А.Вейль

ОСНОВЫ ТЕОРИИ ЧИСЕЛ

ИЗДАТЕЛЬСТВО «МИР», МОСКВА 1972

Монография одного из крупнейших современных математиков, написанная на основе курса лекций, прочитанного автором в Принстонском университете. Содержит изложение теории алгебраических чисел, в том числе теории полей классов, являющееся, по-видимому, на много лет окончательным. Книга представляет интерес не только для специалистов по теории чисел, но и для математиков, занимающихся алгебраической геометрией, теорией автоморфных функций и т. д. Она написана очень четко и доступна студентам старших курсов.

ОГЛАВЛЕНИЕ

ПРИЛОЖЕНИЯ К РУССКОМУ ИЗДАНИЮ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

В этот указатель включены все понятия и термины, определение которых дается или упоминается в тексте, даже если это не было сделано в виде формального определения.

ОТ ИЗДАТЕЛЬСТВА

Главная тема предлагаемой читателю книги — изложение теории полей классов. В соответствии с названием книги эта теория действительно является основой современной алгебраической теории чисел.

Наиболее существенные части теории полей классов были созданы Гильбертом в конце прошлого века. За прошедшее с тех пор время было найдено несколько вариантов изложения, существенно изменился ее язык, но ее роль центрального комплекса идей и результатов алгебраической теории чисел сейчас стала еще более ясной, чем во времена Гильберта.

Перевод книги А. Вейля дает читателю первое на русском языке полное и подробное изложение теории полей классов. Особенностью того построения этой теории, которое избрал автор, является использование аналитических соображений, основанных на понятии ζ-функции. В этом можно видеть возврат к идеям Гильберта и его непосредственных продолжателей — в их работах использование аналитических методов играло большую роль. Только в конце тридцатых годов удалось найти построение теории полей классов, свободное от применения анализа. Однако в книге А. Вейля аналитические понятия появляются в другом виде, чем у основателей теории полей классов — они связаны с интегрированием в локально компактных группах, являющихся произведениями вещественных и p-адических групп Ли. В этом можно видеть только новый язык — другой вариант прежнего изложения. Однако этот язык уже показал свою плодотворность при изучении арифметических аспектов теории алгебраических групп. Благодаря этому книга А. Вейля подводит

читателя к широкому кругу вопросов — арифметике алгебраических групп, в ее связи с алгебраической геометрией и теорией бесконечномерных представлений.

Другая особенность этой книги заключается в том, что вся теория систематически развивается не только на той классической почве, на которой была создана теория полей классов — теория полей алгебраических чисел. В книге впервые вся теория изложена для общего класса полей, называемых автором A-полями, который, кроме полей алгебраических чисел, включает в себя и поля алгебраических функций над конечным полем констант. О значении этого второго типа полей говорят их яркие применения к таким проблемам теории чисел, как оценка числа решений сравнения или рациональной тригонометрической суммы.

Автор начинает изложение с основ теории A-полей, и поэтому чтение книги требует минимальных предварительных знаний. Достаточно знакомства с основами теории полей и колец и теории коммутативных топологических групп. Однако насыщенность книги глубокими идеями и некоторая лаконичность изложения потребуют от читателя, желающего овладеть предметом, напряженной работы.

ПРЕДИСЛОВИЕ К РУССКОМУ ИЗДАНИЮ

Мне очень приятно, что благодаря усилиям И. И. Пятецкого-Шапиро, Л. Н. Вассерштейна и А. Н. Паршина моя книга станет более доступной советским читателям. В предисловии к английскому изданию я охарактеризовал общие цели этой книги. Но, возможно, будет не лишним добавить здесь несколько слов о ее названии.

Во-первых, это книга по теории чисел. Мне кажется, возникла определенная путаница из-за того, что, с начала этого века, слова «аналитическая теория чисел» стали применять к области математики, ценность и важность которой не подлежит никакому сомнению и которая представлена блестящими работами некоторых из наиболее выдающихся современных математиков, но которая, по моему мнению, вовсе не является теорией чисел. Ее технический аппарат и основные методы — это типичные методы аналитиков: неравенства, оценки, порядки величин. Уже давно (после основополагающих работ Хинчина и Колмогорова) стало ясно, что теория вероятностей — это прикладной анализ, другими словами, анализ, применяемый к некоторым вполне определенным типам задач. В точности то же самое можно сказать об «аналитической теории чисел», и я думаю, что если бы такое понимание распространилось более широко, то это способствовало бы уяснению наших взглядов на математику.

Во-вторых, я преднамеренно использовал в названии слово «основы», которое звучит несколько вызывающе и, как я и ожидал, вызвало ряд замечаний. Я хотел подчеркнуть этим словом, что это не просто учебник для будущих теоретико-числовиков. Было время,

когда теория Галуа рассматривалась как вещь трудная и абстрактная, предназначенная лишь для специалистов. Более того, я знавал некоторых превосходных математиков моего поколения, которые открыто признавались в своем совершенном невежестве в теории Галуа и, кажется, даже гордились этим. Теперь все хорошо понимают, что это — один из «основных» разделов, с которым каждый серьезный студент-математик должен познакомиться в первые же годы обучения. На мой взгляд, то же самое относится и к элементарной теории алгебраических числовых полей, до теории полей классов включительно, и я надеюсь, что эта книга будет способствовать тому, чтобы в конечном счете так оно и было. Я буду счастлив, если настоящий перевод поможет в этом отношении новому поколению советских математиков.

Андрэ Вейль

ПРЕДИСЛОВИЕ

Ἀριθμόν, ἔξοχον σοφισμάτων
Αἰσχ., Προμ. Δεσμ.[1])

Первая часть этой книги основана на курсе лекций, читанных в 1961—1962 г. в Принстонском университете. Эти лекции были превосходно записаны Дэвидом Кантором, и моим первоначальным намерением было сделать их доступными для широкой математической публики, после внесения лишь самых незначительных изменений. Затем однако я случайно нашел среди своих старых бумаг давно забытую рукопись Шевалле, еще довоенных времен (забытую, к слову сказать, как мною, так и ее автором), которая несмотря на свой возраст выглядела совсем неплохо, по крайней мере на мой вкус. Она содержала краткое, но по существу полное изложение основных разделов теории полей классов, как локальной, так и глобальной, и не подлежало сомнению, что предполагавшаяся книга стала бы намного полезнее, если бы я включил в нее такую трактовку этих вопросов. Рукопись пришлось несколько дополнить в соответствии с моими планами, но основная канва ее сохранилась без существенных изменений. А в ряде узловых мест я следовал ей совсем близко.

Было бы тщетной, безнадежной попыткой улучшить после Гекке изложение классических аспектов теории алгебраических чисел. Как станет ясным из первых страниц книги, я попытался сделать выводы из достижений последних тридцати лет, когда локально компактные группы, меры и интегрирование стали играть все возрастающую роль в классической теории чисел. Во времена Дирихле, Эрмита и даже Минковского использование непрерывных переменных в арифметических вопросах можно было рассматривать лишь как ловкий трюк. Теперь же, ретроспективно, мы видим, что вещественные числа естественно появляются на сцене как одно из бесконечного числа пополнений простого поля, ничуть не менее интерес-

[1]) [Изобрел для них] науку чисел, из наук важнейшую. Эсхил, Прикованный Прометей (перевод А. Пиотровского). — *Прим. перев.*

ное арифметикам, чем его p-адические напарники. И существуют по меньшей мере один язык и одна техника, а именно техника аделей, позволяющие собрать их под одной крышей и заставить действовать сообща. Здесь не место входить в историю этого вопроса; достаточно упомянуть такие имена, как Гензель, Хассе, Шевалле, Артин, а ближе к нашему времени Ивасава, Тэйт и Тамагава. Каждый из них сделал значительные шаги на этом пути. Само собой разумеется, что, стоит лишь перестать считать недопустимым включение в арифметическое варево такого ингредиента, как вещественное поле, пусть на бесконечно большом расстоянии,—и сразу появляется возможность рассматривать функциональные поля над конечными полями и числовые поля одновременно, а не обособленно или в лучшем случае порознь, но общими методами, как это делалось до сих пор. Я надеюсь, что в этой книге мне удалось убедительно показать, что при подобной трактовке обе теории ничего не теряют и много выигрывают.

Мне неоднократно указывали, что многие важные факты и содержательные результаты, касающиеся локальных полей, могут быть доказаны чисто алгебраическими средствами без использования локальной компактности и потому сохраняют силу при значительно более общих предположениях. Но, быть может, мне позволительно думать, что я ничего не знаю об этом обстоятельстве, равно как и о возможности аналогичного обобщения даже таких глобальных результатов, как теорема Римана — Роха? Мы имеем здесь дело с математикой, а не с теологией. Пусть другие математики думают, что им доступно проникновение в мысли Бога об их любимом предмете; мне это всегда казалось пустым и бессмысленным занятием. Мои намерения в этой книге скромнее. Я пытался показать, что с принятой мной точки зрения можно дать связное изложение затронутых выше вопросов, удовлетворительное как логически, так и эстетически. Мои усилия были бы вполне вознаграждены, если это хотя бы в какой-нибудь степени удалось.

Возможно, некоторые из читателей удивятся, не найдя в моем изложении теории полей классов никакого явного упоминания когомологий. В этом смысле мой подход к теории чисел, будучи «современным» в первой части книги, является в то же время сугубо «несовременным» во второй. Искушенный читатель, конечно, поймет, что все когомологии фактически запрятаны в теорию простых алгебр, и притом ровно в том количестве, в каком это нужно для теории полей классов. Для знающих язык когомологий Галуа будет легким и не бесполезным упражнением перевести на него некоторые определения и результаты глав IX, XII и XIII. В одном или двух местах (из которых наиболее бросающееся в глаза —«теорема

о переносе» из § 5 главы XII) это, пожалуй, даже привело бы к более удовлетворительным доказательствам, чем наши. Однако развивать такой подход систематически означало бы нагружать балластом излишней техники корабль, хорошо оснащенный для нашего ограниченного плавания. Вместо того чтобы улучшить его мореходные качества, это могло бы потопить его.

Прокладывая курс своего корабля, я старался избегать арифметической теории алгебраических групп; это весьма интересный предмет, но он, очевидно, не созрел еще для изложения в книге. Отчасти по этой причине я отказался от всякого обсуждения дзета-функций простых алгебр, более развернутого, чем это нужно для теории полей классов. Исключены также неабелевы L-функции Артина; однако прочитав эту книгу, читатель будет вполне подготовлен к изучению прекрасных работ Артина на эту тему, при условии, что он знает к тому же теорию представлений конечных групп.

Мне остается исполнить приятный долг и выразить благодарность Дэвиду Кантору, который приготовил записи моих лекций в Принстонском университете, вошедшие в книгу как главы I — VII (во многих местах совершенно без изменений), и Шевалле, который великодушно позволил мне использовать упомянутую выше рукопись и написать на ее основе главы XII и XIII. Я благодарен также Ивасаве и Лазару, прочитавшим книгу в рукописи и предложившим много улучшений; Х. Погожельскому за помощь в чтении корректур; Б. Экману за интерес, проявленный им к опубликованию книги, и сотрудникам издательства Шпрингер и типографии Цехнера за их квалифицированное сотрудничество и неоценимую помощь в деле издания этой книги.

Андрэ Вейль

Принстон, май 1967

ХРОНОЛОГИЧЕСКАЯ ТАБЛИЦА

В подражание «Хронологической таблице» («Zeittafel») Гекке, помещенной в конце его «Теории алгебраических чисел», и в качестве частичной замены отсутствующего исторического обзора, мы приводим здесь хронологический список математиков, сделавших, как нам кажется, наиболее значительный вклад в рассматриваемые в этой книге вопросы.

ФЕРМА	(1601—1665)	РИМАН	(1826—1866)
ЭЙЛЕР	(1707—1783)	ДЕДЕКИНД	(1831—1916)
ЛАГРАНЖ	(1736—1813)	ВЕБЕР	(1842—1913)
ЛЕЖАНДР	(1752—1833)	ГЕНЗЕЛЬ	(1861—1941)
ГАУСС	(1777—1855)	ГИЛЬБЕРТ	(1862—1943)
ДИРИХЛЕ	(1805—1859)	ТАКАГИ	(1875—1960)
КУММЕР	(1810—1893)	ГЕККЕ	(1887—1947)
ЭРМИТ	(1822—1901)	АРТИН	(1898—1962)
ЭЙЗЕНШТЕЙН	(1823—1852)	ХАССЕ	(1898)
КРОНЕКЕР	(1823—1891)	ШЕВАЛЛЕ	(1909)

ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ И ОБОЗНАЧЕНИЯ

В этой книге не предполагается никакого знания теории чисел, за исключением самых элементарных фактов о целых числах. Полезно, но не обязательно знакомство с p-адическими нормированиями поля рациональных чисел $\mathbf{Q}$ и определяемыми этими нормированиями его пополнениями $\mathbf{Q}_p$. С другой стороны, если читатель захочет ознакомиться с историей вопросов, трактуемых в первой части книги, то он не найдет ничего лучше, чем непревзойденная «Теория алгебраических чисел» Гекке, или, если он пожелает пойти еще дальше назад, «Теория чисел» Дирихле — Дедекинда (либо 4-е, последнее издание 1894 г., либо 3-е издание 1879 г.), содержащая знаменитое «одиннадцатое дополнение» Дедекинда. Изучающим вторую часть книги можно рекомендовать «Отчет о теории полей классов» Хассе (*Klassenkörperbericht*, J.D.M.V., ч. I, 1926, ч. II, 1930).

Предполагается, что читатель знаком с основными понятиями алгебры (группы, кольца, поля) и линейной алгебры (векторные пространства, тензорные произведения). Теория Галуа в первой части (гл. I — VIII) не используется, за исключением отдельных мест, которые можно опустить при первом чтении. Для чтения второй части (гл. IX — XIII) знание основных фактов теории Галуа (как для конечных, так и для бесконечных расширений) совершенно необходимо.

На протяжении всей книги, начиная с самой первой главы, существенно используются основные свойства локально компактных коммутативных групп, в частности существование и единственность меры Хаара. Прежде чем браться за изучение настоящей книги, читатель должен хотя бы в общих чертах познакомиться с этими вопросами. В гл. X и XI (и лишь там) используется мера Хаара для некоммутативных локально компактных групп. В § 5 гл. II коротко напоминаются основные факты из теории двойственности локально компактных коммутативных групп,

а в § 2 гл. VII — основные факты из теории преобразования Фурье, играющие существенную роль в дальнейшем изложении.

Что касается терминологии и обозначений, то они обычно совпадают с терминологией и обозначениями Бурбаки. В частности, это относится к символам $\mathbf{N}$ (множество «конечных кардинальных», или «натуральных» чисел $0, 1, 2, \ldots$), $\mathbf{Z}$ (кольцо рациональных целых чисел), $\mathbf{Q}$ (поле рациональных чисел), $\mathbf{R}$ (поле вещественных чисел), $\mathbf{C}$ (поле комплексных чисел), $\mathbf{H}$ (поле «классических», «обыкновенных», или «гамильтоновых» кватернионов). Если p — простое число, то мы обозначаем через $\mathbf{F}_p$ простое поле из p элементов, через $\mathbf{Q}_p$ — поле p-адических чисел (пополнение поля $\mathbf{Q}$ по отношению к p-адическому нормированию; см. § 3 гл. I), через $\mathbf{Z}_p$ — кольцо p-адических целых чисел (т. е. замыкание $\mathbf{Z}$ в $\mathbf{Q}_p$). Всегда подразумевается, что поля $\mathbf{R}$, $\mathbf{C}$, $\mathbf{H}$, $\mathbf{Q}_p$, равно как и конечномерные векторные пространства над ними, снабжены их обычной («естественной») топологией. Под $\mathbf{F}_q$ понимается конечное поле из q элементов, если таковое существует, т. е. если q имеет вид p^n, где p — простое число, а n — целое $\geqslant 1$ (см. § 1 гл. I). Символ $\mathbf{R}_+$ обозначает множество всех вещественных чисел $\geqslant 0$.

Предполагается, что все кольца имеют единицу. Единица кольца R обозначается через 1_R или просто 1, если это не может вызвать недоразумений; мультипликативная группа обратимых элементов кольца R обозначается через $R^\times$. В частности, если K — поле (не обязательно коммутативное), $K^\times$ — это мультипликативная группа его ненулевых элементов. Мультипликативную группу вещественных чисел >0 мы обозначаем через $\mathbf{R}_+^\times$. Пусть R — произвольное кольцо. Символ $M_n(R)$ обозначает кольцо матриц с n строками и n столбцами с элементами из R, а 1_n — единицу этого кольца, т. е. матрицу (δ_{ij}), где $\delta_{ij} = 1_R$ или 0, в соответствии с тем, $i = j$ или $i \neq j$; ${}^tX$ обозначает матрицу, транспонированную к матрице $X \in M_n(R)$, а $\mathrm{tr}\,(X)$ — ее след, т. е. сумму диагональных элементов. В случае когда кольцо R коммутативно, через $\det(X)$ обозначаем определитель матрицы X. Иногда мы будем писать $M_{m,n}(R)$ для обозначения множества матриц с элементами из R, имеющих m строк и n столбцов.

Если R — коммутативное кольцо и T — переменная, то мы обозначаем через $R[T]$ кольцо многочленов от T с коэффициентами в R. Многочлен называется *унитарным*, если его старший коэффициент равен 1. Если S — кольцо, содержащее R, и x — его элемент, коммутирующий со всеми элементами из R, то мы обозначаем через $R[x]$ подкольцо в S, порожденное R и x. Оно состоит из элементов кольца S, имеющих вид $F(x)$, где $F \in R[T]$. Если K — коммутативное поле, L — некоторое (не обязательно комму-

тативное) поле, содержащее K, и x — элемент поля L, коммутирующий со всеми элементами из K, то мы обозначаем через $K(x)$ подполе в L, порожденное K и x. Это подполе коммутативно. Мы называем поле L «расширением» поля K, только если оба они коммутативны; обычно этот термин используется в случае, когда поле L конечной степени над K, и тогда $[L : K]$ обозначает его степень, т. е. размерность L, рассматриваемого как векторное пространство над K (индекс группы g' в группе g также обозначается через $|g : g'|$, если он конечен; это не приводит к путанице).

Все топологии предполагаются *хаусдорфовыми*, т. е. удовлетворяющими аксиоме отделимости Хаусдорфа (*отделимыми* в смысле Бурбаки). Слово *гомоморфизм* для групп, колец, модулей, векторных пространств употребляется в следующем смысле: (a) в случае когда имеются топологии, *все гомоморфизмы предполагаются непрерывными*; (b) гомоморфизмы колец предполагаются *унитарными*; это означает, что гомоморфизм кольца R в кольцо S переводит 1_R в 1_S. С другой стороны, в случае групп гомоморфизмы *не предполагаются открытыми* (т. е. переводящими открытые множества в открытые). Поэтому в случае надобности мы говорим об *открытом гомоморфизме*. Слово *морфизм* используется как краткий синоним слова *гомоморфизм*. В некоторых ситуациях в качестве синонима слова гомоморфизм используется также слово *представление*, например для гомоморфизмов заданной группы в $\mathbf{C}^\times$ или для некоторых гомоморфизмов простых алгебр (см. § 2 гл. IX). Под *характером* (не обязательно коммутативной) группы G будем понимать, как обычно, гомоморфизм (или «представление») группы G в подгруппу группы $\mathbf{C}^\times$, определяемую условием $z\bar{z} = 1$. Как было сказано выше, он предполагается непрерывным, если G — топологическая группа. Употребление слов *эндоморфизм*, *автоморфизм*, *изоморфизм* подчиняется тем же ограничениям (a) и (b), что и для слова гомоморфизм. Следовательно, в топологическом случае автоморфизмы и изоморфизмы суть отображения биективные и бинепрерывные. Если f — отображение множества A в множество B, причем оба эти множества снабжены некоторыми структурами (обычно структурами поля) и f определяет изоморфизм A на его образ в B, то иногда, допуская вольность речи, мы говорим, что f — изоморфизм из A в B.

Говорят, что элемент x группы G имеет *порядок* n, если n — наименьшее целое $\geqslant 1$, для которого $x^n = e$, где e — единичный элемент группы G. Если K — поле, то элемент конечного порядка из $K^\times$ называется *корнем из единицы в* K; в согласии с давней традицией корень из единицы порядка, делящего n, называют корнем степени n из единицы в K; его называют *примитивным* корнем

n-й степени из единицы, если его порядок равен n. Таким образом, корни n-й степени из единицы в K являются корнями в K уравнения $X^n = 1$.

Если a, b — элементы из $\mathbf{Z}$, то (a, b) обозначает их наибольший общий делитель, т. е. элемент d из $\mathbf{N}$, такой, что $d\mathbf{Z} = a\mathbf{Z} + b\mathbf{Z}$. Пусть R — произвольное кольцо. Отображение $n \to n \cdot 1_R$ из $\mathbf{Z}$ в R переводит $\mathbf{Z}$ в подкольцо $\mathbf{Z} \cdot 1_R$ кольца R, известное под названием *простого кольца в* R. Ядро морфизма $n \to n \cdot 1_R$ из $\mathbf{Z}$ на $\mathbf{Z} \cdot 1_R$ является подгруппой в $\mathbf{Z}$ и, следовательно, имеет вид $m \cdot \mathbf{Z}$, где $m \in \mathbf{N}$. Если R не равно $\{0\}$ и не имеет делителей нуля, число m либо равно 0, либо просто; его называют *характеристикой* кольца R. Если $m = 0$, то отображение $n \to n \cdot 1_R$ является изоморфизмом кольца $\mathbf{Z}$ на $\mathbf{Z} \cdot 1_R$, что позволяет их отождествлять. Если же характеристика кольца R есть простое число $p > 1$, то простое кольцо $\mathbf{Z} \cdot 1_R$ изоморфно простому полю $\mathbf{F}_p$.

Рассматривая левые и правые модули над некоммутативными кольцами, мы будем использовать следующие обозначения. Пусть R — кольцо, M и N — левые модули над ним. Тогда морфизмы из M в N, сохраняющие их структуры как левых R-модулей, можно рассматривать как *правые операторы* на M; иначе говоря, если α — такой морфизм, то можно записывать его в виде $m \to m\alpha$, где $m \in M$, и свойство быть морфизмом означает, помимо аддитивности, что для всех $r \in R$ и $m \in M$ $r\,(m\alpha) = (rm)\,\alpha$. Это относится, в частности, к эндоморфизмам модуля M. Аналогичным образом морфизмы правых R-модулей можно записывать как левые операторы. Эта запись будет постоянно использоваться, в частности, в гл. IX.

Поскольку морфизмы полей, как указывалось выше, предполагаются унитарными, они всегда инъективны. Поэтому в согласии со сказанным выше морфизм поля K в поле L мы будем иногда называть изоморфизмом или *вложением* поля K в L. В первой части книги для таких отображений будет использоваться «функциональная» запись, а начиная с § 3 гл. VIII, где на сцену выходит теория Галуа,—«экспоненциальная» запись. В первом случае отображение λ записывается в виде $x \to \lambda(x)$, а во втором — в виде $x \to x^\lambda$. Пусть L — расширение Галуа поля K и λ, μ — два его автоморфизма над K. Определим закон композиции $(\lambda, \mu) \to \lambda\mu$ в группе Галуа $\mathfrak{g}$ поля L над K как закон $(\lambda, \mu) \to \lambda \circ \mu$ в первом случае и как противоположный закон во втором случае. Иначе говоря, он определяется соответственно условиями $(\lambda\mu)\,x = \lambda\,(\mu x)$ и $x^{\lambda\mu} = (x^\lambda)^\mu$. Например, если K' — поле, промежуточное между K и L, и $\mathfrak{h}$ — соответствующая подгруппа в $\mathfrak{g}$, состоящая из автоморфизмов, которые оставляют на месте все элементы поля K',

то автоморфизмы поля L над K, совпадающие на K' с заданным автоморфизмом λ, образуют правый класс смежности $\lambda\mathfrak{h}$ в функциональной записи и левый класс $\mathfrak{h}\lambda$ — в экспоненциальной.

Пусть A, B, C — аддитивно записанные коммутативные группы (как правило, с дополнительными структурами), и пусть задан *дистрибутивный* (или *биаддитивный*, или *билинейный*) морфизм $(a, b) \to ab$ из $A \times B$ в C. В этом случае для двух подгрупп X и Y соответственно в A и B принято через $X \cdot Y$ обозначать не образ произведения $X \times Y$ относительно этого отображения, а подгруппу в C, порожденную этим образом, т. е. подгруппу, состоящую из конечных сумм вида $\sum x_i y_i$, где $x_i \in X$ и $y_i \in Y$ для всех i. Это обозначение будет использоваться, например, в гл. V.

По типографским причинам мы часто пишем $\exp(z)$ вместо e^z и $\mathbf{e}(z)$ вместо $\exp(2\pi i z) = e^{2\pi i z}$ для $z \in \mathbf{C}$; обозначение $\mathbf{e}(z)$ применяется, как правило, лишь для $z \in \mathbf{R}$.

Наконец, объясним систему ссылок внутри книги. Мы не скупились на такие ссылки, имея в виду помочь неискушенному читателю. Читатель может не прослеживать ссылки до самого конца, если утверждение уже стало ему ясным. Теоремы нумеруются подряд внутри каждой главы; то же относится к предложениям, леммам, определениям, нумерованным формулам. Теоремы и предложения могут сопровождаться одним или несколькими следствиями. Теоремы, вообще говоря, следует рассматривать как более важные утверждения, чем предложения, но при более глубоком подходе особую разницу между ними обнаружить трудно. Леммы являются существенно вспомогательными результатами. Не все новые понятия вводятся как нумерованные определения; однако все понятия, за исключением предполагающихся известными, приведены в указателе в конце книги со ссылкой на место, где это понятие появляется в первый раз. Нумерация формул производится только для удобства ссылок на них и не означает их важности. Если ссылка имеет вид: «по предложению 2», «по следствию 1 теор. 3» и т. п., речь идет о результатах того же параграфа. Если ссылка имеет вид: «по предложению 2 § 2», «по теореме 3 § 3» и т. п., читатель отсылается к другому параграфу той же главы. Наконец, если ссылка имеет вид: «по предложению 2 гл. IV-2», имеется в виду предложение 2 из § 2 гл. IV. Номера глав и параграфов приведены в колонтитулах вверху страниц.

Далее приведен список наиболее часто встречающихся обозначений в порядке их появления.

СПИСОК ОБОЗНАЧЕНИЙ

ГЛАВА ПЕРВАЯ

§ 2: mod_G, mod_V, mod_K.
§ 3: $|x|_p$, $|x|_\infty$, $\mathbf{Q}_\infty = \mathbf{R}$, $|x|_v$, $\mathbf{Q}_v$ (v — простое число или ∞).
§ 4: K (произвольное p-поле), R, P, π, q, ord_K, ord, $M^\times$, M.

ГЛАВА ВТОРАЯ

§ 3: $1 + P^n$ (как подгруппа в $K^\times$ при $n \geqslant 1$).
§ 5: $\langle g, g^* \rangle_G$, $\langle g, g^* \rangle$, G^* H_*, V^*, L_*, V', $[v, v']_V$, $[v, v']$, χ, ord (χ).

ГЛАВА ТРЕТЬЯ

§ 1: (для точки v $\mathbf{A}$-поля k) $|x|_v$, k_v, r_v, p_v (относительно q_v см. гл. VII-1); ∞ (как точка поля $\mathbf{Q}$), $w \mid v$, $E_v = E \otimes_k k_v$, ε_v, $\mathscr{A}_v$, α_v.
§ 3: End (E), $\mathrm{Tr}_{\mathscr{A}/k}$, $\mathrm{N}_{\mathscr{A}/k}$, $\mathrm{Tr}_{k'/k}$, $\mathrm{N}_{k'/k}$.

ГЛАВА ЧЕТВЕРТАЯ

§ 1: P, P_∞, $k_{\mathbf{A}}(P)$, $k_{\mathbf{A}}$, χ, χ_v, $E_{\mathbf{A}}(P, \varepsilon)$, $E_{\mathbf{A}}$, $\mathscr{A}_{\mathbf{A}}$, $\mathscr{A}_{\mathbf{A}}$ (P, α), $(k'/k)_{\mathbf{A}}$, $(E/k)_{\mathbf{A}}$.
§ 3: Aut E, $\mathscr{A}_{\mathbf{A}}^\times$, $\mathscr{A}_{\mathbf{A}}(P, \alpha)^\times$, $|a|_{\mathbf{A}}$.
§ 4: $k_{\mathbf{A}}^1$, M, $\Omega(P) = k_{\mathbf{A}}(P)^\times$, $\Omega_1(P)$, $E(P)$.

ГЛАВА ПЯТАЯ

§ 2: k_∞, E_∞, $\mathfrak{r}$, L_v.
§ 3: $\mathfrak{p}_v$, $I(k)$, id (a), $P(k)$, h, $\mathfrak{N}(a)$.
§ 4. $|dx \wedge d\bar{x}|$, R, c_k.

ГЛАВА ШЕСТАЯ

deg $(\mathfrak{a})$, $\mathfrak{a} \succ \mathfrak{b}$, div (a), $D(k)$, $P(k)$, $D_0(k)$, g, div (χ).

ГЛАВА СЕДЬМАЯ

§ 1: q_v, ζ_k (см. § 6).
§ 2: Φ^*, $\prod \Phi_v$, $\prod \alpha_v$.
§ 3: $\Omega(G)$, Ω_1, ω_s.
§ 4: $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$, $\Omega(G_k)$, ω_1, ω_s, G_k^1, Ω_1, M, N, ω_v, $\prod \omega_v$, $Z(\omega, \Phi)$.
§ 6: $G_1(s)$, $G_2(s)$, c_k (см. гл. V-4), $G_w(s)$, $\zeta_k(s)$, $Z_k(s)$.
§ 7: $f(v)$, s_v, A, B, N_v, Φ_ω, $\varkappa = \prod \varkappa_v$, $a = (a_v)$, $b = (b_v)$, G_w, $\lambda(v)$, π_v, $L(s, \omega)$, $\mathfrak{f}$, $\Lambda(s, \omega)$.
§ 8: G_P, $I(P)$, $D(P)$.

ГЛАВА ВОСЬМАЯ

§ 1: K, K', n, q, R, P, π, q', R', P', π', f, e, Tr, N, $\mathfrak{N}$, d, $D(K'/K)$, D, ι'.
§ 2: Δ.
§ 3: $\nu(\lambda)$, $\mathfrak{g}_\nu$.
§ 4: $\mathfrak{d}$, ι, $\mathfrak{N}_{k'/k}$, $\mathfrak{N}$, $\mathfrak{D}$.

ГЛАВА ДЕВЯТАЯ

§ 1: A_L, $A \otimes B$, A^0.
§ 2: τ, ν.
§ 3: Cl (A), $B(K)$, $\overline{K}$, K_{sep}, $\mathfrak{C}$, $\mathfrak{H}$, K', $\overline{K'}$, K'_{sep}, $\mathfrak{C}'$, ρ, $H(K)$.
§ 4: $\{\chi, \theta\}$, $[L/K; \chi, \theta]$.
§ 5: $\chi_{n,\xi}$, $\{\xi, \theta\}_n$, $\chi_{p,\xi}$, $\{\xi, \theta\}_p$.

ГЛАВА ДЕСЯТАЯ

§ 1: Hom (V, W), Hom $(V, L; W, M)$, End (V, L), Aut (V, L).
§ 3: $\mathfrak{T}$, $\mathfrak{T}'$, $\mathfrak{T}''$, $\mathfrak{T}$, $\mathfrak{U}$.

ГЛАВА ДВЕНАДЦАТАЯ

§ 1: K_{ab}, $\mathfrak{C}^{(1)}$, $\mathfrak{A}$, X_K, ρ, G_K, $(\chi, g)_K$, $\mathfrak{a}$, G_K^1, U_K, X_0, $\mathfrak{A}_0$, K_0.
§ 2: $h(A)$, η, $(\chi, \theta)_K$ (для $K = \mathbf{R}$, $\mathbf{C}$); $\mathfrak{M}$, K_0, $\mathfrak{H}_0$, K_n, φ_0, X_0, φ, η, $(\chi, \theta)_K$, $\mathfrak{a}$, $h(A)$.
§ 3: U_K, $\mathfrak{A}_0$.

ГЛАВА ТРИНАДЦАТАЯ

§ 1: $\overline{k}$, K_v, k_{sep}, $k_{v,\mathrm{sep}}$, k_{ab}, $k_{v,\mathrm{ab}}$, $\mathfrak{C}$, $\mathfrak{A}$, $\mathfrak{C}_v$, $\mathfrak{A}_v$, ρ_v, X_k, χ_v, $(\chi_v, z)_v$, $(\chi, z)_k$, $\mathfrak{a}$, $k_{\infty+}^{\times}$, F, q, k_0, $\mathfrak{H}_0$, X_0, k_n, $\mathfrak{A}_0$, φ_0, φ, $\overline{\mathbf{Q}}$, ε, $\mathfrak{H}_m$, $\mathfrak{g}$, $\mathfrak{h}$.
§ 3: $h_v(A)$, U_k.
§ 5: $(x, y)_{n,K}$, $(z, z')_n$, $\Omega(P)$ (см. гл. IV-4), $\Omega'(P)$.
§ 7: $(x, z)_{p,K}$, Φ, $\Omega'(m, K)$, $(x, z)_p$, $\Omega'(\mathfrak{m})$.
§ 9: $\mathfrak{B}(L)$, $N(L)$.
§ 10: k', $\mathfrak{g}$, $\mathfrak{h}$, U, $\mathfrak{B}$, U_v, $\mathfrak{B}_v$, γ, γ_v, $\mathfrak{f}(\omega)$, $\mathfrak{D}$.
§ 11: G_P, G'_P, L_P, l_P, pr, $\mathfrak{U}_P$, $J(U, P)$.

ЧАСТЬ ПЕРВАЯ

ЭЛЕМЕНТАРНАЯ ТЕОРИЯ

ГЛАВА ПЕРВАЯ

ЛОКАЛЬНО КОМПАКТНЫЕ ПОЛЯ

§ 1. КОНЕЧНЫЕ ПОЛЯ

Пусть F — конечное (не обязательно коммутативное) поле с единичным элементом 1. Его характеристика является, очевидно, простым числом $p > 1$, а простое кольцо, содержащееся в F, изоморфно простому полю $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, с которым оно может быть отождествлено. Таким образом, F можно рассматривать как векторное пространство над $\mathbf{F}_p$; очевидно, оно имеет конечную размерность f, а число его элементов равно $q = p^f$. Если F — подполе поля F', состоящего из $q' = p^{f'}$ элементов, F' можно также рассматривать, как, скажем, левое векторное пространство над F, и если его размерность равна d, то $f' = df$ и $q' = q^d = p^{df}$.

Теорема 1. *Все конечные поля коммутативны.*

Эта теорема впервые была доказана Веддербарном, и мы воспроизведем здесь принадлежащий Витту вариант его первоначального доказательства. Пусть F — конечное поле характеристики p, Z — его центр, $q = p^f$ — число элементов в Z; если размерность поля F как векторного пространства над Z равна n, то F имеет q^n элементов. Мультипликативную группу $F^\times$ ненулевых элементов поля F можно разбить на классы «сопряженных» элементов, называя два элемента x, x' из $F^\times$ сопряженными, если существует элемент $y \in F^\times$, такой, что $x' = y^{-1}xy$. Для каждого $x \in F^\times$ обозначим через $N(x)$ множество элементов поля F, коммутирующих с x; это — подполе в F, содержащее Z; если $\delta(x)$ — его размерность над Z, то в нем имеется $q^{\delta(x)}$ элементов. Как мы видели выше, n кратно $\delta(x)$ и $\delta(x) < n$ при $x \notin Z$. Поскольку число элементов группы $F^\times$, сопряженных с x, равно индексу группы $N(x)^\times$ в $F^\times$, т. е. $(q^n - 1)/(q^{\delta(x)} - 1)$, получаем

$$q^n - 1 = q - 1 + \sum_x \frac{q^n - 1}{q^{\delta(x)} - 1}, \tag{1}$$

где сумма распространяется на полное множество представителей классов нецентральных сопряженных элементов из $F^\times$. Предположим теперь, что $n > 1$, и обозначим через P «круговой» многочлен $\prod (T - \zeta)$, где произведение берется по всем примитивным корням n-й степени из 1 в поле $\mathbf{C}$ комплексных чисел. По хорошо известной элементарной теореме (легко доказываемой индукцией по n) этот многочлен имеет целые рациональные коэффициенты; ясно, что P делит $(T^n - 1)/(T^\delta - 1)$ для любых δ, делящих n и отличных от n. Следовательно, в (1) все члены, кроме $q - 1$, кратны $P(q)$, так что $P(q)$ должно делить $q - 1$. С другой стороны, каждый множитель в произведении $P(q) = \prod (q - \zeta)$ по абсолютной величине больше $q - 1$. Мы пришли к противоречию, значит $n = 1$, а $F = Z$.

Таким образом, к каждому конечному полю применим следующий элементарный результат.

Лемма 1. *Если K — коммутативное поле, то всякая конечная подгруппа в $K^\times$ циклична.*

Действительно, пусть Γ — такая группа, или, что то же самое, конечная подгруппа группы всех корней из 1 в поле K. Для каждого $n \geqslant 1$ существует не более n корней уравнения $X^n = 1$ в поле K и, следовательно, в Γ; покажем, что всякая конечная коммутативная группа с подобным свойством циклична. Пусть α — элемент группы Γ, имеющий максимальный порядок N. Обозначим через β какой-нибудь элемент из Γ и через n его порядок. Если n не делит N, то для некоторого простого числа p существует такая его степень $q = p^\nu$, что q делит n, но не N. Сразу проверяется, что порядок элемента $\alpha\beta^{n/q}$ есть наименьшее общее кратное N и q, так что он больше N, что противоречит определению N. Следовательно, n делит N. Поэтому уравнение $X^n = 1$ имеет в Γ n различных корней $\alpha^{iN/n}$ с $0 \leqslant i < n$; поскольку β — корень этого уравнения, он обязан быть одним из них. Значит, α порождает группу Γ.

Теорема 2. *Пусть K — алгебраически замкнутое поле характеристики $p > 1$. Тогда для каждого $f \geqslant 1$ поле K содержит одно и только одно поле $F = \mathbf{F}_q$ из $q = p^f$ элементов; поле F состоит из корней уравнения $X^q = X$ в поле K; группа $F^\times$ состоит из корней уравнения $X^{q-1} = 1$ в поле K и является циклической группой порядка $q - 1$.*

Пусть F — произвольное поле из q элементов. Лемма 1 показывает, что $F^\times$ — циклическая группа порядка $q - 1$. Поэтому, если K содержит поле F, группа $F^\times$ должна состоять из корней уравнения $X^{q-1} = 1$, а поле F — из корней уравнения $X^q - X =$

$= 0$, так что оба они однозначно определены. Обратно, если $q = p^f$, то $x \to x^q$ есть автоморфизм поля K, инвариантные элементы которого образуют поле F, состоящее из корней уравнения $X^q - X = 0$; так как, очевидно, многочлен $X^q - X$ имеет в поле K только простые корни, поле F состоит из q элементов.

Следствие 1. *С точностью до изоморфизма существует только одно поле из $q = p^f$ элементов.*

Это сразу следует из теоремы 2 и того факта, что все алгебраические замыкания простого поля $\mathbf{F}_q$ изоморфны. Этим оправдывается обозначение $\mathbf{F}_q$ для рассматриваемого поля.

Следствие 2. *Положим $q = p^f$, $q' = p^{f'}$, где $f \geqslant 1$, $f' \geqslant 1$. Поле $\mathbf{F}_{q'}$ содержит поле $\mathbf{F}_q$ из q элементов в том и только в том случае, когда f делит f'; если это так, то $\mathbf{F}_{q'}$ является циклическим расширением поля $\mathbf{F}_q$ степени f'/f и его группа Галуа над $\mathbf{F}_q$ порождается автоморфизмом $x \to x^q$.*

Как мы уже говорили, если поле $\mathbf{F}_{q'}$ содержит $\mathbf{F}_q$, то оно должно иметь над ним конечную степень d и $q' = q^d$, $f' = df$. Обратно, предположим, что $f' = df$, так что $q' = q^d$, и обозначим через K алгебраическое замыкание поля $\mathbf{F}_{q'}$. В силу теоремы 2 поля $\mathbf{F}_q$ и $\mathbf{F}_{q'}$, содержащиеся в K, состоят из элементов поля K, инвариантных соответственно относительно автоморфизмов α и β, определяемых формулами $x \to x^q$ и $x \to x^{q'}$; поскольку $\beta = \alpha^d$, поле $\mathbf{F}_{q'}$ содержит $\mathbf{F}_q$. Ясно, что α отображает поле $\mathbf{F}_{q'}$ на себя; если φ — автоморфизм поля $\mathbf{F}_{q'}$, индуцированный α, то $\mathbf{F}_q$ состоит из элементов, инвариантных относительно φ и, следовательно, относительно группы автоморфизмов поля $\mathbf{F}_{q'}$, порожденной φ; эта группа конечна, так как φ^d — тождественное отображение; используя теорию Галуа, получаем, что эта группа является группой Галуа поля $\mathbf{F}_{q'}$ над $\mathbf{F}_q$ и имеет порядок d.

Следствие 3. *В тех же обозначениях, что и в следствии 2, предположим, что $f' = df$. Тогда для каждого $n \geqslant 1$ элементы поля $\mathbf{F}_{q'}$, инвариантные относительно отображения $x \to x^{q^n}$, образуют подполе, состоящее из q^r элементов поля $\mathbf{F}_{q'}$, где $r = (d, n)$.*

Пусть K — то же, что и в доказательстве следствия 2. Элементы поля K, инвариантные относительно отображения $x \to x^{q^n}$, образуют подполе F' поля K из q^n элементов; поэтому $F' \cap \mathbf{F}_{q'}$ будет наибольшим подполем, содержащимся как в F', так и в $\mathbf{F}_{q'}$, и поскольку оно содержит $\mathbf{F}_q$, число его элементов должно иметь вид q^r, где r равно, как показывает следствие 2, (d, n).

§ 2. МОДУЛЬ В ЛОКАЛЬНО КОМПАКТНОМ ПОЛЕ

Любое поле, снабженное дискретной топологией, становится локально компактным. Поэтому задача описания и изучения локально компактных полей становится содержательной лишь при условии недискретности рассматриваемого поля.

Напомним определение модуля автоморфизма, которое является основным для дальнейшего. Для наших целей достаточно рассматривать автоморфизмы локально компактных коммутативных групп. Пусть G — такая группа (записываемая аддитивно), λ — автоморфизм группы G и α — мера Хаара на G. Так как мера Хаара определена однозначно с точностью до константы, λ переводит α в меру $c\alpha$, где $c \in \mathbf{R}_+^\times$; постоянный множитель c, который, очевидно, не зависит от выбора меры α, называется *модулем* автоморфизма λ и обозначается символом $\mathrm{mod}_G(\lambda)$. Иначе говоря, он определяется одной из следующих эквивалентных формул:

$$\alpha(\lambda(X)) = \mathrm{mod}_G(\lambda)\,\alpha(X), \tag{2}$$

$$\int f(\lambda^{-1}(x))\,d\alpha(x) = \mathrm{mod}_G(\lambda)\int f(x)\,d\alpha(x),$$

где X — произвольное измеримое множество, f — интегрируемая функция и $0 < \alpha(X) < +\infty$, $\int f\,d\alpha \neq 0$. Вторую формулу символически можно записать так: $d\alpha(\lambda(x)) = \mathrm{mod}_G(\lambda)\,d\alpha(x)$. Если группа G дискретна или компактна, первая формула (примененная соответственно к $X = \{0\}$ и к $X = G$) показывает, что модуль равен 1. Ясно, что если λ, λ' — автоморфизмы группы G, то модуль автоморфизма $\lambda \circ \lambda'$ равен произведению модулей λ и λ'. Нам понадобится следующая лемма:

Лемма 2. *Пусть G' — замкнутая подгруппа группы G и λ — автоморфизм группы G, индуцирующий на G' автоморфизм λ'. Положим $G'' = G/G'$ и обозначим через λ'' автоморфизм группы G'', определяемый λ по модулю G'. Тогда*

$$\mathrm{mod}_G(\lambda) = \mathrm{mod}_{G'}(\lambda')\,\mathrm{mod}_{G''}(\lambda'').$$

В самом деле, как хорошо известно, можно выбрать меры Хаара α, α', α'' на группах G, G', G'' так, чтобы для любой непрерывной функции f на G с компактным носителем выполнялось равенство

$$\int_G f(x)\,d\alpha(x) = \int_{G''}\left(\int_{G'} f(x+y)\,d\alpha'(y)\right)d\alpha''(\dot{x});$$

здесь $\dot{x}$ обозначает образ x в G'', а функция $\int f(x+y)\,d\alpha'(y)$, которая записана как функция от $x \in G$, но фактически постоянна на клас-

сах смежности по подгруппе G', рассматривается очевидным образом как функция от x на группе G''. Применяя к обеим частям автоморфизм λ, получаем утверждение леммы.

Пусть теперь K—произвольное топологическое поле и $a \in K^\times$. Тогда $x \to ax$ и $x \to xa$ — автоморфизмы его аддитивной группы, и если поле K локально компактно, то можно рассматривать их модули. Точно так же если V — топологическое левое векторное пространство над K, то $v \to av$ есть его автоморфизм для любого $a \in K^\times$, и если V локально компактно, можно определить модуль этого автоморфизма. Мы будем обозначать его через $\mathrm{mod}_V(a)$ и считать, что $\mathrm{mod}_V(0)$ равен 0. Иными словами, если μ — мера Хаара на V и X — произвольное измеримое подмножество в V, для которого $0 < \mu(X) < +\infty$ (например, компактная окрестность нуля), то для каждого $a \in K$ модуль $\mathrm{mod}_V(a)$ определяется соотношением

$$\mathrm{mod}_V(a) = \frac{\mu(aX)}{\mu(X)}.$$

В частности, для любого локально компактного поля K мы полагаем $\mathrm{mod}_K(a)$ равным модулю автоморфизма $x \to ax$, если $a \neq 0$, и равным 0, если $a = 0$. Позднее будет показано, что модуль автоморфизма $x \to xa$ тот же самый, что и у автоморфизма $x \to ax$. Ясно, что если $K = \mathbf{R}$, $\mathbf{C}$ или $\mathbf{H}$, то $\mathrm{mod}_K(a)$ равен соответственно $|a|$, $|a|^2 = a\bar{a}$ или $|a|^4 = (a\bar{a})^2$.

Вплоть до конца этого параграфа обозначим раз и навсегда через K недискретное локально компактное поле (коммутативное или нет), а через α — меру Хаара его аддитивной группы.

Предложение 1. *Функция* mod_K *непрерывна на* K, *и* $\mathrm{mod}_K(ab) = \mathrm{mod}_K(a)\,\mathrm{mod}_K(b)$ *для всех* $a, b \in K$.

Последнее утверждение очевидно. Пусть X — компактная окрестность нуля в поле K. Для каждого $a \in K$ и каждого $\varepsilon > 0$ существует открытая окрестность U компактного множества aX, такая, что $\alpha(U) \leqslant \alpha(aX) + \varepsilon$; пусть W — окрестность точки a, для которой $WX \subset U$. Тогда для всех $x \in W$ имеем

$$\mathrm{mod}_K(x) \leqslant \mathrm{mod}_K(a) + \alpha(X)^{-1}\varepsilon.$$

Отсюда видно, что функция mod_K полунепрерывна сверху. В частности, она непрерывна в нуле. А поскольку $\mathrm{mod}_K(x) = \mathrm{mod}_K(x^{-1})^{-1}$ для $x \neq 0$, она также полунепрерывна снизу всюду на $K^\times$ и, следовательно, непрерывна.

Так как поле K недискретно, из предложения 1 следует, что для любого $\varepsilon > 0$ существует такое $a \in K$, что $0 < \mathrm{mod}_K(a) \leqslant \varepsilon$,

а для любого $M > 0$ — такое $b \in K$, что $\mathrm{mod}_K(b) \geqslant M$. Поскольку mod_K — неограниченная функция, K не может быть компактно.

Предложение 2. *Для всех $m > 0$ множество B_m элементов $x \in K$, таких, что $\mathrm{mod}_K(x) \leqslant m$, компактно.*

Пусть V — компактная окрестность нуля в K, W — окрестность нуля, для которой $WV \subset V$. Как и выше, можно выбрать $r \in V \cap W$ так, чтобы $0 < \mathrm{mod}_K(r) < 1$; индукцией по n получаем, что $r^n \in V$ для всех $n \geqslant 1$. Если r' — какая-нибудь предельная точка последовательности $\{r^n\}_{n \geqslant 1}$, то $\mathrm{mod}_K(r')$ должен быть равен нулю, ибо $\mathrm{mod}_K(r^n)$ стремится к нулю при $n \to +\infty$. Таким образом, эта последовательность не имеет других предельных точек, кроме нуля, а так как она содержится в компактном множестве V, ее предел равен нулю. Возьмем теперь $m > 0$ и $a \in B_m$; поскольку $r^n a$ стремится к нулю, существует наименьшее целое $\nu \geqslant 0$, такое, что $r^\nu a \in V$; если a не принадлежит V, то $r^{\nu-1}a \notin V$ и, следовательно, $r^\nu a \in V - (rV)$. Обозначим через X замыкание множества $V - (rV)$. Ясно, что X компактно и 0 не принадлежит X; поэтому если положить $\mu = \inf_{x \in X} \mathrm{mod}_K(x)$, то $\mu > 0$. Пусть N — целое число, для которого $\mathrm{mod}_K(r)^N \leqslant \mu/m$. Тогда для $a \in B_m$, $a \notin V$ и ν, определенного, как выше, имеем

$$\mathrm{mod}_K(r)^N m \leqslant \mu \leqslant \mathrm{mod}_K(r^\nu a) = \mathrm{mod}_K(r)^\nu \, \mathrm{mod}_K(a) \leqslant \mathrm{mod}_K(r)^\nu \, m$$

и, следовательно, $\nu \leqslant N$. Таким образом, B_m содержится в объединении компактных множеств V, $r^{-1}V$, . . ., $r^{-N}V$. Так как из предложения 1 следует, что B_m замкнуто, этим и завершается доказательство.

Следствие 1. *Множества B_m, $m > 0$, образуют фундаментальную систему окрестностей нуля в K.*

Пусть V — произвольная компактная окрестность нуля в поле K. Возьмем $m > \sup_{x \in V} \mathrm{mod}_K(x)$ так, чтобы $B_m \supset V$, обозначим через X замыкание множества $B_m - V$ и положим $m' = \inf_{x \in X} \mathrm{mod}_K(x)$. Тогда $0 \notin X$ и $X \subset B_m$. В силу предложения 2 X компактно. Следовательно, $0 < m' \leqslant m$. Если $0 < \mu < m'$, то $B_\mu \subset B_m$, $B_\mu \cap X = \varnothing$ и потому $B_\mu \subset V$.

Следствие 2. *Для $a \in K$ $\lim_{n \to +\infty} a^n = 0$ в том и только в том случае, когда $\mathrm{mod}_K(a) < 1$.*

Следствие 3. *Дискретное подполе поля K конечно.*

Пусть L — такое поле. Если $a \in L$, то непременно $\mathrm{mod}_K(a) \leqslant 1$, ибо в противном случае последовательность $\{a^{-n}\}_{n\geqslant 0}$ содержалась бы в L в силу предложения 2 и не была бы дискретной. Значит, L есть дискретное подмножество компактного множества B_1 и, следовательно, конечно. Но ясно, что этого не может быть, если K — поле характеристики 0.

Теорема 3. *Пусть V — топологическое левое векторное пространство над полем K и V' — его конечномерное подпространство с базисом $\{v_1, \ldots, v_n\}$. Тогда отображение*

$$(x_1, \ldots, x_n) \longrightarrow \sum_{i=1}^{n} x_i v_i$$

пространства K^n в V' является изморфизмом структур топологических левых векторных пространств на K^n и V'; при этом V' замкнуто в V и локально компактно.

Пусть f — указанное выше отображение. Оно биективно, K-линейно и непрерывно по определению топологического векторного пространства. Чтобы показать, что оно изоморфизм, достаточно доказать, что отображение f^{-1} непрерывно, т. е. что f — открытое отображение; ввиду следствия 1 предл. 2 и линейности f нам нужно только показать, что образ множества $(B_m)^n$ относительно отображения f содержит окрестность нуля в V' для всех $m > 0$. Пусть S — подмножество пространства K^n, определенное условием

$$\sup_i \mathrm{mod}_K(x_i) = 1.$$

Тогда $0 \notin S$; множество S замкнуто в силу предложения 1 и содержится в $(B_1)^n$, а потому компактно согласно предложению 2. Поэтому $0 \notin f(S)$ и $f(S)$ компактно. Следовательно, существуют окрестность нуля W в V и некоторая окрестность нуля в K, имеющая вид B_ε, где $\varepsilon > 0$, такие, что $B_\varepsilon W \subset V - f(S)$, т. е. $yW \cap f(S) = \varnothing$ при $\mathrm{mod}_K(y) \leqslant \varepsilon$. Выберем теперь $m > 0$ и $a \in K$ так, чтобы $0 < \mathrm{mod}_K(a) \leqslant m\varepsilon$. Пусть $v = \sum x_i b_i$ — произвольная отличная от нуля точка в $V' \cap aW$. Подберем h так, чтобы $\sup_i \mathrm{mod}_K(x_i) = \mathrm{mod}_K(x_h)$. Тогда $x_h \neq 0$. Положим $x_i' = x_h^{-1} x_i$, где $1 \leqslant i \leqslant n$, и

$$v' = \sum_1^n x_i' v_i = x_h^{-1} v.$$

Поскольку $(x_1', \ldots, x_n')$ находится в S, имеем $v' \in f(S)$, а так как $v \in aW$, получаем, что $v' \in yW$, где $y = x_h^{-1} a$. По определению W

и ε отсюда следует, что $\mathrm{mod}_K(y) > \varepsilon$ и, следовательно, $\mathrm{mod}_K(x_h) < \varepsilon^{-1}\,\mathrm{mod}_K(a) \leqslant m$. Поэтому $(x_1, \ldots, x_n)$ принадлежит множеству $(B_m)^n$ и v находится в образе этого множества относительно отображения f. Итак, мы показали, что этот образ содержит множество $V' \cap aW$, являющееся окрестностью нуля в V'. Пусть теперь w принадлежит замыканию V' в пространстве V. Применяя только что доказанное к конечномерному подпространству V'', порожденному V' и w, видим, что V' должно быть замкнуто в V''. А так как отсюда вытекает, что $w \in V'$, доказательство теоремы завершено.

Следствие 1. *Каждое конечномерное левое векторное пространство над полем K можно снабдить одной и только одной структурой топологического левого векторного пространства над K.*

Действительно, если V имеет размерность n, то подобную структуру на V можно определить с помощью любого K-линейного биективного отображения K^n на V; единственность немедленно следует из теоремы 3, примененной к пространству V.

Начиная с этого места, мы будем без оговорок предполагать, что каждое такое векторное пространство снабжено структурой, определяемой этим следствием.

Следствие 2. *Если V — локально компактное топологическое левое векторное пространство над полем K, то оно имеет над K конечную размерность d и $\mathrm{mod}_V(a) = \mathrm{mod}_K(a)^d$ для любого $a \in K$.*

Для пространства размерности d последнее утверждение является немедленным следствием теоремы Фубини и того факта, что ввиду следствия 1 каждое такое пространство изоморфно пространству K^d. Предположим теперь лишь, что V локально компактно, и выберем $a \in K$ так, чтобы $0 < \mathrm{mod}_K(a) < 1$. Тогда в силу следствия 2 предл. 2 $\lim a^n = 0$ и потому $\mathrm{mod}_V(a) < 1$. Пусть V' — подпространство в V конечной размерности δ; по теореме 3 оно замкнуто. Положим $V'' = V/V'$. Ввиду леммы 2 получаем

$$\mathrm{mod}_V(a) = \mathrm{mod}_{V'}(a)\,\mathrm{mod}_{V''}(a) = \mathrm{mod}_K(a)^\delta\,\mathrm{mod}_{V''}(a)$$

и, следовательно,

$$\mathrm{mod}_V(a) \leqslant \mathrm{mod}_K(a)^\delta,$$

ибо $\mathrm{mod}_{V''}(a)$ должен быть меньше 1, если $V'' \neq \{0\}$, и равен 1, если $V'' = \{0\}$. Это дает оценку сверху для δ, верную для всех конечномерных подпространств пространства V, следовательно, V само имеет конечную размерность.

Если V — левое векторное пространство над K конечной размерности n, топологизированное так, как было сказано выше, то

из теоремы Фубини немедленно следует, что каждое подпространство размерности $n' < n$ в V имеет меру 0. Пусть теперь A — произвольное K-линейное отображение пространства V в себя; если оно ранга n, то оно является автоморфизмом пространства V также и в топологическом смысле, и мы можем рассмотреть его модуль $\mathrm{mod}_V(A)$. Если же его ранг $n' < n$, то оно отображает V на подмножество меры 0, и мы положим $\mathrm{mod}_V(A)$ равным 0.

Следствие 3. *Пусть A — эндоморфизм левого векторного пространства V конечной размерности над K. Если поле K коммутативно, то* $\mathrm{mod}_V(A) = \mathrm{mod}_K(\det A)$.

Пусть n — размерность пространства V. Если ранг A меньше n, утверждение очевидно. Если нет, то, выбрав в V некоторый базис, отождествим V с пространством K^n. Как хорошо известно, каждый автоморфизм пространства K^n можно записать в виде произведения автоморфизмов следующих трех типов: (a) перестановки координат, (b) отображения вида

$$(x_1, \ldots, x_n) \to (ax_1, x_2, \ldots, x_n),$$

где $a \in K^\times$, (c) отображения вида

$$(x_1, \ldots, x_n) \to \Big(x_1 + \sum_{i=2}^{n} a_i x_i, x_2, \ldots, x_n\Big).$$

Для автоморфизмов типа (a) утверждение очевидно; для автоморфизмов типов (b) и (c) оно получается непосредственным применением теоремы Фубини так же, как и в классическом анализе (где эта теорема доказывается для случая $K = \mathbf{R}$).

Предложение 3. *Функция mod_K индуцирует на группе $K^\times$ открытый гомоморфизм на замкнутую подгруппу Γ группы $\mathbf{R}_+^\times$.*

Обозначим через Γ, Γ' образы групп $K^\times$ и K относительно отображения mod_K. Ясно, что Γ — подгруппа в $\mathbf{R}_+^\times$ и что $\Gamma' = \Gamma \cup \{0\}$. Для каждого $m > 0$ пересечение группы Γ' с замкнутым интервалом $[0, m]$ является образом множества B_m относительно отображения mod_K; в силу предложений 1 и 2 оно компактно и, следовательно, группа Γ' замкнута в $\mathbf{R}_+$, а Γ в $\mathbf{R}_+^\times$. Пусть теперь U — ядро отображения mod_K в $K^\times$, т. е. множество $\{x \in K \mid \mathrm{mod}_K(x) = 1\}$. Обозначим через V произвольную окрестность единицы в $K^\times$ и через V' — ее образ относительно отображения mod_K; чтобы доказать открытость гомоморфизма mod_K из $K^\times$ на Γ, нужно показать, что V' — окрестность единицы в группе Γ. Предположим, что это не так. Тогда существует последовательность (γ_n) в $\Gamma - V'$, такая, что $\lim \gamma_n = 1$. Для каждого n пусть $a_n \in K^\times$ таково, что

$\gamma_n = \mathrm{mod}_K(a_n)$. По предложению 2 последовательность (a_n) имеет по меньшей мере одну предельную точку a; ясно, что $\mathrm{mod}_K(a) = 1$, т. е. $a \in U$. Но UV — окрестность множества U, поэтому существует n, для которого $a_n \in UV$ и, следовательно, $\gamma_n \in V'$. Но это противоречит условию.

Теорема 4. *Существует константа* $A > 0$, *такая, что*

$$\mathrm{mod}_K(x+y) \leqslant A \sup(\mathrm{mod}_K(x), \mathrm{mod}_K(y)) \tag{3}$$

для всех $x \in K$, $y \in K$. *Если неравенство* (3) *выполняется для* $A = 1$, *то образ подгруппы* Γ *в* $K^\times$ *относительно отображения* mod_K *дискретен в* $\mathbf{R}_+^\times$. *Более того, неравенство* (3) *выполняется для*

$$A = \sup_{x \in K,\ \mathrm{mod}_K(x) \leqslant 1} \mathrm{mod}_K(1+x),$$

и это наименьшее значение A, *для которого оно имеет место.*

Определим A последней формулой; ясно, что $1 \leqslant A < +\infty$. Для $x = y = 0$ неравенство (3) очевидно. Поэтому можно считать, поменяв в случае необходимости x и y, что $x \neq 0$ и $\mathrm{mod}_K(y) \leqslant \mathrm{mod}_K(x)$. Положим $z = yx^{-1}$. Тогда $\mathrm{mod}_K(z) \leqslant 1$, $\mathrm{mod}_K(1+z) \leqslant A$ и, следовательно,

$$\mathrm{mod}_K(x+y) = \mathrm{mod}_K(1+z)\,\mathrm{mod}_K(x) \leqslant A\,\mathrm{mod}_K(x).$$

Неравенство (3) доказано. Полагая в формуле (3) $y = 1$ и $x \in B_1$, где B_1 такое же, как и в предложении 2, видим, что выбранное нами значение для A является наименьшим из всех, для которых выполняется (3). Предположим теперь, что $A = 1$. Тогда образ множества $1 + B_1$ относительно отображения mod_K содержится в интервале $[0, 1]$, а так как он в силу предложений 2 и 3 должен содержать окрестность единицы в Γ, подгруппа Γ должна быть дискретной.

Следствие. *Пусть неравенство* (3) *выполняется для* $A = 1$. *Тогда* $\mathrm{mod}_K(x+y) = \mathrm{mod}_K(y)$, *если* $\mathrm{mod}_K(y) < \mathrm{mod}_K(x)$.

Из равенства $(-1)^2 = 1$ вытекает, что $\mathrm{mod}_K(-1) = 1$ и, значит, $\mathrm{mod}_K(-y) = \mathrm{mod}_K(y)$. Так как $x = (x+y) + (-y)$, из наших предположений следует, что

$$\mathrm{mod}_K(x) \leqslant \sup(\mathrm{mod}_K(x+y), \mathrm{mod}_K(y)) \leqslant \mathrm{mod}_K(x),$$

чем наше утверждение и доказано.

Определение 1. *Неравенство* (3) *с* $A = 1$ *называется ультраметрическим неравенством. Если оно выполняется, то говорят, что отображение* mod_K *и само поле* K *ультраметричны.*

§ 3. КЛАССИФИКАЦИЯ ЛОКАЛЬНО КОМПАКТНЫХ ПОЛЕЙ

Нам понадобится следующая элементарная лемма:

Лемма 3. *Пусть F — функция на множестве натуральных чисел* $\mathbf{N}$ *со значениями в* $\mathbf{R}_+$. *Предположим, что для всех m, n имеет место равенство $F(mn) = F(m)\,F(n)$ и что существует $A > 0$, для которого*

$$F(m+n) \leqslant A \sup(F(m),\ F(n))$$

для всех m, n. Тогда или $F(m) \leqslant 1$ для всех m, или для всех m выполняется равенство $F(m) = m^{\lambda}$, где $\lambda > 0$.

Из первого предположения относительно F следует, для $m = 0$, что если функция F не равна тождественно 1, то $F(0) = 0$, а для $m = 1$, что $F(1) = 1$, если F не равна тождественно 0. Из него следует также, что $F(m^k) = F(m)^k$ для всех целых $k \geqslant 1$. Оставляя в стороне тривиальные случаи, когда F — константа, равная 0 или 1, мы можем считать, что $F(0) = 0$ и $F(m^k) = F(m)^k$ для всех целых $k \geqslant 0$. Положим $f(m) = \sup(0, \log F(m))$; подразумевается, что $f(m) = 0$ при $F(m) = 0$. Наша лемма равносильна теперь утверждению, что $f(m) = \lambda \log m$ для всех $m \geqslant 2$, где $\lambda \geqslant 0$ — некоторая константа. Пусть $a = \sup(0, \log A)$. Тогда для всех m, n, k имеем

$$f(m^k) = kf(m);\ f(mn) \leqslant f(m) + f(n),$$
$$f(m+n) \leqslant a + \sup(f(m),\ f(n)).$$

Из последнего соотношения индукцией по r получаем

$$f\Big(\sum_{i=0}^{r} m_i\Big) \leqslant ra + \sup_i (f(m_i)). \tag{4}$$

Если m, n — целые числа $\geqslant 2$, то m можно представить в форме

$$m = \sum_{i=0}^{r} e_i n^i,$$

где $n^r \leqslant m < n^{r+1}$ и $0 \leqslant e_i < n$, $0 \leqslant i \leqslant r$. Положим

$$b = \sup(f(0),\ f(1),\ \ldots,\ f(n-1)).$$

Тогда для каждого i

$$f(e_i n^i) \leqslant b + if(n)$$

и, следовательно, ввиду (4)

$$f(m) \leqslant ra + b + rf(n).$$

Поскольку $n^r \leqslant m$, т. е. $r \log n \leqslant \log m$, отсюда вытекает, что

$$\frac{f(m)}{\log m} \leqslant \frac{a+f(n)}{\log n} + \frac{b}{\log m}.$$

Заменим в этом неравенстве m на m^k; это не изменит левой части. При $k \to +\infty$ получаем

$$\frac{f(m)}{\log m} \leqslant \frac{a+f(n)}{\log n}.$$

Заменим теперь m на n^k. Устремляя k к $+\infty$, получаем

$$\frac{f(m)}{\log m} \leqslant \frac{f(n)}{\log n}.$$

Переставляя m и n, видим, что $f(m)/\log m$ есть константа при $m \geqslant 2$. Как было отмечено выше, отсюда следует утверждение леммы.

Рассмотрим теперь снова недискретное локально компактное поле K. Для большей ясности в оставшейся части этого параграфа единичный элемент поля K мы будем обозначать через 1_K (а не через 1). Простое кольцо в K состоит из элементов вида $m \cdot 1_K$, где $m \in \mathbf{Z}$, и если K — поле характеристики $p > 1$, то $p \cdot 1_K = 0$. Для $m \in \mathbf{N}$ положим $F(m) = \mathrm{mod}_K (m \cdot 1_K)$. Тогда для всех $m \in \mathbf{Z}$ и $x \in K$ имеем $\mathrm{mod}_K (mx) = F(|m|) \mathrm{mod}_K (x)$.

Лемма 4. *Предположим, что функция F ограничена, т. е. что отображение mod_K ограничено на простом кольце в K. Тогда $F \leqslant 1$ и отображение mod_K ультраметрично на K.*

Так как $F(mn) = F(m) F(n)$, первое утверждение очевидно. Пусть A такое же, как и в теореме 4 § 2, $n \geqslant 1$, $N = 2^n$ и $x_1, \ldots, x_N$ — какие-нибудь N элементов поля K. Индукцией по n получаем неравенство

$$\mathrm{mod}_K \Big(\sum_{i=1}^{N} x_i \Big) \leqslant A^n \sup_i (\mathrm{mod}_K (x_i)).$$

Заменяя некоторые из x_i нулями, видим, что это неравенство справедливо и при $N \leqslant 2^n$. Применяя его к соотношению

$$(x+y)^{2^n} = \sum_{i=0}^{2^n} \binom{2^n}{i} x^i y^{2^n - i},$$

находим

$$\mathrm{mod}_K (x+y)^{2^n} \leqslant A^{n+1} \sup_i \left(F\left(\binom{2^n}{i} \right) \mathrm{mod}_K (x)^i \, \mathrm{mod}_K (y)^{2^n - i} \right).$$

Предположим для определенности, что $\mathrm{mod}_K(y) \leqslant \mathrm{mod}_K(x)$. Поскольку $F \leqslant 1$, приходим к неравенству

$$\mathrm{mod}_K(x+y)^{2^n} \leqslant A^{n+1}\,\mathrm{mod}_K(x)^{2^n}.$$

Оно верно для всех $n \geqslant 1$; при $n \to +\infty$ получаем

$$\mathrm{mod}_K(x+y) \leqslant \mathrm{mod}_K(x),$$

т. е. ультраметрическое неравенство.

Напомним теперь определение обычных нормирований поля рациональных чисел $\mathbf{Q}$. Пусть сначала p — простое число. Каждое $x \in \mathbf{Q}^\times$ можно одним и только одним способом записать в виде $p^n a/b$, где n, a, b —целые числа, причем $b > 0$, а a и b взаимно просты друг с другом и с p. Положим $|x|_p = p^{-n}$, а также $|0|_p = 0$. Определенная таким образом на $\mathbf{Q}$ функция $x \to |x|_p$ называется *p-адическим нормированием* поля $\mathbf{Q}$. Оно, очевидно, удовлетворяет ультраметрическому неравенству и задает на $\mathbf{Q}$ некоторую топологию, а именно топологию, определяемую расстоянием

$$\delta(x, y) = |x - y|_p.$$

Пополнение поля $\mathbf{Q}$ по этой метрике называется *полем p-адических чисел*. Это поле обозначается через $\mathbf{Q}_p$. Замыкание множества $\mathbf{Z}$ в этом поле называется *кольцом p-адических целых чисел* и обозначается через $\mathbf{Z}_p$. Ясно, что p-адическое нормирование поля $\mathbf{Q}$ продолжается по непрерывности на $\mathbf{Q}_p$ и остается там ультраметричным; это продолжение обозначается также через $|x|_p$. Легко видеть, что $\mathbf{Z}_p$ компактно (по той причине, что $\mathbf{Z}_p$ есть, так сказать, «проективный предел» конечных групп $\mathbf{Z}/p^n\mathbf{Z}$ при $n \to +\infty$). Поскольку $\mathbf{Z}_p$ — окрестность нуля в $\mathbf{Q}_p$, поле $\mathbf{Q}_p$ локально компактно и, очевидно, недискретно.

В тех случаях, когда это будет удобно, мы будем писать $|x|_\infty$ вместо $|x|$ для обозначения «обычного» абсолютного значения в полях $\mathbf{Q}$ и $\mathbf{R}$. А так как $\mathbf{R}$ — не что иное, как пополнение поля $\mathbf{Q}$ по метрике $|x - y|_\infty$, мы будем иногда писать $\mathbf{Q}_\infty$ вместо $\mathbf{R}$. Таким образом, символом $\mathbf{Q}_v$, где v может быть равно ∞ или простому числу, обозначается любое из пополнений $\mathbf{Q}_\infty = \mathbf{R}$ или $\mathbf{Q}_p$ поля $\mathbf{Q}$.

Теорема 5. *Пусть K — недискретное локально компактное поле; положим $F(m) = \mathrm{mod}_K(m \cdot 1_K)$, $m \in \mathbf{N}$. Тогда либо* (a) *K — поле характеристики $p > 1$ и $F(m) = 0$ при $m \equiv 0 \pmod p$ и $F(m) = 1$ при $(m, p) = 1$, либо* (b) *K — алгебра с делением конечной размерности δ над полем $\mathbf{Q}_v$ и $F(m) = |m|_v^\delta$.*

В силу предложения 1 и теоремы 4 § 2 F удовлетворяет условиям леммы 3 и, следовательно, либо имеет вид $m \to m^\lambda$, где $\lambda > 0$,

либо всюду меньше 1. Предположим, что имеет место последнее; это означает, что последовательность $(m \cdot 1_K)$, $m \in \mathbf{N}$, содержится в B_1, где B_1 — множество из предложения 2 § 2; так как множество B_1 компактно, оно должно иметь по крайней мере одну предельную точку, скажем a. Но тогда, согласно следствию 1 предл. 2, для каждого $\varepsilon > 0$ существует бесконечно много чисел $m \in \mathbf{N}$, таких, что $\mathrm{mod}_K (m \cdot 1_K - a) \leqslant \varepsilon$. Пусть m, m' — два таких числа, $m < m'$. Поскольку из неравенства $F \leqslant 1$ следует, по лемме 4, что отображение mod_K ультраметрично, то мы имеем

$$\mathrm{mod}_K (m' \cdot 1_K - m \cdot 1_K) \leqslant \varepsilon,$$

т. е. $F(m' - m) \leqslant \varepsilon$. Отсюда видно, в частности, что существуют целые числа $n \geqslant 1$, для которых $F(n) < 1$.

Пусть p — наименьшее из таких чисел. Поскольку $F(mn) = F(m) F(n)$, ясно, что p должно быть простым. Для каждого $x \in \mathbf{N}$ имеем $F(px) < 1$ и, значит, $F(1 + px) = 1$ по следствию теор. 4 § 2. Для любого целого $m \geqslant 1$, взаимно простого с p, имеем $m^{p-1} \equiv 1\ (p)$, следовательно, по только что доказанному $F(m^{p-1}) = 1$, откуда $F(m) = 1$. Если K — поле характеристики $p' > 1$, то $F(p') = 0$, так что p' не может быть отлично от p, и функция F такова, как утверждалось в (а). Если K — поле характеристики 0, то $F(p)$ не может равняться нулю и можно считать, что $F(p) = p^{\lambda}$, где $\lambda > 0$. Поэтому $F(m) = |m|_p^{\lambda}$ для всех m, что сразу видно, если записать m в виде $m = p^n m'$, где $(m', p) = 1$. Таким образом, если K — поле характеристики 0, то функция F должна иметь вид $m \to |m|_v^{\lambda}$, где $\lambda > 0$. Отображение $n \to n \cdot 1_K$ кольца $\mathbf{Z}$ в простое кольцо $\mathbf{Z} \cdot 1_K$ поля K является в этом случае алгебраическим (но не обязательно топологическим) изоморфизмом, который можно продолжить до изоморфизма поля $\mathbf{Q}$ на простое подполе в K. Мы будем для простоты отождествлять последнее с полем $\mathbf{Q}$ при помощи этого изоморфизма. Из установленных свойств функции F немедленно следует, что отображение mod_K индуцирует на поле $\mathbf{Q}$ функцию $x \to |x|_v^{\lambda}$. Следовательно, структура топологической группы, индуцированная полем K на поле $\mathbf{Q}$, определяется метрикой $|x - y|_v$. А так как замыкание поля $\mathbf{Q}$ в K локально компактно и, следовательно, полно в этой структуре, мы видим, что оно изоморфно пополнению $\mathbf{Q}_v$ поля $\mathbf{Q}$ по нормированию v. Поскольку простое кольцо, а значит, и простое поле содержатся, очевидно, в центре поля K, то же самое справедливо и для поля $\mathbf{Q}_v$. Поле K можно рассматривать поэтому как векторное пространство над $\mathbf{Q}_v$, имеющее ввиду следствия 2 теор. 3 § 2 конечную размерность δ. Для всех $x \in \mathbf{Q}_v$ имеем $\mathrm{mod}_K (x) = \mathrm{mod}_{\mathbf{Q}_v} (x)^{\delta}$. Чтобы завершить

доказательство, остается только показать, что в случае $v = \infty$ $\mathrm{mod}_{\mathbf{R}}(m) = m$ для $m \in \mathbf{N}$, но это очевидно, а в случае $v = p$ $\mathrm{mod}_{\mathbf{Q}_p}(p) = p^{-1}$. Это следует немедленно из того факта, что кольцо $\mathbf{Z}_p$ есть компактная окрестность нуля в $\mathbf{Q}_p$, а его образ $p \cdot \mathbf{Z}_p$ относительно отображения $x \to px$ является компактной подгруппой в $\mathbf{Z}_p$ индекса p, так что его мера равна $p^{-1}\alpha(\mathbf{Z}_p)$ для любой хааровской меры α на $\mathbf{Q}_p$. Нам будет удобно сформулировать отдельно только что доказанное утверждение.

Следствие. *В случае* (b) *теоремы* 5 $\mathrm{mod}_K(x) = |x|_v^{\delta}$ *для* $x \in \mathbf{Q}_v$.

Определение 2. *Недискретное локально компактное поле* K *называется* p*-полем, если* p *— простое число и* $\mathrm{mod}_K(p \cdot 1_K) < 1$, *и* $\mathbf{R}$*-полем, если оно является алгеброй над полем* $\mathbf{R}$.

В силу лемм 3 и 4 § 2, если K есть p-поле, то образ Γ группы $K^\times$ относительно mod_K дискретен, поэтому такое поле не может быть связным; это показывает, что топологическое поле является $\mathbf{R}$-полем в том и только том случае, когда оно связно и локально компактно. Как хорошо известно, не существует других $\mathbf{R}$-полей, кроме $\mathbf{R}$, $\mathbf{C}$ и поля $\mathbf{H}$ «обычных» (или «классических») кватернионов; доказательство этого факта содержится в гл.I X-4.

§ 4. СТРУКТУРА p-ПОЛЕЙ

В этом параграфе p будет простым числом, а K — некоторым p-полем с единичным элементом 1.

Теорема 6. *Пусть* K *— некоторое* p*-поле, а* R, $R^\times$ *и* P *— подмножества в* K, *определяемые соответственно формулами*

$$R = \{x \in K \mid \mathrm{mod}_K(x) \leqslant 1\},$$
$$R^\times = \{x \in K \mid \mathrm{mod}_K(x) = 1\},$$
$$P = \{x \in K \mid \mathrm{mod}_K(x) < 1\}.$$

Тогда поле K *ультраметрично;* R *— единственное максимальное компактное подкольцо в* K; $R^\times$ *— группа обратимых элементов кольца* R; P *— единственный максимальный левый, правый или двусторонний идеал кольца* R. *Существует элемент* $\pi \in P$, *такой, что* $P = \pi R = R\pi$. *Более того, поле вычетов* $k = R/P$ *есть поле характеристики* p, *и если* q *— число его элементов, то образ* Γ *группы* $K^\times$ *относительно отображения* mod_K *является подгруппой в* $\mathbf{R}_+^\times$, *порожденной* q, *и* $\mathrm{mod}_K(\pi) = q^{-1}$.

Множество R совпадает с введенным ранее множеством B_1; оно компактно, как и $R^\times$. По теореме 5 § 3 $\mathrm{mod}_K \leqslant 1$ на простом кольце поля K; следовательно, по лемме 4 § 3 поле K ультраметрично. В силу теоремы 4 § 2 последнее утверждение эквивалентно равенству $R + R = R$, а так как R, очевидно, замкнуто относительно умножения, мы видим, что R — кольцо. Ясно, что каждое относительно компактное замкнутое по умножению множество содержится в R; следовательно, R — максимальное компактное подкольцо поля K. Обратимые элементы в R — это как раз элементы из $R^\times$. По теореме 4 § 2 Γ — дискретная подгруппа в $\mathbf{R}_+^\times$; пусть γ — наибольший из меньших 1 элементов подгруппы Γ, и пусть $\pi \in K^\times$ таково, что $\mathrm{mod}_K(\pi) = \gamma$. Ясно, что γ порождает Γ; следовательно, для каждого $x \in K^\times$ существует одно и только одно целое n, для которого $\mathrm{mod}_K(x) = \gamma^n$, а тогда элементы $x\pi^{-n}$ и $\pi^{-n}x$ лежат в $R^\times$. Ясно, что $P = \pi R = R\pi$, откуда следует, что P компактно. Поскольку $R - P = R^\times$, P обладает свойствами максимальности, указанными в формулировке теоремы. Так как R — окрестность нуля и $R = R + R$, то R — открытое множество, как и P; а так как R компактно, поле $k = R/P$ конечно. Поскольку $p \cdot 1 \in P$, образ $p \cdot 1$ в поле k есть 0, так что это поле имеет характеристику p. Если в нем q элементов, то индекс $P = \pi R$ в аддитивной группе кольца R равен q. Следовательно, если α — мера Хаара поля K, то $\alpha(R) = q\alpha(\pi R)$ и потому $\mathrm{mod}_K(\pi) = q^{-1}$. Этим доказательство завершено.

Определение 3. *В обозначениях теоремы* 6 *будем называть* q *модулем поля* K, *а любой элемент* π *из* $K^\times$, *для которого* $P = \pi R = R\pi$,— *простым элементом поля* K. *Для каждого* $x \in K^\times$ *будем обозначать через* $\mathrm{ord}_K(x)$ *такое целое число, что* $\mathrm{mod}_K(x) = q^{-\mathrm{ord}_K(x)}$. *Для каждого* $n \in \mathbf{Z}$ *будем писать* $P^n = \pi^n R = R\pi^n$.

Мы будем писать $\mathrm{ord}(x)$ вместо $\mathrm{ord}_K(x)$, если это не может привести к недоразумению. Будем считать также, что $\mathrm{ord}(0) = +\infty$; P^n будет тогда множеством элементов поля K, для которых $\mathrm{ord}(x) \geqslant n$. Пользуясь этими обозначениями, мы можем теперь сформулировать ряд следствий из теоремы 6.

Следствие 1. *Пусть* $(x_0, x_1, \ldots)$ — *произвольная, сходящаяся к нулю последовательность в поле* K. *Тогда ряд* $\sum_0^{+\infty} x_i$ *безусловно сходится в* K.

Для каждого $n \in \mathbf{N}$ положим

$$\varepsilon_n = \sup_{i>n} \mathrm{mod}_K(x_i).$$

Наше предположение означает, что $\lim \varepsilon_n = 0$. Пусть теперь S, S' — две конечные суммы членов ряда $\Sigma\, x_i$, содержащие каждая члены x_0, x_1, . . ., x_n и, возможно, другие члены. Ультраметрическое неравенство дает $\mathrm{mod}_K (S - S') \leqslant \varepsilon_n$. Отсюда немедленно следует требуемое утверждение («фильтр» конечных сумм ряда $\Sigma\, x_i$ является «фильтром Коши» относительно метрики $\mathrm{mod}_K (x—y)$).

Следствие 2. *Пусть ξ — некоторый отличный от нуля элемент множества P, $n = \mathrm{ord}\,(\xi)$ и A — полное множество представителей классов смежности по P^n в R. Тогда для всех $\nu \in \mathbf{Z}$ каждый элемент $x \in P^{n\nu}$ можно одним и только одним способом представить в виде*

$$x = \sum_{i=\nu}^{+\infty} a_i \xi^i,$$

где $a_i \in A$ для всех $i \geqslant \nu$.

Записывая x в виде $x = x'\xi^\nu$, где $x' \in R$, видим, что достаточно рассмотреть случай $\nu = 0$. В этом случае, используя индукцию по N, сразу видим, что можно одним и только одним способом определить элементы $a_i \in A$, удовлетворяющие условию

$$x \equiv \sum_{i=0}^{N} a_i \xi^i \ (P^{n(N+1)})$$

($N = 0, 1, \ldots$). Это эквивалентно тому, что утверждается в нашем следствии.

Следствие 3. *Каждый автоморфизм поля K (как топологического поля) отображает R на R, P на P и имеет модуль 1 как автоморфизм аддитивной группы поля K.*

Следствие 4. *Для всех $a \in K^\times$ автоморфизмы $x \to ax$ и $x \to xa$ аддитивной группы поля K имеют одинаковый модуль.*

Это сразу вытекает из следствия 3, примененного к автоморфизму $x \to a^{-1}xa$. Поскольку для поля $\mathbf{H}$ «обычных» кватернионов аналогичный факт легко проверяется непосредственно, это следствие выполняется для всех локально компактных полей.

Следствие 5. *Пусть K — коммутативное p-поле, K' — алгебра с делением над K. Тогда K' есть p-поле; каждый автоморфизм (в алгебраическом смысле) алгебры K' над K является топологическим автоморфизмом, и если R и R' — максимальные компактные подкольца полей K и K', а P и P' — максимальные идеалы колец R, R', то $R = K \cap R'$ и $P = K \cap P'$.*

Рассматривая K' как конечномерное векторное пространство над K, наделим его «естественной топологией» согласно следствию 1 теор. 3 § 2. Из единственности топологии следует, что она инвариантна относительно всех K-линейных отображений алгебры K' на себя, и в частности относительно всех автоморфизмов K' над K. Отождествляя, как обычно, K с подполем $K \cdot 1_{K'}$ алгебры K', видим, что K' — недискретная алгебра. Остальные утверждения очевидны.

Следствие 6. *Пусть в условиях и обозначениях следствия* 5 q *и* q' *— модули полей* K *и* K' *соответственно,* π *— простой элемент поля* K *и* $e = \mathrm{ord}_{K'}(\pi)$. *Тогда* $q' = q^f$, *где* f *— целое число* $\geqslant 1$ *и размерность поля* K' *над* K *равна* ef.

Положим $k = R/P$ и $k' = R'/P'$; ввиду последнего утверждения следствия 5 можно отождествить поле k с образом кольца R в $k' = R'/P'$. Если f — степень поля k' над k, то $q' = q^f$. Применяя теперь следствие 2 теор. 3 § 2 к $\mathrm{mod}_K(\pi)$ и $\mathrm{mod}_{K'}(\pi)$, получаем сформулированный выше результат.

Последнее следствие показывает, в частности, что число $\mathrm{ord}_{K'}(\pi)$ не меньше 1 и не зависит от выбора простого элемента π в поле K. Этим оправдано следующее определение.

Определение 4. *В условиях и обозначениях следствий* 5 *и* 6 *теор.* 6 *число* e *называется порядком ветвления поля* K' *над* K, *а число* f *— модулярной степенью поля* K' *над* K. *Говорят, что* K' *неразветвлено над* K, *если* $e = 1$, *и вполне разветвлено, если* $f = 1$.

Предложение 4. *Пусть* K *— коммутативное* p*-поле;* K' *— вполне разветвленная алгебра с делением конечной размерности над* K; R, R' *— максимальные компактные подкольца полей* K *и* K' *соответственно;* π' *— простой элемент поля* K'. *Тогда* $K' = K(\pi')$, $R' = R[\pi']$ *и алгебра* K' *коммутативна.*

Пусть P, P' — максимальные идеалы колец R и R' соответственно, A — полное множество представителей классов смежности кольца R по идеалу P. Поскольку поле K' вполне разветвлено над K, следствия 5 и 6 теор. 6 сразу показывают, что A является также полным множеством представителей классов смежности кольца R' по идеалу P'. Применяя следствие 2 теор. 6 к K', R' и P', а также к A и $\xi = \pi'$, получаем, что элементы кольца R', имеющие вид $\sum_{i=0}^{e-1} a_i \pi'^i$, где $a_i \in A$ для $0 \leqslant i \leqslant e-1$, образуют полное множество A' представителей классов смежности по идеалу P'^e. Выберем теперь какой-нибудь простой элемент π поля K и положим $e =$

$= \operatorname{ord}_{K'}(\pi)$; e является порядком ветвления поля K' над K и, следовательно, размерностью поля K' над K (в силу следствия 6 теор. 6). Применяя снова следствие 2 теор. 6 к K', R', P'^e, A' и $\xi = \pi$, видим, что каждый элемент идеала $P'^{e\nu}$ можно записать одним и только одним способом в виде $\sum_{j=\nu}^{+\infty} a'_j \pi^j$, где $a'_j \in A'$ для всех $j \geqslant \nu$. Так как K содержится в центре алгебры K', то π' коммутирует с π, откуда в силу определения множества A' следует, что каждый рассматриваемый элемент записывается в виде

$$\sum_{i=0}^{e-1} \Big(\sum_{j=\nu}^{+\infty} a_{ij}\pi^j\Big)\pi'^i,$$

где $a_{ij} \in A$ для $0 \leqslant i \leqslant e-1$, $j \geqslant \nu$. Это равносильно, ввиду следствия 2 теор. 6, представлению в виде $\sum_{i=0}^{e-1} \alpha_i \pi'^i$, где $\alpha_i \in P^\nu$ для $0 \leqslant i \leqslant e-1$. Отсюда видно, что $K' = K(\pi')$; полагая $\nu = 0$, находим, что $R' = R[\pi']$. Поскольку K содержится в центре алгебры K', то π' коммутирует со всеми элементами поля K; следовательно, поле K' коммутативно.

Следствие 1. *Пусть K — коммутативное p-поле характеристики p. Обозначим через K^p его образ относительно эндоморфизма $x \to x^p$, и пусть π — какой-нибудь простой элемент в K. Тогда K — вполне разветвленное расширение степени p поля K^p и $K = K^p(\pi)$.*

Пусть $K' = K^p$; отображение $x \to x^p$ есть изоморфизм поля K на K', который можно использовать для перенесения топологии поля K на поле K'. Поэтому K можно рассматривать как топологическое векторное пространство над K', имеющее в силу следствия 2 теор. 3 § 2 конечную размерность. Это показывает, что K имеет конечную степень над K'. А так как поля K и K' изоморфны, они имеют одинаковый модуль, и модулярная степень поля K над K' равна 1. Это дает с учетом предложения 4 равенство $K = K'(\pi)$. Поскольку $\pi^p \in K'$, степень поля K над K' должна равняться p или 1. Но так как $\operatorname{ord}_K(\pi) = 1$, то π не принадлежит K^p и, значит, $K \neq K'$. Таким образом, поле K имеет над полем K' степень p.

Следствие 2. *Пусть K — то же, что и в следствии 1, $\overline{K}$ — его алгебраическое замыкание. Тогда для каждого $n \geqslant 0$ поле $\overline{K}$ содержит одно и только одно чисто несепарабельное расширение степени p^n поля K; оно является образом $K^{p^{-n}}$ поля относительно автоморфизма $x \to x^{p^{-n}}$.*

Из следствия 1 немедленно вытекает, что поле $K^{p^{-1}}$ имеет над K степень p; индукцией по n получаем, что степень поля $K^{p^{-n}}$ над K равна p^n. С другой стороны, хорошо известен и легко доказывается тот факт, что если K' — чисто несепарабельное расширение степени $\leqslant p^n$ поля K, то оно содержится в поле $K^{p^{-n}}$. Отсюда сразу следует наше утверждение.

Теорема 7. *Пусть K — некоторое p-поле, q — его модуль, R — максимальное компактное подкольцо и P — максимальный идеал в R. Тогда группа $K^\times$ имеет по меньшей мере одну подгруппу порядка $q-1$ и каждая такая подгруппа циклична. Если $M^\times$ — такая подгруппа, то $M = M^\times \cup \{0\}$ является полным множеством представителей классов смежности кольца R по идеалу P и существует такой простой элемент π поля K, что $\pi M^\times = M^\times \pi$. Если поле K коммутативно, то существует только одна подобная группа $M^\times$, а именно группа корней из единицы в K степени, взаимно простой с p.*

Конструкция группы $M^\times$ основывается на следующей лемме.

Лемма 5. *Для всех $n \geqslant 0$ имеет место включение*

$$(1+P)^{p^n} \subset 1+P^{n+1}.$$

Это утверждение непосредственно проверяется индукцией по n. Его можно переформулировать еще так: $x^{p^n} \equiv 1\ (P^{n+1})$, если $x \equiv 1\ (P)$.

Обозначим теперь через ρ канонический гомоморфизм кольца R на поле $k = R/P$. По теореме 2 § 1 группа $k^\times$ циклична и ее порядок равен $q-1$. В частности, для всех $x \in R^\times$ имеем $\rho(x)^{q-1} = 1$, т. е. $x^{q-1} \equiv 1\ (P)$. Если $q = p^f$, то, согласно лемме 5, $x^{(q-1)q^n} \equiv 1\ (P^{fn+1})$, что можно также записать в виде

$$x^{q^{n+1}} \equiv x^{q^n} \quad (P^{fn+1}).$$

Снова, применяя следствие 1 теор. к ряду

$$x + (x^q - x) + (x^{q^2} - x^q) + \ldots,$$

видим, что он сходится при всех $x \in R^\times$, так что можно написать

$$\omega(x) = \lim_{n \to +\infty} x^{q^n}$$

для $x \in R^\times$ и, конечно, для $x \in P$, а значит, и для всех $x \in R$. Очевидно, $\omega(xy) = \omega(x)\,\omega(y)$, если $xy = yx$; в частности, $\omega(x^\nu) = \omega(x)^\nu$ для всех $x \in R^\times$, $\nu \in \mathbf{Z}$. Как видно из написанного выше

ряда для $\omega(x)$, $\omega(x) \equiv x$ (P) для всех $x \in R$. Очевидно, $\omega(x) = 0$ для $x \in P$, и лемма 5 показывает, что $\omega(x) = 1$ для $x \in 1 + P$. Следовательно, $\omega^{-1}(0) = P$ и $\omega^{-1}(1) = 1 + P$. А так как $x^{q-1} \in 1 + P$ для всех $x \in R^\times$, то $\omega(x)^{q-1} = 1$ при $x \in R^\times$.

Выберем в группе $R^\times$ представитель x_1 образующей циклической группы $k^\times = (R/P)^\times$ и положим $\mu_1 = \omega(x_1)$. Равенство $\mu_1^n = 1$ имеет место для всех $n \in \mathbf{Z}$ в том и только в том случае, когда $\omega(x_1^n) = 1$; а так как последнее условие эквивалентно соотношению $x_1^n \equiv 1$ (P), а значит, ввиду выбора x_1, соотношению $n \equiv 0$ $(q-1)$, это показывает, что μ_1 порождает циклическую подгруппу в $R^\times$ порядка $q-1$. Обратно, пусть Γ — произвольная конечная подгруппа группы $K^\times$, порядок которой взаимно прост с p; ясно, что она является подгруппой группы $R^\times$. Образ числа q в мультипликативной группе $(\mathbf{Z}/n\mathbf{Z})^\times$ целых чисел, взаимно простых с n и взятых по модулю n, должен иметь конечный порядок N; поэтому $q^N \equiv 1$ (n). Поскольку $z^n = 1$ при всех $z \in \Gamma$, мы получаем, что $z^{q^{N\nu}} = z$ для всех $\nu \geqslant 0$ и всех $z \in \Gamma$, откуда $\omega(z) = z$. Таким образом, $z \equiv 1$ (P) влечет $z = 1$. Полученный результат показывает, что ρ индуцирует инъективное отображение группы Γ в $k^\times = (R/P)^\times$; отсюда следует, что группа Γ циклична, что ее порядок делит $q-1$ и что, если он равен $q-1$, то множество $\Gamma \cup \{0\}$ образует полную систему представителей поля R/P в R. В частности, для коммутативного поля K получаем, что отображение ω индуцирует на $R^\times$ морфизм группы $R^\times$ на группу $M^\times$ корней из единицы в K степени $q-1$, отображает кольцо R на множество $M = M^\times \cup \{0\}$ и определяет биекцию поля R/P на M. Кроме того, каждая подгруппа Γ группы $K^\times$, порядок которой взаимно прост с p, содержится в $M^\times$; в частности, $M^\times$ содержит все корни из единицы в K порядка взаимно простого с p. Что касается существования простого элемента поля K, удовлетворяющего требованиям нашей теоремы, то оно очевидно, если поле K коммутативно. Предположим, что это не так, и возьмем какой-нибудь простой элемент π поля K. Для каждого $a \in K^\times$ отображение $x \to axa^{-1}$ есть автоморфизм поля K и, значит, согласно следствию 3 теор. 6, отображает R на R, P на P, определяя тем самым автоморфизм $\lambda(a)$ поля $k = R/P$. Отображение $a \to \lambda(a)$ есть, очевидно, гомоморфизм группы $K^\times$ в группу автоморфизмов поля k. Для $a \in R^\times$ $\lambda(a)$ есть отображение $\xi \to \rho(a)\,\xi\rho(a)^{-1}$, которое тождественно, ибо поле k коммутативно. Поэтому если a — элемент из $K^\times$ с $\operatorname{ord}(a) = n$, то $\lambda(a) = \lambda(\pi)^n$. В силу следствия 2 теор. 2 § 1, примененного к полю k и его простому подполю, $\lambda(\pi)$ имеет вид $\xi \to \xi^{p^r}$; это означает, что для всех $x \in R$

$$\pi x \pi^{-1} \equiv x^{p^r} \ (P),$$

или, что то же самое,

$$\pi x \equiv x^{p^r}\pi \ (P^2).$$

Выберем теперь $M^\times$ так же, как и выше, и положим

$$\pi' = -\sum_{\mu\in M^\times} \mu^{p^r}\pi\mu^{-1}.$$

Как следует из написанных выше сравнений, каждое из $q-1$ слагаемых суммы в правой части сравнимо с π по модулю P^2. Поскольку $q\cdot 1 \in P$, получаем

$$\pi' \equiv (1-q)\,\pi \equiv \pi \ (P^2),$$

откуда следует, что π' — простой элемент поля K. В то же время из определения π' видно, что

$$\pi'\mu = \mu^{p^r}\pi'$$

для всех $\mu \in M^\times$ и, следовательно, $\pi' M^\times = M^\times \pi'$, чем и завершается доказательство. Аналогичными рассуждениями можно доказать, что если $M^\times$ и $N^\times$ — две подгруппы порядка $q-1$ группы $K^\times$, то существует простой элемент поля π, такой, что $\pi M^\times = N^\times \pi$.

Следствие 1. *Если K и M таковы, как в теореме 7, и K — поле характеристики p, то M — подполе поля K. Если при этом поле K коммутативно, то M является алгебраическим замыканием простого поля в K.*

Пусть k_0 — простое поле в K и μ — образующая группы $M^\times$. Тогда $k_0(\mu)$ есть коммутативное поле характеристики p, в котором уравнение $X^q - X = 0$ имеет q корней, являющихся элементами группы M, откуда следует в силу теоремы 2 § 1, что M — поле. Если K коммутативно, то каждый отличный от нуля элемент алгебраического замыкания поля k_0 в K является корнем из единицы степени, взаимно простой с p (снова по теореме 2 § 1), и, значит, должен лежать в M (теорема 7).

Следствие 2. *Пусть K — коммутативное p-поле, q — его модуль, K' — расширение конечной степени поля K, порожденное корнями из единицы степени, взаимно простой с p. Тогда K' неразветвлено и циклично над K, а его группа Галуа над K порождена автоморфизмом φ, индуцирующим перестановку $\mu \to \mu^q$ на группе корней из единицы степени, взаимно простой с p.*

Из следствия 5 теор. 6 вытекает, что K' есть p-поле. Пусть $R, P, q, k, \rho, M^\times$ таковы, как в теореме 7 и ее доказательстве, а $R', P', q', k', \rho', M'^\times$ — аналогичные объекты для поля K'. По теореме 7 K' порождается над K множеством $M'^\times$, т. е. корнями урав-

нения $X^{q'-1} = 1$; поэтому оно есть расширение Галуа поля K, а его автоморфизмы над K однозначно определяются теми перестановками, которые они индуцируют в множестве $M'^{\times}$. По следствию 5 теор. 6 $R = R' \cap K$, $P = P' \cap K$, и, следовательно, мы можем отождествить k с подполем поля k', причем ρ будет отображением, индуцируемым морфизмом ρ' на R. Пусть α — автоморфизм поля K' над K. Он отображает R' на R', P' на P' и оставляет на месте каждый элемент из R; следовательно, он определяет автоморфизм $\lambda(\alpha)$ поля k' над k. При этом λ, т. е. отображение $\alpha \to \lambda(\alpha)$, является морфизмом группы Галуа поля K' над K в группу Галуа поля k' над k. По следствию 2 теор. 2 § 1 $\lambda(\alpha)$ должно иметь вид $\xi \to \xi^{q^s}$. Отсюда получаем, что для всех $\mu \in M'^{\times}$

$$\rho'(\alpha(\mu)) = \rho'(\mu)^{q^s} = \rho'(\mu^{q^s}).$$

По теореме 7 ρ' индуцирует на $M'^{\times}$ изоморфизм группы $M'^{\times}$ на $k'^{\times}$; поэтому $\alpha(\mu) = \mu^{q^s}$. В частности, если $s = 0$, т. е. если $\lambda(\alpha)$ — тождественное отображение, то отображение α также тождественно; это показывает, что λ инъективно; поэтому если n — степень поля K' над K и f — степень k' над k, то $n \leqslant f$. А поскольку $q' = q^f$, из следствия 6 теор. 6 вытекает, что поле K' неразветвлено над K и $n = f$. Таким образом, λ является изоморфизмом группы Галуа поля K' над K на группу Галуа поля k' над k, чем ввиду следствия 2 теор. 2 § 1 и завершается наше доказательство.

Следствие 3. *Пусть K и q таковы, как в следствии* 2; *тогда алгебра с делением конечной размерности над K неразветвлена в том и только в том случае, когда она коммутативна и порождается над K корнями из единицы степени, взаимно простой с p. Для каждого $f \geqslant 1$ поле K имеет с точностью до изоморфизма одно и только одно неразветвленное расширение степени f; это расширение порождается над K примитивным корнем $(q^f - 1)$-й степени из единицы.*

Пусть K' — неразветвленная алгебра с делением размерности f над K и q, q' — соответственно модули алгебр K и K'. Тогда по следствию 6 теор. 6 $q' = q^f$. Возьмем подгруппу $M'^{\times}$ порядка $q' - 1$ в $K'^{\times}$; по теореме 7 она циклична; взяв образующую μ в $M'^{\times}$, получим поле $K'' = K(\mu)$. Ясно, что это поле коммутативно, а так как оно содержит $M'^{\times}$, то модуль его равен по меньшей мере q', так что по следствию 6 теор. 6 его степень над K не меньше f. Следовательно, $K'' = K'$, что вместе со следствием 2 доказывает первую часть нашего следствия. Возьмем теперь любое целое $f \geqslant 1$, положим $q' = q^f$ и обозначим через K' расширение поля K, порожденное примитивным корнем степени $q' - 1$ из единицы,

или, что то же самое, множеством $M'^{\times}$ всех корней уравнения $X^{q'-1} = 1$. По теореме 7 модуль поля K' не меньше q', так что из следствия 6 теор. 6 вытекает, что степень K' над K равна по меньшей мере f. С другой стороны, в силу следствия 2 K' неразветвлено и циклично над K и его группа Галуа порождается определенным в этом следствии автоморфизмом φ. Так как автоморфизм φ^f индуцирует тождественный автоморфизм на $M'^{\times}$, то он тождествен и, следовательно, степень K' над K не больше f. Таким образом, она равна f. Из предыдущих результатов следует, что каждое неразветвленное расширение поля K, имеющее степень f, должно содержать расширение, изоморфное K'. Этим наше доказательство завершается.

Следствие 4. *Пусть K' — конечное расширение коммутативного p-поля K; обозначим через f его модулярную степень над K, а через e порядок ветвления над K. Тогда существует единственное максимальное неразветвленное расширение K_1 поля K, содержащееся в K'. Оно имеет степень f над K, и K' вполне разветвлено и имеет степень e над K_1.*

Это сразу следует из предыдущих результатов, если в качестве K_1 взять поле, порожденное содержащимися в K' корнями из единицы степени, взаимно простой с p.

Определение 5. *Пусть K — коммутативное p-поле и K' — его неразветвленное расширение. Образующая φ группы Галуа поля K' над K, определяемая следствием 2 теор. 7, называется автоморфизмом Фробениуса поля K' над K.*

В следствии 2 теор. 6 можно взять в качестве ξ простой элемент π поля K, а в качестве A — множество M, определенное в теореме 7. Для коммутативных полей характеристики p отсюда получается следующая

Теорема 8. *Каждое коммутативное p-поле характеристики p изоморфно полю формальных степенных рядов от одной переменной с коэффициентами из некоторого конечного поля.*

В обозначениях теоремы 7 следствие 1 из этой теоремы показывает, что M является полем из q элементов. Положив $\xi = \pi$ и $A = M$ в следствии 2 теор. 6, мы получим для каждого $x \in K$ с $\operatorname{ord}(x) \geqslant n$ единственное разложение в ряд

$$x = \sum_{i=n}^{+\infty} \mu_i \pi^i,$$

где $\mu_i \in M$ для всех $i \geqslant n$. Немедленно устанавливается, что эти ряды складываются и умножаются по обычным алгебраическим правилам для формальных степенных рядов (или для сходящихся степенных рядов в классическом анализе). Более того, полученное соответствие является также изоморфизмом и в топологическом смысле, если поле формальных степенных рядов снабдить обычной топологией, в которой фундаментальную систему окрестностей нуля образуют кольцо R_0 «целых» степенных рядов (т. е. рядов, не содержащих степеней переменной с показателем <0) и идеалы в нем, порожденные степенями переменной. Напомним, что в этой топологии кольцо R_0 целых формальных степенных рядов от одной переменной над произвольным конечным полем F компактно, поскольку его аддитивная группа изоморфна, очевидно, произведению счетного числа групп, изоморфных F. Таким образом, соответствующее поле локально компактно. Поскольку в силу теоремы 8 все коммутативные p-поля характеристики p являются полями такого типа, получаем, что (с точностью до изоморфизма) существует взаимно однозначное соответствие между этими полями и конечными полями $\mathbf{F}_q$ с $q = p^n$, $n \geqslant 1$.

Под *локальным полем* будет пониматься в дальнейшем коммутативное недискретное локально компактное поле. Мы только что получили полный список локальных полей характеристики $p > 1$; что же касается полей характеристики 0, то все они даются теоремой 5 из § 3. Это $\mathbf{R}$, $\mathbf{C}$ и конечные алгебраические расширения полей $\mathbf{Q}_p$ для всех p.

Используя ту же идею, что и в доказательстве теоремы 8, можно получить более общий результат для некоммутативного случая.

Предложение 5. *Пусть K — некоторое p-поле, коммутативное или нет, с максимальным компактным подкольцом R. Тогда центр K_0 поля K является p-полем, и если d — его модулярная степень над K_0, то порядок ветвления его над K_0 равен d, а размерность равна d^2. Поле K содержит максимальное коммутативное подполе K_1, которое неразветвлено и имеет степень d над K_0. Кроме того, если K_1 — такое подполе и R_1 — его максимальное компактное подкольцо, то в K существует простой элемент π со следующими свойствами*: (a) *π^d есть простой элемент поля K_0*; (b) *$\{1, \ldots, \pi^{d-1}\}$ есть базис поля K, рассматриваемого как левое векторное пространство над K_1, и порождает R как левый R_1-модуль*; (c) *внутренний автоморфизм $x \to \pi^{-1}x\pi$ поля K индуцирует в K_1 автоморфизм α, порождающий группу Галуа поля K_1 над K_0.*

Пусть обозначения таковы, как в теоремах 6 и 7; выберем M и π так же, как в теореме 7, и применим к ним следствие 2 теор. 6.

Получим, что для всех $n \in \mathbf{Z}$ каждый элемент $x \in P^n$ может быть представлен единственным образом в виде

$$x = \sum_{i=n}^{+\infty} \mu_i \pi^i, \tag{5}$$

где $\mu_i \in M$ для всех $i \geqslant n$. Поэтому элемент поля K находится в центре K_0 этого поля в том и только в том случае, когда он коммутирует с π и с каждым элементом из M (или, что то же самое, с какой-нибудь образующей циклической группы $M^\times$). Так как автоморфизм $x \to \pi^{-1} x \pi$ индуцирует перестановку множества M, то некоторая его степень тождественна на M. Иначе говоря, существует такое $\nu > 0$, что π^ν коммутирует с каждым элементом из M. Поэтому множество K_0 содержит $\pi^{\nu n}$ для всех $n \in \mathbf{Z}$, чем доказана его недискретность, а поскольку оно, очевидно, замкнуто в K, получаем, что поле K локально компактно. Если мы рассмотрим теперь K как векторное пространство и, следовательно, алгебру над K_0, то по следствию 2 теор. 3 § 2 оно имеет конечную размерность над K_0. Следствие 5 теор. 6 показывает теперь, что K_0 есть p-поле. Обозначим через q модуль поля K_0, через d — модулярную степень K над K_0 и через K_1 — поле, порожденное над K_0 множеством M, или, что то же самое, любой образующей циклической группы $M^\times$. Поскольку $M^\times$ имеет порядок $q^d - 1$, такая образующая является примитивным корнем степени $q^d - 1$ из единицы, так что по следствию 3 теор. 7 K_1 неразветвлено и имеет степень d над K_0. Так как отображение $x \to \pi^{-1} x \pi$ индуцирует перестановку на M и тождественное отображение на K_0, оно определяет в K_1 автоморфизм α поля K_1 над K_0. Элементы из K_1 коммутируют со всеми элементами из M; с π они коммутируют в том и только в том случае, когда они инвариантны относительно α. Другими словами, элементы поля K_1, инвариантные относительно α, совпадают с K_0, так что α порождает группу Галуа поля K_1 над K_0. Следовательно, α имеет порядок d, откуда, как мы видели выше, следует, что π^d находится в K_0, а π^ν не принадлежит K_0, если ν не кратно d. Возьмем теперь $x \in K$ и $\mu \in M^\times$ и запишем x в виде (5). Мы получим

$$\mu^{-1} x \mu = \sum_{i=n}^{+\infty} \mu_i' \pi^i,$$

где

$$\mu_i' = \mu^{-1} \mu_i \cdot (\pi^i \mu \pi^{-i}).$$

В последней формуле последний множитель в правой части принадлежит группе $M^\times$, так что элементы μ_i' находятся в M. Ввиду единственности для $x \in K$ разложения (5) отсюда вытекает, что

$x = \mu^{-1}x\mu$ (т. е. x коммутирует с μ) в том и только в том случае, когда $\mu_i' = \mu_i$ для всех i. Ясно, однако, что $\mu_i' = \mu_i$ тогда и только тогда, когда или $\mu_i = 0$, или π^i коммутирует с μ. Следовательно, x коммутирует со всеми элементами из $M^\times$ тогда и только тогда, когда π^i обладает этим свойством для всех i, для которых $\mu_i \neq 0$. В силу доказанного выше последнее имеет место в том и только в том случае, когда $\mu_i = 0$ для всякого i, не являющегося кратным d. Мы можем поэтому написать

$$x = \sum_i \mu_{d_i} (\pi^d)^i.$$

Поскольку $\pi^a \in K_0$, элемент x принадлежит замыканию поля K_1, и, следовательно, ему самому, откуда видно, что K_1 — максимальное коммутативное подполе в K. Ввиду разложения (5) и единственности этого разложения ясно также, что $\{1, \pi, \ldots, \pi^{d-1}\}$ есть базис поля K, рассматриваемого как левое векторное пространство над K_1; что этот базис порождает R как левый R_1-модуль и что π^d есть простой элемент поля K_1 и, следовательно, поля K_0, поскольку он в нем лежит. Так как отсюда следует, что порядок ветвления K над K_0 есть d, доказательство окончено.

Пусть в обозначениях предложения 5 φ — автоморфизм Фробениуса поля K_1 над K_0. Так как он тоже порождает группу Галуа поля K_1 над K_0, то $\varphi = \alpha^r$, где r взаимно просто с d и определено однозначно по модулю d. В гл. XII будет показано, что для данного K_0 числа d и r, удовлетворяющие этим условиям, можно выбирать произвольно и что они однозначно определяют структуру алгебры с делением K. Другими словами, две алгебры с делением конечной размерности над K_0 и с центром K_0 изоморфны тогда и только тогда, когда они имеют одинаковую размерность d^2 над K_0 и целое число r для обеих алгебр одно и то же по модулю d.

Мы завершим эту главу одним результатом о максимальных компактных подкольцах p-полей. Напомним, что если R — произвольное коммутативное кольцо и x — элемент кольца, содержащего R, то этот элемент называется *целым над* R, если он является корнем некоторого унитарного многочлена над R, т. е. некоторого многочлена с коэффициентами из R, старший коэффициент которого равен 1.

Предложение 6. *Пусть K есть p-поле, K_0 — некоторое p-поле, содержащееся в его центре, R, R_0 — максимальные компактные подкольца полей K и K_0 соответственно. Тогда R состоит из элементов поля K, целых над R_0.*

Пусть элемент x принадлежит K и цел над R_0; это означает, что он удовлетворяет уравнению

$$x^n + a_1x^{n-1} + \ldots + a_n = 0,$$

в котором $a_i \in R_0$ для $1 \leqslant i \leqslant n$. Предположим, что x не лежит в R, т. е. что $\mathrm{ord}_K(x) < 0$. Тогда $x \neq 0$ и

$$1 = -a_1x^{-1} - \ldots - a_nx^{-n};$$

все члены в правой части находятся в максимальном идеале P кольца R, так что $1 \in P$, что невозможно. Обратно, пусть x принадлежит R. По следствию 2 теор. 3 § 2 K имеет конечную размерность над K_0; значит, коммутативное поле K', определяемое равенством $K' = K_0(x)$, является конечным расширением поля K_0. Обозначим через F неприводимый унитарный многочлен с коэффициентами из K_0, такой, что $F(x) = 0$. Пусть K'' — содержащееся в каком-нибудь алгебраическом замыкании поля K' поле, порожденное всеми корнями многочлена F, так что F разлагается в K'' на линейные множители. Поскольку K', K'' суть конечные расширения поля K_0, они являются p-полями; пусть R', R'' — их максимальные компактные подкольца. Тогда $R' = K' \cap R = K' \cap R''$, а так как элемент x лежит в R, он принадлежит как R', так и R''. Поскольку многочлен F неприводим, каждый его корень x' в K'' является образом корня x относительно некоторого автоморфизма поля K'' над K_0, а так как такой автоморфизм отображает R'' на R'', все эти корни лежат в R''. Таким образом, все коэффициенты многочлена F находятся в R'', а поскольку они принадлежат K_0, они лежат в R_0, чем доказательство и завершено.

Если поле K коммутативно, предложение 6 можно выразить, сказав, что R является целым замыканием кольца R_0 в K.

ГЛАВА ВТОРАЯ

РЕШЕТКИ И ДВОЙСТВЕННОСТЬ НАД ЛОКАЛЬНЫМИ ПОЛЯМИ

§ 1. НОРМЫ

В этом и следующем параграфах K будет обозначать p-поле, не обязательно коммутативное. Мы будем рассматривать большей частью левые векторные пространства над K; все, однако, может быть распространено очевидным образом и на правые векторные пространства. Все векторные пространства будут конечной размерности; кроме того, всегда будет предполагаться, что они снабжены «естественной» топологией согласно следствию 1 теор. 3 гл. I-2. По теореме 3 гл. I-2 каждое подпространство такого пространства V замкнуто в V. Используя координаты, легко доказать, что все линейные отображения таких пространств друг в друга непрерывны; в частности, непрерывны все линейные формы. Аналогичным образом каждое линейное инъективное отображение такого пространства V в некоторое другое является изоморфизмом V на его образ. Так как K некомпактно, то всякое подпространство в V, кроме $\{0\}$, некомпактно.

Определение 1. *Пусть V — левое векторное пространство над p-полем K. Под K-нормой на V понимается функция N со значениями в $\mathbf{R}_+$, такая, что*: (i) $N(v) = 0$ *в том и только в том случае, когда* $v = 0$; (ii) $N(xv) = \mathrm{mod}_K(x)\, N(v)$ *для всех* $x \in K$ *и всех* $v \in V$; (iii) *для всех* v, w *выполняется ультраметрическое неравенство*

$$N(v + w) \leqslant \sup(N(v),\ N(w)). \tag{1}$$

На K^n можно определить K-норму N_0, положив $N_0(x) = \sup_{1 \leqslant i \leqslant n} (\mathrm{mod}_K(x_i))$ для всех $x = (x_1, \ldots, x_n)$ из K^n. Поскольку каждое векторное пространство конечной размерности над K изоморфно пространству K^n, получаем, что на всех таких пространствах существуют K-нормы.

Ясно, что с помощью произвольной K-нормы на V можно топологизировать V, взяв $N(v - w)$ в качестве метрики.

Предложение 1. *Пусть V — левое векторное пространство конечной размерности над p-полем K. Каждая K-норма N на V определяет на V естественную топологию. В частности, каждая такая норма N непрерывна, и для всех $r > 0$ подмножества L_r в V, определяемые условием $N(v) \leqslant r$, являются компактными окрестностями нуля.*

Что касается первого утверждения, то в силу следствия 1 теор. 3 гл. I-2 нужно только показать, что топология, определяемая нормой N на V, превращает V в топологическое векторное пространство над K. Это сразу следует из неравенства

$$N(x'v' - xv) \leqslant \sup(\mathrm{mod}_K(x')\, N(v' - v),\ \mathrm{mod}_K(x' - x)\, N(v)),$$

которое является непосредственным следствием определения 1. Следовательно, норма N непрерывна, и множества L_r образуют фундаментальную систему замкнутых окрестностей нуля. В частности, для некоторого $r > 0$ множество L_r должно быть компактно. Выберем теперь для произвольного $s > 0$ элемент $a \in K^\times$ так, чтобы $\mathrm{mod}_K(a) \leqslant r/s$; сразу видно, что множество L_s содержится в $a^{-1}L_r$ и, следовательно, компактно.

Следствие 1. *В $V - \{0\}$ существует компактное подмножество A, которое содержит скалярное кратное любого элемента v из $V - \{0\}$.*

Обозначим через q модуль поля K и выберем какую-нибудь K-норму N на V. Если π — простой элемент поля K, то в силу теоремы 6 гл. I-4 $\mathrm{mod}_K(\pi) = q^{-1}$ и потому для всех $n \in \mathbf{Z}$ и всех $v \in V$ имеет место равенство $N(\pi^n v) = q^{-n}N(v)$. Пусть A — подмножество в V, определенное условием $q^{-1} \leqslant N(v) \leqslant 1$; в силу предложения 1 оно компактно, и для каждого $v \neq 0$ можно найти $n \in \mathbf{Z}$, такое, что $\pi^n v \in A$.

Следствие 1 означает, что «проективное пространство», связанное с V, компактно.

Следствие 2. *Пусть φ — произвольная непрерывная функция на $V - \{0\}$ со значениями в $\mathbf{R}$, такая, что $\varphi(av) = \varphi(v)$ для всех $a \in K^\times$ и всех $v \in V - \{0\}$. Тогда φ достигает максимума в некоторой точке v_1 из $V - \{0\}$.*

В самом деле, достаточно взять множество A из следствия 1 и выбрать в качестве v_1 ту точку множества A, в которой φ достигает максимума на A.

Следствие 3. *Пусть f — произвольная линейная форма на V и N — некоторая K-норма на V. Тогда в V существует эле-*

мент $v_1 \neq 0$, *такой, что для всех* $v \neq 0$ *из* V

$$N(v)^{-1} \bmod_K (f(v)) \leqslant N(v_1)^{-1} \bmod_K (f(v_1)). \tag{2}$$

Это частный случай следствия 2, примененного к левой части неравенства (2). Если обозначить правую часть (2) через $N^*(f)$, то $N^*(f)$ будет наименьшим положительным числом, таким, что

$$\bmod_K (f(v)) \leqslant N^*(f)\, N(v)$$

для всех $v \in V$; соответствие $f \to N^*(f)$ будет K-нормой на пространстве, двойственном к V, т. е. на правом векторном пространстве линейных форм на V (сложение форм определяется очевидным образом, а умножение на скаляр производится по правилу $(fa)(v) = f(v)\, a$, где f — форма, а $a \in K$).

Под *гиперплоскостью* в V понимается подпространство коразмерности 1, т. е. подмножество H в V, определенное уравнением $f(v) = 0$, где f — линейная форма, отличная от нуля. Если H задано, то f определяется однозначно с точностью до отличного от нуля скалярного множителя. Далее, если формула (2) выполняется при всех $v \neq 0$ для заданных нормы N, линейной формы $f \neq 0$ и элемента $v_1 \neq 0$, то это же будет верно, если заменить f на fa, где $a \in K^\times$, и v_1 на bv_1, где $b \in K^\times$. Другими словами, справедливость неравенства (2) для всех $v \neq 0$ зависит лишь от свойств гиперплоскости H, определяемой уравнением $f = 0$, и подпространства W в V, порожденного вектором v_1. В случае когда (2) выполняется для всех $v \neq 0$, говорят, что H и W *N-ортогональны* друг другу.

Предложение 2. *Гиперплоскость* H *и подпространство* W *в* V *размерности* 1 *N-ортогональны тогда и только тогда, когда* V *является прямой суммой* H *и* W *и* $N(h + w) = \sup(N(h), N(w))$ *для всех* $h \in H$ *и* $w \in W$.

Пусть H определено уравнением $f(v) = 0$, и пусть H и W N-ортогональны. Тогда, если заменить в (2) v_1 на любое отличное от нуля $w \in W$, то (2) будет справедливо. Отсюда следует, что $f(w)$ не равно нулю; следовательно, V есть прямая сумма H и W. Заменим теперь в (2) v на $h + w$, где $h \in H$; поскольку $f(h + w) = f(w) \neq 0$, из (2) вытекает, что $N(h + w) \geqslant N(w)$. Применяя ультраметрическое неравенство (1) к $h = (h + w) + (-w)$, получаем $N(h) \leqslant N(h + w)$; применение этого неравенства к $h + w$ дает доказываемую формулу при $w \neq 0$, а так как она тривиальна при $w = 0$, необходимость нашего условия доказана. Пусть теперь V есть прямая сумма H и W. Выберем какое-нибудь $v \neq 0$ и запишем его в виде $v = h + w$, где $h \in H$ и $w \in W$, так что $f(v) = f(w)$.

Если $w \neq 0$ и $N(h + w) \geqslant N(w)$, то

$$N(v)^{-1} \bmod_K (f(v)) \leqslant N(w)^{-1} \bmod_K (f(w)).$$

Поскольку правая часть неравенства не изменится, если заменить w любым вектором v_1, порождающим подпространство W, мы видим, что (2) выполняется для каждого такого v_1 и произвольного v, не лежащего в H. При $v \in H$, т. е. при $w = 0$, оно выполняется тривиальным образом, чем доказательство и завершено.

Аналогичным образом будем говорить, что два подпространства V', V'' из V *N-ортогональны* друг другу, если V является их прямой суммой и $N(v' + v'') = \sup(N(v'), N(v''))$ для всех $v' \in V'$ и $v'' \in V''$.

Предложение 3. *Пусть V имеет размерность n над K, и пусть N — некоторая K-норма на V. Тогда существует разложение $V = V_1 + \ldots + V_n$ пространства V в прямую сумму подпространств V_i размерности* 1, *для которого* $N(\Sigma v_i) = \sup_i N(v_i)$ *при* $v_i \in V_i$, $1 \leqslant i \leqslant n$. *Более того, если* $W_1 = V$, $W_2, \ldots, W_n$ — *последовательность подпространств в V, такая, что W_i есть подпространство в W_{i-1} коразмерности* 1, $2 \leqslant i \leqslant n$, *то подпространства V_i можно выбрать так, чтобы $W_i = V_i + \ldots + V_n$ для всех i.*

Это очевидно для $n = 1$. Если $n > 1$, то воспользуемся индукцией по n. В силу следствия 3 предл. 1 можно выбрать v_1 так, чтобы пространство V_1, порожденное v_1, было N-ортогонально к W_2; по предложению 2 тогда $N(v_1' + w_2) = \sup(N(v_1'), N(w_2))$, $v_1' \in V_1$, $w_2 \in W_2$. Применяя предположение индукции к K-норме, индуцированной на W_2 нормой N, и к последовательности $W_2, \ldots, W_n$, получаем наш результат.

Следствие. *Для каждого подпространства W в V существует подпространство W', N-ортогональное к W.*

Выберем последовательность подпространств $W_1, \ldots, W_n$, такую, как в предложении 3, для которой W является одним из ее членов, скажем W_i. Возьмем V_i из предложения 3. Пространство $W' = V_1 + \ldots + V_{i-1}$ будет тогда N-ортогонально к W.

Предложение 4. *Пусть N и N' — две K-нормы на V. Тогда существует разложение $V = V_1 + \ldots + V_n$ пространства V в прямую сумму подпространств V_i размерности* 1, *такое, что* $N(\Sigma v_i) = \sup_i N(v_i)$ *и* $N'(\Sigma v_i) = \sup_i N'(v_i)$ *при* $v_i \in V_i$, $1 \leqslant i \leqslant n$.

Это очевидно для $n = 1$. Для $n > 1$ используем индукцию по n. Применяя следствие 2 предл. 1 к $\varphi = N/N'$, получаем вектор $v_1 \neq 0$, такой, что для всех $v \neq 0$

$$N(v)\,N'(v)^{-1} \leqslant N(v_1)\,N'(v_1)^{-1}.$$

Обозначим через V_1 пространство, порожденное вектором v_1. По следствию предл. 3 существует гиперплоскость W, которая N-ортогональна к V_1; если $f = 0$ — уравнение этой гиперплоскости, то

$$N(v)^{-1} \bmod_K (f(v)) \leqslant N(v_1)^{-1} \bmod_K (f(v_1))$$

для всех $v \neq 0$. Перемножая эти два неравенства, находим

$$N'(v)^{-1} \bmod_K (f(v)) \leqslant N'(v_1)^{-1} \bmod_K (f(v_1));$$

это означает, что W N'-ортогонально к V_1. Применяя теперь предложение 2 к N, V_1, W, а также к N', V_1, W, а предположение индукции к нормам, индуцированным на W нормами N и N', получаем утверждаемый результат.

Следует отметить тесную аналогию между предложениями 3 и 4 с их доказательствами и соответствующими результатами и доказательствами для норм, определяемых положительно определенными квадратичными формами в векторных пространствах над $\mathbf{R}$ или эрмитовыми формами в пространствах над $\mathbf{C}$ или $\mathbf{H}$. Так, например, предложение 4 соответствует одновременному приведению двух квадратичных или эрмитовых форм к диагональному виду.

§ 2. РЕШЕТКИ

В этом параграфе будут использоваться обозначения, введенные в гл. I, и K снова будет обозначать p-поле. В частности, мы по-прежнему будем обозначать через R максимальное компактное подкольцо в K, через P — максимальный идеал в R, через q — модуль поля K и через π — его простой элемент. Для $n \in \mathbf{Z}$ полагаем $P^n = \pi^n R = R\pi^n$.

Мы будем рассматривать R-модули в левом векторном пространстве конечной размерности над K; если V — такое пространство, то R-модуль в V есть подгруппа M в V, такая, что $R \cdot M = M$.

Предложение 5. *Пусть V — левое векторное пространство конечной размерности над K и M — некоторый R-модуль в V. Обозначим через W подпространство в V, порожденное над K множеством M. Множество M открыто и замкнуто в W; оно компактно в том и только в том случае, когда оно конечно порождено как R-модуль.*

Пусть $m_1, \ldots, m_r$ — максимальное множество линейно независимых над K элементов из M; они образуют базис пространства W над K. Согласно теореме 3 гл. I-2, множество $Rm_1 + \ldots + Rm_r$ является открытой подгруппой в W; а поскольку оба множества, M и $W - M$, являются объединениями классов смежности по отношению к этой подгруппе, оба они открыты. Если M компактно, то оно является объединением конечного числа таких классов и, следовательно, конечно порождено; обратное очевидно.

Далее, в силу следствия 2 теор. 6 гл. I-4 замкнутая подгруппа X в V удовлетворяет условию $R \cdot X = X$ в том и только в том случае, когда $\pi X \subset X$ и $aX \subset X$ для каждого a из некоторой полной системы A представителей поля R/P в R. В частности, если $q = p$, т. е. если R/P — простое поле, можно взять $A = \{0, 1, \ldots, p-1\}$, так что $aX \subset X$ для всех $a \in A$, и, значит, X является R-модулем тогда и только тогда, когда $\pi X \subset X$. В случае $K = \mathbf{Q}_p$ можно взять $\pi = p$, тогда каждая замкнутая подгруппа является R-модулем.

В самом K, рассматриваемом как левое векторное пространство над K, каждый R-модуль, не сводящийся к $\{0\}$, является объединением множеств P^n и, следовательно, совпадает или с K, или с одним из этих множеств.

Определение 2. *K-решеткой в левом векторном пространстве V конечной размерности над K называется компактный открытый R-модуль в V.*

Мы будем говорить просто «решетка» вместо «K-решетка», если это не сможет вызвать недоразумений. Если L есть p-поле, содержащееся в K, то каждая K-решетка является L-решеткой; обратное неверно, если $L \neq K$. Если L—решетка в V и W—подпространство в V, то ясно, что $L \cap W$ — решетка в W. Аналогично если f — инъективное линейное отображение пространства V' в V, то $f^{-1}(L)$ —решетка в V', и если f' — сюръективное линейное отображение пространства V на V'', то $f'(L)$ — решетка в V''.

Если N — некоторая K-норма в V, то множества L_r, определяемые условием $N(v) \leqslant r$, являются K-решетками для любого $r > 0$. Действительно, условие (iii) из определения 1 § 1 вместе с условием (ii), примененным к $x = -1$, показывает, что множество L есть подгруппа в V; из (ii) следует тогда, что оно есть R-модуль, а из предложения 1 § 1, что оно есть компактная окрестность нуля в V и, следовательно, открыто, поскольку является подгруппой. Это утверждение допускает обращение. Более общим образом имеет место следующее

Предложение 6. *Пусть M — открытый R-модуль в V; для каждого $v \in V$ положим*

$$N_M(v) = \inf_{x \in K^\times,\, xv \in M} \mathrm{mod}_K(x)^{-1}.$$

Тогда N_M как функция на V удовлетворяет условиям (ii) *и* (iii) *определения* 1 § 1 *и M есть подмножество в V, определяемое уравнением $N_M(v) \leqslant 1$. Функция N_M является K-нормой в том и только в том случае, когда M есть K-решетка в V.*

Если $a \in K^\times$, то $x \cdot av \in M$ тогда и только тогда, когда $x = ya^{-1}$, где $yv \in M$; это дает равенство $N_M(av) = \mathrm{mod}_K(a)\, N_M(v)$, справедливое также и для $a = 0$, ибо $N_M(0) = 0$. Таким образом, N_M удовлетворяет условию (ii) определения 1. Для каждого $v \in V$ пусть M_v — множество элементов x из K, для которых $xv \in M$; поскольку оно — открытый R-модуль в K, то оно совпадает или с K, или с P^n для некоторого $n \in \mathbf{Z}$. Если $M_v = K$, то $N_M(v) = 0$; а если $M_v = P^n$, то $xv \in M$ в том и только в том случае, когда $\mathrm{mod}_K(x) \leqslant q^{-n}$, так что $N_M(v) = q^n$. В частности, $N_M(v) \leqslant 1$ тогда и только тогда, когда $M_v \supset R$, т. е. когда $v \in M$. Пусть v, w принадлежат V и таковы, что $N_M(v) \geqslant N_M(w)$; тогда $M_v \subset M_w$ и $xv \in M$ влечет $xw \in M$, откуда $x(v + w) \in M$. Поэтому $M_{v+w} \supset M_v$ и, следовательно, $N_M(v + w) \leqslant N_M(v)$; этим доказано условие (iii) из определения 1. Наконец, множество M является K-решеткой в том и только в том случае, когда оно компактно, а N_M является K-нормой в том и только в том случае, когда $N_M(v) > 0$ для всех $v \neq 0$, т. е. тогда и только тогда, когда $M_v \neq K$ для $v \neq 0$. По предложению 1 § 1, если N_M есть K-норма, то M компактно. Обратно, предположим, что M компактно, и выберем $v \neq 0$. Тогда M_v есть подмножество в K, соответствующее множеству $(Kv) \cap M$ при изоморфизме $x \to xv$ из K на Kv, поэтому M_v компактно и не может совпадать с K. Доказательство завершено.

Следствие 1. *Открытый R-модуль M в V является K-решеткой в том и только в том случае, когда он не содержит отличных от нуля подпространств в V.*

Как было показано выше, если M некомпактно, то N_M не может быть K-нормой, так что в V существует элемент $v \neq 0$, такой, что $N_M(v) = 0$ и, следовательно, $M_v = K$, т. е. $Kv \subset M$. Обратно, поскольку каждое отличное от нуля подпространство в V замкнуто в V и некомпактно, такое подпространство не может содержаться в множестве M в силу компактности последнего.

Следствие 2. *Пусть M — открытый R-модуль в V, W — максимальное подпространство в V, содержащееся в M, W' — какое-нибудь дополнительное к W подпространство в V. Тогда $M \cap W'$ является K-решеткой в W' и $M = (M \cap W') + W$.*

Первое утверждение есть частный случай следствия 1, второе очевидно.

Предложение 6 показывает, что каждая K-решетка в V может быть определена неравенством $N(v) \leqslant 1$, где N — некоторая K-норма. Вот главная причина, почему мы посвятили § 1 рассмотрению норм. Для заданной K-решетки M норма N_M, определяемая предложением 6, может быть охарактеризована среди всех норм N, для которых M есть множество $N(v) \leqslant 1$, как норма, принимающая свои значения в множестве значений функции mod_K на K, т. е. в множестве $\{0\} \cup \{q^n\}_{n \in \mathbf{Z}}$.

Предложение 7. *Если V имеет над K размерность 1 и если L есть K-решетка в V, то в V существует образующая v, такая, что $L = Rv$.*

Возьмем какую-нибудь образующую w пространства V; подмножество L_w в K, определяемое условием $xw \in L$, должно иметь вид P^n; беря $v = \pi^n w$, получаем $L = Rv$.

Теорема 1. *Пусть L — некоторая K-решетка в левом векторном пространстве V размерности n над K. Тогда в V существует базис $\{v_1, \ldots, v_n\}$, такой, что $L = \Sigma\, Rv_i$. Кроме того, если $W_1 = V$, $W_2, \ldots, W_n$ — последовательность подпространств в V, обладающая тем свойством, что W_i есть подпространство в W_{i-1} коразмерности 1, $2 \leqslant i \leqslant n$, то элементы v_i можно выбрать так, чтобы для каждого i множество $\{v_i, \ldots, v_n\}$ было базисом в W_i.*

Возьмем K-норму N, такую, что L определяется уравнением $N(v) \leqslant 1$. Выберем подпространства $V_1, \ldots, V_n$ из V так же, как в предложении 3 § 1. Тогда $L = \Sigma\,(L \cap V_i)$. Применяя предложение 7 для каждого i к V_i и $L \cap V_i$, получаем базис (v_i).

Теорема 1 применима, например, к случаю, когда K' есть p-поле, содержащее K, а R' — его максимальное компактное подкольцо. Ясно, что если рассматривать K' как левое векторное пространство над K, то R' является K-решеткой в K'. Следовательно, в K' существует базис $\{y_1, \ldots, y_n\}$ над K, такой, что $R' = \Sigma\, Ry_i$. Если записать теперь произвольное $y \in R'$ в виде $yy_i = \Sigma\, a_{ij} y_j$, где $a_{ij} \in K$, $1 \leqslant i, j \leqslant n$, то все a_{ij} должны лежать в R. В частности, если K коммутативно, то из этих соотношений, выполняющих-

ся в коммутативном поле $K(y)$, вытекает, что $\det(y \cdot 1_n - A) = 0$, где 1_n — единичная матрица, а $A = (a_{ij})$, так что мы получаем другое доказательство второй части предложения 6 гл. I-4.

Теорема 2. *Пусть L, L' — две K-решетки в левом векторном пространстве V конечной размерности над K. Тогда в V существуют базис $\{v_1, \ldots, v_n\}$ и последовательность целых чисел $(\nu_1, \ldots, \nu_n)$, такие, что $L = \Sigma\, Rv_i$ и $L' = \Sigma\, P^{\nu_i} v_i$.*

Выберем K-нормы N и N' так, чтобы L определялась уравнением $N(v) \leqslant 1$, а L' — уравнением $N'(v) \leqslant 1$. Построим подпространства $V_1, \ldots, V_n$ в V так же, как в предложении 4 § 1. Тогда $L = \sum (L \cap V_i)$ и $L' = \sum (L' \cap V_i)$. Применим теперь предложение 7 для каждого i к V_i и $L \cap V_i$, а также к V_i и $L' \cap V_i$; это даст нам элементы v_i, такие, что $L \cap V_i = Rv_i$, и элементы v_i', такие, что $L' \cap V_i = Rv_i'$. Записав v_i' в виде $v_i' = x_i v_i$, где $x_i \in K^\times$, и положив $\nu_i = \operatorname{ord}(x_i)$, получим целые числа ν_i, удовлетворяющие требуемым условиям.

Следствие 1. *Пусть V и L таковы, как в теоремах 1 и 2, и M — некоторый R-модуль в V. Тогда в V существуют базис $\{v_1, \ldots, v_n\}$ над K и целые числа r, s и $\nu_1, \ldots, \nu_r$, такие, что $0 \leqslant r \leqslant s \leqslant n$, $L = \Sigma\, Rv_i$ и $M = \sum_{j=1}^{r} P^{\nu_j} v_j + \sum_{h=r+1}^{s} Kv_h$.*

Пусть W — подпространство в V, порожденное множеством M, и W' — максимальное подпространство, содержащееся в M. Обозначим через s размерность пространства W и через r — коразмерность W' в W. Выберем последовательность $W_1, \ldots, W_n$ из теоремы 1 так, чтобы она содержала пространства W и W'. По теореме 1 существует базис $\{w_1, \ldots, w_n\}$ пространства V, который порождает L как R-модуль и содержит базисы пространств W и W'. Нумеруя этот базис очевидным образом, можно добиться того, чтобы $\{w_1, \ldots, w_s\}$ было базисом в W, а $\{w_{r+1}, \ldots, w_s\}$ — базисом в W'. Обозначим через W'' подпространство с базисом $\{w_1, \ldots, w_r\}$. В силу предложения 5 M открыто в W; следовательно, по следствию 2 предл. 6 $M = M' + W'$, где $M' = M \cap W''$ есть K-решетка в W''. Применяя теперь к M' и $L' = L \cap W''$ теорему 2, находим базис $\{v_1, \ldots, v_r\}$ для W'' и целые числа $\nu_1, \ldots, \nu_r$, такие, что $L' = \Sigma\, Rv_j$ и $M' = \Sigma\, P^{\nu_j} v_j$. Положив $v_i = w_i$ для $i > r$, получаем искомый базис.

Следствие 2. *Каждый конечно порожденный R-модуль $\mathfrak{M}$ является прямой суммой конечного числа слагаемых, каждое из которых изоморфно или R, или модулю R/P^ν, где $\nu > 0$. Кроме*

того, число слагаемых типа R и для каждого $\nu > 0$ число слагаемых типа R/P^ν определяются заданием модуля $\mathfrak{M}$ однозначно.

Предположим, что $\mathfrak{M}$ порожден элементами $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Возьмем векторное пространство V размерности n над K с базисом $\{v_1, \ldots, v_n\}$ и положим $L = \sum Rv_i$. Формула

$$\sum x_i v_i \to \sum x_i \mathfrak{m}_i,$$

где x_i при всех $1 \leqslant i \leqslant n$ берутся из R, определяет тогда морфизм из L на $\mathfrak{M}$; следовательно, $\mathfrak{M}$ изоморфно L/M, где M — ядро этого морфизма. Применим теперь следствие 1 к L и M; поскольку $M \subset L$, имеем $\nu_j \geqslant 0$ для всех $1 \leqslant j \leqslant \nu$ и $r = s$. Отсюда сразу следует наше первое утверждение. Что касается второго, то пусть $\mathfrak{M}_i = \pi^i \mathfrak{M}$ для $i \geqslant 0$. Так как все это R-модули, факторы $\mathfrak{N}_i = \mathfrak{M}_i/\mathfrak{M}_{i+1}$ также являются R-модулями; поскольку $\pi n = 0$ для всех $n \in \mathfrak{N}_i$, то $\mathfrak{N}_i$ можно рассматривать как модуль, т. е. как векторное пространство, над полем $k = R/P$; в качестве такового оно имеет размерность n_i, зависящую только от $\mathfrak{M}$ и i. Запишем теперь $\mathfrak{M}$ в виде прямой суммы модулей R и R/P^ν в количествах соответственно N_0 и N_ν; сразу видно, что $n_i = N_0 + \sum\limits_{\nu > i} N_\nu$. Поэтому $N_0 = n_i$ для достаточно больших i и $N_\nu = n_{\nu-1} - n_\nu$.

Следствие 3. *Целые r, s, $\nu_1, \ldots, \nu_r$ из следствия* 1 *зависят только от L и M.*

Поскольку s — размерность подпространства W, порожденного M, а $s - r$ — размерность максимального подпространства, содержащегося в M, они зависят только от M. Положим $L_1 = L \cap W$ и выберем $i \geqslant 0$ так, чтобы $\pi^i L_1 \subset M$; наше утверждение следует теперь немедленно из следствия 2, примененного к R-модулю $M/\pi^i L_1$.

Число изоморфных R слагаемых модуля $\mathfrak{M}$ из следствия 2 называется *рангом* модуля $\mathfrak{M}$; используя это определение, получаем

Следствие 4. *Пусть $\mathfrak{M}$ — конечно порожденный R-модуль и $\mathfrak{M}'$ — его подмодуль. Тогда ранг модуля $\mathfrak{M}$ равен сумме рангов модулей $\mathfrak{M}'$ и $\mathfrak{M}/\mathfrak{M}'$.*

Как и в доказательстве следствия 2, запишем $\mathfrak{M}$ в виде L/M, где L — решетка $\sum Rv_i$ в векторном пространстве V с базисом $\{v_1, \ldots, v_n\}$ и M — некоторый R-модуль. Прообраз $\mathfrak{M}'$ в L будет тогда R-модулем L', и три модуля из нашего следствия изоморфны соответственно L/M, L'/M и L/L'. Пусть W, V' — подпространства в V, порожденные соответственно множествами M и L'. Как сразу вытекает из следствия 1, ранги модулей L/M, L'/M и L/L' равны соответственно коразмерностям W в V, W в V' и V' в V.

§ 3. МУЛЬТИПЛИКАТИВНАЯ СТРУКТУРА ЛОКАЛЬНЫХ ПОЛЕЙ

Сохраним те же обозначения, что и раньше. Для каждого целого $n \geqslant 1$ множество $1 + P^n$ элементов x из R, которые $\equiv 1\ (P^n)$, является, очевидно, открытой и компактной подгруппой в $R^\times$, и эти подгруппы образуют фундаментальную систему окрестностей единицы в $R^\times$. Далее, теорема 7 гл. I-4 показывает, что если $M^\times$ — произвольная подгруппа порядка $q - 1$ в $R^\times$, то $R^\times = M^\times \cdot (1 + P)$, а из теоремы 6 гл. I-4 следует, что $K^\times = \Pi \cdot R^\times$, если Π — дискретная подгруппа в $K^\times$, изоморфная $\mathbf{Z}$ и порожденная простым элементом поля K. Произведения в этих формулах являются «полупрямыми».

Начиная с этого места и до конца параграфа будет предполагаться, что K — коммутативное p-поле; упомянутые произведения являются в этом случае прямыми произведениями, так что можно написать $K^\times = \Pi \times R^\times$ и $R^\times = M^\times \times (1 + P)$; кроме того, по теореме 7 гл. I-4 $M^\times$ будет группой корней из единицы в поле K степени, взаимно простой с p. Исследование структуры группы $K^\times$ сводится, таким образом, к изучению структуры $1 + P$.

Выберем какое-нибудь $x \in 1 + P$; для каждого $a \in \mathbf{Z}$ элемент x^a будет лежать в $1 + P$, и отображение $a \to x^a$ является гомоморфизмом аддитивной группы $\mathbf{Z}$ в мультипликативную группу $1 + P$; так как из леммы 5, использовавшейся при доказательстве теоремы 7 гл. I-4, вытекает, что $x^a \in 1 + P^{n+1}$ при $a \equiv 0\ (p^n)$, т. е. при $|a|_p \leqslant p^{-n}$, то наш гомоморфизм непрерывен, если снабдить $\mathbf{Z}$ p-адической топологией, т. е. топологией, индуцируемой в $\mathbf{Z}$ полем $\mathbf{Q}_p$. Поскольку множество $1 + P$ компактно, этот гомоморфизм однозначно продолжается до непрерывного гомоморфизма, обозначаемого снова через $a \to x^a$, аддитивной группы $\mathbf{Z}_p$ в мультипликативную группу $1 + P$. Если $x \in 1 + P^n$, то x^a лежит в $1 + P^n$ для всех $a \in \mathbf{Z}$ и, следовательно, для всех $a \in \mathbf{Z}_p$. Используя формулу $y^b\,(x^a)^{-1} = (yx^{-1})^b\,x^{b-a}$ и обычные рассуждения, отсюда можно просто вывести, что отображение $(a, x) \to x^a$ группы $\mathbf{Z}_p \times (1 + P)$ в $1 + P$ непрерывно. Немедленно проверяется, что это отображение определяет на группе $1 + P$ структуру $\mathbf{Z}_p$-модуля («сложение» векторов записывается мультипликативно, а «умножение» на элементы из $\mathbf{Z}_p$ — экспоненциально).

Предложение 8. *Если n — целое число, взаимно простое с p, а v — целое число, большее единицы, то отображение $x \to x^n$ индуцирует автоморфизм на группе $1 + P^v$; $(K^\times)^n$ является открытой подгруппой в $K^\times$ индекса $n \cdot (n, q - 1)$, и если n делит $q - 1$, то этот индекс равен n^2.*

Первое утверждение есть частный случай того факта, что если a — обратимый элемент в $\mathbf{Z}_p$, то отображение $x \to x^a$ является автоморфизмом группы $1 + P^v$; отсюда следует, что $(K^\times)^n$ открыто в $K^\times$. Кроме того, как мы видели выше, группа $K^\times$ есть прямое произведение группы Π, изоморфной $\mathbf{Z}$, циклической группы $M^\times$ порядка $q - 1$ и группы $1 + P$. Поэтому индекс $(K^\times)^n$ в $K^\times$ является произведением соответствующих индексов для Π, $M^\times$ и $1 + P$. Ясно, что они равны соответственно n, наибольшему общему делителю $(n, q - 1)$ чисел n и $q - 1$ и 1. Доказательство закончено.

Определим теперь структуру $\mathbf{Z}_p$-модуля на группе $1 + P$. Это зависит от характеристики поля K. Если K — поле характеристики нуль, то, как мы уже отмечали, оно является конечным алгебраическим расширением поля $\mathbf{Q}_p$ и его максимальное компактное подкольцо можно рассматривать как $\mathbf{Q}_p$-решетку в K. Теорема 1 из § 2 показывает тогда, что оно есть прямое произведение множителей, изоморфных $\mathbf{Z}_p$, в числе, равном степени K над $\mathbf{Q}_p$.

Предложение 9. *Пусть K — коммутативное p-поле характеристики нуль с максимальным компактным подкольцом R. Тогда существует целое число $m \geqslant 0$, такое, что $1 + P$ как $\mathbf{Z}_p$-модуль (записываемый мультипликативно) изоморфен $\mathbf{Z}_p$-модулю $R \times (\mathbf{Z}_p/p^m\mathbf{Z}_p)$ (записываемому аддитивно). При этом m есть наибольшее целое, такое, что K содержит примитивный корень p^m-й степени из единицы.*

Для произвольных $x \in R$ и $a \in \mathbf{N}$ биномиальную формулу можно записать в виде

$$(1+x)^a = 1 + ax + ax \sum_{i=2}^{a} \binom{a-1}{i-1} x^{i-1}/i.$$

Для $i \geqslant 2$ обозначим через p^h наибольшую степень p, делящую i; если $h = 0$, то $i - 1 > h$; а если $h > 0$, то, поскольку $i \geqslant p^h$, сразу видно, что $i - 1 > h$, за исключением случая $i = p = 2$, так что всегда $2(i - 1) > h$. В написанной выше формуле сумма в последнем члене в правой части принадлежит, следовательно, pR, если $x \in p^2R$. Для $x \in p^2R$, $a \in \mathbf{N}$ это дает

$$(1 + x)^a \equiv 1 + ax \quad (pax R). \tag{3}$$

Это сравнение остается по непрерывности справедливым для всех $x \in p^2R$ и $a \in \mathbf{Z}_p$ ввиду плотности $\mathbf{N}$ в $\mathbf{Z}_p$. Если теперь обозначить через d степень K над $\mathbf{Q}_p$, то по теореме 1 § 2 можно найти базис $\{v_1, \ldots, v_d\}$ в K над $\mathbf{Q}_p$, такой, что $R = \sum \mathbf{Z}_p v_i$. В силу (3) имеем

для всех $1 \leqslant i \leqslant d$, $\nu \geqslant 1$, $a_i \in \mathbf{Z}_p$

$$(1 + p^2 v_i)^{p^{\nu-1} a_i} \equiv 1 + p^{\nu+1} a_i v_i \qquad (p^{\nu+2} R)$$

и, следовательно,

$$(4) \qquad \prod_{i=1}^{d} (1 + p^2 v_i)^{p^{\nu-1} a_i} \equiv 1 + p^{\nu+1} \sum_{i=1}^{d} a_i v_i \qquad (p^{\nu+2} R).$$

Отсюда вытекает, что если $x_1 \in p^2 R$, то мы можем определить по индукции последовательность $(x_1, x_2, \ldots)$ с $x_\nu \in p^{\nu+1} R$, положив для каждого $\nu \geqslant 1$

$$x_\nu = p^{\nu+1} \sum_i a_{\nu i} v_i,$$

где $a_{\nu i} \in \mathbf{Z}_p$, $1 \leqslant i \leqslant d$. Тогда

$$1 + x_{\nu+1} = (1 + x_\nu) \prod_i (1 + p^2 v_i)^{-p^{\nu-1} a_{\nu i}}.$$

Ясно также, что

$$(5) \qquad 1 + x_1 = \prod_i (1 + p^2 v_i)^{b_i},$$

где b_i задается формулой

$$b_i = \sum_{\nu=1}^{+\infty} p^{\nu-1} a_{\nu i},$$

$1 \leqslant i \leqslant d$. Это показывает, что как мультипликативный $\mathbf{Z}_p$-модуль группа $1 + p^2 R$ порождается d элементами $1 + p^2 v_i$; а поскольку она — открытая подгруппа в компактной группе $1 + P$ и потому конечного индекса в ней и поскольку $1 + P$ как $\mathbf{Z}_p$-модуль порождается элементами $1 + p^2 v_i$ и полной системой представителей классов смежности в $1 + P$ по подгруппе $1 + p^2 R$, то $1 + P$ — конечно порожденная группа. Предположим теперь, что (5) может иметь место при $x_1 = 0$ и b_i не всех равных нулю; взяв тогда в качестве $\nu - 1$ наименьший из порядков b_i в $\mathbf{Q}_p$, можно написать $b_i = p^{\nu-1} a_i$, где $\nu \geqslant 1$ и $a_i \in \mathbf{Z}_p$, $1 \leqslant i \leqslant d$, причем не все a_i принадлежат $p\mathbf{Z}_p$. Сравнение (4) дает тогда $\sum a_i v_i \equiv 0$ (pR), т. е. $\sum (p^{-1} a_i) v_i \in R$, что противоречит определению v_i. Это показывает, что $1 + p^2 R$ как $\mathbf{Z}_p$-модуль является свободным модулем, порожденным элементами $1 + p^2 v_i$, и, следовательно, изоморфен $(\mathbf{Z}_p)^d$. Мы можем теперь применить к модулям $1 + P$ и $1 + p^2 R$ следствие 4 теор. 2 § 2. Поскольку их фактормодуль конечен, его ранг равен нулю; а модуль $1 + p^2 R$ как изоморфный $(\mathbf{Z}_p)^d$

есть модуль ранга d. Поэтому $1 + P$ имеет ранг d и изоморфен по следствию 2 теор. 2 § 2 прямому произведению d сомножителей, изоморфных $\mathbf{Z}_p$, и некоторого конечного числа сомножителей, каждый из которых изоморфен модулю вида $\mathbf{Z}_p/p^{\nu}\mathbf{Z}_p$. Поскольку последние суть конечные группы, их произведение совпадает с группой всех элементов конечного порядка в $1 + P$ и потому само есть конечная группа, порядок которой является некоторой степенью p. Отсюда следует, что она есть группа всех корней из единицы в $1 + P$, и притом циклическая группа порядка p^m, где p^m — наибольший из порядков ее элементов (лемма 1 гл. I-1). Таким образом, как $\mathbf{Z}_p$-модуль эта группа изоморфна $\mathbf{Z}_p/p^m\mathbf{Z}_p$. Записав, наконец, $K^{\times}$ в виде прямого произведения Π, $M^{\times}$ и $1 + P$, мы видим, что каждый корень из единицы, степень которого есть некоторая степень p, содержится в $1 + P$. Доказательство закончено.

