических чисел, то мы и будем предполагать с самого начала, что k — именно такое поле. Нас будет интересовать второе препятствие для задачи погружения, т. е. инварианты, позволяющие ответить на вопрос, когда существует такое решение k^1 задачи погружения $(k/\Omega, G/A_1, \bar{\varphi})$, что для задачи $(k^1/\Omega, G, \varphi_1)$ исчезает первое препятствие. Как известно из работы [1], второе препятствие определяется набором циклических алгебр над подполями поля k , задаваемых характеристам группы A_1 . Для нас не будет важна эта зависимость циклических алгебр от характеров группы A_1 , поэтому в обозначениях алгебр мы исключаем их зависимость от характеров.

Итак, пусть задано конечное число циклических алгебр

$$C_i = (\alpha_i, \beta_i)_{k_i} \quad (k_i \subset k).$$

Спрашивается, когда в поле Ω существует такое число m , что все алгебры C_i представляются в виде $C_i \approx (\alpha_i, m)_{k_i}$ для всех i ? Если такое число существует, то второе препятствие исчезает; если числа m не существует, то второе препятствие не исчезает.

Мы видим, что задача отыскания второго препятствия для задачи погружения сводится к некоторой задаче о циклических алгебрах. Последней задачей мы и будем заниматься. Сформулируем ее.

Задача согласования циклических алгебр. Задано конечное число алгебраических p -расширений $\{k_i\}$ поля алгебраических

чисел Ω и над каждым таким полем k_i задана циклическая алгебра $C_i = (\alpha_i, \beta_i)_{k_i}$ степени p . Каковы условия того, что все алгебры C_i одновременно представляются в виде

$$C_i \approx (\alpha_i, m)_{k_i}, \quad m \in \Omega?$$

Необходимые условия для разрешимости задачи согласования циклических алгебр легко указать. Это локальные условия: для любого простого дивизора p поля Ω должно существовать такое число $m_p \in \Omega_p$ (Ω_p — замыкание Ω по p), что

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i} = \left(\frac{\alpha_i, m_p}{\mathfrak{P}_i} \right)_{k_i}$$

для всех i и всех делителей $\mathfrak{P}_i$ дивизора p в поле k_i . Здесь, как и в дальнейшем,

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i}$$

обозначает символ норменного вычета в точке $\mathfrak{P}_i$.

ЛЕММА 1. Для циклических алгебр $\{C_i\}$, возникших из задачи погружения, выполняются локальные условия для их согласования.

Доказательство. Пусть $(k/\Omega, G, \varphi)$ — задача погружения, из которой возникают алгебры $\{C_i\}$, p — простой дивизор поля Ω , $\mathfrak{P}_i$ — его делители в поле k_i . Нам нужно доказать существование такого числа $m_p \in \Omega_p$, что

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i} = \left(\frac{\alpha_i, m_p}{\mathfrak{P}_i} \right)_{k_i}$$

для всех i и $\mathfrak{P}_i | p$, если алгебры $\{C_i\}$ возникли из задачи погружения. Выясним сначала, что означают локальные условия для алгебр $\{C_i\}$ с точки зрения задач погружения. Мы утверждаем, что локальные условия эквивалентны тому, что для задачи погружения $P_p = (k_p/\Omega_p, G, \varphi)$, где k_p — алгебра, получающаяся из k/Ω расширением Ω до Ω_p , исчезает второе препятствие.

Действительно, из исчезновения первого препятствия для задачи погружения $P = (k/\Omega, G, \varphi)$ следует исчезновение его для задачи P_p . Алгебры $C_i(P_p)$ эквивалентны алгебрам $(\alpha_i, \beta_i)_{k_{i,p}}$, так как переход от задачи P к задаче P_p получается расширением Ω до Ω_p . Если для задачи P_p исчезает второе препятствие, то существует

такое число $m_p \in \Omega_p$, что все алгебры $C_i(P_p)$ представляются в виде

$$C_i(P_p) \approx (\alpha_i, m_p)_{k_{ip}}.$$

Остается заметить, что распадение алгебры над центром, являющимся прямой суммой подалгебр (в нашем случае подполей), эквивалентно тому, что распадаются компоненты алгебры над соответствующими компонентами центра. Так как k_{ip} является прямой суммой полей $k_i \mathfrak{P}_i$, то представление

$$(\alpha_i, \beta_i)_{k_{ip}} \approx (\alpha_i, m_p)_{k_{ip}}$$

эквивалентно тому, что

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i} = \left(\frac{\alpha_i, m_p}{\mathfrak{P}_i} \right)_{k_i}$$

для всех i и $\mathfrak{P}_i | p$.

Следовательно, для доказательства леммы достаточно показать, что для задачи погружения P_p исчезает второе препятствие. Мы покажем больше, а именно, что задача погружения P_p разрешима. Таким образом, речь идет о доказательстве следующего утверждения: для разрешимости задачи погружения $(k/\Omega, G, \varphi)$, где Ω — локальное поле и k — алгебра, достаточно исчезновения первого препятствия. Применить здесь прямо теорему 4 работы [1] нельзя, так как там все рассуждения велись для случая, когда k — поле.

Пусть

$$k = \sum k e^{\sigma_j}$$

— разложение алгебры k в прямую сумму полей $k e^{\sigma_j}$ и H — подгруппа F , действующая в нормальном поле $\kappa = k e$. Тогда имеет место разложение

$$F = \sum H \sigma_j.$$

Рассмотрим задачу погружения $(\kappa/\Omega, \varphi^{-1} H, \varphi)$. Для такой задачи первое препятствие исчезает, поэтому она разрешима по основной теореме работы [1]. Пусть $\mathcal{K}$ — решение этой задачи. Рассмотрим алгебру

$$K = \sum \mathcal{K} e^{\bar{\sigma}_j},$$

являющуюся прямой суммой алгебр, изоморфных $\mathcal{K}$. Здесь $\bar{\sigma}_j$ — прообразы элементов σ_j в G . Группа G представляется в виде

$$G = \sum \varphi^{-1} H \bar{\sigma}_j.$$

Определим действие элементов группы G в K по формуле:

$$(\alpha e^{\bar{\sigma}_j})^{h\bar{\sigma}_i} = \alpha^{h_1} e^{\bar{\sigma}_1},$$

если

$$\bar{\sigma}_j h \bar{\sigma}_i = h_1 \bar{\sigma}_1.$$

Легко видеть, что получающееся представление будет регулярным и что алгебра K является решением задачи погружения $(k/\Omega, G, \varphi)$.

Лемма доказана.

Ввиду леммы 1, для нахождения второго препятствия в задаче погружения нам достаточно ответить на следующий вопрос. Пусть для системы C_i циклических алгебр выполнены локальные условия для их согласования; когда систему алгебр C_i можно согласовать? К этому вопросу мы и переходим.

Рассмотрим в поле Ω совокупность чисел b , обладающих свойством: для любого простого дивизора p из Ω число b в Ω_p представляется в виде

$$b = \prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i, \alpha_i})^{b_{\mathfrak{p}_i} \lambda^p}, \quad (1)$$

где $N_{\mathfrak{p}_i}$ — норма из поля $k_{\mathfrak{p}_i}$ в поле Ω_p , $b_{\mathfrak{p}_i}$ — некоторые целые числа и $\lambda \in \Omega_p$.

Числа b с таким свойством будем называть корневыми. Произведение двух корневых чисел снова будет корневым числом.

Отметим, что корневыми будут, например, все нормы $N_{k_i | \Omega} \alpha_i$, так как такая норма всегда разлагается в произведение локальных норм.

Пусть $\{b\}$ — подгруппа мультипликативной группы поля Ω , порожденная корневыми числами b .

ЛЕММА 2. Фактор-группа $\{b\}/\Omega^{*p}$ конечна.

Доказательство. Рассмотрим нормальную оболочку полей $k_i(\sqrt[p]{\alpha_i})$. Пусть это будет поле k' . Оно будет конечным расширением поля Ω , так как число алгебр C_i конечно.

Для доказательства леммы достаточно показать, что

$$\Omega(\sqrt[p]{b}) \subset k'.$$

В свою очередь, для доказательства последнего включения достаточно установить, что любой простой дивизор p из Ω , полностью разлагающийся в k' , полностью разлагается в $\Omega(\sqrt[p]{b})$. Покажем,

что для такого дивизора p число b является p -й степенью в Ω_p . Действительно, α_i являются p -ми степенями в $k_i \mathfrak{p}_i$:

$$\alpha_i = A_i^p, \quad A_i \in k_i \mathfrak{p}_i,$$

поэтому

$$b = \prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i} \alpha_i)^{b_{\mathfrak{p}_i} \lambda^p} = \left[\prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i} A_i)^{b_{\mathfrak{p}_i} \lambda} \right]^p.$$

Лемма доказана.

Каждому корневому числу b поставим в соответствие выражение:

$$I(b) = \prod_{p, i, \mathfrak{p}_i | p} \left(\frac{\alpha_i, \beta_i}{\mathfrak{p}_i} \right)_{k_i}^{b_{\mathfrak{p}_i}},$$

где $b_{\mathfrak{p}_i}$ получаются из представления (1).

Функции $I(b)$ будем называть корневыми для задачи согласования циклических алгебр $\{C_i\}$.

ЛЕММА 3. Если циклические алгебры $\{C_i\}$ удовлетворяют локальным условиям для их согласования, то корневая функция $I(b)$ не зависит от способа представления числа b в виде (1).

Доказательство. Пусть имеются два представления числа b :

$$b = \prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i} \alpha_i)^{b_{\mathfrak{p}_i} \lambda_p^p}$$

и

$$b = \prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i} \alpha_i)^{b'_{\mathfrak{p}_i} \lambda'_p{}^p}.$$

Тогда

$$1 = \prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i} \alpha_i)^{b_{\mathfrak{p}_i} - b'_{\mathfrak{p}_i} (\lambda_p / \lambda'_p)^p}$$

и достаточно показать, что $I(1) = 1$ для любого представления единицы.

Пусть

$$1 = \prod_{i, \mathfrak{p}_i | p} (N_{\mathfrak{p}_i} \alpha_i)^{n_{\mathfrak{p}_i} \nu_p^p}.$$

Тогда, используя основные свойства символа норменного вычета и то, что алгебры $\{C_i\}$ удовлетворяют локальным условиям для их согласования, получаем:

$$\begin{aligned} I(1) &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i}^{n_{\mathfrak{P}_i}} = \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, m_p}{\mathfrak{P}_i} \right)_{k_i}^{n_{\mathfrak{P}_i}} = \\ &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{N_{\mathfrak{P}_i} \alpha_i, m_p}{p} \right)_{\Omega}^{n_{\mathfrak{P}_i}} = \left(\frac{\prod_{i, \mathfrak{P}_i | p} (N_{\mathfrak{P}_i} \alpha_i)^{n_{\mathfrak{P}_i}}, m_p}{p} \right)_{\Omega} = \\ &= \prod_p \left(\frac{\nu_p^{-p}, m_p}{p} \right)_{\Omega} = 1. \end{aligned}$$

Лемма доказана.

Так как значение $I(b)$ зависит лишь от класса, в который попадает b в $\{b\}/\Omega^{*p}$, то корневых функций имеется только конечное число. Легко проверить, что относительно корневых чисел корневые функции ведут себя мультипликативно, т. е.

$$I(b_1 b_2) = I(b_1) I(b_2).$$

§2. Основные теоремы

ТЕОРЕМА 1. Для разрешимости задачи согласования циклических алгебр, удовлетворяющих локальным условиям, необходимо и достаточно обращение в 1 всех корневых функций.

Доказательство. Пусть задача согласования циклических алгебр разрешима, т. е.

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i} = \left(\frac{\alpha_i, m}{\mathfrak{P}_i} \right)_{k_i}, \quad m \in \Omega,$$

при всех i и $\mathfrak{P}_i | p$ в k_i , и $I(b)$ — корневая функция:

$$\begin{aligned} I(b) &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i}^{b_{\mathfrak{P}_i}}, \\ b &= \prod_{i, \mathfrak{P}_i | p} (N_{\mathfrak{P}_i} \alpha_i)^{b_{\mathfrak{P}_i}} \lambda_p^p. \end{aligned}$$

Тогда, используя основные свойства символа норменного вычета, получаем:

$$\begin{aligned} I(b) &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i}^{b_{\mathfrak{P}_i}} = \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, m}{\mathfrak{P}_i} \right)_{k_i}^{b_{\mathfrak{P}_i}} = \\ &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{N_{\mathfrak{P}_i} \alpha_i, m}{p} \right)_{\Omega}^{b_{\mathfrak{P}_i}} = \prod_p \left(\frac{\prod_{i, \mathfrak{P}_i | p} (N_{\mathfrak{P}_i} \alpha_i)^{b_{\mathfrak{P}_i}}, m}{p} \right)_{\Omega} = \\ &= \prod_p \left(\frac{b \lambda_p^{-p}, m}{p} \right)_{\Omega} = \prod_p \left(\frac{b, m}{p} \right)_{\Omega} = 1. \end{aligned}$$

Таким образом, необходимость условия теоремы доказана. Переходим к доказательству его достаточности.

Пусть $\mathfrak{M}$ — подгруппа идеальных элементов $m = \{m_p\}$, для которых

$$\left(\frac{\alpha_i, m_p}{\mathfrak{P}_i} \right)_{k_i} = 1$$

при всех i и $\mathfrak{P}_i | p$. Рассмотрим также подгруппу $\mathfrak{N} = \mathfrak{M}m$, $m \in \Omega$. По условию теоремы, существует идеальный элемент

$$\overline{m}_0 = \{m_{0p}\},$$

для которого

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i} = \left(\frac{\alpha_i, m_{0p}}{\mathfrak{P}_i} \right)_{k_i}$$

при всех i и $\mathfrak{P}_i | p$. Для доказательства теоремы нужно, следовательно, показать, что $\overline{m}_0 \in \mathfrak{N}$.

Заметим, что подгруппа $\mathfrak{N}$ является допустимой подгруппой (см. [2]). Для того, чтобы убедиться в этом, обозначим через S конечное множество дивизоров в Ω , являющихся либо делителями p , либо такими, что их делители в k_i разветвляются в k_i ($\mathfrak{P}_i | \alpha_i$). Тогда $\mathfrak{N}$ будет содержать множество идеальных элементов A_S (группа A_S определяется как множество идеальных элементов $\bar{n} = \{n_p\}$, для которых $n_p = 1$, если $p \in S$, и n_p — p -адическая единица, если $p \notin S$).

Допустимая подгруппа характеризуется тем, что все ее элементы ортогональны к некоторой конечной совокупности чисел из Ω

(см. [2]). Пусть $b_1, b_2, \dots, b_r$ — такие числа для $\mathfrak{N}$. Покажем, что они являются корневыми числами. Для этого в качестве $\overline{m} = \{m_p\}$ возьмем элемент, для которого m_p произвольно при фиксированном p и $m_q = 1$ при $q \neq p$. Тогда условие

$$\left(\frac{\alpha_i, m_p}{\mathfrak{P}_i} \right)_{k_i} = 1$$

для всех i и $\mathfrak{P}_i | p$ будет означать, что

$$(N_{\mathfrak{P}_i, \alpha_i} m_p)_{\Omega_p} \approx 1,$$

т. е. что m_p ортогонально конечной совокупности чисел из Ω_p . Для числа же b_t должно быть

$$[b_t, \overline{m}] = 1,$$

т. е.

$$(b_t, m_p)_{\Omega_p} \approx 1.$$

Так как ортогональное дополнение к ортогональному дополнению совпадает с первоначальной группой, то

$$b_t = \prod_{i, \mathfrak{P}_i | p} (N_{\mathfrak{P}_i, \alpha_i})^{b_{\mathfrak{P}_i}} \lambda_p^p.$$

Поэтому числа $b_1, b_2, \dots, b_r$ корневые.

Чтобы закончить доказательство теоремы, достаточно показать, что элемент $\overline{m}_0 = \{m_{0p}\}$ ортогонален ко всем корневым числам. Пусть

$$b = \prod_{i, \mathfrak{P}_i | p} (N_{\mathfrak{P}_i, \alpha_i})^{b_{\mathfrak{P}_i}} \lambda_p^p, \quad \lambda_p \in \Omega_p.$$

Тогда имеем:

$$\begin{aligned} [b, \overline{m}_0] &= \prod_p \left(\frac{b, m_{0p}}{p} \right)_{\Omega} = \prod_p \left(\frac{\prod_{i, \mathfrak{P}_i | p} (N_{\mathfrak{P}_i, \alpha_i})^{b_{\mathfrak{P}_i}} \lambda_p^p, m_{0p}}{p} \right)_{\Omega} = \\ &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{N_{\mathfrak{P}_i, \alpha_i}, m_{0p}}{p} \right)_{\Omega}^{b_{\mathfrak{P}_i}} = \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, m_{0p}}{\mathfrak{P}_i} \right)_{k_i}^{b_{\mathfrak{P}_i}} = \\ &= \prod_{p, i, \mathfrak{P}_i | p} \left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i}^{b_{\mathfrak{P}_i}} = I(b) = 1 \end{aligned}$$

(по условию). Теорема доказана.

Пусть, как и прежде, k' обозначает нормальную над Ω оболочку полей $k_i (\sqrt[p]{\alpha_i})$. Обозначим через $g(p)$, где p — простой дивизор в Ω , число делителей p в поле k' .

ТЕОРЕМА 2. Если общий наибольший делитель чисел $g(p)$, $p \in \Omega$, равен единице, то циклические алгебры $\{C_i\}$, которые удовлетворяют локальным условиям, всегда можно согласовать.

Для доказательства теоремы достаточно показать, что все корневые выражения в указанном случае равны 1. Так как мы рассматриваем задачу согласования циклических алгебр C_i над полями k_i , являющимися p -расширениями поля Ω , то и k' будет p -расширением Ω . Поэтому из того, что общий наибольший делитель чисел $g(p)$ равен единице, следует, что существует простой дивизор p_0 поля Ω , для которого $g(p_0) = 1$, т. е. p_0 имеет лишь один делитель $\mathfrak{P}_0$ в k' .

Пусть b — корневое число. Докажем, что $I(b) = 1$. Для этого рассмотрим равенство (1), определяющее число b в точке p_0 :

$$b = \prod_{i, \mathfrak{P}_{0i} | p_0} (N_{\mathfrak{P}_{0i}} \alpha_i)^{b_{\mathfrak{P}_{0i}}} \lambda_0^p, \quad \lambda_0 \in \Omega_{p_0}.$$

Так как у p_0 имеется единственный делитель в k' , то делитель $\mathfrak{P}_{0i}$ в поле k_i тоже будет один. Кроме того, группа разложения дивизора $\mathfrak{P}_0$ будет совпадать со всей группой $\mathfrak{G}(k'/\Omega)$ и локальные нормы $N_{\mathfrak{P}_{0i}}$ будут совпадать с обычными нормами из полей k_i в Ω . Поэтому в точке p_0 мы получаем равенство:

$$b = \prod_i (N_{k_i|\Omega} \alpha_i)^{n_i} \lambda_0^p$$

(числа $b_{\mathfrak{P}_{0i}}$ обозначены здесь через n_i). Рассмотрим число b из основного поля:

$$b' = b \bigg/ \prod_i (N_{k_i|\Omega} \alpha_i)^{n_i}$$

Оно является корневым, так как все числа $N_{k_i|\Omega} \alpha_i$ корневые. Число b является p -й степенью в Ω_{p_0} :

$$b' = \lambda_0^p.$$

Покажем, что оно является p -й степенью и в Ω . Действительно, пусть $b' \neq u^p$, $u \in \Omega$. Тогда поле $\Omega(\sqrt[p]{b'})$ будет промежуточным

между Ω и k' (из доказательства леммы 2 следует, что $\Omega \left(\sqrt[p]{b'} \right)$ является подполем поля k'):

$$\Omega \in \Omega \left(\sqrt[p]{b'} \right) \subset k'.$$

Перейдя в этой цепочке полей к замыканию по $\mathfrak{P}_0$ получим:

$$\Omega_{\mathfrak{p}_0} = \Omega \left(\sqrt[p]{b'} \right)_{\mathfrak{p}_0} \subset k'_{\mathfrak{P}_0},$$

что противоречит тому, что

$$[k'_{\mathfrak{P}_0} : \Omega_{\mathfrak{p}_0}] = [k' : \Omega]$$

при $g(\mathfrak{p}_0) = 1$. Следовательно,

$$b' = u^p, \quad u \in \Omega.$$

Но u^p является корневым числом, для которого $I(u^p) = 1$. Поэтому

$$I(b) = \prod_i I(N_{k_i|\Omega} \alpha_i)^{n_i},$$

и достаточно проверить, что

$$I(N_{k_i|\Omega} \alpha_i) = 1.$$

Напишем для этого разложение $N_{k_i|\Omega} \alpha_i$ в произведение локальных норм:

$$N_{k_i|\Omega} \alpha_i = \prod_{\mathfrak{P}_i|\mathfrak{p}} N_{\mathfrak{P}_i} \alpha_i.$$

Значит, $b_{\mathfrak{P}_i} = 1$, $b_{\mathfrak{P}_j} = 0$ для $j \neq i$. В таком случае

$$I(N_{k_i|\Omega} \alpha_i) = \prod_{\mathfrak{p}, j, \mathfrak{P}_j|\mathfrak{p}} \left(\frac{\alpha_j, \beta_j}{\mathfrak{P}_j} \right)_{k_j}^{b_{\mathfrak{P}_j}} = \prod_{\mathfrak{p}, \mathfrak{P}_i|\mathfrak{p}} \left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i} \right)_{k_i} = 1$$

(по закону взаимности). Теорема доказана.

Следствие 1. Если трехмерная группа когомологий

$$H^3(\mathfrak{G}(k'/\Omega), k'^*) = 1,$$

то алгебры $\{C_i\}$, удовлетворяющие локальным условиям, всегда можно согласовать.

Для доказательства достаточно заметить, что для полей алгебраических чисел трехмерная группа когомологий является циклической, и порядок ее равен наибольшему общему делителю чисел $g(\mathfrak{p})$, $\mathfrak{p} \in \Omega$.

Следствие 2. Если поле k' циклическое над Ω , то алгебры $\{C_i\}$, удовлетворяющие локальным условиям, всегда можно согласовать.

Для доказательства достаточно заметить, что в случае, когда поле k' циклическое над Ω , трехмерная группа когомологий $H^3(\mathfrak{G}(k'/\Omega), k'^*)$ будет единичной, или что по закону плотностей Чеботарева в Ω существует простой дивизор $\mathfrak{p}$, принадлежащий образующему элементу группы $\mathfrak{G}(k'/\Omega)$, а тогда для такого $\mathfrak{p}$ имеем:

$$g(\mathfrak{p}) = 1.$$

Приведем результаты, относящиеся к задаче погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k , непосредственно вытекающее из теоремы 2 и ее следствий.

Пусть дана группа характеров $\mathfrak{A}$ нормального делителя A в задаче погружения. Тогда фактор-группа F естественно отображается в группу автоморфизмов группы $\mathfrak{A}$. Обозначим через F' ядро этого отображения, через k' — подполе, принадлежащее F' в k , через $g(\mathfrak{p})$ — число делителей в k' простого дивизора $\mathfrak{p}$ в Ω .

ТЕОРЕМА 3. Если общий наибольший делитель чисел $g(\mathfrak{p})$, $\mathfrak{p} \in \Omega$, равен 1, то исчезновение первого препятствия для задачи погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k достаточно для ее разрешимости.

Для доказательства достаточно заметить, что при переходе к задаче погружения $(k^1/\Omega, G, \varphi_1)$ условие теоремы сохраняется.

Следствие 1. Если трехмерная группа когомологий

$$H^3(F/F', k'^*) = 1,$$

то исчезновение первого препятствия для задачи погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k достаточно для ее разрешимости.

Следствие 2. Если фактор-группа F индуцирует в группе характеров нормального делителя циклическую группу автоморфизмов, то исчезновение первого препятствия для задачи погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k достаточно для ее разрешимости.

С помощью результатов работы [3] легко получить, что теорема 3 и следствия из нее будут справедливы и для случая, когда G не является p -группой.

Замечание. Хотя доказательства следствий 1 и 2 арифметические, формулировка их чисто алгебраическая. Интересно было бы выяснить, не справедливы ли эти следствия для произвольного поля k . Гипотеза о том, что это имеет место, подтверждается случаем, когда k — локальное поле. В этом случае трехмерных гомологий нет и, действительно, исчезновение первого препятствия достаточно для погружаемости.

§3. Пример

Рассмотрим пример на вычисление второго препятствия (этот пример взят из работы [5]).

Пусть нормальный делитель A в задаче погружения $(k/\Omega, G, \varphi)$ — циклическая группа восьмого порядка $A = \{\alpha\}$. Мы можем предполагать, что любой дивизор p из Ω имеет в поле k' , которое было определено в предыдущем параграфе, либо два, либо четыре делителя (см. теорему 3). Это, в частности, означает, что фактор-группа F индуцирует в группе характеров группы A нециклическую группу автоморфизмов. Но группа автоморфизмов группы A является произведением двух циклических групп второго порядка. Следовательно, группа F должна порождать всю эту группу автоморфизмов, и поэтому поле k' имеет вид:

$$k' = \Omega(\sqrt{a}, \sqrt{b}).$$

Сделаем в задаче погружения $(k/\Omega, G, \varphi)$ первый шаг. Нормальным делителем после первого шага будет

$$A_1 = \{\alpha^2\}.$$

У него имеются два существенных для нас характера χ_1 и χ_2 :

$$\chi_1(\alpha^2) = -1,$$

$$\chi_2(\alpha^2) = i.$$

Пусть x_1 и x_2 — продолжение характеров χ_1 и χ_2 на A . Ясно, что всегда

$$\begin{aligned} F_{x_2} &\subset F_{\chi_2}, \\ F_{x_1} &\subset F_{\chi_1} = F, \\ F_{\chi_2} &\subset F_{\chi_1} = F, \quad F_{x_2} \subset F_{x_1}, \end{aligned}$$

и что индексы всех написанных подгрупп равны либо 1, либо 2. Нетрудно проверить, что в рассматриваемом случае все эти индексы равны 2. Будем считать, что

$$\begin{aligned} k_{x_1} &= \Omega(\sqrt{a}) & [k_{x_2} &= \Omega(\sqrt{a}, \sqrt{b})], \\ k_{\chi_2} &= \Omega(\sqrt{a}) & [k_{\chi_1} &= \Omega]. \end{aligned}$$

Поэтому

$$\begin{aligned} \alpha_{x_2} &= b, \\ \alpha_{x_1} &= a. \end{aligned}$$

Число a будет корневым, но второго препятствия оно дать не может, так как является нормой от $\alpha_{x_1} = a$.

Докажем, что число b тоже будет корневым. Для этого нужно, чтобы

$$b \approx a^{i_p} \prod_{\mathfrak{P}_i | p} (N_{\mathfrak{P}_i} b)^{i_{\mathfrak{P}_i}} \quad \text{в } \Omega_p. \quad (2)$$

Знак $\approx$ означает 2-равенство, т. е. равенство с точностью до квадратов. Так как норма $N_{\mathfrak{P}_i} b$ всегда будет равна b или b^2 независимо от делителя $\mathfrak{P}_i$ дивизора p , то мы будем брать в 2-равенстве (2) только один из делителей дивизора p :

$$b \approx a^{i_p} N_p b^{j_p} \quad (2')$$

($N_p b$ обозначает здесь норму $N_{\mathfrak{P}_i} b$ для одного из делителей $\mathfrak{P}_i$ дивизора p). Если $a \approx 1$ в Ω_p , то

$$N_p b = b,$$

и поэтому в 2-равенстве (2') нужно взять $i_p = 0$, $j_p = 1$. Если $a \not\approx 1$ в Ω_p , то

$$N_p b = b^2 \approx 1.$$

• Поэтому при $b \approx 1$ нужно взять $i_p = 0$, а при $b \neq 1$ должно быть $b \approx a$ ($i_p = 1$), т. е. $ab \approx 1$. Последнее соотношение выполняется, так как в противном случае степень $[\Omega_p(\sqrt{a}, \sqrt{b}) : \Omega_p]$ была бы равна 4, а это означало бы, что у p в поле k' имеется только один делитель.

Следовательно, мы получаем такое представление числа b в виде (2'):

- 1) $b \approx 1$ в Ω_p ; $i_p = 0$, $j_p = 0$;
- 2) $b \not\approx 1$, но $a \approx 1$ в Ω_p ; $i_p = 0$, $j_p = 1$;
- 3) $b \not\approx 1$ и $a \not\approx 1$ в Ω_p ; $i_p = 1$, $j_p = 0$.

Так как мы предполагаем, что первое препятствие для нашей задачи исчезает, то алгебры C_{χ_1} и C_{χ_2} будут иметь вид:

$$C_{\chi_1} \approx (a, \beta_{\chi_1})_{\Omega},$$

$$C_{\chi_2} \approx (b, \beta_{\chi_2})_{\Omega(\sqrt{a})}.$$

Значит, корневая функция $I(b)$ представляется следующим образом:

$$I(b) = \prod_p \left(\frac{a, \beta_{\chi_1}}{p} \right)^{i_p} \prod_p \left(\frac{b, \beta_{\chi_2}}{p} \right)^{j_p}_{\Omega(\sqrt{a})}.$$

Здесь через

$$\left(\frac{b, \beta_{\chi_2}}{p} \right)_{\Omega(\sqrt{a})}$$

обозначен символ норменного вычета

$$\left(\frac{b, \beta_{\chi_2}}{\mathfrak{P}_i} \right)_{\Omega(\sqrt{a})}$$

для одного из делителей $\mathfrak{P}_i$ дивизора p .

Рассмотрим теперь числовой пример. Пусть погружаемое поле $k = R(\sqrt{c}, \sqrt{2}, i)$, где R — поле рациональных чисел. Группа Галуа F поля k/R является прямым произведением групп

$$F_1 = \mathfrak{G}(k_1/R), \quad k_1 = R(\sqrt{c}),$$

и

$$F_2 = \mathfrak{G}(k_2/R), \quad k_2 = R(\sqrt{2}, i).$$

Пусть $G = G_1 \times F_2$, где

$$G_1 = \{\alpha, \beta; \quad \alpha^8 = 1, \quad \beta^2 = \alpha^4, \quad \beta^{-1}\alpha\beta = \alpha^7\}.$$

и $\varphi : G \rightarrow \mathfrak{G}(k/R)$ — гомоморфное отображение группы G на $\mathfrak{G}(k/R)$, задаваемое таким образом: $\varphi(\alpha) = 1$, $\varphi(\beta)$ — образующий элемент группы F_1 , и φ на F_2 является изоморфизмом. Тогда мы имеем задачу погружения $(k/R, G, \varphi)$ с циклическим нормальным делителем восьмого порядка, порождаемым элементом α . Поле k содержит корни восьмой степени из единицы, так как $\sqrt{2} \in k$ и $i \in k$.