Следствие. *Пусть K таково, как в предложении* 9. *Тогда для каждого целого $n \geqslant 1$ $(K^{\times})^n$ является открытой подгруппой в $K^{\times}$ конечного индекса, равного $n \cdot (n, r) \cdot \mathrm{mod}_K\,(n)^{-1}$, где r — порядок группы всех корней из единицы в K.*

Ясно, что последняя группа разлагается в прямое произведение $M^{\times}$ и группы порядка p^m, состоящей из корней из единицы в $1 + P$. Следовательно, она циклична и имеет порядок $r = (q - 1)\,p^m$, а $K^{\times}$ есть прямое произведение Π, этой группы и $\mathbf{Z}_p$-модуля, изоморфного R. Далее, nR есть открытая подгруппа в аддитивной группе кольца R, индекс которой в R по определению функции mod_K равен $\mathrm{mod}_K\,(n)^{-1}$. Используя те же соображения, что и в доказательстве предложения 8, немедленно получаем утверждение следствия.

Предложение 10. *Пусть K — коммутативное p-поле характеристики p. Тогда $1 + P$ как $\mathbf{Z}_p$-модуль является прямым произведением бесконечного счетного семейства модулей, изоморфных $\mathbf{Z}_p$.*

По теореме 8 гл. I-4 K можно рассматривать как поле формальных степенных рядов от одной переменной π с коэффициентами в поле $\mathbf{F}_q$ из $q = p^f$ элементов. В данном случае легко явно указать семейство свободных образующих $\mathbf{Z}_p$-модуля $1 + P$. В самом деле, выберем какой-нибудь базис $\{\alpha_1, \ldots, \alpha_f\}$ поля $\mathbf{F}_q$ над простым полем $\mathbf{F}_p$. В качестве образующих модуля $1 + P$ можно взять элементы $1 + \alpha_i\pi^n$, где $1 \leqslant i \leqslant f$, а n пробегает множество всех целых чисел 0, взаимно простых с p. Для каждого $N > 0$ положим $N = np^{\nu}$, где $\nu \geqslant 0$ и n взаимно просто с p. Для произвольных

целых a_i, $1 \leqslant i \leqslant f$, имеем

$$\prod_{i=1}^{f} (1+\alpha_i\pi^n)^{a_i p^\nu} = \prod_i (1+\beta_i\pi^N)^{a_i} \equiv 1+\left(\sum_i a_i\beta_i\right)\pi^N \qquad (P^{N+1}),$$

где $\beta_i = \alpha_i^{p^\nu}$. Так как отображение $x \to x^{p^\nu}$ есть автоморфизм поля $\mathbf{F}_q$ над $\mathbf{F}_p$, то β_i также образуют базис поля $\mathbf{F}_q$ над $\mathbf{F}_p$; следовательно, для произвольного заданного $\alpha \in \mathbf{F}_q$ можно одним и только одним способом выбрать целые числа a_i так, чтобы $0 \leqslant a_i < p$ и $\sum a_i\beta_i = \alpha$. Возьмем теперь какое-нибудь $x_1 \in P$ и определим по индукции последовательность $(x_1, x_2, \ldots)$, где $x_N \in P^N$ при всех $N \geqslant 1$. Для каждого N положим, как и выше, $N = np^\nu$, где n взаимно просто с p, и выберем целые числа a_i так, чтобы $0 \leqslant a_i < p$ для $1 \leqslant i \leqslant f$ и чтобы

$$y_N = \prod_i (1+\alpha_i\pi^n)^{a_i p^\nu} \equiv 1 + x_N \qquad (P^{N+1}).$$

В силу сказанного выше это можно сделать, и притом только одним способом. Положим теперь

$$1 + x_{N+1} = (1 + x_N)\, y_N^{-1}.$$

Сопоставляя эти формулы, сразу видим, что они дают для $1 + x_1$ представление в виде сходящегося бесконечного произведения множителей типа $(1 + \alpha_i\pi^n)b$, где $1 \leqslant i \leqslant f$, n взаимно просто с p и $b \in \mathbf{Z}_p$. Кроме того, из проведенных вычислений следует, что это представление единственно. Наши утверждения доказаны.

§ 4. РЕШЕТКИ НАД R

Понятие решетки в том виде, как оно было развито для p-полей в § 1, 2, неприменимо к R-полям. Подходящим здесь является следующее

Определение 3. *R-решеткой в векторном пространстве V конечной размерности над некоторым* R*-полем называется дискретная подгруппа L в V, такая, что V/L компактно.*

Напомним теперь некоторые элементарные факты о дискретных подгруппах. Пусть G — топологическая группа, Γ — ее дискретная подгруппа и φ — каноническое отображение группы G на G/Γ. Если U — окрестность единичного элемента e в G, такая, что $U^{-1} \cdot U$ не содержит элементов группы Γ, отличных от e, то φ индуцирует на каждом множестве gU с $g \in G$ гомеоморфизм этого множества на его образ в G/Γ. Это можно выразить, сказав, что φ является

«локальным гомеоморфизмом»; если Γ — нормальная подгруппа в G, то можно сказать, что φ является «локальным изоморфизмом», поскольку в этом случае φ переводит групповой закон на G в групповой закон на G/Γ. Предположим, что группа G локально компактна и что на ней задана правоинвариантная мера α. Тогда, как легко видеть, существует одна и только одна мера α' на G/Γ, такая, что для любого измеримого подмножества X в G, взаимно однозначно отображаемого на его образ $\varphi(X) = X'$ в G/Γ, $\alpha'(X')$ равно $\alpha(X)$. Это справедливо, в частности, для любого измеримого подмножества всякого множества вида gU, где U такое же, как и выше. Если теперь f — произвольная непрерывная функция на G с компактным носителем, то

$$\int_G f(g)\, d\alpha(g) = \int_{G/\Gamma} \left(\sum_{\gamma \in \Gamma} f(g\gamma) \right) d\alpha'(\dot{g}). \tag{6}$$

Здесь мы положили $\dot{g} = \varphi(g)$, и подинтегральное выражение в правой части, хотя и записано как функция от g, может рассматриваться как функция от $\dot{g}$, поскольку оно постоянно на классах смежности $g\Gamma$. В самом деле, это очевидно, если носитель функции f содержится в одном из множеств gU, а общий случай сразу следует отсюда. Кроме того, как хорошо известно из теории интегрирования, справедливость равенства (6) для всех непрерывных функций с компактным носителем влечет его справедливость для всех интегрируемых функций и для всех измеримых функций со значениями в $\mathbf{R}_+$. Ясно, что мера α' инвариантна относительно действия группы G на G/Γ в том и только в том случае, когда мера α левоинвариантна; это, в частности, всегда так, когда множество G/Γ компактно, ибо тогда G/Γ является множеством конечной меры, инвариантной относительно действия группы G. Если при этом подгруппа Γ нормальна в G, то α' есть мера Хаара на G/Γ.

В описанной выше ситуации мера α' называется *образом* меры α в G/Γ, и мы будем обозначать ее просто через α, если это не сможет вызвать недоразумений. Следующая лемма (играющая роль утверждения, которое в классической теории чисел известно как теорема Минковского) теперь очевидна.

Лемма 1. *Пусть G — локально компактная группа с мерой Хаара α, Γ — ее дискретная подгруппа, такая, что множество G/Γ компактно, и X — измеримое подмножество в G, для которого $\alpha(X) > \alpha(G/\Gamma)$. Тогда существуют два различных элемента x, x' из X, такие, что $x^{-1}x' \in \Gamma$.*

Нужно только заметить, что поскольку G/Γ компактно, каждая правоинвариантная мера на G также левоинвариантна и, следо-

вательно, мера Хаара α является двусторонне-инвариантной, а ее образ на G/Γ корректно определен.

Лемма 2. *Пусть G, α и Γ таковы, как в лемме 1, и пусть Γ_1 — дискретная подгруппа группы G, содержащая Γ. Тогда Γ имеет конечный индекс в Γ_1, и этот индекс определяется соотношением*

$$\alpha(G/\Gamma) = [\Gamma_1 : \Gamma]\,\alpha(G/\Gamma_1).$$

Поскольку множество G/Γ компактно, существует непрерывная функция $f_0 \geqslant 0$ на G с компактным носителем, такая, что для всех $g \in G$

$$f_1(g) = \sum_{\gamma\in\Gamma} f_0(g\gamma) > 0.$$

Функция $f = f_0/f_1$ непрерывна на G, имеет тот же носитель, что и f_0, и такова, что сумма $\sum f(g\gamma)$, где суммирование производится по всем $\gamma \in \Gamma$, равна 1 при всех g. Из этого факта вытекает, что аналогичная сумма, взятая по всем $\gamma \in \Gamma_1$, имеет постоянное значение $[\Gamma_1 : \Gamma]$. Применив теперь к G, f и Γ, а также к G, f и Γ_1 формулу (6), получим утверждение нашей леммы.

Выведем теперь из этих фактов следующий классический результат об R-решетках.

Предложение 11. *Пусть L — подгруппа векторного пространства V размерности n над* R. *Следующие три утверждения эквивалентны*: (i) *L является* R*-решеткой в V*; (ii) *L дискретна в V, конечно порождена и содержит базис (v_i) пространства V над* R; (iii) *в V существует базис над* R, *порождающий группу L.*

Пусть имеет место (iii). Рассмотрим изоморфизм

$$(x_1, \ldots, x_n) \to \sum x_i v_i \tag{7}$$

из $\mathbf{R}^n$ на V. Подгруппа L является образом подгруппы $\mathbf{Z}^n$ относительно этого изоморфизма и потому дискретна в V, а факторгруппа V/L изоморфна $(\mathbf{R}/\mathbf{Z})^n$ и потому компактна. Таким образом, (iii) влечет (i) и (ii). Предположим теперь, что выполняется (i). Пусть W — подпространство в V, порожденное решеткой L, а W' — дополнительное к W подпространство в V. Как локально компактная группа V есть прямое произведение W и W', а L есть дискретная подгруппа в W. Следовательно, факторпространство V/L изоморфно прямому произведению W/L и W' и, значит, не может быть компактным, если W' не является таковым. Поэтому W' должно равняться $\{0\}$, а $W = V$, так что L содержит базис про-

странства V над $\mathbf{R}$. Пусть теперь α — мера Хаара на V, для которой $\alpha(V/L) = 1$. Для каждого базиса $B = \{v_1, \ldots, v_n\}$ в V, содержащегося в L, обозначим через φ_B изоморфизм $\mathbf{R}^n$ на V, определяемый формулой (7); он отображает $\mathbf{Z}^n$ на подрешетку L_B в L, порожденную B, а меру Лебега λ на $\mathbf{R}^n$ — в некоторое скалярное кратное $m_B^{-1}\alpha$ меры α. Так как $\lambda(\mathbf{R}^n/\mathbf{Z}^n) = 1$, то имеем $m_B^{-1}\alpha(V/L_B) = 1$. По лемме 2 отсюда следует, что m_B является индексом L_B в L. Выберем теперь B так, чтобы этот индекс имел наименьшее возможное значение, и покажем, что тогда $L_B = L$. Действительно, допустим, что L содержит вектор w, не лежащий в L_B, и запишем его в виде $w = \sum a_i v_i$ с коэффициентами a_i из $\mathbf{R}$. Поскольку w не принадлежит L_B, по крайней мере один из коэффициентов, например a_1, не лежит в $\mathbf{Z}$. Заменяя w на $w - mv_1$, где $m \in \mathbf{Z}$, $m < a_1 < m + 1$, видим, что можно считать, что $0 < a_1 < 1$. Пусть теперь $v_i' = w$, $v_i' = v_i$ для $2 \leqslant i \leqslant n$, и $B' = \{v_1', \ldots, v_n'\}$. Ясно, что B' является базисом пространства V, содержащимся в L. Тривиальное вычисление показывает, что $\varphi_B^{-1} \circ \varphi_{B'}$ является автоморфизмом пространства $\mathbf{R}^n$, задаваемым формулой

$$(x_1, \ldots, x_n) \to (a_1 x_1,\ x_2 + a_2 x_1,\ \ldots,\ x_n + a_n x_1),$$

причем модуль этого автоморфизма равен a_1 (см. следствие 3 теоремы 3 гл. I-2). Возьмем какое-нибудь измеримое подмножество X в $\mathbf{R}^n$ и положим $Y = \varphi_{B'}(X)$ и $Y' = \varphi_{B'}(X)$. По определению m_B, $m_{B'}$ имеем $\alpha(Y) = m_B \lambda(X)$, $\alpha(Y') = m_{B'}\lambda(X)$ и, следовательно, модуль автоморфизма $\varphi_{B'} \circ \varphi_B^{-1}$, отображающего Y на Y', равен $m_{B'}/m_B$. Поскольку автоморфизм $\varphi_{B'} \circ \varphi_B^{-1}$ можно записать в виде $\varphi_{B'} \circ (\varphi_B^{-1} \circ \varphi_{B'}) \circ \varphi_B^{-1}$, у него тот же самый модуль, что и у автоморфизма $\varphi_B^{-1} \circ \varphi_{B'}$. Это дает $m_{B'}/m_B = a_1 < 1$, что противоречит определению B. Таким образом, (i) влечет (ii) и (iii), и доказательство завершено.

§ 5. ДВОЙСТВЕННОСТЬ НАД ЛОКАЛЬНЫМИ ПОЛЯМИ

К числу наиболее важных свойств коммутативных локально компактных групп принадлежат те свойства, которые образуют содержание так называемой теории двойственности. Напомним, что если G — такая группа, то ее *характером* (в смысле этой теории) называется непрерывный гомоморфизм из G в мультипликативную группу комплексных чисел, по модулю равных единице. Если g^* — характер, то его значение в точке g группы G обычно обозначается через $\langle g, g^* \rangle_G$, а иногда просто через $\langle g, g^* \rangle$, если это не может вызвать недоразумений. Будем записывать групповой закон

в G аддитивно. Введем на множестве G^* характеров группы G коммутативную групповую структуру, также записываемую аддитивно, положив

$$\langle g, g_1^* + g_2^* \rangle_G = \langle g, g_1^* \rangle_G \cdot \langle g, g_2^* \rangle_G.$$

Отметим, что единичный элемент группы G^*, который обозначается в аддитивной записи нулем, соответствует *тривиальному* характеру группы G, принимающему во всех точках значение 1. Можно топологизировать группу G^*, снабдив ее топологией равномерной сходимости на компактных подмножествах в G. Группа G^* превращается таким образом в локально компактную группу, именуемую *топологической двойственной* к группе G, или просто двойственной к ней, если это не может привести к путанице. Обратно, характеры группы G^* суть функции $g^* \to \langle g, g^* \rangle_G$, определяемые элементами $g \in G$, и это соответствие определяет изоморфизм между G и двойственной к G^*. Иначе говоря, положив

$$\langle g^*, g \rangle_{G^*} = \langle g, g^* \rangle_G,$$

мы можем отождествить G с двойственной к G^*, и в дальнейшем всегда будет предполагаться, что они отождествлены таким образом. Группа G компактна в том и только том случае, когда группа G^* дискретна, а посему G дискретна тогда и только тогда, когда G^* компактна.

Пусть H — произвольная замкнутая подгруппа в G. Характеры группы G, индуцирующие тривиальный характер на H, образуют замкнутую подгруппу в G^*, которая будет обозначаться через H_*. Будем говорить, что подгруппа H_* *ассоциирована с H по двойственности*. Она изоморфна группе, двойственной к G/H. В случае когда G рассматривается как двойственная к G^*, подгруппа в G, ассоциированная с H_*, есть сама подгруппа H, которая, следовательно, изоморфна двойственной к G^*/H_*. Так как H открыта в G в том и только в том случае, когда G/H дискретна, видим, что это имеет место тогда и только тогда, когда H_* компактна. Таким образом H_* открыта в G^* в том и только в том случае, когда группа H компактна. Аналогично H дискретна в том и только в том случае, когда G^*/H_* компактна, и G/H компактна тогда и только тогда, когда группа H_* дискретна.

Все это применимо к аддитивной группе произвольного левого векторного пространства V конечной размерности над недискретным локально компактным полем K (коммутативным или нет). В этом случае, если V^* — топологическое двойственное к V и $v^* \in V^*$, то для каждого $a \in K$ функция $v \to \langle av, v^* \rangle_V$ является, очевидно, характером группы V, который будет обозначаться через v^*a.

Обращаясь к определениям, немедленно находим, что V^* превращается тем самым в правое векторное пространство над K. В силу следствия 2 теор. 3 гл. I-2 размерность V^* должна быть конечна. Иными словами, структура V^* как правого векторного пространства над K задается формулой

$$\langle av, v^* \rangle_V = \langle v, v^* a \rangle_V. \tag{8}$$

Обратно, если V и V^* — двойственные группы и V^* имеет структуру правого векторного пространства над K, то можно использовать формулу (8) для того, чтобы определить V как левое векторное пространство над K. Итак, мы можем отождествлять V с двойственным к V^*, даже если рассматривать их как векторные пространства над K. Если L — произвольная замкнутая подгруппа в V, то подгруппа L_*, ассоциированная с L по двойственности, состоит из тех элементов v^* из V^*, для которых $\langle v, v^* \rangle_V = 1$ при всех $v \in L$. С учетом формулы (8) отсюда следует, что если L — левый модуль над некоторым подкольцом поля K, то L_* является правым модулем над тем же самым подкольцом, и обратно. В частности, если K — некоторое p-поле и R — его максимальное компактное подкольцо, то L есть левый R-модуль тогда и только тогда, когда L_* — правый R-модуль. Поскольку, как мы видели, L компактен и открыт в V тогда и только тогда, когда L_* таков же в V^*, получаем, что L является K-решеткой в том и только в том случае, когда L_* есть K-решетка. В случае когда это так, будем говорить, что K-решетки L и L_* *двойственны* друг другу; при этом aL и $L_* a^{-1}$ двойственны друг другу при каждом $a \in K^\times$. С другой стороны, ясно, что если K есть $\mathbf{R}$, $\mathbf{C}$ или $\mathbf{H}$, то L является $\mathbf{R}$-решеткой тогда и только тогда, когда L_* есть $\mathbf{R}$-решетка.

Далее, если V таково, как выше, можно рассматривать его *алгебраическое двойственное* V', которое является пространством K-линейных форм на V. Как хорошо известно, если обозначить через $[v, v']_V$ значение в точке v линейной формы v' на пространстве V, то можно наделить V' «естественной» структурой правого векторного пространства над K с помощью формулы

$$[av, v'b]_V = a\,[v, v']_V\,b,$$

выполняющейся для всех $v \in V$, $v' \in V'$ и всех $a, b \in K$. Если χ — какой-нибудь характер аддитивной группы поля K, то для каждого $v' \in V'$ существует элемент v^* из топологического двойственного V^*, для которого $\langle v, v^* \rangle_V = \chi([v, v']_V)$ при всех $v \in V$. Используем это, чтобы установить связь между алгебраическим и топологическим двойственными.

Теорема 3. *Пусть K — недискретное локально компактное поле, V — левое векторное пространство конечной размерности n над K, и пусть χ — нетривиальный характер аддитивной группы поля K. Тогда топологическое двойственное V^* является правым векторным пространством размерности n над K и формула*

$$\langle v, v^* \rangle_V = \chi([v, v']_V) \text{ для всех } v \in V$$

определяет биективное отображение $v' \to v^*$ алгебраического двойственного V' к V в пространство V^*. Если $\chi(xy) = \chi(yx)$ для всех x, y из K, то это отображение является изоморфизмом структур V' и V^* как правых векторных пространств над K.

Пусть X_K — топологическое двойственное к K. Структура K как левого векторного пространства размерности 1 над самим собой определяет структуру правого векторного пространства на X_K; в качестве такового оно имеет конечную размерность d. Подобным образом структура K как правого векторного пространства над K определяет на X_K структуру левого векторного пространства над K некоторой размерности d'. Пусть V таково, как в теореме 3. Выбрав какой-нибудь его базис над K, представим пространство V в виде прямой суммы n подпространств размерности 1. Его двойственное V^* изоморфно, следовательно, как правое векторное пространство, прямой сумме n подпространств, изоморфных X_K, и имеет потому размерность nd. Аналогично двойственное к V^* есть левое векторное пространство размерности ndd', и так как оно изоморфно V, с которым мы договорились его отождествлять, получаем, что $ndd' = n$ и $d = d' = 1$. Пусть характер χ таков, как в теореме 3; он определяет элемент $c^* \neq 0$ в аддитивно записываемой группе X_K, так что $\chi(t) = \langle t, c^* \rangle_K$ для всех $t \in K$. Поскольку $d' = 1$, каждый элемент из X_K можно однозначно записать в виде xc^*, где $x \in K$, и поскольку $d = 1$, каждый элемент из X_K однозначно записывается как c^*y с $y \in K$. Отношение $xc^* = c^*y$ определяет тем самым биекцию α поля K на себя, и немедленно проверяется, что она является автоморфизмом поля. В силу (8) c^*y является характером $t \to \chi(yt)$ поля K и аналогично xc^* является характером $t \to \chi(tx)$. Таким образом, $\chi(tx) = \chi(\alpha(x)\, t)$ для всех x, t из K, чем автоморфизм α и определяется однозначно. В частности, он тождествен на центре поля K и тождествен везде, если $\chi(tx) = \chi(xt)$ для всех x, t из K. Рассмотрим теперь отображение $v' \to v^*$ из V' в V^*, определенное в теореме 3. Выберем $x \in K$, положим $w' = v'x$ и предположим, что исследуемое отображение переводит w' в w^*. Имеем

$$\chi([v, w']_V) = \chi([v, v']_V x) = \chi(\alpha(x)\,[v, v']_V) = \chi([\alpha(x)\, v, v']_V).$$

Ввиду определения v^* и w^* это дает

$$\langle v, w^* \rangle_V = \langle \alpha(x)\, v, v^* \rangle_V = \langle v, v^* \alpha(x) \rangle_V$$

для всех v и, значит, $w^* = v^* \alpha(x)$. Этот факт обычно выражают, говоря, что отображение $v' \to v^*$ *α-полулинейно*. В то же время ясно, что это отображение инъективно. Действительно, равенство $v^* = 0$ означает, что $\chi([v, v']_V)$ равно 1 для всех $v \in V$ и, следовательно, $\chi(x[v, v']_V)$ равно 1 для всех $x \in K$ и всех $v \in V$, а поскольку характер χ нетривиален, отсюда следует, что $[v, v']_V = 0$ при всех v, т. е. $v' = 0$. Так как V' и V^* имеют одинаковую размерность n над K, α-полулинейное отображение из V' в V^* не может быть инъективным, не будучи биективным. Тем самым доказательство закончено.

Для удобства ссылок сформулируем отдельно результат о характерах поля K.

Следствие. *Пусть K и χ таковы, как в теореме 3. Тогда каждый характер поля K может быть записан, и притом единственным образом, в виде $t \to \chi(tx)$, где $x \in K$, или в виде $t \to \chi(yt)$, где $y \in K$.*

Можно было бы сформулировать теорему 3 более «внутренним» образом, сказав, что существует канонический изоморфизм между V^* и тензорным произведением $V^* \otimes_K X_K$, задаваемый формулой из теоремы 3 (и аналогично канонический изоформизм между V^* и $X_K \otimes_K V'$, если V несет структуру правого векторного пространства). Мы предоставляем читателю самому убедиться в этом. Следует также отметить, что всегда существует нетривиальный характер поля K, для которого $\chi(xy) = \chi(yx)$ при всех $x, y \in K$; можно взять, например, $\chi = \chi_0 \circ \tau$, где τ — «приведенный след» в K над центром K_0 (см. гл. IX-2), а χ_0 — нетривиальный характер в K_0. Тот же результат можно было бы вывести и из того факта, что, согласно теореме Сколема — Нётер (которая появится ниже как предложение 4 в гл. IX-1), отображение α из доказательства теоремы 3 должно быть внутренним автоморфизмом поля K. Конечно, различение правого и левого становится совершенно излишним, если рассматриваются только коммутативные поля.

Обычно подразумевается, что раз и навсегда выбран некий характер поля K со свойствами, описанными в теореме 3, чтобы отождествить, с помощью описанного в теореме изоморфизма, топологические и алгебраические двойственные всех векторных пространств над K. При этом χ обычно именуется *базисным характером*. В частности, как показано в следствии теоремы 3, можно при этом отождествлять поле K с его топологическим двойственным.

В случае когда это делается для p-поля K, подгруппа в K, ассоциированная по двойственности с подгруппой вида P^n, должна быть подгруппой того же вида, поскольку вообще двойственное к K-решетке является K-решеткой. Чтобы сформулировать более точное утверждение, введем следующее определение.

Определение 4. *Пусть K — некоторое p-поле, R — его максимальное компактное подкольцо и P — максимальный идеал в R. Порядком нетривиального характера χ поля K называется наибольшее целое число $\nu \in \mathbf{Z}$, такое, что χ равен 1 на $P^{-\nu}$; порядок характера χ будет обозначаться через* $\mathrm{ord}\,(\chi)$.

Иными словами, $P^{-\nu}$ есть двойственная к R K-решетка, если K отождествляется со своим двойственным при помощи χ. Это показывает, что ν конечно.

Предложение 12. *Пусть K — некоторое p-поле, χ — его нетривиальный характер порядка ν. Тогда для любого $n \in \mathbf{Z}$ $\chi(xt) = 1$ при всех $t \in P^n$ в том и только в том случае, когда $x \in P^{-n-\nu}$.*

Это утверждение очевидно. Его можно выразить, сказав, что двойственная к P^n K-решетка есть $P^{-n-\nu}$, если K отождествляется со своим двойственным при помощи χ.

Что касается явной конструкции характеров локальных полей, то для случая поля $\mathbf{R}$ она хорошо известна; в качестве базисного характера можно взять характер, задаваемый формулой $\chi_0(x) = \mathbf{e}(x) = e^{2\pi i x}$. В $\mathbf{C}$ или $\mathbf{H}$ можно взять в качестве базисного любой характер вида $\chi_0 \circ f$, где f — любая отличная от нуля линейная $\mathbf{R}$-форма (например, след над $\mathbf{R}$). Если K — локальное поле характеристики p, его можно представить как поле формальных степенных рядов $x = \Sigma\, a^i T^i$ с коэффициентами из $\mathbf{F}_q$, и в качестве базисного можно взять характер порядка 0, определяемый равенством $\chi(x) = \psi(a_{-1})$, где ψ — какой-нибудь нетривиальный характер аддитивной группы поля $\mathbf{F}_q$. Для $\mathbf{Q}_p$ явная конструкция будет дана в гл. IV-2; она является частью доказательства теоремы 3 этой главы.

ГЛАВА ТРЕТЬЯ

ТОЧКИ А-ПОЛЕЙ

§ 1. А-ПОЛЯ И ИХ ПОПОЛНЕНИЯ

Под *полем алгебраических чисел* обычно понимают всякое конечное алгебраическое расширение поля $\mathbf{Q}$. Основной задачей этой книги, и вообще теории чисел, является изучение полей алгебраических чисел с помощью их вложений в локальные поля. За последнее столетие было, однако, обнаружено, что методы, которые при этом используются, могут быть с очень небольшими изменениями применены к некоторым полям характеристики $p > 1$, причем одновременное изучение этих двух типов полей проливает дополнительный свет на каждый из них. Учитывая это, приведем теперь определение полей, которые и будем, начиная с этого места, изучать.

Определение 1. *Поле называется* **А**-*полем, если оно является или конечным алгебраическим расширением поля* $\mathbf{Q}$, *или конечно порожденным расширением конечного простого поля* $\mathbf{F}_p$, *имеющего над* $\mathbf{F}_p$ *степень трансцендентности* 1.

Итак, если k есть **А**-поле характеристики $p > 1$, оно должно содержать трансцендентный над $\mathbf{F}_p$ элемент t и, следовательно, является конечным алгебраическим расширением поля $\mathbf{F}_p(t)$. Таким образом, если обозначить раз и навсегда независимую переменную через T, так что $\mathbf{F}_p(T)$ есть поле рациональных функций от T с коэффициентами в $\mathbf{F}_p$, то **А**-полями характеристики p будут в точности те поля, которые суть конечные алгебраические расширения поля $\mathbf{F}_p(T)$. Заметим, что такое поле всегда содержит бесконечно много полей, изоморфных $\mathbf{F}_p(T)$.

Мы будем изучать **А**-поля, вкладывая их в локальные поля. В силу теорем 5 и 8 гл. I возможно говорить о множестве всех локальных полей, рассматриваемых с точностью до изоморфизма. В самом деле, для заданного $p > 1$ локальные поля характеристики p находятся, с точностью до изоморфизма, во взаимно однозначном соответствии с конечными полями $\mathbf{F}_q$ из $q = p^n$ элементов, в то

время как локальные p-поля характеристики 0 изоморфны подполям алгебраического замыкания поля $\mathbf{Q}_p$, имеющим конечную степень над $\mathbf{Q}_p$. Позже мы установим (как следствие леммы 1 гл. XI-3), что полей последнего типа лишь счетное число, но здесь это нам не понадобится. Теперь имеет смысл следующее определение, позволяющее говорить о множестве точек A-полей.

Определение 2. *Пусть* λ *— изоморфное вложение* A*-поля* k *в локальное поле* K. *Пара* (λ, K) *называется пополнением поля* k, *если* $\lambda(k)$ *плотно в* K. *Два пополнения* (λ, K) *и* (λ', K') *поля* k *называются эквивалентными, если существует такой изоморфизм* ρ *поля* K *на* K', *что* $\lambda' = \rho \circ \lambda$. *Под точкой поля* K *будем понимать класс эквивалентности его пополнений.*

Определение 3. *Точка* A*-поля* k, *определяемая пополнением* (λ, K), *называется вещественной, если поле* K *изоморфно* $\mathbf{R}$; *мнимой, если* K *изоморфно* $\mathbf{C}$; *бесконечной в обоих этих случаях и конечной в остальных случаях.*

Пусть v — точка поля k. Очевидно, что функция $\mathrm{mod}_K \circ \lambda$ на k одна и та же для всех пополнений (λ, K), принадлежащих v. Будем записывать ее в виде $x \to |x|_v$. Если v — мнимая точка, то $\mathrm{mod}_K (x - y)^{1/2}$ является метрикой на K, во всех остальных случаях это верно для $\mathrm{mod}_K (x - y)$. Следовательно, мы всегда можем получить пополнение поля k, принадлежащее к v, взяв пополнение относительно метрики $|x - y|_v^{\alpha}$, где $\alpha = 1/2$, если v мнимо, и $\alpha = 1$ в остальных случаях. Это пополнение будет обозначаться через k_v и называться *пополнением поля* k *в точке* v. Для всех $x \in k_v$ положим $|x|_v = \mathrm{mod}_{k_v}(x)$. Если v — конечная точка, то мы будем обозначать через r_v максимальное компактное подкольцо поля k_v, а через p_v — его максимальный идеал. Это — подмножества в k_v, задаваемые соответственно условиями $|x|_v \leqslant 1$ и $|x|_v < 1$.

Как видно из теоремы 5 гл. I-2, поле $\mathbf{Q}$ имеет одну бесконечную точку, соответствующую вложению $\mathbf{Q}$ в поле $\mathbf{R} = \mathbf{Q}_\infty$; эта точка будет обозначаться через ∞. Та же теорема показывает, что конечные точки поля $\mathbf{Q}$ находятся во взаимно однозначном соответствии с рациональными простыми числами, с которыми их можно отождествить. Точке p соответствует вложение $\mathbf{Q}$ в $\mathbf{Q}_p$.

Знание точек поля $\mathbf{Q}$ является для нас исходным пунктом при определении точек полей алгебраических чисел, рассматриваемых как конечные алгебраические расширения поля $\mathbf{Q}$. Для того чтобы тем же методом исследовать A-поля характеристики $p > 1$, нужно знать точки поля $\mathbf{F}_p(T)$. Прежде чем заниматься их нахож-

дением, приведем ряд общих результатов о точках алгебраических расширений.

Предложение 1. *Пусть k — произвольное поле, k_0 — его бесконечное подполе и λ — изоморфное вложение k_0 в локальное поле K. Замыкание K_0 множества $\lambda(k_0)$ в K является локальным полем, и замыкание множества $\lambda(k)$ в K есть поле, порожденное $\lambda(k)$ над K_0.*

Первое утверждение сразу вытекает из следствия 3 предл. 2 гл. I-2. По следствию 2 теор. 3 гл. I-2 K должно поэтому иметь конечную степень над K_0, так что в силу теоремы 3 гл. I-2 каждое векторное пространство над K_0, содержащееся в поле K, замкнуто в нем. Поле K_1, порожденное $\lambda(k)$ над K_0, является таким подпространством. С другой стороны, очевидно, что замыкание множества $\lambda(k)$ в K есть поле, содержащее $\lambda(k_0)$, а значит, и K_0 и $\lambda(k)$. Таким образом, оно совпадает с K_1.

Следствие. *Пусть k — некоторое* А*-поле, k' — его конечное алгебраическое расширение и w — точка поля k'. Пусть, далее, λ — естественное вложение поля k' в его пополнение k в w. Тогда k'_w есть конечное алгебраическое расширение замыкания $\lambda(k)$ в k'_w и вложение поля k в это замыкание, индуцируемое вложением λ, определяет точку v поля k.*

В силу наших определений это частный случай предложения 1.

Мы имеем теперь возможность ввести следующее определение.

Определение 4. *Если k и k' таковы, как в следствии предложения* 1, *то говорят, что v — точка поля k, лежащая под w, а w — точка, лежащая над v, и пишут $w \mid v$.*

В описанной ситуации мы будем обычно отождествлять поле k_v с замыканием поля k в k'_w.

Теорема 1. *Пусть k — какое-нибудь* А*-поле, k' — его алгебраическое расширение и v — его точка. Тогда существует точка поля k', лежащая над v, и таких точек может быть лишь конечное число.*

Пусть K — алгебраическое замыкание поля k_v и k'' — алгебраическое замыкание поля k в K. Так как k'' — алгебраически замкнуто, существует по меньшей мере один изоморфизм λ над k из k' в k''. Обозначим через K_λ поле, порожденное над k_v множеством $\lambda(k')$; оно является конечным алгебраическим расширением поля k_v, и потому его можно наделить структурой топологического векторного пространства конечной размерности над k_v (следствие 1

теор. 3 гл. I-2). Тем самым оно превращается в локальное поле. Но тогда по предложению 1 (λ, K_λ) есть пополнение поля k' и определяет точку в k', которая, очевидно, лежит над v. Обратно, пусть w — какая-нибудь точка поля k', лежащая над v. Тогда по следствию предл. 1 существует по меньшей мере один изоморфизм φ над k_v поля k'_w в K. Пусть λ — изоморфизм из k' в K, индуцируемый на k' морфизмом φ. Ясно, что λ отображает k' в k''. В силу предложения 1 поле k'_w порождается над k_v множеством k', так что поле $\varphi(k'_w)$ — это то же самое поле, которое обозначалось выше через K_λ. Далее, снова используя следствие 1 теор. 3 гл. I-2, получаем, что φ есть топологический изоморфизм поля k'_w на K_λ, так что w — та точка поля k', которая определяется пополнением (λ, K_λ). Итак, точек поля k', лежащих над v, существует столько же, сколько имеется различных изоморфизмов λ над k из поля k' в k''. Но хорошо известно (и легко доказывается), что поскольку k' — конечное алгебраическое расширение поля k, таких изоморфизмов существует лишь конечное число.

Следствие. *Всякое* **A**-*поле имеет не более чем конечное число бесконечных точек; оно имеет по меньшей мере одну такую точку, если его характеристика равна нулю, и ни одной в противном случае.*

Последнее утверждение очевидно. Остальные суть частные случаи теоремы 1, ибо точка **A**-поля характеристики 0 бесконечна в том и только в том случае, когда она лежит над точкой ∞ поля $\mathbf{Q}$.

Перейдем теперь к нахождению точек поля $\mathbf{F}_p(T)$. Более общим образом мы определим все точки полей $\mathbf{F}_q(T)$, где $\mathbf{F}_q$ — произвольное конечное поле. Удобно говорить, что многочлен π из $\mathbf{F}_q[T]$ *прост*, если он унитарен, неприводим в кольце $\mathbf{F}_q[T]$ и имеет степень >0.

Теорема 2. *Поле* $k = \mathbf{F}_q(T)$ *имеет одну и только одну точку* v, *для которой* $|T|_v > 1$; *в этой точке* T^{-1} *является простым элементом поля* k_v *и модуль поля* k_v *равен* q. *Для каждого простого многочлена* π *из* $\mathbf{F}_q[T]$ *поле* k *имеет одну и только одну точку* v, *такую, что* $|\pi|_v < 1$; *в этой точке* π *является простым элементом поля* k_v, *модуль которого равен* q^δ, *где* δ — *степень многочлена* π. *Все эти точки различны, и поле* k *не имеет других точек.*

Пусть v — точка поля k. Предположим сначала, что $|T|_v \leqslant 1$. Тогда $\mathbf{F}_q[T]$ содержится в r_v. Обозначим через ρ канонический гомоморфизм кольца r_v на конечное поле r_v/p_v; он индуцирует на $\mathbf{F}_q[T]$ гомоморфизм кольца $\mathbf{F}_q[T]$ на его образ, ядро которого $p_v \cap \mathbf{F}_q[T]$ является, очевидно, простым идеалом в $\mathbf{F}_q[T]$.

Поскольку кольцо $\mathbf{F}_q[T]$ бесконечно, а поле r_v/p_v конечно, этот идеал не может равняться $\{0\}$ и, следовательно, является идеалом $\pi \cdot \mathbf{F}_q[T]$, порожденным в $\mathbf{F}_q[T]$ некоторым простым многочленом π. Поэтому $|\pi|_v < 1$ и $|\alpha|_v = 1$ для каждого многочлена α из $\mathbf{F}_q[T]$, взаимно простого с π. Каждое $\xi \in k^\times$ можно записать в виде $\xi = \pi^n \alpha/\alpha'$, где $n \in \mathbf{Z}$, а α, α' — многочлены из $\mathbf{F}_q[T]$, взаимно простые с π. При этом $|\xi|_v = |\pi|_v^n$. В частности, ξ принадлежит r_v тогда и только тогда, когда $n \geqslant 0$, т. е. когда его можно записать в виде $\xi = \beta/\alpha$, где α, β — многочлены из $\mathbf{F}_q[T]$, причем α взаимно прост с π. Так как $\mathbf{F}_q(T)$ плотно в k_v, области значений, принимаемых функцией $|x|_v$ на $\mathbf{F}_q(T)$ и на k_v, совпадают между собой. Отсюда следует, что π — простой элемент поля k_v. Пусть теперь δ — степень многочлена π. Образ кольца $\mathbf{F}_q[T]$ в r_v/p_v изоморфен полю $\mathbf{F}_q[T]/\pi \cdot \mathbf{F}_q[T]$, которое есть расширение поля $\mathbf{F}_q$ степени δ и состоит потому из q^δ элементов. Ясно, что образ каждого элемента кольца $r_v \cap \mathbf{F}_q(T)$ должен принадлежать этому же полю, которое, поскольку $\mathbf{F}_q(T)$ плотно в k_v, является не чем иным, как полем r_v/p_v. Это показывает, что модуль поля k_v равен q^δ и $|\pi|_v = q^{-\delta}$. Таким образом, функция $|\xi|_v$ на поле k однозначно определяется заданием π, так что при заданном π существует самое большее одна точка v поля k, свойства которой мы только что описали. Предположим теперь, что $|T|_v > 1$. Тогда $|T^{-1}|_v < 1$, и можно поступить точно так же, как и выше, заменив $\mathbf{F}_q[T]$ на $\mathbf{F}_q[T^{-1}]$ и π на T^{-1}. Легко видеть, что если $\xi = \beta/\alpha$, где многочлены β и α из $\mathbf{F}_q[T]$ отличны от нуля и имеют степени соответственно b и a, то $|\xi|_v = q^{b-a}$. Теперь ясно, что если π — простой многочлен, то $|\pi|_v$ не может быть <1, за исключением точки v, описанной выше (если таковая существует), и что то же самое верно для T^{-1}. Докажем существование таких точек. Разберем сначала случай $\pi = T$. Кольцо $\mathbf{F}_q[T]$ можно в этом случае вложить очевидным образом в кольцо формальных степенных рядов $\sum_0^\infty a_i T^i$ с коэффициентами из $\mathbf{F}_q$. Ясно, что, расширяя это вложение на соответствующие поля, можно получить точку поля k, отвечающую многочлену $\pi = T$. Заменяя T на T^{-1}, видим, что то же самое верно для T^{-1}. Возьмем теперь какой-нибудь простой многочлен π степени δ. Поле $\mathbf{F}_q(T)$ содержит $\mathbf{F}_q(\pi)$ и алгебраично над ним. Его степень d над $\mathbf{F}_q(\pi)$ не превосходит δ. Как мы только что доказали, в $\mathbf{F}_q(\pi)$ существует точка w, для которой $|\pi|_w = q^{-1}$. В силу теоремы 1 поле $\mathbf{F}_q(T)$ имеет точку v, лежащую над w. По следствию 2 теор. 3 гл. I-2 имеем $|\pi|_v = |\pi|_w^d = q^{-d}$. Это завершает доказательство, показывая одновременно, что $d = \delta$.

Следствие. *В обозначениях теоремы* 2 *пусть* v *— точка поля* k, *соответствующая простому многочлену* π *степени* δ. *Тогда многочлены степени* $<\delta$ *из* $\mathbf{F}_q[T]$ *образуют полную систему представителей классов смежности кольца* r_v *по модулю идеала* p_v.

Это сразу следует из доказанного выше и из того факта, что эти многочлены образуют полную систему представителей классов кольца $\mathbf{F}_q[T]$ по модулю π.

Условимся, начиная с этого места, говорить, что свойство, относящееся к точке некоторого A-поля, выполняется *почти для всех* (или *для почти всех*) *точек из* k (или выполняется *почти всюду*, в случае когда последнее выражение не может привести к недоразумениям), если оно верно для всех точек, кроме, быть может, конечного числа. Это соглашение используется, например, в формулировке нашего следующего результата.

Теорема 3. *Пусть* k *— некоторое* A*-поле и* ξ *— какой-нибудь его элемент. Тогда* $|\xi|_v \leqslant 1$ *почти для всех точек поля* k.

Если $k = \mathbf{Q}$, то это очевидно, ибо в этом случае ξ можно записать в виде a/b, где a, b — элементы из $\mathbf{Z}$, причем $b \neq 0$ и $|\xi|_p \leqslant 1$ для всех простых p, не делящих b. Пусть теперь k — какое-нибудь A-поле характеристики 0, т. е. поле алгебраических чисел. Тогда ξ удовлетворяет уравнению

$$\xi^n + a_1\xi^{n-1} + \ldots + a_n = 0,$$

коэффициенты которого a_i принадлежат $\mathbf{Q}$. Пусть P — конечное множество, состоящее из ∞ и всех простых чисел, встречающихся в знаменателях чисел a_i. По теореме 1 множество P' точек поля k, лежащих над точками из P, конечно. Выберем какую-нибудь точку v поля k, не принадлежащую P'. Тогда точка p поля $\mathbf{Q}$, лежащая под v, не принадлежит P и, следовательно, $|a_i|_p \leqslant 1$ для $1 \leqslant i \leqslant n$. Таким образом, ξ — целый элемент над $\mathbf{Z}_p$. Ввиду предложения 6 гл. I-4 отсюда следует, что ξ находится в r_v, т. е. $|\xi|_v \leqslant 1$. Что касается A-полей характеристики $p > 1$, то к ним применимо аналогичное доказательство. Можно рассуждать и следующим образом. Если элемент ξ алгебраичен над простым полем, то $|\xi|_v = 1$ или 0 для всех v в соответствии с тем, отличен элемент ξ от нуля или нет. Действительно, если это не так, то k алгебраично над $\mathbf{F}_p(\xi)$. Пусть v — точка поля k и w — точка из $\mathbf{F}_p(\xi)$, лежащая под ней. В силу следствия 2 теор. 3 гл. I-2 $|\xi|_v > 1$ тогда и только тогда, когда $|\xi|_w > 1$. По теореме 2 поле $\mathbf{F}_p(\xi)$ имеет только одну точку с таким свойством. Применение теоремы 1 завершает доказательство.

Следствие 1. *Пусть E — конечномерное векторное пространство над* **A***-полем k и ε, ε' — два конечных подмножества в E, содержащих базисы этого пространства. Положим $E_v = E \otimes_k k_v$ для каждой конечной точки v поля k и через ε_v и ε'_v обозначим r_v-модули, порожденные в E_v соответственно ε и ε'. Тогда $\varepsilon_v = \varepsilon_{v'}$ почти для всех v.*

Здесь, как и всюду далее в подобных ситуациях, мы будем рассматривать E как вложенное в E_v с помощью вложения $e \to e \otimes 1_{k_v}$. Положим $\varepsilon = \{e_1, \ldots, e_r\}$ и $\varepsilon' = \{e'_1, \ldots, e'_s\}$. Поскольку ε содержит базис пространства E над k, e'_j можно записать (вообще говоря, неоднозначно) в виде $e'_j = \sum c_{ji} e_i$, $1 \leqslant j \leqslant s$, с коэффициентами c_{ji} из k. Поэтому $\varepsilon'_v \subset \varepsilon_v$ всякий раз, когда все $|c_{ji}|_v \leqslant 1$, следовательно, почти для всех v. Меняя местами ε и ε', получаем утверждение нашего следствия.

Следствие 2. *Пусть $\mathcal{A}$ — конечномерная алгебра над* **A***-полем k, α — ее конечное подмножество, содержащее какой-нибудь базис алгебры $\mathcal{A}$ над k. Положим $\mathcal{A}_v = \mathcal{A} \otimes_k k_v$ для каждой конечной точки v поля k и через α_v обозначим r_v-модуль, порожденный множеством α в $\mathcal{A}_v$. Тогда почти для всех v α_v — компактное подкольцо алгебры $\mathcal{A}_v$.*

Положим $\alpha = \{a_1, \ldots, a_r\}$ и $\alpha' = \{1, a_1, \ldots, a_r\}$. Так как α содержит базис алгебры $\mathcal{A}$ над k, можно написать $a_i a_j = \sum c_{ijh} a_h$, $1 \leqslant i, j \leqslant r$, где коэффициенты $c_{ijh} \in k$. Следовательно, α_v является подкольцом в $\mathcal{A}_v$, если все $|c_{ijh}|_v \leqslant 1$, т. е. почти для всех v. Очевидно, оно компактно, и $\alpha_v = \alpha'_v$ почти для всех v.

§ 2. ТЕНЗОРНЫЕ ПРОИЗВЕДЕНИЯ КОММУТАТИВНЫХ ПОЛЕЙ

Доказательство теоремы 1 дает для **A**-поля k и его конечного алгебраического расширения k' конструкцию точек поля k', лежащих над заданной точкой поля k. Наряду с этой конструкцией рассмотрим еще одну, основанную на использовании тензорного произведения $k' \otimes_k k_v$. Для простоты ограничимся случаем, когда поле k' сепарабельно над k. Этого достаточно для наших целей в силу следующей леммы.

Лемма 1. *Каждое* **A***-поле характеристики $p > 1$ изоморфно некоторому сепарабельному алгебраическому расширению конечной степени поля $\mathbf{F}_p(T)$.*

Пусть k — такое поле. Представим его в виде $\mathbf{F}_p(x_1, \ldots, x_N)$, где по меньшей мере одно из x_i, например x_1, трансцендентно над

$\mathbf{F}_p$. Докажем индукцией по N, что существует x_i, такое, что k сепарабельно над $\mathbf{F}_p(x_i)$. Это очевидно, если $N = 1$, а также если $x_2, \ldots, x_N$ все алгебраичны над $\mathbf{F}_p$, ибо в этом случае они сепарабельны над $\mathbf{F}_p$ по теореме 2 гл. I-1 и, значит, поле k сепарабельно над $\mathbf{F}_p(x_1)$. Если же это не так, то по предположению индукции при некотором $i \geqslant 2$ поле $\mathbf{F}_p(x_2, \ldots, x_N)$ сепарабельно над некоторым $\mathbf{F}_p(x_i)$, скажем над $\mathbf{F}_p(x_2)$, так что само k сепарабельно над $\mathbf{F}_p(x_1, x_2)$. Поскольку k имеет над $\mathbf{F}_p$ степень трансцендентности 1, в кольце $\mathbf{F}_p[X_1, X_2]$ существует неприводимый многочлен Φ, для которого $\Phi(x_1, x_2) = 0$. Многочлен Φ не является многочленом вида Φ'^p, где $\Phi' \in \mathbf{F}_p[X_1, X_2]$; а так как каждый элемент α из $\mathbf{F}_p$ удовлетворяет уравнению $\alpha^p = \alpha$, то это можно выразить, сказав, что Φ содержит по меньшей мере один член вида $\alpha X_1^a \cdot X_2^b$, где $\alpha \neq 0$ и a или b взаимно просто с p. Пусть для определенности a взаимно просто с p. Тогда x_1 сепарабельно над $\mathbf{F}_p(x_2)$, так что k также сепарабельно над $\mathbf{F}_p(x_2)$.

В оставшейся части этого параграфа будут изучаться чисто алгебраические свойства тензорных произведений вида $k' \otimes_k K$, где k — произвольное поле, k' — его сепарабельное алгебраическое расширение конечной степени и K — некоторое поле, содержащее k. В § 4 эта теория будет применяться к случаю, когда k есть A-поле, а K — его пополнение. Но сначала получим ответ на один технический вопрос.

Лемма 2. *Если коммутативное кольцо B может быть представлено в виде прямой суммы полей, то это можно сделать только одним способом. При этом гомоморфизм кольца B в поле должен равняться нулю на всех слагаемых, кроме одного.*

Пусть B — прямая сумма полей $K_1, \ldots, K_r$. Положим $e_i = 1_{K_i}$. Тогда $K_i = e_i B$ и $1_B = \Sigma e_i$ является единичным элементом в B. Ясно, что решения в B уравнения $X^2 = X$ («идемпотенты» кольца B) будут частичными суммами для Σe_i; поэтому e_i однозначно характеризуются среди решений уравнения $X^2 = X$ тем, что их нельзя представить в виде $e + e'$, где e, e' — решения, отличные от нуля. Если f — гомоморфизм кольца B в поле K', то он должен переводить каждое e_i в решение уравнения $X^2 = X$ в поле K', т. е. в 1 или в 0. Если $f(e_i) = 1$, то $f(e_j) = 0$ для всех $j \neq i$, ибо $e_i e_j = 0$ при $i \neq j$. Отсюда следует, что f равно нулю на на K_j.

Предложение 2. *Пусть k — поле, $k' = k(\xi)$ — его сепарабельное расширение, порожденное корнем ξ неприводимого унитарного многочлена F степени n из $k[X]$. Пусть K — поле, содержащее*

k, и $F_1, \ldots, F_r$ — неприводимые унитарные многочлены из $K[X]$, такие, что $F = F_1 \ldots F_r$. Для каждого i обозначим через ξ_i какой-нибудь корень многочлена F_i в некотором расширении поля K. Тогда алгебра $A = k' \otimes_k K$ над K изоморфна прямой сумме полей $K(\xi_i)$.

Так как k' сепарабельно над k, то F не имеет кратных корней ни в одном расширении поля k, так что все F_i различны. Обозначим через ρ k-линейный гомоморфизм кольца $k[X]$ на поле k', с ядром $F \cdot k[X]$, переводящий X в ξ. Его можно однозначно продолжить до K-линейного гомоморфизма ρ' кольца $K[X]$ на A, с ядром $F \cdot k[X]$, определяющего изоморфизм кольца $A' = K[X]/F \cdot K[X]$ на A. Покажем теперь, что алгебра A' изоморфна прямой сумме B алгебр $B_i = K[X]/F_i \cdot K[X]$ над K; а так как последние изоморфны полям из формулировки предложения, то доказательство тем самым будет завершено. Пусть f — произвольный элемент из $K[X]$; обозначим через $\overline{f}$ его образ в A, а через $\overline{f_i}$ — его образы в кольцах B_i. Очевидно, что каждый элемент $\overline{f_i}$ однозначно определяется элементом $\overline{f}$, так что отображение $\overline{f} \to (\overline{f_1}, \ldots, \overline{f_r})$ является гомоморфизмом φ из A' в B. Хорошо известно (и легко доказывается индукцией по r), что, поскольку F_i взаимно просты, существуют многочлены $p_1, \ldots, p_r$ из $K[X]$, такие, что $F^{-1} = \sum p_i F_i^{-1}$. Отсюда следует, что для всех i и всех $j \neq i$

$$p_i F_i^{-1} F \equiv 1 \ (F_i), \quad p_i F_i^{-1} F \equiv 0 \ (F_j). \tag{1}$$

Возьмем в кольце $K[X]$ r многочленов $f_1, \ldots, f_r$ и для каждого i обозначим через $\overline{f_i}$ образ многочлена f_i в B_i. Положим $f = \sum p_i F_i^{-1} F f_i$ и обозначим через $\overline{f}$ образ f в A'. Элемент $\overline{f}$ однозначно определяется набором $\overline{f_i}$, так что $(\overline{f_1}, \ldots, \overline{f_r}) \to \overline{f}$ есть отображение ψ из B в A'. Ясно, что отображение $\psi \circ \varphi$ тождественно на A'; как показывает (1), $\varphi \circ \psi$ также тождественно на B. Следовательно, φ — изоморфизм кольца A' на B.

Пусть k, k' и K таковы, как в предложении 2. Ясно, что изоморфизм λ из k' в расширение K' поля K индуцирует тождественный морфизм на k в том и только том случае, когда он k-линеен. Такой изоморфизм называется *собственным над K*, если K' порождается над K множеством $\lambda(k')$, а пара (λ, K') называется *собственным вложением k' над K*. Два таких вложения (λ, K') и (λ', K'') называются *эквивалентными*, если найдется K-линейный изоморфизм ρ поля K' на K'', такой, что $\lambda' = \rho \circ \lambda$. Отметим, что эти понятия являются теми алгебраическими понятиями, которые лежат в основе определения 2 и предложения 1 из § 1.

Предложение 3. *Пусть k — поле, k' — его сепарабельное алгебраическое расширение конечной степени n, K — поле, содержащее k, и пусть $A = k' \otimes_k K$. Тогда с точностью до эквивалентности существует только конечное число собственных над K вложений (λ_i, K_i), $1 \leqslant i \leqslant r$, поля k'. Сумма степеней полей K_i над K равна n. Отображение $(\lambda_1, \ldots, \lambda_r)$ поля k' в прямую сумму B полей K_i является k-линейным изоморфизмом из k' в B, а его K-линейное расширение φ на алгебру A является изоморфизмом A на B.*

Пусть $k' = k(\xi)$ и F — неприводимый унитарный многочлен из кольца $k[X]$, имеющий корнем ξ. Применим к k, k', ξ, F и K предложение 2. Получим, что существует K-линейный изоморфизм φ алгебры A на некоторую прямую сумму B полей K_i. Обозначим для каждого i через β_i проекцию из B в K_i; тогда $\mu_i = \beta_i \circ \varphi$ будет K-линейным изоморфизмом алгебры A на K_i, индуцирующим на поле k' k-линейный изоморфизм λ_i в K_i. Очевидно, μ_i есть K-линейное продолжение морфизма λ_i на A, так что отображение φ, или, что то же самое, $(\mu_1, \ldots, \mu_r)$, является K-линейным расширением морфизма $(\lambda_1, \ldots, \lambda_r)$ на A. Если вложение λ_i не собственно над K, то должно существовать поле $K'' \neq K_i$, промежуточное между K и K_i и такое, что λ_i отображает k' в K''; μ_i отображает потому A в K'', но не на K_i. Пусть теперь λ — какой-нибудь k-линейный изоморфизм поля k' в поле K', содержащее K, и μ — его K-линейное продолжение на алгебру A. Очевидно, μ является гомоморфизмом из A в K', так что $\mu \circ \varphi^{-1}$ — гомоморфизм из B в K'. В силу леммы 2 он равен нулю на всех, кроме одного, слагаемых K_i кольца B и, следовательно, может быть записан как $\sigma \circ \beta_i$, где σ — некоторый K-линейный гомоморфизм поля K_i в K'. Поскольку это поле, а гомоморфизм σ не равен нулю, он должен быть изоморфизмом поля K_i на его образ K_i' в K'. Это дает $\mu = \sigma \circ \mu_i$, значит $\lambda = \sigma \circ \lambda_i$. Если $K_i' \neq K'$, то морфизм λ, переводящий k' в K_i', несобствен; следовательно, если λ собствен, то σ — изоморфизм поля K_i на K', так что вложения (λ, K') и (λ_i, K_i) эквивалентны. Наконец, если мы имеем в тоже время $\lambda = \sigma' \circ \lambda_j$, где $j \neq i$ и σ' — изоморфизм из K_j в K', то $\mu = \sigma' \circ \mu_j$, следовательно, $\mu \circ \varphi^{-1} = \sigma' \circ \beta_j$, и $\mu \circ \varphi^{-1}$ должно быть на K_j отлично от нуля. В частности, если λ собствен, то (λ, K') эквивалентно не более чем одному из вложений (λ_i, K_i); это означает, что все эти вложения неэквивалентны, чем и заканчивается доказательство.

Следствие 1. *Пусть в тех же обозначениях, что и выше, λ — произвольный k-линейный изоморфизм из поля k' в поле K', содержащее K. Тогда существуют такое единственное i и такой единственный изоморфизм σ из K_i в K', что $\lambda = \sigma \circ \lambda_i$.*

Это уже доказано выше. Это является также непосредственным следствием предложения 3 и того факта, что для подполя K'' в K', порожденного над K множеством $\lambda(k')$, (λ, K'') есть собственное вложение поля k' над K и, значит, эквивалентно одному из вложений (λ_i, K_i).

Следствие 2. *В тех же обозначениях, что и выше, предположим, что k' есть расширение Галуа поля k с группой Галуа G. Пусть (λ, K') — произвольное собственное вложение поля k' над K. Тогда K' будет расширением Галуа поля K и для каждого автоморфизма ρ поля K' над K найдется единственное $\sigma \in G$, такое, что $\rho \circ \lambda = \lambda \circ \sigma$. Соответствие $\rho \to \sigma$ является изоморфизмом группы Галуа поля K' над K на некоторую подгруппу H группы G. Все собственные вложения поля k' над K имеют, с точностью до эквивалентности, вид $(\lambda \circ \sigma, K')$, где $\sigma \in G$; если $\sigma, \sigma' \in G$, то вложения $(\lambda \circ \sigma', K')$ и $(\lambda \circ \sigma, K)$ эквивалентны тогда и только тогда, когда $\sigma' \in H\sigma$.*

Ясно, что $\lambda(k')$ есть расширение Галуа поля k, а так как K' порождено над K множеством $\lambda(k')$, то K' есть расширение Галуа поля K и ограничение на $\lambda(k')$ автоморфизмов поля K' над K определяет инъективное отображение группы Галуа H_1 поля K' над K в соответствующую группу поля $\lambda(k')$ над k. Но это равносильно первой части нашего следствия. Для любого $\sigma \in G$ вложение $(\lambda \circ \sigma, K')$ является, очевидно, собственным вложением поля k' над K. Если σ, σ' принадлежат G, то $(\lambda \circ \sigma', K)$ и $(\lambda \circ \sigma, K)$ эквивалентны в том и только в том случае, когда существует автоморфизм ρ поля K' над K, такой, что $\lambda \circ \sigma' = \rho \circ \lambda \circ \sigma$, т. е. $\rho \circ \lambda = \lambda \circ (\sigma' \circ \sigma^{-1})$. Последнее выполняется в том и только в том случае, когда $\sigma' \circ \sigma^{-1}$ принадлежит H. Таким образом, число неэквивалентных собственных вложений такого вида равно индексу группы H в G, т. е. n/n', где n, n' — степени соответственно поля k' над k и поля K' над K. Ввиду предложения 3 для любого множества неэквивалентных собственных вложений (λ_i, K_i) поля k' над K сумма степеней полей K_i над K не должна превосходить n. Итак, с точностью до эквивалентности, каждое вложение указанного типа имеет вид $(\lambda \circ \sigma, K')$.

Полезен тот частный случай следствия 2, когда k' есть подполе в K', порождающее K' над K. Тогда в качестве λ можно взять тождественное отображение; собственные вложения поля k' над K будут иметь вид (σ, K'), где $\sigma \in G$, а отображение $\rho \to \sigma$ группы Галуа поля K' над K в группу поля k' над k будет ограничением на k' автоморфизмов поля K' над K.

Следствие 3. *Пусть k и k' таковы, как в предложении* 3, *и пусть K — алгебраически замкнутое или сепарабельно алгебраически замкнутое поле, содержащее k. Тогда существует n, но не более чем n, различных k-линейных изоморфизмов $\lambda_1, \ldots, \lambda_n$ из k' в K. Они линейно независимы над K, и если λ, λ' — любые два из них, а K — алгебраическое замыкание поля k, то найдется автоморфизм α поля K, для которого $\lambda' = \alpha \circ \lambda$.*

Поле K называется *сепарабельно алгебраически замкнутым*, если у него нет сепарабельных алгебраических расширений, отличных от него самого. Первое очевидное утверждение нашего следствия включено в него для удобства ссылок, а также как иллюстрация предложения 3, частным случаем которого оно является. В самом деле, если K таково, как в следствии, то все K_i из этого предложения должны совпадать с K. Второе утверждение (представляющее собой хорошо известную теорему Дедекинда, легко доказываемую и непосредственно) можно извлечь из предложения 3 следующим образом. Предположим, что $\Sigma\, c_i\lambda_i = 0$ для некоторых $c_i \in K$, $1 \leqslant i \leqslant n$, т. е. что $\Sigma\, c_i\lambda_i(\xi) = 0$ для всех $\xi \in k'$. Вводя μ_i и β_i так же, как и в доказательстве предложения 3, находим, что $\Sigma\, c_i\mu_i = 0$ и, значит, $\Sigma\, c_i\beta_i = 0$, что, очевидно, возможно, только если все c_i равны нулю. Из единственности, с точностью до изоморфизма, алгебраического замыкания поля k следует, что каждое λ_i продолжается до изоморфизма алгебраического замыкания $\bar{k}$ поля k' на K. Отсюда немедленно вытекает последнее утверждение следствия, включенное в его формулировку также для удобства ссылок.

Следствие 4. *В предположениях и обозначениях следствия* 3 *предположим еще, что k' есть расширение Галуа над k. Тогда все λ_i отображают k' на одно и то же подполе в K.*

Это вытекает из следствия 2.

§ 3. СЛЕДЫ И НОРМЫ

Напомним сначала понятие полиномиального отображения. Пусть E, E' — векторные пространства конечной размерности над полем k, имеющим бесконечное число элементов, и пусть $\varepsilon = \{e_1, \ldots, e_n\}$ и $\varepsilon' = \{e'_1, \ldots, e'_m\}$ — их базисы над полем k. Отображение f из E в E' называется *полиномиальным*, если в кольце $k[X_1, \ldots, X_n]$ найдутся такие многочлены P_j, что для всех значений x_i из k

$$f\left(\sum_i x_i e_i\right) = \sum_j P_j(x_1, \ldots, x_n)\, e'_j.$$

Ясно, что это определение не зависит от выбора базисов ε, ε'. Далее, поскольку в k бесконечно много элементов, многочлены P_j однозначно определяются по f, ε и ε'. Если $E' = k$, то f называется *полиномиальной функцией*; степень соответствующего многочлена P не зависит от выбора ε и называется *степенью* f. Если K — произвольное поле, содержащее k, и $E_K = E \otimes_k K$, $E'_K = E' \otimes_k K$, то существует одно и только одно полиномиальное отображение из E_K в E'_K, совпадающее с f на E. Оно называется *продолжением* отображения f на E_K и E'_K (или, короче, на K) и обозначается по-прежнему через f. Это продолжение задается, по отношению к базисам ε, ε' пространств E_K, E'_K над K, теми же многочленами, что и раньше.

Пусть E такое же, как и выше. Обозначим через End (E) кольцо его эндоморфизмов, рассматриваемое как алгебра над k. Для $a \in \mathrm{End}\, E$ через $\mathrm{tr}\,(a)$ и $\det(a)$ обозначаются соответственно след и определитель a. Первый является линейной формой, а последний — полиномиальной функцией (степень которой равна размерности пространства F) на пространстве End (E), рассматриваемом как векторное пространство над k.

Пусть теперь $\mathcal{A}$ — алгебра конечной размерности над k; как всегда, мы предполагаем, что у нее есть единичный элемент 1. Для каждого $a \in \mathcal{A}$ обозначим через $\rho(a)$ эндоморфизм $x \to ax$ алгебры $\mathcal{A}$, рассматриваемой как векторное пространство над полем k. Обозначая через End $(\mathcal{A})$ алгебру всех эндоморфизмов этого векторного пространства, мы можем рассматривать ρ как гомоморфизм из $\mathcal{A}$ в End $(\mathcal{A})$. Этот гомоморифзм известен под названием *регулярного представления* алгебры $\mathcal{A}$; поскольку $\mathcal{A}$ имеет единицу, он является изоморфизмом $\mathcal{A}$ на некоторую подалгебру в End $(\mathcal{A})$. След и определитель отображения ρ называются *регулярным следом* и *регулярной нормой* в алгебре $\mathcal{A}$ над k и обозначаются соответственно через $\mathrm{Tr}_{\mathcal{A}/k}$ и $\mathrm{N}_{\mathcal{A}/k}$ или (если не может возникнуть недоразумений) просто Tr и N. Регулярный след есть линейная форма на $\mathcal{A}$, рассматриваемом как векторное пространство над k, а регулярная норма есть полиномиальная функция степени, равной размерности $\mathcal{A}$ над k. Если K — поле, содержащее k, и A расширено над K до алгебры $\mathcal{A}_K = \mathcal{A} \otimes_k K$, то регулярный след и регулярная норма в алгебре $\mathcal{A}_K$ над K являются соответственно продолжениями $\mathrm{Tr}_{\mathcal{A}/k}$ и $\mathrm{N}_{\mathcal{A}/k}$ на $\mathcal{A}_K$ и обозначаются попрежнему через $\mathrm{Tr}_{\mathcal{A}/k}$ и $\mathrm{N}_{\mathcal{A}/k}$. В случае когда A есть поле k' конечной степени над k, слово «регулярный», как правило, опускается и $\mathrm{Tr}_{k'/k}$ и $\mathrm{N}_{k'/k}$ называются соответственно *следом* и *нормой* в поле k' над k. Посмотрим теперь, как эти понятия применяются в ситуации, описанной в § 2.

Предложение 4. *Пусть k — поле, k' — его сепарабельное алгебраическое расширение конечной степени n и K — поле, содержащее k. Положим $A = k' \otimes_k K$, и пусть $(\lambda_i, K_i)_{1 \leqslant i \leqslant r}$ — максимальное множество неэквивалентных собственных вложений поля k' над K и для каждого i μ_i суть K-линейные продолжения λ_i на A. Тогда для всех $a \in A$*

$$\mathrm{Tr}_{k'/k}(a) = \sum_{i=1}^{r} \mathrm{Tr}_{K_i/K}(\mu_i(a)), \quad \mathrm{N}_{k'/k}(a) = \prod_{i=1}^{r} \mathrm{N}_{K_i/K}(\mu_i(a)).$$

Действительно, пусть обозначения будут те же, что использовавшиеся в предложении 3 § 2 и в его доказательстве. Положим $b = \varphi(a)$. Для каждого i проекция элемента b на K_i равна $\beta_i(b) = \mu_i(a)$. Поэтому $\mathrm{Tr}_{k'/k}(a)$ и $\mathrm{N}_{k'/k}(a)$ являются следом и определителем отображения $y \to by$, рассматриваемого как эндоморфизм алгебры B. Выбирая в B базис, являющийся объединением базисов пространств K_i над K, получаем формулы предложения 4.

Следствие 1. *Если k и k' таковы, как в предложении 4, то k-линейная форма $\mathrm{Tr}_{k'/k}$ на k' отлична от нуля.*

Выберем в предложении 4 в качестве K алгебраически замкнутое поле, содержащее k; тогда $K_i = K$ для всех i, а из предложения 4 вытекает, что $\mathrm{Tr}_{k'/k}(a) = \Sigma\, \mu_i(a)$. В тех же обозначениях, что и прежде, положим $b = \varphi(a)$, так что $\beta_i(b) = \mu_i(a)$. Поскольку проекции $\beta_i(b)$ элемента b на слагаемые кольца B можно выбирать произвольно, выберем их так, чтобы $\mathrm{Tr}_{k'/k}(a)$ не равнялся нулю. Так как форма $\mathrm{Tr}_{k'/k}$ на A является продолжением на A k-линейной формы $\mathrm{Tr}_{k'/k}$ на k', а последняя не равна нулю, то и первая не равна нулю.

Следствие 2. *В обозначениях и предположениях предложения 4 имеем для всех $x \in k'$*

$$\mathrm{Tr}_{k'/k}(x) = \sum_i \mathrm{Tr}_{K_i/K}(\lambda_i(x)); \quad \mathrm{N}_{k'/k}(x) = \prod_i \mathrm{N}_{K_i/K}(\lambda_i(x)).$$

Следствие 3. *Пусть k, k' такие же, как в предложении 4, K — алгебраически замкнутое поле, содержащее k, и $\lambda_1, \ldots, \lambda_n$ — различные k-линейные изоморфизмы из k' в поле K. Тогда для всех $x \in k'$*

$$\mathrm{Tr}_{k'/k}(x) = \sum_i \lambda_i(x), \quad \mathrm{N}_{k'/k}(x) = \prod_i \lambda_i(x).$$

Это сразу следует из предложения 4 и следствия 3 предл. 3 § 2.

Следствие 4. *Пусть k, k' таковы, как в предложении 4, и k'' — сепарабельное алгебраическое расширение поля k', имеющее конечную степень. Тогда*

$$\mathrm{Tr}_{k''/k} = \mathrm{Tr}_{k''/k'} \circ \mathrm{Tr}_{k'/k}, \quad \mathrm{N}_{k''/k} = \mathrm{N}_{k''/k'} \circ \mathrm{N}_{k'/k}.$$

Возьмем в качестве K алгебраическое замыкание поля k'' и определим λ_i, как в следствии 3. Обозначим через n' степень поля k'' над k' и через λ'_j, $1 \leqslant j \leqslant n'$, различные k'-линейные изоморфизмы поля k'' в K. Каждое λ_i продолжается до автоморифзма φ_i поля K. Положим $\lambda''_{ij} = \varphi_i \circ \lambda'_j$ при $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n'$; мы получим k-линейные изоморфизмы из k'' в K. Ясно, что если $\lambda''_{ij} = \lambda''_{hl}$, то $i = h$, ибо λ''_{ij} индуцирует на k' отображение λ_i, и $j = l$, ибо $\varphi_i^{-1} \circ \lambda''_{ij} = \lambda'_j$. Далее, если λ'' — произвольный k-линейный изоморфизм из k'' в K, то он должен индуцировать на k' один из изоморфизмов λ_i, следовательно, отображение $\varphi_i^{-1} \circ \lambda''$ k'-линейно и, значит, должно совпадать с одним из λ'_j. Таким образом, $\lambda'' = \lambda''_{ij}$. Следствие 3 дает теперь для $x \in k''$

$$\mathrm{Tr}_{k''/k}(x) = \sum_{i,j} \lambda''_{ij}(x) = \sum_i \varphi_i \left(\sum \lambda'_j(x) \right) =$$

$$= \sum_i \varphi_i (\mathrm{Tr}_{k''/k'}(x)) = \sum_i \lambda_i (\mathrm{Tr}_{k''/k'}(x)) = \mathrm{Tr}_{k'/k} (\mathrm{Tr}_{k''/k'}(x)),$$

чем доказано наше первое утверждение. Формулу для нормы можно вывести в точности тем же способом.

Для полноты рассмотрим вкратце след и норму в несепарабельных расширениях. Пусть k'— произвольное алгебраическое расширение поля k конечной степени. Как хорошо известно, оно содержит единственное максимальное сепарабельное подрасширение k'_0, над которым оно чисто несепарабельно. Пусть $q = p^m$ — степень поля k' над k'_0, где p — характеристика. Легко видеть, что $x^q \in k'_0$ при всех $x \in k'$. Выберем какой-нибудь базис $\{\xi_1, \ldots, \xi_q\}$ поля k' над k'_0 и элемент $a \in k'$. Как векторное пространство над k поле k' есть прямая сумма подпространств $\xi_i k'_0$, $1 \leqslant i \leqslant q$, которые инвариантны относительно отображения $x \to a^q x$, поскольку $a^q \in k'_0$. Следовательно,

$$\mathrm{N}_{k'/k}(a^q) = \mathrm{N}_{k'_0/k}(a^q)^q,$$

откуда сразу вытекает, что

$$\mathrm{N}_{k'/k}(a) = \mathrm{N}_{k'_0/k}(a^q).$$

Обозначим через n_0 степень поля k'_0 над k, так что степень k' над k равна $n = n_0 q$. Если K — алгебраически замкнутое поле, содержащее k, то каждый k-линейный изоморфизм из k'_0 в K может быть

однозначно продолжен до отображения из k' в K. В силу следствия 3 предл. 3 § 2 существует n_0 таких изоморфизмов λ_i, $1 \leqslant i \leqslant n_0$, и, комбинируя приведенную выше формулу для $N_{k'/k}$ со следствием 3 предл. 4 (примененным к k'_0 и k), получаем

$$N_{k'/k}(x) = \prod_i \lambda_i(x)^{n/n_0}$$

при всех $x \in k'$. Пусть теперь k'' — произвольное конечное расширение поля k'. Поступая так же, как и при доказательстве следствия 4 предл. 4, находим, что снова

$$N_{k''/k} = N_{k''/k} \circ N_{k'/k}.$$

Таким образом, это соотношение выполняется независимо от того, сепарабельны поля k' и k'' над k или нет.

Что касается следа, то из элементарных свойств определителя и определения следа и нормы следует, что для произвольной алгебры $\mathcal{A}$ над k $\mathrm{Tr}_{\mathcal{A}/k}(x)$ как линейная форма на $\mathcal{A}$ является суммой членов степени 1 в представлении полиномиальной функции $N_{\mathcal{A}/k}(1 + x)$ как многочлена от координат точки $x \in \mathcal{A}$ в некотором базисе алгебры $\mathcal{A}$. Применяя это к нашей ситуации, находим, что $\mathrm{Tr}_{k'/k}(x)$ есть сумма членов степени 1 в многочлене $N_{k'/k}(1 + x)$. А поскольку последний равен $N_{k'_0/k}(1 + x^q)$, то $\mathrm{Tr}_{k'/k}(x)$ содержит только члены, степень которых кратна q. Это показывает, что $\mathrm{Tr}_{k'/k} = 0$ при $q > 1$. Таким образом, в силу следствия 1 предл. 4 $\mathrm{Tr}_{k'/k} \neq 0$ тогда и только тогда, когда k' сепарабельно над k.

Предложение 5. *Пусть k' — сепарабельное алгебраическое расширение степени n поля k и $\{a_1, \ldots, a_n\}$ — его базис над k. Тогда определитель матрицы*

$$(\mathrm{Tr}_{k'/k}(a_i a_j))_{1 \leqslant i,\, j \leqslant n}$$

не равен 0.

В силу следствия 1 предл. 4 это частный случай следующей леммы, которая нам еще понадобится.

Лемма 3. *Пусть k' — произвольное расширение степени n поля k, E — векторное пространство над k, «несущее» k', и λ — какая-нибудь отличная от нуля линейная форма на E. Тогда отображение $(x, y) \to \lambda(xy)$ является невырожденной билинейной формой на $E \times E$; пространство E можно отождествить с его алгебраическим двойственным E', положив $[x, y] = \lambda(xy)$; определитель матрицы $(\lambda(a_i a_j))$ отличен от нуля для любого базиса $a_1, \ldots, a_n$ поля k' над k.*

Так как λ не равно нулю, существует такое $a \in k'$, что $\lambda(a) \neq 0$. Для каждого $y \in k'$ построим k-линейную форму λ_y на k', положив $\lambda_y(x) = \lambda(xy)$, $x \in k'$. Отображение $y \to \lambda_y$ является морфизмом из E в его двойственное E'. Ядро этого морфизма равно нулю, ибо $y \neq 0$ влечет $\lambda_y(ay^{-1}) \neq 0$, т. е. $\lambda_y \neq 0$. А так как E и E' имеют над k одинаковую размерность, видим, что $y \to \lambda_y$ — это изоморфизм E на E'. Отождествляя E и E' с помощью этого изоморфизма, получаем $[x, y] = \lambda(xy)$. Но по определению это означает невырожденность формы $(x, y) \to \lambda(xy)$. Наконец, если бы определитель матрицы $(\lambda(a_i a_j))$ был равен нулю, то в поле k можно было бы найти такие элементы $y_1, \ldots, y_n$, не все равные нулю, что $\sum_j \lambda(a_i a_j) y_j = 0$, так что, полагая $y = \sum_j a_j y_j$, мы находим, что $\lambda_y(a_i) = 0$ для всех i, и, значит, $\lambda_y = 0$, что противоречит доказанному выше.

§ 4. ТЕНЗОРНЫЕ ПРОИЗВЕДЕНИЯ А-ПОЛЕЙ И ЛОКАЛЬНЫХ ПОЛЕЙ

Пусть k — некоторое **А**-поле, k' — его сепарабельное расширение, v — точка и k_v — пополнение в этой точке. В силу предложения 1 § 1 и его следствия пополнения (λ, K') поля k', индуцирующие на k его естественное вложение в k_v, совпадают с собственными вложениями поля k' над k_v, введенными в § 2. Мы можем, следовательно, использовать предложения 2 и 3 из § 2 для определения точек поля k', лежащих над v. Этим мы сейчас и займемся.

Теорема 4. *Пусть k — некоторое* **А**-*поле, k' — его сепарабельное алгебраическое расширение конечной степени n и α — базис над k. Для каждой точки v поля k обозначим через k_v пополнение поля k в v и положим $A_v = k' \otimes_k k_v$. Далее, для всякой конечной точки v обозначим через r_v максимальное компактное подкольцо в k_v и через α_v обозначим r_v-модуль, порожденный множеством α в A_v. Пусть $w_1, \ldots, w_r$ — точки поля k', лежащие над v; k'_i — пополнения поля k' в точках w_i, λ_i — естественные проекции из k' в k'_i и μ_i — их k_v-линейные продолжения на A_v. Тогда отображение $\Phi_v = (\mu_1, \ldots, \mu_r)$ является изоморфизмом алгебры A_v на прямую сумму B_v полей k'_i и почти для всех v отображает α_v на сумму максимальных компактных подколец r'_i полей k'_i.*

Если в предложении 3 § 2 положить $K = k_v$, то первое утверждение превращается в частный случай этого предложения. Коротко, но несколько вольно это можно выразить, сказав, что пополнения k'_i поля k' в точках, лежащих над v, суть слагаемые алгебры $k' \otimes_k k_v$,

представленной в виде прямой суммы полей. Возьмем теперь в качестве v произвольную конечную точку поля k. Как легко видеть, сумма колец r_i' есть максимальное компактное подкольцо в B_v, а его образ ρ_v относительно Φ_v^{-1} есть, следовательно, максимальное компактное подкольцо в A_v. Нам нужно показать, что почти для всех v оно совпадает с α_v. Но ρ_v является k_v-решеткой в A_v, ибо каждое r_i' содержит r_v. По теореме 1 гл. II-2 найдется такой базис $\{u_{v,1}, \ldots, u_{v,n}\}$ алгебры A_v над k_v, что ρ_v будет r_v-модулем, порожденным этим базисом. По следствию 2 теор. 3 § 1 α_v — компактное подкольцо в A_v, содержащееся поэтому в ρ_v почти для всех v. Обозначим через P конечное множество точек поля k, для которых это не так. Если $\alpha = \{a_1, \ldots, a_n\}$, то для точек v, не содержащихся в P, α_v принадлежит ρ_v и можно написать $a_i = \sum c_{v,ij} u_{v,j}$, где $c_{v,ij} \in r_v$. Матрица $C_v = (c_{v,ij})$ принадлежит, следовательно, кольцу $M_n(r_v)$, и $\alpha_v = \rho_v$ в том и только в том случае, когда эта матрица обратима в $M_n(r_v)$, т. е. когда ее определитель обратим в r_v. Сокращая теперь запись $\mathrm{Tr}_{k'/k}$ до Tr, обозначим через Δ определитель матрицы

$$M = (\mathrm{Tr}\,(a_i a_j))_{1 \leqslant i,j \leqslant n}.$$

Этот определитель лежит в k и в силу предложения 5 § 3 не равен нулю. Применяя к Δ и Δ^{-1} теорему 3 § 1, видим, что $|\Delta|_v = 1$ почти для всех v. С другой стороны, если u — произвольный элемент из A_v, то $\mathrm{Tr}\,(u)$ является следом отображения $x \to ux$ алгебры A_v. Записав $u \cdot u_{v,i} = \sum d_{ij} u_{v,j}$, где $d_{ij} \in k_v$ и $1 \leqslant i, j \leqslant n$, получим $\mathrm{Tr}\,(u) = \sum d_{ii}$. Так как ρ_v — кольцо, то при $u \in \rho_v$ все d_{ij} находятся в r_v. Это показывает, что Tr переводит ρ_v в r_v. Следовательно, если мы обозначим через N_v матрицу $(\mathrm{Tr}\,(u_{v,i}\, u_{v,j}))$, то N_v принадлежит $M_n(r_v)$. Подставляя в матрицу M вместо a_i выражение $\sum c_{v,ij} u_{v,j}$, получаем $M = C_v N_v {}^t C_v$, откуда $\Delta = \det(N_v) \det(C_v)^\alpha$. Здесь N_v лежит в $M_n(r_v)$, равно как и C_v при $v \notin P$, и почти для всех v $|\Delta|_v = 1$. Отсюда, очевидно, следует, что $|\det(C_v)|_v = 1$ почти для всех v, что и требовалось доказать.

В гл. VIII будет показано, что теорема 4 остается справедливой, даже если поле k' не предполагается сепарабельным над k.

Следствие 1. *В предположениях и обозначениях теоремы* 4 *сумма степеней над k_v пополнений k_i' поля k' в точках, лежащих над v, равна степени n поля k' над k.*

В самом деле, эта сумма равна размерности B_v над k_v, а размерность A_v над k_v есть n.

Следствие 2. *Пусть k — алгебраическое расширение степени n поля $\mathbf{Q}$. Обозначим через r_1 число его вещественных точек и через r_2 — число мнимых. Тогда $r_1 + 2r_2 = n$.*

Для доказательства достаточно в следствии 1 заменить k, k', v на $\mathbf{Q}$, k, ∞.

Следствие 3. *В обозначениях и предположениях теоремы 4 продолжения $\mathrm{Tr}_{k'/k}$ и $\mathrm{N}_{k'/k}$ на A_v задаются формулами*

$$\mathrm{Tr}_{k'/k}(x) = \sum_i \mathrm{Tr}_{k'_i/k_v}(\mu_i(x)), \quad \mathrm{N}_{k'/k}(x) = \prod_i \mathrm{N}_{k'_i/k_v}(\mu_i(x)).$$

Это сразу следует из предложения 4 § 3, примененного к ситуации, описываемой теоремой 4.

Следствие 4. *В предположениях и обозначениях теоремы 4 допустим еще, что k' есть расширение Галуа поля k с группой Галуа G. Пусть w — одна из точек w_i поля k'. Тогда пополнение k'_w поля k' в точке w будет расширением Галуа над k_v; ограничение на k' группы Галуа H поля k'_w над k_v определяет изоморфизм этой группы на подгруппу в G, состоящую из автоморфизмов, оставляющих точку w на месте. Точки w_i суть образы точки w относительно G, и все поля k'_i изоморфны полю k'_w.*

Пусть λ — такое изоморфное вложение поля k' в локальное поле K, что $\lambda(k')$ плотно в K. Это вложение задает по определению точку поля k', и ее образ относительно автоморфизма σ поля k' можно рассматривать как точку, определенную вложением $\lambda \circ \sigma$. Применяя следствие 2 предл. 3 § 2 к естественному вложению поля k' в k'_w и учитывая теорему 4, получаем наше утверждение.

ГЛАВА ЧЕТВЕРТАЯ

АДЕЛИ

§ 1. АДЕЛИ А-ПОЛЕЙ

Повсюду в этой главе через k будет обозначаться некоторое А-поле. Если v — точка поля k, то через k_v будет обозначаться пополнение поля k относительно v. Если v — конечная точка поля k, то мы обозначаем через r_v максимальное компактное подкольцо в k_v и через p_v максимальный идеал в r_v; эти подмножества в k_v определяются соответственно условиям $|x|_v \leqslant 1$ и $|x|_v < 1$. Мы обозначаем далее через P_∞ множество всех бесконечных точек поля k и через P — любое конечное множество точек поля k, содержащее P_∞. Для любого такого множества P положим

$$k_{\mathbf{A}}(P) = \prod_{v \in P} k_v \times \prod_{v \notin P} r_v, \tag{1}$$

где второе произведение берется по всем точкам поля k, не лежащим в P. Наделенное обычной топологией произведения множество $k_{\mathbf{A}}(P)$ локально компактно, потому что k_v таковы, а r_v компактны. Наделим $k_{\mathbf{A}}(P)$ структурой кольца, определив сложение и умножение покомпонентно. Ясно, что тем самым мы превратим $k_{\mathbf{A}}(P)$ в топологическое кольцо. Рассматриваемое лишь как множество, $k_{\mathbf{A}}(P)$ можно было бы определить как подмножество в произведении $\prod k_v$, состоящее из тех элементов $x = (x_v)$ этого произведения, для которых $|x_v|_v \leqslant 1$ при всех v, не лежащих в P. Если P' — другое конечное множество точек поля k и $P' \supset P$, то кольцо $k_{\mathbf{A}}(P)$ содержится в $k_{\mathbf{A}}(P')$, причем его топология и кольцевая структура индуцируются топологией и кольцевой структурой на $k_{\mathbf{A}}(P')$ и $k_{\mathbf{A}}(P)$ является открытым подмножеством в $k_{\mathbf{A}}(P')$.

Теперь мы определим локально компактное топологическое кольцо $k_{\mathbf{A}}$ — так называемое кольцо аделей поля k. Как множество оно есть объединение всех множеств $k_{\mathbf{A}}(P)$; другими словами, оно состоит из элементов $x = (x_v)$ произведения $\prod k_v$, которые при почти всех v удовлетворяют условию $|x_v|_v \leqslant 1$. Определим структуру топологического кольца на $k_{\mathbf{A}}$ условием, что всякое

кольцо $k_{\mathbf{A}}(P)$ является открытым подкольцом в $k_{\mathbf{A}}$. Это означает, во-первых, что если $x = (x_v)$ и $y = (y_v)$ лежат в $k_{\mathbf{A}}$, то $x + y = (x_v + y_v)$ и $xy = (x_v y_v)$; ясно, что при этом и сумма, и произведение действительно лежат в $k_{\mathbf{A}}$. Во-вторых, мы получим фундаментальную систему окрестностей нуля в аддитивной группе кольца $k_{\mathbf{A}}$, взяв такую систему в любом из колец $k_{\mathbf{A}}(P)$, например в $k_{\mathbf{A}}(P_\infty)$, которое является наименьшим среди колец $k_{\mathbf{A}}(P)$. Эквивалентным образом мы получим такую систему, взяв все множества вида $\prod U_v$, где U_v — окрестность нуля в k_v для всех v и $U_v = r_v$ почти для всех v.

Определение 1. *Под кольцом $k_{\mathbf{A}}$ аделей* **A**-*поля k мы понимаем объединение множеств $k_{\mathbf{A}}(P)$, определенных формулой* (1), *где в качестве P берутся все конечные множества точек поля k, содержащие множество всех бесконечных точек. Структура топологического кольца на $k_{\mathbf{A}}$ определяется условием, что всякое $k_{\mathbf{A}}(P)$ является открытым подкольцом в $k_{\mathbf{A}}$.*

Элементы кольца $k_{\mathbf{A}}$ будут называться *аделями* поля k.

Возьмем точку v поля k. В случае когда P содержит v, кольцо $k_{\mathbf{A}}(P)$ можно записать как произведение поля k_v и некоторого бесконечного произведения. Обозначая последнее через $k'_{\mathbf{A}}(P, v)$, мы можем проделать с произведениями $k'_{\mathbf{A}}(P, v)$ то же самое, что мы делали с произведениями $k_{\mathbf{A}}(P)$, беря теперь в качестве P все конечные множества точек поля k, содержащие P_∞ и v. Объединение всех $k'_{\mathbf{A}}(P, v)$ будет тогда локально компактным кольцом $k'_{\mathbf{A}}(v)$, и $k_{\mathbf{A}}$, очевидно, изоморфно произведению $k_v \times k'_{\mathbf{A}}(v)$. При этом изоморфизме первый сомножитель k_v последнего произведения, очевидно, отображается на множество тех аделей $x = (x_v)$, для которых $x_w = 0$ для всех точек $w \neq v$. Это множество будет называться *квазисомножителем* в $k_{\mathbf{A}}$, соответствующим v, и будет всегда отождествляться с k_v. Отображение $(x_v) \to x_v$ из $k_{\mathbf{A}}$ на k_v, соответствующее проекции из произведения $k_v \times k'_{\mathbf{A}}(v)$ на первый сомножитель, будет называться *проекцией* из $k_{\mathbf{A}}$ на квазисомножитель k_v; очевидно, эта проекция непрерывна. Ясно также, что вместо одной точки v поля k можно было начать с любого конечного множества P_0 таких точек и прийти к записи $k_{\mathbf{A}}$ в виде произведения полей k_v по $v \in P_0$ и еще одного сомножителя.

Возьмем любой характер χ аддитивной группы кольца $k_{\mathbf{A}}$. Для каждого P он индуцирует на $k_{\mathbf{A}}(P)$ некоторый характер χ_P и для каждого v некоторый характер χ_v на квазисомножителе k_v. Хорошо известно, что характер на бесконечном произведении компактных групп должен индуцировать тривиальный характер 1 на почти всех сомножителях. Применяя это к характеру, инду-

цированному характером χ_P на произведении $\prod r_v$ в (1), мы видим, что χ_v тривиален на r_v почти для всех v. Тогда для всех $x = (x_v)$ из $k_\mathbf{A}$ имеем

$$\chi(x) = \prod_v \chi_v(x_v). \tag{2}$$

Произведение здесь берется по всем точкам v поля k; для всякого $x = (x_v)$ из $k_\mathbf{A}$ почти все сомножители равны 1.

Пусть ξ — элемент из k. Положив $x_v = \xi$ при всех v, мы определим в силу теоремы 3 гл. III-1 некоторый адель $x = (x_v)$. Обозначим его через $\varphi(\xi)$ и назовем φ *каноническим вложением* поля k в $k_\mathbf{A}$. Часто мы будем, если это не может привести к путанице, отождествлять k с его образом в $k_\mathbf{A}$ при вложении φ.

Пусть E — конечномерное векторное пространство размерности n над k. Для всякой точки v поля k будем писать $E_v = E \otimes_k k_v$. Как обычно, мы считаем E «естественно» вложенным в E_v посредством инъективного отображения $e \to e \otimes 1_{k_v}$. С другой стороны, поскольку k вложено в $k_\mathbf{A}$ определенным выше каноническим вложением φ, то мы можем рассмотреть тензорное произведение $E_\mathbf{A} = E \otimes_k k_\mathbf{A}$ и считать E «естественно» вложенным в него посредством отображения $e \to e \otimes \varphi(1)$. Определим топологию на $E_\mathbf{A}$ как самую грубую, в которой $k_\mathbf{A}$-линейные продолжения на $E_\mathbf{A}$ линейных форм на E непрерывны. Эквивалентное определение: возьмем какой-нибудь базис ε в E над k; он определяет изоморфизм k^n на E, а следовательно, изоморфизм $(k_\mathbf{A})^n$ на $E_\mathbf{A}$; топология на $E_\mathbf{A}$ получается перенесением на $E_\mathbf{A}$ посредством этого изоморфизма топологии с $(k_\mathbf{A})^n$; легко проверяется непосредственно, что она не зависит от выбора ε.

Пусть E и E' — конечномерные векторные пространства над k и f — полиномиальное отображение из E в E'. Тогда f можно очевидным образом продолжить до отображения из $E_\mathbf{A}$ в $E'_\mathbf{A}$, а именно, это отображение определяется теми же самыми многочленами, если E, E' отождествлены с пространствами k^n, k^m, а следовательно, $E_\mathbf{A}$, $E'_\mathbf{A}$ с $(k_\mathbf{A})^n$, $(k_\mathbf{A})^m$ при каком-либо выборе базисов в E, E' над k. Это продолжение отображения f будет обозначаться опять через f. Ясно, что оно непрерывно, поскольку сложение и умножение на $k_\mathbf{A}$ непрерывны.

Предложение 1. *Пусть E — векторное пространство конечной размерности n над k, и пусть ε — конечное подмножество в E, содержащее базис векторного пространства E над k. Для всякой конечной точки v поля k обозначим через ε_v r_v-модуль, порожденный подмножеством ε в E_v. Для всякого конечного множества P*

точек поля k, содержащего P_∞, запишем

$$E_{\mathbf{A}}(P, \varepsilon) = \prod_{v \in P} E_v \times \prod_{v \notin P} \varepsilon_v.$$

Тогда все $E_{\mathbf{A}}(P, \varepsilon)$ являются открытыми подгруппами в $E_{\mathbf{A}}$ и $E_{\mathbf{A}}$ есть объединение этих подгрупп.

Это следует понимать в том смысле, что всякое произведение $E_{\mathbf{A}}(P, \varepsilon)$ наделено своей топологией произведения и что последняя совпадает с топологией, индуцированной топологией пространства $E_{\mathbf{A}}$. Ясно, что ε_v является k_v-решеткой в E_v и, следовательно, открытым и компактным подножеством в E_v для всякой конечной точки v. Поэтому $E_{\mathbf{A}}(P, \varepsilon)$ — открытая подгруппа в $E_{\mathbf{A}}(P', \varepsilon)$, если $P \subset P'$. Возьмем какой-нибудь базис ε' в E над k и с его помощью определим изоморфизм k^n на E и, следовательно, $(k_{\mathbf{A}})^n$ на $E_{\mathbf{A}}$. Из наших определений сразу видно, что $E_{\mathbf{A}}$ является объединением множеств $E_{\mathbf{A}}(P, \varepsilon')$ и что эти множества открыты в $E_{\mathbf{A}}$. По следствию 1 из теор. 3 гл. III-1 существует такое конечное множество P_0 точек поля k, содержащее P_∞, что $\varepsilon_v = \varepsilon'_v$ для v, не лежащих в P_0. Отсюда видно, что $E_{\mathbf{A}}$ является объединением множеств $E_{\mathbf{A}}(P, \varepsilon)$, а также что при $P' \supset P \cup P_0$ множество $E_{\mathbf{A}}(P, \varepsilon)$ открыто в $E_{\mathbf{A}}(P', \varepsilon')$, а следовательно, в $E_{\mathbf{A}}$. Разумеется, можно было бы использовать предложение 1 для непосредственного определения топологии на $E_{\mathbf{A}}$, в точности так же, как выше была определена топология на $k_{\mathbf{A}}$; тогда из следствия 1 теор. 3 гл. III-1 вытекала бы независимость этой топологии от выбора ε.

Следствие 1. *В предположениях и обозначениях предложения 1 пусть C — компактное подмножество в $E_{\mathbf{A}}$. Тогда существует такое конечное множество P точек поля k, что $C \subset E_{\mathbf{A}}(P, \varepsilon)$.*

Так как C содержится в объединении открытых множеств $E_{\mathbf{A}}(P, \varepsilon)$, то оно должно содержаться в объединении конечного числа таких множеств $E_{\mathbf{A}}(P_i, \varepsilon)$, а следовательно, в $E_{\mathbf{A}}(P, \varepsilon)$ при $P = \bigcup P_i$.

Пусть $\mathcal{A}$ — любая алгебра конечной размерности над k. Мы будем обозначать через $\mathcal{A}_{\mathbf{A}}$ топологическое кольцо, полученное продолжением на пространство $\mathcal{A}_{\mathbf{A}}$ указанным выше способом закона умножения на $\mathcal{A}$. Ясно, что можно рассматривать $\mathcal{A}_{\mathbf{A}}$ как алгебру над $k_{\mathbf{A}}$, и $k_{\mathbf{A}} \cdot 1_{\mathbf{A}}$ является замкнутым подпространством и подкольцом в $\mathcal{A}_{\mathbf{A}}$, изоморфным $k_{\mathbf{A}}$.

Следствие 2. *Пусть $\mathcal{A}$ — алгебра конечной размерности над k и α — конечное подмножество в $\mathcal{A}$, содержащее базис векторного пространства $\mathcal{A}$ над k. Для всякой конечной точки v поля k*

обозначим через α_v r_v*-модуль, порожденный подмножеством* α *в* $\mathcal{A}_v$. *Для всякого конечного множества* P *точек поля* k, *содержащего* P_∞, *запишем*

$$\mathcal{A}_{\mathbf{A}}(P, \alpha) = \prod_{v \in P} \mathcal{A}_v \times \prod_{v \notin P} \alpha_v.$$

Тогда существует множество P_0, *обладающее тем свойством, что* $\mathcal{A}_{\mathbf{A}}(P, \alpha)$ *является открытым подкольцом в* $\mathcal{A}_{\mathbf{A}}$ *для любого* $P \supset P_0$, *и* $\mathcal{A}_{\mathbf{A}}$ *есть объединение этих подколец.*

Это сразу вытекает из следствия 2 теор. 3 гл. III-1 и из предложения 1.

Возьмем теперь алгебраическое расширение k' поля k конечной степени. Так как k' является **A**-полем, то мы можем применить к нему нашу общую конструкцию и получить таким образом кольцо $k'_{\mathbf{A}}$ его аделей. С другой стороны, мы можем считать k' алгеброй над k и применить к этой алгебре описанную выше конструкцию, что дает кольцо, которое мы обозначим через $(k'/k)_{\mathbf{A}}$. Как мы видели, это — алгебра над $k_{\mathbf{A}}$; она содержит замкнутое подкольцо $k_{\mathbf{A}} \cdot 1_{k'}$, которое мы очевидным образом отождествим с $k_{\mathbf{A}}$. Центральным в теории аделей является тот факт, что определенные таким образом кольца $k'_{\mathbf{A}}$ и $(k'/k)_{\mathbf{A}}$ канонически изоморфны. Это будет доказано сейчас, но лишь для случая, когда k' сепарабельно над k. Несепарабельный случай будет разобран в гл. VII-6.

Теорема 1. *Пусть* k — *некоторое* **A**-*поле и* k' — *его сепарабельное алгебраическое расширение конечной степени над* k. *Тогда существует единственный изоморфизм* Φ *из* $(k'/k)_{\mathbf{A}}$ *на* $k'_{\mathbf{A}}$ *со следующими свойствами*: (i) Φ *индуцирует тождественное отображение на* k', *если* k' *естественно вложено как в* $(k'/k)_{\mathbf{A}}$, *так и в* $k'_{\mathbf{A}}$; (ii) *на всяком квазисомножителе* $(k'/k)_v$ *в* $(k'/k)_{\mathbf{A}}$ *изоморфизм* Φ *индуцирует* k_v*-линейный изоморфизм* Φ_v *алгебры* $(k'/k)_v$ *на произведение квазисомножителей* k'_w *в* $k'_{\mathbf{A}}$, *соответствующих точкам* w *поля* k', *лежащим над* v.

Обозначим через $\mathcal{A}$ алгебру k'/k, т. е. поле k', рассматриваемое как алгебра над k. Тогда в объясненных выше обозначениях $\mathcal{A}_{\mathbf{A}}$ совпадает с $(k'/k)_{\mathbf{A}}$, а $\mathcal{A}_v$ совпадает с $(k'/k)_v$, т. е. с алгеброй $k' \otimes_k k_v$ над k_v, которой мы занимались в гл. III-4. Для конечного числа слагаемых прямая сумма означает то же самое, что произведение. Поэтому мы можем интерпретировать теорему 4 гл. III-4 как определяющую изоморфизм Φ_v из $(k'/k)_v$ на произведение $\prod k'_w$ полей k'_w по всем точкам w, лежащим над v. Этот изоморфизм k_v-линеен и отображает каждый элемент $\xi \in k'$ на элемент $(\xi, \ldots, \xi)$ в $\prod k'_w$;

он однозначно характеризуется этими свойствами. Аналогичным образом если мы выберем какой-нибудь базис α в k' над k, то та же самая теорема показывает, что почти для всех v изоморфизм Φ_v отображает α_v на произведение $\prod r'_w$ максимальных компактных подколец в полях k'_w. Пусть P_0 — такое содержащее P_∞ конечное множество точек поля k, что Φ_v обладает этим свойством для всех v, не лежащих в P_0. Для всякой точки w поля k' обозначим через $f(w)$ точку поля k, лежащую под v. Тогда при $P \supset P_0$ отображения Φ_v очевидным образом определяют изоморфизм Φ_P из $\mathcal{A}_\mathbf{A}(P, \alpha)$ на $k'_\mathbf{A}(f^{-1}(P))$, где $\mathcal{A}_\mathbf{A}(P, \alpha)$ — открытое подкольцо в $\mathcal{A}_\mathbf{A} = (k'/k)_\mathbf{A}$, определенное в следствии 2 предл. 1. Так как каждое множество $f^{-1}(P)$ конечно и каждое конечное множество P' точек поля k' содержится в $f^{-1}(P)$ при $P = f(P')$, то $k'_\mathbf{A}$ является объединением множеств $k'_\mathbf{A}(f^{-1}(P))$ при $P \supset P_0$. Поскольку Φ_{P_1} совпадает с Φ_P на области определения Φ_P при $P_1 \supset P$, то существует изоморфизм Φ из $\mathcal{A}_\mathbf{A}$ на $k'_\mathbf{A}$, который совпадает с Φ_P на его области определения для любого $P \supset P_0$. Теперь ясно, что Φ обладает свойствами, сформулированными в нашей теореме, и что он однозначно характеризуется этими свойствами.

Следствие 1. *В предположениях и обозначениях теоремы* 1 *для каждой точки w поля k' обозначим через $f(w)$ точку поля k, лежащую под w. Тогда если $x = (x_v) \in k_\mathbf{A}$, то $\Phi(x)$ есть такой элемент $y = (y_w)$ в $k'_\mathbf{A}$, что $y_w = x_{f(w)}$ для каждой точки w поля k'.*

Это сразу следует из того факта, что $\Phi(1) = 1$, и из k_v-линейности Φ_v для каждой точки v.

Начиная с этого места, $k_\mathbf{A}$ будет обычно отождествляться со своим образом в $k'_\mathbf{A}$ при изоморфизме, индуцированном на $k_\mathbf{A}$ описанным в следствии 1 изоморфизмом Φ. Ясно, что $k_\mathbf{A}$ будет при этом замкнутым подкольцом в $k'_\mathbf{A}$.

Следствие 2. *Пусть k и k' таковы, как в теореме* 1, *и пусть E/k' — векторное пространство конечной размерности над k'. Обозначим через E/k то же пространство, рассматриваемое как векторное пространство над k. Тогда тождественное отображение из E/k на E/k' может быть однозначно продолжено до $k_\mathbf{A}$-линейного отображения из $(E/k)_\mathbf{A}$ в $(E/k')_\mathbf{A}$, и это продолжение является изоморфизмом из $(E/k)_\mathbf{A}$ на $(E/k')_\mathbf{A}$.*

Для $E = k'$ — это, ввиду следствия 1, простая переформулировка теоремы 1. Отсюда немедленно следует справедливость нашего утверждения для случая $E = k'^n$, а следовательно, и для общего случая, потому что E можно всегда отождествить с пространством k'^n, выбрав некоторый базис.

В соответствии с данными выше определениями k-линейная форма $\mathrm{Tr}_{k'/k}$ и полиномиальная функция $\mathrm{N}_{k'/k}$ на пространстве k', рассматриваемом как векторное пространство над k, могут быть продолжены до отображений $\mathrm{Tr}_{k'/k}$, $\mathrm{N}_{k'/k}$ из $(k'/k)_{\mathbf{A}}$ в $k_{\mathbf{A}}$. При этом $\mathrm{Tr}_{k'/k} \circ \Phi^{-1}$ и $\mathrm{N}_{k'/k} \circ \Phi^{-1}$ суть отображения из $k'_{\mathbf{A}}$ в $k_{\mathbf{A}}$. Упростим формулировку нашего очередного следствия, отождествив $(k'/k)_{\mathbf{A}}$ с $k'_{\mathbf{A}}$ посредством изоморфизма Φ, так что последние наши два отображения можно записать просто как $\mathrm{Tr}_{k'/k}$ и $\mathrm{N}_{k'/k}$.

Следствие 3. *Пусть $x' = (x'_w)$ — любой элемент из $k'_{\mathbf{A}}$. Положим $y = \mathrm{Tr}_{k'/k}(x')$ и $z = \mathrm{N}_{k'/k}(x')$. Тогда y, z являются элементами (y_v), (z_v) из $k_{\mathbf{A}}$, задаваемыми соответственно равенствами*

$$y_v = \sum_{w \mid v} \mathrm{Tr}_{k'_w/k_v}(x'_w), \quad z_v = \prod_{w \mid v} \mathrm{N}_{k'_w/k_v}(x'_w)$$

для каждой точки v поля k, где сумма и произведение берутся по всем точкам w поля k', лежащим над v.

Это непосредственно следует из предложения 4 гл. III-3 и теоремы 1.

§ 2. ОСНОВНЫЕ ТЕОРЕМЫ

Ввиду леммы 1 гл. III-2 каждое $\mathbf{A}$-поле является сепарабельным алгебраическим расширением одного из полей $\mathbf{Q}$ или $\mathbf{F}_p(T)$. Теорема 1 § 1 дает нам возможность доказывать свойства адельных пространств, отправляясь от частных случаев $k = \mathbf{Q}$ и $k = \mathbf{F}_p(T)$. Этот метод принесет вскоре ряд важных результатов, для формулировки которых мы упростим обозначения, отождествив $\mathbf{A}$-поля и векторные пространства над такими полями при помощи объясненного в § 1 способа с их естественными образами в соответствующих адельных пространствах. В доказательствах мы снова используем φ для обозначения канонического вложения $\mathbf{A}$-поля k в $k_{\mathbf{A}}$.

Теорема 2. *Пусть k — некоторое $\mathbf{A}$-поле и E — конечномерное векторное пространство над k. Тогда E дискретно в $E_{\mathbf{A}}$ и факторпространство $E_{\mathbf{A}}/E$ компактно.*

Ввиду следствия 2 теор. 1 § 1 и леммы 1 гл. III-2 достаточно доказать это для $k = \mathbf{Q}$ и $k = \mathbf{F}_p(T)$. Если n — размерность пространства E, то E изоморфно k^n, так что если теорема доказана в случае $E = k$, то она справедлива и в общем случае. Таким образом, нам нужно разобрать только случаи $E = k = \mathbf{Q}$ и $E = k = \mathbf{F}_p(T)$. Начнем с $\mathbf{Q}$.

Для всякого простого числа p обозначим через $\mathbf{Q}^{(p)}$ множество таких ξ из $\mathbf{Q}$, что $|\xi|_{p'} \leqslant 1$ для всех простых p', отличных от p. Ясно, что это — подкольцо в $\mathbf{Q}$, состоящее из чисел вида $p^{-n}a$, где $n \in \mathbf{N}$ и $a \in \mathbf{Z}$.

Лемма 1. *Для каждого простого числа p имеем* $\mathbf{Q}_p = \mathbf{Q}^{(p)} + \mathbf{Z}_p$ *и* $\mathbf{Q}^{(p)} \cap \mathbf{Z}_p = \mathbf{Z}$.

Первое утверждение сразу вытекает из следствия 2 теор. 6 гл. I-4, примененного к $\mathbf{Q}_p$, простому элементу p и множеству представителей $\{0, 1, \ldots, p-1\}$. Второе очевидно.

Лемма 2. *Положим* $A_\infty = \mathbf{R} \times \prod \mathbf{Z}_p$ *и обозначим через* φ *каноническое вложение поля* $\mathbf{Q}$ *в* $\mathbf{Q}_\mathbf{A}$. *Тогда* $\mathbf{Q}_\mathbf{A} = \varphi(\mathbf{Q}) + A_\infty$ *и* $\varphi(\mathbf{Q}) \cap A_\infty = \varphi(\mathbf{Z})$.

Имеем $A_\infty = \mathbf{Q}_\mathbf{A}(\{\infty\})$, где использовано обозначение (1) § 1. Поэтому A_∞ является открытым подкольцом в $\mathbf{Q}_\mathbf{A}$. Второе утверждение леммы очевидно. Возьмем теперь любой элемент $x = (x_v)$ из $\mathbf{Q}_\mathbf{A}$. Обозначим через P множество таких простых p, что x_p не лежит в $\mathbf{Z}_p$; это множество конечно. Первая часть леммы 1 показывает, что для всякого $p \in P$ мы можем записать $x_p = \xi_p + x'_p$, где $\xi_p \in \mathbf{Q}^{(p)}$ и $x'_p \in \mathbf{Z}_p$. Для $p \notin P$ положим $\xi_p = 0$ и $x'_p = x_p$. Положим, далее, $\xi = \sum \xi_p$, где сумма берется по всем p, и $y = x - \varphi(\xi)$. Если $y = (y_v)$, то для каждого простого числа p имеем

$$y_p = x_p - \xi_p - \sum_{p' \neq p} \xi_{p'} = x'_p - \sum_{p' \neq p} \xi_{p'}.$$

По определению $\mathbf{Q}^{(p)}$ все члены в правой части лежат в $\mathbf{Z}_p$. Отсюда видно, что y лежит в A_∞, следовательно, x лежит в $\varphi(\mathbf{Q}) + A_\infty$.

Теперь мы можем доказать нашу теорему для случая $E = k = \mathbf{Q}$. Так как A_∞ открыто в $\mathbf{Q}_\mathbf{A}$, то первое утверждение будет доказано, если показать, что множество $\varphi(\mathbf{Q}) \cap A_\infty$, т. е. $\varphi(\mathbf{Z})$ дискретно в A_∞. Но это очевидно, поскольку проекция множества $\varphi(\mathbf{Z})$ на сомножитель $\mathbf{R}$ произведения A_∞ равна $\mathbf{Z}$, а $\mathbf{Z}$ дискретно в $\mathbf{R}$. Обозначим теперь через I замкнутый интервал $[-1/2, 1/2]$ в $\mathbf{R}$ и положим $C = I \times \prod \mathbf{Z}_p$. Ясно, что $A_\infty = \varphi(\mathbf{Z}) + C$, откуда $\mathbf{Q}_\mathbf{A} = \varphi(\mathbf{Q}) + C$. Поскольку C компактно, этим доказательство и заканчивается.

При $E = k = \mathbf{F}_p(T)$ доказательство аналогично и даже проще. Для всякой точки v поля k обозначим через $k^{(v)}$ множество таких элементов ξ из k, что $|\xi|_w \leqslant 1$ для всех точек w поля k, отличных от v.

Лемма 3. *Для каждой точки v поля k имеем* $k_v = k^{(v)} + r_v$ *и* $k^{(v)} \cap r_v = \mathbf{F}_p$.

Последнее утверждение очевидно ввиду определения функции $|\xi|_v$ на k, которое было дано в доказательстве теоремы 2 гл. III-1. Что касается первого утверждения, то достаточно рассмотреть точку, связанную с неприводимым многочленом π из $\mathbf{F}_p[T]$, поскольку в противном случае мы просто заменим T на T^{-1}. В этом случае наше утверждение сразу вытекает из следствия 2 теор. 6 гл. I-4, примененного к k_v, к простому элементу π и к множеству представителей, которое дается следствием теор. 2 гл. III-1.

Лемма 4. *Положим* $A_0 = \prod r_v$. *Тогда* $k_{\mathbf{A}} = \varphi(k) + A_0$ *и* $\varphi(k) \cap A_0 = \varphi(\mathbf{F}_p)$.

Имеем $A_0 = k_{\mathbf{A}}(\varnothing)$, где опять используется обозначение (1) § 1. Это — компактное открытое подкольцо в $k_{\mathbf{A}}$. Последнее утверждение снова очевидно. Возьмем какое-нибудь $x = (x_v)$ из $k_{\mathbf{A}}$. Лемма 3 показывает, что для каждой v, для которой $|x_v|_v > 1$, мы можем записать $x_v = \xi_v + x'_v$, где $\xi_v \in k^{(v)}$ и $x'_v \in r_v$. Для всех других точек v положим $\xi_v = 0$ и $x'_v = x_v$. Положим далее $\xi = \sum \xi_v$ и $y = x - \varphi(\xi)$. Точно так же, как в доказательстве леммы 2, получаем, что $y \in A_0$.

Наша теорема теперь очевидна для $E = k = \mathbf{F}_p(T)$, поскольку A_0 компактно и открыто в $k_{\mathbf{A}}$ и поле $\mathbf{F}_p$ конечно. Доказательство теоремы закончено.

Теперь мы рассмотрим векторное пространство E над $\mathbf{A}$-полем k, алгебраически двойственное к нему пространство E' и соответствующие адельные пространства $E_{\mathbf{A}}$, $E'_{\mathbf{A}}$. Мы обозначаем через $[e, e']$ значение в точке $e \in E$ линейной формы, определяемой точкой $e' \in E'$, и используем то же самое обозначение для продолжения этой билинейной формы на $E_{\mathbf{A}} \times E'_{\mathbf{A}}$. Так как аддитивная группа пространства $E_{\mathbf{A}}$ является локально компактной коммутативной группой, то можно рассмотреть топологическую двойственную к ней группу, которую обозначим через $E^*_{\mathbf{A}}$. Обозначим, далее, через $\langle e, e^* \rangle$ значение в точке $e \in E_{\mathbf{A}}$ характера, определяемого точкой $e^*_{\mathbf{A}} \in E^*$. В этих обозначениях справедлива

Теорема 3. *Пусть k — некоторое $\mathbf{A}$-поле и χ — нетривиальный характер на $k_{\mathbf{A}}$, тривиальный на k. Пусть E — конечномерное векторное пространство над k, E' — алгебраическое двойственное к нему, а $E^*_{\mathbf{A}}$ — топологическое двойственное к $E_{\mathbf{A}}$. Тогда формула*

$$\langle e, e^* \rangle = \chi([e, e']) \text{ для всех } e \in E_{\mathbf{A}}$$
$$(e' \in E'_{\mathbf{A}},\ e^* \in E^*_{\mathbf{A}})$$

определяет изоморфизм $e' \to e^*$ *из* $E'_{\mathbf{A}}$ *на* $E^*_{\mathbf{A}}$. *Кроме того, если* e' *таков, что* $\chi([e, e']) = 1$ *при всех* $e \in E$, *то* $e' \in E'$.

Последнее утверждение означает, что определенный в нашей теореме изоморфизм $e' \to e^*$ из $E'_{\mathbf{A}}$ на $E^*_{\mathbf{A}}$ отображает E' на подгруппу в $E^*_{\mathbf{A}}$, ассоциированную по двойственности с дискретной подгруппой E в $E_{\mathbf{A}}$.

Мы начнем с рассмотрения случая $E = k = \mathbf{Q}$. Используем снова те же обозначения, что и в первой части доказательства теоремы 2. Ввиду леммы 2 каждый характер на A_∞, тривиальный на $\varphi(\mathbf{Z})$, можно однозначно продолжить до характера на $\mathbf{Q}_{\mathbf{A}}$, тривиального на $\varphi(\mathbf{Q})$. Мы получим такой характер χ, положив $\chi(x) = \mathbf{e}(-x_\infty)$ при $x = (x_v) \in A_\infty$ (напомним, что мы пишем $\mathbf{e}(t) = e^{2\pi i t}$ при $t \in \mathbf{R}$). Если мы продолжим этот характер до характера χ на $\mathbf{Q}_{\mathbf{A}}$, тривиального на $\varphi(\mathbf{Q})$, и для каждой точки v поля $\mathbf{Q}$ обозначим через χ_v характер на квазисомножителе $\mathbf{Q}_v$ в $\mathbf{Q}_{\mathbf{A}}$, индуцированный характером χ, то χ, очевидно, характеризуется следующими свойствами: этот характер тривиален на $\varphi(\mathbf{Q})$; характер χ_p тривиален на $\mathbf{Z}_p$ для каждого простого числа p и $\chi_\infty(x) = \mathbf{e}(-x)$ при $x \in \mathbf{R}$. Для вычисления χ_p рассмотрим снова группу $\mathbf{Q}^{(p)}$, определенную при доказательстве теоремы 2, и возьмем любое число $\xi \in \mathbf{Q}^{(p)}$. Тогда $\xi \in \mathbf{Z}_{p'}$ для всех простых $p' \neq p$, так что по формуле 2 § 1 имеем

$$1 = \chi(\varphi(\xi)) = \chi_\infty(\xi)\,\chi_p(\xi) = \mathbf{e}(-\xi)\,\chi_p(\xi)$$

и потому $\chi_p(\xi) = \mathbf{e}(\xi)$. По лемме 1 характер χ_p вполне определяется этим свойством и тем фактом, что он тривиален на $\mathbf{Z}_p$. Его ядро совпадает с $\mathbf{Z}_p$. Поэтому этот характер имеет порядок 0 в смысле определения 4 гл. II-5.

Пусть теперь χ' — любой характер на $\mathbf{Q}_{\mathbf{A}}$. Для каждой точки v поля $\mathbf{Q}$ обозначим через χ'_v характер, индуцированный на квазисомножителе $\mathbf{Q}_v$ в $\mathbf{Q}_{\mathbf{A}}$ характером χ'. По следствию теор. 3 гл. II-5 можно однозначно записать χ'_v в виде $\chi'_v(x) = \chi_v(a_v x)$, где $a_v \in \mathbf{Q}_v$. Как мы отмечали, когда писали формулу (2) § 1, характер χ'_p должен быть тривиальным на $\mathbf{Z}_p$ почти для всех p, поскольку характер χ' непрерывен на $\mathbf{Q}_{\mathbf{A}}$. Отсюда следует, что $\chi_p(a_p) = 1$ и, следовательно, $a_p \in \mathbf{Z}_p$ почти для всех p. Поэтому $a = (a_v)$ лежит в $\mathbf{Q}_{\mathbf{A}}$, так что по формуле (2) § 1 χ' совпадает с характером χ_a на $\mathbf{Q}_{\mathbf{A}}$, задаваемым равенством $\chi_a(x) = \chi(ax)$ при всех $x \in \mathbf{Q}_{\mathbf{A}}$. Таким образом, мы показали, что отображение $a \to \chi_a$ из $\mathbf{Q}_{\mathbf{A}}$ в пространство $G = \mathbf{Q}^*_{\mathbf{A}}$ (топологическое двойственное к $\mathbf{Q}_{\mathbf{A}}$) сюръективно. Сразу видно, что оно непрерывно и инъективно, так что оно является биективным морфизмом из $\mathbf{Q}_{\mathbf{A}}$ на его двойственное пространство G. Обозначим через Γ подгруппу в G, ассоциированную по двойственности

с $\varphi(\mathbf{Q})$, т. е. состоящую из характеров на $\mathbf{Q}_\mathbf{A}$, тривиальных на $\varphi(\mathbf{Q})$. Поскольку характер χ обладает последним свойством, то это же верно для χ_a при всех $a \in \varphi(\mathbf{Q})$, так что $a \to \chi_a$ отображает $\varphi(\mathbf{Q})$ в Γ. Обратно, пусть b таков, что $\chi_b \in \Gamma$. Как и в доказательстве теоремы 2 для $\mathbf{Q}$, положим $C = I \times \prod \mathbf{Z}_p$, где $I = [-1/2, 1/2]$. Мы показали там, что $\mathbf{Q}_\mathbf{A} = \varphi(\mathbf{Q}) + C$. Поэтому можно записать b в виде $b = \varphi(\xi) + c$, где $c \in C$, $\xi \in \mathbf{Q}$, и, значит, $\chi_c \in \Gamma$. Записав $c = (c_v)$ и используя тот факт, что $c_p \in \mathbf{Z}_p$ при всех p, имеем

$$1 = \chi_c(\varphi(1)) = \chi(c) = \chi_\infty(c_\infty) = \mathbf{e}(-c_\infty),$$

откуда $c_\infty = 0$, ибо $c_\infty \in I$. Поэтому характер χ_c тривиален на $A_\infty = \mathbf{R} \times \prod \mathbf{Z}_p$. Так как он тривиален и на $\varphi(\mathbf{Q})$, то лемма 2 показывает, что он тривиален на $\mathbf{Q}_\mathbf{A}$, так что $c = 0$, откуда $b \in \varphi(\mathbf{Q})$. Поэтому $a \to \chi_a$ отображает $\varphi(\mathbf{Q})$ на Γ. Наконец, поскольку подгруппа $\varphi(\mathbf{Q})$ дискретна в $\mathbf{Q}_\mathbf{A}$ и $\mathbf{Q}_\mathbf{A}/\varphi(\mathbf{Q})$ компактна, из теории двойственности следует, что Γ дискретна в G и что G/Γ компактна. Следовательно, $a \to \chi_a$ определяет биективный морфизм компактной группы $\mathbf{Q}_\mathbf{A}/\varphi(\mathbf{Q})$ на компактную группу G/Γ. Хорошо известно, что такой морфизм обязан быть изоморфизмом. Так как G «локально изоморфна» с G/Γ, а $\mathbf{Q}_\mathbf{A}$ с $\mathbf{Q}_\mathbf{A}/\varphi(\mathbf{Q})$, отсюда следует, что отображение $a \to \chi_a$ непрерывно в обе стороны, так что оно является изоморфизмом. Этим заканчивается наше доказательство для $E = k = \mathbf{Q}$.

Возьмем теперь $E = k = \mathbf{F}_p(T)$. По аналогии со случаем $k = \mathbf{Q}$ обозначим через ∞ точку поля k, для которой T^{-1} является простым элементом (хотя это, разумеется, не бесконечная точка). Имеем $|T^{-1}|_\infty = p^{-1}$. Мы можем теперь применить к k_∞, к простому элементу T^{-1} и к множеству представителей $\mathbf{F}_p$ следствие 2 теор. 6 гл. I-4 и, согласно этому следствию, отождествить k_∞ с полем формальных степенных рядов

$$x = \sum_{i=n}^{+\infty} a_i T^{-i}, \tag{3}$$

где $n \in \mathbf{Z}$ и $a_i \in \mathbf{F}_p$ при всех $i \geqslant n$. Обозначим через ψ характер аддитивной группы поля $\mathbf{F}_q$, для которого $\psi(1) = \mathbf{e}(1/p)$. Определим характер χ_∞ на k_∞, положив $\chi_\infty(x) = \psi(-a_1)$, где x задается формулой (3); при $x \in \mathbf{F}_p(T)$ имеем $a_1 = 0$, откуда $\chi_\infty(x) = 1$. Положим теперь $A_\infty = k_\infty \times \prod r_v$, где произведение берется по всем точкам v поля k, отличным от ∞. Используя обозначение (1) § 1, получаем $A_\infty = k_\mathbf{A}(\{\infty\})$. Это — открытое подкольцо в $k_\mathbf{A}$, содержащее множество A_0, определенное в лемме 4, так что по этой лемме $k_\mathbf{A} = \varphi(k) + A_\infty$. Если $\xi \in k$, то $\varphi(\xi)$ лежит в A_∞ в том

и только в том случае, когда $|\xi|_v \leqslant 1$ для всех точек v поля k, связанных с неприводимыми многочленами из $\mathbf{F}_p(T)$, т. е. в том и только в том случае, когда ξ лежит в $\mathbf{F}_p(T)$. Это означает, что $\varphi(k) \cap A_\infty = \varphi(\mathbf{F}_p[T])$. В соответствии с этим каждый характер на A_∞, тривиальный на $\varphi(\mathbf{F}_p[T])$, можно однозначно продолжить до характера на $k_\mathbf{A}$, тривиального на $\varphi(k)$. Применяя это к характеру χ на A_∞, для которого $\chi(x) = \chi_\infty(x_\infty)$ при $x = (x_v) \in A_\infty$, получаем характер χ на $k_\mathbf{A}$, который можно охарактеризовать следующими свойствами: χ тривиален на $\varphi(k)$; для каждой точки $v \neq \infty$ характер χ_v, индуцированный на k_v характером χ, тривиален на r_v; χ индуцирует на k_∞ характер χ_∞, определенный выше. Для вычисления характера χ_v, где точка v связана с неприводимым многочленом π степени δ из $\mathbf{F}_p(T)$, обозначим через $k_0^{(v)}$ множество таких элементов ξ из k, что $|\xi|_w \leqslant 1$ для всех точек w поля k, отличных от v, и $|\xi|_\infty < 1$. Те же самые рассуждения, что и использовавшиеся в доказательстве леммы 3, показывают сейчас, что k_v разлагается в прямую сумму $k_0^{(v)}$ и r_v. Так как характер χ_v тривиален на r_v, он вполне определен своими значениями на $k_0^{(v)}$. Возьмем $\xi \in k_0^{(v)}$; этот элемент можно записать как $\xi = \pi^{-n}\alpha$, где $n \in \mathbf{N}$ и α — многочлен степени $< n\delta$ из $\mathbf{F}_p[T]$. Обозначим через a_1 коэффициент при $T^{n\delta-1}$ в α. Так как многочлен π унитарен, то его можно записать в виде $T^\delta\omega$, где ω лежит в $\mathbf{F}_p[T^{-1}]$ и имеет свободный член, равный 1. Отсюда вытекает, что

$$\xi = \pi^{-n}\alpha = \omega^{-n}T^{-n\delta}\alpha \equiv a_1T^{-1} \quad (T^{-2})$$

в кольце r_∞, откуда $\chi_\infty(\xi) = \psi(-a_1)$ по определению χ_∞. По формуле (2) § 1 имеем

$$1 = \chi(\varphi(\xi)) = \chi_\infty(\xi)\,\chi_v(\xi) = \psi(-a_1)\,\chi_v(\xi),$$

поэтому $\chi_v(\xi) = \psi(a_1)$, чем завершается определение характера χ_v. Далее, если ξ таков, как выше, и отличен от нуля, то обозначим через d степень многочлена α и через a коэффициент при T^d в α. Тогда $\chi_v(\xi T^{n\delta-1-d})$ принимает значение $\psi(a)$, которое не равно 1, поскольку $a \neq 0$. Это показывает, что если ξ — ненулевой элемент в $k_0^{(v)}$, то $\chi_v(\xi t)$ не может равняться 1 при всех $t \in r_v$. Так как характер χ_v тривиален на r_v и так как $k_v = k_0^{(v)} + r_v$, то с учетом предложения 12 гл. II-5 заключаем, что характер χ_v имеет порядок 0 в смысле определения 4 гл. II-5. Другими словами, если элемент x из k_v таков, что $\chi_v(xt) = 1$ при всех $t \in r_v$, то x должен лежать в r_v.

Теперь мы можем продолжить доказательство точно так же, как в случае $k = \mathbf{Q}$. Пусть χ' — любой характер на $k_\mathbf{A}$. Для всякой точки v поля k характер χ'_v, индуцированный на k_v характером χ, можно записать в виде $\chi'_v(x) = \chi_v(a_v x)$, где $a_v \in k_v$. Из того факта,

что характер χ'_v должен быть тривиален на r_v почти для всех v, вытекает, что элемент $a = (a_v)$ лежит в k_A, так что χ' совпадает с характером χ_a, определенным формулой $\chi_a(x) = \chi(ax)$. Как и прежде, мы видим, что отображение $a \to \chi_a$ является биективным морфизмом из k_A на группу $G = k_A^*$ (топологическую двойственную к k_A) и что этот морфизм отображает $\varphi(k)$ в подгруппу $\Gamma \subset G$, ассоциированную по двойственности с $\varphi(k)$. Предположим, что $\chi_b \in \Gamma$ при некотором $b \in k_A$. Согласно лемме 4 мы можем записать b в виде $b = \varphi(\xi) + c$, где $\xi \in k$, $c \in A_0$. Очевидно, χ_c тривиален на $\varphi(k)$. Положим $c = (c_v)$, так что $c_v \in r_v$ при всех v. Существует такой элемент $\gamma \in \mathbf{F}_p$, что $c_\infty \equiv \gamma\ (T^{-1})$. Заменяя ξ на $\xi + \gamma$ и c на $c - \varphi(\gamma)$, получаем, что $c_\infty \equiv 0\ (T^{-1})$. Далее имеем

$$1 = \chi_A(\varphi(1)) = \chi(c) = \chi_\infty(c_\infty),$$

откуда ввиду определения χ_∞ следует, что c_∞ лежит в $T^{-2}r_\infty$ и, значит, $\chi_\infty(c_\infty t) = 1$ при всех $t \in r_\infty$. Следовательно, характер χ_c тривиален на A_0, а потому и на k_A (лемма 4). Таким образом, $c = 0$ и, значит, $b \in \varphi(k)$. Заканчивается доказательство точно так же, как в случае $k = \mathbf{Q}$.

Теперь мы можем завершить доказательство нашей теоремы чисто формальным рассуждением. Обозначим через $T(E/k, \chi)$ утверждение теоремы 3. То, что мы уже доказали, можно выразить, сказав, что для каждого из полей $k = \mathbf{Q}$ и $k = \mathbf{F}_p(T)$ существует характер χ на k_A, для которого выполняется $T(k/k, \chi)$. Отсюда, очевидно, следует справедливость $T(k^n/k, \chi)$ для каждого n, так что $T(E/k, \chi)$ выполняется для каждого векторного пространства E над k. Возьмем, в частности, конечное алгебраическое расширение k' поля k. Как и в лемме 3 гл. III-3, обозначим через E пространство k', рассматриваемое как векторное пространство над k; выберем k-линейную форму λ на E, отличную от 0, и отождествим E с алгебраическим двойственным к нему пространством E', полагая $[x, y] = \lambda(xy)$. Мы можем тогда продолжить λ до отображения из E_A в k_A и тем самым продолжить отождествление пространств E и E' до отождествления пространств E_A и E'_A. Поэтому мы имеем опять $[x, y] = \lambda(xy)$ при $x, y \in E_A = (k'/k)_A$. Положим $\chi' = \chi \circ \lambda$. Это, очевидно, нетривиальный характер на E_A, тривиальный на E. Предположим теперь, что k' сепарабельно над k. Тогда мы можем отождествить E_A с k'_A посредством изоморфизма Φ, описанного в теореме 1 § 1. При этом χ' перейдет в нетривиальный характер на k'_A, тривиальный на k', и утверждение $T(E/k, \chi)$ превращается в точности в утверждение $T(k'/k', \chi')$. Так как в качестве k' можно взять любое $\mathbf{A}$-поле, взяв в качестве k или $\mathbf{Q}$,

или $\mathrm{F}_p(T)$, то мы убеждаемся, что для каждого A-поля $\boldsymbol{k}$ теорема 3 верна по меньшей мере при одном выборе характера χ. Предположим теперь, что $T(\boldsymbol{k}/\boldsymbol{k}, \chi)$ справедливо для всякого такого поля, и пусть χ_1 — еще один характер с указанными в теореме 3 свойствами. Из $T(\boldsymbol{k}/\boldsymbol{k}, \chi)$ следует, что χ_1 имеет вид $\chi_1(x) = \chi(ax)$, где $a \in \boldsymbol{k}$ и $a \neq 0$. Тогда отображение $e' \to e^*$, определенное, как в теореме 3, но с помощью χ_1, является композицией аналогичного отображения, определенного с помощью χ, и отображения $e' \to ae'$ из $E'_{\mathbf{A}}$ в себя. Так как последнее отображение является, очевидно, автоморфизмом пространства $E'_{\mathbf{A}}$, отображающим E' на себя, то мы видим, что $T(E/k, \chi)$ эквивалентно $T(E/k, \chi_1)$. Этим наше доказательство завершено.

Следствие 1. *Пусть характер χ такой, как в теореме* 3. *Обозначим для каждой точки v поля k через χ_v характер, индуцированный характером χ на квазисомножителе k_v в k. Тогда для каждой точки v характер χ_v нетривиален и почти для всех конечных точек v поля k характер χ_v имеет порядок* 0 *в смысле определения* 4 *гл.* II-5.

Для всякого $a \in \boldsymbol{k}_{\mathbf{A}}$ обозначим через χ_a характер на $k_{\mathbf{A}}$, определенный формулой $\chi_a(x) = \chi(ax)$. Если бы χ был тривиален на квазисомножителе $\boldsymbol{k}_v$, то этот квазисомножитель лежал бы в ядре морфизма $a \to \chi_a$ из $\boldsymbol{k}_{\mathbf{A}}$ в топологическое двойственное к нему пространство. Поскольку по теореме 3 этот морфизм является изоморфизмом, это привело бы к противоречию. В частности, для каждой конечной точки v поля $\boldsymbol{k}$ мы можем положить $\nu(v) = \mathrm{ord}(\chi_v)$ в смысле определения 4 гл. II-5. Для всякого отображения $v \to n(v)$ множества конечных точек поля $\boldsymbol{k}$ в $\mathbf{Z}$ обозначим через $G(n)$ группу тех элементов $x = (x_v)$ из $\boldsymbol{k}_{\mathbf{A}}$, для которых $\mathrm{ord}(x_v) \geqslant n(v)$ для всех конечных точек v, и через $H(n)$ — подгруппу в $G(n)$, состоящую из таких элементов $x = (x_v)$ из $G(n)$, что $x_w = 0$ для всех бесконечных точек w поля $\boldsymbol{k}$. В силу определения топологии на $\boldsymbol{k}_{\mathbf{A}}$ (§ 1) очевидно, что группа $G(n)$ открыта в $k_{\mathbf{A}}$ тогда и только тогда, когда $n(v) \leqslant 0$ почти для всех v. Ясно также, что подгруппа $H(n)$ компактна, если $n(v) \geqslant 0$ почти для всех v. Обратно, по следствию 1 предл. 1 § 1 каждое компактное подмножество в $\boldsymbol{k}_{\mathbf{A}}$ содержится в одном из множеств $k_{\mathbf{A}}(P)$ (мы применяем обозначение (1) § 1), так что подгруппа $H(n)$ не может быть компактной, за исключением случая, когда $n(v) \geqslant 0$ почти для всех v. Поэтому это условие необходимо и достаточно для компактности $H(n)$. Теперь предложение 12 гл. II-5 в сочетании с тем фактом, что характер χ_w нетривиален для любой бесконечной точки поля $\boldsymbol{k}$, показывает, что множество тех элементов x из $k_{\mathbf{A}}$, для которых $\chi(xy) = 1$

при всех $y \in G(0)$, совпадает с $H(-\nu)$ и что множество тех элементов x, для которых $\chi(xy) = 1$ при всех $y \in H(0)$, совпадает с $G(-\nu)$. Отождествляя $k_{\mathbf{A}}$ с топологическим двойственным к нему пространством посредством изоморфизма, описанного в теореме 3, мы видим, что $H(-\nu)$ и $G(-\nu)$ являются подгруппами в $k_{\mathbf{A}}$, ассоциированными по двойственности с $G(0)$ и $H(0)$ соответственно. Так как группа $G(0)$ открыта, а $H(0)$ компактна, то из теории двойственности вытекает, что подгруппа $H(-\nu)$ должна быть компактной, а $G(-\nu)$ — открытой. Как мы уже видели, отсюда следует, что $-\nu(v) \geqslant 0$ почти для всех v и что $-\nu(v) \leqslant 0$ почти для всех v.

Следствие 2. *Пусть E — конечномерное векторное пространство над k, и пусть v — любая точка поля k. Тогда подгруппа $E + E_v$ всюду плотна в $E_{\mathbf{A}}$.*

Если это справедливо для $E = k$, то, очевидно, верно и для $E = k^n$, а потому и для любого E. Если бы подгруппа $k + k_v$ не была плотна в $k_{\mathbf{A}}$, то существовал бы нетривиальный характер на $k_{\mathbf{A}}$, который был бы тривиален как на k, так и на k_v; но это противоречит следствию 1.

Как и в случае локальных полей, часто бывает удобно, выбрав раз и навсегда *базисный характер* χ со свойствами, описанными в теореме 3, отождествлять для всех конечномерных векторных пространств E над k топологическое двойственное к $E_{\mathbf{A}}$ с пространством $E'_{\mathbf{A}}$ посредством изоморфизма из этой теоремы. Для каждого квазисомножителя k_v и $k_{\mathbf{A}}$ в качестве базисного характера будет при этом браться характер χ_v, индуцированный на k_v характером χ, и этот характер χ_v будет использоваться для отождествления топологических и алгебраических двойственных к векторным пространствам над k_v, как объяснялось в гл. II-5. Имея все это в виду, получаем

Следствие 3. *Пусть предположения и обозначения таковы, как в предложении 1 § 1, и пусть E — векторное пространство над k и E' — алгебраическое двойственное к нему. Пусть, далее, ε, ε' — конечные подмножества в E и в E' соответственно, содержащие базисы этих пространств над k. Для каждой точки v поля k отождествим E'_v с топологическим двойственным к E_v, как описано выше. Тогда почти для всех конечных точек v поля k k_v-решетка ε'_v двойственна к ε_v.*

Для $E = E' = k$ и $\varepsilon = \varepsilon' = \{1\}$ это просто переформулировка следствия 1; в случае когда $\varepsilon = \{e_1, \ldots, e_n\}$ является базисом в E и $\varepsilon' = \{e'_1, \ldots, e'_n\}$ — двойственный базис в E' (для которого

$[e_i, e'_j] = 1$ при $i = j$ и 0 при $i \neq j$), это немедленно вытекает из того же следствия. Отсюда с помощью следствия 1 теор. 3 гл. III-1 сразу получаем наше утверждение в общем случае.

§ 3. ИДЕЛИ

Как и прежде (см. гл. III-3), если E — векторное пространство конечной размерности над полем k, то мы обозначаем через End (E) кольцо эндоморфизмов пространства E, рассматриваемое как алгебра над k. Мы будем обозначать через Aut (E) группу автоморфизмов пространства E, т. е. группу End $(E)^\times$ обратимых элементов в End (E). Эта группа совпадает с подмножеством в End (E), определяемым условием $\det(a) \neq 0$. Поэтому если k — топологическое поле, то Aut (E) является открытым подмножеством в End (E). Ясно, что в топологии, индуцированной топологией из End (E), Aut (E) является топологической группой. Если K — поле, содержащее поле k, то End (E_K) совпадает с End $(E)_K$ = End $(E) \otimes_k K$ и определитель на End (E_K) совпадает с продолжением на это пространство определителя на End (E).

Пусть $\mathcal{A}$ — алгебра конечной размерности над k. Обозначим через ρ ее регулярное представление в End $(\mathcal{A})$, определенное в гл. III-3, и как обычно обозначим через $\mathcal{A}^\times$ группу обратимых элементов из $\mathcal{A}$. Возьмем произвольный элемент a из $\mathcal{A}$. Очевидно, $\rho(a)$ есть эндоморфизм $x \to ax$ векторного пространства $\mathcal{A}$. Если $\rho(a)$ — автоморфизм, то он сюръективен, так что существует $b \in \mathcal{A}$, для которого $ab = 1_{\mathcal{A}}$. Тогда $b = a^{-1}$ и $a \in \mathcal{A}^\times$. Поскольку обратное утверждение тривиально, отсюда видно, что $\mathcal{A}^\times$ совпадает с подмножеством в $\mathcal{A}$, определенным условием $N_{\mathcal{A}/k}(a) \neq 0$. Поэтому если k — топологическое поле, то $\mathcal{A}^\times$ — открытое подмножество в $\mathcal{A}$. Кроме того, тогда ρ является топологическим изоморфизмом из $\mathcal{A}$ на подалгебру в End $(\mathcal{A})$, отображающим $\mathcal{A}^\times$ на $\rho(\mathcal{A}) \cap$ Aut $(\mathcal{A})$. Отсюда следует, что $\mathcal{A}^\times$ является тогда топологической группой в топологии, индуцированной топологией из $\mathcal{A}$.

Пусть теперь $\mathcal{A}$ — алгебра конечной размерности над A-полем k. Рассмотрим группу $\mathcal{A}_{\mathrm{A}}^\times$ обратимых элементов кольца $\mathcal{A}_{\mathrm{A}}$. Простейшие примеры в случае $\mathcal{A} = k$ показывают, что отображение $x \to x^{-1}$ не является непрерывным на этой группе в топологии, индуцированной топологией из $\mathcal{A}_{\mathrm{A}}$. Снабдим эту группу самой грубой топологией, для которой ее вложение в $\mathcal{A}_{\mathrm{A}}$ и отображение $x \to x^{-1}$ непрерывны. Более удобным образом это сделано в следующем определении.

Определение 2. *Пусть $\mathcal{A}$ — алгебра конечной размерности над* **A**-*полем* k. *Тогда мы обозначаем через $\mathcal{A}_{\mathbf{A}}^{\times}$ группу обратимых элементов кольца $\mathcal{A}_{\mathbf{A}}$, наделенную топологией, для которой отображение $x \to (x, x^{-1})$ является гомеоморфизмом $\mathcal{A}_{\mathbf{A}}^{\times}$ на ее образ в $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$.*

Обычно (особенно в случае $\mathcal{A} = k$) группу $\mathcal{A}_{\mathbf{A}}^{\times}$ с такой топологией называют *идельной группой* алгебры $\mathcal{A}$, а ее элементы называют *иделями* алгебры $\mathcal{A}$. Очевидно, что отображения $(x, y) \to xy$ и $x \to x^{-1}$ непрерывны на $\mathcal{A}_{\mathbf{A}}^{\times}$, так что наше определение превращает ее в топологическую группу. В то же время, если мы обозначим через f отображение $(x, y) \to xy$ из $\mathcal{A} \times \mathcal{A}$ в $\mathcal{A}$ и его естественное продолжение на $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$, то наше определение говорит, что множество $\mathcal{A}_{\mathbf{A}}^{\times}$ гомеоморфно подмножеству $f^{-1}(\{1\})$ последнего пространства. Так как отображение f непрерывно, то это подмножество замкнуто, так что группа $\mathcal{A}_{\mathbf{A}}^{\times}$ локально компактна. Ясно также, что группа $\mathcal{A}^{\times}$ канонически вложена в группу $\mathcal{A}_{\mathbf{A}}^{\times}$. Поскольку при отображении $x \to (x, x^{-1})$ группа $\mathcal{A}^{\times}$ переходит в пересечение множества $f^{-1}(\{1\})$ с дискретным подмножеством $\mathcal{A} \times \mathcal{A}$ в $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$, то это — дискретная подгруппа в $\mathcal{A}_{\mathbf{A}}^{\times}$.

Используя следствие 2 теор. 3 гл. III-1 и следствие 2 предл. 1 § 1, можно дать другое определение идельной группы алгебры $\mathcal{A}$, эквивалентное определению 2. Как и в упомянутых утверждениях, возьмем конечное подмножество α в $\mathcal{A}$, содержащее базис $\mathcal{A}$ над k, и для всякой конечной точки v поля k обозначим через α_v r_v-модуль, порожденный подмножеством α в $\mathcal{A}_v$. По следствию 2 теор. 3 гл. III-1 существует такое содержащее P_∞ конечное множество P_0 точек поля k, что для всех v, не лежащих в P_0, α_v является компактным подкольцом в $\mathcal{A}_v$ (содержащим единичный элемент). Для всякой точки v, как мы видели, $\mathcal{A}_v^{\times}$ есть открытое подмножество в $\mathcal{A}_v$ и отображение $x \to x^{-1}$ непрерывно на этом подмножестве. Поэтому отображением $x \to (x, x^{-1})$ оно гомеоморфно переводится в свой образ в $\mathcal{A}_v \times \mathcal{A}_v$. Для v, не лежащих в P_0, $\alpha_0^{\times}$ есть множество тех элементов из $\mathcal{A}_v^{\times}$, которые отображением $x \to (x, x^{-1})$ переводятся в $\alpha_v \times \alpha_v$, поэтому $\alpha_v^{\times}$ является открытой компактной подгруппой в $\mathcal{A}_v^{\times}$ и открытым компактным подмножеством в α_v. Мы докажем сейчас следующий результат, аналогичный следствию 2 предл. 1 § 1.

Предложение 2. *Пусть $\mathcal{A}$, α, α_v и P_0 таковы, как указано выше, и пусть P — любое конечное множество точек поля k,*

содержащее P_0. *Тогда группа*

$$\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times} = \prod_{v \in P} \mathcal{A}_v^{\times} \times \prod_{v \notin P} \alpha_v^{\times} \tag{4}$$

является открытой подгруппой в $\mathcal{A}_{\mathbf{A}}^{\times}$; *топологии, индуцированные на ней топологиями из* $\mathcal{A}_{\mathbf{A}}^{\times}$ *и из* $\mathcal{A}_{\mathbf{A}}$, *совпадают обе с топологией произведения в правой части формулы* (4); $\mathcal{A}_{\mathbf{A}}^{\times}$ *является объединением этих групп.*

Пусть множество $\mathcal{A}_{\mathbf{A}}(P, \alpha)$ определено, как в следствии 2 предл. 1 § 1. Топология, индуцированная на $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ топологией из $\mathcal{A}_{\mathbf{A}}$, индуцирована также топологией из $\mathcal{A}_{\mathbf{A}}(P, \alpha)$ и потому совпадает с топологией произведения в правой части формулы (4). Для всякой точки v подмножество $\mathcal{A}_v^{\times}$ открыто в $\mathcal{A}_v$ и отображение $x \to x^{-1}$ непрерывно на нем. Поэтому отображение $x \to x^{-1}$ непрерывно на группе $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$, наделенной топологией произведения. Отсюда следует, что отображение $x \to (x, x^{-1})$ есть гомеоморфизм из $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ на образ этой группы в $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$. Поэтому топология произведения на этой группе индуцирована также топологией из $\mathcal{A}_{\mathbf{A}}^{\times}$. Далее, $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ совпадает с тем подмножеством в $\mathcal{A}_{\mathbf{A}}^{\times}$, которое отображением $x \to (x, x^{-1})$ переводится в $\mathcal{A}_{\mathbf{A}}(P, \alpha) \times \mathcal{A}_{\mathbf{A}}(P, \alpha)$. Так как последнее множество открыто в $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$ и так как $\mathcal{A}_{\mathbf{A}} \times \mathcal{A}_{\mathbf{A}}$ является объединением множеств такого вида, это завершает доказательство.

Следствие. *Элемент* $a = (a_v)$ *из* $k_{\mathbf{A}}$ *лежит в* $k_{\mathbf{A}}^{\times}$ *в том и только том случае, когда* $a_v \neq 0$ *для всех* v *и* $|a_v|_v = 1$ *почти для всех* v. *Для каждого конечного множества* P *точек поля* k, *содержащего* P_∞, *группа*

$$k_{\mathbf{A}}(P)^{\times} = \prod_{v \in P} k_v^{\times} \times \prod_{v \notin P} r^{\times}$$

является открытой подгруппой в $k_{\mathbf{A}}^{\times}$ *и* $k_{\mathbf{A}}^{\times}$ *есть объединение таких групп.*

Первое утверждение очевидно; остальные утверждения — частный случай предложения 2.

Для каждого элемента $a = (a_v)$ из $k_{\mathbf{A}}^{\times}$ положим

$$|a|_{k_{\mathbf{A}}} = \prod_v |a_v|_v,$$

где произведение берется по всем точкам v поля k; ввиду следствия предл. 2 почти все сомножители в этом произведении равны 1 для

любого a из $k_{\mathbf{A}}^{\times}$. Обычно, когда ясно, о каком поле идет речь, мы будем писать $|a|_{\mathbf{A}}$ вместо $|a|_{k_{\mathbf{A}}}$; иногда $|a|_{\mathbf{A}}$ будем называть *модулем* иделя a.

Предложение 3. *Пусть E — векторное пространство конечной размерности n над k, $\mathcal{A} = \mathrm{End}(E)$ и $a = (a_v)$ — некоторый элемент из $\mathcal{A}_{\mathbf{A}}$. Тогда следующие утверждения эквивалентны*: (i) *a лежит в $\mathcal{A}_{\mathbf{A}}^{\times}$*; (ii) $\det(a)$ *лежит в $k_{\mathbf{A}}^{\times}$*; (iii) *$e \to ae$ есть изоморфизм пространства $E_{\mathbf{A}}$. В случае когда эти утверждения выполняются, модуль последнего автоморфизма равен $|\det(a)|_{\mathbf{A}}$. Кроме того, отображения $a \to \det(a)$ и $a \to |\det(a)|_{\mathbf{A}}$ являются морфизмами из $\mathcal{A}_{\mathbf{A}}^{\times}$ в $k_{\mathbf{A}}^{\times}$ и в $\mathbf{R}_{+}^{\times}$ соответственно.*

Выберем какой-нибудь базис ε в E над k и используем его для отождествления E с k^n и $\mathcal{A}$ с $M_n(k)$. Тогда базис α в $\mathcal{A}$ над k задается «матричными единицами» $a_{\lambda\mu}$ с $1 \leqslant \lambda, \mu \leqslant n$, где $a_{\lambda\mu}$ — матрица (x_{ij}), $x_{\lambda\mu} = 1$ и $x_{ij} = 0$ при $(i, j) \neq (\lambda, \mu)$. Для каждой точки v поля k элемент a_v из $M_n(k_v)$ обратим в $M_n(k_v)$ тогда и только тогда, когда $\det(a_v) \neq 0$. Для каждой конечной точки v поля k элемент a_v из $M_n(r_v)$ обратим в $M_n(r_v)$ тогда и только тогда, когда $\det(a_v)$ обратим в r_v, т. е. тогда и только тогда, когда $|\det(a_v)|_v = 1$. В обозначениях предложения 2 и его следствия это означает, что a лежит в $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ в том и только том случае, когда $\det(a)$ лежит в $k_{\mathbf{A}}(P)^{\times}$. Ясно, что отсюда следует эквивалентность утверждений (i) и (ii) нашего предложения; это показывает также, что отображение $a \to \det(a)$ из $\mathcal{A}_{\mathbf{A}}^{\times}$ в $k_{\mathbf{A}}^{\times}$ непрерывно на $\mathcal{A}_{\mathbf{A}}(P, \alpha)^{\times}$ для каждого P, а значит, непрерывно на $\mathcal{A}_{\mathbf{A}}^{\times}$. Поскольку, очевидно, отображение $z \to |z|_{\mathbf{A}}$ из $k_{\mathbf{A}}^{\times}$ в $\mathbf{R}_{+}^{\times}$ непрерывно на $k_{\mathbf{A}}(P)^{\times}$ для каждого P, а следовательно и на $k_{\mathbf{A}}^{\times}$, то отображение $a \to |\det(a)|_{\mathbf{A}}$ есть непрерывный морфизм из $\mathcal{A}_{\mathbf{A}}^{\times}$ в $\mathbf{R}_{+}^{\times}$. Если элемент a лежит в $\mathcal{A}_{\mathbf{A}}^{\times}$, то обратный элемент a^{-1} лежит в $\mathcal{A}_{\mathbf{A}}$ и эндоморфизм $e \to ae$ пространства $E_{\mathbf{A}}$ имеет обратный $e \to a^{-1}e$, т. е. является автоморфизмом. Обратно, возьмем любой элемент $a = (a_v)$ из $\mathcal{A}_{\mathbf{A}}$. Предложение 1 § 1, примененное к $\mathcal{A}$ и α, показывает, что a_v содержится в $M_n(k_v)$ для всех v и в $M_n(r_v)$ почти для всех v. Это же предложение, примененное к E и ε, показывает, что в $E_{\mathbf{A}}$ фундаментальную систему окрестностей нуля образуют множества $U = \prod U_v$, где U_v — окрестность нуля в $E_v = (k_v)^n$ для всех v и $U_v = (r_v)^n$ почти для всех v. Если отображение $e \to ae$ есть автоморфизм пространства $E_{\mathbf{A}}$, то оно должно отображать каждую окрестность нуля на окрестность нуля. Отсюда следует, что элемент a_v обратим в $M_n(k_v)$ при всех v и что почти

для всех v образ множества $(r_v)^n$ относительно a_v содержит $(r_v)^n$, т. е. что a_v^{-1} лежит в $M_n(r_v)$ почти для всех v. Как мы заметили выше, это равносильно тому, что a лежит в $\mathcal{A}_{\mathbf{A}}^{\times}$. Пусть теперь P — конечное множество точек поля k, содержащее P_∞ и такое, что a_v лежит в $M_n(r_v)^{\times}$ для всех v, не лежащих в P. Так как множество $E_{\mathbf{A}}(P, \varepsilon)$ открыто в $E_{\mathbf{A}}$ и инвариантно относительно отображения $e \to ae$, то модуль автоморфизма $e \to ae$ на $E_{\mathbf{A}}$ совпадает с его модулем на множестве $E_{\mathbf{A}}(P, \varepsilon)$. В силу определения этого множества (предложение 1 § 1) последний модуль равен произведению модулей автоморфизмов $e_v \to a_v e_v$ на сомножителях произведения $E_{\mathbf{A}}(P, \varepsilon)$. По следствию 3 теор. 3 гл. I-2 эти модули равны $|\det(a_v)|_v$, чем и заканчивается наше доказательство.

Следствие. *Пусть $\mathcal{A}$ — алгебра конечной размерности над k и a — элемент из $\mathcal{A}_{\mathbf{A}}$. Тогда следующие утверждения эквивалентны*: (i) *a лежит в $\mathcal{A}_{\mathbf{A}}$*; (ii) *$\mathrm{N}_{\mathcal{A}/k}(a)$ лежит в $k_{\mathbf{A}}^{\times}$*; (iii) *$x \to ax$ есть автоморфизм аддитивной группы алгебры $\mathcal{A}_{\mathbf{A}}$. В случае когда эти утверждения выполняются, модуль последнего автоморфизма равен $|\mathrm{N}_{\mathcal{A}/k}(a)|_{\mathbf{A}}$. Кроме того, $a \to \mathrm{N}_{\mathcal{A}/k}(a)$ и $a \to |\mathrm{N}_{\mathcal{A}/k}(a)|_{\mathbf{A}}$ суть морфизмы группы $\mathcal{A}_{\mathbf{A}}^{\times}$ в $k_{\mathbf{A}}^{\times}$ и в $\mathbf{R}_+^{\times}$ соответственно.*

Поскольку (как мы всегда предполагаем) $\mathcal{A}$ содержит единицу, то из (iii) следует (i). Все остальные наши утверждения сразу вытекают из предложения 3, примененного к алгебре $\mathcal{A}$, рассматриваемой как векторное пространство E над k, и к вложению алгебры $\mathcal{A}$ в $\mathrm{End}(E)$, задаваемому регулярным представлением ρ.

Разумеется, все, что мы сказали про эндоморфизм $x \to ax$ алгебры $\mathcal{A}$, столь же применимо к эндоморфизму $x \to xa$. Определитель $\mathrm{N}'(a)$ последнего эндоморфизма называется иногда *корегулярной нормой* на $\mathcal{A}$. Как и регулярная норма, это — полиномиальная функция, степень которой равна размерности $\mathcal{A}$ над k; модуль автоморфизма $x \to xa$ аддитивной группы алгебры $\mathcal{A}_{\mathbf{A}}$, для $a \in \mathcal{A}_{\mathbf{A}}^{\times}$, равен $|\mathrm{N}'(a)|_{\mathbf{A}}$. Очевидно, что $\mathrm{N}' = \mathrm{N}_{\mathcal{A}/k}$, если алгебра $\mathcal{A}$ коммутативна; известно, что то же самое верно для всех полупростых алгебр; для простых алгебр, в частности для алгебр с делением, это будет доказано в гл. IX; здесь нам это не понадобится.

Теорема 4. *Пусть D — алгебра с делением конечной размерности над k. Для каждого вещественного числа $\mu \geqslant 1$ обозначим через D_μ множество таких элементов d из $D_{\mathbf{A}}^{\times}$, что модули автоморфизмов $x \to dx$ и $x \to xd$ группы $D_{\mathbf{A}}$ соответственно $\leqslant \mu$ и $\geqslant \mu^{-1}$. Тогда D_μ является замкнутым подмножеством в $D_{\mathbf{A}}^{\times}$ и его образ в $D_{\mathbf{A}}^{\times}/D^{\times}$ компактен.*

Обозначим через N регулярную норму $N_{D/k}$ и через N′ корегулярную норму, определенную выше. По следствию предл. 3 отображение $d \to |\,N\,(d)\,|_{\mathbf{A}}$ непрерывно на $D_{\mathbf{A}}^{\times}$; по аналогичным причинам это верно и для отображения $d \to |\,N'\,(d)\,|_{\mathbf{A}}$. Ввиду того же следствия отсюда вытекает замкнутость D_{μ}. По теореме 2 § 2 D есть дискретное подмножество в $D_{\mathbf{A}}$ и факторгруппа $D_{\mathbf{A}}/D$ компактна. Поэтому существует мера Хаара α на $D_{\mathbf{A}}$, для которой $\alpha\,(D_{\mathbf{A}}/D) = 1$; эта мера определяется указанным в гл. II-4 способом. Так как группа $D_{\mathbf{A}}$ некомпактна, то мы можем выбрать компактное подмножество C в $D_{\mathbf{A}}$, для которого $\alpha\,(C) > \mu$. Обозначим через C' образ множества $C \times C$ при отображении $(x, y) \to x - y$ из $D_{\mathbf{A}} \times D_{\mathbf{A}}$ в $D_{\mathbf{A}}$ и через C'' образ множества $C' \times C'$ при отображении $(x, y) \to xy$ из $D_{\mathbf{A}} \times D_{\mathbf{A}}$ в $D_{\mathbf{A}}$. Поскольку эти отображения непрерывны, то C' и C'' компактны. Возьмем *любой* элемент $d \in D_{\mu}$. Так как модуль автоморфизма $x \to xd$ не меньше μ^{-1}, то он отображает C на множество Cd, мера которого больше 1. Поэтому в силу леммы 1 гл. II-4 существуют такие два элемента x, y в C, что элемент $xd - yd$ лежит в D и отличен от нуля, т. е. этот элемент лежит в $D^{\times}$. Запишем $c_1 = x - y$ и $\delta_1 = c_1 d$. Тогда $c_1 \in C'$ и $\delta_1 \in D^{\times}$. Аналогично автоморфизм $x \to d^{-1}x$, являясь обратным к автоморфизму $x \to dx$, имеет модуль не меньше μ^{-1} и, значит, отображает C на множество $d^{-1}C$ меры >1; как и выше, заключаем, что существует $c_2 \in C'$, для которого элемент $\delta_2 = d^{-1}c_2$ лежит в $D^{\times}$. Тогда $\delta_1\delta_2 = c_1c_2$, так что $\delta_1\delta_2$ лежит в $D^{\times} \cap C''$. Но это пересечение — конечное множество, поскольку подмножество D дискретно, а C'' компактно в $D_{\mathbf{A}}$. Обозначим через $\gamma_1, \ldots, \gamma_N$ все различные элементы множества $D^{\times} \cap C''$. Элемент c_1c_2 равен одному из них, скажем γ_i, так что $\gamma_i^{-1}c_1c_2 = 1$. Отсюда видно, что элемент c_2 обратим в $D_{\mathbf{A}}$ и обратный элемент c_2^{-1} равен $\gamma_i^{-1}c_1$. Поскольку $d\delta_2 = c_2$, мы заключаем, что $d\delta_2$ принадлежит множеству X тех элементов x из $D_{\mathbf{A}}^{\times}$, образы которых при отображении $x \to (x, x^{-1})$ лежат в объединении множеств $C' \times (\gamma_i^{-1}C')$, $1 \leqslant i \leqslant N$. В силу определения 2 X является компактным подмножеством в $D_{\mathbf{A}}^{\times}$. Так как $D_{\mu} \subset X \cdot D^{\times}$, то образ множества D_{μ} в $D_{\mathbf{A}}^{\times}/D^{\times}$ содержится в образе множества X, чем наша теорема и доказана.

§ 4. ИДЕЛИ А-ПОЛЕЙ

Здесь мы рассмотрим более подробно случай $\mathcal{A} = k$.

Теорема 5. *Пусть k — произвольное* А*-поле. Тогда морфизм $z \to |\,z\,|_{\mathbf{A}}$ группы $k_{\mathbf{A}}^{\times}$ в $\mathbf{R}_{+}^{\times}$ индуцирует на $k^{\times}$ отображение, тождественно равное* 1.

Если $\xi \in k^\times$, то $x \to \xi x$ есть автоморфизм группы $k_\mathbf{A}$, отображающий k в себя. По теореме 2 § 2 поле k дискретно в $k_\mathbf{A}$ и факторгруппа $k_\mathbf{A}/k$ компактна. Поэтому модуль автоморфизма $x \to \xi x$, который по предложению 3 § 3 совпадает с $|\xi|_\mathbf{A}$ (если взять в этом предложении $E = k$), равен 1, например по лемме 2 гл. I-2.

Теорема 5 известна как *формула произведения Артина*. Начиная с этого места, мы будем обозначать через $k_\mathbf{A}^1$ ядро морфизма $z \to |z|_\mathbf{A}$, т. е. подгруппу в $k_\mathbf{A}^\times$, задаваемую условием $|z|_\mathbf{A} = 1$; по теореме 5 $k_\mathbf{A}^1 \supset k^\times$.

Следствие 1. *Если k — поле характеристики $p > 1$, то $k_\mathbf{A}^\times$ разлагается в прямое произведение подгруппы $k_\mathbf{A}^1$ и некоторой дискретной подгруппы, изоморфной* $\mathbf{Z}$.

Для каждой точки v поля k поле k_v имеет характеристику p, так что $|x|_v$ для каждого $x \in k_v^\times$ лежит в подгруппе в $\mathbf{R}_+^\times$, порожденной элементом p. Поэтому то же самое верно для $|z|_\mathbf{A}$ при каждом $z \in k_\mathbf{A}^\times$. Другими словами, образ группы $k_\mathbf{A}^\times$ при морфизме $z \to |z|_\mathbf{A}$ является подгруппой в группе, порожденной элементом p в $\mathbf{R}_+^\times$. Так как этот образ, очевидно, не сводится к $\{1\}$, то он порождается некоторым целым числом $Q = p^N$, где $N \geqslant 1$ — целое число. Возьмем $z_1 \in k_\mathbf{A}^\times$, для которого $|z_1|_\mathbf{A} = Q$. Тогда $k_\mathbf{A}^\times$ разлагается в прямое произведение подгруппы $k_\mathbf{A}^1$ и подгруппы, порожденной элементом z_1, которая, очевидно, дискретна и изоморфна группе $\mathbf{Z}$.

Следствие 2. *Предположим, что характеристика поля k равна нулю. Для каждого $\lambda \in \mathbf{R}_+^\times$ обозначим через $z(\lambda)$ идель (z_v), такой, что $z_v = 1$ для всех конечных точек v и $z_w = \lambda$ для всех бесконечных точек w поля k. Тогда отображение $\lambda \to z(\lambda)$ есть изоморфизм группы $\mathbf{R}_+^\times$ на замкнутую подгруппу M в $k_\mathbf{A}^\times$ и $k_\mathbf{A}^\times$ разлагается в прямое произведение подгрупп $k_\mathbf{A}^1$ и M.*

В обозначениях следствия предл. 2 § 3 очевидно, что $\lambda \to z(\lambda)$ есть изоморфизм из $\mathbf{R}_+^\times$ на подгруппу M в $k_\mathbf{A}(P_\infty)^\times$. Определение модуля $|z|_\mathbf{A}$ вместе со следствием 2 теор. 4 гл. III-4 показывают, что $|z(\lambda)|_\mathbf{A} = \lambda^n$, где n — *степень поля k* над $\mathbf{Q}$. Наше последнее утверждение теперь очевидно.

Теорема 6. *Пусть $k_\mathbf{A}^1$ — подгруппа в $k_\mathbf{A}^\times$, определенная условием $|z|_\mathbf{A} = 1$. Тогда $k^\times$ является дискретной подгруппой в $k_\mathbf{A}^1$, факторгруппа $k_\mathbf{A}^1/k^\times$ компактна и $k_\mathbf{A}^\times/k^\times$ разлагается в прямое произведение этой компактной группы и группы, изоморфной* $\mathbf{R}_+^\times$

в случае характеристики нуль и изоморфной $\mathbf{Z}$ *в случае ненулевой характеристики.*

Первое утверждение содержится в теореме 5; второе является частным случаем теоремы 4 § 3 при $D = k$, $\mu = 1$; остальные утверждения немедленно вытекают из следствий теор. 5.

Теперь мы исследуем более подробно структуру различных подгрупп в $k_{\mathbf{A}}^{\times}$ и в $k^{\times}$ и некоторых их факторгрупп. Условимся обозначать через $\Omega(P)$ группу, которая в следствии предл. 2 § 3 обозначалась через $k_{\mathbf{A}}(P)^{\times}$. Другими словами, начиная с этого места, мы будем писать

$$\Omega(P) = \prod_{v \in P} k_v^{\times} \times \prod_{v \notin P} r_v^{\times} . \tag{5}$$

Как всегда, P предполагается конечным множеством точек поля k, содержащим множество P_∞ всех бесконечных точек; P может быть пустым, но только не в случае характеристики нуль. Напомним, что $\Omega(P)$ всегда является открытой подгруппой в $k_{\mathbf{A}}^{\times}$; ясно, что она компактна тогда и только тогда, когда P пусто. Мы будем также писать

$$\Omega_1(P) = \Omega(P) \cap k_{\mathbf{A}}^1.$$

В случае когда характеристика поля k равна $p > 1$, мы можем взять здесь $P = \varnothing$, тогда $\Omega_1(\varnothing) = \Omega(\varnothing)$.

Т е о р е м а 7. *Если P не пусто, то группа $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(P)$ конечна. Если характеристика поля k равна $p > 1$, то группа $k_{\mathbf{A}}^1/k^{\times}\Omega(\varnothing)$ конечна и $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(\varnothing)$ разлагается в прямое произведение этой группы на группу, изоморфную* $\mathbf{Z}$.

Во всех случаях группа $k_{\mathbf{A}}^1/k^{\times}\Omega_1(P)$ изоморфна факторгруппе группы $k_{\mathbf{A}}^1/k^{\times}$ по образу в $k_{\mathbf{A}}^1/k^{\times}$ группы $\Omega_1(P)$. Так как группа $\Omega_1(P)$ открыта в $k_{\mathbf{A}}^1$, то и этот образ открыт; так как факторгруппа $k_{\mathbf{A}}^1/k^{\times}$ компактна по теореме 6, то указанная выше факторгруппа по этому образу конечна. Если k имеет характеристику нуль, то $\Omega(P)$ содержит группу M, определенную в следствии 2 теор. 5, и это следствие показывает, что $\Omega(P)$ разлагается в прямое произведение подгрупп $\Omega_1(P)$ и M, так что можно отождествить $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(P)$ с $k_{\mathbf{A}}^1/k^{\times}\Omega_1(P)$. Предположим теперь, что k имеет характеристику $p > 1$. Поскольку $\Omega(\varnothing) = \Omega_1(\varnothing)$, следствие 1 теор. 5 показывает, что $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(\varnothing)$ разлагается в прямое произведение конечной группы $g = k_{\mathbf{A}}^1/k^{\times}\Omega(\varnothing)$ и группы γ, изоморфной $\mathbf{Z}$. Если $P \neq \varnothing$, то $\Omega(P)$ содержит $\Omega(\varnothing)$ и не содержится в $k_{\mathbf{A}}^1$. Поэтому $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(P)$ совпадает с факторгруппой группы $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(\varnothing)$,

т. е. группы $g \times \gamma$, по образу в ней группы $k^\times \Omega(P)$, и этот образ не содержится в образе g группы $k_{\mathbf{A}}^1$. Отсюда видно, что эта факторгруппа конечна.

Следствие. *В обозначениях теоремы 7 можно выбрать P так, чтобы $k_{\mathbf{A}}^\times = k^\times \Omega(P)$.*

Возьмем любое непустое P' и выберем полное множество представителей $z_1, \ldots, z_N$ для классов в $k_{\mathbf{A}}^\times$ по модулю $k^\times \Omega(P')$. Так как $k_{\mathbf{A}}^\times$ есть объединение всех групп $\Omega(P)$, то можно выбрать $P \supset P'$ так, чтобы все z_i лежали в $\Omega(P)$. Тогда P будет обладать требуемым свойством.

В случае когда k — после алгебраических чисел и $P = P_\infty$, теорема 1, как будет показано в следующей главе, по существу совпадает с классической теоремой о конечности числа классов идеалов в k.

Теорема 8. *Пусть F — множество тех элементов ξ из k, для которых $|\xi|_v \leqslant 1$ для всех точек v поля k. Положим $E = F - \{0\}$. Тогда E совпадает с конечной циклической группой, состоящей из всех корней из 1 в k.*

Множество F является пересечением поля k с множеством тех элементов (x_v) из $k_{\mathbf{A}}$, для которых $|x_v|_v \leqslant 1$ для всех v. Ясно, что последнее множество компактно, а по теореме 2 § 2 k дискретно в $k_{\mathbf{A}}$. Поэтому F конечно. Если $\xi \in E$, то теорема 5 показывает, что для всех v должно выполняться равенство $|\xi|_v = 1$. Поэтому E является подгруппой конечного порядка в $k^\times$, откуда, согласно лемме 1 гл. I-1, следует цикличность E. Обратно, очевидно, что каждый корень из 1 в k должен содержаться в E.

Следствие. *Если k — поле характеристики $p > 1$, то множество F, определенное в теореме 8, является конечным полем, которое совпадает с алгебраическим замыканием в k простого поля в k.*

Множество F можно в этом случае записать в виде $F = k \cap (\prod r_v)$, где произведение берется по всем точкам v поля k. Отсюда видно, что F является кольцом; поскольку $E = F - \{0\}$ есть группа, то F — поле. По теореме 2 гл. I-1 если отличный от нуля элемент поля k алгебраичен над простым полем, то он является корнем из 1 и, значит, лежит в E по теореме 8.

В случае когда k имеет характеристику $p > 1$, конечное поле F, определенное в следствии теор. 8, называется *полем констант* в k.

Пусть множество P то же, что и выше. Определим подгруппу $E(P)$ в $k^\times$, положив

$$E(P) = k^\times \cap \Omega(P) = k^\times \cap \left(\prod_{v \in P} k_v^\times \times \prod_{v \notin P} r_v^\times\right).$$

Эта подгруппа состоит из тех элементов ξ группы $k^\times$, для которых $|\xi|_v = 1$ для всех v, не лежащих в P. Очевидно, что $E(P)$ содержит группу E, определенную в теореме 8. Так как $k^\times$ дискретна в $k_{\mathbf{A}}^\times$, то $E(P)$ является дискретной подгруппой в $\Omega(P)$, а также ввиду теоремы 5 в $\Omega_1(P)$. Можно еще описать $E(P)$ как группу $k(P)^\times$ обратимых элементов (или, в традиционной терминологии, «единиц») подкольца $k(P)$ в k, задаваемого равенством

$$k(P) = k \cap \left(\prod_{v \in P} k_v \times \prod_{v \notin P} r_v\right)$$

и состоящего из элементов ξ в k, таких, что $|\xi|_v \leqslant 1$ для всех v, не лежащих в P. Для определения структуры группы $E(P)$ нам понадобится одна элементарная лемма.

Лемма 5. *Пусть G — группа, изоморфная группе $\mathbf{R}^r \times \mathbf{Z}^{s+1-r}$, где $s \geqslant r \geqslant 0$. Пусть λ в случае $r > 0$ есть какой-нибудь морфизм группы G в $\mathbf{R}$, нетривиальный на $\mathbf{R}^r$, а в противном случае — любой нетривиальный морфизм группы G в $\mathbf{Z}$. Пусть, далее, G_1 — ядро морфизма λ и Γ — такая дискретная подгруппа в G, что факторгруппа G_1/Γ компактна. Тогда подгруппа Γ изоморфна $\mathbf{Z}^s$.*

Можно считать, что $G = \mathbf{R}^r \times \mathbf{Z}^{s+1-r}$. Тогда каждый элемент x из G можно записать в виде $(x_0, \ldots, x_s)$, где $x_i \in \mathbf{R}$ при $0 \leqslant i < r$ и $x_i \in \mathbf{Z}$ при $i \geqslant r$, а λ можно записать в виде

$$x = (x_0, \ldots, x_s) \longrightarrow \lambda(x) = \sum_{i=0}^{s} a_i x_i,$$

где $a_i \in \mathbf{R}$ при всех i, если $r > 0$, и $a_i \in \mathbf{Z}$ при всех i, если $r = 0$; в обоих случаях в силу наших предположений относительно λ можно считать, что $a_0 \neq 0$, а в первом случае можно считать, что $a_0 = 1$. Рассмотрим группу G как очевидным образом вложенную в векторное пространство $V = \mathbf{R}^{s+1}$ над $\mathbf{R}$. Тогда приведенная выше формула определяет λ как линейную форму на V. Пусть V_1 — подпространство в V, определенное уравнением $\lambda(x) = 0$, так что $G_1 = G \cap V_1$. Для $1 \leqslant j \leqslant s$ обозначим через e_j точку (x_i) в V, для которой $x_0 = -a_j$, $x_j = a_0$ и $x_i = 0$ при $i \neq 0$ и $i \neq j$. Так как множество $\{e_1, \ldots, e_s\}$ является базисом в V_1, то оно порождает $\mathbf{R}$-решетку H в V_1, так что факторгруппа V_1/H компактна. Поскольку $H \subset G_1$ и G_1 замкнуто в V_1, отсюда следует компактность фактор-

группы V_1/G_1. Поэтому если подгруппа Γ такая, как в нашей лемме, то факторгруппа V_1/Γ компактна, так что Γ является $\mathbf{R}$-решеткой в V_1 и, следовательно, изоморфна $\mathbf{Z}^s$ согласно предложению 11 гл. II-4.

Теорема 9. *Пусть P — любое конечное множество точек поля k, содержащее P_∞, и пусть $E(P)$ — подгруппа в $k^\times$, состоящая из тех элементов ξ в $k^\times$, для которых $|\xi|_v = 1$ для всех v, не лежащих в P. Тогда $E(P)$ разлагается в прямое произведение группы E всех корней из 1 в k и группы, изоморфной $\mathbf{Z}^s$, где $s = 0$, если P пусто, и $s = \operatorname{card}(P) - 1$ в противном случае* [1]).

Если P пусто, то наша теорема содержится в теореме 8, поэтому можно считать, что $P \neq \varnothing$. Обозначим через ν морфизм из $\Omega(P)$ в $\mathbf{R}_+^\times$, индуцированный отображением $z \to |z|_{\mathbf{A}}$. Его ядро совпадает с $\Omega_1(P)$ и открыто в $k_{\mathbf{A}}^1$. Канонический морфизм из $k_{\mathbf{A}}^1$ на $k_{\mathbf{A}}^1/k^\times$ индуцирует на $\Omega_1(P)$ морфизм этой подгруппы на ее образ в $k_{\mathbf{A}}^1/k^\times$; ядро этого морфизма равно $E(P)$, ибо $k^\times \cap \Omega_1(P)$ совпадает с $k^\times \cap \Omega(P)$. Поэтому факторгруппа $\Omega_1(P)/E(P)$ изоморфна открытой подгруппе в $k_{\mathbf{A}}^1/k^\times$ и, следовательно, компактна по теореме 6. С другой стороны, обозначим для всякой точки v поля k через U_v компактную подгруппу в $k_v^\times$, определенную условием $|x|_v = 1$; эта подгруппа совпадает с $r_v^\times$, в случае когда v — конечная точка. Положим $U = \prod U_v$, где произведение берется по всем точкам поля k. Это — компактная подгруппа в $\Omega(P)$ и в $\Omega_1(P)$. Положим, далее, $G = \Omega(P)/U$. Ясно, что эта группа изоморфна произведению групп $k_v^\times/U_v$ по $v \in P$. Поскольку группа $k_v^\times/U_v$ изоморфна группе $\mathbf{R}_+^\times$ или, что то же самое, группе $\mathbf{R}$, в случае когда v — бесконечная точка, и изоморфна $\mathbf{Z}$ в противном случае, то G изоморфна $\mathbf{R}^r \times \mathbf{Z}^{s+1-r}$, где r — число бесконечных точек поля k, а s — число из формулировки теоремы. Так как U содержится в ядре $\Omega_1(P)$ морфизма ν группы $\Omega(P)$, то ν определяет на группе G морфизм этой группы в $\mathbf{R}_+^\times$; этот морфизм, очевидно, нетривиален на каждом из сомножителей $k_v^\times/U_v$ в G, и в частности на тех из них, которые изоморфны $\mathbf{R}$, если таковые сомножители имеются, т. е. если $r > 0$. С другой стороны, если $r = 0$, то по следствию 1 теор. 5 $|z|_{\mathbf{A}}$ принимает значения в группе, изоморфной $\mathbf{Z}$, так что с точностью до изоморфизма λ отображает G в $\mathbf{Z}$. Поэтому G и λ удовлетворяют предположениям леммы 5; ядро G_1 морфизма λ равно в рассматриваемом случае образу группы $\Omega_1(P)$ в G, т. е. $\Omega_1(P)/U$. Обозначим

[1]) Здесь $\operatorname{card}(P)$ — это число точек в P. — *Прим. перев.*

теперь через Γ образ группы $E(P)$ в G. Если W — любая компактная окрестность единицы в $\Omega(P)$, то множество WU компактно и потому имеет конечное пересечение с $E(P)$. Так как образ этого пересечения в G совпадает с пересечением подгруппы Γ с образом множества WU в G и так как последний образ является окрестностью единицы в G, отсюда видно, что подгруппа Γ дискретна в G. Факторгруппа G_1/Γ изоморфна $\Omega_1(P)/E(P)\,U$, т. е. факторгруппе компактной группы $\Omega_1(P)/E(P)$, и потому компактна. Мы можем теперь применить к G, λ и Γ лемму 5; получаем, что группа Γ изоморфна $\mathbf{Z}^s$. Так как $E(P) \cap U = E$, то у морфизма группы $E(P)$ на Γ, индуцированного каноническим морфизмом группы $\Omega(P)$ на G, ядро равно E. Пусть теперь $e_1, \ldots, e_s$ — представители в $E(P)$ множества свободных образующих группы Γ. Очевидно, они порождают в $E(P)$ подгруппу, изоморфную $\mathbf{Z}^s$, и $E(P)$ разлагается в прямое произведение группы E и этой подгруппы. Доказательство нашей теоремы закончено.

Попутно мы доказали также следующее

Следствие. *Предположим, что P не пусто и группа $E(P)$ такова, как в теореме* 9. *Положим $\Omega_1(P) = \Omega(P) \cap k_{\mathbf{A}}^1$ и $G_1 = \Omega_1(P)/U$, где U — группа тех элементов (z_v) из $k_{\mathbf{A}}^{\times}$, для которых $|z_v|_v = 1$ при всех v. Тогда образ Γ группы $E(P)$ в G_1 дискретен в G_1 и факторгруппа G_1/Γ компактна.*

В случае когда k — поле алгебраических чисел и $P = P_\infty$, теорема 9, как будет показано в следующей главе, совпадает со знаменитой «теоремой об единицах» Дирихле.

ГЛАВА ПЯТАЯ

ПОЛЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

§ 1. ПОРЯДКИ В АЛГЕБРАХ НАД Q

Нам понадобятся некоторые элементарные результаты о векторных пространствах над $\mathbf{Q}$, связанные со следующим понятием.

Определение 1. *Пусть E — векторное пространство конечной размерности над $\mathbf{Q}$. Под $\mathbf{Q}$-решеткой в E мы понимаем конечно порожденную подгруппу в E, содержащую базис векторного пространства E над $\mathbf{Q}$.*

Предложение 1. *Пусть E — векторное пространство конечной размерности над $\mathbf{Q}$, и пусть L, L' — две $\mathbf{Q}$-решетки в E. Тогда существует такое целое число $m > 0$, что $mL \subset L'$.*

Пусть $\{e_1, \ldots, e_r\}$ и $\{e'_1, \ldots, e'_s\}$ — конечные множества образующих для L и L' соответственно. Так как второе множество должно содержать базис для E над $\mathbf{Q}$, то e_i можно записать (вообще говоря, не единственным способом) в виде $e_i = \sum a_{ij}e'_j$, $1 \leqslant i \leqslant r$, где коэффициенты $a_{ij} \in \mathbf{Q}$. Возьмем в качестве m такое целое положительное число, что $ma_{ij} \in \mathbf{Z}$ при всех i, j. Тогда $mL \subset L'$.

Следствие 1. *Пусть E таково, как в предложении 1. Тогда каждая $\mathbf{Q}$-решетка L в E порождается некоторым базисом векторного пространства E над $\mathbf{Q}$.*

Пусть β — какой-нибудь базис в E над $\mathbf{Q}$, содержащийся в L, и пусть L' — $\mathbf{Q}$-решетка, порожденная множеством β. Согласно предложению 1, существует такое целое число $m > 0$, что $mL \subset L'$. Рассмотрим E как подмножество в $E_{\mathbf{R}} = E \otimes_{\mathbf{Q}} \mathbf{R}$. Согласно предложению 11 гл. II-4 L' является $\mathbf{R}$-решеткой в $E_{\mathbf{R}}$. Так как L содержится в $m^{-1}L'$, то то же самое предложение показывает, во-первых, что L также является $\mathbf{R}$-решеткой в $E_{\mathbf{R}}$, а во-вторых, что L порождается некоторым базисом в $E_{\mathbf{R}}$ над $\mathbf{R}$. Поскольку этот базис содержится в E, то он, очевидно, является базисом векторного пространства E над $\mathbf{Q}$.

Следствие 2. *Пусть E и L таковы, как в следствии* 1. *Тогда каждая подгруппа L' в L, содержащая базис пространства E над* **Q**, *является* **Q**-*решеткой в* E.

Пусть β' — базис пространства E над **Q**, содержащийся в L', и пусть L'' — **Q**-решетка, порожденная множеством β'. Согласно предложению 1, существует такое целое $m > 0$, что $mL \subset L''$. Тогда $m^{-1}L'' \supset L \supset L' \supset L''$. Ясно, что L'' имеет индекс m^n в $m^{-1}L''$, где n — размерность E над **Q**. Следовательно, L'' имеет конечный индекс в L'. Поскольку L' порождается множеством β' и любым полным множеством представителей классов L'/L'', наше следствие доказано.

Определение 2. *Пусть $\mathcal{A}$ — алгебра конечной размерности над* **Q**. *Подкольцо в $\mathcal{A}$ будем называть порядком в $\mathcal{A}$, если оно является* **Q**-*решеткой в алгебре $\mathcal{A}$, рассматриваемой как векторное пространство над* **Q**.

Здесь, как всегда, подразумевается, что подкольцо в $\mathcal{A}$ содержит единицу алгебры $\mathcal{A}$.

Предложение 2. *Каждая алгебра $\mathcal{A}$ конечной размерности над* **Q** *содержит по крайней мере один порядок.*

Пусть $\{a_1, \ldots, a_N\}$ — какое-нибудь конечное подмножество в $\mathcal{A}$, содержащее базис векторного пространства $\mathcal{A}$ над **Q**. Тогда для всех i, j мы можем записать $a_i a_j = \sum c_{ijh} a_h$, где коэффициенты $c_{ijh} \in \mathbf{Q}$. Пусть m — такое целое положительное число, что $mc_{ijh} \in \mathbf{Z}$ для всех i, j, h. Тогда **Q**-решетка, порожденная элементами $1, ma_1, \ldots, ma_N$, является порядком.

Возьмем для примера $\mathcal{A} = \mathbf{Q}$. По следствию 1 предл. 1 каждая **Q**-решетка в **Q** имеет вид $a\mathbf{Z}$, где $a \in \mathbf{Q}^\times$. Если эта решетка является порядком, то $a^2 \in a\mathbf{Z}$, так что $a \in \mathbf{Z}$, и $1 \in a\mathbf{Z}$, так что $a^{-1} \in \mathbf{Z}$, откуда $a = \pm 1$. Это показывает, что **Z** является единственным порядком в **Q**.

Предложение 3. *Пусть a — произвольный элемент некоторого порядка в алгебре $\mathcal{A}$, конечномерной над* **Q**. *Тогда a цел над* **Z** *и* $\mathrm{Tr}_{\mathcal{A}/\mathbf{Q}}(a)$, $\mathrm{N}_{\mathcal{A}/\mathbf{Q}}(a) \in \mathbf{Z}$.

Пусть R — порядок, содержащий элемент a, и пусть $\{a_1, \ldots, a_N\}$ — конечное множество образующих для R. Тогда при $1 \leqslant i \leqslant N$ можно записать $a \cdot a_i = \sum c_{ij} a_j$, где коэффициенты $c_{ij} \in \mathbf{Z}$. Это равенство можно переписать в виде $\sum (\delta_{ij} a - c_{ij}) a_j = 0$, где (δ_{ij}) — единичная матрица 1_N. Обозначим через $D(T)$ опре-

делитель матрицы $(\delta_{ij}T - c_{ij})$, где T — независимая переменная, и через $D_{ij}(T)$ — миноры этой матрицы, $1 \leqslant i, \leqslant N$; $D(T)$ и $D_{ij}(T)$ являются многочленами из $\mathbf{Z}[T]$, и

$$\sum_i D_{ih}(T) \cdot (\delta_{ij}T - c_{ij}) = \delta_{hj} D(T)$$

при $1 \leqslant h, j \leqslant N$. Подставляя a вместо T, умножая справа на a_j и суммируя по всем j от 1 до N, получаем $D(a)\, a_h = 0$ при всех h; следовательно, $D(a)\, x = 0$ при всех x. При $x = 1$ это дает $D(a) = 0$, чем доказано наше первое утверждение, поскольку многочлен $D(T)$ имеет целые коэффициенты и старший коэффициент равен 1. В силу следствия 1 предл. 1 можно считать, что в качестве множества $\{a_1, \ldots, a_N\}$ взят базис для $\mathcal{A}$ над $\mathbf{Q}$. Тогда $\mathrm{Tr}_{\mathcal{A}/\mathbf{Q}}(a)$ и $\mathrm{N}_{\mathcal{A}/\mathbf{Q}}(a)$ равны следу и определителю матрицы (c_{ij}) и, значит, являются целыми числами.

§ 2. РЕШЕТКИ НАД ПОЛЯМИ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Начиная с этого места и до конца главы k обозначает некоторое поле алгебраических чисел. Мы будем использовать обозначения, введенные в гл. IV. В частности, для любой точки v поля k через k_v обозначается соответствующее пополнение поля k; если v — конечная точка, то r_v — максимальное компактное подкольцо в k_v и p_v — максимальный идеал в r_v. Через $k_{\mathbf{A}}$ обозначается кольцо аделей поля k, а через φ — каноническое вложение $k \to k_{\mathbf{A}}$. Каноническое вложение любого конечномерного векторного пространства E над k в соответствующее адельное пространство $E_{\mathbf{A}}$ будет обозначаться через φ_E; как было показано в гл. IV-1, при этом вложении $e \to e \otimes \varphi$ (1).

Рассмотрим теперь алгебру $k \otimes_{\mathbf{Q}} \mathbf{R}$ над $\mathbf{R}$; в теореме 1 гл. IV-1 эта же алгебра обозначалась через $(k/\mathbf{Q})_\infty$. Имеется изоморфизм Φ_∞ этой алгебры на прямое произведение $\prod k_w$ пополнений поля k по всем его бесконечным точкам w; этот изоморфизм вполне характеризуется свойствами, сформулированными в теореме 4 гл. III-4. Для упрощения обозначений отождествим посредством Φ_∞ алгебру $(k/\mathbf{Q})_\infty$ с $\prod k_w$ и будем обозначать обе алгебры через k_∞. Аналогично если E — любое конечномерное векторное пространство над k, то будем писать E_∞ вместо $E \otimes_{\mathbf{Q}} \mathbf{R}$; в следствии 2 теор. 1 гл. IV-1 это же пространство обозначалось через $(E/\mathbf{Q})_\infty$; поскольку это пространство совпадает также с $E \otimes_k k_\infty$, мы отождествляем его с произведением $\prod E_w$, взятым по всем бесконечным точкам w поля k.

Открытую подгруппу $k_{\mathbf{A}}(P_\infty) \subset k_{\mathbf{A}}$, задаваемую формулой (1) гл. IV-1, можно теперь записать как $k_\infty \times (\prod r_v)$, где последнее произведение берется по всем конечным точкам v поля k и является компактным. В этой и в аналогичных ситуациях оказывается полезной следующая теоретико-групповая лемма.

Лемма 1. *Пусть G — локально компактная группа с открытой подгруппой G_1 вида $G_1 = G' \times G''$, где G' локально компактна, а G'' компактна, и пусть Γ — такая дискретная подгруппа в G, что пространство G/Γ компактно. Обозначим через Γ' проекцию группы $\Gamma \cap G_1$ на G'. Тогда множество Γ' дискретно в G', а множество G'/Γ' компактно.*

Пусть W — компактная окрестность нейтрального элемента в G' (нет необходимости предполагать, что группы G, G', G'' коммутативны, хотя в дальнейшем будет использоваться только этот случай). Поскольку множество $W \times G''$ компактно, его пересечение с Γ конечно. Так как проекция этого пересечения на G' совпадает с $W \cap \Gamma'$, то множество Γ' дискретно. Множества $G_1\Gamma$ и $G - G_1\Gamma$ открыты, поскольку они являются объединениями левых смежных классов по открытой подгруппе G_1. Поэтому образ группы G_1 в G/Γ открыт и замкнут там и, следовательно, компактен. Так как он изоморфен G_1/Γ_1, где $\Gamma_1 = \Gamma \cap G_1$, то существует такое компактное подмножество C в G_1, что $G_1 = C \cdot \Gamma_1$. Но тогда $G' = C' \cdot \Gamma'$, где C' — проекция C на G', чем и доказана компактность G'/Γ'.

Теорема 1. *Пусть k — некоторое поле алгебраических чисел. Положим $\mathfrak{r} = \bigcap\limits_v (k \cap r_v)$, где v пробегает все конечные точки поля k. Тогда $\mathfrak{r}$ есть порядок в k; это единственный максимальный порядок в k, и он совпадает с целым замыканием кольца $\mathbf{Z}$ в k.*

Как объяснялось выше, запишем $k_{\mathbf{A}}(P_\infty)$ в виде произведения $k_\infty \times (\prod r_v)$. Ясно, что элемент $\xi \in k$ лежит в $\mathfrak{r}$ в том и только в том случае, когда $\varphi(\xi)$ лежит в этом произведении; обозначим в этом случае через $\varphi_\infty(\xi)$ и $\psi(\xi)$ проекции $\varphi(\xi)$ на k_∞ и на $\prod r_v$ соответственно. Очевидно, $\mathfrak{r}$ является подкольцом в k. Теперь применим лемму 1 к $G = k_{\mathbf{A}}$, $G_1 = k_{\mathbf{A}}(P_\infty)$, $G' = k_\infty$, $G'' = \prod r_v$, $\Gamma = \varphi(k)$. Согласно этой лемме $\Gamma' = \varphi_\infty(\mathfrak{r})$ является $\mathbf{R}$-решеткой в k_∞. Так как φ_∞ совпадает с вложением, индуцированным на $\mathfrak{r}$ естественным вложением поля k в $k_\infty = k \otimes_{\mathbf{Q}} \mathbf{R}$, отсюда следует, что $\mathfrak{r}$ является $\mathbf{Q}$-решеткой в k. Следовательно, $\mathfrak{r}$ есть порядок. Пусть $\mathfrak{r}'$ — любое подкольцо в k, аддитивная группа которого конечно порождена. Ясно, что r_v-модуль, порожденный

множеством $\mathfrak{r}'$ в k_v, является компактным подкольцом в k_v. Этот модуль содержит r_v, поскольку $\mathfrak{r}'$ содержит 1; поэтому он совпадает с r_v, так что $\mathfrak{r}' \subset r_v$. Так как это справедливо для всех v, то $\mathfrak{r}' \subset \mathfrak{r}$. Согласно предложению 3 § 1 $\mathfrak{r}$ содержится в целом алгебраическом замыкании кольца $\mathbf{Z}$ в k. Обратно, если некоторый элемент поля k цел над $\mathbf{Z}$, то предложение 6 гл. I-4 показывает, что этот элемент лежит в r_v при всех v, а следовательно, лежит в $\mathfrak{r}$.

Отображение $\psi\colon \mathfrak{r} \to \prod r_v$, определенное в доказательстве теоремы 1, будем называть *каноническим вложением* кольца $\mathfrak{r}$ в произведение $\prod r_v$. При этом вложении каждому $\xi \in \mathfrak{r}$ сопоставляется элемент (x_v) этого произведения с $x_v = \xi$ при всех v. Отображение ψ осуществляет изоморфизм кольца $\mathfrak{r}$ на кольцо $\psi(\mathfrak{r})$; сложение и умножение в $\prod r_v$ определяются покоординатно. В этих обозначениях справедливо

Следствие 1. *Пусть k, $\mathfrak{r}$ и ψ таковы, как выше. Тогда кольцо $\psi(\mathfrak{r})$ плотно в $\prod r_v$ и его проекция на каждое частичное произведение плотна там. В частности, r_v совпадает с замыканием $\mathfrak{r}$ в k_v.*

Пусть G, G_1, G', G'', Γ таковы, как в доказательстве теормы 1. По следствию 2 теор. 3 гл. IV-2 кольцо $k_\infty + \varphi(k)$, которое мы теперь обозначаем через $G'\Gamma$, плотно в $G = k_\mathbf{A}$, так что его пересечение с G_1 должно быть плотно в G_1. Так как это пересечение равно $k_\infty + \varphi(\mathfrak{r})$, отсюда следует, что его проекция на $G'' = \prod r_v$, совпадающая с проекцией $\psi(\mathfrak{r})$ кольца $\varphi(\mathfrak{r})$ на G'', плотна там. Второе утверждение нашего следствия тривиальным образом следует из первого.

Следствие 2. *Если k' — конечное алгебраическое расширение поля k, то максимальный порядок в k' совпадает с целым замыканием кольца $\mathfrak{r}$ в k'.*

Это снова вытекает из предложения 6 гл. I-4; рассуждения в точности те же, что и в доказательстве теоремы 1.

Определение 3. *Пусть k — некоторое поле алгебраических чисел, $\mathfrak{r}$ — максимальный порядок в k и E — векторное пространство конечной размерности над k. Всякий конечно порожденный $\mathfrak{r}$-модуль, содержащий базис векторного пространства E над k, будем называть k-решеткой в E.*

Если k' — конечное алгебраическое расширение поля k, $\mathfrak{r}'$ — максимальный порядок в k' и E — векторное пространство конечной размерности над k', то, очевидно, $\mathfrak{r}'$-модуль в E является

k'-решеткой тогда и только тогда, когда он является k-решеткой в E, рассматриваемом как векторное пространство над k.

Пусть E — векторное пространство конечной размерности над k, L — некоторая k-решетка в E и ε — конечное подмножество в E, порождающее L как $\mathfrak{r}$-модуль. Тогда для каждой конечной точки v поля k r_v-модуль ε_v, порожденный множеством ε, совпадает с r_v-модулем L_v, порожденным решеткой L. Согласно предложению 1 гл. IV-1 $E_{\mathbf{A}}(P_\infty, \varepsilon)$ совпадает с $E_\infty \times \prod L_v$ и является открытой подгруппой в $E_{\mathbf{A}}$. Для каждого $e \in L$ можно определить элемент (e_v) в $\prod L_v$, положив $e_v = e$ при всех v. Обозначим этот элемент через $\psi_L(e)$; отображение ψ_L будем называть *каноническим вложением* решетки L в $\prod L_v$. Имеет место

Предложение 4. *Пусть E — векторное пространство конечной размерности над k и L — некоторая k-решетка в E. Для каждой конечной точки v поля k через L_v обозначим r_v-модуль, порожденный решеткой L в E_v. Пусть $\psi_L\colon L \to \prod L_v$ — соответствующее каноническое вложение. Тогда образ $\psi_L(L)$ плотен в $\prod L_v$ и его проекции на каждое частичное произведение плотны там; в частности, L_v для каждой точки v совпадает с замыканием L в E_v.*

Пусть $\varepsilon = \{e_1, \ldots, e_N\}$ — какое-нибудь конечное подмножество в L, порождающее L как $\mathfrak{r}$-модуль. Возьмем любой элемент $(e_v) \in \in \prod L_v$. Для каждой точки v можно записать e_v в виде $e_v = \sum x_v^{(i)} e_i$, где коэффициенты $x_v^{(i)} \in r_v$. Положим $x_i = (x_v^{(i)})$ при $1 \leqslant i \leqslant N$. Тогда $x_i \in \prod r_v$. По следствию 1 теор. 1 можно найти такие $\xi_i \in \mathfrak{r}$, что для каждого i элементы $\psi(\xi_i)$ сколь угодно близки к x_i. Тогда, очевидно, элемент $\psi_L(\sum \xi_i e_i)$ может быть сделан сколь угодно близким к e_v.

Теорема 2. *Пусть k — некоторое поле алгебраических чисел, E — векторное пространство конечной размерности над k и L — некоторая k-решетка в E. Для каждой конечной точки v поля k пусть L_v — замыкание решетки L в E_v и M_v — произвольная k_v-решетка в E_v. Тогда k-решетка M в E, замыкание которой в E_v совпадает с M_v при всех v, существует в том и только том случае, когда $M_v = L_v$ почти для всех v; при этом существует только одна такая k-решетка; она задается равенством $M = \bigcap\limits_v (E \cap M_v)$.*

Предположим, что такая k-решетка M существует. Тогда ввиду предложения 4 равенство $M_v = L_v$ почти для всех v есть простая переформулировка следствия 1 теор. 3 гл. III-1. Предположим

теперь, что $M_v = L_v$ почти для всех v. В силу предложения 1 гл. IV-1 отсюда следует открытость множества $E_\infty \times \prod M_v$ в $E_\mathbf{A}$. Поэтому к $G = E_\mathbf{A}$, $G' = E_\infty$, $G'' = \prod M_v$, $\Gamma = \varphi_E(E)$, где φ_E: $E \to E_\mathbf{A}$ — каноническое вложение, можно применить лемму 1. Ясно, что если положить $M = \bigcap (E \cap M_v)$, то $\varphi_E(M)$ совпадает с $\varphi_E(E) \cap G_1$, где $G_1 = G' \times G''$. По лемме 1 M является $\mathbf{R}$-решеткой в E_∞ и, следовательно, $\mathbf{Q}$-решеткой в E. Так как, очевидно, M есть $\mathfrak{r}$-модуль, то M является k-решеткой. По следствию 2 теор. 3 гл. IV-2 группа $E_\infty + \varphi_E(E)$ плотна в $E_\mathbf{A}$, поэтому ее пересечение $E_\infty + \varphi_E(M)$ с G_1 плотно в G_1. Другими словами, проекция $\varphi_E(M)$ на $G'' = \prod M_v$ плотна там; следовательно, решетка M плотна в M_v для каждой точки v. Как и выше, обозначим через ψ_M каноническое вложение $M \to \prod M_v$. Предположим, далее, что существует другая k-решетка M' в E с замыканиями M_v в E_v для всех v. Ясно, что $M' \subset M$. Кроме того, согласно предложению 4, образ $\psi_M(M')$ плотен в $\prod M_v$, а следовательно, и в $\psi_M(M)$. По предложению 1 существует такое целое число $m > 0$, что $M' \supset mM$. Обозначим через G_m образ G_1 при автоморфизме $e \to \varphi(m)e$ пространства $E_\mathbf{A}$. Можно записать G_m в виде $G_m = G' \times G''_m$, где $G''_m = \prod (mM_v)$. Ясно, что $mM_v = M_v$ почти для всех v (а именно для всех конечных точек поля k, которые не лежат над простыми делителями числа m в $\mathbf{Z}$) и G''_m является открытой подгруппой в G''. Далее, $\varphi_E(mM)$ совпадает с $\varphi_E(E) \cap G_m$, а следовательно, и с $\varphi_E(M) \cap G_m$ и содержится в $\psi_M(M')$. Другими словами, $\psi_M(M) \cap G''_m \subset \psi_M(M')$. Возьмем теперь произвольный элемент $\mu \in M$. Так как группа $\psi_M(M')$ плотна в $\psi_M(M)$, то существует такой элемент $\mu' \in M'$, что $\psi_M(\mu - \mu') \in G''_m$. Тогда $\psi_M(\mu - \mu') \in \psi_M(M')$, так что $\mu - \mu' \in M'$ и $\mu \in M'$. Это рассуждение показывает, что $M = M'$. Доказательство теоремы закончено.

Следствие. *Пусть L, L' — две k-решетки в E. Тогда $L + L'$ и $L \cap L'$ являются k-решетками в E и для каждой конечной точки v поля k замыкания этих решеток в E_v выражаются через замыкания L_v, L'_v решеток L, L' формулами*

$$(L + L')_v = L_v + L'_v, \quad (L \cap L')_v = L_v \cap L'_v.$$

Утверждения о $L + L'$ сразу следуют из предложения 4. Рассмотрим пересечение $L \cap L'$. Положим $M_v = L_v \cap L'_v$. Для каждой точки v это — k_v-решетка в E_v, и M_v совпадает с L_v почти для всех v. Поэтому существует k-решетка M в E с замыканием M_v в E_v для каждой v, и M задается как $\bigcap (E \cap M_v)$. Но по теореме 2 последнее множество совпадает с $L \cap L'$.

§ 3. ИДЕАЛЫ

В этом параграфе через k будет обозначаться некоторое поле алгебраических чисел и через $\mathfrak{r}$ — максимальный порядок в k. Результаты § 2 будут применяться к случаю $E = k$. Ясно, что отличный от $\{0\}$ $\mathfrak{r}$-модуль в k является k-решеткой в том и только том случае, когда он конечно порожден. Согласно предложению 1 § 1, для любой k-решетки $\mathfrak{a}$ в k существует такое целое число $m > 0$, что $m\mathfrak{a} \subset \mathfrak{r}$. Тогда, очевидно, $m\mathfrak{a}$ является идеалом в кольце $\mathfrak{r}$. Поэтому в силу следствия 2 предл. 1 § 1 каждый идеал в $\mathfrak{r}$, отличный от $\{0\}$, является k-решеткой. Отсюда видно, что подмножество в k является k-решеткой тогда и только тогда, когда оно имеет вид $\xi\mathfrak{a}$, где $\mathfrak{a}$ — идеал в $\mathfrak{r}$, отличный от $\{0\}$, а $\xi \in k^\times$.

Определение 4. *Всякую k-решетку в k будем называть дробным идеалом в k; дробный идеал в k будем называть целым, если он содержится в $\mathfrak{r}$.*

В соответствии с этим определением $\{0\}$ не является дробным идеалом.

Пусть $\mathfrak{a}$ — дробный идеал в k и L — некоторая k-решетка в конечномерном векторном пространстве E над k. Под $\mathfrak{a}L$ будем понимать подгруппу в E, порожденную всеми элементами вида αe, где $\alpha \in \mathfrak{a}$, $e \in L$. Ясно, что $\mathfrak{a}L$ является k-решеткой в E. Пусть v — произвольная конечная точка поля k. Обозначим, как выше, через $\mathfrak{a}_v$ замыкание $\mathfrak{a}$ в k_v и через L_v, $(\mathfrak{a}L)_v$ — замыкания L, $\mathfrak{a}L$ в E_v. Согласно предложению 4 § 2, эти замыкания порождаются как r_v-модули соответственно множествами $\mathfrak{a}$ и L, $\mathfrak{a}L$. Отсюда ясно, что $(\mathfrak{a}L)_v$ совпадает с подгруппой $\mathfrak{a}_v L_v \subset E_v$, порожденной элементами αe с $\alpha \in \mathfrak{a}_v$, $e \in L_v$.

В частности, если $\mathfrak{a}$, $\mathfrak{b}$ — два дробных идеала в k, то $\mathfrak{ab}$ есть подгруппа аддитивной группы поля k, порожденная элементами вида $\alpha\beta$, где $\alpha \in \mathfrak{a}$, $\beta \in \mathfrak{b}$; $\mathfrak{ab}$ является дробным идеалом в k, и $(\mathfrak{ab})_v = \mathfrak{a}_v\mathfrak{b}_v$ для каждой конечной точки v поля k. Если p_v — максимальный идеал в r_v, то каждая k_v-решетка в k_v имеет вид p_v^n, где $n \in \mathbf{Z}$. В частности, можно записать $\mathfrak{a}_v = p_v^a$, $\mathfrak{b}_v = p_v^b$, где a, $b \in \mathbf{Z}$, и очевидно, что $\mathfrak{a}_v\mathfrak{b}_v = p_v^{a+b}$.

Теорема 3. *Пусть k — поле алгебраических чисел и $\mathfrak{r}$ — его максимальный порядок. Для каждой конечной точки v поля k положим $\mathfrak{p}_v = \mathfrak{r} \cap p_v$. Тогда отображение $v \to \mathfrak{p}_v$ является биекцией множества конечных точек поля k на множество простых идеалов в $\mathfrak{r}$, отличных от $\{0\}$. Относительно операции $(\mathfrak{a}, \mathfrak{b}) \to \mathfrak{ab}$ множество дробных идеалов в k является группой с нейтральным*

элементом $\mathfrak{r}$; *это — свободная абелева группа, порожденная простыми идеалами в* $\mathfrak{r}$; *отличные от* $\{0\}$ *идеалы в* $\mathfrak{r}$ *образуют моноид, порожденный этими простыми идеалами.*

Для каждого дробного идеала $\mathfrak{a}$ в k запись $\mathfrak{a}_v = p_v^{a(v)}$ определяет отображение $v \to a(v)$ множества конечных точек поля k в $\mathbf{Z}$. Для $\mathfrak{a} = \mathfrak{r}$ все $a(v)$ равны нулю. Теорема 2 § 2 показывает, что заданному отображению $v \to a(v)$ тогда и только тогда соответствует некоторый дробный идеал $\mathfrak{a}$, когда $a(v) = 0$ почти для всех v, и что в случае когда это так, $\mathfrak{a}$ определен однозначно, а именно $\mathfrak{a} = \bigcap (k \cap p_v^{a(v)})$. Если $\mathfrak{b}$ соответствует аналогично отображению $v \to b(v)$, то, как показано выше, $\mathfrak{ab}$ соответствует отображению $v \to a(v) + b(v)$. Ясно также, что $\mathfrak{a} \subset \mathfrak{b}$ в том и только том случае, когда $a(v) \geqslant b(v)$ при всех v; в частности, дробный идеал $\mathfrak{a}$ цел тогда и только тогда, когда $a(v) \geqslant 0$ при всех v. Для любого заданного v положим $a(v) = 1$ и $a(v') = 0$ при всех $v' \neq v$ и обозначим через $\mathfrak{p}_v$ соответствующий идеал $\mathfrak{p}_v = \mathfrak{r} \cap p_v$. Ясно, что дробные идеалы образуют свободную абелеву группу, порожденную идеалами $\mathfrak{p}_v$. Так как p_v — простой идеал в r_v, то $\mathfrak{p}_v$ — простой идеал в $\mathfrak{r}$. Покажем теперь, что этими идеалами исчерпываются все ненулевые простые идеалы кольца $\mathfrak{r}$. Пусть $\mathfrak{a}$ — произвольный идеал в $\mathfrak{r}$, так что $a(v) \geqslant 0$ при всех v. Если идеал $\mathfrak{a}$ отличен от $\mathfrak{r}$ и всех $\mathfrak{p}_v$, то мы можем записать его в виде $\mathfrak{a}'\mathfrak{a}''$, где $\mathfrak{a}'$, $\mathfrak{a}'$ — идеалы в $\mathfrak{r}$, отличные от $\mathfrak{r}$. Тогда $\mathfrak{a}'$ содержит $\mathfrak{a}$ и не совпадает с $\mathfrak{a}$, так что множество $\mathfrak{a}' - \mathfrak{a}$ непусто; то же самое справедливо для $\mathfrak{a}'' - \mathfrak{a}$. Возьмем элементы $\alpha' \in \mathfrak{a}' - \mathfrak{a}$ и $\alpha'' \in \mathfrak{a}'' - \mathfrak{a}$. Тогда $\alpha'\alpha'' \in \mathfrak{a}$, хотя ни α', ни α'' не лежат в $\mathfrak{a}$; следовательно, идеал $\mathfrak{a}$ не прост. Доказательство теоремы закончено.

Следствие 1. *Пусть* $\mathfrak{a}$, $\mathfrak{b}$ *— два дробных идеала в* k. *Для каждой точки* v *обозначим через* $a(v)$ *и* $b(v)$ *показатели степеней при* $\mathfrak{p}_v$ *в разложениях* $\mathfrak{a}$ *и* $\mathfrak{b}$ *в произведения степеней простых идеалов в* $\mathfrak{r}$. *Тогда* $\mathfrak{a} + \mathfrak{b}$ *и* $\mathfrak{a} \cap \mathfrak{b}$ *являются дробными идеалами в* k, *и показатели степеней при* $\mathfrak{p}_v$ *в аналогичных разложениях этих идеалов равны соответственно* $\min(a(v), b(v))$ *и* $\max(a(v), b(v))$.

Это немедленно вытекает из теоремы 3 и следствия теор. 2 § 2.

Как обычно, два идеала $\mathfrak{a}$, $\mathfrak{b}$ в $\mathfrak{r}$ называются взаимно простыми, если $\mathfrak{a} + \mathfrak{b} = \mathfrak{r}$.

Следствие 2. *Каждый дробный идеал* $\mathfrak{a}$ *в* k *может быть одним и только одним способом записан в виде* $\mathfrak{bc}^{-1}$, *где* $\mathfrak{b}$ *и* $\mathfrak{c}$ *— взаимно простые идеалы в* $\mathfrak{r}$.

Это немедленно следует из теоремы 3 и следствия 1.

По аналогии со случаем $k = \mathbf{Q}$ идеалы $\mathfrak{b}$, $\mathfrak{c}$ из следствия 2 называются соответственно *числителем* и *знаменателем* дробного идеала $\mathfrak{a}$.

Группу дробных идеалов поля k будем обозначать через $I(k)$. Если $a = (a_v)$ — произвольный элемент из $k_{\mathbf{A}}^{\times}$, то по следствию предл. 2 гл. IV-3 $|a_v|_v = 1$ и, значит, $a_v r_v = r_v$ почти для всех конечных точек v поля k. Поэтому по теореме 3 существует один и только один дробный идеал $\mathfrak{a}$ в k, такой, что $\mathfrak{a}_v = a_v r_v$ для всех конечных точек v; обозначим этот идеал через $\mathrm{id}(a)$. Отображение $a \to \mathrm{id}(a)$ группы $k_{\mathbf{A}}^{\times}$ в $I(k)$, очевидно, сюръективно. Обозначим через Ω_∞ ядро этого отображения, которое, очевидно, равно $k_\infty^{\times} \times (\prod r_v^{\times})$, т. е. $k_{\mathbf{A}}(P_\infty)^{\times}$ в обозначениях следствия предложения 2 гл. IV-3 и $\Omega(P_\infty)$ в обозначениях формулы (5) гл. IV-4. Так как подгруппа Ω_∞ открыта в $k_{\mathbf{A}}^{\times}$, то отображение $a \to \mathrm{id}(a)$ есть морфизм группы $k_{\mathbf{A}}^{\times}$ на группу $I(k)$, наделенную дискретной топологией. Таким образом, можно отождествить $I(k)$ с $k_{\mathbf{A}}^{\times}/\Omega_\infty$.

В частности, для каждого $\xi \in k^{\times}$ имеем $\mathrm{id}(\xi) = \xi\mathfrak{r}$. Этот $\mathfrak{r}$-модуль, порожденный элементом ξ в k, часто обозначается через (ξ), а его числитель и знаменатель, определенные выше, называются *числителем* и *знаменателем* элемента ξ. Дробный идеал называется *главным*, если он имеет вид $\xi\mathfrak{r}$, где $\xi \in k^{\times}$. Главные идеалы образуют подгруппу $P(k)$ в $I(k)$, которая является образом группы $k^{\times}$ относительно морфизма, индуцированного отображением $a \to \mathrm{id}(a)$. Отождествляя $I(k)$ с факторгруппой $k_{\mathbf{A}}^{\times}/\Omega_\infty$, мы видим, что $P(k)$ совпадает с образом группы $k^{\times}$ в этой факторгруппе. Поэтому можно отождествить $I(k)/P(k)$ с группой $k_{\mathbf{A}}^{\times}/k^{\times}\Omega_\infty$, которая конечна по теореме 7 гл. IV-4. Элементы группы $I(k)/P(k)$, другими словами, смежные классы в $I(k)$ по модулю $P(k)$, известны как *классы идеалов* поля k. Число этих классов, т. е. индекс подгруппы $P(k)$ в $I(k)$, будет обозначаться через h.

Теорема 4. *Пусть k — поле алгебраических чисел, E — конечномерное векторное пространство над k и L, M — две k-решетки в E, такие, что $L \supset M$. Для каждой конечной точки v поля k обозначим через L_v, M_v замыкания решеток L, M в E_v и через λ_v — естественный гомоморфизм $L/M \to L_v/M_v$. Тогда отображение $x \to (\lambda_v(x))$, где v пробегает все конечные точки поля k, является изоморфизмом $\mathfrak{r}$-модулей $L/M \to \prod_v (L_v/M_v)$. Здесь $\mathfrak{r}$ — максимальный порядок в k.*

Обозначим рассматриваемое отображение через λ. Очевидно, оно является гомоморфизмом $\mathfrak{r}$-модулей. Пусть x — любой эле-

мент из L/M и e — его представитель в L. Если $\lambda(x) = 0$, то e должен лежать в M_v при всех v. По теореме 2 § 2 отсюда следует, что $e \in M$ и $x = 0$. Поэтому гомоморфизм λ инъективен. Возьмем теперь любой элемент $y = (y_v) \in \prod (L_v/M_v)$ и для каждого v представитель $e_v \in L_v$ элемента y_v. Положим $e = (e_v)$. Так как $M_v = L_v$ почти для всех v, то подгруппа $\prod M_v$ открыта в $\prod L_v$. Поэтому, согласно предложению 4 § 2, существует такой элемент $e_0 \in L$, что $\psi_L(e_0) - e \in \prod M_v$, где ψ_L обозначает каноническое вложение $L \to \prod L_v$. Другими словами, если x_0 — образ элемента e_0 в L/M, то $\lambda(x_0) = y$, чем доказана сюръективность гомоморфизма λ.

Следствие 1. *В обозначениях и предположениях теоремы* 4 $[L : M] = \prod [L_v : M_v]$.

Это очевидно. Следует заметить, что $L_v = M_v$ почти для всех v и M_v является открытой подгруппой компактной группы L_v, так что число $[L_v : M_v]$ всегда конечно и почти всегда равно 1. Конечность индекса $[L : M]$ неявно содержится в предложении 1 § 1, а также в лемме 2 гл. II-4.

Следствие 2. *Пусть v — конечная точка поля k, и пусть $\mathfrak{p}_v = \mathfrak{r} \cap p_v$ — соответствующий точке v простой идеал в максимальном порядке $\mathfrak{r}$ поля k. Тогда естественный гомоморфизм $\mathfrak{r}/\mathfrak{p}_v \to r_v/p_v$ является изоморфизмом кольца $\mathfrak{r}/\mathfrak{p}_v$ на поле вычетов r_v/p_v кольца r_v.*

Следствие 3. *Пусть $\mathfrak{a}$, $\mathfrak{b}$ — два дробных идеала в k, $\mathfrak{a} \supset \mathfrak{b}$, и пусть $\mathfrak{a}^{-1}\mathfrak{b} = \prod \mathfrak{p}_v^{n(v)}$ — разложение дробного идеала $\mathfrak{a}^{-1}\mathfrak{b}$ в произведение степеней простых идеалов кольца $\mathfrak{r}$. Тогда $[\mathfrak{a} : \mathfrak{b}] = \prod [\mathfrak{r} : \mathfrak{p}_v]^{n(v)}$.*

По следствию 1 индекс $[\mathfrak{a} : \mathfrak{b}]$ равен произведению индексов $[\mathfrak{a}_v : \mathfrak{b}_v]$ по всем v. Для данного v можно записать $\mathfrak{a}_v = p_v^a$, $\mathfrak{b}_v = p_v^b$. Поэтому $b - a = n(v)$. Следствие 2 теор. 6 гл I-4 показывает, что $[p_v^a : p_v^b] = q^{b-a}$, где $q = [r_v : p_v]$. Отсюда и из следствия 2 немедленно вытекает наше утверждение.

Определение 5. *Пусть k — некоторое поле алгебраических чисел, $\mathfrak{r}$ — его максимальный порядок и $\mathfrak{a} \to \mathfrak{N}(\mathfrak{a})$ — такой гомоморфизм группы дробных идеалов поля k в $\mathbf{Q}^\times$, что $\mathfrak{N}(\mathfrak{p}) = [\mathfrak{r} : \mathfrak{p}]$ для всех простых идеалов $\mathfrak{p}$ в $\mathfrak{r}$. Тогда число $\mathfrak{N}(\mathfrak{a})$ называется нормой дробного идеала $\mathfrak{a}$ в k.*

Следствие 3 теор. 5 можно теперь переформулировать следующим образом: если $\mathfrak{a}$, $\mathfrak{b}$ — дробные идеалы в k и $\mathfrak{a} \supset \mathfrak{b}$, то $[\mathfrak{a} : \mathfrak{b}] = \mathfrak{N}(\mathfrak{b})/\mathfrak{N}(\mathfrak{a})$. В частности, если $\mathfrak{a}$ цел, то $[\mathfrak{r} : \mathfrak{a}] = \mathfrak{N}(\mathfrak{a})$.

Предложение 5. *Пусть* $a=(a_v)$ *— произвольный элемент из* $k_{\mathbf{A}}^{\times}$. *Тогда* $\mathfrak{N}(\mathrm{id}(a))=\prod|a_v|_v^{-1}$, *где произведение берется по всем конечным точкам поля* k.

В силу определения 5 достаточно проверить это равенство в случае, когда $\mathrm{id}(a)$ — простой идеал в $\mathfrak{r}$, т. е. когда a_v — простой элемент в k_v для некоторой конечной точки v и $|a_{v'}|_{v'}=1$ для всех конечных точек $v'\neq v$ поля k. Но в этом случае равенство очевидно.

Следствие 1. *Для всякого элемента* $\xi\in k^{\times}$ *имеет место равенство* $\mathrm{N}_{k/\mathbf{Q}}(\xi)=(-1)^{\rho}\mathfrak{N}(\mathrm{id}(\xi))$, *где* ρ *— число вещественных точек* w *поля* k, *для которых образ элемента* ξ *в* k_w *строго отрицателен*.

Комбинируя предложение 5 с теоремой 5 гл. IV-4, немедленно получаем, что норма $\mathfrak{N}(\mathrm{id}(\xi))$ равна произведению $\prod|\xi|_w$, взятому по бесконечным точкам w поля k.

Для всякой вещественной точки w поля k и всякого $x\in k_w^{\times}$ имеем $x=(\mathrm{sign}\,x)\cdot|x|_w$; для всякой мнимой точки w поля k и всякого $x\in k_w^{\times}$ имеем $\mathrm{N}_{k_w/\mathbf{R}}(x)=x\bar{x}=|x|_w$. Наше утверждение немедленно вытекает теперь из следствия 3 теор. 4 гл. III-4, примененного к k, $\mathbf{Q}$ и точке ∞ поля $\mathbf{Q}$.

Следствие 2. *Элемент* ξ *максимального порядка* $\mathfrak{r}$ *поля* k *обратим в* $\mathfrak{r}$ *тогда и только тогда, когда* $\mathrm{N}_{k/\mathbf{Q}}(\xi)=\pm 1$.

Ясно, что ξ обратим в $\mathfrak{r}$, тогда и только тогда, когда $\xi\mathfrak{r}=\mathfrak{r}$. Так как $\xi\mathfrak{r}$ — это то же самое, что $\mathrm{id}(\xi)$, то наше утверждение немедленно вытекает из следствия 1 и того факта, что $[\mathfrak{r}:\mathfrak{a}]=\mathfrak{N}(\mathfrak{a})$ для каждого идеала $\mathfrak{a}$ в кольце $\mathfrak{r}$.

Элементы группы $\mathfrak{r}^{\times}$, т. е. обратимые элементы кольца $\mathfrak{r}$, называются по традиции «единицами» в k. В обозначениях гл. IV-4 $\mathfrak{r}^{\times}=E(P_{\infty})$; структура этой группы описывается теоремой 9 гл. IV-4: если число бесконечных точек поля k равно $r+1$, то группа $\mathfrak{r}^{\times}$ изоморфна прямому произведению циклической группы E всех корней из 1 в k и группы, изоморфной $\mathbf{Z}^r$. Это — «теорема об единицах» Дирихле.

§ 4. ФУНДАМЕНТАЛЬНЫЕ МНОЖЕСТВА

Пусть Γ — дискретная подгруппа в локально компактной группе G. Под *фундаментальным множеством в* G относительно Γ по традиции понимается полное множество X представителей клас-

сов смежности группы G по модулю Γ, причем требуется, чтобы X было измеримо, и обычно предполагается, что X обладает некоторыми дополнительными свойствами, например является борелевским множеством и т. п. Тогда формула 6 гл. II-4, примененная к G, к Γ, к мере Хаара α на G и к характеристической функции множества X, показывает, что $\alpha(X) = \alpha(G/\Gamma)$. Таким образом, меру $\alpha(G/\Gamma)$ иногда можно эффективно вычислить с помощью построения подходящего фундаментального множества. Более общим образом, назовем измеримое подмножество X в G *фундаментальным порядка* ν относительно Γ, если оно содержит в точности ν точек из каждого смежного класса по модулю Γ; тогда та же самая формула дает $\alpha(X) = \nu\alpha(G/\Gamma)$. Применим теперь все это к случаям $G = k_{\mathbf{A}}$ и $G = k_{\mathbf{A}}^{\times}$.

Пусть k и $\mathfrak{r}$ такие, как выше, и n — степень поля k над $\mathbf{Q}$. Так как $\mathfrak{r}$ является $\mathbf{Q}$-решеткой в k, рассматриваемом как векторное пространство над $\mathbf{Q}$, то, согласно предложению 11 гл. II-4, $\mathfrak{r}$ порождается некоторым базисом $\{\xi_1, \ldots, \xi_n\}$ в k над $\mathbf{Q}$. Поэтому этот базис является также базисом в $k_\infty = k \otimes_{\mathbf{Q}} \mathbf{R}$ над $\mathbf{R}$. Следовательно, положив $\theta(u) = \sum u_i\xi_i$ для $u = (u_1, \ldots, u_n) \in \mathbf{R}^n$, мы определим изоморфизм $\theta\colon \mathbf{R}^n \to k_\infty$.

Предложение 6. *Пусть k, $\mathfrak{r}$ и θ такие, как выше; обозначим через I интервал $0 \leqslant t < 1$ в $\mathbf{R}$. Тогда множество $\theta(I^n) \times \prod_v r_v$, где произведение взято по всем конечным точкам v поля k, является фундаментальным множеством в $k_{\mathbf{A}}$ относительно k.*

Обозначим рассматриваемое множество через X. Оно, очевидно, измеримо. Нам надо показать, что каждый элемент $x \in k_{\mathbf{A}}$ может быть записан одним и только одним способом в виде $x_0 + \xi$, где $x_0 \in X$ и $\xi \in k$. По следствию 2 теор. 3 гл. IV-2 группа $k_\infty + k$ плотна в $k_{\mathbf{A}}$. Следовательно, поскольку подгруппа $k_\infty \times \prod r_v$ открыта, для любого $x \in k_{\mathbf{A}}$ существует такой $\eta \in k$, что $x - \eta \in k_\infty \times \prod r_v$. Из определения $\mathfrak{r}$ видно, что элемент $\eta' \in k$ обладает таким же свойством тогда и только тогда, когда $\eta' - \eta \in \mathfrak{r}$. Полагая $y = x - \eta$ и обозначая через y_∞ проекцию этого элемента из произведения $k_\infty \times \prod r_v$ на k_∞, можно записать $y_\infty = \theta(u)$, где $u = (u_1, \ldots, u_n) \in \mathbf{R}^n$. Для каждого i найдем такое $a_i \in \mathbf{Z}$, что $a_i \leqslant u_i < a_i + 1$, т. е. $u_i - a_i \in I$. Положим $\xi = \eta - \sum_i a_i\xi_i$ и $x_0 = x - \xi$. Так как $\xi - \eta \in \mathfrak{r}$, то $x_0 \in k_\infty \times \prod r_v$. Далее, проекция элемента x_0 на k_∞, равная

$$y_\infty - \sum_i a_i\xi_i = \sum_i (u_i - a_i)\xi_i,$$

лежит в $\theta(I^n)$. Ясно также, что последнее условие не будет выполняться ни при каком другом выборе целых чисел a_i. Тем самым наше утверждение доказано.

Предложение 6 будет сейчас использовано для вычисления меры $\alpha(k_{\mathbf{A}}/k)$ для явно заданной меры Хаара α на $k_{\mathbf{A}}$. Такую меру можно построить следующим образом. Для каждой точки v поля k выберем меру Хаара α_v на k_v. Если $\alpha_v(r_v) = 1$ почти для всех v, то произведение мер $\prod \alpha_v$ корректно определено и является мерой Хаара на каждой из открытых подгрупп $k_{\mathbf{A}}(P) \subset k_{\mathbf{A}}$, определенных формулой (1) гл. IV-1. Ясно, что существует одна и только одна мера Хаара на $k_{\mathbf{A}}$, которая совпадает с этими мерами на их областях определения и которую мы будем обозначать через $\prod \alpha_v$. В частности, обозначим через β меру Хаара $\prod \beta_v$, которая получается, если взять $\beta_v(r_v) = 1$ для всех конечных точек v поля k, а для бесконечных точек определить меру следующим образом. Если w — вещественная точка, то пусть β_w — мера Лебега на $k_w = \mathbf{R}$, т. е. $d\beta_w(x) = dx$. Если же w — мнимая точка, то меру β_w на $k_w = \mathbf{C}$ выберем так, чтобы $d\beta_w(x) = |\, dx \wedge d\bar{x}\,|$; это означает, что если мы положим $x = u + iv$, где $u, v \in \mathbf{R}$, так что $dx \wedge d\bar{x} = -2i\,(du \wedge dv)$, то β_w есть мера, соответствующая дифференциальной форме $2du \wedge dv$; другими словами, $\beta_w/2$ есть мера Лебега на плоскости u, v.

Для вычисления $\beta(k_{\mathbf{A}}/k)$ нам понадобится еще одно определение. В уже много раз применявшихся выше обозначениях рассмотрим матрицу

$$M = (\mathrm{Tr}_{k/\mathbf{Q}}(\xi_i \xi_j))_{1 \leqslant i,j \leqslant n} \tag{1}$$

и обозначим через D ее определитель. По предложению 5 гл. III-3 $D \neq 0$; по предложению 3 § 1 $M \in M_n(\mathbf{Z})$, так что $D \in \mathbf{Z}$. Если $k = \mathbf{Q}$, то $\mathfrak{r} = \mathbf{Z}$, так что $\xi_1 = \pm 1$ и, следовательно, $D = 1$. Если $\{\eta_1, \ldots, \eta_n\}$ — другое множество образующих для $\mathfrak{r}$ и N — матрица, полученная заменой в (1) ξ_i на η_i, то можно записать $\eta_i = \sum a_{ij}\xi_j$, где $a_{ij} \in \mathbf{Z}$ при всех i, j. Тогда $N = AM^tA$, где A — матрица (a_{ij}). Аналогично можно записать $\xi_i = \sum b_{ij}\eta_j$, где $b_{ij} \in \mathbf{Z}$ при всех i, j. Обозначая через B матрицу (b_{ij}), получаем $AB = 1$; следовательно, $\det(A)\det(B) = 1$. Так как $\det(A)$ и $\det(B)$ лежат в $\mathbf{Z}$, отсюда вытекает, что $\det(A) = \pm 1$, значит $\det(N) = \det(M)$. Другими словами, определитель D матрицы M не зависит от выбора базиса. Этим оправдано следующее

Определение 6. *Пусть k и $\{\xi_1, \ldots, \xi_n\}$ таковы, как выше. Тогда определитель D матрицы M, задаваемой формулой* (1), *называется дискриминантом поля k.*

Предложение 7. *Пусть* $\beta = \prod \beta_v$ — *мера Хаара на* $k_{\mathbf{A}}$, *причем* $\beta_v(r_v) = 1$ *для всех конечных точек* v, $d\beta_w(x) = dx$ *для всех вещественных точек* w *и* $d\beta_w(x) = |dx \wedge d\bar{x}|$ *для всех мнимых точек* w *поля* k. *Тогда* $\beta(k_{\mathbf{A}}/k) = |D|^{1/2}$, *где* D — *дискриминант поля* k.

Обозначим через β_∞ меру $\prod \beta_w$ на $k_\infty = \prod k_w$, где произведения берутся по всем бесконечным точкам w поля k. По предложению 6 $\beta(k_{\mathbf{A}}/k)$ совпадает с $\beta_\infty(\theta(I^n))$, поэтому наше предложение будет доказано, если мы покажем, что

$$d\beta_\infty(\theta(u)) = |D|^{1/2}\, du_1 \ldots du_n.$$

Обозначим через r_1 и r_2 соответственно число вещественных и мнимых точек поля k и положим $r = r_1 + r_2 - 1$. Пусть $w_0, \ldots, w_r$ — бесконечные точки поля k, упорядоченные так, что точка w_i вещественна при $i < r_1$ и мнима при $i \geqslant r_1$. Для каждого i обозначим через k_i пополнение поля k относительно w_i, через λ_i — естественное вложение $k \to k_i$ и через μ_i — $\mathbf{R}$-линейное продолжение вложения λ_i на k_∞. Если, как это было сделано выше, отождествить k_∞ с $\prod k_i$, то теорема 4 гл. III-4 показывает, что μ_i является проекцией из k_∞ на k_i. По следствию 1 предл. 3 гл. III-2 каждое изоморфное вложение $\lambda'\colon k \to \mathbf{C}$ имеет вид $\sigma \circ \lambda_i$, где σ — некоторый $\mathbf{R}$-линейный изоморфизм поля k_i в $\mathbf{C}$; очевидно, что если $k_i = \mathbf{R}$, т. е. если $i < r_1$, то σ есть естественное вложение поля k_i в $\mathbf{C}$, а если $k_i = \mathbf{C}$, т. е. $i \geqslant r_1$, то σ — это одно из двух отображений $x \to x$ или $x \to \bar{x}$ поля $\mathbf{C}$ на $\mathbf{C}$. Поэтому, если положить $\lambda'_i = \lambda_i$ при $0 \leqslant i \leqslant r$ и $\lambda'_{r_2+i} = \bar{\lambda}_i$ при $r_1 \leqslant i \leqslant r$, то вложениями λ'_h, $0 \leqslant h \leqslant n-1$, будут исчерпываться все различные изоморфизмы поля k в $\mathbf{C}$. Обозначая теперь $\mathbf{R}$-линейное продолжение вложения λ'_h на k_∞ через μ'_h, имеем

$$\mu'_h(\theta(u)) = \sum_{i=1}^{n} \lambda'_h(\xi_i)\, u_i,$$

где $u = (u_1, \ldots, u_n) \in \mathbf{R}^n$ и $0 \leqslant h \leqslant n-1$. Обозначим через N матрицу коэффициентов $(\lambda'_h(\xi_i))$ в правой части равенства. Согласно следствию 3 предложения 4 гл. III-3, $\mathrm{Tr}_{k/\mathbf{Q}}(\xi) = \sum \lambda'_h(\xi)$ при всех $\xi \in k$; поскольку λ'_h суть изоморфизмы, отсюда вытекает, что

$$M = \Big(\sum_h \lambda'_h(\xi_i)\, \lambda'_h(\xi_j)\Big) = {}^tN \cdot N,$$

следовательно, $D = \det(N)^2$. В то же время во внешней алгебре дифференциальных форм на $\mathbf{R}^n$ выполняются соотношения

$$(2)\quad \prod_h d\mu'_h(\theta(u)) = \pm \prod_{0 \leqslant i < r_1} d\mu_i(\theta(u)) \wedge$$
$$\wedge \prod_{r_1 \leqslant j \leqslant r} (d\mu_j(\theta(u)) \wedge d\bar{\mu}_j(\theta(u))) = \pm \det(N)\, du_1 \wedge \ldots \wedge du_n.$$

Ввиду определения мер β_w доказательство предложения 7 закончено. Можно заметить, что если умножить (2) на i^{r_2}, то получится вещественная дифференциальная форма на $\mathbf{R}^n$. Поэтому $i^{r_2}\det(N)$ — вещественное число; другими словами, $(-1)^{r_2} D > 0$.

Следствие 1. *Если* $k \neq \mathbf{Q}$, *то* $|D| > 1$.

Придерживаясь введенных выше обозначений, для $0 \leqslant i \leqslant r$ выберем $c_i \in \mathbf{R}_+^\times$ и обозначим через $Y(c)$ множество таких элементов $y = (y_v) \in k_\mathbf{A}$, что $|y_v|_v \leqslant 1$ для всех конечных точек v поля k и $|y_{w_i}|_{w_i} \leqslant c_i/2$ при $0 \leqslant i \leqslant r$. Для каждой бесконечной точки w и каждого $c \in \mathbf{R}_+^\times$ подмножество в k_w, задаваемое неравенством $|x|_w \leqslant c/2$, является интервалом длины c, если w — вещественная точка, и кругом β_w-меры πc, если w — мнимая точка. С учетом определения β это дает $\beta(Y(c)) = \pi^{r_2} \prod c_i$. Если это число больше, чем $|D|^{1/2}$, то лемма 1 гл. II-4 в сочетании с предложением 7 показывает, что существуют такие $y, y' \in Y(c)$, что $\eta = y - y' \in k^\times$. Тогда $|\eta|_v \leqslant 1$ для всех конечных точек v поля k, $(\eta)_{w_i} \leqslant c_i$, если w_i — вещественная точка, и, очевидно, $|\eta|_{w_i} \leqslant 2c_i$, если w_i — мнимая точка. Отсюда ввиду теоремы 5 гл. IV-4 вытекает, что $2^{r_2} \prod c_i \geqslant 1$. Предположим, что $r_2 > 0$. Тогда если бы $|D| = 1$, то, выбрав c_i так, чтобы $\prod c_i$ было $> \pi^{-r_2}$ и $< 2^{-r_2}$, мы получили бы противоречие. Теперь предположим, что $r_2 = 0$, так что $r_1 = n$, и $|D| = 1$. Тогда при любом выборе c_i, удовлетворяющем условию $\prod c_i > 1$, существует $\eta \in k^\times$ с указанными выше свойствами. Ясно, что множество элементов $x = (x_v) \in k_\mathbf{A}$, таких, что $|x_v|_v \leqslant 1$ для всех конечных точек v и $|x_w|_w \leqslant 2$ для всех бесконечных точек w, компактно и потому содержит лишь конечное число элементов $\eta_1, \ldots, \eta_N$ поля k. Следовательно, можно выбрать $c' > 1$ так, чтобы ни одно из η_ν не удовлетворяло неравенствам $1 \leqslant |\eta_\nu|_{w_0} \leqslant c'$. Выберем теперь c_i так, чтобы выполнялись неравенства $\prod c_i > 1$, $1 < c_0 < c'$, $c_0 < 2$ и $c_i < 1$ при $1 \leqslant i \leqslant n-1$. Тогда существует $\eta \in k^\times$, для которого $|\eta|_{w_i} \leqslant c_i$ при $0 \leqslant i \leqslant n-1$ и $|\eta|_v \leqslant 1$ для всех конечных точек v. Ввиду нашего выбора c' и c_i отсюда следует, что $|\eta|_{w_i} < 1$ при $i > 0$ и $|\eta|_{w_0} \leqslant 1$. Но если $n \neq 1$, это противоречит теореме 5 гл. IV-4.

Следствие 2. *Существует лишь конечное число полей алгебраических чисел заданной степени n над $\mathbf{Q}$ и с заданным дискриминантом D.*

Поскольку это утверждение нигде в дальнейшем не используется, мы дадим лишь набросок доказательства. Рассуждая точно так же, как выше, мы видим, что существует такое число $\eta \in k^\times$, что $|\eta|_v \leqslant 1$ для всех конечных точек v поля k и $|\eta|_w < 1$ для всех бесконечных точек w, кроме одной такой точки w_0, причем образ $\lambda_0(\eta)$ числа η в k_{w_0} лежит в интервале $|x| \leqslant 2|D|^{1/2}$, если точка w_0 вещественна, и в прямоугольнике, задаваемом неравенствами $|u| \leqslant 1$, $|v| \leqslant |D|^{1/2}$, $x = u + iv$, если точка w_0 мнима. Поскольку должно выполняться неравенство $|\eta|_{w_0} > 1$, из последнего условия следует, что число $\lambda_0(\eta)$ невещественно, если точка w_0 мнима. Отсюда вытекает, что $k = \mathbf{Q}(\eta)$. Действительно, в противном случае обозначим через u точку поля $\mathbf{Q}(\eta)$, лежащую под w_0; тогда $|\eta|_w > 1$ для всех точек w поля k, лежащих над u, если таких точек больше одной, и число $\lambda_0(\eta)$ должно быть вещественным, если точка u вещественна, а w_0 мнима; поскольку это не так, следствие 1 теор. 4 гл. III-4 показывает, что степень k над $\mathbf{Q}(\eta)$ не может быть больше 1. Отсюда следует, что все $\lambda'_h(\eta)$, $0 \leqslant h \leqslant n-1$, различны, так что $\prod(x - \lambda'_h(\eta))$ — неприводимый многочлен в $\mathbf{Q}[x]$ со старшим коэффициентом 1 и с корнем η. Коэффициенты этого многочлена, очевидно, ограничены по модулю некоторым числом, зависящим от $|D|$; все они лежат в $\mathbf{Z}$, ибо $|\eta|_v \leqslant 1$ для всех конечных точек v поля k, другими словами, $\eta \in \mathfrak{r}$, т. е. элемент η цел над $\mathbf{Z}$. Поэтому таких многочленов, а следовательно, и чисел η, может быть при заданном D лишь конечное число.

Теперь мы рассмотрим соответствующие вопросы для $k_{\mathbf{A}}^\times/k^\times$. Как и выше, обозначим через Ω_∞ ядро отображения $a \to \mathrm{id}(a)$. Это не что иное, как группа $k_\infty^\times \times \prod r_v^\times \subset k_{\mathbf{A}}$, или $\Omega(P_\infty)$ в обозначениях гл. IV-4. Будем писать Ω_1 вместо $\Omega_1(P_\infty)$ для обозначения $\Omega_\infty \cap k_{\mathbf{A}}^1$. Как и в гл. IV-4, обозначим через U группу таких элементов $(z_v) \in k_{\mathbf{A}}^\times$, что $|z|_v = 1$ для всех точек v, конечных и бесконечных; это компактная подгруппа в Ω_1. Как было отмечено в § 3, $\mathfrak{r}^\times$ совпадает с группой, обозначавшейся в гл. IV-4 через $E(P_\infty)$. По-прежнему будем обозначать через E циклическую группу корней из 1 в k. Запишем опять бесконечные точки $w_0, \ldots, w_r$ поля k в каком-нибуь порядке. Для каждого аделя $z = (z_v) \in \Omega_\infty$ положим

$$l(z) = (\log(|z_{w_0}|_{w_0}, \ldots, \log(|z_{w_r}|_{w_r})). \tag{3}$$

Отображение l: $\Omega_\infty \to \mathbf{R}^{r+1}$, определенное формулой (3), является, очевидно, морфизмом (мультипликативно записываемой) группы Ω_∞ на (аддитивно записываемую) группу $\mathbf{R}^{r+1}$; ядро этого морфизма совпадает с U. Пусть λ — линейная форма на $\mathbf{R}^{r+1}$, задаваемая равенством $\lambda(x) = \sum x_i$, где $x = (x_0, \ldots, x_r)$. Тогда $\log(|z|_A) = \lambda(l(z))$ при $z \in \Omega_\infty$. Поэтому если H — гиперплоскость в $\mathbf{R}^{r+1}$, определяемая уравнением $\lambda(x) = 0$, то множество $l^{-1}(H)$, являющееся ядром отображения $\lambda \circ l$, совпадает с Ω_1 и l индуцирует морфизм из Ω_1 на H с ядром U. Этот морфизм мы можем использовать для отождествления группы $G_1 = \Omega_1/U$ с векторным пространством H. Положим $\Gamma = l(\mathfrak{r}^\times)$. По следствию теор. 9 гл. IV-4 Γ есть дискретная подгруппа в H, и факторгруппа H/Γ компактна; другими словами, Γ есть $\mathbf{R}$-решетка в H. Отсюда следует (так же, как и при доказательстве теоремы 9 гл. IV-4), что r элементов $\varepsilon_1, \ldots, \varepsilon_r$ из $\mathfrak{r}^\times$ будут свободными образующими для некоторой подгруппы в $\mathfrak{r}^\times$ тогда и только тогда, когда их образы $l(\varepsilon_i)$ в $\mathbf{R}^{r+1}$ образуют базис в H, и что $\mathfrak{r}^\times$ разлагается в прямое произведение подгруппы E и этой подгруппы в том и только в том случае, когда эти образы порождают группу Γ; в этом случае будем говорить, что ε_i образуют *систему свободных образующих для* $\mathfrak{r}^\times$ *по модулю* E. Предположим теперь, что такая система образующих уже выбрана. Для $0 \leqslant i \leqslant r$ обозначим через δ_i степень поля k_{w_i} над $\mathbf{R}$; $\delta_i = 1$ или 2 в соответствии с тем, вещественна или мнима точка w_i. По следствию 2 теор. 4 гл. III-4 $\sum_i \delta_i = n$, т. е. $\lambda(\delta) = n$, если обозначить через δ вектор $(\delta_0, \ldots, \delta_r)$ в $\mathbf{R}^{r+1}$. Отсюда следует, что δ вместе с векторами $l(\varepsilon_i)$, $1 \leqslant i \leqslant r$, образует базис в $\mathbf{R}^{n+1}$, так что можно следующим образом определить автоморфизм F пространства $\mathbf{R}^{n+1}$:

$$t = (t_1, \ldots, t_r) \to F(t) = n^{-1} t_0 \delta + \sum_{i=1}^{n} t_i l(\varepsilon_i). \tag{4}$$

Имеем $\lambda(F(t)) = t_0$ и

$$l\left(\eta \prod_i \varepsilon_i^{n_i}\right) = F(0, n_1, \ldots, n_r), \tag{5}$$

где $\eta \in E$ и $(n_1, \ldots, n_r) \in \mathbf{Z}^r$.

Предложение 8. *Положим* $\Omega_\infty = k_\infty^\times \times \prod r_v^\times$, *и пусть* l *— морфизм из* Ω_∞ *на* $\mathbf{R}^{n+1}$, *задаваемый формулой* (3); $\{a_1, \ldots, a_h\}$ *— полное множество представителей смежных классов по модулю* $k^\times \Omega_\infty$ *в* $k_\mathbf{A}^\times$; E *— группа всех корней из* 1 *в* k; e *— порядок этой группы*; $\{\varepsilon_1, \ldots, \varepsilon_r\}$ *— система свободных образующих*

для $\mathfrak{r}^\times$ *по модулю* E; F *— автоморфизм пространства* $\mathbf{R}^{r+1}$, *задаваемый формулой* (4), *и* I *— интервал* $0 \leqslant t < 1$ *в* $\mathbf{R}$. *Тогда объединение множеств* $a_i l^{-1}(F(\mathbf{R} \times I^r))$, $1 \leqslant i \leqslant h$, *является фундаментальным множеством порядка* e *в* $k_\mathbf{A}^\times$ *по модулю* $k^\times$.

Возьмем произвольный элемент $z = (z_v)$ в $k_\mathbf{A}^\times$. Существует один и только один индекс i, для которого $a_i^{-1} z \in k^\times \Omega_\infty$. Можно записать $z = a_i \xi z'$, где $\xi \in k^\times$, $z' \in \Omega_\infty$, причем элемент z' однозначно определен по модулю $k^\times \cap \Omega_\infty$, т. е. по модулю $\mathfrak{r}^\times$. Положим $F^{-1}(l(z')) = (t_0, \ldots, t_r)$. Для $1 \leqslant i \leqslant r$ возьмем такие $n_i \in \mathbf{Z}$, что $n_i \leqslant t_i < n_i + 1$. Положим $\varepsilon = \prod \varepsilon_i^{n_i}$, $z'' = \varepsilon^{-1} z'$ и $\varepsilon' = \xi\varepsilon$. Тогда $z = \xi' a_i z''$ и ввиду (4) и (5) $l(z'') \in F(\mathbf{R} \times I^r)$. Далее ясно, что этими условиями элемент z'' определен однозначно по модулю E. Доказательство предложения закончено.

Как мы видели в § 3, морфизм $z \to \mathrm{id}(z)$ из $k_\mathbf{A}^\times$ на $I(k)$ определяет изоморфизм группы $k_\mathbf{A}^\times / k^\times \Omega_\infty$ на группу $I(k)/P(k)$ классов идеалов поля k. Поэтому число h, фигурирующее в формулировке предложения 8, совпадает с порядком этой группы, и идеалы a_i из этого предложения могут быть охарактеризованы тем свойством, что дробные идеалы $\mathrm{id}(a_i)$ являются представителями классов идеалов поля k.

Теперь определим меру Хаара γ на $k_\mathbf{A}^\times$. Как и в случае $k_\mathbf{A}$, это можно сделать, выбрав для каждой точки v меру Хаара γ_v на $k_\mathbf{A}^\times$ так, чтобы $\gamma_v(r_v^\times) = 1$ почти для всех v, и потребовав, чтобы γ совпадала с $\prod \gamma_v$ на каждой группе $k_\mathbf{A}(P_\infty)^\times$. Полученную меру γ будем обозначать через $\prod \gamma_v$. Как и в случае $k_\mathbf{A}$, нам понадобится одно определение.

Определение 7. *Во введенных выше обозначениях пусть* L *— матрица, составленная из строчек* $n^{-1}\delta$, $l(\varepsilon_1)$, ..., $l(\varepsilon_r)$. *Тогда* $R = |\det(L)|$ *называется регулятором поля* k.

Так как L является матрицей автоморфизма F: $\mathbf{R}^{n+1} \to \mathbf{R}^{n+1}$, задаваемого формулой (4), то F имеет определитель $\pm R$. Наше определение будет оправдано, если мы докажем независимость R от выбора ε_i. Это легко можно было бы сделать таким же способом, как и для дискриминанта. Но мы получим этот факт как следствие приводимого ниже предложения.

Предложение 9. *Пусть* $\gamma = \prod \gamma_v$ *— мера Хаара на* $k_\mathbf{A}^\times$, *где* $\gamma_v(r_v^\times) = 1$ *для всех конечных точек* v *поля* k, $d\gamma_w(x) = |x|^{-1} dx$ *для каждой вещественной точки* w *и* $d\gamma_w(x) = (x\bar{x})^{-1} |dx \wedge d\bar{x}|$ *для каждой мнимой точки* w. *Для каждого числа* $m > 1$ *в* $\mathbf{R}$ *обозна-*

чим через $C(m)$ *образ в* $k_{\mathbf{A}}^{\times}/k^{\times}$ *подмножества в* $k_{\mathbf{A}}^{\times}$, *определенного неравенствами* $1 \leqslant |z|_{\mathbf{A}} \leqslant m$. *Тогда* $\gamma(C(m)) = c_k \log(m)$, *где*

$$c_k = 2^{r_1}(2\pi)^{r_2} hR/e.$$

Здесь, как и выше, r_1 и r_2 — это соответственно число вещественных и число мнимых точек поля k, h — число классов идеалов, R — регулятор и e — порядок группы E всех корней из 1 в k, который всегда четен, так как $\pm 1 \in k$. Очевидно, $e = 2$ при $r_1 > 0$, поскольку $\mathbf{R}$ не содержит никаких корней из 1, кроме ± 1.

Доказательство предложения начнем с того, что заменим представителей a_i смежных классов в $k_{\mathbf{A}}^{\times}$ по модулю $k^{\times}\Omega_\infty$, введенных в предложении 8. А именно для каждого i заменим a_i на $a_i b_i^{-1}$, где $b_i \in \Omega_\infty$ и $|b_i|_{\mathbf{A}} = |a_i|_{\mathbf{A}}$. Теперь $|a_i|_{\mathbf{A}} = 1$ при $1 \leqslant i \leqslant h$ и, согласно предложению 8, $e\gamma(C(m)) = h\gamma(X)$, где X — пересечение множества $l^{-1}(F(\mathbf{R} \times I^r))$ с множеством $1 \leqslant |z|_{\mathbf{A}} \leqslant m$ в $k_{\mathbf{A}}^{\times}$. Как мы видели выше, если $z \in \Omega_\infty$ и $F^{-1}(l(z)) = (t_0, \ldots, t_r)$, то

$$\log(|z|_{\mathbf{A}}) = \lambda(l(z)) = \lambda(F(t)) = t_0.$$

Поэтому множество X может быть записано в виде $l^{-1}(F(J \times I^r))$, где J — интервал $0 \leqslant t \leqslant \log(m)$ в $\mathbf{R}$. Поскольку l — морфизм из Ω_∞ на $\mathbf{R}^{r+1}$ с компактным ядром U, то для любого компактного подмножества $Y \subset \mathbf{R}^{r+1}$ прообраз $l^{-1}(Y)$ является компактным подмножеством в Ω_∞ и отображение $Y \to \gamma(l^{-1}(Y))$ определяет меру Хаара на $\mathbf{R}^{r+1}$, которая, как известно, есть некоторое кратное $c\alpha$ меры Лебега α на $\mathbf{R}^{r+1}$, где постоянная $c > 0$. Отсюда вытекает, что $\gamma(x) = c\alpha(F(J \times I^r))$. По определению регулятор R равен модулю определителя автоморфизма F пространства $\mathbf{R}^{r+1}$, откуда

$$\gamma(X) = c\alpha(F(J \times I^r)) = cR\alpha(J \times I^r) = cR \log(m).$$

Осталось только найти c. Возьмем $Y = J^{n+1}$, так что $\alpha(Y) = (\log m)^{r+1}$. Тогда $l^{-1}(Y)$ есть множество элементов $(z_v) \in \Omega_\infty$, таких, что $1 \leqslant |z|_w \leqslant m$ для всех бесконечных точек w поля k. Ввиду нашего определения меры γ имеем $\gamma(l^{-1}(Y)) = a^{r_1}b^{r_2}$, где

$$a = 2\int_1^m x^{-1}\,dx = 2\log m,$$

$$b = \iint\limits_{1 \leqslant x\bar{x} \leqslant m} (x\bar{x})^{-1} |dx \wedge d\hat{x}| = 2\pi \log m.$$

Это дает $c = 2^{r_1}(2\pi)^{r_2}$, чем и заканчивается доказательство.

Предложение 9 показывает, что R не зависит от выбора ε_i, как и утверждалось.

ГЛАВА ШЕСТАЯ

ТЕОРЕМА РИМАНА — РОХА

Классическая теория полей алгебраических чисел, изложенная в гл. V, опирается на тот факт, что в таких полях имеется непустое множество точек, а именно бесконечных точек, выделяющихся своими внутренними свойствами. Можно было бы развить аналогичную теорию для A-полей характеристики $p > 1$ с произвольно выделенным конечным множеством точек; эта точка зрения была принята Дедекиндом и Вебером на ранних стадиях развития теории. Какому бы методу ни следовать, изучение таких полей очень скоро приводит к результатам, которые нельзя как следует понять без использования понятий, относящихся к алгебраической геометрии, которая лежит в стороне от основного содержания этой книги. Излагаемые здесь результаты надо рассматривать главным образом как иллюстрацию развитых выше методов и как введение в более общую теорию.

Начиная с этого места во всей главе k обозначает некоторое A-поле характеристики $p > 1$. В следствии теор. 8 гл. IV-4 было определено конечное поле F, названное *полем констант* в k. Это — алгебраическое замыкание простого поля в k и, следовательно, оно может быть описано как максимальное конечное поле, содержащееся в k. Начиная с этого места число элементов в поле F обозначается через q и F отождествляется с $\mathbf{F}_q$. Тогда для каждой точки v поля k пополнение k_v содержит $\mathbf{F}_q$. В силу следствия 1 теор. 7 гл. I-4 и следствия 2 теор. 2 гл. I-1 отсюда вытекает, что модуль q_v поля k_v имеет вид q^d, где d — целое число $\geqslant 1$, называемое *степенью точки* v и обозначаемое через $\deg v$.

Под *дивизором* поля k понимается элемент свободной абелевой группы $D(k)$, порожденной точками поля k. Будучи записываема аддитивно, эта группа состоит из формальных сумм $\sum_v a(v) \cdot v$, где $a(v) \in \mathbf{Z}$ для каждой точки v поля k и $a(v) = 0$ почти для всех v. Для дивизора $\mathfrak{a} = \sum a(v) \cdot v$ будем писать $\mathfrak{a} > 0$, если $a(v) \geqslant 0$ при всех v. Пусть $\mathfrak{a}$, $\mathfrak{b}$ — два дивизора. Мы пишем

$\mathfrak{a} \succ \mathfrak{b}$, если $\mathfrak{a} - \mathfrak{b} \succ 0$. Для каждого дивизора $\mathfrak{a} = \sum a(v) \cdot v$ положим $\deg(\mathfrak{a}) = \sum a(v) \deg(v)$ и назовем это число *степенью* дивизора $\mathfrak{a}$. Ясно, что отображение $\mathfrak{a} \to \deg(\mathfrak{a})$ есть нетривиальный морфизм $D(k) \to \mathbf{Z}$; в гл. VII-5 будет доказано, что этот морфизм сюръективен. Ядро этого морфизма, т. е. группа дивизоров степени 0, будет обозначаться через $D_0(k)$. Очевидно, что если $\mathfrak{a} \succ 0$, то $\deg(\mathfrak{a}) \geqslant 0$, причем $\deg(\mathfrak{a}) > 0$ при $\mathfrak{a} \neq 0$, и что если $\mathfrak{a} \succ \mathfrak{b}$, то $\deg \mathfrak{a} \geqslant \deg \mathfrak{b}$.

Пусть $a = (a_v)$ — произвольный элемент из $k_{\mathbf{A}}^{\times}$. Для каждой точки v можно написать $a_v r_v = p_v^{a(v)}$, где $a(v) = \operatorname{ord}_v(a_v)$. Почти для всех v имеем $|a_v|_v = 1$, следовательно, $a(v) = 0$, так что $\sum a(v) \cdot v$ — дивизор поля k. Этот дивизор будем обозначать через $\operatorname{div}(a)$. Ясно, что отображение $\operatorname{div}: k_{\mathbf{A}}^{\times} \to D(k)$ есть сюръективный морфизм, ядром которого является $\prod_v r_v^{\times}$ — та самая группа, которую мы обозначали в гл. IV-4 через $\Omega(\varnothing)$. Поэтому этот морфизм можно использовать для отождествления $D(k)$ с $k_{\mathbf{A}}^{\times}/\Omega(\varnothing)$. Из определения $|a|_{\mathbf{A}}$ сразу видно, что если $a \in k_{\mathbf{A}}^{\times}$ и $\mathfrak{a} = \operatorname{div}(a)$, то $|a|_{\mathbf{A}} = q^{-\deg(\mathfrak{a})}$. Следовательно, $D_0(k)$ совпадает с образом в $D(k)$ группы $k_{\mathbf{A}}^1$ при морфизме $a \to \operatorname{div}(a)$; в частности, образ $P(k)$ группы $k^{\times}$ в $D(k)$ при этом морфизме содержится в $D_0(k)$. Группу $P(k)$ принято называть группой *главных дивизоров*. Морфизм $a \to \operatorname{div}(a)$ определяет, очевидно, изоморфизмы групп $k_{\mathbf{A}}^1/\Omega(\varnothing)$, $k_{\mathbf{A}}^1/k^{\times}\Omega(\varnothing)$ и $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(\varnothing)$ на $D_0(k)$, $D_0(k)/P(k)$ и $D(k)/P(k)$ соответственно. Группу $D(k)/P(k)$ принято называть группой *классов дивизоров* поля k, а $D_0(k)/P(k)$ — группой классов дивизоров степени 0. Теорема 7 гл. IV-4 показывает, что последняя группа конечна, а предыдущая является прямым произведением этой последней и группы, изоморфной группе $\mathbf{Z}$.

Рассмотрим теперь векторные пространства над k. Имеет место следующий результат, частный случай которого уже встречался в гл. IV.

Предложение 1. *Пусть E — векторное пространство конечной размерности над k и ε — некоторый базис в E над k. Для каждой точки v поля k пусть ε_v — r_v-модуль, порожденный множеством ε в E_v, и L_v — некоторая k_v-решетка в E_v. Подгруппа $\prod L_v$ открыта и компактна в $E_{\mathbf{A}}$ в том и только в том случае, когда $L_v = \varepsilon_v$ почти для всех v.*

Если P — такое конечное множество точек, что $L_v \subset \varepsilon_v$ для всех точек v, не лежащих в P, то $\prod L_v$ — компактная подгруппа

в $E_{\mathbf{A}}(P, \varepsilon)$, а следовательно, и в $E_{\mathbf{A}}$; обратное утверждение немедленно вытекает из следствия 1 предл. гл. IV-1. Предположим теперь, что $\prod L_v$ — компактная подгруппа в $E_{\mathbf{A}}$, т. е. $L_v \subset \varepsilon_v$ почти для всех v. Эта подгруппа открыта тогда и только тогда, когда она содержит некоторую окрестность нуля. Предложение 1 гл. IV-1 показывает, что это имеет место в том и только в том случае, когда $L_v \supset \varepsilon_v$ почти для всех v. Доказательство закончено.

В обозначениях предложения 1 систему $L = (L_v)$ будем называть *когерентной системой* k_v-решеток или, короче, когерентной системой, соответствующей векторному пространству E, если $L_v = \varepsilon_v$ почти для всех точек v. В этом случае будем писать $U(L) = \prod L_v$ и $\Lambda(L) = E \cap U(L)$. Согласно предложению 1, подгруппа $U(L)$ открыта и компактна. Кроме того, она является модулем над открытым и компактным подкольцом $\prod r_v$ в $k_{\mathbf{A}}$. Что касается группы $\Lambda(L)$, то это — конечная подгруппа в E, поскольку подгруппа E дискретна, а подгруппа $U(L)$ компактна в $E_{\mathbf{A}}$. Далее, $\Lambda(L)$ является модулем над кольцом $k \cap (\prod r_v)$. Поскольку это кольцо по теореме 8 гл. IV-4 и ее следствию совпадает с полем констант $\mathbf{F}_q$ поля k, отсюда вытекает, что $\Lambda(L)$ является векторным пространством над $\mathbf{F}_q$. Размерность этого пространства обозначим через $\lambda(L)$. Тогда $\Lambda(L)$ состоит из $q^{\lambda(L)}$ элементов.

Предложение 2. *Положим* $\mathcal{A} = \mathrm{End}(E)$, *и пусть* $L = (L_v)$, $M = (M_v)$ — *две когерентные системы, соответствующие пространству* E. *Тогда существует такой элемент* $a = (a_v) \in \mathcal{A}_{\mathbf{A}}^{\times}$, *что* $M_v = a_v L_v$ *для всех точек* v. *Кроме того, дивизор* $\mathrm{div}(\det(a))$ *однозначно определяется по* L *и* M.

По теореме 1 гл. II-2 для каждой точки v существуют такие базисы α_v, β_v в E_v над k_v, что L_v, M_v являются r_v-модулями, порожденными соответственно множествами α_v и β_v. Обозначим через a_v автоморфизм пространства E_v, который отображает базис α_v на β_v. Тогда $M_v = a_v L_v$. Положим $d_v = \det(a_v)$. Если μ_v — произвольная мера Хаара на E_v, то по следствию 3 теор. 3 гл. I-2 $|d_v|_v = \mu_v(M_v)/\mu_v(L_v)$, так что $|d_v|_v$ не зависит от выбора базисов α_v и β_v. Далее, по условию $L_v = M_v$, откуда $|d_v|_v = 1$, почти для всех v. В силу предложения 3 гл. IV-3 отсюда следует, что $a = (a_v) \in \mathcal{A}_{\mathbf{A}}^{\times}$ и $d = (d_v) = \det(a) \in k_{\mathbf{A}}^{\times}$. Поскольку $|d_v|_v$ зависит только от L_v и M_v, то и $\mathrm{div}(d)$ зависит только от L и M.

Будем писать $M = aL$ в ситуации, описанной в предложении.

Следствие 1. *Пусть* ε — *базис пространства* E *над* k. *Положим* $L_0 = (\varepsilon_v)$, *и пусть* L — *произвольная когерентная систе-*

ма, соответствующая пространству E. Тогда существует такой элемент $a \in \mathcal{A}_A^\times$, что $L = aL_0$. Дивизор $\mathfrak{d} = \operatorname{div}(\det(a))$ зависит только от L и ε, а его класс и степень зависят только от L.

Лишь последнее утверждение нуждается в доказательстве. Заменим ε каким-нибудь другим базисом ε', положим $L_0' = (\varepsilon_v')$ и обозначим через α автоморфизм пространства E над k, который отображает ε' на ε. Тогда $L_0 = \alpha L_0'$ и, следовательно, $L = a\alpha L_0'$, так что $\mathfrak{d}$ надо заменить на $\mathfrak{d} + \operatorname{div}(\det(a))$. Но второе слагаемое в последней сумме является главным дивизором, и, значит, его степень равна 0.

Следствие 2. *Существует такая мера Хаара μ на E_A, что $\mu(\prod \varepsilon_v) = 1$ для каждого базиса ε в E над k. Если L и $\mathfrak{d}$ таковы, как в следствии* 1, *то для этой меры $\mu(U(L)) = q^{-\delta(L)}$, где $U(L) = \prod L_v$ и $\delta(L) = \deg(\mathfrak{d})$.*

Возьмем какой-нибудь базис ε и выберем μ так, чтобы $\mu(\prod \varepsilon_v) = 1$. Если a таково, как в следствии 1, то $U(L)$ совпадает с образом группы $U(L_0) = \prod \varepsilon_v$ при отображении $e \to ae$. Поэтому мера $\mu(U(L))$ равна модулю этого автоморфизма, который совпадает с $|\det(a)|_A$ по предложению 3 гл. IV-3. В силу наших определений это число равно $q^{-\delta(L)}$, что и утверждается в нашем следствии. Согласно следствию 1, это число не зависит от ε, поэтому при замене ε на какой-нибудь другой базис ε' мы получим такую меру μ', что $\mu'(U(L))$ совпадает с $\mu(U(L))$, откуда $\mu' = \mu$, так что $\mu(\prod \varepsilon_v') = 1$.

Как и в гл. IV-2, выберем теперь какой-нибудь нетривиальный характер χ на k_A, тривиальный на k, и обозначим через χ_v характер, индуцированный характером χ на k_v. Для каждой точки v характер χ_v нетривиален по следствию 1 теор. 3 гл. IV-2. Пусть E такое, как выше, и E' — алгебраическое двойственное к нему. Как объяснялось в гл. IV-2, отождествим с помощью χ пространство E_A' с топологическим двойственным к E_A посредством изоморфизма, описанного в теореме 3 гл. IV-2, а также для каждой точки v отождествим с помощью χ_v пространство E_v' с топологическим двойственным к E_v посредством изоморфизма, описанного в теореме 3 гл. IV-2. Пусть $L = (L_v)$ — когерентная система, соответствующая пространству E. Для каждой точки v обозначим через L_v' решетку, двойственную с L_v. С учетом только что сделанных отождествлений L_v' является k_v-решеткой в E_v' и $\prod L_v'$ является подгруппой в E_A, ассоциированной по двойственности с подгруппой $U(L) = \prod L_v$

в $E_{\mathbf{A}}$. Так как подгруппа $U(L)$ компактна, то подгруппа $\prod L'_v$ открыта, а так как $U(L)$ открыта, то $\prod L'_v$ компактна. В силу предложения 1 отсюда вытекает, что $L' = (L'_v)$ есть когерентная система, соответствующая пространству E' (этот факт вытекает также из следствия 3 теор. 3 гл. IV-2). Система L' называется *двойственной* к L.

Теорема 1. *Для каждого* **A**-*поля* k *характеристики* $p > 1$ *существует целое число* $g \geqslant 0$ *со следующим свойством. Если* E — *векторное пространство конечной размерности* n *над* k, L — *произвольная когерентная система, соответствующая пространству* E, *и* L' — *система, двойственная к* L, *то*

$$\lambda(L) = \lambda(L') - \delta(L) - n(g-1).$$

Положим $U = U(L)$, $U' = U(L')$. Как мы только что видели, U' есть подгруппа в $E'_{\mathbf{A}}$, ассоциированная по двойственности с подгруппой U в $E_{\mathbf{A}}$. По определению $\lambda(L)$ и $\lambda(L')$ равны соответственно размерностям векторных пространств $\Lambda = E \cap U$ и $\Lambda' = E' \cap U'$ над полем констант $\mathbf{F}_q$ поля k. По теореме 3 гл. IV-2 подгруппой в $E'_{\mathbf{A}}$, ассоциированной по двойственности с подгруппой $E \subset E_{\mathbf{A}}$, является E'. Поэтому подгруппой в $E'_{\mathbf{A}}$, ассоциированной по двойственности с $E + U$, является Λ', так что группа $E_{\mathbf{A}}/(E+U)$ двойственна к Λ' и имеет то же самое число элементов $q^{\lambda(L')}$, что и Λ'. Ясно, что группа $E_{\mathbf{A}}/(E+U)$ изоморфна $(E_{\mathbf{A}}/E)/(E+U/E)$. Возьмем меру Хаара μ на $E_{\mathbf{A}}$, определенную следствием 2 предл. 2, и обозначим снова через μ ее образ в $E_{\mathbf{A}}/E$ (см. гл. II-4). Так как индекс подгруппы $(E+U)/E$ в $E_{\mathbf{A}}/E$ равен $q^{\lambda(L')}$, то

$$\mu(E_{\mathbf{A}}/E) = q^{\lambda(L')}\,\mu(E + U/E).$$

Канонический морфизм $E_{\mathbf{A}} \to E_{\mathbf{A}}/E$ отображает U на $(E+U)/E$ и имеет конечное ядро $\Lambda = E \cap U$. Поскольку Λ состоит из $q^{\lambda(L)}$ элементов, отсюда вытекает, например по лемме 2 гл. II-4, что

$$\mu(U) = q^{\lambda(L)}\,\mu(E + U/E).$$

Комбинируя эти формулы со следствием 2 предл. 2, согласно которому $\mu(U) = q^{-\delta(L)}$, получаем, что

$$\mu(E_{\mathbf{A}}/E) = q^{\lambda(L')-\lambda(L)-\delta(L)}.$$

Отсюда видно, что число $\mu(E_{\mathbf{A}}/E)$ имеет вид q^r, где $r \in \mathbf{Z}$. В частности, применяя следствие 2 предл. 2 к $E = k$ и к базису $\varepsilon = \{1\}$, получаем такую меру Хаара μ_1 на $k_{\mathbf{A}}$, что $\mu_1(\prod r_v) = 1$, и мы видим, что $\mu_1(k_{\mathbf{A}}/k) = q^{\gamma}$, где $\gamma \in \mathbf{Z}$. Отождествим теперь наше

пространство E с k^n, выбрав некоторый базис $\mathfrak{e}$ в E над k. Ясно, что мера μ на $E_{\mathbf{A}}$, определенная следствием 2 предл. 2, является произведением $(\mu_1)^n$ мер μ_1 на n сомножителях произведения $E_{\mathbf{A}} = (k_{\mathbf{A}})^n$, откуда $q^r = (q^\gamma)^n$, т. е. $r = \gamma n$. Это дает нам искомую формулу с $g = \gamma + 1$. Остается только показать, что $g \geqslant 0$. Для этого применим нашу формулу к случаю $E = k$, $L_v = r_v$ при всех v. Тогда $\Lambda = \mathbf{F}_q$, $\lambda(L) = 1$ и, очевидно, $\delta(L) = 0$, откуда $g = \lambda(L')$. Но последняя величина неотрицательна по определению.

Следствие 1. *Пусть* μ *— мера Хаара на* $E_{\mathbf{A}}$, *определенная следствием* 2 *предл.* 2. *Тогда* $\mu(E_{\mathbf{A}}/E) = q^{n(q-1)}$. *В частности, если* μ_1 *— мера Хаара на* $k_{\mathbf{A}}$, *для которой* $\mu_1(\prod r_v) = 1$, *то* $\mu_1(k_{\mathbf{A}}/k) = q^{g-1}$.

Это было доказано выше.

Следствие 2. *В обозначениях теоремы* 2 $E_{\mathbf{A}} = E + U$ *тогда и только тогда, когда* $\lambda(L') = 0$.

Это частный случай того, что было доказано выше.

Определение 1. *Целое число* g, *определенное в теореме* 1, *называется родом поля* k.

Приведем теперь полученные выше результаты к более явному виду для случая $E = k$. В этом случае когерентная система $L = (L_v)$ задается набором $L_v = p_v^{-a(v)}$, где $a(v) = 0$ почти для всех v. Следовательно, такие системы находятся во взаимно однозначном соответствии с дивизорами поля k. Поэтому для дивизора $\mathfrak{a} = \sum a(v) \cdot v$ когерентную систему $(p_v^{-a(v)})$ будем обозначать через $L(\mathfrak{a})$, так что $L(0)$ — это когерентная система (r_v), и мы видим, что $L(\mathfrak{a})$ — это когерентная система $a^{-1}L(0)$, где $a \in k_{\mathbf{A}}^\times$ и $\mathfrak{a} = \operatorname{div}(a)$. Для $L = L(\mathfrak{a})$ будем писать $U(\mathfrak{a})$, $\Lambda(\mathfrak{a})$, $\lambda(\mathfrak{a})$, $\delta(\mathfrak{a})$ вместо $U(L)$, $\Lambda(L)$, $\lambda(L)$, $\delta(L)$. Очевидно, $\delta(\mathfrak{a}) = -\deg(\mathfrak{a})$. По определению группа $\Lambda(\mathfrak{a})$ может быть записана как $\bigcap_v (k \cap p_v^{-a(v)})$; другими словами, она состоит из нуля и тех элементов $\xi \in k^\times$, для которых $\operatorname{ord}_v(\xi) \geqslant -a(v)$ при всех v, или, что то же самое, для которых $\operatorname{div}(\xi) \succ -\mathfrak{a}$. Так как степень дивизора $\operatorname{div}(\xi)$ равна нулю для всех $\xi \in k^\times$, отсюда видно, что $\Lambda(\mathfrak{a}) = \{0\}$ и, следовательно, $\lambda(\mathfrak{a}) = 0$, если $\deg(\mathfrak{a}) < 0$.

Выберем теперь, как выше, базисный характер χ на $k_{\mathbf{A}}$. Для каждой точки v поля k обозначим через $\nu(v)$ порядок характера χ_v (см. определение 4 гл. II-5), индуцированного на k_v характером χ. По следствию 1 теор. 3 гл. IV-2 $\nu(v) = 0$ почти для всех v, так

что $\mathfrak{c} = \sum \nu(v) \cdot v$ — дивизор поля k. Назовем его *дивизором характера* χ и обозначим через $\operatorname{div}(\chi)$. Если χ_1 — другой такой характер, то по теореме 3 гл. IV-2 он может быть записан как $x \to \chi(\xi x)$ с $\xi \in k^\times$, и сразу видно, что $\operatorname{div}(\chi_1) = \operatorname{div}(\chi) + \operatorname{div}(\xi)$. Таким образом, когда χ пробегает все нетривиальные характеры на $k_{\mathbf{A}}$, тривиальные на k, дивизоры $\operatorname{div}(\chi)$ образуют смежный класс дивизоров по модулю группы $P(k)$ главных дивизоров поля k. Этот класс принято называть *каноническим классом*, а его элементы — *каноническими дивизорами*.

Как и раньше, отождествим при помощи χ группу $k_{\mathbf{A}}$ с топологической двойственной к ней и положим $\mathfrak{c} = \operatorname{div}(\chi)$. Используя предложение 12 гл. II-5, сразу видим, что система, двойственная к $L(\mathfrak{a})$, совпадает с $L(\mathfrak{c} - \mathfrak{a})$. Теорема 1 дает теперь следующий результат.

Теорема 2. *Пусть* $\mathfrak{c}$ *— канонический дивизор поля* k. *Тогда*

$$\lambda(\mathfrak{a}) = \lambda(\mathfrak{c} - \mathfrak{a}) + \deg(\mathfrak{a}) - g + 1$$

для каждого дивизора $\mathfrak{a}$ *поля* k.

Следствие 1. *Если* $\mathfrak{c}$ *— канонический дивизор, то* $\deg(\mathfrak{c}) = 2g - 2$ *и* $\lambda(\mathfrak{c}) = g$.

Первое равенство получается, если заменить в теореме 2 $\mathfrak{a}$ на $\mathfrak{c} - \mathfrak{a}$, а второе, если взять $\mathfrak{a} = 0$.

Следствие 2. *Если* $\mathfrak{a}$ *— дивизор степени* $> 2g - 2$, *то* $\lambda(\mathfrak{a}) = \deg(\mathfrak{a}) - g + 1$.

Действительно, в этом случае $\deg(\mathfrak{c} - \mathfrak{a}) < 0$, откуда, как мы отмечали выше, вытекает равенство $\lambda(\mathfrak{c} - \mathfrak{a}) = 0$, а значит, по теореме 2, и доказываемое равенство.

Следствие 3. *Пусть* $\mathfrak{a} = \sum a(v) \cdot v$ *— дивизор степени* $> 2g - 2$. *Тогда* $k_{\mathbf{A}} = k + \left(\prod_v p_v^{-a(v)}\right)$.

Это утверждение является частным случаем следствия 2 теор. 1 при $E = k$, $L = L(\mathfrak{a})$, ибо в этом случае, как показано выше, $L' = L(\mathfrak{c} - \mathfrak{a})$ и $\lambda(L') = 0$.

Теорема 2 — это *теорема Римана — Роха* для «функционального поля» k с *конечным* полем констант. Доказательство в общем случае может быть получено совершенно аналогичным путем; понятие плотности следует заменить понятием «линейной плотности» для векторных пространств над произвольным полем K, наде-

ляемым дискретной топологией; вместо меры Хаара следует использовать «относительную размерность» компактных и открытых подпространств локально компактных векторных пространств над K. Мы не будем здесь рассматривать это обобщение.

Отметим еще один момент, имеющий некоторое значение. Вместо того чтобы с помощью базисного характера отождествлять пространство G, топологическое двойственное к $k_{\mathbf{A}}$, с самим пространством $k_{\mathbf{A}}$, рассмотрим G как $k_{\mathbf{A}}$-модуль, полагая $\langle x, ax^* \rangle = \langle ax, x^* \rangle$, где $x \in k_{\mathbf{A}}$, $x^* \in G$, $a \in k_{\mathbf{A}}$. Обозначим через Γ подгруппу в G, ассоциированную по двойственности с k. Тогда теорема 3 гл. IV-2 может быть выражена следующим образом: для любого отличного от нуля элемента γ в Γ отображение $x \to x\gamma$ является изоморфизмом из $k_{\mathbf{A}}$ на G, отображающим k на Γ. В частности, подгруппа Γ обладает «внутренне» присущей ей структурой векторного пространства размерности 1 над k. Теперь можно «канонически» определить дифференцирование из k в Γ, т. е. отображение $x \to dx$ из k в Γ, для которого $d(xy) = x \cdot dy + y \cdot dx$ при всех x, $y \in k$, и пространство Γ можно отождествить с k-модулем всех формальных сумм $\sum y_i\, dx_i$, где x_i, $y_i \in k$. Это остается справедливым для каждого сепарабельного алгебраического расширения конечной степени над любым полем $K(T)$, где T — неизвестная над основным полем K. Даже для изучаемого здесь случая конечного поля констант эту тему трудно разрабатывать должным образом, не расширяя основного поля до его алгебраического замыкания, и мы нигде в дальнейшем не будем возвращаться к этой теме.

ГЛАВА СЕДЬМАЯ

ДЗЕТА-ФУНКЦИЯ А-ПОЛЕЙ

§1. СХОДИМОСТЬ ЭЙЛЕРОВА ПРОИЗВЕДЕНИЯ

Начиная с этого места k будет обозначать произвольное **A**-поле характеристики нуль или $p > 1$. Обозначения будут прежними: если v — точка поля k, то k_v — это соответствующее пополнение поля k; если v — конечная точка, то r_v — это максимальное компактное подкольцо в k_v, а p_v — максимальный идеал в r_v. Кроме того, в последнем случае условимся раз и навсегда обозначать через q_v модуль поля k_v и через π_v — простой элемент в k_v, так что по теореме 6 гл. I-4 r_v/p_v — это поле из q_v элементов и $|\pi_v|_v = q_v^{-1}$. Если k — поле характеристики $p > 1$, то будем обозначать через q число элементов в его поле констант и отождествлять это поле с $\mathbf{F}_q$. Тогда в соответствии с определениями гл. VI $q_v = q^{\deg(v)}$ для каждой точки v.

Под *эйлеровым произведением*, соответствующим полю k, будем понимать любое произведение вида

$$\prod_v (1 - \theta_v q_v^{-s})^{-1},$$

где $s \in \mathbf{C}$, $\theta_v \in \mathbf{C}$ и $|\theta_v| \leqslant 1$ при всех v; произведение берется по всем или почти всем конечным точкам поля k. Это же название употребляют для произведений более общего типа, но последние нам здесь не встретятся. Основной результат о сходимости эйлеровых произведений формулируется так:

Предложение 1. *Пусть k — произвольное* **A**-*поле. Тогда произведение*

$$\zeta_k(\sigma) = \prod_v (1 - q_v^{-\sigma})^{-1},$$

где $\sigma \in \mathbf{R}$, а v пробегает все конечные точки поля k, сходится при $\sigma > 1$ и стремится к 1 при $\sigma \to +\infty$.

Предположим сперва, что характеристика поля k равна нулю, и обозначим через n степень поля k над $\mathbf{Q}$. По следствию 1 теор. 4

гл. III-4 имеется не более n точек поля k, лежащих над фиксированной точкой p поля $\mathbf{Q}$. Для каждой такой точки v поле k_v является p-полем, так что q_v имеет вид p^{ν}, где $\nu \geqslant 1$, и поэтому $q_v \geqslant p$. При $\sigma > 0$ это дает

$$1 < \zeta_k(\sigma) \leqslant \prod (1 - p^{-\sigma})^{-n},$$

где произведение берется по всем простым числам p. Теперь запишем

$$\zeta(\sigma) = \prod (1 - p^{-\sigma})^{-1} = \prod (1 + p^{-\sigma} + p^{-2\sigma} + \ldots).$$

Раскрывая скобки в последнем произведении, получаем

$$\zeta(\sigma) = \sum_{\nu=1}^{+\infty} \nu^{-\sigma},$$

ибо каждое целое число $\nu \geqslant 1$ может быть однозначно представлено в виде произведения степеней простых чисел. Далее, при $\sigma > 1$ имеем

$$1 < \zeta(\sigma) < 1 + \sum_{\nu=2}^{+\infty} \int_{\nu-1}^{\nu} t^{-\sigma}\, dt = 1 + \int_{1}^{+\infty} t^{-\sigma}\, dt = 1 + (\sigma - 1)^{-1},$$

откуда видно, что $\zeta(\sigma)$ сходится при $\sigma > 1$ и стремится к 1 при $\sigma \to +\infty$. Таким образом, наше предложение доказано в случае числового поля k.

Теперь предположим, что k — поле характеристики $p > 1$. Тогда, согласно лемме 1 гл. III-2, k можно представить как сепарабельное алгебраическое расширение конечной степени n поля $\mathbf{F}_p(T)$. По теореме 2 гл. III-1 поле $\mathbf{F}_p(T)$ имеет точку ∞, соответствующую простому элементу T^{-1}, а все остальные точки находятся во взаимно однозначном соответствии с неприводимыми многочленами π из $\mathbf{F}_p[T]$. Очевидно, достаточно доказать утверждение нашего предложения не для самого произведения $\zeta_k(\sigma)$, а для аналогичного произведения $\eta(\sigma)$, взятого по всем точкам v поля k, не лежащим над точкой ∞ поля $\mathbf{F}_p(T)$. Точно так же, как в случае характеристики нуль, мы видим, что $1 < \eta(\sigma) \leqslant \zeta_p(\sigma)^n$, где через $\zeta_p(\sigma)$ обозначено произведение

$$\zeta_p(\sigma) = \prod (1 - p^{-\deg(\pi)\sigma})^{-1} = \prod (1 + p^{-\deg(\pi)\sigma} + p^{-2\deg(\pi)\sigma} + \ldots),$$

взятое по всем унитарным неприводимым многочленам π из $\mathbf{F}_p[T]$. Так как каждый унитарный многочлен из $\mathbf{F}_p[T]$ может быть однозначно представлен в виде произведения степеней унитарных неприводимых многочленов, то

$$\zeta_p(\sigma) = \sum p^{-\deg(\mu)\sigma},$$

где сумма берется по всем унитарным многочленам μ из $\mathbf{F}_p[T]$. Поскольку для каждого $\delta \geqslant 0$ имеется ровно p^δ унитарных многочленов степени δ, мы получаем, что

$$\zeta_p(\sigma) = \sum_{\sigma=0}^{+\infty} p^{\delta(1-\sigma)} = (1-p^{1-\sigma})^{-1},$$

чем завершено доказательство в случае ненулевой характеристики.

Следствие 1. *Пусть P — конечное множество точек поля k, содержащее P_∞, и для каждой точки v, не лежащей в P, выбрано число $\theta_v \in \mathbf{C}$, такое, что $|\theta_v| \leqslant 1$. Для всякого $s \in \mathbf{C}$ положим*

$$E(s) = \prod_{v \notin P} (1 - \theta_v q_v^{-s})^{-1}.$$

Тогда при $\mathrm{Re}(s) > 1$ произведение $E(s)$ абсолютно сходится, голоморфно по s и не равно нулю и $E(s) \to 1$ равномерно относительно $\mathrm{Im}(s)$ при $\mathrm{Re}(s) \to +\infty$.

В самом деле, для $\sigma = \mathrm{Re}(s)$ ряд $\log E(s)$ мажорируется рядом $\log \zeta_k(\sigma)$. Утверждение следствия немедленно вытекает поэтому из предложения 1 и хорошо известных элементарных теорем о равномерно сходящихся рядах голоморфных функций.

Следствие 2. *Пусть k_0 — некоторое А-поле, содержащееся в k, и пусть M — такое множество конечных точек поля k, что почти для всех $v \in M$ модулярная степень $f(v)$ поля k_v над замыканием поля k_0 в k_v больше 1. Тогда произведение*

$$p(M, \sigma) = \prod_{v \in M} (1 - q_v^{-\sigma})^{-1}$$

абсолютно сходится при $\sigma > 1/2$.

Если характеристика поля k равна нулю, то поля k и k_0 имеют конечную степень над $\mathbf{Q}$; если же k — поле характеристики $p > 1$ и T — любой элемент из k_0, не алгебраичный над простым полем $\mathbf{F}_p$, то k и k_0 имеют конечную степень над $\mathbf{F}_p(T)$. В обоих случаях k имеет конечную степень n над k_0. Пусть v — конечная точка поля k и u — точка поля k_0, лежащая под v. Тогда замыкание поля k_0 в k_v равно $(k_0)_u$ и k порождает поле k_v над $(k_0)_u$. Поэтому степень поля k_v над $(k_0)_u$ не превосходит n, так что $1 \leqslant f(v) \leqslant n$. Таким образом, M является объединением множеств $M_1, \ldots, M_n$, состоящих соответственно из тех точек $v \in M$, для которых $f(v) = f$, где $1 \leqslant f \leqslant n$. Наше предположение относительно M означает, что множество M_1 конечно, так что достаточно доказать наше утверждение для каждого из множеств M_f, $f \geqslant 2$. По следствию 1 теор. 4

гл. III-4 над всякой конечной точкой u поля k_0 имеется не более n/f точек $v \in M_f$. Поэтому произведение $p(M_f, \sigma)$ мажорируется произведением $\zeta_{k_0}(f\sigma)^{n/f}$, которое при $\sigma > 1/f$ абсолютно сходится по предложению 1.

Следствие 3. *Пусть M таково, как в следствии 2, и пусть для каждой точки $v \in M$ выбрано число $\theta_v \in \mathbf{C}$, для которого $|\theta_v| \leqslant 1$. Тогда при $\mathrm{Re}(s) > 1/2$ произведение*

$$\prod_{v \in M} (1 - \theta_v q_v^{-s})^{-1}$$

абсолютно сходится, голоморфно по s и отлично от нуля.

Доказательство аналогично доказательству следствия 1, надо только учесть следствие 2.

§ 2. ПРЕОБРАЗОВАНИЯ ФУРЬЕ И СТАНДАРТНЫЕ ФУНКЦИИ

Теория дзета-функций существенно связана с преобразованиями Фурье на группах k_v, $k_{\mathbf{A}}$, соответствующих $\mathbf{A}$-полю k. Начнем с того, что напомним результаты, которые нам понадобятся.

Пусть G, G^* и $\langle g, g^* \rangle$ таковы, как в гл. II-5, и пусть Φ — непрерывная функция на G, интегрируемая по мере Хаара α, заданной на G. Тогда функция Φ^* на G^*, определенная формулой

$$\Phi^*(g^*) = \int_G \Phi(g) \langle g, g^* \rangle \, d\alpha(g),$$

называется *преобразованием Фурье функции* Φ относительно меры α. Легко проверяется, что эта функция непрерывна на G^*. Если заменить α на $c\alpha$, $c \in \mathbf{R}_+^\times$, то, очевидно, Φ^* заменится на $c\Phi^*$.

Лемма 1. *Пусть $g \to \lambda g$ — автоморфизм группы G, $\mathrm{mod}_G(\lambda)$ — модуль автоморфизма λ и $g^* \to g^*\lambda^*$ — автоморфизм группы G^*, для которого $\langle \lambda g, g^* \rangle = \langle g, g^*\lambda^* \rangle$ при всех $g \in G$, $g^* \in G^*$. Тогда если Φ^* — преобразование Фурье функции Φ, то преобразованием Фурье функции $g \to \Phi(\lambda^{-1}g)$ является функция $g^* \to \mathrm{mod}_G(\lambda)\, \Phi^*(g^*\lambda^*)$.*

Это немедленно получается, если заменить g на λg в интеграле, определяющем преобразование Фурье от $\Phi(\lambda^{-1}g)$.

Согласно теории преобразований Фурье, существует такая мера Хаара α^* на G^*, что для любой интегрируемой функции Φ^* на G^*, определяемой написанным выше интегралом, Φ задается следую-

щей «формулой обращения Фурье»:

$$\Phi(g) = \int_{G^*} \Phi^*(g^*) \langle -g, g^* \rangle \, d\alpha^*(g^*).$$

Мы говорим тогда, что Φ есть *обратное преобразование Фурье* функции Φ^*. Мера α^* называется *двойственной к мере* α. Ясно, что двойственной мерой к $c\alpha$, $c \in \mathbf{R}_+^\times$, является мера $c^{-1}\alpha^*$. В частности, если предположить, что группа G^* отождествлена с G при помощи некоторого изоморфизма $G \to G^*$, то $\alpha^* = m\alpha$, где $m \in \mathbf{R}_+^\times$, и поскольку двойственной к $c\alpha$ будет мера $c^{-1}m\alpha$, существует одна и только одна мера Хаара на G, а именно $m^{1/2}\alpha$, которая совпадает со своей двойственной при заданном отождествлении G и G^*. Эта мера называется *самодвойственной мерой Хаара* на G. Если группа G компактна, то группа G^* дискретна. В этом случае, взяв $\Phi = 1$, мы сразу видим, что если α — мера Хаара на G, для которой $\alpha(G) = 1$, то $\alpha^*(\{0\}) = 1$ для двойственной меры α^* на G^*.

Функцию Φ на G будем называть *допустимой* для G, если она непрерывна и интегрируема и ее преобразование Фурье Φ^* является интегрируемой функцией на G^*. Пусть теперь Γ — такая дискретная подгруппа в G, что факторгруппа G/Γ компактна, и пусть Γ_* — подгруппа в G^*, ассоциированная по двойственности с Γ. Так как G/Γ компактна, то Γ_* дискретна; так как Γ дискретна, то G^*/Γ_* компактна. Возьмем меру Хаара α на G, для которой $\alpha(G/\Gamma) = 1$. Функцию Φ на G будем называть *допустимой для* (G, Γ), если она допустима для G и оба ряда

$$\sum_{\gamma \in \Gamma} \Phi(g + \gamma), \quad \sum_{\gamma^* \in \Gamma_*} \Phi^*(g^* + \gamma^*)$$

абсолютно сходятся, равномерно на каждом компактном подмножестве относительно g и g^*. Первый из этих рядов определяет тогда непрерывную функцию F на G, постоянную на каждом классе смежности по модулю Γ. Эту функцию можно очевидным образом рассматривать как функцию на G/Γ. Так как группа Γ_* двойственна к G/Γ, то функция F имеет преобразованием Фурье

$$\gamma^* \to \int_{G/\Gamma} \Big(\sum_{\gamma \in \Gamma} \Phi(g + \gamma) \Big) \langle g, \gamma^* \rangle \, d\alpha(\dot{g}),$$

где, как обычно, $\dot{g}$ — образ элемента g в G/Γ при каноническом гомоморфизме $G \to G/\Gamma$; подинтегральная функция, хоть она и записана как функция от g, но, будучи постоянна на каждом классе смежности по модулю Γ, рассматривается как функция от $\dot{g}$. Согласс-

но формуле 6 гл. II-4, этот интеграл равен $\Phi^*(\gamma^*)$, так что преобразование Фурье функции F, рассматриваемой как функция на G/Γ, совпадает с функцией, которую Φ^* индуцирует на Γ_*. Так как функция Φ по предположению допустима для (G, Γ), то Φ^* интегрируема на Γ_*, так что по формуле обращения Фурье для G/Γ и Γ_* находим

$$F(g) = \sum_{\gamma \in \Gamma} \Phi(g+\gamma) = \sum_{\gamma^* \in \Gamma_*} \Phi^*(\gamma^*) \cdot \langle -g, \gamma^* \rangle.$$

При $g = 0$ получаем

$$\sum_{\gamma \in \Gamma} \Phi(\gamma) = \sum_{\gamma^* \in \Gamma_*} \Phi^*(\gamma^*). \tag{1}$$

Эту формулу принято называть *формулой суммирования Пуассона*. Ее справедливость доказана нами для любой допустимой для (G, Γ) функции Φ и для такой меры α, что $\alpha(G/\Gamma) = 1$.

Предположим, что существуют допустимые для (G, Γ) функции Φ, для которых обе части равенства (1) отличны от нуля. Это предположение (которое легко следует из общей теории преобразований Фурье) мы проверим с помощью явного построения в том единственном интересующем нас случае, когда $G = E_{\mathfrak{A}}$, $\Gamma = E$, где E — векторное пространство конечной размерности над $\mathfrak{A}$-полем. Обозначим через α^* меру, двойственную к α, положим $\alpha^*(G^*/\Gamma_*) = c$ и поменяем в проведенных выше вычислениях G и G^* ролями, отправляясь от функции Φ^* и беря ее обратное преобразование Фурье относительно меры Хаара $c^{-1}\alpha^*$ на G^*. Так как это преобразование совпадает с $c^{-1}\Phi$, то мы получим как конечный результат формулу (1), в которой вместо Φ будет стоять $c^{-1}\Phi$, откуда $c = 1$. Таким образом, доказано, что меры Хаара α, α^* на G, G^*, задаваемые условиями $\alpha(G/\Gamma) = 1$, $\alpha^*(G^*/\Gamma_*) = 1$, двойственны друг другу. В частности, пусть существует изоморфизм из G на G^*, который отображает Γ на Γ_*; если использовать его для отождествления G с G^*, то самодвойственная мера на G — это та мера Хаара, для которой $\alpha(G/\Gamma) = 1$.

Теперь мы построим некоторые специальные типы допустимых функций для интересующих нас групп. Эти функции будут называться «стандартными» функциями. Функция, заданная на топологическом пространстве, называется *локально постоянной*, если для любой точки существует такая ее окрестность, на которой функция постоянна. Если f — локально постоянная функция, то множество $f^{-1}(\{a\})$ открыто для каждого значения a и в то же время замкнуто, так как его дополнение является объединением открытых множеств $f^{-1}(\{b\})$, $b \neq a$. На связном пространстве,

например на любом векторном пространстве над $\mathbf{R}$, локально постоянными функциями являются только константы.

Определение 1. *Пусть E — векторное пространство конечной размерности над р-полем K. Под стандартной функцией на E мы понимаем комплекснозначную локально постоянную функцию на E с компактным носителем.*

Нам будет достаточно рассмотреть случай коммутативного поля K. Пусть E^* — топологическая двойственная к E группа, т. е. группа, двойственная к пространству E, рассматриваемому как локально компактная группа. Способом, описанным в гл. II-5, определим на E^* структуру векторного пространства над K; как мы там доказали, векторное пространство E^* над K имеет ту же самую размерность, что и E. В этих обозначениях имеем

Предложение 2. *Функция Φ на E стандартна тогда и только тогда, когда существуют такие K-решетки L, M в E, что $L \supset M$, Φ равна нулю вне L и постоянна на смежных классах в L по модулю M. Если это имеет место и если L_*, M_* — двойственные к L, M K-решетки, то $M_* \supset L_*$ и преобразование Фурье Φ^* функции Φ равно нулю вне M_* и постоянно на классах смежности в M_* по модулю L_*.*

Если Φ, L, M обладает свойствами, указанными в предложении, то Φ, очевидно, стандартна. Обратно, предположим, что Φ стандартна. Возьмем какую-нибудь K-норму N на E и обозначим через μ верхнюю грань нормы N на носителе функции Φ. Тогда, как мы видели в главе II-2, множество L, определенное неравенством $N(e) \leqslant \mu$, является K-решеткой, и эта решетка содержит носитель Φ. Так как множества $\Phi^{-1}(\{a\})$, $a \in \mathbf{C}$, открыты, а множество L компактно, то L содержится в объединении конечного числа таких множеств. Другими словами, функция Φ на L принимает лишь конечное число значений $a_1, \ldots, a_n$. Выберем такое $\varepsilon > 0$, что $|a_i - a_j| > \varepsilon$ при $i \neq j$. Поскольку Φ равномерно непрерывна на L, существует такое $\delta > 0$, что $|\Phi(e) - \Phi(e')| \leqslant \varepsilon$ при $N(e - e') \leqslant \delta$, где $e, e' \in L$. Тогда множество M, определяемое неравенством $N(e) \leqslant \delta$, является K-решеткой, содержащейся в L при $\delta \leqslant \mu$, причем Φ постоянна на классах смежности в L по модулю M. Рассмотрим теперь преобразование Фурье

$$\Phi^*(e^*) = \int_E \Phi(e) \langle e, e^* \rangle \, d\alpha(e),$$

где α — произвольная мера Хаара на E. Так как Φ равна нулю вне L, то интеграл не изменится, если мы возьмем его по L. Заменим

e^* на $e_1^* + e_1^*$, где $e_1^* \in L_*$. Поскольку по определению $\langle e, e_1^* \rangle = 1$ при всех $e \in L$, интеграл при этом не изменится. Следовательно, Φ^* постоянна на классах смежности в E^* по модулю L_*. С другой стороны, поскольку M — открытая подгруппа в компактной группе L, то L есть объединение конечного числа классов смежности $e_i + M$. Так как Φ постоянна на каждом из этих классов, то

$$\Phi^*(e^*) = \sum_i \Phi(e_i) \int_M \langle e_i + e, e^* \rangle \, d\alpha(e) = \tag{2}$$

$$= \sum_i \Phi(e_i) \langle e_i e^* \rangle \int_M \langle e, e^* \rangle \, d\alpha(e).$$

Поскольку последний интеграл, очевидно, равен нулю, если характер $e \to \langle e, e^* \rangle$ нетривиален на M, т. е. если $e^* \notin M_*$, то функция Φ^* равна нулю вне M_*.

Следствие 1. *Если Φ — характеристическая функция K-решетки L в E, то $\alpha(L)^{-1}\Phi^*$ — характеристическая функция K-решетки L_* в E^*, двойственной к L, и $\alpha^*(L_*) = \alpha(L)^{-1}$, где α^* — мера, двойственная к α.*

Первое утверждение немедленно вытекает из (2) при $L = M$, $\Phi(0) = 1$, поэтому обратное преобразование Фурье функции Φ^* равно $\alpha^*(L_*)\alpha(L)\Phi$. Поскольку последняя функция должна совпасть с Φ, получаем наше второе утверждение.

Следствие 2. *Каждая стандартная функция на E допустима для E.*

Это — очевидное следствие предложения 2 и определений.

В нашем очередном следствии отождествим K с топологическим двойственным к нему при помощи характера χ на K способом, объясненным в гл II-5, т. е. принимая, что $\langle x, y \rangle = \chi(xy)$ при $x, y \in K$. После такого отождествления можно говорить о самодвойственной мере на K.

Следствие 3. *Пусть R — максимальное компактное подкольцо в K, φ — его характеристическая функция, χ — нетривиальный характер на K порядка ν и α — самодвойственная мера на K при отождествлении K с его двойственным при помощи χ. Пусть элемент $a \in K^\times$ таков, что $\mathrm{ord}_K(a) = \nu$. Тогда $\alpha(R) = \mathrm{mod}_K(a)^{1/2}$ и преобразованием Фурье функции φ является функция $y \to \mathrm{mod}_K(a)^{1/2}\varphi(ay)$.*

Применим к $E = K$, $L = R$ следствие 1. Тогда по предложению 12 гл. II-5 $L_* = P^{-\nu}$, т. е. $L_* = a^{-1}R$, если элемент a таков,

как сказано выше. Характеристическая функция K-решетки L_* равна $\varphi(ay)$, и $\alpha(L_*) = \mathrm{mod}_K(a)^{-1}\alpha(R)$. Теперь наше утверждение немедленно вытекает из следствия 1.

Определение 2. *Пусть E — векторное пространство конечной размерности над* $\mathbf{R}$. *Под стандартной функцией на E мы будем понимать любую функцию вида $e \to p(e)\exp(-q(e))$, где p — комплексная полиномиальная функция на E, а q — вещественная положительно определенная квадратичная форма на E.*

Предложение 3. *Пусть E таково, как в определении* 2. *Тогда каждая стандартная функция на E обладает преобразованием Фурье, причем последнее также является стандартной функцией, и каждая стандартная функция допустима для (E, L), где L — любая* $\mathbf{R}$*-решетка в E.*

Выберем такой базис в E над $\mathbf{R}$, чтобы при отождествлении E с $\mathbf{R}^n$ при помощи этого базиса квадратичная форма q имела вид $q(x) = \pi\sum x_\nu^2$. Очевидно, что наше первое утверждение достаточно доказать для функции $M(x)\exp(-q(x))$, где $M(x)$ — одночлен от x_ν. По теореме 3 гл. II-5 мы можем отождествить пространство $\mathbf{R}^n$ с двойственным к нему, полагая $\langle x, y\rangle = \mathbf{e}(\sum x_\nu y_\nu)$. Мы видим, что достаточно рассмотреть случай $n = 1$, т. е. показать, что преобразование Фурье функции $x^m\exp(-\pi x^2)$ является стандартной функцией на $\mathbf{R}$ для каждого целого числа $m \geqslant 0$. Но, как следует из хорошо известной формулы

$$\exp(-\pi y^2) = \int \exp(-\pi x^2 + 2\pi i x y)\,dx,$$

преобразованием Фурье функции $\exp(-\pi x^2)$ является функция $\exp(-\pi y^2)$. Дифференцируя обе части формулы m раз по y и используя индукцию по m, немедленно убеждаемся, что левая часть будет иметь вид $p_m(y)\exp(-\pi y^2)$, где p_m — многочлен степени m, а в правой части дифференцирование может быть внесено под знак интеграла. Это дает

$$p_m(y)\exp(-\pi y^2) = \int (2\pi i x)^m \exp(-\pi x^2 + 2\pi i x y)\,dx,$$

чем доказано первое утверждение предложения. Пусть теперь L — некоторая $\mathbf{R}$-решетка в E. По предложению 11 гл. II-4 существует базис векторного пространства E над $\mathbf{R}$, порождающий группу L. Другими словами, отождествляя E с $\mathbf{R}^n$ посредством этого базиса, можно считать, что $E = \mathbf{R}^n$ и $L = \mathbf{Z}^n$. Для того чтобы доказать, что стандартные функции на $\mathbf{R}^n$ допустимы для $(\mathbf{R}^n, \mathbf{Z}^n)$, достаточно показать, что для любой такой функции Φ ряд $\sum|\Phi(x+\nu)|$,

взятый по всем $\nu \in \mathbf{Z}^n$, равномерно сходится на каждом компактном подмножестве C в $\mathbf{R}^n$. Положим $\Phi(x) = p(x) \exp(-q(x))$ и $r(x) = \sum x_\nu^2$. Выберем такое $\delta > 0$, чтобы квадратичная форма $q - \delta r$ была положительно определена; для этого достаточно взять $\delta < \mu$, где μ — нижняя грань функции q на сфере $r = 1$. Тогда $\Phi(y) \exp(\delta r(y - x)) \to 0$ при $r(y) \to \infty$ равномерно по $x \in C$. Отсюда следует, что эта функция ограничена при $x \in C$ и при всех $y \in \mathbf{R}^n$. Поэтому, заменяя y на $x + u$, получаем, что для некоторого $A > 0$

$$|\Phi(x + u)| \leqslant A \exp(-\delta r(u))$$

при всех $x \in C$, откуда

$$\sum_\nu |\Phi(x+\nu)| \leqslant A \sum_\nu \exp\Big(-\delta \sum_i \nu_i^2\Big) = A\Big(\sum_{\nu=-\infty}^{+\infty} \exp(-\delta\nu^2)\Big)^n,$$

чем и заканчивается доказательство.

Для некоторых специальных случаев предложения 3, в которых $E = \mathbf{R}$ или $\mathbf{C}$, нам понадобятся более точные утверждения. Выберем *базисный* характер χ на $\mathbf{R}$ (соотв. на $\mathbf{C}$) и отождествим с помощью этого характера пространство $\mathbf{R}$ (соотв. $\mathbf{C}$) с топологическим двойственным к нему подобно тому, как мы делали это выше для p-полей (см. гл. II-5). Самодвойственные меры будем брать относительно этого отождествления.