Необходимым и достаточным условием исчезновения первого препятствия для такой задачи является распадение циклической алгебры

$$C_0 = (-1, -1)_{R(\sqrt{-c}, \sqrt{2})}.$$

Распадение алгебры C_0 означает, что в поле $R(\sqrt{-c}, \sqrt{2})$ разрешимо уравнение

$$x^2 + y^2 + z^2 = 0.$$

Поле k' будет в данном случае равно $R(\sqrt{-c}, \sqrt{2})$, причем

$$k_{\chi_1} = R(\sqrt{-c}).$$

Для того, чтобы в поле $R(\sqrt{-c}, \sqrt{2})$ не исчезал трехмерный цикл (чтобы число 2 было корневым), должно выполняться такое условие: если $-c \not\approx 1$ в R_p , то либо $2 \approx 1$, либо $-2c \approx 1$ в R_p . Для задачи, которую мы сейчас рассматриваем, алгебры C_{χ_1} и C_{χ_2} , получающиеся после первого шага (построения поля $k^1 = R(\sqrt{\mu}, \sqrt{c}, \sqrt{2}, i)$, где μ — произвольное число из R), будут иметь вид:

$$C_{\chi_1} \approx (\mu, -c)_R;$$

$$C_{\chi_2} \approx (2, \mu)_{R(\sqrt{-c})} \otimes (-1, -1)_{R(\sqrt{-c})}.$$

Значит, корневая функция $I(2)$ будет выражаться следующим образом:

$$I(2) = \prod_p \left(\frac{\mu, -c}{p} \right)_R^{i_p} \prod_p \left(\frac{2, \mu}{p} \right)_{R(\sqrt{-c})}^{j_p} \prod_p \left(\frac{-1, -1}{p} \right)_{R(\sqrt{-c})}^{j_p}.$$

Мы знаем, что корневая функция не зависит от числа μ , поэтому в выражении $I(2)$ можно взять $\mu = 1$. Кроме того,

$$\left(\frac{-1, -1}{p} \right)_{R(\sqrt{-c})} = 1$$

для всех $p \neq 2$. Поэтому

$$\begin{aligned} I(2) &= \prod_p \left(\frac{1, -c}{p} \right)_R^{i_p} \prod_p \left(\frac{2, 1}{p} \right)_{R(\sqrt{-c})}^{j_p} \left(\frac{-1, -1}{2} \right)_{R(\sqrt{-c})}^{j_2} \\ &= \left(\frac{-1, -1}{2} \right)_{R(\sqrt{-c})}^{j_2}. \end{aligned}$$

Для того, чтобы не исчезало второе препятствие, необходимо и достаточно выполнение следующих условий:

$$\left(\frac{-1, -1}{2} \right)_{R(\sqrt{-c})} = -1 \quad \text{и} \quad j_2 = 1.$$

Покажем, что если за c взять любое произведение простых чисел вида $16n + 7$, то для задачи погружения $(k/R, G, \varphi)$ будут выполнены все перечисленные выше условия.

Для такой задачи первое препятствие исчезает, так как $-c \equiv 1 \pmod{8}$, $-c$ является квадратом в R_2 и уравнение $x^2 + y^2 + z^2 = 0$ разрешимо в $R_2(\sqrt{2})$. Решением последнего уравнения будет, например,

$$\begin{aligned} x &= -1 + \sqrt{-c} + (1 + \sqrt{-c})\sqrt{2}, \\ y &= -1 - \sqrt{-c} + (-1 + \sqrt{-c})\sqrt{2}, \\ z &= \sqrt{6(c-1)}. \end{aligned}$$

Легко видеть, что корень из числа $6(c-1)$ извлекается.

Далее, выполняется условие того, что степень

$$[R_p(\sqrt{-c}, \sqrt{2}) : R_p] < 4$$

для любого простого числа p . В самом деле, если $p = 2$, то $-c \approx 1$ в R_2 ; если $p|c$, то $\left(\frac{2}{p}\right) = 1$ и $2 \approx 1$ в R_p ; если $p \neq 2$, не делит c и

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{-c}{p}\right) = -1,$$

то

$$\left(\frac{-2c}{p}\right) = \left(\frac{2}{p}\right) \left(\frac{-c}{p}\right) = 1,$$

и $-2c \approx 1$ в R_p .

В то же время, уравнение $x^2 + y^2 + z^2 = 0$ неразрешимо в R_2 . Это означает, что

$$\left(\frac{-1, -1}{2} \right)_{R_2} = -1.$$

Кроме того, $j_2 = 1$, так как $2 \not\approx 1$ в R_2 и $-c \approx 1$ в R_2 .

Таким образом, для задачи погружения $(R(\sqrt{c}, \sqrt{2}, i)/R, G, \varphi)$ при условии, что c имеет лишь простые делители вида $16n + 7$, второе препятствие не исчезает. Следовательно, эта задача погружения не разрешима.

ЛИТЕРАТУРА

1. Демушкин С.П. и Шафаревич И. Р., *Задача погружения для локальных полей*, Известия Ак. наук СССР, серия матем. **23** (1959), 823–840.
2. Вейль Г., *Алгебраическая теория чисел*, ИЛ, М., 1947.
3. Kochendörffer R., *Zwei Reduktionssätze zum Einbettungsproblem für Abelsche Algebren*, Math. Nachr. **10**, N 1-2 (1953), 75–84.
4. Делоне Б. Н., Фаддеев Д. К., *Исследования по геометрии теории Галуа*, Матем. сборн. **15** (57) :2 (1944), 243–276.
5. Фаддеев Д. К., *Об одной гипотезе Хассе*, Доклады Ак. наук СССР **94**, N 6 (1954), 1013–1016.

ПОЛЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

PROC. INT. CONGR. MATH. STOCKHOLM 1962

Введение

Теория алгебраических чисел имеет две стороны. Одна из них — это построение общей теории полей алгебраических чисел, имеющее целью их полную классификацию и описание их арифметики. Другая сторона связана с приложением этой общей теории к таким конкретным вопросам, как, например, диофантовы уравнения, комплексное умножение эллиптических и абелевых функций или интегрирование алгебраических дифференциалов.

В этом обзоре будут рассмотрены некоторые вопросы, лежащие в первом направлении.

Образцом для всех будущих теорий здесь служит теория полей классов, которая исчерпывающим образом описывает все абелевы (имеющие коммутативную группу Галуа) расширения фиксированного поля алгебраических чисел. В области расширений с неабелевой группой Галуа наши знания очень далеки от такой полноты. Часто неясно даже, как следует ставить вопросы и в каких терминах искать их решение. Иногда легче найти правильную постановку вопроса, если посмотреть на эту область с более общей точки зрения.

Поля алгебраических чисел и содержащиеся в них кольца целых алгебраических чисел являются простейшими примерами и в то же время отправными пунктами для гораздо более общих теорий. Особенно большое значение эти связи имеют для самой теории алгебраических чисел, так как они помогают найти новые постановки вопросов, сопоставляя эту теорию с другими, которые ей во многом аналогичны, но в которых мы можем использовать аналитический аппарат или геометрическую интуицию. Это объясняет, почему дальше речь будет идти часто о вопросах, не относящихся, строго говоря, к теории алгебраических чисел.

§1. Поля алгебраических функций

Особенно большую роль в развитии теории алгебраических чисел играли ее связи и аналогии с теорией алгебраических функций одной переменной. Пусть k — поле алгебраических функций одной переменной с полем констант k_0 . Нас интересует проблема классификации конечных расширений поля k . Решение ее хорошо известно, если $k_0 = \mathbb{C}$ — поле комплексных чисел. В этом случае полю k может быть сопоставлена его риманова поверхность $\mathfrak{R}$. Если k'/k — конечное расширение k , то его риманова поверхность $\mathfrak{R}'$ естественным образом непрерывно отображается на $\mathfrak{R} : \mathfrak{R}' \rightarrow \mathfrak{R}$. Таким образом, поверхность $\mathfrak{R}'$ является накрывающей для поверхности $\mathfrak{R}$. Это накрытие имеет ту же степень, что и расширение k'/k , и обладает конечным числом точек ветвления. Из теоремы существования Римана легко вытекает, что мы получаем таким образом взаимно однозначное соответствие между конечными расширениями поля k и разветвленными накрытиями конечной степени его римановой поверхности $\mathfrak{R}$. Задача сводится, таким образом, к топологическому вопросу, ответ на который хорошо известен. Фиксируем конечное множество $S = \{p_1, \dots, p_m\}$ точек поверхности $\mathfrak{R}$ и рассмотрим накрытия конечной степени $\mathfrak{R}' \rightarrow \mathfrak{R}$, разветвленные только в точках этого множества. Они соответствуют неразветвленным накрытиям поверхности $\mathfrak{R} - S$, которые, в свою очередь, находятся во взаимно однозначном соответствии с подгруппами конечного индекса фундаментальной группы $\pi_1(\mathfrak{R} - S)$ этой поверхности. Наконец, группа $\pi_1(\mathfrak{R} - S)$ хорошо известна — она имеет $m + 2g$ образующих $u_1, \dots, u_m, s_1, t_1, \dots, s_g, t_g$ (g — род поверхности $\mathfrak{R}$), связанных одним соотношением

$$u_1 \dots u_m s_1 t_1^{-1} t_1^{-1} \dots s_g t_g s_g^{-1} t_g^{-1} = 1. \quad (1)$$

Заметим, что хотя источники этих результатов аналитические, им может быть придана алгебраическая формулировка. Действительно, точки поверхности $\mathfrak{R}$ соответствуют простым дивизорам поля k , и, в частности, точки ветвления накрытия $\mathfrak{R}' \rightarrow \mathfrak{R}$ могут быть характеризованы в терминах расширения k'/k как критические простые дивизоры (делители дискриминанта). Группа $\pi_1(\mathfrak{R} - S)$ также может быть описана в алгебраических терминах. Для этого рассмотрим поле $\mathfrak{K}_S$, являющееся объединением всех расширений k'/k , критические простые дивизоры которых принадлежат множеству S . Это расширение бесконечно, и его группа Галуа $\mathfrak{G}_S$ является топологической группой. Таким образом, группа $\mathfrak{G}_S$ может быть определена для произвольного поля алгебраических функций. Ее знание дает возможность перечислить все расширения

k'/k с указанным выше свойством, так как они, согласно основной теореме теории Галуа, соответствуют ее подгруппам конечного индекса. Если $k_0 = \mathbb{C}$, то $\mathfrak{G}_S$ является пополнением группы $\pi_1(\mathfrak{X} - S)$ в топологии, определенной всеми подгруппами конечного индекса. Таким образом, соотношение (1) определяет $\mathfrak{G}_S$ как топологическую группу.

Известно, что среди полей алгебраических функций к полям алгебраических чисел ближе всего стоят те, у которых поле k_0 конечно. Ввиду этого с точки зрения теории полей алгебраических чисел было бы интересно получить для этого класса полей результат, аналогичный сформулированному выше. Решение, однако, известно только в промежуточном случае, когда поле констант k_0 алгебраически замкнуто.

Если характеристика поля k_0 равна 0, то можно применить известный “принцип Лефшеца”. Задача легко сводится к случаю, когда поле коэффициентов k_0 имеет конечную степень трансцендентности над полем рациональных чисел, а путем вложения такого поля в поле комплексных чисел — к разобранному случаю $k_0 = \mathbb{C}$. Из этих соображений следует, что для любого поля алгебраических функций с алгебраически замкнутым полем констант k_0 характеристики 0 группы $\mathfrak{G}_S$ такая же, как и в случае $k_0 = \mathbb{C}$.

Для алгебраически замкнутого поля k_0 характеристики $p > 0$ аналогичный результат получен А. Гротендиком [1] для расширений, степень которых взаимно проста с p . Для описания этого результата построим поле $\mathcal{L}_S$, так же как раньше строилось поле $\mathfrak{K}_S$, ограничиваясь, однако, теперь только нормальными полями, степени которых взаимно просты с p . Оказывается что группа Галуа $\mathfrak{H}_S$ поля $\mathcal{L}_S$ опять та же, что и в классическом случае $k_0 = \mathbb{C}$. Доказательство основывается на сведении к случаю поля характеристики 0 путем редукции таких полей по модулю p . Таким образом, в основе доказательства лежит такой глубокий аналитический факт, как теорема существования Римана.

Вернемся теперь к случаю конечного поля констант k_0 , который для нас особенно интересен. Обозначим через $\bar{k}_0$ алгебраическое замыкание поля k_0 и через $\bar{k}$ — композит полей k и $\bar{k}_0$. Очевидно, что $k \subset \bar{k} \subset \mathcal{L}_S$. Группа Галуа $\mathfrak{H}_S$ поля $\mathcal{L}_S/\bar{k}$ описана теоремой Гротендика, а группа Галуа $\mathfrak{F}$ поля $\bar{k}/k$ хорошо известна — она является свободной топологической группой с одной образующей. Так как $\mathfrak{H}/\bar{\mathfrak{H}}_S = \mathfrak{F}$, то определение группы $\mathfrak{H}_S$ — это задача теории расширений групп. Ввиду того, что группа $\mathfrak{F}$ свободная, соответствующее расширение распадается, и, следовательно, структура группы $\mathfrak{H}_S$ определяется тем, как образующий элемент группы $\mathfrak{F}$ (так называемый автоморфизм Фробениуса) действует на группу $\mathfrak{H}_S$.

К сожалению, об этом ничего не известно, даже в самых простых случаях (например, в случае p -расширений).

§2. Локальные поля

Прежде чем приступить к исследованию полей алгебраических чисел, естественно исследовать локальные поля, т.е. пополнения полей алгебраических чисел по их простым дивизорам.

Пусть k — локальное поле, содержащее поле p -адических чисел R_p . Согласно теории ветвления Дедекинда-Гильберта в любом нормальном расширении K/k содержится максимальное подполе k_1/k , не имеющее высшего ветвления. Степень поля K/k_1 является степенью p . Таким образом, всякое расширение локального поля в некотором смысле составлено из поля без высшего ветвления и p -расширения. Структура полей без высшего ветвления весьма проста, как следует из той же теории Дедекинда-Гильберта. Поэтому можно думать, что основная трудность в классификации локальных полей — это классификация p -расширений.

Сейчас имеется довольно полная картина строения p -расширений локального поля. Для их описания рассмотрим аналогично тому, как мы это делали в случае алгебраических функций, поле $\mathfrak{K}$, являющееся объединением всех конечных p -расширений локального поля k , и обозначим через $\mathfrak{G}$ группу Галуа расширения $\mathfrak{K}/k$. Группа $\mathfrak{G}$ является топологической p -группой и содержит в себе довольно полную информацию о p -расширениях поля k , так как они находятся во взаимно однозначном соответствии с подгруппами конечного индекса группы $\mathfrak{G}$. Поэтому основные усилия были направлены на вычисление этой группы.

Обозначим через ν степень $[k : R_p]$. Строение группы $\mathfrak{G}$ зависит от этого числа и от того, содержится ли в поле k первообразный корень ζ степени p из единицы.

Имеют место следующие результаты:

1. Если $\zeta \notin k$, то группа $\mathfrak{G}$ является свободной топологической p -группой с $\nu + 1$ образующими [2].
2. Если $\zeta \in k$, то группа $\mathfrak{G}$ имеет $\nu + 2$ образующие и определена (как топологическая p -группа) одним определяющим соотношением ([3] и [4]).

В этих результатах утверждения о числе образующих легко следуют из известной теоремы Бернсайда [5].

Доказательство утверждений о числе соотношений основывается на соображениях, которые мы рассмотрим сразу в более общей ситуации.

Пусть k — произвольное поле и $\mathfrak{K}$ его p -расширение (конечное или нет) с группой Галуа $\mathfrak{G}$. Легко видеть, что число r незави-

симых соотношений, связывающих минимальную систему образующих группы $\mathfrak{G}$, равно числу образующих ее двумерной группы гомологий:

$$r = \dim_{\mathbf{Z}_p} H^2(\mathfrak{G}, \mathbf{Z}_p),$$

где $\mathbf{Z}_p$ — группа порядка p .

Пусть K_α — семейство подполей $\mathfrak{K}$, конечных над k , и G_α — их группы Галуа. Определены гомоморфизмы

$$j_\alpha : H^2(G_\alpha, \mathbf{Z}_p) \rightarrow H^2(\mathfrak{G}, \mathbf{Z}_p),$$

и $H^2(\mathfrak{G}, \mathbf{Z}_p)$ является объединением групп $j_\alpha H^2(G_\alpha, \mathbf{Z}_p)$. Каждый элемент $\xi \in H^2(G_\alpha, \mathbf{Z}_p)$ определяет некоторое расширение G_α^ξ группы G_α при помощи $\mathbf{Z}_p$. Легко видеть, что $j_\alpha \xi = 0$ тогда и только тогда, когда поле K_α погружаемо в поле $K' \subset \mathfrak{K}$, имеющее группу Галуа G_α^ξ . Это дает возможность определить группу $H^2(\mathfrak{G}, \mathbf{Z}_p)$ (а значит, и число соотношений r в группе $\mathfrak{G}$), если мы умеем решать соответствующую задачу погружения. Несколько неточно можно сказать, что r равно числу условий, которые должны выполняться, чтобы эта задача погружения была разрешима. В частности, результат 2 непосредственно вытекает из этих соображений, так как условием разрешимости задачи погружения является, согласно известному критерию Брауера [6], обращение в 1 некоторого элемента группы $B(k)_p$, где $B(k)$ — группа Брауера поля k , а $B(k)_p$ — ее подгруппа, состоящая из элементов периода p . Известно, что для любого n группа $B(k)_n$ имеет одну образующую. Отсюда и следует, что $r = 1$.

Результат 1 описывает группу $\mathfrak{G}$ полностью. В случае 2 остается найти соотношение, определяющее группу $\mathfrak{G}$. Это было сделано С. П. Демушкиным [7]. Оказалось, что если μ — наибольшее число, такое что поле k содержит первообразный корень степени p^μ из 1, то соотношение имеет вид (при $p \neq 2$ или $p = 2, \mu \neq 1$)

$$s_1^{p^\mu} (s_1, s_2)(s_3, s_4) \dots (s_{\nu+1}, s_{\nu+2}) = 1, \quad (2)$$

где (s, t) означает $sts^{-1}t^{-1}$. Случай $p = 2, \mu = 1$ (который имеет место, например, если $k = R_2$) до сих пор не разобран.

Этот результат носит, по существу, теоретико-групповой характер и связан с интересным вопросом — исследованием топологических p -групп, определяемых одним соотношением. Соотношение f , определяющее некоторую p -группу G , называется полным, если его нельзя преобразовать подходящей заменой образующих в такое соотношение, которое не содержит какой-либо из образующих. Это требование равносильно тому, что группа G не разлагается в свободное произведение. Соотношение f называется m -полным, если

то же имеет место для группы $G/G^{(m)}$, где $G^{(m)}$ — m -й член убывающего центрального ряда группы G .

Для группы $\mathfrak{G}$ (группы Галуа максимального p -расширения локального поля k) нетрудно вычислить группу $\mathfrak{G}/\mathfrak{G}^{(2)}$ и проверить, что соотношение, определяющее $\mathfrak{G}$, 2-полно. Демушкин доказывает для произвольной p -группы G , определенной одним соотношением f (ограничиваясь, правда, группами с четным числом образующих), что если f 2-полно, то группа G однозначно определяется группой $G/G^{(2)}$. Отсюда легко вытекает классификация всех соотношений такого типа — они всегда могут быть приведены к виду (2) с некоторым μ . То, что для группы $\mathfrak{G}$ число m имеет указанный выше смысл, получается из рассмотрения группы G/G^1 .

Было бы очень интересно продолжать эти исследования и выяснить, как обобщаются эти результаты при переходе к m -полным соотношениям при произвольном m . Отметим одно теоретико-групповое следствие этой теоремы о локальных полях — подгруппа конечного индекса p -группы, определенной соотношением (2), сама определена одним соотношением такого же типа (возможно с другим μ и ν). Естественно возникает вопрос, обобщается ли этот факт на случай любой p -группы с таким соотношением, и можно ли в этом случае придать какой-нибудь смысл словам “соотношение того же типа”.

Естественно надеяться, что изучение любых конечных расширений локальных полей может быть сведено к изучению расширений без высшего ветвления и p -расширений. Этот вопрос равносильен вычислению группы Галуа алгебраического замыкания локального поля. Задача еще не решена, хотя Х.Кох (см. [8] и диссертацию, представленную в Университет им. Гумбольдта в Берлине) нашел ряд свойств этой группы и доказал, что она однозначно определяется простыми инвариантами поля k .

§3. Поля алгебраических чисел

Естественно попытаться использовать в теории полей алгебраических чисел тот же подход, которым мы пользовались в полях алгебраических функций и в локальных полях. Пусть k — некоторое поле алгебраических чисел, конечное расширение поля рациональных чисел R . Обозначим через S некоторое конечное множество простых дивизоров поля k и рассмотрим все конечные расширения k'/k , критическими простыми дивизорами (т.е. делителями дискриминантов) которых являются только простые дивизоры множества S . Объединение всех этих полей обозначим через $\mathfrak{K}_S$, а группу Галуа поля $\mathfrak{K}_S/k$ через $\mathfrak{G}_S$. По-видимому, одной из основных задач теории алгебраических чисел является исследование групп $\mathfrak{G}_S$.

По аналогии с тем, что, как мы видели, имеет место в полях алгебраических функций, возникают два вопроса:

Будет ли группа $\mathfrak{G}_S$ обладать конечной системой образующих?

Если это так, то можно ли (при фиксированном поле k) ограничить число образующих в зависимости только от числа дивизоров в множестве S ?

Ответы на эти вопросы неизвестны. Положительный ответ на второй из них означал бы, что для любого конечного нормального расширения K/k число образующих его группы Галуа ограничено в зависимости от числа критических простых дивизоров. Этот вопрос интересен уже для самых простых расширений. Пусть, например, k совпадает с полем рациональных чисел R . Обозначим через L/R квадратичное расширение с простым дискриминантом p и возьмем за K Гильбертово поле классов поля L (т.е. его максимальное абелево неразветвленное расширение). Очевидно, что K/R имеет только одно критическое простое число p . Так как группа Галуа K/L совпадает с группой классов дивизоров L , а число образующих группы Галуа K/L отличается, как легко видеть, от числа образующих группы Галуа K/R не больше, чем на 1, то интересующий нас вопрос эквивалентен в этом случае следующему:

Ограничены ли числа образующих групп классов дивизоров квадратичных полей с простым дискриминантом?

Этим кругом вопросов интересовался еще Гаусс, который называл квадратичное поле регулярным, если его группа классов дивизоров циклическая [9].

По своему обыкновению Гаусс составил таблицы [9], из которых следует, что для $p < 3000$ и для $9000 < p < 10000$ число образующих равно 1 или 2, причем во втором случае одна образующая имеет порядок 3.

Уже этот простой пример показывает, что исследование групп $\mathfrak{G}_S$ связано с очень большими трудностями. По-видимому, в настоящее время в этом направлении не известно никаких общих результатов. Можно сказать гораздо больше, если ограничиться рассмотрением p -расширений. Фиксируем некоторое простое число p и обозначим через $\mathfrak{P}_S$ группу Галуа объединения всех p -расширений поля k , критические простые дивизоры которых содержатся в множестве S . Очевидно, что группа $\mathfrak{P}_S$ является максимальной p -факторгруппой группы $\mathfrak{G}_S$.

Легко видеть, что оба вопроса, поставленные выше для групп $\mathfrak{G}_S$, имеют для групп $\mathfrak{P}_S$ положительный ответ.

Обозначим минимальное число образующих группы $\mathfrak{P}_S$ через $d(S)$. Это число является довольно тонким инвариантом поля k и простых дивизоров, составляющих множество S .

По порядку величины $d(S)$ близко числу элементов множества S . Точнее говоря, существуют такие две постоянные c_1 и c_2 , зависящие только от поля k , что

$$c_1 \leq d(S) - m \leq c_2,$$

где m обозначает число простых дивизоров, входящих в S , для которых $\zeta \in k_p$.

Особенно интересен случай, когда множество S пусто. Группу $\mathfrak{P}_S$ мы будем тогда обозначать просто через $\mathfrak{P}$. Она является, очевидно, группой Галуа максимального неразветвленного p -расширения поля k . Из теории полей классов следует, что все факторы ряда коммутантов группы $\mathfrak{P}$ конечны. Обрывается ли этот ряд, т.е. конечна ли группа $\mathfrak{P}$ — неизвестно. Этот вопрос составляет содержание так называемой проблемы p -башни.

Близкий случай, когда все простые дивизоры из S взаимно просты с p . Здесь тоже факторы ряда коммутантов конечны. Вопрос об обрыве ряда близок к тому же вопросу для группы $\mathfrak{P}$.

Аналогично тому, как мы поступали в теории полей алгебраических функций и в теории локальных полей, естественно попытаться найти соотношения, определяющие группы $\mathfrak{P}_S$. Удастся оценить сверху их число. Это можно сделать, пользуясь тем общим методом определения числа соотношений в p -группе, который был описан в §2. Определение числа соотношений связано, как мы видели, с решением некоторой задачи погружения. В нашем случае эта задача погружения поля, все критические простые дивизоры которого содержатся в S , в поле такого же типа. Исследуя эту задачу, можно получить следующий результат:

Число соотношений $r(\mathfrak{P}_S)$, определяющих группу $\mathfrak{P}_S$, удовлетворяет неравенству

$$r(\mathfrak{P}_S) \leq \gamma + m + c,$$

где γ обозначает число образующих p -компоненты группы классов поля k , m — число простых дивизоров в S , для которых $\zeta \in k_p$, а c — постоянная, зависящая только от степени $[k : R]$.

Например, для группы $\mathfrak{P}$ мы получаем неравенство

$$r(\mathfrak{P}) \leq \gamma + c.$$

Легко видеть, что $d(\mathfrak{P}) = \gamma$ так, что

$$r(\mathfrak{P}) \leq d(\mathfrak{P}) + c. \quad (3)$$

Из грубых теоретико-групповых соображений следует, что если для некоторого семейства p -групп G , $r(G) \leq d(G) + c$, где c — постоянная, то класс групп G стремится к бесконечности вместе с $d(G)$. Отсюда вытекает следующий результат:

Для полей k фиксированной степени класс группы $\mathfrak{P}$ неограниченно возрастает вместе с числом образующих p -компоненты группы классов поля k .

Шольц [10] построил некоторые примеры полей k , у которых группы $\mathfrak{P}$ имеют сколь угодно большой класс. Из предшествующего результата следует, что что на самом деле общая закономерность. Гипотезу (несколько более частного характера) высказывал Фрелих [11].

Возникает, однако, чувство, что число соотношений, удовлетворяющее неравенству (3), при $d(\mathfrak{P})$ достаточно большом, сравнительно с c , вообще слишком мало, чтобы определить конечную p -группу. Действительно, самая простая группа — прямое произведение d групп $\mathbf{Z}_p$ определяется $d(d+1)/2$ соотношениями

$$\sigma_i^p = 1, i = 1, \dots, d; \quad \sigma_i \sigma_j = \sigma_j \sigma_i \quad (1 \leq i < j \leq d).$$

В связи с этим мне кажется очень принципиальным следующий вопрос, к которому я хотел бы привлечь внимание специалистов по теории групп:

Каково наименьшее число соотношений, необходимое для того, чтобы определить конечную p -группу с d образующими?

Поставим этот вопрос точно. Определим функцию $\varrho(d)$ следующим образом:

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

где минимум берется по всем конечным группам, минимальное число образующих которых равно d . Речь идет об оценке снизу функции $\varrho(d)$ при росте d . Из рассмотрения факторгруппы по коммутанту следует, что $\varrho(d) \geq d$. Если бы можно было показать, что при $d \rightarrow \infty$

$$\varrho(d) - d \rightarrow \infty,$$

что мне кажется правдоподобным, то отсюда следовало бы отрицательное решение проблемы p -башни со всеми вытекающими из этого следствиями: существованием полей, не вкладывающихся в поля с однозначным разложением на множители, оценкой истинного порядка роста минимального дискриминанта полей алгебраических чисел и т.д. Так как $r(G) = \dim_{\mathbf{Z}_p} H^2(G, \mathbf{Z}_p)$, $d(G) = \dim_{\mathbf{Z}_p} H^1(G, \mathbf{Z}_p)$, то этот вопрос эквивалентен вопросу об оценке

порядка второй группы гомологий конечной p -группы при фиксированной первой группе гомологий.

В заключение заметим, что все сказанное относится также и к группам $\mathfrak{P}_S$, если все простые дивизоры множества S взаимно просты с p .

§4. Критические простые дивизоры алгебраических многообразий над полями алгебраических чисел

Вопросы, связанные с критическими простыми дивизорами полей алгебраических чисел, могут быть поставлены и для алгебраических многообразий, определенных над полями алгебраических чисел и приводят нас к интересным задачам и некоторым результатам.

До сих пор мы не формулировали определение критического простого дивизора расширения k'/k . Чтобы привести это определение, рассмотрим простой дивизор $\mathfrak{p}$ поля k , его локальное кольцо $\sigma_{\mathfrak{p}}$ и целое замыкание $\sigma'_{\mathfrak{p}}$ кольца $\sigma_{\mathfrak{p}}$ в k' . Кольцо $\sigma'_{\mathfrak{p}}/\mathfrak{p}$ является алгеброй над полем $k(\mathfrak{p}) = \sigma_{\mathfrak{p}}/\mathfrak{p}$. Если эта алгебра сепарабельна, то $\mathfrak{p}$ называется некритическим простым дивизором, в противном случае — критическим.

Рассмотрим теперь полное неособое алгебраическое многообразие X , определенное над полем алгебраических чисел k , и простой дивизор $\mathfrak{p}$ поля k . Редукция $X/\mathfrak{p}$ многообразия X по модулю $\mathfrak{p}$ (определение которой дано, например, в [12]) является алгебраическим множеством над полем $k(\mathfrak{p})$. $X/\mathfrak{p}$ может уже иметь особые точки. Это значит, что локальные кольца некоторых его точек не будут регулярными. В случае кольца $\sigma'_{\mathfrak{p}}/\mathfrak{p}$ условие регулярности локальных колец его простых идеалов совпадает с сепарабельностью. Это приводит нас к следующему определению: простой дивизор $\mathfrak{p}$ поля k называется некритическим для полного неособого многообразия X , определенного над k , если $X/\mathfrak{p}$ — неособое многообразие над полем $k(\mathfrak{p})$; в противном случае $\mathfrak{p}$ называется критическим. В [12] доказано, что X имеет только конечное число критических простых дивизоров.

Понятию критического простого дивизора удобно придать бирационально инвариантную форму, связав его с полем алгебраических функций, а не с многообразием X — моделью этого поля. Пусть K — поле рациональных функций на некотором полном неособом алгебраическом многообразии X , определенном над k . Простой дивизор $\mathfrak{p}$ поля k называется некритическим для поля K , если существует хотя бы одно неособое полное многообразие X' , для которого K является полем функций, а $\mathfrak{p}$ — некритическим простым дивизором в смысле предшествующего определения.

Одна из основных теорем алгебраических чисел, связанная с понятием дискриминанта — это теорема Эрмита, утверждающая, что число расширений k'/k с заданной степенью и с заданным дискриминантом конечно. Этой теореме можно придать следующую форму: число расширений k'/k заданной степени, критические простые дивизоры которых принадлежат заданному конечному множеству S , конечно.

В такой форме это утверждение может быть сформулировано, хотя бы как вопрос, для алгебраических многообразий любой размерности n или соответствующих полей алгебраических функций. Теорема Эрмита соответствует случаю $n = 0$. Мы рассмотрим следующий по сложности случай $n = 1$, т.е. случай алгебраических кривых или полей алгебраических функций K одной переменной. Мы будем считать, что поле K определено над полем алгебраических чисел k и что k алгебраически замкнуто в K . При этих предположениях имеет место следующий результат, аналогичный теореме Эрмита:

Существует конечное число полей алгебраических функций K/k заданного рода $g \neq 1$, критические простые дивизоры которых принадлежат заданному конечному множеству S .