Предложение 4. *Самодвойственной мерой на* $\mathbf{R}$, *соответствующей базисному характеру* $\chi(x) = \mathbf{e}(-ax)$, *где* $a \in \mathbf{R}^\times$, *является мера* $d\alpha(x) = |a|^{1/2}\, dx$. *Если* $\varphi_A(x) = x^A \exp(-\pi x^2)$, *где* $A = 0$ *или* 1, *то преобразованием Фурье функции* φ_A *является функция* $\varphi'_A(y) = i^{-A}|a|^{1/2} \varphi_A(ay)$.

Положим $d\alpha(x) = c \cdot dx$, где $c \in \mathbf{R}_+^\times$. Тогда φ'_0 задается формулой

$$\varphi'_0(y) = c \int_{\mathbf{R}} \exp(-\pi x^2 - 2\pi i a x y)\, dx;$$

как уже отмечалось, последнее выражение равно $c\varphi_0(ay)$. Применяя теперь формулу обращения Фурье и лемму 1, получаем $c = |a|^{1/2}$. Дифференцируя обе части формулы для $\varphi'_0(y)$ по y, получаем преобразование Фурье функции φ_1.

Предложение 5. *Самодвойственной мерой на* $\mathbf{C}$, *соответствующей базисному характеру* $\chi(x) = \mathbf{e}(-ax - \bar{a}\bar{x})$, *где* $a \in \mathbf{C}^\times$, *является мера* $d\alpha(x) = (a\bar{a})^{1/2} |dx \wedge d\bar{x}|$. *Если* $\varphi_A(x) =$

$= x^A \exp(-2\pi x\bar{x})$, *где* A *— целое неотрицательное число, то преобразованием Фурье функции* φ_A *является функция* $i^{-A}(a\bar{a})^{1/2}\overline{\varphi_A(ay)}$, *а преобразованием Фурье функции* $\overline{\varphi_A}$ *— функция* $i^A(a\bar{a})^{1/2}\varphi_A(ay)$.

Доказательства утверждений относительно α и относительно преобразования Фурье функции φ_0 совершенно аналогичны доказательствам аналогичных утверждений в предложении 4. Дифференцируя A раз по y формулу для преобразования Фурье функции φ_0, получаем преобразование Фурье от φ_A из которого немедленно получается преобразование Фурье функции $\overline{\varphi}_A$.

Определение 3. *Пусть* E *— векторное пространство конечной размерности над* А*-полем* k, ε *— базис в* E *над* k, *и пусть для каждой конечной точки* v *поля* k ε_v *есть* r_v*-модуль, порожденный в* E_v *базисом* ε. *Под стандартной функцией на* $E_{\mathbf{A}}$ *будем понимать функцию вида*

$$e = (e_v) \to \Phi(e) = \prod_v \Phi_v(e_v),$$

где Φ_v *— стандартная функция на* E_v *для каждой точки* v *поля* k *и* Φ_v *— характеристическая функция модуля* ε_v *почти для всех* v.

Следствие 1 теор. 3 гл. III-1 показывает, что последнее условие не зависит от выбора базиса ε. Формула, которая определяет функцию Φ и которую мы будем записывать короче так: $\Phi = \prod \Phi_v$, имеет смысл в силу предложения 1 гл. IV-1, согласно которому почти все сомножители в правой части равны 1 для любого e из $E_{\mathbf{A}}$. Это предложение показывает также, что функция Φ равна нулю вне $E_{\mathbf{A}}(P, \varepsilon)$ для подходящего P, т. е. что Φ непрерывна.

Аналогично случаю $k_{\mathbf{A}}$ в гл. V-4 меру Хаара на $E_{\mathbf{A}}$ можно определить, выбрав для каждой точки v меру Хаара α_v на E_v так, чтобы $\alpha_v(\varepsilon_v) = 1$ почти для всех v. В случае когда меры α_v удовлетворяют последнему условию, будем говорить, что они *когерентны*. В этом случае существует единственная мера α на $E_{\mathbf{A}}$, которая совпадает с произведением мер $\prod \alpha_v$ на каждой открытой подгруппе $E_{\mathbf{A}}(P, \varepsilon)$ в $E_{\mathbf{A}}$. Для этой меры будем писать $\alpha = \prod \alpha_v$. Ясно, что для любой меры Хаара α на $E_{\mathbf{A}}$ можно найти когерентную систему мер α_v, для которой $\alpha = \prod \alpha_v$, выбирая какое-нибудь множество когерентных мер на пространствах E_v и соответствующим образом изменяя каждую из них.

Начиная с этого места, мы раз и навсегда выберем *базисный* характер χ на $k_{\mathbf{A}}$, т. е. нетривиальный характер на $k_{\mathbf{A}}$, тривиальный на k. Обозначим через χ_v характер на k_v, индуцированный характером χ. Этот характер нетривиален по следствию 1 теор. 3

гл. IV-2. Для любого векторного пространства E конечной размерности над k обозначим через E' алгебраическое двойственное к нему и с помощью χ и χ_v отождествим топологические двойственные к $E_{\mathbf{A}}$ и E_v с $E'_{\mathbf{A}}$ и E'_v соответственно, способом, описанным в гл. IV-2, т. е. используя теорему 3 гл. IV-2 в случае первого пространства и теорему 3 гл. II-5 в случае второго для каждой точки v.

Теорема 1. *Пусть E — векторное пространство конечной размерности над* **A***-полем k, α_v — когерентные меры Хаара на пространствах E_v и $\Phi = \prod \Phi_v$ — стандартная функция на $E_{\mathbf{A}}$. Тогда преобразованием Фурье функции Φ относительно меры $\alpha = \prod \alpha_v$ на $E_{\mathbf{A}}$ является стандартная функция на $E'_{\mathbf{A}}$, задаваемая равенством $\Phi' = \prod \Phi'_v$, где для каждой v функция Φ'_v есть преобразование Фурье функции Φ_v относительно меры α_v. При этом Φ допустима для $(E_{\mathbf{A}}, E)$.*

Пусть ε, ε' — базисы в E, E' над k. Для каждой конечной точки v определим ε_v, как выше, и ε'_v аналогичным образом. По следствию 3 теор. 3 гл. IV-2 существует такое содержащее P_∞ конечное множество P точек поля k, что k_v-решетка ε'_v двойственна к ε_v для v, не лежащих в P. Ввиду нашего предположения о α_v можно считать, что множество P выбрано так, что $\alpha_v(\varepsilon_v) = 1$ при $v \notin P$. Тогда по следствию 1 предл. 2 преобразование Фурье характеристической функции модуля ε_v будет характеристической функцией модуля ε'_v и $\alpha'_v(\varepsilon'_v) = 1$ для двойственной к α_v меры α'_v при всех $v \notin P$. Пусть теперь $\Phi = \prod \Phi_v$ — стандартная функция на $E_{\mathbf{A}}$. Для каждой точки v обозначим через Φ'_v преобразование Фурье функции Φ_v относительно меры α_v. Из только что сказанного и из предложений 2 и 3 следует, что $\Phi' = \prod \Phi'_v$ — стандартная функция на $E'_{\mathbf{A}}$. Покажем, что эта функция является преобразованием Фурье от Φ. Заменяя, если это необходимо, P большим множеством, можно считать, что Φ_v является характеристической функцией модуля ε_v при $v \notin P$. Тогда носитель функции Φ содержится в $E_{\mathbf{A}}(P, \varepsilon)$, так что преобразование Фурье Φ'' функции Φ задается интегралом

$$\Phi''(e') = \int \Phi(e)\,\chi([e, e'])\,d\alpha(e),$$

взятым по $E_{\mathbf{A}}(P, \varepsilon)$. В силу наших определений подинтегральная функция здесь задается следующим образом:

$$\Phi(e)\,\chi([e; e']) = \prod_v (\Phi_v(e_v)\,\chi_v([e_v, e'_v])),$$

где $e=(e_v)$, $e'=(e'_v)$. Далее, при фиксированном e' сомножители в правой части равенства, соответствующие точкам v, имеют почти для всех v постоянное значение 1 на ε_v. Согласно определению группы $E_{\mathrm{A}}(P, \varepsilon)$ в предложении 1 гл. IV-1, отсюда следует, что $\Phi''(e')$ совпадает с $\Phi'(e')$.

Для того чтобы доказать допустимость Φ для (E_{A}, E), достаточно показать, что ряд

$$\sum_{\eta\in E}|\Phi(e+\eta)|=\sum_{\eta\in E}\Big|\prod_v\Phi_v(e_v+\eta)\Big| \tag{3}$$

равномерно сходится на каждом компактном подмножестве $C\subset E_{\mathrm{A}}$. По следствию 1 предложения 1 гл. IV-1 C содержится в некотором множестве $E_{\mathrm{A}}(P, \varepsilon)$. Выберем P так, чтобы множество $E_{\mathrm{A}}(P, \varepsilon)$ содержало помимо множества C еще и носитель функции Φ. Для каждой точки v из P обозначим через C_v проекцию множества C на E_v. Для каждой конечной точки из P обозначим через C'_v носитель функции Φ_v. Для v, не лежащих в P, положим $C_v=C'_v=\varepsilon_v$. Так как $\prod C_v$ компактно и содержит C, достаточно будет доказать наше утверждение для $C=\prod C_v$. Предположим сначала, что k — поле характеристики $p>1$. Тогда функция Φ равна нулю вне компактного множества $C'=\prod C'_v$, так что все слагаемые в (3) равны нулю, кроме членов, соответствующих элементам $\eta\in E\cap C''$, где C'' — образ множества $C\times C'$ при отображении $(e, e')\to e'-e$. Так как C'' компактно, то $E\cap C''$ конечно, и наше утверждение очевидно. Пусть теперь характеристика поля k равна нулю. Для каждой конечной точки $v\in P$ возьмем некоторую k_v-норму N_v на E_v и обозначим через L_v k_v-решетку тех e_v, для которых $\mathrm{N}_v(e_v)\leqslant\leqslant\mu$, где μ — верхняя грань значений нормы N_v на компактном множестве $C_v\cup C'_v$. Для точек v, не лежащих в P, положим $L_v=\varepsilon_v$. Положим, далее, $L=\bigcap(E\cap L_v)$, где v пробегает все конечные точки поля k. По теореме 2 гл. V-2 L является k-решеткой в E с замыканиями L_v в E_v для всех конечных v. Для $e=(e_v)\in C$, очевидно, $\Phi_v(e_v+\eta)=0$ при $\eta\notin E\cap L_v$, так что $\Phi(e+\eta)=0$ при η, не лежащих в L. Кроме того, если A_v — верхняя грань $|\Phi_v|$ для каждой конечной точки v поля k, то $A_v=1$ почти для всех v. Полагая $A=\prod A_v$, мы видим, что при $e\in C$ ряд (3) мажорируется рядом

$$A\sum_{\eta\in L}\Big|\prod_w\Phi_w(e_w+\eta)\Big|,$$

где произведение берется по бесконечным точкам w поля k. Как объяснялось в гл. V-2, положим $E_\infty=E\otimes_{\mathbf{Q}}\mathbf{R}$ и отождествим это

пространство с произведением $\prod E_w$, взятым по бесконечным точкам поля k. Очевидно, что функция Φ_∞ на E_∞, определенная при $e_\infty = (e_w)$ формулой

$$\Phi_\infty(e_\infty) = \prod_w \Phi_w(e_w),$$

стандартна. Поскольку L есть k-решетка в E, то L является $\mathbf{Q}$-решеткой в E, рассматриваемом как векторное пространство над $\mathbf{Q}$, а следовательно, и $\mathbf{R}$-решеткой в E_∞. Теперь остается воспользоваться предложением 3.

Следствие 1. *Если α_v — когерентные меры на E_v, то двойственные к ним меры α'_v также когерентны; мерой, двойственной к $\alpha = \prod \alpha_v$, является мера $\alpha' = \prod \alpha'_v$. Если $\alpha(E_\mathbf{A}/E) = 1$, то $\alpha'(E'_\mathbf{A}/E') = 1$.*

Первое утверждение было доказано выше; второе немедленно следует из теоремы 1 и определений. Что касается последнего утверждения, то, согласно теореме 3 гл. IV-2, E' является подгруппой в $E'_\mathbf{A}$, ассоциированной по двойственности с подгруппой E в $E_\mathbf{A}$. Поэтому, как мы уже видели, наше утверждение следует из формулы Пуассона, при условии что мы можем предъявить допустимую для $(E_\mathbf{A}, E)$ функцию Φ, для которой левая часть равенства (1) отлична от нуля. Но по теореме 1 любая стандартная функция $\Phi \geqslant 0$, для которой $\Phi(0) > 0$, обладает этим свойством.

Важен частный случай $E = E' = k$, $[x, y] = xy$. Отождествляя, как и раньше, пространства $k_\mathbf{A}$ и k_v с двойственными к ним при помощи характеров χ, χ_v, мы получаем в этом случае

Следствие 2. *Пусть α, α_v — самодвойственные меры на $k_\mathbf{A}$, k_v. Тогда меры α_v когерентны, $\alpha = \prod \alpha_v$ и $\alpha(k_\mathbf{A}/k) = 1$.*

Возьмем любые когерентные меры β_v на группах k_v. По следствию 1 двойственные к ним меры β'_v когерентны, откуда вытекает, что $\beta_v = \beta'_v$ почти для всех v. Другими словами, мера β_v совпадает с самодвойственной мерой α_v почти для всех v и, значит, меры α_v когерентны. Остальные наши утверждения немедленно вытекают теперь из следствия 1.

В обозначениях следствия 1 мера α на $E_\mathbf{A}$, для которой $\alpha(E_\mathbf{A}/E) = 1$, известна как *мера Тамагавы* на $E_\mathbf{A}$; следствие 1 показывает, что двойственная к ней мера является мерой Тамагавы на $E'_\mathbf{A}$. В частности, на $k_\mathbf{A}$ мера Тамагавы — это то же самое, что самодвойственная мера.

Для каждой конечной точки v поля k обозначим через $\nu(v)$ порядок характера χ_v; по следствию 1 теор. 3 гл. IV-2 $\nu(v) = 0$ почти для всех v. Выберем такие $a_v \in k_v^\times$, что $\mathrm{ord}_v(a_v) = \nu(v)$. Далее, для каждой вещественной точки v поля k применим к характеру $x \to \mathbf{e}(-x)$ следствие теор. 3 гл. II-5, которое показывает, что существует один и только один элемент $a_v \in k_v^\times$, такой, что $\chi_v(x) = \mathbf{e}(-a_v x)$ при всех $x \in k_v$. Аналогично для каждой мнимой точки v существует один и только один элемент $a_v \in k_v^\times$, для которого $\chi_v(x) = \mathbf{e}(-a_v x - \bar{a}_v \bar{x})$ при всех $x \in k_v$. Так как $\nu(v) = 0$ почти для всех v, то $(a_v) \in k_\mathbf{A}^\times$.

Определение 4. *Пусть χ — нетривиальный характер на $k_\mathbf{A}$, тривиальный на k и индуцирующий для каждой точки v характер χ_v на k_v. Идель $a = (a_v)$ поля k будем называть дифферентным иделем, связанным с χ, если $\mathrm{ord}_v(a_v)$ равен порядку $\nu(v)$ характера χ_v для каждой конечной точки v поля k, $\chi_v(x) = \mathbf{e}(-a_v x)$ для каждой вещественной точки v и $\chi_v(x) = \mathbf{e}(-a_v x - \bar{a}_v \bar{x})$ для каждой мнимой точки v поля k.*

Ясно, что для заданного χ дифферентный идель a однозначно определен по модулю $\prod r_v^\times$, где произведение берется по всем конечным точкам v поля k. Если χ_1 — другой такой характер, то по теореме 3 гл. IV-2 его можно записать в виде $\chi_1(x) = \chi(\xi x)$, где $\xi \in k^\times$. Тогда ξa, где идель a такой, как выше, будет дифферентным иделем, связанным с χ_1. Следовательно, множество всех дифферентных иделей является классом смежности в $k_\mathbf{A}^\times$ по модулю $k^\times \prod r_v^\times$. Если k — поле характеристики $p > 1$, то a тогда и только тогда является дифферентным иделем, связанным с χ, когда $\mathrm{div}(a) = \mathrm{div}(\chi)$ в смысле, объясненном в гл. VI; откуда следует, что $\mathrm{div}(a)$ лежит в каноническом классе.

Предложение 6. *Пусть a — дифферентный идель. Тогда, если характеристика поля k равна нулю, то $|a|_\mathbf{A} = |D|^{-1}$, где D — дискриминант поля k, а если k — поле характеристики $p > 1$, $\mathbf{F}_q$ — его поле констант и g — его род, то $|a|_\mathbf{A} = q^{2-2g}$.*

Последнее утверждение эквивалентно равенству $\deg(\mathrm{div}(a)) = 2g - 2$; так как $\mathrm{div}(a)$ является каноническим дивизором, то это утверждение совпадает со следствием 1 теор. 2 гл. VI. В случае характеристики нуль пусть α, α_v — самодвойственные меры на $k_\mathbf{A}$, k_v, так что $\alpha = \prod \alpha_v$ (следствие 2 теор. 1). Пусть мера $\beta = \prod \beta_v$ такова, как в предложении 7 гл. V-4. Применяя следствие 3 пред-

ложения 2 и предложения 4 и 5, получаем, что $\alpha = |a|_A^{1/2}\beta$. Так как по следствию 2 теор. 1 $\alpha(k_A/k) = 1$ и по предложению 7 гл. V-4 $\beta(k_A/k) = |D|^{1/2}$, то $|a|_A = |D|^{-1}$.

§ 3. КВАЗИХАРАКТЕРЫ

Сначала мы изложим некоторые вспомогательные результаты. Как обычно, для всякого $z \in \mathbf{C}$ обозначаем через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ его вещественную и мнимую части и полагаем $|z| = (z\bar{z})^{1/2}$, $|z|_\infty = \mathrm{mod}_{\mathbf{C}}(z) = z\bar{z}$.

Лемма 2. *Характер ω группы G тривиален, если $\mathrm{Re}(\omega(g)) > 0$ при всех $g \in G$.*

Если $z \in \mathbf{C}$, $|z| = 1$, $z \neq 1$ и $\mathrm{Re}(z) > 0$, то $z = \mathbf{e}(t)$, где $t \in \mathbf{R}$, $0 < |t| < 1/4$. Обозначим через n наименьшее целое число, для которого $n|t| > 1/4$. Тогда $(n-1)|t| \leqslant 1/4$, следовательно, $1/4 < n|t| < 1/2$ и $\mathrm{Re}(z^n) < 0$. Поэтому подмножество в $\mathbf{C}$, определенное условиями $|z| = 1$, $\mathrm{Re}(z) > 0$, не содержит иных подгрупп в $\mathbf{C}^\times$, кроме $\{1\}$.

Лемма 3. *Каждый гомоморфизм ω компактной группы G в $\mathbf{C}^\times$ является характером на G.*

В самом деле, отображение $g \to |\omega(g)|$ должно переводить G в компактную подгруппу в $\mathbf{R}_+^\times$, а таких подгрупп там нет, за исключением $\{1\}$.

Группа G называется *вполне несвязной*, если существует фундаментальная система окрестностей нейтрального элемента в G, состоящая из подгрупп G. Например, если K — некоторое p-поле с максимальным компактным подкольцом R и максимальным идеалом P в R, то группы K и $K^\times$ вполне несвязны: подгруппы P^n в K и подгруппы $1 + P^n$ в $K^\times$, $n \geqslant 1$, образуют такие фундаментальные системы.

Лемма 4. *Пусть группа G локально компактна и вполне несвязна. Тогда каждое представление $G \to \mathbf{C}^\times$ локально постоянно. Если G компактна, то каждое такое представление является характером конечного порядка на G. Обратно, если G — компактная коммутативная группа и каждое ее представление имеет конечный порядок, то G вполне несвязна.*

Если G локально компактна и вполне несвязна, то леммы 2 и 3 показывают, что каждое представление $G \to \mathbf{C}^\times$ тривиально на некоторой открытой подгруппе в G и, следовательно, локально

постоянно. Если G компактна, то любая открытая подгруппа в G имеет конечный индекс, откуда вытекает второе утверждение леммы. Если G коммутативна и компактна, то двойственная к ней группа G^* дискретна. Так как G может быть отождествлена с группой, двойственной к G^*, то в этом случае существует фундаментальная система окрестностей нуля в G, состоящая из множеств, определенных условиями вида $|\omega_i(g) - 1| \leqslant \varepsilon$ $(1 \leqslant i \leqslant N)$, где ω_i — характеры на G. Если все ω_i имеют конечный порядок, то можно найти такое $\varepsilon > 0$, что из этих неравенств следуют равенства $\omega_i(g) = 1$ при $1 \leqslant i \leqslant N$, тогда таким образом определенная окрестность является подгруппой в G.

Начиная с этого места, нас будут интересовать главным образом представления в $\mathbf{C}^\times$ групп вида $K^\times$, где K — локальное поле, и вида $k_{\mathbf{A}}^\times/k^\times$, где k — некоторое $\mathbf{A}$-поле. Все эти группы обладают свойством, описанным в следующем определении.

Определение 5. *Группу G будем называть квазикомпактной, если она разлагается в прямое произведение компактной коммутативной группы G_1 и группы, изоморфной $\mathbf{R}$ или $\mathbf{Z}$. Представление такой группы G в $\mathbf{C}^\times$ будем называть квазихарактером на G.*

Нетрудно было бы показать, что группа G квазикомпактна в том и только в том случае, когда она коммутативна и локально компактна, а двойственная к ней группа G^* локально изоморфна $\mathbf{R}$, т. е. имеет открытую подгруппу, изоморфную $\mathbf{R}$ или $\mathbf{R}/\mathbf{Z}$; последнее условие можно даже заменить следующим более слабым: G^* имеет окрестность нуля, гомеоморфную $\mathbf{R}$. Отсюда легко вывести, что G квазикомпактна в том и только в том случае, когда в ней имеется такая компактная подгруппа G_1, что группа G/G_1 изоморфна $\mathbf{R}$ или $\mathbf{Z}$. Эти факты нам не понадобятся в последующем. Ясно, что если G обладает свойством, описанным в определении 5, то G_1 является ее единственной максимальной компактной подгруппой.

Определение 6. *Для квазикомпактной группы G квазихарактер на G будем называть главным, если он тривиален на максимальной компактной подгруппе G_1 в G.*

Квазихарактеры квазикомпактной группы G очевидным образом образуют группу, которую мы будем обозначать через $\Omega(G)$ и записывать мультипликативно. Иными словами, если $\omega, \omega' \in \Omega(G)$, то мы обозначаем через $\omega\omega'$ квазихарактер $g \to \omega(g)\,\omega'(g)$ на G. Ясно, что главные квазихарактеры образуют подгруппу Ω_1 в $\Omega(G)$.

Предложение 7. *Пусть G — квазикомпактная группа и G_1 — ее максимальная компактная подгруппа. Тогда G имеет нетривиальные представления в $\mathbf{R}_+^\times$; если ω_1 — такое представление, то его ядро совпадает с G_1 и каждое представление $G \to \mathbf{R}_+^\times$ может быть записано одним и только одним способом в виде $g \to \omega_1(g)^\sigma$, где $\sigma \in \mathbf{R}$.*

Пусть $G = G_1 \times N$, где группа N изоморфна $\mathbf{R}$ или $\mathbf{Z}$. По лемме 3 каждое представление ω: $G \to \mathbf{R}_+^\times$ тривиально на G_1; записывая элементы из G в виде пар (g_1, n) с $g_1 \in G_1$, $n \in N$, мы видим, что ω должно иметь вид $(g_1, n) \to \varphi(n)$, где φ — представление $N \to \mathbf{R}_+^\times$. Отождествим N с группой $\mathbf{R}$ или $\mathbf{Z}$, той, которой она изоморфна. В первом случае условие на φ означает, что отображение $n \to \log \varphi(n)$ определяет эндоморфизм группы $\mathbf{R}$ и, значит, имеет вид $n \to an$, где $a \in \mathbf{R}$, так что $\varphi(n) = \exp(an)$. В случае $N = \mathbf{Z}$ представление φ, очевидно, имеет вид $\varphi(n) = b^n$, где $b \in \mathbf{R}_+^\times$, и может быть записано в виде $\varphi(n) = \exp(an)$, где $a = \log b$. В обоих случаях φ нетривиально, если $a \neq 0$. Поэтому если ω_1 таково, как в предложении 7, то оно может быть записано в виде $\omega_1(g_1, n) = \exp(a_1 n)$, где $a_1 \neq 0$. Ядро этого представления, очевидно, равно G_1. Далее, если ω, φ, a таковы, как выше, то $\omega = (\omega_1)^\sigma$, где $\sigma = a/a_1$, причем элемент σ определен однозначно.

Следствие 1. *Пусть G, G_1 и ω_1 таковы, как в предложении 7. Тогда группа Ω_1 главных квазихарактеров на G изоморфна $\mathbf{C}$ или $\mathbf{C}^\times$, смотря по тому, чему изоморфна группа G/G_1, группе $\mathbf{R}$ или группе $\mathbf{Z}$. Каждый такой квазихарактер имеет вид*

$$g \to \omega_s(g) = \omega_1(g)^s,$$

где $s \in \mathbf{C}$. Отображение $s \to \omega_s$ является морфизмом из $\mathbf{C}$ на Ω_1. Ядро этого морфизма равно $\{0\}$ или имеет вид $a\mathbf{Z}$, где $a \in \mathbf{R}_+^\times$, смотря по тому, изоморфна G/G_1 группе $\mathbf{R}$ или $\mathbf{Z}$.

Пусть ω — произвольный квазихарактер на G. Во введенных выше обозначениях предложение 7, примененное к отображению $g \to |\omega(g)|$, показывает, что $|\omega| = \omega_\sigma$, где $\sigma \in \mathbf{R}$. Поэтому $\omega' = \omega_\sigma^{-1}\omega$ является характером на G. Если ω тривиален на G_1, то это же верно для ω', и применяя те же обозначения, что и в доказательстве предложения 7, можно записать $\omega'(g_1, n) = \psi(n)$, где ψ — характер на N. Как и в том доказательстве, отождествим группу N с изоморфной ей группой $\mathbf{R}$ или $\mathbf{Z}$; в обоих случаях $\omega_1(g, n) = \exp(a_1 n)$. Каждый характер на N может быть записан в виде $\psi(n) = \mathbf{e}(\tau n)$, где $\tau \in \mathbf{R}$; этот факт очевиден для $N = \mathbf{Z}$ и хорошо известен (и является частным случаем теоремы 3 гл. II-5) для $N = \mathbf{R}$. Отсюда вытекает, что $\omega = \omega_s$, где $s = \sigma + 2\pi i\tau/a_1$.

При этом σ и ψ однозначно определяются по ω; τ однозначно определяется по ψ в случае $N = \mathbf{R}$ и однозначно определяется по модулю $\mathbf{Z}$ в случае $N = \mathbf{Z}$. Отсюда видно, что $s \to \omega_s$ является изоморфизмом из $\mathbf{C}$ на Ω_1, если $N = \mathbf{R}$, а если $N = \mathbf{Z}$, то мы имеем $\omega(g_1, n) = u^n$, где $u = \exp(a_1 s)$ и $u \to \omega$ есть изоморфизм из $\mathbf{C}^\times$ на Ω_1. Доказательство закончено.

Следствие 2. *Пусть G — квазикомпактная группа, а именно прямое произведение компактной группы G_1 и группы N, изоморфной $\mathbf{R}$ или $\mathbf{Z}$. Тогда группа $\Omega(G)$ квазихарактеров на G разлагается в прямое произведение группы Ω_1, фигурирующей в следствии 1, и группы характеров на G, тривиальных на N; последняя группа изоморфна группе, двойственной к G_1.*

Как уже было отмечено выше, каждый квазихарактер ω на G может быть однозначно представлен в виде $\omega_\sigma\psi$, где ψ — характер на G и $\sigma \in \mathbf{R}$. Ясно, что ψ можно однозначно записать как $\psi_1\psi_2$, где ψ_1 тривиален на G_1, а ψ_2 тривиален на N. Поэтому $\omega = (\omega_\sigma\psi_1)\psi_2$ и $\omega_\sigma\psi_1 \in \Omega_1$. Последнее утверждение нашего следствия очевидно.

До сих пор мы ни слова не говорили о топологии на $\Omega(G)$. Введем на Ω_1 не только топологию, но даже комплексную структуру с помощью морфизма $s \to \omega_s$ из $\mathbf{C}$ на Ω_1, определенного в следствии 1 предл. 7. Введем на $\Omega(G)$ топологию, в которой Ω_1 является открытой подгруппой в $\Omega(G)$, и определим на $\Omega(G)$ комплексную структуру, перенеся при помощи трансляций комплексную структуру с Ω_1 на каждый класс смежности по модулю Ω_1. Тогда группа $\Omega(G)/\Omega_1$ дискретна и, следовательно, топологически изоморфна группе, двойственной к G_1, потому что та группа тоже дискретна. Компоненты связности в $\Omega(G)$ являются классами смежности по модулю Ω_1, и все они изоморфны $\mathbf{C}$ или $\mathbf{C}^\times$, в зависимости от того, какая реализуется из двух возможностей для G/G_1.

Ясно, что изложенные выше понятия и результаты можно применить к случаю $G = K^\times$, где K — любое локальное поле с представлением $\omega_1(x) = \mathrm{mod}_K(x)$. В качестве N можно взять подгруппу $\mathbf{R}_+^\times$ в $K^\times$, если $K = \mathbf{R}$ или $\mathbf{C}$, и группу, порожденную любым простым элементом π в K, если K есть p-поле. В последнем случае это дает

Предложение 8. *Пусть K — некоторое p-поле и π — простой элемент в K. Тогда главные квазихарактеры на $K^\times$ — это отображения вида $x \to \mathrm{mod}_K(x)^s$, где $s \in \mathbf{C}$. Группа $\Omega(K^\times)$ квазихарактеров на $K^\times$ разлагается в прямое произведение группы главных квазихарактеров и группы характеров ψ на $K^\times$, для которых $\psi(\pi) = 1$.*

По лемме 4 каждый квазихарактер на $K^\times$ локально постоянен. Если буквы R и P имеют свои обычные значения, то группы $R^\times$ и $1 + P^n$ при $n \geqslant 1$ открыты в $K^\times$ и образуют фундаментальную систему окрестностей единицы. Этим оправдано следующее определение.

Определение 7. *Пусть K — некоторое p-поле, R — его максимальное компактное подкольцо и P — максимальный идеал в R. Пусть, далее, ω — квазихарактер на $K^\times$ и f — наименьшее из тех неотрицательных целых чисел, для которых $\omega(x) = 1$ при $x \in R^\times$, $x - 1 \in P^f$. Тогда P^f называется ведущим идеалом для ω.*

Очевидно, что квазихарактер ω является главным в том и только в том случае, когда $f = 0$, т. е. когда его ведущий идеал совпадает с R; в этом случае мы будем говорить, что ω *неразветвлен*.

Для $K = \mathbf{R}$ или $\mathbf{C}$ имеет место следующий результат.

Предложение 9. *Каждый квазихарактер на $\mathbf{R}^\times$ можно одним и только одним способом записать в виде $x \to x^{-A} |x|^s$, где $A = 0$ или 1 и $s \in \mathbf{C}$. Каждый квазихарактер на $\mathbf{C}^\times$ можно одним и только одним способом записать в виде $x \to x^{-A}\bar{x}^{-B}(x\bar{x})^s$, где A и B — целые числа, $\inf(A, B) = 0$ и $s \in \mathbf{C}$.*

Для $\mathbf{R}^\times$ это немедленно вытекает из предложения 7 и его следствий, поскольку здесь $G_1 = \{\pm 1\}$. Для $G = \mathbf{C}^\times$ группа G_1 определяется уравнением $x\bar{x} = 1$. Так как эта группа двойственна группе $\mathbf{Z}$, то ее характеры — это функции $x \to x^n$, где $n \in \mathbf{Z}$. Каждую такую функцию можно записать при $n \leqslant 0$ в виде $x \to (x/|x|)^{-A}$, где $A = -n \geqslant 0$, а при $n \geqslant 0$ в виде $x \to (\bar{x}/|x|)^{-B}$, где $B = n \geqslant 0$. Отсюда и из предложения 7 немедленно следует наше утверждение.

§ 4. КВАЗИХАРАКТЕРЫ А-ПОЛЕЙ

По теореме 6 гл. IV-4 группа $k_\mathbf{A}^\times/k^\times$ квазикомпактна для любого $\mathbf{A}$-поля k. Начиная с этого места, будем писать $G_k = k_\mathbf{A}^\times/k^\times$. Эта группа известна как *группа классов иделей* поля k. Обозначим через $\Omega(G_k)$ группу квазихарактеров на G_k, наделенную топологией и комплексной структурой, определенными в § 3. Квазихарактеры на G_k будем очевидным образом отождествлять с представлениями $k_\mathbf{A}^\times \to \mathbf{C}^\times$, тривиальными на $k^\times$.

Поскольку $z \to |z|_{\mathbf{A}}$ есть нетривиальное представление $k_{\mathbf{A}}^{\times} \to \mathbf{R}_{+}^{\times}$, тривиальное на $k^{\times}$, то оно определяет нетривиальное представление $G_k \to \mathbf{R}_{+}^{\times}$, которое будем обозначать через ω_1 и к которому можно применить предложение 7 § 3 и его следствия, снова записывая $\omega_s = (\omega_1)^s$ при $s \in \mathbf{C}$. В частности, ядро $G_k^1 = k_{\mathbf{A}}^1/k^{\times}$ представления ω_1 является максимальной компактной подгруппой в G_k; $s \to \omega_s$ есть морфизм группы $\mathbf{C}$ на группу Ω_1 главных квазихарактеров на G_k; если ω — произвольный квазихарактер на G_k, то существует одно и только одно число $\sigma \in \mathbf{R}$, для которого $|\omega| = \omega_\sigma$.

Если характеристика поля k равна нулю, то по следствию 2 теор. 5 гл. IV-4 группа G_k разлагается в прямое произведение подгруппы G_k^1 и образа N в G_k группы M, определенной в этом следствии. С другой стороны, если k — поле характеристики $p > 1$, то выберем какой-нибудь элемент $z_1 \in k_{\mathbf{A}}^{\times}$ среди тех, для которых $|z|_{\mathbf{A}}$ принимает свое наименьшее значение $Q > 1$. Поскольку, как мы видели в гл. VI, все значения $|z|_{\mathbf{A}}$ имеют вид q^n с $n \in \mathbf{Z}$, если полем констант поля k является $\mathbf{F}_q$, то $Q = q^{\nu}$, где $\nu \geqslant 1$; позже мы убедимся, что $\nu = 1$ и $Q = q$ (см. следствие 6 теорема 2 § 5). Обозначим через M подгруппу в $k_{\mathbf{A}}^{\times}$, порожденную элементом z_1, и через N — ее образ в G_k. Во всех случаях (нулевой и ненулевой характеристики) мы будем отождествлять группу N с ее образом в $\mathbf{R}_{+}^{\times}$ при отображении ω_1, так что ω_1 можно рассматривать как проекцию произведения $G_k = G_k^1 \times N$ на сомножитель N. Таким образом, $N = \mathbf{R}_{+}^{\times}$, если характеристика поля k равна нулю, а в противном случае N есть подгруппа в $\mathbf{R}_{+}^{\times}$, порожденная элементом Q. Отсюда вытекает, что в последнем случае морфизм $s \to \omega_s$ из $\mathbf{C}$ на Ω_1 имеет то же самое ядро, что и морфизм $s \to Q^s$ из $\mathbf{C}$ на $\mathbf{C}^{\times}$, т. е. $2\pi i\,(\log Q)^{-1}\,\mathbf{Z}$.

Пусть ω — произвольный квазихарактер на G_k. Рассматривая его как представление $k_{\mathbf{A}}^{\times} \to \mathbf{C}^{\times}$, тривиальное на $k^{\times}$, обозначим для каждой точки v поля k через ω_v индуцированный им квазихарактер на $k_v^{\times}$. Поскольку группы $k_{\mathbf{A}}(P)^{\times}$, определенные в следствии предложения 2 гл. IV-3, открыты в $k_{\mathbf{A}}^{\times}$, каждая окрестность единицы в $k_{\mathbf{A}}^{\times}$ содержит подгруппу вида $\prod_{v \in P} r_v^{\times}$. Поэтому в силу леммы 2 § 3 ω тривиален на некоторой подгруппе такого вида, другими словами, квазихарактер ω_v не разветвлен почти для всех v. Следовательно, для всех $z = (z_v) \in k_{\mathbf{A}}^{\times}$ мы имеем $\omega(z) = \prod \omega_v(z_v)$, где произведение берется по всем точкам v поля k; для каждого z почти все сомножители в произведении равны 1. Мы будем писать для краткости $\omega = \prod \omega_v$.

Теперь мы можем сформулировать главную цель настоящей главы. Это — исследование интегралов вида

$$Z(\omega, \Phi) = \int\limits_{k_{\mathbf{A}}^{\times}} \Phi(j(z))\,\omega(z)\,d\mu(z), \tag{4}$$

где обозначения имеют следующий смысл. В качестве μ берется мера Хаара на $k_{\mathbf{A}}^{\times}$; в качестве ω — квазихарактер на $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$, рассматриваемый как функция на $k_{\mathbf{A}}^{\times}$; в качестве Φ — стандартная функция на $k_{\mathbf{A}}$. Через j обозначается естественная биекция группы $k_{\mathbf{A}}^{\times}$ на множество обратимых элементов кольца $k_{\mathbf{A}}$; согласно предложению 2 гл. IV-3, это — непрерывное отображение $k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}$. Допуская вольность в обозначениях, мы будем обычно писать $\Phi(z)$ вместо $\Phi(j(z))$.

Что касается меры μ, как уже было замечено в гл. V-4 в случае характеристики нуль, такую меру можно определить, выбрав для каждой точки v меру Хаара μ_v на $k_v^{\times}$ таким образом, чтобы $\mu_v(r_v^{\times}) = 1$ почти для всех v. Мы пишем $\mu = \prod \mu_v$ для обозначения меры, которая совпадает с произведением мер $\prod \mu_v$ на каждой подгруппе $k_{\mathbf{A}}(P)^{\times}$. Меры μ_v устроены так.

Лемма 5. *Пусть K — локальное поле и α — мера Хаара на K. Тогда формула $d\mu(x) = \mathrm{mod}_K(x)^{-1}\,d\alpha(x)$ определяет меру Хаара μ на $K^{\times}$. При этом, если K — некоторое p-поле, q — его модуль и R — максимальное компактное подкольцо, то $\mu(R^{\times}) = (1 - q^{-1})\,\alpha(R)$.*

По определению функции mod_K, при $\alpha \in K^{\times}$ отображение $x \to ax$ оставляет меру μ инвариантной, чем доказано первое утверждение. Второе немедленно следует из теоремы 6 гл. I-4.

Предложение 10. *Пусть $\Phi = \prod \Phi_v$ — стандартная функция на $k_{\mathbf{A}}$, $\omega = \prod \omega_v$ — квазихарактер на $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$ и $\mu = \prod \mu_v$ — мера Хаара на $k_{\mathbf{A}}^{\times}$. Предположим, что $|\omega| = \omega_{\sigma}$, где $\sigma > 1$. Тогда интеграл $Z(\omega, \Phi)$ в (4) абсолютно сходится и его значение задается также абсолютно сходящимся произведением*

$$Z(\omega, \Phi) = \prod_v \Big(\int\limits_{k_v^{\times}} \Phi_v(x)\,\omega_v(x)\,d\mu_v(x) \Big). \tag{5}$$

Для каждой конечной точки v поля k положим $\Psi_v = |\Phi_v|$; для каждой бесконечной точки w поля k выберем такую стандартную

функцию Ψ_w на k_w, что $\Psi_w \geqslant |\Phi_w|$. Тогда, очевидно, $\Psi = \prod \Psi_v$ будет стандартной функцией на $k_{\mathbf{A}}$, мажорирующей $|\Phi|$, и $Z(\omega_\sigma, \Psi)$ мажорирует $Z(\omega, \Phi)$. Обозначим через $I(P)$, $J(P)$ интегралы по $k_{\mathbf{A}}(P)^\times$ от $\Phi\omega\, d\mu$ и $\Psi\omega_\sigma\, d\mu$ соответственно и через I_v, J_v интегралы по $k_v^\times$ от $\Phi_v\omega_v\, d\mu_v$ и $\Psi_v\,|\,\omega_v\,|\,d\mu_v$ соответственно; для каждой конечной точки v обозначим через I_v', J_v' те же интегралы, но взятые по $r_v^\times$, а не по $k_v^\times$; I_v является отвечающим точке v сомножителем в правой части равенства (5). Почти для всех конечных точек v поля k функция Φ_v является характеристической функцией кольца r_v, квазихарактер ω_v неразветвлен и $\mu_v(r_v^\times) = 1$; пусть P_0 — такое конечное множество точек, содержащее P_∞, что эти свойства имеют место при всех v, не лежащих в P_0. Тогда $I_v' = J_v' = 1$ при $v \notin P_0$. Отсюда вытекает, что при всех $P \supset P_0$

$$I(P) = \prod_{v \in P} I_v, \quad J(P) = \prod_{v \in P} J_v.$$

Поэтому $Z(\omega_\sigma, \Psi) < +\infty$ при условии, что все интегралы J_v и бесконечное произведение сходятся. Если мы покажем, что это условие выполняется, отсюда будет следовать также, что $Z(\omega, \Phi)$, интегралы I_v и произведение $\prod I_v$ все абсолютно сходятся и что интеграл $Z(\omega, \Phi)$ равен последнему произведению, а именно это мы и хотим доказать. Для любой точки v возьмем какую-нибудь меру Хаара α_v на k_v. Тогда по лемме 5 $d\mu_v(x) = m_v\,|\,x\,|_v^{-1}\, d\alpha_v(x)$ при некотором $m_v \in \mathbf{R}_+^\times$. Это дает

$$J_v = m_v \int\limits_{k_v^\times} \Psi_v(x)\,|\,x\,|_v^{\sigma-1}\, d\alpha_v(x).$$

Из нашего определения стандартной функции сразу видно, что последний интеграл сходится при $\sigma \geqslant 1$; на самом деле для сходимости достаточно, чтобы выполнялось неравенство $\sigma > 0$, но нам это здесь не нужно. С другой стороны, для точки v, не лежащей в P, имеем

$$J_v = \sum_{\nu=0}^{+\infty} \int\limits_{u_\nu} |\,x\,|_v^\sigma\, d\mu_v(x) = \sum_{\nu=0}^{+\infty} q_v^{-\nu\sigma} = (1 - q_v^{-\sigma})^{-1},$$

поскольку $k_v^\times \cap r_v$ является объединением попарно непересекающихся множеств $u_\nu = \pi_v^\nu r_v^\times$, $\nu \geqslant 0$. Предложение 1 § 1 показывает теперь, что произведение $\prod J_v$ сходится. Доказательство закончено.

Метод вычисления, который мы только что применили для J_v, можно применить и для интеграла I_v. Получающийся при этом результат сформулируем как следующее

Предложение 11. *Пусть K — некоторое p-поле, q — его модуль, R — его максимальное компактное подкольцо и μ — мера Хаара на $K^\times$, для которой $\mu(R^\times) = 1$. Обозначим через φ характеристическую функцию кольца R. Тогда при* $\operatorname{Re}(s) > 0$

$$\int_{K^\times} \varphi(x) \operatorname{mod}_K(x)^s \, d\mu(x) = (1 - q^{-s})^{-1}.$$

В самом деле, мы можем представить $K^\times \cap R$ как объединение попарно непересекающихся множеств $U_\nu = \pi^\nu R^\times = P^\nu - P^{\nu+1}$, $\nu \geqslant 0$. Тогда интеграл можно записать в виде ряда

$$\sum_{\nu=0}^{+\infty} \int_{U_\nu} \operatorname{mod}_K(x)^s \, d\mu(x) = \sum_{\nu=0}^{+\infty} q^{-\nu s},$$

который абсолютно сходится при $\operatorname{Re}(s) > 0$ и имеет указанное выше значение.

§ 5. ФУНКЦИОНАЛЬНОЕ УРАВНЕНИЕ

Прежде всего мы выберем некоторую меру Хаара на $k_{\mathbf{A}}^\times$. А именно на компактной группе G_k^1 возьмем меру Хаара μ_1, для которой $\mu_1(G_k^1) = 1$. На группе N возьмем меру ν, для которой $dv(n) = n^{-1}\,dn$, если $N = \mathbf{R}_+^\times$, и $\nu(\{1\}) = 1$ в противном случае. На $G_k = G_k^1 \times N$ возьмем меру $\mu = \mu_1 \times \nu$. Наконец, на $k_{\mathbf{A}}^\times$ возьмем такую меру μ, образ которой в $G_k = k_{\mathbf{A}}^\times / k^\times$ совпадает (в объясненном в гл. II-4 смысле) с только что определенной мерой.

Лемма 6. *Пусть F_1 — измеримая функция на N, причем $0 \leqslant F_1 \leqslant 1$ и существует компактный интервал $[t_0, t_1]$ в $\mathbf{R}_+^\times$, для которого $F_1(n) = 1$ при $n \in N$, $n < t_0$, и $F_1(n) = 0$ при $n \in N$, $n > t_1$. Тогда интеграл*

$$\lambda(s) = \int_N n^s F_1(n) \, dv(n)$$

абсолютно сходится при $\operatorname{Re}(s) > 0$. *Функцию $\lambda(s)$ можно аналитически продолжить до функции, мероморфной на всей s-плоскости.*

Если положить $\lambda_0(s) = s^{-1}$ *в случае* $N = \mathbf{R}_+^\times$ *и* $\lambda_0(s) = \frac{1}{2}(1 + Q^{-s}) \times (1 - Q^{-s})^{-1}$ *в случае* $N = \{Q^\nu\}_{\nu \in \mathbf{Z}}$, *то* $\lambda - \lambda_0$ *будет целой функцией от* s. *Наконец, если* $F_1(n) + F_1(n^{-1}) = 1$ *при всех* $n \in N$, *то* $\lambda(s) + \lambda(-s) = 0$.

Возьмем сначала в качестве F_1 функцию f_1, для которой $f_1(n) = 1$ при $n < 1$, $f_1(1) = 1/2$, $f_1(n) = 0$ при $n > 1$. Тогда функция λ равна интегралу $\int\limits_0^1 n^{s-1}\,dn$ в случае $N = \mathbf{R}_+^\times$ и ряду $\frac{1}{2} + \sum\limits_1^{+\infty} Q^{-\nu s}$ в случае $N = \{Q^\nu\}$. В обоих случаях при $\mathrm{Re}(s) > 0$ имеют место абсолютная сходимость и равенство $\lambda = \lambda_0$. Для произвольной функции F_1 это дает

$$\lambda(s) - \lambda_0(s) = \int\limits_N n^s (F_1(n) - f_1(n))\, d\nu(n).$$

Так как $F_1 - f_1$ есть ограниченная измеримая функция с компактным носителем на N, то последний интеграл абсолютно сходится при всех s, причем сходимость равномерна на каждом компактном подмножестве s-плоскости. Следовательно, этот интеграл определяет целую функцию от s. Предположим теперь, что $F_1(n) + F_1(n^{-1}) = 1$. Так как функция f_1 обладает тем же свойством, то для функции $F_2 = F_1 - f_1$ имеем $F_2(n^{-1}) = -F_2(n)$. Заменяя в последнем интеграле n на n^{-1} и учитывая равенство $\lambda_0(-s) = -\lambda_0(s)$, получаем, что $\lambda(-s) = -\lambda(s)$.

Из леммы 6 следует, что в точке $s = 0$ функция λ имеет вычет 1, если $N = \mathbf{R}_+^\times$, и вычет $(\log Q)^{-1}$, если $N = \{Q^\nu\}$. Здесь и ниже подразумевается, что вычеты берутся относительно переменной s. Напомним, что если функция $f(s)$ от s имеет простой полюс в точке $s = s_0$, то ее вычет равен $\lim (s - s_0) f(s)$ при $s \to s_0$.

Теорема 2. *Пусть* Φ — *стандартная функция на* $k_\mathbf{A}$. *Тогда функция* $\omega \to Z(\omega, \Phi)$, *определенная формулой* (4) § 4 *в случае, когда интеграл в* (4) *абсолютно сходится, может быть аналитически продолжена до функции, мероморфной на всем комплексном многообразии* $\Omega(G_k)$. *Эта функция удовлетворяет уравнению*

$$Z(\omega, \Phi) = Z(\omega_1 \omega^{-1}, \Phi'),$$

где Φ' — *преобразование Фурье функции* Φ *относительно меры Тамагавы на* $k_\mathbf{A}$. *Кроме того,* $Z(\omega, \Phi)$ *голоморфна всюду на* $\Omega(G_k)$, *за исключением простых полюсов* ω_0 *и* ω_1 *с вычетами соответственно* $-\rho\Phi(0)$ *и* $\rho\Phi'(0)$, *где* $\rho = 1$, *если* $N = \mathbf{R}_+^\times$, *и* $\rho = (\log Q)^{-1}$, *если* $N = \{Q^\nu\}$.

Выберем на $\mathbf{R}_+^\times$ две непрерывные функции F_0, F_1 со следующими свойствами: (i) $F_0 \geqslant 0$, $F_1 \geqslant 0$, $F_0 + F_1 = 1$; (ii) существует такой компактный интервал $[t_0, t_1]$ в $\mathbf{R}_+^\times$, что $F_0(t) = 0$ при $0 < t < t_0$ и $F_1(t) = 0$ при $t > t_1$. Возьмем любое $B > 1$. Тогда при $\sigma \in \mathbf{R}$, $\sigma \leqslant B$, $t \in \mathbf{R}_+^\times$ имеем $t^\sigma F_0(t) \leqslant t_0^{\sigma - B} t^B$. Для $i = 0, 1$ запишем

$$Z_i = Z_i(\omega, \Phi) = \int\limits_{k_{\mathbf{A}}^\times} \Phi(z)\, \omega(z)\, F_i(|z|_{\mathbf{A}})\, d\mu(z).$$

Положим, как и прежде, $|\omega| = \omega_\sigma$, где $\sigma \in \mathbf{R}$. По предложению 10 § 4 Z_0 и Z_1 абсолютно сходятся при $\sigma > 1$. С другой стороны, при $\sigma \leqslant B$ интеграл Z_0 мажорируется интегралом

$$\int\limits_{k_{\mathbf{A}}^\times} |\Phi(z)| \cdot |z|_{\mathbf{A}}^\sigma F_0(|z|_{\mathbf{A}})\, d\mu(z) \leqslant t_0^{\sigma - B} \int\limits_{k_{\mathbf{A}}^\times} |\Phi(z)| \cdot |z|_{\mathbf{A}}^B\, d\mu(z),$$

который сходится по предложению 10 § 4. В частности, $Z_0(\omega_s \omega, \Phi)$ абсолютно сходится при всех $s \in \mathbf{C}$, и легко проверяется, что эта сходимость равномерна по s, принадлежащим любому компактному подмножеству в $\mathbf{C}$. Так как квазихарактеры $\omega_s \omega$ при $s \in \mathbf{C}$ образуют компоненту связности элемента $\omega \in \Omega(G_k)$ и комплексная структура на этой компоненте определяется переменной s, отсюда видно, что функция $\omega \to Z_0(\omega, \Phi)$ голоморфна на всем пространстве $\Omega(G_k)$.

Теперь применим к группе $k_{\mathbf{A}}^\times$, дискретной подгруппе $k^\times$ и интегралам Z_0, Z_1 формулу (6) гл. II-4. Мы получим

$$Z_i = \int\limits_{\dot{G}_k} \Big(\sum_{\xi \in k^\times} \Phi(z\xi) \Big)\, \omega(z)\, F_i(|z|_{\mathbf{A}})\, d\mu(\dot{z}),$$

где $\dot{z}$ — образ элемента $z \in k_{\mathbf{A}}^\times$ в $G_k = k_{\mathbf{A}}^\times / k^\times$ и подинтегральное выражение рассматривается как функция от $\dot{z}$. Здесь интегралы для Z_0, Z_1 абсолютно сходятся, если этим свойством обладают исходные интегралы для Z_0, Z_1, т. е. абсолютно сходятся при $\sigma > 1$ в случае Z_1 и при всех σ в случае Z_0.

Для каждого $z \in k_{\mathbf{A}}^\times$ к автоморфизму $x \to z^{-1}x$ группы $k_{\mathbf{A}}$ применима лемма 1 § 2; применяя формулу Пуассона, т. е. формулу (1) из § 2, к функции $x \to \Phi(zx)$, получаем

$$\Phi(0) + \sum_{\xi \in k^\times} \Phi(z\xi) = |z|_{\mathbf{A}}^{-1} \Big(\Phi'(0) + \sum_{\xi \in k^\times} \Phi'(\xi z^{-1}) \Big),$$

следовательно,

$$Z_1 = \int\limits_{G_k} \Big(\sum_{\xi \in k^\times} \Phi'(\xi z^{-1}) + \Phi'(0) - |z|_{\mathbf{A}} \Phi(0) \Big) |z|_{\mathbf{A}}^{-1} \omega(z) F_1(|z|_{\mathbf{A}})\, d\mu(\dot{z}).$$

Но то, что мы доказали для $\mathbf{Z}_0$, остается верным при замене ω на $\omega_1\omega^{-1}$, Φ на Φ' и F_0 на функцию $t \to F_1(t^{-1})$. Обозначая через Z_0' результат этой замены, получаем

$$Z_0' = \int\limits_{\mathbf{A}^\times} \Phi'(z) |z|_{\mathbf{A}} \omega(z)^{-1} F_1(|z_1|_{\mathbf{A}}^{-1})\, d\mu(z),$$

где интеграл абсолютно сходится и голоморфен на всем пространстве $\Omega(G_k)$. Заменим в этом интеграле z на z^{-1}. Тогда мера Хаара μ заменится на меру Хаара $c\mu$, где $c^2 = 1$, поскольку мы имеем дело с автоморфизмом второго порядка группы $k_{\mathbf{A}}^\times$. Следовательно, $c = 1$. После указанной замены переменной снова применим формулу 6 гл. II-4 к $k_{\mathbf{A}}^\times$ и $k^\times$. Это даст

$$Z_0' = \int\limits_{G_k} \Big(\sum_{\xi \in k^\times} \Phi'(\xi^{-1} z^{-1}) \Big) |z|_{\mathbf{A}}^{-1} \omega(z) F_1(|z|_{\mathbf{A}})\, d\mu(\dot{z}),$$

где интеграл опять абсолютно сходится при всех ω. Поскольку $\xi \to \xi^{-1}$ есть биекция группы $k^\times$ на себя, мы видим, что

$$Z_1 - Z_0' = \int\limits_{G_k} (\Phi'(0) - |z|_{\mathbf{A}} \Phi(0)) |z|_{\mathbf{A}}^{-1} \omega(z) F_1(|z|_{\mathbf{A}})\, d\mu(\dot{z}),$$

где интеграл абсолютно сходится при $\sigma > 1$, потому что этим свойством обладают интегралы Z_1 и Z_0'. По следствию 2 предложения 7 § 3 $\omega = \omega_s\psi$, где ψ — характер на G_k, тривиальный на N. В силу нашего определения μ как меры $\mu_1 \times \nu$ на $G_k = G_k' \times N$ последняя формула может быть переписана следующим образом:

$$Z_1 - Z_0' = \Big(\int\limits_{G_k^1} \psi\, d\mu_1 \Big) \cdot \Big(\int\limits_N (\Phi'(0) - n\Phi(0)) n^{s-1} F_1(n)\, d\nu(n) \Big).$$

Первый сомножитель в правой части есть 1 или 0 в зависимости от того, тривиален или нет характер ψ, т. е. является или не является главным квазихарактер ω. Обозначим этот сомножитель через δ_ω. Второй сомножитель можно сразу вычислить с помощью леммы 6. В результате получаем

$$Z_1 - Z_0' = \delta_\omega (\Phi'(0) \lambda(s-1) - \Phi(0) \lambda(s)),$$

где λ — функция, определенная в упомянутой лемме. Поскольку $Z(\omega, \Phi) = Z_0 + Z_1$, нами доказано, что функцию $Z(\omega, \Phi)$ можно продолжить до функции, голоморфной всюду на $\Omega(G_k)$, кроме компоненты связности Ω_1 точки $\omega_0 = 1$, а на этой компоненте — до мероморфной функции, имеющей самое большее те же полюсы, что и функции $\lambda(s-1)$ и $\lambda(s)$. Что касается последних полюсов и их вычетов, то они даются леммой 6 и являются именно такими, как утверждается в теореме.

Наконец, предположим, что мы выбрали F_0, F_1 так, что $F_0(t) = F_1(t^{-1})$ при всех t. Это можно сделать, взяв в качестве F_1 такую непрерывную при $t \geqslant 1$ функцию, что $0 \leqslant F_1(t) \leqslant 1$ при всех $t \geqslant 1$, $F_1(1) = 1/2$ и $F_1(t) = 0$ при $t \geqslant t_1$, и положив $F_1(t) = 1 - F_1(t^{-1})$ при $0 < t < 1$ и $F_0 = 1 - F_1$. При таком выборе имеем $Z_0' = Z_0(\omega_1\omega^{-1}, \Phi')$ и потому

$$Z(\omega, \Phi) = Z_0(\omega, \Phi) + Z_0(\omega_1\omega^{-1}, \Phi') + \delta_\omega(\Phi'(0)\lambda(s-1) - \Phi(0)\lambda(s)).$$

Заменим в этой формуле ω на $\omega_1\omega^{-1}$ и Φ на Φ'. В силу формулы обращения Фурье функция Φ' перейдет при этом в функцию Φ'', для которой $\Phi''(x) = \Phi(-x)$. Так как квазихарактер ω тривиален на $k^\times$, то $\omega(-1) = 1$ и, значит, $\omega(-z) = \omega(z)$ при всех z, так что $Z_0(\omega, \Phi'')$ совпадает с $Z_0(\omega, \Phi)$. Поэтому наша замена приводит просто к перестановке первых двух членов в правой части формулы. Поскольку при этом s заменяется на $1 - s$, то согласно лемме 6 последний член не меняется. Этим завершается вывод «функционального уравнения» в теореме 2.

Следствие 1. *Пусть P — конечное множество точек поля k, содержащее P_∞. Тогда произведение*

$$p(k, P, s) = \prod_{v \notin P} (1 - q_v^{-s})^{-1}$$

абсолютно сходится при $\operatorname{Re}(s) > 1$ и функция $(s-1)\,p(k, P, s)$ стремится при $s \to 1$ к конечному строго положительному пределу.

Первое утверждение содержится в следствии 1 предл. 1 § 1. Далее, возьмем такие же меры Хаара α_v на k_v и μ_v на $k_v^\times$, как и выше. По лемме 5 § 4 для каждой точки v имеем $d\mu_v(x) = m_v |x|_v^{-1} d\alpha_v(x)$, где $m_v > 0$. Возьмем такую стандартную функцию Φ, что Φ_v есть характеристическая функция кольца r_v при всех $v \notin P$, $\Phi_v \geqslant 0$ и $\Phi_v(0) > 0$ при всех v. Применим к $Z(\omega_s, \Phi)$ при $\operatorname{Re}(s) > 1$ предложение 10 § 4. Сомножитель I_v, соответствующий точке v, в правой части этого предложения может быть теперь

записан в виде

$$I_v = m_v \int\limits_{k_v^\times} \Phi_v(x)\,|x|_v^{s-1}\,d\alpha_v(x).$$

При $v \notin P$ согласно предложению 11 § 4 I_v отличается от $(1 - q_v^{-s})^{-1}$ лишь скалярным множителем $\mu_v(r_v^\times)$, который всегда > 0 и который равен 1 почти для всех v. Для $v \in P$, как легко проверить, функция I_v непрерывна при $\mathrm{Re}\,(s) \geqslant 1$ (легко показать, что на самом деле эта функция голоморфна при $\mathrm{Re}\,(s) > 0$, и в следующем параграфе будет получен намного более точный результат при одном специальном выборе Φ, но сейчас нам это не нужно). При $s \to 1$ имеем $I_v \to m_v \int \Phi_v\,d\alpha_v > 0$. Отсюда видно, что функция $Z(\omega_s, \Phi)$ отличается от произведения $p(k, P, s)$ из нашего следствия лишь на множитель, который стремится к конечному положительному пределу при $s \to 1$. С другой стороны, теорема 2 показывает, что $Z(\omega_s, \Phi)$ имеет простой полюс в точке $s = 1$ с вычетом $\rho\Phi'(0)$, где $\rho > 0$. Поскольку $\Phi'(0) = \int \Phi\,d\alpha$ и последний интеграл, очевидно, положителен, наше доказательство закончено.

Следствие 2. *Пусть P — таково, как выше, и пусть ω — такой нетривиальный характер на $k_\mathbf{A}^\times$, тривиальный на $k^\times$, что ω_v неразветвлен для всех $v \notin P$; для таких v положим $\lambda(v) = \omega_v(\pi_v)$, где π_v — простой элемент в k_v. Тогда произведение*

$$p(k, P, \omega, s) = \prod_{v \in P} (1 - \lambda(v)\,q_v^{-s})^{-1}$$

абсолютно сходится при $\mathrm{Re}\,(s) > 1$ и стремится к конечному пределу при $s \to 1$; если характер ω^2 нетривиален, то этот предел отличен от нуля.

Так как ω — характер, то $|\lambda(v)| = 1$ для всех $v \notin P$, так что первое утверждение содержится опять в следствии 1 предл. 1 § 1. Возьмем такие же α_v, μ_v, как и выше, и выберем Φ так, чтобы Φ_v была характеристической функцией кольца r_v при $v \notin P$. Применим к $Z(\omega_s, \omega, \Phi)$ при $\mathrm{Re}\,(s) > 1$ предложение 10 § 4. Сейчас сомножитель I_v имеет вид

$$I_v = m_v \int\limits_{k_v^\times} \Phi_v(x)\,\omega_v(x)\,|x|_v^{s-1}\,d\alpha_v(x).$$

При $v \notin P$ характер ω_v неразветвлен и может быть записан в виде $\omega_v(x) = |x|_v^{s_v}$, где s_v определяется равенством $\lambda(v) = q_v^{-s_v}$. Предло-

жение 11 § 4 показывает, что I_v отличается от $(1-\lambda(v)\,q_v^{-1})^{-1}$ лишь скалярным множителем $\mu_v(r_v^{\times})$, который равен 1 почти для всех v. Как и выше, замечаем, что для $v \in P$ функция I_v непрерывна при $\mathrm{Re}(s) \geqslant 1$. Учитывая для бесконечных точек предложение 9, легко получаем, что для каждой точки $v \in P$ функцию Φ_v можно выбрать так, чтобы $I_v \neq 0$ при $s = 1$; мы будем предполагать, что она так и выбрана (при некоторых специальных выборах Φ_v интеграл I_v будет точно подсчитан в § 7). Мы видим, что функция $Z(\omega_s\omega, \Phi)$ отличается от произведения $p(k, P, \omega, s)$ из нашего следствия лишь множителем, который при $s \to 1$ стремится к конечному, отличному от нуля пределу. Ввиду теоремы 2 этим доказано второе утверждение нашего следствия. Для доказательства последнего утверждения следствия нам понадобится следующая лемма.

Лемма 7. Для $t \in \mathbf{C}$, $\lambda \in \mathbf{C}$ *положим* $\varphi(\lambda, t) = (1-t)^3 \times (1-\lambda t)^4 (1-\lambda^2 t)$. *Тогда* $|\varphi(\lambda, t)| < 1$ *при* $t \in \mathbf{R}$, $0 < t < 1$, $\lambda\bar{\lambda} = 1$.

В самом деле, мы имеем

$$\log|\varphi(\lambda, t)|^2 = \log(\varphi(\lambda, t)\,\varphi(\bar{\lambda}t)) =$$

$$= -\sum_{n=1}^{\infty} \frac{t^n}{n}(6 + 4\lambda^n - 4\bar{\lambda}^n + \lambda^{2n} + \bar{\lambda}^{2n}) =$$

$$= -\sum_{n=1}^{\infty} \frac{t^n}{n}(2 + \lambda^n + \bar{\lambda}^n)^2 < 0.$$

Если теперь функция $\varphi(\lambda, t)$ определена, как в лемме, то $p(k, P, s)^3\, p(k, P, \omega, s)^4\, p(k, P, \omega^2, s) = \prod_{v \notin P} \varphi(\lambda(v)\, q_v^{-s})^{-1}$. Согласно лемме, это произведение по абсолютной величине > 1 при $s \in \mathbf{R}$, $s > 1$, так что оно не может стремиться к 0 при $s \to 1$. При s, стремящемся к 1, как было показано выше, $p(k, P, \omega^2, s)$ стремится к конечному пределу, если характер ω^2 нетривиален, и $p(k, P, \omega, s)$ есть произведение сомножителя, стремящегося к отличному от нуля конечному пределу, и функции $Z(\omega_s\omega, \Phi)$, которая голоморфна в некоторой окрестности точки $s = 1$. Поэтому если $p(k, \omega, P, s)$ стремится к нулю, то эта функция должна иметь вид $F(s)(s-1)$, где функция F ограничена. Ввиду следствия 1 отсюда следует, что левая часть последней формулы стремится к нулю при $s \to 1$, чем и заканчивается наше доказательство.

Отметим тот важный факт, что заключение нашего следствия остается справедливым даже для $\omega^2 = 1$; доказательство этого

факта, которое потребует совершенно других методов, будет дано в гл. XIII-12.

Следствие 3. *Пусть k_0 — некоторое* А-*поле, содержащееся в k, и пусть V — такое множество конечных точек поля k, что почти для всех конечных точек $v \notin V$ поля k модулярная степень поля k_v над замыканием поля k_0 в k_v больше единицы. Тогда произведение*

$$q(k, V, s) = \prod_{v \notin V} (1 - q_v^{-s})^{-1}$$

абсолютно сходится при $\mathrm{Re}\,(s) > 1$ *и функция* $(s-1)\,q(k, V, s)$ *стремится при* $s \to 1$ *к конечному строго положительному пределу.*

В самом деле, в обозначениях следствия 1 $p(k, P_\infty, s)$ есть произведение нашего произведения $q(k, V, s)$ на аналогичное произведение, взятое по множеству M всех конечных точек v поля k, не лежащих в V. Применяя к последнему произведению следствие 3 предл. 1 § 1, а к $p(k, P_\infty, s)$ — следствие 1, немедленно получаем наше утверждение. Разумеется, из нашего следствия вытекает, что множество V не может быть конечным, другими словами, что существует бесконечно много точек v поля k, для которых соответствующая модулярная степень равна единице.

Следствие 4. *Пусть k_0 и V таковы, как в следствии* 3, *и пусть k' — сепарабельное алгебраическое расширение поля k конечной степени n. Предположим, что над каждой точкой $v \in V$ существует n различных точек поля k'. Тогда $k' = k$.*

Обозначим через V' множество точек поля k', лежащих над точками из V. По следствию 1 теор. 4 гл. III-4, если $v \in V$ и w лежит над v, то $k'_w = k_v$, следовательно $q'_w = q_v$. Для любой точки v поля k и любой лежащей над v точки w поля k' модулярная степень k'_w над замыканием поля k_0 в k_v не меньше модулярной степени поля k_v над этим замыканием. Поэтому почти для всех $v \notin V$, или, что то же самое, почти для всех $w \notin V'$, модулярная степень > 1. Теперь мы можем применить следствие 3 к произведениям $q(k, V, s)$ и $q(k', V', s)$. Так как последнее произведение равно $q(k, V, s)^n$, мы получаем $n = 1$.

Следствие 5. *Пусть k — некоторое* А-*поле характеристики $p > 1$ и P — конечное множество точек поля k. Тогда существует такой дивизор $\mathfrak{m} = \sum m(v) \cdot v$ степени* 1 *поля k, что $m(v) = 0$ при всех $v \in P$.*

Обозначим через ν наибольший общий делитель степеней всех точек v, не лежащих в P. Нам надо показать, что $\nu = 1$. Пусть $F = \mathbf{F}_q$ — поле констант поля k. По теореме 2 гл. I-1 в алгебраическом замыкании поля k существует поле F' из q^ν элементов и это поле сепарабельно над F. Обозначим через k' композит полей k и F' и через n его степень над k; поле k' сепарабельно над k. Пусть v — произвольная точка поля k, не лежащая в P, и w — некоторая точка поля k', лежащая над v. По предложению 1 гл. III-1 k'_w порождается над k_v полем k', а следовательно, и полем F'. По определению числа ν модуль поля k_v имеет вид $q^{\nu r}$, где r — целое число. Поэтому из следствия 1 теор. 7 гл. I-4 в сочетании со следствием 2 теор. 2 гл. I-1 вытекает, что k_v содержит подполе из q^ν элементов. По теореме 2 гл. I-1 k'_w не может содержать более одного поля из q^ν элементов. Поэтому $F' \subset k_v$ и, значит, $k'_w = k_v$. Следствие 1 теор. 4 гл. III-4 показывает теперь, что над каждой не лежащей в P точкой v поля k имеется n различных точек поля k'. Полагая в следствии 4 $k_0 = k$ и беря в качестве V дополнение множества P, получаем $k' = k$ и, следовательно, $F' \subset F$, т. е. $\nu = 1$.

Следствие 6. *Пусть поле k таково, как в следствии* 5, *и $\mathbf{F}_q$ — его поле констант. Тогда группа N значений нормы $|z|_\mathbf{A}$ на $k_\mathbf{A}^\times$ порождается элементом q.*

Как мы видели в § 4, N порождается группами значений норм $|x|_v$ на $k_v^\times$, а следовательно, модулями $q_v = q^{\deg(v)}$ при всех v. Поэтому она имеет образующую $Q = q^\nu$, где ν — наибольший общий делитель всех степеней $\deg(v)$. По следствию 5 $\nu = 1$.

Учитывая следствие 6, можно следующим образом переформулировать последнее утверждение теоремы 2 в случае характеристики $p > 1$.

Следствие 7. *Пусть k и $\mathbf{F}_q$ таковы, как в следствии* 6, *и обозначения таковы, как в теореме* 2. *Тогда функция $Z(\omega_s, \Phi) + \Phi(0)(1 - q^{-s})^{-1}$ голоморфна в точке $s = 0$.*

Это сразу следует из только что упомянутых результатов и того факта, что функция $(1 - q^{-s})^{-1}$ имеет в точке $s = 0$ вычет $(\log q)^{-1}$.

§ 6. ДЕДЕКИНДОВА ДЗЕТА-ФУНКЦИЯ

Специальный выбор функции Φ в $Z(\omega, \Phi)$ приводит к определению важных функций на компонентах связности пространства $\Omega(G_k)$; сейчас эти функции будут подробно исследованы. Мы начнем с рассмотрения компоненты связности Ω_1 точки $\omega_0 = 1$ в $\Omega(G_k)$,

т. е. группы главных квазихарактеров на G_k. Функцию Φ выберем следующим образом. Для любой конечной точки v поля k возьмем в качестве Φ_v характеристическую функцию кольца r_v. В случае когда точка v вещественна, т. е. $k_v = \mathbf{R}$, возьмем $\Phi_v(x) = \exp(-\pi x^2)$. В случае когда точка v мнима, т. е. $k_v = \mathbf{C}$, возьмем $\Phi_v(x) = \exp(-2\pi x\bar{x})$. Теперь нам следует вычислить сомножители в произведении (5) для $Z(\omega, \Phi)$ при сделанном выборе Φ и при $\omega = \omega_s$. Для конечных точек v значения этих сомножителей даются предложением 11 § 4 с точностью до скалярного множителя, зависящего от μ. Для бесконечных точек эти сомножители таковы.

Лемма 8. *Пусть G_1, G_2 определены для всех $s \in \mathbf{C}$ формулами*

$$G_1(s) = \pi^{-s/2}\,\Gamma(s/2), \quad G_2(s) = (2\pi)^{1-s}\,\Gamma(s).$$

Тогда при $\mathrm{Re}(s) > 0$ *имеем*

$$\int_{\mathbf{R}^\times} \exp(-\pi x^2)\,|x|^{s-1}\,dx = G_1(s),$$

$$\int_{\mathbf{C}^\times} \exp(-2\pi x\bar{x})\,(x\bar{x})^{s-1}\,|dx \wedge d\bar{x}| = G_2(s).$$

Это сразу становится видно, если сделать очевидную замену переменных, а именно $|x| = t^{1/2}$ в первом интеграле и $x = t^{1/2}\mathbf{e}(u)$ во втором, где $t \in \mathbf{R}_+^\times$, $u \in \mathbf{R}$, $0 \leqslant u < 1$; в последнем случае $|dx \wedge d\bar{x}| = 2\pi\,dt\,du$.

Рассмотрим теперь меру $\gamma = \prod \gamma_v$ на $k_\mathbf{A}^\times$, где γ_v таковы, что $\gamma_v(r_v^\times) = 1$ для каждой конечной точки v, $d\gamma_v(x) = |x|^{-1}\,dx$, если точка v вещественна, и $d\gamma_v(x) = (x\bar{x})^{-1}\,|dx \wedge d\bar{x}|$, если точка v мнима. Для поля k характеристики нуль эта мера уже рассматривалась в предложении 9 гл. V-4. Соотношение между мерой γ и мерой μ, введенной в начале § 5, таково.

Предложение 12. *Пусть мера μ такая, как в* § 5, *а мера γ такая, как выше. Если характеристика поля k равна нулю, то $\gamma = c_k\mu$, где c_k — число, определенное в предложении* 9 *гл.* V-4. *Если k — поле характеристики $p > 1$ с полем констант $\mathbf{F}_q$ и h — число классов дивизоров степени* 0 *поля k, то $\gamma = c_k\mu$, где $c_k = h/(q-1)$.*

Ввиду нашего определения меры μ первое утверждение есть просто переформулировка предложения 9 гл. V-4. Пусть теперь

характеристика поля k равна $p > 1$. Положим $U = \prod r_v^\times$. Эта группа обозначалась в гл. IV-4 через Ω ($\varnothing$); это открытая подгруппа в $k_\mathrm{A}^\times$. По определению $\gamma(U) = 1$. Как и в гл. II-4, будем обозначать по-прежнему через γ образ меры γ в $G_k = k_\mathrm{A}^\times/k^\times$. Если, как и выше, G_k^1 — образ в G_k группы k_A^1, то мера μ определяется условием $\mu(G_k^1) = 1$, так что $\gamma = c_k\mu$, где $c_k = \gamma(G_k^1)$. Обозначим через U' образ в G_k группы U. По теореме 8 гл. IV-4 и ее следствию ядро морфизма группы U на U', индуцированного каноническим морфизмом группы $k_\mathrm{A}^\times$ на G_k, совпадает с $\mathbf{F}_q^\times$, так что мы можем подсчитать $\gamma(U')$, положив в лемме 2 гл. II-4 $G = U$, $\Gamma_1 = \mathbf{F}_q^\times$, $\Gamma = \{1\}$. Это дает $\gamma(U') = (q-1)^{-1}$. Ясно, что индекс подгруппы U' в G_k^1 равен индексу подгруппы $k^\times U$ в k_A^1. Но, как мы видели в гл. VI, группу $k_\mathrm{A}^1/k^\times U$ можно отождествить с группой $D_0(k)/P(k)$ классов дивизоров степени 0 поля k, поэтому наш индекс равен h. Следовательно, $\gamma(G_k^1) = h/(q-1)$.

Для каждой бесконечной точки w поля k положим $G_w = G_1$, если эта точка вещественна, и $G_w = G_2$, если она мнима. Комбинируя предложение 10 § 4, предложение 11 § 4, лемму 8 и предложение 12, мы получаем, что при $\mathrm{Re}(s) > 1$ для функции Φ, выбранной, как указано выше, имеет место равенство

$$Z(\omega_s, \Phi) = c_k^{-1} \prod_{w \in P_\infty} G_w(s) \prod_{v \notin P_\infty} (1 - q_v^{-s})^{-1}, \tag{6}$$

где c_k те же, что в предложении 12. По теореме 2 § 5 левую часть можно продолжить до функции, мероморфной на всей s-плоскости. Поскольку то же самое можно сделать для сомножителей G_w, последнее произведение в правой части также можно продолжить до функции, мероморфной на всей s-плоскости. Этим оправдано следующее определение.

Определение 8. *Мероморфная функция ζ_k на s-плоскости, задаваемая при $\mathrm{Re}(s) > 1$ произведением*

$$\zeta_k(s) = \prod_v (1 - q_v^{-s})^{-1},$$

взятым по всем конечным точкам v поля k, называется дедекиндовой дзета-функцией поля k.

Если функция Φ такова, как выше, то ее преобразование Фурье Φ' немедленно дается теоремой 1 § 2 и ее следствием 2 в сочетании со следствием 3 предложения 2 § 2 и предложениями 4 и 5 § 2. А именно

$$\Phi'(y) = |a|_\mathrm{A}^{1/2} \Phi(ay),$$

где a — дифферентный идель, связанный с базисным характером χ. Ввиду определения функции $Z(\omega, \Phi)$ (формула (4) § 4) имеем

$$Z(\omega, \Phi') = |a|_{\mathbf{A}}^{1/2} \omega(a)^{-1} Z(\omega, \Phi);$$

в частности, при $\omega = \omega_s$, т. е. в случае $\omega(x) = |x|_{\mathbf{A}}^s$, получаем

$$Z(\omega_s, \Phi') = |a|_{\mathbf{A}}^{1/2-s} Z(\omega_s, \Phi), \tag{7}$$

причем значение $|a|_{\mathbf{A}}$ дается предложением 6 § 2.

Теперь мы подготовлены к формулировке наших основных результатов о дзета-функции.

Т е о р е м а 3. *Пусть k — некоторое поле алгебраических чисел с r_1 вещественными точками и r_2 мнимыми точками. Обозначим через ζ_k дзета-функцию этого поля и положим*

$$Z_k(s) = G_1(s)^{r_1} G_2(s)^{r_2} \zeta_k(s).$$

Тогда Z_k является мероморфной функцией на s-плоскости, голоморфной всюду, кроме точек $s = 0$ и $s = 1$, в которых у нее простые полюсы, и имеет место функциональное уравнение

$$Z_k(s) = |D|^{\frac{1}{2}-s} Z_k(1-s),$$

где D — дискриминант поля k. Вычеты функции Z_k в точках $s = 0$ и $s = 1$ равны соответственно — c_k и $|D|^{-1/2} c_k$, где

$$c_k = 2^{r_1} (2\pi)^{r_2} hR/e;$$

здесь h — число классов идеалов поля k, R — его регулятор и e — число корней из 1 в k.

Эта теорема немедленно следует из формул (6) и (7), предложения 6 § 2 и теоремы 2 § 5.

С л е д с т в и е. *Дедекиндова дзета-функция $\zeta_k(s)$ имеет в точке $s = 1$ вычет $|D|^{-1/2} c_k$.*

Это следует из теоремы 3 и хорошо известного равенства $G_1(1) = G_2(1) = 1$.

Т е о р е м а 4. *Пусть k — некоторое А-поле характеристики $p > 1$, $\mathbf{F}_q$ — его поле констант и g — его род. Тогда его дзета-функция может быть записана в виде*

$$\zeta_k(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})},$$

где P — многочлен степени $2g$ с коэффициентами в $\mathbf{Z}$, для которого

$$P(u) = q^g u^{2g} P(1/qu). \tag{8}$$

Кроме того, $P(0) = 1$, *а* $P(1)$ *равно числу* h *классов дивизоров степени* 0 *поля* k.

В самом деле, следствие 6 теоремы 2 § 5 показывает, что морфизм $s \to \omega_s$ имеет то же самое ядро, что и морфизм $s \to q^{-s}$, так что функция $\zeta_k(s)$ может быть записана в виде $R(q^{-s})$, где R — мероморфная на $\mathbf{C}^\times$ функция с простыми полюсами в 1 и в q^{-1}. Далее, следствие 1 предложения 1 § 1 показывает, что $R(u) \to 1$ при $u \to 0$, так что функция R голоморфна в этой точке и $R(0) = 1$. Поэтому можно записать $R(u) = P(u)/(1-u)(1-qu)$, где P — целая функция на u-плоскости и $P(0) = 1$. Теперь формула (7) в сочетании с формулой (6) и предложением 6 § 2 дает формулу (8) нашей теоремы, из которой очевидно следует, что P является многочленом степени $2g$. Наконец, следствие 7 теоремы 2 § 5 вместе с предложением 12 дает $P(1) = h$.

§ 7. L-ФУНКЦИИ

Сейчас мы обобщим полученные выше результаты на случай произвольного квазихарактера на G_k. Для этого примем следующие обозначения. Пусть ω — любой квазихарактер на G_k. Как мы видели в § 3—4, $|\omega| = \omega_\sigma$, где $\sigma \in \mathbf{R}$. Для каждой точки v обозначим через ω_v квазихарактер на $k_v^\times$, индуцированный квазихарактером ω. Для каждой конечной точки v обозначим через $p_v^{f(v)}$ ведущий идеал квазихарактера ω_v; при этом $f(v) = 0$ в том и только в том случае, когда ω_v неразветвлен, что, как мы видели в § 4, имеет место почти для всех конечных точек поля k. Для неразветвленного ω_v запишем $\omega_v(x) = |x|_v^{s_v}$, где $s_v \in \mathbf{C}$. Очевидно, $\mathrm{Re}(s_v) = \sigma$. К бесконечным точкам поля k применимо предложение 9 § 3, которое показывает, что ω_v можно записать в виде $\omega_v(x) = x^{-A}|x|^{s_v}$ в случае вещественной точки v, где $A = 0$ или 1 и $s_v \in \mathbf{C}$, и в виде $\omega_v(x) = x^{-A}\bar{x}^{-B}(x\bar{x})^{s_v}$ в случае мнимой точки v, где $\inf(A, B) = 0$ и $s_v \in \mathbf{C}$. В первом случае положим $N_v = A$, так что $\mathrm{Re}(s_v) = N_v + \sigma$, а во втором случае положим $N_v = \sup(A, B)$, так что $\mathrm{Re}(s_v) = (N_v/2) + \sigma$. Поскольку компонента связности квазихарактера ω в группе $\Omega(G_k)$ всех квазихарактеров на G_k состоит из квазихарактеров $\omega_s\omega$, $s \in \mathbf{C}$, то целые числа $f(v)$ и N_v постоянны на этой компоненте. Они все равны нулю, если ω — главный квазихарактер или, более общим образом, когда ω тривиален на группе U тех иделей (z_v), для которых $|z_v|_v = 1$ для всех точек v поля k. Структура группы квазихарактеров, обладающих таким свойством, легко определяется с помощью методов, использованных при доказательстве теоремы 9 гл. IV-4.

Далее, применяя те же самые обозначения, что и выше, сопоставим каждому ω некую стандартную функцию $\Phi_\omega = \prod \Phi_v$ на k_A, определенную следующим образом. Для каждой конечной точки v, для которой $f(v) = 0$, т. е. квазихарактер ω_v неразветвлен, возьмем в качестве Φ_v, как и прежде, характеристическую функцию кольца r_v. Для каждой конечной точки v, для которой $f(v) \geqslant 1$, положим функцию Φ_v равной ω_v^{-1} на $r_v^\times$ и нулю вне $r_v^\times$. Для каждой бесконечной точки v возьмем $\Phi_v(x) = x^A \exp(-\pi x^2)$, если эта точка вещественна, и $\Phi_v(x) = x^A \bar{x}^{-B} \exp(2\pi x\bar{x})$, если она мнима, где целые числа A, B такие, как сказано выше. Определенную таким образом функцию Φ_ω будем называть *стандартной функцией, связанной с* ω. Ясно, что она не меняется при замене ω на $\omega_s\omega$ с любым $s \in \mathbf{C}$ и что функцией, связанной с $\bar{\omega}$, с $\omega^{-1} = \omega_{-2\sigma}\bar{\omega}$ и с $\omega' = \omega_1\omega^{-1}$, будет одна и та же функция $\bar{\Phi}_\omega$.

Нам нужно знать преобразование Фурье от Φ_ω, или, что ввиду теоремы 1 § 2 то же самое, преобразования Фурье функций Φ_v, определенных выше. Для вычисления этих преобразований достаточно полученных ранее результатов, за исключением случая конечной точки v с разветвленным ω_v. Для этого случая докажем следующее

Предложение 13. *Пусть K — некоторое p-поле, R — его максимальное компактное подкольцо, P — максимальный идеал в R и ω — квазихарактер на $K^\times$ с ведущим идеалом P^f, где $f \geqslant 1$. Пусть, далее, χ — характер порядка ν на K, α — самодвойственная мера на K, соответствующая характеру χ, $b \in K^\times$, $\operatorname{ord}_K(b) = \nu + f$, и пусть φ — функция на K, равная ω^{-1} на $R^\times$ и нулю вне $R^\times$. Тогда преобразованием Фурье функции φ является функция*

$$\varphi'(y) = \varkappa \bmod_K (b)^{1/2} \overline{\varphi(by)},$$

где $\varkappa$ — комплексное число, удовлетворяющее условию $\varkappa\bar{\varkappa} = 1$ и задаваемое формулой

$$\varkappa = \bmod_K (b)^{-1/2} \int_{R^\times} \omega(x)^{-1} \chi(b^{-1}x)\, d\alpha(x).$$

По предложению 12 гл. II-5 K-решетка P^f двойственна к $P^{-f-\nu}$. Так как функция φ постоянна на классах смежности в K по модулю P^f, то предложение 2 § 2 показывает, что φ' равна нулю вне $P^{-f-\nu} = b^{-1}R$. По определению φ имеем

$$\varphi'(y) = \int_{R^\times} \omega(x)^{-1} \chi(xy)\, d\alpha(x). \tag{9}$$

Очевидно, что мера, индуцированная на $R^\times$ мерой α, является мерой Хаара на $R^\times$ (это следует также из леммы 5 § 4). Возьмем элемент y, для которого $\mathrm{ord}_K(y) \geqslant -f-\nu+1$. Тогда по предложению 12 гл. II-5 функция $x \to \chi(xy)$ постоянна на классах смежности по модулю P^{f-1}. Предположим сначала, что $f=1$. Тогда $\chi(xy)=1$ на R, так что (9) есть интеграл по $R^\times$ от $\omega^{-1}\,d\alpha$; этот интеграл равен нулю, потому что ω является нетривиальным характером на компактной группе $R^\times$. Предположим теперь, что $f>1$. Тогда интеграл (9) является суммой аналогичных интегралов, взятых по классам смежности по модулю P^{f-1}, содержащимся в $R^\times$, т. е. по классам смежности в $R^\times$ по подгруппе $1+P^{f-1}$. Поскольку из определения ведущего идеала следует, что квазихарактер ω нетривиален на подгруппе $1+P^{f-1}$, то по той же причине, что и раньше, получаем снова, что $\varphi'(y)=0$ в рассматриваемом случае. Теперь возьмем в (9) $y=b^{-1}u$, где $u \in R^\times$. Заменяя $u^{-1}x$ на x, получаем $\varphi'(b^{-1}u)=\omega(u)\,\varphi'(b^{-1})$. Этим доказано, что φ' имеет вид $c\overline{\varphi(by)}$, где $c \in \mathbf{C}^\times$. Применяя формулу обращения Фурье и лемму 1 § 2, получаем $c\bar{c}=\mathrm{mod}_K(b)$. Поскольку $c=\varphi'(b^{-1})$, для $\varkappa$ имеет место формула из формулировки предложения. Равенство $\varkappa\bar{\varkappa}=1$ для $\varkappa$, определенного этой формулой, легко проверяется непосредственно. Заметим еще, что поскольку подинтегральная функция постоянна на классах смежности в R по модулю P^f, то наш интеграл можно переписать как некоторую сумму по R/P^f. Такого типа суммы известны как *гауссовы суммы*.

Предложение 14. *Пусть ω — квазихарактер на G_k и Φ_ω — стандартная функция, связанная с ω. Тогда преобразование Фурье функции Φ_ω, соответствующее базисному характеру χ на $k_\mathbf{A}$, определяется формулой*

$$\Phi'(y)=\varkappa\,|\,b\,|_\mathbf{A}^{1/2}\overline{\Phi_\omega(by)}=\varkappa\,|\,b\,|_\mathbf{A}^{1/2}\Phi_{\bar{\omega}}(by),$$

где $\varkappa=\prod\varkappa_v$, $\varkappa_v \in \mathbf{C}$, $\varkappa_v\bar{\varkappa}_v=1$ при всех v, $b=(b_v) \in k_\mathbf{A}^\times$ и $\varkappa_v$, b_v задаются следующим образом. Пусть $a=(a_v)$ — дифферентный идель, связанный с χ; тогда $b_v=a_v$ для всякой бесконечной точки v и $\mathrm{ord}_v(b_v a_v^{-1})=f(v)$ для всякой конечной точки v поля k. Для каждой бесконечной точки v поля k имеем $\varkappa_v=i^{-N_v}$, для каждой конечной точки v, в которой $f(v)=0$, $\varkappa_v=1$, для остальных точек

$$\varkappa_v=|\,b_v\,|_v^{-1/2}\int\limits_{r_v^\times}\omega_v(x)^{-1}\chi_v(b_v^{-1}x)\,d\alpha_v(x),$$

где α_v — самодвойственная мера Хаара на k_v, связанная с характером χ_v.

Это немедленно следует из предложения 13, предложений 4 и 5 § 2 и следствия 3 предложения 2 § 2.

Следствие. *Пусть квазихарактер* ω *таков, как в предложении* 14. *Положим* $\omega' = \omega_1\omega^{-1}$. *Тогда* $Z(\omega, \Phi_\omega) = \varkappa \mid b \mid_{\mathbf{A}}^{-1/2} \times$ $\times\ \omega(b)\, Z(\omega', \Phi_{\omega'})$.

Согласно теореме 2 § 5, $Z(\omega, \Phi_\omega) = Z(\omega', \Phi')$ при всех ω, где функция Φ' такова, как в предложении 14. Выразим $Z(\omega', \Phi')$ как интеграл (4) § 4, в предположении, что этот интеграл сходится; сразу видно, что это предположение выполняется при $\sigma < 0$. Представляя Φ', как в предложении 14, и производя в интеграле замену переменной $z \to b^{-1}z$, получаем правую часть формулы нашего следствия. По теореме 2 § 5 обе части можно продолжить аналитически на всю компоненту связности квазихарактера ω в $\Omega(G_k)$, так что результат справедлив всюду.

Применим теперь к $Z(\omega, \Phi_\omega)$ предложение 10 § 4. При $\sigma > 1$ это даст нам бесконечное произведение, все сомножители которого известны, за исключением сомножителей, соответствующих тем точкам v поля k, для которых $f(v) > 0$. Что касается таких сомножителей, то при нашем выборе Φ_v они, очевидно, равны $\mu_v(r_v^\times)$. Положим, как в § 6, $G_w = G_1$ в случае вещественной точки и $G_w = G_2$ в случае мнимой точки w. Учитывая предложение 11 § 4, лемму 8 § 6 и предложение 12 § 6, получаем, что при $\sigma > 1$

$$Z(\omega, \Phi_\omega) = c_k^{-1} \prod_{w \in P_\infty} G_w(s_w) \prod_{v \notin P} (1 - q_v^{-s_v})^{-1}, \tag{10}$$

где P — множество, состоящее из всех бесконечных точек и тех конечных точек v, для которых $f(v) > 0$.

Для каждой точки v поля k, не принадлежащей к только что определенному множеству P, положим $\lambda(v) = q_v^{-s_v}$. Таким образом, мы определили $\lambda(v)$ для тех конечных точек, в которых квазихарактер ω_v неразветвлен. По определению чисел s_v для таких точек можно записать $\lambda(v) = \omega_v(\pi_v)$, где π_v — простой элемент поля k_v, или $\lambda(v) = \omega(\pi_v)$, если считать группу $k_v^\times$ вложенной как квазисомножитель в $k_{\mathbf{A}}^\times$. Ясно, что $|\lambda(v)| = q_v^{-\sigma}$.

Заменим теперь в (10) ω на $\omega_s\omega$, где $s \in \mathbf{C}$. При этом, как отмечалось выше, Φ_ω не изменится, а правая часть равенства (10) перейдет в произведение, которое абсолютно сходится при $\mathrm{Re}(s) > 1 - \sigma$. Теорема 2 § 5 показывает, что функцию $Z(\omega_s\omega, \Phi_\omega)$ можно аналитически продолжить на всю s-плоскость (как голоморфную функцию, если квазихарактер ω не главный). То же самое верно для

сомножителей G_w, $w \in P_\infty$. Поэтому мы можем ввести мероморфную функцию $L(s, \omega)$, задаваемую при $\mathrm{Re}\,(s) > 1 - \sigma$ произведением

$$L(s, \omega) = \prod_v (1 - \lambda(v)\, q_v^{-s})^{-1}, \tag{11}$$

взятым по всем конечным точкам v, в которых ω_v неразветвлен.

Для формулировки нашего конечного результата в случае характеристики нуль введем в рассмотрение идеал $\mathfrak{f} = \prod \mathfrak{p}_v^{f(v)}$ в $\mathfrak{r}$. Он называется *ведущим идеалом квазихарактера* ω.

Теорема 5. *Пусть k — некоторое поле алгебраических чисел и ω — неглавный квазихарактер на $G_k = k_\mathbf{A}^\times / k^\times$ с ведущим идеалом $\mathfrak{f}$. Тогда функция*

$$\Lambda(s, \omega) = \prod_{w \in P_\infty} G_w(s + s_w) \cdot L(s, \omega)$$

является целой функцией от s и удовлетворяет функциональному уравнению

$$\Lambda(s, \omega) = \varkappa\omega(b)\,(|D|\,\mathfrak{N}(\mathfrak{f}))^{\frac{1}{2}-s}\,\Lambda(1-s, \omega^{-1}),$$

где $\varkappa$ и b такие, как в предложении 14.

Это непосредственно вытекает из следствия предложения 14, если заменить ω на $\omega_s\omega$ и учесть определения a, b, $\mathfrak{f}$ и тот факт, что $|a|_\mathbf{A} = |D|^{-1}$. Как хорошо известно, $\Gamma(s)^{-1}$ есть целая функция, поэтому то же верно для функций $G_w(s + s_w)^{-1}$, и из теоремы 5 следует, что $L(s, \omega)$ является целой функцией от s.

Как вытекает из их определения, введенные выше функции не зависят по существу от выбора ω в заданной компоненте связности пространства $\Omega(G_k)$. Более точно, они не зависят от такого выбора с точностью до трансляции в s-плоскости, поскольку для любого $t \in \mathbf{C}$ функция $L(s, \omega_t\omega)$ совпадает с $L(s + t, \omega)$ и аналогичное утверждение справедливо для $\Lambda(s, \omega)$. Поэтому ввиду следствия 2 предложения 7 § 3 всегда можно считать, заменяя, если необходимо, ω на $\omega_{-t}\omega$ с $t \in \mathbf{C}$, что ω является характером на $k_\mathbf{A}^\times$, тривиальным на $k^\times$, а также на группе M, определенной в следствии 2 теор. 5 гл. IV-4. Последнее предположение можно записать так: $\sum (\delta_v s_v - N_v) = 0$, где сумма берется по бесконечным точкам поля k, s_v и N_v таковы, как выше, а $\delta_v = 1$ или 2 соответственно тому, $k_v = \mathbf{R}$ или $\mathbf{C}$. Отсюда следует, что ω является характером и, значит, $\sigma = 0$.

С другой стороны, если k — поле характеристики $p > 1$, то введем дивизор $\mathfrak{f} = \sum f(v) \cdot v$ и назовем его *ведущим дивизором для* ω.

Теорема 6. *Пусть k — некоторое* **A***-поле характеристики $p > 1$, $\mathbf{F}_q$ — его поле констант, g — его род и ω — неглавный квазихарактер на $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$ с ведущим дивизором $\mathfrak{f}$. Тогда $L(s, \omega) = P(q^{-s}, \omega)$, где $P(u, \omega)$ — многочлен степени $2g - 2 + \deg(\mathfrak{f})$ от u и*

$$P(u, \omega) = \varkappa\omega(b) \cdot (q^{1/2}u)^{2g-2+\deg(\mathfrak{f})} \cdot P(1/qu, \omega^{-1}),$$

где $\varkappa$ и b такие, как в предложении 14.

Тот факт, что $L(s, \omega) = P(q^{-s}, \omega)$, где функция $P(u, \omega)$ голоморфна на всей u-плоскости, доказывается точно так же, как соответствующий факт в теореме 4. Последняя формула нашей теоремы непосредственно вытекает теперь из следствия предложения 14, если заменить там ω на $\omega_s\omega$ и учесть определения a, b, $\mathfrak{f}$ и тот факт, что $|a|_{\mathbf{A}} = q^{2-2g}$. Эта формула показывает, что $P(u, \omega)$ является многочленом нужной степени.

Отметим здесь снова, что для $t \in \mathbf{C}$ функция $P(u, \omega_t\omega)$ совпадает с $P(q^{-t}u, \omega)$. Учитывая следствие 6 теор. 2 § 5, имеем $k_{\mathbf{A}}^{\times} = k_{\mathbf{A}}^{1} \times M$, где M — подгруппа в $k_{\mathbf{A}}^{\times}$, порожденная элементом z_1 с $|z_1|_{\mathbf{A}} = q$, т. е. таким элементом z_1, что $\operatorname{div}(z_1)$ имеет степень -1. Следствие 2 предл. 7 § 3 показывает, что, заменив, если необходимо, ω на $\omega_{-t}\omega$ с подходящим $t \in \mathbf{C}$, можно считать, что $\omega(z_1) = 1$. Это же следствие показывает поэтому, что ω есть характер на $k_{\mathbf{A}}^{\times}$, т. е. $\sigma = 0$. Кроме того, сопоставляя этот факт с леммой 4 § 3 и тем очевидным обстоятельством, что в рассматриваемом сейчас случае группа $k_{\mathbf{A}}^{\times}$, а значит, и группы $k_{\mathbf{A}}^{1}$, G_k, G_k^1 вполне несвязны, убеждаемся, что ω является характером конечного порядка на $k_{\mathbf{A}}^{\times}$.

§ 8. КОЭФФИЦИЕНТЫ L-РЯДОВ

Пусть задано эйлерово произведение типа стоящего в правой части равенства (11). Возникает вопрос, можно ли его получить, исходя из некоторого квазихарактера ω на $k_{\mathbf{A}}^{\times}/k^{\times}$. Ответ на этот вопрос, а также на несколько более общий вопрос, который будет вскоре поставлен, вытекает из следующего результата.

Предложение 15. *Пусть P — конечное множество точек поля k, содержащее P_∞, и пусть G_P — подгруппа в $k_{\mathbf{A}}^{\times}$, состоящая из тех иделей (z_v), для которых $z_v = 1$ при всех $v \in P$. Тогда подгруппа $k^{\times}G_P$ плотна в $k_{\mathbf{A}}^{\times}$.*

Положим $k_P = \coprod k_v$, где произведение берется по $v \in P$. Обозначим через A_P подгруппу в $k_\mathbf{A}$, состоящую из аделей (x_v), для которых $x_v = 0$ при всех $v \in P$. Тогда $k_\mathbf{A} = k_P \times A_P$, $k_\mathbf{A}^\times = k_P^\times \times \times G_P$, и наше утверждение состоит в том, что проекция из $k_\mathbf{A}^\times$ на $k_P^\times$ отображает $k^\times$ на всюду плотную подгруппу в $k_P^\times$. Но действительно $k_P^\times$ является открытым подмножеством в k_P и его топология индуцирована топологией из k_P. Наше утверждение немедленно вытекает поэтому из следствия 2 теор. 3 гл. IV-2, которое показывает, что проекция из $k_\mathbf{A}$ на k_P отображает k на всюду плотное подмножество в k_P.

Из предложения 15 сразу следует, что непрерывное представление ω группы $k_\mathbf{A}^\times$ в любую группу Γ, тривиальное на $k^\times$, однозначно определено, если почти для всех v известны его значения на группах $k_v^\times$. В частности, в случае когда $\Gamma = \mathbf{C}^\times$ или в том более общем случае, когда группа Γ такова, что каждый морфизм $k_\mathbf{A}^\times \to \Gamma$ тривиален на $r_v^\times$ почти для всех v, представление ω однозначно определено, если почти для всех v заданы значения $\omega(\pi_v)$. Ясно, что всякая конечная группа обладает таким свойством, потому что ядро каждого морфизма из $k_\mathbf{A}^\times$ в конечную группу открыто в $k_\mathbf{A}^\times$ и, следовательно, содержит $\coprod_{v \notin P} r_v^\times$ при некотором P. По тем же самым причинам, что и для $\mathbf{C}^\times$, тем же свойством обладает всякая группа Γ, не содержащая произвольно малых подгрупп. Другой интересный случай представлен следующим предложением.

Предложение 16. *Пусть K — некоторое p-поле, и пусть характеристика поля k не равна p. Тогда каждый морфизм $\omega: k_\mathbf{A}^\times \to K^\times$ тривиален на $r_v^\times$ почти для всех v и локально постоянен на $k_v^\times$, если k_v не является p-полем.*

Так как характеристика поля k не равна p, то $|p|_v = 1$ почти для всех v, а для точек v, удовлетворяющих этому условию, поле k_v не является p-полем. Поскольку каждый морфизм связной группы во вполне несвязную, очевидно, тривиален, то ω тривиален на $k_v^\times$, если $k_v = \mathbf{C}$, и на $\mathbf{R}_+^\times$, если $k_v = \mathbf{R}$. Обозначим через R максимальное компактное подкольцо в K и через P — его максимальный идеал. Пусть v — любая конечная точка поля k, для которой k_v не является p-полем, и пусть $m \geqslant 1$ таково, что ω отображает $1 + p_v^m$ в $1 + P$. Согласно предложению 8 гл. II-3, для любого $n \geqslant 0$ каждый элемент $z \in 1 + p_v^m$ можно записать в виде $z' {}^{p^n}$, где $z' \in 1 + p_v^m$, поэтому $\omega(z) \in (1 + P)^{p^n}$, а следовательно,

$\omega(z) \in 1 + P^{n+1}$, по лемме 5 гл. I-4. Поскольку число n произвольно, отсюда видно, что ω тривиален на $1 + p_v^m$, а следовательно, локально постоянен на $k_v^\times$. В поле K имеется лишь конечное число корней из 1, что вытекает из теоремы 7 гл. I-4 в случае характеристики p и из этой же теоремы и предложения 9 гл. II-3 в случае характеристики нуль. Поэтому можно выбрать такое $v > 0$, что в $1 + P^v$ не содержится корней из 1, отличных от 1. Возьмем окрестность единицы в $k_\mathbb{A}^\times$, которая морфизмом ω отображается в $1 + P^v$. Поскольку почти для всех v эта окрестность содержит $r_v^\times$, мы видим, что почти для всех v морфизм ω тривиален на $1 + p_v$ и на группе всех корней из 1 в k_v, а следовательно, и на $r_v^\times$.

Для каждого конечного множества P точек поля k, содержащего P_∞, положим $G'_P = \prod_{v \notin P} r_v^\times$. Это — открытая подгруппа в G_P, определенная в предложении 15. Она состоит из тех иделей (z_v), для которых $z_v = 1$ при $v \in P$ и $z_v \in r_v^\times$, т. е. $|z_v|_v = 1$ при $v \notin P$. Пусть Γ — любая группа, обладающая описанным выше свойством, и ω — любой морфизм группы $k_\mathbb{A}^\times$ в Γ. Тогда существует такое множество P, что ω тривиален на G'_P и потому определяет морфизм $\varphi\colon G_P/G'_P \to \Gamma$. Если, кроме того, ω тривиален на $k^\times$, то предложение 15 показывает, что ω однозначно определяется по φ. Обсудим теперь условия на φ, при которых такой морфизм ω существует.

Пусть k — некоторое поле алгебраических чисел и P таково, как выше. Будем говорить, что дробный идеал в k *взаимно прост* с P, если не существует простого идеала $\mathfrak{p}_v$, соответствующего точке $v \in P$ и входящего в идеал с отличным от нуля показателем. Аналогично для поля k характеристики $p > 1$ мы будем говорить, что данный дивизор *взаимно прост* с P, если не существует точки $v \in P$, входящей в этот дивизор с отличным от нуля коэффициентом. Будем обозначать через $I(P)$ (соотв. через $D(P)$) группу дробных идеалов поля k (соотв. группу дивизоров поля k), взаимно простых с P. Ясно, что морфизм $z \to \mathrm{id}(z)$ из $k_\mathbb{A}^\times$ на $I(k)$ (соотв. морфизм $z \to \mathrm{div}(z)$ из $k_\mathbb{A}^\times$ на $D(k)$) определяет изоморфизм из G_P/G'_P на $I(P)$ (соотв. на $D(P)$), с помощью которого можно отождествить эти группы друг с другом или, что то же самое, со свободной абелевой группой, порожденной точками поля k, не лежащими в P. В частности, каждый морфизм $v \to \lambda(v)$ множества этих точек в коммутативную группу Γ можно единственным образом продолжить до морфизма φ из $I(P)$ (соответственно из $D(P)$) в Γ; при этом $\varphi \circ (\mathrm{id})$ (соответственно $\varphi \circ (\mathrm{div})$) есть морфизм $G_P \to \Gamma$, тривиальный на G'_P.

Предложение 17. *Пусть* φ — *морфизм из* $I(P)$ (*соотв. из* $D(P)$) *в коммутативную группу* Γ. *Для каждой точки* $v \in P$ *пусть* g_v — *открытая подгруппа в* $k_v^\times$, *содержащаяся в* $r_v^\times$, *если точка* v *конечна. Тогда морфизм* $\varphi \circ (\mathrm{id})$ (*соотв.* $\varphi \circ (\mathrm{div})$) *группы* G_P *в* Γ *в том и только в том случае может быть продолжен до морфизма* ω: $k_{\mathbf{A}}^\times \to \Gamma$, *тривиального на* $k^\times$, *когда для каждой точки* $v \in P$ *можно найти такой морфизм* ψ_v: $g_v \to \Gamma$, *что* $\varphi(\mathrm{id}(\xi))$ (*соотв.* $\varphi(\mathrm{div}(\xi))$) *совпадает с* $\prod \psi_v(\xi)$ *при всех* $\xi \in \bigcap (k^\times \cap g_v)$. *В этом случае морфизм* ω *единствен и индуцирует* ψ_v^{-1} *на* g_v *для всех* $v \in P$.

Положим $g = \prod_{v \in p} g_v$. Эту группу можно очевидным образом рассматривать как подгруппу в $k_{\mathbf{A}}^\times$. Тогда группа $g \cdot G_P$ является открытой подгруппой в $k_{\mathbf{A}}^\times$ и разлагается в прямое произведение подгрупп g и G_P. Следовательно, $k^\times g \cdot G_P$ является открытой подгруппой в $k_{\mathbf{A}}^\times$ и, значит, в силу предложения 15 совпадает с $k_{\mathbf{A}}^\times$. Теперь очевидно, что морфизм $g \cdot G_P \to \Gamma$ в том и только в том случае можно продолжить до морфизма группы $k_{\mathbf{A}}^\times = k^\times g \cdot G_P$, тривиального на $k^\times$, когда он тривиален на группе $\gamma = k^\times \cap \bigcap (g \cdot G_P)$, и что в этом случае продолжение единственно. Ясно, что γ совпадает с группой $\bigcap (k^\times \cap g_v)$ из формулировки предложения. Так как морфизм $z \to \mathrm{id}(z)$ (соотв. $z \to \mathrm{div}(z)$) тривиален на g, то он отображает $g \cdot G_P = g \times G_P$ на $I(P)$ (соотв. на $D(P)$). Поэтому если обозначить через φ_1 морфизм $\varphi \circ (\mathrm{id})$ (соотв. $\varphi \circ (\mathrm{div})$) из G_P в Γ, то мы видим, что его продолжения на $g \cdot G_P$ имеют вид $\psi^{-1}\varphi_1$, где ψ — произвольный морфизм из g в Γ. Обозначая через ψ_v морфизм, индуцированный на g_v морфизмом ψ, получаем наше утверждение.

Очевидно, что если условия предложения 17 выполняются при данном выборе групп g_v и морфизмов ψ_v, то они будут выполняться также, если заменить каждую группу g_v любой ее открытой подгруппой g_v', а ψ_v — индуцированным на ней морфизмом. Например, в случае $k_v = \mathbf{R}$ всегда можно взять $g_v = \mathbf{R}_+^\times$; в случае когда v — конечная точка, можно взять в качестве g_v любую из групп $1 + p_v^m$ с $m \geqslant 1$. На той же идее основано следующее

Следствие. *В условиях предложения* 17 *предположим, что группа* Γ *либо* (a) *дискретна, либо* (b) *совпадает с* $\mathbf{C}^\times$, *либо* (c) *совпадает с группой* $K^\times$, *где* $K^\times$ — *некоторое локальное* p-*поле. Тогда продолжение* ω *существует в том и только в том случае, когда можно найти группы* g_v *и морфизмы* ψ_v, *обладающие свойствами, указанными в предложении* 17, *и следующим дополнительным свойством: в случае* (a) $\psi_v = 1$ *для всех* $v \in P$; *в случае* (b) $\psi_v = 1$ *для всех конеч-*

ных точек $v \in P$; *в случае* (c) $\psi_v = 1$ *для всех точек* $v \in P$, *для которых* k_v *не является p-полем.*

В самом деле, предположим, что условия предложения 17 выполняются при некотором выборе групп g_v и морфизмов ψ_v. Тогда в случае (a) мы можем для каждой точки $v \in P$ заменить g_v ядром g_v' морфизма ψ_v, поскольку это ядро является открытой подгруппой в g_v; при этом ψ_v заменится на 1. В случае (b) можно сделать аналогичную замену для каждой конечной точки $v \in P$ (лемма 4 § 3); по тем же причинам можно точно так же поступить и в случае любой группы Γ, не обладающей произвольно малыми подгруппами. Случай (c) рассматривается аналогично с использованием предложения 16.

Очевидно, достаточно проверять выполнение условий предложения 17 не для всех ξ из группы $\gamma = \bigcap (k^\times \cap g_v)$, а лишь на множестве образующих этой группы. В этой связи оказывается иногда полезным следующий результат.

Предложение 18. *В обозначениях предложения* 17 *предположим, что* k *— поле алгебраических чисел и* $\mathfrak{r}$ *— максимальный порядок в* k. *Тогда группа* $\gamma = \bigcap (k^\times \cap g_v)$ *порождается множеством* $\gamma \cap \mathfrak{r}$.

Возьмем любой элемент $\xi \in \gamma$ и запишем $\xi\mathfrak{r} = \mathfrak{b}\mathfrak{a}^{-1}$, где $\mathfrak{a}$, $\mathfrak{b}$— взаимно простые идеалы в $\mathfrak{r}$. Для каждой конечной точки $v \in P$ имеем $\xi \in \mathfrak{r}_v^\times$, так что $\mathfrak{p}_v$ не делит $\mathfrak{a}$ или $\mathfrak{b}$. Применяя следствие 1 теор. 1 гл. V-2 к проекции $\mathfrak{r} \to \prod \mathfrak{r}_v$, где произведение берется по тем конечным точкам v поля k, которые либо лежат в P, либо соответствуют простым идеалам, делящим $\mathfrak{a}$, мы видим, что существует такой элемент $\alpha \in \mathfrak{r}$, что $\alpha \in g_v$ для каждой конечной точки $v \in P$, $\alpha \in \mathfrak{a}$ и $\alpha \neq 0$. Тогда элемент α^2 удовлетворяет тем же самым условиям и содержится в g_v для каждой бесконечной точки v, так что он содержится в γ, а следовательно, и в $\gamma \cap \mathfrak{r}$. Следовательно, и $\xi\alpha^2 \in \gamma \cap \mathfrak{r}$, чем и доказано наше предложение.

Пусть, в частности, $g_v = 1 + \mathfrak{p}_v^{m(v)}$, где $m(v) \geqslant 1$ для каждой конечной точки $v \in P$. Положим $\mathfrak{m} = \prod \mathfrak{p}_v^{m(v)}$ и обозначим через $v_1, \ldots, v_\rho$ все вещественные точки поля k, для которых $g_v = \mathbf{R}_+^\times$. Тогда сразу видно, что множество $\gamma \cap \mathfrak{r}$ из предложения 17 состоит из тех элементов кольца $\mathfrak{r}$, которые $\equiv 1\ (\mathfrak{m})$ и образы которых в k_{v_i} строго положительны для $1 \leqslant i \leqslant \rho$.

ГЛАВА ВОСЬМАЯ

СЛЕДЫ И НОРМЫ

§ 1. СЛЕДЫ И НОРМЫ В ЛОКАЛЬНЫХ ПОЛЯХ

В § 1—3 мы будем рассматривать исключительно локальные поля (предполагаемые коммутативными). Обозначим через K рассматриваемое локальное поле и через K' — алгебраическое расширение поля K конечной степени n над K. Если K является $\mathbf{R}$-полем, то $K' \neq K$ только в случае $K = \mathbf{R}$, $K' = \mathbf{C}$, $n = 2$; в этом случае по следствию 3 предл. 4 гл. III-3 $\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}(x) = x + \bar{x}$ и $\mathrm{N}_{\mathbf{C}/\mathbf{R}}(x) = x\bar{x}$, причем $\mathrm{Tr}_{\mathbf{C}/\mathbf{R}}$ отображает $\mathbf{C}$ на $\mathbf{R}$, а $\mathrm{N}_{\mathbf{C}/\mathbf{R}}$ отображает $\mathbf{C}^\times$ на группу $\mathbf{R}_+^\times$, которая является подгруппой индекса 2 в $\mathbf{R}^\times$.

Начиная с этого места вплоть до конца § 3 мы предполагаем, что K есть p-поле, и используем наши обычные обозначения для таких полей, так что q — это модуль поля K, R — его максимальное компактное подкольцо, P — максимальный идеал в R и π — простой элемент в K. Для поля K', введенного выше, мы применяем аналогичные обозначения, а именно q', R', P', π'. Обозначим, далее, через f модулярную степень поля K' над K и через e индекс ветвления поля K' над K (см. определение 4 в гл. I-4). Тогда $q' = q^f$ и $n = ef$ по следствию 6 теор. 6 гл. I-4. Так как $e = \mathrm{ord}_{K'}(\pi)$, то R'-модуль в K', порожденный множеством $P^\nu = \pi^\nu R$, при любом $\nu \in \mathbf{Z}$ совпадает с $P'^{e\nu}$; мы будем обозначать его через $\iota(P^\nu)$.

Согласно следствию 1 предл. 4 гл. III-3 и замечаниям, сделанным после этого предложения, $\mathrm{Tr}_{K'/K} \neq 0$ в том и только в том случае, когда расширение K' над K сепарабельно; в этом случае, будучи K-линейным, след отображает K' на K. По определению нормы и по следствию 3 теор. 3 гл. I-2 при всех $x' \in K'$ имеем

$$\mathrm{mod}_{K'}(x') = \mathrm{mod}_K(\mathrm{N}_{K'/K}(x')). \tag{1}$$

Ввиду теоремы 6 гл. I-4 отсюда следует, что $x' \in R'$ в том и только в том случае, когда $\mathrm{N}_{K'/K}(x') \in R$, и $x' \in R'^\times$ в том и только в том случае, когда $\mathrm{N}_{K'/K}(x') \in R^\times$. Так как $\mathrm{mod}_K(\pi) = q^{-1}$ и $\mathrm{mod}_{K'}(\pi') = q'^{-1}$, то при $x' \neq 0$ равенство (1) можно записать

также следующим образом:

$$\operatorname{ord}_K(\mathrm{N}_{K'/K}(x')) = f \cdot \operatorname{ord}_{K'}(x'). \tag{2}$$

Начиная с этого места, мы будем писать Tr, N вместо $\mathrm{Tr}_{K'/K}$, $\mathrm{N}_{K'/K}$, кроме тех случаев, когда одновременно рассматриваются более чем два поля K, K'. Для каждого $v \in \mathbf{Z}$ будем писать $\mathfrak{P}(P'^v) = P^v$; согласно (2), это есть R-модуль в K, порожденный образом P'^v при отображении N.

Предложение 1. *Пусть поле K' сепарабельно над K. Тогда если $x' \in R'$, то* $\mathrm{Tr}(x') \in R$, *а если $x' \in P'$, то* $\mathrm{Tr}(x') \in P$ *и* $\mathrm{N}(1+x') = 1 + \mathrm{Tr}(x') + y$, *где* $y \in R \cap x'^2 R'$.

Пусть $\bar{K}$ — алгебраическое замыкание поля K'. Обозначим через $\lambda_1, \ldots, \lambda_n$ различные K-линейные изоморфизмы $K' \to \bar{K}$. Тогда по следствию 3 предл. 4 гл. III-3 имеем

$$\mathrm{Tr}(x') = \sum_i \lambda_i(x'), \qquad \mathrm{N}(1+x') = \prod_i (1+\lambda_i(x')). \tag{3}$$

Обозначим через K'' композит полей $\lambda_i(K')$, который является наименьшим расширением Галуа поля K в $\bar{K}$, содержащим поле K'. Определим R'', P'' для K'' так же, как R, P определены для K. По следствию 5 теор. 6 гл. I-4 имеем $\lambda_i(R') \subset R''$ и $\lambda_i(P') \subset P''$ при всех i, так что $\mathrm{Tr}(x')$ лежит в R'' при $x' \in R'$ и в P'' при $x' \in P'$. Поскольку то же самое следствие показывает, что $R = K \cap R''$ и $P = K \cap P''$, справедливость утверждений относительно Tr доказана. Предположим теперь, что $x' \in R'$, $x' \neq 0$, и положим

$$y = \mathrm{N}(1+x') - 1 - \mathrm{Tr}(x').$$

Ввиду (3) это есть сумма одночленов степени $\geqslant 2$ от $\lambda_i(x')$. Так как один из изоморфизмов λ_i тождествен и изоморфизмы λ_i по следствию 2 предл. 3 гл. III-2 отличаются друг от друга лишь на автоморфизмы поля K'' над K, то все $\lambda_i(x')$ имеют тот же порядок в K'', что и x', так что $yx'^{-2} \in R''$, если $x' \in R'$. Поскольку $R' = K' \cap R''$, этим доказано наше последнее утверждение. В силу того факта, что $\mathrm{Tr} = 0$, если поле K' не сепарабельно над K, и в силу относящихся к этому случаю замечаний в гл. III-3 наше предложение верно (но не интересно) и в несепарабельном случае.

Следствие. *Если $x' \in P'^{-e+1}$, то* $\mathrm{Tr}(x') \in R$.

По определению $e = \operatorname{ord}_{K'}(\pi)$. Поэтому наше условие означает, что $\pi x' \in P'$, откуда $\mathrm{Tr}(\pi x') \in P$ по предложению 1, следовательно $\mathrm{Tr}(x') \in R$ ввиду K-линейности Tr.

Определение 1. *Пусть поле K' сепарабельно над K и d — наибольшее из целых чисел ν, таких, что* $\mathrm{Tr}\,(x') \in R$ *при всех* $x' \in P'^{-\nu}$. *Тогда* P'^{d} *называется дифферентой поля K' над K, а d — показателем дифференты.*

Дифференту мы будем обозначать через $D\,(K'/K)$ или просто через D. Если поле K' несепарабельно над K, то $\mathrm{Tr} = 0$, так что след отображает $P'^{-\nu}$ в R при всех ν; в этом случае положим $d = +\infty$, $D\,(K'/K) = 0$.

Согласно следствию предл. 1, $d \geqslant e - 1$. В частности, если $d = 0$, то $e = 1$, так что поле K' неразветвлено над K. Обратное утверждение тоже верно; оно будет вытекать из следующих результатов.

Предложение 2. *Пусть поле K' неразветвлено над K. Обозначим через ρ, ρ' канонические гомоморфизмы $R \to k = R/P$ и $R' \to k' = R'/P'$ соответственно. Тогда при $x' \in R'$ имеем*

$$\rho\,(\mathrm{Tr}\,(x')) = \mathrm{Tr}_{k'/k}\,(\rho'\,(x')), \quad \rho\,(\mathrm{N}\,(x')) = \mathrm{N}_{k'/k}\,(\rho'\,(x')).$$

Как и в теореме 7 гл. I-4 и ее следствиях, обозначим через $M'^{\times}$ группу корней из 1 в K', порядок которых взаимно прост с p. По следствию 2 из этой теоремы K' является циклическим расширением степени f над K и его группа Галуа порождается автоморфизмом Фробениуса, который индуцирует на $M'^{\times}$ перестановку $\mu \to \mu^q$. Ввиду следствия 2 теор. 2 гл. I-1 это означает в точности то, что автоморфизмы поля K' над K определяют на $k' = R'/P'$ автоморфизмы, составляющие всю группу Галуа поля k' над k. Наше утверждение немедленно следует теперь из этого факта, из формул $\mathrm{Tr}\,(x') = \sum \lambda_i\,(x')$, $\mathrm{N}\,(x') = \prod \lambda_i\,(x')$ и из аналогичных формул для k и k', т. е. из следствия 3 предл. 4 гл. III-3, примененного сначала к K и K', а затем к k и k'.

Предложение 3. *Пусть поле K' неразветвлено над K. Тогда* Tr *сюръективно отображает P'^{ν} на P^{ν} для каждого $\nu \in \mathbf{Z}$, а* N *сюръективно отображает $R'^{\times}$ на $R^{\times}$.*

Пусть k, k' такие, как в предложении 2. Так как k' сепарабельно над k, то $\mathrm{Tr}_{k'/k} \neq 0$. Первая формула из предложения 2 показывает, что образ $\mathrm{Tr}\,(R')$ кольца R' при отображении Tr не содержится в P. Поскольку этот образ содержится в R согласно предложению 1 и поскольку он является R-модулем, ибо R' является R-модулем, а Tr K-линеен, то он совпадает с R. Так как поле K' неразветвлено, то простой элемент π в K является также простым элементом в K'. Поэтому $P'^{\nu} = \pi^{\nu} P'$ при $\nu \in \mathbf{Z}$. Ввиду K-линейности отображения

Tr получаем

$$\mathrm{Tr}\,(P'^{\nu}) = \pi^{\nu}\mathrm{Tr}\,(R') = \pi^{\nu}R = P^{\nu}.$$

Что касается нормы, то положим $G_0 = R^{\times}$, $G_0' = R'^{\times}$, $G_{\nu} = 1 + P^{\nu}$ и $G_{\nu}' = 1 + P'^{\nu}$ при всех $\nu \geqslant 1$. Последнее утверждение предложения 1 показывает, что для каждого $\nu \geqslant 1$ норма N отображает G_{ν}' в G_{ν}, а также с учетом только что доказанного для следа, что она определяет на $G_{\nu}'/G_{\nu+1}'$ сюръективный морфизм этой группы на $G_{\nu}/G_{\nu+1}$. С другой стороны, обозначим через φ автоморфизм Фробениуса поля K' над K и через μ образующую группы $M'^{\times}$ корней из 1 в $K^{\times}$, порядок которых взаимно прост с p. Тогда элемент μ имеет порядок $q' - 1$, т. е. $q^f - 1$, а его норма равна

$$\mathrm{N}(\mu) = \prod_{i=0}^{f-1} \mu^{\varphi^i} = \prod_{i=0}^{f-1} \mu^{q^i} = \mu^{1+q+\ldots+q^{f-1}} = \mu^{(q^f-1)/(q-1)}.$$

Ясно, что это — корень степени $q - 1$ из 1, а следовательно, образующая группы $M^{\times}$ корней из 1 в K, порядок которых взаимно прост с p. Так как $M^{\times}$ образует полное множество представителей смежных классов в $G_0 = R^{\times}$ по модулю $G_1 = 1 + P$, отсюда видно, что N определяет на G_0'/G_1' сюръективный морфизм этой группы на G_0/G_1. Теперь для каждого элемента $x_0 \in R^{\times}$ мы можем индуктивно определить такие две последовательности (x_{ν}), (x_{ν}'), что $x_{\nu} \in G_{\nu}$, $x_{\nu}' \in G_{\nu}'$, $\mathrm{N}(x_{\nu}') \in x_{\nu}G_{\nu+1}$ и $x_{\nu+1} = \mathrm{N}(x_{\nu}')^{-1}x_{\nu}$ при всех $\nu \geqslant 0$. Поэтому для $y_{\nu}' = x_0'x_1' \ldots x_{\nu-1}'$ имеем $\mathrm{N}(y_{\nu}') = x_0x_{\nu}^{-1}$. Ясно, что последовательность (y_{ν}') стремится к некоторому пределу $y' \in R'^{\times}$ и что $\mathrm{N}(y') = x_0$.

Следствие. *Пусть K' — произвольное расширение конечной степени поля K. Тогда дифферента поля K' над K равна R' (т. е. $d = 0$) в том и только в том случае, когда поле K' неразветвлено над K.*

Предложение 3 показывает, что $d = 0$, если поле K' неразветвлено над K. Обратно, если $d = 0$, то K' сепарабельно над K и, как мы уже отмечали выше, из следствия 1 предл. 1 вытекает, что $e = 1$.

Предложение 4. *Пусть поле K' сепарабельно над K и P'^{d} — его дифферента над K. Тогда для каждого $\nu \in \mathbf{Z}$ образ P'^{ν} в K при отображении* Tr *равен P^{μ}, где целое число μ определяется условием $e\mu \leqslant \nu + d < e(\mu + 1)$.*

Так как след Tr K-линеен и отличен от нуля, он отображает каждую K-решетку в K' и, в частности, каждое множество P'^{ν} на K-решетку в K, т. е. на множество вида P^{μ}. Пусть μ удовлетворяет условию нашего предложения. Тогда поскольку $\mathrm{ord}_{K'}(\pi) = e$,

то P'^{ν} содержится в $\pi^{\mu}P'^{-d}$ и содержит $\pi^{\mu+1}P'^{-d-1}$. Ввиду определения числа d и K-линейности следа Tr, отсюда следует, что $\mathrm{Tr}\,(P'^{\nu})$ содержится в $\pi^{\mu}R = P^{\mu}$ и не содержится в $\pi^{\mu+1}R = P^{\mu+1}$. Доказательство закончено.

Следствие 1. *Для каждого* $x' \in K'^{\times}$ *имеем*
$\mathrm{ord}_{K'}(\mathrm{Tr}\,(x')) = e \cdot \mathrm{ord}_K(\mathrm{Tr}\,(x')) \geqslant \mathrm{ord}_{K'}(x') + d - e + 1$.

В самом деле, если положить $\nu = \mathrm{ord}_{K'}(x')$ и определить μ как в предложении 4, то левая часть неравенства в нашем следствии будет не меньше $e\mu$, согласно упомянутому предложению, а $e\mu > \nu + d - e$ по определению μ.

Следствие 2. *Тогда и только тогда* $\mathrm{Tr}\,(R') = R$, *когда* $d = e - 1$.

В самом деле, по предложению 4 из равенств $\mu = \nu = 0$ вытекает неравенство $d < e$. Так как по следствию предл.1 $d \geqslant e - 1$, то получаем $d = e - 1$.

Если $d = e - 1$, то говорят, что поле K' *хорошо разветвлено* над K.

Следствие 3. *Пусть* χ — *характер порядка* μ *на* K. *Тогда* $\chi \circ \mathrm{Tr}$ — *характер порядка* $d + e\mu$ *на* K'.

Наше предположение означает, что характер χ тривиален на $P^{-\mu}$, но не на $P^{-\mu-1}$. Положим $\nu = d + e\mu$. Предложение 4 показывает, что $\mathrm{Tr}\,(P'^{-\nu}) = P^{-\mu}$, а $\mathrm{Tr}\,(P'^{-\nu-1}) = P^{-\mu-1}$. Поэтому отображение $\chi \circ \mathrm{Tr}$ тривиально на $P'^{-\nu}$, но не на $P'^{-\nu-1}$, что и требовалось доказать.

В нашем очередном следствии мы рассмотрим алгебраическое расширение конечной степени K'' над K'; R'', P'' будут иметь тот же самый смысл для K'', что R, P для K. Для всякого $\nu \in \mathbf{Z}$ будем обозначать через $\iota'(P'^{\nu})$ R''-модуль в K'', порожденный множеством P'^{ν}; если $e' = \mathrm{ord}_{K'}(\pi')$ — степень ветвления поля K'' над K', то $\iota'(P'^{\nu}) = P''^{e'\nu}$. В этих обозначениях имеет место

Следствие 4. *Пусть* K, K', K'' *таковы, как выше, и пусть* $D = P'^{d}$, $D' = P''^{d'}$, $D'' = P''^{d''}$ — *дифференты соответственно поля* K' *над* K, *поля* K'' *над* K' *и поля* K'' *над* K. *Тогда* $D'' = \iota'(D) \cdot D'$ *и* $d'' = e'd + d'$, *где* e' — *индекс ветвления поля* K'' *над* K'.

Это утверждение тривиально, если поле K'' несепарабельно над K, ибо тогда $D'' = 0$ и либо D, либо D' равна нулю. Поэтому можно считать, что поле K'' сепарабельно над K. Нам нужно доказать, что $d'' = \delta$, где $\delta = e'd + d'$. В самом деле, по предложению 4 $\mathrm{Tr}_{K''/K'}$ отображает $P''^{-\delta}$ на P'^{-d} и $P''^{-\delta-1}$ на P'^{-d-1}, а $\mathrm{Tr}_{K'/K}$

отображает P'^{-d} на R и P'^{-d-1} на P^{-1}. Наше утверждение немедленно следует теперь из «транзитивности следов», т. е. из следствия 4 предл. 4 гл. III-3.

Следствие 5. *Пусть K и K' такие, как выше, и пусть K_1 — максимальное неразветвленное расширение поля K, содержащееся в K'. Тогда K' имеет ту же самую дифференту над K, что и над K_1.*

Определение K_1 см. в следствии 4 теор. 7 гл. I-4. Наше утверждение немедленно вытекает из следствия 4 в сочетании со следствием предл. 3.

Предложение 5. *Пусть K, K' таковы, как в предложении 4. Тогда норма* N *определяет открытый морфизм группы $K'^{\times}$ на некоторую открытую подгруппу в $K^{\times}$.*

Как и выше, обозначим через P'^{d} дифференту поля K' над K и положим $G_\nu = 1 + P^\nu$, $G'_\nu = 1 + P'^\nu$ при $\nu \geqslant 1$. Возьмем любое $\mu > 2d$ и положим $\nu = e\mu - d$. По предложению 4 $\mathrm{Tr}\,(P'^\nu) = P^\mu$. Кроме того, имеем $e(\mu - 1) \geqslant 2d$, откуда $2\nu \geqslant e(\mu + 1)$, следовательно, $P'^{2\nu} \subset \pi^{\mu+1}R'$, а потому $K \cap P'^{2\nu} \subset P^{\mu+1}$. Теперь последняя часть предложения 1 показывает, что N, во-первых, отображает G'_ν в G_μ, а во-вторых, определяет сюръективный морфизм из G'_ν на $G_\mu/G_{\mu+1}$. Взяв любой элемент $x_0 \in G_\mu$, мы можем теперь построить по индукции две такие последовательности (x_i), (x'_i), что $x_i \in G_{\mu+i}$, $x'_i \in G'_{\nu+ei}$, $\mathrm{N}(x'_i) \in x_i G_{\mu+i+1}$ и $x_{i+1} = \mathrm{N}(x'_i)^{-1} x_i$ при всех $i \geqslant 0$. Полагая $y'_i = x'_0 x'_1 \ldots x'_i$, имеем $\mathrm{N}(y'_i) = x_0 x_{i+1}^{-1}$. Ясно, что последовательность (y'_i) сходится к некоторому пределу $y' \in G'_\nu$, причем $\mathrm{N}(y') = x_0$. Это показывает, что N отображает G'_ν на G_μ, чем и доказано наше предложение, поскольку группы G_μ, G'_ν ($\mu > 2d$, $\nu = e\mu - d$) образуют фундаментальные системы окрестностей единицы в $K^{\times}$ и в $K'^{\times}$ соответственно.

Используя следствие 2 предл. 4 гл. I-4 и результаты гл. III-3, можно было бы легко показать, что заключение нашего предложения остается верным для любого расширения конечной степени K' поля K, не обязательно сепарабельного. Очевидно, что оно выполняется также для **R**-полей.

§ 2. ВЫЧИСЛЕНИЕ ДИФФЕРЕНТЫ

Обозначения и предположения в этом параграфе те же, что и в § 1. Если рассматривать K' как векторное пространство размерности n над K, то R' является K-решеткой, к которой можно применить теорему 1 гл. II-2. В результате мы получаем, что в K' над K существует базис $\{\alpha_1, \ldots, \alpha_n\}$, для которого $R' = \sum R\alpha_i$.

Предположим теперь, что K' сепарабельно над K, так что $\mathrm{Tr} \neq 0$. Тогда по лемме 3 гл. III-3 можно отождествить векторное пространство K' над K с алгебраическим двойственным к нему, положив $[x', y'] = \mathrm{Tr}\,(x', y')$. Базис $\{\beta_1, \ldots, \beta_n\}$, двойственный к $\{\alpha_1, \ldots, \alpha_n\}$, определяется равенствами $\mathrm{Tr}\,(\alpha_i\beta_j) = \delta_{ij}$ при $1 \leqslant i, j \leqslant n$.

Предложение 6. *Пусть поле K' сепарабельно над K и $D = P'^{d}$ — его дифферента. Пусть $\{\alpha_1, \ldots, \alpha_n\}$ — такой базис в K' над K, что $R' = \sum R\alpha_i$, и пусть $\{\beta_1, \ldots, \beta_n\}$ — базис в K' над K, определяемый условием $\mathrm{Tr}\,(\alpha_i, \beta_j) = \delta_{ij}$ при $1 \leqslant i, j \leqslant n$. Тогда $D^{-1} = P'^{-d} = \sum R\beta_i$.*

В самом деле, возьмем любые элементы $x' \in R'$, $y' \in K'$ и запишем их в виде $x' = \sum x_i\alpha_i$ и $y' = \sum y_i\beta_i$, где $x_i \in R$ и $y_i \in K$ при $1 \leqslant i \leqslant n$. Тогда $\mathrm{Tr}\,(x', y') = \sum x_iy_i$, откуда видно, что в том и только в том случае $\mathrm{Tr}\,(x'y') \in R$ при всех $x' \in R'$, т. е. Tr отображает $R'y'$ в R, когда $y_i \in R$ при всех i. По определению дифференты это означает, что $y' \in P'^{-d}$ тогда и только тогда, когда $y' \in \sum R\beta_i$, что и требовалось доказать.

Следствие 1. *В предположениях предложения 6 обозначим через Δ определитель матрицы*

$$M = (\mathrm{Tr}\,(\alpha_i\alpha_j))_{1 \leqslant i,\ j \leqslant n}.$$

Тогда $\mathrm{ord}_K(\Delta) = fd$ и $\Delta R = \mathfrak{N}(D)$.

Запишем $\alpha_i = \sum a_{ij}\beta_j$, где $a_{ij} \in K$ при $1 \leqslant i, j \leqslant n$. Умножив обе части на α_j и взяв след, получим, что $\mathrm{Tr}\,(\alpha_i\alpha_j) = a_{ij}$ и, следовательно, $M = (a_{ij})$. Поэтому автоморфизм векторного пространства K' над K, переводящий базис $\{\beta_1, \ldots, \beta_n\}$ в базис $\{\alpha_1, \ldots, \alpha_n\}$ и, следовательно, отображающий K-решетку D^{-1} на R', представляется в первом из этих базисов матрицей (a_{ij}), причем его модуль равен $\mathrm{mod}_K(\Delta)$ по следствию 3 теор. 3 гл. I-2. Так как автоморфизм $x' \to \pi'^{d}x'$ также отображает $D^{-1} = P'^{-d}$ на R', то его модуль $\mathrm{mod}_{K'}(\pi'^{d})$ должен совпадать с $\mathrm{mod}_K(\Delta)$. Это дает равенство $fd = \mathrm{ord}_K(\Delta)$, откуда $\mathfrak{N}(D) = \Delta R$.

Заметим, что наше следствие остается справедливым и в несепарабельном случае, потому что тогда $\mathrm{Tr} = 0$ и $D = 0$. Из нашего результата, очевидно, вытекает, что $\mathrm{ord}_K(\Delta)$ не зависит от выбора $\alpha_1, \ldots, \alpha_n$. Этим фактом, который можно было бы легко проверить и непосредственно, оправдано следующее определение.

Определение 2. *Пусть* Δ *таково, как в следствии предложения* 6. *Тогда идеал* ΔR *в* R *называется дискриминантом поля* K' *над* K.

Предположим дополнительно, что K' — сепарабельное расширение степени n над K, и обозначим через $\overline{K}$ алгебраическое замыкание поля K'. Как и в § 1, пусть $\lambda_1, \ldots, \lambda_n$ суть n различных K-линейных изоморфизмов $K' \to \overline{K}$. Среди них есть тождественный изоморфизм, пусть это будет λ_1. Возьмем любой элемент $\xi \in K'$ и положим $\xi_i = \lambda_i(\xi)$ при $1 \leqslant i \leqslant n$, так что, в частности, $\xi_1 = \xi$. Если ν — степень поля K' над $K(\xi)$, то имеется ν различных $K(\xi)$-линейных изоморфизмов $K' \to \overline{K}$. Следовательно, среди изоморфизмов λ_i имеется ровно ν таких, которые оставляют элемент ξ неподвижным. Это показывает, что $K(\xi) = K'$ в том и только в том случае, когда $\xi_i \neq \xi$ при всех $i \neq 1$.

Пусть теперь X — неизвестная над K. С помощью способа, описанного в гл. III-3, мы можем продолжить K-линейное отображение Tr: $K' \to K$ и полиномиальное отображение N: $K' \to K$ до отображения из $K'[X] = K' \otimes_K K[X]$ в $K[X]$, которые мы обозначим опять через Tr и N. Положим, далее,

$$F(X) = \mathrm{N}(X - \xi) = \prod_{i=1}^{n} (X - \xi_i) = X^n + \sum_{i=1}^{n} a_i X^{n-i}. \tag{4}$$

Это — унитарный многочлен из $K[X]$. Обозначая через F' его формальную производную, имеем

$$F'(\xi) = \prod_{i=2}^{n} (\xi - \xi_i).$$

Согласно доказанному выше, $K(\xi) = K'$ в том и только в том случае, когда $F'(\xi) \neq 0$. Хорошо известно и легко проверяется, что $F(X)^{-1}$ допускает в $\overline{K}(X)$ «разложение на простейшие дроби», задаваемое формулой

$$\frac{1}{F(X)} = \sum_{i=1}^{n} \frac{1}{F'(\xi_i)(X - \xi_i)}.$$

Рассматривая поле $\overline{K}(X)$ как очевидным образом вложенное в поле формальных степенных рядов от X^{-1} с коэффициентами в $\overline{K}$, получаем отсюда

$$X^{-n}\left(1 + \sum_{i=1}^{n} a_i X^{-i}\right)^{-1} = \sum_{i=1}^{n} F'(\xi_i)^{-1} \sum_{\nu=0}^{+\infty} \xi_i^{\nu} X^{-\nu-1},$$

что можно переписать еще так:

$$X^{-n}\sum_{\nu=0}^{+\infty}\Big(\sum_{i=1}^{n}a_iX^{-i}\Big)^{\nu}=\sum_{\nu=0}^{\nu+\infty}\operatorname{Tr}\left(F'(\xi)^{-1}\xi^{\nu}\right)X^{-\nu-1}.$$

Сравнивая коэффициенты в левой и правой частях, находим

$$P_{\nu}(a)=\operatorname{Tr}\left(F'(\xi)^{-1}\xi^{\nu}\right) \tag{5}$$

при $\nu\geqslant 0$, где $P_{\nu}(a)$ при всех ν является многочленом из $\mathbf{Z}[a_1,\ \ldots,\ a_n]$, $P_{\nu}=0$ при $0\leqslant\nu<n-1$ и $P_{n-1}=1$.

Предложение 7. *Пусть K' — сепарабельное расширение степени n над K, D — его дифферента, и для любого $\xi\in K'$ пусть F — многочлен, определенный формулой* (4). *Тогда все коэффициенты a_i многочлена F лежат в R, если $\xi\in R'$, и в P, если $\xi\in P'$. Кроме того, если $\xi\in R'$, то $F'(\xi)\,D^{-1}$ содержится в $R[\xi]$, и это — наибольший R'-модуль, содержащийся в $R[\xi]$.*

Утверждения относительно a_i доказываются точно так же, как утверждения о следе в предложении 1. В самом деле, если $\xi_i=\lambda_i(\xi)$ определены, как выше, то из предположения $\xi\in R'$ (соотв. $\xi\in P'$) следует, что $\xi_i\in\lambda_i(R')$ (соотв. $\xi_i\in\lambda_i(P')$) для всякого i, а потому ξ_i лежит в максимальном компактном подкольце R'' композита K'' полей $\lambda_i(K')$ (соотв. в максимальном идеале P'' кольца R''). Формула (4) показывает тогда, что все a_i лежат в R'', а следовательно в $R=K\cap R''$ (соотв. в P'', а следовательно в $P=K\cap P''$). Что касается утверждения относительно $F'(\xi)$, то предположим сначала, что $F'(\xi)=0$. Как мы видели, это имеет место в том и только в том случае, когда $K(\xi)\neq K'$. В этом случае поле $K(\xi)$, а следовательно и $R[\xi]$, не может содержать никакого R'-модуля, отличного от $\{0\}$, чем и доказано наше утверждение. Предположим теперь, что $F'(\xi)\neq 0$. Тогда $K'=K(\xi)$, так что $\{1,\ \xi,\ \ldots,\ \xi^{n-1}\}$ есть базис в K' над K. Поскольку многочлен F унитарен и содержится в $R[X]$, а $F(\xi)=0$, то из хорошо известного элементарного рассуждения вытекает, что $R[\xi]$ совпадает с R-модулем $\sum_{i=0}^{n-1}R\xi^i$. Возьмем теперь любой элемент $x'\in K'$. Запишем $F'(\xi)\,x'=\sum_{i=0}^{n-1}x_i\xi^i$, где $x_i\in K$ при $0\leqslant i\leqslant n-1$. Умножая обе части на $F'(\xi)^{-1}\xi^{\nu}$ и беря следы, получаем в силу формулы (5)

$$\operatorname{Tr}(x'\xi^{\nu})=\sum_{i=0}^{n-1}x_iP_{\nu+i}(a) \tag{6}$$

при всех $v \geqslant 0$. В частности, при $0 \leqslant v \leqslant n-1$ имеем

$$x_{n-v-1} = \mathrm{Tr}(x'\xi^v) = \sum_{i=n-v}^{n-1} x_i P_{v+i}(a). \tag{7}$$

Предположим сначала, что $x' \in D^{-1}$. Используя формулу (7) и индукцию по v для $0 \leqslant v \leqslant n-1$, находим, что все $x_i \in R$, т. е. $F'(\xi)\, x' \in R[\xi]$, так что $F'(\xi)\, D^{-1} \subset R[\xi]$. Предположим теперь, что $x_i \in R$ при $0 \leqslant i \leqslant n-1$, т. е. что $F'(\xi)\, x' \in R[\xi]$. Тогда формула (6) при $v = 0$ показывает, что $\mathrm{Tr}(x') \in R$. Заменяя x' на $x'y'$ с $y' \in R'$, мы видим, что если x' таков, что $F'(\xi)\, x'R' \subset R[\xi]$, то $x' \in D^{-1}$. Этим доказано наше последнее утверждение.

Следствие 1. *В обозначениях и предположениях предложения 7* $D = F'(\xi)\, R'$ *тогда и только тогда, когда* $R' = R[\xi]$.

Это сразу вытекает из второй части предложения 7.

Следствие 2. *В обозначениях и предположениях предложения 7 допустим дополнительно, что* K' *вполне разветвлено над* K, *и положим*

$$F(X) = \mathrm{N}(X - \pi') = X^n + \sum_{i=1}^{n} a_i X^{n-i},$$

где π' *— любой простой элемент в* K'. *Тогда* $\mathrm{ord}_K(a_i) \geqslant 1$ *при* $1 \leqslant i \leqslant n$, $\mathrm{ord}_K(a_n) = 1$ *и* $D = F'(\pi')\, R'$.

Взяв в предложении 7 $\xi = \pi'$, мы получим первое утверждение. Второе очевидно ввиду формулы 2 § 1, поскольку $a_n = \mathrm{N}(-\pi')$. Последнее утверждение немедленно вытекает из следствия 1, с учетом предложения 4 гл. I-4.

Следствие 3. *В обозначениях и предположениях следствия 2 поле* K' *хорошо разветвлено тогда и только тогда, когда* n *взаимно просто с* p.

Поскольку K' вполне разветвлено, то в наших обычных обозначениях $f = 1$ и $n = e$. По следствию 2 $d = \mathrm{ord}_{K'}(F'(\pi'))$, и все члены в $F'(\pi')$, кроме первого члена $n\pi'^{n-1}$, имеют порядок $\geqslant e = \mathrm{ord}_{K'}(\pi)$ в K'. Поэтому тогда и только тогда $d = e - 1$, т. е. K' хорошо разветвлено, когда $\mathrm{ord}_{K'}(n) = 0$, т. е. когда n взаимно просто с p.

Многочлен F, удовлетворяющий условиям следствия 2, т. е. унитарный многочлен $X^n + \sum_{i=1}^{n} a_i X^{n-i}$ в $K[X]$, для которого $\mathrm{ord}_K(a_i) \geqslant$

$\geqslant 1$ при всех i и $\operatorname{ord}_K(a_n) = 1$, называется *многочленом Эйзенштейна* над K.

Предложение 8. *Пусть F — многочлен Эйзенштейна над K. Тогда F неприводим в $K[X]$, и если π' — корень многочлена F в произвольном расширении поля K, то поле $K(\pi')$ является хорошо разветвленным расширением поля K, а π' — простым элементом в $K(\pi')$.*

Предположим, что $F = GH$, где $G,\ H \in K[X]$. Пусть $a,\ b$ — наименьшие целые числа, для которых многочлены $G_1 = \pi^a G$ и $H_1 = \pi^b H$ лежат в $R[X]$. Положим $F_1 = \pi^{a+b}F$, так что $F_1 = G_1H_1$. Положим, далее, $k = R/P$ и обозначим через $F_0,\ G_0,\ H_0$ многочлены из $k[X]$, получаемые заменой каждого коэффициента в многочленах $F_1,\ G_1,\ H_1$ соответственно образом этого коэффициента в R/P при каноническом гомоморфизме $R \to R/P$. Ввиду определения чисел $a,\ b$ многочлены G_0 и H_0 отличны от нуля, так что $F_0 \neq 0$. Отсюда следует, что $a + b = 0$, $F_1 = F$ и $F_0 = X^n$, а значит, существует такое ν, что $G_0 = X^\nu$, $H_0 = X^{n-\nu}$. Поэтому степени многочленов G_1 и H_1 не меньше соответственно ν и $n - \nu$. Поскольку $F_1 = G_1H_1$, они равны соответственно ν и $n - \nu$. Если $\nu > 0$, $n - \nu > 0$, то обозначим через g и h свободные члены в G_1 и H_1 соответственно. Так как $G_0 = X^\nu$ и $H_0 = X^{n-\nu}$, то $g,\ h \in P$. Поскольку свободный член в F равен теперь gh, то он лежит в P^2, что противоречит определению многочлена Эйзенштейна. Пусть теперь π' — корень многочлена F в некотором расширении поля K, которое можно считать алгебраически замкнутым. Так как F неприводим, то различные K-линейные изоморфизмы поля $K' = K(\pi')$ в это расширение отображают π' на все различные корни многочлена F, так что $F(X) = \mathrm{N}(X - \pi')$, откуда по определению многочлена Эйзенштейна $\operatorname{ord}_K(\mathrm{N}(\pi')) = 1$. В силу формулы 2 § 1 отсюда следует, что $f = 1$ и что π' — простой элемент в K'.

§ 3. ТЕОРИЯ ВЕТВЛЕНИЯ

В этом параграфе нам будет удобно записывать изоморфизмы и автоморфизмы полей экспоненциально, т. е. как $x \to x^\lambda$ и т. п. Далее, удобно будет следующим образом продолжить ord_K, где поле K такое же, как выше, на все алгебраические расширения поля K. Пусть x' — любой элемент такого расширения; K' — любое расширение конечной степени поля K, содержащее x'; π, как и прежде,— простой элемент в K. Положим

$$\operatorname{ord}_K(x') = \operatorname{ord}_{K'}(x')/\operatorname{ord}_{K'}(\pi).$$

Если заменить здесь K' любым аналогичным полем K'', содержащим K', то $\mathrm{ord}_K(x')$ и $\mathrm{ord}_{K'}(\pi)$ умножатся оба на индекс ветвления поля K'' над K', так что наше определение $\mathrm{ord}_K(x')$ не зависит от выбора K'; разумеется, можно взять в определении $K' = K(x')$. Пользуясь этой возможностью выбора подходящего K', мы видим, что ord_K совпадает на $K^\times$ с ранее определенным отображением ord_K: $K^\times \to \mathbf{Z}$ и определяет отображение каждого алгебраического расширения поля K в $\mathbf{Q} \cup \{+\infty\}$, причем $\mathrm{ord}_K(x') = +\infty$ в том и только в том случае, когда $x' = 0$.

Пусть, как и прежде, K' — расширение степени n поля K; предположим, что это расширение сепарабельно. Сохраним в силе обозначения § 1—2. В частности, $D = P'^d$ — дифферента поля K' над K. Обозначим через K_1 максимальное неразветвленное расширение поля K, содержащееся в K' (согласно следствию 4 теор. 7 гл. I-4 K_1 определено однозначно). Тогда поле K' имеет степень e над K_1 и по следствию 5 предл. 4 § 1 его дифферента над K_1 равна D. Положим

$$F(X) = \mathrm{N}_{K'/K_1}(X - \pi').$$

По следствию 2 предл. 7 § 2 это — многочлен Эйзенштейна над K_1 и $D = F'(\pi')R'$.

Пусть L — любое содержащее K' расширение Галуа конечной степени над K. Например, в качестве L можно взять композит образов поля K' при всех различных K-линейных изоморфизмах поля K' в некоторое его алгебраическое замыкание $\bar{K}$. Для каждого K-линейного изоморфизма $x' \to x'^\lambda$ из K' в L положим

$$\begin{aligned} v(\lambda) &= \min_{x' \in R'} \mathrm{ord}_{K'}(x' - x'^\lambda) = \\ &= \min_{x' \in R'} \mathrm{ord}_L(x' - x'^\lambda)/\mathrm{ord}_L(\pi'). \end{aligned}$$

Так как $\mathrm{ord}_L(x' - x'^\lambda)$ — целое неотрицательное число или $+\infty$, то функция v определена корректно; она принимает значение $+\infty$ в том и только в том случае, когда λ есть тождественное отображение, т. е. естественное вложение поля K' в L, которое мы будем обозначать через ε. Согласно теореме 7 гл. I-4 и ее следствиям 3 и 4 поле K_1 порождено над K корнями из 1 в K', порядок которых взаимно прост с p, и эти корни вместе с нулем образуют полное множество представителей для R'/P' в R'. Поэтому если автоморфизм λ индуцирует на K_1 не тождественное отображение, то существует такой корень ζ, для которого $\zeta^\lambda \neq \zeta$. Тогда $\zeta - \zeta^\lambda$ лежит в K', но не в P', так что, беря $x' = \zeta$, получаем $v(\lambda) = 0$. Предположим теперь, что λ индуцирует на K_1 тождественное отображение. Так как K' хорошо разветвлено над K_1, то предложение 4

гл. I-4 показывает, что $R' = R_1[\pi']$, где R_1 — максимальное компактное подкольцо в K_1, так что каждый элемент $x' \in R'$ может быть записан в виде $G(\pi')$, где $G \in R_1[X]$. Это дает

$$x' - x'^{\lambda} = G(\pi') - G(\pi'^{\lambda}) = (\pi' - \pi'^{\lambda}) H(\pi', \pi'^{\lambda}),$$

где $H \in R_1[X, Y]$. Как уже отмечалось в доказательстве предложения 1, π'^{λ} имеет тот же самый порядок в L, что и π'. Отсюда следует, что $\operatorname{ord}_{K'}(\pi'^{\lambda}) = \operatorname{ord}_{K'}(\pi') = 1$, так что

$$\operatorname{ord}_{K'}(x' - x'^{\lambda}) \geqslant \operatorname{ord}_{K'}(\pi' - \pi'^{\lambda}) \geqslant 1,$$

поэтому для любого изоморфизма λ, тождественного на K_1, имеем

$$\nu(\lambda) = \operatorname{ord}_{K'}(\pi' - \pi'^{\lambda}) \geqslant 1, \tag{8}$$

откуда следует, что $\operatorname{ord}_{K'}(\pi' - \pi'^{\lambda})$ не зависит от выбора π'. Далее, для F, определенного, как выше, имеем по формуле (4) § 2

$$F(X) = \prod_{\lambda} (X - \pi'^{\lambda}),$$

где произведение берется по всем различным K_1-линейным изоморфизмам λ: $K' \to L$, откуда

$$F'(\pi') = \prod_{\lambda \neq \varepsilon} (\pi' - \pi'^{\lambda}),$$

где произведение берется по тем же самым изоморфизмам, кроме тождественного. Это дает

$$d = \operatorname{ord}_{K'}(F'(\pi')) = \sum_{\lambda \neq \varepsilon} \nu(\lambda),$$

где сумма берется по тем же самым изоморфизмам, а также

$$d - e + 1 = \sum_{\lambda \neq \varepsilon} (\nu(\lambda) - 1),$$

ибо число таких изоморфизмов равно $e - 1$. Поскольку $\nu(\lambda) = 0$, если изоморфизм λ нетождествен на K_1, полученные формулы можно переписать так:

$$d = \sum_{\lambda \neq \varepsilon} \nu(\lambda), \quad d - e + 1 = \sum_{\lambda \neq \varepsilon} (\nu(\lambda) - 1)^{+}. \tag{9}$$

Здесь суммы берутся теперь по всем различным K-линейным изоморфизмам $K' \to L$, отличным от тождественного; кроме того, в последней сумме число членов, больших нуля, не превосходит $e - 1$.

Если само K' является расширением Галуа поля K, то мы можем взять $L = K'$. Тогда изоморфизмы λ — это автоморфизмы поля K' над K. Они образуют группу Галуа $\mathfrak{g}$ поля K' над K. Из определения $v(\lambda)$ видно, что теперь это — целое число или $+\infty$. Если $\lambda \neq \varepsilon$, то $v(\lambda)$ — наибольшее из целых чисел v, таких, что λ определяет тождественное отображение на кольце R/P^v. Для всякого $v \geqslant 0$ автоморфизмы λ поля K' над K, для которых $v(\lambda) \geqslant v$, образуют подгруппу $\mathfrak{g}_v$ в $\mathfrak{g}$; группа $\mathfrak{g}_0$ совпадает с $\mathfrak{g}$, а группы $\mathfrak{g}_v$ при $v \geqslant 1$ известны как *высшие группы ветвления* поля K' над K. Группа $\mathfrak{g}_1$, которую принято по традиции называть *группой инерции* поля K', состоит, как мы видели выше, из автоморфизмов поля K', индуцирующих тождественное отображение на K_1; иными словами, это есть подгруппа в $\mathfrak{g}_0 = \mathfrak{g}$, связанная с K_1 в смысле теории Галуа. Порядок группы $\mathfrak{g}_1$ равен e, и группу $\mathfrak{g}_0/\mathfrak{g}_1$ можно отождествить с группой Галуа поля K_1 над K, которая, как мы знаем, является циклической группой порядка f и порождается автоморфизмом Фробениуса поля K_1 над K.

По-прежнему считая K' расширением Галуа поля K, обозначим через g_v порядок группы $\mathfrak{g}_v$ для каждого $v \geqslant 0$. Тогда $g_v - 1$ есть число отличных от ε элементов λ из $\mathfrak{g}$, для которых $v(\lambda) \geqslant v$. Поэтому мы можем переписать (9) следующим образом:

$$d = \sum_{v=1}^{+\infty} (g_v - 1), \quad d - e + 1 = \sum_{v=2}^{+\infty} (g_v - 1). \tag{10}$$

Предложение 9. *Пусть K' — расширение Галуа поля K с группой Галуа $\mathfrak{g} = \mathfrak{g}_0$, и пусть $\mathfrak{g}_v$, $v \geqslant 1$, — высшие группы ветвления. Положим $G'_0 = R'^{\times}$ и $G'_v = 1 + P'^v$ при $v \geqslant 1$. Тогда для всякого $v \geqslant 1$ группа $\mathfrak{g}_v$ состоит из тех элементов $\lambda \in \mathfrak{g}_1$, для которых $\pi'^{\lambda}\pi'^{-1} \in G'_{v-1}$. Для таких λ образ $\gamma(\lambda)$ элемента $\pi'^{\lambda}\pi'^{-1}$ в группе $\Gamma_v = G'_{v-1}/G'_v$ не зависит от выбора простого элемента π' в K', и отображение $\lambda \to \gamma(\lambda)$ есть морфизм $\mathfrak{g}_v \to \Gamma_v$ с ядром $\mathfrak{g}_{v+1}$.*

Первое утверждение немедленно следует из соотношения (8) и определений. Заменим π' каким-нибудь другим простым элементом в K', который можно записать в виде $\pi' u$, где $u \in R'^{\times}$. Для $\lambda \in \mathfrak{g}_v$ это вызовет лишь появление в $\pi'^{\lambda}\pi'^{-1}$ добавочного множителя $u^{\lambda}u^{-1}$, который по определению $\mathfrak{g}_v$ лежит в $1 + P'^v$, т. е. в G'_v. Это показывает, что $\gamma(\lambda)$ не зависит от выбора π'. Пусть $\lambda, \mu \in \mathfrak{g}_v$. Положим $u = \pi'^{\lambda}\pi'^{-1}$, $v = \pi'^{\mu}\pi'^{-1}$. Тогда $\pi'^{\lambda\mu}\pi'^{-1} = (u^{\mu}u^{-1})uv$. Так как $u \in R'^{\times}$, то $u^{\mu}u^{-1} \in G'_v$. Это показывает, что отображение $\lambda \to \gamma(\lambda)$ есть морфизм и, очевидно, что его ядро совпадает с $\mathfrak{g}_{v+1}$.

Следствие 1. *Для каждого* $v \geqslant 0$ *группа* $\mathfrak{g}_v/\mathfrak{g}_{v+1}$ *коммутативна. При* $v = 0$ *эта группа является циклической группой порядка* f; *при* $v = 1$ — *циклической группой порядка* e_0, *делящего* $q' - 1$, *где* q' — *модуль поля* K'; *при* $v \geqslant 2$ *она изоморфна некоторой подгруппе аддитивной группы кольца* R'/P' *и ее порядок делит* q'.

Для $v = 0$ это было доказано выше. Положим теперь $k' = R'/P'$. Это — поле из q' элементов. Канонический морфизм из R' на k' индуцирует на G_0' морфизм из G_0' на $k'^{\times}$ с ядром G_1', так что Γ_1 является циклической группой порядка $q' - 1$. Аналогично при $v \geqslant 2$ отображение $x' \to 1 + \pi'^{v-1}x'$ из R' на G_{v-1}' определяет изоморфизм из R'/P' на Γ_v. Наши утверждения для $v \geqslant 1$ немедленно вытекают из этих фактов и предложения 9.

Следствие 2. *В предположениях и обозначениях следствия* 1 $e = e_0 p^N$, *где* $N \geqslant 0$ *и* e_0 *взаимно просто с* p.

Это очевидно ввиду следствия 1, поскольку $\mathfrak{g}_1$ имеет порядок e.

Следствие 3. *Если* $v(\lambda)$ *имеет одно и то же значение* v *при всех* $\lambda \neq \varepsilon$ *в* $\mathfrak{g}$, *то* $\mathfrak{g}$ *есть коммутативная группа, порядок которой делит* $q - 1$, *если* $v = 1$, *и делит* q, *если* $v \geqslant 2$.

В самом деле, мы имеем $\mathfrak{g}_v = \mathfrak{g}$, $\mathfrak{g}_{v+1} = \{\varepsilon\}$. Кроме того, если $v \geqslant 1$, то $e = n$, а значит, $f = 1$ и $q = q'$.

Наконец, числа $v(\lambda)$ обладают важными «свойствами транзитивности». Пусть, как и выше, K' — сепарабельное расширение конечной степени n поля K, но не обязательно расширение Галуа, K'' — сепарабельное расширение конечной степени поля K'. Возьмем в качестве L расширение Галуа конечной степени над K, содержащее K''. Пусть K_2 — максимальное неразветвленное расширение поля K, содержащееся в K''. Обозначим через K_2' композит полей K' и K_2, через e' индекс ветвления поля K'' над K' и через f' — его модулярную степень над K'. Так как K' имеет тот же самый модуль q', что и K_1, и K'' и K_2' имеют тот же самый модуль, что и K_2, то K_2 является неразветвленным расширением степени f' над K_1 и K_2' является максимальным неразветвленным расширением поля K', содержащимся в K'', причем его степень над K' равна f'. Поскольку степень поля K' над K_1 равна e, отсюда следует, что степень поля K_2' над K_1 равна ef'. Поэтому степень поля K_2' над K_2 равна e. Всякий K_2-линейный изоморфизм $\sigma\colon K_2' \to L$ индуцирует K_1-линейный изоморфизм $\lambda\colon K' \to L$. Поскольку K_2 является композитом полей K', K_2, то два таких изоморфизма σ, σ' не могут совпадать на K' при $\sigma \neq \sigma'$. Так как имеется ровно e таких изоморфизмов и столько же K_1-линейных изоморфизмов из K' в L,

то $\sigma \to \lambda$ есть биекция первого множества на второе. В частности, каждый изоморфизм λ: $K' \to L$, тождественный на K_1, можно однозначно продолжить до изоморфизма σ: $K_2' \to L$, тождественного на K_2.

Пусть теперь π'' — какой-нибудь простой элемент в K''. Положим

$$G(X) = \mathrm{N}_{K''/K_2'}(X - \pi'') = X^{e'} + \sum_{i=1}^{e'} \alpha_i X^{e'-i}.$$

По следствию 2 предл. 7 § 2 это — многочлен Эйзенштейна над K_2'. В частности, $\alpha_{e'}$ — простой элемент в K_2', равно как и π', ибо K_2' неразветвлено над K'. Пусть λ — любой нетождественный автоморфизм из K' в L, тождественный на K_1. Как мы видели выше, его можно единственным образом продолжить до изоморфизма σ: $K_2' \to L$, тождественного на K_2. Обозначим через G^σ многочлен, полученный применением σ к каждому коэффициенту многочлена G. Тогда

$$G(X) - G^\sigma(X) = \alpha_{e'} - \alpha_{e'}^\sigma + \sum_{i=1}^{e'-1} (\alpha_i - \alpha_i^\sigma) X^{e'-i}.$$

Так как $\alpha_{e'}$ и π' — простые элементы в K_2' и так как K_2' неразветвлено над K', то с учетом уже доказанного имеем

$$\mathrm{ord}_{K_2'}(\alpha_{e'} - \alpha_{e'}^\sigma) = \mathrm{ord}_{K_2'}(\pi' - \pi'^\sigma) = \mathrm{ord}_K(\pi' - \pi'^\lambda) = \nu(\lambda),$$

$$\mathrm{ord}_{K_2'}(\alpha_i - \alpha_i^\sigma) \geqslant \mathrm{ord}_{K_2'}(\pi' - \pi'^\sigma) = \nu(\lambda) \quad (1 \leqslant i \leqslant e'),$$

откуда

$$\mathrm{ord}_K\ (G(\pi'') - G^\sigma(\pi'')) = \nu(\lambda).$$

Но $G(\pi'') = 0$. С другой стороны, G^σ — это унитарный многочлен, корни которого суть образы π''^τ элемента π'' при различных автоморфизмах τ: $K'' \to L$, совпадающих на K_2' с σ. Другими словами,

$$G^\sigma(\pi'') = \prod_\tau (\pi'' - \pi''^\tau),$$

где произведение берется по различным автоморфизмам τ: $K'' \to L$, индуцирующим λ на K' и тождественным на K_2. Пусть теперь функция $\nu'(\tau)$ определена для K, K'', τ так же, как $\nu(\lambda)$ была определена для K, K', λ. Другими словами, положим $\nu'(\tau) = 0$, если автоморфизм τ нетождествен на K_2, а в противном случае положим

$$\nu'(\tau) = \mathrm{ord}_{K''}(\pi'' - \pi''^\tau).$$

Поскольку $\operatorname{ord}_{K''} = e' \cdot \operatorname{ord}_{K'}$, то из предыдущих формул вытекает равенство

$$e'\mathbf{v}(\lambda) = \sum_{\tau} v'(\tau), \tag{11}$$

где сумму можно брать по всем изоморфизмам $\tau\colon K'' \to L$, совпадающим с λ на K', ибо автоморфизмы, нетождественные на K_2, не вносят никакого вклада в сумму в правой части. По аналогичной причине равенство (11) остается справедливым, в случае когда $\lambda\colon K' \to L$ — изоморфизм, нетождественный на K_1. Сопоставляя формулы (9) и (11), получаем еще одно доказательство следствия 4 предл. 4 § 1.

Пусть теперь L — расширение Галуа поля K не обязательно конечной степени. Обозначим через $\mathfrak{G}$ его группу Галуа, топологизированную обычным образом (в качестве фундаментальной системы окрестностей единицы берутся все подгруппы в $\mathfrak{G}$, соответствующие содержащимся в L расширениям конечной степени поля K). Тогда группа $\mathfrak{G}$ компактна и формулы (11) и (9) в совокупности со следствием 4 предл. 4 § 1 можно интерпретировать, сказав, что на семействе всех открытых и замкнутых подмножеств в $\mathfrak{G}$ существует конечно аддитивная функция $\mathbf{H}$ со следующим свойством. Пусть K' — любое расширение конечной степени поля K, содержащееся в L, e — его индекс ветвления над K и d — показатель его дифференты. Обозначим через $\mathfrak{H}$ открытую и замкнутую подгруппу в $\mathfrak{G}$, состоящую из автоморфизмов, тождественных на K'. Тогда $\mathbf{H}(\mathfrak{H}) = d/e$ и $\mathbf{H}(\mathfrak{H}\lambda) = -v(\lambda)/e$ для каждого класса смежности $\mathfrak{H}\lambda$ в $\mathfrak{G}$, отличного от $\mathfrak{H}$ (определение $v(\lambda)$ см. выше). Поэтому мы получим линейную форму $f \to \mathbf{H}(f)$, т. е. «распределение» на пространстве всех локально постоянных функций f на $\mathfrak{G}$, положив $\mathbf{H}(f) = \mathbf{H}(\mathfrak{H}\lambda)$ для характеристической функции f любого класса смежности $\mathfrak{H}\lambda$, где $\lambda \in \mathfrak{G}$ и подгруппа $\mathfrak{H}$ такая, как выше. Линейная форма $\mathbf{H}$ определяется этим соглашением однозначно, потому что всякая локально постоянная функция на $\mathfrak{G}$ может быть записана как конечная линейная комбинация указанных характеристических функций. Мы будем называть $\mathbf{H}$ *распределением Хербранда* на $\mathfrak{G}$. Из наших предыдущих результатов следует, что знание $\mathbf{H}$ дает нам знание свойств ветвления любых полей K'' над K', где K'', K' имеют конечную степень над K и $K \subset K' \subset K'' \subset L$.

§ 4. СЛЕДЫ И НОРМЫ В А-ПОЛЯХ

В этом параграфе мы рассматриваем некоторое **А**-поле k и некоторое сепарабельное алгебраическое расширение k' поля k конечной степени n над k. Объяснения обозначений см. в гл. IV.

Теорема 1. *Пусть k — некоторое* **A***-поле и k' — сепарабельное расширение конечной степени поля k. Тогда k'_w неразветвлено над замыканием k_v поля k в k'_w почти для всех конечных точек w поля k'.*

Пусть χ — базисный характер для k, т. е. нетривиальный характер на $k_{\mathbf{A}}$, тривиальный на k. Положим $\chi' = \chi \circ \mathrm{Tr}_{k'/k}$. Это — характер на $k'_{\mathbf{A}}$, тривиальный на k'. Так как след $\mathrm{Tr}_{k'/k}$ не равен нулю и так как он k-линеен на k', то существует элемент $\xi \in k'$, для которого $\mathrm{Tr}_{k'/k}(\xi) = 1$. Поскольку продолжение следа $\mathrm{Tr}_{k'/k}$ на $k'_{\mathbf{A}}$ является $k_{\mathbf{A}}$-линейным, отсюда следует, что оно отображает $k'_{\mathbf{A}}$ на $k_{\mathbf{A}}$ сюръективно, так что характер χ' нетривиален на $k'_{\mathbf{A}}$. Пусть w — конечная точка поля k' и v — та точка поля k, над которой лежит w. Обозначим через χ_v и χ'_w соответственно характеры, индуцированные характерами χ на k_v и χ' на k'_w. По следствию 3 теор. 1 гл. IV-1 имеем $\chi'_w = \chi_v \circ \mathrm{Tr}_{k'_w/k_v}$. По следствию 1 теор. 3 гл. IV-2 χ_v имеет порядок 0 почти для всех v и χ'_w имеет порядок 0 почти для всех w. Отсюда и из следствия 3 предл. 4 § 1 немедленно вытекает наше утверждение.

Следствие. *В предположениях теоремы* 1 $\mathrm{N}_{k'/k}$ *является открытым морфизмом из $k'^{\times}_{\mathbf{A}}$ на открытую подгруппу в $k^{\times}_{\mathbf{A}}$.*

Согласно следствию 3 теор. 1 гл. IV-1 $\mathrm{N}_{k'/k}$ индуцирует $\mathrm{N}_{k'_w/k_v}$ на $k'^{\times}_w$ почти для всех точек w поля k'. По предложению 5 § 1 индуцированная норма для всех w, включая бесконечные точки, является открытым морфизмом из $k'^{\times}_w$ на открытую подгруппу в $k^{\times}_v$. По теореме 1 (в совокупности с предложением 3 § 1) она отображает $r'^{\times}_w$ на $r^{\times}_v$ почти для всех v. В силу следствия предложения 2 гл. IV-3 наше утверждение немедленно вытекает из этих фактов.

Если k'_w и k_v такие, как выше, то поле k'_w, которое порождается над k_v полем k', сепарабельно над k_v, так что в случае, когда v и, следовательно, w — конечные точки, дифферента поля k'_w над k_v отлична от нуля и может быть записана как $p'^{d(w)}_w$, где $d(w) \geqslant 0$. Этим оправдано следующее определение.

Определение 3. *Пусть k', k такие, как в теореме* 1. *Для каждой конечной точки w поля k' пусть $p'^{d(w)}_w$ — дифферента поля k'_w над замыканием k_v поля k в k'_w. Тогда под дифферентой*

поля k' над k мы понимаем идеал $\prod \mathfrak{p}_w'^{d(w)}$ в k', в случае если k, k' — поля характеристики нуль, и дивизор $\sum d(w) \cdot w$ поля k', в случае если k, k' — поля характеристики $p > 1$. Мы будем обозначать дифференту через $\mathfrak{d}_{k'/k}$ или просто через $\mathfrak{d}$, если это не может привести к путанице.

Теперь мы рассмотрим раздельно случаи характеристики нуль и характеристики $p > 1$.

Предложение 10. *Пусть k — некоторое поле алгебраических чисел, k' — конечное алгебраическое расширение поля k, $\mathfrak{r}$, $\mathfrak{r}'$ — их максимальные порядки и $\mathfrak{d}$ — дифферента поля k' над k. Тогда $\mathfrak{d}^{-1}$ совпадает с множеством тех элементов $\eta \in k'$, для которых $\mathrm{Tr}(\xi\eta) \in \mathfrak{r}$ при всех $\xi \in \mathfrak{r}'$.*

Возьмем любое $\xi \in \mathfrak{r}'$ и любое $\eta \in \mathfrak{d}^{-1}$. Тогда $\xi\eta \in \mathfrak{d}^{-1}$. По определению это означает, что $\xi\eta \in k'$ и $\xi\eta \in p_w'^{-d(w)}$ для всех конечных точек w поля k'. Отсюда следует, что для всех таких точек $\mathrm{Tr}_{k'_w/k_v}(\xi\eta) \in r_v$, поэтому согласно следствию 3 теор. 1 гл. IV-1, $\mathrm{Tr}_{k'_w/k_v}(\xi\eta)$ лежит в $k \cap r_v$ при всех v, и следовательно, лежит в $\mathfrak{r}$. Обратно, предположим, что $\mathrm{Tr}(\xi\eta) \in \mathfrak{r}$ при всех $\xi \in \mathfrak{r}'$ для некоторого $\eta \in k'$. Возьмем $x' = (x'_w) \in k'_{\mathbf{A}}$ и положим $z = \mathrm{Tr}_{k'/k}(x'\eta)$. Тогда по следствию 3 теор. 1 гл. IV-1 $z = (z_v)$ задается формулой

$$z_v = \sum_{w|v} \mathrm{Tr}_{k'_w/k_v}(x'_w\eta).$$

Пусть v — конечная точка поля k. Согласно следствию 1 теор. 1 гл. V-2 проекция кольца $\mathfrak{r}'$ на произведение $\prod r'_w$, взятое по всем точкам w, лежащим над v, всюду плотна в этом произведении. Так как по нашему предположению $z_v \in r_v$ для любого $x' \in \mathfrak{r}'$ и так как z_v непрерывно зависит от x', то $z_v \in r_v$ при любом выборе $x'_w \in r'_w$ для всех точек w, лежащих над v. Отсюда вытекает, что $\mathrm{Tr}_{k'_w/k_v}$ отображает $\eta r'_w$ в r_v, а значит, по определению дифференты, $\eta \in p_w'^{-d(w)}$. Поскольку это имеет место для всех w, элемент η должен лежать в $\mathfrak{d}^{-1}$.

Следствие. *Если $\mathfrak{a}'$ — любой дробный идеал в k', то множество тех элементов $\eta \in k'$, для которых $\mathrm{Tr}_{k'/k}(\xi\eta) \in \mathfrak{r}$ при всех $\xi \in \mathfrak{a}'$, совпадает с дробным идеалом $\mathfrak{a}'^{-1}\mathfrak{d}^{-1}$.*

В самом деле, ввиду предложения 10 это множество состоит из всех η, для которых $\eta\mathfrak{a}' \subset \mathfrak{d}^{-1}$.

Теперь введем два морфизма ι, $\mathfrak{N}$ групп $I(k)$, $I(k')$ дробных идеалов полей k, k' друг в друга. Для этого рассмотрим снова морфизм $a \to \mathrm{id}(a)$ из $k_{\mathbf{A}}^{\times}$ на $I(k)$ с ядром $\Omega_\infty = k_{\mathbf{A}}(P_\infty)^{\times}$, который был определен в гл. V-3. Как там отмечалось, с помощью этого морфизма можно отождествить $I(k)$ с $k_{\mathbf{A}}^{\times}/\Omega_\infty$. Напомним, что $\Omega_\infty = k_\infty^{\times} \times \prod r_v^{\times}$ — это группа, состоящая из иделей (z_v), для которых $|z_v|_v = 1$ для всякой конечной точки v поля k. Если Ω'_∞ — аналогичная группа для поля k', то мы можем также отождествить $I(k')$ с $k_{\mathbf{A}}'^{\times}/\Omega'_\infty$. Обозначим теперь через ι естественное вложение $k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}'^{\times}$. По следствию 1 теор. 1 гл. IV-1 оно отображает каждый элемент $z = (z_v) \in k_{\mathbf{A}}^{\times}$ в такой элемент $\iota(z) = (z'_w) \in k_{\mathbf{A}}'^{\times}$, что $z'_w = z_v$ для любой точки w, лежащей над v. Тогда $|z_v|_v = 1$ влечет $|z'_w|_w = 1$, так что $\iota(z) \in \Omega'_\infty$ тогда и только тогда, когда $z \in \Omega_\infty$. Отсюда видно, что ι определяет инъективный морфизм $I(k) \to I(k')$, который мы будем называть *естественным вложением* группы $I(k)$ в $I(k')$ и который будет обозначаться также через ι. В этих обозначениях имеем $(\mathrm{id}) \circ \iota = \iota \circ (\mathrm{id})$; это равенство можно рассматривать также как определение инъекции $\iota\colon I(k) \to I(k')$. Ясно, что если k'' — расширение конечной степени поля k' и если морфизмы $\iota'\colon k_{\mathbf{A}}'^{\times} \to k_{\mathbf{A}}''^{\times}$ и $\iota''\colon k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}''^{\times}$ определены так же, как был определен морфизм $\iota\colon k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}'^{\times}$, то $\iota'' = \iota' \circ \iota$; поэтому соответствующее соотношение выполняется и для естественных вложений $I(k) \to I(k'')$, $I(k') \to I(k'')$ и $I(k) \to I(k')$. С другой стороны, следствие 3 теор. 1 гл. IV-1 в сочетании с формулой (1) § 1 показывает, что норма $N_{k'/k}$ отображает Ω'_∞ в Ω_∞ и потому определяет морфизм $I(k') \to I(k)$, который тоже принято называть *нормой*; обозначим его через $\mathfrak{N}_{k'/k}$. Имеем $(\mathrm{id}) \circ N_{k'/k} = \mathfrak{N}_{k'/k} \circ (\mathrm{id})$; это равенство можно рассматривать как определение $\mathfrak{N}_{k'/k}$. Если k'' таково, как выше, то $\mathfrak{N}_{k''/k} = \mathfrak{N}_{k'/k} \circ \mathfrak{N}_{k''/k'}$; это немедленно вытекает из соответствующего соотношения для обычных норм. Далее, если n — степень поля k' над k, то $N_{k'/k}(x) = x^n$ для всех $x \in k$; это непосредственно следует из определения $N_{k'/k}$. Отсюда сразу вытекает соответствующее соотношение для продолжения нормы $N_{k'/k}$ на $k_{\mathbf{A}}$. Для $z \in k_{\mathbf{A}}^{\times}$ мы можем записать это соотношение в виде $N_{k'/k}(\iota(z)) = z^n$, откуда следует, что $\mathfrak{N}_{k'/k}(\iota(\mathfrak{a})) = \mathfrak{a}^n$ при всех $\mathfrak{a} \in I(k)$.

По теореме 3 гл. V-3 $I(k)$ и $I(k')$ являются свободными группами, порожденными соответственно простыми идеалами $\mathfrak{p}_v$, $\mathfrak{p}'_w$ в $\mathfrak{r}$, $\mathfrak{r}'$. Сейчас мы дадим описание морфизмов ι, $\mathfrak{N}_{k'/k}$ в терминах этих образующих.

Предложение 11. *Для всякой конечной точки v поля k и всякой точки w поля k', лежащей над v, обозначим через $e(w)$ индекс ветвления и через $f(w)$ модулярную степень поля k'_w над k_v. Тогда*

$$\iota(\mathfrak{p}_v) = \prod_{w|v} \mathfrak{p}_w^{e(w)}, \quad \mathfrak{N}_{k'/k}(\mathfrak{p}'_w) = \mathfrak{p}_v^{f(w)}, \quad \sum_{w|v} e(w) f(w) = n,$$

где произведение в первой формуле и сумма в последней берутся по всем точкам w поля k', лежащим над v.

Первая формула сразу следует из определений, а вторая — из определений, следствия 3 теор. 1 гл. IV-1 и формулы (1) § 1. Что касается последней формулы, то она вытекает из следствия 1 теор. 4 гл. III-4, поскольку $e(w) f(w)$ совпадает со степенью поля k'_w над k_v; она непосредственно следует также из первых двух формул и равенства $\mathfrak{N}_{k'/k}(\iota(\mathfrak{p}_v)) = \mathfrak{p}_v^n$.

Следствие. *Пусть k — некоторое поле алгебраических чисел и $\mathfrak{a}$ — дробный идеал в k. Тогда $\mathfrak{N}_{k/\mathbf{Q}}(\mathfrak{a})$ совпадает с дробным идеалом $\mathfrak{N}(\mathfrak{a})\mathbf{Z}$ в $\mathbf{Q}$, где $\mathfrak{N}$ — норма, введенная в определении 5 гл. V-3.*

Это сразу вытекает из последнего определения и второй формулы предложения 11, примененной к полям k и $\mathbf{Q}$.

Так как каждый идеал в кольце $\mathbf{Z}$ имеет вид $m\mathbf{Z}$, где $m \in \mathbf{N}$, то каждый дробный идеал в $\mathbf{Q}$ может быть одним и только одним способом записан в виде $r\mathbf{Z}$, где $r \in \mathbf{Q}$, $r > 0$. Поэтому можно отождествить группу $I(\mathbf{Q})$ дробных идеалов поля $\mathbf{Q}$ с группой $\mathbf{Q}_+^\times = \mathbf{Q}^\times \cap \mathbf{R}_+^\times$ при помощи изоморфизма $r \to r\mathbf{Z}$ первой группы на вторую. Тогда норма $\mathfrak{N}$ из определения 5 гл. V-3 совпадает с нормой $\mathfrak{N}_{k/\mathbf{Q}}$, определенной выше.

Предложение 12. *Пусть χ — характер на $\mathbf{Q}_\mathbf{A}$, тривиальный на $\mathbf{Q}$, для которого $\chi_\infty(x) = \mathbf{e}(-x)$; k — некоторое поле алгебраических чисел, $\chi' = \chi \circ \mathrm{Tr}_{k/\mathbf{Q}}$; $a = (a_v)$ — дифферентный идель, связанный с χ'. Тогда $a_v = 1$ для каждой бесконечной точки v поля k и $\mathrm{id}(a)$ совпадает с дифферентой $\mathfrak{d}_{k/\mathbf{Q}}$ поля k над $\mathbf{Q}$.*

Характер χ таков же, как введенный в первой части доказательства теоремы 3 гл. IV-2. Там показано, что он однозначно определен сформулированным выше условием и что χ_p имеет порядок 0 для каждой точки p поля $\mathbf{Q}$. Наше первое утверждение непосредственно следует теперь из определения дифферентного иделя в гл. VII-2, если учесть следствие 3 теор. 1 гл. IV-1. Наше последнее утверждение вытекает из того же результата, если учесть следствие 3 предл. 4 § 1.

Следствие. *Пусть поле k таково, как в предложении* 12, *и D — его дискриминант. Тогда* $|D| = \mathfrak{N}(\mathfrak{d}_{k/\mathbf{Q}})$.

Если идель a таков, как в предложении 12, то $|a|_{\mathbf{A}} = |D|^{-1}$ по предложению 6 гл. VII-2. С другой стороны, поскольку $a_v = 1$ для всех бесконечных точек v поля k, то из определения нормы $\mathfrak{N}$ немедленно следует, что $|a|_{\mathbf{A}} = \mathfrak{N}(\mathrm{id}(a))^{-1}$. В силу предложения 12 наше утверждение доказано.

Теперь мы следующим образом обобщим определение дискриминанта, т. е. определение 6 гл. V-4.

Определение 4. *Пусть k — некоторое поле алгебраических чисел, k' — конечное расширение поля k и $\mathfrak{d}$ — дифферента поля k' над k. Тогда идеал $\mathfrak{D} = \mathfrak{N}_{k'/k}(\mathfrak{d})$ в максимальном порядке $\mathfrak{r}$ поля k называется дискриминантом поля k' над k.*

Следует обратить внимание на то, что в соответствии с этим определением дискриминантом поля k над $\mathbf{Q}$ является не D, а идеал $D\mathbf{Z} = |D|\,\mathbf{Z}$ в $\mathbf{Z}$. По заданному идеалу D определяется согласно замечанию в конце доказательства предложения 7 гл. V-4 с помощью формулы $D = (-1)^{r_2}|D|$.

Предложение 13. *Пусть k, k', k'' — поля алгебраических чисел и $k \subset k' \subset k''$, и пусть $\mathfrak{d}$ и $\mathfrak{D}$, $\mathfrak{d}'$ и $\mathfrak{D}'$, $\mathfrak{d}''$ и $\mathfrak{D}''$ — дифференты и дискриминанты соответственно поля k' над k, поля k'' над k', поля k'' над k. Тогда*

$$\mathfrak{d}'' = \iota'(\mathfrak{d})\,\mathfrak{d}', \quad \mathfrak{D}'' = \mathfrak{D}^{n'}\mathfrak{N}_{k'/k}(\mathfrak{D}'),$$

где ι' — естественное вложение $I(k') \to I(k'')$ и n' — степень поля k'' над k'.

Первая формула сразу следует из соответствующего локального результата, т. е. из следствия 4 предл. 4 § 1. Отсюда и из определения 4, с учетом свойства транзитивности норм, вытекает вторая формула.

Пусть теперь k — некоторое $\mathbf{A}$-поле характеристики $p > 1$ и k' — сепарабельное расширение поля k конечной степени n. Так как отображение $a \to \mathrm{div}(a)$ есть морфизм из $k_{\mathbf{A}}^{\times}$ на группу $D(k)$ дивизоров поля k с ядром $\prod \mathfrak{r}_v^{\times}$, то точно так же, как в случае числовых полей, мы видим, что естественное вложение $k_{\mathbf{A}}^{\times} \to k_{\mathbf{A}}'^{\times}$ определяет инъективный морфизм $\iota: D(k) \to D(k')$, который мы будем называть естественным вложением группы $D(k)$ в $D(k')$. Аналогично норме-

ное отображение $N_{k'/k} : k_A'^{\times} \to k_A^{\times}$ определяет морфизм $D(k') \to D(k)$, который мы будем обозначать через $\mathfrak{S}_{k'/k}$ (обозначение $\mathfrak{N}$ было бы здесь неудобно, поскольку группа дивизоров записывается аддитивно). Свойства морфизмов ι и $\mathfrak{S}$ совершенно аналогичны свойствам морфизмов ι и $\mathfrak{N}$ в случае числовых полей. В частности, $\mathfrak{S}_{k'/k}(\iota(\mathfrak{a})) = n\mathfrak{a}$ для каждого дивизора $\mathfrak{a}$ поля k и, в обозначениях предложения 11,

$$\iota(v) = \sum_{w|v} e(w) \cdot w, \quad \mathfrak{S}_{k'/k}(w) = f(w) \cdot v, \quad \sum_{w|v} e(w) f(w) = n,$$

причем доказательство остается прежним. Пусть $\mathbf{F}_q$, $\mathbf{F}_{q'}$ — поля констант в k и k', и пусть f_0 — степень второго поля над первым. Тогда, по определению $f(w)$ и степени точки, $f_0 \deg(w) = f(w) \deg(v)$ и, следовательно, сначала для точек, а затем и для произвольных дивизоров мы получаем

$$\deg(\mathfrak{S}_{k'/k}(\mathfrak{a}')) = f_0 \deg(\mathfrak{a}'), \quad \deg(\iota(\mathfrak{a})) = (n/f_0) \deg(\mathfrak{a}), \tag{12}$$

где $\mathfrak{a}'$ — произвольный дивизор поля k', а $\mathfrak{a}$ — произвольный дивизор поля k.

Пусть $\mathfrak{d}$ — дифферента поля k' над k. Определим *дискриминант* поля k' над k как дивизор $\mathfrak{S}_{k'/k}(\mathfrak{d})$ поля k. В обозначениях, аналогичных обозначениям предложения 13, имеем

$$\mathfrak{d}'' = \iota'(\mathfrak{d}) + \mathfrak{d}', \quad \mathfrak{D}'' = n'\mathfrak{D} + \mathfrak{S}_{k'/k}(\mathfrak{D}').$$

Предложение 14. *Пусть k и k' такие, как выше, $\mathfrak{d}$ — дифферента поля k' над k и $\mathfrak{c}$ — канонический дивизор поля k. Тогда дивизор $\iota(\mathfrak{c}) + \mathfrak{d}$ является каноническим дивизором поля k'.*

По определению канонического дивизора существует базисный характер χ, для которого $\mathfrak{c} = \operatorname{div}(\chi)$. Тогда следствие 3 предл. 4 § 1 в сочетании со следствием 3 теор. 1 гл. IV-1 и с определениями немедленно показывает, что $\operatorname{div}(\chi \circ \mathrm{Tr}_{k'/k}) = \iota(\mathfrak{c}) + \mathfrak{d}$.

Следствие. *Пусть k, k' и $\mathfrak{d}$ таковы, как в предложении* 14, *g — род поля k, n — степень поля k' над k и f_0 — степень поля констант в k' над полем констант в k. Тогда род g' поля k' задается формулой*

$$2g' - 2 = (n/f_0)(2g - 2) + \deg(\mathfrak{d}).$$

Это сразу вытекает из предложения 14, следствия 1 теор. 2 гл. VI и второй из формул (12). Отсюда следует, что степень дифференты всегда четна; более точный результат будет получен в гл. XIII-12.

§ 5. РАСЩЕПИМЫЕ ТОЧКИ В СЕПАРАБЕЛЬНЫХ РАСШИРЕНИЯХ

Теорему 1 § 4 можно переформулировать следующим образом: в предположениях и обозначениях этой теоремы почти для всех точек w поля k' степень поля k'_w над k_v равна модулярной степени поля k'_w над k_v. Поэтому следствия 2 и 3 предл. 1 гл. VII-1 и следствия 3 и 4 теор. 2 гл. VII-5 остаются справедливыми при замене «степени» на «модулярную степень», если дополнительно предположить сепарабельность поля k над k_0. Мы рассмотрим сейчас некоторые следствия из этих результатов.

Как и прежде, пусть k — некоторое **A**-поле, k' — сепарабельное расширение поля k конечной степени n и v — некоторая точка поля k. Мы можем записать $k' = k(\xi)$, где ξ — корень некоторого неприводимого унитарного многочлена $F \in k[X]$ степени n. Сопоставление теоремы 4 гл. III-4 с предложением 2 гл. III-2 показывает, что точки w поля k', лежащие над v, находятся во взаимно однозначном соответствии с неприводимыми унитарными многочленами из $k_v[X]$, делящими F. Если для каждой такой точки w обозначить через F_w соответствующий ей многочлен, то степень поля k'_w над k_v равна степени многочлена F_w. По теореме 1 § 4 почти для всех v эта степень равна модулярной степени поля k'_w над k_v. Мы видели также, что лежащие над v точки w, для которых $k'_w = k_v$, находятся во взаимно однозначном соответствии с корнями многочлена F в k_v. По следствию 1 теор. 4 гл. III-4 тогда и только тогда имеется n различных точек поля k', лежащих над v, когда $k'_w = k_v$ для каждой такой точки. В случае когда это так, говорят, что точка v *вполне расщепима* в k'; это имеет место в том и только в том случае, когда F имеет n различных корней в k_v. Если L — расширение Галуа поля k, то по следствию 4 теор. 4 гл. III-4 пополнения поля L по его точкам, лежащим над v, все между собой изоморфны. Поэтому если $L_u = k_v$ для одной такой точки u, то точка v вполне расщепима в L. Пусть $k' = k(\xi)$ — поле, промежуточное между k и L. Тогда определенный выше многочлен F разлагается в $L[X]$ на линейные множители и наименьшее расширение Галуа L' поля k, содержащееся в L и содержащее k', является подполем в L, порожденным над k корнями F в L. Если теперь t — точка поля L', лежащая над v, то L'_t порождается над k_v корнями многочлена F, так что $L'_t = k_v$ в том и только в том случае, когда точка v вполне расщепима в k'. В этом случае, как мы уже видели, она расщепима также и в L'.

Предложение 15. *Пусть k', k'' — два расширения поля k, содержащиеся оба в некотором сепарабельном расширении L конечной степени над k, и пусть X — множество таких точек v поля k,*

что $k'_w = k_v$ по крайней мере для одной точки w поля k', лежащей над v. Тогда если почти все точки $v \in X$ вполне расщепимы в k'', то k'' содержится в k'.

Можно считать, что L есть композит полей k' и k''. Обозначим через W множество тех точек w поля k', для которых точки v, лежащие под w, вполне расщепимы в k'' и $k'_w = k_v$. Пусть u — точка поля L, лежащая над w, и t — точка поля k'', лежащая под u. Поле L_u порождается над k_v полем L, а следовательно, полями k'_w и k''_t. Поэтому если $w \in W$, то $L_u = k_v$. Это показывает, что все точки из W вполне расщепимы в L. Рассмотрим теперь точку w поля k', не лежащую в W. Обозначим через v точку поля k, лежащую под w. Если $k_v = k'_w$, то точка $v \in X$, так что она должна содержаться в конечном подмножестве в X, состоящем из тех точек в X, которые не вполне расщепимы в k''. Если $k_v \neq k'_w$, то степень поля k'_w над k_v больше 1. По теореме 1 § 4 эта степень совпадает с модулярной степенью, если исключить некоторое конечное множество точек. Таким образом, показано, что модулярная степень поля k'_w над k_v больше 1 почти для всех точек w поля k', не лежащих в W. Применяя теперь к k, k' и L следствие 4 теор. 2 гл. VII-5 (в этом следствии надо заменить k_0, k, k' на k, k', L), получаем, что $k' = L$, т. е. $k'' \subset k'$.

Следствие. *Пусть k', k'' — два расширения Галуа поля k, содержащиеся в некотором расширении конечной степени поля k. Пусть S' и S'' — множества точек поля k, вполне расщепимых в k' и k'' соответственно. Тогда k' содержит k'' в том и только в том случае, когда S'' содержит почти все точки $v \in S'$.*

Если $k' \supset k''$, то, очевидно, точки поля k, вполне расщепимые в k', вполне расщепимы и в k''. Обратно, поскольку k' — расширение Галуа, то S' совпадает с множеством X из предложения 15 и наше утверждение следует из этого предложения. В частности, мы видим, что k' должно совпадать с k'', если S' и S'' различаются лишь конечным числом элементов.

§ 6. ПРИМЕНЕНИЕ К НЕСЕПАРАБЕЛЬНЫМ РАСШИРЕНИЯМ

Сейчас мы докажем, что один из основных наших результатов, а именно теорема 1 гл. IV-1 об изоморфизме между k'_A и $(k'/k)_A$, сформулированная и доказанная для сепарабельных расширений, остается справедливым и без предположения сепарабельности. Для этого нам понадобится одна лемма.

Лемма 1. *Пусть k — некоторое* **A**-*поле характеристики $p > 1$. Тогда поле k чисто несепарабельно и имеет степень p над своим образом k^p при эндоморфизме $x \to x^p$.*

По лемме 1 гл. III-2 можно записать поле k в виде $k = \mathbf{F}_p(x_0, \ldots, x_N)$, где элемент x_0 трансцендентен над $\mathbf{F}_p$, а элементы x_i сепарабельно алгебраичны над $\mathbf{F}_p(x_0)$ для $1 \leqslant i \leqslant N$. Тогда $k^p = \mathbf{F}_p(x_0^p, \ldots, x_N^p)$. Положим $k' = k^p(x_0) = \mathbf{F}_p(x_0, x_1^p, \ldots, x_N^p)$. Так как каждый элемент x_i чисто несепарабелен над $\mathbf{F}_p(x_i^p)$ и сепарабелен над $\mathbf{F}_p(x_0)$, то поле k одновременно чисто несепарабельно и сепарабельно над k', так что $k = k'$. Отсюда следует, что k есть чисто несепарабельное расширение степени 1 или p над k^p. Если бы поле k совпадало с k^p, то оно содержало бы элемент y, такой, что $y^p = x_0$. Ясно, что элемент y не может содержаться в $\mathbf{F}_p(x_0)$, так что он чисто несепарабелен над $\mathbf{F}_p(x_0)$, вопреки предположению о сепарабельности поля k над $\mathbf{F}_p(x_0)$.

Теперь для распространения теоремы 1 гл. IV-1 на случай несепарабельного расширения k' поля k достаточно, очевидно, доказать справедливость в этом случае теоремы 4 гл. III-4, поскольку лишь эта теорема используется при доказательстве теоремы 1 гл. IV-1. Сначала мы сделаем это для чисто несепарабельного расширения степени p поля k. Пусть k' — такое расширение. Тогда для любого $x' \in k'$ должно существовать такое целое $n \geqslant 0$, что $x'^{p^n} \in k$, и если n — наименьшее среди таких чисел, то степень элемента x' над k равна p^n. Так как эта степень должна быть $\leqslant p$, то $n = 0$ или 1. Это показывает, что $k'^p \subset k \subset k'$; следовательно, в силу леммы 1 $k = k'^p$. Для этого случая докажем следующее

Предложение 16. *Пусть k' — некоторое* **A**-*поле характеристики $p > 1$, и пусть $k = k'^p$. Тогда над каждой точкой v поля k лежит одна и только одна точка w поля k'. Эта точка является образом точки v при изоморфизме $x \to x^{1/p}$ поля k в k', $k_v = (k'_w)^p$ и k_v-линейное продолжение Φ_v естественного вложения поля k' в k'_w на $A_v = k' \otimes_k k_v$ является изоморфизмом из A_v на k'_w. Кроме того, если α — какой-либо базис в k' над k и α_v для каждой точки v есть r_v-модуль, порожденный в A_v множеством α, то Φ_v отображает α_v на максимальное компактное подкольцо r'_w в k'_w почти для всех v.*

Пусть v — точка поля k и w — точка поля k', лежащая над v. По следствию предложения 1 гл. III-1 поле k'_w порождается над k_v полем k', следовательно, оно чисто несепарабельно над k_v и его степень равна 1 или p. В первом случае каждый элемент из k должен быть p-й степенью в k_v, что невозможно, поскольку k плотно в k_v

и, значит, содержит хотя бы один простой элемент поля k_v. Поэтому согласно следствию 2 предл. 4 гл. I-4 поле k'_w определено однозначно с точностью до изоморфизма и отображение $y \to y^p$ есть изоморфизм из k'_w на k_v. Пусть λ — естественное вложение $k' \to k'_w$. Это вложение должно индуцировать на k естественное вложение $\lambda_0 : k \to k_v$. Поэтому для каждого $\xi \in k'$ имеем $\lambda_0(\xi^p) = \lambda(\xi)^p$. Так как это равенство однозначно определяет $\lambda(\xi)$, то мы видим, что точка w однозначно определяется по точке v, а также что точка w является образом точки v при изоморфизме $x \to x^{1/p}$. Если теперь отображение Φ_v таково, как в нашем предложении, то, очевидно, оно является сюръективным гомоморфизмом из A_v на k'_w. Так как оба пространства имеют размерность p над k_v, то Φ_v является изоморфизмом. Наконец, пусть α — какой-либо базис в k' над k. Ввиду следствия 1 теор. 3 гл. III-1 и леммы 1 гл. III-2 можно считать, что α содержит такой элемент a, что k' является сепарабельным алгебраическим расширением поля $\mathbf{F}_p(a)$. Пусть точки v и w такие, как выше, и пусть u — точка поля $k_0 = \mathbf{F}_p(a)$, лежащая под w. По теореме 1 § 4 почти для всех w поле k'_w неразветвлено над $(k_0)_u$. Возьмем точку w, для которой это имеет место. Поскольку, как показывает теорема 2 гл. III-3, поле k_0 имеет в точности одну точку u, для которой $|a|_u > 1$, то можно считать также, что w не лежит над этой точкой. Тогда по той же теореме существует такой многочлен $\pi \in \mathbf{F}_p[T]$, что $\pi(a)$ есть простой элемент в $(k_0)_u$ и, следовательно, в k'_w, ибо k'_w неразветвлено над $(k_0)_u$. Далее, по следствию 2 теор. 3 гл. III-1 α_v есть компактное подкольцо в A_v почти для всех v. Отсюда следует, что оно содержит 1 и поэтому $r_v \cdot 1$. Поскольку это кольцо содержит a, оно содержит также $\pi(a)$, а следовательно, содержит кольцо $r_v[\pi(a)]$ и, значит, согласно предложению 4 гл. I-4 и его следствиям, совпадает с r'_w.

Ясно, что из предложения 16 вытекает справедливость теоремы 4 гл. III-4 для случая, когда $k = k'^p$. Рассмотрим теперь произвольное расширение k' конечной степени над k. Обозначим через k'_0 максимальное сепарабельное алгебраическое расширение поля k, содержащееся в k'. Пусть p^m — степень поля k над k'_0 и $x' \in k'$. Тогда существует такое $n \geqslant 0$, что $x'^{p^n} \in k'_0$, и если n — наименьшее среди таких чисел, то x' имеет степень p^n над k'_0, так что $n \leqslant m$. Это показывает, что $k' \supset k'_0 \supset k'^{p^m}$. Применяя к последовательности полей k', k'^p, . . ., k'^{p^m} лемму 1, мы видим, что каждое из этих полей имеет степень p над последующим, так что k' имеет степень p^m над полем k'^{p^m}, которое поэтому совпадает с k'_0. Теперь проведем индукцию по m. Допустим, что теорема 4 гл. III-4 справедлива для расширения k'^p поля k; нам следует доказать ее справедли-

вость для расширения k' поля k. Положим $k'' = k'^p$. Пусть v — некоторая точка поля k. Обозначим через $w'_1, \ldots, w'_r$ точки поля k'', лежащие над v, и для каждого i обозначим через k''_i пополнение поля k'' относительно w'_i. По предложению 16 для каждого i существует одна и только одна точка w поля k', лежащая над w'_i, и пополнение k'_i поля k' относительно w_i может быть отождествлено с $k' \otimes_{k''} k''_i$. По предположению индукции имеет место изоморфизм Φ'_v из $A'_v = k'' \otimes_k k_v$ на прямую сумму полей k'', удовлетворяющий условиям, указанным в формулировке теоремы. По свойствам тензорных произведений произведение $A_v = k' \otimes_k k_v$ очевидным образом канонически изоморфно произведению $k' \otimes_{k''} A'_v$, а значит, прямой сумме произведений $k' \otimes_{k''} k''_i$ и, следовательно, прямой сумме полей k'_i. Очевидно, что так определенный изоморфизм Φ_v из A_v в последнюю сумму обладает всеми нужными свойствами. Что касается последнего утверждения теоремы, то его можно аналогичным способом вывести из нашего предположения индукции с помощью предложения 16, если взять какой-нибудь базис α' в k'' над k, какой-нибудь базис β в k' над k'' и в качестве базиса в k' над k взять базис α, состоящий из всех произведений $a'b$ элементов $a' \in \alpha'$ и $b \in \beta$.

ЧАСТЬ ВТОРАЯ

ТЕОРИЯ ПОЛЕЙ КЛАССОВ

ГЛАВА ДЕВЯТАЯ

ПРОСТЫЕ АЛГЕБРЫ

§ 1. СТРУКТУРА ПРОСТЫХ АЛГЕБР

По существу эта глава чисто алгебраическая. Это означает, что мы будем иметь дело с основным полем, на которое не налагается никаких ограничений, кроме коммутативности, и которое не наделяется никакими дополнительными структурами. Предполагается, что все поля коммутативны, а все алгебры содержат единицу, конечномерны над своим основным полем и центральны (алгебра A над K называется *центральной*, если ее центр совпадает с K). Если A, B — алгебры над K с указанными свойствами, то такова же и алгебра $A \otimes_K B$; если A — алгебра над K с указанными свойствами и L — поле, содержащее поле K, то $A_L = A \otimes_K L$ есть алгебра над L с теми же свойствами. В дальнейшем подразумевается, что тензорные произведения берутся над основным полем. Таким образом, мы пишем просто $A \otimes B$ вместо $A \otimes_K B$, в случае когда A, B — алгебры над K, и пишем просто A_L или $A \otimes L$ вместо $A \otimes \otimes_K L$, в случае когда A — алгебра над K, а L — поле, содержащее K; A_L всегда рассматривается как алгебра над L.

Пусть A — алгебра над K с единицей 1_A. Все модули над A будут предполагаться унитарными (это означает, скажем, для левого модуля M, что $1_A \cdot m = m$ при всех $m \in M$) и конечномерными над K, если ввести на них структуру векторного пространства над K, положив (скажем, для левого модуля M) $\xi m = (\xi \cdot 1_A)\, m$ при всех $m \in M$ и $\xi \in K$. Если M' — подмножество в левом A-модуле M, то его *аннулятором в* A называется множество тех элементов $x \in A$, для которых $xm = 0$ при всех $m \in M'$; это — левый идеал в A. Аннулятор всего M в A является двусторонним идеалом в A. Если этот аннулятор сводится к $\{0\}$, модуль M называется *точным*.

Определение. 1. *Пусть A — алгебра над K. Данный A-модуль называется простым, если он отличен от $\{0\}$ и не обладает другими подмодулями, кроме $\{0\}$ и самого себя. Алгебра A называется простой, если она не обладает другими двусторонними идеалами, кроме $\{0\}$ и самой себя.*

Для каждой алгебры A всегда существуют простые A-модули. Например, любой отличный от $\{0\}$ левый идеал в A минимальной размерности над K является таким модулем.

Предложение 1. *Пусть A — алгебра над K и M — точный простой левый A-модуль. Тогда всякий левый A-модуль разлагается в прямую сумму модулей, каждый из которых изоморфен M.*

Докажем сначала наше утверждение для самой алгебры A, рассматриваемой как левый A-модуль. В M имеются конечные подмножества, аннуляторы которых в A равны $\{0\}$ (примером такого подмножества является любой базис модуля M над K); возьмем любое минимальное множество $\{m_1, \ldots, m_n\}$ с этим свойством. Для $0 \leqslant i \leqslant n$ обозначим через A_i аннулятор множества $\{m_{i+1}, \ldots, m_n\}$ в A; для $i \geqslant 1$ положим $M_i = A_i m_i$. Ясно, что $A_0 = \{0\}$, $A_n = A$. При $i \geqslant 1$ имеем $A_i \supset A_{i-1}$ и $A_i \neq A_{i-1}$, ибо в противном случае из равенств $xm_j = 0$ при $j > i$ следовало бы, что $xm_i = 0$ и элемент m_i не мог бы содержаться среди $m_1, \ldots, m_n$. Пусть $i \geqslant 1$. Тогда A_i — левый идеал в A, M_i — подмодуль в M и отображение $x \to xm_i$ индуцирует на A_i морфизм из A_i на M_i с ядром A_{i-1}, так что этот морфизм определяет изоморфизм из A_i/A_{i-1} на M_i, согласованный со структурами левых A-модулей. Так как $A_i \neq A_{i-1}$, то $M_i \neq 0$, поэтому $M_i = M$. С помощью индукции по i, $0 \leqslant i \leqslant n$, немедленно получаем, что $x \to (xm_1, \ldots, xm_i)$ индуцирует на A_i биективное отображение из A_i на произведение $M^i = M \times \ldots \times M$, где каждый из i сомножителей равен модулю M; очевидно, что это — изоморфизм левых A-модулей. При $i = n$ получаем утверждение нашего предложения для A.

Теперь рассмотрим произвольный левый A-модуль M' и какое-нибудь конечное множество $\{m'_1, \ldots, m'_r\}$, порождающее M' (например, любой базис модуля M' над K). Тогда отображение $A^r \to M'$, при котором $(x_i)_{1 \leqslant i \leqslant r} \to \sum x_i m'_i$, является сюръективным морфизмом левых A-модулей. Ввиду только что доказанного изоморфизма A как левого A-модуля с M^n при некотором n отсюда видно, что существует сюръективный морфизм из M^{nr} на M', или, что то же самое, сюръективный морфизм F из прямой суммы $s = nr$ модулей M_i, изоморфных M, на M'. Обозначим через N ядро морфизма F и возьмем максимальное подмножество $\{M_{i_1}, \ldots, M_{i_h}\} \subset \{M_1, \ldots, M_s\}$, для которого сумма $N' = N + \sum M_{i_\lambda}$ прямая. Переходя, если надо, к другой нумерации M_i, мы можем считать, что выбранное нами подмножество есть $\{M_1, \ldots, M_h\}$. Тогда при $j > h$ сумма $N' + M_j$ не является прямой, так что $N' \cap M_j \neq \{0\}$. Так как это пересечение является подмодулем в M_j, изоморфном

M, то оно совпадает с M_j, откуда $M_j \subset N'$ для всех $j > h$. Поэтому F отображает N' на M'. Поскольку его ядро совпадает с N, отображение F определяет изоморфизм из $\sum_{i=1}^{h} M_i$ на M'.

Предложение 2. *Пусть A и M таковы, как в предложении* 1, *и пусть D — кольцо эндоморфизмов модуля M. Тогда D является алгеброй с делением над K и алгебра A изоморфна $M_n(D)$ для некоторого $n \geqslant 1$.*

Напомним, что здесь, как это объяснялось на стр. 16, мы рассматриваем D как кольцо правых операторов на M и соответственно определяется умножение в этом кольце. Так как D — подпространство кольца всех эндоморфизмов векторного пространства M над K, то D — конечномерное векторное пространство над K. Каждый элемент из D отображает M на подмодуль в M, а следовательно, на M или на $\{0\}$. Поэтому если этот элемент ненулевой, то он является автоморфизмом и, следовательно, обратим. Отсюда видно, что D — алгебра с делением над своим центром, который конечномерен над K. Согласно предложению 1, для некоторого $n \geqslant 1$ существует изоморфизм алгебры A, рассматриваемой как левый A-модуль, на M^n. Он определяет изоморфизм между кольцами эндоморфизмов этих двух левых A-модулей. Ясно, что кольцо эндоморфизмов модуля M^n состоит из отображений

$$(m_j)_{1 \leqslant j \leqslant n} \longrightarrow \left(\sum m_i d_{ij}\right)_{1 \leqslant j \leqslant n},$$

где $d_{ij} \in D$ при $1 \leqslant i, j \leqslant n$, и потому может быть отождествлено с кольцом $M_n(D)$ матриц (d_{ij}) над D. С другой стороны, для всякого эндоморфизма f алгебры A, рассматриваемой как левый A-модуль, имеем $f(xy) = xf(y)$ при всех $x, y \in A$. Полагая $y = 1_A$, мы видим, что f можно записать в виде $x \to xa$, где $a = f(1_A)$. Итак, кольцо таких эндоморфизмов можно отождествить с алгеброй A, которая, таким образом, изоморфна $M_n(D)$. Поскольку центр кольца $M_n(D)$, очевидно, изоморфен центру кольца D, отсюда следует, что последний совпадает с K, чем и завершается наше доказательство.

Теорема 1. *Алгебра A над K проста тогда и только тогда, когда она изоморфна некоторой алгебре $M_n(D)$, где D — алгебра с делением над K. По заданной алгебре A число n определяется однозначно, а алгебра D — однозначно с точностью до изоморфизма.*

Пусть алгебра A проста. Возьмем любой простой левый A-модуль M. Так как аннулятор модуля M в A является двусторонним идеалом в A, отличным от A, то он равен $\{0\}$. Поэтому модуль M точен, и мы можем применить к A и M предложение 2, которое показывает, что алгебра A изоморфна алгебре $M_n(D)$.

Обратно, пусть $A = M_n(D)$. Для $1 \leqslant h, k \leqslant n$ обозначим через e_{hk} матрицу (x_{ij}), для которой $x_{hk} = 1$, $x_{ij} = 0$ при $(i, j) \neq (h, k)$. Если $a = (a_{ij})$ — произвольная матрица из $M_n(D)$, то при всех i, j, h, k имеем $e_{ij}ae_{hk} = a_{jh}e_{ik}$. Отсюда видно, что при $a \neq 0$ двусторонний идеал в A, порожденный элементом a, содержит все e_{ik}, а следовательно, совпадает с A, так что алгебра A проста. Пусть теперь M — левый идеал, порожденный элементом e_{11} в A. Он состоит из матриц (a_{ij}), для которых $a_{ij} = 0$ при $j \geqslant 2$. Если a —такая матрица, то $e_{ij}a = a_{j1}e_{i1}$, откуда следует, что при $a \neq 0$ левый идеал, порожденный матрицей $a \in M$, совпадает с модулем M, который поэтому является минимальным левым идеалом и простым левым A-модулем. Пусть теперь f — эндоморфизм левого A-модуля M. Положим $f(e_{11}) = a$, где $a = (a_{ij})$, $a_{ij} = 0$ при $j \geqslant 2$. Записав $f \cdot (e_{ij}e_{11}) = e_{ij}a$, видим, что $a_{j1} = 0$ при $j \geqslant 2$. Далее, для $x = (x_{ij})$ с $x_{ij} = 0$ при $j \geqslant 2$ получаем $f(x) = f(xe_{11}) = xa = (x_{ij}a_{11})$. Отсюда вытекает, что кольцо эндоморфизмов модуля M изоморфно D. Так как по предложению 1 все простые левые A-модули изоморфны M, это показывает, что с точностью до изоморфизма D определяется по A однозначно. Поскольку размерность A над K в n^2 раз больше размерности D над K, число n также однозначно определяется по A.

Напомним, что *противоположной алгеброй* для алгебры A называется алгебра A°, совпадающая с A как векторное пространство над K, но наделенная законом умножения $(x, y) \to yx$ вместо $(x, y) \to xy$.

Предложение 3. *Пусть A — алгебра над K, A° — противоположная алгебра и $C = A \otimes A^\circ$. Для $a, b \in A$ обозначим через $f(a, b)$ эндоморфизм $x \to axb$ векторного пространства A. Пусть F есть K-линейное отображение $C \to \mathrm{End}_K(A)$, для которого $F(a \otimes b) = f(a, b)$ при всех a, b. Тогда алгебра A проста в том и только том случае, когда F отображает C на $\mathrm{End}_K(A)$ сюръективно. В случае когда это имеет место, F является изоморфизмом из C на $\mathrm{End}_K(A)$.*

Сразу видно, что F есть гомоморфизм из C в $\mathrm{End}_K(A)$. Если N — размерность алгебры A над K, то как C, так и $\mathrm{End}_K(A)$ имеют размерность N^2 над K, поэтому F является изоморфизмом из C на $\mathrm{End}_K(A)$ в том и только в том случае, когда он сюръективен, и в том и только в том случае, когда он инъективен. Предположим, что алгебра A непроста, т. е. имеет двусторонний идеал I, отличный от $\{0\}$ и от A. Тогда $f(a, b)$ отображает I в I при всех a, b, поэтому то же самое верно для $F(c)$ при всех $c \in C$, так что образ алгебры C

при отображении F не совпадает со всей алгеброй $\mathrm{End}_K(A)$. Предположим теперь, что алгебра A проста, и обозначим через M векторное пространство A над K, на котором определена структура левого C-модуля с помощью закона $(c, x) \to F(c)x$. Любой подмодуль M' в M переходит в себя при всех отображениях $x \to axb$, где $a, b \in A$, и, значит, является двусторонним идеалом в A. Так как алгебра A проста, это показывает, что модуль M прост.

Эндоморфизм φ модуля M — это отображение φ, для которого $\varphi(axb) = a\varphi(x)b$ при всех $a, x, b \in A$. При $x = b = 1_A$ это дает $\varphi(a) = a\varphi(1_A)$, следовательно, $axb\varphi(1_A) = ax\varphi(1_A)b$, так что $\varphi(1_A)$ лежит в центре K алгебры A, другими словами, φ имеет вид $x \to \xi x$, где $\xi \in K$. Обозначим через C' аннулятор модуля M в C, который совпадает с ядром морфизма F. Мы можем применить к алгебре C/C', ее центру Z и модулю M предложение. 2. Поскольку в данном случае $D = K$, это предложение показывает, что алгебра C/C' изоморфна некоторой алгебре $M_n(K)$; значит, ее центр Z изоморфен K. Но тогда, как мы видели при доказательстве теоремы 1, размерность M над K должна равняться n, так что $n = N$. Так как C/C' имеет ту же самую размерность N^2 над K, что и C, мы получаем $C' = \{0\}$, чем наше доказательство и заканчивается.

Следствие 1. *Пусть L — поле, содержащее K. Тогда алгебра $A_L = A \otimes L$ над L проста в том и только в том случае, когда проста алгебра A.*

В самом деле, пусть C_L, F_L определены для A_L так же, как C, F были определены для A в предложении 3. Сразу видно, что $C_L = C \otimes L$ и что F_L является L-линейным продолжением отображения F на C_L. Наше утверждение следует поэтому из предложения 3.

Следствие 2. *Пусть L — алгебраически замкнутое поле, содержащее K. Тогда алгебра A проста в том и только в том случае, когда алгебра A_L изоморфна некоторой алгебре $M_n(L)$.*

Если D — алгебра с делением над полем K, то расширение поля K, порожденное в D любым элементом $\xi \in D - K$, является алгебраическим расширением поля K, отличным от K. В частности, если поле L алгебраически замкнуто, то не существует алгебр с делением над L, отличных от L. Поэтому в силу теоремы 1 алгебра над L проста тогда и только тогда, когда она изоморфна некоторой алгебре $M_n(L)$. Наше утверждение вытекает поэтому из следствия 1.

Следствие 3. *Размерность всякой простой алгебры A над K равна n^2, где n — некоторое натуральное число.*

В самом деле, пусть L — алгебраическое замыкание поля K. По следствию 2 алгебра A_L изоморфна некоторой алгебре $M_n(L)$, так что ее размерность над L, которая совпадает с размерностью алгебры A над K, равна n^2.

Следствие 4. *Пусть A и B — две простые алгебры над K. Тогда алгебра $A \otimes B$ также проста над K.*

Возьмем какое-нибудь алгебраическое замыкание L поля K; алгебра $(A \otimes B)_L$ совпадает с $A_L \otimes B_L$. Поскольку для всех m, n и всех полей K алгебра $M_n(K) \otimes M_m(K)$, очевидно, изоморфна алгебре $M_{nm}(K)$, наше заключение вытекает из следствия 2.

Следствие 5. *Пусть A — простая алгебра размерности n^2 над K; L — поле, содержащее K, и F — некоторый K-линейный гомоморфизм из A в $M_n(L)$. Тогда L-линейное продолжение F_L гомоморфизма F на A_L является изоморфизмом из A_L на $M_n(L)$.*

Ясно, что F_L — гомоморфизм алгебры A_L в $M_n(L)$, так что его ядро является двусторонним идеалом в A_L. Поскольку алгебра A_L проста согласно следствию 1 и поскольку $F_L \neq 0$, упомянутое ядро равно $\{0\}$, т. е. гомоморфизм F_L инъективен. Так как A_L и $M_n(L)$ имеют одну и ту же размерность n^2 над L, отсюда следует биективность гомоморфизма F_L, так что F_L есть изоморфизм из A_L на $M_n(L)$.

Следствие 6. *Пусть L — расширение поля K степени n, и пусть A — простая алгебра размерности n^2 над K, содержащая подполе, изоморфное полю L. Тогда алгебра A_L изоморфна $M_n(L)$.*

Можно считать, что A содержит L. Тогда отображение $(x, \xi) \to x\xi$, где $x \in A$, $\xi \in L$, определяет на A структуру векторного пространства над L; обозначим это векторное пространство через V. Ясно, что размерность V над L равна n. Для каждого элемента $a \in A$ отображение $x \to ax$ можно рассматривать как эндоморфизм векторного пространства V, задаваемый в некотором фиксированном базисе пространства V над L матрицей $F(a) \in M_n(L)$. Наше утверждение вытекает поэтому из следствия 5.

Предложение 4. *Пусть A — простая алгебра над K. Тогда каждый автоморфизм α алгебры A над K имеет вид $x \to a^{-1}xa$, где $a \in A^\times$.*

Выберем какой-нибудь базис $\{a_1, \ldots, a_N\}$ в A над K. Тогда каждый элемент из $A \otimes A^0$ одним и только одним способом можно записать в виде $\sum a_i \otimes b_i$, где $b_i \in A^0$ при $1 \leqslant i \leqslant N$. По предложению 3 автоморфизм α можно записать в виде $x \to \sum a_i x b_i$. Поскольку

ку $\alpha(xy) = \alpha(x)\alpha(y)$ при всех x, y, получаем

$$0 = \sum a_i x y b_i - \sum a_i x b_i \alpha(y) = \sum a_i x (y b_i - b_i \alpha(y)).$$

Для всякого $y \in A$ это выполняется при всех x. Поэтому в силу предложения 3 имеем $y b_i = b_i \alpha(y)$. В частности, $y(b_i z) = b_i \alpha(y)$ при всех y, $z \in A$; следовательно, $b_i A$ является двусторонним идеалом в A, т. е. $b_i A = A$ или $\{0\}$ при всех i, так что элемент b_i или равен нулю, или обратим в A. Так как α — автоморфизм, то все b_i не могут равняться нулю. Беря $a = b_i \neq 0$, получаем наше утверждение.

Следствие. *Пусть α и a таковы, как в предложении* 4, *и пусть элемент $a' \in A$ таков, что $a'\alpha(x) = xa'$ при всех $x \in A$. Тогда $a' = \xi a$, где $\xi \in K$.*

В самом деле, наше предположение можно записать в виде равенства $a'a^{-1}x = xa'a^{-1}$ при всех x, которое означает, что $a'a^{-1}$ лежит в центре K алгебры A.

Предложение 4 общеизвестно как *теорема Сколема — Нётер* (хотя иногда это название резервируют для более общего утверждения, охватывающего и случай простых подалгебр в A). Совершенно аналогично можно доказать, что каждое дифференцирование алгебры A имеет вид $x \to xa - ax$, где $a \in A$.

Нам понадобится также одно уточнение следствия 2 предл. 3, которое появится как следствие приводимого ниже предложения.

Предложение 5. *Пусть D — алгебра с делением над K, отличная от K. Тогда D содержит сепарабельное алгебраическое расширение поля K, отличное от K.*

Мы воспроизведем доказательство Артина. В алгебре D, рассматриваемой как векторное пространство над K, возьмем подпространство E, дополнительное к $K = K \cdot 1_D$, и обозначим через φ проекцию из $D = E \oplus K \cdot 1_D$ на E. Тогда для каждого целого числа $m \geqslant 1$ $x \to \varphi(x^m)$ есть полиномиальное отображение из D в E, продолжение которого на D_L и E_L, где L — любое поле, содержащее K, записывается опять в виде $x \to \varphi(x^m)$, где той же буквой φ обозначено L-линейное продолжение проекции φ до отображения $D_L \to E_L$. Обозначим через N размерность алгебры D над K. Ясно, что каждый элемент $\xi \in D$, не лежащий в K, порождает над K расширение $K(\xi)$, степень которого > 1 и $\leqslant N$. Далее, если это расширение не чисто несепарабельно над K, то оно содержит сепарабельное расширение поля K, отличное от K.

Предположим теперь, что наше предложение несправедливо для D. Тогда K имеет несепарабельные расширения, откуда следует что его характеристика $p > 1$ и что K не является конечным полем. Кроме того, каждый элемент $\xi \in D$ должен быть чисто несепарабельным над K и, следовательно, удовлетворять уравнению $\xi^{p^n} = x \in K$, где p^n — его степень над K. Так как эта степень $\leqslant N$, то она делит наибольшую степень q числа p, не превосходящую N, так что $\xi^q \in K$. Поэтому, если E и φ такие, как выше, то полиномиальное отображение $x \to \varphi(x^q)$ переводит D в 0. Так как поле K бесконечно, отсюда следует, что то же верно для продолжения этого отображения до отображения $D_L \to E_L$, где L — любое поле, содержащее K. Другими словами, отображение $x \to x^q$ переводит алгебру D_L в ее центр $L \cdot 1_D$ для всех L. Но это явно невозможно в случае, когда поле L алгебраически замкнуто. Действительно, в этом случае алгебра D_L изоморфна некоторой алгебре $M_n(L)$, и, взяв, например, $x = e_{11}$ (в обозначениях, использовавшихся при доказательстве теоремы 1), мы получим $x^q = e_{11}$, а этот элемент не лежит в центре алгебры $M_n(L)$.

Следствие. *Пусть A — простая алгебра над K и L — сепарабельно алгебраически замкнутое поле, содержащее K. Тогда алгебра A_L изоморфна некоторой алгебре $M_n(L)$.*

Наше предположение означает, что L не имеет сепарабельных алгебраических расширений, отличных от L. Поэтому предложение 5 показывает, что не существует алгебр с делением над L, отличных от L. Наше заключение немедленно вытекает теперь из теоремы 1 в сочетании со следствием 1 предл. 3.

§ 2. ПРЕДСТАВЛЕНИЯ ПРОСТОЙ АЛГЕБРЫ

Пусть A — простая алгебра над K. По следствию 3 предл. 3 § 1 ее размерность N над K можно записать в виде $N = n^2$. Для любого поля L, содержащего K, обозначим через $\mathfrak{M}_L$ пространство K-линейных отображений $A \to M_n(L)$. Каждое такое отображение F можно однозначно продолжить до L-линейного отображения $F_L : A_L \to M_n(L)$. Если выбран какой-нибудь базис $\alpha = \{a_1, \ldots, a_N\}$ в A над K, то F однозначно определяется N матрицами $X_i = F(a_i)$, так что, при данном выборе базиса, $\mathfrak{M}_L$ отождествляется с пространством наборов $(X_i)_{1 \leqslant i \leqslant N}$ из N матриц, лежащих в $M_n(L)$. Очевидно, что размерность последнего пространства над L равна N^2.

По следствию 5 предл. 3 § 1 тогда и только тогда отображение $F \in \mathfrak{M}$ является изоморфизмом из A в $M_n(L)$, а его продолжение

F_L на A_L является изоморфизмом из A_L на $M_n(L)$, когда F есть гомоморфизм, т. е. когда $F(1_A) = 1_n$ и $F(ab) = F(a)F(b)$ при всех a, b из A, или, что то же самое, при всех a, b из базиса α. В случае когда это имеет место, мы говорим, что F является *L-представлением* алгебры A. Если мы обозначим через $K(F)$ поле, порожденное над полем K коэффициентами матриц $F(a)$ при всех $a \in A$, или, что дает то же самое поле, при всех $a \in \alpha$, то F является также $K(F)$-представлением алгебры A.

При подходящем выборе поле L (например, по следствию 2 предл. 3 § 1 для алгебраически замкнутого L или даже для сепарабельно алгебраически замкнутого L, по следствию предл. 3 § 7) множество L-представлений алгебры A непусто. Далее, если F и F' принадлежат этому множеству, то $F'_L \circ F_L^{-1}$ есть автоморфизм алгебры $M_n(L)$ и, значит, по предложению 4 § 1, имеет вид $X \to Y^{-1}XY$, где $Y \in M_n(L)^\times$. Таким образом, $F'_L(F_L^{-1}(X)) = Y^{-1}XY$. При $a \in A$ и $X = F(a)$ отсюда следует, что $F'(a) = Y^{-1}F(a)Y$; это соотношение мы будем записывать в виде равенства $F' = Y^{-1}FY$. При этом, согласно следствию предложения 4 § 1, по заданным F, F' элемент Y определяется однозначно с точностью до множителя из центра $L^\times$ группы $M_n(L)^\times$.

Предложение 6. *Пусть A — простая алгебра размерности n^2 над K. Тогда существуют такая K-линейная форма $\tau \neq 0$ и такая K-значная функция ν на A, что если L — любое поле, содержащее K, и F — любое L-представление алгебры A, то $\tau(a) = \operatorname{tr}(F(a))$ и $\nu(a) = \det(F(a))$ для всех $a \in A$. Если поле K бесконечно, то ν является полиномиальной функцией степени n на A.*

Положим $N = n^2$ и выберем какой-нибудь базис $\{a_1, \ldots, a_N\}$ в A над K. Возьмем сначала в качестве L «сепарабельное алгебраическое замыкание» поля K, т. е. объединение всех сепарабельных алгебраических расширений поля K в некотором алгебраически замкнутом поле, содержащем K; поле L всегда бесконечно. Согласно следствию предложения 5, существует хотя бы одно L-представление F алгебры A. Как мы видели выше, всякое другое такое представление можно записать в виде $F' = Y^{-1}FY$, где $Y \in M_n(L)^\times$. Ясно, что отображение $a \to \operatorname{tr}(F_L(a))$ есть L-линейная форма τ на A_L и отображение $a \to \det(F_L(a))$ есть полиномиальная функция ν степени n на A. Так как F_L — изоморфизм из A_L на $M_n(L)$, то $\tau \neq 0$. Ни τ, ни ν не изменятся, если заменить F на $F' = Y^{-1}FY$. Записывая a в виде $a = \sum x_i a_i$, где $x_i \in L$ при $1 \leqslant i \leqslant N$, мы можем представить τ и ν соответственно как линейную форму и как однородный многочлен степени n от x_i с коэффициентами из L. Пусть σ — произвольный автоморфизм поля L над K. Будем

обозначать через τ^σ и ν^σ соответственно многочлены от x_i, полученные заменой каждого коэффициента в τ и ν образом этого коэффициента при автоморфизме σ. Аналогично мы будем писать F^σ для обозначения L-представления алгебры A, для которого $F^\sigma(a)$ совпадает с образом $F(a)^\sigma$ матрицы $F(a)$ под действием автоморфизма σ (т. е. $F(a)^\sigma$ — матрица, коэффициенты которой суть образы соответствующих коэффициентов матрицы $F(a)$) при каждом a из базиса $\{a_1, \ldots, a_N\}$. Тогда, очевидно, $\tau^\sigma(a)$ и $\nu^\sigma(a)$ при всех $a \in A$ являются соответственно следом и определителем матрицы $F^\sigma(p)$. Поэтому, как мы видели выше, они должны совпадать с $\tau(a)$, $\nu(a)$ при всех $a \in A_L$. Отсюда следует, что все коэффициенты в τ и ν, записанных как многочлены от x_i, инвариантны относительно автоморфизмов поля L над K; следовательно, эти коэффициенты лежат в K. Этим доказано наше утверждение для L-представлений с выбранным выше L. Очевидно, что оно остается справедливым и для L'-представлений, где L' — любое поле, содержащее L. Поскольку каждое поле, содержащее K, изоморфно над K некоторому подполю такого поля L', доказательство нашего предложения закончено.

Функции τ и ν на A, определенные в предложении 6, называются соответственно *приведенным следом* и *приведенной нормой*. Ясно, что $\tau(xy) = \tau(yx)$ и $\nu(xy) = \nu(x)\nu(y)$ при всех x, y из A; в частности, ν определяет морфизм группы $A^\times$ в $K^\times$.

Следствие 1. *Пусть A и ν такие, как в предложении* 6. *Тогда для всякого $a \in A$ определители эндоморфизмов $x \to ax$, $x \to xa$ векторного пространства A над K равны оба $N_{A/K}(a) = \nu(a)^n$.*

Очевидно, достаточно проверить это для алгебры A_L с подходящим L. Возьмем такое L, чтобы алгебра A_L была изоморфна алгебре $M_n(L)$. Тогда видно, что достаточно проверить наше утверждение для алгебры $M_n(L)$ над L; но для нее это утверждение очевидно.

Этот результат был анонсирован в замечаниях, предшествовавших теореме 4 гл. IV-3.

Следствие 2. *Пусть D — алгебра с делением над K, и пусть τ_0, ν_0 — приведенный след и приведенная норма на D. Для любого $m \geqslant 1$ положим $A = M_m(D)$ и обозначим через τ, ν приведенный след и приведенную норму на A. Тогда $\tau(x) = \sum_i \tau_0(x_{ii})$ для каждой матрицы $x = (x_{ij})$ из A, а если матрица $x = (x_{ij}) \in A$ треугольна, т. е. если $x_{ij} = 0$ при $1 \leqslant j < i \leqslant m$, то $\nu(x) = \prod_i \nu_0(x_{ii})$.*

Возьмем такое L, чтобы алгебра D имела L-представление F. Тогда отображение, которое матрице $x = (x_{ij})$ из $M_m(D)$ сопоставляет матрицу, получающуюся заменой каждого элемента x_{ij} в x матрицей $F(x_{ij})$, является L-представлением алгебры A. Используя это представление для определения τ и ν, немедленно получаем наше утверждение.

Следствие 3. *В обозначениях и предположениях следствия* 2 *имеем* $\nu(A^\times) = \nu_0(D^\times)$.

Мы можем рассмотреть A как кольцо эндоморфизмов левого векторного пространства $V = D^m$ над D. Тогда $A^\times$ будет группой автоморфизмов этого пространства. Имеет место элементарный результат (уже использовавшийся при доказательстве следствия 3 теор. 3 гл. I-2, правда лишь для векторного пространства над коммутативным полем), согласно которому всякий автоморфизм пространства V можно разложить в произведение автоморфизмов, каждый из которых либо является перестановкой координат, либо имеет вид

$$(x_1, \ldots, x_m) \longrightarrow (\sum_i x_i a_i, x_2, \ldots, x_m),$$

где $a_1 \in D^\times$ и $a_i \in D$ при $2 \leqslant i \leqslant m$. По следствию 2 последний автоморфизм имеет приведенную норму $\nu_0(a_1)$. Что касается перестановки координат, то то же самое L-представление алгебры A, которое было использовано при доказательстве следствия 2, немедленно показывает, что ее приведенная норма равна 1, если размерность d^2 алгебры D над K четна, и равна ± 1, если эта размерность нечетна. Поскольку $\nu_0(-1_D) = (-1)^d$, тем самым показано, что множество значений $\nu(A^\times)$ содержит $\nu_0(D^\times)$ и содержится в нем.

§ 3. СИСТЕМЫ ФАКТОРОВ И ГРУППА БРАУЭРА

Рассматриваемые с точностью до изоморфизма, все алгебры над фиксированным полем K образуют множество, поскольку структуры алгебры, которые можно ввести на заданном векторном пространстве над K, образуют множество, и каждое такое пространство изоморфно пространству K^n для некоторого n.

Начиная с этого места, мы будем рассматривать только *простые* алгебры над K. По-прежнему предполагается, что они конечномерны и центральны над K. Рассмотрим две такие алгебры A, A'. По теореме 1 § 1 они изоморфны алгебрам $M_n(D)$, $M_{n'}(D')$, где D, D' — алгебры с делением над K, определяемые по A, A' однозначно с точностью до изоморфизма. Говорят, что алгебры A и A' *подобны*,

а также что они *принадлежат одному классу*, если алгебры D и D' изоморфны над K. Ясно, что в каждом классе простых алгебр существует с точностью до изоморфизма одна и только одна алгебра с делением и не более одной алгебры заданной размерности над K. Алгебра называется *тривиальной* над K, если она подобна K, т. е. изоморфна алгебре $M_n(K)$ для некоторого n. Символом $\mathrm{Cl}(A)$ мы будем обозначать класс простых алгебр, подобных алгебре A.

Пусть A, A' — две простые алгебры, изоморфные $M_n(D)$ и $M_{n'}(D')$ соответственно, где D, D' — алгебры с делением над K. По следствию 4 предл. 3 § 1 алгебра $D \otimes D'$ проста и, следовательно, изоморфна некоторой алгебре $M_m(D'')$, где D'' — алгебра с делением над K, с точностью до изоморфизма однозначно определяемая по D, D' и, следовательно, по A, A'. В силу ассоциативности тензорных произведений алгебра $A \otimes A'$ изоморфна $M_{nn'm}(D'')$. Это показывает, что класс алгебры $A \otimes A'$ однозначно определяется классами алгебр A, A'. Положим теперь

$$\mathrm{Cl}(A \otimes A') = \mathrm{Cl}(A) \cdot \mathrm{Cl}(A')$$

и рассмотрим это соотношение как закон композиции на множестве классов простых алгебр над K. Эта композиция ассоциативна и коммутативна, и для нее имеется нейтральный элемент, а именно класс $\mathrm{Cl}(K)$ тривиальных алгебр над K. Кроме того, если A° — алгебра, противоположная алгебре A, то, согласно предложению 3 § 1, алгебра $A \otimes A^\circ$ тривиальна, так что класс $\mathrm{Cl}(A^\circ)$ является противоположным для $\mathrm{Cl}(A)$ относительно нашего закона композиции. Поэтому относительно этого закона классы простых алгебр над K образуют группу, которую принято называть *группой Брауэра* поля K; мы будем обозначать ее через $B(K)$. Если K' — любое поле, содержащее поле K, и A — простая алгебра над K, то, очевидно, класс алгебры $A_{K'}$ однозначно определяется классом алгебры A и отображение $\mathrm{Cl}(A) \to \mathrm{Cl}(A_{K'})$ является морфизмом из $B(K)$ в $B(K')$; мы будем называть его *естественным морфизмом* из $B(K)$ в $B(K')$.

Покажем теперь, что группу Брауэра можно определить другим способом, с помощью так называемых *систем факторов*. Это потребует некоторых предварительных определений. Выберем раз и навсегда какое-нибудь алгебраическое замыкание $\bar{K}$ поля K. Мы будем обозначать через K_{sep} максимальное сепарабельное расширение поля K в $\bar{K}$, т. е. объединение всех сепарабельных расширений конечной степени поля K, содержащихся в $\bar{K}$. Обозначим через $\mathfrak{G}$ группу Галуа поля K_{sep} на K, топологизированную обычным образом: в качестве фундаментальной системы окрестностей единицы ε

берутся все подгруппы в $\mathfrak{G}$, соответствующие сепарабельным расширениям конечной степени поля K. В такой топологии группа $\mathfrak{G}$, очевидно, вполне несвязна и компактна. Так как поле $\bar{K}$ чисто несепарабельно над K_{sep}, то каждый автоморфизм поля K_{sep} можно однозначно продолжить до автоморфизма поля $\bar{K}$, так что группу $\mathfrak{G}$ можно отождествить с группой всех автоморфизмов поля $\bar{K}$ над K.

Определение 2. *Пусть* $\mathfrak{G}^{(m)} = \mathfrak{G} \times \ldots \times \mathfrak{G}$ — *произведение* m *сомножителей, равных* $\mathfrak{G}$, *и* $\mathfrak{H}$ — *открытая подгруппа в* $\mathfrak{G}$. *Тогда отображение* f *из* $\mathfrak{G}^{(m)}$ *в некоторое множество* S *называется* $\mathfrak{H}$*-регулярным, если оно постоянно на каждом из левых классов смежности в* $\mathfrak{G}^{(m)}$ *по* $\mathfrak{H}^{(m)}$.

Иными словами, $f(\sigma_1, \ldots, \sigma_m)$ зависит только от левых классов смежности $\mathfrak{H}\sigma_1, \ldots, \mathfrak{H}\sigma_m$, определяемых элементами σ_i в $\mathfrak{G}$. В этом случае отображение f локально постоянно, или, что то же самое, оно непрерывно при наделении S дискретной топологией. Обратно, пусть f — отображение из $\mathfrak{G}^{(m)}$ в S. Если оно локально постоянно, то оно непрерывно, если S наделено дискретной топологией, а значит, поскольку группа $\mathfrak{G}$ компактна, оно равномерно непрерывно. Отсюда следует, что существует открытая подгруппа $\mathfrak{H}$ в $\mathfrak{G}$, для которой отображение f является $\mathfrak{H}$-регулярным.

Определение 3. *Пусть группа* $\mathfrak{G}^{(m)}$ *такова, как в определении* 2. *Тогда отображение* f *из* $\mathfrak{G}^{(m)}$ *в* $M_n(K_{\text{sep}})$, *где* $n \geqslant 1$, *называется ковариантным, если оно локально постоянно и удовлетворяет условию*

$$f(\sigma_1\lambda, \ldots, \sigma_m\lambda) = f(\sigma_1, \ldots, \sigma_m)^{\lambda}$$

для всех $\sigma_1, \ldots, \sigma_m, \lambda$ *из* $\mathfrak{G}$.

Лемма 1. *Пусть* $\mathfrak{H}$ — *открытая подгруппа в* $\mathfrak{G}$, *и пусть* L — *подполе в* K_{sep}, *состоящее из элементов, инвариантных относительно* $\mathfrak{H}$. *Тогда* $\mathfrak{H}$*-регулярное отображение из* $\mathfrak{G}$ *в* K_{sep} *ковариантно в том и только в том случае, когда оно имеет вид* $\sigma \to \xi^{\sigma}$, *где* $\xi \in L$.

Пусть x, т. е. $\sigma \to x(\sigma)$,— некоторое отображение из $\mathfrak{G}$ в K_{sep}. Положим $\xi = x(\varepsilon)$. Если x ковариантно, то $x(\sigma) = \xi^{\sigma}$ при всех σ, а если это отображение $\mathfrak{H}$-регулярно, то ξ должно лежать в L. Обратное утверждение очевидно.

Лемма 2. *Пусть* $\mathfrak{H}$ — *открытая подгруппа в* $\mathfrak{G}$. *Обозначим через* X_m *пространство* $\mathfrak{H}$*-регулярных ковариантных отображений из* $\mathfrak{G}^{(m)}$ *в* K_{sep}, *рассматриваемое как векторное пространство*

над K. Обозначим, далее, через X'_m пространство всех $\mathfrak{H}$-регулярных отображений из $\mathfrak{G}^{(m)}$ в K_{sep}, рассматриваемое как векторное пространство над K_{sep}. Тогда $X'_m = X_m \otimes_K K_{\text{sep}}$ и размерности пространств X_m над K и X'_m над K_{sep} равны обе n^m, где n — индекс подгруппы $\mathfrak{H}$ в $\mathfrak{G}$.

Пусть поле L таково, как в лемме 1. Оно имеет степень n над K. Возьмем полное семейство $\mathfrak{a} = \{\alpha_1, \ldots, \alpha_n\}$ представителей классов смежности $\mathfrak{H}\alpha$ в $\mathfrak{G}$ по $\mathfrak{H}$. Тогда изоморфизмы $\lambda_1, \ldots, \lambda_n$, индуцированные на L соответственно автоморфизмами α_i, суть n различных K-линейных изоморфизмов из L в K_{sep}. Любое отображение $x \in X'_m$ однозначно определяется своими значениями на $\mathfrak{a} \times \ldots \times \mathfrak{a}$, которые можно выбирать произвольно. Поэтому X'_m имеет размерность n^m над K_{sep}, и каждую линейную форму l на X'_m можно записать в виде

$$l(x) = \sum_{(i)} a_{i_1 \ldots i_m} x(\alpha_{i_1}, \ldots, \alpha_{i_m}),$$

где коэффициенты $a_{(i)} \in K_{\text{sep}}$.

Теперь применим индукцию по m. Для $m = 1$ лемма 1 показывает, что X_1 как векторное пространство над K изоморфно L и, значит, его размерность равна n, так что остается лишь показать, что X_1 порождает X'_1 как векторное пространство над K_{sep}. Если бы это было не так, то существовала бы отличная от нуля линейная форма l на X'_1, на X_1 равная нулю. Записав l, как выше, и применив лемму 1, мы получили бы тогда, что $0 = \Sigma a_i \xi^{\lambda_i}$ при всех $\xi \in L$. Но это противоречит линейной независимости изоморфизмов λ_i над K_{sep} (см. следствие 3 предл. 3 гл. III-2).

Пусть теперь m произвольно. Рассмотрим взятое над K тензорное произведение $Y_m = X_1 \otimes \ldots \otimes X_1$, где все m сомножителей равны X_1, и аналогичное произведение $Y'_m = X'_1 \otimes \ldots \otimes X'_1$, взятое над K_{sep}. Как мы только что показали, X'_1 совпадает с $X_1 \otimes_K K_{\text{sep}}$, поэтому мы очевидным образом можем отождествить Y'_m с $Y_m \otimes_K \otimes_K K_{\text{sep}}$. Обозначим через φ такое K_{sep}-линейное отображение из Y'_m в X'_m, которое каждому элементу $x_1 \otimes \ldots \otimes x_m$ из Y'_m сопоставляет отображение

$$(\sigma_1, \ldots, \sigma_m) \to x_1(\sigma_1) \ldots x_m(\sigma_m)$$

из $\mathfrak{G}^{(m)}$ в K_{sep}. Отображение φ сюръективно. Действительно, если линейная форма l на X'_m равна нулю на $\varphi(Y'_m)$, то для всех $x_1, \ldots, x_m$ из X'_1 мы должны иметь

$$0 = \sum_{(i)} a_{i_1 \ldots i_m} x_1(\alpha_{i_1}) \ldots x_m(\alpha_{i_m}),$$

откуда, очевидно, следует, что все a_i равны нулю. Так как Y'_m имеет ту же самую размерность n^m, что и X'_m, это показывает, что φ является изоморфизмом из Y'_m на X'_m. Выберем теперь базис $\{f_1, \ldots, f_n\}$ в X_1 над K. Тогда n^m элементов $f_{i_1} \otimes \ldots \otimes f_{i_m}$ образуют базис в Y_m над K и, следовательно, в Y'_m над K_{sep}, так что их образы при отображении φ образуют базис в X'_m над K_{sep}. Иными словами, каждый элемент из X'_m может быть однозначно записан в виде

$$(\sigma_1, \ldots, \sigma_m) \to \sum_{(i)} x_{i_1 \ldots i_m} f_{i_1}(\sigma_1) \ldots f_{i_m}(\sigma_m),$$

где коэффициенты $x_{(i)} \in K_{\text{sep}}$. Записывая теперь для этого элемента условие принадлежности к X_m, т. е. условие ковариантности, мы видим, что оно выполняется в том и только в том случае, когда все $x_{(i)}$ инвариантны относительно $\mathfrak{G}$, т. е. когда все они лежат в K. Поэтому φ отображает Y_m на X_m. Доказательство закончено.

Пусть теперь K' — любое поле, содержащее поле K, и пусть $\bar{K}'$, K'_{sep}, $\mathfrak{G}'$ определены для K' так же, как для K были определены $\bar{K}$, K_{sep}, $\mathfrak{G}$. Поскольку поле $\bar{K}$ определялось лишь с точностью до изоморфизма, мы в такой ситуации будем всегда считать, что в качестве $\bar{K}$ взято алгебраическое замыкание поля K в $\bar{K}'$. Очевидно, что тогда K_{sep} содержится в K'_{sep}. Каждый автоморфизм σ' поля $\bar{K}'$ над K' индуцирует на $\bar{K}$ автоморфизм σ поля $\bar{K}$ над K (более точно, над $\bar{K} \cap K'$). Ясно, что отображение $\sigma' \to \sigma$ является непрерывным морфизмом ρ группы $\mathfrak{G}'$ в $\mathfrak{G}$. Этот морфизм будем называть *морфизмом ограничения*. Он инъективен, если поле K' алгебраично над K, ибо тогда $\bar{K}' = \bar{K}$. В этом случае группу $\mathfrak{G}'$ будем обычно отождествлять с ее образом в $\mathfrak{G}$, который всегда является замкнутой подгруппой в $\mathfrak{G}$, причем этот образ открыт в $\mathfrak{G}$, если K' имеет конечную степень над K. Если $\mathfrak{H}$ — любая открытая подгруппа в $\mathfrak{G}$ и L — соответствующее подполе в K_{sep}, т. е. подполе, состоящее из элементов, инвариантных относительно $\mathfrak{H}$, то подгруппа $\mathfrak{H}' = \rho^{-1}(\mathfrak{H})$ в $\mathfrak{G}'$ открыта и соответствующим подполем в K'_{sep} является поле, порожденное над K' полем L.

Пусть f, как в определении 2, есть отображение группы $\mathfrak{G}^{(m)}$ в некоторое множество S. Сохраняя введенные выше обозначения, обозначим через $f \circ \rho$ отображение

$$(\sigma'_1, \ldots, \sigma'_m) \to f(\rho(\sigma'_1), \ldots, \rho(\sigma'_m))$$

из $\mathfrak{G}'^{(m)}$ в S. Это отображение, очевидно, непрерывно, т. е. локально постоянно, если f таково. Если f $\mathfrak{H}$-регулярно, то $f \circ \rho$

является $\mathfrak{H}'$-регулярным для $\mathfrak{H}' = \rho^{-1}(\mathfrak{H})$. Если $S = M_n(K_{\text{sep}})$ и f ковариантно, то $f \circ \rho$ ковариантно. Если K' алгебраично над K, то $\mathfrak{G}'$ является подгруппой в $\mathfrak{G}$, а ρ — ее естественным вложением в $\mathfrak{G}$; при этом $f \circ \rho$ есть ограничение отображения f на $\mathfrak{G}'^{(m)}$.

После этих приготовлений мы можем вернуться к нашей основной теме.

Теорема 2. *Пусть A — простая алгебра размерности n^2 над K, $\mathfrak{H}$ — открытая подгруппа в $\mathfrak{G}$, L — соответствующее подполе в K_{sep} и F — L-представление алгебры A. Тогда существует такое $\mathfrak{H}$-регулярное ковариантное отображение Y из $\mathfrak{G} \times \mathfrak{G}$ в $M_n(K_{\text{sep}})^\times$, что $F^\sigma = Y(\rho, \sigma)^{-1} F^\rho Y(\rho, \sigma)$ при всех ρ, σ из $\mathfrak{G}$. Для любого такого Y существует $\mathfrak{H}$-регулярное ковариантное отображение f из $\mathfrak{G} \times \mathfrak{G} \times \mathfrak{G}$ в $K_{\text{sep}}^\times$, для которого*

$$f(\rho, \sigma, \tau)\, Y(\rho, \tau) = Y(\rho, \sigma)\, Y(\sigma, \tau) \tag{1}$$

при всех ρ, σ, τ из $\mathfrak{G}$, и это отображение удовлетворяет условию

$$f(\rho, \sigma, \tau)\, f(\nu, \rho, \tau) = f(\nu, \sigma, \tau)\, f(\nu, \rho, \sigma) \tag{2}$$

при всех ν, ρ, σ, τ из $\mathfrak{G}$.

Для каждого $\lambda \in \mathfrak{G}$ отображение F^λ является K_{sep}-представлением алгебры A и, следовательно, имеет вид $Z(\lambda)^{-1} F Z(\lambda)$, где $Z(\lambda) \in M_n(K_{\text{sep}})^\times$. Так как F^λ зависит только от левого класса смежности $\mathfrak{H}\lambda$, то с самого начала можно предполагать $\mathfrak{H}$-регулярность отображения $\lambda \to Z(\lambda)$, а тогда легко проверяется, что отображение $Y(\rho, \sigma) = Z(\sigma\rho^{-1})^\rho$ удовлетворяет всем условиям первой части нашей теоремы, за возможным исключением условия $\mathfrak{H}$-регулярности. Для того чтобы доказать, что и это условие выполняется, мы следующим образом усовершенствуем нашу конструкцию.

Возьмем полное множество Λ представителей двойных классов смежности $\mathfrak{H}\lambda\mathfrak{H}$ в $\mathfrak{G}$ по $\mathfrak{H}$. Для каждого $\lambda \in \Lambda$ отображения F и F^λ являются оба L'-представлениями, где L' — композит $L \cdot L^\lambda$ поля L и его образа L^λ относительно отображения λ. Выберем теперь $Z(\lambda)$ в $M_n(L')^\times$ так, чтобы $F^\lambda = Z(\lambda)^{-1} F Z(\lambda)$. Каждый элемент $\rho \in \mathfrak{G}$ можно записать в виде $\rho = \alpha\lambda\beta$ с однозначно определенным $\lambda \in \Lambda$ и с $\alpha, \beta \in \mathfrak{H}$. Если одновременно $\rho = \alpha'\lambda\beta'$, где $\alpha', \beta' \in \mathfrak{H}$, то

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

так что, полагая $\gamma = \beta'\beta^{-1}$, имеем $\gamma \in \mathfrak{H}$ и $\gamma \in \lambda^{-1}\mathfrak{H}\lambda$, откуда следует, что γ оставляет неподвижными все элементы поля L и поля L^λ, а следовательно, и поля $L \cdot L^\lambda$; в частности, матрица $Z(\lambda)$ инва-

риантна относительно γ. Поэтому если положить $Z(\rho) = Z(\lambda)^{\beta}$, то $Z(\rho)$ будет зависеть только от ρ, но не от выбора α, β, подчиненных указанному выше условию. Легко проверить, что $Y(\rho, \sigma) = Z(\sigma\rho^{-1})^{\rho}$ удовлетворяет всем условиям, сформулированным в нашей теореме. Далее для всех ρ, σ, τ имеем

$$F^{\tau} = Y(\sigma, \tau)^{-1} F^{\sigma} Y(\sigma, \tau) =$$
$$= Y(\sigma, \tau)^{-1} Y(\rho, \sigma)^{-1} F^{\rho} Y(\rho, \sigma) Y(\sigma, \tau).$$

В то же время $F^{\tau} = Y(\rho, \tau)^{-1} F^{\rho} Y(\rho, \tau)$. Как мы отмечали выше, отсюда ввиду следствия предложения 4 § 1 вытекает, что $Y(\rho, \sigma)\, Y(\sigma, \tau)$ отличается от $Y(\rho, \tau)$ лишь скалярным множителем $f(\rho, \sigma, \tau)$, чем доказано равенство (1). Теперь равенство (2) проверяется прямым вычислением. Остальные утверждения очевидны.

Следствие. *В предположениях и обозначениях теоремы* 2 *пусть* K' *— поле, содержащее поле* K; $\rho\colon \mathfrak{G}' \to \mathfrak{G}$ *— морфизм ограничения, где группа* $\mathfrak{G}'$ *такая же, как выше;* $F_{K'}$ *—* K'*-линейное продолжение представления* F *на* $A_{K'}$. *Тогда* $Y \circ \rho$ *и* $f \circ \rho$ *связаны с* $F_{K'}$ *таким же образом, как* Y *и* f *с* F.

Это очевидно.

В случае когда Y и f связаны с L-представлением F алгебры A, описанным в теореме 2 способом, мы будем говорить, что они *относятся к* A.

Определение 4. *Ковариантное отображение* f *из* $\mathfrak{G} \times \mathfrak{G} \times \mathfrak{G}$ *в* $K_{\mathrm{sep}}^{\times}$ *называется системой факторов над* K, *если оно удовлетворяет условию* (2) *при всех* ν, ρ, σ, τ *из* $\mathfrak{G}$.

Ясно, что системы факторов над K образуют группу $\zeta(K)$ относительно умножения. Если K', $\mathfrak{G}'$ и ρ такие же, как выше, то отображение $f \to f \circ \rho$ является, очевидно, морфизмом из $\zeta(K)$ в $\zeta(K')$.

Пусть z — любое ковариантное отображение из $\mathfrak{G} \times \mathfrak{G}$ в $K_{\mathrm{sep}}^{\times}$. Ясно, что отображение

$$(\rho, \sigma, \tau) \to z(\rho, \sigma)\, z(\sigma, \tau)\, z(\rho, \tau)^{-1} \tag{3}$$

ковариантно, и немедленно проверяется, что это — система факторов.

Определение 5. *Система факторов, определенная формулой* (3), *называется кограницей отображения* z. *Система факторов над* K *называется тривиальной, если она является кограницей некоторого ковариантного отображения из* $\mathfrak{G} \times \mathfrak{G}$ *в* $K_{\mathrm{sep}}^{\times}$.

Тривиальные системы факторов образуют подгруппу $\beta(K)$ группы $\zeta(K)$ всех систем факторов над K. Факторгруппу $\zeta(K)/\beta(K)$ будем обозначать через $H(K)$, а ее элементы, т. е. классы в $\zeta(K)$ по модулю $\beta(K)$, будем называть *классами факторов* над K. Если K' и ρ такие же, как прежде, то очевидно, отображение $f \to f_\rho$ переводит когранницы в когранницы, так что ρ определяет морфизм из $H(K)$ в $H(K')$, который мы обозначим опять через ρ.

Предложение 7. *Системы факторов, относящиеся к простой алгебре A над K, образуют класс факторов над K.*

Пусть $\mathfrak{H}$, L, F, Y и f такие, как в теореме 2; z — любое ковариантное отображение из $\mathfrak{G} \times \mathfrak{G}$ в $K_{\mathrm{sep}}^{\times}$; $\mathfrak{H}'$ — такая открытая подгруппа в $\mathfrak{H}$, что z является $\mathfrak{H}'$-регулярным; L' — подполе в K_{sep}, соответствующее $\mathfrak{H}'$. Тогда F является также L'-представлением, $Y' = zY$ связано с F таким же образом, как и Y, и определяет систему факторов $f' = f_0 f$, где f_0 — кограница отображения z. Это показывает, что все системы факторов в классе, содержащем f, относятся к A. С другой стороны, пусть $\mathfrak{H}'$, L', F', Y', f' связаны с A таким же образом, как $\mathfrak{H}$, L, F, Y и f. Положим $\mathfrak{H}'' = \mathfrak{H} \cap \mathfrak{H}'$ и обозначим через L'' соответствующее подполе в K_{sep}, которое является композитом полей L и L'. Тогда существует такая матрица $Z \in M_n(L'')^{\times}$, что $F' = Z^{-1}FZ$. Тривиальным вычислением получается равенство $F'^{\sigma} = W^{-1}F'^{\rho}W$, где $W = (Z^{\rho})^{-1}Y(\rho, \sigma)Z^{\sigma}$, так что $Y'(\rho, \sigma)$ может отличаться от W лишь скалярным множителем. Если обозначить этот множитель через $z(\rho, \sigma)$, то

$$Y'(\rho, \sigma) = z(\rho, \sigma)(Z^{\rho})^{-1}Y(\rho, \sigma)Z^{\sigma},$$

откуда следует, что отображение z ковариантно и $\mathfrak{H}''$-регулярно. Поэтому $f'f^{-1}$ есть кограница от z, чем и заканчивается доказательство.

Следствие. *Пусть K' — поле, содержащее поле K. Тогда класс факторов над K', определяемый алгеброй $A_{K'}$, является образом класса факторов над K, определяемого алгеброй A, при морфизме ограничения ρ из $\mathfrak{G}'$ в $\mathfrak{G}$.*

Это очевидно ввиду следствия теор. 2.

Если A — простая алгебра над K, то класс факторов над K, состоящий из систем факторов, относящихся к A, будем называть *относящимся к A* или *связанным с A*.

Теорема 3. *Отображение, которое каждой простой алгебре A над K сопоставляет связанный с A класс факторов над K, посто-*

янно на всяком классе простых алгебр над K и определяет изоморфизм группы $B(K)$ таких классов на группу $H(K)$ классов факторов над K.

Возьмем сначала две простые алгебры A, A' над K и обозначим через n^2, n'^2 их размерности над K. Пусть L, F, Y и f определены для A, как в теореме 2, и пусть L', F', Y', f' аналогично определены для A'. Обозначим через L'' композит полей L и L'. Мы можем отождествить $M_n(L'') \otimes M_{n'}(L'')$ с $M_{nn'}(L'')$. Тогда, если мы положим $A'' = A \otimes A'$ и через $F'' = F \otimes F'$ обозначим K-линейное отображение $A'' \to M_{nn'}(L'')$, задаваемое формулой $F''(a \otimes a') = F(a) \otimes F'(a')$ для всех $a \in A$ и $a' \in A'$, то F'' будет L''-представлением алгебры A'' и сразу видно, что $Y'' = Y \otimes Y'$ и $f'' = ff'$ связаны с A'' и F'', как в теореме 2. Это показывает, что класс факторов, связанный с A'', является произведением классов факторов, связанных с A и с A'. Если $A = M_n(K)$, то в качестве F можно взять тождественное отображение из A на $M_n(K)$ и, далее, взять $Y = 1$, и, следовательно, $f = 1$. Поэтому класс факторов, связанный с тривиальной алгеброй, тривиален, и классы факторов, связанные с A' и с $M_n(A')$, совпадают. Этим доказано первое утверждение нашей теоремы и показано, что отображение μ из $B(K)$ в $H(K)$, определенное таким образом, является морфизмом. Теперь будут доказаны сначала инъективность, а затем сюръективность отображения μ. Это будет сделано в несколько шагов, которые мы оформим в виде лемм.

Лемма 3. *Пусть $\mathfrak{H}$ — открытая подгруппа в $\mathfrak{G}$; L — соответствующее $\mathfrak{H}$ подполе в K_{sep}; Y — некоторое $\mathfrak{H}$-регулярное ковариантное отображение из $\mathfrak{G} \times \mathfrak{G}$ в $M_n(K_{\mathrm{sep}})^\times$, причем $Y(\rho, \tau) = Y(\rho, \sigma) Y(\sigma, \tau)$ при всех ρ, σ, τ из $\mathfrak{G}$. Тогда существует такая матрица $Z \in M_n(L)^\times$, что $Y(\rho, \sigma) = (Z^\rho)^{-1} Z^\sigma$ при всех ρ, σ из $\mathfrak{G}$.*

Возьмем полное множество $\mathfrak{a}$ представителей классов смежности $\mathfrak{H}\alpha$ в $\mathfrak{G}$ по $\mathfrak{H}$. Как было отмечено при доказательстве леммы 2, элементы из $\mathfrak{a}$ индуцируют на L все различные K-линейные изоморфизмы $L \to K_{\mathrm{sep}}$, причем эти изоморфизмы линейно независимы над K_{sep}, как было показано в следствии 3 предл. 3 гл. III-2. Пусть $M_n(K_{\mathrm{sep}})$ действует справа как умножение на матрицы на пространстве $M_{1,n}(K_{\mathrm{sep}})$ векторов-строк над K_{sep} и аналогичным образом действует слева на пространстве векторов-столбцов. Для всякого $u \in M_{1,n}(L)$ положим

$$z = \sum_{\alpha \in \mathfrak{a}} u^\alpha Y(\alpha, \varepsilon).$$

Для любого $\rho \in \mathfrak{G}$ множество $\mathfrak{a}\rho$ снова является полным множеством представителей классов смежности в $\mathfrak{G}$ по $\mathfrak{H}$. Поскольку Y ковариантно, мы имеем

$$z^\rho = \sum_\rho u^{\alpha\rho} Y(\alpha\rho, \rho) = \sum_\alpha u^\alpha Y(\alpha, \rho).$$

Беря $\rho \in \mathfrak{H}$, мы видим, что элемент z инвариантен относительно $\mathfrak{H}$, т. е. лежит в $M_{1,n}(L)$. Поэтому если мы обозначим через φ определенное выше отображение $u \to z$, то φ отображает $M_{1,n}(L)$ в себя. Покажем теперь, что в $M_{1,n}(L)$ имеется n векторов $u_1, \ldots, u_n$, для которых векторы $\varphi(u_i)$ линейно независимы над L. В самом деле, если бы это было не так, то в $M_{n,1}(L)$ существовал бы отличный от нуля вектор-столбец v, для которого при всех $u \in M_{1,n}(L)$ выполнялось бы равенство $\varphi(u)\, v = 0$. Это равенство можно переписать в виде $\sum u^\alpha (Y(\alpha, \varepsilon))v = 0$, откуда ввиду линейной независимости всех α над L вытекало бы, что $Y(\alpha, \varepsilon)\, v = 0$ при всех α и, следовательно, что $v = 0$. Фиксируем какие-нибудь n векторов u_i, для которых $\varphi(u_i)$ линейно независимы над L, обозначим через U матрицу в $M_n(L)$, составленную из строк u_i, и положим $Z = \sum U^\alpha Y(\alpha, \varepsilon)$. Поскольку строками матрицы Z являются векторы $\varphi(u_i)$, то эта матрица обратима в $M_n(L)$. Точно так же, как выше, при всех ρ, σ имеем

$$Z^\rho = \sum_\alpha U^\alpha Y(\alpha, \rho), \quad Z^\sigma = \sum_\alpha U^\alpha Y(\alpha, \sigma),$$

откуда $Z^\sigma = Z^\rho Y(\rho, \sigma)$ в силу наших предположений относительно Y. Тем самым показано, что матрица Z обладает требуемым свойством.

Теперь нетрудно показать, что определенный выше морфизм μ из $B(K)$ в $H(K)$ инъективен. В самом деле, предположим, что простая алгебра A над K имеет тривиальную систему факторов. Ввиду предложения 7 отсюда следует, что мы можем выбрать $\mathfrak{H}$, L, F и Y (такие, как в теореме 2) таким образом, чтобы тождество (1) выполнялось с $f = 1$. Пусть, далее, матрица Z такова, как в лемме 3. Положим $F' = ZFZ^{-1}$. Сразу видно, что $F'^\sigma = F'^\rho$ при всех ρ, σ из $\mathfrak{G}$. Это означает, что F' является K-представлением алгебры A, т. е. изоморфизмом из A на $M_n(K)$, так что алгебра A тривиальна.

Наконец, утверждение о сюръективности морфизма μ покрывается следующим более точным результатом.

Лемма 4. *Пусть $\mathfrak{H}$ и L таковы, как в лемме* 3, *n — степень поля L над K и f — некоторая $\mathfrak{H}$-регулярная система факторов над K. Тогда можно таким образом выбрать A, F и Y, обладающие*

описанными в теореме 2 *свойствами, чтобы система факторов, определяемая тождеством* (1), *совпадала с заданной системой* f *и чтобы алгебра* A *содержала подполе, изоморфное полю* L.

Для доказательства леммы будет использована явная конструкция, принадлежащая Р. Брауэру. Заметим прежде всего, что если в формуле (2) теор. 2, определяющей системы факторов, взять $\nu = \rho = \sigma$, то мы получим $f(\rho, \rho, \tau) = f(\rho, \rho, \rho)$. Поскольку f ковариантно, это дает $f(\rho, \rho, \tau) = a^{\rho}$ с $a = f(\varepsilon, \varepsilon, \varepsilon)$. Теперь применим лемму 2 к случаю $m = 2$. Мы получим два пространства X_2, X_2' размерности n^2 над K и над K_{sep} соответственно, причем $X_2' = X_2 \otimes_K K_{\text{sep}}$. Возьмем полное множество $\mathfrak{a}$ представителей классов смежности $\mathfrak{H}\alpha$ в $\mathfrak{G}$ по $\mathfrak{h}$. Для любых x, y из X_2' и любых ρ, σ из $\mathfrak{G}$ положим

$$z(\rho, \sigma) = \sum_{\alpha \in \mathfrak{a}} f(\sigma, \alpha, \rho)\, x(\rho, \alpha)\, y(\alpha, \sigma).$$

Ясно, что z, т. е. отображение $(\rho, \sigma) \to z(\rho, \sigma)$, лежит в X_2' и что $z \in X_2$, если x, $y \in X_2$. Более точно, $(x, y) \to z$ есть билинейное отображение из $X_2' \times X_2'$ в X_2', индуцирующее на $X_2 \times X_2$ билинейное отображение из $X_2 \times X_2$ в X_2. Покажем, что этот закон композиции, записываемый как $(x, y) \to xy$, превращает X_2 в алгебру A с нужными свойствами. В самом деле, положим для всякого $\rho \in \mathfrak{G}$ и всякого $x \in X_2'$

$$\Phi_\rho(x) = (f(\beta, \alpha, \rho)\, x(\alpha, \beta))_{\alpha, \beta \in \mathfrak{a}}.$$

Упорядочив каким-либо образом множество $\mathfrak{a}$, мы можем отождествить отображения $\mathfrak{a} \times \mathfrak{a} \to K_{\text{sep}}$ с матрицами из $M_n(K_{\text{sep}})$. Тогда каждое Φ_ρ можно рассматривать как отображение из X_2' в $M_n(K_{\text{sep}})$, которое, очевидно, K_{sep}-линейно и биективно. С помощью формулы (2) немедленно проверяется, что $\Phi_\rho(xy) = \Phi_\rho(x)\, \Phi_\rho(y)$ при всех x, y из X_2'. Обозначим через e элемент в X_2', задаваемый условием: $e(\rho, \sigma) = (a^\rho)^{-1}$, где $a = f(\varepsilon, \varepsilon, \varepsilon)$, в случае когда σ лежит в том же классе смежности $\mathfrak{H}\rho$, что и ρ, и $e(\rho, \sigma) = 0$ в противном случае. Ясно, что $e \in X_2$. Так как $f(\alpha, \alpha, \rho) = a^\alpha$ при всех α, ρ, то $\Phi_\rho(\varepsilon) = 1_n$. Поэтому очевидно, что Φ_ρ для каждого ρ изоморфно отображает пространство X_2' с умножением $(x, y) \to xy$ на алгебру $M_n(K_{\text{sep}})$, причем единицей в X_2' является e. Поскольку $X_2' = X_2 \otimes_K K_{\text{sep}}$, отсюда согласно следствию 1 предл. 3 § 1 вытекает, что это умножение превращает X_2 в простую алгебру A над K с $1_A = e$. Для любого $\xi \in L$ и любого $x \in A$ обозначим через ξx элемент в X_2, соответствующий отображению $(\rho, \sigma) \to \xi^\rho x(\rho, \sigma)$. Тем самым мы определим на X_2 структуру

левого векторного пространства над L. Далее, ясно, что $(\xi x)\, y = \xi\,(xy)$ при всех $\xi \in L$ и всех x, y из A. Поэтому $\xi \to \xi e$ есть изоморфизм из L в A и $\xi x = (\xi e)\, x$ при всех $\xi \in L$ и всех $x \in A$.

Теперь мы построим F и Y, обладающие указанными в нашей лемме свойствами. Для любых ρ, σ из $\mathfrak{G}$ обозначим через $D(\rho, \sigma)$ такую диагональную матрицу:

$$D(\rho, \sigma) = (\delta_{\alpha\beta} f(\alpha, \rho, \sigma))_{\alpha, \beta \in \mathfrak{a}},$$

где $\delta_{\alpha\beta} = 1$ или 0, в соответствии с тем, $\alpha = \beta$ или нет. С помощью формулы (2) сразу проверяется, что при всех ρ, σ и всех $x \in X_2'$ справедливо равенство

$$D(\rho, \sigma)\, \Phi_\sigma(x) = \Phi_\rho(x)\, D(\rho, \sigma). \tag{4}$$

Выберем теперь какой-нибудь базис $\{\xi_1, \ldots, \xi_n\}$ в L над K, и пусть $\{\eta_1, \ldots, \eta_n\}$ — двойственный базис (мы отождествляем L с двойственным к нему пространством, полагая $[\xi, \eta] = \mathrm{Tr}_{L/K}(\xi\eta)$). Так как элементы α из $\mathfrak{a}$ индуцируют на L все n различных K-линейных изоморфизмов из L в K_{sep}, то для каждого $\xi \in L$ имеем $\mathrm{Tr}_{L/K}(\xi) = \sum_\alpha \xi^\alpha$, так что определение η_i можно записать следующим образом:

$$\delta_{ij} = \mathrm{Tr}_{L/K}(\xi_i \eta_j) = \sum_{\alpha \in \mathfrak{a}} \xi_i^\alpha \eta_j^\alpha.$$

Поэтому мы можем положить

$$X = (\xi_i^\alpha)_{1 \leqslant i \leqslant n;\ \alpha \in \mathfrak{a}}, \quad X^{-1} = (\eta_i^\alpha)_{\alpha \in \mathfrak{a};\ 1 \leqslant i \leqslant n}.$$

Для каждого ρ положим, далее, $F_\rho = X \Phi_\rho X^{-1}$. Тогда

$$F_\rho(x) = \Big(\sum_{\alpha,\ \beta \in \mathfrak{a}} \xi_i^\alpha f(\beta, \alpha, \rho)\, x(\alpha, \beta)\, \eta_j^\beta\Big)_{1 \leqslant i,\ j \leqslant n}.$$

Предположим, что $x \in A$, т. е. что отображение x ковариантно. Так как f ковариантно и так как для каждого λ множество $\mathfrak{a}\lambda$ является полным множеством представителей классов смежности в $\mathfrak{G}$ по $\mathfrak{H}$, то

$$F_\rho(x)^\lambda = \Big(\sum_{\alpha,\ \beta \in \mathfrak{a}} \xi_i^\alpha f(\beta, \alpha, \rho\lambda)\, x(\alpha, \beta)\, \eta_j^\beta\Big)_{1 \leqslant i,\ j \leqslant n} = F_{\rho\lambda}(x).$$

В частности, полагая $F = F_\varepsilon$, получаем, что $F_\rho = F^\rho$ для каждого ρ. По определению F_ρ это дает $F^\rho = F$ при $\rho \in \mathfrak{H}$, т. е. $F(x)^\rho = F(x)$ для каждого $x \in A$ и каждого $\rho \in \mathfrak{H}$. Другими словами, F отображает A в $M_n(L)$, так что F является L-представлением алгебры A. Для всех $\rho \in \mathfrak{G}$ имеем $F^\rho = X \Phi_\rho X^{-1}$. Ввиду (4) это дает $F^\sigma =$

$= Y(\rho, \sigma)^{-1} F^{\rho} Y(\rho, \sigma)$, где мы положили

$$Y(\rho, \sigma) = XD(\rho, \sigma) X^{-1} = \Big(\sum_{\alpha \xi a} \xi_i^{\alpha} f(\alpha, \rho, \sigma) \eta_j^{\alpha}\Big)_{1 \leqslant i \leqslant n}.$$

Теперь легко проверяется, что Y вместе с A и F удовлетворяет всем требованиям нашей леммы. Для дальнейшего заметим еще, что приведенный след τ и приведенную норму ν на A можно вычислить с помощью любого из K_{sep}-представлений Φ_{ρ} алгебры A, скажем с помощью Φ_{ε}; а именно $\tau(x) = \operatorname{tr}(\Phi_{\varepsilon}(x))$, $\nu(x) = \det(\Phi_{\varepsilon}(x))$ при всех $x \in A$, в частности

$$\tau(\xi \cdot 1_A) = \operatorname{Tr}_{L/K}(\xi), \quad \nu(\xi \cdot 1_A) = \operatorname{N}_{L/K}(\xi)$$

при всех $\xi \in L$.

Доказательство леммы 4, а с ним и доказательство теоремы 3 закончены.

Следствие 1. *Пусть K' — поле, содержащее поле K, ρ — морфизм ограничения из $\mathfrak{G}'$ в $\mathfrak{G}$, A — простая алгебра над K и f — система факторов, относящаяся к A. Тогда алгебра $A_{K'}$ тривиальна в том и только в том случае, когда тривиальна система факторов $f \circ \rho$.*

Это сразу вытекает из теоремы 3 и следствия теоремы 2.

Следствие 2. *Пусть $\mathfrak{H}$ — открытая подгруппа в $\mathfrak{G}$ и f — некоторая $\mathfrak{H}$-регулярная система факторов над K. Эта система тривиальна в том и только в том случае, когда она является кограницей некоторого $\mathfrak{H}$-регулярного ковариантного отображения из $\mathfrak{G} \times \mathfrak{G}$ в $K_{\text{sep}}^{\times}$.*

Предположим, что система факторов f тривиальна. Построим A, F и Y, как в лемме 4. По теореме 3 алгебра A тривиальна, так что существует изоморфизм F' из A на $M_n(K)$. Тогда $F = Z^{-1} F' Z$, где $Z \in M_n(L)^{\times}$; следовательно, $F^{\sigma} = Y'(\rho, \sigma)^{-1} F^{\rho} Y'(\rho, \sigma)$, где $Y'(\rho, \sigma) = (Z^{\rho})^{-1} Z^{\sigma}$. Значит, $Y(\rho, \sigma) = z(\rho, \sigma) Y'(\rho, \sigma)$, где z $\mathfrak{H}$-регулярно и ковариантно. Поэтому f является кограницей от z.

Следствие 3. *Пусть L — сепарабельное расширение поля K степени n над K, A — простая алгебра над K. Тогда алгебра A_L тривиальна в том и только в том случае, когда существует алгебра A' размерности n^2 над K, подобная алгебре A и содержащая подполе, изоморфное полю L. В случае когда такая алгебра A' существует, она единственна с точностью до изоморфизма.*

Последнее утверждение очевидно. В силу следствия 6 предл. 3 § 1 из существования алгебры A' вытекает тривиальность алгебры A'_L,

а следовательно, и алгебры A_L. Обратно, предположим, что существует изоморфизм алгебры A_L на матричную алгебру $M_n(L)$. Этот изоморфизм индуцирует на A некоторое L-представление F. По теореме 2 мы можем построить $\mathfrak{H}$-регулярную систему факторов f, относящуюся к A. Поэтому согласно лемме 4 можно построить алгебру A', удовлетворяющую требуемым условиям.

Группы $B(K)$ и $H(K)$ часто отождествляют при помощи изоморфизма μ, описанного в теореме 3. При этом отождествлении, как показывают следствия теоремы 2 и предл. 7, для любого содержащего K поля K' естественный морфизм из $B(K)$ в $B(K')$, который отображает класс каждой простой алгебры A над K на класс алгебры $A_{K'}$, совпадает с морфизмом ограничения ρ из $H(K)$ в $H(K')$.

§ 4. ЦИКЛИЧЕСКИЕ СИСТЕМЫ ФАКТОРОВ

Здесь мы обсудим подробнее один особенно важный тип систем факторов, связанный с циклическими расширениями основного поля K. Как всегда, под «циклическим расширением» понимается расширение Галуа (следовательно, по определению, сепарабельное расширение) с циклической группой Галуа. В обозначениях § 3 циклические расширения поля K — это подполя L в K_{sep}, соответствующие открытым подгруппам $\mathfrak{H}$ в $\mathfrak{G}$ с циклической факторгруппой $\mathfrak{G}/\mathfrak{H}$. Для таких L и $\mathfrak{H}$ группа $\mathfrak{G}/\mathfrak{H}$ изоморфна группе всех корней n-й степени из 1 в $\mathbf{C}$, где n — степень поля L над K. Всякий изоморфизм из $\mathfrak{G}/\mathfrak{H}$ на последнюю группу можно рассматривать как характер χ на $\mathfrak{G}$ с ядром $\mathfrak{H}$. Любой такой характер, порядок которого равен n, будем называть *связанным с* L. Если α — представитель в $\mathfrak{G}$ какой-нибудь образующей для группы $\mathfrak{G}/\mathfrak{H}$, то существует один и только один связанный с L характер χ на $\mathfrak{G}$, для которого $\chi(\alpha) = \mathbf{e}(1/n)$.

Обратно, пусть χ — произвольный гомоморфизм из $\mathfrak{G}$ в $\mathbf{C}^\times$. По леммам 3 и 4 гл. VII-3 он является характером на $\mathfrak{G}$ конечного порядка n; его ядро $\mathfrak{H}$ является поэтому открытой подгруппой в $\mathfrak{G}$ с циклической факторгруппой порядка n и подполе L в K_{sep}, соответствующее подгруппе $\mathfrak{H}$, циклично степени n над K. Мы будем говорить в этом случае, что L *связано с* χ.

Пусть обозначения такие же, как выше. Так как характер χ локально постоянен на $\mathfrak{G}$, то можно, бесконечно многими способами, выбрать локально постоянное отображение Φ из $\mathfrak{G}$ в $\mathbf{R}$, для которого $\chi(\sigma) = \mathbf{e}(\Phi(\sigma))$ при всех $\sigma \in \mathfrak{G}$. Например, мы можем выбрать Φ так, чтобы было $0 \leqslant \Phi(\sigma) < 1$ при всех σ; отображе-

ние Φ определяется этим условием однозначно; оно $\mathfrak{H}$-регулярно, поскольку отображение χ таково. В любом случае Φ отображает $\mathfrak{G}$ в $(1/n)\mathbf{Z}$, потому что χ имеет порядок n. Рассмотрим теперь отображение

$$(5) \qquad (\rho, \sigma, \tau) \to e(\rho, \sigma, \tau) = \Phi(\sigma\rho^{-1}) + \Phi(\tau\sigma^{-1}) - \Phi(\tau\rho^{-1})$$

из $\mathfrak{G} \times \mathfrak{G} \times \mathfrak{G}$ в $\mathbf{R}$. Так как Φ локально постоянно, то таково же и e; так как χ — характер, то сразу видно, что e отображает $\mathfrak{G} \times \mathfrak{G} \times \mathfrak{G}$ в $\mathbf{Z}$. Для любого $\theta \in K^\times$ положим, далее,

$$(6) \qquad f(\rho, \sigma, \tau) = \theta^{e(\rho, \sigma, \tau)}.$$

Очевидно, что f — ковариантное отображение из $\mathfrak{G} \times \mathfrak{G} \times \mathfrak{G}$ в $K_{\mathrm{sep}}^\times$ (точнее, в $K^\times$); легко проверяется, что оно удовлетворяет условию (2) теоремы 2 § 3, т. е. является системой факторов. Любую систему факторов, определенную таким образом, будем называть *циклической системой факторов.*

Пусть Φ' — какое-нибудь другое локально постоянное отображение из $\mathfrak{G}$ в $\mathbf{R}$, для которого $\chi(\sigma) = \mathbf{e}(\Phi'(\sigma))$ при всех σ, и f' — система факторов, определенная с помощью Φ' и θ так же, как f, была определена с помощью Φ и θ. Положим $\Psi = \Phi' - \Phi$. Ясно, что Ψ отображает $\mathfrak{G}$ в $\mathbf{Z}$. Полагая $z(\rho, \sigma) = \theta^{\Psi(\sigma\rho^{-1})}$, немедленно убеждаемся, что $f'f^{-1}$ — когранича от z. Отсюда следует, что класс системы факторов f по модулю группы $\beta(K)$ тривиальных систем факторов однозначно определяется по χ и θ. Этот класс будем обозначать через $\{\chi, \theta\}$ и каждый такой класс факторов будем называть *циклическим.*

Предложение 8. *Для всякого $\theta \in K^\times$ отображение $\chi \to \{\chi, \theta\}$ является морфизмом группы характеров на $\mathfrak{G}$ в группу $H(K)$ классов факторов над K. Для всякого характера χ на $\mathfrak{G}$ отображение $\theta \to \{\chi, \theta\}$ является морфизмом из $K^\times$ в $H(K)$.*

Это очевидным образом вытекает из определений.

Пусть K' — поле, содержащее поле K. Как и в § 3, предположим, что поле $\bar{K}$ содержится в $\bar{K}'$, и обозначим через ρ как морфизм ограничения из $\mathfrak{G}'$ в $\mathfrak{G}$, так и индуцируемые им (см. § 3) морфизмы систем факторов и классов факторов. Если χ — произвольный характер на $\mathfrak{G}$, то $\chi' = \chi \circ \rho$ — характер на $\mathfrak{G}'$. Если χ имеет порядок n, то порядок n' характера χ' делит n. Если $\mathfrak{H}$ — ядро характера χ, то ядром характера χ' будет $\mathfrak{H}' = \rho^{-1}(\mathfrak{H})$, а ρ определяет инъективный морфизм из $\mathfrak{G}'/\mathfrak{H}'$ в $\mathfrak{G}/\mathfrak{H}$. Если L — циклическое расширение поля K, связанное с χ, то циклическим расши-

рением поля K', связанным с χ', будет композит полей L, K', который является циклическим расширением степени n'. Поэтому для каждого $\theta \in K^\times$

$$\{\chi, \theta\} \circ \rho = \{\chi \circ \rho, \theta\}. \tag{7}$$

Предложение 9. *Пусть χ — характер на $\mathfrak{G}$, L — циклическое расширение поля K, связанное с χ, и A — простая алгебра над K. Тогда алгебра A_L тривиальна в том и только в том случае, если класс факторов, связанный с A, можно записать в виде $\{\chi, \theta\}$, где $\theta \in K^\times$.*

Обозначим через $\mathfrak{H}$ ядро характера χ. Это — подгруппа в $\mathfrak{G}$, соответствующая полю L. Если $\{\chi, \theta\}$ — класс факторов, связанный с A, то класс факторов, связанный с A_L, задается формулой (7), где ρ — морфизм ограничения из $\mathfrak{H}$ в $\mathfrak{G}$. Поэтому $\chi \circ \rho$, будучи характером, индуцированным на $\mathfrak{H}$ характером χ, тривиален, так что алгебра A_L тривиальна. Обратно, предположим, что алгебра A_L тривиальна. Тогда если n — степень поля L над K, то следствие 3 теор. 3 § 3 показывает, что, заменив в случае надобности алгебру A подобной ей алгеброй, мы можем считать, что A имеет размерность n^2 над K. Пусть F — некоторое L-представление алгебры A, индуцированное на A изоморфизмом из A_L на $M_n(L)$. Так как порядок характера χ равен n, можно выбрать $\alpha \in \mathfrak{G}$, для которого $\chi(\alpha) = \mathbf{e}(1/n)$. Тогда группа $\mathfrak{G}/\mathfrak{H}$ порождается образом α в этой группе. Далее, существует такая матрица $X \in M_n(L)^\times$, что $F^\alpha = X^{-1}FX$; отсюда индукцией по i получаем $F^{\alpha^i} = X_i^{-1}FX_i$, где положено

$$X_i = XX^{\alpha} \ldots X^{\alpha^{i-1}}$$

для всех $i > 0$. Возьмем $i = n$. Поскольку автоморфизм α^n тождествен на L, то $F^{\alpha^n} = F$. Поэтому матрица X_n должна иметь вид $\theta \cdot 1_n$, где $\theta \in L^\times$. Применяя α к обеим частям формулы, определяющей X_n, получаем $X_n^\alpha = X^{-1}X_nX$, откуда $\theta^\alpha = \theta$, так что θ лежит в $K^\times$. Возьмем любое $i \in \mathbf{Z}$, запишем его в виде $i = n\nu + j$, где $n, j \in \mathbf{Z}$ и $1 \leqslant j \leqslant n$, и положим $X_i = \theta^\nu X_j$. Легко проверяется, что для $i > 0$ так определенные X_i совпадают с определенными выше X_i, что $X_{i+j} = X_iX_j^{\alpha^i}$ при $i, j \in \mathbf{Z}$ и что $X_{n\nu} = \theta^\nu \cdot 1_n$ при всех ν из $\mathbf{Z}$. Рассмотрим теперь такую локально постоянную функцию Φ на $\mathfrak{G}$, что $\chi(\sigma) = \mathbf{e}(\Phi(\sigma))$, так что $n\Phi(\sigma) \in \mathbf{Z}$ при всех σ, и положим $Y(\rho, \sigma) = (X_{n\Phi(\sigma\rho^{-1})})^\rho$ при всех ρ, σ из $\mathfrak{G}$. Легко видеть, что по отношению к A и F отображение Y обладает всеми свойствами, требуемыми в теореме 2 § 3, и что система факторов f, определенная с помощью Y по формуле (1) теор. 2, совпадает с задаваемой формулами (5) и (6).

Предложение 10. *Пусть* χ *и* L *таковы, как в предложении* 9. *Тогда ядро морфизма* $\theta \to \{\chi, \theta\}$ *из* $K^\times$ *в* $H(K)$ *совпадает с группой* $N_{L/K}(L^\times)$.

В доказательстве предложения 9 возьмем $A = M_n(K)$. В этом случае в качестве F можно взять тождественное отображение, и поскольку $F^\alpha = F$, можно взять $X = \xi \cdot 1_n$ с любым $\xi \in L^\times$. Тогда $\theta = N_{L/K}(\xi)$ и класс факторов $\{\chi, \theta\}$ тривиален, ибо тривиальна алгебра A. Обратно, предположим, что элемент $\theta \in K^\times$ таков, что класс факторов $\{\chi, \theta\}$ тривиален. Возьмем Φ, для которого $\chi(\sigma) = \mathbf{e}(\Phi(\sigma))$ и $0 \leqslant \Phi(\sigma) < 1$ при всех σ. Тогда $\Phi(\alpha^i) = i/n$ при $0 \leqslant i \leqslant n-1$ и Φ является $\mathfrak{H}$-регулярным, так что если мы определим f формулами (5) и (6), то f будет $\mathfrak{H}$-регулярной системой факторов. Так как эта система тривиальна, то согласно следствию 2 теор. 3 § 3 она является кограницей некоторого $\mathfrak{H}$-регулярного ковариантного отображения z из $\mathfrak{G} \times \mathfrak{G}$ в $K_{\mathrm{sep}}^\times$. Поскольку $\mathfrak{H}$ — нормальная подгруппа в $\mathfrak{G}$, то левые и правые классы смежности в $\mathfrak{G}$ по $\mathfrak{H}$ совпадают. Отсюда следует, что при всех ρ, σ из $\mathfrak{G}$ элемент $z(\rho, \sigma)$ инвариантен относительно всех $\lambda \in \mathfrak{H}$ и потому лежит в $L^\times$. Для всякого $\sigma \in \mathfrak{G}$ положим $w(\sigma) = z(\varepsilon, \sigma)$; кроме того, положим $w_i = w(\alpha^i)$ для всех i. Тогда $z(\rho, \sigma) = w(\sigma\rho^{-1})\rho$. Запишем теперь, что система факторов $f(\rho, \sigma, \tau)$, задаваемая формулой (6), равна кограницe отображения z, задаваемого формулой (3) § 3, при $\rho = \varepsilon$, $\sigma = \alpha^i$, $\tau = \alpha^{i+1}$. Для $0 \leqslant i \leqslant n-2$ мы получим $1 = w_i (w_1)^{\alpha^i} w_{i+1}^{-1}$, а для $i = n-1$ получим $\theta = w_{n-1} (w_1)^{\alpha^{n-1}} w_0^{-1}$. Поэтому $\theta = N_{L/K}(w_1)$, чем и заканчивается наше доказательство.

Пусть χ и L таковы, как в предложениях 9 и 10, и $\mathfrak{H}$, α таковы, как в доказательствах этих предложений. Если Φ выбрано так, как в доказательстве предложения 10, то имеем $f(\alpha^{-j}, \alpha^{-i}, \varepsilon) = 1$ или θ, соответственно тому, $i \leqslant j$ или $i > j$; в частности $f(\varepsilon, \varepsilon, \varepsilon) = 1$. К этой системе факторов мы можем применить теперь конструкцию, описанную в доказательстве леммы 4 § 3, и указанным там способом определить алгебру A. Как отмечалось выше, из того факта, что $\mathfrak{H}$ является нормальной подгруппой в $\mathfrak{G}$, вытекает, что каждое $\mathfrak{H}$-регулярное ковариантное отображение из $\mathfrak{G} \times \mathfrak{G}$ в K_{sep} переводит $\mathfrak{G} \times \mathfrak{G}$ в L. Для $i \in \mathbf{Z}$ определим u_i как такое отображение из $\mathfrak{G} \times \mathfrak{G}$ в L, для которого $u_i(\rho, \sigma)$ равно 1 при $\sigma\rho^{-1} \in \mathfrak{H}\alpha^i$ и нулю в противном случае. Ясно, что $u_i \in A$ и $u_{n+i} = u_i$ при всех i и что u_0 совпадает с единицей $e = 1_A$ алгебры A. Пусть $0 \leqslant i$, $j \leqslant n-1$; легко проверяется, что $u_i u_j = u_{i+j}$ при $i + j \leqslant n-1$.

Как и в доказательстве леммы 4, определим ξx для $\xi \in L$, $x \in A$ как элемент, задаваемый отображением $(\rho, \sigma) \to \xi^\rho x(\rho, \sigma)$. Легко

видеть, что $\xi x = (\xi \cdot 1_A)\, x$. Аналогично определим $x\xi$ как элемент, задаваемый отображением $(\rho, \sigma) \to x\,(\rho,\ \sigma)\ \xi^{\sigma}$. Тогда $x\xi = x\,(\xi \cdot 1_A)$. Ясно, что $\xi u_i = u_i \xi^{\alpha^i}$ при всех $\xi \in L$ и всех i. Так как алгебра A имеет размерность n^2 над K, то ее размерность над L равна n, рассматривать ли ее как левое векторное пространство с операцией $(\xi,\ x) \to \xi x$ или как правое векторное пространство с операцией $(\xi,\ x) \to x\xi$. При этом $\{u_0,\ u_1,\ \ldots,\ u_{n-1}\}$ является базисом для обоих этих пространств. В самом деле, если $x = \sum \xi_i u_i$, где $\xi_i \in L$ при $0 \leqslant i \leqslant n-1$, то $x\,(\varepsilon,\ \alpha^{-i}) = \xi_i$, так что если $x = 0$, то $\xi_i = 0$ при всех i. Аналогичное доказательство проходит, если рассматривать A как правое векторное пространство. Наконец, как было отмечено в конце доказательства леммы 4 § 3, определенный там изоморфизм Φ_{ε} из A в $M_n(K_{\mathrm{sep}})$, который является с другой точки зрения L-представлением алгебры A, можно использовать для вычисления приведенного следа τ и приведенной нормы ν на A. Беря $\{\varepsilon,\ \alpha^{-1},\ \ldots,\ \alpha^{-n+1}\}$ в качестве полной системы $\mathfrak{a}$ представителей для $\mathfrak{G}/\mathfrak{H}$ в $\mathfrak{G}$, используемой в определении Φ_{ε}, немедленно получаем, что при всех $\xi \in L$

$$\tau\,(\xi \cdot 1_A) = \mathrm{Tr}_{L/K}(\xi), \quad \tau\,(\xi u_i) = 0 \quad (1 \leqslant i \leqslant n-1), \tag{8}$$

$$\nu\,(\xi \cdot 1_A) = \mathrm{N}_{L/K}(\xi), \quad \nu\,(u_i) = (-1)^{i(n-i)}\,\theta^i \quad (1 \leqslant i \leqslant n-1). \tag{9}$$

Предложение 11. *Пусть L — циклическое расширение поля K степени n; α — образующая группы Галуа этого расширения; X — левое векторное пространство размерности n над L с базисом $\{u_0,\ u_1,\ \ldots,\ u_{n-1}\}$. Тогда для всякого $\theta \in K^{\times}$ существует одно и только одно K-билинейное ассоциативное отображение $(x,\ y) \to xy$ из $X \times X$ в X, для которого*: (i) $\xi x = (\xi u_0)\, x$ *и* $x u_0 = x$ *при всех* $\xi \in L$ *и всех* $x \in X$; (ii) $u_i = (u_1)^i$ *при всех* $1 \leqslant i \leqslant n-1$; (iii) $(u_1)^n = \theta u_0$; (iv) $\xi u_1 = u_1\,(\xi^{\alpha} u_0)$. *Это отображение превращает X в простую алгебру A над K, приведенный след и приведенная норма на которой удовлетворяют формулам* (8) *и* (9), *а класс факторов над K, связанный с A, равен $\{\chi,\ \theta\}$, где χ — такой связанный с L характер на $\mathfrak{G}$, для которого* $\chi(\alpha) = \mathbf{e}(1/n)$.

Поскольку для построенной выше алгебры A все это уже было доказано, нам остается лишь показать, что условия (i) — (iv) вместе с условием ассоциативности однозначно определяют умножение. Но в самом деле индукцией по i получаем из условия (iv), что $\xi u_i = u_i\,(\xi^{\alpha^i} u_0)$ при $0 \leqslant i \leqslant n-1$. Далее, используя (i) и ассоциативность умножения, находим, что при $0 \leqslant i,\ j \leqslant n-1$ для

всех ξ, η

$$(\xi u_i)\,(\eta u_j) = (\xi u_0)\,(u_i\,(\eta u_0))\,u_j = (\xi u_0)\,(\eta^{\alpha^{-i}} u_i)\,u_j =$$

$$= (\xi u_0)\,(\eta^{\alpha^{-i}} u_0)\,u_i u_j = \xi\eta^{\alpha^{-i}} u_i u_j.$$

Если $i + j \leqslant n - 1$, то по (ii) $u_i u_j = u_{i+j}$; если $i + j \geqslant n$, то $u_i u_j = \theta u_{i+j-n}$ по (ii) и (iii). Отсюда следует, что, используя (i) — (iv) и ассоциативность, можно однозначно записать $(\xi u_i)\,(\eta u_j)$ в виде ζu_k, где $\zeta \in L$, чем заканчивается доказательство нашего предложения.

О п р е д е л е н и е 6. *В предположениях и обозначениях предложения* 11 *определенную там алгебру* A *будем называть циклической алгеброй* $[L/K;\ \chi,\ \theta]$.

Иллюстрацией этого понятия, которое более подробно будет рассмотрено в следующих главах, служат алгебры с делением над коммутативным p-полем K. В самом деле, предложение 5 гл. I-4 означает в точности то, что каждую такую алгебру D можно представить как циклическую алгебру $[K_1/K;\ \chi,\ \pi]$, где K_1 — некоторое неразветвленное расширение поля K, χ — характер, связанный с K_1, и π — подходящий простой элемент в K. Но мы можем сказать больше: из предложения 10 в сочетании с предложением 3 гл. VIII-1 вытекает тривиальность $\{\chi,\ \xi\}$ при $\xi \in R^\times$, так что $\{\chi,\ \pi\}$ не зависит от выбора π; следовательно, и алгебра $[K_1/K;\ \chi,\ \pi]$ не зависит от выбора π, ибо с точностью до изоморфизма в заданном классе может существовать лишь одна алгебра заданной размерности над K.

В качестве еще одной иллюстрации изложенной выше теории применим ее к полю $K = \mathbf{R}$. Мы можем отождествить $\bar{K}$ с $\mathbf{C}$. Группа $\mathfrak{G}$ имеет только два элемента — тождественный автоморфизм ε и автоморфизм σ поля $\mathbf{C}$, определяемый равенством $\sigma(z) = \bar{z}$, и на $\mathfrak{G}$ имеется лишь один нетривиальный характер χ, для которого имеем $\chi(\sigma) = -1$. Циклическим расширением поля $\mathbf{R}$, связанным с χ, является $\mathbf{C}$. Комбинируя теперь следствие 2 предл. 3 § 1, следствие 3 теор. 3 § 3 и предложения 9 и 11, мы видим, что каждый класс простых алгебр над $\mathbf{R}$ содержит некоторую циклическую алгебру $[\mathbf{C}/\mathbf{R};\ \chi,\ \theta]$. Так как группа $N_{\mathbf{C}/\mathbf{R}}(\mathbf{C}^\times)$ совпадает с $\mathbf{R}^\times_+$ и имеет индекс 2 в $\mathbf{R}^\times$, то предложение 10 показывает, что с точностью до изоморфизма существуют ровно две такие алгебры, а именно тривиальная алгебра и алгебра $\mathbf{H} = [\mathbf{C}/\mathbf{R};\ \chi,\ -1]$. Последняя является алгеброй с делением. В самом деле, она имеет над $\mathbf{R}$ размерность 4. Записывая ее в виде $M_n(D)$, где D — алгебра с делением над $\mathbf{R}$, и обозначая через d^2 размерность алгебры D над $\mathbf{R}$, получаем $nd = 2$, откуда $n = 1$, ибо алгебра $\mathbf{H}$ нетривиальна. Записывая

алгебру $\mathbf{H}$ указанным в предложении 11 способом, мы видим, что она имеет базис над $\mathbf{C}$, состоящий из двух элементов $u_0 = 1$ и u_1, следовательно, она имеет базис над $\mathbf{R}$, состоящий из 1, i, $j = u_1$ и $k = iu_1$. Тривиально проверяется, что таблица умножения для 1, i, j, k — это хорошо известная таблица для «кватернионных единиц» в алгебре $\mathbf{H}$ «классических» кватернионов.

§ 5. СПЕЦИАЛЬНЫЕ ЦИКЛИЧЕСКИЕ СИСТЕМЫ ФАКТОРОВ

Теперь мы применим результаты § 4 к характерам, связанным с *расширениями Куммера* и *расширениями Артина — Шреера* поля K.

В первом случае пусть n таково, что K содержит n различных корней n-й степени из 1; эти корни образуют циклическую группу E порядка n. Разумеется, если K — поле характеристики $p > 1$, то из нашего предположения следует, что n взаимно просто с p. Пусть ψ — изоморфизм из E на группу корней n-й степени из 1 в $\mathbf{C}$. Он однозначно определен, если мы выберем какую-нибудь образующую ε_1 в E и потребуем, чтобы $\psi(\varepsilon_1) = \mathbf{e}(1/n)$. Возьмем произвольный элемент $\xi \in K^\times$, и пусть x — любой из корней уравнения $X^n = \xi$ в $\overline{K}$. Тогда $x \in K_{\text{sep}}^\times$ и уравнение $X^n = \xi$ имеет n различных корней εx с $\varepsilon \in E$. В частности, для всякого $\sigma \in \mathfrak{G}$ элемент x^σ должен быть одним из этих корней, так что $x^\sigma x^{-1} \in E$. Положим теперь

$$\chi_{n,\xi}(\sigma) = \psi(x^\sigma x^{-1}).$$

Так как $E \subset K$, то правая часть не изменяется, если заменить x на εx с $\varepsilon \in E$, и, следовательно, не зависит от выбора корня x уравнения $X^n = \xi$. По аналогичной причине для всех ρ, σ из $\mathfrak{G}$ имеем

$$x^{\rho\sigma}x^{-1} = (x^\rho x^{-1})^\sigma (x^\sigma x^{-1}) = (x^\rho x^{-1})(x^\sigma x^{-1}),$$

поэтому

$$\chi_{n,\xi}(\rho\sigma) = \chi_{n,\xi}(\rho)\,\chi_{n,\xi}(\sigma),$$

откуда видно, что $\chi_{n,\xi}$ — характер на $\mathfrak{G}$. Возьмем теперь любое $\eta \in K^\times$ и обозначим через y какой-нибудь корень уравнения $X^n = \eta$. Тогда xy является корнем уравнения $X^n = \xi\eta$ и для всех $\sigma \in \mathfrak{G}$ мы имеем

$$(xy)^\sigma (xy)^{-1} = (x^\sigma x^{-1})(y^\sigma y^{-1}),$$

а значит,

$$\chi_{n,\xi\eta} = \chi_{n,\xi}\chi_{n,\eta},$$

откуда видно, что $\xi \to \chi_{n,\xi}$ есть морфизм из $K^\times$ в группу характеров на $\mathfrak{G}$. Очевидно, характер $\chi_{n,\xi}$ тривиален в том и только в том случае, когда из корней уравнения $X^n = \xi$ в K лежит хотя бы один, а значит, и все, т. е. когда $\xi \in (K^\times)^n$. Другими словами, $(K^\times)^n$ есть ядро отображения $\xi \to \chi_{n,\xi}$. Было бы нетрудно показать, что образ группы $K^\times$ при этом морфизме состоит из всех характеров на $\mathfrak{G}$, порядок которых делит n, но нам это не понадобится в дальнейшем.

Теперь, для ξ и θ из $K^\times$ положим

$$\{\chi_{n,\xi},\ \theta\} = \{\xi,\ \theta\}_n.$$

Это — известный *символ Гильберта*. Следует заметить, что он зависит от выбора ψ, или, что то же самое, от выбора образующей ε_1 группы E корней n-й степени из 1 в K. Согласно предложению 8 § 4, имеем

$$(10)\quad \{\xi\xi',\ \theta\}_n = \{\xi,\ \theta\}_n \cdot \{\xi',\ \theta\}_n, \qquad \{\xi,\ \theta\theta'\}_n = \{\xi,\ \theta\}_n \cdot \{\xi,\ \theta'\}_n$$

при всех ξ, ξ', θ, θ' из $K^\times$.

Обозначим снова через x какой-нибудь корень уравнения $X^n = \xi$. Ясно, что ядро $\mathfrak{H}$ морфизма $\chi_{n,\xi}$ состоит из тех элементов $\sigma \in \mathfrak{G}$, для которых $x^\sigma = x$, так что соответствующим подполем в K_{sep}, являющимся циклическим расширением поля K, связанным с $\chi_{n,\xi}$, будет $L = K(x)$. Обозначим через d порядок характера $\chi_{n,\xi}$. Тогда $\chi_{n,\xi}$ определяет изоморфизм из $\mathfrak{G}/\mathfrak{H}$ на группу всех корней d-й степени из 1 в $\mathbf{C}$. Число d делит n и равняется степени поля L над K. Поэтому различными сопряженными к элементу x над K, т. е. его образами при d различных автоморфизмах поля L над K, являются элементы εx, где ε пробегает группу E' всех корней d-й степени из 1 в K. Запишем $e = n/d$ и для всякого элемента $\zeta \in K$ положим

$$\omega = \prod_{\nu=0}^{e-1} (\zeta - \varepsilon_1^\nu x),$$

где ε_1, как и прежде,— некоторая образующая группы E. Поскольку элементы ε_1^ν при $0 \leqslant \nu \leqslant e-1$ образуют полное множество представителей классов смежности в E по E', имеем

$$\mathrm{N}_{L/K}(\omega) = \prod_{\varepsilon \in E} (\zeta - \varepsilon x) = \zeta^n - \xi.$$

Беря $\zeta = 0$ и $\zeta = 1$, мы видим, что $-\xi$ и $1 - \xi$ лежат в $\mathrm{N}_{L/K}(L)$. В силу предложения 10 § 4 это дает

$$(11)\qquad \{\xi,\ -\xi\}_n = 1, \quad \{\xi,\ 1-\xi\}_n = 1,$$

где формулы справедливы всякий раз, когда они имеют смысл, т. е. первая формула при всех $\xi \in K^\times$, а вторая при всех $\xi \neq 1$ в $K^\times$. Заменяя в первой формуле ξ на $\xi\eta$, где $\xi, \eta \in K^\times$, и применяя (10), получаем

$$\{\xi, -\xi\}_n \cdot \{\xi, \eta\}_n \cdot \{\eta, -\xi\}_n \cdot \{\eta, \eta\}_n = 1.$$

Ввиду (11) первый сомножитель в левой части равен 1, а последний равен $\{\eta, -1\}_n$. Снова применяя (10), получаем

$$\{\xi, \eta\}_n \cdot \{\eta, \xi\}_n = 1. \tag{12}$$

Эта формула известна как *закон взаимности* для символа $\{\xi, \eta\}_n$.