Этот результат имеет место, если его надлежащим образом модифицировать, для полей рода $g = 1$. Для этого нужно, кроме рода, рассмотреть другой важный инвариант полей алгебраических функций рода 1 — общий наибольший делитель d степеней всех дивизоров поля, называемый показателем поля. Известно [13], что показатель может принимать сколь угодно большие значения. Если ограничиться рассмотрением полей рода 1 с заданным показателем d , то сформулированная выше теорема конечности остается верной. Например, при $k = R$ и в простейшем случае $d = 1$ (когда K является полем функций на эллиптической кривой) имеется 24 поля K с единственным критическим простым числом 2. Соответствующие эллиптические кривые задаются уравнениями:

$$y^2 = x(x^2 - a), \quad a = \pm 1, \pm 2, \pm 4, \pm 8.$$

$$y^2 = x(x - a\alpha)(x - a\alpha'), \quad a = \pm 1, \pm 2, \\ \alpha = 1 + \sqrt{-1}, \quad 1 + \sqrt{2}, \quad (1 + \sqrt{2})^2, \quad 2 + \sqrt{2}.$$

Можно ли рассчитывать на то, чтобы получить достаточно полную классификацию полей алгебраических функций одной переменной по их множествам критических простых дивизоров?

Простейший случай, когда род g поля K равен 0, говорит в пользу такого предположения. В этом случае, как известно, поле функций имеет в качестве модели кривую, задаваемую уравнением

$$ax^2 + by^2 = 1.$$

Эта модель определяется полем K однозначно с точностью до проективного преобразования. Классификация полей совпадает, следовательно, с классификацией тройничных квадратичных форм с точностью до линейной эквивалентности. Из теории квадратичных форм следует, что, во всяком случае, при $k = R$, поле рода 0 однозначно определяется множеством своих критических простых чисел. Совокупность всех полей, критические простые числа которых содержатся в заданном множестве $S = \{p_1, \dots, p_m\}$, образуют абелеву группу, изоморфную прямому произведению m групп $\mathbb{Z}_2$.

Второй фундаментальной теоремой теории алгебраических чисел, связанной с критическими простыми числами, является теорема Минковского, согласно которой всякое конечное расширение K/R поля рациональных чисел R имеет хотя бы одно критическое простое число. Было бы очень интересно выяснить, в какой мере этот результат обобщается на произвольные алгебраические многообразия. Вопрос в случае полей алгебраических функций одной переменной заключается в следующем:

Существуют ли поля алгебраических функций одной переменной с полем констант R , не имеющие критических простых чисел и отличные от поля рациональных функций $R(x)$?

Ответ на этот вопрос мне неизвестен. Для расширений произвольного поля алгебраических чисел k вопрос решается отрицательно. Больше того, существуют такие поля K алгебраических функций одной переменной, имеющие полем констант поле R , что для некоторого поля алгебраических чисел k поле $K \cdot k$ не имеет критических простых дивизоров над k . Примером является поле $R(x, y)$, где x и y связаны соотношением

$$x^3 + y^3 = 1,$$

если за k взять поле $R(\sqrt[3]{2}, \sqrt[3]{-3})$.

Можно получить более тонкие инварианты, чем только совокупность критических простых дивизоров, если вернуться от рассмотрения полей к рассмотрению отдельных моделей. Для описания этой ситуации удобно пользоваться языком схем [14]. Пусть K/k — расширение конечного типа поля алгебраических чисел k , а

X — схема над кольцом целых чисел σ поля k . Предположим, что схема X — целая, плоская и собственная над σ , что K является ее полем рациональных функций и что схема $X \otimes k$ (являющаяся алгебраическим многообразием над k) не особая. Понятие критического простого дивизора p схемы X определяется, как и раньше, путем рассмотрения схемы X/p . Но в этом случае критическим простым дивизорам p_i можно приписать некоторые кратности r_i и определить дискриминант схемы $D(X) = \prod p_i^{r_i}$. Не останавливаясь на том, как определяются числа r_i , скажу только, что это определение основывается на введенном Э.Келером [15] понятии дифференты (которая в этих терминах является замкнутой подсхемой схемы X), так же, как определение дискриминанта поля алгебраических чисел основывается на определении его дифференты.

Если поле K/k имеет степень трансцендентности 1, т.е. $X \otimes k$ является алгебраической кривой, то род поля K/k назовем родом схемы X . Имеет место следующий результат:

Существует только конечное число схем X заданного рода $g \neq 1$ (или рода 1 и заданного показателя d) с заданным дискриминантом.

Понятие дискриминанта схемы связано, по-видимому, и с другими вопросами арифметики алгебраических многообразий. Например, А.Нерон [16] доказал, что для $g = 1$ среди всех схем X , соответствующих одному и тому же полю K , имеется одна, в определенном смысле минимальная. Можно показать, что эта схема обладает минимальным дискриминантом. Если, как можно надеяться, теорема о существовании минимальной модели имеет место для случая произвольного рода $g > 0$, то эта минимальная модель будет также обладать минимальным дискриминантом.

§5. Сравнение с алгебраической геометрией

Вопросы об алгебраических кривых над полем алгебраических чисел k интересно сравнить с аналогичными вопросами для случая, когда k — поле алгебраических функций одной переменной, подобно тому, как мы уже делали в этом докладе в связи с другими вопросами теории алгебраических чисел.

Пусть k — поле алгебраических функций одной переменной с алгебраически замкнутым полем коэффициентов k_0 , являющееся полем рациональных функций на полной алгебраической кривой T . Рассмотрим, аналогично тому, как мы поступали в §4, поле алгебраических функций одной переменной K с полем коэффициентов k .

Так как K имеет над k_0 степень трансцендентности 2, то оно является полем рациональных функций на алгебраической поверхности X , которую можно считать неособой. Вложение поля k в K

определяет рациональное отображение $f : X \rightarrow T$. Пользуясь известными приемами теории алгебраических поверхностей, можно свести вопрос к случаю, когда отображение f регулярно. Таким образом, аналогом той ситуации, которая обсуждалась в §4, является регулярное отображение неособой алгебраической поверхности X на неособую алгебраическую кривую T . Для всех точек t кривой T , кроме, быть может, конечного числа их, прообраз $f^{-1}(t)$ будет неособой алгебраической кривой одного и того же рода g , равного роду поля K/k . Те точки, прообразы которых являются кривыми с особенностями, и служат аналогом критических простых дивизоров.

Мы будем называть их критическими точками.

Говоря другими словами, мы имеем расслоение поверхности X на семейство алгебраических кривых $f^{-1}(t)$. Критические точки соответствуют вырождающимся слоям, которые являются кривыми с особыми точками.

Обратимся к вопросу о полях без критических точек.

Таким полям будут соответствовать расслоения без вырожденных слоев. В нашем случае расслоения действительно существуют. Примером их являются прямые произведения $X = F \times T$ базисной кривой T на произвольную кривую F . Более общий класс примеров дают "постоянные" расслоения, у которых все слои бирегулярно эквивалентны друг другу. Эти расслоения являются алгебраическими расслоенными пространствами, локально тривиальными при $k_0 = \mathbb{C}$ и локально изотривиальными [17] при произвольном k_0 . Вопрос о полях без критических точек приобретает теперь следующую форму:

Совпадает ли всякое расслоение без вырожденных слоев, база T которого является проективной прямой, с "постоянным расслоением"?

Этому вопросу можно придать другую форму, если рассмотреть многообразие модулей M_g алгебраических кривых рода g . Сопоставляя слою $f^{-1}(t)$ ($t \in T$) точку, изображающую эту кривую в многообразии M_g , мы определим регулярное отображение проективной прямой T в M_g . Вопрос заключается в том, чтобы выяснить, существуют ли такие отображения, кроме отображений в точку. Их заведомо нет, если многообразие M_g аффинное, как это имеет место при $g = 2$ ¹.

Перейдем к рассмотрению расслоений, содержащих вырожденные слои. Здесь удобно (и, возможно, не теряя общности) ограни-

¹D. Mumford сообщил мне, что К. Kodaira построил пример не "постоянного" расслоения без вырожденных слоев с базой, отличной от проективной прямой.

читаться рассмотрением минимальных расслоений, т.е. таких расслоений $X \xrightarrow{f} T$, что не существует расслоения $X' \xrightarrow{f'} T$ и такого регулярного бирационального отображения $g : X \rightarrow X'$, что треугольник

$$\begin{array}{ccc} X & \xrightarrow{g} & X' \\ f \searrow & & \swarrow f' \\ & T & \end{array}$$

коммутативен.

Вопросу о полях с заданными критическими точками может быть придана следующая форма:

Конечно ли число расслоений на кривые заданного рода $g \neq 1$, если фиксирована базисная кривая T и множество S критических точек расслоения?

В ряде частных случаев (например, если все слои гипер-эллиптические) можно показать, что этот вопрос имеет положительный ответ. Доказательство в общем случае должно быть, по-видимому, значительно труднее доказательства аналогичного факта для кривых над полями алгебраических чисел, аналогично тому, как конечность числа расширений с заданными точками ветвления поля алгебраических функций доказывается гораздо сложнее [18], чем теорема Эрмита в теории алгебраических чисел. В связи с этим было бы интересно исследовать этот вопрос в случае $k_0 = \mathbb{C}$, пользуясь топологическими методами.

В §1 мы видели, что при $k_0 = \mathbb{C}$ классификация конечных расширений поля алгебраических функций может быть сведена к топологической классификации накрытий.

Связи, которые существуют между теорией регулярных отображений алгебраических поверхностей на алгебраические кривые и соответствующей топологической задачей — теорией дифференцируемых отображений четырехмерных дифференцируемых многообразий на двумерные — по-видимому, совсем не исследованы. Здесь возникают три вопроса:

Какова классификация дифференцируемых отображений четырехмерных многообразий на двумерные?

Какие дифференцируемые отображения четырехмерного многообразия на алгебраическую кривую реализуются как регулярные отображения алгебраических поверхностей на эту кривую?

Могут ли два различных регулярных отображения алгебраической поверхности на алгебраическую кривую быть диффеоморфными?

Последний вопрос аналогичен тому, который Г.Граuert [19] решил в положительную сторону для расслоений с векторным слоем

над многообразием Штейна.

Заключение

В этом докладе я не ставил своей целью дать сколько-нибудь полный обзор результатов, полученных в последнее время в теории алгебраических чисел. Здесь рассмотрен только один круг идей в теории полей алгебраических чисел и собраны примыкающие к этим идеям результаты и проблемы в самой теории алгебраических чисел и в близких к ней областях.

ЛИТЕРАТУРА

1. Grothendieck A., *Géométrie formelle et géométrie algébrique*, Séminaire Bourbaki Mai, 1959, 182, 1—28.
2. Шафаревич И. Р., *О p -расширениях*, Математический сборник 20, 2 (1947), 351—363.
3. Kawada J., *On the structure of the Galois group of some infinite extensions. I*, J. Fac. Sci Univ. Tokyo Sec. I, 7, 1 (1954), 1—18.
4. Фаддеев Д. К., Скопин А. И., *К доказательству одной теоремы Кавада*, Доклады АН СССР 127, 3 (1959), 529—530.
5. Zassenhaus H., *Lehrbuch der Gruppentheorie*, Leipzig, 1937.
6. Brauer R., *Über die Konstruktion der Schiefkörper, die von endlichem Rang in Bezug auf ein gegebenes Zentrum sind*, J. reine angew. Math. 168, 1 (1932), 44—64.
7. Демущкин С. П., *Группа максимального p -расширения локального поля*, Известия Акад. наук СССР, серия матем. 25, 3, 329—346.
8. Koch H., *Über galoissche Erweiterungen p -adischer Zahlkörper*, J. reine angew. Math. 209, 1—2 (1962), 9—12.
9. Гаусс К. Ф., *Арифметические исследования*, К. Ф. Гаусс, Труды по теории чисел, Москва, 1959.
10. Scholz A., *Zwei Bemerkungen zum Klassenkörperturm*, J. reine angew. Math. 161, 4 (1929), 201—208.
11. Fröhlich A., *A note on the class field tower*, Quart. J. Math. (Oxford), 5 5 (1954), 141—144.
12. Shimura G., *Reduction of algebraic varieties with respect to a discrete valuation of the basic field*, Amer. J. Math. 77, 1 (1955), 134—176.
13. Шафаревич И. Р., *Показатели эллиптических кривых*, Доклады АН СССР 114, 4 (1957), 714—716.
14. Grothendieck A. & Dieudonné J., *Eléments de géométrie algébrique*, I. Publ. Math., (I.H.E.S.), Paris, 8.
15. Kähler E., *Geometria arithmetica*, Ann. Mat. Pura Appl. Ser. IV, 45 (1958), 1—399.
16. Néron A., *Modèles p -minimaux des variétés abéliennes*, Bourbaki Décembre (1961, 227), 1—16.
17. Serre J.-P., *Espaces fibrés algébriques*, Séminaire C. Chevalley Exp. 1 (1958), École Normale Supérieure, 1—37.

-
18. Lang S. & Serre J.-P., *Sur les revêtements non ramiliés des variétés algébriques*, Amer. J. Math. **79**, 2 (1957), 319—330.
 19. Grauert H., *Analytische Faserungen über holomorph-vollständige Räume*, Math. Ann. **135** (1958), 263, 273.

РАСШИРЕНИЯ С ЗАДАНЫМИ ТОЧКАМИ ВЕТВЛЕНИЯ

PUBL. MATH. INST. HAUT. ETUD. SCI. 18, (1964) 295-319

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 $\mathfrak{p} \in S$. 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 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 $\mathfrak{G}_S/\mathfrak{G}_S^{(1)}$, $\mathfrak{G}_S^{(1)} = \mathfrak{G}_S^l(\mathfrak{G}_S, \mathfrak{G}_S)$. 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 $p \in S$. 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

$$\mathcal{U}_S = \{a | a_p \in \mathcal{U}_p, \quad a = 1 \text{ для } p \in S\}.$$

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

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

(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 $\zeta \in k_p$,

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

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 $\mathcal{U}_S J^l k$ и

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

Положим

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

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

Рассмотрим последовательность групп и гомоморфизмов:

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

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

f_1 — естественное отображение группы на факторгруппу

$$H = H_S/(\mathfrak{U} \cdot J^l \cdot k/\mathfrak{U}_S J^l k)$$

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

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 идеаль $\mathfrak{a}$, 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 идеала $\mathfrak{a}$. От этого выбора $f_3(\alpha)$ не зависит, так как, если

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

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

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

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

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

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

$$\text{Ker } F_2 = \text{Im } f_3$$

Наконец,

$$\text{Ker } f_3 = \{\alpha | \alpha \in V, \quad \alpha \in J^l \mathfrak{U}_S\} = \text{Im } f_4$$

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).

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

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 $(\alpha) = \mathfrak{a}^l$ и отображение $\varphi_1 : \alpha \rightarrow \mathfrak{a}$ 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:

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

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 бикompактная 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 $\mathfrak{F}_1 = \mathfrak{F}^l(\mathfrak{F}, \mathfrak{F})$, $\mathfrak{G}_1 = \mathfrak{G}^l(\mathfrak{G}, \mathfrak{G})$. 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 $\text{Ext}(\mathfrak{G}, Z_l)$, 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

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

Очевидно, что последовательность

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

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

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

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

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

Таким путем определяется отображение

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

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

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

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

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

Если мы положим

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

то получим, что

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

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

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

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

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

определяет элемент

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

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

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

(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

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

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_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 $\bar{K}$

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

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

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

Мы будем говорить о K -задаче погружения, если фиксировано расширение K/k и требуется найти $\bar{\bar{K}}$ 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 $\text{Hom}(\mathfrak{a}_K, Z_l)$, где $\mathfrak{a}_K$ — группа Галуа максимального абелевого расширения поля K . Наоборот, каждый элемент χ группы $\hat{\mathfrak{a}}_K = \text{Hom}(\mathfrak{a}_K, Z_l)$ определяет некоторое поле — то, которое соответствует подгруппе $\text{Ker } \chi$ группы $\mathfrak{a}_K$ и гомоморфизм группы Галуа этого поля в Z_l . Таким образом, “расширения” в смысле этой новой структуры совпадают с элементами группы $\hat{\mathfrak{a}}_K = \text{Hom}(\mathfrak{a}_K, Z_l)$. Такая трактовка имеется, например, еще в работе [8]. Нам важно сейчас, что групповая операция переносится, таким образом, с группы $\mathfrak{a}_K = \text{Hom}(\mathfrak{a}_K, Z_l)$ 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 $K \otimes k_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} K_{\mathfrak{P}}$. 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 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 $K_{\mathfrak{P}}/k_p$, $\mathfrak{P}|p$ 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 $p \nmid l$ 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 $\overline{K}/k$, 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 $\overline{K}$ — одно решение задачи погружения, то любое другое решение имеет вид $\overline{K} = \overline{K} \circ K_0$, 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 неразветвлен-

ное 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 $K_0 = K_p \cdot \hat{k}_p$ — тривиальное расширение, а $\hat{k}_p/k_p$ — расширение с группой Галуа, изоморфной Z_l или 1 (утверждение 4). Как всякое расширение поля k_p , $\hat{k}_p$ соответствует элементу φ группы $\text{Hom}(\mathfrak{a}_{K_p}, Z_l)$. Согласно локальной теории полей классов $\text{Hom}(\mathfrak{a}_{K_p}, Z_l) = \text{Hom}(k_p, Z_l) = \hat{k}_p$. 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_l или 1. Такому расширению соответствует элемент $\varphi_0 \in \hat{k}_p$, обладающий свойством $\varphi_0|_{\mathfrak{u}_p} = 1$.

Мы видим, что φ определен с точностью до множителя такого типа. Иными словами, однозначно определен характер $\psi \in \text{Hom}(\mathfrak{u}_p, Z_l) = \hat{\mathfrak{u}}_p$. 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 $\hat{\mathfrak{u}}_p$. 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 $\psi \in \hat{\mathfrak{u}}_p$, 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 $\prod_{p \notin S} \hat{\mathfrak{u}}_p = \hat{\mathfrak{u}}_S$. 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 $\text{Hom}(J/k, Z_l) = \widehat{J/k}$. Если $\bar{\psi} \in \widehat{J/k}$, то соответствующие $\bar{\psi}_p \in \hat{\mathfrak{u}}_p$ получаются, очевидно, из вложения $\mathfrak{u}_p \rightarrow J/k$. Мы имеем, таким образом, стандартные гомоморфизмы:

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

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 $\psi \in \text{Im } \hat{\varphi}$.

Очевидно, что элемент $\psi \cdot \text{Im } \hat{\varphi}$ группы $\hat{\mathcal{U}}_S / \text{Im } \hat{\varphi} = \text{Coker } \hat{\varphi}$ 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 $\psi(\xi) \in \hat{\mathcal{U}}_S / \text{Im } \hat{\varphi} = \text{Coker } \hat{\varphi}$, 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 $\text{Coker } \hat{\varphi}$.

§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

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

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

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

если $S = \emptyset$, $\zeta \in k$.

Доказательство. Согласно теореме 2

$$r(S) = \text{Sup}_\alpha \dim_{Z_1} E(G_\alpha) / E(G_\alpha)^0.$$

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

$$\dim_{Z_1} E(G_\alpha) / E(G_\alpha)^0 = \dim_{Z_1} E(G_\alpha) / \widetilde{E(G_\alpha)} + \dim_{Z_1} \widetilde{E(G_\alpha)} / E(G_\alpha)^0. \quad (11)$$

Согласно теореме 3 существует $t(S) - \delta$ гомоморфизмов группы $E(G_\alpha)$ в Z_1 , пересечение ядер которых совпадает с $\widetilde{E(G_\alpha)}$. Отсюда следует, что

$$\dim_{Z_1} E(G_\alpha) / \widetilde{E(G_\alpha)} \leq t(S) - \delta, \quad (12)$$

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

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

в которой гомоморфизм f определен формулой:

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

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 $\mathfrak{a}$ в этом разложении.

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

Отсюда следует, что $\alpha \in V_S$ и $i = f(\alpha)$. Если же $f(\alpha) = 1$, то в равенстве $\alpha = i\alpha^l$ 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. $\mathfrak{G}$ 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, а 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 $\mathfrak{p}_\infty$. Примером такого поля является поле рациональных чисел R . Возьмем за S множество, состоящее из двух простых дивизоров l и $\mathfrak{p}_\infty$.

В этом случае $t(S) = 2$, $\delta = 1$ и так же, как и в случае 1, $\delta(S) = 0$. 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 $\mathfrak{G}_S/(\mathfrak{G}_S, \mathfrak{G}_S)$ 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 p_∞ . Обозначим той же буквой σ изоморфизм поля всех алгебраических чисел в поле всех комплексных чисел $\mathbb{C}$, продолжающий этот изоморфизм поля k . Наконец, через τ обозначим автоморфизм поля $\mathbb{C}$, 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 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. Маркштайсом [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 $\zeta \notin k$ 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 $\zeta \notin k$. 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

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

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

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

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

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

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

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:

¹Если 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 $l = 2$, $n = 2$, $k = m = 1$).

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

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

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 $\mathfrak{G}_S/\mathfrak{G}_S^{(2)}$ 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 $h(G) \leq h$

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

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 разрешимости 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 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 $R(\sqrt{\mathcal{D}})$, 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 $[k : R] = l$. Для k , как легко видеть, $\gamma \geq t - 1$. Это следует из того, что все поля $k_i k / k$ 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 независимыми 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 $s = 2^h$. 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 s , 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).

I. 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. $N \subset F_2$. 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

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

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

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

Из **A** 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

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

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

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

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

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

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

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

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

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

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

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

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 $\mathfrak{F}_{c+1}$:

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

то существовала бы зависимость с теми же коэффициентами

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

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

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

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 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.

I. 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

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

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 обрывается².

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]³ приведен пример замкнутой группы с тремя образующими. В связи с этим возникает следующий вопрос:

² Другое доказательство этого утверждения о связи между гипотезой (27) и проблемой башни полей классов, опирающееся на результаты работы [23], см. в [22].

³ На эту работу внимание автора обратил J.-P. Serre.

II. Существуют ли замкнутые группы со сколь угодно большим числом образующих? В частности, существуют ли замкнутые группы более, чем с тремя образующими?

Замкнутыми группами являются, конечно, циклические группы

$$Z_{l^n}, \quad n \geq 1,$$

группы обобщенных кватернионов

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

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

и группы

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

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

(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]⁴).

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:

$$bab^{-1} = a^{1+l^m}, \quad b^{l^n} = a^{l^k}, \quad (31)$$

⁴Эту работу автору указал J.Browkin.

$$m \leq k \leq n.$$

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]⁵) примеры замкнутых групп. Интересно было бы знать, каковы замкнутые группы с двумя образующими, другими словами:

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 $k = R$, $l > 2$, $S = \{p_1, p_2\}$

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

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 $R(\sqrt{-4027})$ и $R(\sqrt{-3299})$. 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.

⁵Эту работу указал автору А.И.Кострикин.

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. **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 **127** N 3 (1959), 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. **50** (1949), 736–761.
8. C. Chevalley, *La théorie du corps de classes*, Ann. of Math. **41** (1940), 391–418.
9. A. Scholtz, *Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung. I.*, Math. Zeitschrift **42** (1936), 161–188.
10. H. Reichardt, *Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung*, J. reine und angew. Math. **177** (1937), 1–5.
11. И. Р. Шафаревич, *О p -расширениях*, Матем. сб. **20** (62) N 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. **168** (1932), 44–64.
13. Г. Н. Маркшайтис, *О p -расширениях с одним критическим простым числом*, Известия Ака. Наук СССР, серия матем. **27** N 2 (1963).
14. W. Magnus, *Beziehungen zwischen Gruppen und Idealen in einem speziellen Ring*, Math. Ann. **III** (1935), 259–284.
15. А. И. Скопин, *Факторгруппы одного верхнего центрального ряда*, Доклады Ака. Наук СССР **LXXIV**, 13 (1950), 425–428.
16. J. Schur, *Untersuchungen über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine und angew. Math. **132** (1907), 85–137.
17. J. Mennicke, *Einige Gruppen mit drei Erzeugenden und drei Relationen*, Archiv der Math. **10** (1959), 409.
18. С. П. Демупкин, *Группа максимального расширения локального поля*, Известия Акад. Наук СССР, серия матем. **25**, N 3 (1961), 329–346.
19. I. D. Macdonald, *On a class of finitely presented groups*, Canadian Journ. of Math. **XIV** (1962), 602–614.
20. A. Frölich, *On fields of class two*, Proc. Lond. Math. Soc. **IV** (1954), 235–256.
21. A. Scholtz und O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginärquadratischer Zahlkörper*, J. reine und angew. Math. **171** (1934), 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), **35** (1956), 189–192.
24. B. Neumann, *On some finite groups with trivial multiplier*, Publ. Math. Debrecen **4** (1956), 190–194.

Поступило 6 марта 1963 г.

О БАШНЕ ПОЛЕЙ КЛАССОВ

(С Е. С. ГОЛОДОМ)

ИЗВ. АКАД. НАУК СССР, СЕР. МАТЕМ., 28 (1964), 261–272

В работе доказывается существование бесконечных неразветвленных расширений полей алгебраических чисел и полей, которые не могут быть вложены в одноклассные.

Введение

Одним из авторов было доказано, что проблема башни полей классов имеет отрицательное решение, если верна следующая гипотеза:

$$r(G) - d(G) \rightarrow \infty,$$

где $d(G)$ и $r(G)$ – минимальное число образующих и число соотношений, определяющих группу G , а предел берется по всем конечным p -группам (см. [3] и [4]; другое изложение см. в [2]). При этом число соотношений понимается в смысле теории про- p -групп (см. §1).

В настоящей работе мы доказываем эту гипотезу, точнее для любой конечной p -группы G доказывается неравенство

$$r(G) > \left(\frac{d(G) - 1}{2} \right)^2.$$

Доказательство этого утверждения сводится к доказательству аналогичного утверждения о некоммутативных локальных кольцах. Эта редукция проведена в §1.

§2 содержит доказательство теоремы о p -группах.

Наконец, в §3 мы резюмируем следствия, относящиеся к теории алгебраических чисел.

Лемма 1 и построение комплекса M , содержащиеся в п. 3 §2, принадлежат И. Р. Шафаревичу, леммы 2 и 3 – Е. С. Голоду.

Авторы глубоко благодарны С. П. Демушкину, беседы с которым чрезвычайно стимулировали эту работу.

§1. Редукция к локальным кольцам

Напомним сначала некоторые определения и простые факты, изложение которых можно найти в работе [2].

Про- p -группой называется группа, которая является проективным пределом конечных p -групп.

Групповым кольцом про- p -группы называется проективный предел групповых колец ее конечных фактор-групп.

Групповое кольцо про- p -группы $\mathfrak{G}$ над полем Z_p из p элементов (только этот случай и будет дальше рассматриваться) будет обозначаться через $Z_p[\mathfrak{G}]$. Это кольцо нульмерно и компактно. Имеется каноническое вложение $\mathfrak{G} \rightarrow Z_p[\mathfrak{G}]$, пользуясь которым мы будем отождествлять элементы $\mathfrak{G}$ с соответствующими элементами $Z_p[\mathfrak{G}]$.

Кольцо $Z_p[\mathfrak{G}]$ имеет единственный максимальный идеал, порожденный элементами вида $1 - \sigma$, $\sigma \in \mathfrak{G}$. Таким образом, оно является локальным кольцом.

Сопоставление про- p -группе $\mathfrak{G}$ группового кольца $Z_p[\mathfrak{G}]$ является функтором из категории про- p -групп в категорию компактных локальных колец.

Свободной про- p -группой с d образующими (d – натуральное число) называется группа $\mathfrak{F}_d$, которая является проективным пределом p -фактор-групп свободной группы с d образующими. Любая про- p -группа $\mathfrak{G}$ с d образующими представима в виде $\mathfrak{F}_d/\mathfrak{N}$, где $\mathfrak{N}$ – замкнутый нормальный делитель группы $\mathfrak{F}_d$. Если выбрать представление $\mathfrak{G} = \mathfrak{F}_d/\mathfrak{N}$, при котором образующие $\sigma_1, \dots, \sigma_d$ группы $\mathfrak{F}_d$ переходят в минимальную систему образующих группы $\mathfrak{G}$, то

$$\mathfrak{N} \subset \mathfrak{F}_d^p(\mathfrak{F}_d, \mathfrak{F}_d),$$

где $(\mathfrak{F}_d, \mathfrak{F}_d)$ – коммутатор группы $\mathfrak{F}_d$, а $\mathfrak{F}_d^p$ – ее подгруппа, порожденная p -ми степенями ее элементов.

Обозначим через O_d кольцо формальных степенных рядов от d некоммутативных переменных $x_1, \dots, x_d$ с коэффициентами в Z_p . Это локальное кольцо с максимальным идеалом $I = (x_1, \dots, x_d)$. Множество $1 + I$ является группой, которую мы обозначим через O_d^+ .

Отображение

$$\mu: \mathfrak{F}_d \rightarrow O_d,$$

заданное условиями

$$\mu\sigma_i = 1 + x_i,$$

определяет гомоморфизм группы $\mathfrak{F}_d$ в группу O_d^+ . Этот гомоморфизм является вложением и даже определяет изоморфизм

$$\bar{\mu}: Z_p[\mathfrak{F}_d] \rightarrow O_d.$$

Доказательство следует из того, что наряду с естественно определяемым гомоморфизмом $\bar{\mu} : Z_p[\mathfrak{F}_d] \rightarrow O_d$ легко строится и обратный гомоморфизм $\nu : O_d \rightarrow Z_p[\mathfrak{F}_d]$, определяемый тем, что

$$\nu(x_i) = \sigma_i - 1.$$

Очевидно, что для $\sigma \in \mathfrak{F}_d$ $\mu\sigma \in O_d^+$.

Кроме этих общеизвестных фактов, нам понадобится следующий простой результат.

ЛЕММА 1. Пусть про- p -группа $\mathfrak{G}$ представлена в виде

$$\mathfrak{G} = \mathfrak{F}_d/\mathfrak{N}, \quad (1)$$

где нормальный делитель $\mathfrak{N}$ порожден элементами $\varphi_1, \dots, \varphi_r \in \mathfrak{F}_d$.

Положим

$$\mu\varphi_i = 1 + f_i, \quad (f_1, \dots, f_r) = \mathfrak{A}, \quad (2)$$

$$O_d/\mathfrak{A} = A. \quad (3)$$

Тогда алгебры A и $Z_p[\mathfrak{G}]$ изоморфны.

Доказательство. Обозначим через π гомоморфизм $\mathfrak{F}_d \rightarrow \mathfrak{G}$, соответствующий представлению (1), а через λ – гомоморфизм $O_d \rightarrow A$, соответствующий представлению (3), и покажем, что можно построить такой гомоморфизм $\tau : \mathfrak{G} \rightarrow A^*$ (группу обратимых элементов A), чтобы диаграмма

$$\begin{array}{ccc} & \mathfrak{F}_d & \\ \pi \swarrow & & \downarrow \lambda \circ \mu \\ \mathfrak{G} & & A \\ & \searrow \tau & \end{array} \quad (4)$$

была коммутативна.