То же самое можно было бы доказать, используя явную конструкцию простой алгебры, соответствующей последнему классу факторов. Мы дадим лишь краткий набросок доказательства для случая, когда оба уравнения $X^n = \xi$, $X^n = \eta$ неприводимы над K. Положим $L = K(x)$, где x — какой-нибудь корень уравнения $X^n = \xi$. Пусть A — циклическая алгебра $[L/K;\ \chi_{n,\xi},\ \eta]$. По предложению 11 § 4, где вместо u_1 мы пишем теперь y, алгебра A имеет базис над L, состоящий из элементов y^j, $0 \leqslant j \leqslant n-1$; следовательно, элементы $x^i y^j$, $0 \leqslant i,\ j \leqslant n-1$, образуют базис алгебры A над K, причем элементы этого базиса связаны следующими соотношениями: $x^n = \xi$, $y^n = \eta$, $xy = \varepsilon_1 yx$. Если мы поменяем местами ξ и η, а также x и y, то алгебра A, очевидно, заменится на противоположную алгебру A^0, откуда и следует (12).

Пусть теперь K — поле характеристики $p > 1$. Отождествим простое подполе в K с $\mathbf{F}_p$ и обозначим через ψ характер аддитивной группы поля $\mathbf{F}_p$, задаваемый условием $\psi(1) = \mathbf{e}(1/p)$. Возьмем произвольный элемент $\xi \in K$, и пусть x — какой-нибудь из корней уравнения $X - X^p = \xi$. Тогда x лежит в K_{sep}, и это уравнение имеет p различных корней $x + a$, где $a \in \mathbf{F}_p$. В частности, для всякого $\sigma \in \mathfrak{G}$ элемент x^σ должен быть одним из этих корней, так что $x^\sigma - x$ лежит в $\mathbf{F}_p$. Положим

$$\chi_{p,\xi}(\sigma) = \psi(x^\sigma - x).$$

Так как правая часть не изменяется, если заменить x на $x + a$ с $a \in \mathbf{F}_p$, то она не зависит от выбора x. Вычисления, совершенно аналогичные тем, которые были проведены для $\chi_{n,\xi}$, показывают, что $\chi_{p,\xi}$ является характером на $\mathfrak{G}$ и что отображение $\xi \to \chi_{p,\xi}$ есть морфизм аддитивной группы поля K в (мультипликативную) группу характеров на $\mathfrak{G}$. Ядром этого морфизма является образ поля K при отображении $\xi \to \xi \to \xi^p$ поля K в себя, и снова легко было бы показать, что образ этого морфизма состоит из $\chi = 1$ и всех характеров на $\mathfrak{G}$, порядок которых равен p. Для всех $\xi \in K$ и всех $\theta \in K^\times$ положим

теперь

$$\{\chi_{p,\xi}, \theta\} = \{\xi, \theta\}_p.$$

Тогда

(13) $\{\xi + \xi', \theta\}_p = \{\xi, \theta\}_p \cdot \{\xi', \theta\}_p,$

$$\{\xi, \theta\theta'\}_p = \{\xi, \theta\}_p \cdot \{\xi, \theta'\}_p$$

при всех ξ, ξ' из K и всех θ, θ' из $K^\times$. Предположим, что x не лежит в K. Тогда $L = K(x)$ есть циклическое расширение поля K, связанное с $\chi_{p,\xi}$, и его степень над K равна p. Уравнение $X^p - X + \xi = 0$ должно быть поэтому неприводимым уравнением для x над K, так что $N_{L/K}(x) = (-1)^p\xi = -\xi$. В силу предложения 10 § 4 отсюда следует, что

(14) $$\{\xi, -\xi\}_p = 1.$$

Таким образом, это равенство справедливо для любого x, не лежащего в K. Если $x \in K$, то характер $\chi_{p,\xi}$ тривиален, так что формула (14) справедлива всякий раз, когда она имеет смысл, т. е. при всяком $\xi \neq 0$. Таким образом, формула (14) имеет место при всех $\xi \in K^\times$.

ГЛАВА ДЕСЯТАЯ

ПРОСТЫЕ АЛГЕБРЫ НАД ЛОКАЛЬНЫМИ ПОЛЯМИ

§ 1. ПОРЯДКИ И РЕШЕТКИ

Пусть D — алгебра с делением конечной размерности над некоторым полем K. Мы будем рассматривать левые векторные пространства над D; размерность их всегда будет предполагаться конечной и отличной от нуля. Если V и W — два таких пространства, то мы обозначаем через $\mathrm{Hom}\,(V, W)$ пространство всех гомоморфизмов из V в W. Пусть оно действует на V справа; другими словами, если α — такой гомоморфизм и $v \in V$, то мы обозначаем через $v\alpha$ образ элемента v при гомоморфизме α. Пространство $\mathrm{Hom}\,(V, W)$ можно очевидным образом рассматривать как векторное пространство над K; как таковое, оно имеет конечную размерность, будучи подпространством пространства всех K-линейных отображений из V в W. Как обычно, мы пишем $\mathrm{End}\,(V)$ вместо $\mathrm{Hom}\,(V, V)$.

Если V, V', V'' — левые векторные пространства над D и $\alpha \in \mathrm{Hom}\,(V, V')$, $\beta \in \mathrm{Hom}\,(V', V'')$, то мы обозначаем через $\alpha\beta$ морфизм $v \to (v\alpha)\beta$ из V в V''. В случае $V = V' = V''$ мы превращаем тем самым $\mathrm{End}\,(V)$ в кольцо. Как обычно, мы используем символ $\mathrm{Aut}\,(V)$ для обозначения $\mathrm{End}\,(V)^\times$ — группы автоморфизмов пространства V. При $V = V'$, $V'' = W$ получаем структуру левого $\mathrm{End}\,(V)$-модуля на $\mathrm{Hom}\,(V, W)$. При $V' = V'' = W$ получаем структуру правого $\mathrm{End}\,(W)$-модуля на $\mathrm{Hom}\,(V, W)$.

Пусть D и V такие, как выше, d^2 — размерность алгебры D над K и m — размерность пространства V над D. Выберем какой-нибудь базис $\{v_1, \ldots, v_m\}$ в V над D. Для каждого $\xi \in \mathrm{End}\,(V)$ запишем $v_i\xi = \sum_j x_{ij}v_j$, где $x_{ij} \in D$, $1 \leqslant i, j \leqslant m$. Этим определяется отображение $\xi \to (x_{ij})$ из $\mathrm{End}\,(V)$ в $M_m\,(D)$, которое, очевидно, является изоморфизмом из $\mathrm{End}\,(V)$ на $M_m\,(D)$. В частности, отсюда видно, что $\mathrm{End}\,(V)$ — простая алгебра размерности $m^2 d^2$ над K. Ясно, что пространство V, рассматриваемое как правый $\mathrm{End}\,(V)$-модуль, является простым. Поэтому в силу предложения 1 гл. IX-1

каждый такой модуль разлагается в прямую сумму модулей, изоморфных V.

Пусть V и W — левые векторные пространства над D и m и n — их размерности. Положим $A = \mathrm{End}\,(V)$, $B = \mathrm{End}\,(W)$, $H = \mathrm{Hom}\,(V, W)$. Как правый B-модуль H разлагается в прямую сумму модулей, изоморфных W. Сравнивая размерности над K, сразу видим, что число прямых слагаемых равно m. Аналогично, как левый A-модуль H разлагается в прямую сумму m модулей, изоморфных пространству $V' = \mathrm{Hom}\,(V, D)$, двойственному к V; V' является простым левым A-модулем и правым векторным пространством размерности m над D. Легко можно было бы убедиться, что каждый эндоморфизм левого A-модуля H имеет вид $\lambda \to \lambda\beta$ с $\beta \in B$ и что каждый эндоморфизм правого B-модуля H имеет вид $\lambda \to \alpha\lambda$, где $\alpha \in A$.

Пусть D, V и $A = \mathrm{End}\,(V)$ такие, как выше, и пусть ν — приведенная норма на A. По следствию 1 предл. 6 гл. IX-2 для любого $\alpha \in A$ определитель эндоморфизмов $x \to \alpha x$ и $x \to x\alpha$ векторного пространства A над K равен $\nu(\alpha)^{md}$. В частности, $\alpha \in A^\times$ в том и только в том случае, когда $\nu(\alpha) \neq 0$.

Если K — локальное поле, то все рассматриваемые выше пространства, будучи конечномерными векторными пространствами над K, могут быть одним и только одним способом топологизированы как таковые согласно следствию 1 теор. 3 гл. I-2. Обратно, по по следствию 2 той же теоремы требование конечномерности над K можно было бы везде заменить условием локальной компактности. Положим снова $A = \mathrm{End}\,(V)$. Тогда группа $A^\times = \mathrm{Aut}\,(V)$ является открытым подмножеством в A, определяемым условием $\nu(\alpha) \neq 0$, а потому локально компактной группой. Кроме того, мера Хаара на ней и право- и левоинвариантна. Это вытекает из следующей леммы, которая обобщает лемму 5 гл. VII-4.

Лемма 1. *Пусть K — локальное поле, D, V и $A = \mathrm{End}\,(V)$ таковы, как выше, и α — мера Хаара на A. Тогда мера μ на $A^\times$, задаваемая формулой*

$$d\mu(x) = \mathrm{mod}_K(N_{A/K}(x))^{-1}\, d\alpha(x) = \mathrm{mod}_K(\nu(x))^{-md}\, d\alpha(x),$$

является одновременно левоинвариантной и правоинвариантной мерой на $A^\times$.

Это немедленно вытекает из следствия 1 предл. 6 гл. IX-2 в сочетании со следствием 3 теор. 3 гл. I-2.

В оставшейся части этого параграфа мы предполагаем, что K — коммутативное p-поле. Следовательно, алгебра с делением D над K также является p-полем (которое некоммутативно при $d \neq 1$). Обозначим через R и R_D максимальные компактные подкольца в K и в D и через P и P_D — максимальные идеалы в R и в R_D соответственно.

Пусть V и W такие, как выше, L — некоторая D-решетка в V и M — некоторая D-решетка в W. Обозначим через $\mathrm{Hom}(V, L; W, M)$ множество всех морфизмов из V в W, отображающих L в M. Выберем базисы $\{v_1, \ldots, v_m\}$, $\{w_1, \ldots, w_n\}$ в V и в W в соответствии с теоремой 1 гл. II-2, т. е. так, чтобы $L = \sum R_D v_i$ и $M = \sum R_D w_j$. Для всякого $\lambda \in \mathrm{Hom}(V, W)$ мы можем записать $v_i\lambda = \sum x_{ij} w_j$, где $x_{ij} \in D$ при $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, и определить таким образом биекцию $\lambda \to (x_{ij})$ из $\mathrm{Hom}(V, W)$ на пространство $M_{m,n}(D)$ всех матриц над D с m строками и n столбцами. Ясно, что $\lambda \in \mathrm{Hom}(V, L; W, M)$ в том и только в том случае, когда матрица (x_{ij}) лежит в $M_{m,n}(R_D)$. В частности, отсюда следует, что $\mathrm{Hom}(V, L; W, M)$ является K-решеткой в пространстве $\mathrm{Hom}(V, W)$, рассматриваемом как векторное пространство над K, а также что $\mathrm{Hom}(V, L; W, M)$ можно отождествить с пространством всех морфизмов R_D-модуля L в R_D-модуль M. Мы будем писать $\mathrm{End}(V, L)$ вместо $\mathrm{Hom}(V, L; V, L)$. Это — K-решетка и открытое компактное подкольцо в $\mathrm{End}(V)$, которое можно отождествить с $\mathrm{End}(L)$. Далее, будем писать $\mathrm{Aut}(V, L)$ вместо $\mathrm{End}(V, L)^\times$. Это — группа автоморфизмов решетки L.

Предложение 1. *Пусть K — некоторое p-поле, D — алгебра с делением над K, V — левое векторное пространство над D и L — некоторая D-решетка в V, и пусть ν — приведенная норма на алгебре $A = \mathrm{End}(V)$ над K. Тогда группа $\mathrm{Aut}(V, L)$ состоит из тех элементов $\xi \in \mathrm{End}(V, L)$, для которых $\mathrm{mod}_K(\nu(\xi)) = 1$.*

Возьмем элемент $\xi \in A$; он лежит в $A^\times$ тогда и только тогда, когда $\nu(\xi) \neq 0$. Модуль автоморфизма $x \to x\xi$ алгебры A равен $\mathrm{mod}_K(\nu(\xi))^{md}$, где m, d такие, как выше. Поскольку A как правый A-модуль разлагается в прямую сумму m модулей, изоморфных V, отсюда следует, что модуль автоморфизма $v \to v\xi$ пространства V равен $\mathrm{mod}_K(\nu(\xi))^d$. Предположим теперь, что $\xi \in \mathrm{End}(V, L)$. Тогда эндоморфизм ξ отображает L на D-решетку $L' = L\xi$, содержащуюся в L, так что его модуль равен $[L : L']^{-1}$. Отсюда видно, что $L = L'$ в том и только в том случае, когда $\mathrm{mod}_K(\nu(\xi)) = 1$. Наше предложение доказано.

Следствие. *В обозначениях предложения* 1 *группа* Aut (V, L) *является компактным открытым подмножеством в* End (V, L) *и в* End (V) *и компактной открытой подгруппой в* Aut (V).

Это очевидно.

Предложение 2. *Пусть* V *таково, как в предложении* 1, *и пусть* X *— замкнутое относительно умножения подмножество в* End (V). *Тогда* X *относительно компактно в* End (V) *в том и только в том случае, когда существует такая* D*-решетка* L *в* V, *что* $X \subset \mathrm{End}\,(V, L)$.

Пусть X относительно компактно в End (V). Заменяя в случае надобности X на его замыкание, можно считать, что X компактно. Пусть L — любая D-решетка в V. Обозначим через L' множество тех векторов $v \in L$, для которых $v\xi \in L$ при всех $\xi \in X$. Ясно, что L' является R_D-модулем и, следовательно, замкнуто в силу предложения 5 гл. II-2. Так как $L' \subset L$, то L' — компакт. Так как X компактно, а L открыто, то L' открыто. Поэтому множество L' является D-решеткой. Поскольку X мультипликативно замкнуто, то $v\xi$ лежит в L' при всех $v \in L'$ и всех $\xi \in X$, так что $X \subset \mathrm{End}\,(V, L')$. Обратное утверждение очевидно.

Предложение 3. *Пусть* V *такое, как выше, и пусть* L, L' *— две* D*-решетки в* V. *Тогда или* Aut (V, L) *не содержится в* End (V, L'), *или существует такое* $x \in D^\times$, *что* $L' = xL$.

По теореме 2 гл. II-2 существует такой базис $\{v_1, \ldots, v_m\}$ в V и такие целые числа ν_i, что $L = \Sigma\, R_D v_i$ и $L' = \Sigma\, P_D^{\nu_i} v_i$. Каждая перестановка элементов v_i определяет автоморфизм пространства V, который содержится в Aut (V, L). Если все эти автоморфизмы содержатся в End (V, L'), то все ν_i должны совпадать между собой. Пусть ν — их общее значение. Тогда $L' = \pi_D^\nu L$ для любого простого элемента $\pi_D \in D$.

Теорема 1. *Пусть* D *— алгебра с делением над* p*-полем* K, V *— левое векторное пространство над* D. *Тогда максимальные компактные подкольца в алгебре* $A = \mathrm{End}\,(V)$ *— это кольца* End (V, L), *а максимальные компактные подгруппы в* $A^\times$ *— это группы* Aut (V, L), *где в качестве* L *берутся всевозможные* D*-решетки в* V.

По предложению 2 любое компактное подкольцо в End (V) должно содержаться в некотором кольце End (V, L) и, следовательно, совпадать с ним, если оно максимально. Теперь предположим, что для некоторой решетки L кольцо End (V, L) содержится в компактном подкольце $X \in \mathrm{End}\,(V)$. Тогда X в свою очередь должно содер-

жаться в некотором кольце End (V, L'). По предложению 3, $L' = xL$ для некоторого $x \in D^\times$, откуда End $(V, L') =$ End (V, L) и, следовательно, $X =$ End (V, L). Аналогично компактная подгруппа в $A^\times =$ Aut (V) должна содержаться в некотором кольце End (V, L) и, следовательно, в End $(V, L)^\times$, т. е. в Aut (V, L). Если последняя группа содержится в компактной подгруппе $X \subset$ $\subset$ Aut (V), то эта подгруппа должна содержаться в некотором кольце End (V, L'), и точно так же, как прежде, мы получаем, что $L' = xL$ и $X =$ Aut (V, L). В формулировке теоремы 1 можно потребовать, чтобы L пробегало не все D-решетки в V, а лишь некоторое полное множество представителей классов эквивалентности, причем решетка L считается эквивалентной решетке L', если $L' = xL$, где $x \in D^\times$.

Компактные открытые подкольца простой алгебры над p-полем называются также *порядками*. Таким образом, первая часть теоремы 1 утверждает существование *максимальных порядков* в алгебре $A =$ End (V); а именно таковы все кольца End (V, L). Как было показано выше, все они изоморфны кольцу $M_m(R_D)$, где m — размерность пространства V над D. Ясно, что они переводятся друг в друга автоморфизмами пространства V (поскольку всякий базис в V над D можно перевести таким автоморфизмом в любой другой базис). Другими словами, они переводятся друг в друга внутренними автоморфизмами алгебры A.

Предложение 4. *Пусть алгебра D такая, как выше; V, W — левые векторные пространства над D; M, M' — компактные открытые подгруппы в* Hom (V, W); *X — множество тех элементов ξ из* End (V), *для которых $\xi M \subset M'$. Тогда X является компактной открытой подгруппой в* End (V). *Если $M = M'$, то X — подкольцо в* End (V).

Очевидно, что X — подгруппа в End (V) и что X — подкольцо в End (V), если $M = M'$. Так как подгруппа M компактна, а подгруппа M' открыта, то подгруппа X открыта. Положим теперь $H =$ $=$ Hom (V, W). Поскольку подгруппа M открыта, в ней содержится базис $\{\mu_1, \ldots, \mu_r\}$ векторного пространства H над K. Если мы теперь рассмотрим H как левый End (V)-модуль, то аннулятор этого базиса в End (V) совпадает с аннулятором всего H и, следовательно, равен $\{0\}$, поскольку алгебра End (V) проста, а $W \neq$ $\neq \{0\}$. Поэтому отображение $\xi \to (\xi\mu_1, \ldots, \xi\mu_r)$ из End (V) в $H^r = H \times \ldots \times H$ инъективно и, следовательно, является изоморфизмом векторного пространства End (V) над K на его образ в H^r, а значит, и изоморфизмом соответствующих топологических структур. Отсюда следует, что множество X' тех элементов ξ из

End (V), для которых $\xi\mu_i \in M'$ при $1 \leqslant i \leqslant r$, компактно. Так как X — подгруппа в X', открытая в End (V), она является открытой подгруппой в X' и, следовательно, замкнута в X', а потому компактна.

В случае $M = M'$ определенное в предложении 4 кольцо X называется *левым порядком* для M. Меняя ролями правое и левое, мы видим, что множество Y тех элементов η из End (W), для которых $M\eta \subset M$, является компактным открытым подкольцом в End (W); это кольцо называется *правым порядком* для M. Сейчас мы покажем, что если один из этих порядков максимален, то и другой тоже максимален. Это вытекает из следующей теоремы.

Теорема 2. *Пусть K и D такие, как в теореме* 1; *V и W — левые векторные пространства над D*; *L — некоторая D-решетка в V*; *N — такая компактная открытая подгруппа в* Hom (V, W), *что $\xi N \subset N$ при всех ξ из* End (V, L). *Тогда существует D-решетка M в W, для которой* $N = \mathrm{Hom}\,(V, L; W, M)$ *и правым и левым порядками для N являются* End (V, L) *и* End (W, M) *соответственно.*

По теореме 1 гл. II-2 мы можем выбрать такой базис $\{v_1, \ldots, v_m\}$ в V над D, что $L = \Sigma R_D v_i$. Как объяснялось выше, мы можем при помощи этого базиса отождествить End (V) с $M_m(D)$ и End (V, L) с $M_m(R_D)$, сопоставив каждому элементу ξ из End (V) матрицу (x_{ij}), определяемую равенствами $v_i\xi = \Sigma x_{ij}v_j$. Рассмотрим теперь отображение $\alpha \to (v_1\alpha, \ldots, v_m\alpha)$ из Hom (V, W) в W^m — прямую сумму m пространств, изоморфных W. Ясно, что это — биекция из Hom (V, W) на W^m. Обозначим ее через φ и положим $N' = \varphi(N)$, где N — множество из теоремы 2. Если $\alpha \in \mathrm{Hom}\,(V, W)$, $\varphi(\alpha) = (w_1, \ldots, w_m)$ и ξ и (x_{ij}) такие, как выше, то $\varphi(\xi\alpha) = (w_1', \ldots, w_m')$, где $w_i' = \Sigma x_{ij}w_j$, $1 \leqslant i \leqslant m$. Согласно нашему предположению относительно N элемент $\varphi(\xi\alpha)$ должен лежать в N', каковы бы ни были $(w_1, \ldots, w_m) \in N'$ и $x_{ij} \in R_D$. Обозначим через e_{ij} «матричные единицы» в $M_m(D)$, определенные в доказательстве теоремы 1 гл. IX-4. Беря сначала в качестве (x_{ij}) матричную единицу e_{hh}, мы видим, что при $(w_1, \ldots, w_m) \in N'$ каждый из элементов $(0, \ldots, 0, w_h, 0, \ldots, 0)$, $1 \leqslant h \leqslant m$, также должен лежать в N'. Другими словами, если мы обозначим через $W_1, \ldots, W_m$ прямые слагаемые в сумме W^m и положим $N_h' = N' \cap W_h$ при $1 \leqslant h \leqslant m$, то $N' = \Sigma N_h'$. Аналогично взяв в качестве (x_{ij}) матричную единицу e_{hk}, мы видим, что $N_h' = N_k'$ для всех h и k. Обозначим их общее значение через M, так что $M = N_h'$ для любого h. Наконец, взяв в качестве (x_{ij}) матрицу $x \cdot 1_m$ с $x \in R_D$, мы видим, что M является R_D-модулем. Так как группа N открыта и компактна в Hom (V, W), то такова же и груп-

па N' в W^m, а следовательно, и N'_h в W_h и M в W. Поэтому M является D-решеткой в W. Теперь мы видим, что элемент α из $\mathrm{Hom}\,(V, W)$ лежит в N тогда и только тогда, когда элементы $v_i\alpha$ лежат в M при $1 \leqslant i \leqslant m$. Другими словами, $N = \mathrm{Hom}\,(V, L; W, M)$. Значит, левый и правый порядки для N содержат $\mathrm{End}\,(V, L)$ и $\mathrm{End}\,(W, M)$ соответственно. Поскольку последние порядки максимальны, доказательство теоремы закончено.

Следствие 1. *Пусть A — простая алгебра над K, R_A — максимальное компактное подкольцо в A и I — левый идеал в R_A. Тогда идеал I открыт в A в том и только в том случае, когда его можно записать в виде $I = R_A\alpha$, где $\alpha \in R_A \cap A^\times$.*

Мы можем предположить, что $A = \mathrm{End}\,(V)$, где V таково, как в теореме 2. Ввиду теоремы 1 можно считать, что $R_A = \mathrm{End}\,(V, L)$, где решетка L такова, как в теореме 2. Если идеал I открыт, то к нему можно применить теорему 2, взяв $W = V$ и $N = I$. Это дает $I = \mathrm{Hom}\,(V, L; V, M)$, где M — некоторая D-решетка в V. Возьмем такие базисы $\{v_1, \ldots, v_m\}$, $\{w_1, \ldots, w_m\}$ в V, что $L = \Sigma\, R_D v_i$ и $M = \Sigma\, R_D w_i$, и обозначим через ξ автоморфизм пространства V, который отображает первый из этих базисов на второй. Тогда $M = L\xi$ и $I = R_A\xi$. Так как автоморфизм ξ лежит в I, то он лежит в R_A. Обратное утверждение очевидно.

Следствие 2. *Пусть A и R_A таковы, как в следствии* 1, *и пусть J — компактный двусторонний R_A-модуль в A, отличный от $\{0\}$. Тогда множество J открыто в A. Если $A = \mathrm{End}\,(V)$ и $R_A = \mathrm{End}\,(V, L)$, где V и L таковы, как в теореме* 2, *то J можно записать в виде $J = \mathrm{Hom}\,(V, L; V, \pi_D^{\nu} L)$, где $\nu \in \mathbf{Z}$ и π_D — простой элемент в D.*

Так как R_A является K-решеткой в A, то мы можем выбрать базис $\{\alpha_1, \ldots, \alpha_N\}$ в A над K, содержащийся в R_A. Если ξ лежит в A и отличен от нуля, то двусторонний идеал, порожденный в A элементом ξ, совпадает с A, поскольку алгебра A проста. Поэтому элементы $\alpha_i\xi\alpha_j$ при $1 \leqslant i, j \leqslant N$ порождают A как векторное пространство над K, так что порожденный ими R-модуль в A является K-решеткой, а следовательно, открыт. Отсюда следует, что наше множество J должно быть открытым. По теореме 2 мы можем записать его в виде $J = \mathrm{Hom}\,(V, L; V, M)$, где M — такая D-решетка в V, что $\mathrm{End}\,(V, M)$ содержит $\mathrm{End}\,(V, L)$. Применяя предложение 3, получаем, что $M = xL$, где $x \in D^\times$. Поэтому $M = \pi_D^{\nu} L$, где $\nu = \mathrm{ord}_D\,(x)$.

Если V и W таковы, как в теореме 2, то всякое множество N, обладающее описанными там свойствами, т. е. всякое множество, которое можно записать в виде $N = \mathrm{Hom}(V, L; W, M)$ при подходящем выборе D-решеток L в V и M в W, будем называть *нормальной решеткой* в $\mathrm{Hom}(V, W)$.

§ 2. СЛЕДЫ И НОРМЫ

Как и прежде, мы будем рассматривать локальное поле K, алгебру с делением D размерности d^2 над K и простую алгебру A над K, изоморфную алгебре $M_m(D)$ для некоторого $m \geqslant 1$. Обозначим через τ и τ_D приведенные следы на A и на D и через ν и ν_D приведенные нормы на A и на D соответственно. Сначала рассмотрим случай p-поля.

Предложение 5. *Пусть K — некоторое p-поле, D — алгебра с делением размерности d^2 над K, R_D — максимальное компактное подкольцо в D и π_D — простой элемент в D. Для любого $m \geqslant 1$ положим $A = M_m(D)$ и $R_A = M_m(R_D)$, и пусть τ — приведенный след на A. Тогда множество таких элементов x в A, что $\tau(xy) \in R$ при всех $y \in R_A$, совпадает с $\omega R_A = R_A\omega$, где $\omega = \pi_D^{1-d} \cdot 1_m$.*

Предположим сначала, что $m = 1$, $A = D$, $R_A = R_D$. Как уже было замечено в гл. IX-4, из предложения 5 гл. I-4 следует, что D можно рассматривать как циклическую алгебру $[K_1/K; \chi, \pi]$ над K, где K_1 — неразветвленное расширение поля K степени d, χ — характер, связанный с этим расширением, и π — простой элемент в K. Поэтому сопоставление упомянутого предложения с определением циклической алгебры в предложении 11 гл. IX-4 показывает, что u_1 из последнего предложения является простым элементом в D. Утверждение нашего предложения инвариантно относительно замены π_D на u_1, поэтому мы можем положить $\pi_D = u_1$. Тогда в обозначениях предложения 11 гл. IX-4 имеем $u_i = \pi_D^i$ при $0 \leqslant i \leqslant d-1$ и $\pi = \pi_D^d$. Обозначим через R_1 максимальное компактное подкольцо в K_1. Согласно пункту (b) предложения 5 гл. I-4 R_D совпадает с левым R_1-модулем, порожденным элементами $u_0, \ldots, u_{d-1}$. Поэтому элемент $x \in D$ тогда и только тогда обладает свойствами, указанными в формулировке нашего предложения, когда $\tau_D(x\eta\pi_D^j) \in R$ при всех $\eta \in R_1$ и $0 \leqslant j \leqslant d-1$. Снова используя пункт (b) предложения 5 гл. I-4, мы можем записать x в виде $x = \sum_i \xi_i \pi_D^i$, где $\xi_i \in K_1$ для $0 \leqslant i \leqslant d-1$. Применяя для приведенного следа τ_D на D формулу (8) гл. IX-4, при $j = 0$ получаем,

что $\mathrm{Tr}_{K_1/K}(\xi_0\eta) \in R$ для всех $\eta \in R_1$. Но согласно предложению 3 гл. VIII-1 это имеет место в том и только в том случае, когда $\xi_0 \in R_1$. Аналогичным образом, для $1 \leqslant j \leqslant d-1$ наше условие можно записать в виде $\mathrm{Tr}_{K_1/K}(\xi_{d-j}\eta'\pi) \in R$, где $\eta' = \eta^\beta$, $\beta = \alpha^{j-d}$. Так как каждый автоморфизм β поля K_1 отображает R_1 на себя, то последнее условие должно выполняться при всех $\eta' \in R_1$, а это, как и прежде, эквивалентно тому, что $\xi_{d-j} \in \pi^{-1}R_1$. Поэтому множество, определенное в нашем предложении, совпадает с R_1-модулем, порожденным элементами $1, \pi^{-1}\pi_D, \ldots, \pi^{-1}\pi_D^{d-1}$, т. е. элементами $\omega_D\pi_D^i$, $0 \leqslant i \leqslant d-1$, если $\omega_D = \pi^{1-d}_D$. Ввиду пункта (*b*) предл. 5 гл. I-4 этим завершено наше доказательство для случая $m = 1$. Для $m > 1$ наше утверждение легко вытекает из уже доказанного и из следствия 2 предл. 6 гл. IX-2, которое утверждает, что $\tau(x) = \Sigma\, \tau_D(x_{ii})$ при $x = (x_{ij}) \in A$.

Следствие 1. *В предположениях и обозначениях предложения* 5 *пусть* χ *— характер на* K *порядка* 0. *Отождествим* A *с топологическим двойственным к нему, полагая* $\langle x, y\rangle = \chi(\tau(xy))$. *Тогда* K*-решеткой, двойственной к* R_A, *будет* ωR_A.

В самом деле, эта двойственная решетка определяется как множество тех элементов x из A, для которых $\chi(\tau(xy)) = 1$ при всех $y \in R_A$. Ввиду K-линейности следа τ последнее условие означает в точности то, что $\chi(\tau(xy)z) = 1$ при всех $y \in R_A$ и всех $z \in R$, что по предложению 12 гл. II-5 эквивалентно условию $\tau(xy) \in R$ при всех $y \in R_A$.

Следствие 2. *Пусть* A *— простая алгебра над* K, τ *— приведенный след на* A, χ *— характер порядка* 0 *на* K. *Отождествим* A *с топологическим двойственным к нему, полагая* $\langle x, y\rangle = \chi(\tau(xy))$. *Пусть* M *и* M' *— две* K*-решетки в* A, *двойственные друг другу в* A, *причем как* M, *так и* M' *являются подкольцами в* A. *Тогда алгебра* A *тривиальна над* K, M *— максимальное компактное подкольцо в* A *и* $M = M'$.

По теореме 1 § 1 M содержится в некотором максимальном компактном подкольце $R_A \subset A$. Используя тот факт, что алгебра A изоморфна некоторой алгебре вида $M_m(D)$, мы можем отождествить A с $M_m(D)$ и R_A с $M_m(R_D)$ (обозначения такие же, как в предложении 5). Поскольку $M \subset R_A$, следствие 1 показывает, что $M' \supset \omega R_A \supset R_A$, откуда по теореме 1 § 1 $M' = \omega R_A = R_A$. Отсюда, очевидно, следует, что $d = 1$, т. е. что алгебра A тривиальна, а тогда в силу того же следствия 1 $M = R_A$.

Предложение 6. *Пусть K — некоторое p-поле, A — простая алгебра над K и ν — приведенная норма на A. Тогда* $\nu(A^\times) = K^\times$.

Ввиду следствия 3 предл. 6 гл. IX-2 достаточно рассмотреть случай $A = D$. В этом случае мы можем так же, как и выше, записать D как циклическую алгебру и использовать для v_D формулу (9) гл. IX-4. Применяя обозначения из доказательства предложения 5, мы видим, что, во-первых, $v_D(D^\times)$ содержит группу $N_{K_1/K}(R_1^\times)$, которая по предложению 3 гл. VIII-1 совпадает с $R^\times$, и, во-вторых, $v_D(D^\times)$ содержит $v_D(u_1) = \pi$. Поскольку $R^\times$ и π порождают $K^\times$, наше предложение доказано.

В случае $\mathbf{R}$-полей заключение предложения 6, конечно, справедливо для $A = M_m(K)$, где $K = \mathbf{R}$ или $\mathbf{C}$, но не для $K = \mathbf{R}$ и $A = M_n(\mathbf{H})$. В самом деле, как мы видели в гл. IX-4, алгебра $\mathbf{H}$ «классических» кватернионов имеет базис над $\mathbf{R}$, состоящий из «кватернионных единиц» $1, i, j, k$, удовлетворяющих соотношениям $i^2 = -1$, $j^2 = -1$, $k = ij = -ji$, из которых следуют соотношения $k^2 = -1$, $i = jk = -kj$, $j = ki = -ik$. Очевидно, что $\mathbf{R}$-линейная биекция $x \to \bar{x}$ алгебры $\mathbf{H}$ на себя, переводящая $1, i, j, k$ соответственно в $1, -i, -j, -k$, является антиизоморфизмом, т. е. переводит xy в $\bar{y}\bar{x}$ при всех x, y. Для определения приведенного следа τ и приведенной нормы ν на $\mathbf{H}$ нужно какое-нибудь $\mathbf{C}$-представление F алгебры $\mathbf{H}$. Используя результаты гл. IX или с помощью непосредственных вычислений, находим, что такое представление задается следующим образом:

$$F(1) = 1_2, \quad F(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad F(j) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad F(k) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Тогда для $x = t + ui + vj + wk$, где $t, u, v, w \in \mathbf{R}$, имеем

$$\tau(x) = x + \bar{x} = 2t, \quad \nu(x) = x\bar{x} = \bar{x}x = t^2 + u^2 + v^2 + w^2.$$

Отсюда видно, что ν отображает $\mathbf{H}^\times$ на $\mathbf{R}_+^\times$. Поэтому, согласно следствию 3 предл. 6 гл. IX-2, то же верно для $A = M_m(\mathbf{H})$ при любом $m \geqslant 1$.

§ 3. ВЫЧИСЛЕНИЕ НЕКОТОРЫХ ИНТЕГРАЛОВ

В порядке подготовки к вычислению дзета-функции простой алгебры в гл. XI мы произведем здесь некоторые локальные вычисления, дающие обобщения предложения 11 гл. VII-4 и леммы 8 гл. VII-6.

Возьмем сначала некоторое p-поле K и некоторую алгебру с делением D над K. Обозначим через R_D максимальное компактное подкольцо в D, через P_D — максимальный идеал в R_D и через π_D — простой элемент в D. Для всякого $e \geqslant 0$ выберем полное множество $A(e)$ представителей классов в R_D по модулю P_D^e. Далее, для заданного $m \geqslant 1$ следующим образом определим подмножества $\mathfrak{T}$, $\mathfrak{T}'$ и $\mathfrak{T}''$ в $M_m(D)^\times$. Под $\mathfrak{T}$ будем понимать группу *треугольных* матриц из $M_m(D)^\times$, состоящую из тех матриц $t = (t_{ij})$, для которых $t_{ij} = 0$ при $1 \leqslant j < i \leqslant m$ и $t_{ii} \neq 0$ при $1 \leqslant i \leqslant m$. Под $\mathfrak{T}'$ будем понимать подмножество в $\mathfrak{T}$, состоящее из таких матриц $t = (t_{ij}) \in \mathfrak{T}$, что $t_{ij} \in R_D$ при всех i, j и каждое t_{ii}, $1 \leqslant i \leqslant m$, имеет вид $\pi_D^{e_i}$, где $e_i \geqslant 0$. Под $\mathfrak{T}''$ будем понимать подмножество в $\mathfrak{T}'$, состоящее из таких матриц $t = (t_{ij}) \in \mathfrak{T}'$, что $t_{ij} \in A(e_j)$ при $1 \leqslant i < j \leqslant m$, где e_j задается условием $t_{jj} = \pi_D^{e_j}$. В этих обозначениях имеет место

Лемма 2. *Пусть V — левое векторное пространство размерности m над D; L — некоторая D-решетка в V; $\{v_1, \ldots, v_m\}$ — такой базис в V, что $L = \sum R_D v_i$; L' — некоторая D-решетка в V, содержащаяся в L. Тогда существует один и только один базис $\{v_1', \ldots, v_m'\}$ в V, для которого $L' = \sum R_D v_i'$ и $v_i' = \sum_j t_{ij} v_j$ при $1 \leqslant i \leqslant m$, где матрица $t = (t_{ij})$ принадлежит множеству $\mathfrak{T}''$.*

Для $1 \leqslant i \leqslant m$ обозначим через W_i подпространство в V, порожденное элементами $v_1, \ldots, v_i$. Пусть $\{w_1, \ldots, w_m\}$ — какой-нибудь базис в V. Запишем его в виде $w_i = \sum x_{ij} v_j$. Ясно, что матрица $x = (x_{ij})$ в том и только в том случае лежит в $\mathfrak{T}$, т. е. треугольна, когда $\{w_1, \ldots, w_i\}$ является базисом в W_i для всякого i. По теореме 1 гл. II-2 можно выбрать такой базис, для которого $L' = \sum R_D w_i$. Поскольку $L' \subset L$, все x_{ij} лежат в R_D. Запишем $x_{ii} = y_i \pi_D^{e_i}$, где $y_i \in R_D^\times$ и $e_i \in \mathbf{Z}$ при $1 \leqslant i \leqslant m$, и заменим векторы w_i на векторы $y_i^{-1} w_i$, которые, очевидно, обладают теми же свойствами. После замены имеем $(x_{ij}) \in \mathfrak{T}'$. Предположим теперь, что существуют такие векторы $v_1', \ldots, v_m'$, как требуется в лемме. Запишем $v_i' = \sum z_{ij} w_j$. Ясно, что матрица (z_{ij}) должна быть тогда треугольной, а поскольку $L' = \sum R_D v_i' = \sum R_D w_i$, она должна лежать в $M_m(R_D)^\times$. Для треугольной матрицы (z_{ij}) последнее условие выполняется в том и только в том случае, когда $z_{ii} \in R_D^\times$ и $z_{ij} \in R_D$ при всех i, j. Поэтому коэффициент при v_i в v_i' равен $z_{ii} \pi_D^{e_i}$, а так как он должен иметь вид π_D^e, z_{ii} должно равняться 1.

Далее, коэффициент t_{ij} при v_j в v_i', $1 \leqslant i < j \leqslant m$, задается равенством

$$t_{ij} = x_{ij} - \sum_{h=i+1}^{j-1} z_{ih} x_{hj} + z_{ij} \pi_D^{e_j},$$

и доказательство леммы будет закончено, если мы покажем, что z_{ij} при $1 \leqslant i < j \leqslant m$ можно единственным образом выбрать в R_D так, чтобы $t_{ij} \in A(e_j)$ при $1 \leqslant i < j \leqslant m$. Но для каждого i это легко проверяется с помощью индукции по j, $i+1 \leqslant j \leqslant m$.

Лемма 3. *Множество $\mathfrak{T}''$ является полным множеством представителей для тех классов смежности в $M_m(D)^\times$ по $M_m(R_D)^\times$, которые содержатся в $M_m(R_D)$.*

Возьмем левое векторное пространство V размерности m над D, D-решетку L в V и базис $\{v_1, \ldots, v_m\}$ в V, для которого $L = \sum R_D v_i$. Как и прежде, отождествим $\mathrm{End}(V)$ с $M_m(D)$, сопоставив всякому $\xi \in \mathrm{End}(V)$ матрицу (x_{ij}), задаваемую условиями $v_i \xi = \sum x_{ij} v_j$. Положим $A = \mathrm{End}(V)$ и $R_A = \mathrm{End}(V, L)$. Тогда $R_A = M_m(R_D)$ и $R_A^\times$, т. е. $M_m(R_D)^\times$ состоит из таких автоморфизмов ξ пространства V, что $L\xi = L$. Поэтому два элемента α, β из $A^\times$ лежат в одном левом классе смежности по модулю $R_A^\times$ тогда и только тогда, когда $L\alpha = L\beta$. Этот левый класс смежности содержится в R_A тогда и только тогда, когда $L\alpha \subset L$. В то же время по лемме 2 каждая D-решетка L' в V, содержащаяся в L, может быть одним и только одним способом записана в виде $\sum R_D v_i'$, где $v_i' = \sum t_{ij} v_j$ и $(t_{ij}) \in \mathfrak{T}''$. Другими словами, она может быть одним и только одним способом записана как $L\tau$ с $\tau \in \mathfrak{T}''$, чем наша лемма и доказана.

Предложение 7. *Пусть K — некоторое p-поле; q — его модуль; D — алгебра с делением размерности d^2 над K; A — простая алгебра над K, изоморфная $M_m(D)$; R_A — максимальный порядок в A; φ — его характеристическая функция; ν — приведенная норма на A; μ — мера Хаара на $A^\times$, для которой $\mu(R_A^\times) = 1$. Тогда интеграл*

$$I(s) = \int_{A^\times} \varphi(x) \bmod_K (\nu(x))^s \, d\mu(x),$$

где $s \in \mathbf{C}$, при $\mathrm{Re}(s) > d(m-1)$ абсолютно сходится и имеет значение

$$I(s) = \prod_{i=0}^{m-1} (1 - q^{di-s})^{-1}.$$

Как и прежде, отождествим A с $\mathrm{End}(V)$ и R_A с $\mathrm{End}(V, L)$, где V — левое векторное пространство размерности m над D, а L — D-решетка в V. По предложению 1 § 1 подинтегральная функция в $I(s)$ постоянна на каждом левом классе смежности в $A^\times$ по $R_A^\times$. Ввиду определения меры μ отсюда следует, что

$$I(s) = \sum_{\tau} \mathrm{mod}_K (\nu(\tau))^s,$$

где сумма берется по любому полному множеству представителей классов смежности в $A^\times$ по $R_A^\times$, содержащихся в R_A, например по множеству $\mathfrak{T}''$ из леммы 3. Если отождествить, как и прежде, A с $M_m(D)$ и R_A с $M_m(R_D)$, то $\mathfrak{T}''$ состоит из таких треугольных матриц $t = (t_{ij})$, что $t_{ii} = \pi_D^{e_i}$ и $t_{ij} \in A(e_j)$ при всех i, j, где e_i — целые неотрицательные числа. По следствию 2 предл. 6 гл. IX-2 имеем $\nu(t) = \prod \nu_D(t_{ii}) = \nu_D(\pi_D)^E$, где $E = \sum e_i$ и ν_D — приведенная норма на D. Как мы видели в § 2, $\nu_D(\pi_D)$ является простым элементом в K при подходящем выборе π_D. Значит, то же самое верно при любом выборе π_D. Это дает равенство $\mathrm{mod}_K(\nu(t)) = q^{-E}$. С другой стороны, предложение 5 гл. I-4 показывает, что модуль p-поля D равен q^d, так что для всякого $e \geqslant 0$ множество $A(e)$ состоит из q^{de} элементов. Поэтому для заданного множества $e_1, \ldots, e_m$ целых чисел существует в точности q^{dN} матриц $t \in \mathfrak{T}''$, где $N = \sum_i (i-1) e_i$. Таким образом, получаем

$$I(s) = \prod_{i=1}^{m} \Big(\sum_{e=0}^{+\infty} (q^{d(i-1)-s})^e \Big).$$

Ясно, что это выражение абсолютно сходится при $\mathrm{Re}(s) > d(m-1)$ и при этом условии имеет указанное в нашем предложении значение.

Следствие. *Пусть функция $I(s)$ такова, как в предложении 7, и пусть функция $I_0(s)$ определена аналогичным образом для алгебры $A_0 = M_n(K)$, где $n = dm$. Тогда при $\mathrm{Re}(s) > n-1$ имеем*

$$I(s)\, I_0(s)^{-1} = \prod_{\substack{0<h<n \\ h \not\equiv 0 \ (d)}} (1 - q^{h-s}).$$

Это сразу следует из предложения 7.

Нам понадобятся также соответствующие результаты для $\mathbf{R}$-полей. В этом случае либо $K = \mathbf{R}$ и $D = \mathbf{R}$ или $\mathbf{H}$, либо $K = D = \mathbf{C}$. В обоих случаях отображение $x \to \bar{x}$ является антиизомор-

физмом алгебры D, для которого $x\bar{x} > 0$ при всех $x \in D^\times$. Это отображение тождественно для $D = \mathbf{R}$, является нетривиальным автоморфизмом поля $\mathbf{C}$ над $\mathbf{R}$ для $D = \mathbf{C}$ и определено в конце § 2 для $D = \mathbf{H}$. Как обычно, если $x = (x_{ij})$ — любая матрица из $M_m(D)$, то мы обозначаем через ${}^t x$ транспонированную к ней матрицу и через $\bar{x}$ матрицу $(\bar{x}_{ij})$. Тогда отображение $x \to {}^t\bar{x}$ есть антиизоморфизм алгебры $M_m(D)$. Мы будем обозначать через $\mathfrak{T}$ множество треугольных матриц $(t_{ij}) \in M_m(D)$, для которых $t_{ii} \in \mathbf{R}_+^\times$ при $1 \leqslant i \leqslant m$; ясно, что это — подгруппа в $M_m(D)$. Пусть теперь V — левое векторное пространство размерности m над D. Хоть это и не вполне согласуется с установившейся терминологией, будем для краткости говорить, что отображение f из $V \times V$ в D является *эрмитовой формой* на V, если в V существует такой базис $\{v_1, \ldots, v_m\}$, что

$$f\left(\sum x_i v_i, \quad \sum y_i v_i\right) = \sum x_i \bar{y}_i$$

при всех x_i, y_i из D. Каждый базис в V с таким свойством будем называть *ортогональным относительно* f. Сразу видно, что базис $\{w_1, \ldots, w_m\}$ ортогонален относительно f тогда и только тогда, когда $f(w_i, w_j) = \delta_{ij}$ при всех i, j или даже когда это так при $1 \leqslant i \leqslant j \leqslant m$. Наделим пространство всех эрмитовых форм на V *топологией равномерной сходимости на компактных подмножествах* в $V \times V$. Другими словами, для всякого компактного подмножества C в $V \times V$ и всякого $\varepsilon > 0$ множество таких эрмитовых форм f', что $\mathrm{mod}_D(f' - f) \leqslant \varepsilon$ на C, является окрестностью формы f, и такие окрестности образуют фундаментальную систему окрестностей формы f в пространстве всех эрмитовых форм.

Лемма 4. *Для $D = \mathbf{R}$, $\mathbf{H}$ или $\mathbf{C}$ пусть V — левое векторное пространство над D с базисом $\{v_1, \ldots, v_m\}$ и f — эрмитова форма на V. Тогда существует один и только один ортогональный базис $\{v_1', \ldots, v_m'\}$ относительно f, для которого $v_i' = \sum t_{ij} v_j$, где $t_{ij} \in \mathfrak{T}$, и этот базис непрерывно зависит от f.*

Этот факт доказывается непосредственно, и доказательство его так хорошо известно, что может быть здесь опущено.

Пусть V такое, как выше, и f — эрмитова форма на V с ортогональным базисом $\{v_1, \ldots, v_m\}$. Пусть, далее, $\{w_1, \ldots, w_m\}$ — базис в V, для которого $w_i = \sum u_{ij} v_j$, где $u = (u_{ij}) \in M_m(D)$. Тривиальное вычисление показывает, что этот базис ортогонален относительно f тогда и только тогда, когда $u \cdot {}^t\bar{u} = 1_m$. Ясно, что матрицы u, обладающие этим свойством, образуют компактную

подгруппу в $M_m(D)^\times$; мы будем обозначать ее через $\mathfrak{U}$. Пусть теперь α — любой автоморфизм пространства V. Будем обозначать через f^α сопряжение f с помощью α, т. е. отображение, для которого $f^\alpha(v, w) = f(v\alpha^{-1}, w\alpha^{-1})$ при всех v, w из V. Это — эрмитова форма с ортогональным базисом $\{v_1\alpha, \ldots, v_m\alpha\}$. Ясно, что если, как и прежде, отождествить $A = \mathrm{End}(V)$ с $M_m(D)$ при помощи базиса $\{v_1, \ldots, v_m\}$, то $\mathfrak{U}$ будет подгруппой в $A^\times = M_m(D)$, состоящей из таких автоморфизмов ξ пространства V, что $f^\xi = f$.

Лемма 5. *Для определенных выше подгрупп $\mathfrak{T}$ и $\mathfrak{U}$ в $A^\times = M_m(D)^\times$ отображение $(u, t) \to ut$ является гомеоморфизмом из $\mathfrak{U} \times \mathfrak{T}$ на $A^\times$.*

Пусть V, f и ортогональный базис $\{v_1, \ldots, v_m\}$ такие, как выше. Снова отождествим с помощью этого базиса $A = \mathrm{End}(V)$ с $M_m(D)$, а значит, $A^\times$ с $M_m(D)^\times$. Пусть $\alpha, \beta \in A^\times$. Тогда $f^\alpha = f^\beta$ в том и только в том случае, когда $f = f^{\beta\alpha^{-1}}$, т. е. когда $\beta\alpha^{-1} \in \mathfrak{U}$, или $\beta \in \mathfrak{U}\alpha$. Теперь для произвольного $\alpha \in A^\times$ применение к f^α леммы 4 показывает, что существует одна и только одна такая матрица $(t_{ij}) \in \mathfrak{U}$, что векторы $v_i' = \sum t_{ij}v_j$ образуют ортогональный относительно f^α базис. Другими словами, автоморфизм τ пространства V, который соответствует этой матрице, т. е. который отображает $\{v_1, \ldots, v_m\}$ на $\{v_1', \ldots, v_m'\}$, переводит f в $f^\tau = f^\alpha$. Далее, по лемме 4 матрица (t_{ij}) непрерывно зависит от f^α и, следовательно, от α. Выражая все это в терминах матриц x, u, t из $M_m(D)^\times$, соответствующих автоморфизмам α, $\alpha\tau^{-1}$, τ соответственно, получаем утверждение нашей леммы.

Лемма 6. *В обозначениях леммы 5 пусть μ — мера Хаара на $A^\times$. Для каждой непрерывной функции F на $\mathfrak{T}$ с компактным носителем обозначим через F' функцию на $A^\times$, для которой $F'(ut) = F(t)$ при всех $u \in \mathfrak{U}$ и всех $t \in \mathfrak{T}$. Тогда F' является непрерывной функцией на $A^\times$ с компактным носителем и существует такая правоинвариантная мера θ на $\mathfrak{T}$, что $\int F'\,d\mu = \int F\,d\theta$ при всех F.*

Первое утверждение немедленно следует из леммы 5 и компактности группы $\mathfrak{U}$. Так как мера μ правоинвариантна на $A^\times$ по лемме 1 § 1, то, очевидно, отображение $F \to \int F\,d\mu$ инвариантно относительно правых трансляций на $\mathfrak{T}$. Из теории меры Хаара следует поэтому, что θ является образом некоторой меры Хаара, т. е. некоторой левоинвариантной меры на $\mathfrak{T}$, относительно гомеоморфизма $t \to t^{-1}$ группы $\mathfrak{T}$ в себя.

Лемма 7. *Пусть* α *— мера Хаара на* D. *Положим* $\delta = [K : \mathbf{R}]$ *и для* $t = (t_{ij}) \in \mathfrak{T}$ *положим*

$$d\theta(t) = \prod_{i=1}^{m} (t_{ii}^{-\delta d^2(i-1)-1}\, dt_{ii}) \cdot \prod_{1 \leqslant i < j \leqslant m} d\alpha(t_{ij}).$$

Это равенство определяет правоинвариантную меру на $\mathfrak{T}$.

Так как размерность алгебры D над $\mathbf{R}$ равна δd^2, то следствие 2 теор. 3 гл. I-2 показывает, что для каждого $a \in \mathbf{R}_+^\times$ модуль автоморфизма $x \to xa$ пространства D равен $a^{\delta d^2}$. Прямым вычислением сразу получаем, что, во-первых, мера θ из леммы 7 инвариантна относительно отображения $t \to tt'$ для любой диагональной матрицы $t' \in \mathfrak{T}$ и что, во-вторых, эта мера инвариантна относительно отображения $t \to tt''$ для любой матрицы $t'' = (t''_{ij}) \in \mathfrak{T}$, для которой $t''_{ii} = 1$ при $1 \leqslant i \leqslant m$. Поскольку каждая матрица из $\mathfrak{T}$ может быть записана в виде $t't''$, наша лемма доказана.

Предложение 8. *Пусть либо* $K = \mathbf{R}$ *и* $D = \mathbf{R}$ *или* $\mathbf{H}$, *либо* $K = D = \mathbf{C}$. *Обозначим через* δ *размерность поля* K *над* $\mathbf{R}$ *и через* d^2 *— размерность алгебры* D *над* K. *Обозначим, далее, через* τ *приведенный след и через* ν *— приведенную норму на алгебре* $A = M_m(D)$ *над* K. *Пусть, наконец,* μ *— мера Хаара на* $A^\times$. *Тогда интеграл*

$$I(s) = \int_{A^\times} \exp(-\pi\delta\tau({}^t\bar{x} \cdot x)) \bmod_K (\nu(x))^s\, d\mu(x)$$

абсолютно сходится при $\operatorname{Re}(s) > d(m-1)$ *и при подходящем выборе меры* μ *имеет в этой области значение*

$$I(s) = (\pi\delta d)^{-m\delta\, ds/2} \prod_{i=0}^{m-1} \Gamma(\delta d(s - di)/2).$$

Ясно, что первый сомножитель подинтегральной функции в интеграле $I(s)$ постоянен на каждом классе смежности в $A^\times$ по $\mathfrak{U}$. Положим $z = \nu(u)$ для любого элемента $u \in \mathfrak{U}$. Если $D = K$, то это означает, что $z = \det(u)$, так что из $u \in \mathfrak{U}$ следует, что $z\bar{z} = 1$, откуда $\bmod_K(z) = 1$. Если $K = \mathbf{R}$ и $D = \mathbf{H}$, то при всех $x \in A$ имеем $\nu(x) = \det(F(x))$, где F — некоторый изоморфизм из A в $M_{2m}(\mathbf{C})$. Но тогда $x \to {}^tF({}^t\bar{x})$ тоже является таким изоморфизмом, так что $\nu({}^t\bar{x}) = \nu(x)$. Отсюда следует, что $\nu(u)^2 = 1$ при $u \in \mathfrak{U}$, а значит, $\nu(u) = 1$, ибо, как мы убедились в § 2, ν отображает $M_m(\mathbf{H})^\times$ в $\mathbf{R}_+^\times$. Итак, во всех случаях второй сомножитель

в подинтегральной функции в интеграле $I(s)$ также постоянен на каждом левом классе смежности в $A^\times$ по $\mathfrak{U}$. Поэтому леммы 6 и 7 показывают, что при подходящем выборе меры μ интеграл $I(s)$ совпадает с интегралом от той же самой подинтегральной функции, но взятым по пространству $\mathfrak{T}$ с мерой $d\theta(t)$. Приведенный след τ_D на D задается равенством $\tau_D(x) = x$ при $D = K$ и равенством $\tau_D(x) = x + \bar{x}$ при $K = \mathbf{R}$ и $D = \mathbf{H}$. Ввиду следствия 2 предл. 6 гл. IX-2 при $t = (t_{ij}) \in \mathfrak{T}$ мы имеем

$$\tau({}^t\bar{t} \cdot t) = d \cdot \sum_{1 \leqslant i \leqslant j \leqslant m} \bar{t}_{ij} t_{ij}, \qquad \nu(t) = \prod_{1 \leqslant i \leqslant m} (t_{ii})^d.$$

Это дает

$$I(s) = \prod_{i=1}^{m} \left(\int_0^{+\infty} \exp(-\pi\delta\, dt^2)\, t^{s_i - 1}\, dt \right) \cdot \left(\int_D \exp(-\pi\delta\, d\bar{t}t)\, d\alpha(t) \right)^{\frac{m(m-1)}{2}},$$

где $s_i = \delta d(s - di + d)$, $1 \leqslant i \leqslant m$. Последний сомножитель не зависит от s и положителен. Остальные сомножители с помощью очевидной замены переменной можно преобразовать в обычные интегралы для гамма-функции. Мы получили искомый результат с точностью до постоянного строго положительного множителя, который можно сделать равным 1, произведя соответствующую замену меры Хаара μ.

Следствие. *В условиях предложения* 8 *предположим, что* $K = \mathbf{R}$ *и* $D = \mathbf{H}$. *Пусть* $I(s)$ — *определенный там интеграл и* $I_0(s)$ — *аналогично определенный интеграл для алгебры* $A_0 = M_n(\mathbf{R})$, *где* $n = 2m$. *Тогда при* $\operatorname{Re}(s) > n - 1$ *имеем*

$$I(s)\, I_0(s)^{-1} = \gamma \prod_{\substack{0 < h < n \\ h \not\equiv 0 \,(2)}} (s - h),$$

где γ — *некоторая строго положительная константа.*

Это — непосредственное следствие предложения 8 и тождеств

$$\Gamma(s+1) = s\Gamma(s),$$

$$\Gamma(s) = \pi^{-1/2}\, 2^{s-1}\, \Gamma\left(\frac{s}{2}\right) \Gamma\left(\frac{s+1}{2}\right)$$

из теории гамма-функции.

ГЛАВА ОДИННАДЦАТАЯ

ПРОСТЫЕ АЛГЕБРЫ НАД А-ПОЛЯМИ

§ 1. ВЕТВЛЕНИЕ

В этой главе k будет обозначать некоторое А-поле. Мы будем использовать все обозначения, введенные для таких полей в предыдущих главах, такие, как $k_{\mathbf{A}}$, k_v, r_v и т. п. Нас будут интересовать главным образом простые алгебры A над k. Как мы условились в гл. IX, всегда предполагается, что алгебра A центральна, т. е. что ее центр совпадает с k, и что она имеет конечную размерность над k; по следствию 3 предл. 3 гл. IX-1 эта размерность равна n^2, где n — целое число $\geqslant 1$. Как объяснялось в главах III и IV, мы используем символ A_v для обозначения алгебры $A \otimes k_v$ над k_v, где в соответствии с соглашениями гл. IX подразумевается, что тензорное произведение берется над k. По следствию 1 предл. 3 гл. IX-1 это — простая алгебра над k_v. Поэтому в силу теоремы 1 гл. IX-1 она изоморфна некоторой алгебре $M_{m(v)}(D(v))$, где $D(v)$ — алгебра с делением над k_v. Размерность алгебры $D(v)$ над k_v может быть записана как $d(v)^2$, и мы имеем $m(v)\,d(v) = n$. Алгебра $D(v)$ определена однозначно с точностью до изоморфизма, и числа $m(v)$, $d(v)$ определены однозначно. Говорят, что алгебра A *неразветвлена* или *разветвлена* в точке v в соответствии с тем, тривиальна алгебра A_v над k_v или нет, т. е. $d(v) = 1$ или $d(v) > 1$.

Теорема 1. *Пусть A — простая алгебра над* А*-полем k, и пусть α — конечное подмножество в A, содержащее базис в A над k. Для всякой конечной точки v поля k через α_v обозначим r_v-модуль в A_v, порожденный множеством α. Тогда почти для всех v алгебра A_v тривиальна над k_v и α_v является максимальным компактным подкольцом в A_v.*

Ввиду следствия 1 теор. 3 гл. III-1 мы можем предположить, что α является базисом в A над k и что 1_A содержится в α. Обозначим через τ приведенный след на A. По предложению 6 гл. IX-2 этот след отличен от нуля и его k_v-линейное продолжение на A_v

является приведенным следом на A_v. По лемме 3 гл. III-3 мы можем отождествить векторное пространство A над k с алгебраическим двойственным к нему, полагая $[x, y] = \tau(xy)$. Теперь возьмем, как в теореме 3 гл. IV-2, какой-нибудь базисный характер χ на $k_{\mathbf{A}}$. По следствию 1 из этой теоремы χ_v имеет порядок 0 почти для всех v; по следствию 3 из той же теоремы k_v-решетка α_v двойственна с собой почти для всех v, если отождествить пространство A_v с топологическим двойственным к нему, полагая $\langle x, y\rangle = \chi_v(\tau(xy))$. По следствию 2 теор. 3 гл. III-1 α_v является компактным подкольцом в A_v почти для всех v. Поэтому почти для всех точек v поля k выполняются предположения следствия 2 предл. 5 гл. X-2, откуда и следует утверждение нашей теоремы.

Первая часть теоремы 1 утверждает, что алгебра A неразветвлена почти во всех точках поля k. Цель § 2 — показать, что эта алгебра может быть неразветвлена во всех точках поля k, только если она тривиальна.

§ 2. ДЗЕТА-ФУНКЦИЯ ПРОСТОЙ АЛГЕБРЫ

Пусть все обозначения таковы, как в § 1, и пусть α — базис в A над k. По теореме 1 § 1 α_v является максимальным компактным подкольцом в A_v почти для всех v. Поэтому мы можем для каждой конечной точки v поля k выбрать максимальное компактное подкольцо R_v в A_v таким образом, чтобы $R_v = \alpha_v$ почти для всех v. Сделав это, обозначим через Φ_v характеристическую функцию кольца R_v. Для всякой бесконечной точки v поля k выберем какой-нибудь изоморфизм алгебры A_v с алгеброй $M_{m(v)}(D(v))$, где $D(v)$ есть $\mathbf{R}$, $\mathbf{H}$ или $\mathbf{C}$, и отождествим A_v с этой алгеброй при помощи этого изоморфизма. Определим функцию Φ_v на A_v, полагая $\Phi_v(x) = \exp(-\pi\delta\tau({}^t\overline{x}\cdot x))$ при всех $x \in A_v$, где обозначения те же, что и в предложении 8 гл. X-3. Тогда $\Phi = \prod \Phi_v$ — стандартная функция на $A_{\mathbf{A}}$. Пусть μ — какая-нибудь мера Хаара на $A_{\mathbf{A}}^{\times}$. Имеет место следующее

Предложение 1. *Интеграл*

$$Z_{\mathbf{A}}(s) = \int_{A_{\mathbf{A}}^{\times}} \Phi(z)\,|\nu(z)|_{\mathbf{A}}^{s}\, d\mu(z)$$

при $\operatorname{Re}(s) > n$ *абсолютно сходится, и его значение дается формулой*

$$Z_{\mathbf{A}}(s) = C \prod_{i=0}^{n-1} Z_k(s-i) \cdot \prod_v \Big(\prod_{\substack{0<h<n \\ h\neq 0 \ d(v))}} (1 - q_v^{h-s}) \Big) \Big(\prod_{\substack{0<h<n \\ h\neq 0 \ (2)}} (s-h) \Big)^{\rho},$$

где Z_k — это либо функция, определенная в теореме 3 *гл.* VII-6, *либо дзета-функция поля k в соответствии с тем, равна характеристика поля k нулю либо нет*; ρ — *число вещественных точек v поля k, для которых $D(v) = \mathbf{H}$, а C — некоторая строго положительная константа.*

Для всякой точки v выберем меру Хаара μ_v на $A_v^\times$ так, чтобы $\mu_v(R_v^\times) = 1$ для всех конечных точек. Можно считать, что в качестве μ взята мера $\mu = \prod \mu_v$, в смысле, объясненном в гл. VII-4 для случая $A = k$. Следуя шаг за шагом доказательству предложения 10 гл. VII-4, находим, что интеграл $Z_A(s)$ абсолютно сходится и равен бесконечному произведению

$$\prod_v \left(\int_{A_v^\times} \Phi_v(x) \, |\nu(x)|_v^s \, d\mu_v(x) \right),$$

при условии, что все сомножители в этом произведении и само произведение абсолютно сходятся. Эти сомножители были вычислены в предложениях 7 и 8 гл. X-3. Из этих предложений, в сочетании с предложением 1 гл. VII-1, немедленно вытекает абсолютная сходимость интеграла $Z_A(s)$ при $\mathrm{Re}(s) > n$. Из тех же предложений, с учетом определений гл. VII-6, вытекает последняя формула нашего предложения в случае $A = M_n(k)$. Отсюда с помощью следствий предл. 7 и 8 гл. X-3 сразу получаем эту формулу в общем случае.

Следует заметить, что среднее произведение в формуле для $Z_A(s)$ в предложении 1 является фактически конечным произведением, ибо по теореме 1 § 1 $d(v) = 1$ почти для всех точек поля k. Стоит также отметить, что вычисление константы C в этой формуле для некоторой явно заданной меры Хаара μ на $A_A^\times$ не представляет трудностей и что это бывает иногда важно, например при нахождении *числа Тамагавы* подгруппы $A^{(1)}$ в $A^\times$, определяемой условием $\nu(x) = 1$. Поскольку этот вопрос лежит в стороне от основной тематики настоящей книги, мы не будем к нему больше возвращаться.

Предложение 2. *Пусть D — алгебра с делением размерности d^2 над k, и пусть функция $Z_D(s)$ определена, как в предложении* 1. *Тогда если характеристика поля k равна нулю, то $Z_D(s)$ не имеет других полюсов, кроме полюсов в точках $s = 0$ и $s = d$, а если k — поле характеристики $p > 1$ и $\mathbf{F}_q$ — его поле констант, то $Z_D(s)$ не имеет других полюсов, кроме нулей функции $(1 - q^{-s}) \times (1 - q^{d-s})$.*

Докажем это, следуя шаг за шагом доказательству теоремы 2 гл. VII-5. По аналогии с тем доказательством удобно принять следующие обозначения. Для $z \in D_{\mathbf{A}}^{\times}$ и $s \in \mathbf{C}$ положим $\omega_s(z) = |\nu(z)|_{\mathbf{A}}^{s}$. Тогда ω_1 есть морфизм из $D_{\mathbf{A}}^{\times}$ в $\mathbf{R}_{+}^{\times}$. При $\xi \in D^{\times}$ имеем $\nu(\xi) \in k^{\times}$. Поэтому в силу теоремы 5 гл. IV-4 морфизм ω_1 тривиален на $D^{\times}$. Рассмотрим сначала случай, когда k имеет характеристику $p > 1$. По предложению 6 гл. X-2 ν отображает $D_v^{\times}$ на $k_v^{\times}$ при всех v, так что ω_1 отображает $D_v^{\times}$ на подгруппу в $\mathbf{R}_{+}^{\times}$, порожденную элементом q_v. По следствию 6 теор. 2 гл. VII-5 отсюда следует, что ω_1 отображает $D_{\mathbf{A}}^{\times}$ на подгруппу в $\mathbf{R}_{+}^{\times}$, порожденную элементом q, если полем констант в k служит $\mathbf{F}_q$. В этом случае возьмем элемент $z_1 \in D_{\mathbf{A}}^{\times}$, для которого $\omega_1(z_1) = q$, и обозначим через M подгруппу в $D_{\mathbf{A}}^{\times}$, порожденную элементом z_1. Тогда $D_{\mathbf{A}}^{\times}$ разлагается в произведение подгруппы M и ядра $D_{\mathbf{A}}^{1}$ морфизма ω_1.

Если k — поле характеристики нуль, обозначим через M подгруппу в $k_{\mathbf{A}}^{\times}$, определенную в следствии 2 теор. 5 гл. IV-4. Отождествляя k с центром алгебры D, можно рассматривать $k_{\mathbf{A}}^{\times}$ как подгруппу в $D_{\mathbf{A}}^{\times}$. Поскольку $\nu(z) = z^l$ при $z \in k$, только что упомянутое следствие показывает, что ω_1 отображает M на $\mathbf{R}_{+}^{\times}$, так что $D_{\mathbf{A}}^{\times}$ опять разлагается в произведение своей подгруппы M и ядра $D_{\mathbf{A}}^{1}$ морфизма ω_1. В обоих случаях из теоремы 4 гл. IV-3 вытекает компактность множества $D_{\mathbf{A}}^{1}/D^{\times}$.

Как и в доказательстве теоремы 1 § 1, возьмем какой-нибудь базисный характер χ на $k_{\mathbf{A}}$. Отождествим пространство $D_{\mathbf{A}}$ с топологическим двойственным к нему, полагая $\langle x, y\rangle = \chi(\tau(xy))$, и для каждой точки v отождествим пространство D_v с топологическим двойственным к нему, полагая $\langle x, y\rangle = \chi_v(\tau(xy))$. Далее, для всякой точки v обозначим через α_v самодвойственную меру Хаара на D_v. Тогда по следствию 1 теор. 1 гл. VII-2 меры α_v когерентны и $\alpha = \prod \alpha_v$ является мерой Тамагавы на $D_{\mathbf{A}}$.

Пусть снова $\Phi = \prod \Phi_v$ — стандартная функция на $D_{\mathbf{A}}$, которая использовалась выше при построении $Z_D(s)$, и пусть $\Psi = \prod \Psi_v$ — любая стандартная функция на $D_{\mathbf{A}}$. Обозначим через $Z(\Psi, s)$ интеграл, полученный заменой Φ на Ψ в определении $Z_D(s)$. В этих обозначениях можно написать

$$Z(\Psi, s) = \int_{D_{\mathbf{A}}^{\times}} \Psi(z)\, \omega_s(z)\, d\mu(z).$$

Мы собираемся показать, что этот интеграл абсолютно сходится при $\mathrm{Re}(s) > d$ и что он может быть продолжен до мероморфной

функции на всей s-плоскости, не имеющей других полюсов, кроме упомянутых в предложении 2; это утверждение содержит наше предложение как частный случай. Что касается сходимости, то почти для всех v мы имеем $\Psi_v = \Phi_v$ по определению стандартной функции. Для каждой конечной точки v носитель R_v функции Φ_v является открытой подгруппой в D_v и носитель S_v функции Ψ_v компактен. Выбирая $a_v \in k_v^\times$ так, чтобы $a_v S_v \subset R_v$, и полагая $\gamma_v = \sup |\Psi_v|$, имеем $|\Psi_v(x)| \leqslant \gamma_v \Phi_v(a_v x)$ при всех $x \in D_v$. Аналогично из определения стандартных функций сразу видно, что для любой бесконечной точки v можно найти такие ε_v, γ_v в $\mathbf{R}_+^\times$, что $|\Psi_v(x)| \leqslant \gamma_v \Phi_v(\varepsilon_v x)$ при всех $x \in D_v$. Это показывает, что существуют такие $a \in k_\mathbf{A}^\times$, $\gamma \in \mathbf{R}_+^\times$, что $|\Psi(x)| \leqslant \gamma \Phi(ax)$ при всех $x \in D_\mathbf{A}$. Поэтому интеграл $Z(\Psi, s)$ при $\mathrm{Re}(s) = \sigma$ мажорируется интегралом

$$\gamma \int_{D_\mathbf{A}^\times} \Phi(az)\, \omega_\sigma(z)\, d\mu(z) = \gamma \omega_\sigma(a^{-1})\, Z_D(\sigma),$$

который по предложению 1 сходится при $\sigma > d$.

Возьмем теперь те же две функции F_0, F_1, что и в доказательстве теоремы 2 гл. VII-5. Тогда $Z(\Psi, s)$ равен сумме двух интегралов

$$Z_i = \int_{D_\mathbf{A}^\times} \Phi(z)\, \omega_s(z)\, F_i(\omega_1(z))\, d\mu(z).$$

Точно так же, как в том доказательстве (но беря теперь $B > d$), мы видим, что Z_0 абсолютно сходится при всех s и определяет поэтому целую функцию от s и что то же самое верно для интеграла Z_0', полученного заменой в определении интеграла Z_0 функции Ψ на ее преобразование Фурье Ψ', s на $d - s$ и F_0 на $t \to F_1(t^{-1})$. Как и прежде, мы можем применить к функции $x \to \Psi(zx)$ на $D_\mathbf{A}$ формулу суммирования Пуассона (т. е. формулу (1) гл. VII-2) в сочетании с леммой 1 гл. VII-2. Применяя последнюю лемму, следует учесть тот факт, что модуль автоморфизма $x \to z^{-1}x$ группы $D_\mathbf{A}$ при $z \in D_\mathbf{A}^\times$ равен

$$|\mathrm{N}_{D/K}(z^{-1})|_\mathbf{A} = |\nu(z)|_\mathbf{A}^{-d} = \omega_{-d}(z).$$

Далее, действуя точно так же, как в доказательстве теоремы 2 гл. VII-5, находим, что интеграл $Z(\Psi, s)$ равен сумме двух целых функций $Z_0 + Z_0'$ и интеграла

$$f(s) = \int_{D_\mathbf{A}^\times / D^\times} (\Psi'(0) - \omega_d(z)\, \Psi(0))\, \omega_{s-d}(z)\, F_1(\omega_1(z))\, d\mu(z).$$

Подинтегральная функция здесь постоянна на каждом классе смежности в группе $G = D_A^\times/D^\times$ по ее компактной подгруппе $G_1 = D_A^1/D^\times$. Так как G_1 является ядром морфизма из G в $\mathbf{R}_+^\times$, определенного морфизмом ω_1, то мы можем отождествить G/G_1 с образом N группы G в $\mathbf{R}_+^\times$ при этом морфизме. Последний образ равен $\mathbf{R}_+^\times$ или группе, порожденной элементом q, в зависимости от того, какова характеристика поля k. Беря в качестве ν меру из леммы 6 гл. VII-5, имеем в силу этой леммы (с точностью до постоянного множителя, который можно сделать равным 1 при помощи подходящего выбора меры μ)

$$f(s) = \int_N (\Psi'(0) - n^d \Psi(0))\, n^{s-d} F_1(n)\, d\nu(n) =$$
$$= \Psi'(0)\,\lambda(s-d) - \Psi(0)\,\lambda(s),$$

где λ — функция, определенная в упомянутой лемме. Ввиду содержащегося в этой лемме утверждения о полюсах функции λ наше доказательство закончено.

Сравнение предложений 1 и 2 дает нам теперь основной результат этой главы.

Теорема 2. *Простая алгебра A над* А*-полем k тривиальна тогда и только тогда, когда она всюду неразветвлена, т. е. тогда и только тогда, когда алгебра A_v тривиальна над k_v для каждой точки v поля k.*

Ясно, что достаточно доказать теорему для алгебры с делением D. Если алгебра D_v тривиальна при всех v, то предложение 1 показывает, что дзета-функция $Z_D(s)$ с точностью до постоянного множителя задается формулой

$$Z_D(s) = \prod_{i=0}^{d-1} Z_k(s-i).$$

Ввиду теорем 3 и 4 гл. VII-6 если $d > 1$, то эта функция имеет полюсы порядка 2 в точках $s = 1, 2, \ldots, d-1$. По предложению 2 этого не может быть. Поэтому $d = 1$ и $D = k$.

Фактически совокупность предложений 1 и 2 позволяет вывести более сильное заключение, чем заключение теоремы 2. Например, сразу видно, что при $d > 1$ алгебра D должна разветвляться по меньшей мере в двух точках поля k. Но нет надобности делать это сейчас, потому что намного более сильные результаты будут получены в гл. XIII.

§ 3. НОРМЫ НА ПРОСТЫХ АЛГЕБРАХ

В качестве первого применения теоремы 2 мы воспроизведем сейчас принадлежащее Эйхлеру доказательство следующего предложения.

Предложение 3. *Пусть A — простая алгебра над k-полем k, и пусть v — приведенная норма на A. Тогда $v(A^\times)$ совпадает с подгруппой γ в $k^\times$, состоящей из элементов, образ которых в k_v строго положителен для каждой вещественной точки v поля k, в которой алгебра A разветвлена.*

Это доказательство основано на следующих леммах.

Лемма 1. *Пусть K — коммутативное p-поле, $L = K(\xi)$ — сепарабельное алгебраическое расширение степени n поля k. Положим*

$$F(X) = N_{L/K}(X - \xi) = X^n + \sum_{i=1}^{n} a_i X^{n-i}.$$

Пусть $G(X) = \sum_{i=1}^{n} b_i X^{n-i}$ — многочлен степени $n-1$ из $K[X]$. Тогда если все коэффициенты многочлена G достаточно близки к нулю в K, то многочлен $F+G$ неприводим над K и имеет корень в L.

Удобно продолжить mod_K до отображения $x \to |x|$ алгебраического замыкания $\bar{K}$ поля L со значениями в $\mathbf{R}_+$, полагая $|x| = \mathrm{mod}_{K'}(x)^{1/v}$, если $K(x) \subset K' \subset \bar{K}$ и K' имеет степень v над K; по следствию 2 теор. 3 гл. I-2 это определение для заданного x в $\bar{K}$ не зависит от выбора K'. Возьмем такое $A \in \mathbf{R}_+^\times$, что $|a_i| \leqslant A^i$ при $1 \leqslant i \leqslant n$, и предположим, что $|b_i| \leqslant B^i$ при $1 \leqslant i \leqslant n$ для некоторого $B < A$. Пусть η — любой корень многочлена $F+G$ в $\bar{K}$. Тогда

$$\eta^n = -\sum_{i=1}^{n} (a_i + b_i)\,\eta^{n-i},$$

поэтому

$$|\eta|^n \leqslant \sup_i (A^i\,|\eta|^{n-i}),$$

и, следовательно, $|\eta| \leqslant A$. Обозначим через $\xi_1, \ldots, \xi_n$ корни многочлена F. Все они различны, поскольку поле L сепарабельно над K, и все они являются образами корня ξ при автоморфизмах поля $\bar{K}$ над K. То, что мы уже доказали для η, можно применить

к ξ_ν, взяв $G = 0$. Поэтому $|\xi_\nu| \leqslant A$ при $1 \leqslant \nu \leqslant n$. Положим теперь

$$\alpha = \inf_{1 \leqslant \mu < \nu \leqslant n} |\xi_\nu - \xi_\mu|.$$

Имеем $0 < \alpha \leqslant A$. Предположим, что мы взяли $B < A\,(\alpha/A)^n$. Поскольку η — корень многочлена $F + G$, имеем

$$\prod_{\nu=1}^{n} (\eta - \xi_\nu) = -\sum_{i=1}^{n} b_i \eta^{n-i},$$

откуда

$$\inf_\nu |\eta - \xi_\nu|^n \leqslant \sup_i (B^i A^{n-1}) \leqslant B A^{n-1} < \alpha^n,$$

так что существует ν, для которого $|\eta - \xi_\nu| < \alpha$. Отсюда, очевидно, следует, что $|\eta - \xi_\mu| \geqslant \alpha$ при всех $\mu \neq \nu$. Пусть σ — автоморфизм поля $\bar{K}$ над K, отображающий ξ_ν на ξ. Заменив элемент η на элемент η^σ, который также является корнем многочлена $F + G$, мы видим, что $|\eta - \xi| < \alpha$ и $|\eta - \xi_\nu| \geqslant \alpha$ при всех $\xi_\nu \neq \xi$. Предположим, что L не содержится в $K(\eta)$. Тогда существует такой автоморфизм τ поля $\bar{K}$ над $K(\eta)$, что $\xi^\tau \neq \xi$. Так как этот автоморфизм должен оставлять $|\eta - \xi|$ инвариантным, мы получаем противоречие. Поэтому $K(\eta) \supset L$. Поскольку степень элемента η над K не больше n, отсюда следует, что $K(\eta) = L$ и что многочлен $F + G$ неприводим.

Между прочим, поскольку каждое расширение степени n поля K может быть, очевидно, порождено корнем нормированного многочлена F степени n с коэффициентами в максимальном компактном подкольце поля K, из леммы 1 немедленно следует, что поле K имеет лишь конечное число сепарабельных расширений заданной степени, а значит, в силу следствия 2 предл. 4 гл. I-4, лишь конечное число алгебраических расширений заданной степени [1]).

Лемма 2. *Пусть K — коммутативное p-поле, R — его максимальное компактное подкольцо и L — неразветвленное расширение*

[1]) Это неверное утверждение сохранено здесь в точности в том же виде, как и в английском оригинале, отчасти для того, чтобы позабавить читателя, отчасти же как типичный пример ошибок, которые делают даже пишущие тщательно (к категории которых, как смеет надеяться автор этой книги, его можно отнести), когда они начинают опускать полные доказательства или пробуют заменить их такими словами, как «аналогично», «легко видеть, что», «очевидно» и т. п. На самом деле указанное выше утверждение для поля K характеристики $p > 0$ находится в прямом противоречии с фактами, приведенными в § 3 гл. II, если сопоставить их с результатами гл. XII. В случае когда K — поле характеристики 0, утверждение справедливо. — *Прим. автора к русскому изданию.*

поля K. Тогда для каждого $x \in R^\times$ существует такое $y \in L$, что $N_{L/K}(y) = x$ и $K(y) = L$.

Пусть n — степень поля L над K, и пусть δ — число делителей числа n. Так как поле L циклично над K, то δ совпадает с числом различных полей, промежуточных между K и L. Построим сначала $\varepsilon \in L$, для которого $N_{L/K}(\varepsilon) = 1$ и $L = K(\varepsilon^i)$ при $1 \leqslant i \leqslant \delta$. Возьмем какое-нибудь общее кратное D чисел $1, 2, \ldots, \delta$, скажем $D = \delta!$. Обозначим через α некоторую образующую группы Галуа поля L над K. Для $1 \leqslant h \leqslant n-1$ рассмотрим отображение

$$\xi \to P_h(\xi) = (\xi\alpha^{h+1}\xi)^D - (\xi\alpha^h\xi\alpha)^D$$

поля L в себя. Это — полиномиальное отображение векторного пространства L над K, что сразу видно, если выбрать какой-нибудь базис в L над K и записать ξ с помощью этого базиса. Снова взяв в качестве $\bar{K}$ алгебраическое замыкание поля L, мы можем продолжить отображение P_h на алгебру $\mathfrak{L} = L \otimes_K \bar{K}$ над $\bar{K}$. Теперь к этой алгебре и к n различным изоморфизмам α^i поля L в $\bar{K}$, $0 \leqslant i \leqslant n-1$, применим предложение 3 гл. III-2. Как и там, обозначим через μ_i $\bar{K}$-линейное продолжение отображения α^i на L и положим $\varphi = (\mu_0, \ldots, \mu_{n-1})$. Упомянутое предложение показывает, что φ есть изоморфизм из L на $\bar{K}^n$. Отображение $\mu_0 \circ P_h \circ \varphi^{-1}$ из $\bar{K}^n$ в K действует следующим образом:

$$(x_0, \ldots, x_{n-1}) \to (x_{h+1}x_0)^D - (x_hx_1)^D,$$

где в случае $h = n-1$ подразумевается, что $x_n = x_0$. Так как это отображение ненулевое и так как поле K бесконечно, мы видим, что никакое из отображений P_h не равно нулю и что можно выбрать такой элемент $\xi \in L$, для которого $P_h(\xi) \neq 0$ при $1 \leqslant h \leqslant n-1$. Для выбранного так ξ положим $\varepsilon = \xi\alpha\xi^{-1}$. Тогда $N_{L/K}(\varepsilon) = 1$ и образы $(\varepsilon^{\alpha h})^D$ элемента ε^D при автоморфизмах α^h с $1 \leqslant h \leqslant n-1$ все $\neq \varepsilon^D$, так что $L = K(\varepsilon^D)$. Поскольку D делится на i при $1 \leqslant i \leqslant \delta$, то для каждого такого i имеем $\varepsilon^D = (\varepsilon^i)^{D/i}$, откуда $K(\varepsilon^D) \subset K(\varepsilon^i)$, так что $L = K(\varepsilon^i)$. Возьмем теперь любой элемент $x \in R^\times$. По предложению 3 гл. VIII-1 мы можем записать его в виде $x = N_{L/K}(y_1)$, где $y_1 \in L^\times$. Рассмотрим бесконечную последовательность полей $K_i = K(\varepsilon^i y_i)$, $i \geqslant 0$. Из них различных полей может быть самое большее δ, поэтому существуют такие пары (i, j) целых чисел, что $0 \leqslant i < j$ и $K_i = K_j$, и если мы возьмем такую пару, для которой $j - i$ принимает наименьшее значение, то $0 < j - i \leqslant \delta$. Поскольку элементы $\varepsilon^i y_1$ и $\varepsilon^j y_1$ лежат оба в K_i, то ε^{j-i} лежит в K_i. Ввиду нашего выбора ε отсюда следует,

что $K_i = L$. Таким образом, $y = \varepsilon^i y_1$ удовлетворяет требованиям нашей леммы.

Мы можем теперь приступить к доказательству предложения 3. Обозначим через n^2 размерность заданной алгебры A над k и через R_∞ множество бесконечных точек поля k, в которых она разветвлена. Если точка v лежит в R_∞, то она должна быть вещественной, а алгебра A_v должна быть изоморфна алгебре $M_m(\mathbf{H})$. Поскольку отсюда следует, что $n = 2m$, это может случиться только тогда, когда n четно и когда, разумеется, характеристика поля k равна нулю. Как мы видели в гл. X-2, приведенная норма ν отображает $M_m(\mathbf{H})^\times$ на $\mathbf{R}_+^\times$, поэтому $\nu(A^\times)$ содержится в группе γ, определенной в предложении 3.

Выберем непустое множество R' конечных точек поля k, содержащее все конечные точки поля k, в которых алгебра A разветвлена, и положим $R = R' \cup R_\infty$. Возьмем любую точку v из R' и некоторый простой элемент π_v из k_v. По предложению 6 гл. X-2 существует $x_v \in A_v$, для которого $\nu(x_v) = \pi_v$. Применяя к A и некоторой точке v_0 поля k, не лежащей в R', следствие 2 теор. 3 гл. IV-2, получаем, что можно так выбрать элемент $\alpha \in A$, чтобы его образ в A_v был произвольно близок к x_v и чтобы его образ в A_w при всех $w \neq v$ был произвольно близок к 1. Ввиду непрерывности нормы ν это можно сделать так, чтобы образ элемента $\nu(\alpha)$ в k_v был настолько близок к π_v, чтобы являлся простым элементом в k_v и чтобы его образ в k_w для каждой точки $w \neq v$ из R' был настолько близок к 1, чтобы лежал в $r_v^\times$. Тогда $\alpha \in A^\times$, поскольку $\nu(\alpha) \neq 0$. Для всякой точки $v \in R'$ выберем элемент $\alpha_v \in A^\times$ указанным способом.

Возьмем теперь произвольный элемент ξ в подгруппе $\gamma \subset k^\times$, определенной в нашем предложении. Мы хотим показать, что ξ лежит в $\nu(A^\times)$. Для всякой точки v из R' положим $n(v) = \mathrm{ord}_v(\xi)$ и $\alpha = \prod \alpha_v^{n(v)}$. Заменив ξ на $\xi\nu(\alpha)^{-1}$, мы видим, что достаточно доказать наше утверждение при дополнительном предположении, что $\mathrm{ord}_v(\xi) = 0$ для всех $v \in R'$. Для всякой точки $v \in \mathbf{R}'$ возьмем некоторое неразветвленное расширение k_v' поля k_v степени n над k_v. По лемме 2 существует $y_v \in k_v'$, для которого $\xi = \mathrm{N}_{k_v'/k_v}(y_v)$ и $k_v' = k_v(y_v)$. Так как элемент y_v имеет тогда степень n над k_v, то он является корнем неприводимого многочлена F_v степени n над k_v, задаваемого равенством

$$F_v(X) = \mathrm{N}_{k_v'/k_v}(X - y_v) = X^n + \sum_{i=1}^{n-1} a_{i,v} X^{n-i} + (-1)^n \xi,$$

где $a_{i,v} \in k_v$ при $1 \leqslant i \leqslant n-1$. Для всякой точки $v \in R_\infty$ положим $a_{i,v} = 0$ при $1 \leqslant i \leqslant n-1$. Поскольку из существования такой точки следует четность n, имеем

$$F_v(X) = X^n + (-1)^n \xi = X^n + \xi.$$

Так как по нашему предположению $\xi \in \gamma$, то многочлен F_v не имеет корней в $k_v = \mathbf{R}$, и значит, то же самое справедливо для каждого унитарного многочлена степени n над $\mathbf{R}$, коэффициенты которого достаточно близки к коэффициентам многочлена F_v. Применяя к полю k и к некоторой точке v_0 поля k, не лежащей в R, следствие 2 теор. 3 гл. IV-2, мы видим, что можно так выбрать элементы $\omega_i \in k$, $1 \leqslant i \leqslant n-1$, чтобы их образы в k_v были произвольно близки к $a_{i,v}$ для каждой точки $v \in R$. Ввиду леммы 1 и только что сказанного этот выбор можно произвести так, чтобы многочлен

$$F(X) = X^n + \sum_{i=1}^{n-1} \omega_i X^{n-i} + (-1)^n \xi$$

обладал следующими свойствами: (a) для каждой точки $v \in R'$ многочлен F неприводим над k_v и имеет корень в k'_v, (b) для каждой точки $v \in R_\infty$ многочлен F не имеет корня в $k_v = \mathbf{R}$. Так как R' непусто, то из (a) следует, что многочлен F неприводим над k и не имеет кратных корней. Обозначим через ζ корень многочлена F в некотором алгебраическом замыкании поля k и положим $k' = k(\zeta)$. Возьмем любую точку $v \in R'$ и точку w поля k', лежащую над v. Так как пополнение поля k' относительно этой точки должно порождаться над k_v корнем многочлена F, то это пополнение, согласно (a), изоморфно полю k'_v, с которым мы и можем его отождествить. Поскольку его степень над k_v равна n, следствие 1 теор. 4 гл. III-4 показывает, что w является единственной точкой поля k', лежащей над v, а сама эта теорема показывает, что мы можем отождествить $k'_w = k'_v$ с $k' \otimes_k k_v$. Аналогично (b) показывает, что при $v \in R_\infty$ все точки поля k', лежащие над v, мнимы.

Теперь рассмотрим алгебру $A' = A_{k'}$ над k'. Возьмем любую точку w поля k' и обозначим через v точку поля k, лежащую под w. В силу элементарных свойств тензорных произведений алгебру A'_w, которая совпадает с алгеброй $A' \otimes_{k'} k'_w$ над k'_w, можно очевидным образом отождествить с $A_v \otimes_{k_v} k'_w$. Так как алгебра A_v тривиальна над k_v для точек v, не лежащих в R, отсюда видно, что алгебра A'_w также должна быть в этом случае тривиальной. При $v \in R_\infty$ точка w мнима, так что $k'_w = \mathbf{C}$ и алгебра A'_w тривиальна. Наконец, пусть v лежит в R'. Запишем A_v в виде $M_{m(v)}(D(v))$, где $D(v)$ — алгебра

с делением над k_v. Если ее размерность над k_v равна $d(v)^2$, то $n = m(v)\,d(v)$, так что $d(v)$ делит n. Поэтому поле k'_w, неразветвленное и, следовательно, являющееся циклическим расширением степени n поля k_v, содержит поле k'' степени $d(v)$ над k_v, которое, конечно, неразветвлено над k_v. По предложению 5 гл. I-4 $D(v)$ содержит поле, изоморфное k''. Поэтому в силу следствия 6 предл. 3 гл. IX-1 алгебра $D(v)_{k''}$ тривиальна над k''. Отсюда, очевидно, вытекает, что алгебра $(A_v)_{k''}$ тривиальна над k'', а значит, алгебра $A'_w = (A_v)_{k'_w}$ тривиальна над k'_w.

Доказав таким образом неразветвленность алгебры A' во всех точках поля k', мы можем по теореме 2 § 2 заключить, что эта алгебра тривиальна над k', т. е. что A обладает k'-представлением в $M_n(k')$. Поэтому в силу теоремы 2 гл. IX-3 A имеет $\mathfrak{H}$-регулярную систему факторов, где $\mathfrak{H}$ — группа Галуа над k' сепарабельного алгебраического замыкания k_{sep} поля k'. Следовательно, по лемме 4 гл. IX-3 мы можем построить некоторую алгебру размерности n^2 над k, содержащую поле, изоморфное полю k', с той же самой системой факторов, что и A. Поскольку отсюда следует, что эта алгебра подобна алгебре A, и поскольку она имеет ту же размерность над k, что и A, то она изоморфна алгебре A и ее можно отождествить с ней. При этом, как было там показано, мы имеем $\nu(\xi \cdot 1_A) = \mathrm{N}_{k'/k}(\xi) = \xi$.

§ 4. ПРОСТЫЕ АЛГЕБРЫ НАД ПОЛЯМИ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Сейчас мы объединим результаты § 1 с некоторыми результатами гл. V и получим несколько основных результатов теории идеалов в простых алгебрах над полями алгебраических чисел.

В этом параграфе k будет некоторым полем алгебраических чисел, $\mathfrak{r}$ — его максимальным порядком; все алгебры будут простыми алгебрами над k. Напомним, что по предложению 4 гл. V-2 если L — любая k-решетка в векторном пространстве E над k и если v — конечная точка поля k, то замыкание L_v решетки L в E_v является r_v-модулем, порожденным решеткой L в E_v.

Пусть D — алгебра с делением над k, и пусть, как и в гл. X-1, V, V', V'' — левые векторные пространства конечной размерности над D, отличные от $\{0\}$. Положим $H = \mathrm{Hom}(V, V')$, $H' = \mathrm{Hom}(V', V'')$, $H'' = \mathrm{Hom}(V, V'')$. Если X, X' — подгруппы аддитивных групп H, H' соответственно, то мы как обычно обозначаем через XX' подгруппу в H'', порожденную элементами вида $\xi\xi'$, где $\xi \in X$, $\xi' \in X'$. Легко показать, например выбрав базисы в V, V', V'' над D, что $HH' = H''$. Пусть теперь L, L' — две

k-решетки в группах H и H' соответственно (последние рассматриваются как векторные пространства над k). Тогда LL' является, очевидно, конечно порожденным $\mathfrak{r}$-модулем в H''; поскольку $H'' = HH'$, это k-решетка в H''.

Предложение 4. *Пусть A — простая алгебра над k. Тогда в A существуют максимальные порядки. Они являются k-решетками в A, и k-решетка R в A является максимальным порядком тогда и только тогда, когда ее замыкание R_v в A_v является максимальным порядком в A_v для каждой конечной точки v поля k. Каждый порядок в A содержится в некотором максимальном порядке.*

Пусть R — произвольный порядок в A. Тогда $\mathfrak{r}$-модуль, порожденный им в A, также является порядком и одновременно k-решеткой. Отсюда видно, что если порядок R не является k-решеткой, то он не максимален. Пусть X — любая k-решетка в A. Последняя часть теоремы 1 § 1 утверждает, что X_v является максимальным порядком в A_v почти для всех v. Поэтому теорема 2 гл. V-2 показывает, что имеется взаимно однозначное соответствие между порядками R в A, являющимися k-решетками, и всевозможными наборами порядков R_v в A_v по всем конечным точкам v поля k, подчиненным следующему условию: R_v является k_v-решеткой для всех v и $R_v = X_v$ почти для всех v. Для заданного R порядки R_v — это его замыкания в A_v, а по заданным R_v порядок R определяется формулой $R = \bigcap (A \cap R_v)$. Ввиду теоремы 1 гл. X-1 все наши утверждения теперь очевидны.

Предложение 5. *Пусть D — алгебра с делением над k, V, W — два левых векторных пространства конечной размерности над D. Положим $H = \mathrm{Hom}(V, W)$ и $A = \mathrm{End}(V)$, и пусть M, M' — две k-решетки в H. Тогда множество X элементов ξ из A, для которых $\xi M \subset M'$, является k-решеткой в A, замыкание которой в A_v для каждой конечной точки v поля k совпадает с множеством X_v тех элементов x из A_v, для которых $xM_v \subset M'_v$. Если $M = M'$, то X является порядком в A.*

Для каждой точки v по предложению 4 гл. X-1 X_v является k_v-решеткой в A_v; она является порядком, если $M_v = M'_v$. Пусть L — произвольная k-решетка в A. Как мы видели выше, LM является k-решеткой в H, замыкание которой в H_v для каждой точки v совпадает, очевидно, с L_vM_v. Поэтому почти для всех v имеем $L_vM_v = M_v = M'_v$. Отсюда следует, что почти для всех v решетка X_v является порядком и содержит L_v. Так как L_v — максимальный порядок в A_v почти для всех v, мы видим, что $X_v = L_v$ почти для всех v. Поэтому по теореме 2 гл. V-2 существует k-решетка $X' =$

$= \bigcap (A \bigcap X_v)$ в A с замыканиями X_v для всех v. Ясно, что $X \subset X'$. Обратно, поскольку $X'M \subset M'_v$ для каждой точки v и $M' = \bigcap (H \bigcap M'_v)$, то мы имеем $X' \subset X$. Тем самым доказательство предложения завершено, ибо последнее утверждение теперь очевидно.

В обозначениях и предположениях предложения 5 множество X в случае $M = M'$ называется *левым порядком* для M. Меняя ролями правое и левое, мы видим, что множество элементов η из $B = \mathrm{End}\,(W)$, для которых $M\eta \subset M$, является порядком в B; этот порядок называется *правым порядком* для M.

Предложение 6. *Пусть V, W и M таковы, как в предложении* 5. *Предположим, что существует такой максимальный порядок R в $A = \mathrm{End}\,(V)$, что M является левым R-модулем. Тогда R есть левый порядок для модуля M, а его правым порядком является максимальный порядок в $B = \mathrm{End}\,(W)$.*

Это немедленное следствие предложения 5, если учесть теорему 2 гл. X-1.

В тех же обозначениях и предположениях, что и в предложениях 5 и 6, k-решетку M в $\mathrm{Hom}\,(V, W)$ с левым порядком R и правым порядком S будем называть (R, S)-решеткой; будем называть ее *нормальной решеткой*, если либо R, либо S, а значит и R и S, являются максимальными порядками. В случае когда $V = W$ и, следовательно, $H = A = B$, нормальную решетку принято также называть *нормальным дробным идеалом*. Ясно, что в этом случае три соотношения $M \cdot M \subset M$, $M \subset R$, $M \subset S$ эквивалентны. Если они выполняются, то решетка M является левым идеалом в кольце R и правым идеалом в кольце S; ее называют в этом случае *нормальным идеалом*, или (R, S)-*идеалом*. Используя изложенные выше результаты и результаты гл. X, легко показать, что для любых двух максимальных порядков R и S в A всегда существуют (R, S)-идеалы. Далее, если нормальная (R, S)-решетка M является максимальным левым идеалом в R, т. е. если $M \subset R$, $M \neq R$ и не существует левых идеалов, отличных от R и M и промежуточных между R и M, то M есть максимальный правый идеал в S в том же смысле. В случае когда это имеет место, для всех конечных точек v поля k, кроме одной, должно быть $M_v = R_v = S_v$. Если ограничить закон умножения $(M, M') \to MM'$ на те пары (M, M') нормальных решеток в A, для которых правые порядки для M совпадают с левыми порядками для M', то нормальные решетки образуют относительно этого закона так называемый *группоид*, единицами которого являются максимальные порядки в A. Легко

убедиться также, что относительно этого закона каждый нормальный идеал может быть записан, правда, вообще говоря, не однозначно, в виде произведения максимальных идеалов. Для двусторонних идеалов и (R, R)-решеток имеется следующий более точный результат.

Предложение 7. *Пусть R — максимальный порядок в A. Тогда (R, R)-решетки в A образуют коммутативную группу относительно закона $(M, M') \to MM'$. Это — свободная группа, порожденная максимальными двусторонними идеалами в R. Для каждого простого идеала $\mathfrak{p}$ в $\mathfrak{r}$ существует один и только один такой идеал, заключенный между R и $\mathfrak{p}R$.*

Это непосредственно вытекает из изложенных выше результатов и следствия 2 теор. 2 гл. X-1.

ГЛАВА ДВЕНАДЦАТАЯ

ЛОКАЛЬНАЯ ТЕОРИЯ ПОЛЕЙ КЛАССОВ

§ 1. ФОРМАЛИЗМ ТЕОРИИ ПОЛЕЙ КЛАССОВ

Цель теории полей классов — дать описание абелевых расширений полей изучаемого в этой книге типа, а именно локальных полей и A-полей. В этом параграфе изложен формальный аппарат, общий для обоих этих случаев.

Лемма 1. *Пусть $G = G_1 \times N$ — квазикомпактная группа, где группа G_1 компактна, а группа N изоморфна* $\mathbf{R}$ *или* $\mathbf{Z}$, *и пусть H — открытая подгруппа в G. Тогда, если подгруппа H содержится в G_1 (т. е. если она компактна), то группа N изоморфна* $\mathbf{Z}$ *и H имеет конечный индекс в G_1; в противном случае H имеет конечный индекс в G.*

Положим $H_1 = H \cap G_1$. Так как это пересечение открыто в G_1, а группа G_1 компактна, то H_1 имеет конечный индекс в G_1, чем доказано наше первое утверждение. Поскольку пересечение $H \cap N$ является открытой подгруппой в N, то оно совпадает с N, если группа N изоморфна $\mathbf{R}$. Значит в этом случае $H = H_1 \times N$ и группа G/H изоморфна G_1/H_1. Пусть группа N изоморфна $\mathbf{Z}$ и n_1 — какая-нибудь образующая группы N. Тогда если H не содержится в G_1, то в H имеется элемент вида $g_1 n_1^{\mu}$, где $g_1 \in G_1$, $\mu \in \mathbf{Z}$, $\mu \neq 0$. Поскольку факторгруппа G_1/H_1 конечна, существует $\nu \neq 0$, для которого $g_1^{\nu} \in H_1$. Поэтому $n_1^{\mu\nu}$ лежит в H, так что H содержит группу H', порожденную подгруппой H_1 и элементом $n_1^{\mu\nu}$. Тем самым наша лемма доказана, так как, очевидно, H' имеет конечный индекс в G.

Теорему 7 гл. IV-4 можно рассматривать как частный случай леммы с $G = k_{\mathrm{A}}^{\times}/k^{\times}$, если взять в качестве H образ группы $\Omega(P)$ в $k_{\mathrm{A}}^{\times}/k^{\times}$.

Лемма 2. *Пусть $G = G_1 \times N$, $G' = G_1' \times N'$ — квазикомпактные группы, где группы G_1 и G_1' компактны, а группы N, N'*

изоморфны **R** *или* **Z**, *и пусть* F — *морфизм из* G' *в* G, *но не в* G'. *Тогда* $F^{-1}(G_1) = G'_1$, *ядро морфизма* F *компактно, образ* $F(G')$ *замкнут в* G *и факторгруппа* $G/F(G')$ *компактна.*

Поскольку G_1 — максимальная компактная подгруппа в G, то $F(G'_1)$ содержится в G_1. Для $n' \in N'$ обозначим через $f(n')$ проекцию элемента $F(n') \in G$ в N. Тогда f есть нетривиальный морфизм из N' в N. Следовательно, f является изоморфизмом группы N' на некоторую замкнутую подгруппу в N, факторгруппа по которой компактна. Отсюда сразу вытекают первое и второе утверждения. Кроме того, мы видим теперь, что F индуцирует на группе N' изоморфизм этой группы на группу $F(N')$ и что $F(N') \cap G_1 = \{1\}$. Поэтому группа $F(G')$ разлагается в прямое произведение своих подгрупп $F(G'_1)$ и $F(N')$, причем подгруппа $F(G')$ замкнута в G. Наконец, факторгруппа $G/G_1F(N')$, очевидно, изоморфна факторгруппе $N/f(N')$ и, следовательно, компактна. Так как ядро естественного морфизма из $G/F(G')$ на $G/G_1F(N')$ совпадает с образом группы G_1 в $G/F(G')$ и, следовательно, компактно, то факторгруппа $G/F(G')$ также должна быть компактной.

В этом параграфе объектом нашего рассмотрения, начиная с этого места, будет некоторое поле K; потом это будет или локальное поле, или **A**-поле. Как и в гл. IX, обозначим через $\overline{K}$ алгебраическое замыкание поля K, через K_{sep} — объединение всех сепарабельных расширений поля K, содержащихся в $\overline{K}$, и через $\mathfrak{G}$ — группу Галуа расширения K_{sep} над K, топологизированную обычным образом. Через K_{ab} будем обозначать максимальное абелево расширение поля K, содержащееся в $\overline{K}$; оно совпадает с объединением всех абелевых расширений конечной степени поля K, содержащихся в $\overline{K}$, т. е. всех содержащихся в $\overline{K}$ расширений Галуа конечной степени поля K с коммутативной группой Галуа. По определению K_{ab} содержится в K_{sep}. Обозначим через $\mathfrak{G}^{(1)}$ подгруппу в $\mathfrak{G}$, соответствующую расширению K_{ab}. Это — наименьшая замкнутая нормальная подгруппа в $\mathfrak{G}$, для которой факторгруппа $\mathfrak{G}/\mathfrak{G}^{(1)}$ коммутативна. Поэтому $\mathfrak{G}^{(1)}$ совпадает с *топологическим коммутантом* группы $\mathfrak{G}$, т. е. с замыканием подгруппы в $\mathfrak{G}$, порожденной коммутаторами элементов из $\mathfrak{G}$. Группу Галуа поля K_{ab} над K, которую можно отождествить с факторгруппой $\mathfrak{G}/\mathfrak{G}^{(1)}$, обозначим через $\mathfrak{A}$; это — компактная коммутативная группа.

Пусть χ — любой характер на $\mathfrak{G}$. Как и в гл. IX-4, обозначим через $\mathfrak{H}$ ядро этого характера и через L — соответствующее группе $\mathfrak{H}$ подполе в K_{sep}, являющееся связанным с χ циклическим расши-

рением поля K. Ясно, что $L \subset K_{ab}$ и $\mathfrak{H} \supset \mathfrak{G}^{(1)}$, так что мы можем отождествить χ с некоторым характером на $\mathfrak{A}$, который обозначим также через χ. Обратно, каждый характер на $\mathfrak{A}$ очевидным способом определяет характер на $\mathfrak{G}$, с которым мы его и отождествляем. Таким образом, группа характеров на $\mathfrak{G}$, которую мы будем обозначать через X_K, отождествлена с группой характеров на $\mathfrak{A}$. Последняя группа — это не что иное, как группа $\mathfrak{A}^*$, двойственная к $\mathfrak{A}$, но групповую операцию на X_K мы будем всегда записывать мультипликативно. Мы наделяем X_K дискретной топологией, что согласуется с тем фактом, что группа, двойственная к компактной группе, дискретна. По теории двойственности пересечение ядер всех характеров на $\mathfrak{A}$ состоит из одного нейтрального элемента. Иными словами, пересечение ядер $\mathfrak{H}$ всех характеров χ на $\mathfrak{G}$ совпадает с $\mathfrak{G}^{(1)}$, или, что означает то же самое, поле K_{ab} порождено всеми циклическими расширениями L поля K; последний факт, разумеется, общеизвестен.

Пусть K' — любое поле, содержащее поле K. Как и в гл. IX-3, возьмем какое-нибудь алгебраическое замыкание $\overline{K}'$ поля K' и предположим, что в качестве $\overline{K}$ взято алгебраическое замыкание поля K в $\overline{K}'$. Тогда, как мы уже видели там, K_{sep} содержится в K'_{sep}, и если $\mathfrak{G}'$ — группа Галуа расширения K'_{sep} над K', то морфизм ограничения $\rho: \mathfrak{G}' \longrightarrow \mathfrak{G}$ отображает каждый автоморфизм поля K'_{sep} над K' на его ограничение на K_{sep}. Очевидно, ρ отображает $\mathfrak{G}'^{(1)}$ в $\mathfrak{G}^{(1)}$, так что он определяет морфизм из $\mathfrak{A}' = \mathfrak{G}'/\mathfrak{G}'^{(1)}$ в $\mathfrak{A} = \mathfrak{G}/\mathfrak{G}^{(1)}$, который мы обозначим снова через ρ и назовем гомоморфизмом ограничения из $\mathfrak{A}'$ в $\mathfrak{A}$. Другими словами, K_{ab} содержится в K'_{ab} и ρ переводит элемент $\alpha' \in \mathfrak{A}'$, т. е. автоморфизм поля K'_{ab} над K', в его ограничение на K_{ab}. Соответственно отображение $\chi \longrightarrow \chi \circ \rho$ есть морфизм из X_K в $X_{K'}$.

В теории полей классов определяется «спаривание» группы X_K характеров на $\mathfrak{G}$ (или, что то же самое, на $\mathfrak{A}$) с некоторой локально компактной коммутативной группой G_K, инвариантным образом связанной с K. В этой главе, где K будет локальным полем, мы возьмем $G_K = K^\times$; в следующей главе, где K будет **A**-полем, мы возьмем сначала $G_K = K_A^\times$, а затем $G_K = K_A^\times/K^\times$. Спаривание, о котором идет речь и которое мы будем называть *каноническим спариванием*,— это отображение из $X_K \times G_K$ в $\mathbf{C}^\times$; для $\chi \in X_K$, $g \in G_K$ его значения мы будем записывать как $(\chi, g)_K$. Прежде всего мы примем, что оно удовлетворяет следующим условиям:

[I] (i) *Для всех* $\chi, \chi' \in X_K$ *и всех* $g, g' \in G_K$

$$(\chi\chi', g)_K = (\chi, g)_K \cdot (\chi', g)_K,$$
$$(\chi, gg')_K = (\chi, g)_K \cdot (\chi, g')_K;$$

(ii) $(\chi, g) \to (\chi, g)_K$ *есть непрерывное отображение из* $X_K \times G_K$ *в* $\mathbf{C}^\times$.

Поскольку группа X_K дискретна, то спаривание непрерывно (т. е. условие [I (ii)] выполняется) в том и только в том случае, когда $g \to (\chi, g)_K$ есть непрерывное отображение из G_K в $\mathbf{C}^\times$ для каждого $\chi \in G_K$; в этом случае из [I (i)] вытекает, что это отображение является характером на G_K, причем порядок этого характера делит порядок характера χ. Обратно, если имеет место [I (i)], то условие [I (ii)] эквивалентно следующему:

[I (ii′)] *Для каждого* $\chi \in X_K$ *ядро морфизма* $g \to (\chi, g)_K$ *является открытой подгруппой в* G_K.

Предположим, что такое спаривание задано. Тогда для всякого $g \in G_K$ отображение $\chi \to (\chi, g)_K$ является характером на X_K. Поскольку X_K — двойственная к $\mathfrak{A}$ группа, то, согласно теории двойственности, последний характер можно однозначно записать в виде $\chi \to \chi(\alpha)$, где $\alpha \in \mathfrak{A}$. Определенное таким образом отображение $g \to \alpha$ из G_K в $\mathfrak{A}$ мы будем обозначать через $\mathfrak{a}$, или, если необходимо, через $\mathfrak{a}_K$. Очевидно, что $\mathfrak{a}(gg') = \mathfrak{a}(g)\,\mathfrak{a}(g')$ при всех g, g' из G_K. Непрерывность нашего спаривания, т. е. условие [I (ii)], сразу влечет за собой непрерывность $\mathfrak{a}$. Таким образом, $\mathfrak{a}$ — морфизм из G_K в $\mathfrak{A}$, определенный соотношением

$$(\chi, g)_K = \chi(\mathfrak{a}(g)), \tag{1}$$

которое выполняется при всех $\chi \in X_K$ и всех $g \in G_K$. Мы будем называть $\mathfrak{a}$ *каноническим морфизмом* из G_K в $\mathfrak{A}$.

Теперь мы предположим дополнительно, что выполняется условие

[II] *Если* $(\chi, g)_K = 1$ *при всех* $g \in G_K$, *то* $\chi = 1$.

Ввиду [I] это условие эквивалентно каждому из следующих условий:

[II′] *Отображение* $\chi \to \chi \circ \mathfrak{a}$ *есть инъективный морфизм из* X_K *в группу характеров на* G_K.

[II″] *Образ* $\mathfrak{a}(G_K)$ *группы* G_K *при морфизме* $\mathfrak{a}$ *всюду плотен в* $\mathfrak{A}$.

К нашим предположениям мы добавим еще условие квазикомпактности группы G_K, фактически даже более жесткое условие, которое выглядит следующим образом.

[III] *Либо* (a) G_K *разлагается в прямое произведение некоторой компактной группы* G_K^1 *и группы* N, *изоморфной* $\mathbf{R}$, *либо* (b) G_K *разлагается в прямое произведение компактной группы* G_K^1 *и груп-*

пы N, изоморфной $\mathbf{Z}$, и для всякого целого числа $n \geqslant 1$ существует такой характер $\chi \in X_K$ порядка n, что $(\chi, g)_K = 1$ при всех $g \in G_K^1$.

На эти два случая в [III] мы будем ссылаться ниже как на случаи [III (a)] и [III (b)] соответственно. В обоих случаях, как было отмечено в гл. VII-3, G_K^1 можно охарактеризовать как единственную максимальную компактную подгруппу в G_K.

Начиная с этого места, мы будем обозначать через U_K ядро канонического морфизма $\mathfrak{a}$ из G_K в $\mathfrak{A}$; это — пересечение ядер характеров $\chi \circ \mathfrak{a}$ на G_K, т. е. характеров $g \to (\chi, g)_K$, по всем $\chi \in X_K$.

Предложение 1. *В случае* [III (a)] *канонический морфизм $\mathfrak{a}$ определяет изоморфизм группы G_K/U_K на $\mathfrak{A}$; каждый характер на G_K, тривиальный на U_K, можно однозначно записать в виде $\chi \circ \mathfrak{a}$, где $\chi \in X_K$ и $\chi \to \chi \circ \mathfrak{a}$ — инъективный морфизм группы X_K в группу характеров конечного порядка на G_K.*

Так как каждый характер χ на $\mathfrak{A}$ имеет конечный порядок, то последнее утверждение есть просто переформулировка условия [II']. Для каждого $\chi \in X_K$ характер $\chi \circ \mathfrak{a}$ индуцирует на подгруппе $N \subset G_K$ некоторый характер конечного порядка. Поскольку группа N изоморфна $\mathbf{R}$, других таких характеров, кроме тривиального, не существует. Поэтому $N \subset U_K$. Если положить $U_K^1 = U_K \cap G_K^1$, то $U_K = U_K^1 \times N$ и факторгруппу G_K/U_K можно отождествить с G_K^1/U_K^1. Поскольку последняя группа компактна, $\mathfrak{a}$ определяет изоморфизм этой группы на замкнутую подгруппу в $\mathfrak{A}$, а следовательно, в силу [II'] на саму группу $\mathfrak{A}$. Поэтому согласно теории двойственности морфизм $\chi \to \chi \circ \mathfrak{a}$ «двойствен», или «транспонирован» к $\mathfrak{a}$ и, следовательно, является изоморфизмом из X_K на подгруппу в группе характеров на G_K, ассоциированную с U_K по двойственности; эта подгруппа состоит из характеров на G_K, тривиальных на U_K.

Следствие. *В случае* [III (a)] *каждый характер на G_K^1, тривиальный на $U_K^1 = U_K \cap G_K^1$, можно однозначно продолжить до характера на G_K вида $\chi \circ \mathfrak{a}$.*

В самом деле, каждый такой характер можно однозначно продолжить до характера на G_K, тривиального на N. Последний будет тривиален на U_K и будет иметь нужный вид.

Предложение 2. *В случае* [III (b)] *обозначим через X_0 подгруппу в X_K, состоящую из таких характеров χ, что $(\chi, g)_K = 1$ при всех $g \in G_K^1$. Пусть n_1 — образующая подгруппы N в G_K. Тогда отображение $\chi \to (\chi, n_1)_K$ есть изоморфизм группы X_0 на группу всех корней из 1 в $\mathbf{C}$.*

Так как каждый характер $\chi \in X_K$ имеет конечный порядок, то $(\chi, g)_K$ всегда является корнем из 1 (для всех χ и всех g). Поскольку G_K^1 и n_1 порождают всю группу G_K, то всякий характер на G_K, тривиальный на G_K^1, однозначно определяется своим значением на элементе n_1. Отсюда в силу [II'] следует, что $\chi \to (\chi, n_1)_K$ — инъективный морфизм группы X_0 в группу корней из 1 в **C**. В частности, этот морфизм переводит каждый характер χ порядка n, содержащийся в X_0, в некоторый примитивный корень n-й степени из 1 в **C**. Согласно [III (b)], такие характеры существуют для каждого $n \geqslant 1$. Поэтому образ группы X_0 при нашем морфизме содержит все корни из 1 в **C**.

Следствие 1. *В предположениях и обозначениях предложения 2 группа G_K^1 состоит из тех элементов $g \in G_K$, для которых $(\chi, g)_K = 1$ при всех $\chi \in X_0$.*

Пусть ν — любое отличное от нуля целое число. Согласно предложению 2, существует характер $\chi \in X_0$, для которого $(\chi, n_1^\nu)_K \neq 1$, откуда $(\chi, n_1^\nu g)_K \neq 1$ при всех $g \in G_K^1$. Так как G_K является объединением классов смежности $n_1^\nu G_K^1$, $\nu \in \mathbf{Z}$, наше утверждение доказано.

Следствие 2. *В случае* [III (b)] *ядро U_K канонического морфизма $\mathfrak{a}$ содержится в G_K^1, $\mathfrak{a}$ определяет изоморфизм факторгруппы G_K^1/U_K на пересечение $\mathfrak{A}_0$ ядер в $\mathfrak{A}$ характеров $\chi \in X_0$ и $\mathfrak{a}^{-1}(\mathfrak{A}_0) = G_K^1$.*

Первое и последнее утверждения сразу вытекают из следствия 1. Положим $\mathfrak{B} = \mathfrak{a}(G_K^1)$. Ясно, что группа $\mathfrak{B}$ компактна и $\mathfrak{a}$ определяет изоморфизм факторгруппы G_K^1/U_K на $\mathfrak{B}$. Кроме того, по определению группы X_0 характер χ на $\mathfrak{A}$ принадлежит X_0 в том и только в том случае, когда он тривиален на $\mathfrak{B}$, так что $\mathfrak{B} = \mathfrak{A}_0$.

Следствие 3. *В случае* [III (b)] *каждый характер на G_K^1, тривиальный на U_K, имеет конечный порядок и может быть продолжен до характера на G_K вида $\chi \circ \mathfrak{a}$, где χ — характер на $\mathfrak{A}$.*

По следствию 2 каждый характер на G_K^1, тривиальный на U_K, можно записать в виде $\chi_1 \circ \mathfrak{a}_1$, где χ_1 — характер на $\mathfrak{A}_0$ и $\mathfrak{a}_1$ — морфизм группы G_K^1 на $\mathfrak{A}_0$, индуцированный морфизмом $\mathfrak{a}$. Поскольку χ_1 можно (хотя и неоднозначно) продолжить до характера χ на $\mathfrak{A}$ и поскольку каждый характер на $\mathfrak{A}$ имеет конечный порядок, отсюда вытекает наше утверждение.

Следствие 4. *В случае* [III (b)] *отображение $\chi \to \chi \circ \mathfrak{a}$ является биективным морфизмом группы X_K на группу характе-*

ров конечного порядка на G_K, тривиальных на U_K, и этот морфизм отображает X_0 на группу характеров конечного порядка на G_K, тривиальных на G_K^1.

Единственное, что нам надо показать,— это сюръективность наших отображений. Возьмем сначала характер ψ конечного порядка на G_K, тривиальный на G_K^1. Поскольку $\psi(n_1)$ является тогда корнем из 1 в $\mathbf{C}$, предложение 2 показывает, что существует $\chi \in X_0$, для которого $(\chi, n_1)_K = \psi(n_1)$. Но тогда $\chi \circ \mathfrak{a}$ совпадает с ψ на G_K^1 и на n_1, а значит и на G_K. Теперь возьмем любой характер ψ конечного порядка на G_K, тривиальный на U_K. По следствию 3 мы можем найти такой характер $\chi \in X_K$, что ψ совпадает с $\chi \circ \mathfrak{a}$ на G_K^1. Тогда характер $\psi' = \psi \cdot (\chi \circ \mathfrak{a})^{-1}$ тривиален на G_K^1 и имеет конечный порядок, так что в силу только что доказанного его можно записать в виде $\chi' \circ \mathfrak{a}$, чем наше доказательство и завершено.

Предложение 3. *Предположим, что выполняются условия* [I], [II] *и* [III], *и пусть $\mathfrak{a}$ — канонический морфизм из G_K в $\mathfrak{A}$. Для каждого расширения конечной степени L над K, содержащегося в K_{ab}, обозначим через $\mathfrak{B}(L)$ подгруппу в $\mathfrak{A}$, соответствующую расширению L, и положим $N(L) = \mathfrak{a}^{-1}(\mathfrak{B}(L))$. Тогда $\mathfrak{B}(L)$ является замыканием группы $\mathfrak{a}(N(L))$ в $\mathfrak{A}$; L состоит из элементов поля K_{ab}, инвариантных относительно $\mathfrak{a}(g)$ при всех $g \in N(L)$; $\mathfrak{a}$ определяет изоморфизм группы $G_K/N(L)$ на группу Галуа расширения L над K; отображение $L \to N(L)$ осуществляет взаимно однозначное соответствие между подполями L в K_{ab} конечной степени над K и открытыми подгруппами в G_K конечного индекса в G_K, содержащими U_K.*

Поскольку группа $\mathfrak{B}(L)$ открыта в $\mathfrak{A}$, группа $N(L)$ открыта в G_K. Согласно [II″], группа $\mathfrak{a}(G_K)$ плотна в $\mathfrak{A}$, откуда следует, что группа $\mathfrak{a}(N(L))$ плотна в $\mathfrak{B}(L)$ и что $\mathfrak{a}$ определяет изоморфизм группы $G_K/N(L)$ на группу $\mathfrak{A}/\mathfrak{B}(L)$, которая совпадает с группой Галуа расширения L над K. Поскольку действие группы $\mathfrak{A}$ на K_{ab} непрерывно, каждый элемент поля K_{ab}, инвариантный относительно $\mathfrak{a}(N(L))$, инвариантен относительно ее замыкания $\mathfrak{B}(L)$, так что он лежит в L. Наконец, пусть H — любая открытая подгруппа конечного индекса n в G_K, содержащая U_K. Пусть ψ_i, $1 \leqslant i \leqslant n$, — все различные характеры на G_K, тривиальные на H. Тогда H является пересечением ядер этих характеров. По предложению 1 в случае [III (a)] и по следствию 4 предл. 2 в случае [III (b)] мы можем записать $\psi_i = \chi_i \circ \mathfrak{a}$, $1 \leqslant i \leqslant n$, где χ_i — характеры на $\mathfrak{A}$. В силу [II′] характеры χ_i однозначно определены; они образуют конечную подгруппу в X_K, ибо ψ_i образуют конечную подгруппу в группе всех характеров на G_K. Обозначим через

$\mathfrak{B}$ пересечение ядер характеров χ_i на $\mathfrak{A}$. Это — открытая подгруппа индекса n в $\mathfrak{A}$, поэтому подполе L в K_{ab}, соответствующее подгруппе $\mathfrak{B}$, имеет степень n над K. Ясно, что $H = \mathfrak{a}^{-1}(\mathfrak{B})$, откуда $H = N(L)$. Доказательство завершено.

Следствие. *В случае* [III (b)] *обозначим через* K_0 *подполе в* K_{ab}, *соответствующее подгруппе* $\mathfrak{A}_0 = \mathfrak{a}(G_K^1)$ *в* $\mathfrak{A}$. *Тогда для всякого целого числа* $\nu \geqslant 1$ *поле* K_0 *содержит одно и только одно расширение* K_ν *поля* K *степени* ν; K_ν *является циклическим расширением поля* K, *связанным с любым из характеров порядка* ν, *содержащихся в* X_0; $N(K_\nu)$ *совпадает с подгруппой в* G_K, *порожденной подгруппой* G_K^1 *и элементом* n_1^ν.

По следствию 2 предл. 2 имеем $G_K^1 = \mathfrak{a}^{-1}(\mathfrak{A}_0)$. Поэтому для таких L и $N(L)$, как в предложении 3, $L \subset K_0$ в том и только в том случае, когда $N(L) \supset G_K^1$. Отсюда следует, что G_K^1 и n_1^ν порождают всю группу $N(L)$, если ν — индекс подгруппы $N(L)$ в G_K. По предложению 3 L является циклическим расширением степени ν над K, и если χ — характер на $\mathfrak{A}$, связанный с L, то $N(L)$ есть ядро морфизма $\chi \circ \mathfrak{a}$, так что χ принадлежит к X_0 и имеет порядок ν. Обратно, для такого характера χ ядро морфизма $\chi \circ \mathfrak{a}$ порождено подгруппой G_K^1 и элементом n_1^ν, так что L является циклическим расширением, связанным с χ.

Теперь рассмотрим циклическое расширение K' поля K, содержащееся в K_{sep}. Мы используем введенные выше обозначения $\mathfrak{G}'$, $\mathfrak{G}'^{(1)}$, $\mathfrak{A}' = \mathfrak{G}'/\mathfrak{G}'^{(1)}$. Кроме того, обозначим через ρ морфизм ограничения из $\mathfrak{G}'$ в $\mathfrak{G}$, равно как и морфизм ограничения из $\mathfrak{A}'$ в $\mathfrak{A}$. Так как поле K' циклично над K, то $\mathfrak{G}'$ — открытая нормальная подгруппа в $\mathfrak{G}$ с циклической факторгруппой. Следовательно, $\mathfrak{G} \supset \mathfrak{G}' \supset \mathfrak{G}^{(1)} \supset \mathfrak{G}'^{(1)}$, и $\mathfrak{G}'^{(1)}$ является нормальной подгруппой в $\mathfrak{G}$. Для каждого $\lambda \in \mathfrak{G}$ внутренний автоморфизм $\sigma \longrightarrow \lambda\sigma\lambda^{-1}$ индуцирует на группе $\mathfrak{G}'$ автоморфизм этой группы. Поэтому для любого характера χ' на $\mathfrak{G}'$ мы можем определить характер χ'^{λ} на $\mathfrak{G}'$, полагая $\chi'^{\lambda}(\sigma') = \chi'(\lambda\sigma'\lambda^{-1})$ для каждого $\sigma' \in \mathfrak{G}'$. Ясно, что $\chi'^{\lambda} = \chi'$, если $\lambda \in \mathfrak{G}'$, так что отображение $\chi' \to \chi'^{\lambda}$ определяет действие группы Галуа $\mathfrak{G}/\mathfrak{G}'$ поля K' над K на группе $X_{K'}$ всех характеров на $\mathfrak{G}'$.

Далее, предположим, что заданы канонические спаривания $(\chi, g)_K$, $(\chi', g')_{K'}$ групп X_K с G_K и $X_{K'}$ с $G_{K'}$, причем оба спаривания удовлетворяют условиям [I], [II], [III]. Для упрощения обозначений положим $G = G_K$, $G' = G_{K'}$, $G_1 = G_K^1$, $G_1' = G_{K'}^1$. Обозначим через $\mathfrak{a}$ и $\mathfrak{a}'$ соответственно канонические морфизмы группы G в $\mathfrak{A}$ и группы G' в $\mathfrak{A}'$, определяемые этими спариваниями.

Предположим также, что $\mathfrak{G}$ действует на G' и что это действие, записываемое для любого $\lambda \in \mathfrak{G}$ как $g' \to g'^{\lambda}$, удовлетворяет следующему условию:

[IV] (i) *Для* $\lambda \in \mathfrak{G}'$ *отображение* $g' \to g'^{\lambda}$ *тождественно на* G'.

(ii) *Для всякого* $\lambda \in \mathfrak{G}$ *отображение* $g' \to g'^{\lambda}$ *есть автоморфизм групп* G' *и* $g'^{\lambda} g'^{-1} \in G'_1$ *при всех* $g' \in G'$.

(iii) *Для всех* $\chi' \in X_{K'}$, $g' \in G'$ *и* $\lambda \in \mathfrak{G}$ *имеем*

$$(\chi'^{\lambda}, g'^{\lambda})_{K'} = (\chi', g')_{K'}.$$

Наконец, предположим, что задан некоторый морфизм F из G' в G, удовлетворяющий следующему условию:

[V] (i) *Для всех* $g' \in G'$ *и всех* $\lambda \in \mathfrak{G}$ *имеем* $F(g'^{\lambda}) = F(g')$.

(ii) *Для всех* $\chi \in X_K$ *и всех* $g' \in G'$ *имеем*

$$(\chi \circ \rho, g')_{K'} = (\chi, F(g'))_K.$$

Ясно, что [V (ii)] можно записать также в виде $\rho \circ \mathfrak{a}' = \mathfrak{a} \circ F$.

Предложение 4. *Пусть* K' *— циклическое расширение поля* K, *и пусть* $\mathfrak{a}$, $\mathfrak{a}'$ *— канонические морфизмы, определенные соответственно каноническими спариваниями групп* X_K *с* G *и* $X_{K'}$ *с* G', *причем для обоих спариваний выполняются условия* [I], [II], [III]. *Предположим, что группа Галуа* $\mathfrak{G}$ *расширения* K_{sep} *действует на* G', *что* F *— морфизм из* G' *в* G *и что выполняются условия* [IV] *и* [V]. *Тогда* $U \cap F(G'_1) = F(U' \cap G'_1)$, *где* U, U' *— ядра морфизмов* $\mathfrak{a}$ *и* $\mathfrak{a}'$. *Кроме того,* $U \cap F(G') = F(U')$, *если либо* G' *удовлетворяет условию* [III (a)], *либо* G, G' *удовлетворяют условию* [III (b)] *и* F *не отображает* G' *в* G_1.

Согласно [V (ii)], имеем $\rho \circ \mathfrak{a}' = \mathfrak{a} \circ F$. Поэтому $F(U')$ содержится в U, а следовательно, в $U \cap F(G')$, и если положить $U'_1 = U' \cap G'_1$, то $F(U'_1)$ содержится в $U \cap F(G'_1)$. Пусть ψ — характер на G, тривиальный на $F(U'_1)$. Тогда $\psi \circ F$ — характер на G', тривиальный на U'_1. Применяя теперь следствие предл. 1 в случае [III (a)] и следствие 3 предл. 2 в случае [III (b)] к характеру, индуцированному на G'_1 морфизмом $\psi \circ F$, мы видим, что $\psi \circ F$ совпадает на G'_1 с некоторым характером вида $\chi' \circ \mathfrak{a}'$, где $\chi' \in X_{K'}$. Другими словами, при всех $g' \in G'_1$ имеем

$$\psi(F(g')) = (\chi', g')_{K'}.$$

Согласно [IV (ii)], это равенство сохранится, если заменить g' на $g'^{\lambda} g'^{-1}$ с любым $g' \in G'$ и любым $\lambda \in \mathfrak{G}$. Ввиду [V (i)] это дает

$$1 = (\chi', g'^{\lambda} g'^{-1})_{K'} = (\chi', g'^{\lambda})_{K'} \cdot (\chi', g')_{K'}^{-1},$$

поэтому в силу [IV (iii)]

$$(\chi',\ g')_{K'} = (\chi',\ g'^{\lambda})_{K'} = (\chi'^{\lambda^{-1}},\ g')_{K'}.$$

С учетом [II] это показывает, что характер χ' инвариантен относительно λ для любого $\lambda \in \mathfrak{G}$; более точно, он инвариантен относительно всех автоморфизмов группы $\mathfrak{G}'$, индуцированных на $\mathfrak{G}'$ внутренними автоморфизмами группы $\mathfrak{G}$. Поэтому то же самое должно быть верно для ядра $\mathfrak{H}'$ характера χ', так что $\mathfrak{H}'$, будучи открытой подгруппой в $\mathfrak{G}'$ с циклической факторгруппой, является нормальной подгруппой в $\mathfrak{G}$. Пусть α — какой-нибудь представитель в $\mathfrak{G}$ образующей циклической группы $\mathfrak{G}/\mathfrak{G}'$, и пусть β — какой-нибудь представитель в $\mathfrak{G}'$ образующей факторгруппы $\mathfrak{G}'/\mathfrak{H}'$. Тогда $\mathfrak{H}'$ и β порождают $\mathfrak{G}'$, а $\mathfrak{G}'$ и α порождают $\mathfrak{G}$, следовательно, $\mathfrak{H}'$, β и α порождают $\mathfrak{G}$. Таким образом, группа $\mathfrak{G}/\mathfrak{H}'$ порождается образами α', β' в $\mathfrak{G}/\mathfrak{H}'$ элементов α, β. Поскольку характер χ' инвариантен относительно отображения $\sigma' \to \alpha\sigma'\alpha^{-1}$, то при $\sigma' = \beta$ мы получаем, что $\chi'(\beta) = \chi'(\alpha\beta\alpha^{-1})$. Отсюда видно, что $\alpha\beta\alpha^{-1}\beta^{-1}$ лежит в ядре $\mathfrak{H}'$ характера χ', так что α' коммутирует с β' в $\mathfrak{G}/\mathfrak{H}'$. Следовательно, группа $\mathfrak{G}/\mathfrak{H}'$ коммутативна. Поэтому характер на $\mathfrak{G}'/\mathfrak{H}'$, определяемый характером χ', можно продолжить до характера на $\mathfrak{G}/\mathfrak{H}'$. Иными словами, χ' можно продолжить до характера χ на $\mathfrak{G}$, так что мы имеем $\chi' = \chi \circ \rho$. Ввиду [V (ii)] из определения χ' следует, что

$$\psi(F(g')) = (\chi \circ \rho,\ g')_{K'} = (\chi,\ F(g'))_{K'}$$

при всех $g' \in G'_1$. Другими словами, характер ψ совпадает с $\chi \circ a$ на $F(G'_1)$, так что он тривиален на $U \cap F(G'_1)$. Поскольку $F(U'_1)$ — компактная подгруппа в G и поскольку, как уже доказано, каждый характер ψ на G, тривиальный на $F(U'_1)$, тривиален на $U \cap F(G'_1)$, мы видим, что $F(U'_1) \supset U \cap F(G'_1)$. Ввиду доказанного выше этим завершается доказательство первой части нашего предложения.

Если G и G' удовлетворяют условию [III (b)], то мы имеем $U' \subset G'_1$ и $U \subset G_1$ по следствию 2 предл. 2. Если F не отображает G' в G_1, то мы имеем $F^{-1}(G_1) = G'_1$ по лемме 2. Поэтому $U \cap F(G'_1)$ совпадает с $U \cap F(G')$, чем и завершается доказательство второй части для этого случая. Предположим теперь, что $G' = G'_1 \times N'$, причем группа N' изоморфна $\mathbf{R}$. Как мы уже убедились, для каждого $\chi' \in X_{K'}$ характер группы N', индуцированный на ней морфизмом $\chi' \circ a'$, будучи характером конечного порядка, тривиален, так что $N' \subset U'$, откуда $U' = U'_1 \times N'$. Те же рассуждения, примененные к характеру, индуцированному на N' морфизмом $\chi \circ a \circ F$ при $\chi \in X_K$, показывают, что $F(N') \subset U$, а поэтому

$$U \cap F(G') = (U \cap F(G'_1)) \cdot F(N') = F(U'_1)\,F(N') = F(U').$$

§ 2. ГРУППА БРАУЭРА ЛОКАЛЬНОГО ПОЛЯ

Начиная с этого места, K будет локальным полем. Как и в главе IX, мы обозначаем через $B(K)$ группу Брауэра этого поля и через $H(K)$ группу его классов факторов. Мы отождествляем эти группы друг с другом с помощью теоремы 3 гл. IX-3. В гл. IX-4 мы уже вычислили эти группы в случаях $K = \mathbf{R}$, $K = \mathbf{C}$, и мы начнем с того, что напомним полученные там результаты и введем некоторые дополнительные обозначения, которые будут полезны в следующей главе. Так как группа $B(\mathbf{R})$ состоит из двух элементов, то существует единственный изоморфизм η этой группы на подгруппу $\{\pm 1\}$ в $\mathbf{C}^\times$. Для любой простой алгебры A над $\mathbf{R}$ положим $h(A) = \eta(\mathrm{Cl}(A))$. Мы будем называть $h(A)$ *инвариантом Хассе* алгебры A; этот инвариант равен $+1$ или -1 в соответствии с тем, тривиальна алгебра A или нет. Группа $B(\mathbf{C})$ состоит только из одного элемента, и мы обозначим через η единственное ее отображение в $\{+1\}$; для каждой простой алгебры A над $\mathbf{C}$ мы пишем $h(A) = \eta(\mathrm{Cl}(A)) = +1$ и называем это *инвариантом Хассе* алгебры A. В случае $K = \mathbf{R}$ группа Галуа $\mathfrak{G}$ поля K_{sep} над K состоит из тождественного автоморфизма ε и автоморфизма $x \to \bar{x}$ поля $\mathbf{C}$ над $\mathbf{R}$; в случае $K = \mathbf{C}$ имеем $\mathfrak{G} = \{\varepsilon\}$. Для каждого характера χ на $\mathfrak{G}$ и каждого $\theta \in K^\times$ в гл. IX-4 был определен класс факторов $\{\chi, \theta\}$. Отождествляя, как сказано выше, $H(K)$ с $B(K)$, мы можем теперь для $K = \mathbf{R}$ или $\mathbf{C}$ написать

$$(\chi, \theta)_K = \eta(\{\chi, \theta\}).$$

Ясно, что это равно 1, если $K = \mathbf{C}$ или если $K = \mathbf{R}$ и χ — тривиальный характер на $\mathfrak{G}$; в случае когда $K = \mathbf{R}$ и χ — нетривиальный характер на $\mathfrak{G}$, как показывают результаты гл. IX-4, $(\chi, \theta)_K$ равно $+1$ или -1, в соответствии с тем, положительно или отрицательно θ. Без труда проверяется, что определенное таким образом спаривание является каноническим спариванием группы X_K с $K^\times$ в смысле § 1 и что оно удовлетворяет условиям [I], [II], [III (a)]; ядро U_K канонического морфизма совпадает с $\mathbf{C}^\times$ в случае $K = \mathbf{C}$ и равно $\mathbf{R}_+^\times$ в случае $K = \mathbf{R}$.

Начиная с этого места, K будет всегда обозначать коммутативное p-поле, но иногда мы будем отмечать справедливость некоторых наших результатов для $K = \mathbf{R}$ или $\mathbf{C}$. Как обычно, через R обозначается максимальное компактное подкольцо в K, через q — модуль p-поля K, через P — максимальный идеал в R и через π — простой элемент в K. Кроме того, мы используем обозначения $\bar{K}$, K_{sep}, $\mathfrak{G}$, K_{ab}, $\mathfrak{A}$ из § 1.

Обозначим через $\mathfrak{M}$ множество всех корней из 1 в $\overline{K}$, порядок которых взаимно прост с p. Ясно, что $\mathfrak{M}$ — подгруппа в $K_{\text{sep}}^{\times}$. Положим $K_0 = K(\mathfrak{M})$, и пусть $\mathfrak{H}_0$ — замкнутая подгруппа в $\mathfrak{G}$, соответствующая полю K_0, т. е. состоящая из тех автоморфизмов поля K_{sep} над K, которые оставляют инвариантными все элементы поля K_0, или, что то же самое, все элементы множества $\mathfrak{M}$. По следствию 2 теор. 7 гл. I-4 каждое конечное подмножество в $\mathfrak{M}$ порождает над K некоторое неразветвленное расширение поля K. Обратно, каждое расширение поля K, содержащееся в неразветвленном расширении, само неразветвлено, так что по следствию 3 теор. 7 гл. I-4 оно порождается некоторым конечным подмножеством в $\mathfrak{M}$. Кроме того, по тому же следствию существует одно и только одно такое расширение K_n степени n над K для каждого $n \geqslant 1$. Следовательно, K_0 есть объединение полей K_n, $n \geqslant 1$. Снова используя следствие 2 той же теоремы, получаем, что отображение $\mu \to \mu^q$ группы $\mathfrak{M}$ в себя является автоморфизмом этой группы и что для каждого $n \geqslant 1$ существует один и только один автоморфизм поля K_n над K, а именно автоморфизм Фробениуса, который совпадает с этим отображением на $\mathfrak{M} \cap K_n$. Отсюда, очевидно, следует, что существует один и только один автоморфизм φ_0 поля K_0 над K, который индуцирует на $\mathfrak{M}$ отображение $\mu \to \mu^q$. Этот автоморфизм мы будем называть *автоморфизмом Фробениуса* поля K_0 над K, и каждый автоморфизм φ поля K_{sep} над K, который на K_0 индуцирует φ_0, будем называть *автоморфизмом Фробениуса* поля K_{sep} над K. Таким образом, автоморфизмы Фробениуса поля K_{sep} над K образуют класс смежности $\mathfrak{H}_0\varphi$ в $\mathfrak{G}$.

Определение 1. *Характер χ на $\mathfrak{G}$ называется неразветвленным, если неразветвлено связанное с ним циклическое расширение поля K. Множество всех неразветвленных характеров на $\mathfrak{G}$ будем обозначать через X_0.*

Ввиду сказанного выше ясно, что характер χ неразветвлен в том и только в том случае, когда циклическое расширение, связанное с χ, содержится в K_0, или, что то же самое, когда характер χ тривиален на подгруппе $\mathfrak{H}_0$ в $\mathfrak{G}$, соответствующей расширению K_0 над K. Поэтому X_0 является подгруппой в группе X_K всех характеров на $\mathfrak{G}$.

Предложение 5. *Пусть φ — некоторый автоморфизм Фробениуса поля K_{sep} над K. Тогда отображение $\chi \to \chi(\varphi)$ есть изоморфизм группы X_0 неразветвленных характеров на $\mathfrak{G}$ на группу всех корней из 1 в $\mathbf{C}$; этот изоморфизм не зависит от выбора φ.*

Ясно, что это отображение является морфизмом группы X_0 в группу корней из 1 в $\mathbf{C}$. В указанных выше обозначениях циклическое расширение поля K, связанное с неразветвленным характером χ порядка n, совпадает с K_n. Так как φ индуцирует на K_n автоморфизм Фробениуса поля K_n над K, порождающий группу Галуа поля K_n над K, то $\chi(\varphi)$ есть примитивный корень n-й степени из 1. Поэтому морфизм из формулировки нашего предложения и инъективен, и сюръективен. Последнее утверждение предложения вытекает из того факта, что два автоморфизма Фробениуса могут отличаться лишь на элемент группы $\mathfrak{H}_0$, а каждый неразветвленный характер тривиален на $\mathfrak{H}_0$.

Теорема 1. *Пусть K — коммутативное p-поле, π — простой элемент в K и X_0 — группа неразветвленных характеров на $\mathfrak{G}$. Тогда отображение $\chi \to \{\chi, \pi\}$ есть изоморфизм группы X_0 на группу $H(K)$ классов факторов поля K, и этот изоморфизм не зависит от выбора π.*

Мы можем отождествить $H(K)$ с группой Брауэра $B(K)$ поля K. Каждый элемент группы $B(K)$, т. е. каждый класс простых алгебр над K, содержит одну и только одну алгебру с делением над K. Как уже отмечалось в гл. IX-4 и еще раз в гл. X-2, из предложения 5 гл. I-4 вытекает, что такую алгебру можно записать в виде $[K_n/K; \chi, \pi_1]$, где n^2 — размерность алгебры над K, χ — некоторый характер, связанный с K_n, и π_1 — подходящий простой элемент в K. Поэтому нашей алгебре отвечает класс факторов $\{\chi, \pi_1\}$. Комбинируя предложение 10 гл. IX-4 с предложением 3 гл. VIII-1, мы видим, что этот класс факторов не зависит от выбора π_1, так что он совпадает с $\{\chi, \pi\}$. Следовательно, отображение $\chi \to \{\chi, \pi\}$ есть сюръективный морфизм группы X_0 на группу $H(K)$. Поскольку K_n является неразветвленным расширением степени n над K, его модулярная степень над K равна n. Поэтому π не может содержаться в $N_{K_n/K}(K_n^\times)$, если $n \neq 1$. Отсюда, снова используя предложение 10 гл. IX-4, получаем, что $\{\chi, \pi\} \neq 1$ для χ, связанного с K_n, если только $n \neq 1$, т. е. если $\chi \neq 1$. Доказательство завершено.

Следствие 1. *Пусть K и π таковы, как в теореме 1, и пусть K_n — неразветвленное расширение степени n над K и χ — некоторый характер, связанный с K_n. Тогда $[K_n/K; \chi, \pi]$ — алгебра с делением над K.*

Во всяком случае это — алгебра вида $M_m(D)$, где D — некоторая алгебра с делением над K. Если d^2 — размерность алгебры D над K, то D можно записать в виде $[K_d/K; \chi', \pi]$, где χ' — харак-

тер, связанный с K_d. По теореме 1 отсюда следует, что $\chi' = \chi$, поэтому $n = d$ и $m = 1$.

Следствие 2. *Пусть* φ — *автоморфизм Фробениуса поля* K_{sep} *над* K. *Тогда существует один и только один изоморфизм* η *группы* $H(K)$ *на группу всех корней из* 1 *в* $\mathbf{C}$, *для которого* $\eta(\{\chi, \pi\}) = \chi(\varphi)$ *при всех* $\chi \in X_0$, *и этот изоморфизм не зависит от выбора* π *и* φ.

Это сразу вытекает из теоремы 1 в сочетании с предложением 5

Следствие 3. *Во введенных выше обозначениях пусть* X_K — *группа всех характеров на* $\mathfrak{G}$. *Для всех* $\chi \in X_K$ *и всех* $\theta \in K^\times$ *положим*

$$(\chi, \theta)_K = \eta(\{\chi, \theta\}).$$

Это равенство определяет спаривание между X_K *и* $K^\times$, *которое удовлетворяет условиям* [I] *и* [III (b)] § 1.

Условие [I (i)] выполняется по предложению 8 гл. IX-4. Условие [I (ii)'] выполняется по предложению 10 гл. IX-4 и предложению 5 гл. VIII-1. Что касается условия [III (b)], то здесь можно взять $G_K = K^\times$, $G'_K = R^\times$, а в качестве N взять подгруппу в $K^\times$, порожденную элементом π. Тогда [III (b)] выполняется, если брать в качестве χ любой характер, связанный с неразветвленным расширением K_n над K степени n, что сразу вытекает из предложения 10 гл. IX-4 и предложения 3 гл. VIII-1.

Следствие 4. *Для всех* $\chi \in X_0$ *и всех* $\theta \in K^\times$ *имеем* $(\chi, \theta)_K = \chi(\varphi)^{\operatorname{ord}\theta}$. *Если* π — *любой простой элемент в* K, *то* $(\chi, \pi)_K = \chi(\varphi)$.

Последнее утверждение является переформулировкой следствия 2. Поэтому первое утверждение выполняется при $\theta = \pi$, а также, как показано при доказательстве следствия 3, при $\theta \in R^\times$. Отсюда сразу вытекает справедливость этого утверждения в общем случае.

Следствие 5. *Пусть* K_1 — *некоторое поле, изоморфное полю* K, $\overline{K}_1$ — *алгебраическое замыкание поля* K_1 *и* λ — *изоморфизм поля* $\overline{K}$ *на поле* $\overline{K}_1$, *переводящий* K *в* K_1. *Для каждого характера* χ *на* $\mathfrak{G}$ *обозначим через* χ^λ *его преобразование с помощью* λ, *т. е. характер группы Галуа* $\mathfrak{G}_1$ *поля* $(K_1)_{\text{sep}}$ *над* K_1, *для которого* $\chi^\lambda(\sigma_1) = \chi(\lambda\sigma_1\lambda^{-1})$ *при всех* $\sigma_1 \in \mathfrak{G}_1$. *Тогда* $(\chi, \theta)_K = (\chi^\lambda, \theta^\lambda)_{K_1}$ *при всех* $\chi \in X_K$ *и всех* $\theta \in K^\times$.

Это сразу вытекает из следствия 2, ибо, очевидно, λ переводит простой элемент в K в простой элемент в K_1 и преобразует авто-

морфизм Фробениуса поля K_{sep} над K в автоморфизм Фробениуса поля $(K_1)_{\text{sep}}$ над K_1.

Начиная с этого места, спаривание группы X_K с $K^\times$, определенное в следствии 3, будем называть *каноническим спариванием* для K. При помощи этого спаривания, как объяснялось в § 1, строится некоторый морфизм $\mathfrak{a}$ группы $K^\times$ в группу Галуа $\mathfrak{A}$ поля K_{ab} над K, который мы будем называть *каноническим морфизмом* для K; он определяется соотношением $(\chi, \theta)_K = \chi(\mathfrak{a}(\theta))$, которое должно выполняться для всех $\chi \in X_K$ и всех $\theta \in K^\times$. Следствие 4 теор. 1 показывает, что $\mathfrak{a}(\pi)$ индуцирует на K_0 автоморфизм Фробениуса поля K_0 над K, где π — любой простой элемент в K.

Поскольку мы отождествляем группу Брауэра $B(K)$ с группой $H(K)$, рассматривавшейся в теореме 1 и ее следствиях, то отображение η, определенное в следствии 2 теор. 1, можно считать изоморфизмом группы $B(K)$ на группу корней из 1 в $\mathbf{C}$. Для каждой простой алгебры A над K введем число $h(A) = \eta(\mathrm{Cl}(A))$; мы будем называть это число *инвариантом Хассе* алгебры A; этот инвариант равен 1 в том и только в том случае, когда алгебра A тривиальна.

Теорема 2. *Пусть K' — расширение конечной степени поля K, содержащееся в $\overline{K}$; $\mathfrak{G}$, $\mathfrak{G}'$ — группы Галуа полей K_{sep} над K и K'_{sep} над K' соответственно; ρ — морфизм ограничения из $\mathfrak{G}'$ в $\mathfrak{G}$. Тогда для каждого $\chi \in X_K$ и каждого $\theta' \in K'^\times$ имеем*

$$(\chi \circ \rho, \theta')_{K'} = (\chi, \mathrm{N}_{K'/K}(\theta'))_K. \tag{2}$$

Пусть f — модулярная степень поля K' над K. Тогда модуль поля K' равен q^f, и если φ, φ' — автоморфизмы Фробениуса полей K_{sep} над K и K'_{sep} над K' соответственно, то φ' совпадает с φ^f на группе $\mathfrak{M}$ всех корней из 1 в $\overline{K}$, порядок которых взаимно прост с p, а следовательно, и на $K_0 = K(\mathfrak{M})$, так что $\rho(\varphi')\varphi^{-f}$ содержится в подгруппе $\mathfrak{H}_0$ в $\mathfrak{G}$, соответствующей полю K_0.

Предположим сначала, что характер χ в (2) неразветвлен и, следовательно, тривиален на $\mathfrak{H}_0$, так что $\chi(\rho(\varphi')) = \chi(\varphi)^f$. Как было замечено в гл. IX-4, циклическое расширение поля K', связанное с $\chi \circ \rho$, является композитом поля K' и циклического расширения поля K, связанного с χ. Так как последнее расширение неразветвлено, а значит порождается элементами из $\mathfrak{M}$, то же самое верно и для первого расширения, так что характер $\chi \circ \rho$ неразветвлен. Теперь мы можем к обеим частям равенства (2) применить следствие 4 теор. 1. Согласно этому следствию, левая часть равна $\chi(\rho(\varphi'))^r$ с $r = \mathrm{ord}_{K'}(\theta')$, а правая часть равна $\chi(\varphi)^s$ с $s =$

$= \mathrm{ord}_K(\mathrm{N}_{K'/K}(\theta'))$, откуда $s = fr$ по формуле (2) гл. VIII-1. Итак, равенство (2) для неразветвленного характера χ доказано.

В общем случае обозначим через n порядок характера χ. Поскольку обе части равенства (2) не меняются при замене θ' на $\theta'\eta'^n$ с $\eta' \in K'^\times$, можно считать, что $r = \mathrm{ord}_{K'}(\theta') \neq 0$. Как было только что показано, если χ_1 — произвольный неразветвленный характер на $\mathfrak{G}$, то $(\chi_1 \circ \rho, \theta')_{K'} = \chi_1(\varphi)^{fr}$. Ввиду предложения 5 χ_1 можно выбрать так, чтобы $\chi_1(\varphi)^{fr}$ равнялось любому заданному корню из 1 в $\mathbf{C}$, в частности левой части равенства (2). Но это равенство уже доказано для неразветвленных характеров, поэтому будет достаточно, после замены χ на $\chi\chi_1^{-1}$, доказать наш результат при том дополнительном предположении, что левая часть равна 1. Предположив это, обозначим через L циклическое расширение поля K, связанное с χ. Тогда циклическим расширением поля K', связанным с $\chi \circ \rho$, будет композит L' полей K' и L. Так как левая часть равенства (2) равна 1, то предложение 10 гл. IX-4 показывает, что существует такое $\eta' \in L'$, что $\theta' = \mathrm{N}_{L'/K'}(\eta')$. Отсюда в силу результатов гл. III-3 вытекает, что $\mathrm{N}_{K'/K}(\theta') = \mathrm{N}_{L'/K}(\eta') = \mathrm{N}_{L/K}(\mathrm{N}_{L'/L}(\eta'))$, и то же самое предложение показывает, что правая часть равенства (2) равна 1. Доказательство теоремы закончено.

Следствие 1. *Если* $\mathfrak{a}$, $\mathfrak{a}'$ — *канонические морфизмы для* K *и для* K' *соответственно, то* $\rho \circ \mathfrak{a}' = \mathfrak{a} \circ \mathrm{N}_{K'/K}$.

В силу наших определений это не что иное, как другой способ записи равенства (2).

Следствие 2. *Пусть* K, K' *таковы, как в теореме* 2. *Обозначим через* n *степень поля* K' *над* K. *Тогда для каждой простой алгебры* A *над* K *имеем* $h(A_{K'}) = h(A)^n$.

По теореме 1 класс факторов, соответствующий алгебре A, можно записать как $\{\chi, \pi\}$. По формуле (7) гл. IX-4 морфизм ограничения из $H(K)$ в $H(K')$ отображает класс $\{\chi, \theta\}$ на класс $\{\chi \circ \rho, \theta\}$ для каждого $\chi \in X_K$ и каждого $\theta \in K^\times$; кроме того, при $\theta \in K^\times$ имеем $\mathrm{N}_{K'/K}(\theta) = \theta^n$. Согласно теореме 2, отсюда вытекает, что $h(A_{K'}) = (\chi \circ \rho, \pi)_{K'} = (\chi, \pi^n)_K = h(A)^n$.

Следствие 3. *Если* χ — *нетривиальный характер на* $\mathfrak{G}$, *то* $\theta \to (\chi, \theta)_K$ — *нетривиальный характер на* $K^\times$.

Обозначим через n и d порядки этих двух характеров. Ясно, что d делит n. Обозначим через L циклическое расширение поля K, связанное с χ. Пусть χ_1 — неразветвленный характер порядка n на $\mathfrak{G}$, и пусть K_n — неразветвленное расширение степени n над K.

Положим $D = [K_n/K;\ \chi_1,\ \pi]$. По следствию 2 теор. 1 имеем $h(D) = \chi_1(\varphi)$, так что $h(D)$ является примитивным корнем n-й степени из 1. Поэтому согласно следствию 2 $h(D_L) = h(D)^n = 1$, так что алгебра D_L тривиальна. Другими словами, D обладает L-представлением в $M_n(L)$. По предложению 9 гл. IX-4 класс факторов, связанный с D, можно поэтому записать в виде $\{\chi, \theta\}$, где $\theta \in K^\times$, и мы имеем $h(D) = (\chi, \theta)_K$. Значит, $d = n$. Тем самым показано, что наше каноническое спаривание удовлетворяет условию [II] § 1.

Следствие 4. *Если L — любое циклическое расширение степени n над K, то $N_{L/K}(L^\times)$ является открытой подгруппой индекса n в $K^\times$.*

В самом деле, по предложению 10 гл. IX-4 эта подгруппа является ядром морфизма $\theta \to (\chi, \theta)_K$, где χ — характер *на* $\mathfrak{G}$, связанный с L, а мы только что показали, что порядок этого характера равен n.

Если $K' = K$ или $\chi = 1$, то формула (2) теоремы 2 тривиальна; если K' — циклическое расширение поля K, связанное с χ, то равенство (2) эквивалентно предложению 10 гл. IX-4, ибо в этом случае $\chi \circ \rho = 1$. Как сразу видно, никаких других случаев и не может быть, если K есть $\mathbf{R}$-поле. Поэтому теорема 2 справедлива и для $K = \mathbf{R}$ или $\mathbf{C}$, а стало быть, верны и ее следствия.

Предложение 6. *Характер χ на $\mathfrak{G}$ неразветвлен тогда и только тогда, когда $(\chi, \theta)_K = 1$ при всех $\theta \in R^\times$.*

Обозначим через X_0' группу характеров, обладающих последним свойством. Как и прежде, пусть X_0 — группа неразветвленных характеров на $\mathfrak{G}$. По следствию 4 теор. 1 имеем $X_0 \subset X_0'$. По предложению 2 § 1 отображение $\chi \to (\chi, \pi)_K$ есть изоморфизм группы X_0' на группу всех корней из 1 в $\mathbf{C}$. Из теоремы 1 в сочетании с предложением 5 следует, что этот изоморфизм индуцирует на X_0 изоморфизм группы X_0 на ту же самую группу. Поэтому $X_0' = X_0$.

Следствие. *Циклическое расширение L поля K неразветвлено тогда и только тогда, когда $N_{L/K}(L^\times)$ содержит $R^\times$.*

Ввиду предложения 10 гл. IX-4 это сразу получается, если к характеру на $\mathfrak{G}$, связанному с L, применить предложение 6.

§ 3. КАНОНИЧЕСКИЙ МОРФИЗМ

Итак, мы показали, что для канонического спаривания $(\chi, \theta)_K$ выполнены условия [I], [II], [III (b)], сформулированные в § 1, а также что подгруппа X_0 в X_K, определенная с помощью этого

спаривания в § 1, совпадает в рассматриваемой сейчас ситуации с группой X_0 неразветвленных характеров на $\mathfrak{G}$. Как и в § 1, будем теперь обозначать через U_K ядро канонического морфизма $\mathfrak{a}$ группы $K^\times$ в $\mathfrak{A}$. Основной результат этого параграфа состоит в том, что $U_K = \{1\}$. Применяя здесь результаты § 1, следует иметь в виду, что G_K^1 нужно теперь заменить на $R^\times$, n_1 — на простой элемент π в K и N — на подгруппу в $K^\times$, порожденную элементом π. Следствие 2 предложения 2 § 1 показывает, что U_K содержится в $R^\times$ и что $\mathfrak{a}$ определяет морфизм группы $R^\times$ на пересечение $\mathfrak{A}_0$ ядер характеров $\chi \in X_0$, рассматриваемых как характеры на $\mathfrak{A}$. Здесь X_0 согласно предложению 6 § 2 состоит из тех характеров на $\mathfrak{G}$, которые тривиальны на подгруппе $\mathfrak{H}_0$ в $\mathfrak{G}$, соответствующей объединению K_0 всех неразветвленных расширений поля K. Поэтому $\mathfrak{A}_0$ является образом группы $\mathfrak{H}_0$ в $\mathfrak{A}$, т. е. подгруппой в $\mathfrak{A}$, соответствующей подполю K_0 в K_{ab}, или, другими словами, группой Галуа поля K_{ab} над K_0.

Предложение 7. *Пусть K_0 — объединение всех неразветвленных расширений поля K, содержащихся в K_{sep}; φ_0 — автоморфизм Фробениуса поля K_0 над K; $\mathfrak{a}$ — канонический морфизм группы $K^\times$ в группу Галуа $\mathfrak{A}$ поля K_{ab} над K. Тогда для каждого $\theta \in K^\times$ автоморфизм $\mathfrak{a}(\theta)$ индуцирует на K_0 автоморфизм φ_0^r, где $r = \mathrm{ord}(\theta)$.*

В самом деле, следствие 4 теор. 1 § 2 означает, что $\chi(\mathfrak{a}(\theta)) = \chi(\varphi)^r$ для любого $\chi \in X_0$, где φ — автоморфизм поля K_{sep} над K, индуцирующий φ_0 на K_0. Иными словами, если φ индуцирует φ' на K_{ab}, то $\mathfrak{a}(\theta)\varphi'^{-r}$ является пересечением ядер всех характеров $\chi \in X_0$, т. е. (в силу определения группы $\mathfrak{A}_0$ и поля K_0) $\mathfrak{a}(\theta)\varphi'^{-r}$ индуцирует на K_0 тождественное отображение, что и требовалось доказать.

Следствие. *В обозначениях предложения 7 пусть φ' — некоторый автоморфизм поля K_{ab} над K, индуцирующий φ_0 на K_0. Тогда $\mathfrak{a}$ отображает $R^\times$ на $\mathfrak{A}_0$ и $K^\times$ на объединение классов смежности $\mathfrak{A}_0\varphi'^n$ по $n \in \mathbf{Z}$, и это объединение всюду плотно в $\mathfrak{A}$.*

Это сразу вытекает из предложения 7 и условия [II″] § 1.

Теперь мы рассмотрим ядро U_K морфизма $\mathfrak{a}$. По определению оно является пересечением ядер характеров $\theta \to (\chi, \theta)_K$ на $K^\times$, где в качестве χ берутся все характеры на $\mathfrak{G}$. По предложению 10 гл. IX-4 последнее пересечение совпадает с пересечением групп $\mathrm{N}_{L/K}(L^\times)$, где в качестве L берутся все циклические расширения поля K.

Предложение 8. *Пусть K' — абелево расширение конечной степени над K. Тогда $U_K = N_{K'/K}(U_{K'})$.*

Предположим сначала, что расширение K' над K циклично. Тогда мы можем применить предложение 4 § 1, взяв $F = N_{K'/K}$. В самом деле, условия [IV (i)] и [IV (ii)], очевидно, удовлетворяются для автоморфизмов $x \to x^\lambda$ группы $K'^\times$ при всех $\lambda \in \mathfrak{G}$; условие [IV (iii)] выполняется по следствию 5 теор. 1 § 2; условие [V (i)] очевидно, а условие [V (ii)] справедливо по теореме 2 § 2. Группы U и U' из предложения 4 совпадают сейчас с U_K и $U_{K'}$ соответственно. При этом, как мы уже видели, U_K содержится в группе $N_{K'/K}(K'^\times)$, которая в предложении 4 обозначалась через $F(G')$. Этим доказано наше утверждение для циклического расширения K' над K.

В общем случае мы можем найти такую последовательность $K, K_1, \ldots, K_m = K'$ полей, промежуточных между K и K', что каждое последующее поле циклично над предыдущим. Применим индукцию по m. По предположению индукции $U_{K_1} = N_{K'/K_1}(U_{K'})$, а по доказанному выше $U_K = N_{K_1/K}(U_{K_1})$, откуда и вытекает наше утверждение.

Это доказательство можно приспособить и для любого разрешимого расширения, но это нам не понадобится.

Предложение 9. *Предположим, что K содержит n различных корней n-й степени из 1. Тогда пересечение ядер характеров $\theta \to (\chi_{n,\xi}, \theta)_K$ на $K^\times$ по всем $\xi \in K^\times$ совпадает с $(K^\times)^n$.*

Из нашего предположения относительно поля K следует, что n не делится на характеристику поля K; $\chi_{n,\xi}$ здесь такое, как в гл. IX-5. По определению $\chi_{n,\xi}$ наше множество является пересечением ядер всех морфизмов $\theta \to \{\xi, \theta\}_n$ группы $K^\times$ в $H(K)$. По формуле (12) гл. IX-5 («закон взаимности») это пересечение состоит из всех элементов θ группы $K^\times$, для которых $\{\theta, \xi\}_n = 1$, т. е. $\{\chi_{n,\theta}, \xi\} = 1$, т. е. $(\chi_{n,\theta}, \xi)_K = 1$, при всех $\xi \in K^\times$. По следствию 3 теор. 2 § 2 последнее равенство эквивалентно равенству $\chi_{n,\theta} = 1$, которое, как было отмечено в гл. IX-5, имеет место тогда и только тогда, когда $\theta \in (K^\times)^n$.

Следствие. *Пусть K — любое p-поле. Если n не делится на характеристику поля K, то $U_K \subset (K^\times)^n$.*

Из нашего предположения относительно n следует, что существует n различных корней n-й степени из 1 в K_{sep}. Эти корни порождают абелево расширение K' поля K. По предложению 9

имеем $U_{K'} \subset (K'^{\times})^n$. По предложению 8 отсюда вытекает, что

$$U_K = N_{K'/K}(U_{K'}) \subset N_{K'/K}((K'^{\times})^n) \subset (K'^{\times})^n.$$

Предложение 10. *Предположим, что поле K имеет характеристику p. Тогда пересечение ядер характеров $\theta \to (\chi_{p,\xi}, \theta)_K$ на $K^{\times}$ по всем $\xi \in K$ равно $(K^{\times})^p$.*

Обозначим рассматриваемое пересечение через Z. Поскольку всякий характер $\chi_{p,\xi}$ имеет порядок p или 1, то Z является подгруппой в $K^{\times}$, содержащей $(K^{\times})^p$. Поскольку $\chi_{p,\xi} = 1$ при $\xi = 0$, то Z можно определить как множество, состоящее из таких элементов θ группы $K^{\times}$, для которых $\{\xi, \theta\}_p = 1$ при всех $\xi \in K^{\times}$, или, что то же самое, $\{\xi\theta, \theta\}_p = 1$ при всех $\xi \in K^{\times}$. По формуле (13) и (14) гл. IX-4 при всех $\xi \in K^{\times}$, $\theta \in K^{\times}$ имеем

$$1 = \{\xi\theta, -\xi\theta\}_p = \{\xi\theta, -\xi\}_p \cdot \{\xi\theta, \theta\}_p,$$

так что Z совпадает также с множеством тех элементов θ группы $K^{\times}$, для которых $\{\xi\theta, -\xi\}_p = 1$ при всех $\xi \in K^{\times}$. По первой из формул (13) гл. IX-5 $Z \cup \{0\}$ является аддитивной подгруппой в K. Так как Z является подгруппой в $K^{\times}$, содержащей $(K^{\times})^p$, мы видим, что $Z \cup \{0\}$ является подполем в K, содержащим K^p. В силу следствия 1 предл. 4 гл. I-4 это подполе совпадает с K или с K^p. Если бы $Z \cup \{0\}$ совпадало с K, то все характеры вида $\chi_{p,\xi}$ были бы тривиальны. Как было замечено в гл. IX-5, ядро морфизма $\xi \to \chi_{p,\xi}$ совпадает с образом поля K при отображении $x \to x - x^p$. Из теоремы 8 гл. I-4 сразу следует, что этот образ не может содержать никакого элемента вида π^{-1}, где π — простой элемент в K. Поэтому характер $\chi_{p,\xi}$ нетривиален при $\xi = \pi^{-1}$. Это показывает, что $Z \cup \{0\} = K^p$, откуда $Z = (K^{\times})^p$.

Следствие. *Если характеристика поля K равна p, то $U_K \subset (U_K)^p$.*

По предложению 10 $U_K \subset (K^{\times})^p$, так что каждый элемент $\theta \in U_K$ можно записать как η^p с $\eta \in K^{\times}$. Возьмем любое циклическое расширение L поля K. По предложению 8 $U_K = N_{L/K}(U_L)$, и по предложению 10 $U_L \subset (L^{\times})^p$.

Поэтому θ можно записать как $N_{L/K}(\zeta^p)$ с $\zeta \in L^{\times}$. Это дает $\eta^p = N_{L/K}(\zeta)^p$. Поскольку p — характеристика поля K, отсюда следует, что $\eta = N_{L/K}(\zeta)$. Таким образом, показано, что η лежит в пересечении групп $N_{L/K}(L^{\times})$ по всем циклическим расширениям L поля K. Так как последнее пересечение совпадает с U_K, наше следствие доказано.

Теорема 3. *Отображение* $\chi \to \chi \circ \mathfrak{a}$ *является биективным морфизмом группы* X_K *характеров на* $\mathfrak{A}$ *на группу характеров конечного порядка на* $K^\times$.

Возьмем произвольное целое число $n \geqslant 1$. Если характеристика поля K не равна p, то по следствию предл. 9 имеем $U_K \subset (K^\times)^n$. Если характеристика поля K равна p, то запишем n в виде $n = n'p^i$, где n' взаимно просто с p и $i \geqslant 0$, и возьмем любой элемент $\theta \in U_K$. По тому же самому следствию можно записать θ в виде $\theta = \xi^{n'}$, где $\xi \in K^\times$. Из следствия предл. 10 с помощью индукции по i немедленно получаем, что $U_K \subset (U_K)^{p^i}$, так что $\theta = \eta^{p^i}$, где $\eta \in U_k$. Выберем такие целые числа a, b, что $n'a + p^ib = 1$. Тогда $\theta = (\xi^b\eta^a)^n$. Отсюда видно, что во всех случаях $U_K \subset (K^\times)^n$, так что каждый характер на $K^\times$, порядок которого делит n, тривиален на U_K. Поскольку это имеет место при всех n, наше заключение сразу вытекает теперь из следствия 4 предл. 2 § 1.

Следствие 1. *Канонический морфизм* $\mathfrak{a}$ *группы* $K^\times$ *в группу Галуа* $\mathfrak{A}$ *поля* K_{ab} *над* K *инъективен.*

По лемме 2 § 1, примененной к эндоморфизму $x \to x^n$ группы $K^\times$, $(K^\times)^n$ является замкнутой подгруппой в $K^\times$ для каждого $n \geqslant 1$. Отсюда следует, что $(K^\times)^n$ совпадает с пересечением ядер всех характеров на $K^\times$, порядок которых делит n. В таком случае теорема 3 показывает, что ядро U_K морфизма $\mathfrak{a}$ совпадает с пересечением U' групп $(K^\times)^n$ по всем $n \geqslant 1$. Ясно, что U' содержится в $R^\times$. Поскольку, очевидно, компактная группа $R^\times$ вполне несвязна, лемма 4 гл. VII-3 показывает, что все характеры этой группы имеют конечный порядок. Если π — простой элемент в K, то каждый характер на $R^\times$ можно однозначно продолжить до характера ω на $K^\times$, для которого $\omega(\pi) = 1$ и который поэтому будет иметь конечный порядок. Отсюда следует, что U' содержится в ядре каждого характера на $R^\times$, так что $U' = \{1\}$.

Следствие 2. *Канонический морфизм* $\mathfrak{a}$ *индуцирует на группе* $R^\times$ *изоморфизм этой группы на группу Галуа* $\mathfrak{A}_0$ *поля* K_{ab} *над объединением* K_0 *всех неразветвленных расширений поля* K, *содержащихся в* $\overline{K}$.

Это сразу вытекает из следствия 1 и следствия предл. 7.

Теорема 4. *Пусть* K' *— расширение конечной степени над* K, *содержащееся в* $\overline{K}$. *Положим* $L = K' \cap K_{\mathrm{ab}}$. *Тогда при* $\theta \in K^\times$ *автоморфизм* $\mathfrak{a}(\theta)$ *тождествен на* L *тогда и только тогда, когда* θ *лежит в* $\mathrm{N}_{K'/K}(K'^\times)$.

Обозначим через ρ морфизм ограничения из $\mathfrak{A}'$ в $\mathfrak{A}$ и положим $\mathfrak{B} = \rho(\mathfrak{A}')$. Элемент поля K_{ab} инвариантен относительно $\mathfrak{B}$ в том и только в том случае, когда он лежит в K', а тогда он лежит в L. Поэтому $\mathfrak{B}$ является подгруппой в $\mathfrak{A}$, соответствующей полю L. Положим $X = \mathfrak{a}^{-1}(\mathfrak{L})$ и $X' = N_{K'/K}(K'^{\times})$. Нам нужно доказать, что $X = X'$. По лемме 2 § 1 X' является замкнутой подгруппой в $K^{\times}$. Если n — степень поля K' над K, то $N_{K'/K}(\theta) = \theta^n$ при $\theta \in K^{\times}$, так что $X' \supset (K^{\times})^n$. Поэтому если ψ — характер на $K^{\times}$, тривиальный на X', то он тривиален на $(K^{\times})^n$ и, следовательно, его порядок делит n, а значит по теореме 3 его можно записать в виде $\chi \circ \mathfrak{a}$, где $\chi \in X_K$. Поэтому характер $\chi \circ \mathfrak{a} \circ N_{K'/K}$ тривиален на $K'^{\times}$. Но по следствию 1 теор. 2 § 2 этот характер совпадает с $\chi \circ \rho \circ \mathfrak{a}'$, так что должен быть тривиальным характер $\chi \circ \rho$ на $\mathfrak{A}'$ и, следовательно, характер χ на $\rho(\mathfrak{A}') = \mathfrak{B}$, а значит, характер ψ на X. Отсюда видно, что $X' \supset X$. Обратно, если $\theta = N_{K'/K}(\theta')$ с $\theta' \in K'^{\times}$, то следствие 1 теор. 2 § 2 дает равенство $\mathfrak{a}(\theta) = \rho(\mathfrak{a}'(\theta'))$. Так как последний элемент лежит в $\mathfrak{B}$, то мы видим, что $X' \subset X$, чем и завершается доказательство нашей теоремы.

Следствие 1. *В предположениях и обозначениях теоремы* 4 *пусть* $\mathfrak{B}$ *— подгруппа в* $\mathfrak{A}$, *соответствующая полю* L. *Тогда* $N_{L/K}(L^{\times}) = N_{K'/K}(K'^{\times}) = \mathfrak{a}^{-1}(\mathfrak{B})$.

Последнее равенство является точной переформулировкой теоремы 4. Применяя теорему 4 к $K' = L$, получаем, что $N_{L/K}(L^{\times}) = \mathfrak{a}^{-1}(\mathfrak{B})$.

Следствие 2. *Для каждого расширения* L *конечной степени над* K, *содержащегося в* K_{ab}, *обозначим через* $\mathfrak{B}(L)$ *подгруппу в* $\mathfrak{A}$, *соответствующую полю* L, *и положим* $N(L) = N_{L/K}(L^{\times})$. *Тогда* $N(L) = \mathfrak{a}^{-1}(\mathfrak{B}(L))$; $\mathfrak{B}(L)$ *является замыканием подгруппы* $\mathfrak{a}(N(L))$ *в* $\mathfrak{A}$; L *состоит из элементов поля* K_{ab}, *инвариантных относительно* $\mathfrak{a}(\theta)$ *при всех* $\theta \in N(L)$, *и* $\mathfrak{a}$ *определяет изоморфизм группы* $K^{\times}/N(L)$ *на группу Галуа* $\mathfrak{A}/\mathfrak{B}(L)$ *поля* L *над* K. *Кроме того,* $L \to N(L)$ *является биективным отображением подполей в* K_{ab} *конечной степени над* K *на открытые подгруппы конечного индекса в* $K^{\times}$.

Если учесть теоремы 3 и 4, то все это является переформулировкой предложения 3 § 1.

В случае когда L и $N(L)$ таковы, как в нашем следствии, принято говорить, что L — *поле классов* для подгруппы $N(L)$ в $K^{\times}$. При применении последнего следствия часто полезно иметь в виду,

что, согласно лемме 1 § 1, открытая подгруппа в $K^\times$ имеет конечный индекс в $K^\times$ тогда и только тогда, когда она не содержится в $R^\times$.

Следствие 3. *Пусть K и K' таковы, как в теореме* 4, *и пусть M — подполе в K_{ab} конечной степени над K. Обозначим через M' композит полей M и K'. Тогда*

$$N_{M'/K'}(M'^\times) = N_{K'/K}^{-1}(N_{M/K}(M^\times)).$$

По следствию 2 группа $N_{M/K}(M^\times)$, совпадающая с $N(M)$, состоит из тех элементов θ в $K^\times$, для которых автоморфизм $\alpha(\theta)$ оставляет инвариантным каждый элемент поля M. Аналогичным образом $N_{M'/K'}(M'^\times)$ состоит из тех элементов θ' в $K'^\times$, для которых $\alpha'(\theta')$ оставляет инвариантным каждый элемент поля M'. Последнее условие выполняется в том и только в том случае, когда $\rho(\alpha'(\theta'))$ оставляет инвариантным каждый элемент поля M. В силу следствия 1 теор. 2 § 2 это означает, что $\alpha(N_{K'/K}(\theta'))$ оставляет инвариантным каждый элемент из M, т. е. что $N_{K'/K}(\theta')$ содержится в $N_{M/K}(M^\times)$.

Легко видеть, что теорема 4 и ее следствия сохраняют силу и для R-полей; то же относится и к теореме 3.

§ 4. ВЕТВЛЕНИЕ АБЕЛЕВЫХ РАСШИРЕНИЙ

Изложенная выше теория была бы неполной без описания свойств ветвления абелевых расширений поля K и, в частности, их дифферент и дискриминантов. Как показано в гл. VIII-3, эти свойства можно полностью выразить с помощью распределения Хербранда на группе Галуа $\mathfrak{A}$ поля K_{ab} над K. Мы начнем с некоторых предварительных результатов, первый из которых не имеет прямого отношения к абелевым расширениям и может быть рассматриваем как добавление к гл. VIII-3.

Принимая те же обозначения, что и в гл. VIII-3 (например, в предложении 9 этой главы), обозначим через K' расширение Галуа поля K степени n с группой Галуа $\mathfrak{g} = \mathfrak{g}_0$ и через $\mathfrak{g}_\nu$, $\nu \geqslant 1$,— высшие группы ветвления поля K' над K. Обозначим, далее, через R, R' максимальные компактные подкольца в K, K' и через P, P' — максимальные идеалы в R, R' соответственно. Через ε будем обозначать нейтральный элемент группы $\mathfrak{g}$.

Предложение 11. *Пусть e — индекс ветвления поля K' над K, и пусть P'^d — дифферента этого расширения. Возьмем $h \geqslant 1$, $z \in P'^h$ и положим*

$$N_{K'/K}(X - z) = X^n + a_1X^{n-1} + \ldots + a_n,$$

где X — независимая переменная. Тогда:

(i) *если* $v(\lambda) \leqslant h+1$ *при всех* $\lambda \neq \varepsilon$, *то при* $1 \leqslant i \leqslant n$ *имеем*

$$e \cdot \mathrm{ord}_K(a_i) \geqslant h + d - e + 1;$$

(ii) *если* $v(\lambda) \leqslant h$ *при всех* $\lambda \neq \varepsilon$, *то при* $2 \leqslant i \leqslant n$ *имеем*

$$e \cdot \mathrm{ord}_K(a_i) > h + d - e + 1;$$

(iii) *если* $v(\lambda) \geqslant h+1$ *при всех* $\lambda \neq \varepsilon$, *то при* $1 \leqslant i \leqslant n$ *имеем*

$$\mathrm{ord}_K(a_i) \geqslant h;$$

(iv) *если* $v(\lambda) \geqslant h+2$ *при всех* $\lambda \neq \varepsilon$, *то при* $1 \leqslant i \leqslant n-1$ *имеем*

$$\mathrm{ord}_K(a_i) > h.$$

Поскольку $-a_1 = \mathrm{Tr}_{K'/K}(z)$, то неравенство в (i) при $i=1$ сводится к следствию 1 предл. 4 гл. VIII-1, причем его справедливость не зависит от сделанного в (i) предположения относительно $v(\lambda)$. В общем случае имеем

$$(-1)^i a_i = \sum z^{\lambda_1} z^{\lambda_2} \dots z^{\lambda_i}, \tag{3}$$

где сумма берется по всем наборам из i различных элементов группы $\mathfrak{g}$, или, что то же самое, по всем подмножествам $\mathfrak{f} = \{\lambda_1, \dots, \lambda_i\}$ в $\mathfrak{g}$, состоящим из i элементов. Для всякого такого подмножества $\mathfrak{f}$ положим

$$z(\mathfrak{f}) = z^{\lambda_1} z^{\lambda_2} \dots z^{\lambda_i}.$$

Возьмем какое-нибудь такое подмножество $\mathfrak{f}$ и для всякого $\sigma \in \mathfrak{g}$ обозначим через $\mathfrak{f}\sigma$ образ подмножества $\mathfrak{f}$ при трансляции $\lambda \longrightarrow \lambda\sigma$ группы $\mathfrak{g}$. Пусть $\mathfrak{h}$ — подгруппа в $\mathfrak{g}$, состоящая из таких элементов σ, для которых $\mathfrak{f}\sigma = \mathfrak{f}$. Обозначим через l порядок группы $\mathfrak{h}$ и выберем некоторую полную систему $\{\rho_1, \dots, \rho_r\}$ представителей левых классов смежности $\mathfrak{h}\rho$ в $\mathfrak{g}$ по $\mathfrak{h}$. Ясно, что $\mathfrak{f}$ является дизъюнктным объединением правых классов смежности $\mu\mathfrak{h}$ в $\mathfrak{g}$ по $\mathfrak{h}$. Возьмем какое-нибудь полное множество $\mathfrak{m} = \{\mu_1, \dots, \mu_m\}$ представителей этих классов смежности, так что $\mathfrak{f}$ является дизъюнктным объединением классов смежности $\mu_1\mathfrak{h}, \dots, \mu_m\mathfrak{h}$; при этом $i = ml$. Положим $w = z(\mathfrak{m})$ и обозначим через K'' подполе в K', соответствующее подгруппе $\mathfrak{h}$ в $\mathfrak{g}$. Мы имеем

$$z(\mathfrak{f}) = \prod_{\sigma \in \mathfrak{h}} w^\sigma = \mathrm{N}_{K'/K''}(w).$$

В силу нашего определения группы $\mathfrak{h}$ множества $\mathfrak{h}\rho_1, \dots, \mathfrak{h}\rho_r$ попарно не пересекаются. Поскольку в каждом из них столько же

элементов, сколько и в $\mathfrak{j}$ (а именно i), то все члены $z(\mathfrak{j}\rho_j)$, $1 \leqslant j \leqslant r$, встречаются в правой части равенства (3). Так как ρ_j индуцируют на K'' все различные изоморфизмы поля K'' в $\overline{K}$, то сумма этих членов равна

$$\sum_{\mathfrak{j}} z(\mathfrak{j}\rho_j) = \sum_{\mathfrak{j}} z(\mathfrak{j})^{\rho_j} = \sum_{\mathfrak{j}} \mathrm{N}_{K'/K''}(\omega)^{\rho_j} = \mathrm{Tr}_{K''/K}(\mathrm{N}_{K'/K''}(w)). \tag{4}$$

Следовательно, правую часть равенства (3) можно записать как сумму членов, каждый из которых имеет вид, указанный в правой части равенства (4). Далее для каждого из этих членов имеем $ml = i$, где l — порядок группы $\mathfrak{h}$, т. е. степень поля K' над K''. Теперь остается только доказать наши неравенства для всякого члена такого вида, причем $\mathrm{ord}_{K'}(w) \geqslant mh$ ввиду нашего предположения относительно z и определения w. Обозначим через e' индекс ветвления и через f' модулярную степень поля K' над K'', так что $l = e'f'$ по следствию 6 теор. 6 гл. I-4. Тогда по формуле (2) гл. VIII-1 порядок элемента $\mathrm{N}_{K'/K''}(w)$ в K'' не меньше $f'mh$. Обозначим через e'' индекс ветвления и через d'' показатель дифференты поля K'' над K. Если ω — порядок в K правой части равенства (4), то по следствию 1 предл. 4 гл. VIII-1 имеем

$$e''\omega \geqslant f'mh + d'' - e'' + 1.$$

Поскольку $e = e'e''$, $i = ml$ и $e'f' = l$, отсюда следует неравенство

$$e\omega \geqslant ih + e'd'' - e + e'.$$

Если теперь обозначить через d' показатель дифференты поля K' над K'', то следствие предл. 4 гл. VIII-1 дает равенство $d = e'd'' + d'$, так что наше последнее неравенство можно переписать так:

$$e\omega \geqslant ih + (d - e + 1) - (d' - e' + 1).$$

Согласно формуле (9) гл. VIII-3, примененной к K' и K'', имеем

$$d' - e' + 1 = \sum_{\lambda} (v(\lambda) - 1)^+,$$

где сумма берется по всем $\lambda \neq \varepsilon$ в $\mathfrak{h}$, причем, как было там отмечено, число положительных членов в этой сумме не превосходит $e' - 1$. Если выполняется предположение части (i), то каждый из этих членов не больше h, что дает

$$d' - e' + 1 \leqslant (e' - 1)\,h,$$

а потому

$$e\omega - (h + d - e + 1) \geqslant (i - e')\,h.$$

Поскольку $e' \leqslant l \leqslant i$, этим доказана часть (i) нашего предложения. Если выполняется предположение части (ii), то тем же самым способом получаем неравенство

$$d' - e' + 1 \leqslant (e' - 1)(h - 1),$$

откуда

$$e\omega - (h + d - e + 1) \geqslant i - 1 + (i - e')(h - 1);$$

правая часть не может обращаться в нуль при $i \neq 1$; тем самым доказано (ii). Далее, если мы применим формулу (9) гл. VIII-3 к K' и K, то получим, что

$$(d - e + 1) - (d' - e' + 1) = \sum (v(\lambda) - 1)^+,$$

где сумма берется теперь по всем $\lambda \in \mathfrak{g} - \mathfrak{h}$ и состоит из $n - l$ членов, так что она не меньше $(n - l)\,h$, если выполняется предположение части (iii). Мы приходим к неравенству

$$e(\omega - h) \geqslant (i + n - l - e)\,h,$$

чем доказано (iii), поскольку $l \leqslant i$ и $e \leqslant n$. Аналогичным образом из предположения части (iv) вытекает неравенство

$$e(\omega - h) \geqslant (i + n - l - e)\,h + n - l.$$

Так как $l \leqslant i$, $e \leqslant n$, $l \leqslant n$, то правая часть не может равняться нулю, за исключением случая, когда $l = i$, $e = n$, $l = n$ и, значит, $i = n$. Тем самым доказано и (iv).

Следствие 1. *В обозначениях предложения* 11 *пусть снова* $h \geqslant 1$ *и* $z \in P'^h$. *Тогда*:

(i) *если* $v(\lambda) \leqslant h + 1$ *при всех* $\lambda \neq \varepsilon$, *то*

$$e \cdot \mathrm{ord}_K (\mathrm{N}_{K'/K}(1 + z) - 1) \geqslant h + d - e + 1;$$

(ii) *если* $v(\lambda) \leqslant h$ *при всех* $\lambda \neq \varepsilon$ *и* $h = \rho e - (d - e + 1)$, *где* $\rho \in \mathbf{Z}$, *то*

$$\mathrm{N}_{K'/K}(1 + z) \equiv 1 \ (P^\rho), \quad \mathrm{N}_{K'/K}(1 + z) \equiv 1 + \mathrm{Tr}_{K'/K}(z) \ (P^{\rho+1});$$

(iii) *если* $v(\lambda) \geqslant h + 1$ *при всех* $\lambda \neq \varepsilon$, *то*

$$\mathrm{N}_{K'/K}(1 + z) \equiv 1 \quad (P^h);$$

(iv) *если* $v(\lambda) \geqslant h + 2$ *при всех* $\lambda \neq \varepsilon$, *то*

$$\mathrm{N}_{K'/K}(1 + z) \equiv 1 + \mathrm{N}_{K'/K}(z) \quad (P^{h+1}).$$

В самом деле, в обозначениях предложения 11 имеем

$$\mathrm{N}_{K'/K}(1 + z) = 1 + \sum_{i=1}^{n} (-1)^i a_i.$$

Четыре утверждения нашего следствия немедленно вытекают поэтому из соответствующих утверждений предложения 11.

Следствие 2. *В предположениях части* (ii) *следствия* 1 *имеем*

$$N_{K'/K}(1 + P'^h) = 1 + P^\rho.$$

Так как $d - e + 1 \geqslant 0$, то из этих предположений следует, что $h \leqslant \rho e$, откуда $\rho \geqslant 1$. Согласно части (ii) следствия 1 $N_{K'/K}(1 + P'^h)$ содержится в $1 + P^\rho$. Обратно, возьмем любой элемент $x_0 \in P^\rho$. Тогда по индукции можно определить две последовательности $(x_0, x_1, \ldots)$ и $(z_0, z_1, \ldots)$ с $x_i \in P^{i+\rho}$ и $z_i \in P'^{ie+h}$ при всех $i \geqslant 0$, выбирая для всякого $i \geqslant 0$ элемент $z_i \in P'^{ie+h}$, для которого $\mathrm{Tr}_{K'/K}(z_i) = x_i$, что можно сделать в силу предложения 4 гл. VIII-1, и полагая затем

$$x_{i+1} = (1 + x_i) N_{K'/K}(1 + z_i)^{-1} - 1.$$

Из части (ii) следствия 1 сразу вытекает, что этот элемент лежит в $P^{i+1+\rho}$, что и требовалось. Очевидно, $1 + x_0 = N_{K'/K}(y)$, где y задается сходящимся произведением $y = \prod_{i=0}^{\infty}(1 + z_i)$. Поскольку y лежит в $1 + P'^h$, наше следствие доказано.

Предложение 12. *Пусть K и K' такие, как выше. Предположим, что $\mathfrak{v}(\lambda)$ принимает одно и то же значение $i \geqslant 2$ для всех $\lambda \neq \varepsilon$ в $\mathfrak{g}$. Тогда $N_{K'/K}(1 + P'^h) \subset 1 + P^h$ при $1 \leqslant h \leqslant i$ и $N_{K'/K}(1 + P'^{i-1}) \subset 1 + P^i$ в том и только в том случае, когда степень n поля K' над K равна модулю q поля K.*

При наших предположениях высшие группы ветвления поля K' над K задаются следующим образом: $\mathfrak{g}_\mathfrak{v} = \mathfrak{g}$ при $\mathfrak{v} \leqslant i$ и $\mathfrak{g}_\mathfrak{v} = \{\varepsilon\}$ при $\mathfrak{v} \geqslant i + 1$. Поскольку $\mathfrak{g}_1 = \mathfrak{g}$, то $e = n$. Поле K' имеет модулярную степень $f = 1$ над K и тот же модуль q, что и K. По формуле (9) гл. VIII-3 имеем $d = (n - 1)\, i$. Беря $h = i$ в части (i) следствия 1 предл. 11, получаем для этого случая наше первое утверждение. В случае $h < i$ это утверждение сразу вытекает из части (iii) следствия 1 того же предложения. По следствию 3 предл. 9 гл. VIII-3 степень n поля K' над K делит q. В силу того же предложения если мы возьмем простой элемент π' в K' и положим $y_\lambda = \pi'^\lambda \pi'^{-1}$ при всех $\lambda \in \mathfrak{g}$, то отображение $\lambda \to y_\lambda$ переводит $\mathfrak{g}$ в множество Y элементов из $1 + P'^{i-1}$, попарно несравнимых друг с другом по модулю P'^i. В частности, Y образует полное множество представителей классов смежности в $1 + P'^{i-1}$ по

$1 + P'^i$ в том и только в том случае, когда $n = q$. Так как, очевидно, $N_{K'/K}(y_\lambda) = 1$ при всех λ, отсюда видно, что $N_{K'/K}(1 + P'^{i-1})$ совпадает с $N_{K'/K}(1 + P'^i)$ при $n = q$. Следовательно, если $n = q$, то $N_{K'/K}(1 + P'^{i-1})$ содержится в $1 + P^i$. Для доказательства обратного утверждения возьмем $z \in K'^\times$, для которого $\mathrm{ord}_{K'}(z) = i - 1$. Как и в доказательстве предложения 11, запишем

$$N_{K'/K}(X - z) = X^n + \sum_{j=1}^{n} a_j X^{n-j}.$$

Тогда $a_n = N_{K'/K}(-z)$, так что по формуле (2) гл. VIII-1 $\mathrm{ord}_K(a_n) = i - 1$. Полагая $h = i - 1$ в части (i) предложения 11, получаем, что $\mathrm{ord}_K(a_j) \geqslant i - 1$ при $1 \leqslant j \leqslant n$, так что если положить $b_j = a_j/a_n$, то все b_j будут лежать в R. Возьмем теперь любой элемент y из $1 + P'^{i-1}$. Поскольку $(1 - y)/z$ лежит в R' и K' имеет тот же самый модуль, что и K, то существует $\alpha \in R$, для которого $(1 - y)/z \equiv \alpha$ по модулю P', или, что то же самое, $y = (1 - \alpha z)\,u$, где $u \in 1 + P'^i$. Поэтому $N_{K'/K}(u)$ лежит в $1 + P^i$, так что мы имеем

$$N_{K'/K}(y) \equiv N_{K'/K}(1 - \alpha z) =$$

$$= 1 + \sum_{j=1}^{n} a_j \alpha^j = 1 + a_n\left(\alpha^n + \sum_{j=1}^{n-1} b_j \alpha^j\right) \quad (P^i).$$

Для $1 \leqslant j \leqslant n - 1$ обозначим через $\bar{b}_j$ образ элемента b_j в поле R/P при каноническом гомоморфизме кольца R на это поле. Тогда написанная выше формула показывает, что $N_{K'/K}(y)$ содержится в $1 + P^i$ в том и только в том случае, когда образ элемента α в том же поле является корнем многочлена $T^n + \sum \bar{b}_j T^j$. В частности, если это имеет место при всех y, то все элементы поля R/P должны быть корнями последнего многочлена, так что $n \geqslant q$, чем и завершается наше доказательство.

Предложение 13. *Пусть π — простой элемент в K. Для всякого $\nu \geqslant 1$ обозначим через N_ν подгруппу в $K^\times$, порожденную элементом π и подгруппой $1 + P^\nu$, и через K_ν подполе в K_{ab}, для которого $N(K_\nu) = N_\nu$ в смысле следствия 2 теор. 4 § 3. Пусть $\mathfrak{g}^{(\nu)}$ — группа Галуа поля K_ν над K и α_ν — морфизм группы $K^\times$ на $\mathfrak{g}^{(\nu)}$ с ядром N_ν, определенный каноническим морфизмом α группы $K^\times$. Пусть $\mathfrak{g}_i^{(\nu)}$, $i \geqslant 1$, — высшие группы ветвления поля K_ν над K. Тогда $\mathfrak{g}_1^{(\nu)} = \mathfrak{g}^{(\nu)}$; при $1 \leqslant \rho \leqslant \nu$ и $q^{\rho-1} < i \leqslant q^\rho$ имеем $\mathfrak{g}_i^{(\nu)} = \alpha_\nu(N_\rho)$.*

Фиксируем некоторое $v \geqslant 1$ и упростим обозначения, употребляя символ N вместо N_v, L вместо K_v, $\mathfrak{g}$ вместо $\mathfrak{g}^{(v)}$, $\mathfrak{g}_i$ вместо $\mathfrak{g}_i^{(v)}$. Как и в гл. VIII-3, для всякого $i \geqslant 1$ обозначим через g_i число элементов в $\mathfrak{g}_i$. Тогда g_i делит g_j при $i \geqslant j$. Поскольку группа $\mathfrak{g}$ изоморфна группе $K^\times/N$, то степень поля L над K равна индексу подгруппы N в $K^\times$, который равен $n = (q-1)\,q^{v-1}$. По следствию предл. 6 § 2 для максимального неразветвленного расширения L' поля K, содержащегося в L, имеем $N(L'^\times) = R^\times N$. Поскольку $R^\times N = K^\times$, то мы получаем, что $L' = K$. Другими словами, поле L вполне разветвлено над K, его индекс ветвления равен $e = n$, и мы имеем $\mathfrak{g}_1 = \mathfrak{g}$. Кроме того, L имеет тот же самый модуль q, что и K, и то же самое должно выполняться для всех полей, промежуточных между K и L, так что если $K \subset K' \subset K'' \subset L$, то поле K'' вполне разветвлено над K'. По следствию 1 предл. 9 гл. VIII-3 g_i/g_{i+1} делит q при всех $i \geqslant 2$. Поэтому $g_1/g_2 = q-1$.

Положим $r_1 = 0$ и $r_i = (g_2 + \ldots + g_i)/n$ при всех $i \geqslant 2$. Для всякого целого числа $\rho \geqslant 0$ обозначим через $i(\rho)$ наибольшее среди всех i, для которых $r_i \leqslant \rho$. Предположим, что $r_i < \rho < r_{i+1}$ при некотором $\rho \geqslant 0$ и $i \geqslant 1$. Тогда $0 < \rho n - (g_2 + \ldots + g_i) < g_{i+1}$, что явно невозможно, поскольку $n, g_2, \ldots, g_i$ делятся на g_{i+1}. Поэтому при всех ρ имеем $r_{i(\rho)} = \rho$. Далее $i(0) = 1$ и $i(\rho) > 1$ при $\rho > 0$. Возьмем любое ρ, для которого $0 \leqslant \rho < v$, и положим $i = i(\rho)$. Пусть K', K'' — подполя в L, состоящие из элементов, инвариантных относительно $\mathfrak{g}_i$ и $\mathfrak{g}_{i+1}$ соответственно. Тогда группу Галуа $\mathfrak{g}''$ поля K'' над K' можно отождествить с $\mathfrak{g}_i/\mathfrak{g}_{i+1}$. Если $\rho = 0$, то $i = 1$ и степень поля K'' над K' равна $g_1/g_2 = q-1$.

Начиная с этого места предположим, что $1 \leqslant \rho < v$. Покажем, что в этом случае степень поля K'' над K' равна q. Заметим сначала, что высшие группы ветвления $\mathfrak{g}_j''$ поля K'' над K' задаются с помощью формулы (11) гл. VIII-3, примененной к K', K'' и L. Поскольку поле K'' вполне разветвлено над K', его индекс ветвления совпадает с его степенью над K' и упомянутая формула сразу показывает, что $v(\sigma'') = i$ при всех $\sigma'' \in \mathfrak{g}''$, кроме тождественного автоморфизма, так что $\mathfrak{g}_j'' = \mathfrak{g}''$ при $j \leqslant i$ и $\mathfrak{g}_j'' = \{\varepsilon\}$ при $j \geqslant i+1$.

Аналогично для группы Галуа поля K' над K запишем $\mathfrak{g}' = \mathfrak{g}/\mathfrak{g}_i$ и обозначим через $\mathfrak{g}_j'$ высшие группы ветвления этого расширения. В точности тем же способом находим, что $\mathfrak{g}_j'$ совпадают с образом $\mathfrak{g}_j/\mathfrak{g}_i$ группы $\mathfrak{g}_j$ в $\mathfrak{g}'$ при $j < i$ и что $\mathfrak{g}_j' = \{\varepsilon\}$ при $j \geqslant i$. Пусть R', R'' — максимальные компактные подкольца в K', K'' и P', P'' — максимальные идеалы в R', R'' соответственно. Поскольку поле K' вполне разветвлено над K, его индекс ветвления e' совпадает с его степенью $n' = n/g_i$. Поэтому если $P'^{d'}$ —

его дифферента над K, то формула (10) гл. VIII-3 дает

$$d' - e' + 1 = \sum_{j=2}^{i} ((g_j/g_i) - 1) = r_i n/g_i - i + 1 = \rho n' - i + 1.$$

Возьмем любое $z \in L$, для которого $\mathrm{ord}_L(z) \geqslant i - 1$, и положим $v = \mathrm{N}_{L/K''}(z)$, так что $v \in P''^{i-1}$. Применяя к K'' и L часть (iv) следствия 1 предл. 11 с $h = i - 1$, получаем

$$\mathrm{N}_{L/K''}(1 + z) \equiv 1 + v \quad (P''^i).$$

Определим теперь элемент w в K' равенством

$$1 + w = \mathrm{N}_{L/K'}(1 + z) = \mathrm{N}_{K''/K'}(\mathrm{N}_{L/K''}(1 + z)).$$

Применяя к K', K'' первое утверждение предложения 12 с $h = i$, получаем

$$1 + w \equiv \mathrm{N}_{K''/K'}(1 + v) \quad (P'^i).$$

Полагая $h = i - 1$ в том же утверждении предложения 12, находим, что $w \in P'^{i-1}$. Теперь к K и K' можно применить часть (ii) следствия 1 предл. 11, взяв $h = i - 1$. Это даст

$$\mathrm{N}_{L/K}(1 + z) = \mathrm{N}_{K'/K}(1 + w) \equiv 1 + \mathrm{Tr}_{K'/K}(w) \quad (P^{\rho+1}).$$

По определению поля K_ν и следствию 2 теор. 4 § 3 последний элемент должен лежать в $N_\nu = N$ и, следовательно, в $N_\nu \cap R^\times$, т. е. в $1 + P^\nu$. Так как $\rho < \nu$, отсюда следует, что $\mathrm{Tr}_{K'/K}(w)$ лежит в $P^{\rho+1}$. Учитывая найденные выше значения для e' и $d' - e' + 1$, убеждаемся с помощью предложения 4 гл. VIII-1, что $\mathrm{Tr}_{K'/K}$ отображает P'^{i-1} на P^ρ и P'^i на $P^{\rho+1}$. В частности, существует такое $w' \in P'^{i-1}$, что $\mathrm{Tr}_{K'/K}(w')$ не лежит в $P^{\rho+1}$. Если бы $\mathrm{ord}_{K'}(w) = i - 1$, то элемент $w'w^{-1}$ лежал бы в R', так что имело бы место сравнение $w'w^{-1} \equiv \alpha\ (P')$, где $\alpha \in R$, ибо K' имеет тот же самый модуль, что и K; это сравнение можно было бы переписать в виде $w' \equiv \alpha w\ (P'^i)$, откуда следовало бы, что

$$\mathrm{Tr}_{K'/K}(w') \equiv \alpha\, \mathrm{Tr}_{K'/K}(w) \equiv 0 \quad (P^{\rho+1})$$

вопреки нашему предположению. Отсюда видно, что w лежит в P'^i, другими словами, что $\mathrm{N}_{K''/K'}(1 + v)$ лежит в $1 + P'^i$, только если $v = \mathrm{N}_{L/K''}(z)$, где $z \in L$ и $\mathrm{ord}_L(z) \geqslant i - 1$. Выберем теперь такое $z_0 \in L^\times$, что $\mathrm{ord}_L(z_0) = i - 1$, и положим $v_0 = \mathrm{N}_{L/K''}(z_0)$, так что $\mathrm{ord}_{K''}(v_0) = i - 1$. Обозначим через $M^\times$ группу корней $(q - 1)$-й степени из 1 в K и возьмем $z = \mu z_0$ с $\mu \in M^\times$. Так как степень поля L над K'' равна g_{i+1} и так как g_j/g_{j+1} делит q при всех $j \geqslant 2$, то $v = \mu^Q v_0$, где $Q = g_{i+1}$ делит некоторую степень числа q

и, следовательно, взаимно просто с $q-1$, так что $\mu \to \mu^Q$ есть автоморфизм группы $M^\times$. Поэтому, когда μ пробегает множество $M = M^\times \cup \{0\}$, $1+v$ пробегает некоторое полное множество представителей классов смежности в $1+P''^{i-1}$ по модулю $1+P''^{i}$. Так как $N_{K''/K'}(1+v)$ лежит в $1+P'^{i}$ для всех таких элементов v, то предложение 12 показывает прежде всего, что $N_{K''/K'}(1+P''^{i-1})$ содержится в $1+P'^{i}$, и далее, что степень поля K'' над K' равна поэтому q.

Другими словами, мы показали, что $g_{i(\rho)}/g_{i(\rho)+1} = q$ при $1 \leqslant \rho \leqslant \nu-1$, а раньше было установлено, что при $\rho = 0$ эта дробь принимает значение $q-1$. Поскольку

$$n = (q-1)q^{\nu-1} = \sum_{i=1}^{\infty} (g_i/g_{i+1}),$$

отсюда следует, что $g_i = g_{i+1}$ для любого i, отличного от $i(0)=1$, $i(1), \ldots, i(\nu-1)$. Поэтому $\mathfrak{g}_j = \mathfrak{g}_{i(\rho)+1}$ при $i(\rho) < j \leqslant i(\rho+1)$, так что подгруппа $\mathfrak{g}_{i(\rho+1)}$ в $\mathfrak{g}_{i(\rho)}$ имеет индекс q при $1 \leqslant \rho < \nu$, в то время как при $\rho = 0$ этот индекс равен $q-1$. Индукцией по ρ сразу получаем, что $g_{i(\rho)} = q^{\nu-\rho}$ при $1 \leqslant \rho \leqslant \nu$. Из определения целых чисел r_i вытекает теперь, что

$$r_{i(\rho+1)} - r_{i(\rho)} = (g_{i(\rho)+1} + \ldots + g_{i(\rho+1)})/n = \\ = (i(\rho+1) - i(\rho))\, q^{\nu-\rho-1} n^{-1}$$

при $0 \leqslant \rho < \nu$. Поскольку $r_{i(\rho)} = \rho$, то левая часть равна 1, откуда

$$i(\rho+1) - i(\rho) = (q-1)\, q^{\rho}.$$

Поэтому с помощью индукции по ρ находим, что $i(\rho) = q^\rho$.

Чтобы завершить доказательство, заметим, что найденные выше значения для e' и $d' - e' + 1$ позволяют применить к полю K и полю K', введенному выше, следствие 2 предл. 11 с $h = i-1$. В силу этого следствия $1+P^\rho$ совпадает с $N_{K'/K}(1+P'^{i-1})$ и, следовательно, содержится в группе $N' = N_{K'/K}(K'^\times)$, связанной с K' согласно следствию 2 теор. 4 § 3. Так как N' содержит группу $N = N_\nu$, связанную с $L = K_\nu$, то N' содержит π и, следовательно, группу N_ρ, порожденную элементом π и подгруппой $1+P^\rho$. Пусть α_ν — определенный в нашем предложении морфизм группы $K^\times$ на $\mathfrak{g} = \mathfrak{g}^{(\nu)}$ с ядром N_ν. По следствию 2 теор. 4 § 3 этот морфизм отображает N' на подгруппу $\mathfrak{g}_{i(\rho)}$ в $\mathfrak{g}$, соответствующую полю K'. Поэтому $\mathfrak{g}_{i(\rho)}$ содержит $\alpha_\nu(N_\rho)$ при $1 \leqslant \rho < \nu$. В силу наших определений то же самое очевидно верно и для $\rho = 0$, если положить $N_0 = K^\times$, а также для $\rho = \nu$.

Теперь индукцией по ρ докажем, что $\mathfrak{g}_{i(\rho)} = \mathfrak{a}_\nu(N_\rho)$ при $0 \leqslant \rho \leqslant \nu$. Это верно при $\rho = 0$. Предположим, что $\mathfrak{g}_{i(\rho-1)} = \mathfrak{a}_\nu(N_{\rho-1})$, и пусть N' такое, как выше. Мы уже видели, что группа N' содержит N_ρ; далее, она содержится в $N_{\rho-1}$, поскольку $\mathfrak{g}_{i(\rho)}$ содержится в $\mathfrak{g}_{i(\rho-1)}$. Ее индекс в $N_{\rho-1}$ совпадает с индексом подгруппы $\mathfrak{g}_{i(\rho)}$ в $\mathfrak{g}_{i(\rho-1)}$, который равен $q-1$ при $\rho = 1$ и равен q при $\rho > 1$. Тем самым ее индекс совпадает с индексом подгруппы N_ρ в $N_{\rho-1}$, и мы получаем, что $N' = N_\rho$. С учетом уже доказанного этим завершается доказательство нашего предложения.

Следствие. *В обозначениях предложения* 13 *индекс ветвления поля K_ν над K совпадает с его степенью и задается формулой $e_\nu = (q-1)\,q^{\nu-1}$. Если d_ν — показатель дифференты поля K_ν над K, то $d_\nu/e_\nu = \nu - (q-1)^{-1}$.*

Значение e_ν уже было вычислено выше; значение d_ν можно сразу получить, применяя предложение 13 и формулу (10) гл. VIII-3. В результате получаем искомую формулу.

Как будет вскоре показано, в предложении 13 по существу вычисляется распределение Хербранда на группе Галуа $\mathfrak{A}$ поля K_{ab} над K, являющееся главным объектом изучения в этом параграфе. Напомним, что это распределение было определено в гл. VIII-3 как некоторая линейная форма $f \to \mathbf{H}(f)$ на пространстве всех локально постоянных функций на $\mathfrak{A}$. Как там объяснялось, характеристическая функция f_X любого открытого и замкнутого подмножества X в $\mathfrak{A}$ локально постоянна; для таких функций мы пишем $\mathbf{H}(X)$ вместо $\mathbf{H}(f_X)$. Таким образом, $X \to \mathbf{H}(X)$ есть конечно аддитивная функция от X.

Лемма 3. *Пусть $\mathbf{H}$ — распределение Хербранда на $\mathfrak{A}$. Тогда существует единственное распределение $\mathbf{H}_0$ на $\mathfrak{A}_0$, для которого $\mathbf{H}(f) = \mathbf{H}_0(f_0)$ для любой локально постоянной функции f на $\mathfrak{A}$ и индуцированной ею функции f_0 на $\mathfrak{A}_0$.*

Пусть $\mathfrak{B}$ — произвольная открытая подгруппа в $\mathfrak{A}$ и L — подполе в K_{ab}, соответствующее группе $\mathfrak{B}$. Пусть, далее, K_0 то же, что и в § 2, т. е. объединение всех неразветвленных расширений поля K, так что $\mathfrak{A}_0$ — подгруппа в $\mathfrak{A}$, соответствующая полю K_0. Тогда максимальное неразветвленное расширение L_0 поля K, содержащееся в L, совпадает с $K_0 \cap L$ и соответствует подгруппе $\mathfrak{B}\mathfrak{A}_0$ в $\mathfrak{A}$. Если $\mathfrak{B}\alpha$ — произвольный, отличный от $\mathfrak{B}$ класс смежности в $\mathfrak{A}$ по $\mathfrak{B}$ и α индуцирует на L автоморфизм λ, то число $\mathbf{H}(\mathfrak{B}\alpha)$ по определению равно $-\nu(\lambda)/e$, где e — индекс ветвления поля L над K; это число равно 0, если автоморфизм λ нетождествен на L_0,

т. е. если $\mathfrak{B}\alpha$ не содержится в $\mathfrak{B}\mathfrak{A}_0$, другими словами, если $\mathfrak{B}\alpha \cap \mathfrak{A}_0 = \varnothing$. Так как функция $\mathbf{H}$ конечно аддитивна, отсюда следует, что $\mathbf{H}(X) = 0$, если $X \cap \mathfrak{A}_0 = \varnothing$, и $\mathbf{H}(f) = 0$, если локально постоянная функция f равна нулю на $\mathfrak{A}_0$.

С другой стороны, возьмем любую локально постоянную функцию f_0 на $\mathfrak{A}_0$. Поскольку $\mathfrak{A}_0$ — компакт, то функция f_0 равномерно непрерывна, так что существует открытая подгруппа $\mathfrak{B}$ в $\mathfrak{A}$, такая, что f_0 постоянна на каждом классе смежности в $\mathfrak{A}_0$ по $\mathfrak{B} \cap \mathfrak{A}_0$. Поэтому f_0 можно однозначно продолжить до функции f на $\mathfrak{A}$, постоянной на каждом классе смежности в $\mathfrak{A}$ по $\mathfrak{B}$ и равной нулю вне $\mathfrak{B}\mathfrak{A}_0$. Если положить теперь $\mathbf{H}_0(f_0) = \mathbf{H}(f)$, то $\mathbf{H}_0$, очевидно, будет удовлетворять требованию нашей леммы.

С очевидными изменениями в обозначениях лемма и ее доказательство остаются верными и для распределения Хербранда на группе Галуа любого расширения поля K, не обязательно абелева. Но это нам не понадобится.

Поскольку канонический морфизм $\mathfrak{a}$ из $K^\times$ в $\mathfrak{A}$ изоморфно отображает $R^\times$ на $\mathfrak{A}_0$, мы можем с помощью обратного изоморфизма перенести на $R^\times$ распределение $\mathbf{H}_0$ из леммы 3. Тем самым мы определим некоторое распределение $\mathbf{H}_R$ на $R^\times$. Продолжим его до распределения $\mathbf{H}_K$ на $K^\times$, полагая $\mathbf{H}_K(X) = \mathbf{H}_R(X \cap R^\times)$ для каждого открытого и замкнутого подмножества X в $K^\times$. Мы будем называть $\mathbf{H}_K$ *распределением Хербранда* на $K^\times$. В очевидном смысле носитель этого распределения содержится в $R^\times$. В силу определения распределения $\mathbf{H}_0$ имеем $\mathbf{H}(f) = \mathbf{H}_K(f \circ \mathfrak{a})$ для каждой локально постоянной функции f на $\mathfrak{A}$ и $\mathbf{H}(X) = \mathbf{H}_K(\mathfrak{a}^{-1}(X))$ для каждого открытого и замкнутого подмножества X в $\mathfrak{A}$. Описание распределения $\mathbf{H}_K$ дается следующей теоремой.

Теорема 5. *Пусть $\mathbf{H}_K$ — распределение Хербранда на $K^\times$. Тогда его носитель совпадает с $R^\times$; $\mathbf{H}_K(R^\times) = 0$; $\mathbf{H}_K(1 + P^\nu) = \nu - (q-1)^{-1}$ при всех $\nu \geqslant 1$. Если $0 \leqslant \rho < \nu$, $\xi \in R^\times$ и $\operatorname{ord}_K(1 - \xi) = \rho$, то*

$$\mathbf{H}_K((1 + P^\nu)\,\xi) = -q^{\rho+1-\nu}(q-1)^{-1}.$$

По определению распределения Хербранда имеем $\mathbf{H}(\mathfrak{A}) = 0$. Отсюда $\mathbf{H}_K(K^\times) = 0$ и, следовательно, $\mathbf{H}_K(R^\times) = 0$. Пусть K_ν, N_ν, d_ν, e_ν таковы, как в предложении 13 и его следствии. Для подгруппы $\mathfrak{B}_\nu$ в $\mathfrak{A}$, соответствующей полю K_ν, по определению распределения Хербранда имеем $\mathbf{H}(\mathfrak{B}_\nu) = d_\nu/e_\nu$. Так как по следствию 2 теор. 4 § 3 $N_\nu = \mathfrak{a}^{-1}(\mathfrak{B}_\nu)$ и так как $N_\nu \cap R^\times = 1 + P^\nu$,

отсюда и из следствия предл. 13 получаем для $\mathbf{H}_K(1+P^{\nu})$ значение, указанное в нашей теореме.

Наконец, пусть ξ таково, как в нашей теореме. Обозначим через λ автоморфизм поля K_{ν}, индуцированный автоморфизмом $\mathfrak{a}(\xi)$. По определению распределения Хербранда $\mathbf{H}(\mathfrak{R}_{\nu}, \mathfrak{a}(\xi))$ равно $-\nu(\lambda)/e_{\nu}$, или, что то же самое, $-i/e_{\nu}$, где i — наибольшее целое число, для которого $\lambda \in \mathfrak{g}_i^{(\nu)}$. По предложению 13 $i = q^{\rho}$, где ρ — наибольшее целое число, для которого $\lambda \in \mathfrak{a}_{\nu}(N_{\rho})$, другими словами, для которого $\xi \in N_{\rho}$; это ρ задается формулой $\rho = \operatorname{ord}_K(1-\xi)$. С другой стороны, $\mathbf{H}(\mathfrak{R}_{\nu}\mathfrak{a}(\xi))$ совпадает с $\mathbf{H}_K(N_{\nu}\xi)$ и с $\mathbf{H}_K((1+P^{\nu})\xi)$. Доказательство завершено.

Следствие 1. *Пусть χ — характер на $\mathfrak{A}$, и пусть P^f — ведущий идеал характера $\chi \circ \mathfrak{a}$ на $K^{\times}$. Тогда* $f = \mathbf{H}(\chi) = \mathbf{H}_K(\chi \circ \mathfrak{a})$.

Положим $\omega = \chi \circ \mathfrak{a}$. Если $f = 0$, то характер ω тривиален на $R^{\times}$, так что $\mathbf{H}_K(\omega) = \mathbf{H}_K(R^{\times}) = 0$ по теореме 5. Предположим теперь, что $f \geqslant 1$, и обозначим через φ_0 характеристическую функцию множества $R^{\times}$, а через φ_i — характеристическую функцию множества $1+P^i$, $1 \leqslant i \leqslant f$. Тогда

$$\mathbf{H}_K(\omega) = \sum_{i=0}^{f-1} \mathbf{H}_K((\varphi_i - \varphi_{i+1})\omega) + \mathbf{H}_K(\varphi_f \omega).$$

По определению ведущего идеала характер ω тривиален на $1+P^f$, так что последний член равен $\mathbf{H}_K(1+P^f)$, или же $f-(q-1)^{-1}$ по теореме 5. По той же теореме 5, с учетом того факта, что характер ω постоянен на каждом классе смежности в $R^{\times}$ по $1+P^f$, имеем при $0 \leqslant i \leqslant f-1$

$$\mathbf{H}_K((\varphi_i - \varphi_{i+1})\omega) = -q^{i+1-f}(q-1)^{-1}(S_i - S_{i+1}),$$

где S_i равняется сумме $\sum \omega(\xi)$, взятой по полному множеству представителей классов смежности в $R^{\times}$ по модулю $1+P^f$, если $i=0$, или классов смежности в $1+P^i$ по модулю $1+P^i$, если $i \geqslant 1$. По определению ведущего идеала характер ω нетривиален на $R^{\times}$ и на $1+P^i$ при любом $i<f$. Поэтому $S_i = 0$ при $i<f$ и $S_f = 1$. Отсюда немедленно вытекает наше утверждение.

Следствие 2. *Пусть L — абелево расширение конечной степени над K, и пусть $\omega_1, \ldots, \omega_n$ — все различные характеры на $K^{\times}$, тривиальные на подгруппе $N(L) = \mathrm{N}_{L/K}(L^{\times})$ в $K^{\times}$, ассоциированной с L. Для каждого i обозначим через P^{f_i} ведущий идеал*

характера ω_i. *Тогда дискриминант поля* L *над* K *равен* P^{δ}, *где* $\delta = \sum_i f_i$.

Обозначим через $\mathfrak{B}$ замыкание подгруппы $\mathfrak{a}(N(L))$ в $\mathfrak{A}$. По следствию 2 теор. 4 § 3 $\mathfrak{B}$ является подгруппой в $\mathfrak{A}$, соответствующей полю L, и $\mathfrak{a}$ определяет изоморфизм группы $K^{\times}/N(L)$ на $\mathfrak{A}/\mathfrak{B}$. Поэтому для всякого i имеем $\omega_i = \chi_i \circ \mathfrak{a}$, где χ_i — характер на $\mathfrak{A}$, тривиальный на $\mathfrak{B}$. Тогда χ_i, $1 \leqslant i \leqslant n$, исчерпывают все характеры на $\mathfrak{A}$, тривиальные на $\mathfrak{B}$, так что характеристическая функция подмножества $\mathfrak{B}$ в $\mathfrak{A}$ равна $n^{-1}\sum_i \chi_i$. Обозначим через e, f и d соответственно индекс ветвления, модулярную степень и показатель дифференты поля L над K. Тогда $n = ef$ и по следствию предл. 6 гл. VIII-2 дискриминант поля L над K равен P^{fd}. По определению распределения Хербранда имеем $\mathbf{H}(\mathfrak{B}) = d/e$, что можно записать еще так:

$$d/e = \mathbf{H}\left(n^{-1}\sum_i \chi_i\right) = n^{-1}\sum_i \mathbf{H}(\chi_i).$$

Поэтому $fd = \sum_i f_i$ согласно следствию 1, чем и завершается наше доказательство.

§ 5. ПЕРЕНОС

В принятых выше обозначениях пусть K' — расширение конечной степени над K. Обозначим через $\mathfrak{a}$ и $\mathfrak{a}'$ канонические морфизмы из $K^{\times}$ в $\mathfrak{A}$ и из $K'^{\times}$ в $\mathfrak{A}'$ соответственно. Поскольку морфизм $\mathfrak{a}$ инъективен, мы можем определить отображение t образа $\mathfrak{a}(K^{\times})$ группы $K^{\times}$ в $\mathfrak{A}$ в образ $\mathfrak{a}'(K'^{\times})$ группы $K'^{\times}$ в $\mathfrak{A}'$ с помощью соотношения $t(\mathfrak{a}(\theta)) = \mathfrak{a}'(\theta)$ для каждого $\theta \in K^{\times}$, другими словами, с помощью соотношения $t \circ \mathfrak{a} = \mathfrak{a}' \circ j$, где j — естественное вложение группы $K^{\times}$ в $K'^{\times}$. Возникает вопрос, можно ли охарактеризовать это отображение в теоретико-групповых терминах и можно ли его продолжить по непрерывности до морфизма t из $\mathfrak{A}$ в $\mathfrak{A}'$. На этот вопрос сейчас будет дан положительный ответ. Для простоты мы будем предполагать, что расширение K' сепарабельно над K; в общем случае формулировки сложнее, а результаты ничуть не ценнее.

Итак, пусть K' — подполе в K_{sep} конечной степени n над K. Как и прежде, обозначим через $\mathfrak{G}'$ подгруппу в $\mathfrak{G}$, соответствующую полю K', и отождествим $\mathfrak{A}$ с $\mathfrak{G}/\mathfrak{G}^{(1)}$ и $\mathfrak{A}'$ с $\mathfrak{G}'/\mathfrak{G}'^{(1)}$. Мы покажем, что искомый морфизм представляет собой не что иное,

как так называемый *морфизм переноса* t из $\mathfrak{A}$ в $\mathfrak{A}'$. Напомним, что этот морфизм определяется следующим образом. Возьмем полное множество $\{\sigma_1, \ldots, \sigma_n\}$ представителей правых классов смежности $\sigma\mathfrak{G}'$ в $\mathfrak{G}$ по $\mathfrak{G}'$. Для каждого $\sigma \in \mathfrak{G}$ отображение $\sigma_i\mathfrak{G}' \to \sigma\sigma_i\mathfrak{G}'$ является перестановкой этих классов смежности, так что для всякого i имеет место равенство $\sigma\sigma_i\mathfrak{G}' = \sigma_{j(i)}\mathfrak{G}'$, где $i \to j(i)$ — перестановка множества $\{1, \ldots, n\}$, которое можно переписать еще так: $\sigma\sigma_i = \sigma_{j(i)}\tau_i$, где $\tau_i \in \mathfrak{G}'$.

Далее, как легко заметить, образ элемента $\tau_1 \ldots \tau_n$ в $\mathfrak{A}' = \mathfrak{G}'/\mathfrak{G}'^{(1)}$ при каноническом морфизме группы $\mathfrak{G}'$ на $\mathfrak{A}'$ не зависит ни от выбора представителей σ_i, ни от их упорядочения. Поэтому если обозначить этот образ через $\alpha(\sigma)$, то отображение $\sigma \to \alpha(\sigma)$ из $\mathfrak{G}$ в $\mathfrak{A}'$ зависит только от $\mathfrak{G}$ и $\mathfrak{G}'$. Сразу видно, что $\alpha(\sigma\sigma') = \alpha(\sigma)\alpha(\sigma')$ при всех $\sigma, \sigma' \in \mathfrak{G}$. Кроме того, подгруппа $\mathfrak{G}''$ в $\mathfrak{G}$, состоящая из тех элементов σ, для которых $\sigma\sigma_i \in \sigma_i\mathfrak{G}'$ при всех i, является пересечением открытых подгрупп $\sigma_i\mathfrak{G}'\sigma_i^{-1}$, $1 \leqslant i \leqslant n$, и, следовательно, сама является открытой подгруппой в $\mathfrak{G}$. Поскольку отображение $\sigma \to \alpha(\sigma)$, очевидно, непрерывно на $\mathfrak{G}''$, оно непрерывно на $\mathfrak{G}$, а следовательно, является морфизмом группы $\mathfrak{G}$ в $\mathfrak{A}'$. Так как группа $\mathfrak{A}'$ коммутативна, ядро этого морфизма должно содержать $\mathfrak{G}^{(1)}$ так что он определяет некоторый морфизм t группы $\mathfrak{A} = \mathfrak{G}/\mathfrak{G}^{(1)}$ в $\mathfrak{A}'$, который по определению и является *гомоморфизмом переноса* из $\mathfrak{A}$ в $\mathfrak{A}'$.

Теорема 6. *Пусть K' — расширение конечной степени над K, содержащееся в K_{sep}; $\mathfrak{a}$, $\mathfrak{a}'$ — канонические морфизмы из $K^\times$ в $\mathfrak{A}$ и из $K'^\times$ в $\mathfrak{A}'$ соответственно; t — гомоморфизм переноса из $\mathfrak{A}$ в $\mathfrak{A}'$ и j — естественное вложение группы $K^\times$ в $K'^\times$. Тогда $t \circ \mathfrak{a} = \mathfrak{a}' \circ j$.*

Пусть $\mathfrak{G}$, $\mathfrak{G}'$ такие, как выше, L — любое расширение Галуа конечной степени над K, содержащее K' и содержащееся в K_{sep}, и пусть $\mathfrak{H}$ — подгруппа в $\mathfrak{G}$, соответствующая расширению L. Тогда $\mathfrak{H}$ — открытая нормальная подгруппа в $\mathfrak{G}$, содержащаяся в $\mathfrak{G}'$. Группа Галуа поля L над K равна $\mathfrak{g} = \mathfrak{G}/\mathfrak{H}$, и подгруппой в $\mathfrak{g}$, соответствующей полю K', служит $\mathfrak{g}' = \mathfrak{G}'/\mathfrak{H}$. Пусть K'' — любое поле, промежуточное между K и L, и пусть $\mathfrak{G}''$ и $\mathfrak{g}'' = \mathfrak{G}''/\mathfrak{H}$ — подгруппы в $\mathfrak{G}$ и в $\mathfrak{g}$ соответственно, соответствующие полю K''. Канонический морфизм $\mathfrak{a}''$ для K'' является поэтому морфизмом из $K''^\times$ в $\mathfrak{A}'' = \mathfrak{G}''/\mathfrak{G}''^{(1)}$, который каждому $\xi \in K''^\times$ сопоставляет автоморфизм $\mathfrak{a}''(\xi)$ поля K''_{ab} над K''; мы будем обозначать через $\mathfrak{b}(K''; \xi)$ автоморфизм поля $L \cap K''_{\mathrm{ab}}$ над K'', индуцированный на этом поле автоморфизмом $\mathfrak{a}''(\xi)$. Поскольку подгруппой в $\mathfrak{G}$, соответствующей полю $L \cap K''_{\mathrm{ab}}$, является $\mathfrak{H}\mathfrak{G}''^{(1)}$, то отоб-

ражение $\xi \to \mathfrak{b}(K''; \xi)$ есть морфизм из $K''^{\times}$ в группу $\mathfrak{G}''/\mathfrak{H}\mathfrak{G}''^{(1)}$. Ясно, что последнюю группу можно отождествить с $\mathfrak{g}''/\mathfrak{g}''^{(1)}$, где $\mathfrak{g}''^{(1)}$ — коммутант группы $\mathfrak{g}''$. В частности, $\theta \to \mathfrak{b}(K; \theta)$ — морфизм из $K^{\times}$ в $\mathfrak{g}/\mathfrak{g}^{(1)}$. Будем обозначать через t_0 гомоморфизм переноса, определенный для $\mathfrak{g}$ и $\mathfrak{g}'$ точно так же, как гомоморфизм t был определен выше для $\mathfrak{G}$ и $\mathfrak{G}'$; это — морфизм из $\mathfrak{g}/\mathfrak{g}^{(1)}$ в $\mathfrak{g}'/\mathfrak{g}'^{(1)}$. Наша теорема будет доказана, если мы покажем, что $\mathfrak{b}(K'; \theta) = t_0(\mathfrak{b}(K; \theta))$ при всех $\theta \in K^{\times}$. Действительно, отсюда следует, что $\mathfrak{a}'(\theta)$ может отличаться от $t(\mathfrak{a}(\theta))$ лишь на элемент из образа группы $\mathfrak{H}\mathfrak{G}'^{(1)}$ в $\mathfrak{G}'/\mathfrak{G}'^{(1)}$, т. е. на элемент, сколь угодно близкий к единице, ибо мы можем в качестве $\mathfrak{H}$ взять сколь угодно малую открытую подгруппу в $\mathfrak{G}'$, являющуюся нормальной подгруппой в $\mathfrak{G}$.

Будем обозначать через h, h' канонические морфизмы из $\mathfrak{g}$ на $\mathfrak{g}/\mathfrak{g}^{(1)}$ и из $\mathfrak{g}'$ на $\mathfrak{g}'/\mathfrak{g}'^{(1)}$ соответственно. Морфизм h совпадает с *морфизмом ограничения*, который каждому автоморфизму поля L над K сопоставляет его ограничение на $L \cap K_{\mathrm{ab}}$; морфизм h' можно интерпретировать аналогичным образом. Если теперь K'' — некоторое поле между K и L, соответствующее подгруппе $\mathfrak{g}''$ в $\mathfrak{g}$, то $K'' \cap K_{\mathrm{ab}}$ — подполе в L, соответствующее подгруппе $\mathfrak{g}''\mathfrak{g}^{(1)}$ в $\mathfrak{g}$, или, что эквивалентно, подполе в $L \cap K_{\mathrm{ab}}$, соответствующее подгруппе $h(\mathfrak{g}'')$ в группе Галуа $\mathfrak{g}/\mathfrak{g}^{(1)}$ поля $L \cap K_{\mathrm{ab}}$ над K. Следовательно, в силу теоремы 4 §3 и нашего определения $\mathfrak{b}(K; \theta)$ подгруппа $\mathrm{N}_{K''/K}(K''^{\times})$ в $K^{\times}$ состоит из тех элементов θ в $K^{\times}$, для которых $\mathfrak{b}(K; \theta)$ лежит в $h(\mathfrak{g}'')$. Предположим теперь, что группа $\mathfrak{g}''$ коммутативна, так что $\xi \to \mathfrak{b}(K''; \xi)$ отображает $K''^{\times}$ в $\mathfrak{g}''$. Тогда, аналогичным образом, применяя к K и K'' следствие 1 теор. 2 §2, мы видим, что при всех $\xi \in K''^{\times}$ имеет место равенство

$$h(\mathfrak{b}(K''; \xi)) = \mathfrak{b}(K; \mathrm{N}_{K''/K}(\xi)). \tag{5}$$

Если $K'' \supset K'$, т. е. $\mathfrak{g}'' \subset \mathfrak{g}'$, то имеет место аналогичная формула с K', h' вместо K и h.

Для заданного $\theta \in K^{\times}$ мы можем теперь выбрать циклическую подгруппу Γ в $\mathfrak{g}$, для которой $\mathfrak{b}(K; \theta)$ лежит в $h(\Gamma)$; в качестве Γ можно взять, скажем, группу, порожденную любым автоморфизмом $\gamma \in \mathfrak{g}$, для которого $h(\gamma) = \mathfrak{b}(K; \theta)$. Тогда, как мы видели выше, если Z — подполе в L, соответствующее группе Γ, то θ можно записать в виде $\mathrm{N}_{Z/K}(\zeta)$, где $\zeta \in Z^{\times}$. Возьмем полное множество представителей $\{\lambda_1, \ldots, \lambda_r\}$ двойных классов смежности $\Gamma\lambda\mathfrak{g}'$ в $\mathfrak{g}$ по Γ и $\mathfrak{g}'$ и обозначим через γ_1 какую-нибудь образующую группы Γ. Для всякого i двойной класс смежности $\Gamma\lambda_i\mathfrak{g}'$ является объединением по $\gamma \in \Gamma$ правых классов смежности $\gamma\lambda_i\mathfrak{g}'$

по $\mathfrak{g}'$. Если $\gamma, \gamma' \in \Gamma$, то $\gamma\lambda_i\mathfrak{g}'$ совпадает с $\gamma'\lambda_i\mathfrak{g}'$ в том и только в том случае, когда $\gamma^{-1}\gamma'$ лежит в группе $\Gamma_i = \Gamma \cap \lambda_i\mathfrak{g}'\lambda_i^{-1}$. Обозначим через d_i индекс подгруппы Γ_i в Γ. Очевидно, Γ_i порождается элементом $\gamma_1^{d_i}$, причем d_i является также наименьшим числом среди всех целых d, для которых $\lambda_i^{-1}\gamma_1^d\lambda_i \in \mathfrak{g}'$. Таким образом, $\Gamma\lambda_i\mathfrak{g}'$ является дизъюнктным объединением классов смежности $\gamma_1^j\lambda_i\mathfrak{g}'$ по $0 \leqslant j < d_i$. Следовательно, элементы $\gamma_1^j\lambda_i$, $1 \leqslant i \leqslant r$, $0 \leqslant j < d_i$, образуют полное множество представителей правых классов смежности в $\mathfrak{g}$ по $\mathfrak{g}'$, и мы можем использовать это множество для вычисления переноса $t_0(\gamma)$ любого элемента $\gamma \in \Gamma$. Беря прежде всего $\gamma = \gamma_1$, сразу находим, что в этом случае

$$t_0(\gamma) = h'\left(\prod_{i=1}^{r}(\lambda_i^{-1}\gamma^{d_i}\lambda_i)\right) = \prod_{i=1}^{r} h'(\lambda_i^{-1}\gamma^{d_i}\lambda_i). \tag{6}$$

Это соотношение, будучи верным для $\gamma = \gamma_1$, остается, очевидно, верным также и для $\gamma = \gamma_1^j$ при всех j, другими словами, для всех $\gamma \in \Gamma$.

Для всякого i положим $Z_i = Z^{\lambda_i}$ и обозначим через Z_i' композит полей Z_i и K'. Ясно, что (λ_i, Z_i') — собственное вложение поля Z над K' в смысле гл. III-2. Пусть (λ, Z') — любое такое вложение. Заменяя его в случае надобности на эквивалентное, можно считать, что Z' содержится в K_{sep} и, следовательно, в L, так что изоморфизм λ из Z в Z' можно продолжить до автоморфизма λ поля L над K. Вложение (λ, Z') эквивалентно вложению (λ_i, Z_i') в том и только в том случае, когда существует K'-линейный изоморфизм поля Z' в Z_i', который мы можем тогда продолжить до такого автоморфизма σ поля L над K', что λ совпадает с $\lambda_i\sigma$ на Z. Поэтому $\lambda = \gamma\lambda_i\sigma$, где $\gamma \in \Gamma$ и $\sigma \in \mathfrak{g}'$. Следовательно, вложение (λ, Z') эквивалентно одному и только одному вложению (λ_i, Z_i'). Далее, предложение 4 гл. III-3 дает

$$\theta = \mathrm{N}_{Z/K}(\xi) = \prod_{i=1}^{r} \mathrm{N}_{Z_i'/K'}(\xi^{\lambda_i}).$$

Поскольку для всякого i к K' и к $K'' = Z_i'$ применима формула (5), мы видим, что

$$\mathfrak{b}(K'; \theta) = \prod_{i=1}^{r} h'(\mathfrak{b}(Z_i'; \xi^{\lambda_i})). \tag{7}$$

Положим $\gamma = \mathfrak{b}(Z; \xi)$. По определению $\mathfrak{b}$ этот элемент лежит в Γ. Поэтому согласно следствию 5 теор. 1 § 2 имеем

$$\mathfrak{b}(Z_i, \xi^{\lambda_i}) = \lambda_i^{-1}\gamma\lambda_i.$$

Мы можем теперь применить формулу (5) к полям Z_i, Z_i' вместо полей K, K'', заменяя одновременно h на тождественное отображение, ибо группа Галуа поля L над Z_i совпадает с коммутативной группой $\lambda_i^{-1}\Gamma\lambda_i$. Группа Галуа поля L над Z_i' является пересечением последней группы с группой $\mathfrak{g}'$. В тех же обозначениях, что и прежде, это пересечение совпадает с $\lambda_i^{-1}\Gamma_i\lambda_i$ и имеет индекс d_i в $\lambda_i^{-1}\Gamma\lambda_i$, так что d_i есть степень поля Z_i' над Z_i. Так как ζ^{λ_i} содержится в Z_i, то $N_{Z_i'/Z_i}(\zeta^{\lambda_i}) = (\zeta^{\lambda_i})^{d_i}$. Поэтому формула (5), примененная к Z_i, Z_i' и ζ^{λ_i}, дает

$$\mathfrak{b}(Z_i'; \zeta^{\lambda_i}) = \mathfrak{b}(Z_i; (\zeta^{\lambda_i})^{d_i}) = (\lambda_i^{-1}\gamma\lambda_i)^{d_i}.$$

Ввиду (6) и (7) отсюда сразу вытекает наше утверждение.

ГЛАВА ТРИНАДЦАТАЯ

ГЛОБАЛЬНАЯ ТЕОРИЯ ПОЛЕЙ КЛАССОВ

§ 1. КАНОНИЧЕСКОЕ СПАРИВАНИЕ

В этой главе k будет некоторым **A**-полем и будут использоваться те же обозначения, что и в предыдущих главах, например k_v, r_v, q_v, $k_{\mathbf{A}}$ и т. д. Возьмем какое-нибудь алгебраическое замыкание $\bar{k}$ поля k и для всякой точки v поля k выберем алгебраическое замыкание K_v поля k_v, содержащее $\bar{k}$. Обозначим через k_{sep}, $k_{v,\,\mathrm{sep}}$ максимальные сепарабельные расширения поля k в $\bar{k}$ и поля k_v в K_v соответственно. Через k_{ab}, $k_{v,\,\mathrm{ab}}$ обозначим максимальные абелевы расширения поля k в k_{sep} и поля k_v в $k_{v,\,\mathrm{sep}}$ соответственно. Из леммы 1 гл. XI-3 легко можно было бы вывести, что $k_{v,\,\mathrm{sep}}$ порождается над k_v полем k_{sep} и что поэтому K_v порождается над k_v полем $\bar{k}$; кроме того, как мы увидим в § 9 этой главы, $k_{v,\mathrm{ab}}$ порождается над k_v полем k_{ab}; но все эти факты использоваться не будут.

Мы обозначаем через $\mathfrak{G}$ и $\mathfrak{A} = \mathfrak{G}/\mathfrak{G}^{(1)}$ группы Галуа полей k_{sep} и k_{ab} соответственно над полем k; мы обозначаем через $\mathfrak{G}_v$ и $\mathfrak{A}_v = \mathfrak{G}_v/\mathfrak{G}_v^{(1)}$ группы Галуа полей $k_{v,\,\mathrm{sep}}$ и $k_{v,\,\mathrm{ab}}$ соответственно над полем k_v. Через ρ_v мы обозначаем морфизм ограничения из $\mathfrak{G}_v$ в $\mathfrak{G}$, а также, как объяснялось в гл. XII-1, и морфизм ограничения из $\mathfrak{A}_v$ в $\mathfrak{A}$. Через X_k обозначается группа характеров на $\mathfrak{G}$, или, что то же самое, на $\mathfrak{A}$. Для всякого $\chi \in X_k$ мы полагаем $\chi_v = \chi \circ \rho_v$; это — характер на $\mathfrak{G}_v$, или, что то же самое, на $\mathfrak{A}_v$.

Предложение 1. *Возьмем любой характер $\chi \in X_k$ и обозначим через L циклическое расширение поля k, связанное с χ. Пусть v — произвольная точка поля k, L' — циклическое расширение поля k_v, связанное с $\chi_v = \chi \circ \rho_v$, w — любая точка поля L, лежащая над v. Тогда существует k_v-линейный изоморфизм поля L' на L_w.*

Как было замечено в гл. IX-4, L' является композитом полей L и k_v в K_v. Так как поле L' имеет конечную степень над k_v, оно является локальным полем, и предложение 1 гл. III-1 показывает,

что L плотно в нем. Поэтому оно является пополнением поля L относительно некоторой точки, лежащей над v. Наше заключение сразу вытекает поэтому из следствия 4 теор. 4 гл. III-4.

Следствие. *В обозначениях предложения* 1 *характер* χ_v *неразветвлен почти для всех* v. *Если характер* χ_v *тривиален почти для всех* v, *то и характер* χ *тривиален.*

Первое утверждение сразу вытекает из теоремы 1 гл. VIII-4 в сочетании с предложением 1. Второе аналогичным образом вытекает из следствия 4 теор. 2 гл. VII-5, если там в качестве V взять множество всех конечных точек v поля k, для которых характер χ_v тривиален.

К k_v и χ_v применимы определения и результаты гл. XII-2. Для любого $z \in k_v^\times$ мы будем писать $(\chi_v, z)_v$ вместо $(\chi_v, z)_{k_v}$. Канонический морфизм из $k_v^\times$ в $\mathfrak{A}_v$ будем обозначать через $\mathfrak{a}_v$. Для всех $z \subset k_v^\times$ имеем $(\chi_v, z)_v = \chi_v(\mathfrak{a}_v(z))$. Автоморфизм $\rho_v(\mathfrak{a}_v(z))$ поля k_{ab} над k для каждого $z \in k_v^\times$ индуцирован автоморфизмом $\mathfrak{a}_v(z)$ поля $k_{v,\mathrm{ab}}$ над k_v.

Возьмем теперь $z = (z_v) \in k_{\mathbf{A}}^\times$. Почти для всех v компонента z_v лежит в $r_v^\times$ и по следствию предл. 1 характер χ_v неразветвлен, так что $(\chi_v, z_v)_v = 1$ по следствию 4 теор. 1 гл. XII-2. Поэтому в произведении

$$(\chi, z)_k = \prod_v (\chi_v, z_v)_v, \tag{1}$$

взятом по всем точкам поля k, почти все сомножители равны 1, так что это произведение корректно определено. Из непрерывности отображения $z_v \to (\chi_v, z_v)_v$ для всякой точки v с учетом упомянутых выше фактов вытекает непрерывность на $k_{\mathbf{A}}^\times$ отображения $z \to (\chi, z)_k$. Поэтому последнее отображение является характером на $k_{\mathbf{A}}^\times$. Порядок этого характера конечен, потому что он делит порядок характера χ. Спаривание группы X_K с $k_{\mathbf{A}}^\times$, задаваемое формулой (1), будем называть *каноническим спариванием* для k. Ясно, что оно удовлетворяет условию [I] гл. XII-1. Что касается условия [II], предположим, что характер $z \to (\chi, z)_k$ тривиален на $k_{\mathbf{A}}^\times$; тогда характер $z_v \to (\chi_v, z_v)_v$ должен быть тривиальным для каждой точки v. Так как [II] выполняется для локальных полей, отсюда следует тривиальность всех характеров χ_v, откуда по следствию предл. 1 вытекает тривиальность характера χ. Таким образом, условие [II] для спаривания (1) также выполняется.

Как объяснялось в гл. XII-1, мы можем определить *канонический морфизм* $\mathfrak{a}$ *группы* $k_{\mathbf{A}}^{\times}$ в $\mathfrak{A}$, полагая

$$\chi(\mathfrak{a}(z)) = (\chi, z)_k = \coprod_v (\chi_v, z_v)_v \tag{2}$$

для всех $z = (z_v) \in k_{\mathbf{A}}^{\times}$ и всех $\chi \in X_k$. Согласно условию [II″] гл. XII-1, $\mathfrak{a}$ отображает $k_{\mathbf{A}}^{\times}$ на всюду плотную подгруппу в $\mathfrak{A}$.

Предложение 2. *Пусть* j_v *— естественное вложение группы* $k_v^{\times}$ *в* $k_{\mathbf{A}}^{\times}$, *отображающее* $k_v^{\times}$ *на квазисомножитель* $k_v^{\times}$ *в* $k_{\mathbf{A}}^{\times}$. *Тогда* $\mathfrak{a} \circ j_v = \rho_v \circ \mathfrak{a}_v$.

В самом деле, если $z_v \in k_v^{\times}$, то $z = j_v(z_v)$ — идель, координаты которого все равны 1, за исключением одной координаты, соответствующей точке v, которая равна z_v. Положим $\alpha = \mathfrak{a}_v(z_v)$. Формула (2) дает

$$\chi(\mathfrak{a}(z)) = (\chi_v, z_v)_v = \chi_v(\alpha) = \chi(\rho_v(\alpha)).$$

Так как это имеет место для всех характеров χ на $\mathfrak{A}$, то $\mathfrak{a}(z) = \rho_v(\alpha)$, что и требовалось доказать.

Теорема 1. *Пусть* k' *— расширение конечной степени над* k, *содержащееся в* k, $\mathfrak{G}$ *и* $\mathfrak{G}'$ *— группы Галуа полей* k_{sep} *над* k *и* k'_{sep} *над* k' *соответственно и* ρ *— морфизм ограничения из* $\mathfrak{G}'$ *в* $\mathfrak{G}$. *Тогда для каждого характера* $\chi \in X_k$ *и каждого* $z' \in k'^{\times}_{\mathbf{A}}$ *имеем*

$$(\chi \circ \rho, z')_{k'} = (\chi, \mathrm{N}_{k'/k}(z'))_k.$$

В силу наших определений эта теорема немедленно следует из теоремы 2 гл. XII-2 в сочетании со следствием 3 теор. 1 гл. IV-1.

Следствие 1. *Если* $\mathfrak{a}$ *и* $\mathfrak{a}'$ *— канонические морфизмы для* k *и для* k' *соответственно, то* $\rho \circ \mathfrak{a}' = \mathfrak{a} \circ \mathrm{N}_{k'/k}$.

Это просто переформулировка теоремы 1.

Следствие 2. *В предположениях и обозначениях теоремы* 1 $\mathrm{N}_{k'/k}(k'^{\times}_{\mathbf{A}})$ *содержится в ядре характера* $\chi \circ \mathfrak{a}$ *тогда и только тогда, когда* k' *содержит циклическое расширение поля* k, *связанное с* χ.

В самом деле, теорема 1 показывает, что $\mathrm{N}_{k'/k}(k'^{\times}_{\mathbf{A}})$ содержится в этом ядре в том и только в том случае, когда характер $\chi \circ \rho \circ \mathfrak{a}'$ тривиален, а значит, ввиду [II] в том и только в том случае, когда тривиален характер $\chi \circ \rho$. Пусть L — циклическое расширение поля k, связанное с χ. Тогда циклическим расширением поля k', связанным с $\chi \circ \rho$, будет композит L' полей k' и L, и характер

$\chi \circ \rho$ тривиален в том и только в том случае, когда $L' = k'$, т. е. когда $k' \supset L$.

В этой главе нашим основным делом будет нахождение ядра канонического морфизма $\mathfrak{a}$. Пока мы заметим лишь, что для каждой точки v это ядро должно содержаться в ядре морфизма $\mathfrak{a}_v$, каковое равно $\{1\}$, если точка v конечна, но совпадает с $\mathbf{R}_+^\times$, если точка v вещественна, и совпадает с $\mathbf{C}^\times$, если точка v мнима. Будем обозначать через $k_{\infty+}^\times$ произведение последних ядер, т. е. группу тех иделей (z_v), для которых $z_v = 1$ для каждой конечной точки v и $z_v > 0$ для каждой вещественной точки v. Эта группа содержится в ядре морфизма $\mathfrak{a}$; разумеется, она сводится к $\{1\}$, если k — поле характеристики $p > 1$.

Дадим теперь для некоторых частных случаев явную формулу для $(\chi, z)_k$. Сначала рассмотрим поле k характеристики $p > 1$. Пусть F — поле констант в k, q — число элементов в F и $\bar{F}$ — алгебраическое замыкание поля F в $\bar{k}$. По теореме 2 гл. I-1 $\bar{F}^\times$ есть группа корней из 1 в $\bar{k}$, причем все эти корни имеют порядок, взаимно простой с p. Через k_0 будем обозначать композит полей k и $\bar{F}$, через $\mathfrak{H}_0$ — подгруппу в $\mathfrak{G}$, соответствующую полю k_0, и через X_0 — подгруппу в X_k, состоящую из всех характеров на $\mathfrak{G}$, тривиальных на $\mathfrak{H}_0$. Ясно, что каждое расширение конечной степени над k, содержащееся в k_0, порождено над k конечным множеством элементов из $\bar{F}$, а следовательно, некоторым расширением F' конечной степени над F. Более точно, имеет место следующая

Лемма 1. *Пусть F' — расширение степени n над F, содержащееся в $\bar{k}$. Тогда композит k' полей k и F' является циклическим расширением степени n над k, поле констант этого расширения совпадает с F' и морфизм ограничения группы Галуа поля k' над k в группу Галуа поля F' над F является изоморфизмом этих двух групп.*

Обозначим через F'' поле констант в k', через n' — степень поля k' над k и через n'' — степень поля F'' над F; ясно, что $n' \leqslant n \leqslant n''$. Возьмем такое $\zeta \in F''$, что $F'' = F(\zeta)$, и обозначим через P неприводимый унитарный многочлен в $F[X]$ с корнем ζ. Если Q — нормированный многочлен в $k[X]$, делящий P в $k[X]$, то все его корни лежат в $\bar{F}$, так что его коэффициенты лежат в $\bar{F} \cap k$, т. е. в F. Поэтому многочлен P неприводим в $k[X]$, так что $n' \geqslant n''$, откуда $n' = n = n''$. Утверждение о группах Галуа можно поэтому рассматривать как частный случай следствия 1 предл. 3 гл. III-2

или как следствие равенства $k' = F' \otimes_F k$, которое немедленно вытекает из предложения 2 гл. III-2.

Если k и k' таковы, как в лемме 1, то мы говорим, что k' является *константным расширением* поля k. В силу теоремы 2 гл. I-1 для каждого целого числа $n \geqslant 1$ существует одно и только одно такое расширение степени n над k; мы будем обозначать это расширение через k_n. Тогда k_0 является объединением циклических расширений k_n по всем $n \geqslant 1$. В частности k_0 содержится в k_{ab}. Будем обозначать через $\mathfrak{A}_0$ подгруппу в $\mathfrak{A}$, соответствующую полю k_0, т. е. группу Галуа поля k_{ab} над k_0. Мы можем рассматривать X_0 как группу всех характеров на $\mathfrak{A}$, тривиальных на $\mathfrak{A}_0$. Характер $\chi \in X_k$ принадлежит X_0 в том и только в том случае, когда циклическое расширение поля k, связанное с χ, содержится в k_0, и, следовательно, в том и только в том случае, когда это расширение совпадает с одним из полей k_n.

Из следствия 2 теор. 2 гл. I-1 в сочетании с леммой 1 вытекает, что для каждого $n \geqslant 1$ существует один и только один автоморфизм поля k_n над k, индуцирующий на поле констант $F_n = \bar{F} \cap k_n$ в k_n автоморфизм $x \to x^q$, где q, как и прежде,— число элементов в поле F; кроме того, этот автоморфизм порождает группу Галуа поля k_n над k. Значит, существует один и только один автоморфизм φ_0 поля k_0 над k, индуцирующий на $\bar{F}$ автоморфизм $x \to x^q$. Этот автоморфизм будем называть *автоморфизмом Фробениуса* поля k_0 над k. Каждый автоморфизм φ поля k_{sep} над k, индуцирующий φ_0 на k_0, будем называть *автоморфизмом Фробениуса* поля k_{sep} над k. Очевидно, автоморфизмы Фробениуса поля k_{sep} над k образуют класс смежности $\mathfrak{H}_0\varphi$ в $\mathfrak{G}$.

Предложение 3. *Пусть k — некоторое* **A**-*поле характеристики $p > 1$ с полем констант $F = \mathbf{F}_q$; χ — характер на $\mathfrak{G}$, принадлежащий X_0, т. е. такой, что циклическое расширение поля k, связанное с χ, является константным расширением поля k, и пусть φ — любой автоморфизм Фробениуса поля k_{sep} над k. Возьмем $z \in k_{\mathbf{A}}^{\times}$ и положим $|z|_{\mathbf{A}} = q^{-r}$. Тогда $(\chi, z)_k = \chi(\varphi)^r$.*

Положим $z = (z_v)$. Пусть v — точка поля k степени d, т. е. такая, что модуль q_v поля k_v равен q^d. Пусть L — циклическое расширение поля k, связанное с χ. Это расширение порождено над k некоторым расширением F' поля F, а следовательно, корнями из 1, порядок которых взаимно прост с p. Поэтому расширение поля k_v, связанное с χ_v, будучи порожденным над k_v полем F',

неразветвлено, так что характер χ_v неразветвлен. Далее, автоморфизм Фробениуса поля $k_{v,\,\mathrm{sep}}$ над k_v индуцирует на $\overline{F}$ автоморфизм $x \to x^{q^d}$ и потому совпадает с φ^d на $\overline{F}$, а значит, на k_0. По следствию 4 теор. 1 гл. XII-2 отсюда вытекает, что $(\chi_v, z_v)_v = \chi(\varphi^d)^{\nu}$, где $\nu = \mathrm{ord}_v(z_v)$. Но $|z_v|_v = q^{-d\nu}$ и $|z|_{\mathbf{A}} = \prod |z_v|_v$, и мы получаем наше утверждение.

Следствие 1. *В предположениях и обозначениях предложения 3 пусть* $\mathfrak{a}$ *— канонический морфизм для* k. *Тогда* $\mathfrak{a}(z)$ *совпадает с* φ^r *на* k_0.

В самом деле, эти автоморфизмы могут отличаться лишь на элемент, принадлежащий к ядрам всех характеров $\chi \in X_0$, а пересечение этих ядер совпадает с $\mathfrak{H}_0$ — группой, оставляющей k_0 инвариантным.

Следствие 2. *Если* $\chi \in X_0$ *и* $\theta \in k^{\times}$, *то* $(\chi, \theta)_k = 1$.

Это сразу вытекает из предложения 3 и того факта, что по теореме 5 гл. IV-4 $|\theta|_{\mathbf{A}} = 1$.

Следствие 3. *Характер* χ *на* $\mathfrak{G}$ *принадлежит* X_0 *тогда и только тогда, когда* $(\chi, z)_k = 1$ *при всех* $z \in k_{\mathbf{A}}^1$.

Если $\chi \in X_0$, то предложение 3 показывает, что χ обладает указанным свойством. Теперь предположим, что χ обладает этим свойством. По следствию 6 теор. 2 гл. VII-5 существует такое $z_1 \in k_{\mathbf{A}}^{\times}$, что $|z_1|_{\mathbf{A}} = q$; значит, группа $k_{\mathbf{A}}^{\times}$ порождена подгруппой $k_{\mathbf{A}}^1$ и элементом z_1. Пусть n — порядок характера χ. Тогда $(\chi, z_1)_k$ — примитивный корень n-й степени из 1 в $\mathbf{C}$. Поскольку φ индуцирует на k_n образующую группы Галуа поля k_n над k, существует характер χ', связанный с k_n, для которого $\chi'(\varphi) = (\chi, z_1)_k$. По предложению 3 имеем $(\chi', z_1)_k = \chi'(\varphi)^{-1}$, откуда $(\chi\chi', z_1)_k = 1$; поэтому $(\chi\chi', z)_k = 1$ при всех $z \in k_{\mathbf{A}}^{\times}$, в силу предложения 3 и нашего предположения относительно χ. Отсюда следует, что $\chi = \chi'^{-1}$, так что $\chi \in X_0$.

В случае когда k — поле характеристики нуль, не существует столь удобного инструмента исследования, каким являются константные расширения в случае характеристики $p > 1$. Наилучшим заменителем служат так называемые «циклотомические» расширения. Здесь мы рассмотрим лишь случай $k = \mathbf{Q}$. Тогда $\mathfrak{G}$ — группа Галуа поля $\overline{\mathbf{Q}} = \mathbf{Q}_{\mathrm{sep}}$ над $\mathbf{Q}$. Для $m \geqslant 1$ пусть ε—примитивный корень m-й степени из 1 в $\overline{\mathbf{Q}}$. Обозначим через $\mathfrak{H}_m$ подгруппу в $\mathfrak{G}$, соответствующую полю $\mathbf{Q}(\varepsilon)$, так что группа Галуа поля $\mathbf{Q}(\varepsilon)$

над $\mathbf{Q}$ равна $\mathfrak{g} = \mathfrak{G}/\mathfrak{H}_m$. Как хорошо известно, $\mathfrak{g}$ состоит из автоморфизмов, определяемых подстановкой $\varepsilon \to \varepsilon^x$, где в качестве x берутся все целые числа по модулю m, взаимно простые с m. Таким образом, эту группу можно отождествить с $(\mathbf{Z}/m\mathbf{Z})^\times$, т. е. с мультипликативной группой кольца $\mathbf{Z}/m\mathbf{Z}$. Пусть χ — произвольный характер на $\mathfrak{g}$ с ядром $\mathfrak{h}$. Очевидным образом отождествим этот характер с характером на $\mathfrak{G}$, который обозначим также через χ. Последний характер имеет ядро $\mathfrak{H} \supset \mathfrak{H}_m$. С другой стороны, отождествляя $\mathfrak{g}$ с $(\mathbf{Z}/m\mathbf{Z})^\times$, мы отождествляем тем самым χ с некоторой функцией на последней группе и, значит, с некоторой функцией на множестве всех целых чисел, взаимно простых с m, которую мы также обозначим через χ и которая обладает тем свойством, что $\chi(ab) = \chi(a)\chi(b)$ для любых двух таких целых чисел a и b. Эту функцию можно однозначно продолжить до характера на подгруппе в $\mathbf{Q}^\times$, состоящей из дробей вида a/b, где $a, b \in \mathbf{Z}$ взаимно просты с m; последний характер будем обозначать тоже через χ. В этих обозначениях имеет место

Предложение 4. *Пусть характер χ таков, как выше, и пусть Z — циклическое расширение поля $\mathbf{Q}$, связанное с χ. Тогда для каждого простого числа p, не делящего m, характер χ_p неразветвлен и $(\chi_p, z)_p = \chi(|z|_p^{-1})$ для каждого $z \in \mathbf{Q}_p^\times$; для каждого $z \in \mathbf{R}^\times$ имеем $(\chi_\infty, z)_\infty = \chi(\operatorname{sgn} z)$.*

Пусть p — любое простое число, не делящее m, w — точка поля Z, лежащая над p, и u — точка поля $L = \mathbf{Q}(\varepsilon)$, лежащая над w. По предложению 1 гл. III-1 поле L_u порождено над $\mathbf{Q}_p$ элементом ε. Так как порядок m этого элемента не делится на p, поле L_u неразветвлено; поэтому неразветвлено и поле Z_w, а значит, в силу предложения 1 неразветвлен характер χ_p. Автоморфизм Фробениуса φ над $\mathbf{Q}_p$ алгебраического замыкания поля $\mathbf{Q}_p$ индуцирует на L_u и, следовательно, на L автоморфизм, определяемый подстановкой $\varepsilon \to \varepsilon^p$, так что в соответствии с данными выше объяснениями насчет обозначений $\chi(\varphi)$ совпадает с $\chi(p)$. Поэтому наше утверждение относительно $(\chi_p, z)_p$ немедленно вытекает из следствия 4 теор. 1 гл. XII-2 и равенства $|z|_p = p^{-\operatorname{ord}(z)}$.

Аналогично пусть w — точка поля Z, лежащая над точкой ∞ поля $\mathbf{Q}$, и u — точка поля L, лежащая над w. Если $m = 1$ или 2, то характер χ тривиален и наше последнее утверждение очевидно. Если $m > 2$, то поле $L_u = \mathbf{R}(\varepsilon) = \mathbf{C}$ имеет нетривиальный автоморфизм $x \to \bar{x}$ над $\mathbf{R}$. Этот автоморфизм определяется подстановкой $\varepsilon \to \varepsilon^{-1}$, так что если $\mathfrak{g}$ и $\mathfrak{h}$ таковы, как указано выше, то он индуцирует на Z_w автоморфизм, соответствующий образу -1 в $\mathfrak{g}/\mathfrak{h}$. Если $\chi(-1) = 1$, то -1 лежит в $\mathfrak{h}$, $Z_w = \mathbf{R}$ и характер χ_∞

тривиален; если $\chi(-1) = -1$, то -1 не лежит в $\mathfrak{h}$, $Z_w = \mathbf{C}$ и характер χ_∞ нетривиален. Отсюда и из результатов, сформулированных в начале гл. XII-2, сразу вытекает последнее утверждение предложения 4.

Следствие 1. *В принятых выше обозначениях и предположениях пусть w — точка поля Z. Если w лежит над рациональным простым числом p, не делящим m, то степень поля Z_w над $\mathbf{Q}_p$ равна порядку элемента $\chi(p)$ в группе $\mathbf{C}^\times$; если же w лежит над ∞, то степень поля Z_w над $\mathbf{R}$ равна порядку элемента $\chi(-1)$ в $\mathbf{C}^\times$.*

Последнее утверждение уже доказано выше. Что касается первого, то предложение 1 показывает, что наша степень равна порядку характера $z \to (\chi_p, z)_p$ на $\mathbf{Q}_p^\times$, откуда ввиду предложения 4 и следует доказываемое утверждение.

Следствие 2. *Пусть характер χ таков, как выше. Возьмем такое $z = (z_v) \in \mathbf{Q}_\mathbf{A}^\times$, что $\mathrm{ord}_p(z_p) = 0$ и $(\chi_p, z_p)_p = 1$ для каждого простого числа p, делящего m. Тогда $(\chi, z)_\mathbf{Q} = \chi(r(z))$, где $r(z)$ задается формулой*

$$r(z) = \mathrm{sgn}(z_\infty) \prod_p |z_p|_p^{-1}.$$

В последней формуле произведение берется по всем простым числам или (что приводит к тому же результату в силу наших предположений относительно z) по всем простым числам, не делящим m; поэтому значение $\chi(r(z))$ определено корректно. Наше утверждение сразу вытекает из предложения 4 и определений.

Следствие 3. *Пусть характер χ таков, как выше. Тогда для каждого простого числа p, делящего m, можно выбрать такую открытую подгруппу g_p в $\mathbf{Q}_p^\times$, что $(\chi, \xi)_\mathbf{Q} = 1$ при всех $\xi \in \bigcap (\mathbf{Q}^\times \cap g_p)$.*

Для всякого простого числа p, делящего m, пусть p^μ — наибольшая степень p, делящая m; тогда $1 + m\mathbf{Z}_p$ совпадает с подгруппой $1 + p^\mu \mathbf{Z}_p$ в $\mathbf{Q}_p^\times$. Возьмем теперь для всякого p, делящего m, в качестве g_p пересечение подгруппы $1 + m\mathbf{Z}_p$ в $\mathbf{Q}_p^\times$ с ядром морфизма $z \to (\chi_p, z)_p$ группы $\mathbf{Q}_p^\times$. Следствие 2 показывает, что для такого ξ, как указано в нашем следствии, $(\chi, \xi)_\mathbf{Q} = \chi(r(\xi))$. По теореме 5 гл. IV-4 $r(\xi)$ совпадает с $\mathrm{sgn}(\xi) \cdot |\xi|_m$, т. е. с ξ. Запишем ξ в виде $\xi = a/b$, где a, b из $\mathbf{Z}$ и $(a, b) = 1$. Если p — простое число, делящее m, то ξ лежит в $\mathbf{Z}_p$, так что b взаимно просто с p. Для p^μ, такого, как выше, ξ лежит в $1 + p^\mu \mathbf{Z}_p$, так что $a \equiv b$ по модулю p^μ. Поэто-

му a и b оба взаимно просты с m и $a \equiv b$ по модулю m. Следовательно, $\chi(a) = \chi(b)$, а значит в силу наших определений $\chi(\xi) = 1$, чем и завершается доказательство.

§ 2. ОДНА ЭЛЕМЕНТАРНАЯ ЛЕММА

Как и выше, пусть χ — характер на $(\mathbf{Z}/m\mathbf{Z})^\times$, рассматриваемый снова как функция на множестве целых чисел, взаимно простых с m. Сопоставим χ функцию ψ на $\mathbf{Z}$, для которой $\psi(x) = \chi(x)$, если x взаимно просто с m, и $\psi(x) = 0$ в противном случае. Обычно, допуская вольность речи, такую функцию ψ называют *мультипликативным характером по модулю* m, или, короче, *характером по модулю* m на $\mathbf{Z}$. Очевидно, что функция ψ на $\mathbf{Z}$ является таким характером в том и только в том случае, когда $\psi(x + m) = \psi(x)$ при всех $x \in \mathbf{Z}$, $\psi(x) = 0$ при $(x, m) \neq 1$, $\psi(1) = 1$ и $\psi(ab) = \psi(a)\psi(b)$ при всех a и b из $\mathbf{Z}$. Такой характер будем называть *тривиальным*, если он не принимает значений, отличных от 0 и 1, и *характером порядка* n, если тривиален характер ψ^n. Если ψ и ψ' — характеры по модулям m и m' соответственно, то $\psi\psi'$ будет характером по модулю mm'.

Цель этого параграфа — доказать лемму 3; эта лемма и ее доказательство принадлежат ван дер Вардену. Мы начнем с одного частного случая.

Лемма 2. *Пусть l — простое число, n — целое число $\geqslant 1$ и $a_1, \ldots, a_r$ — целые числа > 1. Тогда существует такой мультипликативный характер ψ на $\mathbf{Z}$, что $\psi(a_i)$ для каждого i является корнем из 1, порядок которого делится на l^n; более того, такой характер ψ можно выбрать так, чтобы его порядок был степенью числа l, а в случае $l = 2$ так, чтобы кроме того $\psi(-1) = 1$.*

Ясно, что порядок элемента $\psi(a_i)$ делится на порядок элемента $\psi(a_i^2)$. Если $l = 2$, заменим каждое a_i на a_i^2. Сделав это, мы можем считать, что в этом случае $a_i \equiv 0$ или 1 по модулю 4. Для всякого i определим теперь последовательность простых чисел $p_{i,\nu}$ ($\nu = 0, 1, \ldots$) следующим образом. Если $a_i \not\equiv 1$ по модулю l, то в качестве $p_{i,\nu}$ возьмем любой простой делитель целого числа

$$\frac{a_i^{l^{\nu+1}} - 1}{a_i^{l^\nu} - 1} = 1 + a_i^{l^\nu} + \ldots + a_i^{l^\nu(l-1)}. \tag{3}$$

Поскольку $l^{\nu+1} \equiv 1$ по модулю $l - 1$, то ясно, что числитель в левой части сравним с $a_i - 1$ по модулю l, значит он не делится на l,

а следовательно, $p_{i,\nu} \neq l$. С другой стороны, если $a_i \equiv 1$ по модулю l, то запишем $a_i^{l^\nu}$ в виде $a_i^{l^\nu} = 1 + l^\alpha b$, где $\alpha \geqslant 1$ и $b \not\equiv 0$ по модулю l; если $l = 2$, то $\alpha \geqslant 2$ в силу нашего предположения относительно a_i для этого случая. Имеем

$$a_i^{l^{\nu+1}} = (1 + l^\alpha b)^l \equiv 1 + l^{\alpha+1} b \qquad (l^{\alpha+2}).$$

Отсюда видно, что левая часть равенства (3) делится на l, но не на l^2, а из рассмотрения правой части этого равенства видно, что левая $> l$; в качестве $p_{i,\nu}$ мы можем поэтому взять любой простой делитель левой части, отличный от l.

Теперь покажем, что во всех случаях $p_{i,\nu}$ не может делить знаменатель в левой части равенства (3). В самом деле, в противном случае все члены в правой части были бы сравнимы с 1 по модулю $p_{i,\nu}$, так что правая часть была бы $\equiv l$ по модулю $p_{i,\nu}$, но поскольку она делится на $p_{i,\nu}$, а $p_{i,\nu} \neq l$, этого не может быть. Отсюда видно, что образ элемента a_i в группе $(\mathbf{Z}/p_{i,\nu}\mathbf{Z})^\times$ имеет порядок, в точности равный $l^{\nu+1}$; в частности, для всякого i все $p_{i,\nu}$ различны. Поэтому, если целое число ρ таково, что $l^\rho > r$, можем для всякого i выбрать такое целое число $\nu_i \geqslant n + \rho - 2$, что простые числа $p_i = p_{i,\nu_i}$ не делят ни одно из чисел $a_1, \ldots, a_r$. Для всякого i группа $(\mathbf{Z}/p_i\mathbf{Z})^\times$ является циклической группой порядка $p_i - 1$, и образ элемента a_i в этой группе имеет порядок l^{ν_i+1}. Обозначим через χ_i образующую группы характеров на этой группе, и пусть l^{λ_i} — наибольшая степень числа l, делящая $p_i - 1$. Положим $\mu = \lambda_i - \nu_i + n + \rho - 2$, $m = l^{-\mu}(p_i - 1)$ и $\chi_i' = \chi_i^m$; ясно, что $\lambda_i > \nu_i$, так что $\mu > 0$. Тогда χ_i' — характер порядка l^μ, и легко проверяется, что $\chi_i'(a_i)$ является корнем из 1 порядка $l^{n+\rho-1}$. Для всякого i продолжим, как объяснялось выше, характер χ_i' до мультипликативного характера ψ_i по модулю p_i на $\mathbf{Z}$. Пусть M — такое целое число, что l^M делится на порядок всех характеров χ_i', а значит и всех характеров ψ_i. Так как всякое p_i взаимно просто со всеми a_j, то

$$\psi_i(a_j) = \mathbf{e}(l^{-M} b_{ij}),$$

где $b_{ij} \in \mathbf{Z}$ при $1 \leqslant i, j \leqslant r$; кроме того, для всякого i наибольшая степень числа l, делящая b_{ii}, равна $l^{M-n-\rho+1}$. Далее, рассмотрим l^{Mr} характеров

$$\omega_x = \prod_{i=1}^{r} (\psi_i)^{x_i},$$

где $0 \leqslant x_i < l^M$ при $1 \leqslant i \leqslant r$; разумеется, они не обязаны быть все попарно различными. Для всякого j имеем

$$\omega_x(a_j) = \mathbf{e}\left(l^{-M} \sum_{i=1}^{r} b_{ij} x_i\right).$$

Это — корень из 1, порядок которого делит l^M; этот порядок делится на l^n, если он не делит l^{n-1}, т. е. если не выполняется сравнение

$$b_{jj} x_j \equiv -\sum_{i \neq j} b_{ij} x_i. \qquad (l^{M-n+1})$$

Для заданного j и для всякого набора значений x_i при $i \neq j$ это сравнение или вовсе не имеет решений x_j, или имеет ровно $l^{M-\rho}$ решений по модулю l^M. Поэтому для всякого j имеется самое большее $l^{Mr-\rho}$ наборов значений x_i, которые удовлетворяют неравенствам $0 \leqslant x_i < l^M$ при $1 \leqslant i \leqslant r$ и для которых $\omega_x(a_j)$ имеет порядок, делящий l^{n-1}. Следовательно, существует самое большее $rl^{Mr-\rho}$ таких наборов, для которых по меньшей мере одно из чисел $\omega_x(a_j)$ имеет порядок, делящий l^{n-1}. Так как $r < l^\rho$, то число таких наборов меньше, чем l^{Mr}. Отсюда следует, что можно выбрать x, для которого порядок $\omega_x(a_j)$ делится на l^n при всех j. Тогда $\psi = \omega_x$ и будет искомым характером, за возможным исключением случая $l = 2$, поскольку мы хотим, чтобы в этом случае дополнительно выполнялось условие $\psi(-1) = -1$. В этом случае если $\omega_x(-1) = 1$, то берем $\psi = \omega_x$. Если это не так, то возьмем простое p_0, делящее $4a_1a_2 \ldots a_r - 1$ и сравнимое с -1 по модулю 4; ясно, что по крайней мере одно такое простое число существует. Тогда группа $(\mathbf{Z}/p_0\mathbf{Z})^\times$ является циклической группой порядка $2m_0$, где $m_0 = (p_0 - 1)/2 \equiv 1\ (2)$, так что на ней имеется ровно один характер χ_0 порядка 2. Для этого характера имеем $\chi_0(-1) = -1$. Если продолжить χ_0 до мультипликативного характера ψ_0 по модулю p_0 на $\mathbf{Z}$, то сразу видно, что $\psi = \psi_0\omega_x$ удовлетворяет всем нашим требованиям, при условии, что взято $n \geqslant 2$, что, конечно, всегда можно предположить. Доказательство леммы 2 закончено.

Лемма 3. *Пусть* $a_1, \ldots, a_r$, $n_1, \ldots, n_r$ — *целые числа, большие* 1. *Тогда существует такой мультипликативный характер* ψ *на* $\mathbf{Z}$, *что* $\psi(-1) = -1$, *причем* $\psi(a_i)$ *для каждого* i *есть корень из* 1 *порядка, делящегося на* n_i.

Положим $N = 2\prod n_i$. Для каждого простого числа l, делящего N, пусть l^n — наибольшая степень числа l, делящая N, и пусть

для каждого i характер ψ_l выбран в соответствии с леммой 2, так что его порядок является степенью числа l, порядок корня $\psi_l(a_i)$ делится на l^i и $\psi_l(-1) = -1$ в случае $l = 2$. В случае же когда l нечетно, корень $\psi_l(-1)$, который может быть равным ± 1, будучи нечетного порядка, равен 1. Поэтому ясно, что $\psi = \prod \psi_l$ решает нашу задачу.

§ 3. ЗАКОН ВЗАИМНОСТИ ХАССЕ

Как и в гл. XI, если A — простая алгебра над k и v — произвольная точка поля k, то мы обозначаем через A_v алгебру $A \otimes_k k_v$ над k_v. Как мы видели в гл. IX-3, отображение $\mathrm{Cl}(A) \to \mathrm{Cl}(A_v)$ является тогда морфизмом группы Брауэра $B(k)$ поля k в группу Брауэра $B(k_v)$ поля k_v. Как показано в гл. XII-2, инвариант Хассе h определяет изоморфизм группы $B(k_v)$ на группу H_v, состоящую из всех корней из 1 в $\mathbf{C}$, если точка v конечна, из ± 1, если точка v вещественна, и из 1, если точка v мнима. Начиная с этого места, для любой простой алгебры A над k положим $h_v(A) = h(A_v)$; это число будем называть *инвариантом Хассе алгебры A в точке v*. По теореме 1 гл. XI-1 имеем $h_v(A) = 1$ почти для всех v. Поэтому отображение $A \to (h_v(A))$ определяет морфизм $\mathbf{h}$ группы $B(k)$ в прямую сумму групп H_v по всем v, т. е. в подмножество H в $\prod_v H_v$, состоящее из тех элементов (η_v) этого произведения, для которых $\eta_v = 1$ почти для всех v. По теореме 2 гл. XI-2 ядро морфизма $\mathbf{h}$ состоит лишь из класса тривиальных алгебр над k, так что этот морфизм инъективен. Как мы покажем в § 6, $\mathbf{h}(B(k))$ состоит из тех элементов (η_v) в H, для которых $\prod_v \eta_v = 1$. В этом параграфе мы покажем, что $\prod_v h_v(A) = 1$ для каждой простой алгебры A над k.

Пусть, как и в § 1, χ — характер на $\mathfrak{G}$ и L — циклическое расширение поля k, связанное с χ. Для любого $\theta \in k^\times$ рассмотрим циклическую алгебру $A = [L/k; \chi, \theta]$, соответствующую классу факторов $\{\chi, \theta\}$. Как мы видели в гл. IX-4, морфизм ограничения переводит класс факторов $\{\chi, \theta\}$ поля k в класс факторов $\{\chi_v, \theta\}$ поля k_v, так что A_v принадлежит последнему классу. Поэтому для всех v по определению инварианта Хассе имеем

$$h_v(A) = (\chi_v, \theta)_v, \qquad \prod_v h_v(A) = (\chi, \theta)_k. \tag{4}$$

С другой стороны, пусть k' — расширение конечной степени поля k. Для любой простой алгебры A над k положим $A' = A \otimes_k k'$.

Пусть w — точка поля k' и v — точка поля k, лежащая под w. Из свойств транзитивности тензорных произведений сразу вытекает, что алгебру $(A')_w = A' \otimes_{k'} k'_w$ над k'_w можно отождествить с алгеброй $A_v \otimes_{k_v} k'_w$. Поэтому в силу следствия 2 теор. 2 гл. XII-2 имеем $h_w(A') = h_v(A)^{n(w)}$, где $n(w)$ — степень поля k'_w над k_v. В частности, ввиду сказанного выше алгебра A' тривиальна в том и только в том случае, когда $h_v(A)^{n(w)} = 1$ для каждой точки w поля k'.

Предложение 5. *Для любого $\chi \in X_k$ пусть L — циклическое расширение поля k, связанное с χ, и A — простая алгебра над k. Тогда следующие утверждения эквивалентны*: (i) *алгебра A_L тривиальна*; (ii) *для каждой точки v поля k и каждой точки w поля L, лежащей над v, степень поля L_w над k_v делится на порядок элемента $h_v(A)$ в группе $\mathbf{C}^\times$*; (iii) *алгебра A подобна циклической алгебре $(L/k; \chi, \theta)$ для некоторого $\theta \in k^\times$*; (iv) *существует такой элемент $z = (z_v)$ в $k_{\mathbf{A}}^\times$, что $h_v(A) = (\chi_v, z_v)_v$ для каждой точки v поля k. Кроме того, если θ таково, как в* (iii), *а z таково, как в* (iv), *то $\theta^{-1}z$ лежит в $\mathrm{N}_{L/k}(L_{\mathbf{A}}^\times)$.*

Эквивалентность утверждений (i) и (ii) является частным случаем только что доказанного. Эквивалентность утверждений (i) и (iii) вытекает из предложения 9 гл. IX-4. Предположим, что имеет место (iii). Тогда в силу формул (4) условие (iv) выполняется, если взять $z = \theta$. Предположим, что имеет место (iv). Тогда порядок элемента $h_v(A)$ делит порядок характера χ_v, который по предложению 1 § 1 равен степени поля L_w над k_v для каждой точки w поля L, лежащей над v, так что выполняется (ii). Наконец, пусть θ таково, как в (iii), а z таково, как в (iv). Положим $z' = \theta^{-1}z$. Тогда в силу формул (4) имеем $(\chi_v, z'_v)_v = 1$ при всех v. По предложению 10 гл. IX-4 и предложению 1 § 1 отсюда следует, что если w — произвольная точка поля L, лежащая над v, то z'_v содержится в $\mathrm{N}_{L_w/k_v}(L_w^\times)$. Для каждой точки v поля k выберем $t_w \in L_w^\times$ для всех точек w поля L, лежащих над v, так, чтобы $z'_v = \mathrm{N}_{L_w/k_v}(t_w)$ для одной из этих точек, лежащих над v, и $t_w = 1$ для всех других. Поскольку $|z'_v|_v = 1$ почти для всех v, отсюда следует, что $|t_w|_w = 1$ почти для всех w, так что $t = (t_w)$ содержится в $L_{\mathbf{A}}^\times$. Значит, $z' = \mathrm{N}_{L/k}(t)$.

Теперь мы с помощью предложения 5 докажем, что каждая простая алгебра A над k подобна некоторой алгебре весьма специального типа. Для этого нам понадобятся две леммы.

Лемма 4. *Пусть k — поле характеристики $p > 1$. Для каждой точки v поля k пусть $\nu(v)$ — целое число, не меньшее* 1,

и пусть $\nu(v) = 1$ *почти для всех* v. *Тогда существует такое константное расширение* k' *поля* k, *что если* v — *любая точка поля* k *и* w — *точка поля* k', *лежащая над* v, *то степень поля* k'_w *над* k_v *делится на* $\nu(v)$.

Пусть $F = \mathbf{F}_q$ — поле констант в k. Для точки v поля k, степень которой равна $d(v)$, модуль поля k_v совпадает с $q^{d(v)}$. Поэтому согласно следствию 3 теор. 7 гл. I-4, если k'_w содержит примитивный корень из 1 порядка $q^{d(v)f} - 1$, то степень поля k'_w над k_v должна делиться на f. Следовательно, условие леммы 4 будет выполняться, если в качестве k' мы возьмем константное расширение поля k, степень которого над k делится на все целые числа $d(v)\,\nu(v)$, отвечающие конечному числу точек v, в которых $\nu(v) > 1$.

Лемма 5. *Пусть характеристика поля* k *равна нулю. Для каждой точки* v *поля* k *пусть* $\nu(v)$ — *такое целое число, не меньшее* 1, *что* $\nu(v) = 1$ *почти для всех* v, $\nu(v) = 1$ *или* 2 *в случае вещественной точки* v *и* $\nu(v) = 1$ *в случае мнимой точки* v. *Тогда существуют такое целое число* $m \geqslant 1$ *и такое циклическое расширение* Z *поля* $\mathbf{Q}$, *содержащееся в расширении* $\mathbf{Q}(\varepsilon)$, *порожденном примитивным корнем* ε m-*й степени из* 1, *что* (a) *если* v — *любая точка поля* k *и* w — *лежащая над* v *точка композита* k' *полей* k *и* Z, *то степень поля* k'_w *над* k_v *делится на* $\nu(v)$; (b) $|m|_v = 1$ *для любой конечной точки* v *поля* k, *такой, что* $\nu(v) > 1$.

Для начала пусть Z — любое расширение поля $\mathbf{Q}$ и k' — его композит с k. Пусть, далее, v — любая точка поля k, w — точка поля k', лежащая над v, u — точка поля Z, лежащая под w, и t — точка поля $\mathbf{Q}$, лежащая под u. Тогда k_v, Z_u и $\mathbf{Q}_t$ являются соответственно замыканиями полей k, Z и $\mathbf{Q}$ в k'_w, так что t лежит также под v. Имеем

$$[k'_w : k_v] = [k'_w : Z_u] \cdot [Z_u : \mathbf{Q}_t] \cdot [k_v : \mathbf{Q}_t]^{-1},$$

поэтому, полагая

$$\nu'(v) = \nu(v) \cdot [k_v : \mathbf{Q}_t],$$

мы видим, что если $[Z_u : \mathbf{Q}_t]$ делится на $\nu'(v)$, то $[k'_w : k_v]$ будет делиться на $\nu(v)$. Теперь для каждой конечной точки t поля $\mathbf{Q}$, над которой имеется такая точка v поля k, что $\nu(v) > 1$, обозначим через $n(t)$ какое-нибудь общее кратное целых чисел $\nu'(v)$ для всех точек v поля k, лежащих над t; для всех других конечных точек t поля $\mathbf{Q}$ положим $n(t) = 1$. Положим, далее, $n(\infty) = 2$; как сразу видно, 2 делится на $\nu'(v)$ для каждой бесконечной точки v поля k. Тогда m и Z будут удовлетворять требованиям нашей леммы, если $[Z_u : \mathbf{Q}_t]$ всегда делится на $n(t)$, $|m|_t = 1$ при $t \neq \infty$

и $n(t) > 1$. Другими словами, достаточно доказать нашу лемму для $k = \mathbf{Q}$.

Обозначим в этом случае через $p_1, \ldots, p_r$ простые числа p, для которых $n(p) > 1$. Применяя к целым числам $a_i = p_i$, $n_i = n(p_i)$ лемму 3 § 2, получаем мультипликативный характер ψ на $\mathbf{Z}$ по модулю некоторого целого числа m, причем $\psi(-1) = -1$, и для всякого i порядок корня $\psi(p_i)$ из 1 делится на $n(p_i)$. Так как $\psi(x) = 0$, если x не является взаимно простым с m, то m взаимно просто со всеми p_i, т. е. $|m|_p = 1$, если $n(p) > 1$. Пусть χ — характер группы $(\mathbf{Z}/m\mathbf{Z})^\times$, определенный с помощью ψ. Рассмотрим его как характер на группе Галуа поля $\mathbf{Q}(\varepsilon)$ над $\mathbf{Q}$, где ε — примитивный корень m-й степени из 1, и обозначим через Z циклическое расширение поля $\mathbf{Q}$, связанное с χ. Следствие 1 предл. 4 § 1 показывает, что m и Z удовлетворяют всем требованиям нашей леммы.

Теорема 2. *Пусть A — произвольная простая алгебра над k. Тогда $\prod\limits_v h_v(A) = 1$, где произведение берется по всем точкам v поля k.*

Если k — поле характеристики $p > 1$, то, как показывают предложение 5 и лемма 4, алгебра A подобна циклической алгебре $[k'/k;\ \chi,\ \theta]$, где k' — константное расширение поля k, χ — характер, связанный с k' и $\theta \in k^\times$. Поэтому χ содержится в X_0 (определение X_0 см. в § 1), и наше утверждение сразу следует из (4) и из следствия 2 предл. 3 § 1. Если k — поле характеристики нуль, то применяем предложение 5 и лемму 5, беря в последней лемме в качестве $\nu(v)$ порядок элемента $h_v(A)$ в $\mathbf{C}^\times$. В результате получаем, что алгебра A подобна циклической алгебре $[k'/k;\ \chi',\ \theta]$, где поле k' такое, как в лемме 5, χ' — любой характер, связанный с k' и $\theta \in k^\times$. Ввиду (4) все, что нам осталось доказать, это что $(\chi',\ \theta)_k = 1$.

Пусть m и Z такие, как в лемме 5. Тогда можно взять $\chi' = \chi \circ \rho$, где ρ — морфизм ограничения из группы Галуа поля $\bar{\mathbf{Q}}$ над k в группу Галуа поля $\bar{\mathbf{Q}}$ над $\mathbf{Q}$, а χ — характер на последней группе, связанный с Z. Пусть $v_1, \ldots, v_M$ — все точки поля k, лежащие над некоторым простым числом, делящим m. Для всякого i выберем какую-нибудь точку w_i поля k', лежащую над v_i, и обозначим через $w_i', \ldots, w_N'$ все отличные от w_i точки поля k', лежащие над v_i. Для всякого i обозначим через k_i, k_i' пополнения поля k относительно v_i и поля k' относительно w_i соответственно. Наконец, для всякого j пусть k_j'' — пополнение поля k' относитель-

но w'_j. Согласно условию (b) леммы 5 и в силу нашего выбора чисел $\nu(v)$ имеем $h_{v_i}(A) = 1$ при всех i. Поэтому из формул (4), предложения 1 § 1 и предложения 10 гл. IX-4 следует, что для всякого i можно записать θ в виде $\theta = \mathrm{N}_{k'_i/k_i}(z_i)$, где $z_i \in k'^{\times}_i$.

По следствию 2 теор. 3 гл. IV-2 существует элемент ζ в k', образы которого в k'_i при $1 \leqslant i \leqslant M$ сколь угодно близки к z_i и образы которого в k''_j при $1 \leqslant j \leqslant N$ сколь угодно близки к 1. Ввиду следствия 3 теор. 1 гл. IV-1 отсюда вытекает, что можно выбрать $\zeta \in k'^{\times}$ так, чтобы образ элемента $\theta_1 = \theta \mathrm{N}_{k'/k}(\zeta)^{-1}$ в k_i был сколь угодно близок к 1 при $1 \leqslant i \leqslant M$. По предложению 10 гл. IX-4 класс факторов $\{\chi', \theta\}$ не изменится, если заменить θ на θ_1. Следовательно, при такой замене не изменятся и инварианты $h_v(A) = (\chi'_v, \theta)_v$ алгебры A. Поэтому достаточно будет доказать наше равенство $(\chi', \theta)_k = 1$ при дополнительном предположении, что образ элемента θ в k_i при $1 \leqslant i \leqslant M$ лежит в заданной окрестности единицы. По следствию 3 теор. 1 гл. IV-1 эти окрестности можно выбрать таким образом, чтобы образ элемента $\mathrm{N}_{k/\mathbf{Q}}(\theta)$ в $\mathbf{Q}_p$ был произвольно близок к 1 для каждого простого числа p, делящего m. Поскольку $\chi' = \chi \circ \rho$ и поскольку в силу теоремы 1 § 1

$$(\chi \circ \rho, \theta)_k = (\chi, \mathrm{N}_{k/\mathbf{Q}}(\theta))_{\mathbf{Q}},$$

наше утверждение вытекает из следствия 3 предл. 4 § 1.

Следствие. *Для каждого* $\chi \in X_k$ *и каждого* $\theta \in k^{\times}$ *имеем* $(\chi, \theta)_k = 1$.

Это сразу вытекает из формул (4) и теоремы 2.

Следствие теор. 2 известно как *закон взаимности Артина*, ибо этот результат был (по существу) установлен Артином, который также показал, что «закон взаимности» классической теории чисел легко выводится из него с помощью чисто локальных рассмотрений. Теорема 2 принадлежит Хассе; ее близкая связь с законом Артина объясняет, почему ее обычно называют «законом взаимности Хассе».

Следствие теор. 2 можно выразить, сказав, что для каждого $\chi \in X_k$ характер $z \to (\chi, z)_k$ на $k^{\times}_{\mathbf{A}}$ тривиален на $k^{\times}$, или, еще, сказав, что $k^{\times}$ содержится в ядре канонического морфизма. Следовательно, мы можем смотреть на спаривание $(\chi, z)_k$ как на спаривание между X_k и *группой классов иделей* $G_k = k^{\times}_{\mathbf{A}}/k^{\times}$ поля k. Чтобы не усложнять обозначений, мы не вводим никакого нового символа для обозначения этого спаривания, но тем не менее будем применять к нему все результаты гл. XII-1.

Ясно, что это спаривание удовлетворяет условиям [I] и [II] гл. XII-1, потому что они были проверены в § 1 для $(\chi, z)_k$, рассматриваемого как спаривание групп X_k и $k_{\mathbf{A}}^{\times}$. По теореме 6 гл. IV-4 группа G_k квазикомпактна и $G_k^1 = k_{\mathbf{A}}^1/k^{\times}$. Если характеристика поля k равна нулю, то выполняется условие [III (a)] гл. XII-1. В случае когда k — поле характеристики $p > 1$, следствие 3 предл. 3 § 1 вместе с леммой 1 § 1 показывают, что условие [III (b)] гл. XII-1 выполняется, если в качестве χ в этом условии берется характер, связанный с константным расширением степени n над k; они также показывают, что группа, обозначавшаяся в § 1 через X_0 и состоящая из характеров, связанных с константными расширениями поля k, совпадает в рассматриваемом случае с группой, обозначавшейся тем же символом в гл. XII-1. Поэтому мы можем применить следствие 2 предл. 2 гл. XII-1, которое показывает, что канонический морфизм $\mathfrak{a}$ отображает $k_{\mathbf{A}}^1$ на подгруппу $\mathfrak{A}_0$ в $\mathfrak{A}$, соответствующую объединению k_0 константных расширений поля k. Аналогично если характеристика поля k равна нулю, то в силу предложения 1 гл. XII-1 $\mathfrak{a}$ отображает $k_{\mathbf{A}}^{\times}$ на $\mathfrak{A}$. Обозначим снова через U_k ядро морфизма $\mathfrak{a}$. Оно содержит $k^{\times}$, и для поля k характеристики $p > 1$, как вытекает из следствия 2 предл. 2 гл. XII-1, $U_k \subset k_{\mathbf{A}}^1$. С другой стороны, если k — поле характеристики нуль и подгруппа $k_{\infty+}^{\times}$ в $k_{\mathbf{A}}^{\times}$ определена, как в § 1, то U_k содержит замыкание подгруппы $k^{\times} k_{\infty+}^{\times}$. В § 8 будет показано, что U_k совпадает с этим замыканием, если характеристика поля k равна нулю, и что в противном случае $U_k = k^{\times}$.

Переформулируем для определенного выше спаривания между X_k и G_k предложение 4 гл. XII-1. Пусть k' — циклическое расширение поля k. Тогда отображение $\xi \to \xi^{\lambda}$ для каждого $\lambda \in \mathfrak{G}$ и отображение $\xi \to \mathrm{N}_{k'/k}(\xi)$ суть полиномиальные отображения из k' в k' и в k соответственно, где k' рассматривается как векторное пространство над k; при всех ξ имеем $\mathrm{N}_{k'/k}(\xi^{\lambda}) = \mathrm{N}_{k'/k}(\xi)$. В гл. IV-1 было выяснено, что $\mathrm{N}_{k'/k}$ как отображение из $k'_{\mathbf{A}}$ в $k_{\mathbf{A}}$ является продолжением на эти пространства полиномиального отображения $\mathrm{N}_{k'/k}$ из k' в k; теперь мы подобным же образом продолжим на $k'_{\mathbf{A}}$ k-линейное отображение $\xi \to \xi^{\lambda}$ из k' на k'. Имеем $\mathrm{N}_{k'/k}(x'^{\lambda}) = \mathrm{N}_{k'/k}(x')$ для всех $x' \in k'_{\mathbf{A}}$, в частности для всех $x' \in k_{\mathbf{A}}'^{\times}$. Поскольку в то же самое время в силу следствия предл. 3 гл. IV-3 $|z'| = |\mathrm{N}_{k'/k}(z')|_{\mathbf{A}}$ при всех $z' \in k_{\mathbf{A}}'^{\times}$, то $|z'^{\lambda}|_{\mathbf{A}} = |z'|_{\mathbf{A}}$ при всех $z' \in k_{\mathbf{A}}'^{\times}$ и всех $\lambda \in \mathfrak{G}$. Так как морфизмы $z' \to z'^{\lambda}$, $z' \to \mathrm{N}_{k'/k}(z')$ из $k_{\mathbf{A}}'^{\times}$ на $k_{\mathbf{A}}'^{\times}$ и из $k_{\mathbf{A}}'^{\times}$ в $k_{\mathbf{A}}^{\times}$ отображают $k'^{\times}$ на $k'^{\times}$ и в $k^{\times}$ соответственно, они определяют морфизмы из $G_{k'}$ на $G_{k'}$ и в G_k соответственно. Возьмем их в качестве отображений $g' \to g'^{\lambda}$,

$g' \to F(g')$ в предложении 4 гл. XII-1. Ясно, что эти отображения удовлетворяют условиям [IV (i) — (ii)] и [V (i)]; утверждение [VI (iii)] немедленно вытекает из наших определений и из следствия 5 теор. 1 гл. XII-2 (это утверждение допускает очевидное обобщение, совершенно аналогичное последнему следствию). Условие [V (ii)] совпадает в нашем случае с утверждением теоремы 1 § 1. Таким образом, выполнены все условия применимости предложения 4 гл. XII-1, и мы заключаем, что в теперешних наших обозначениях

$$U_k \cap k^\times \mathrm{N}_{k'/k}(k'^\times_{\mathbf{A}}) = k^\times \mathrm{N}_{k'/k}(U_{k'}), \tag{5}$$

где k — любое $\mathbf{A}$-поле, k' — любое циклическое расширение поля k и U_k, $U_{k'}$ — ядра канонических морфизмов для k и для k' соответственно.

§ 4. ТЕОРИЯ ПОЛЕЙ КЛАССОВ ДЛЯ Q

Полученные к настоящему моменту результаты уже позволяют легко завершить наше исследование в частном случае $k = \mathbf{Q}$; это удается сделать благодаря следующему факту.

Лемма 6. *Имеет место разложение в прямое произведение*

$$\mathbf{Q}_{\mathbf{A}}^\times = \mathbf{Q}^\times \times \mathbf{R}_+^\times \times \coprod_p \mathbf{Z}_p^\times,$$

где произведение берется по всем простым числам p.

Здесь $\mathbf{R}_+^\times$ и $\mathbf{Z}_p^\times$ рассматриваются как подгруппы квазисомножителей $\mathbf{R}^\times = \mathbf{Q}_\infty^\times$ и $\mathbf{Q}_p^\times$ группы $\mathbf{Q}_{\mathbf{A}}^\times$. Как и в следствии 2 предл. 4 § 1, определим морфизм r из $\mathbf{Q}_{\mathbf{A}}^\times$ в $\mathbf{Q}^\times$, полагая

$$r(z) = \operatorname{sign}(z_\infty) \coprod_p |z_p|_p^{-1}$$

для $z = (z_v) \in \mathbf{Q}_{\mathbf{A}}^\times$. Как уже отмечалось (в доказательстве следствия 3 предл. 4 § 1), r индуцирует на $\mathbf{Q}^\times$ тождественное отображение; это сразу вытекает из теоремы 5 гл. IV-4. Поэтому если R — ядро морфизма r, то r определяет разложение в прямое произведение $\mathbf{Q}_{\mathbf{A}}^\times = \mathbf{Q}^\times \times R$ и является проекцией этого произведения на первый сомножитель. Ясно, что $R = \mathbf{R}_+^\times \times \coprod_p \mathbf{Z}_p^\times$, чем лемма и доказана.

Очевидно, подгруппа $\coprod \mathbf{Z}_p^\times$ в $\mathbf{Q}_{\mathbf{A}}^\times$ вполне несвязна, так что по лемме 4 гл. VII-3 все ее характеры имеют конечный порядок.

Поэтому из леммы 6 в сочетании со следствием 2 предл. 7 гл. VII-3 сразу вытекает, что каждый квазихарактер на $\mathbf{Q}_\mathbf{A}^\times$, тривиальный на $\mathbf{Q}^\times$, имеет вид $\omega_s\psi$, где характер ψ тривиален на $\mathbf{Q}^\times \times \mathbf{R}_+^\times$, а ω_s, как и в гл. VII, обозначает квазихарактер $z \to |z|_\mathbf{A}^s$, причем этот характер тривиален на $\mathbf{Q}^\times$ и на $\prod \mathbf{Z}_p^\times$; очевидно, ψ является характером конечного порядка. Напомним, что для любого тривиального на $\mathbf{Q}^\times$ квазихарактера ω на $\mathbf{Q}_\mathbf{A}^\times$ его ведущий идеал в соответствии с определением, данным в гл. VII-7 для произвольного числового поля, совпадает с идеалом $\prod p^{f(p)}$ в $\mathbf{Z}$, где $p^{f(p)}$ для всякого простого числа p есть ведущий идеал квазихарактера ω_p, индуцированного на $\mathbf{Q}_p^\times$ квазихарактером ω; здесь, как обычно, мы отождествляем ненулевой идеал в $\mathbf{Z}$ с порождающим его целым положительным числом.

Как объяснялось в § 1, если ε — примитивный корень m-й степени из 1 в $\overline{\mathbf{Q}}$, то мы отождествляем группу Галуа $\mathfrak{g}$ поля $\mathbf{Q}(\varepsilon)$ над $\mathbf{Q}$ с $(\mathbf{Z}/m\mathbf{Z})^\times$ и каждый характер χ на $\mathfrak{g}$ с характером группы Галуа $\mathfrak{G}$ поля $\overline{\mathbf{Q}}$ над $\mathbf{Q}$, т. е. с характером группы Галуа $\mathfrak{A}$ поля $\mathbf{Q}_{\mathrm{ab}}$ над $\mathbf{Q}$. Разумеется, $\mathbf{Q}(\varepsilon) \subset \mathbf{Q}_{\mathrm{ab}}$ при всех m.

Теорема 3. *Для любого $m > 1$ пусть ε — примитивный корень m-й степени из 1 в $\overline{\mathbf{Q}}$, и пусть $\mathfrak{g} = (\mathbf{Z}/m\mathbf{Z})^\times$ — группа Галуа поля $\mathbf{Q}(\varepsilon)$ над $\mathbf{Q}$. Тогда отображение $\chi \to \chi \circ \mathfrak{a}$ есть изоморфизм группы характеров на $\mathfrak{g}$ на группу характеров на $\mathbf{Q}_\mathbf{A}^\times$, тривиальных на $\mathbf{Q}^\times \times \mathbf{R}_+^\times$, ведущий идеал которых делит m.*

Обозначим последнюю группу через Γ. Пусть P — множество, состоящее из ∞ и простых чисел p, делящих m. Для всякого простого числа p из P положим $g_p = 1 + p^\mu\mathbf{Z}_p$, где p^μ — наибольшая степень числа p, делящая m. Обозначим через H подгруппу в $\mathbf{Q}_\mathbf{A}^\times$, состоящую из тех иделей (z_v), для которых $z_\infty > 0$, $z_p \in g_p$ для каждого простого числа $p \in P$ и $z_p \in \mathbf{Z}_p^\times$ для p, не лежащих в P. Тогда Γ есть группа характеров ω на $\mathbf{Q}_\mathbf{A}^\times$, тривиальных на $\mathbf{Q}^\times$ и на H. Положим $g_\infty = \mathbf{R}^\times$ и $g = \prod g_v$, где произведение берется по всем $v \in P$. Как и в гл. VII-8, обозначим через G_P подгруппу в $\mathbf{Q}_\mathbf{A}^\times$, состоящую из тех иделей (z_v), для которых $z_v = 1$ при всех $v \in P$. Поскольку $g \times G_P$ — открытая подгруппа в $\mathbf{Q}_\mathbf{A}^\times$ и подгруппа $\mathbf{Q}^\times G_P$ плотна в $\mathbf{Q}_\mathbf{A}^\times$ по предложению 15 гл. VII-8, то $\mathbf{Q}_\mathbf{A}^\times = \mathbf{Q}^\times \cdot (g \times G_P)$. Поэтому морфизм r из $\mathbf{Q}_\mathbf{A}^\times$ на $\mathbf{Q}^\times$, определенный в доказательстве леммы 6, отображает $g \times G_P$ на подгруппу $\mathbf{Q}^{(m)}$ в $\mathbf{Q}^\times$,

состоящую из дробей a/b, где a и b лежат в $\mathbf{Z}$ и взаимно просты с m. Ядро морфизма из $g \times G_P$ на $\mathbf{Q}^{(m)}$, индуцированного морфизмом r, совпадает с определенной выше группой H.

Поскольку каждый характер из Γ тривиален на H, отсюда следует, что для любого $\omega \in \Gamma$ существует такой характер χ на $\mathbf{Q}^{(m)}$, что $\chi \circ r$ совпадает с ω на $g \times G_P$. Поэтому если $a \in \mathbf{Z}$ и $a \equiv 1$ по модулю m, то $a \in g \times G_P$ и $r(a) = a$, откуда $\chi(a) = \omega(a) = 1$. Следовательно, χ определяет характер группы $(\mathbf{Z}/m\mathbf{Z})^\times$. Этот характер мы будем обозначать также через χ и будем рассматривать его как характер на $\mathfrak{g}$ и, значит, на $\mathfrak{G}$. Следствие 2 предл. 4 § 1 показывает, что $(\chi, z)_\mathbf{Q} = \chi(r(z))$ при всех $z \in g' \times G_P$, где g' — подходящая открытая подгруппа в g. Это означает, что $\chi \circ \mathfrak{a}$ совпадает на $g' \times G_P$ с $\chi \circ r$ и, следовательно, с ω. Поскольку $\mathbf{Q}_\mathbf{A}^\times = \mathbf{Q}^\times \cdot (g' \times G_P)$ в силу предложения 15 гл. VII-8 и поскольку характеры $\chi \circ \mathfrak{a}$ и ω оба тривиальны на $\mathbf{Q}^\times$, этим доказано, что $\chi \circ \mathfrak{a} = \omega$.