Для этого достаточно проверить, что

$$(\lambda \circ \mu)\mathfrak{N} = 1.$$

Но это очевидно, так как все элементы из $\mathfrak{N}$ являются пределами произведений элементов вида $\psi^{-1}\varphi_i^{\pm 1}\psi$, $\psi \in \mathfrak{F}_d$, $\lambda \circ \mu$ – непрерывный гомоморфизм, а $(\lambda \circ \mu)\varphi_i = 1$ ввиду (2).

Гомоморфизм τ определяет гомоморфизм колец:

$$\bar{\tau} : Z_p[\mathfrak{G}] \rightarrow A,$$

про который мы и докажем, что он является изоморфизмом. Гомоморфизм π определяет гомоморфизм колец

$$\bar{\pi}: Z_p[\mathfrak{F}_d] \rightarrow Z_p[\mathfrak{G}],$$

причем диаграмма

$$\begin{array}{ccc} & Z_p[\mathfrak{F}_d] & \\ \bar{\pi} \swarrow & & \downarrow \lambda \circ \bar{\mu} \\ Z_p[\mathfrak{G}] & & A \\ \searrow \bar{\tau} & & \end{array}$$

коммутативна. Гомоморфизм $\bar{\tau}$ эпиморфен, так как $\lambda \circ \bar{\mu}$ эпиморфен. Чтобы убедиться, что $\bar{\tau}$ – изоморфизм, достаточно проверить, что

$$\text{Ker}(\lambda \circ \bar{\mu}) \subset \text{Ker } \bar{\pi}.$$

Но идеал $\text{Ker}(\lambda \circ \bar{\mu})$ порождается элементами $\nu f_i = \varphi_i - 1$, а

$$\bar{\pi}(\varphi_i - 1) = \bar{\pi}(\varphi_i) - 1 = 0.$$

Лемма доказана.

Немного отклоняясь от общепринятой терминологии, мы будем называть алгебру A с единицей нильпотентной, если она конечного ранга над основным полем k и $A/\mathfrak{m} = k$, где $\mathfrak{m}$ – радикал A . Минимальное число образующих d алгебры A совпадает с $\dim_k \mathfrak{m}/\mathfrak{m}^2$. Очевидно, что существует представление $A = O_d/\mathfrak{A}$. Число образующих идеала $\mathfrak{A}$ мы будем называть числом соотношений A . Как известно из теории локальных колец, образующие $\bar{x}_i = x_i \bmod \mathfrak{A}$ тогда и только тогда составляют минимальную систему образующих алгебры A , когда $\mathfrak{A} \subset I^2$.

Следствие. Если существует конечная p -группа G с минимальной системой из d образующих, определенная r соотношениями, то существует нильпотентная алгебра A над Z_p , имеющая минимальную систему из d образующих и определенная r соотношениями.

Мы возьмем за A алгебру $Z_p[G]$. Если G имеет минимальную систему из d образующих $\sigma_1, \dots, \sigma_d$ и определена r соотношениями, то A имеет систему из d образующих $(1 - \sigma_i)$. Так как $\mathfrak{N} \subset \mathfrak{F}_d^p(\mathfrak{F}_d, \mathfrak{F}_d)$, то $\mathfrak{A} \subset I^2$, и, значит, система образующих $1 - \sigma_i$ минимальная. Согласно лемме 1, алгебра A определена r соотношениями.

§2. О числе образующих и соотношений p -группы

Нашей целью является доказательство следующих результатов.

ТЕОРЕМА 1. Если конечная p -группа G с минимальным числом образующих d определена r соотношениями, то $r > \left(\frac{d-1}{2}\right)^2$.

При этом мы говорим, что группа G определена r соотношениями, если она имеет представление

$$G = \mathfrak{F}_d / \mathfrak{N}, \quad (5)$$

где $\mathfrak{N}$ – нормальный делитель свободной про- p -группы $\mathfrak{F}_d$, порожденной (топологически) r элементами. Очевидно, если имеется представление $G = F_d/N$, где F_d – дискретная свободная группа, а нормальный делитель N порожден r элементами, то, переходя к пополнениям, мы получим представление (5), так что теорема 1 тем более верна при обычном (нетопологическом) задании группы соотношениями.

ТЕОРЕМА 2. Если нильпотентная алгебра A над некоторым полем k имеет минимальную систему из d образующих и определена r соотношениями, то $r > \left(\frac{d-1}{2}\right)^2$.

Очевидно, что ввиду следствия леммы 1, теорема 1 непосредственно следует из теоремы 2. Доказательство теоремы 2 вытекает из ряда вспомогательных предложений.

1. Рассмотрим представление A в виде $O_d/\mathfrak{A}$. Филътрация в O_d , определенная степенями идеала $I = (x_1, \dots, x_d)$, определяет филътрацию $\mathfrak{m}^n$ в A . Пусть

$$\hat{A} = \sum_{n=0}^{\infty} \mathfrak{m}^n / \mathfrak{m}^{n+1}$$

– присоединенная алгебра. Как градуированная алгебра она является фактором кольца многочленов R_d от некоммутативных переменных $x_1, \dots, x_d$ по идеалу $\hat{\mathfrak{A}}$, порожденному начальными формами элементов из $\mathfrak{A}$. Идеал $\hat{\mathfrak{A}}$ содержится в идеале $\bar{\mathfrak{A}}$, порожденном всеми однородными составляющими образующих идеала $\mathfrak{A}$. Для доказательства теоремы 2 достаточно, очевидно, доказать, что при $r \leq \left(\frac{d-1}{2}\right)^2$ градуированная алгебра $\bar{A} = R_d/\bar{\mathfrak{A}}$ бесконечномерна. Если алгебра A определена r соотношениями $f_1, \dots, f_r \in I^2 \subset O_d$, то базис идеала $\bar{\mathfrak{A}}$ состоит из r форм степени 2, r форм степени 3 и т. д. (некоторые из них могут быть равными нулю). То, что

фактор-алгебра $R_d/\overline{\mathfrak{A}}$ по такому идеалу $\overline{\mathfrak{A}}$ всегда бесконечномерна, будет доказано в лемме 5.

2. Пусть A – градуированная алгебра над полем k и $A = \sum_{n=0}^{\infty} A_n$ – ее разложение на однородные составляющие. Предположим, что числа

$$b_n = \dim_k A_n, \quad n \geq 0,$$

все конечны. Функция

$$P_A(t) = \sum_{n=0}^{\infty} b_n t^n$$

называется функцией Пуанкаре алгебры A .

3. Резольвента градуированной алгебры. Дальнейшие рассуждения используют конструкцию некоторого вспомогательного комплекса M , являющегося некоммутативным аналогом комплекса Козюля в локальной алгебре.

Предположим, что задана конечная или бесконечная последовательность однородных многочленов $f_1, f_2, \dots$ степеней ≥ 2 в кольце R_d , причем в этой последовательности имеется только конечное число многочленов заданной степени i . Это число обозначим через r_i ($i \geq 2$). При этом некоторые из многочленов f_i могут быть равны нулю, однако им все равно должна быть приписана определенная степень. Таким образом, 0 может встречаться в нашей последовательности бесконечное число раз, но только на некотором числе мест ему может приписываться заданная степень.

Обозначим через $\mathfrak{A}$ идеал кольца R_d , порожденный всеми формами f_i ($i = 1, 2, \dots$), и положим $A = R_d/\mathfrak{A}$. Очевидно, что A – градуированная алгебра. Рассмотрим последовательность переменных $u_1, u_2, \dots$, находящихся во взаимно однозначном соответствии с формами $f_1, f_2, \dots$, и обозначим через M алгебру некоммутативных полиномов от $x_1, \dots, x_d, u_1, u_2, \dots$ с коэффициентами из k .

Базис алгебры M над k состоит, следовательно, из выражений вида

$$a_0 u_{i_1} a_1 u_{i_2} \dots a_{k-1} u_{i_k} a_k, \quad (6)$$

где $a_0, \dots, a_k$ пробегает все одночлены от $x_1, \dots, x_d$.

Размерностью одночлена в M назовем число входящих в него переменных u_i . Таким образом, (6) – общий вид одночлена размерности k . Линейное пространство всех однородных многочленов размерности k обозначим через $M^{(k)}$. Очевидно, что $M = \sum_{k=0}^{\infty} M^{(k)}$ и M превращается таким способом в градуированную алгебру.

Определим в M дифференциал ∂ , положив $\partial x_i = 0$, $\partial u_i = f_i$ и продолжив его так, чтобы выполнялась обычная формула:

$$\partial(v \cdot w) = \partial v \cdot w + (-1)^m v \cdot \partial w,$$

где m — размерность v . В явном виде этот дифференциал задается так:

$$\partial(a_0 u_{i_1} \dots a_{k-1} u_{i_k} a_k) = \sum_{l=1}^k (-1)^l a_0 u_{i_1} \dots a_{l-1} f_{i_l} a_l \dots u_{i_k} a_k. \quad (7)$$

Легко проверить, что $\partial^2 = 0$ и что ∂ уменьшает размерность на 1.

Очевидно, что $H_0(M) = A$ и ∂ определяет последовательность гомоморфизмов R_d -модулей

$$0 \leftarrow A \leftarrow M^{(0)} \xleftarrow{\partial} M^{(1)} \xleftarrow{\partial} M^{(2)} \leftarrow \dots,$$

которая точна в членах A и $M^{(0)}$ и, вообще говоря, не точна в других членах, т. е., вообще говоря, эта резольвента алгебры A не является ациклической.

Введем понятие степени элемента из M , приписав x_i степень 1, а u_i — степень n_i , где n_i — степень формы f_i . Ввиду этого условия дифференциал не меняет степени.

Обозначим через M_n совокупность всех однородных многочленов степени n . Очевидно, что M_n — векторное пространство над k , размерность которого конечна ввиду того, что существует только конечное число форм f_i заданной степени. Ясно, что $M = \sum_{n=0}^{\infty} M_n$ и что таким образом мы определяем другую градуировку в M .

Положим $M_n^{(k)} = M_n \cap M^{(k)}$. Очевидно, что $M_n = \sum M_n^{(k)}$ и M_n является подкомплексом в комплексе M . Наконец, градуировка $A = \sum_{n=0}^{\infty} A_n$ совпадает с градуировкой

$$H_0(M) = \sum_{n=0}^{\infty} H_0(M_n),$$

т. е.

$$\dim_k H_0(M_n) = \dim_k A_n = b_n.$$

4. ЛЕММА 2. В предложениях п. 3

$$P_A(t) \left(1 - dt + \sum_{i=2}^{\infty} r_i t^i \right) \geq 1,$$

причем неравенство между степенными рядами понимается покомпонентно.

Доказательство. Если $n \geq 1$, то в M_n содержится подкомплекс $\sum_{i=1}^d M_{n-1} x_i$, изоморфный (как комплекс) комплексу M_{n-1}^d — сумме d экземпляров комплекса M_{n-1} . Положим

$$M_n / \sum_{i=1}^d M_{n-1} x_i = \widetilde{M}_n.$$

Каждый одночлен в M_n имеет в качестве крайнего правого множителя или некоторое x_i , или некоторое u_j . Поэтому как векторное пространство мы можем отождествить $\widetilde{M}_n$ с $\sum_{n_i \leq n} M_{n-n_i} u_i$, причем, ввиду условия на степени форм f_i , сумма будет конечной.

Найдем действие ∂ в $\widetilde{M}_n$. Если в члене (6) $a_k = 1$, $u_{i_k} = u_i$, то этот член входит в $M_{n-n_i} u_i$. В формуле (7) последнее k -е слагаемое содержится в $\sum_{i=1}^d M_{n-1} x_i$ и поэтому равно 0 в $\widetilde{M}_n$. Оставшаяся часть формулы (7) совпадает с формулой для дифференциала члена $a_0 u_{i_1} a_1 \dots u_{i_{k-1}} a_{k-1}$ размерности $k-1$. Таким образом, мы имеем изоморфизм комплексов

$$\widetilde{M}_n^{(k)} \simeq \sum_{n_i \leq n} M_{n-n_i}^{(k-1)}.$$

В частности,

$$H_0(\widetilde{M}_n) = 0, \quad H_q(\widetilde{M}_n) = \sum_{n_i \leq n} H_{q-1}(M_{n-n_i}). \quad (8)$$

Из точной последовательности комплексов

$$0 \rightarrow \sum_{i=1}^d M_{n-1} x_i \rightarrow M_n \rightarrow \widetilde{M}_n \rightarrow 0$$

следует точная последовательность когомологий, первые члены которой дают:

$$0 \leftarrow H_0(\widetilde{M}_n) \leftarrow H_0(M_n) \leftarrow H_0\left(\sum_{i=1}^d M_{n-1}x_i\right) \leftarrow H_1(\widetilde{M}_n),$$

или, ввиду (8),

$$0 \leftarrow H_0(M_n) \leftarrow H_0(M_{n-1}^d) \leftarrow \sum_{n_i \leq n} H_0(M_{n-n_i}). \quad (9)$$

Для размерности пространств, входящих в эту последовательность, получаем неравенство:

$$b_n \geq d \cdot b_{n-1} - \sum_{n_i \leq n} b_{n-n_i} \quad (n \geq 1).$$

Умножая это неравенство на t^n и складывая по всем $n \geq 1$, получаем неравенство для рядов:

$$\sum_{n=1}^{\infty} b_n t^n \geq \sum_{n=1}^{\infty} d \cdot b_{n-1} \cdot t^n - \sum_{n_i \leq n} t^n b_{n-n_i}. \quad (10)$$

Положив в последней сумме $n = n_i + m$, мы получим, что она равна

$$\sum_{n_i, m} t^{n_i+m} \cdot b_m = \sum_i t^{n_i} \sum_{m=0}^{\infty} b_m t^m = \left(\sum_{i=2}^{\infty} r_i t^i \right) P_A(t).$$

С другой стороны,

$$\sum_{n=1}^{\infty} b_n t^n = P_A(t) - 1$$

(так как $b_0 = 1$), а

$$\sum_{n=1}^{\infty} d \cdot b_{n-1} \cdot t^n = dt P_A(t).$$

Поэтому неравенство (10) дает:

$$P_A(t) - 1 \geq dt P_A(t) - \left(\sum_{i=2}^{\infty} r_i t^i \right) P_A(t),$$

откуда имеем:

$$P_A(t) \left(1 - dt + \sum_{i=2}^{\infty} r_i t^i \right) \geq 1. \quad (11)$$

Лемма 2 доказана.

Разумеется, не представляет труда интерпретировать точную последовательность (9) в терминах алгебры A , не прибегая к построению комплекса M .

ЛЕММА 3. Если коэффициенты степенного ряда $\left(1 - dt + \sum_{i=2}^{\infty} r_i t^i \right)^{-1}$ неотрицательны, то

$$P_A(t) \geq \left(1 - dt + \sum_{i=2}^{\infty} r_i t^i \right)^{-1} \quad (12)$$

и алгебра A бесконечна.

Неравенство (12) получается из (11) путем умножения обеих его частей на степенной ряд

$$F(t) = \left(1 - dt + \sum_{i=2}^{\infty} r_i t^i \right)^{-1}, \quad (13)$$

который по предположению имеет неотрицательные коэффициенты. Остается доказать, что алгебра A бесконечна. Для этого достаточно доказать, что $b_n > 0$ для бесконечного числа значений n , а это будет следовать из (13), если мы докажем, что степенной ряд $F(t)$ не является многочленом от t .

Положим

$$1 + \sum_{i=2}^{\infty} r_i t^i = U(t).$$

Согласно (13),

$$F(t)(U(t) - dt) = 1,$$

т. е.

$$F(t)U(t) = 1 + dtF(t).$$

Так как степенной ряд $U(t)$ имеет неотрицательные коэффициенты, то это равенство возможно только если $F(t)$ – бесконечный степенной ряд.

Замечание. Если числа r_i удовлетворяют неравенствам $r_i \leq s_i$ и все коэффициенты степенного ряда $\left(1 - dt + \sum_{i=2}^{\infty} s_i t^i\right)^{-1}$ неотрицательны, то лемма 3 также применима. Это следует из того, что если F и G — два степенных ряда со свободным членом 1, причем $F \leq G$ и $G^{-1} \geq 0$, то $F^{-1} \geq G^{-1}$. Действительно, $F = G - U$, где U — степенной ряд без свободного члена с неотрицательными коэффициентами. Имеем:

$$F = G(1 - UG^{-1}),$$

откуда находим:

$$F^{-1} = G^{-1}(1 - UG^{-1})^{-1}.$$

Так как $U \geq 0$ и $G^{-1} \geq 0$, то $(1 - UG^{-1})^{-1} \geq 1$. Умножив обе части этого неравенства на неотрицательный степенной ряд G^{-1} , получим $F^{-1} \geq G^{-1}$.

ЛЕММА 4. Если $b \leq \left(\frac{a}{2}\right)^2$, $c \leq \frac{a}{2}$, то все коэффициенты ряда

$$\frac{1 - ct}{1 - at + bt^2}$$

положительны.

Действительно, если $b \leq \left(\frac{a}{2}\right)^2$, то $1 - at + bt^2 = (1 - \alpha t)(1 - \beta t)$, где α и β вещественны, $\alpha \geq \beta \geq 0$, $\alpha + \beta = a$. Если $\alpha > \beta$, то, разлагая на простейшие дроби, получаем:

$$\frac{1 - ct}{1 - at + bt^2} = \frac{\alpha - c}{\alpha - \beta} \cdot \frac{1}{1 - \alpha t} + \frac{c - \beta}{\alpha - \beta} \cdot \frac{1}{1 - \beta t},$$

откуда имеем:

$$\frac{1 - ct}{1 - at + bt^2} = \sum_{n=0}^{\infty} \frac{(\alpha - c)\alpha^n + (c - \beta)\beta^n}{\alpha - \beta} \cdot t^n.$$

Так как $\alpha > c$, то все коэффициенты положительны. Если $\alpha = \beta = \frac{a}{2}$, то лемма очевидна.

ЛЕММА 5. Если идеал $\overline{\mathfrak{A}} \subset R_d$ порожден r формами степени 2, r формами степени 3 и т. д. и $r \leq \left(\frac{d-1}{2}\right)^2$, то алгебра $R_d/\overline{\mathfrak{A}}$ бесконечна.

Действительно, в обозначениях леммы 2 мы имеем:

$$r_i = r, \quad i = 2, 3, \dots$$

Рассмотрим ряд

$$\frac{1}{1 - dt + r \sum_{i=2}^{\infty} t^i} = \frac{1 - t}{1 - (d+1)t + (d+r)t^2}. \quad (14)$$

В силу леммы 4, если $r + d \leq \left(\frac{d+1}{2}\right)^2$, т. е. если $r \leq \left(\frac{d-1}{2}\right)^2$, то все коэффициенты ряда (14) будут положительны, а поэтому, ввиду леммы 3, алгебра A бесконечна.

§3. Применения

Как доказано в работе [4], если k – поле алгебраических чисел и $\mathfrak{G}$ – группа Галуа его максимального неразветвленного p -расширения, то минимальное число образующих d группы $\mathfrak{G}$ и ее число соотношений r (как про- p -группы) удовлетворяют условию $r \leq d + \rho$, где ρ – число образующих группы единиц поля k .

Напомним, что d равно числу образующих γ p -компоненты группы классов дивизоров поля k .

Из теоремы 1 следует, что группа $\mathfrak{G}$ заведомо бесконечна, если

$$\left(\frac{\gamma - 1}{2}\right)^2 \geq \gamma + \rho.$$

Неравенство выполнено, если $\gamma \geq 3 + 2\sqrt{\rho + 2}$. Отсюда вытекает

ТЕОРЕМА 3. *Над полем алгебраических чисел k существуют бесконечные неразветвленные расширения, если число образующих γ его группы классов дивизоров и число образующих ρ его группы единиц связаны соотношением*

$$\gamma \geq 3 + 2\sqrt{\rho + 2}. \quad (15)$$

В случае квадратичного мнимого поля $\rho = 1$ и неравенство (15) удовлетворяется, если $\gamma \geq 7$. Простейшим примером является поле

$$k = R(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}) = R(\sqrt{-4849845}),$$

у которого 2-компонента группы классов дивизоров имеет 7 образующих. Это следует из теоремы Гаусса о родах, а элементарно можно проверить, что $\gamma \geq 7$. Действительно, поля

$$k(\sqrt{-3}), k(\sqrt{5}), k(\sqrt{-7}), k(\sqrt{-11}), k(\sqrt{13}), k(\sqrt{17}), k(\sqrt{-19})$$

являются, как легко видеть, неразветвленными независимыми квадратичными расширениями поля k . Таким образом, над этим полем существует бесконечное неразветвленное 2-расширение.

Напомним, что башней полей классов поля k называется последовательность $k = K_0 \subset K_1 \subset K_2 \subset \dots$, в которой K_i – максимальное абелево неразветвленное расширение поля K_{i-1} . Из теоремы 3 следует, что для полей указанного там типа башня классов бесконечна. В частности, это верно для поля $R(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$.

Как известно, если башня полей классов поля k бесконечна, то поле k нельзя вложить в одноклассное поле алгебраических чисел. Действительно, если бы $K \supset k$ было одноклассным конечным расширением, то поле $K_1 K / K$ было бы абелевым неразветвленным расширением поля K , а так как K одноклассное, то $K_1 K$, согласно теории полей классов, должно было бы совпадать с K . Аналогично и все $K_i \subset K$, а это означало бы, что башня полей классов поля k конечна.

Из теоремы 3 вытекает, таким образом,

ТЕОРЕМА 4. Если для поля k выполнено условие (15), то k не содержится ни в каком одноклассном поле алгебраических чисел.

В частности, таким полем является поле

$$k = R(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19}).$$

Наконец, как заметил Э. Артин, вопрос о башне полей классов связан с вопросом о росте минимального дискриминанта поля алгебраических чисел степени n . Обозначим через D_n наименьшее значение абсолютной величины дискриминанта поля алгебраических чисел степени n . По лемме Минковского существует такая константа $c > 1$, что

$$\sqrt[n]{D_n} > c.$$

Например, согласно результату Роджерса [1], мы можем положить $c = 32$ для всех достаточно больших n .

С другой стороны, если над полем k имеется бесконечная последовательность неразветвленных расширений K_i , причем $[K_i : k] = n_i$, $[k : R] = n_0$, то

$$|D(K_i/R)| = |D_0|^{n_i}, \quad [K_i : R] = n_i n_0,$$

где $D(K_i/R)$ – дискриминант поля K_i/R , а D_0 – дискриминант поля k/R . Поэтому

$$n_0^{n_i} \sqrt[n_0 n_i]{D_{n_0 n_i}} \leq \sqrt[n_0]{|D_0|}.$$

Таким образом, из теоремы 3 следует

ТЕОРЕМА 5. Существуют такие бесконечные последовательности натуральных чисел $n_1 < n_2 < \dots$ и такие соответствующие им константы c, c' , что

$$c' > \sqrt[n_i]{D_{n_i}} > c.$$

В частности, результат Роджерса и пример поля

$$R(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19})$$

показывают, что

$$4405 > \sqrt[n]{D_n} > 32$$

при $n = 2^k$ и всех достаточно больших n .

Поступило 19.XII.1963

ЛИТЕРАТУРА

1. Rogers C. A., *The product of n real homogeneous linear forms*, Acta Math. **82** (1950), 185–208.
2. Serre J.-P., *Leçons sur la cohomologie galoisienne*, Collège de France, 1962–63.
3. Шафаревич И. Р., *Поля алгебраических чисел*, Proceedings of the International Congress of Mathematicians, Stockholm, 1962, pp. 163–176.
4. Шафаревич И. Р., *Расширения с заданными точками ветвления*, Publications Mathématiques de l'Institut des Hautes Etudes Scientifiques **18** (1963).

О РАНГЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ (С ДЖ. ТЕЙТОМ)

ДОКЛ. АКАД. НАУК СССР, Т.175, N 4 (1967)

Пусть k – конечное поле, $K = k(t)$ и A – эллиптическая кривая, определенная над K . Цель этой заметки – показать, что ранг группы рациональных точек A_K может принимать сколь угодно большие значения при надлежащем выборе кривой A и фиксированном поле K . Над полем $k(t)$, когда k – алгебраически замкнутое поле характеристики 0, аналогичные примеры были построены А.И.Лапиным [1].

Начнем с построения более простых примеров, в которых поле K не будет фиксировано. Обозначим через k_f поле из p^f элементов и через $\bar{k}$ – алгебраическое замыкание любого из полей k_f . Пусть C – геометрически неприводимая полная кривая, а A – эллиптическая кривая, причем обе определены над полем k . Рассматривая A как кривую над полем $L = k(C)$, обозначим через r ранг группы A_L . Как известно, r совпадает с рангом группы $\text{Hom}_k(J(C), A)$, где $J(C)$ – якобиево многообразие кривой C . Обозначим через $P_C(U)$ и $P_A(U)$ числители ζ -функций $Z_C(U)$ и $Z_A(U)$ кривых C и A . Из результатов работы [2] вытекает (теорема 1), что

$$r = 2h, \tag{1}$$

если $P_C = P_A^h \cdot G$ и P_A неприводим над Q или $P_C = P_A^{h/2} \cdot G$ и $P_A = F^2$, причем $(P_A, G) = 1$.

В связи с этим мы начнем с вычисления в явном виде многочлена $P_C(U)$ для некоторых кривых C .

ТЕОРЕМА 1. Пусть C – полная неособая модель кривой, определенной над k_1 уравнением

$$y^e = \gamma x^f + \delta,$$

причем выполнены условия: $\gamma, \delta \in k_1^*$, $p \nmid ef$, $2 \leq e \leq f$, $m = \text{o.n.}\kappa(e, f)$ делит $p^n + 1$ при некотором n . Обозначим через G прямое

произведение циклических групп $\{\xi\}$ и $\{\eta\}$ порядков e и f и для $\varphi \in \text{Hom}(G, \bar{k}^*)$ положим $k_\varphi = k_1(\varphi(\xi), \varphi(\eta))$, $d_\varphi = [k_\varphi : k_1]$.

Если

$$\varphi(\xi) \neq 1, \quad \varphi(\eta) \neq 1, \quad \varphi(\xi\eta) \neq 1, \quad (2)$$

то число d_φ четно: $d_\varphi = 2c_\varphi$ и

$$P_C(U) = \prod (1 + p^{c_\varphi} U^{d_\varphi}), \quad (3)$$

где произведение распространено на все φ , удовлетворяющие условию (2), причем из каждого класса гомоморфизмов, сопряженных относительно действия группы Галуа поля k_φ/k_1 , берется только один представитель.

Мы воспользуемся результатами работы [3], часть из которых приведем для удобства читателя.

Введем следующие обозначения: ζ — первообразный корень степени m из 1 в $\bar{k}$; $\varphi(\xi) = \zeta^{maf^{-1}}$; $\varphi(\eta) = \zeta^{mbf^{-1}}$; m_φ — порядок φ ; $a_0 = m_\varphi af^{-1}$; $b_0 = m_\varphi bf^{-1}$; w — образующий элемент группы k_φ^* , выбранный так, что

$$\zeta^{mm_\varphi^{-1}} = w^{(p^{d_\varphi} - 1)m_\varphi^{-1}}$$

и χ — такой характер группы k_φ^* , что $\chi(w) = e^{2\pi i m_\varphi^{-1}}$.

В этих обозначениях формулы, приведенные на стр. 493 [3], дают

$$P_C(U) = \prod L_\varphi(U),$$

где φ пробегает те же значения, что и в (3), и

$$L_\varphi(U) = 1 + \chi((\gamma^{-1}\delta)^{a_0}(-\delta)^{b_0})jU^{d_\varphi}; \quad (4)$$

$$j = \sum_{x+y+1=0} \chi(x)^{a_0} \chi(y)^{b_0}, \quad x, y \in k_\varphi^* \quad (5)$$

Так как m_φ является общим наименьшим кратным порядков $\varphi(\xi)$ и $\varphi(\eta)$ в группе k_φ^* , то $k_\varphi = k_1(\zeta^{mm_\varphi^{-1}})$ и d_φ является наименьшим целым числом, для которого $m_\varphi | (p^{d_\varphi} - 1)$. Таким образом, в группе $(\mathbf{Z}/m_\varphi \mathbf{Z})^*$ элемент $p + m_\varphi \mathbf{Z}$ имеет порядок d_φ , а $p^n + m_\varphi \mathbf{Z}$ — порядок 2, так как $m_\varphi | m$, по условию $m | (p^n + 1)$ и $m_\varphi > 2$ ввиду (2). Отсюда легко следует, что $d_\varphi = 2(n, d_\varphi)$ и, в частности, d_φ четно. Мы видим также, что

$$p^{c_\varphi} \equiv p^n \equiv -1 \pmod{m_\varphi}, \quad c_\varphi = d_\varphi/2. \quad (6)$$

Заметим, что $\chi = 1$ на $k_{c_\varphi}^*$. Действительно, $k_{c_\varphi}^* = \{w^{p^{c_\varphi}+1}\}$, а

$$\chi(w^{p^{c_\varphi}+1}) = e^{(2\pi i m_\varphi^{-1})(p^{c_\varphi}+1)} = 1$$

ввиду (6). В частности, $\chi = 1$ на $k_{c_\varphi}^*$. Докажем теперь, что в нашем случае

$$j = p^{c_\varphi}, \quad (7)$$

где j – сумма Якоби, определенная равенством (5). Для этого воспользуемся соотношением

$$j = p^{-d_\varphi} g(a_0)g(b_0)g(-a_0 - b_0) \quad (8)$$

([3], формула 7), где $g(r)$ – гауссова сумма:

$$g(r) = \sum_{x \in k_\varphi^*} \chi(x)^r \psi(x),$$

а ψ – стандартный характер аддитивной группы поля k_φ . Мы докажем, что

$$g(r) = \chi(c)^r p^{c_\varphi}, \quad (9)$$

если $r = a_0, b_0$ или $-a_0, -b_0$ и $c \in k_{d_\varphi}^*$ – элемент, след которого относительно подполя k_{c_φ} равен 0. Очевидно, что (7) следует из (8) и (9). Формула (9) вытекает из следующей леммы при $k = k_{d_\varphi}$, $k_0 = k_{c_\varphi}$, так как, ввиду (2), $m \nmid r$ и, значит, χ^r не тривиален на $k_{d_\varphi}^*$.

ЛЕММА. Пусть k – квадратичное расширение конечного поля k_0 из q элементов; θ – неединичный характер группы k^* , тривиальной на k_0^* , и ψ – стандартный аддитивный характер k . Тогда

$$\sum_{x \in k^*} \theta(x) \psi(x) = \theta(c)q,$$

где $c \in k^*$ таков, что $\text{Tr}_{k/k_0}(c) = 0$.

Пусть

$$k^* = \cup a_i k_0^*$$

разложение k^* на классы смежности по k_0^* . Так как $\theta = 1$ на k_0^* , то

$$\sum_{x \in k^*} \theta(x) \psi(x) = \sum_i \theta(a_i) \sum_{y \in k_0^*} \psi(a_i y).$$

Но

$$\sum_{y \in k_0^*} \psi(a_i y) = \sum_{y \in k_0} \psi(a_i y) - 1 = \begin{cases} -1, & \text{если } \psi \neq 1 \text{ на } a_i k_0, \\ q - 1, & \text{если } \psi = 1 \text{ на } a_i k_0. \end{cases}$$

Воспользуемся еще тем, что $\sum_i \theta(a_i) = 0$, так как $\theta \neq 1$ на k^*/k_0^* . Мы получаем, что

$$\sum_{x \in k^*} \theta(x) \psi(x) = \left(\sum_i \theta(a_i) \right) q, \quad (10)$$

где сумма распространена на те i , для которых $\psi = 1$ на $a_i k_0$. Таким a_i является, в частности, элемент c : ввиду определения характера ψ

$$\psi(cy) = \psi_0(\text{Tr}_{k/k_1}(cy)),$$

где ψ_1 — характер группы k_1 , а

$$\text{Tr}_{k/k_1}(cy) = \text{Tr}_{k_0/k_1}(\text{Tr}_{k/k_0}(cy)), \quad \text{Tr}_{k/k_0}(cy) = 0$$

ввиду выбора c .

С другой стороны, в сумму (10) не могут входить два различных слагаемых a_i и a_j , так как иначе ψ было бы тривиально на $k = a_i k_0 + a_j k_0$, а это не так. Этим доказана лемма и (9). Так как, сверх того, $\chi = 1$ на k_1^* , а $\gamma, \delta \in k_1^*$, то $L_\varphi = 1 + p^{c_\varphi} U^{d_\varphi}$, что и доказывает (3).

Предположим теперь, что соотношение $m|(p^n + 1)$ выполнено при нечетном n . Тогда из соотношения $d_\varphi = 2(n, d_\varphi)$ следует, что c_φ нечетно и каждый из множителей $L_\varphi(U)$ делится на $1 + pU^2$. Как известно, $1 + pU^2 = P_A(U)$, где A — суперсингулярная эллиптическая кривая, определенная над полем k_1 . Поэтому в рассматриваемом случае число h в формуле (1) равно числу всех классов гомоморфизмов φ , удовлетворяющих условию (2). В частности, если $e = 2$, то это число равно числу делителей многочлена $x^f - 1$, неприводимых над k_1 и отличных от $x - 1$ и при $2|f$ от $x + 1$. Таким образом, имеет место:

Следствие. Если A — суперсингулярная эллиптическая кривая, определенная над полем k_1 , C определена уравнением

$$y^2 = \gamma x^f + \delta, \quad (11)$$

причем $f|(p^n + 1)$, $2 \nmid n$, $p \neq 2$, то ранг кривой A над полем $k_1(C)$ равен $2h$, где h — число неприводимых над k_1 делителей многочлена $x^f - 1$, отличных от $x - 1$ и при $2|f$ от $x + 1$.

Заметим, что всегда существует суперсингулярная кривая A , определенная над полем k_1 . Для этого достаточно, ввиду результатов работы [4], показать, что p является нормой целого элемента кватернионной алгебры $\mathfrak{A}$ над $\mathbb{Q}$, разветвленной только в p и ∞ . Но если $p \equiv -1 \pmod{4}$, то $\mathfrak{A} = (-p, -1)$, а если $p \equiv 1 \pmod{4}$, то $\mathfrak{A} = (-p, -q)$, где q — простое число, $q \equiv -1 \pmod{4}$, $(q/p) = -1$. В обоих случаях в $\mathfrak{A}$ содержится такой элемент u , что $u^2 + p = 0$.

Перейдем теперь к построению кривой, определенной над полем $k_1(x)$. Для этого рассмотрим на кривой C , заданной уравнением (11), автоморфизм $s: s(x) = x, s(y) = -y$ и на поверхности $C \times A$ автоморфизм $\sigma(c, a) = (s(c), -a)$, $c \in C, a \in A$. Проекция $C \times A \rightarrow C$ определяет отображение $(C \times A)/\sigma \rightarrow C/s = \mathbb{P}^1$. Поэтому мы можем рассматривать поле $\mathcal{K} = k_1(V)$, $V = (C \times A)/\sigma$, как поле степени трансцендентности 1 над полем $k_1(\mathbb{P}^1) = k_1(x)$.

Легко видеть, что род поля $\mathcal{K}/k_1(x)$ равен 1.

Если кривая A задается уравнением $v^2 = u^3 + au^2 + bu + c$, то поле $\mathcal{K}/k_1(x)$ есть поле рациональных функций на кривой, заданной уравнением

$$v^2 = u^3 + a(\gamma x^f + \delta)u^2 + b(\gamma x^f + \delta)^2u + c(\gamma x^f + \delta)^3. \quad (12)$$

Ранг кривой (12) над $k_1(x)$ равен, как легко видеть, рангу группы таких отображений, определенных над k_1 , $f: C \rightarrow A$, что

$$f(c^s) = -f(c). \quad (13)$$

Для любого отображения $f: C \rightarrow A$ отображение $c \rightarrow f(c) + f(c^s)$ постоянно, так как оно равно композиции отображения $C \rightarrow \mathbb{P}^1$ и некоторого отображения $\mathbb{P}^1 \rightarrow A$. Из того, что группа A_{k_1} конечна, следует, что группа отображений, удовлетворяющих (13), имеет конечный индекс в группе точек A , рациональных над $k_1(C)$. Поэтому ранг кривой (12) над $k_1(x)$ равен рангу кривой A над $k_1(C)$, который определяется теоремой 1 и следствием. Тем самым доказана

ТЕОРЕМА 2. Ранг кривой (12) над полем $k_1(x)$ при $f|(p^n + 1)$, $2 \nmid n$, $p \neq 2$ равен $2h$, где h — число неприводимых над k_1 делителей многочлена $x^f - 1$, отличных от $x - 1$ и при $2|f$ от $x + 1$.

Предположим, в частности, что $f = p^n + 1$ и n — простое число. Тогда число неприводимых делителей многочлена $x^f - 1$, отличных

от $x + 1$, равно, как легко убедиться, $(p^n - p)/2n + (p - 1)/2$, и мы видим, что ранг кривой (12) над полем $k_1(x)$ при $f = p^n + 1$, $p \neq 2$ и n простым равен $(p^n - p)/n + p - 1$.

Таким образом, ранг может принимать сколь угодно большие значения.

Поступило 3.V.1967

ЛИТЕРАТУРА

1. А. И. Лапин, Изв. АН СССР, сер. матем. **28**, **953** (1964).
2. J. Tate, Inventiones Math. **2**, N **2**, **134** (1966).
3. A. Weil, Trans. Am. Math. Soc. **73**, N **3**, **487** (1952).
4. M. Deuring, Abh. Math. Sem. Hamburg **14**, **197** (1941).

ВПЕЧАТЛЕНИЯ ОТ МЕЖДУНАРОДНОГО МАТЕМАТИЧЕСКОГО КОНГРЕССА В ЭДИНБУРГЕ

УСПЕХИ МАТ. НАУК СССР Т. XIV, ВЫП. 2 (86), 1959

Для меня наиболее интересным в конгрессе было то, что он подтвердил и еще обострил чувство, складывавшееся и раньше под влиянием математической литературы, — что в последние 10 лет в математике произошли принципиальные изменения, не просто продвинувшие ее вперед по тому направлению, по которому она раньше развивалась, но изменившие само направление ее развития. В разнообразных областях математики достигнуты успехи, опирающиеся на очень близкие друг другу идеи, и начал вырабатываться некий общий для всех этих областей язык.

Области, которые я имею в виду, — это алгебраическая теория чисел, алгебраическая геометрия, теория аналитических многообразий (в частности, теория аналитических функций многих переменных), теория дифференцируемых многообразий и топология. Эти области имеют много точек соприкосновения с аналитической теорией чисел, группами Ли и функциональным анализом.

Мне кажется особенно важным, что, несмотря на разнообразие конкретного материала, который здесь охвачен, можно все же говорить об одном направлении в математике, основывающемся на небольшом числе новых идей и понятий. Этой основой, которая связывает все это новое направление, является гомологическая алгебра. Такие понятия, как группы когомологий модулей и групп, спектральные последовательности и группы когомологий пучков, которых еще не существовало лет 10–15 назад, сейчас превратились в стандартный аппарат.

По-видимому, эти новые идеи оказывают косвенное влияние и на такие исследования, в которых они непосредственно не применяются (например, в работах Ботта и Мильнора о порядках гомотопических групп сфер связь с числами Бернулли устанавливается при помощи техники, разработанной Хирцебрухом в связи с его исследованиями по теории гомологий пучков и теореме Римана–Роха).

Далее я хочу рассказать о тех из доложенных на съезде результатах, которые показались мне особенно интересными. Конечно, далеко не все они непосредственно связаны с гомологической алгеброй, но мне кажется, что то обстоятельство, которое особенно ярко было заметно на конгрессе, — а именно, что как общее количество, так и значительность работ в этих областях возросли в последние годы, — находится в связи с появлением идей гомологической алгебры.

Наиболее плодотворно когомологические методы применяются сейчас, пожалуй, в алгебраической геометрии. На съезде когомологической теории алгебраических многообразий был посвящен обзорный доклад Гротендика. В своем докладе Гротендик сообщил, что ему удалось “разумным образом” определить понятие групп Бетти для алгебраических многообразий, определенных над произвольным полем. “Разумность” понимается в том смысле, что сохраняются обычные теоремы о поведении групп Бетти при непрерывных (в данном случае рациональных) отображениях, в частности теорема Лефшеца о неподвижных точках. По-видимому, из этой теории должны следовать для произвольных алгебраических многообразий результаты, аналогичные тем, которые получил Вейль для алгебраических кривых. Это привело бы к очень интересным следствиям в теории сравнений со многими неизвестными.

Другой интересный результат Гротендика был изложен в обзорном докладе Хирцебруха. Речь идет об обобщении теоремы Римана–Роха. Обобщение заключается в том, что находится закон преобразования рода Тодда при рациональных отображениях. Первоначальная теорема Римана–Роха в формулировке Хирцебруха получается из этого результата, если рассматривать отображения многообразия в точку. Доказательство этого обобщения оказывается значительно проще, чем доказательство теоремы Римана–Роха, найденное Хирцебрухом. В частности, оно алгебраическое, так что приложимо к многообразиям над произвольным полем, и не использует теории внутренних гомотетий Тома, на которой основывалось доказательство Хирцебруха.

Разумеется, на съезде можно было услышать о многих результатах, которые не докладывались. В числе таких результатов было новое обоснование теории пересечений алгебраических многообразий, построенное Серром при помощи теории гомотетий локальных колец.

Методы гомологической алгебры в топологии были темой обзорного доклада Эйленберга. Он рассказал об очень красивом способе индуктивного вычисления групп когомологий пространств $K(\Pi, n)$. Оказывается, что группы когомологий пространства $K(\Pi, n)$ могут

быть выражены в терминах теории гомологий колец (так называемой относительной теории гомологий), причем за кольцо берется кольцо когомологий пространства $K(\Pi, n-1)$.

Очень большое впечатление произвел доклад молодого тополога Адамса. Основываясь на теории вторичных когомологических операций, он показал, что отображения с хопфовским инвариантом 1 могут существовать только у сфер размерности 2, 4 и 8. Отсюда следует доказательство знаменитой гипотезы: над полем действительных чисел существуют алгебры с делением только размерностей 1, 2, 4 и 8. Интересно, что последний результат был независимо получен и также доложен на съезде Кервайром, который получил его исходя из более слабого топологического результата — он доказал непараллелезуемость сфер размерностей, отличных от 1, 3 и 7.

Сенсацией было сообщение Мюрре о том, что любое компактное аналитическое вещественное n -мерное многообразие аналитически вкладывается в $(2n+1)$ -мерное евклидово пространство. До сих пор не было известно даже, существует ли на таком многообразии непостоянная аналитическая функция. Об очень сильных теоремах вложения дифференцируемых многообразий сообщил Хирш. Так, он доказал, что трехмерное компактное многообразие можно вложить в четырехмерное евклидово пространство, и шестимерное проективное пространство — в семимерное евклидово.

Из области топологии я хочу в заключение упомянуть о двух результатах Мильнора. Первый результат был сообщен в обзорном докладе Хирцебруха. Он заключается в том, что дается необходимое и достаточное условие для того, чтобы набор целых чисел был набором чисел Черна некоторого компактного почти комплексного многообразия. Ввиду роли, которую играют числа Черна в алгебраической геометрии, ясна значительность этой теоремы. Второй результат относится к порядкам гомотопических групп сфер. Он показывает, что порядок определенной подгруппы этой группы (образа гомоморфизма Уайтхеда) делится на целое число, которое я не буду выписывать и которое определяется исходя из бернуллиевых чисел. Вероятно даже, что порядок указанной подгруппы равен этому числу. Таким образом, появляется надежда, что хотя бы порядки гомотопических групп сфер могут быть вычислены явным образом.

Теория функций многих комплексных переменных была представлена обзорными докладами Картана и Граuertа. В докладе Картана речь шла о таком обобщении понятия комплексного аналитического многообразия, которое соответствует переходу от алгебраического многообразия без особых точек к многообразию с особен-

ностями. Таким образом приходят к так называемым аналитическим пространствам, которые локально эквивалентны не области n -мерного комплексного пространства, а подмножеству этого пространства, определенному конечным числом аналитических уравнений. Аналитические пространства часто встречаются в качестве фактор-пространств аналитических многообразий по дискретным группам, если преобразования этих групп имеют неподвижную точку. Картан рассказал о ряде результатов, связанных с трудностями, которые вызывает переход от аналитических многообразий к аналитическим пространствам, например, в связи с интегрированием дифференциальных форм (ввиду “особенностей” интегралы расходятся) и с погружением одних пространств в другие.

Доклад Граурта был посвящен теории аналитических пучков и аналитических косых произведений с комплексной группой Ли в качестве структурной группы. Интересно, что в виде очень частного случая его теории получаются результаты Биркгофа–Лаппо–Данилевского о существовании систем дифференциальных уравнений с заданной группой монодромии.

Промежуточное место между теорией функций многих переменных и одной переменной занимал доклад Берса. В этом докладе речь шла о таком фундаментальном и в то же время неисследованном понятии, как пространство всех компактных римановых поверхностей заданного рода p . После результатов Римана, доказавшего, что это пространство имеет размерность $6p - 6$ (при $p > 1$), в этой области не было получено почти никаких принципиальных результатов, но сейчас она, видимо, снова оживает. Так, Берс показал, как ввести в этом пространстве структуру аналитического и даже келерова многообразия.

Переходя к алгебре, естественно упомянуть в первую очередь сенсационный результат Нагата — отрицательное решение XIV проблемы Гильберта. Именно Нагата построил пример такой группы G линейных преобразований от 32-х переменных $x_1, \dots, x_{32}$, что в кольце многочленов от $x_1, \dots, x_{32}$ те многочлены, которые инвариантны относительно преобразований G , образуют подкольцо с бесконечным числом образующих.

В докладе Шевалле был дан обзор области, которой сейчас очень много занимаются — теории алгебраических групп. Под этим подразумеваются группы, являющиеся в то же время алгебраическими многообразиями, причем групповой закон должен выражаться рациональными функциями от координат переменных точек. Согласно теореме Шевалле–Барсотти–Розенлихта, в каждой такой группе есть наибольший нормальный делитель, являющийся алгебраической подгруппой матриц (линейные группы), причем фактор-

группа по нему является абелевым многообразием (в случае комплексного основного поля это значит, что она компактна). Абелевы многообразия за последние 15 лет были глубоко изучены Вейлем и его школой. В семинаре, который Шевалле вел в прошлом году, были исследованы простые линейные алгебраические группы. Доказано, что если основное поле "достаточно мощное", то получаются группы, в точности соответствующие классическим простым группам. Этот результат можно применить к исследованию групп над конечным полем, которые приводят к конечным простым группам. Как показал Хертциг, таким образом получаются известные до сих пор простые конечные группы и две новые.

Из области теории чисел я хочу упомянуть о теории неопределенных уравнений, число переменных в которых достаточно велико сравнительно со степенью. Этому вопросу был посвящен обзорный доклад Дэвенпорта. Большое количество кулуарных разговоров на эту тему создало впечатление, что этим вопросом сейчас многие интересуются. Здесь имеются три гипотезы возрастающей трудности: I. Уравнение $f(x_1, \dots, x_m) = 0$, где f — целочисленная форма степени n и $m > n^2$ имеет ненулевое решение как сравнение по любому модулю. II. Если форма f — неопределенная, то при тех же предположениях уравнение $f = 0$ имеет целочисленное ненулевое решение. III. Если коэффициенты формы f — вещественные, а остальные предположения те же, что и в II, то неравенство $|f| < \epsilon$, $\epsilon > 0$ имеет целочисленное ненулевое решение. Гипотеза I доказана при $n=2$ и 3, гипотеза II только при $n = 2$, а гипотеза III ни для какого n . Дэвенпорт доказал II при любом n , но с заменой условия $m > n^2$ условием " m достаточно велико сравнительно с n ", и получил аналогичный результат для III при $n=2$.

В заключение я хочу подчеркнуть, что эти поневоле отрывочные впечатления никак не могут дать достаточно полной картины работы конгресса хотя бы в тех областях, которых я касался. Это объясняется, не говоря уже об неизбежной субъективности точки зрения, просто невозможностью достаточно внимательно следить за деятельностью большого числа параллельно работающих секций. Я не упомянул также и о докладах советских математиков, так как их работы у нас и так хорошо известны.

**К 150-ЛЕТИЮ СО ДНЯ
РОЖДЕНИЯ АЛЬФРЕДА КЛЕБША***

MATH. ANN. **266**, 135–140, 1983

Основатель этого журнала, Альфред Клебш, был ярким и оригинальным математиком — даже по меркам своего столетия, столь богатого математическими талантами.

Клебш был очень многосторонним математиком, и его влияние испытали — и продолжают испытывать в определенной степени до сих пор — разные области нашей науки. Но главным делом его жизни был его вклад в развитие алгебраической геометрии. Благодаря работам Клебша алгебраическая геометрия превратилась в науку, с теми постановками вопросов и представлениями об ее области исследования, которые в основных чертах сохранились до сих пор.

Начало геометрической деятельности Клебша приходится на 1860 г. К этому времени лицо области, которая позже будет названа алгебраической геометрией, было сформировано работами Понселе, Шаля, Кэли, Сильвестра, Сальмона, Мебиуса, Гессе и Плюккера. К этому времени стали привычными проективный подход и использование точек с комплексными координатами. Была детально разработана проективная теория кривых и поверхностей второго порядка. Были открыты многие свойства плоских кривых степени 3 (например, конфигурация их 9 точек перегиба), степени 4 (28 двойных касательных) и поверхности степени 3 (с их 27 прямыми). Результаты общего характера, которые относились к плоским кривым произвольной степени, были получены Плюккером: формулы, носящие его имя, связывали степень кривой, ее класс и число ее двойных точек и двойных касательных. Имелось множество конкретных фактов, которые позволяли предположить существование общих результатов и концепций.

*Работа впервые опубликована по-немецки. Здесь публикуется русский оригинал.

Глубокая и смелая идея Клебша состояла в том, что эти общие концепции следует искать не в самой геометрии, а в только что (1856 г.) появившихся работах Римана, которые в то время понимались как часть теории функций и которые были посвящены интегралам и Θ -функциям и базировались на аналитическом вариационном принципе Дирихле. В сущности говоря, это было истолкование идей Абеля и Римана, перевод их на другой язык, но перевод в высшей степени не тривиальный. Если для Абеля уравнение $F(w, z) = 0$, где F — многочлен, есть “иррациональность” w , а для Римана оно определяет алгебраическую функцию w (заданную на некоторой римановой поверхности), то для Клебша это уравнение — алгебраическая кривая, и каждый новый факт для этого уравнения соответствует некоторому геометрическому свойству кривой. Все три способа рассмотрения существуют до сих пор, что отразилось, например, в разговоре двух ныне живущих известных специалистов в алгебраической геометрии. Когда один из них воскликнул: “Неужели со словами “алгебраическая кривая” Вы не связываете никакого наглядного образа?”, другой ответил: “Напротив, вот он”. И он написал: “ $F(X, Y) = 0$ ”.

Новую концепцию Клебш впервые развил в 1863 г. в статье “О применении абелевых функций в геометрии”, опубликованной в журнале Крелля. Мне кажется, что эту статью можно рассматривать как свидетельство о рождении алгебраической геометрии, как первый крик новорожденного.

В статье “О теореме Штайнера и некоторых вопросах теории кривых степени 3”, которая была написана лишь на месяц ранее упомянутой выше работы и появилась в том же томе журнала, Клебш рассматривает лишь кривые степени 3. Он доказывает, что они параметризуются эллиптическими функциями (по-видимому, этот факт установлен здесь впервые) и дает геометрическую интерпретацию теореме сложения эллиптических функций: точки P, P', P'' некоторой кривой 3-й степени лежат на одной прямой в том и только в том случае, когда для соответствующих им аргументов z, z', z'' эллиптической функции сумма $z + z' + z''$ является периодом. Отсюда следуют все ранее известные свойства точек перегиба и другие результаты Штайнера просто как утверждения о положении в параллелограмме периодов точек, n -кратное которых есть период.

В статье о применении абелевых функций аналогичные исследования проведены для кривых произвольной степени с произвольными особыми точками. Теорема Абеля и решенная Риманом проблема обращения для абелевых функций дают очень точные сведения о тех мероморфных функциях на римановой поверхности, опреде-

ляемой уравнением $F(w, z) = 0$, которые имеют заданные нули и полюса. При переводе на геометрический язык это приводит к исчерпывающему описанию кривых, которые с заданной степенью касаются заданной выше кривой в заданных точках. Этот метод приводит к целому водопаду выдающихся геометрических результатов: теорема Плюккера о том, что кривая 4-й степени имеет 28 двойных касательных (т.е. прямых, которые касаются ее в двух точках), является простейшим примером.

Следующие годы Клебш со своими сотрудниками и учениками посвятил систематической разработке нового направления. В законченном виде это проявилось в “Лекциях о геометрии”, которые читались Клебшем в 1871–1872 гг. и были изданы Линдеманом (том I). Удивительно, насколько продвинулась теория за 8 лет. Мы встречаемся здесь с понятием однозначного (теперь: бирационального) преобразования алгебраических кривых и с ясным пониманием того, что основная задача состоит в изучении кривых с точностью до таких преобразований. Определен род (это название принадлежит Клебшу), причем чисто геометрически — через степень кривой и кратности ее двойных точек. Доказана инвариантность рода при “однозначных преобразованиях”. Так же геометрически доказана теорема Римана–Роха, откуда следует, что кривые рода 0 параметризуются рациональными функциями, а кривые рода 1 — эллиптическими. Найдена модель минимальной степени для кривых заданного рода и показано, что число “модулей”, от которых с точностью до “однозначных преобразований” зависят кривые рода p , равно $3p - 3$. Построены интегралы первого, второго и третьего рода (причем чисто алгебраически, т.е. определены подынтегральные выражения). Доказана теорема Абеля. Построено якобиево многообразие (в современной терминологии) кривой. Все изложение вполне синтетическое (мы сказали бы: “над произвольным полем”), но связь с топологическим и аналитическим подходом Римана также всегда прослеживается. И, конечно, эта теория прилагается к большому числу конкретных геометрических задач.

Следующий шаг состоял в переходе к рассмотрению алгебраических многообразий более высокой размерности, прежде всего к алгебраическим поверхностям. И здесь Клебш вводит понятие однозначного (т.е. бирационального) преобразования и рассматривает в первую очередь поверхности, которые “однозначно” отображаются на плоскость, т.е. рациональные поверхности. Он устанавливает рациональность поверхностей 3-й степени, различных особых поверхностей степеней 4 и 5 и “двойной плоскости”, которая определяется уравнением $f(x, y) = z^2$, где f — многочлен 4-й степени. Наконец, в короткой заметке в “Comptes Rendus” за 1868 г. он вводит

понятие, которое затем будет играть основополагающую роль в геометрии алгебраических поверхностей. Он определяет двукратный интеграл первого рода, зависящий от алгебраической поверхности, и “род поверхности” — как число линейно независимых интегралов первого рода. Без доказательства утверждается инвариантность рода при “однозначных” (бirationальных) преобразованиях. В качестве основной задачи Клебш предлагает построение общей теории “однозначных преобразований”, в которой теория инвариантов (относительно проективных отображений) должна быть лишь введением; очевидно, что перед его взором возникли общие контуры “бirationальной алгебраической геометрии”.

Некоторые исследования Клебша были продолжены лишь через десятилетия. Так, он изучал (в современных терминах) рациональные поверхности над алгебраически не замкнутым полем, рассматривал обобщенное якобиево многообразие особой рациональной кривой, нашел бирегулярную классификацию рациональных регулярных поверхностей.

Как часто бывает, этот переворот — создание новой области науки — произошел почти скачкообразно, менее чем за 10 лет, между первой работой Клебша 1863 г. и его смертью в 1872 г.

На втором месте после алгебраической геометрии в творчестве Клебша стояла теория инвариантов. Для характеристики вклада Клебша в эту область сошлось на математика, внесшего наибольший вклад в эту область: на Гильберта. В докладе на Международном математическом конгрессе 1893 г. Гильберт делит развитие каждой области математики на три периода: наивный, формальный и критический. По его мнению в теории инвариантов его собственные работы представляют третий период, в то время как второй характеризуется работами Клебша и Гордана.

Основной вопрос, на котором концентрировались усилия математиков, состоял в нахождении полной системы инвариантов для форм заданной степени n от заданного числа m переменных, т.е. в построении такой конечной системы инвариантов, через которые все прочие можно выразить в виде многочленов. Для бинарных форм (т.е. для $m = 2$) существование такой конечной полной системы инвариантов доказано Горданом, долготлетним сотрудником Клебша. Для форм произвольного числа переменных этот результат был получен Гильбертом. Доказательство Гильберта распадается на две разнородные части. Одна из них относится — с современной точки зрения — к основаниям коммутативной алгебры (теорема Гильберта о базисе) или к гомологической алгебре (теорема о сизигиях). Другая, напротив, использует существование некоторого дифференциального оператора, который инвариантен относи-

тельно группы $SL(m)$, проектора на кольцо инвариантов.

Идею последнего рассуждения Гильберт приписывает (Ges. Abh. Bd II. S. 248) Клебшу (хотя дифференциальные операторы в теории инвариантов применялись ранее также Сильвестром и Кэли). Так как первая часть доказательства Гильберта никак не зависит от того, что мы ищем инварианты именно группы $SL(m)$, Гильберт ставит вопрос (“14-я проблема Гильберта”), не верна ли аналогичная теорема конечности для инвариантов произвольной подгруппы $G \subset SL(m)$. В 1958 г. Нагата дал отрицательный ответ на этот вопрос. Таким образом, глубокая причина существования конечной полной системы инвариантов коренится в существовании того дифференциального оператора, который был найден Клебшем. Теперь мы знаем, что существование аналогичного проектора для произвольной (алгебраической) группы G эквивалентно редуцируемости группы G (см. Nagata “Lectures on the Fourteenth Problem of Hilbert”, Bombay, 1965).

Уровень, который был достигнут в теории инвариантов ко времени Клебша, отразился в его книге “Теория бинарных алгебраических форм”. В ней большую роль играет метод представления формы $f(x_1, x_2; y_1, y_2)$, зависящей от пар переменных (возможно, разной степени однородности), через “поляры” формы, которые зависят лишь от одной пары. Если рассмотреть пространство S_n форм степени n как модуль представления для группы $SL(2)$ (как известно, так получаются все конечномерные неприводимые представления этой группы), то пространство форм $f(x_1, x_2; y_1, y_2)$ степени n по x_1, x_2 и степени m по y_1, y_2 будет модулем представления $S_n \otimes S_m$. Формула из книги Клебша (так называемая формула Клебша–Гордана) дает явное разложение этого представления на неприводимые, т.е. определяет структуру кольца неприводимых представлений группы $SL(2)$. Эта формула ввиду связи между группами $SL(2)$, $O(3)$ и группой Лоренца имеет множество приложений, особенно в квантовой механике (см., например, Н. Weil “Gruppentheorie und Quantenmechanik”).

В анализе Клебшем было получено фундаментальное условие для полной интегрируемости системы линейных дифференциальных уравнений в частных производных, которое теперь называется теоремой Фробениуса (статья Клебша в журнале Крелля, т.65). Клебш является также автором работ по физике, а именно, по оптике, теории упругости и гидродинамике.

Следует упомянуть также об его исследованиях по движению твердого тела без внешних сил в идеальной жидкости, где он нашел два случая полной интегрируемости соответствующих уравнений (Math. Ann. Bd.3, 1887). Этот вопрос в самое последнее

время получил новое освещение благодаря теоретико-групповой интерпретации. В основе лежит наблюдение о том, что орбита произвольной группы Ли G в пространстве L ее коприсоединенного представления обладает естественной симплектической структурой (“структура Кириллова”). Если на L задать некоторую гамильтонову функцию (обычно берется квадратичная форма), то получим гамильтонову (на каждой орбите общего положения) динамическую систему. Если взять, например, $G=SO(3)$, то этим способом получим уравнения движения твердого тела без внешних сил. Подобным же способом можно получить также уравнения движения твердого тела в идеальной жидкости: они связаны с группой $G=E(3)=SO(3)\cdot\mathbb{R}^3$ всех движений трехмерного пространства. Многие получаемые таким способом системы дифференциальных уравнений оказываются вполне интегрируемыми. Например, новые случаи полной интегрируемости получаются для уравнений, которые связаны с группой $SO(4)$ (“движения четырехмерного твердого тела с фиксированной точкой”). Алгебру Ли группы $SO(4)$ можно получить при помощи “деформации” из алгебры Ли группы $E(3)$. При этом оказывается, что вновь полученные случаи полной интегрируемости являются “деформацией” тех, которые рассматривались Клебшем. Находятся также другие случаи полной интегрируемости уравнений, связанных с $E(3)$, которые являются аналогами случая Клебша. Таким образом, упомянутая работа Клебша в последнее время стала отправной точкой при поиске новых вполне интегрируемых уравнений, определенных различными группами Ли. [См. В.И. Арнольд. Математические методы классической механики, 1978; С.П. Новиков. Успехи матем. наук, 37 (1982), N 5; В.В. Трофимов и А.Т. Фоменко. Труды семинара по векторному анализу, вып. 21, МГУ.]

Клебш принадлежал к новому, только нарождавшемуся типу математика: для него характерна напряженнейшая педагогическая деятельность, живое общение с молодыми математиками, другими словами — создание школы. Этим он порывает с классическим образом, наиболее ярким представителем которого в XIX веке был Гаусс. Его предшественниками были Якоби и Дирихле, его наследниками — Клейн, Гильберт и многие другие. Теперь, более чем столетие спустя, мы замечаем также отрицательные стороны этого типа организации научной деятельности: определенная стандартизация научного мышления, некоторая механизация творческого процесса, опасность окостенения и вырождения школы. Однако, в то время это был лишь нарождавшийся стиль математической жизни, который предвещал колоссальный успех в будущем.

Вокруг Клебша собралась плеяда полных энтузиазма сотрудни-

ков и учеников: Гордан, Брилли, Люрот, Цейтен и наиболее знаменитые: Петер и Клейн. Они остро чувствовали новизну своего направления: в их работах постоянно встречаются термины “Новая геометрия” (алгебраическая геометрия), “Новая алгебра” (теория инвариантов и, пожалуй, теория Галуа). По-видимому, Гордан также примыкал к этому направлению. Клейн писал (в “Лекциях о развитии математики в XIX веке”, стр. 341): “Когда Клебш столь неожиданно скончался в 1872 г., личные отношения между нами, выбравшими его своим руководителем, и большей частью других математиков носили, как это обыкновенно бывает, обостренный характер”. Именно выразителем этого нового направления был основанный Клебшем (совместно с К.Нейманом) журнал “Mathematische Annalen”. Это сплоченное направление, которое хорошо сознавало свою “авангардную” роль, вероятно, можно сравнить с бурбакизмом в XX веке. Клебш был его основателем и душой. Клейн писал, что при оценке вклада Клебша следует учитывать работы всех математиков его школы. Действительно, часто можно видеть, как в их работах реализуются идеи Клебша. Самым выдающимся примером, по-видимому, является грандиозное здание бирациональной алгебраической геометрии, которое было построено Нетером согласно замыслу Клебша. Эта особая роль объясняет то большое влияние, которое оказывал Клебш на своих современников (например, это видно из некролога, опубликованного его учениками в 7-м томе журнала “Mathematische Annalen”, или из посвященных Клебшу страниц книги Клейна). Эта роль, возможно, объясняет также, почему его, пожалуй, не так ценят сейчас, как он того заслуживает.

МАТЕМАТИЧЕСКОЕ МЫШЛЕНИЕ И ПРИРОДА*

COMMENTARII MATHEMATICI UNIVERSITATIS

SANCTI PAULI VOL. 43, N 1, 1994

Для меня большая честь — представить этот доклад вниманию Вашего Общества. Я сердечно благодарен за предложение прочесть его.

Вопрос, который я собираюсь обсудить, можно коротко сформулировать в виде следующих четырех предложений.

1) Человечество переживает сейчас всеобъемлющий экологический кризис. Все слышали о нем и его возможных последствиях. Исчезновение многих видов животных; уничтожение лесов, которыми дышит Планета; потепление атмосферы, которое превратит за 30 или 50 лет многие сейчас плодородные земли в пустыни и вызывающее таяние арктических льдов, так что океан может затопить многие страны; накопление радиоактивных отходов, которые будут продолжать оставаться радиоактивными еще тысячи и десятки тысяч лет, и т.д. и т.д. — все это представляет реальную угрозу живой части природы — и человеку в том числе.

2) Этот кризис не является результатом какой-то случайной, легко исправимой ошибки. Напротив, он является логическим следствием развития некоторой, очень специфической цивилизации, распространившейся сейчас на весь мир. Она называется Технологической Цивилизацией, так как основывается на максимальном использовании техники во всех областях человеческой деятельности. Техника всегда считается более надежной и эффективной, чем Природа, и всюду вытесняет Природу, если это только возможно. Один социолог описал эту цивилизацию как попытку человека уничтожить природу, заменив ее искусственной природой — техникой.

3) Идеологической основой Технологической Цивилизации является Научная Идеология или Сциентизм. Она основана на вере в существование небольшого числа точно формулируемых законов при-

* Доклад, прочитанный на собрании Японского Математического общества 28 сентября 1993 г.

роды; на их основе все в Природе предсказуемо и манипулируемо. Космос рассматривается как гигантская машина, которой можно управлять, если известен принцип ее функционирования. Эта научная идеология часто играет роль религии Технологической Цивилизации (как заметил еще Э.Мэх).

4) Основная догма научной идеологии — это вера в математизацию. Она утверждает, что все (или, по крайней мере, все существенное) в Природе может быть измерено, превращено в числа (или другие математические объекты) и что путем совершения над ними различных математических манипуляций можно предсказать и подчинить своей воле все явления Природы и Общества. Кант говорил, что каждая область знания является наукой настолько, насколько в ней содержится математика. Пуанкаре писал, что окончательная, идеальная фаза развития любой научной концепции это ее математизация. В некотором смысле можно сказать, что мы живем в Математической Цивилизации — и, может быть, умираем вместе с нею. Ввиду сказанного выше математику естественно проявить интерес к этим взаимосвязанным явлениям.

Научная идеология имеет сейчас уже длинную историю. Еще Галилей говорил, что “книга науки написана на языке геометрии” (геометрией тогда называли математику). Приблизительно в то же время (1605) Кеплер писал в письме своему другу: “Моя цель — показать, что небесную машину нужно сравнивать не с божественным организмом, а с часовым механизмом”. Декарт сравнивал животное с машиной, а столетие спустя Ламетри с книге “Человек — машина” распространил этот принцип и на человека.

Однако, лишь во времена Ньютона механическая концепция мира полностью покорила себе умы. Ньютон и его последователи называли его теорию “Системой Мира”. Она вдохновляла не только его современников, но и многие следующие поколения. Казалось, что можно развить полную картину Природы на основе небольшого числа законов, из которых все остальное может быть дедуцировано при помощи решения дифференциальных уравнений, разложения функций в степенные ряды и других математических процедур.

Но больше всех зачарован этой картиной был сам Ньютон. Не случайно свое главное сочинение он назвал “Математические начала натуральной философии”. В конце его он прокламирует применение тех же принципов к живым существам, чтобы и эта часть природы была включена в его “Систему Мира”. Он пишет: “Теперь следовало бы кое-что добавить о некотором тончайшем эфире, проникающем все сплошные тела и в них содержащемся, коего силою (. . .) возбуждается всякое чувство, заставляющее члены животных двигаться по желанию, передаваясь именно колебания-

ми этого эфира через тончайшие нити нервов от внешних органов чувств мозгу и от мозга мускулам. Но это не может быть изложено кратко, к тому же нет и достаточного запаса опытов, коими законы действия этого эфира были бы точно определены и показаны". Очевидно, Ньютон имеет в виду механическую теорию эфира и дает понять, что лишь недостаток места и неполнота экспериментальной базы мешают ему развить механическую теорию функционирования тел животных на базе теории эфира.

В то же время стали слышны и встревоженные голоса. Задавались вопросом: остается ли в этой Механической Системе Мира место для Бога? Можно было бы даже спросить — для чего-либо живого? Вселенная выглядела как гигантская машина, функционирующая исключительно на основе механических законов. И опять, наиболее встревожен был сам Ньютон. Религиозные убеждения Ньютона и до сих пор остаются несколько загадочными. Но несомненно, он был глубоко религиозным человеком. Бесспорно, противоречие между его Механической Системой Мира и его религиозными чувствами было для него очень болезненным. Он ясно выразил это в своей переписке. Когда ему было около 50 лет, Ньютон пережил тяжелый нервный кризис, некоторые исследователи говорят даже о психическом заболевании. Он не мог спать по несколько дней и ночей подряд. Его память была спутанной. Он переживал глубокую депрессию. А.И.Лапин обратил внимание на сходство этих симптомов с симптомами кризиса, пережитого Л.Толстым примерно в том же возрасте. Есть основания считать, что в обоих случаях мы имеем дело с кризисом мировоззрения.

Как бы то ни было, в более поздних публикациях Ньютона мы встречаем очень интересные новые идеи. Например, во втором издании "Начал" появилось знаменитое "Общее поучение", в котором мы находим такие высказывания: "Шесть главных планет обращаются вокруг Солнца приблизительно по кругам, концентрическим с Солнцем, по тому же направлению и приблизительно в той же плоскости. Десять лун обращаются вокруг Земли, Юпитера и Сатурна по концентрическим кругам, по одному направлению в плоскости орбит самих планет. Невозможно представить, что все эти правильные движения имеют началом механические причины, ибо кометы носятся во всех областях неба по весьма эксцентрическим орбитам. Вследствие движений такого рода кометы проходят через орбиты планет весьма быстро и легко, в своих же афелиях, где они движутся медленнее и остаются дольше, они весьма далеко отстоят друг от друга и весьма мало притягивают друг друга. Такое изящнейшее соединение Солнца, планет и комет не могло произойти иначе, как по намерению и по власти могущественного и премудро-

го существа”. (Здесь Ньютон явно имеет в виду очень специальное взаиморасположение планет, обеспечивающее устойчивость солнечной системы, так что одни планеты не падают на Солнце, а другие не уносятся в пространство.)

В “Оптике” Ньютон формулирует “вопросы” или “сомнения” (Queries), например, “Вопрос 23” (о механическом принципе): “На основании только этого принципа в мире никогда не было бы движения. Какой-то другой принцип был необходим, чтобы привести тела в движение, а сейчас, когда они движутся, необходим другой принцип для сохранения их движения”. В неопубликованном “Вопросе”, подготовленном для одного из изданий “Оптики”, читаем: “Если Вы думаете, что эта живая сила достаточна для сохранения движения, прошу указать мне эксперименты, из которых Вы делаете эти выводы. Знаете ли Вы из экспериментов, что биение сердца не придает дополнительного движения крови? и т.д. Если да, сообщите Ваши эксперименты, если нет — Ваши суждения ненадежны. Рассуждения, не основанные на экспериментах, весьма обманчивы”. Очевидно, весь дух и буква этих утверждений противоречит тому, о чем можно прочесть в конце “Начал”: здесь выражается сомнение в возможности объяснить деятельность живого организма при помощи “механического принципа”. Этот принцип считается применимым лишь к неживой природе, — и даже здесь с очень значительными ограничениями. Конечно, всегда остается трудный вопрос о границе между живой и неживой природой. Здесь тоже мы встречаемся с очень оригинальными взглядами Ньютона. В неопубликованном отрывке под заглавием “О не связанных с памятью законах природы” он пишет: “Земля напоминает громадное животное или скорее неодушевленное растение, вдыхающее эфир, подкрепляясь им ежедневно и выделяющее его мощным выдохом. И аналогично другим живым существам должна иметь свое время начала, молодости, старости и гибели”.

Ньютон был в высшей степени неоднoplanовым мыслителем. Его научные идеи и религиозные убеждения, видимо, не согласовывались: во всяком случае, в одном и том же его произведении можно найти противоречащие друг другу точки зрения. Но совершенно независимо от его внутреннего конфликта, его “Механическая Система Мира” оказала грандиозное влияние. Совершенно справедливо Ван дер Варден считает Ньютона, а не какого-либо короля или политического деятеля “самой значительной исторической фигурой XVII века”.

Не кто иной, как Вольтер, положил начало культу Ньютона во Франции, используя его авторитет как орудие в борьбе с Церковью. Однако кульминация научной идеологии и культа Ньютона связана

со школой Сен-Симона. В первой четверти XIX века Сен-Симон создал социалистическую систему, впоследствии оказавшую большое влияние на Маркса и Энгельса. Создатель философии позитивизма О.Конт был последователем и одно время секретарем Сен-Симона. Немецкий поэт Г.Гейне был страстным сен-симонистом.

Основой сен-симонизма была научная идеология. Вот несколько высказываний ведущих деятелей сен-симонизма. “Законы, управляющие человеческим обществом, столь же точны, как и те, которые управляют падением камня”. “Искусство и наука должны быть созданы с математической точностью, как учат рассчитывать мосты в Школе”. (Имеется в виду Норманская Школа в Париже.) Сен-Симон предлагал учредить поклонение Ньютону в особых храмах. Согласно его идее, общество должно управляться “Великим Ньютонианским Советом”, состоящим из лучших математиков, физиков, химиков и физиологов мира. В качестве председателя они должны избрать математика. Все провинции управляются “Малыми Ньютонианскими Советами”. Интересно, что среди ближайших последователей Сен-Симона были не только будущие революционеры и социалисты, но некоторые из самых преуспевших финансистов, впоследствии основавших крупнейшие французские банки и сети железных дорог. Так что во всех отношениях сен-симонизм повлиял как на развитие социалистических учений, так и современного капитализма.

Эта смесь сциентизма с техницизмом определяет и дух современной идеологии технической цивилизации. Великий биолог XX века Конрад Лоренц писал: “Категория морали применима к некоторому действию только, если оно направлено на нечто живое. Современный человек имеет дело главным образом с искусственными объектами. В результате он отучается оценивать свои действия с точки зрения морали и судит о них лишь с точки зрения эффективности. Поэтому встречаясь с чем-то живым, он его быстро уничтожает”. Современный социолог С.Рамо предлагает: “Сейчас мы должны планировать сосуществование с машинами. Мы становимся партнерами. Машины нуждаются для оптимального функционирования в некотором типе общества. Мы тоже имеем свои предпочтения. Но мы нуждаемся в том, что может дать машина и поэтому должны идти на компромисс. Мы должны так изменить законы общества, чтобы мы были совместимы”. Согласно принципам идеологии Технологической Цивилизации, все жизненные явления, которые не функционируют согласно “оптимальным правилам” машин, т.е. не могут быть механизированы, считаются ненадежными и неважными. Более того, они постепенно вытесняются. Людвиг фон Бартаманфи пишет: “Это (быть может, ис-

ключая атомную бомбу) является величайшим открытием нашего века: возможность редуцировать человека к автомату, “покупающему” все — от зубной пасты и Битлсов, до президентов, атомной войны и самоуничтожения”. Установка, рассматривающая любую деятельность человека как чисто технологическую, разрешает нам разрушать леса, губить китов, планировать и осуществлять социологические эксперименты в масштабе целых стран. Современный социолог Мак Лейш говорит: “После Хиросимы стало ясным, что наука лояльна не по отношению к человечеству, но к истине — ее собственной истине — что закон науки не есть закон блага — но закон возможного. Что для науки возможно, то она и должна сделать”.

Основная догма научной идеологии — это вера в то, что все измеримо, все может быть выражено в числах, переведено на язык математики.

Эта вера содержится уже в призыве Галилея: “Измерить все, что измеримо, и сделать измеримым то, что неизмеримо”. Особенно интересна вторая часть этой программы: как нам быть с любовью, состраданием, мужеством, нежностью? Очевидно, всем этим сторонам жизни нет места в математизированной концепции мира. В научной идеологии математизация играет ту же роль, что стандартизация в технике. Простейший путь применения математики — это счет. Но считать можно только однородные объекты. Пусть нам даны, скажем: яблоко, цветок, собака, дом, солдат, девушка, луна. Мы можем сосчитать их и сказать, что их 7 — но 7 чего? Единственный ответ — 7 предметов. Различия между собакой и луной, между яблоком и солдатом — исчезают: они все потеряли свою индивидуальность и превратились в лишенные признаков “предметы”. Счет убивает индивидуальность. Это самый примитивный пример, но во всех случаях присутствует тот же принцип. Другая особенность математики, очень существенная для научной идеологии — это ее способность трансформировать решение глубоких проблем в стандартизированные логические схемы. Например, квадратирование параболы или спирали в античности было проблемой, требующей усилий такого гениального математика как Архимед, основывалось на красивом арифметическом тождестве. Сейчас школьник старших классов может стандартным приемом вычислить $\int x^n dx$ при любом n . Более того, такое вычисление легко совершает компьютер. Возникает чувство, что вся математика может быть сведена к работе грандиозного компьютера.

Но большинство математиков несомненно согласится с тем, что их работа в принципе отличается от работы компьютера. Этот вопрос был предметом интересной дискуссии между Пуанкаре и

Гильбертом в начале нашего века. Та же проблема ставилась тогда иначе: формализуема ли математика? Ответ Гильберта был: “да” — и на этом пути он надеялся получить доказательство непротиворечивости арифметики. Пуанкаре не соглашался с ним. Позже теорема неполноты Геделя, по-видимому, решила вопрос в пользу Пуанкаре.

Пуанкаре подчеркивает роль интуиции в математическом рассуждении. Он говорит, что математическое рассуждение имеет “род творческой силы” и тем отличается от цепи силлогизмов. Особенно он выделяет математическую индукцию, которая, по его словам, “содержит бесконечное число силлогизмов, как бы сжатое в одной формуле”. Когда он говорит, что математик в принципе отличается от шахматиста, что он не может быть заменен никаким механическим устройством, то кажется, что ему лишь не хватало нужного термина, чтобы сформулировать свою мысль короче: “математик не может быть заменен компьютером”.

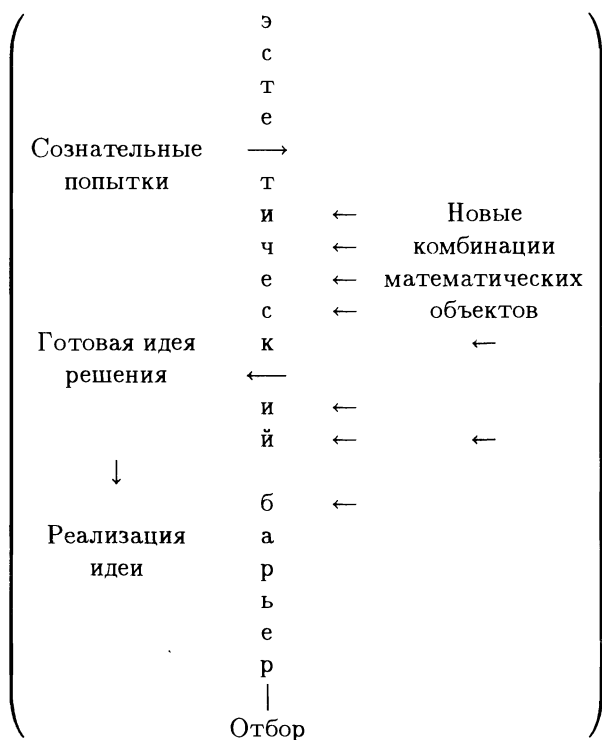
Особенно интересны взгляды Пуанкаре на роль эстетического чувства в математическом творчестве. Он говорит, что математическое открытие приносит чувство наслаждения, оно привлекательно как раз ввиду содержащегося в нем эстетического элемента. Если бы математика была лишь собранием силлогизмов, она была бы доступна всем — для этого была бы нужна лишь хорошая память. Но известно, что большинству людей математика дается с трудом. Пуанкаре видит причину в том, что силлогизмы складываются в математике в “структуру”, обладающую красотой. Чтобы понимать математику, надо “увидеть” эту красоту, а это требует эстетических способностей, которыми не все обладают.

Пуанкаре предлагает очень интересную схему математического творчества. Он связывает его с делением человеческой психики на сознательную и бессознательную части (см. рисунок). Процесс начинается с сознательных усилий, направленных на решение некоторой проблемы. Эти усилия повышают активность бессознательной части психики. Там появляется множество новых комбинаций математических объектов — как бы возможных фрагментов решения. Они появляются в громадном количестве и с колоссальной скоростью. Сейчас мы могли бы сравнить эту фазу с работой грандиозного компьютера. Но подавляющая часть этих комбинаций бесполезна для решения проблем. Они не достигают сознания, только очень небольшая их часть рассматривается сознанием. Чтобы достигнуть сознания, они проходят отбор, основанный на эстетическом принципе. Некий эстетический барьер позволяет лишь очень небольшому их числу проникнуть в сознание. Они появляются там как готовая идея решения, причем это сопровождается

очень сильным субъективным чувством уверенности в правильности идеи. Дальше остается лишь техническая работа по осуществлению найденной идеи.

Сознательная психика

Бессознательная психика



Эта схема очевидно напоминает картину эволюции, основанную на мутациях и естественном отборе, и, вероятно, возникла под ее влиянием. Гораздо позже, видимо, не зная об идеях Пуанкаре, Конрад Лоренц высказал аналогичные мысли. Он рассматривает жизнь как “процесс обучения”, “познавательный процесс”. Он подчеркивает черты, общие обоим явлениям — мышлению и эволюции — такие, как “творческое озарение”, “творческий акт”, когда после долгих поисков “почти мгновенно” возникает новая идея или новый вид. Но можно эту аналогию обратить и взглянуть на эволюцию как на результат деятельности некоего гигантского интеллекта или души Природы. Концепция “*anima mundi*” (души Природы) возникла в различных философских и мистических учениях: у Платона,

в христианстве. Когда в молодости я читал работы Пуанкаре, мне пришла в голову мысль об эволюции как процессе мышления и показалась очень привлекательной. Только много позже я узнал, что еще до Дарвина знаменитый естествоиспытатель Л.Агассиз рассматривал эволюцию как “мышление Бога”. Но если продолжить эту аналогию, то насколько красивее окажется точка зрения Пуанкаре сравнительно с принятой сейчас концепцией! Решающим фактором в эволюции оказывается не “борьба за существование”, а эстетический критерий. Тогда становится понятным, почему Природа порождает не только прекрасные растения и животные, но и решения проблемы адаптации видов, которые по красоте не уступают самым совершенным научным теориям.

Но профессиональным математикам вряд ли нужны какие-либо аргументы в пользу важности эстетического элемента в математике: в разговорах математика все время можно услышать: “изящное доказательство”, “прекрасная статья” ... Каждый математик знает, что в его работе эстетическое чувство не только дает удовлетворение, помогающее ему и облегчающее необходимые усилия, но и является рабочим средством, не менее важным, чем чисто логическое рассуждение. Он не будет следовать некоторой линии мыслей, так как она приводит к несимметричным, некрасивым формулам и он будет верить в некоторую гипотезу и не пожалеет сил для ее доказательства только потому, что она очень красива. С этой точки зрения математика играет противоположную анти-технологическую роль. Мы видим, как под воздействием технологической цивилизации красота все больше исчезает из нашей жизни: из живописи и музыки, из архитектуры наших городов и из окружающей нас Природы: в виде прекрасных бабочек, цветов и птиц. Математика (вместе с математической физикой) остается почти единственным островом, в котором это загадочное явление сохраняется в полной силе. Иисус спросил: “Что есть истина?” Явление красоты не менее загадочно. Очевидно, что это — одна из фундаментальных форм взаимодействия с внешним миром, столь же существенная для большинства живых существ, как феномен истины и морали — для человека.

Один мой друг, геолог, высказал следующую мысль. Многие виды гибли из-за гипертрофированного развития признаков, первоначально очень полезных для их выживания. Например, громадная броня гигантских третичных ящеров. Для Homo Sapiens эту роль может сыграть его интеллект: способность к холодному, рациональному мышлению, но ограниченному моралью или жалостью. Математика несомненно как-то связана со способностью к такому алгоритмическому, машинообразному мышлению. С другой сторо-

ны, она глубоко связана с эстетическим чувством, которое способно служить противовесом для этой тенденции. И математик имеет свободу выбора принять участие в том или другом направлении развития человечества.

ТАК СДЕЛАЙТЕ НЕВОЗМОЖНОЕ!
(К 80-ЛЕТИЮ Л. С. ПОНТРЯГИНА)
ГАЗЕТА "СОВЕТСКАЯ РОССИЯ" 16.04.1989

Оценивая сделанное Понтрягиным в науке, все чаще прихожу к мысли, что он принадлежит в числу лучших математиков, которых дала Россия, что он — один из самых ярких математических умов своего поколения. Одних только понятий и теорем, носящих его имя, прочно вошедших в понятийный аппарат, десятки: “понтрягинский квадрат”, “принцип максимума Понтрягина”, “характеристические классы Понтрягина” и многое другое. Сосредоточившись уже только на этом, можно было бы писать характер ученого, недостижимого в своих математических открытиях даже для тех, кого природа одарила щедро. Но значение человеческой личности Понтрягина, ее масштаб — значительно, глубже всего, сделанного в науке.

В молодости он начал заниматься одним из самых тогда перспективных разделов математики — топологией. Как известно, математика состоит из многих разделов, но один из них играет обычно особую роль. Выработанные в нем идеи, точки зрения, общие понятия находят применение и в других разделах, особенно сильно влияют на их развитие. Математики обычно говорят, что это сейчас “модный” раздел. Роль подобной “лаборатории идей” перемещается каждые 20–30 лет от одного раздела математики к другому. Как раз в 30-е и 40-е годы нашего века ею была топология. В одном современном романе герой вспоминает, чему обучался на математическом факультете: “Топология... стратосфера человеческой мысли”. Одним из нескольких создателей этой “стратосферы” и был Лев Семенович Понтрягин.

Он добился здесь многого: к 50-м годам стал одним из крупнейших авторитетов в математическом мире. И вдруг решил изменить область своих исследований.

Я много раз спрашивал его, почему он это сделал. Лев Семенович обычно говорил:

- Да вот меня часто спрашивали, зачем нам то, чем вы, теоретики, занимаетесь?

Молодым человеком он вообще не собирался становиться математиком, а его интересы были больше технического характера.

Интерес к конкретным вопросам жизни у него проявлялся всегда, в том числе и в некоторых ранних работах. Думаю, что в конце концов все решалось не какими-то внешними стимулами, а внутренней логикой его развития. Тем не менее это был очень трудный и болезненный процесс. Ведь долгая работа в одной области дает большой опыт, владение многими приемами, множество пока не реализованных, хранимых “про запас” наблюдений. Завоеванное признание коллег придает чувство уверенности в себе. От всего этого пришлось отказаться, все создавалось заново. Из “мэтров” Понтрягин вернулся в “начинающие” и перешел от одной из самых абстрактных областей математики к такой, которая была неразрывно связана с техникой. Как он рассказывал, много лет и громадный труд был им потрачен на беседы с техниками, на попытки уяснить себе их технические проблемы, понять их математический смысл и почувствовать, какие принципиально новые концепции математики за этими проблемами скрываются. На столь резкое изменение всего стиля научного мышления способны немногие. Но Понтрягин и в этой области сумел пройти путь от “начинающего” до “мэтра”, признанного во всем мире.

Математика имеет удивительное свойство высасывать всего человека, забирать все силы. Для занятий ею не нужны ни сложные лаборатории, ни экспедиции, все зависит от самого человека. К тому же, оперируя очень абстрактными понятиями, она не требует жизненного опыта, в принципе математическое творчество доступно и подростку. Благодаря этому создается необычный накал чувств, захватывающий человека целиком, порой с очень раннего возраста. Накал бывает столь велик, что не оставляет сил на другие стороны жизни — причем как раз у наиболее выдающихся математиков. Целиком отдавая себя науке, они жертвуют многим, в том числе бледнеют и некоторые аспекты их личности. И здесь, как во многих других отношениях, Л.С.Понтрягин был исключением: его поразительно яркая индивидуальность не только бросалась в глаза, но мощно влияла на всю жизнь математического сообщества и далеко за его пределами. Психологический импульс, который двигал им, Лев Семенович не раз описывал мне. “Я всю жизнь боялся”, — не раз говорил Лев Семенович, и, зная его, я принимал это за шутку или даже кокетство. Пока не обратил внимание на то, чего же он боялся. Он действительно всегда опасался неудачи своего дела. Того, что начатое математическое исследование не удастся, и

затраченные громадные усилия пропадут даром, что напечатанная работа окажется неверной, что важное начинание натолкнется на противодействие . . . И этот страх заставлял его напроочь забывать о том, чего бояться "обычные" люди: переутомления, испорченных отношений, неудовольствия начальства, притеснений. Именно этим бесстрашием прославился Лев Семенович сначала среди математиков, а потом и гораздо шире. Например, математик В.А.Ефремович рассказывал мне, что весь срок, который он в сталинское время отбывал в лагере, ему регулярно шли письма Л.С.Понтрягина, — это в то время, когда человек, пославший и одно такое письмо, гордился этим. На бесстрашии и основывалась во многом та особая роль, которую Понтрягин играл в общественной жизни. Я очень хорошо помню, как впервые услышал о нем. Это было в 1939 году в связи с выборами в Академию наук. Был выдвинут один математик, и ходил слух (впоследствии не подтвердившийся), что в ЦК есть желание, чтобы он остался единственным кандидатом. На заседании Московского математического общества Лев Семенович нарушил это своеобразное табу и в яркой, аргументированной речи предложил кандидатуру А.Н.Колмогорова — одного из ведущих математиков того поколения. Он стал в итоге академиком. В то время понтрягинская "непокорность" могла стоить дорого.

Вспоминается и другой, гораздо более драматичный случай, свидетелем которого я уже был сам. Это был конец 40-х — эпоха громких постановлений о литературе, музыке, биологии. Не трогали только физиков, они были в привилегированном положении, особом, некоторых даже вернули из лагерей. Думаю, после создания атомной бомбы наши властелины стали бояться, что ученые и техники выйдут из-под контроля. Тут, пожалуй, и возникла идея: для острастки физиков устроить погром у соседей — математиков. Как из-под земли возникло письмо, подписанное тремя малоизвестными ленинградскими "коллегами", в котором требовалось "пересмотреть" положение в советской математике, указывалось на враждебные "декадентские" течения в ней. Сегодня это смешно, а тогда для обсуждения письма было создано расширенное заседание Ученого совета Математического института Академии наук. После оглашения послания противников математического декаданса председательствующий предложил высказываться. Наступила тишина, и в эти секунды, быть может, решалась судьба нашей математики на целые годы. Начни тогда кто-то призывать к "исправлению ошибок" — и можно себе представить последствия по уже состоявшимся прецедентам. Вдруг раздался спокойный, как будто даже скучающий голос Понтрягина: "А почему, собственно, мы обсуждаем это письмо на Ученом совете?" Председательству-

ющий разъяснил, что это “письмо трудящихся”, присланное нам через ЦК.

- Институт получает немало писем “преобразователей математики”, почему обсуждаем на Ученом совете именно это?

Не помню, какой ответ был получен, но гипнотизирующая атмосфера страха рассеялась. Сначала робко, потом посмелее члены совета стали возражать авторам, и заседание закончилось резолюцией, берущей математику под защиту, хотя и со всей осторожностью и оговорками, типичными для того времени.

Нежелание покоряться “авторитетам” определяло деятельность Понтрягина и в других сферах. Уже в последние годы жизни он почувствовал трагичность экологической ситуации в нашей стране и очень много сделал для борьбы с проектом “поворота рек”, потратив на это массу энергии. В Математическом институте он создал семинар, работы которого помогли показать всю необоснованность расчетов, лежащих в основе “проекта века”. Он создал также лабораторию математических вопросов экологии при руководимом им отделе, был среди подписавших письмо против поворота рек. Решительно выступал на встрече в ЦК КПСС, куда были приглашены авторы письма.

Но, пожалуй, наиболее широкое, воистину всенародное влияние на жизнь оказала деятельность Л.С.Понтрягина, связанная с преподаванием математики в средней школе. В 70-е годы у нас сложился совершенно новый стиль преподавания математики, были созданы новые, в корне отличающиеся от прежних учебники. Принцип, заимствованный с некоторым опозданием с Запада, заключался в разрыве с интуицией, в крайней формализации изложения. Причем проблема была глубже, чем может показаться с первого взгляда. Дело в том, что в математике (и в той, которая преподается в школе тоже), кроме ее “прикладного” значения, имеется еще эстетический элемент. Это очень своеобразная красота — красота идеи. Для творчески работающего математика она часто убедительнее формального рассуждения, он говорит: это рассуждение так красиво, что должно быть верным. Чувство красоты математического рассуждения доступно практически каждому и является важной частью общей культуры. Новая же система преподавания ее разбивала. Получалось так, как если бы в художественном училище обучение живописи начиналось не с копирования классических статуй, а с подражания Пикассо. И аргументация была похожей. Когда школьники, ничего не понимая ни в классе, ни из учебника, обращались к родителям, а те, сами ничего не поняв, протестовали, то им отвечали: это замечательно, что вы ничего не поняли, у вас старый багаж, а мы преподаем новую науку!

Многие математики осознавали серьезные последствия сложившегося положения: терялась часть культуры, математика теряла потенциальные таланты; но изменить его было очень нелегко. Создание новых учебников было в своем роде тоже проектом поворота, только не рек, а преподавания математики, и поддержка его была столь же массивной. Сломить ее удалось Льву Семеновичу. Больше года он боролся, сочетая бурный натиск и дипломатию, пока, наконец, ему не удалось опубликовать свои взгляды в журнале "Коммунист". В этом ему очень помогли журналисты. В конце концов дорога к пересмотру учебников была открыта. В их реанимации потом участвовало много людей, но прорыв, право на ее проведение завоевал Л.С.Понтрягин. Мне кажется, у нас пока нет ясных и прозрачных учебников по математике, какие были несколько десятилетий назад, но все же "геркулесовы столбы" формалистического творчества остались позади, положение в какой-то степени нормализуется, и результат сказывается на десятках миллионов подростков, на их умах и душах.

Страстная, темпераментная индивидуальность Льва Семеновича проявилась и в его личных отношениях. Он был необыкновенным другом — я наблюдал это не раз, испытал на себе самом. Он не просто соглашался помочь своему другу — его проблемы он усваивал, как свои, все время думал, какими способами разрешить их, пробовал различные пути, не жалея ни сил, ни нервов, ни отношений с влиятельными лицами. Мой однокурсник, ныне покойный Владимир Абрамович Рохлин, во время войны попал в окружение. Долго его скрывали крестьяне, но все же он был обнаружен немцами и оказался в концлагере, а в конце войны, после освобождения, перекочевал в проверочный лагерь уже на нашей стороне фронта. Лев Семенович знал его как способного студента. И взялся ему помочь. В результате бесчисленных писем, телефонных звонков, хождения по "инстанциям" удалось добиться, чтобы Рохлин был освобожден и зачислен в Математический институт в качестве помощника Льва Семеновича. И ведь поразительно, что Рохлин не был даже его прямым учеником, он окончил университет по другой специальности, у него был другой научный руководитель, но хлопоты взял на себя Лев Семенович. В результате совместной работы он заинтересовал Рохлина топологией, и тот стал одним из наиболее известных продолжателей идей Л.С.Понтрягина в этой области. Аналогичных случаев в жизни Понтрягина немало.

Не менее темпераментно, чем симпатии, проявлялись, правда, и антипатии Льва Семеновича. Лишь после смерти я узнал, что одним из любимых произведений Понтрягина было жизнеописание Бенвенуто Челлини, и это сделало мне более понятным Льва Семеновича. У обоих было действительно много общего, и мне представляется, что если бы почтенный академик жил во времена Челлини,

он тоже многие споры решал бы при помощи собственной шпаги и уж, во всяком случае, не обращался бы к помощи наемных убийц. Как и у Челлини, у Понтрягина было немало недоброжелателей. Его не раз обвиняли в субъективности и агрессивности, изображали “антисемитом” и чуть ли не человеконенавистником. На самом деле его отношение к людям было гораздо глубже таких примитивных характеристик.

В подражание Челлини Лев Семенович подготовил рукопись воспоминаний “Жизнеописание Льва Семеновича Понтрягина, написанное им самим”. Это замечательное произведение, и я очень надеюсь увидеть его опубликованным. Только оно может дать полное представление о том постоянном напряжении духовных сил, которое было обычным стилем жизни автора. Он исключительно ярко описывает мучения, которые испытывал, когда заметил, что в лекциях, прочитанных в одном из американских университетов, оказалась серьезная ошибка. О том, как целый месяц мучился, не мог взяться за ее исправление, а потом вдруг мелькнула идея, он работал, почти не переставая, еще месяц — и ошибку исправил. Вся жизнь его протекала в каком-то более мощном ритме, чем у других людей. Плутарх говорит, что знавшие Александра Македонского уверяли, будто его тело теплее, чем у обычных людей. Я не удивился бы, если бы энцефалограмма показала, что какие-то ритмы мозговой активности Понтрягина тоже выходили за пределы нормы.

Мне запомнился один телефонный разговор. Собеседник отказался сделать то, на чем настаивал Лев Семенович, дескать, это невозможно. “Так сделайте невозможное!” — воскликнул Понтрягин. Тогда мне показалось — “красное словцо”, риторический оборот. Но позже я понял, что он просто говорил о подходе к жизни, который для него-то был обычным! Лев Семенович все время делал то, что другие сочли бы невозможным. Борьба со страшным несчастьем, которое в молодости на него обрушилось, возможно, как раз выковала его характер. Понтрягин нашел свой путь — он отказался признать это несчастье, объявил ему войну и победил. Он никогда не пользовался приспособлениями для слепых — книгами с особым шрифтом, например. Лекции в университете он не записывал, а все запоминал и потом ночами, лежа в постели, курил и продумывал их. Он предпочитал ходить один, без помощи других, часто падал, ушибался, у него постоянно были рубцы и ссадины. И, что самое трудное, он сумел полностью избежать психологии в чем-то неполноценного человека. Никто о нем никогда не думал как о слепом. На это указывал и такой тонкий барометр, как его отношение к женщинам и их отношение к нему.

Почему Лев Семенович успел сделать так много? Я думаю, потому, что никогда не спрашивал себя, хватит ли у него сил на

какое-либо дело. Брался за дело, а силы находились сами. Он постоянно перешагивал через границы возможного.

АБЕЛЕВА И НЕАБЕЛЕВА МАТЕМАТИКА

*THE MATH. INTELLIGENCER, 13, 67-7, 1991**

Многие теории, принадлежащие к числу самых красивых глав математики XIX и XX вв., имеют общее алгебраическое ядро — теорию двойственности абелевых групп и их групп характеров. Естественно предположить, что ряд принципиальных трудностей математики объясняется тем, что неизвестно обобщение этой двойственности на неабелевы группы. Такая точка зрения сформулирована в работе А.Вейля [6]. Философия “неабелевой математики будущего” вдохновляла и меня, когда я только начинал заниматься математикой. Сейчас, полвека спустя, мне кажется интересным подвести итог того, что в этом направлении достигнуто. Тем более, что нерешенных вопросов здесь по-прежнему остается гораздо больше, чем решенных, так что старая программа, видимо, может вдохновлять еще не одно поколение. Цель нижеследующего обзора — дать хотя бы самое общее представление о переплетении возникших здесь идей.

I. Абелева математика

1. Двойственность между конечномерным векторным пространством V и его сопряженным V^* может быть задана при помощи спаривания $(x, y) \in \mathbb{R}$, $x \in V$, $y \in V^*$, линейного по каждому аргументу. Это спаривание должно быть невырожденным, т.е. если $(x, y) = 0$ для всех $y \in V^*$, то $x = 0$ и аналогично с перестановкой x и y . Подпространству $W \subset V$ соответствует ортогональное подпространство $W^\perp = \{y \in V^*; (x, y) = 0 \text{ для } x \in W\}$. Соответствие $W \rightarrow W^\perp$ есть предмет теории линейных уравнений. Переход к проективным пространствам $\mathbb{P}(V)$ и $\mathbb{P}(V^*)$ приводит к двойственности в проективной и алгебраической геометрии. Если V — банахово пространство, то таково же и V^* , а их единичные

*В журнале опубликован английский перевод. Здесь публикуется русский оригинал.

сферы — двойственные выпуклые множества (например, икосаэдр и додекаэдр, куб и октаэдр — двойственны друг другу).

Важнейший пример спаривания дает интегрирование дифференциальных форм. Если, например, ω — одномерная дифференциальная форма, а σ — кривая на многообразии X , то $\int_{\sigma} \omega$ можно рассматривать как спаривание (σ, ω) . Точнее, спаривание определено между пространством одномерных гомологий $H_1(X, \mathbb{R})$ и факторпространством $\{\omega, d\omega = 0\} / \{\omega = df\}$. Невырожденность этого спаривания и его обобщений на m -мерные цепи и формы гарантирует теорема де Рама (можно так же всюду заменить $\mathbb{R}$ на $\mathbb{C}$).

Задание на V невырожденной симметрической формы определяет изоморфизм $V^* \simeq V$. Если вещественное пространство V ориентировано, то операция $W \rightarrow W^{\perp}$ переносится на соответствующие разложимые поливекторы и определяет изоморфизм $*$: $\Lambda^m V \simeq \Lambda^{n-m} V^*$, $n = \dim V$. Эта операция переносится на дифференциальные формы на многообразиях. Например, электрическому и магнитному полям, заданным векторами $E = (E_1, E_2, E_3)$ и $H = (H_1, H_2, H_3)$ соответствует двумерная форма в 4-х мерном пространстве времени $\mathbb{R}^4$: $\omega = \sum_1^3 E_i dx_i \wedge dt + H_1 dx_2 \wedge dx_3 + H_2 dx_3 \wedge dx_1 + H_3 dx_1 \wedge dx_2$. Если метрика в $\mathbb{R}^4$ имеет вид $dt^2 - \sum_1^3 dx_i^2$, то $*\omega = -\sum H_i dx_i \wedge dt + E_1 dx_2 \wedge dx_3 + E_2 dx_3 \wedge dx_1 + E_3 dx_1 \wedge dx_2$. Операция $*$ отражает двойственность электрического и магнитного поля. Уравнения Максвелла в отсутствии токов имеют вид: $d\omega = 0$, $d(*\omega) = 0$. Аналогичные соотношения на произвольном римановом многообразии приводят к теории гармонических дифференциальных форм и теории Ходжа.

2. Характеры конечной абелевой группы A — это гомоморфизмы $\chi: A \rightarrow U(1)$ в одномерную унитарную группу $U(1) = \{z \in \mathbb{C}, |z| = 1\}$. Двойственность между группой A и группой характеров $X(A)$ также задается невырожденным спариванием $(a, \chi) = \chi(a) \in U(1)$, $a \in A$, $\chi \in X(A)$. Гомоморфизм $f: A \rightarrow B$ определяет гомоморфизм $X(f): X(B) \rightarrow X(A)$, который переводит $\chi \in X(B)$ в композицию f и χ . Если f есть вложение A в B , то $X(f)$ — отображение на все $X(A)$. Ядро гомоморфизма $X(f)$ в этом случае обозначается $A^{\perp}$ и обладает всеми свойствами ортогонального подпространства. В частности,

$$X(B/A) \simeq A^{\perp} \quad (1)$$

Характеры $\chi \in X(A)$ образуют базис пространства $F(A)$ комплекснозначных функций на A , $\dim F = |A|$, т.е. порядку A . Разло-

жение $\varphi = \sum_{\chi} c(\chi)\chi$ для $\varphi \in F(A)$ называется разложением Фурье функции φ .

Если для всех $a \in A$, $a^m = 1$, то значения характеров группы A — корни степени m из 1. Предположим, что все они содержатся в поле K . Они образуют группу, обозначаемую μ_m . Далее, чтобы сократить формулировки, мы будем всегда рассматривать поля характеристики 0. Пусть V — конечномерное векторное пространство над полем K , в котором задано действие группы A (т.е. в V задано ее представление). Тогда существует разложение

$$V = \oplus e_i K, \quad (2)$$

в котором одномерные подпространства $e_i K$ инвариантны относительно действия группы A , т.е. $a \cdot e_i = \chi_i(a)e_i$, где $\chi_i \in X(A)$.

Изложенные выше понятия обобщаются на топологические локально-бикомпактные группы — это теория двойственности Понтрягина. В такой общности они содержат теорию рядов и интегралов Фурье и математическое описание квантово-механической двойственности волна-частица.

Отметим простейшие примеры.

(а) Группы $\mathbb{Z}$ и $U(1)$ двойственны друг другу: спаривание $n \in \mathbb{Z}$ и $\alpha \in U(1)$ есть $(n, \alpha) = \alpha^n$.

(б) Группа $\mathbb{R}$ (по сложению) двойственна себе: спаривание есть $(x, y) = e^{2\pi i xy}$.

(с) То же верно для группы $\mathbb{C}$: $(z_1, z_2) = e^{2\pi \operatorname{Re}(z_1 \bar{z}_2)}$.

3. Теория Галуа абелевых расширений. Поле комплексных чисел $\mathbb{C}$ имеет два автоморфизма, сохраняющих вещественные числа: единичный и $\tau(z) = \bar{z}$. Иначе говоря, $G = \{1, \tau\}$ — это группа Галуа расширения $\mathbb{C}/\mathbb{R}$ (записывается как $\operatorname{Gal}(\mathbb{C}/\mathbb{R}) = G$). В этом смысле $\mathbb{C}$ является представлением группы G и разложение (2) имеет вид $\mathbb{C} = \mathbb{R} + i\mathbb{R}$. Это связано с тем, что $\mathbb{R} \cup i\mathbb{R}$ — единственные комплексные числа z , для которых $z^2 \in \mathbb{R}$.

Пусть вообще L/K — расширение Галуа, $G = \operatorname{Gal}(L/K)$ и $\mu_m \subset K$ для некоторого целого $m > 0$. Если L содержит радикал $\sqrt[m]{a}$ для $a \in K$, $a \neq 0$, то для любого $\sigma \in G$ $(\sigma(\sqrt[m]{a}))^m = a$ и значит $\sigma(\sqrt[m]{a})/\sqrt[m]{a} \in \mu_m$. Тем самым определяется спаривание между группой G и группой X тех $a \in K$, $a \neq 0$, для которых $\sqrt[m]{a} \in L$: $(\sigma, a) = \sigma(\sqrt[m]{a})/\sqrt[m]{a}$. Группа $\{a \in K, a \neq 0\}$ (по умножению) обозначается K^* . Легко видеть, что (σ, a) есть спаривание между G и X/K^{*m} , где $K^{*m} = \{a^m, a \in K^*\}$. Если поле L порождается радикалами $\sqrt[m]{a}$, $a \in X$, то мы будем писать $L = K(\sqrt[m]{X})$. В этом случае спаривание (σ, a) невырождено, так что $G = X(X/K^{*m})$ и,

в частности, группа G коммутативна. Расширения с коммутативной группой Галуа называются абелевыми. Разложение (2) в этом случае принимает вид

$$L = \bigoplus_{a \in X/K^{*m}} \sqrt[m]{a}K.$$

Наоборот, если G — такая абелева группа, что $g^m = 1$ для всех $g \in G$ и $\mu_m \subset K$, то любое расширение L/K с группой Галуа G имеет вид $L = K(\sqrt[m]{X})$ для некоторой группы X , $K^* \supset X \supset K^{*m}$. Это и есть теория Абеля решения в радикалах уравнений “с коммутативной группой Галуа”, хотя теперь она называется теорией Куммера. Ей можно придать еще более изящный вид, рассмотрев объединение K_m^{ab} всех расширений поля K с группами Галуа указанного типа при заданном числе m . Как правило, это бесконечное расширение: например, при $K = \mathbb{Q}$, $m = 2$ оно получается присоединением к $\mathbb{Q}$ $\sqrt{-1}$ и всех $\sqrt{p}$, где p — простые числа. Группа Галуа бесконечного расширения, как и вообще группа преобразований бесконечного множества, имеет естественную топологию: окрестностями единицы являются стабилизаторы конечных множеств. В этой топологии она бикompактна и теория Куммера утверждает, что группа $\text{Gal}(K_m^{ab}/K)$ двойственна дискретной группе K^*/K^{*m} .

4. Теория абелевых функций. Речь идет об аналоге теории Куммера для случая, когда K является полем рациональных функций $\mathbb{C}(S)$ на алгебраической кривой S . Например, если S задана (в аффинных координатах) уравнением $F(x, y) = 0$, то $\mathbb{C}(S) = \mathbb{C}(x, y)$, где x и y связаны этим соотношением. Кривая S считается вложенной в некоторое проективное пространство $\mathbb{P}^N$ и как его замкнутое подмножество сама является топологическим пространством, ориентируемой поверхностью: сферой с g ручками, g называется родом кривой S и поля K . Если $K = \mathbb{C}(S)$ и $K' \supset K$ — конечное расширение, то $K' = \mathbb{C}(S')$, где S' — другая алгебраическая кривая и вложение $K \subset K'$ определяется рациональным отображением $\varphi: S' \rightarrow S$, являющимся конечнолиственным накрытием. Мы рассмотрим случай, когда φ — неразветвленное накрытие, т.е. все точки $s \in S$ имеют одинаковое число прообразов. Это число равно степени $[K': K]$ расширения K'/K . Тогда и K'/K называется неразветвленным расширением.

В этом случае задача является по существу топологической. Действительно, из основных результатов теории алгебраических кривых и римановых поверхностей следует, что топологический тип накрытия $S' \rightarrow S$ уже однозначно определяет кривую S' и поле $K = \mathbb{C}(S')$ (с точностью до изоморфизма), и любое неразветвленное

ное конечнолистное топологическое накрытие определяется некоторой кривой S' . Таким образом, совокупность всех неразветвленных расширений K'/K “изоморфна” совокупности топологических конечнолистных накрытий. Последние же, как известно, описываются подгруппами конечного индекса фундаментальной группы $\pi_1(S)$ кривой S , которая тоже полностью известна — она имеет $2g$ образующих $a_1, \dots, a_g, b_1, \dots, b_g$ и определяется одним соотношением:

$$a_1 b_1 a_1^{-1} b_1^{-1} \dots a_g b_g a_g^{-1} b_g^{-1} = 1.$$

Это описание, однако, основано на топологических и аналитических соображениях и возникает задача — найти его алгебраический эквивалент. Ответ известен для случая абелевых неразветвленных накрытий.

Неразветвленные топологические накрытия с абелевой группой автоморфизмов соответствуют подгруппам конечного индекса факторгруппы группы $\pi_1(S)$ по ее коммутанту, которая изоморфна группе $H_1(S, \mathbb{Z})$. Эта группа изоморфна $\mathbb{Z}^{2g}$. Далее мы будем обозначать ее H . Алгебраическая интерпретация подгрупп конечного индекса $\Gamma \subset H$ связана с вложением $H \subset \mathbb{C}^g$, использующим двойственность гомологий и форм из п.1. Именно, на S существует g линейно независимых голоморфных 1-форм $\omega_1, \dots, \omega_g$ (“дифференциалов 1-го рода”). Сопоставление $\sigma \rightarrow (\int_{\sigma} \omega_1, \dots, \int_{\sigma} \omega_g)$, $\sigma \in H$ определяет вложение $H \subset \mathbb{C}^g$, причем $\mathbb{C}^g = H \cdot \mathbb{R}$. Факторгруппа $\mathbb{C}^g/H$ является g -мерным комплексным тором. Он называется якобианом кривой S и обозначается $J(S)$. Кривая S может быть в него вложена (при $g > 0$). Именно, выберем некоторую точку $s_0 \in S$ и соединим любую точку $s \in S$ путем σ с s_0 . Отображение

$$j(s) = \left(\int_{\sigma} \omega_1, \dots, \int_{\sigma} \omega_g \right) \bmod H \quad (3)$$

не зависит от выбора пути σ и определяет вложение S в $J(S)$.

Якобиан является проективным алгебраическим многообразием и при помощи отображения (3) может быть построен чисто алгебраически. Мы скажем об этом позже, а пока изложим описание подгрупп конечного индекса $\Gamma \subset H$, $(H : \Gamma) < \infty$ в терминах якобиана.

Индекс пересечения определяет в H кососимметрическую целочисленную унимодулярную форму $\langle a, b \rangle$, которую мы распространим по линейности на $\mathbb{C}^g = H \cdot \mathbb{R}$. Функция $\langle x, y \rangle = e^{2\pi i \langle x, y \rangle}$, $x, y \in \mathbb{C}^g$, определяет спаривание $\mathbb{C}^g$ с собой, при котором $H^{\perp} = H$. Отсюда ввиду (1) в п.2

$$J(S) \simeq X(H). \quad (4)$$

Если $\Gamma \subset H$, то $\Gamma^\perp \supset H$, $(\Gamma^\perp : H) = (H : \Gamma)$. Если $(H : \Gamma) < \infty$, то группа $\Gamma^\perp/H \subset \mathbb{C}^g/H$ является конечной подгруппой тора $J(S)$ и так получаются все его конечные подгруппы. Отсюда следует, что существует взаимно-однозначное соответствие между конечными подгруппами $\Gamma' \subset J(S)$ и абелевыми неразветвленными расширениями K'/K . При этом, как легко видеть, $\text{Gal}(K'/K) = X(\Gamma')$.

Если мы введем, как в п.3, максимальное абелево неразветвленное расширение K_{nr}^{ab} поля K , то этот результат выражается формулой

$$\text{Gal}(K_{nr}^{ab}/K) = X(J(S)_{\text{tors}}),$$

где вообще $\mathcal{A}_{\text{tors}}$ обозначает подгруппу элементов конечного порядка абелевой группы $\mathcal{A}$.

Конечно, подгруппа Γ' может быть охарактеризована и как ядро гомоморфизма торов $\mathbb{C}^g/H \rightarrow \mathbb{C}^g/\Gamma^\perp$ и определяется однозначно гомоморфизмом $\mathbb{C}^g/\Gamma \rightarrow \mathbb{C}^g/H$. В последнем случае и само накрытие $S' \rightarrow S$ восстанавливается как прообраз S (точнее, $j(S) \subset \mathbb{C}^g/H$) при этом гомоморфизме.

Остается привести алгебраическое описание якобиана. Оно основывается на следующих понятиях. Формальная комбинация $D = m_1 s_1 + \dots + m_r s_r$, $m_i \in \mathbb{Z}$, $s_i \in S$ называется дивизором на кривой S . Все они образуют группу $\text{Div}(S)$. Число $\sum m_i = \deg D$ называется степенью дивизора D . Дивизоры степени 0 образуют подгруппу $\text{Div}^0(S) \subset \text{Div}(S)$. Если функция $f \in \mathbb{C}(S)$, $f \neq 0$, имеет нули и полюса $s_1, \dots, s_r$ на S кратностей $m_1, \dots, m_r$ ($m_i > 0$ для нуля и $m_i < 0$ для полюса), то $(f) = \sum m_i s_i$ называется дивизором функции. Все дивизоры (f) , $f \in \mathbb{C}(S)$, $f \neq 0$ образуют группу $P(S) \subset \text{Div}(S)$. Всегда $\deg(f) = 0$ (число нулей равно числу полюсов), поэтому $P(S) \subset \text{Div}^0(S)$.

Теорема Абеля–Якоби утверждает, что

$$\text{Div}^0(S)/P(S) \simeq J(S). \quad (5)$$

Изоморфизм (5) задается условием

$$\varphi\left(\sum m_i s_i\right) = \sum m_i j(s_i),$$

где справа знак $\sum$ обозначает сумму в группе $J(S)$.

Это и есть алгебраическая характеристика якобиана $J(S)$. Она дает возможность описать его в чисто алгебраических терминах

как g -мерное алгебраическое многообразие в проективном пространстве.

Существует другая его важная интерпретация. Она основывается на том, что дивизор $D = \sum m_i s_i$ можно задать, указав функции f_i , имеющие в точках $s_i \in S$ нули или полюса кратностей m_i . При этом мы допускаем замены $f_i \rightarrow f_i u_i$, где $u_i(s_i) \neq 0, \infty$. Можно даже считать, что в любой точке $s \in S$ задана функция $f_s \neq 0$, $f_s(s) \neq 0, \infty$ для почти всех $s \in S$. "Почти все" означает — все, кроме конечного числа.

Тогда

$$\text{Div}(S) = \{f_s, f_s \neq 0, f_s(s) \neq 0, \infty$$

для почти всех $s \in S\} / \{u_s, u_s(s) \neq 0, \infty \text{ для всех } s \in S\}.$

Пусть дивизор D задан точками $s_1, \dots, s_r$ и функциями $f_1, \dots, f_r$. Рассмотрим такие окрестности $U_i \ni s_i$, что $f_i \neq 0, \infty$ в $U_i \setminus s_i$, введем еще одно такое открытое множество U_0 , что $U_0 \cup (\cup U_i) = S$ и положим для него $f_0 = 1$. По этим данным можно построить расслоение E_D над S со слоем $\mathbb{C}$. Над U_i оно имеет вид $U_i \times \mathbb{C}$, и точки $(s, z) \in U_i \times \mathbb{C}$ и $(s, z') \in U_j \times \mathbb{C}$ отождествляются, если $s \in U_i \cap U_j$, $f_i z' = f_j z$. Так как в $U_i \cap U_j$ функция $f_j^{-1} f_i \neq 0, \infty$, то это — изоморфное отображение, E_D — локально тривиальное комплексное расслоение. Оно зависит только от дивизора D : замена $f_i \rightarrow f_i u_i$, $u_i \neq 0, \infty$ в U_i не меняет его типа. Но оно не меняется и при замене $f_i \rightarrow f f_i$, т.е. зависит лишь от образа D в группе $\text{Div}(S)/P(S)$. Топологический тип расслоения E_D определяется числом $\deg D$ (т.е. его классом Черна $c_1(E_D)$). Таким образом группа $J(S) = \text{Div}^0(S)/P(S)$ описывает множество локально-тривиальных аналитических (или алгебраических) расслоений над S со слоем $\mathbb{C}$, которые топологически тривиальны.

Вся изложенная теория обобщается на разветвленные накрытия: для описания накрытий, разветвленных в конечном множестве $\Sigma \subset S$ надо использовать группу $H_1(S - \Sigma, \mathbb{Z})$. Она обобщается и на алгебраические многообразия произвольной размерности n .

5. Теория полей классов — это теория абелевых расширений полей алгебраических чисел, т.е. конечных расширений поля рациональных чисел $\mathbb{Q}$. Мы начнем с самого поля $\mathbb{Q}$. Примером его абелева расширения является поле $K_n = \mathbb{Q}(\mu_n)$, полученное присоединением всех корней степени n из 1. Его автоморфизмы имеют вид $\sigma_a(\xi) = \xi^a$, $\xi \in \mu_n$, где $(a, n) = 1$ и a определено лишь $(\text{mod } n)$. Значит, $\text{Gal}(K_n/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$ — группе обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$.

Фундаментальная теорема Кронекера–Вебера утверждает, что любое абелево расширение $K/\mathbb{Q}$ содержится в некотором K_n . Зна-

чит, объединение $\mathbb{Q}^{ab}$ всех абелевых расширений, совпадает с $\bigcup_n K_n$. Это позволяет найти его группу Галуа. Легко видеть, что $\bigcup_n K_n = \bigcup_p K^{(p)}$, где для простого числа p : $K^{(p)} = \bigcup_{m>0} K_{p^m}$ и $\text{Gal}(\bigcup_n K_n/\mathbb{Q}) = \prod_p \text{Gal}(K^{(p)}/\mathbb{Q})$. Автоморфизм поля $K^{(p)}$ определяется последовательностью вычетов $a_m \pmod{p^m}$, удовлетворяющих условиям:

- (1) $a_{m+1} \equiv (a_m \pmod{p^m})$,
- (2) $(a_m, p) = 1$.

Последовательность вычетов a_m , удовлетворяющая условию (1), определяет целое p -адическое число $\alpha \in \mathbb{Z}_p$, а (2) означает, что α обратимо, т.е. $\alpha \in \mathbb{Z}_p^*$. Таким образом, $\text{Gal}(K^{(p)}/\mathbb{Q}) \simeq \mathbb{Z}_p^*$ и

$$\text{Gal}(\mathbb{Q})^{ab}/\mathbb{Q} \simeq \prod_p \mathbb{Z}_p^*. \quad (6)$$

Если K — произвольное поле алгебраических чисел, то роль простых чисел играют его простые дивизоры. Множество их обозначим S . Каждому $p \in S$ соответствует p -адическое пополнение K_p из поля K . Пусть $O_p \subset K_p$ множество его целых элементов.

Рассмотрим множество $\prod_p K_p^*$ последовательностей $\{\alpha_p \in K_p^*, p \in S\}$. Его элемент $\{\alpha_p, p \in S\}$ называется идэлем, если $\alpha_p \in O_p^*$ для почти всех $p \in S$. Группа идэлей обозначается $I(K)$. Каждый элемент $\alpha \in K^*$ определяет идэль ввиду вложения $K \subset K_p^*$ для всех $p \in S$.

Группой классов идэлей называется группа $C(K) = I(K)/K_+^*$, где K_+^* состоит из тех $\alpha \in K^*$, у которых все сопряженные положительны (если они вещественны).^{*} Теория полей классов устанавливает изоморфизм групп $C(K)$ и $\text{Gal}(K^{ab}/K)$. При $K = \mathbb{Q}$ легко видеть, что $I(\mathbb{Q}) = \mathbb{Q}_+^* \prod_p \mathbb{Z}_p^*$ и этот изоморфизм превращается в (6).

Обратим внимание на аналогию этого описания с тем, которое дано в п.4. Простые дивизоры из поля K аналогичны точкам s кривой S , идэлы — наборам функций $\{f_s, s \in S, f_s(s) \neq 0, \infty \text{ для почти всех } s \in S\}$, а элементы $\alpha \in K_+^*$ — дивизорам $(f) \in P(S)$, $f \in K(S)^*$. Остается различие в том, что при определении дивизоров $D \in \text{Div}(S)$ мы факторизуем наборы функций $\{f_s\}$ по наборам $\{u_s, u_s(s) \neq 0, \infty \text{ для } s \in S\}$. Но это различие связано с тем, что в п.4 мы рассматривали лишь неразветвленные абелевы расширения

^{*}Вместо K_+^* должно стоять замыкание $\overline{K_+^*}$ этой группы в $I(K)$ (при $K = \mathbb{Q}$ она замкнута). (Примечание добавлено автором в настоящем издании.)

K'/K . Описание аналогичных расширений поля K также требует факторизации группы $C(K)$ по совершенно аналогичной подгруппе $\{\alpha_p \in O_p^*, p \in S\}$.

Еще проще описать “локальный” аналог теории полей классов, когда K — конечное расширение поля p -адических чисел $\mathbb{Q}_p$. В этом случае роль группы $C(K)$ играет просто группа K^* : конечные абелевы расширения L/K взаимно-однозначно соответствуют подгруппам конечного индекса этой группы. В частности, если $\mu_m \subset K$, то $\text{Gal}(K_m^{ab}) = K^*/K^{*m}$. Сравнивая это с куммеровской теорией (п.3), мы видим, что $K^*/K^{*m} = \text{Gal}(K_m^{ab}) = X(K^*/K^{*m})$, т.е. существует невырожденное спаривание $(a, b) \in \mu_m$ группы K^*/K^{*m} с собой. Например, при $K = \mathbb{Q}_p$, $m = 2, p \neq 2$, $(a, b) = \left(\frac{a^* b^{-r}}{p}\right)$, если $a = p^r a', b = p^s b', a', b' \in \mathbb{Z}_p$ и не делятся на p , а $\left(\frac{x}{p}\right)$ — символ Лежандра. Если же $p = 2$, a и b нечетны, то $(a, b) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}$.

В случае полей алгебраических чисел теория полей классов не только описывает группу $\text{Gal}(K^{ab}/K)$, но ввиду арифметического характера этого описания, позволяет детально изучить арифметику абелевых расширений K'/K : законы разложения простых дивизоров поля K в поле K' и законы взаимности.

Предположим, что $K \supset \mu_m$, в этом случае можно опять сопоставить теорию полей классов и куммерову теорию.

Мы видим, что опять существует спаривание $(\alpha, \beta) \in \mu_m$, где $\alpha \in C(K)$, $\beta \in K^*$ или, что то же самое, спаривание (α, β) , $\alpha \in I(K)$, $\beta \in K^*$, равное 1 при $\alpha \in K^{*+}$ или $\beta \in (K^*)^m$. Явное вычисление этого спаривания приводит к его записи $(\alpha, \beta) = \prod_{p \in S} (\alpha_p, \beta)$,

если $\alpha = \{\alpha_p, p \in S\}$ и (α_p, β) — то спаривание группы K_p^*/K_p^{*m} с собой, которое мы выявили из локальной теории полей классов. Соотношение $(\alpha, \beta) = 1$ при $\alpha = \alpha \in K_+^*$ дает классические законы взаимности. Например, при $K = \mathbb{Q}$ и $m = 2$ соотношение $\prod_p (a, b)_p = 1$ дает, как легко убедиться, квадратичный закон взаимности Гаусса.

II. Неабелева математика

6. Алгебра представлений конечной группы. Если G — конечная, но не обязательно коммутативная группа, то естественным аналогом характеров являются неприводимые представления $\varphi: G \rightarrow GL(V)$ в группу линейных преобразований комплексного конечномерного пространства V . С точностью до эквивалентности, определенной изоморфизмом пространств V , их имеется конечное

число разных: $\varphi_1, \dots, \varphi_h$.

В множестве $\Delta = \{\varphi_1, \dots, \varphi_h\}$ определена операция тензорного произведения: для $\varphi_i : G \rightarrow GL(V_i)$, $i = 1, 2$, $(\varphi_1 \times \varphi_2)(g) = \varphi_1(g) \otimes \varphi_2(g) \in GL(V_1 \otimes V_2)$. Представление $\varphi_i \otimes \varphi_j$, вообще говоря, приводимо и является прямой суммой неприводимых представлений с некоторыми кратностями:

$$\varphi_i \otimes \varphi_j = \sum_{k=1}^h n_{ij}^{(k)} \varphi_k, \quad n_{ij}^{(k)} \in \mathbb{Z}, \quad n_{ij}^{(k)} \geq 0. \quad (7)$$

Единичное представление: $\varphi_1(g) = 1 \in GL(1, \mathbb{C})$ играет для этой операции роль единичного элемента: $\varphi_1 \otimes \varphi_i = \varphi_i$. Аналогом обратного является представление $\varphi^\times(g) = \varphi(g^{-1})^T \in GL(V^*)$. Оно “обратно” в том смысле, что это единственное неприводимое представление, для которого в разложении $\varphi \otimes \varphi^\times = \sum n_i \varphi_i$ коэффициент n_1 при единичном представлении φ_1 положителен. Таким образом, множество $\Delta = \{\varphi_1, \dots, \varphi_h\}$ сохраняет, в слабой степени, некоторые свойства группы.

Число h неприводимых представлений равно числу классов сопряженных элементов группы G , а коэффициенты $n_{ij}^{(k)}$ в (7) могут быть найдены, исходя из умножения этих классов. Именно, если C_i и C_j — два класса сопряженных элементов, то в множестве $C_i C_j = \{ab, a \in C_i, b \in C_j\}$ все элементы класса C_k встречаются одинаковое число раз. Обозначив это число $m_{ij}^{(k)}$, пишем

$$C_i C_j = \sum m_{ij}^{(k)} C_k. \quad (8)$$

Из того, что $ba = (bab^{-1})b$ следует, что $C_i C_j = C_j C_i$, т.е. $m_{ji}^{(k)} = m_{ij}^{(k)}$. Таким образом, даже некоммутативную группу можно разбить на меньшие подмножества, умножение которых все еще коммутативно, хотя они уже образуют не группу, а таблицу умножения (8). Здесь опять единичный класс $C_1 = \{e\}$ играет роль единичного элемента, а класс $C^{-1} = \{c^{-1}, c \in C\}$ роль обратного — в том же смысле, как и в таблице (7). Отсюда легко вытекает, что коммутативная алгебра A с таблицей умножения (8) полупроста и разлагается в сумму $\oplus \mathbb{C}$. Проекция на i -е слагаемое определяет ее гомоморфизм: $\chi_i : A \rightarrow \mathbb{C}$. Это — характер неприводимого представления φ_i , $i = 1, \dots, h$. Именно так впервые ввел характеры Фробениус. Их умножение как функций на множестве Γ классов сопряженных элементов (после “усреднения” по классу) дают таблицу умножения (7). Мы видим, что множества Γ и Δ — обра-

зуют таблицы, двойственные друг другу, подобно абелевой группе и группе характеров.

Таким образом, описание множества Δ неприводимых представлений группы G и даже их таблицы умножения (7) все же связано с некоторой коммутативной алгеброй (хотя и не группой). Мы имеем дело лишь с “полунеабелевой” математикой. Тем не менее, в применении к конкретным ситуациям, аналогичным рассмотренным нами в п.4 и п.5 на этом пути получаются очень содержательные результаты: см. п.7 и п.8. Но прежде два замечания.

1) Аналогичная ситуация (двойственность между множествами Δ и Γ) имеет место для компактных групп. Для компактных групп Ли множество неприводимых представлений описывается формулой Г.Вейля для характеров. Отсюда можно найти закон умножения в Δ . Например, для $G = SU(2)$ или $SO(3)$ — это так называемая формула Клебша–Гордана: представления $\varphi_n \in \Delta$ задаются целым индексом $n > 0$ и при $n \geq m$

$$\varphi_n \otimes \varphi_m = \sum_{\substack{n-m \leq k \leq n+m \\ k \equiv n+m(2)}} \varphi_k.$$

Вероятно, на этом пути можно описать и множество Γ , естественную меру на нем и закон умножения в виде интеграла по нему. Насколько мне известно, это не сделано. Тем более, неизвестно описание меры и закона умножения Γ для случая интересной компактной p -адической группы Ли: группы элементов x из алгебры с делением над $\mathbb{Q}_p$, для которых $N(x) = 1$, хотя теоретико-множественно Γ описывается просто. Это было бы интересно в связи с p -адическими гипотезами Ленглендса (ср. п. 8).

2) Двойственность между множествами Δ и Γ может быть определена для любых “таблиц умножения”

$$a \cdot b = \sum p_{a,b}^{(c)} c \quad (9)$$

при условии существования единичного элемента e и обратного $a^* (p_{a,a^*}^{(e)} > 0)$. Если заменить классы C_i их “средними” $z_c = \frac{1}{|C_i|} c_i$ ($|C_i|$ — число элементов в классе C_i), то для соответствующей таблицы будет $\sum_k p_{ij}^{(k)} = 1$, $p_{ij}^{(k)} \geq 0$. Множество $\{z_1, \dots, z_h\}$ можно рассматривать как “вероятностную группу”, в которой произведение $z_i z_j$ есть элемент z_k с вероятностью $p_{ij}^{(k)}$. Такая переформулировка возможна для любой таблицы (9) с $p_{a,b}^{(c)} \geq 0$. Подобные, правда бесконечные, таблицы образуют многие классические системы

ортогональных многочленов: $\{\cos nx\}$, полиномы Лежандра, Лягерра, Чебышева, Эрмита, Гегенбауэра. Например, для многочленов Лежандра:

$$P_n P_m = \sum_{\substack{k=n-m \\ k \equiv m+n(2)}} c_{n,m}^{(k)} P_{n+m-2k}$$

при $m \leq n$, где

$$c_{n,m}^{(k)} = \frac{1}{4} \binom{k}{n+m+1} \frac{\alpha_{n+m-k} \cdot \alpha_{n-m+k} \cdot \alpha_{m-n+k}}{\alpha_{n+m+k}}, \quad \alpha_m = \binom{m/2}{m}.$$

В связи с этим естественно спросить — вытекает ли из условия $p_{a,b}^{(c)} \geq 0$ аналогичное условие для двойственной таблицы? В начале 50-х годов С.П.Демушкин (тогда еще студент) построил простые примеры, когда это не так. Интересно было бы найти условие того, что соотношение $p_{a,b}^{(c)} \geq 0$ сохраняется для двойственной таблицы, как это имеет место для Δ и Γ . Еще интересней понять на этом пути двойственность двух теорем, “число элементов класса сопряженных элементов (соответственно степень неприводимого представления) делит порядок группы”. Очевидно, она относится к таблицам (9) с $p_{a,b}^{(c)} \in \mathbb{Z}$. Возможно, она связана с перенесением на них операции $C \rightarrow C^k : \{c\} \rightarrow \{c^k\}$ в множестве классов (“операции Адамса”).

7. Векторные расслоения. В п.4 мы установили соответствие между а) одномерными унитарными представлениями группы $H_1(S, \mathbb{Z})$ (или, что то же самое, $\pi_1(S)$), б) Классами дивизоров степени 0 на S (т.е. $J(S)$ ср. (4)) и в) Расслоениями над S со слоем $\mathbb{C}$, тривиальными топологически. Сейчас мы опишем обобщение этой теории на любые неприводимые унитарные представления группы $\pi_1(S)$.

Самый естественный путь “некоммутативного” обобщения какой-либо теории — это заменить в ней числа матрицами. Так, по аналогии с п. 4, n -мерным матричным дивизором называется задание в r точках $s_1, \dots, s_r$ обратимых матриц $M_1, \dots, M_r \in GL(n, K)$ с коэффициентами в поле $K = \mathbb{C}(S)$. При этом допустима замена $M_i \rightarrow M_i P_i$, где элементы матриц P_i принадлежат кольцу O_{s_i} функций, регулярных в точке s_i и $(\det P_i)(s_i) \neq 0$, т.е. $P_i \in GL(n, O_{s_i})$. По аналогии с п. 4 множество $\text{Div}_n(S)$ n -мерных матричных дивизоров можно записать в виде

$$\text{Div}_n(S) = \{M_s, s \in S, M_s \in GL(n, K), M_s \in GL(n, O_s)\}$$

$$\text{почти для всех } s \} / \{P_s \in GL(n, O_s)\}.$$

Дивизоры $\{M_s, s \in S\}$ и $\{M'_s, s \in S\}$ называются эквивалентными, если $M'_x = CM_x$, $C = GL(n, K)$. Эквивалентные дивизоры образуют один класс.

Совершенно так же, как в п. 4, классу n -мерных матричных дивизоров сопоставляется расслоение E над S со слоем $\mathbb{C}^n$. Если $\{M_{s_1}, \dots, M_{s_r}\}$ — дивизор этого класса, то над достаточно малыми окрестностями $U_i \ni s_i$, $E \simeq U_i \times \mathbb{C}^n$, а над $U_i \cap U_j$, $U_i \times \mathbb{C}^n$ и $U_j \times \mathbb{C}^n$ склеиваются при помощи матрицы $M_{s_i} M_{s_j}^{-1}$.

Соответствие между аналитическими (или, что то же — алгебраическими) векторными расслоениями (с точностью до изоморфизма) и классами матричных дивизоров — взаимно однозначно.

Наконец, любому представлению $\varphi: \pi_1(S) \rightarrow GL(n, \mathbb{C})$ соответствует некоторое векторное расслоение E : если U — универсальная накрывающая кривой S и $S = U/G$, $G \simeq \pi_1(S)$, то $E = (U \times \mathbb{C})/\pi_1(S)$, где $\pi_1(S)$ действует на $U \times \mathbb{C}$ при помощи φ , а на U — как G . Однако это сопоставление — ни вложение, ни отображение “на”. Опишем сначала его образ.

Беря детерминант каждой матрицы M_{s_i} , мы можем сопоставить каждому матричному дивизору $\{M_{s_1}, \dots, M_{s_r}\}$, а значит, и каждому векторному расслоению E обычный дивизор, обозначаемый $\det E$. Число $\deg(\det E)$ обозначается $\deg E$ — это класс Черна $c_1(E)$ расслоения E . Легко видеть, что для расслоения E , соответствующего представлению группы $\pi_1(S)$, $\deg E = 0$. Обратное верно, если E не разложимо в прямую сумму представлений. В общем случае условие заключается в том, что $\deg E_i = 0$, если $E = \oplus E_i$ — разложение в прямую сумму неразложимых расслоений.

Однако, по аналогии с п. 4, нас интересуют неприводимые унитарные представления $\varphi: \pi_1(S) \rightarrow U(n) \subset GL(n, \mathbb{C})$. Два такие представления приводят к изоморфным расслоениям только, если они эквивалентны. Расслоения E (обязательно с $\deg E = 0$), соответствующие неприводимым унитарным представлениям, являются стабильными. Мы не приводим их определения, хотя оно несложно. Значение их в том, что множество стабильных расслоений E заданной размерности n с заданным значением $\deg E = d$ обладает структурой конечномерного алгебраического многообразия. Для простоты рассматриваются расслоения с фиксированным классом $\det E = \delta$. Они образуют многообразие $S(n, \delta)$. Но, так как все многообразия $S(n, \delta)$ с $\deg \delta = d$ изоморфны, то пишут просто $S(n, d)$.

Если $(n, d) = 1$, то многообразие $S(n, d)$ гладко и проективно. Его размерность равна $(g - 1)(n^2 - 1)$, где g — род кривой S . Например, для кривой рода 2, заданной уравнением $y^2 = \prod_{i=0}^5 (x - \lambda_i)$ многообразие $S(2, 1)$ задается в $\mathbb{P}^5$ уравнениями

$$\prod_{i=0}^5 x_i^2 = 0, \quad \prod_{i=0}^5 \lambda_i x_i^2 = 0.$$

А многообразие $S(2, 0)$ имеет вид $\mathbb{P}^3 \setminus V$, где V — так называемая Куммерова поверхность.

По-видимому, векторным расслоениям размерности > 1 принадлежит особенно большая будущность в теории алгебраических многообразий размерности > 1 . В то время, как множество одномерных расслоений $J(S)$ на кривой S в существенном определяет кривую S на алгебраической поверхности совокупность одномерных расслоений может быть очень бедной. Во многих вопросах расслоения размерности > 1 выступают как естественные обобщения классов дивизоров, полноценно отражая геометрию многообразия.

В математической физике векторные расслоения над сферой S^4 (рассматриваемой как компактификация 4-х мерного пространства-времени) с компактной группой Ли G в качестве структурной группы, приводят к “неабелеву” обобщению уравнений Максвелла — уравнениям Янга–Миллса. Уравнения Максвелла являются их частным случаем при $G = U(1)$. Аналогичная теория существует и для других многообразий, отличных от S^4 , и дает “неабелев” аналог теории Ходжа (п. 1). Существенной чертой этого обобщения является то, что “неабелевость” влечет нелинейность соответствующих дифференциальных уравнений.

8. Гипотезы Ленглендса. Речь идет о целой системе гипотез, цель которых — построить обобщение теории полей классов (п.5), аналогичное обобщению теории абелевых функций (п. 4), описанному в п. 7. Эти гипотезы доказаны лишь в очень частных случаях, но их правдоподобие основывается на их согласованности друг с другом и связях с другими важными вопросами.

Проще описать “локальный” вариант, касающийся расширений локального поля K (конечного расширения поля p -адических чисел $\mathbb{Q}_p$). В этом случае основную роль играет “алгебра с делением” D_n (это значит, что любой элемент $x \in D_n$, $x \neq 0$, имеет обратный), имеющая центром поле K и ранг n^2 над этим полем. Общая теория утверждает, что ранг любой алгебры с делением с центром K есть полный квадрат. Такие алгебры ранга n^2 естественно со-

ответствуют $\varphi(n)$ вычетам $\bmod n$, взаимно простым с n . Алгебра D_n соответствует вычету 1. Элементы $x \in D_n$, $x \neq 0$ образуют группу D_n^* . В этом случае гипотеза утверждает, что существует взаимно однозначное соответствие между неприводимыми представлениями группы $\text{Gal}(\bar{K}/K)$, где $\bar{K}$ — алгебраическое замыкание поля K , степень которых делит заданное число n , и неприводимыми представлениями группы D_n^* , ядра которых — открытые подгруппы конечного индекса. Гипотеза доказана при $(n, p) = 1$, $n = p$.

Здесь мне трудно удержаться от очень личного воспоминания. В 1944–45 г.г. я был безумно увлечен гипотезой о том, что группа $\text{Gal}(\bar{K}/K)/N$, где N — пересечение ядер всех неприводимых представлений группы $\text{Gal}(\bar{K}/K)$, степени которых делят n , изоморфна некоторой факторгруппе группы D_n^* , и что этот изоморфизм прольет свет на таинственный “ведущий модуль” (conductor), введенный Артином. Просчитав, однако, достаточно далеко группы и $\text{Gal}(\bar{K}/K)$ и D_n^* , я убедился, что такого изоморфизма нет. Если гипотеза Ленглендса верна (а на это много указаний), то мы имеем интересный пример неизоморфных групп, у которых одна и та же алгебра Δ неприводимых представлений (ср. п.6). Множество Γ классов сопряженных элементов группы D_n^* очень просто — это множество неприводимых многочленов $f(t) \in K[t]$ со старшим коэффициентом 1, степень которых делит n . Вычисление алгебры Γ могло бы быть полезным для уяснения всей ситуации.

Существует другой вариант той же гипотезы, в которой те же представления группы $\text{Gal}(\bar{K}/K)$ сопоставляются неприводимым унитарным бесконечным представлениям группы $GL(n, K)$. Именно этот вариант имеет аналог для случая $K = \mathbb{Q}$. В этом случае основную роль играет группа адзелей $GL(n, \mathbb{A}) \subset GL(n, \mathbb{R}) \times \prod_p GL(n, \mathbb{Q}_p)$, выделенная тем условием, что $\alpha = \alpha_\infty \prod_p \alpha_p$, $\alpha_\infty \in GL(n, \mathbb{R})$, $\alpha_p \in GL(n, \mathbb{Q}_p)$, $\alpha_p \in GL(n, \mathbb{Z}_p)$ для почти всех p . Очевидно, $GL(n, \mathbb{Q}) \subset GL(n, \mathbb{A})$. Множество классов смежности $GL(n, \mathbb{A})/GL(n, \mathbb{Q})$ является не группой, а однородным пространством относительно $GL(n, \mathbb{A})$. Аналогом “его неприводимых представлений” являются неприводимые унитарные бесконечномерные представления группы $GL(n, \mathbb{A})$, содержащиеся в естественном представлении в пространстве функций $L^2(GL(n, \mathbb{A})/GL(n, \mathbb{Q}))$. Точная формулировка гипотезы в этом случае потребовала бы слишком большого числа технических деталей. Гипотеза распространяется и на любые конечные расширения K поля $\mathbb{Q}$. Ее интерес увеличивается тем, что она давала бы точные сведения об очень интересных арифметических инвариантах поля K — его L -рядах.

9. Нильрасширения числовых полей. В п.п. 7 и 8 мы ви-

дели, как богато содержанием множество неприводимых представлений группы $\pi_1(S)$ и ее аналога $\text{Gal}(\overline{K}/K)$ для числовых полей (при этом мы даже не привлекали операцию $\otimes$ в множестве неприводимых представлений). Пока мы не вышли за пределы “полу-неабелевой” математики. Что же можно сказать в духе “неабелевой математики” о группе $\pi_1(S)$ или $\text{Gal}(\overline{K}/K)$? Сейчас кое-что известно лишь о нильпотентных факторгруппах этих групп. Так как нильпотентная конечная группа есть произведение конечных p -групп, то мы рассмотрим объединение $K^{(p)}$ всех расширений Галуа K'/K , для которых $\text{Gal}(K'/K)$ — p -группа.

Пусть сначала $K = \mathbb{Q}_p$ (поле p -адических чисел). Если $q \neq p$, то группа $\text{Gal}(\mathbb{Q}_p^{(q)}/\mathbb{Q}_p)$ устроена очень просто и мы опустим ее описание. Если $p \neq 2$, то $\text{Gal}(\mathbb{Q}_p^{(q)}/\mathbb{Q}_p)$ имеет две образующие, не связанные никакими соотношениями (свободная p -группа). Таким образом, расширения $K/\mathbb{Q}_p$, для которых $\text{Gal}(K/\mathbb{Q}_p)$ — p -группа, такие же, как и аналогичные неразветвленные накрытия восьмерки:

∞

Самой любопытной является группа $\text{Gal}(\mathbb{Q}_2^{(2)}/\mathbb{Q}_2)$: она имеет 3 образующие x, y, z , связанные соотношением $x^2 y^4 (y, z) = 1$, где $(y, z) = yzy^{-1}z^{-1}$. Было бы интересно иметь какое-то ее геометрическое описание. Аналогичные результаты известны для конечных расширений поля $\mathbb{Q}_p$.

В случае поля $\mathbb{Q}$ или его конечного расширения K естественно рассматривать расширение $K_\Sigma^{(p)}$ — объединение расширений K'/K , для которых $\text{Gal}(K'/K)$ — p -группа и которые разветвлены лишь в конечном множестве Σ простых дивизоров поля K . Группа $\text{Gal}(K_\Sigma^{(p)})/K$ имеет конечное число образующих, а иногда можно определить и задающие ее соотношения.

Известно, что $\mathbb{Q}_\Sigma^{(p)} = \mathbb{Q}$, если Σ пусто. Если $\Sigma = \{2\}$, то группа $\text{Gal}(\mathbb{Q}_\Sigma^{(2)}/\mathbb{Q})$ имеет 2 образующие x, y с единственным соотношением $x^2 = 1$. Если $\Sigma = \{p_1, p_2\}$, $p \neq 2$, $p_i \equiv 1 \pmod{p}$, $p_i \not\equiv 1 \pmod{p^2}$, $i = 1, 2$, $p_1 \not\equiv x^p \pmod{p_2}$, то $\text{Gal}(\mathbb{Q}_\Sigma^{(p)}/\mathbb{Q})$ является некоммутативной группой порядка p^3 и показателя p^2 . Если $k = \mathbb{Q}(\sqrt[p]{1})$, простое число p регулярно и $\Sigma = \{\pi\}$, $\pi = 1 - \sqrt[p]{1}$, то $\text{Gal}(K_\Sigma^{(p)}/K)$ является свободной группой с $\frac{p+1}{2}$ образующими. Если Σ пусто, $K = \mathbb{Q}(\sqrt{-5})$, то $K_\Sigma^{(2)} = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$. Если Σ пусто и группа классов идеалов поля K имеет достаточно много образующих сравнительно со степенью $[K : \mathbb{Q}]$, то $K_\Sigma^{(p)}$ бесконечно для

некоторого p . Например, при $p = 2$: $K = \mathbb{Q}(\sqrt{-3 \cdot 7 \cdot 17 \cdot 19})$. Такие поля невозможно вложить в поля с однозначным разложением дивизоров на простые множители.

Так, здесь мы часто можем найти красивое описание группы $\text{Gal}(K_\Sigma^{(p)}/K)$ при помощи образующих и соотношений, похожее, например, на задание фундаментальной группы трехмерного многообразия. Чего, однако, явно не хватает — это конкретного описания таких групп, какое дается в коммутативном случае теорией яacobianов и теорией полей классов.

10. Итерированные интегралы. В случае поля функций $\mathbb{C}(S)$ на римановой поверхности S существует красивый подход к изучению накрытий (мы ограничимся неразветвленными) с нильпотентной группой Галуа. Так как изложенная в п.4 теория абелевых накрытий основывалась на интегрировании дифференциальных форм, то этот подход связан с “неабелевым” обобщением интегрирования. Пусть $\omega_1, \dots, \omega_r$ — одномерные дифференциальные формы на S и $\gamma: (\varphi: I \rightarrow X, I = [0, 1])$ — путь. Итерированный интеграл $\int_\gamma \omega_1 \cdots \omega_r$ определяется индуктивно: полагая $\xi_1(t) =$

$$\int_0^t \varphi^* \omega_1, \quad \xi_2(t) = \int_0^t \xi_1 \varphi^* \omega_2, \dots, \text{полагаем } \int \omega_1 \dots \omega_r = \int_0^1 \xi_{r-1} \varphi^* \omega_r.$$

Такая конструкция встречается, например, при построении решения обыкновенного дифференциального уравнения методом последовательных приближений.

Если T^i — i -я тензорная степень пространства одномерных дифференциальных форм, то итерированный интеграл $\int_\gamma$ определяет

$$\text{линейную функцию на пространстве } T = \bigoplus T^i: \int_\gamma \omega_1 \otimes \cdots \otimes \omega_r = \int_\gamma \omega_1 \dots \omega_r.$$

Можно явно выписать условие того, что для $\omega \in T$ $\int_\gamma \omega$ зависит лишь от гомотопического класса пути γ . Например, если $\omega = \mu + \sum \mu_i \otimes \mu'_i$, $\mu \in T^1$, $\sum \mu_i \otimes \mu'_i \in T^2$, то условие заключается в том, что $d\mu + \sum \mu_i \wedge \mu'_i = 0$, $\sum \alpha_i \mu'_i = \sum \alpha'_i \mu_i = 0$, если $d\mu_i = \alpha_i \Omega$, $d\mu'_i = \alpha'_i \Omega$, а Ω — некоторая стандартная двумерная форма на S . Тензорная форма $\omega \in T$, удовлетворяющая этим условиям, определяет функцию на группе $\pi_1(S)$.

Точно так же, для некоторых элементов $\omega \in T$: $\int_\gamma \omega = 0$ для всех $\gamma \in \pi_1(S)$. Например, если $\omega = f d\mu + \mu \otimes df$, $f \in T^0$, $\mu \in T^1$. Такие элементы тоже можно описать. В результате получается явное описание некоторого пространства функций на группе $\pi_1(S)$ и значит линейных функций на ее групповом кольце $\mathbb{C}[\pi_1(S)]$.

Пусть $\xi = \int_{\gamma} \omega$ — одна из возникающих таким образом функций, причем $\omega \in \bigoplus_{i \geq r} T^i$. Оказывается, что тогда $\xi(x) = 0$ для $x \equiv 1(J^{r+1})$, где J — идеал, состоящий из элементов вида $\sum \alpha_{\gamma} \gamma$, $\sum \alpha_{\gamma} = 0$. Таким образом, $\xi(x)$ является линейной функцией на алгебре $\mathbb{C}[\pi_1(S)]/J^{r+1}$ и функцией на группе $\Gamma_r = \pi_1(S)/\pi_1(S)^{(r)}$, где $\pi_1(S)^{(r)} = \{\gamma \in \pi_1(S), \gamma \equiv 1(J^{r+1})\}$. Группы $\pi_1(S)^{(r)}$ совпадают с членами убывающего центрального ряда группы $\pi_1(S)$ (ввиду специфических свойств этой группы). Нильпотентная группа Γ_r вкладывается в алгебру $\mathbb{C}[\pi_1(S)]/J^{r+1}$ и имеет в ней “алгебраическую оболочку”, совпадающую с ее так называемым мальцевским пополнением. Это аналог сопоставления $A \rightarrow A \otimes \mathbb{C}$ для абелевой группы A . Мальцевское пополнение группы Γ мы тоже будем обозначать $G = \Gamma \otimes \mathbb{C}$ — это алгебраическая группа. Очевидно, $\Gamma \subset G(\mathbb{C})$ и можно отождествить Γ с $G(\mathbb{Z})$. В случае групп Γ_r и $G_r = \Gamma_r \otimes \mathbb{C}$, $G_r \subset \mathbb{C}[\pi_1(S)]/J^{r+1}$ и поэтому, если $\mathfrak{G}_r$ — алгебра Ли группы G_r , то $\mathfrak{G}_r \subset \mathbb{C}[\pi_1(S)]/J^{r+1}$ (операция Ли в $\mathbb{C}[\pi_1(S)]/J^{r+1}$ определяется как $[x, y] = xy - yx$). При $r = 1$, $G_1 = H_1(X, \mathbb{Z}) \otimes \mathbb{C} = H_1(X, \mathbb{C})$. Система групп G_r , $r = 1, 2, \dots$ (и их дискретных подгрупп $G_r(\mathbb{Z})$) определяет башню алгебраических групп, содержащую описание неразветвленных накрытий $S' \rightarrow S$ с нильпотентной группой Галуа, а итерированные интегралы играют ту же роль, что теория Де Рама при $r = 1$.

До сих пор речь шла о чисто топологической теории. Если же S — риманова поверхность, то это отражается в разбиении любой 1-формы $\mu \in T^1$ в сумму $\mu = \mu' + \mu''$, где локально $\mu' = u' dz$, $\mu'' = u'' d\bar{z}$, z — локальный параметр. Аналогично форму $\omega \in T^r$ можно разбить на однородные составляющие $\omega = \sum \omega^p$, где в ω^p входит p раз множитель dz . То описание пространства $\mathbb{C}[\pi_1(S)]/J^{r+1}$ при помощи итерированных интегралов, о котором мы говорили выше, дает возможность перенести такое разбиение на это пространство. В частности, в нем выделяется подпространство $\mathcal{H} \subset \mathbb{C}[\pi_1(S)]/J^{r+1}$ — ядро всех функций $\int \omega$, $\omega \in \bigoplus_{i \leq r} T^i$ для тех ω , в которые хоть один раз входит dz . Это подпространство является подалгеброй Ли, а пересечение $\mathfrak{G} \cap \mathcal{H}$ — подалгеброй Ли в $\mathfrak{G} = \text{Lie } G_r$. Ей, в свою очередь, соответствует подгруппа $G_r^0 \subset G_r$. Факторпространство G_r/G_r^0 является комплексным однородным пространством. При $r = 1$ оно совпадает, как легко проверить, с пространством $\mathbb{C}^g \simeq H_1(S, \mathbb{R})$ из п.4. Группа $\pi_1(S)^{(r)} = G_r(\mathbb{Z})$ является ее дискретной подгруппой и действует умножением слева на пространстве G_r/G_r^0 , а фактор $G_r(\mathbb{Z}) \setminus G_r/G_r^0$ дает “нильпотентное” обобщение якобиева много-

образа из п. 4. Интегрирование $\int_{s_0}^s \omega$ $\omega \in \oplus T^i$, определяет отображение $S \rightarrow G_r(\mathbb{Z}) \setminus G_r/G_r^0$, обобщающее отображение j (см. (2) п.4).

Теория, набросок которой мы привели, еще далеко не имеет законченного характера. “Неабелевы якобианы”, как правило, — не алгебраические и даже не кэлеровы многообразия, а естественные отображения их друг на друга — не аналитические, так что трудно даже поставить вопрос об их алгебраической интерпретации. Тем не менее, ясно, что здесь имеется существенное продвижение в теории неабелевых нильпотентных накрытий.

Сопоставление фактов, изложенных в последних двух пунктах, приводит к мысли, что в ближайшем будущем можно надеяться на построение, если не “неабелевой математики” вообще, то, как первого шага — “нильпотентной математики”. Обратить внимание на эту возникающую новую область — и было основным стимулом для написания настоящего обзора.

ЛИТЕРАТУРА

По поводу сопряженных векторных пространств, представлений групп и теории Куммера:

1. S. Lang, *Algebra*, Addison-Wesley, 1965.

В менее алгебраическом духе ср.

2. Weyl H., *Gruppentheorie und Quantenmechanik*, Leipzig, 1923.

Теория абелевых функций:

3. Weyl H., *Idee dre Riemannschen Flächen*, Berlin, 1923.

Алгебраический аспект:

4. J.P.Serre, *Groupes algebriques et corps des classes*, Paris, 1959.

Теория полей классов

5. Cassels J.W.S., Frohlich A., *Algebraic Number Theory*, Academic Press, 1967.

Векторные расслоения. Основопологающая работа:

6. Weil A., *Generalisation des fonction abeliennes*, Collected Papers, vol. 1.

Обзор современного состояния:

7. Ramanan S., *Vector bundles on algebraic curves*, Proc. Int. Cong. Math. Helsinki.

Гипотезы Ленгленда:

8. Gelbart S., *An elementary introduction to the Langlands program*, Bull. Amer. Math. Soc 10, N 2, (1984).

Расширения полей алгебраических чисел:

9. Koch H., *Gloissche Theorie der p-Erweiterungen*, Berlin, 1970.

Итерированные интегралы: обзор

10. Cartier P., *Seminaire Bourbaki Exp. N. 687*.

Издание осуществлено АО "Прима В"

121183. г.Москва., Б.Академическая ул 83 - 87

лр 060727 от 17.02.92.

Подписано в печать 6.06.96. Формат 60х88/16. Бумага офсетная № 1.

Объем 28 п.л. Печать офсетная. Тираж 3000 экз. Заказ № 73.

Отпечатано в АООТ «Оригинал».

101898, Москва, Центр, Хохловский пер., 7.