Обратно, пусть χ — произвольный характер на $\mathfrak{g} = (\mathbf{Z}/m\mathbf{Z})^\times$. Как и в § 1, рассмотрим его как функцию на множестве всех целых чисел, взаимно простых с m, и продолжим до характера χ на $\mathbf{Q}^{(m)}$. Тогда $\chi \circ r$ будет характером на $g \times G_P$. Возьмем $\xi \in \mathbf{Q}^\times \cap (g \times G_P)$. Очевидно, $r(\xi) = \xi$ и, как и в доказательстве следствия 3 предл. 4 § 1, сразу видно, что $\xi \in \mathbf{Q}^{(m)}$ и $\chi(\xi) = 1$. Поэтому характер $\chi \circ r$ тривиален на $\mathbf{Q}^\times \cap (g \times G_P)$, так что его можно однозначно продолжить до характера ω на $\mathbf{Q}_\mathbf{A}^\times = \mathbf{Q}^\times \cdot (g \times G_P)$, тривиального на $\mathbf{Q}^\times$. Поскольку морфизм r тривиален на H, характер ω также тривиален на H и, значит, принадлежит Γ. Как и выше, следствие 2 предл. 4 § 1 показывает, что $\chi \circ \mathfrak{a}$ совпадает на $g' \times G_P$ с $\chi \circ r$ и, следовательно, с ω, где g' — подходящая открытая подгруппа в g. Как и выше, получаем отсюда, что $\chi \circ \mathfrak{a} = \omega$, чем и завершается наше доказательство.

Мы видим также, что $\chi \circ \mathfrak{a}$ совпадает с $\chi \circ r$ не только на $g' \times G_P$, но даже на $g \times G_P$; другими словами, при условии, что $z_p \in g_p$ для каждого простого числа $p \in P$, справедливо заключение следствия предл. 4 § 1. Мы не будем формулировать это как отдельный результат, но используем при доказательстве очередного следствия

Следствие 1. *Пусть ε таково, как в теореме* 3. *Возьмем любое $z = (z_v)$ в $\prod \mathbf{Z}_p^\times$ и положим $\alpha = \mathfrak{a}(z)^{-1}$. Тогда существует такое целое число a, что $a \in z_p + m\mathbf{Z}_p$ для каждого простого числа p, и для каждого такого a имеет место равенство $\varepsilon^\alpha = \varepsilon^a$.*

Условие на a можно записать также в таком виде: $a \equiv z_p$ по модулю p^μ для каждого простого числа p, делящего m, где p^μ — наибольшая степень числа p, делящая m. Как хорошо известно, эти сравнения имеют единственное решение по модулю m (этот факт можно рассматривать как частный случай следствия 1 теор. 1 гл. V-2). Поскольку $z_p \in \mathbf{Z}_p^\times$ при всех p, то a взаимно просто с p; в частности, $a \neq 0$. Положим $z' = a^{-1}z$. Тогда $z'_p \in g_p$ для всех простых чисел $p \in P$. Поэтому, как было показано в конце доказательства теоремы 3, $\chi(\mathfrak{a}(z')) = \chi(r(z'))$. Поскольку морфизм $\mathfrak{a}$ тривиален на $\mathbf{Q}^\times$, то $\mathfrak{a}(z') = \mathfrak{a}(z) = \alpha^{-1}$. Так как $r(a) = a$ и $r(z) = 1$, то $\chi(\alpha) = \chi(a)$. Поскольку это имеет место для всех характеров χ на $\mathfrak{g}$, отсюда видно, что автоморфизм поля $\mathbf{Q}(\varepsilon)$, индуцированный посредством α, определяется подстановкой $\varepsilon \to \varepsilon^a$.

Следствие 2. *Ядро канонического морфизма* $\mathfrak{a}$ *для* $\mathbf{Q}$ *совпадает с* $\mathbf{Q}^\times \times \mathbf{R}_+^\times$, *и* $\mathfrak{a}$ *определяет изоморфизм группы* $\prod \mathbf{Z}_p^\times$ *на группу Галуа* $\mathfrak{A}$ *поля* $\mathbf{Q}^{ab}$ *над* $\mathbf{Q}$.

В самом деле, как мы уже знаем, ядро морфизма $\mathfrak{a}$ содержит $\mathbf{Q}^\times \times \mathbf{R}_+^\times$, а теорема 3 показывает, что он содержится в этой группе. Последнее утверждение сразу вытекает поэтому из леммы 6 и предложения 1 гл. XII-1.

Следствие 3. *Поле* $\mathbf{Q}_{ab}$ *порождено над* $\mathbf{Q}$ *корнями из* 1 *в алгебраическом замыкании* $\bar{\mathbf{Q}}$ *поля* $\mathbf{Q}$.

Пусть K — расширение поля $\mathbf{Q}$, порожденное этими корнями; оно совпадает с объединением полей $\mathbf{Q}(\varepsilon)$ по всем $m > 1$, где ε — примитивный корень m-й степени из 1. Пусть $\mathfrak{B}$ — подгруппа в $\mathfrak{A}$, соответствующая полю K. Тогда если характер χ таков, как в теореме 3, то он тривиален на $\mathfrak{B}$, так что характер $\chi \circ \mathfrak{a}$ тривиален на $\mathfrak{a}^{-1}(\mathfrak{B})$. Поэтому в силу теоремы 3 группа $\mathfrak{a}^{-1}(\mathfrak{B})$ должна содержаться в $\mathbf{Q}^\times \times \mathbf{R}_+^\times$. Но по следствию 2 $\mathbf{Q}^\times \times \mathbf{R}_+^\times$ совпадает с ядром морфизма $\mathfrak{a}$ и, значит, $\mathfrak{B} = \{1\}$, откуда $K = \mathbf{Q}_{ab}$.

§ 5. СИМВОЛ ГИЛЬБЕРТА

Определение ядра канонического морфизма в общем случае основано на двух результатах, соответствующих предложениям 9 и 10 гл. XII-3. В этом параграфе мы будем иметь дело с первым из этих результатов; нам потребуются некоторые вспомогательные результаты.

Под n будем понимать любое целое число, большее 1.

Лемма 7. *Пусть G — квазикомпактная группа, γ — группа всех характеров на G, порядок которых делит n, и X — пересечение ядер всех этих характеров. Тогда каждый характер на G, тривиальный на X, содержится в γ.*

По лемме 2 гл. XII-1, примененной к эндоморфизму $x \to x^n$ группы G, G^n есть замкнутая подгруппа в G и группа G/G^n компактна. Поэтому в группе, двойственной к G, подгруппа, ассоциированная по двойственности с G^n, дискретна. Эта подгруппа состоит из всех характеров на G, которые тривиальны на G^n, т. е. порядок которых делит n. Следовательно, группа γ дискретна, а значит, замкнута в группе, двойственной к G. Наше утверждение вытекает теперь из теории двойственности.

Предложение 6. *Пусть K — локальное поле, содержащее n различных корней n-й степени из 1. Для x, y из $K^\times$ положим $(x, y)_{n,K} = (\chi_{n,x}, y)_K$. Тогда*

$$(y, x)_{n,K} = (x, y)_{n,K}^{-1}$$

при всех x, y из $K^\times$; $(K^\times)^n$ совпадает с множеством тех элементов $y \in K^\times$, для которых $(x, y)_{n,K} = 1$ при всех $x \in K^\times$; если $\mathrm{mod}_K(n) = 1$ и R — максимальное компактное подкольцо в K, то множество тех элементов $y \in K^\times$, для которых $(x, y)_{n,K} = 1$ при всех $x \in R^\times$, совпадает с $(K^\times)^n R^\times$.

В силу определений гл. IX-5 и гл. XII-2 $(x, y)_{n,K}$ совпадает с $\eta(\{x, y\}_n)$, где η — изоморфизм, определенный в следствии 2 теор. 1 гл. XII-2. Наше первое утверждение есть не что иное, как формула (12) гл. IX-5. Второе тождественно предложению 9 гл. XII-3, если K есть p-поле, тривиально, если $K = \mathbf{C}$, и легко проверяется, если $K = \mathbf{R}$, ибо в этом случае из нашего предположения о корнях n-й степени из 1, содержащихся в K, вытекает, что $n = 2$. Что касается нашего последнего утверждения, то из предположения о том, что $\mathrm{mod}_K(n) = 1$, вытекает, что K является p-полем, где p взаимно просто с n. Ввиду нашей первой формулы и предложения 6 гл. XII-2 доказываемое утверждение сводится к утверждению, что характер $\chi_{n,y}$ неразветвлен в том и только в том случае, когда $y \in (K^\times)^n R^\times$.

Обозначим через q модуль поля K. Из нашего предположения относительно корней n-й степени из 1 вытекает, что n делит $q - 1$. В алгебраическом замыкании $\overline{K}$ поля K возьмем какой-нибудь примитивный корень ζ из 1 порядка $n(q-1)$. Для любого $f \geqslant 1$ пусть K_f — неразветвленное расширение степени f над K, содер-

жащееся в $\overline{K}$. Тогда $\zeta \in K_f$ в том и только в том случае, когда $n\,(q-1)$ делит q^f-1, т. е. в том и только в том случае, когда $1+q+\ldots+q^{f-1} \equiv 0$ по модулю n. Так как $q \equiv 1$ по модулю n, последнее сравнение выполняется в том и только в том случае, когда $f \equiv 0$ по модулю n. Отсюда видно, что $K(\zeta) = K_n$.

Положим $\varepsilon = \zeta^n$. Так как это — примитивный корень $(q-1)$-й степени из 1, он содержится в K. Ввиду определений гл. IX-5 мы показали, таким образом, что $\chi_{n,\varepsilon}$ является неразветвленным характером порядка n, связанным с K_n. Поэтому в силу предложения 5 гл. XII-2 он порождает группу неразветвленных характеров, порядок которых делит n. В частности, для $y \in K^\times$ характер $\chi_{n,y}$ неразветвлен в том и только в том случае, когда он равен $(\chi_{n,\varepsilon})^v$ при некотором $v \in \mathbf{Z}$, т. е. когда $y\varepsilon^{-v}$ лежит в ядре морфизма $x \to \chi_{n,x}$. Как мы видели в гл. IX-5, это ядро совпадает с $(K^\times)^n$. Следовательно, характер $\chi_{n,y}$ неразветвлен в том и только в том случае, когда y содержится в подгруппе в $K^\times$, порожденной подгруппой $(K^\times)^n$ и элементом ε. По предложению 8 гл. II-3 $(K^\times)^n$ содержит $1+P$. Так как $1+P$ и ε порождают $R^\times$, наше утверждение доказано.

Следствие. *Для каждого локального поля K, содержащего n различных корней n-й степени из* 1, *символ $(x, y)_{n,K}$ определяет локально постоянное отображение из $K^\times \times K^\times$ в группу корней n-й степени из* 1 *в* **C**.

Это очевидно, если $K = \mathbf{R}$ или $\mathbf{C}$. Если K — некоторое p-поле, то это немедленно вытекает из предложения 6 и того факта (имеющего место в силу предложения 8 гл. II-3, в случае когда K — поле характеристики p, ибо тогда n должно быть взаимно простым с p, и в силу следствия предл. 9 гл. II-3 в противном случае), что $(K^\times)^n$ —открытая подгруппа конечного индекса в $K^\times$.

Про символ $(x, y)_{n,K}$ можно сказать, что он определяет двойственность конечной группы $K^\times/(K^\times)^n$ самой себе, с помощью которой эта группа может быть отождествлена со своей двойственной.

Предложение 7. *Пусть k — некоторое* **A**-*поле, содержащее n различных корней n-й степени из* 1. *Тогда при всех $z = (z_v)$, $z' = (z'_v)$ из $k_{\mathbf{A}}^\times$ почти все сомножители в произведении*

$$(z, z')_n = \prod_v (z_v, z'_v)_{n,k_v},$$

взятом по всем точкам v поля k, равны 1, *и это произведение определяет локально постоянное отображение из $k_{\mathbf{A}}^\times \times k_{\mathbf{A}}^\times$ в группу*

корней n-й степени из 1 *в* $\mathbf{C}$ *и удовлетворяет условию* $(z, z')_n = (z', z)_n^{-1}$ *при всех* z, z'. *Кроме того,* $(k_{\mathbf{A}}^{\times})^n$ *совпадает с множеством тех элементов* z *из* $k_{\mathbf{A}}^{\times}$, *для которых* $(z, z')_n = 1$ *при всех* $z' \in k_{\mathbf{A}}^{\times}$.

Если k — поле характеристики $p > 1$, то из нашего предположения относительно k вытекает, что n взаимно просто с p. Следовательно, во всех случаях $|n|_v = 1$ почти для всех v. Поскольку z_v, z_v' лежат в $r_v^{\times}$ почти для всех v, то наше первое утверждение сразу вытекает из предложения 6. Тот же самый факт в сочетании со следствием предл. 6 показывает, что $(z, z')_n$ есть локально постоянное отображение. По предложению 6 если z содержится в ядрах всех характеров $z \to (z, z')_n$, то $z_v \in (k_v^{\times})^n$ при всех v. Поэтому из равенства $z_v = t_v^n$, где $t_v \in k_v^{\times}$, и того факта, что $z_v \in r_v^{\times}$ почти для всех v, вытекает, что то же верно для t_v, так что $t = (t_v) \in k_{\mathbf{A}}^{\times}$ и $z = t^n$.

Следствие 1. *Для каждого конечного множества* P *точек поля* k, *содержащего все те точки, для которых* $|n|_v \neq 1$, *положим*

$$\Omega(P) = \prod_{v \in P} k_v^{\times} \times \prod_{v \notin P} r_v^{\times}, \quad \Omega'(P) = \prod_{v \in P} (k_v^{\times})^n \times \prod_{v \notin P} r_v^{\times}.$$

Это — открытые подгруппы в $k_{\mathbf{A}}^{\times}$, *и множество тех элементов* $z \in k_{\mathbf{A}}^{\times}$, *для которых* $(z, z')_n = 1$ *при всех* $z' \in \Omega(P)$ (*соотв. при всех* $z' \in \Omega'(P)$), *совпадает с* $(k_{\mathbf{A}}^{\times})^n \Omega'(P)$ (*соотв. с* $(k_{\mathbf{A}}^{\times})^n \Omega(P)$).

Относительно определения P следует заметить, что $|n_v| > 1$ для каждой бесконечной точки поля k, так что P содержит все эти точки. Поэтому $\Omega(P)$ совпадает с открытой подгруппой в $k_{\mathbf{A}}^{\times}$, обозначавшейся тем же символом в гл. IV-4. Как мы видели выше, подгруппа $(k_v^{\times})^n$ открыта в $k_v^{\times}$ при всех v, так что группа $\Omega'(P)$ открыта в $\Omega(P)$. Первое множество, рассматриваемое в нашем следствии, состоит из тех иделей (z_v), для которых $(z_v, z_v')_{n, k_v} = 1$ при всех $z_v' \in k_v^{\times}$, если $v \in P$, и при всех $z_v' \in r_v^{\times}$, если $v \notin P$. Следовательно, наше утверждение вытекает из предложения 6. Другое множество рассматривается аналогичным образом.

Следствие 2. *Пусть* P *таково, как в следствии* 1. *Предположим дополнительно, что* $k_{\mathbf{A}}^{\times} = k^{\times} \Omega(P)$. *Тогда*

$$(k^{\times})^n = k^{\times} \cap (k_{\mathbf{A}}^{\times})^n \Omega'(P).$$

Ясно, что $(k^{\times})^n$ содержится в правой части последнего равенства. Обратно, пусть ξ — элемент из правой части равенства.

Тогда по следствию 1 $(\xi, z)_n = 1$ при всех $z \in \Omega(P)$. По определению это равносильно тому, что $\Omega(P)$ содержится в ядре характера $z \to (\chi_{n,\xi}, z)_k$ на $k_{\mathbf{A}}^{\times}$. Поскольку это ядро содержит $k^{\times}$ по следствию теор. 2 § 3 и поскольку $k_{\mathbf{A}}^{\times} = k^{\times}\Omega(P)$, отсюда следует, что характер $\chi_{n,\xi}$ тривиален, а значит $\xi \in (k^{\times})^n$.

Символ $(z, z')_n$, определенный в предложении 7, можно назвать *символом Гильберта* для k. Из последнего утверждения предложения 7 вытекает, что $(k_{\mathbf{A}}^{\times})^n$ является замкнутой подгруппой в $k_{\mathbf{A}}^{\times}$, поэтому основное содержание этого предложения можно выразить, сказав, что символ Гильберта определяет двойственность группы $k_{\mathbf{A}}^{\times}/(k_{\mathbf{A}}^{\times})^n$ самой себе, с помощью которой она может быть отождествлена со своей двойственной. Как замечено выше, при всех $\xi \in k^{\times}$, $z \in k_{\mathbf{A}}^{\times}$ имеем

$$(\xi, z)_n = (\chi_{n,\xi}, z)_k = \chi_{n,\xi}(\mathfrak{a}(z)),$$

следовательно, в силу следствия теор. 2 § 3 $(\xi, \eta)_n = 1$ для всех ξ, η из $k^{\times}$.

Предложение 8. *Пусть поле k содержит n различных корней n-й степени из* 1. *Тогда $k^{\times}(k_{\mathbf{A}}^{\times})^n$ совпадает с множеством тех элементов $z \in k_{\mathbf{A}}^{\times}$, для которых $(\xi, z)_n = 1$ при всех $\xi \in k^{\times}$, и это множество содержит ядро U_k морфизма $\mathfrak{a}$.*

Обозначим рассматриваемое множество через X_n. Его можно описать также как пересечение ядер характеров $\chi_{n,\xi}$ на $k_{\mathbf{A}}^{\times}$, где ξ пробегает $k^{\times}$. Очевидно, $X_n \supset U_k$. Как и прежде, положим $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$. Применяя к G_k и к эндоморфизму $x \to x^n$ группы G_k лемму 2 гл. XII-1, мы видим, что $k^{\times}(k_{\mathbf{A}}^{\times})^n$ является замкнутой подгруппой в $k_{\mathbf{A}}^{\times}$ с компактной факторгруппой. Применяя к G_k и к группе характеров на G_k, определяемых характерами на $k_{\mathbf{A}}^{\times}$ вида $\chi_{n,\xi} \circ \mathfrak{a}$ с $\xi \in k^{\times}$, лемму 7, мы видим, что каждый характер на $k_{\mathbf{A}}^{\times}$, тривиальный на X_n, имеет такой же вид. Ясно, что $X_n \supset k^{\times}(k_{\mathbf{A}}^{\times})^n$. Так как обе эти подгруппы замкнуты в $k_{\mathbf{A}}^{\times}$, то наше предложение будет доказано, если мы покажем, что существуют сколь угодно малые окрестности U единицы в $k_{\mathbf{A}}^{\times}$, для которых X_n содержится в $k^{\times}(k_{\mathbf{A}}^{\times})^n U$.

Чтобы показать это, поступим следующим образом. Пусть P_0 — конечное множество точек поля k, содержащее все такие точки v, что $|n|_v \neq 1$, и удовлетворяющее условию из следствия теор. 7

гл. IV-4, т. е. такое, что $k_{\mathbf{A}}^{\times} = k^{\times}\Omega(P_0)$. Тогда каждое конечное множество точек $P \supset P_0$ обладает теми же свойствами. Возьмем любое такое множество P и положим $U = \prod U_v$, где U_v — произвольная окрестность единицы в $(k_v^{\times})^n$ при $v \in P$ и $U_v = r_v^{\times}$ при $v \notin P$. Ясно, что U есть окрестность единицы в $k_{\mathbf{A}}^{\times}$ и что эту окрестность можно сделать сколь угодно малой с помощью подходящего выбора P и окрестностей U_v для $v \in P$. Сразу видно, что $(k_{\mathbf{A}}^{\times})^n U$ совпадает с $(k_{\mathbf{A}}^{\times})^n \Omega'(P)$, где $\Omega'(P)$ — группа, которая была определена в следствии 1 предл. 7.

Нам надо доказать, что X_n содержится в группе $W(P) = k^{\times}(k_{\mathbf{A}}^{\times})^n \Omega'(P)$, другими словами, что $X_n W(P) = W(P)$. По лемме 1 гл. XII-1, примененной к $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$ и к образу в G_k группы $W(P)$, последняя группа имеет конечный индекс в $k_{\mathbf{A}}^{\times}$. Таким образом, достаточно будет показать, что $W(P)$ и $X_n W(P)$ имеют одинаковый индекс в $k_{\mathbf{A}}^{\times}$.

Индекс подгруппы $X_n W(P)$ в $k_{\mathbf{A}}^{\times}$ равен числу различных характеров на $k_{\mathbf{A}}^{\times}$, тривиальных на X_n и на $W(P)$. Будучи тривиальным на X_n, такой характер должен иметь вид $\chi_{n,\xi} \circ \mathfrak{a}$, где $\xi \in k^{\times}$. Поскольку X_n содержит $k^{\times}(k_{\mathbf{A}}^{\times})^n$, то характер $\chi_{n,\xi} \circ \mathfrak{a}$ тривиален на $M(P)$ в том и только в том случае, когда он тривиален на $\Omega'(P)$, т. е. в силу следствия 1 предл. 7, когда ξ содержится в $(k_{\mathbf{A}}^{\times})^n \Omega(P)$. Но ввиду наших предположений относительно P

$$(k_{\mathbf{A}}^{\times})^n \Omega(P) = (k^{\times}\Omega(P))^n \Omega(P) = (k^{\times})^n \Omega(P).$$

Как и в гл. IV-4, положим $E(P) = k^{\times} \cap \Omega(P)$. Мы видим, что рассматриваемые характеры суть в точности характеры вида $\chi_{n,\xi} \circ \mathfrak{a}$ с $\xi \in (k^{\times})^n E(P)$, и нам надо вычислить число различных таких характеров, которое совпадает с индексом в $(k^{\times})^n E(P)$ ядра морфизма $\xi \to \chi_{n,\xi} \circ \mathfrak{a}$. Это ядро совпадает с ядром морфизма $\xi \to \chi_{n,\xi}$, которое равно $(k^{\times})^n$. Следовательно, наш индекс совпадает с индексом подгруппы $E(P)^n$ в $E(P)$. В силу теоремы 9 гл. IV-4 и того факта, что n делит порядок группы всех корней из 1 в k, последний индекс равен n^c, где $c = \operatorname{card}(P)$.

Теперь нам нужно вычислить индекс подгруппы $W(P)$ в $k_{\mathbf{A}}^{\times}$. Рассмотрим группы $G = k^{\times} \times \Omega(P)$, $G' = k^{\times} \times \Omega'(P)$ и морфизм f из G в $k_{\mathbf{A}}^{\times}$, для которого $f(\xi, u) = \xi u$ при $\xi \in k^{\times}$, $u \in \Omega(P)$. Обозначим через H ядро морфизма f; оно состоит из элементов $(\xi, \xi^{-1}) \in G$ с $\xi \in E(P)$. Ввиду нашего предположения относительно P морфизм f отображает G на $k_{\mathbf{A}}^{\times}$; далее, он отображает G' на $W(P)$,

как показывает формула

$$W(P) = k^\times (k_\mathbf{A}^\times)^n \Omega'(P) = k^\times (k^\times \Omega(P))^n \Omega'(P) =$$
$$= k^\times (\Omega(P)^n \Omega'(P)) = k^\times \Omega'(P).$$

Это дает $f^{-1}(W(P)) = HG'$, следовательно,

$$[k_\mathbf{A}^\times : W(P)] = [G : HG'] = [G : G'] \cdot [HG' : G']^{-1}.$$

Здесь $[G : G']$ задается формулой

$$[G : G'] = [\Omega(P) : \Omega'(P)] = \prod_{v \in P} [k_v^\times : (k_v^\times)^n].$$

В правой части каждый сомножитель, соответствующий мнимой точке v, равен 1, а значит, равен $n^2 \mid n \mid_v^{-1}$, ибо в этом случае $\mid n \mid_v = n^2$. Если точка v вещественна, то n должно равняться 2, потому что поле $k_v = \mathbf{R}$ должно содержать примитивный корень n-й степени из 1. Поэтому соответствующий сомножитель равен 2, т. е. опять-таки равен $n^2 \mid n_v \mid^{-1}$. Сомножители, отвечающие конечным точкам $v \in P$, задаются следствием предл. 9 гл. II-3, в случае когда характеристика поля k равна нулю, и предложением 8 гл. II-3 в противном случае; здесь следует учесть, что n делит порядок группы корней из 1 в k, а значит, и в k_v и что поэтому n взаимно просто с p, если характеристика поля k равна p. Мы видим, что рассматриваемые сомножители опять равны $n^2 \mid n \mid_v^{-1}$. Поэтому

$$[G : G'] = \prod_{v \in P} (n^2 \mid n \mid_v^{-1}) = n^{2c} \prod_v \mid n \mid_v^{-1} = n^{2c},$$

ибо $\mid n \mid_v = 1$ при всех $v \notin P$.

Мы завершим наше доказательство, если покажем, что индекс $[HG' : G'] = n^c$. Но этот индекс совпадает с индексом подгруппы $H \cap G'$ в H, или в силу определений H и G' с индексом подгруппы $E(P) \cap \Omega'(P)$ в $E(P)$. По следствию 2 предл. 7 $E(P) \cap \Omega'(P)$ содержится в $E(P) \cap (k^\times)^n$, т. е. в $E(P)^n$, и очевидно, что $E(P) \cap \Omega'(P)$ содержит $E(P)^n$. Поэтому искомый индекс совпадает с индексом подгруппы $E(P)^n$ в $E(P)$. Как мы уже нашли выше, этот индекс равен n^c, чем и завершается наше доказательство.

§ 6. ГРУППА БРАУЭРА А-ПОЛЯ

Как мы убедились в § 3, класс простой алгебры A над k однозначно определяется локальными инвариантами $h_v(A)$, где $h_v(A) = 1$ почти для всех v, $h_v(A) = 1$ для всех мнимых точек v и $h_v(A) = 1$ или -1 для всех вещественных точек v; мы доказали также,

что $\sum h_v(A) = 1$. Поэтому группа Брауэра $H(k)$ будет полностью описана, если мы докажем следующую теорему.

Теорема 4. *Пусть k — некоторое* A*-поле, и для всякой точки v поля k пусть η_v — корень из* 1 *в* C. *Предположим, что $\eta_v = 1$ почти для всех v, $\eta_v = 1$ для каждой мнимой точки v, $\eta_v = 1$ или -1 для каждой вещественной точки v и $\prod_v \eta_v = 1$. Тогда существует простая алгебра A над k с инвариантами $h_v(A) = \eta_v$.*

Доказательство теоремы для поля k характеристики нуль мы отложим на конец параграфа, а сейчас проведем доказательство для поля k характеристики $p > 1$. Как и в гл. VI, обозначим через $D(k)$ группу дивизоров поля k, через $D_0(k)$ — группу дивизоров степени нуль и через $P(k)$ — группу главных дивизоров. Пусть h — число классов дивизоров степени нуль, т. е. индекс подгруппы $P(k)$ в $D_0(k)$, и пусть $v_1, \ldots, v_N$ — все точки поля k, для которых $\eta_v \neq 1$. Взяв в качестве n целое число, не меньшее 1, для которого $(\eta_{v_i})^n = 1$ при всех i, мы можем написать $\eta_{v_i} = \mathbf{e}(a_i/n)$, где $a_i \in \mathbf{Z}$ при $1 \leqslant i \leqslant N$. Так как $\prod \eta_v = 1$, то $\sum a_i = na$, где $a \in \mathbf{Z}$. Заменяя в случае надобности a_1 на $a_1 - na$, можно считать, что $\sum a_i = 0$.

Для всякого i обозначим через d_i степень точки v_i. Пусть $d = \prod d_i$ и $\mathfrak{m} = \sum (a_i d/d_i)\, v_i$. Тогда $\deg(\mathfrak{m}) = \sum a_i d = 0$, $\mathfrak{m} \in D_0(k)$, откуда $h\mathfrak{m} \in P(k)$, так что существует такой элемент $\theta \in k^\times$, что $\operatorname{div}(\theta) = h\mathfrak{m}$, т. е. $\operatorname{ord}_{v_i}(\theta) = ha_i d/d_i$ при $1 \leqslant i \leqslant N$ и $\operatorname{ord}_v(\theta) = 0$, если $\eta_v = 1$. Теперь рассмотрим константное расширение k' поля k степени hnd над k. Пусть φ — автоморфизм Фробениуса поля k' над k и χ — характер на группе Галуа поля k' над k, для которого $\chi(\varphi) = \mathbf{e}(1/hnd)$. Так же, как и в доказательстве предложения 3 § 1, сразу видим, применяя следствие 4 теор. 1 гл. XII-2, что для любой точки v поля k имеет место равенство $(\chi_v, \theta)_v = \chi(\varphi^\delta)^\nu$, где $\nu = \operatorname{ord}_v(\theta)$, δ — степень точки v. Ввиду нашего выбора θ и χ отсюда следует, что $(\chi_v, \theta)_v = \eta_v$ при всех v. Поэтому в силу формул (4) § 3 циклическая алгебра $A = [k'/k;\ \chi, \theta]$ и будет искомой алгеброй.

Предложение 9. *Для всякого $\chi \in X_k$ обозначим через $U(\chi)$ ядро характера $\chi \circ a$ на $k_\mathbf{A}^\times$. Тогда* (a) *если k' — циклическое расширение поля k, связанное с χ, то $U(\chi) = k^\times N_{k'/k}(k_\mathbf{A}'^\times)$;* (b) *для каждого целого $n \geqslant 1$, взаимно простого с p, где $p > 1$ — характеристика поля k, пересечение U_n ядер $U(\chi)$ по всем характерам $\chi \in X_k$ порядка, делящего n, совпадает с $k^\times (k_\mathbf{A}^\times)^n$.*

Положим $U'(\chi) = k^\times N_{k'/k}(k_A'^\times)$, где χ, k' такие же, как и выше, и положим $U_n' = k^\times (k_A^\times)^n$. Применяя к эндоморфизму $x \to x^n$ группы $G_k = k_A^\times / k^\times$ лемму 2 гл. XII-1, видим, что группа U_n' замкнута в $k_A^\times$; применяя ту же лемму к морфизму из $G_{k'}$ в G_k, определяемому морфизмом $N_{k'/k}$ из $k_A'^\times$ в $k_A^\times$, видим, что группа $U'(\chi)$ тоже замкнута в $k_A^\times$. Если χ имеет порядок n и поле k' таково, как в (a), то n есть степень поля k' над k, так что $N_{k'/k}(z) = z^n$ при $z \in k$, а значит и при $z \in k_A$, и, следовательно, $U'(\chi) \supset U_n'$.

Характер на $k_A^\times$ тривиален на $(k_A^\times)^n$ в том и только в том случае, когда его порядок делит n. Поэтому характер на $k_A^\times$, тривиальный на $k^\times$, имеет порядок, делящий n, в том и только в том случае, когда он тривиален на U_n'. Как и прежде, обозначим через U_k ядро морфизма $\mathfrak{a}$; как мы знаем, оно содержит $k^\times$. Если характеристика поля k равна нулю, то применим предложение 1 гл. XII-1 к спариванию между X_k и G_k, определенному с помощью $(\chi, z)_k$; в противном случае применим следствие 4 предл. 2 гл. XII-2. В обоих случаях мы видим, что каждый характер конечного порядка на $k_A^\times$, тривиальный на U_k, можно однозначно записать в виде $\chi \circ \mathfrak{a}$, где $\chi \in X_k$. Отсюда следует, что группа U_n является пересечением ядер характеров на $k_A^\times$, тривиальных на U_n' и на U_k. Поэтому она совпадает с замыканием подгруппы $U_n' U_k$, и $U_n = U_n'$ тогда и только тогда, когда $U_n' \supset U_k$. Мы видим также, что каждый характер на $k_A^\times$, тривиальный на $U'(\chi)$ и на U_k, должен иметь вид $\chi' \circ \mathfrak{a}$ с $\chi' \in X_k$.

По следствию 2 теор. 1 § 1 характер $\chi' \circ \mathfrak{a}$ тривиален на $U'(\chi)$ в том и только в том случае, когда циклическое расширение поля k, связанное с χ, содержится в k', т. е. в том и только в том случае, когда $\chi' = \chi^\nu$ для некоторого $\nu \in \mathbf{Z}$. Так как пересечение ядер $U(\chi^\nu)$ по $\nu \in \mathbf{Z}$, очевидно, совпадает с $U(\chi)$, отсюда видно, что $U(\chi)$ совпадает с замыканием подгруппы $U'(\chi) U_k$ и что $U(\chi) = U'(\chi)$ в том и только в том случае, когда $U'(\chi) \supset U_k$.

Теперь рассмотрим сначала случай характеристики нуль. Применим индукцию по n. Пусть для всех полей k характеристики нуль свойство (a) выполняется для каждого характера χ порядка $< n$. Тогда $U_k \subset k^\times N_{k'/k}(k_A'^\times)$ для любого такого поля k и любого его циклического расширения k' степени $< n$. В силу формулы (5) в самом конце § 3 отсюда следует, что $U_k = k^\times N_{k'/k}(U_k)$. Пусть L — расширение поля k, порожденное каким-нибудь примитивным корнем n-й степени из 1. Поскольку это расширение абелево и его степень над k меньше n, можно найти последовательность полей $k_0 = L, k_1, \ldots, k_r = k$, промежуточных между L и k, такую,

что при $1 \leqslant i \leqslant r$ поле k_{i-1} является циклическим расширением степени $< n$ над k_i. Поэтому при $1 \leqslant i \leqslant r$ имеем

$$U_{k_i} = k_i^{\times} N_{k_{i-1}/k_i}(U_{k_{i-1}}).$$

Индукцией по i для $1 \leqslant i \leqslant r$ сразу убеждаемся, что U_{k_i} содержится в $k_i^{\times}((k_i)_{\mathbf{A}}^{\times})^n$ (для $i = 0$ это имеет место по предложению 8). При $i = r$ получаем, что $U_k \subset U_n'$. Как мы видели выше, этим доказано (b); кроме того, отсюда следует, что $U_k \subset U'(\chi)$ для каждого χ порядка n, чем доказано (a) для таких характеров и завершена наша индукция.

Пусть теперь k — поле характеристики $p > 1$. Возьмем χ и k', такие, как в (a), и выберем $z \in U(\chi)$ так, чтобы $(\chi, z)_k = 1$. Тогда если положить $z = (z_v)$ и $\eta_v = (\chi_v, z_v)_v$, то выполняются условия теоремы 4. Поскольку эта теорема уже доказана для случая характеристики $p > 1$, то мы заключаем, что существует простая алгебра A над k с инвариантами $h_v(A) = \eta_v$. Но это означает, что выполнено условие (iv) предложения 5 § 3. В силу последнего утверждения этого предложения имеем $z \in U'(\chi)$, чем доказано (a). Так же, как и выше, мы выводим отсюда, с помощью формулы (5) § 3, что $U_k = k^{\times} N_{k'/k}(U_{k'})$ для всех циклических расширений k' поля k. Предполагая, что n взаимно просто с p, возьмем в качестве k' константное расширение поля k, порожденное примитивным корнем n-й степени из 1. Согласно предложению 8, $U_{k'} \subset k'^{\times}(k_{\mathbf{A}}'^{\times})^n$, поэтому то же самое верно для k.

Теперь мы можем доказать теорему 4 в случае характеристики нуль. Для каждой точки v поля k обозначим через $\nu(v)$ порядок элемента η_v в $\mathbf{C}^{\times}$. Существует такой характер χ, что для каждой точки v порядок характера χ_v делится на $\nu(v)$. Например, это условие будет выполняться, если в качестве χ взять характер, связанный с циклическим расширением k' поля k, описанным в лемме 5 § 3. Для каждой точки v морфизм $z \to (\chi_v, z)_v$ является характером на $k_v^{\times}$, и порядок этого характера, будучи равным порядку характера χ_v, делится на $\nu(v)$. Поэтому можно так выбрать $z_v \in k_v^{\times}$, чтобы $(\chi_v, z_v)_v = \eta_v$; при этом мы будем брать $z_v = 1$, если $\eta_v = 1$. Тогда $z = (z_v) \in k_{\mathbf{A}}^{\times}$ и из предположенного равенства $\prod \eta_v = 1$ вытекает, что z содержится в ядре характера $\chi \circ a$. Поэтому по предложению 9 $z \in k^{\times} N_{k'/k}(k_{\mathbf{A}}'^{\times})$, где k' — циклическое расширение поля k, связанное с χ. Записывая z в виде $z = 0 N_{k'/k}(z')$, где $z' \in k_{\mathbf{A}}'^{\times}$, и сочетая предложение 10 гл. IX-4 со следствием 3 теор. 1

гл. IV-1 и с предложением 1 § 1, мы видим, что циклическая алгебра $A = [k'/k; \chi, \theta]$ обладает требуемыми локальными инвариантами $h_v(A) = \eta_v$, чем и завершено доказательство теоремы 4.

§ 7. p-СИМВОЛ ГИЛЬБЕРТА

Как это обнаружится в следующем параграфе, к настоящему моменту в части, касающейся полей алгебраических чисел, наше исследование по существу уже завершено. Для случая характеристики $p > 1$ нам понадобится еще один символ, аналогичный изученному в § 5 символу Гильберта, но основанный на классах факторов $\{\xi, \theta\}_p$ гл. IX-5.

Для любого поля K характеристики $p > 1$ будем обозначать через Φ эндоморфизм $x \to x - x^p$ аддитивной группы поля K; ядро этого эндоморфизма совпадает с простым полем $\mathbf{F}_p$. Начнем с рассмотрения локального p-поля K характеристики p. Как обычно, обозначим через R максимальное компактное подкольцо в K, через P — максимальный идеал в R и через q — модуль поля K. Очевидно, Φ отображает R в R, а P в P; если $\operatorname{ord}(x) = v < 0$, то $\operatorname{ord}(\Phi(x)) = pv < 0$, так что $\Phi^{-1}(R) = R$.

Предложение 10. *Пусть K, R, P и Φ такие, как выше. Для $x \in K$, $z \in K^\times$ положим $(x, z)_{p,K} = (\chi_p, x, z)_K$. Тогда $\Phi(K)$ содержит P, но не содержит R; множество тех элементов $x \in K$, для которых $(x, z)_{p,K} = 1$ при всех $z \in K^\times$ (соотв. при всех $z \in R^\times$), совпадает с $\Phi(K)$ (соотв. с $R + \Phi(K)$); множество тех элементов $z \in K^\times$, для которых $(x, z)_{p,K} = 1$ при всех $x \in K$ (соотв. при всех $x \in R$), совпадает с $(K^\times)^p$ (соотв. с $(K^\times)^p R^\times$).*

Для $x \in P$ положим $\Psi(x) = \sum_{n=0}^{\infty} x^{p^n}$. Ясно, что эта сумма сходится и определяет эндоморфизм аддитивной группы P, и сразу видно, что как $\Phi \circ \Psi$, так и $\Psi \circ \Phi$ индуцируют на P тождественное отображение. Поэтому Φ индуцирует на P автоморфизм аддитивной группы P, так что $P \subset \Phi(K)$. Обозначим через F алгебраическое замыкание простого поля $\mathbf{F}_p$ в K. По теореме 7 гл. I-4 F есть поле из q элементов и $R = F + P$, так что $\Phi(R) = \Phi(F) + P$. Поскольку эндоморфизм, индуцированный посредством Φ на конечном поле F, имеет ядро $\mathbf{F}_p$, он не сюръективен. Поэтому $\Phi(R) \neq R$. Поскольку $\Phi^{-1}(R) = R$, отсюда видно, что R не содержится в $\Phi(K)$.

Если $(x, z)_{p,K} = 1$ при всех $z \in K^\times$, то характер $\chi_{p,K}$ должен быть тривиальным. Как мы видели в гл. IX-5, это имеет место

в том и только в том случае, когда $x \in \Phi(K)$. Возьмем любое $x \in R + \Phi(K)$. Поскольку $R = F + P$ и $P \subset \Phi(K)$, то можно записать x в виде $x = a + \Phi(u)$, где $a \in F$, $u \in K$. Тогда $\chi_{p,x}$ совпадает с $\chi_{p,a}$ и является характером, связанным с циклическим расширением поля K, порождаемым любым корнем α уравнения $X - X^p = a$. Так как элемент α алгебраичен над F, то он либо равен нулю, либо является корнем из 1, порядка взаимно простого с p, так что поле $K(\alpha)$ и, следовательно, характер $\chi_{p,x}$ неразветвлены. Поэтому $(x, z)_{p,K} = 1$ при всех $z \in R^\times$.

Теперь возьмем какой-нибудь корень ζ уравнения $X - X^q = 1$ в некотором алгебраическом замыкании поля K и положим $\varepsilon = \zeta - \zeta^p$. Группа Галуа поля $K(\zeta)$ над K порождена автоморфизмом Фробениуса, который отображает ζ в $\zeta^q = \zeta - 1$, поскольку элемент ζ алгебраичен над F. Следовательно, элемент ε инвариантен относительно этой группы, а значит, $\varepsilon \in F$, $K(\zeta)$ является неразветвленным расширением степени p над K и $\chi_{p,\varepsilon}$ является характером, связанным с этим расширением. Поэтому неразветвленные характеры над K порядка p или 1 — это характеры вида $(\chi_{p,\varepsilon})^\nu$, где $\nu \in \mathbf{Z}$. Следовательно, характер $\chi_{p,x}$ неразветвлен в том и только в том случае, когда он может быть записан в таком виде, т. е. в том и только в том случае, когда $x = \nu\varepsilon + \Phi(u)$, где $u \in K$, и в этом случае $x \in R + \Phi(K)$.

Что касается последних двух утверждений, то одно из них есть не что иное, как предложение 10 гл. XII-3. Наконец, если ε таково, как выше, то ядро морфизма $z \to (\varepsilon, z)_{p,K}$ является подгруппой индекса p в $K^\times$, содержащей $R^\times$, т. е. это ядро совпадает с $(K^\times)^p R^\times$. Для каждого $x \in R$, как мы видели, характер $\chi_{p,x}$ неразветвлен и имеет порядок p или 1, так что ядро морфизма $z \to (x, z)_{p,K}$ содержит $(K^\times)^p R^\times$. Наше доказательство завершено.

Следствие. *Для всякого целого числа $m \geqslant 0$ обозначим через $\Omega'(m, K)$ множество таких элементов $z \in K^\times$, что $(x, z)_{p,K} = 1$ при всех $x \in P^{-m}$. Это множество является открытой подгруппой в $K^\times$, содержащей $(K^\times)^p$; индекс этой подгруппы в $K^\times$ равен $pq^{m-m'}$, где m' — наибольшее целое число, не превосходящее m/p. Для каждой окрестности U единицы в $K^\times$ существует такое $m \geqslant 0$, что $\Omega'(m, K) \subset (K^\times)^p U$. Кроме того, $\Omega'(0, K) = (K^\times)^p R^\times$, и для каждого $m \geqslant 0$ множество тех элементов x в K, для которых $(x, z)_{p,K} = 1$ при всех $z \in \Omega'(m, K)$, совпадает с $P^{-m} + \Phi(K)$.*

Пусть F — такое конечное поле, как выше, и π — простой элемент в K. По теореме 8 гл. I-4 поле K можно отождествить с полем формальных степенных рядов от π с коэффициентами из F. Поэтому, если обозначить через V_m пространство многочленов степени $\leqslant m$

от π^{-1} с коэффициентами из F, то P^{-m} разлагается в прямую сумму своих подпространств V_m и P; размерность векторного пространства V_m над F равна $m+1$. Кроме того, как сразу проверяется, $V_m \cap \Phi(K) = \Phi(V_{m'})$, где m' таково, как в нашем следствии. По предложению 10 подгруппа $\Omega'(m, K)$ является пересечением ядер характеров $z \to (x, z)_{p,\kappa}$ на $K^\times$ по всем $x \in V_m$. Поэтому эта подгруппа открыта и содержит $(K^\times)^p$; по лемме 7 § 5 все характеры на $K^\times$, тривиальные на $\Omega'(m, K)$, имеют указанный вид. Отсюда следует, что индекс подгруппы $\Omega'(m, K)$ в $K^\times$ равен числу различных характеров такого вида, которое совпадает с индексом подпространства $V_m \cap \Phi(K)$ в V_m. Поскольку V_m и $V_{m'}$ имеют соответственно q^{m+1} и $q^{m'+1}$ элементов и поскольку ядром морфизма Φ из $V_{m'}$ на $V_m \cap \Phi(K)$ служит $\mathbf{F}_p$, последний индекс равен $p \cdot q^{m-m'}$.

По лемме 2 гл. XII-1 и лемме 7 § 5 группа $G' = K^\times/(K^\times)^p$ компактна, и ее характеры определяются характерами $z \to (x, z)_{p,\kappa}$ на $K^\times$, где $x \in K$. Поэтому пересечения ядер конечных подмножеств таких характеров образуют фундаментальную систему окрестностей единицы в G'. Иными словами, если U — произвольная окрестность единицы в $K^\times$, то можно найти конечное число характеров $z \to (x_i, z)_{p,\kappa}$, пересечение W ядер которых содержится в $(K^\times)^p U$. Поэтому W содержит $\Omega'(m, K)$, если $m \geqslant 0$ таково, что $-m \leqslant \leqslant \operatorname{ord}(x_i)$ при всех i. По предложению 10 $\Omega'(0, K) = (K^\times)^p R^\times$. Наконец, если характер $z \to (y, z)_{p,\kappa}$ тривиален на $\Omega'(m, K)$, то он должен совпадать с характером $z \to (x, z)_{p,\kappa}$ для некоторого $x \in V_m$. Согласно предложению 10, это эквивалентно тому, что $y \in V_m + \Phi(K)$. Поскольку $\Phi(K) \supset P$ и $V_m + P = P^{-m}$, этим доказано последнее утверждение нашего следствия.

Начиная с этого места, в настоящем параграфе, k будет $\mathbf{A}$-полем характеристики p. Нам понадобится следующая лемма.

Лемма 8. *Если v — произвольная точка поля k, то $k \cap (k_v)^p = k^p$.*

Ясно, что поле $k \cap (k_v)^p$ расположено между k и k^p. По лемме 1 гл. VIII-5 оно должно совпадать с k или с k^p. Поскольку поле $(k_v)^p$ не содержит простых элементов поля k_v, оно не плотно в k_v. Поскольку поле k плотно в k_v, то $(k_v)^p$ не может содержать k.

Предложение 11. *Для всех $x = (x_v) \in k_{\mathbf{A}}$ и всех $z = (z_v) \in k_{\mathbf{A}}^\times$ почти все сомножители в произведении*

$$(x, z)_p = \prod_v (x_v, z_v)_{p,\, k_v}$$

равны 1; *это произведение определяет локально постоянное отображение из* $k_{\mathbf{A}} \times k_{\mathbf{A}}^{\times}$ *в группу корней* p*-й степени из* 1 *в* $\mathbf{C}$; *множество тех элементов* $x \in k_{\mathbf{A}}$ (*соотв. тех элементов* $z \in k_{\mathbf{A}}^{\times}$), *для которых* $(x, z)_p = 1$ *при всех* $z \in k_{\mathbf{A}}^{\times}$ (*соотв. при всех* $x \in k_{\mathbf{A}}$), *совпадает с* $\Phi(k_{\mathbf{A}})$ (*соотв. с* $(k_{\mathbf{A}}^{\times})^p$).

Все это сразу следует из предложения 10.

Следствие 1. *Для каждого дивизора* $\mathfrak{m} = \sum m(v) \cdot v > 0$ *положим*

$$\Omega'(\mathfrak{m}) = \coprod_v \Omega'(m(v), k_v).$$

Это — открытая подгруппа в $k_{\mathbf{A}}^{\times}$, *содержащая* $(k_{\mathbf{A}}^{\times})^p$. *Для каждой окрестности* U *единицы в* $k_{\mathbf{A}}^{\times}$ *существует такой дивизор* $\mathfrak{m}$, *что* $\Omega'(\mathfrak{m}) \subset (k_{\mathbf{A}}^{\times})^p U$. *Множество тех элементов* $x \in k_{\mathbf{A}}$, *для которых* $(x, z)_p = 1$ *при всех* $z \in \Omega'(\mathfrak{m})$, *совпадает с*

$$\left(\prod_v p_v^{-m(v)}\right) + \Phi(k_{\mathbf{A}}).$$

Множество $\Omega'(m(v), k_v)$ при всех v является открытой подгруппой в $k_v^{\times}$, содержащей $(k_v^{\times})^p$, а $m(v) = 0$ почти для всех v, так что $\Omega'(m(v), k_v)$ содержит $r_v^{\times}$. Этим доказано наше первое утверждение. Что касается второго утверждения, то достаточно рассмотреть окрестности вида $U = \coprod U_v$, где U_v — окрестность единицы в $k_v^{\times}$ для всех v и $U_v = r_v^{\times}$ почти для всех v; поэтому наше утверждение сразу вытекает из следствия предл. 10. Предположим, наконец, что $x = (x_v)$ таково, как в нашем последнем утверждении. Тогда по тому же следствию можно записать x_v в виде $x_v = y_v + \Phi(u_v)$, где $y_v \in p_v^{-m(v)}$, $u_v \in k_v$ при всех v и $y_v = x_v$, причем $u_v = 0$ при $m(v) = 0$ и $x_v \in r_v$, стало быть, почти для всех v. Итак, $y = (y_v)$ и $u = (u_v)$ лежат в $k_{\mathbf{A}}$ и $x = y + \Phi(u)$, $y \in \prod p_v^{-m(v)}$.

Следствие 2. *В обозначениях следствия* 1 *предположим, что* $\deg(\mathfrak{m}) > 2g - 2$. *Тогда* $(k^{\times})^p = k^{\times} \cap \Omega'(\mathfrak{m})$.

Ясно, что правая часть последней формулы содержит $(k^{\times})^p$. Возьмем теперь $\xi \in k^{\times}$. Если $\xi \subset \Omega'(\mathfrak{m})$, то $(x, \xi)_p = 1$ при всех $x \in \prod p_v^{-m(v)}$, а также при всех $x \in k$, значит и при всех $x \in k_{\mathbf{A}}$ согласно следствию 3 теор. 2 гл. VI. По предложению 11 отсюда следует, что $\xi \in (k_{\mathbf{A}}^{\times})^p$, откуда $\xi \in (k^{\times})^p$ по лемме 8.

Следствие 3. *В обозначениях следствия* 1 *пусть* $\mathfrak{n} = \sum n(v) \cdot v$ — *дивизор поля* k *степени* $> 2g - 2$, *и пусть* $\mathfrak{m} > p\mathfrak{n}$. *Тогда множество тех элементов* $x \in k_{\mathbf{A}}$, *для которых* $(x, z)_p = 1$

при всех $z \in \Omega'(\mathfrak{m})$, *совпадает с*

$$(\prod_v p_v^{-m(v)}) + \Phi(k).$$

Применяя снова следствие 3 теор. 2 гл. VI, видим, что

$$\Phi(k_{\mathbf{A}}) = \Phi(k) + \Phi(\prod_v p_v^{-n(v)}).$$

Из нашего предположения вытекает, что второй член в правой части является подгруппой в $\prod p_v^{-m(v)}$. Наше утверждение вытекает поэтому из последнего утверждения следствия 1.

Предложение 12. *Множество тех элементов* $z \in k_{\mathbf{A}}^{\times}$, *для которых* $(\xi, z)_p = 1$ *при всех* $\xi \in k$, *совпадает с* $k^{\times}(k_{\mathbf{A}}^{\times})^p$.

Обозначим это множество через X_p; оно совпадает с пересечением ядер всех характеров $\chi_{p,\xi} \circ \mathfrak{a}$ на $k_{\mathbf{A}}^{\times}$ по $\xi \in k$ и содержит $k^{\times}(k_{\mathbf{A}}^{\times})^p$. По лемме 2 гл. XII-1, примененной к $G_k = k_{\mathbf{A}}^{\times}/k^{\times}$, $k^{\times}(k_{\mathbf{A}}^{\times})^p$ является замкнутой подгруппой в $k_{\mathbf{A}}^{\times}$ с компактной факторгруппой. По лемме 7 § 5 каждый характер на $k_{\mathbf{A}}^{\times}$, тривиальный на X_p, должен иметь вид $\chi_{p,\xi}$, где $\xi \in k$. Выберем какой-нибудь дивизор $\mathfrak{n} > 0$ поля k степени $> 2g - 2$. Ввиду следствия 1 предл. 11 нам достаточно показать, что X_p содержится в $M(\mathfrak{m}) = k^p\,\Omega'(\mathfrak{m})$ для всех дивизоров $\mathfrak{m} = \Sigma\, m(v) \cdot v > p\mathfrak{n}$. По лемме 1 гл. XII-1 $W(\mathfrak{m})$ имеет конечный индекс в $k_{\mathbf{A}}^{\times}$.

Поэтому будет достаточно показать, что $X_p W(\mathfrak{m})$ и $W(\mathfrak{m})$ имеют одинаковый индекс в $k_{\mathbf{A}}^{\times}$.

Индекс N подгруппы $X_p W(\mathfrak{m})$ равен числу различных характеров на $k_{\mathbf{A}}^{\times}$ вида $\chi_{p,\xi} \circ \mathfrak{a}$, или, что то же самое, вида $z \longrightarrow (\xi, z)_p$, с $\xi \in k$, тривиальных на $\Omega'(\mathfrak{m})$. По следствию 3 предл. 11 такой характер тривиален на $\Omega'(\mathfrak{m})$ в том и только в том случае, когда $\xi \in U(\mathfrak{m}) + \Phi(k)$, где $U(\mathfrak{m}) = \prod p_v^{-m(v)}$.

Как и в гл. VI, положим $\Lambda(\mathfrak{m}) = k \cap U(\mathfrak{m})$. Тогда, очевидно, N является индексом подгруппы $\Phi(k)$ в $\Lambda(\mathfrak{m}) + \Phi(k)$, или, что то же самое, индексом подгруппы $\Lambda(\mathfrak{m}) \cap \Phi(k)$ в $\Lambda(\mathfrak{m})$. Положим $\mathfrak{m}' = \sum m'(v) \cdot v$, где $m'(v)$ для всякой точки v есть наибольшее целое число, не превосходящее $m(v)/p$. Пусть m, m', n — степени дивизоров $\mathfrak{m}$, $\mathfrak{m}'$, $\mathfrak{n}$ соответственно. Тогда $m \geqslant m' \geqslant n > 2g - 2$. Ясно, что $\Lambda(\mathfrak{m}) \cap \Phi(k)$ совпадает с $\Phi(\Lambda(\mathfrak{m}'))$. Следствие 2 теор. 2 гл. VI показывает, что $\Lambda(\mathfrak{m})$, $\Lambda(\mathfrak{m}')$ суть векторные пространства размерности $m - g + 1$ и $m' - g + 1$ соответственно над полем констант F в k. Поскольку Φ отображает $\Lambda(\mathfrak{m}')$ на $\Lambda(\mathfrak{m}) \cap \Phi(k)$ с ядром $\mathbf{F}_p$, мы видим, что последняя группа имеет $p^{-1}q^{m'-g+1}$

элементов, в то время как $\Lambda(\mathfrak{m})$ имеет q^{m-g+1} элементов. Следовательно, $N = p \cdot q^{m-m'}$.

Теперь нам надо вычислить индекс подгруппы $W(\mathfrak{m})$ в $k_{\mathbf{A}}^{\times}$. Возьмем какое-нибудь конечное множество P точек поля k, содержащее все точки v, для которых $m(v) > 0$, и удовлетворяющее условию следствия теор. 7 гл. IV-4, т. е. такое, что $k_{\mathbf{A}}^{\times} = k^{\times}\,\Omega(P)$. Положим

$$\Omega'' = \prod_{v \in P} \Omega'(m(v), k_v) \times \prod_{v \notin P} r_v^{\times}.$$

Ясно, что эта группа содержит $\Omega(P)^p$ и $\Omega'(\mathfrak{m}) = (k_{\mathbf{A}}^{\times})^p\,\Omega''$, откуда

$$W(\mathfrak{m}) = k^{\times}(k_{\mathbf{A}}^{\times})^p\,\Omega'' = k^{\times}(k^{\times}\Omega(P))^p\,\Omega'' = k^{\times}\Omega''.$$

Положим теперь $G = k^{\times}\Omega(P)$, $G' = k^{\times} \times \Omega''$ и обозначим через f морфизм из G в $k_{\mathbf{A}}^{\times}$, для которого $f(\xi, u) = \xi u$ при $\xi \in k^{\times}$, $u \in \Omega(P)$; пусть H — ядро морфизма f. Тогда f отображает G на $k_{\mathbf{A}}^{\times}$, а G' на $W(\mathfrak{m})$, и H состоит из элементов (ξ, ξ^{-1}) с $\xi \in E(P) = k^{\times} \cap \Omega(P)$. Далее,

$$[k_{\mathbf{A}}^{\times} : W(\mathfrak{m})] = [G : HG'] = [G : G'] \cdot [HG' : G']^{-1},$$

причем в силу следствия предл. 10 индекс $[G : G']$ равен

$$[G : G'] = [\Omega(P) : \Omega''] = \prod_{v \in P} [k_v^{\times} : \Omega'(m(v), k_v)] = p^c q^{m-m'},$$

где $c = \operatorname{card}(P)$. Наконец, индекс $[HG' : G']$ совпадает с индексом подгруппы $H \cap G'$ в H, т. е. с индексом подгруппы $E(P) \cap \Omega''$ в $E(P)$. Ясно, что $E(P) \cap \Omega''$ содержится в группе $k^{\times} \cap \Omega'(\mathfrak{m})$, которая по следствию 2 предл. 11 совпадает с $(k^{\times})^p$, и содержит $E(P)^p$. Поскольку $E(P) \cap (k^{\times})^p$ совпадает с $E(P)^p$, мы видим, что $E(P) \cap \Omega'' = E(P)^p$, и из теоремы 9 гл. IV-4 сразу следует, что индекс этой подгруппы в $E(P)$ равен P^{c-1}. Доказательство закончено.

Следствие. *Если поле k такое, как выше, и U_k — ядро канонического морфизма* $\mathfrak{a}$, *то* $U_k \subset k^{\times}(U_k)^p$.

Согласно предложению 12, U_k содержится в $k^{\times}(k_{\mathbf{A}}^{\times})^p$, так что любой элемент u из U_k можно записать в виде $u = \xi v^p$, где $\xi \in k^{\times}$, $v \in k_{\mathbf{A}}^{\times}$. Возьмем любой характер $\chi \in X_k$ и обозначим через k' циклическое расширение поля k, связанное с χ. По предложению 9 § 6, ядро $U(\chi)$ характера $\chi \circ \mathfrak{a}$ равно $k^{\times}N_{k'/k}(k_{\mathbf{A}}'^{\times})$. Поскольку $U_k \subset U(\chi)$, отсюда по формуле (5) в конце § 3 следует, что $U_k = k^{\times}N_{k'/k}(U_{k'})$. Снова по предложе-

нию 12 $U_{k'}$ содержится в $k'^{\times}(k'^{\times}_{\mathbf{A}})^p$, так что U_k содержится в $k^{\times}N_{k'/k}(k'^{\times}_{\mathbf{A}})^p$. Поэтому для такого u, как выше, можно записать u в виде $u=\eta N_{k'/k}(w)^p$, где $\eta\in k^{\times}$, $w\in k'^{\times}_{\mathbf{A}}$. Это дает $\xi\eta^{-1}=v^pN_{k'/k}(w)^p$. Так как элемент $\xi\eta^{-1}$ содержится в $k^{\times}$ и в $(k^{\times}_{\mathbf{A}})^p$, то он по лемме 8 лежит в $(k^{\times})^p$. Записывая его как ζ^p с $\zeta\in k^{\times}$, получаем, что $v=\zeta^{-1}N_{k'/k}(w)$, ибо p — характеристика нашего поля. Отсюда видно, что $v\in U(\chi)$. Поскольку это имеет место при всех $\chi\in X_k$, то $v\in U_k$, чем и завершается наше доказательство.

§ 8. ЯДРО КАНОНИЧЕСКОГО МОРФИЗМА

Теперь мы в состоянии найти U_k во всех случаях.

Теорема 5. *Пусть k — некоторое* A*-поле и $\mathfrak{a}$ — канонический морфизм группы $k^{\times}_{\mathbf{A}}$ в группу Галуа $\mathfrak{A}$ поля k_{ab} над k. Тогда отображение $\chi\to\chi\circ\mathfrak{a}$ есть биективный морфизм группы X_k характеров на $\mathfrak{A}$ на группу характеров конечного порядка на $k^{\times}_{\mathbf{A}}$, тривиальных на $k^{\times}$.*

Каждый характер порядка n на $k^{\times}_{\mathbf{A}}$, тривиальный на $k^{\times}$, тривиален на $k^{\times}(k^{\times}_{\mathbf{A}})^n$, а значит, в силу предложения 9 § 6, и на U_k, если характеристика поля k равна нулю; в этом случае наше заключение сразу получается, если применить к $G_k=k^{\times}_{\mathbf{A}}/k^{\times}$ предложение 1 гл. XII-1. Пусть теперь k имеет характеристику $p>1$, и пусть ω — характер порядка n на $k^{\times}_{\mathbf{A}}$, тривиальный на $k^{\times}$. Запишем n в виде $n=n'p^i$, где n' взаимно просто с p и $i\geqslant 0$. Взяв целые числа a, b, для которых $n'a+p^ib=1$, имеем $\omega=\omega'\omega''$, где $\omega'=\omega^{p^{ib}}$ — характер порядка n', $\omega''=\omega^{n'a}$ — характер порядка p^i, причем оба эти характера тривиальны на $k^{\times}$. Точно так же, как выше, с помощью предложения 9 § 6 заключаем, что характер ω' тривиален на U_k. С другой стороны, из следствия предл. 12 § 7 индукцией по i легко вывести, что U_k содержится в $k^{\times}(U_k)^{p^i}$ и, следовательно, в $k^{\times}(k^{\times}_{\mathbf{A}})^{p^i}$, а значит, как и выше, характер ω'' тривиален на U_k. Отсюда видно, что характер ω тривиален на U_k. Применяя к $G_k=k^{\times}_{\mathbf{A}}/k^{\times}$ следствие 4 предл. 2 гл. XII-1, получаем наше утверждение.

Следствие 1. *Ядро U_k морфизма $\mathfrak{a}$ совпадает с пересечением замкнутых подгрупп $k^{\times}(k^{\times}_{\mathbf{A}})^n$ в $k^{\times}_{\mathbf{A}}$ по всем $n\geqslant 1$.*

Замкнутость этих подгрупп уже отмечалась при доказательстве предложения 9 § 6. Поэтому ясно, что $k^{\times}(k^{\times}_{\mathbf{A}})^n$ является пересе-

чением ядер всех характеров на $k_{\mathbf{A}}^{\times}$, тривиальных на $k^{\times}$, порядок которых делит n. Отсюда в силу теоремы 5 сразу вытекает наше утверждение.

Следствие 2. *Если k — поле характеристики $p > 1$, то $U_k = k^{\times}$.*

Имеем $G_k = G_k^1 \times N$, где $G_k^1 = k_{\mathbf{A}}^1/k$ и группа N изоморфна $\mathbf{Z}$. Поскольку группа G_k^1 компактна и, очевидно, вполне несвязна, то лемма 4 гл. VII-3 показывает, что все характеры этой группы имеют конечный порядок. Каждый такой характер можно однозначно продолжить до характера на G_k, тривиального на N, который также будет иметь конечный порядок и, следовательно, по теореме 5 будет тривиален на образе группы U_k в G_k. Поскольку в силу следствия 2 предл. 2 гл. XII-1 этот образ содержится в G_k^1, он должен поэтому совпадать с $\{1\}$, а это и означает, что $U_k = k^{\times}$.

Следствие 3. *Если характеристика поля k равна нулю, то U_k совпадает с замыканием подгруппы $k^{\times}k_{\infty+}^{\times}$ в $k_{\mathbf{A}}^{\times}$, где $k_{\infty+}^{\times}$ — группа тех иделей (z_v), для которых $z_v > 0$ для всех вещественных точек v и $z_v = 1$ для всех конечных точек v поля k.*

Имеем $G_k = G_k^1 \times N$, где $G_k^1 = k_{\mathbf{A}}^1/k^{\times}$, N — образ в G_k группы M, определенной в следствии 2 теор. 5 гл. IV-4. Обозначим через U' замыкание подгруппы $k^{\times}k_{\infty+}^{\times}$ в $k_{\mathbf{A}}^{\times}$, через U'' — образ группы U' в G_k и положим $U_1'' = U'' \cap G_k^1$. Очевидно, группа $k_{\mathbf{A}}^{\times}/k_{\infty+}^{\times}$ вполне несвязна; значит, то же верно и для $k_{\mathbf{A}}^{\times}/U'$ и, следовательно, для G_k/U''. Поскольку M содержится в U', то N содержится в U'', так что $U'' = U_1'' \times N$ и G_k/U'' можно отождествить с G_k^1/U_1''. Таким образом, факторгруппа G_k/U'' компактна. Отсюда видно, что каждый характер на G_k, тривиальный на U_1'', другими словами, каждый характер на $k_{\mathbf{A}}^{\times}$, тривиальный на U', имеет конечный порядок. Следовательно, группа U_k содержится в U'. Поскольку, как мы уже знаем, она содержит U', то $U_k = U'$.

Для того, чтобы получить более точные результаты о группе U_k в случае характеристики нуль, нам нужна одна алгебраическая лемма.

Лемма 9. *Пусть l — простое число, K — поле, характеристика которого отлична от l, и $\overline{K}$ — алгебраическое замыкание поля K. Для всякого $n \geqslant 0$ обозначим через K_n расширение поля K, порожденное примитивным корнем l^n-й степени из 1 в $\overline{K}$. Тогда если $l \neq 2$ или если $l = 2$ и $K = K_2$, то $K^{\times} \cap (K_n^{\times})^{l^n} =$*

$= (K^\times)^{l^n}$ *при всех* n. *Если* $l=2$, $K \neq K_2$, $2 \leqslant m < n$ *и* $K_2 \neq K_{m+1}$, *то* $K^\times \cap (K_n^\times)^{2^n} \subset (K^\times)^{2^{n-m}}$.

Возьмем $a \in K^\times \cap (K_n^\times)^{l^n}$. Предположим сначала, что a не содержится в $(K_1^\times)^{l^n}$, и пусть i — наименьшее целое число, для которого a лежит в $(K_{i+1}^\times)^{l^n}$, но не лежит в $(K_i^\times)^{l^n}$. Тогда $1 \leqslant i < n$, $K_i \neq K_{i+1}$ и можно записать a в виде $a = x^{l^n}$, где x содержится в K_{i+1}, но не содержится в K_i. Обозначим через η примитивный корень l^{i+1}-й степени из 1 в K_{i+1} и положим $\varepsilon = \eta^l$, $\zeta = \eta^{l^i}$; ε и ζ суть корни из 1 порядка l^i и l соответственно, и они содержатся в K_i. Имеем $K_{i+1} = K_i(\eta)$, $\eta^l = \varepsilon$, $\varepsilon \in K_i$ и $\varepsilon \neq 1$. Поэтому K_{i+1} является циклическим расширением степени l над K_i с группой Галуа, порожденной автоморфизмом σ, для которого $\eta^\sigma = \zeta\eta$. Положим $\theta = x^\sigma x^{-1}$. Тогда $\theta \in K_{i+1}$ и $\theta^{l^n} = 1$, так что θ является корнем из 1 некоторого порядка l^ν, делящего l^n. Поэтому элемент θ^σ должен иметь вид θ^s, где $s \in \mathbf{Z}$.

Далее, если $\nu \leqslant i$, то $\theta \in K_i$, так что можно взять $s=1$, а если $\nu > i$, то $\eta = \theta^r$ для некоторого $r \in \mathbf{Z}$, откуда $\eta^\sigma = \eta^s$, $\zeta = \eta^{s-1}$ и потому $s \equiv 1 + l^i$ по модулю l^{i+1}. Индукцией по h сразу получаем, что $x^{\sigma^h} = x\theta^{1+s+\ldots+s^{h-1}}$. При $h=l$ это дает сравнение $1 + s + \ldots + s^{l-1} \equiv 0$ по модулю l^ν. Если $\nu \leqslant 1$, то $s=1$, так что последнее сравнение влечет неравенство $\nu \leqslant 1$. Если $\nu > i$, то $s = 1 + al^i$, где $a \equiv 1$ по модулю l; отсюда следует, что если $l \neq 2$ или если $l=2$ и $i \geqslant 2$, то $s^l = 1 + bl^{i+1}$, где $b \equiv 1$ по модулю l, а это показывает, что $(s^l - 1)/(s-1)$ не может делиться на l^2 и, следовательно, на l^ν. Поскольку это противоречит доказанному выше, мы заключаем, что $\nu \leqslant 1$, исключая, быть может, случай $l=2$, $i=1$. Поэтому, исключая этот случай, мы можем записать θ в виде $\theta = \zeta^t$, где $l \in \mathbf{Z}$. Записывая теперь x' в виде $x' = \eta^{-t}x$, имеем $x'^\sigma = x'$, так что $x' \in K_i$ и $a = x'^{l^n}$; но это противоречит определению i. Тем самым доказано, что $a \in (K_1^\times)^{l^n}$ в случае $l \neq 2$ и что в случае $l=2$, если a не содержится в $(K_1^\times)^{2^n}$, то $a \in (K_2^\times)^{2^n}$. В первом случае запишем $a = y^{l^n}$, где $y \in K_1$. Группа Галуа поля K_1 над K является подгруппой в $(\mathbf{Z}/l\mathbf{Z})^\times$, поэтому степень d поля K_1 над K делит $l-1$ и взаимно проста с l. Пусть $1 = de + l^n f$. Имеем $a^d = b^{l^n}$, где $b = N_{K_1/K}(y)$, откуда $a = (a^f b^e)^{l^n}$. Если $l=2$, то $K_1 = K$. Поэтому если $a \notin (K^\times)^{2^n}$, то обязательно $K \neq K_2$ и мы можем применить доказанное выше, с $i=1$. Если в то же самое время $K_2 \neq K_{m+1}$, то порядок 2^ν элемента θ не может делиться на 2^{m+1}, так что он делит 2^m. Пола-

гая $b=x^{2^m}$, имеем $b^\sigma=b$, так что $b\in K_1=K$, и если $n>m$, то $a=b^{2^{n-m}}$.

В случае $l=2$, $K\neq K_2$, используя аналогичные аргументы, легко показать, что $(K^\times)^{2^n}$ является подгруппой индекса 2 в $K^\times\cap$ $\cap\ (K_n^\times)^{2^n}$, причем последняя группа порождена подгруппой $(K^\times)^{2^n}$ и элементом $(1+\omega)^{2^n}$, где ω — образующая группы всех корней u из 1 в K_2, порядок которых делит 2^n и которые удовлетворяют условию $N_{K_2/K}(u)=1$. Эти факты не будут использоваться далее.

Предложение 13. *Пусть P — конечное множество точек поля k, содержащее P_∞. Положим $H=\prod\limits_{v\notin P} k_v^\times$. Тогда $U_k\cap H=k_{\infty+}^\times$, если характеристика поля k равна нулю, и $U_k\cap H=\{1\}$, если k имеет характеристику $p>1$.*

Последнее утверждение очевидно, ибо в этом случае $U_k=k^\times$. Пусть k — поле характеристики нуль. По следствию 1 теор. 5 $U_k\cap H$ совпадает с пересечением всех групп $k^\times(k_{\mathbf{A}}^\times)^N\cap H$, $N\geqslant 1$. Элемент из $k_{\mathbf{A}}^\times$ принадлежит последней группе в том и только в том случае, когда его можно записать в виде ξz^N, где $\xi\in k^\times$, $z=(z_v)\in$ $\in k_{\mathbf{A}}^\times$ и $\xi=z_v^{-N}$ при всех $v\notin P$. Пусть $N=l^n$, где l — некоторое простое число; k' — расширение поля k, порожденное примитивным корнем N-й степени из 1 в $\bar{k}$, и k'' — расширение поля k', порожденное любым корнем уравнения $X^N=\xi$ в $\bar{k}$. Ясно, что для всех точек w поля k', которые не лежат над точками $v\in P$, имеем $\xi\in$ $\in(k_w'^\times)^N$. Поэтому в силу следствия 4 теор. 2 гл. VII-5 $k''=k'$, так что $\xi\in(k'^\times)^N$. По лемме 9 отсюда следует, что $\xi\in(k^\times)^N$, если $l\neq 2$. В случае $l=2$ обозначим через k_2 расширение поля k, порожденное примитивным корнем 4-й степени из 1. Если $k_2=k$, то опять $\xi\in(k^\times)^N$. Если же $k_2\neq k$, то обозначим через 2^m наибольшую степень двойки, делящую порядок группы всех корней из 1 в k_2. Согласно лемме 9, $\xi\in(k^\times)^{N'}$, где $N'=2^{-m}N$, при условии, что $n>m$. Беря $N=2^{m+\mu}$ в этом последнем случае и $N=l^\mu$ в противном случае, убеждаемся, что $k^\times(k_{\mathbf{A}}^\times)^N\cap H$ содержится в множестве $(k_{\mathbf{A}}^\times)^{l^\mu}\cap H$, совпадающем с H^{l^μ}. Отсюда видно, что $U_k\cap H$ содержится в H^{l^μ} для всех простых l и всех $\mu>0$.

Возьмем любое целое число $M>1$. Для каждого простого делителя l числа M пусть l^μ — наибольшая степень числа l, деля-

щая M. Можно найти такие целые числа $a(l)$, что $1/M = \sum l^{-\mu} a(l)$. Возьмем произвольный элемент $h \in U_k \cap H$ и для всякого l запишем h в виде $h = (h_l)^{l^\mu}$, где $h_l \in H$. Тогда $h = h'^M$, где $h' = \prod (h_l)^{a(l)}$. Поэтому $U_k \cap H \subset H^M$ при всех $M > 1$. Как было показано в следствии 1 теор. 3 гл. XII-3, пересечение всех групп $(k_v^\times)^M$ для заданной конечной точки v поля k равно $\{1\}$. Это же пересечение, очевидно, равно $\mathbf{C}^\times$, если $k_v = \mathbf{C}$, и равно $\mathbf{R}_+^\times$, если $k_v = \mathbf{R}$. Поэтому пересечение всех групп H^M совпадает с $k_{\infty+}^\times$, так что $U_k \cap H$ содержится в $k_{\infty+}^\times$. Поскольку обратное включение очевидно, наше доказательство закончено.

Следствие. *Для каждой точки v поля k поле $k_{v,\mathrm{ab}}$ порождает над k_v поле k_{ab}.*

Это утверждение тривиально, если $k_v = \mathbf{C}$, и очевидно, если $k_v = \mathbf{R}$, ибо тогда поле $k_{v,\mathrm{ab}}$ совпадает с $\mathbf{C}$ и порождается примитивным корнем 4-й степени из 1 в $\bar{k}$. Предположим теперь, что v — конечная точка. Объединение $k_{v,0}$ всех неразветвленных расширений поля k_v порождено над k_v корнями из 1. Поэтому подполе k' в $k_{v,\mathrm{ab}}$, порожденное над k_v полем k_{ab}, содержит $k_{v,0}$. Как и в § 1, пусть $\mathfrak{A}_v$ — группа Галуа поля $k_{v,\mathrm{ab}}$ над k_v, и пусть ρ_v — морфизм ограничения из $\mathfrak{A}_v$ в $\mathfrak{A}$. Автоморфизм α поля $k_{v,\mathrm{ab}}$ над k_v тождествен на k' в том и только в том случае, когда он тождествен на k_{ab}, т. е. в том и только в том случае, когда тождествен автоморфизм $\rho_v(\alpha)$. Предположим, что это имеет место. Тогда, поскольку $k_{v,0} \subset k'$, автоморфизм α содержится в группе Галуа поля $k_{v,\mathrm{ab}}$ над $k_{v,0}$, так что по следствию 2 теор. 3 гл. XII-3 его можно записать в виде $\alpha = \mathfrak{a}_v(z)$ с $z \in r_v^\times$. По предложению 2 § 1 $\rho_v(\alpha) = \mathfrak{a}(j_v(z))$, где j_v — естественное вложение поля $k_v^\times$ в $k_{\mathbf{A}}^\times$. Если автоморфизм $\rho_v(\alpha)$ тождествен, то элемент $j_v(z)$ должен содержаться в U_k. Беря в предложении 13 в качестве P множество, содержащее v, мы видим, что автоморфизм α сам должен быть тождественным. Наше следствие доказано.

В качестве примера применим это следствие к случаю $k = \mathbf{Q}$. Учитывая следствие 3 теор. 3 § 4, получаем, что для каждого простого числа p максимальное абелево расширение поля $\mathbf{Q}_p$ в алгебраическом замыкании поля $\mathbf{Q}_p$ порождается всеми корнями из 1. Разумеется, этот факт можно было бы вывести непосредственно из результатов гл. XII.

§ 9. ОСНОВНЫЕ ТЕОРЕМЫ

Основные результаты теории полей классов либо являются непосредственными следствиями из найденных выше результатов, либо выводятся из них с помощью рассуждений, в точности повторяющих доказательства соответствующих теорем гл. XII.

Теорема 6. *Если характеристика поля k равна нулю, то канонический морфизм α определяет изоморфизм группы $k_{\mathbf{A}}^{\times}/U_k$ на группу Галуа $\mathfrak{A}$ поля k_{ab} над k, где U_k — замыкание подгруппы $k^{\times}k_{\infty+}^{\times}$ в $k_{\mathbf{A}}^{\times}$. Если k — поле характеристики $p>1$, то морфизм α определяет биективный морфизм группы $k_{\mathbf{A}}^{\times}/k^{\times}$ на некоторую плотную подгруппу в $\mathfrak{A}$ и изоморфизм группы $k_{\mathbf{A}}^{1}/k^{\times}$ на группу Галуа $\mathfrak{A}_0$ поля k_{ab} над объединением k_0 всех расширений поля k, соответствующих расширению поля констант.*

Если учесть следствие 3 теор. 5 § 8, то первое утверждение нашей теоремы просто повторяет часть предложения 1 гл. XII-1. Второе утверждение повторяет часть следствия 2 предл. 2 гл. XII-1 и утверждение [II″] гл. XII-1, если принять во внимание равенство $U_k = k^{\times}$ и определение $\mathfrak{A}_0$ в § 1.

Теорема 7. *Пусть k' — расширение конечной степени над k, содержащееся в k. Положим $L = k' \cap k_{\mathrm{ab}}$. Тогда при $z \in k_{\mathbf{A}}^{\times}$ автоморфизм $\alpha(z)$ индуцирует тождественный автоморфизм на L в том и только в том случае, когда z содержится в $k^{\times}N_{k'/k}(k'^{\times}_{\mathbf{A}})$.*

Доказательство этой теоремы повторяет доказательство теоремы 4 гл. XII-3, только, разумеется, надо использовать теорему 5 § 8 вместо теоремы 3 гл. XII-3 и следствие 1 теор. 1 § 1 вместо следствия 1 теор. 2 гл. XII-2.

Следствие 1. *В предположениях и обозначениях теоремы 7 пусть $\mathfrak{B}$ — подгруппа в $\mathfrak{A}$, соответствующая полю L. Тогда*

$$k^{\times}N_{L/k}(L_{\mathbf{A}}^{\times}) = k^{\times}N_{k'/k}(k_{\mathbf{A}}'^{\times}) = \alpha^{-1}(\mathfrak{B}).$$

Последнее равенство является переформулировкой теоремы 7. Применяя эту теорему к $k' = L$, получаем, что $k^{\times}N_{L/k}(L_{\mathbf{A}}^{\times}) = \alpha^{-1}(\mathfrak{B})$.

Следствие 2. *Для каждого расширения L конечной степени над k, содержащегося в k_{ab}, обозначим через $\mathfrak{B}(L)$ подгруппу в $\mathfrak{A}$, соответствующую полю L, и положим $N(L) = k^{\times}N_{L/k}(L_{\mathbf{A}}^{\times})$. Тогда $N(L) = \alpha^{-1}(\mathfrak{B}(L))$; $\mathfrak{B}(L)$ является замыканием подгруппы $\alpha(N(L))$ в $\mathfrak{A}$; L состоит из всех элементов поля k_{ab}, инвариантных относительно $\alpha(z)$ при всех $z \in N(L)$ и α определяет изоморфизм*

группы $k_{\mathbf{A}}^{\times}/N(L)$ *на группу Галуа* $\mathfrak{A}/\mathfrak{B}(L)$ *поля* L *над* k. *Кроме того, отображение* $L \to N(L)$ *биективно отображает подполя в* k_{ab} *конечной степени над* k *на открытые подгруппы конечного индекса в* $k_{\mathbf{A}}^{\times}$, *содержащие* $k^{\times}$.

Если учесть следствия теор. 5 § 8, то все это просто пересказ предложения 3 гл. XII-1. Следует заметить, что в случае, когда характеристика поля k равна нулю, группа $k_{\infty}^{\times}$, будучи произведением конечного числа сомножителей, изоморфных $\mathbf{R}_{+}^{\times}$ или $\mathbf{C}^{\times}$, порождается всякой своей окрестностью единицы и потому содержится в каждой открытой подгруппе в $k_{\mathbf{A}}^{\times}$.

Следствие 3. *В обозначениях следствия* 2 *пусть* Γ — *группа всех характеров на* $\mathfrak{A}$, *тривиальных на* $\mathfrak{B}(L)$. *Тогда связанная с* L *подгруппа* $N(L)$ *в* $k_{\mathbf{A}}^{\times}$ *является пересечением ядер характеров* $\omega = \chi \circ \mathfrak{a}$ *на* $k_{\mathbf{A}}^{\times}$, *где* χ *пробегает* Γ, *и отображение* $\chi \to \chi \circ \mathfrak{a}$ *есть изоморфизм группы* Γ *на группу* γ *всех характеров на* $k_{\mathbf{A}}^{\times}$, *тривиальных на* $N(L)$.

Первое утверждение является простой переформулировкой в других терминах равенства $N(L) = \mathfrak{a}^{-1}(\mathfrak{B}(L))$. Аналогичным образом наше второе утверждение есть переформулировка того факта, что $\mathfrak{a}$ определяет изоморфизм группы $k_{\mathbf{A}}^{\times}/N(L)$ на $\mathfrak{A}/\mathfrak{B}(L)$.

Следствие 4. *Пусть* χ — *произвольный характер на* $\mathfrak{A}$, *и пусть* L — *циклическое расширение поля* k, *связанное с* χ. *Тогда связанная с* L *подгруппа* $N(L)$ *совпадает с ядром характера* $\omega = \chi \circ \mathfrak{a}$ *на* $k_{\mathbf{A}}^{\times}$.

Это — частный случай следствия 3, соответствующий выбору в качестве группы Γ группы, порожденной элементом χ.

Следствие 5. *Пусть* k *и* k' *таковы, как в теореме* 7, *и пусть* M — *подполе в* k_{ab} *конечной степени над* k. *Обозначим через* M' *композит полей* M *и* k'. *Пусть* $U = k^{\times} N_{M/k}(M_{\mathbf{A}}^{\times})$ *и* $U' = k'^{\times} N_{M'/k'}(M_{\mathbf{A}}'^{\times})$ — *открытые подгруппы в* $k_{\mathbf{A}}^{\times}$ *и в* $k_{\mathbf{A}}'^{\times}$, *связанные с абелевыми расширениями* M *над* k *и* M' *над* k' *соответственно согласно следствию* 2. *Тогда* $U' = N_{k'/k}^{-1}(U)$.

Доказательство идентично доказательству следствия 3 теор. 4 гл. XII-3.

Теорема 8. *Пусть* k' — *расширение конечной степени над* k, *содержащееся в* k_{sep}, *и* $\mathfrak{a}$, $\mathfrak{a}'$ — *канонические морфизмы из* $k_{\mathbf{A}}^{\times}$ *в* $\mathfrak{A}$ *и из* $k_{\mathbf{A}}'^{\times}$ *в группу Галуа* $\mathfrak{A}'$ *поля* k'_{ab} *над* k' *соответственно.*

Пусть t — гомоморфизм переноса из $\mathfrak{A}$ в $\mathfrak{A}'$ и j — естественное вложение группы $k_{\mathbf{A}}^{\times}$ в $k_{\mathbf{A}}'^{\times}$. Тогда $t \circ \mathfrak{a} = \mathfrak{a}' \circ j$.

Доказательство идентично доказательству теоремы 6 гл. XII-5, за тем, разумеется, исключением, что теперь следует использовать теорему 7 вместо теоремы 4 гл. XII-3.

§ 10. ЛОКАЛЬНОЕ ПОВЕДЕНИЕ АБЕЛЕВЫХ РАСШИРЕНИЙ

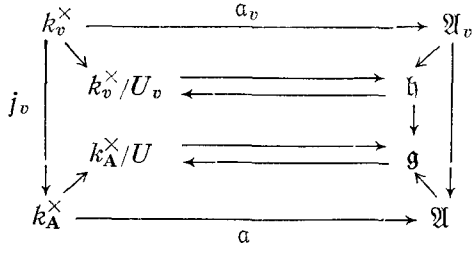
Пусть поле k такое, как выше, и пусть v — произвольная точка поля k. Как и в § 1, выберем какое-нибудь алгебраическое замыкание K_v поля k_v, содержащее алгебраическое замыкание $\bar{k}$ поля k. Предложение 1 гл. III-1 показывает, что если k' — любое расширение конечной степени над k, содержащееся в $\bar{k}$, то подполе в K_v, порожденное над k_v полем k', можно отождествить с пополнением k'_w поля k' относительно одной из точек w, лежащей над v. Если k' — расширение Галуа поля k с группой Галуа $\mathfrak{g}$, то можно, как мы это уже делали в подобных случаях ранее, применить следствие 4 теор. 4 гл. III-4, которое показывает, что k'_w является расширением Галуа поля k_v; если $\mathfrak{h}$ — его группа Галуа над k_v, то морфизм ограничения из $\mathfrak{h}$ в $\mathfrak{g}$ инъективен и можно с его помощью отождествить $\mathfrak{h}$ с некоторой подгруппой в $\mathfrak{g}$; поэтому пополнения поля k' относительно точек поля k', лежащих над v, находятся во взаимно однозначном соответствии с классами смежности в $\mathfrak{g}$ по $\mathfrak{h}$, и все эти пополнения изоморфны k'_w.

Применим это к случаю, когда поле k' абелево над k. Тогда по следствию 2 теор. 7 § 9 группа Галуа $\mathfrak{g}$ этого поля изоморфна группе $k_{\mathbf{A}}^{\times}/U$, где $U = N(k') = k^{\times} N_{k'/k}(k_{\mathbf{A}}'^{\times})$, так что U является открытой подгруппой конечного индекса в $k_{\mathbf{A}}^{\times}$. Более точно, если $\mathfrak{B}$ — подгруппа группы Галуа $\mathfrak{A}$ поля k_{ab} над k, соответствующая полю k', то канонический морфизм $\mathfrak{a}$ определяет изоморфизм группы $k_{\mathbf{A}}^{\times}/U$ на группу $\mathfrak{g} = \mathfrak{A}/\mathfrak{B}$. С другой стороны, если k_v, k'_w такие, как выше, то k'_w является абелевым расширением поля k_v, которому следствие 2 теор. 4 гл. XII-3 сопоставляет открытую подгруппу $U_v = N_{k'_w/k_v}(k_w'^{\times})$ в $k_v^{\times}$. Обозначим, как и прежде, через $\mathfrak{A}_v$ группу Галуа поля $k_{v,\mathrm{ab}}$ над k_v и обозначим через $\mathfrak{B}_v$ подгруппу в $\mathfrak{A}_v$, соответствующую полю k'_w. То же самое следствие показывает, что канонический морфизм $\mathfrak{a}_v$ из $k_v^{\times}$ в $\mathfrak{A}_v$ определяет изоморфизм группы $k_v^{\times}/U_v$ на $\mathfrak{h} = \mathfrak{A}_v/\mathfrak{B}_v$. Связь между всеми этими группами дается следующим предложением.

Предложение 14. *В принятых выше обозначениях и предположениях подгруппа U_v в $k_v^\times$, ассоциированная с k'_w, задается равенством $U_v = k_v^\times \cap U$. Если группу $\mathfrak{g}$ отождествить с группой $k_\mathbf{A}^\times/U$ посредством изоморфизма $\mathfrak{a}$ и группу $\mathfrak{h}$ с группой k_v/U_v посредством изоморфизма $\mathfrak{a}_v$, то морфизм ограничения из $\mathfrak{h}$ в $\mathfrak{g}$ совпадает с морфизмом из $k_v^\times/U_v$ в $k_\mathbf{A}^\times/U$, определяемым естественным вложением j_v группы $k_v^\times$ в $k_\mathbf{A}^\times$, и точки поля k', лежащие над v, находятся во взаимно однозначном соответствии с классами смежности в $k_\mathbf{A}^\times$ по $k_v^\times U$.*

Возьмем любое $z_v \in k_v^\times$ и положим $\alpha = \mathfrak{a}_v(z_v)$. По предложению 2 § 1 автоморфизм поля k_{ab}, индуцированный посредством α, совпадает с $\rho_v(\alpha) = \mathfrak{a}(z)$, где $z_v = j_v(z_v)$. Поскольку поле k'_w порождено над k_v полем k', то α индуцирует тождественное отображение на k'_w в том и только в том случае, когда $\rho_v(\alpha)$ индуцирует тождественное отображение на k'. Ввиду следствия 2 теор. 4 гл. XII-3 и следствия 2 теор. 7 § 9 это означает в точности то, что z_v содержится в U_v в том и только в том случае, когда $j_v(z_v)$ содержится в U; это можно записать в виде равенства $U_v = k_v^\times \cap U$. Второе утверждение нашего предложения сразу вытекает из тех же фактов; из этих фактов следует также, что образ в $\mathfrak{g}$ группы $\mathfrak{h}$ можно отождествить с образом в $k_\mathbf{A}^\times/U$ группы $k_v^\times$, который совпадает с $k_v^\times U/U$, и что группу $\mathfrak{g}/\mathfrak{h}$ можно отождествить с группой $k_\mathbf{A}^\times/k_v^\times U$. Как мы упоминали выше, точки поля k', лежащие над v, находятся во взаимно однозначном соответствии с классами смежности в $\mathfrak{g}$ по $\mathfrak{h}$ и, следовательно, с классами смежности в $k_\mathbf{A}^\times$ по $k_v^\times U$. Этим завершается доказательство.

Наше предложение и его доказательство остаются справедливыми и в том случае, когда v — бесконечная точка, потому что теорема 4 гл. XII-3 и ее следствия сохраняют силу для $\mathbf{R}$ и $\mathbf{C}$, как было отмечено в свое время. Связи между различными группами и морфизмами, рассмотренными выше, иллюстрируются следующей диаграммой:



Следствие 1. *Пусть γ — группа характеров на $k_{\mathbf{A}}^{\times}$, тривиальных на U, и пусть γ_v — группа характеров на $k_v^{\times}$, тривиальных на U_v. Тогда отображение, которое каждому $\omega \in \gamma$ сопоставляет характер ω_v, индуцированный на $k_v^{\times}$ характером ω, является сюръективным морфизмом из γ на γ_v и порядок ядра этого морфизма равен числу точек поля k', лежащих над v.*

Ясно, что отображение $\omega \to \omega_v$ есть морфизм из γ в γ_v. Каждый характер на $k_v^{\times}$, тривиальный на U_v, можно однозначно продолжить до характера на $k_v^{\times}U$, тривиального на U, а этот характер в свою очередь можно продолжить до характера на $k_{\mathbf{A}}^{\times}$, который будет лежать в γ. Поэтому наш морфизм сюръективен. Его ядро состоит из характеров на $k_{\mathbf{A}}^{\times}$, тривиальных на $k_v^{\times}U$. Значит, оно двойственно факторгруппе $k_{\mathbf{A}}^{\times}/k_v^{\times}U$. В силу последнего утверждения предложения 14 порядок этой группы именно таков, как утверждается в нашем следствии.

Следствие 2. *В сделанных выше предположениях пусть v — конечная точка поля k. Тогда модулярная степень f и индекс ветвления e поля k'_w над k_v задаются формулами*

$$f = [k_v^{\times} : r_v^{\times}U_v] = [k_v^{\times}U : r_v^{\times}U],$$
$$e = [r_v^{\times}U_v : U_v] = [r_v^{\times}U : U].$$

По следствию предл. 6 гл. XII-2 и следствию 2 теор. 4 гл. XII-3 максимальное неразветвленное расширение поля k_v, содержащееся в k'_w, ассоциировано с подгруппой $r_v^{\times}U_v$ в $k_v^{\times}$. Отсюда сразу вытекает первая часть нашего следствия.

Следствие 3. *В предположениях следствия 2 поле k'_w неразветвлено над k_v тогда и только тогда, когда $U \supset r_v^{\times}$. В этом случае автоморфизм поля k' над k, индуцированный автоморфизмом Фробениуса поля k'_w над k_v, совпадает с образом в $\mathfrak{g} = k_{\mathbf{A}}^{\times}/U$ любого простого элемента π_v поля k_v и является элементом порядка f в $\mathfrak{g}$.*

Неразветвленность поля k'_w над k_v означает в точности то, что $e = 1$, так что наше первое утверждение является частным случаем следствия 2. Второе сразу вытекает из предложения 14 в сочетании со следствием 4 теор. 1 гл. XII-2, которое утверждает, в нашей ситуации, что a_v (π_v) есть автоморфизм Фробениуса поля k'_w над k_v.

Как мы знаем из следствия предл. 3 гл. VIII-1, поле k'_w, в обозначениях следствий 2 и 3, неразветвлено над k_v в том и только

в том случае, когда его дифферента над k_v совпадает с r'_w. В силу определений дифференты и дискриминанта (гл. VIII-4) и того факта, что пополнения поля k' относительно всех точек поля k', лежащих над v, изоморфны, это означает в точности то, что поле k'_w неразветвлено над k_v в том и только в том случае, когда v не входит в дискриминант поля k' над k. По следствию 3 предл. 14 это имеет место в том и только в том случае, когда $U \supset r_v^\times$. Этот качественный результат можно уточнить следующим образом.

Теорема 9. *Пусть k' — расширение конечной степени над k, содержащееся в k_{ab}, и пусть $U = k^\times N_{k'/k}(k_{\mathbf{A}}'^\times)$ — подгруппа в $k_{\mathbf{A}}^\times$, ассоциированная с k'. Обозначим через γ группу всех характеров на $k_{\mathbf{A}}^\times$, тривиальных на U. Для всякого $\omega \in \gamma$ обозначим, далее, через $\mathfrak{f}(\omega)$ ведущий идеал характера ω. Тогда дискриминант $\mathfrak{D}$ поля k' над k задается равенством $\mathfrak{D} = \prod\limits_{\omega \in \gamma} \mathfrak{f}(\omega)$ или равенством $\mathfrak{D} = \sum\limits_{\omega \in \gamma} \mathfrak{f}(\omega)$ в соответствии с тем, равна или не равна нулю характеристика поля k.*

Пусть обозначения те же самые, что и в следствии 2 предл. 14, и пусть p_v — максимальный идеал в максимальном компактном подкольце r_v в k_v. Обозначим через p_v^δ дискриминант поля k'_w над k_v и через ν — число точек поля k', лежащих над v. Поскольку пополнения поля k' относительно всех этих точек изоморфны k'_w, они вносят одинаковый вклад в дискриминант $\mathfrak{D}$, так что их совместный вклад равен $\mathfrak{p}_v^{\delta\nu}$ (соответственно $\delta\nu \cdot v$). Пусть группа γ_v такова, как в следствии 1 предл. 14. Обозначим через ω'_i, $1 \leqslant i \leqslant d$, различные элементы группы γ_v и для всякого i обозначим через $p_v^{f(i)}$ ведущий идеал характера ω'_i. По следствию 2 теор. 5 гл. XII-4 имеем $\delta = \sum f(i)$. По следствию 1 предл. 14 всякий характер ω'_i индуцирован на $k_v^\times$ в точности ν характерами $\omega \in \gamma$. Теперь наше утверждение очевидно.

Теорема 10. *В предположениях и обозначениях теоремы 9 дедекиндова дзета-функция поля k' задается равенством $\zeta_{k'}(s) = \prod\limits_{\omega \in \gamma} L(s, \omega)$.*

Достаточно проверить это в случае $\mathrm{Re}\,(s) > 1$ когда бесконечные произведения для этих функций абсолютно сходятся. В этом случае достаточно показать, что для всякой конечной точки v поля k вклад в $\zeta_{k'}(s)$ точек поля k', лежащих над v, равен произведению вкладов точки v в произведения $L(s, \omega)$. Если f таково, как в следствии 2

предл. 14, то вклад точки w в произведение $\zeta_{k'}(s)$ равен $(1 - q_v^{-fs})^{-1}$; это будет также вкладом всякой точки поля k', лежащей над v, так что если ν — число таких точек, то общий вклад равен $(1 - q_v^{fs})^{-\nu}$.

С другой стороны, при $\omega \in \gamma$ вклад точки v в $L(s, \omega)$ равен 1, если только характер ω_v не является неразветвленным, и равен $(1 - \omega_v(\pi_v) q_v^{-s})^{-1}$, если он неразветвлен. Ввиду следствия 1 предл. 14 произведение этих вкладов равно $\prod (1 - \omega'(\pi_v) q_v^{-s})^{-\nu}$, где произведение берется по всем различным характерам ω' на $k_v^\times$, тривиальным на U_v и на $r_v^\times$, т. е. тривиальным на $r_v^\times U_v$. По следствию 2 предл. 14 группа $k_v^\times / r_v^\times U_v$ имеет порядок f. Ясно, что эта группа порождена образом в ней элемента π_v и, следовательно, циклична. Поэтому существует ровно f характеров ω', и их значения в точке π_v суть все корни f-й степени из 1 в $\mathbf{C}$. Отсюда следует, что произведение $\prod (1 - \omega'(\pi_v) t)$ для каждого $t \in \mathbf{C}$ равно $1 - t^f$, чем наше доказательство и завершено.

Следствие. *В обозначениях и предположениях теорем* 9 *и* 10 *пусть* k *— некоторое поле алгебраических чисел.*

Тогда

$$Z_{k'}(s) = \pi^{n\rho/2} \prod_{\omega \in \gamma} \Lambda(s, \omega),$$

где n *— степень поля* k' *над* k *и* ρ *— число вещественных точек поля* k*, для которых лежащие над ними точки поля* k' *мнимы.*

Здесь $Z_{k'}(s)$ и $\Lambda(s, \omega)$ — функции, определенные в теореме 3 гл. VII-6 и в теореме 5 гл. VII-7 соответственно. Ввиду теоремы 10 единственное, что надо доказать,— это что всякая бесконечная точка v поля k дает одни и те же G-сомножители в обеих частях формулы нашего следствия. Определим ν, как выше. Тогда общий вклад в $Z_{k'}(s)$ всех ν точек поля k', лежащих над v, равен $G_1(s)^\nu$ или $G_2(s)^\nu$ в соответствии с тем, вещественна точка w или нет. Вклад точки v в $\Lambda(s, \omega)$ равен $G_1(s + s_v)$ или $G_2(s + s_v)$ соответственно тому, вещественна точка v или нет; s_v зависит от ω_v описанным в гл. XII-7 образом.

Характер ω_v, который тривиален на U_v, открытой подгруппе в $k_v^\times$, должен быть тривиальным на $\mathbf{C}^\times$ в случае $k_v = \mathbf{C}$ и на $\mathbf{R}^\times$ или $\mathbf{R}_+^\times$ в случае $k_v = \mathbf{R}$. Если характер ω_v тривиален на $k_v^\times$, то мы должны положить $s_v = 0$, а если нет, то имеем $k_v = \mathbf{R}$, $U_v = \mathbf{R}_+^\times$ и $\omega_v(x) = x^{-1} \mid x \mid$, откуда $s_v = 1$. Поскольку степень поля k'_w над k_v равна $[k_v^\times : U_v]$, то в последнем случае она равна 2, а в первом равна 1. Принимая во внимание следствие 1 предл. 14, мы видим,

что вклад точки v в $\Pi\Lambda$ $(s,\ \omega)$ равен $G_1(s)^{\nu}$, если точки v и w вещественны, $G_2(s)^{\nu}$, если обе они мнимы, и $G_1(s)^{\nu}G_1(s+1)^{\nu}$, если точка v вещественна, а точка w мнима. В последнем случае $\nu = n/2$, например по следствию 1 теор. 4 гл. III-4. Наше следствие вытекает из этих фактов и из тождества $G_2(s) = \pi G_1(s)\,G_1(s+1)$, которое совпадает с известным тождеством для гамма-функций, уже приводившимся в конце гл. X.

§ 11. «КЛАССИЧЕСКАЯ» ТЕОРИЯ ПОЛЕЙ КЛАССОВ

Перевод наших результатов на традиционный язык теории полей классов основан на следующих фактах:

(a) Пусть $\mathfrak{U}$ — множество всех открытых подгрупп в $k_{\mathbf{A}}^{\times}$, содержащих $k^{\times}$, $\mathfrak{U}'$ — множество тех из них, которые имеют конечный индекс в $k_{\mathbf{A}}^{\times}$, и $\mathfrak{U}''$ — множество тех из них, которые содержатся в $k_{\mathbf{A}}^{1}$ и имеют конечный индекс в $k_{\mathbf{A}}^{1}$. Лемма 1 гл. XII-1 показывает, что $\mathfrak{U} = \mathfrak{U}'$ и $\mathfrak{U}'' \neq \varnothing$, если k — поле алгебраических чисел, и что $\mathfrak{U} = \mathfrak{U}' \cup \mathfrak{U}''$, если k — поле характеристики $p > 1$.

(b) Пусть $\mathfrak{K}$ — множество всех полей конечной степени над k, промежуточных между k и k_{ab}; в случае когда поле k имеет характеристику $p > 1$, пусть $\mathfrak{K}_0$ — множество всех полей конечной степени над k_0, расположенных между k_0 и k_{ab}. Следствие 2 теор. 7 § 9 определяет взаимно однозначное соответствие между $\mathfrak{U}'$ и $\mathfrak{K}$; из последнего утверждения теор. 6 § 9 и из теории Галуа следует, что в случае, когда k имеет характеристику $p > 1$, существует взаимно однозначное соответствие между $\mathfrak{U}''$ и $\mathfrak{K}$.

(c) Поскольку открытые подгруппы любой группы являются ядрами ее морфизмов на дискретные группы, постольку описанные в (a) открытые подгруппы группы $k_{\mathbf{A}}^{\times}$ можно рассматривать как ядра таких морфизмов, а сами эти морфизмы описывать в терминах морфизмов групп $I(P)$, $D(P)$ указанным в гл. VII-8 способом.

Для нашей теперешней цели будет удобнее дать новую интерпретацию результатов гл. VII-8, следующим образом модифицировав обозначения этой главы.

Как и в гл. VII-8, для любого конечного множества P точек поля k, содержащего P_∞, обозначим через G_P группу тех иделей (z_v) поля k, для которых $z_v = 1$ при $v \in P$, и через G'_P группу тех иделей, для которых $z_v = 1$ при $v \in P$ и $z_v \in r_v^{\times}$, т. е. $|z_v|_v = 1$, при $v \notin P$. Будем обозначать через L_p свободную группу, порожденную точками v, не содержащимися в P; эту группу будем записывать мульти-

пликативно. Группу L_P можно очевидным образом отождествить с группой $I(P)$ или $D(P)$ из гл. VII-8, в зависимости от того, какова характеристика поля k. Обозначим через l_P морфизм из G_P на L_P с ядром G'_P, задаваемый следующим образом: $(z_v) \to \coprod_{v \nmid P} v^{r(v)}$, где $r(v) = \operatorname{ord}_v(z_v)$. Кроме того, для каждого $\xi \in k^\times$, такого, что $\xi \in r_v^\times$ для всех конечных точек $v \in P$, положим $\operatorname{pr}(\xi) = \coprod_{v \notin P} v^{\rho(v)}$, где $\rho(v) = \operatorname{ord}_v(\xi)$ при $v \notin P$.

Определение 1. *Подгруппу J в L_P будем называть конгруэнцгруппой, если для каждой точки $v \in P$ можно найти такую открытую подгруппу g_v в $k_v^\times$, содержащуюся в $r_v^\times$ в случае, когда точка v конечна, что $\operatorname{pr}(\xi) \in J$ при всех $\xi \in \bigcap (k^\times \cap g_v)$; группу $g = \coprod_{v \in P} g_v$ будем при этом называть определяющей группой для J.*

Ясно, что ничего не изменится, если в качестве g_v для каждой конечной точки $v \in P$ брать лишь подгруппы вида $1 + p_v^m$ с $m \geqslant 1$.

Предложение 15. *В принятых выше обозначениях пусть $\mathfrak{U}(P)$ — множество всех открытых подгрупп в $k_\mathbf{A}^\times$, содержащих $k^\times$ и содержащих $r_v^\times$ для всех $v \notin P$. Тогда для всякой подгруппы $U \in \mathfrak{U}(P)$ формула $U \cap G_P = l_P^{-1}(J)$ определяет конгруэнцподгруппу $J = J(U, P)$ в L_P; группа $g = \coprod g_v$, где g_v таковы, как в определении 1, является определяющей группой для J тогда и только тогда, когда она содержится в U; подгруппа U совпадает с замыканием подгруппы $k^\times l_P^{-1}(J)$ в $k_\mathbf{A}^\times$, и канонический гомоморфизм из $k_\mathbf{A}^\times$ на $k_\mathbf{A}^\times/U$ определяет изоморфизм группы L_P/J на $k_\mathbf{A}^\times/U$. Кроме того, отображение $U \to J(U, P)$ биективно отображает $\mathfrak{U}(P)$ на множество всех конгруэнцподгрупп в L_P.*

Возьмем $U \in \mathfrak{U}(P)$ и обозначим через ω канонический гомоморфизм группы $k_\mathbf{A}^\times$ на дискретную группу $\Gamma = k_\mathbf{A}^\times/U$. Поскольку морфизм группы G_P в Γ, индуцированный посредством ω, тривиален на на G'_P, его можно записать в виде $\varphi \circ l_P$, где φ — морфизм из L_P в Γ. Ясно, что ядро морфизма φ совпадает с J. По следствию предл. 17 гл. VII-8 отсюда следует, что J является конгруэнцподгруппой в L_P. Поэтому согласно предложению 17 гл. VII-8 ω является единственным продолжением морфизма $\varphi \circ l_P$ на $k_\mathbf{A}^\times$, тривиальным на $k^\times$, и морфизм ω тривиален на определяющей группе g для J, так что $g \subset U$. По предложению 15 гл. VII-8 группа $k^\times G_P$ плотна в $k_\mathbf{A}^\times$. Отсюда вытекает, что композиция $\varphi_0 l_P$ сюръективно отображает G_P на Γ, так что $\varphi(L_P) = \Gamma$, а также что подгруппа $U \cap (k^\times G_P)$ плотна в U; эта подгруппа совпадает с $k^\times \cdot (U \cap G_P)$, т. е. с $k^\times l_P^{-1}(J)$.

Обратно, пусть J — любая конгруэнцподгруппа в L_P и φ — канонический гомоморфизм группы L_P на дискретную группу $\Gamma = L_P/J$. Снова по предложению 17 гл. VII-8 отображение $\varphi \circ l_P$ можно однозначно продолжить до морфизма ω группы $k_{\mathbf{A}}^{\times}$ в Γ, тривиального на $k^{\times}$. Поэтому если U — ядро морфизма ω, то $U \in \mathfrak{U}(P)$ и $J = J(U, P)$. Наконец, если группы g_v таковы, как в определении 1, и $g = \prod g_v$, то каждый элемент ξ из $\bigcap (k^{\times} \cap g_v)$ содержится в $g \times G_P$, так что в случае $g \subset U$ проекция элемента ξ на G_P содержится в $U \cap G_P$ и образ этой проекции в L_P, который совпадает с $\mathrm{pr}(\xi)$, содержится в J. Таким образом, g является определяющей группой для J.

Следствие 1. *В обозначениях предложения* 15 *пусть P' — конечное множество точек поля k, содержащее P. Тогда если J — конгруэнцподгруппа в L_P, то $J' = J \cap L_{P'}$ — конгруэнцподгруппа в $L_{P'}$; если $J = J(U, P)$, где $U \in \mathfrak{U}(P)$, то $J' = J(U, P')$.*

Здесь имеется в виду, что $L_{P'}$ при $P' \supset P$ можно очевидным образом рассматривать как подгруппу в L_P. Ясно, что при этом $\mathfrak{U}(P) \subset \mathfrak{U}(P')$. Если теперь $U \in \mathfrak{U}(P)$ и $U \cap G_P = l_P^{-1}(J)$, то, очевидно, $U \cap G_{P'} = l_{P'}^{-1}(J')$, где $J' = J \cap L_{P'}$. Отсюда и из предложения 15 и вытекает наше следствие.

Следствие 2. *Пусть P, P' — два конечных множества точек поля k, содержащие P_∞, и пусть J, J' — конгруэнцподгруппы в L_P и в $L_{P'}$ соответственно. Тогда $k^{\times} l_P^{-1}(J)$ и $k^{\times} l_{P'}^{-1}(J')$ имеют одно и то же замыкание U в $k_{\mathbf{A}}^{\times}$ в том и только в том случае, когда существует такое конечное множество P'', содержащее P и P', что $J \cap L_{P''} = J' \cap L_{P''}$; в этом случае то же верно для всех конечных множеств P'', содержащих P и P', и U содержится в $\mathfrak{U}(P \cap P')$.*

Обозначим через U, U' замыкания двух наших множеств. По предложению 15 $J = J(U, P)$ и $J' = J(U', P')$. Если $U = U'$, то из предложения 15 сразу вытекает, что $U \in \mathfrak{U}(P \cup P')$. Поэтому в силу следствия 1, если $P'' \supset P \cup P'$, то группы $J \cap L_{P''}$ и $J' \cap L_{P''}$ совпадают обе с $J(U, P'')$. С другой стороны, если существуют такие P'', J'', что $P'' \supset P \cup P'$ и $J'' = J \cap L_{P''} = J' \cap L_{P''}$, то, согласно следствию 1, $J'' = J(U, P'') = J(U', P'')$, откуда $U = U'$ по предложению 15.

В случае когда две конгруэнцгруппы J, J' таковы, как в следствии 2, говорят, что они *эквивалентны*. Поскольку каждая открытая подгруппа U и $k_{\mathbf{A}}^{\times}$, содержащая $k^{\times}$, принадлежит $\mathfrak{U}(P)$ при подходящем выборе P, то ясно, что существует взаимно однозначное соответствие между множеством $\mathfrak{U}$ всех таких групп и множеством

классов эквивалентности конгруэнцгрупп. Поэтому взаимно однозначное соответствие между $\mathfrak{U}$ и $\mathfrak{N}$ (соотв. $\mathfrak{N} \cup \mathfrak{N}_0$), упомянутое выше в (b), определяет взаимно однозначное соответствие между $\mathfrak{N}$ (соотв. $\mathfrak{N} \cup \mathfrak{N}_0$) и классами эквивалентности конгруэнцгрупп. Опишем это соответствие более подробно.

Прежде всего в силу предложения 15 и его следствий очевидно, что для любого заданного класса конгруэнцгрупп найдется наименьшее множество P, такое, что в L_P содержится конгруэнцподгруппа J, принадлежащая этому классу. В самом деле, если U — открытая подгруппа в $k_{\mathbf{A}}^{\times}$, соответствующая этому классу, то P состоит из всех бесконечных точек и всех таких конечных точек v, для которых $r_v^{\times}$ не содержится в U. Если мы положим $U_v = U \cap k_v^{\times}$ при всех v, то последнее условие равносильно тому, что $r_v^{\times} \not\subset U_v$.

Аналогичным образом существует наибольшая определяющая группа для J; она равна $\prod\limits_{v \in P} g_v$, где $g_v = U_v$ для каждой бесконечной точки v и $g_v = U_v \cap r_v^{\times}$ для каждой конечной точки $v \in P$. Если рассматривать лишь такие определяющие группы, для которых группа g_v, в случае когда точка v конечна, имеет вид $1 + p_v^m$, где $m \geqslant 1$, то для всякой конечной точки $v \in P$ надо взять наименьшее целое число $m(v) \geqslant 1$, для которого $1 + p_v^{m(v)} \subset U_v$.

Если k — поле характеристики $p > 1$, то дивизор $\sum m(v) \cdot v$ называется *кондуктором* группы U и каждой конгруэнцгруппы, эквивалентной J. Если k — поле характеристики нуль, то полагаем $m(v) = 0$ или 1 для всякой вещественной точки v поля k в зависимости от того, совпадает U_v с $\mathbf{R}^{\times}$ или с $\mathbf{R}_+^{\times}$; для всех мнимых точек v поля k полагаем $m(v) = 0$. Сопоставим еще всякой бесконечной точке v поля k символ $\mathfrak{p}_v$, называемый *бесконечным простым*. Символ $\prod\limits_{v \in P} \mathfrak{p}_v^{m(v)}$ называют *кондуктором* группы U, группы J и конгруэнцгрупп, эквивалентных J.

Очевидно, что в случае характеристики $p > 1$ конгруэнцподгруппа J в L отвечает некоторой открытой подгруппе U в $k_{\mathbf{A}}^1$ в том и только в том случае, когда она состоит из дивизоров степени 0, причем L_P отождествляется с группой $D(P)$ дивизоров, взаимно простых с P. Начиная с этого места, мы исключаем этот случай. Другими словами, в случае когда характеристика поля k не равна нулю, мы рассматриваем лишь открытые подгруппы конечного индекса в $k_{\mathbf{A}}^{\times}$, абелевы расширения конечной степени поля k и конгруэнцгруппы, которые содержат по крайней мере один дивизор степени $\neq 0$. Договорившись об этом, мы можем применить предложение 14 § 10 и его следствия. В частности, если k' — абелево рас-

ширение поля k, соответствующее открытой подгруппе U в $k_{\mathbf{A}}^{\times}$, то следствие 4 указанного предложения показывает, что U содержит $r_v^{\times}$ в том и только в том случае, когда поле k'_w неразветвлено над k_v для всех точек w, лежащих над v, т. е. в том и только в том случае, когда v не входит в дискриминант $\mathfrak{D}$ поля k' над k.

Будем обозначать через Δ множество, состоящее из всех бесконечных точек поля k и всех точек, входящих в дискриминант $\mathfrak{D}$. Тогда конгруэнцподгруппа J в L_P, соответствующая U, существует в том и только в том случае, когда $P \supset \Delta$. Что касается кондуктора для U, то, если оставить в стороне бесконечные точки, он в очевидном смысле равен $\sup_{\omega \in \gamma} (\mathfrak{f}(\omega))$ в обозначениях теоремы 9 § 10. Что до бесконечных точек, то доказательство следствия теор. 10 § 10 показывает, что такая точка в том и только в том случае входит в кондуктор, когда она вещественна, а все лежащие над ней точки поля k' мнимы.

Прежде чем обсуждать связь между конгруэнцгруппами, ассоциированными с U, и автоморфизмами Фробениуса, введем некоторые определения, имеющие смысл для произвольного расширения Галуа k' конечной степени над k. Обозначим через $\mathfrak{g}$ группу Галуа поля k' над k, и пусть v — любая точка поля k, а w — точка поля k', лежащая над v. По следствию 4 теор. 4 гл. III-4 группу Галуа $\mathfrak{h}$ поля k'_w над k_v можно отождествить с некоторой подгруппой в $\mathfrak{g}$ с помощью морфизма ограничения из $\mathfrak{h}$ в $\mathfrak{g}$. Если v — конечная точка и поле k'_w неразветвлено над k_v, то группа $\mathfrak{h}$ циклична и порождена автоморфизмом Фробениуса φ_w поля k'_w над k_v; после отождествления группы $\mathfrak{h}$ с ее образом в $\mathfrak{g}$ можно рассматривать φ_w как элемент группы $\mathfrak{g}$; этот элемент называется *автоморфизмом Фробениуса поля k' над k в точке w*. Пусть w' — другая точка поля k' над v. То же самое следствие показывает, что существует k_v-линейный изоморфизм поля k'_w на $k'_{w'}$, определяемый некоторым автоморфизмом σ поля k' над k. Тогда автоморфизм Фробениуса поля k' над k в точке w' равен $\sigma^{-1}\varphi_w\sigma$. Ясно, что автоморфизм φ_w тождествен в том и только в том случае, когда точка v вполне расщепима в k'.

Пусть, в частности, k, k' — поля алгебраических чисел, $\mathfrak{r}$, $\mathfrak{r}'$ — их максимальные порядки, $\mathfrak{p}_v$, $\mathfrak{p}'_w$ — простые идеалы в $\mathfrak{r}$ и $\mathfrak{r}'$, отвечающие соответственно точкам v и w. Тогда $\mathfrak{r}/\mathfrak{p}_v$, $\mathfrak{r}'/\mathfrak{p}'_w$ суть конечные поля из $q = q_v$ и $q' = q'_w$ элементов соответственно и φ_w есть автоморфизм поля k' над k, который определяет на $\mathfrak{r}'/\mathfrak{p}'_w$ автоморфизм $x \longrightarrow x^q$. Этот автоморфизм можно определить так же, как такой автоморфизм φ поля k' над k, что $\xi^{\varphi} \equiv \xi^q (\mathfrak{p}'_w)$ для каждого $\xi \in \mathfrak{r}'_w$.

Предположим, в дополнение к сделанным выше предположениям, что поле k' абелево над k, т. е. что группа $\mathfrak{g}$ коммутативна. Тог-

да автоморфизм φ_w один и тот же для всех точек w, лежащих над v. В таком случае единственный этот автоморфизм φ_w называется *автоморфизмом Фробениуса поля k' над k в точке v*. Будем обозначать его через $(k'/k|\, v)$ или, если нет опасности перепутать, через $(k' \mid v)$. Тогда мы можем следующим образом проинтерпретировать следствие 3 предл. 14 § 10.

Как и в этом следствии, обозначим через U открытую подгруппу в $k_\Lambda^\times$, связанную с k', и отождествим группу Галуа $\mathfrak{g}$ поля k' над k с $k_\Lambda^\times/U$ при помощи канонического морфизма. Возьмем $P \supset \Delta$, где Δ было определено выше. Канонический гомоморфизм группы $k_\Lambda^\times$ на группу $\mathfrak{g} = k_\Lambda^\times/U$ тривиален на $r_v^\times$ для каждой точки $v \notin \Delta$, так что он индуцирует на G_P морфизм этой группы в группу $\mathfrak{g}$, тривиальный на G'_P; последний морфизм определяет морфизм φ группы $L_P = G_P/G'_P$ в $\mathfrak{g}$. Следствие 3 предл. 14 § 10 утверждает теперь, что $\varphi(v)$ для каждой точки $v \notin P$ совпадает с автоморфизмом Фробениуса $\varphi_v = (k' \mid v)$ поля k' над k в точке v, определенным выше. Этот морфизм φ группы L_P в $\mathfrak{g}$, определенный при $P \supset \Delta$, будем записывать так: $\mathfrak{m} \to (k'/k|\, \mathfrak{m})$. Будем писать $(k' \mid \mathfrak{m})$ вместо $(k'/k \mid \mathfrak{m})$, если нет опасности путаницы; этот символ называется *символом Артина*. Его можно охарактеризовать как морфизм группы L_P (или, что равносильно, группы идеалов $I(P)$, или группы дивизоров $D(P)$, в зависимости от того, какова характеристика) в группу $\mathfrak{g}$, который переводит каждую точку $v \notin P$ в автоморфизм Фробениуса поля k' над k в этой точке. Ввиду предложения 15 этот морфизм сюръективен и его ядро $J = J(U, P)$ является конгруэнцподгруппой в L_P. Когда в качестве P берутся всевозможные конечные множества точек, содержащие Δ, ядра $J(U, P)$ образуют класс эквивалентных конгруэнцгрупп; все эти группы содержатся в группе $J(k') = J(U, \Delta)$.

Из изложенных выше результатов вытекает также, что конечная точка v поля k вполне расщепима в k' в том и только в том случае, когда она содержится в $J(k')$. Поэтому предложение 15 гл. VIII-5 показывает, что если k'' — сепарабельное расширение поля k, содержащееся в $\bar{k}$, и если почти все точки поля k, содержащиеся в $J(k')$, вполне расщепимы в k'', то k'' содержится в k'. Отсюда, очевидно, следует, что существует бесконечно много точек поля k, содержащихся в $J(k')$. Как мы увидим в § 12, то же самое верно для всех классов смежности в L_Δ по $J(k')$. Следствие предл. 15 гл. VIII-5 показывает также, что если k'' — расширение Галуа поля k, то оно содержит k' в том и только в том случае, когда почти все точки поля k, вполне расщепимые в k'', лежат в $J(k')$. Отсюда следует, что если k' и k'' — два абелева расширения поля k, содержащиеся в $\bar{k}$, то $k'' \supset k'$ в том и только в том случае, когда существует такое P, что $J(k'') \cap$

$\bigcap L_P \subset J(k') \bigcap L_P$. Этот факт вытекает также из результатов § 9 в сочетании с предложением 15 этого параграфа. В частности, поле k' однозначно определяется классом эквивалентности конгруэнцгрупп, определенным по $J(k')$; это тоже немедленно вытекает из результатов § 9 и предложения 15 этого параграфа. Принято говорить, что k' — «поле классов», для класса эквивалентности конгруэнцгрупп или для любой группы из такого класса.

Данная выше характеризация класса конгруэнцгрупп, для которого k' является полем классов, основана исключительно на символе Артина; можно дать и другую характеризацию, используя тот факт, что $U = k^{\times} N_{k'/k}(k'^{\times}_{\mathrm{A}})$. Более общо, если взять в качестве k' любое расширение конечной степени над k, то теорема 7 § 9 и ее следствия показывают, что группа $U = k^{\times} N_{k'/k}(k'^{\times}_{\mathrm{A}})$ является открытой подгруппой конечного индекса в $k^{\times}_{\mathrm{A}}$, ассоциированной с максимальным абелевым расширением L поля k, содержащимся в k'. Возьмем любое конечное множество P точек поля k, содержащее P_{∞}, и для всякой точки $v \in P$ возьмем открытую подгруппу g_v в $k_v^{\times}$, содержащуюся в $r_v^{\times}$ в случае конечной точки v. Положим $\mathfrak{g} = \prod_{v \in P} g_v$, $U_{\mathfrak{g}} = k^{\times} \mathfrak{g} G'_P$ и $J_{\mathfrak{g}} = J(U_{\mathfrak{g}}, P)$. Тогда в обозначениях определения 1 $J_{\mathfrak{g}}$ является подгруппой в L_P, состоящей из элементов вида $\mathrm{pr}(\xi)$, где $\xi \in \bigcap (k^{\times} \bigcap g_v)$. Поскольку группа $U_{\mathfrak{g}} U$ содержит G'_P, она определяет конгруэнцгруппу $J = J(U_{\mathfrak{g}} U, P)$, задаваемую равенством $l_P^{-1}(J) = U_{\mathfrak{g}} U \bigcap G_P$. Обозначим через H_P группу тех иделей (z'_w) поля k', для которых $z'_w = 1$ для каждой точки w поля k', лежащей над некоторой точкой $v \in P$, и через H'_P — группу тех иделей (z'_w) поля k', для которых $z'_w = 1$, в случае, когда w лежит над некоторой точкой $v \in P$, и $|z'_w|_w = 1$ в противном случае. Тогда $L'_P = H_P / H'_P$ есть свободная группа, порожденная точками поля k', не лежащими над точками из P. Поскольку $\mathrm{N}_{k'/k}$ отображает H_P в G_P и H'_P в G'_P, то $\mathrm{N}_{k'/k}$ определяет морфизм $\mathfrak{N}$ группы L'_P в L_P, который совпадает с морфизмом $\mathfrak{N}_{k'/k}$ (соотв. $\mathfrak{S}_{k'/k}$) гл. VIII-4, если L'_P, L_P интерпретировать как группы идеалов (соотв. дивизоров) полей k' и k. По предложению 15 гл. VII-8 подгруппа $k'^{\times} H_P$ плотна в $k'^{\times}_{\mathrm{A}}$, так что подгруппа $k^{\times} \mathrm{N}_{k'/k}(H_P)$ плотна в U. Поскольку группа $U_{\mathfrak{g}}$ открыта в $k^{\times}_{\mathrm{A}}$, откуда следует, что

$$U_{\mathfrak{g}} U = k^{\times} \mathfrak{g} G'_P \cdot N_{k'/k}(H_P).$$

Отсюда немедленно вытекает, что J есть подгруппа в L_P, порожденная подгруппами $J_{\mathfrak{g}}$ и $\mathfrak{N}(L'_P)$. Обозначим через k'' поле классов для конгруэнцгруппы J; это — абелево расширение поля k, ассоциированное с открытой подгруппой $U_{\mathfrak{g}} U$ в $k^{\times}_{\mathrm{A}}$, так что оно содержится в абелевом расширении L поля k, ассоциированном с U. Пусть n,

n_0 — степени полей k' и L соответственно над k. Ясно, что индекс подгруппы J в L_P, который равен индексу подгруппы $U_g U$ в $k_{\mathbf{A}}^{\times}$ и степени поля k'' над k, не превосходит n_0 и что он равен n_0 в том и только в том случае, когда $U_g \subset U$, откуда $k'' = L$; это будет иметь место, если множество P взять достаточно большим, а группу g достаточно малой. В то же самое время мы видим, что индекс подгруппы J в L_P всегда $\leqslant n$ и что он равен n в том и только в том случае, когда поле k' абелево над k и является полем классов для J. Другими словами, для заданной конгруэнцподгруппы J в L_P расширение k' конечной степени над k абелево и является полем классов для J в том и только в том случае, когда группа J содержит $\mathfrak{N}(L'_P)$ и ее индекс в L_P равен степени поля k' над k.

Наконец, мы можем дать такую интерпретацию следствия 5 теор. 7 § 9. Как и прежде, пусть k' — расширение конечной степени поля k и M — абелево расширение поля k, содержащееся в некотором расширении поля k'. Обозначим через M' композит полей M и k' и предположим, что M — поле классов для конгруэнцподгруппы J в L_P. Пусть v — точка поля k, w — точка поля k', лежащая над v, u' — точка поля M', лежащая над w, и u — точка поля M, лежащая под u'. Поле $M'_{u'}$ является композитом полей k'_u и M', а значит, полей k'_w и M и тем самым полей k'_w и M_u. Если $v \notin P$, то поле M_u неразветвлено над k_v. Отсюда следует, что в этом случае поле $M'_{u'}$ неразветвлено над k'_w. Поэтому M' является полем классов для некоторой конгруэнцподгруппы J' в L'_P.

Пусть теперь U, U' — открытые подгруппы в $k_{\mathbf{A}}^{\times}$ и в $k_{\mathbf{A}}^{\prime\times}$ соответственно, ассоциированные с M и с M'; по следствию 5 теор. 7 §9 $U' = N_{k'}^{-1}{}_{/k}(U)$. По предложению 15 J и J' можно определить соответственно формулой $l_{\mathfrak{P}}^{-1}(J) = U \cap G^P$ и аналогичной формулой для J', U'. Поэтому элемент $\mathfrak{m}'$ из L'_P содержится в J' в том и только в том случае, когда он является образом элемента $z' \in H_P$, такого, что $z' \in U'$, т. е. $\mathrm{N}_{k'/k}(z') \in U$. Поскольку $\mathrm{N}_{k'/k}$ отображает H_P в G_P, последнее условие эквивалентно тому, что $\mathrm{N}_{k'/k}(z') \in U \cap G_P$, откуда $\mathfrak{N}(\mathfrak{m}') \in J$. Поэтому $J' = \mathfrak{N}^{-1}(J)$.

Для иллюстрации применим сказанное выше к случаю $k = \mathbf{Q}$, который был изучен в § 4 с другой точки зрения. Возьмем поле $k' = \mathbf{Q}(\varepsilon)$, где ε — примитивный корень m-й степени из 1. Как и прежде, отождествим группу Галуа g этого поля с $(\mathbf{Z}/m\mathbf{Z})^{\times}$, сопоставляя каждому автоморфизму $\varepsilon \to \varepsilon^x$ с $x \in \mathbf{Z}$, $(x, m) = 1$, образ числа x в $(\mathbf{Z}/m\mathbf{Z})^{\times}$. Как отмечалось выше, для каждого простого числа p, не делящего m, и для каждой точки w поля k', лежащей над p, поле k'_w, очевидно, неразветвлено над $\mathbf{Q}_p$ и автоморфизм Фробениуса поля k' над $\mathbf{Q}$ в точке p — это отображение $\varepsilon \to \varepsilon^p$ (точка p отождествляется со своим образом в $(\mathbf{Z}/m\mathbf{Z})^{\times}$). Следовательно, в дискрими-

нанте поля k' над $\mathbf{Q}$ могут встречаться лишь простые числа, делящие m, и k' является полем классов для некоторой конгруэнцподгруппы J в группе L_m дробных идеалов поля $\mathbf{Q}$, взаимно простых с m; группу L_m можно очевидным образом отождествить с группой дробей вида $r = a/b$, где a, b — целые строго положительные числа, взаимно простые с m.

Далее, символ Артина $r \to (k'/\mathbf{Q} \mid r)$ является морфизмом группы L_m в $(\mathbf{Z}/m\mathbf{Z})^\times$, переводящим каждое простое число p, не делящее m, в его образ в $(\mathbf{Z}/m\mathbf{Z})^\times$. Ясно, что этот морфизм переводит каждое целое число $a > 0$, взаимно простое с m, в его образ в $(\mathbf{Z}/m\mathbf{Z})^\times$, и ядро J этого морфизма состоит из элементов вида a/b в L_m, для которых $a \equiv b$ по модулю m.

Легко проверяется, что *кондуктор* для группы J равен 1, если $m = 1$ или 2; равен $\mathfrak{p}_\infty (m/2)$, если m четно, а $m/2$ нечетно, и равен $\mathfrak{p}_\infty m$ во всех других случаях. Исключая тривиальные случаи $m = 1$ и 2, когда $k' = \mathbf{Q}$, это можно сказать еще следующим образом: кондуктор равен $\mathfrak{p}_\infty m'$, где m' — наименьшее целое число, такое, что поле $\mathbf{Q}(\varepsilon)$ порождено над $\mathbf{Q}$ примитивным корнем m'-й степени из 1. Как мы видели, отсюда следует, что простые числа, встречающиеся в дискриминанте поля $\mathbf{Q}(\varepsilon)$ над $\mathbf{Q}$,— это простые делители числа m'. С помощью теоремы 9 § 10 нетрудно было бы теперь вычислить и сам дискриминант.

Из сказанного выше вытекает также, что если k' — любое поле алгебраических чисел и ε, как и выше,— примитивный корень m-й степени из 1, то $k(\varepsilon)$ является полем классов для конгруэнцподгруппы J' в группе L'_m дробных идеалов поля k, взаимно простых с m, состоящей из тех дробных идеалов $\mathfrak{m}$, для которых $\mathfrak{N}(\mathfrak{m}) \in J$, где группа J такая же, как выше.

§ 12. «CORONIDIS LOCO»[1])

Результаты § 10 позволяют ответить на вопрос, который не мог быть разрешен в гл. VII-5.

Т е о р е м а 11. *Пусть* ω — *произвольный нетривиальный характер на* $k_{\mathrm{A}}^\times$, *тривиальный на* $k^\times$. *Тогда* $L(1, \omega) \neq 0$.

За исключением случая $\omega^2 = 1$, это утверждение вытекает из следствия 2 теор. 2 гл. VII-5. Предположим поэтому, что характер ω имеет порядок 2. Обозначим через U его ядро, которое является открытой подгруппой в $k_{\mathrm{A}}^\times$ индекса 2, содержащей $k^\times$. По следствию 2 теор. 7 § 9 существует квадратичное расширение k' поля k, ассоциированное с U. По теореме 10 § 10 имеем

$$\zeta_{k'}(s) = \zeta_k(s)\, L(s, \omega).$$

[1]) Вместо заключения (*лат.*). —*Прим. ред.*

Если характеристика поля k равна нулю, то по следствию теор. 1 гл. VII-6 обе функции ζ_k и $\zeta_{k'}$ имеют простой полюс в точке $s = 3$ и их вычеты в этой точке, значения которых приведены в этом следствии, положительны. То же по теореме 4 гл. VII-6 верно и в случае, когда k — поле характеристики $p > 1$. Поэтому $L(1, \omega) > 0$.

Следует заметить, что данное выше доказательство можно очевидным образом приспособить для любого нетривиального характера ω конечного порядка на $k_\Lambda^\times$, тривиального на $k^\times$, применяя теорему 10 § 10 к циклическому расширению k' поля k, ассоциированному с ядром U характера ω. В той мере, в которой это касается заключения теоремы 11, это не добавляет ничего нового к уже доказанному другими методами в следствии 2 теор. 2 гл. VII-5, зато дает некоторые важные соотношения между числами классов полей k и k', с одной стороны, и значениями соответствующих L-функций в точке $s = 1$ — с другой. Вообще, как сразу видно из теоремы 10 § 10, подобные соотношения имеются для всех абелевых расширений конечной степени над k. Следует также отметить, что, заменяя в теореме 11 ω на $\omega_{it}\omega$, где ω_s, $s \in \mathbf{C}$, — характер, определенный в гл. VII, мы сразу получаем, что $L(1 + it, \omega) \neq 0$ при $t \in \mathbf{R}$.

Следствие. *Пусть k_0 — некоторое* **A**-*поле, содержащееся в k, и пусть V — такое множество конечных точек поля k, что почти для всех конечных точек v поля k, не лежащих в V, замыкание поля k_0 в k_v не совпадает с k_v. Пусть ω — нетривиальный характер на $k_\Lambda^\times$, тривиальный на $k^\times$, причем характер ω_v неразветвлен над всеми точками $v \in V$. Тогда произведение*

$$q(k, V, \omega, s) = \prod_{v \notin V} (1 - \omega_v(\pi_v)\, q_v^{-s})^{-1}$$

абсолютно сходится при $\mathrm{Re}(s) > 1$ *и стремится к отличному от нуля конечному пределу при* $s \to 1$.

По теореме 1 гл. VIII-4 почти для всех v поле k_v неразветвлено над замыканием $(k_0)_u$ поля k_0 в k_v, так что его модулярная степень над $(k_0)_u$ равна его степени над тем же полем. Ввиду этого сделанное выше предположение относительно V равносильно предположению из следствия 3 теор. 2 гл. VII-5. Применяя те же рассуждения, что и при доказательстве этого следствия, убеждаемся, что наше утверждение немедленно вытекает из теоремы 11 в сочетании со следствием 3 предл. 1 гл. VII-1.

Теорема 12. *Пусть L — некоторое* **A**-*поле, k_0 — некоторое* **A**-*поле, содержащееся в L, и α — автоморфизм поля L над k_0. Тогда существует бесконечно много точек w поля L, для которых поле L_w*

неразветвлено над замыканием поля k_0 в L_w и автоморфизм Фробениуса поля L_w над этим замыканием индуцирует α на L.

Обозначим через k подполе в L, состоящее из элементов, неподвижных относительно α. Поскольку $k_0 \subset k \subset L$, поле L имеет конечную степень d над k. Поэтому из теории Галуа следует, что поле L циклично над k, причем его группа Галуа $\mathfrak{g}$ порождена элементом α. Для всякой точки v поля k обозначим через u точку поля k_0, лежащую под v. Пусть w — любая точка поля L, лежащая над v. Тогда замыкание поля k_0 в L_w совпадает с $(k_0)_u$. По теореме 1 гл. VII-4 существует такое содержащее P_∞ конечное множество P точек поля k, что при $v \notin P$ поле k_v неразветвлено над $(k_0)_u$ и поле L_w неразветвлено над k_v, а значит и над $(k_0)_u$.

Обозначим через φ автоморфизм Фробениуса поля L_w над $(k_0)_u$. Так как этот автоморфизм порождает группу Галуа поля L_w над $(k_0)_u$, он не оставляет неподвижными никаких элементов поля L_w, за исключением элементов из $(k_0)_u$. Поэтому если он индуцирует α на L, то обязательно $k \subset (k_0)_u$, откуда $k_v = (k_0)_u$, а тогда в силу определений § 11 α является автоморфизмом Фробениуса поля L над k в точке v.

Обозначим через M_0 множество тех точек v поля k, не лежащих в P, для которых $k_v \neq (k_0)_u$. Далее, для каждой точки v поля k, не лежащей в $P \cup M_0$, обозначим через φ_v автоморфизм Фробениуса поля L над k в точке v. Наконец, обозначим через M_1 множество тех точек v поля k, не лежащих в $P \cup M_0$, для которых $\varphi_v = \alpha$, и через V — дополнение множества $P \cup M_0 \cup M_1$ в множестве всех точек поля k. Ясно, что утверждение нашей теоремы сводится к тому, что множество M_1 не является конечным и что конечно оно в том и только в том случае, когда V обладает свойствами, описанными в следствии теор. 11. Предположив, что V обладает этими свойствами, мы придем сейчас к противоречию.

Как обычно, пусть χ — характер на $\mathfrak{A}$, связанный с циклическим расширением L поля k; здесь, разумеется, $\mathfrak{A}$ — группа Галуа поля k_{ab} над k и L рассматривается как подполе в k_{ab}. Пусть $\mathfrak{B}$ — подгруппа в $\mathfrak{A}$, соответствующая полю L. Тогда $\mathfrak{g} = \mathfrak{A}/\mathfrak{B}$ и группа характеров на $\mathfrak{g}$ состоит из характеров χ^i, $0 \leqslant i < d$. Положим $\omega = \chi \circ \alpha$. По следствию 3 предл. 14 § 10 характер ω_v неразветвлен в том и только в том случае, когда поле L_w неразветвлено над k_v, а тогда автоморфизм Фробениуса φ_v поля L над k в точке v совпадает с образом в $\mathfrak{g}$ элемента π_v относительно морфизма из $k_{\mathbf{A}}^{\times}$ в $\mathfrak{g}$, определенного с помощью α. Это дает, в обозначениях следствия теор. 11,

$$q(k, V, \omega^i, s) = \prod_{v \in V} (1 - \chi^i(\varphi_v)\, q_v^{-s})^{-1}.$$

Для краткости обозначим это выражение через $q_i(s)$. Имеем

$$\log q_i(s) = \sum_{v \in V} \sum_{n=1}^{+\infty} \chi^i(\varphi_v)^n q_v^{-ns}/n.$$

Этот ряд абсолютно сходится при $\mathrm{Re}(s) > 1$, и

$$\sum_{i=0}^{d-1} \chi^i(\alpha^{-1}) \log q_i(s) = \sum_{v \in V} \left(\sum_{i=0}^{d-1} \chi^i(\alpha^{-1}\varphi_v) \right) q_v^{-s} + \\ + \sum_{v \in V} \sum_{n=2}^{+\infty} \sum_{i=0}^{d-1} \chi^i(\alpha^{-1}\varphi_v^n)\, q_v^{-ns}/n.$$

В правой части все коэффициенты первого ряда равны нулю, потому что $\varphi_v \neq \alpha$ при $v \notin V$. Далее, $q_v \geqslant 2$ при всех v, так что для всякой точки v при $\mathrm{Re}(s) > 1$ имеем

$$\sum_{n=2}^{+\infty} |q_v^{-ns}|/n \leqslant \frac{1}{2} \sum_{n=2}^{+\infty} q_v^{-n} \leqslant q_v^{-2}.$$

Поэтому второй ряд в правой части предыдущей формулы мажорируется рядом $d \sum\limits_v q_v^{-2}$, который сходится по предложению 1 гл. VII-1. Таким образом, показано, что левая часть ограничена при $\mathrm{Re}(s) > 1$. С другой стороны, следствие теоремы 11 показывает, что функция $\log q_i(s)$ при $1 \leqslant i < d$ ограничена при s, стремящемся к 1, а следствие 2 теор. 2 гл. VII-5 показывает, что для функции $\log q_0(s)$ это не имеет места. Мы получили противоречие.

Следствие. *В обозначениях определения* 1 § 11 *пусть* J — *конгруэнцподгруппа в* L_P; *в случае когда* k — *поле характеристики* $p > 1$, *предположим, что* J *содержит дивизор степени* $\neq 0$. *Тогда в каждом классе смежности в* L_P *по* J *имеется бесконечно много точек поля* k.

В самом деле, пусть k' — поле классов для J в смысле § 11. Обозначим через $\mathfrak{g}$ его группу Галуа над k. Как было показано в § 11, точки v поля k в заданном классе смежности в L_P по J — это не лежащие в P точки с заданным автоморфизмом Фробениуса поля k' над k. Наше утверждение является поэтому частным случаем теоремы 12.

В качестве иллюстрации к теореме 12 возьмем $k_0 = \mathbf{Q}$ и рассмотрим в качестве L поле, порожденное примитивным корнем m-й степени из 1. Тогда наша теорема утверждает, что если a — любое целое число, взаимно простое с m, то существует бесконечно много простых чисел, сравнимых с a по модулю m. Это — *теорема об арифметических прогрессиях* Дирихле, а приведенное выше дока-

зательство теоремы 12 является непосредственным обобщением первоначального доказательства Дирихле.

В заключение пусть ω, k и k' снова таковы, как при доказательстве теоремы 11, так что

$$\zeta_{k'}(s) = \zeta_k(s)\, L(s, \omega).$$

Если характеристика поля k равна нулю, то по следствию теор. 10 § 10 имеем также

$$Z_{k'}(s) = \pi^{\rho} Z_k(s)\, \Lambda(s, \omega),$$

где ρ таково, как указано в этом следствии. Запишем теперь, что функции в этих формулах удовлетворяют функциональным уравнениям из теорем 3 и 4 гл. VII-6 и теорем 5 и 6 гл. VII-7. Тот факт, что экспоненциальные сомножители в функциональных уравнениях должны совпадать для обеих частей, не дает ничего нового: получаемые при этом соотношения немедленно следуют из теоремы 8 § 9. Приравнивая постоянные сомножители в обеих частях, получаем соотношение $\varkappa\omega(b) = 1$, где $\varkappa$ и b определены в теоремах 5 и 6 гл. VII—7.

Применим это к одному частному случаю. Предположим, что в качестве ω взят характер порядка 2 на $k_{\mathbf{A}}^{\times}$, тривиальный на $k^{\times}\Omega(P_{\infty})$, или, что то же самое, тривиальный на $k^{\times}$, тривиальный на $k_v^{\times}$ для любой бесконечной точки v и тривиальный на $r_0^{\times}$ для любой конечной точки v. Согласно предложению 14 гл. VII-7, имеем $\varkappa_v = 1$ при всех v, откуда $\varkappa = 1$ и идель b совпадает с дифферентным иделем a. Поэтому для каждого такого характера ω имеем $\omega(a) = 1$. Здесь, если k — поле алгебраических чисел, можно считать, что a выбрано так, как в предложении 12 гл. VIII-4, т. е. так, что $\mathrm{id}(a)$ является дифферентой $\mathfrak{d}$ поля k над $\mathbf{Q}$; если k — поле характеристики $p > 1$, то, как мы знаем (см. определение дифферентного иделя в гл. VII-2), $c = \mathrm{div}(a)$ есть дивизор из канонического класса. С другой стороны, условия, наложенные на ω, означают в точности то, что он тривиален на группе $k^{\times}(k_{\mathbf{A}}^{\times})^2\Omega(P_{\infty})$. Поэтому a содержится в последней группе. Поскольку группу $k_{\mathbf{A}}^{\times}/k^{\times}\Omega(P_{\infty})$ можно отождествить с группой $I(k)/P(k)$ классов идеалов поля k, если k — поле алгебраических чисел, и с группой $D(k)/P(k)$ классов дивизоров поля k, если k — поле характеристики $p > 1$, то тем самым доказана следующая теорема (для случая поля алгебраических чисел принадлежащая Гекке).

Теорема 13. *Если k — поле алгебраических чисел, то существует класс идеалов поля k, квадрат которого равен классу, определяемому дифферентой поля k над $\mathbf{Q}$. Если k—поле характеристики $p > 1$, то существует класс дивизоров поля k, квадрат которого равен каноническому классу поля k.*

ПРИЛОЖЕНИЯ К РУССКОМУ ИЗДАНИЮ

ПРИЛОЖЕНИЕ I (К ГЛ. XII-5 И XIII-9)

Мы изложим здесь вкратце другое, независимое доказательство «теорем переноса» теории полей классов. Легко видеть, что в обозначениях гл. XII-2 и XII-5 локальная «теорема переноса» (т. е. теорема 6 гл. XII-5) эквивалентна следующему утверждению: *для всех* $\chi' \in X_{K'}$ *и всех* $\theta \in K^\times$ *выполняется равенство* $(\chi' \circ t, \theta)_K = (\chi', \theta)_{K'}$. Как в гл. IX-3, выберем сначала произвольное поле K и его расширение K' конечной степени n, содержащееся в K_{sep}. Группы Галуа поля K_{sep} над полями K и K' обозначим соответственно через $\mathfrak{G}$ и $\mathfrak{G}'$. Выберем, так же как в гл. XII-5, полное множество представителей $\{\sigma_1, \ldots, \sigma_n\}$ правых классов $\sigma\mathfrak{G}'$ смежности подгруппы $\mathfrak{G}'$ в $\mathfrak{G}$ и обозначим буквой t гомоморфизм переноса из $\mathfrak{G}/\mathfrak{G}^{(1)}$ в $\mathfrak{G}'/\mathfrak{G}'^{(1)}$. Пусть f' — произвольное множество факторов в K'. Для любых ρ, σ, τ из $\mathfrak{G}$ и всех $1 \leqslant i \leqslant n$ $\rho\sigma_i$, $\sigma\sigma_i$, $\tau\sigma_i$ можно записать единственным образом в виде

$$\rho\sigma_i = \sigma_j\alpha_i, \qquad \sigma\sigma_i = \sigma_k\beta_i, \qquad \tau\sigma_i = \sigma_e\gamma_i, \tag{1}$$

где $1 \leqslant j, k, l \leqslant n$, а $\alpha_i, \beta_i, \gamma_i$ принадлежат $\mathfrak{G}'$. Формула

$$(\rho, \sigma, \tau) \longrightarrow f(\rho, \sigma, \tau) = \prod_{1 \leqslant i \leqslant n} f'(\alpha_i, \beta_i, \gamma_i)^{\sigma_i^{-1}}$$

определяет тогда множество f факторов поля K. Будем писать $f = \nu(f')$. Если z' — ковариантное отображение группы $\mathfrak{G}' \times \mathfrak{G}'$ в $K_{\text{sep}}^\times$, то аналогичным образом определяется ковариантное отображение $z = \nu(z')$ из $\mathfrak{G} \times \mathfrak{G}$ в $K_{\text{sep}}^\times$; и если f' — когранича отображения z', то $\nu(f')$ является кограничей отображения $\nu(z')$. Таким образом, ν переводит когранича в когранича и определяет морфизм, обозначаемый также через ν, классов факторов поля K' в классы факторов поля K. Морфизм ν, рассматриваемый на множестве факторов, зависит от выбора представителей $\sigma_1, \ldots, \sigma_n$, соответствующее отображение классов факторов от этого выбора

уже не зависит; поскольку в дальнейшем этот факт не будет использоваться, мы предоставляем его проверку читателю.

Далее используются обозначения гл. IX-4 и XII-1.

Лемма A. *Для всех* $\chi' \in X_{K'}$ *и всех* $\theta \in K^\times$

$$\{\chi' \circ t,\ \theta\}_K = \nu\left(\{\chi',\ \theta\}_{K'}\right).$$

Как и в гл. IX-4, будем писать $\chi' = e \circ \Phi'$, где Φ' — отображение группы $\mathfrak{G}'$ в $\mathbf{R}$. Тогда обе части равенства из леммы A определены как классы некоторых множеств факторов поля K, и нужно только проверить, что эти множества отличаются на когранницу некоторого ковариантного отображения z из $\mathfrak{G} \times \mathfrak{G}$ в K_{sep}. Имеем $\chi' \circ t = \mathbf{e} \circ \Phi$, где мы положили $\Phi(\rho) = \Phi'\left(\coprod_i \alpha_i\right)$, $\rho \in \mathfrak{G}$, а α_i те же, что и в (1). Определим теперь α_i, β_i для всех ρ, σ из $\mathfrak{G}$ так же, как в (1), и положим

$$z(\rho,\ \sigma) = \theta^{\sum\limits_i \Phi'(\beta_i \alpha_i^{-1}) - \Phi'\left(\coprod\limits_i \beta_i \alpha_i^{-1}\right)}.$$

Это выражение имеет требуемые свойства; проверка тривиальна и предоставляется читателю.

Лемма B. *Для всех* $\chi \in X_K$ *и всех* $\theta' \in K'^\times$

$$\{\chi,\ N_{K'/K}\theta'\}_K = \nu\left(\{\chi \circ \rho,\ \theta'\}_{K'}\right).$$

Доказательство аналогично доказательству леммы A. Пишем $\chi = e \circ \Phi$; обе части доказываемого равенства будут тогда по определению классами множеств факторов, и непосредственно проверяется, что они отличаются на когранницу ковариантного отображения z, определяемого соотношением

$$z(\rho,\sigma) = \coprod_i \left(\theta^{\,{}^{i}\left(\sigma^{-1}\right)\ \Phi(\sigma\rho^{-1}) - \Phi(\sigma^{-1}\sigma\rho^{-1}\sigma_j) + \Phi(\sigma_j) + \Phi(\sigma_k)}_{k}\right).$$

Пусть теперь K — коммутативное p-поле. Для большей ясности будем обозначать через η_K символ η, введенный в гл. XII-2, и через $\eta_{K'}$ — аналогичный символ для поля K'. Пусть f' — множество факторов поля K'; положим $f = \nu(f')$ и обозначим через $\mathrm{Cl}\, f$, $\mathrm{Cl}\, f'$ классы множеств f и f'. В силу леммы A теорема о переносе будет

доказана, если мы покажем, что для каждого f' η_K (Cl f) = $= \eta_{K'}$ (Cl f'). В этом равенстве Cl f' можно записать в виде $\{\chi', \theta'\}$, где χ' — неразветвленный характер группы $\mathfrak{G}'$ и $\theta' \in K'^{\times}$. Характер χ' мы можем записать в виде $\chi' = \chi \circ \rho$, где χ — неразветвленный характер группы $\mathfrak{G}$. Если χ' соответствует циклическому расширению $L' = K'(\mu)$, где μ — корень из единицы порядка, взаимного простого с p, то в качестве χ можно взять подходящий характер, связанный с полем $K(\mu)$. Наше утверждение получается теперь немедленно, если сопоставить лемму B с теоремой 2 гл. XII-2.

Чтобы получить глобальную теорему (теорема 8 гл. XIII-9) из локальной, сделаем следующее замечание. В обозначениях гл. XIII-10, пусть k' — расширение конечной степени поля k, содержащееся в k_{sep}. Для каждой точки w поля k', лежащей над v, пусть $\mathfrak{A}'_w$ — группа Галуа поля $k'_{w,\text{ab}}$ над k'_w и ρ'_w — отображение ограничения группы $\mathfrak{A}'_w$ в группу Галуа $\mathfrak{A}'$ поля k'_{ab} над k'. Обозначим буквами t и t_w гомоморфизмы переноса соответственно групп $\mathfrak{A}$ в $\mathfrak{A}'$ и $\mathfrak{A}_v$ в $\mathfrak{A}_w$. Тогда $t \circ \rho_v = \prod_{w \mid v} (\rho'_w \circ t_w)$, где произведение берется по всем точкам w поля k', лежащим над v. Доказательство этого факта является легким (и чисто теоретико-групповым) и предоставляется в качестве упражнения читателю. Принимая это утверждение, получаем глобальную теорему о переносе как немедленное следствие локальной теоремы и определений.

ПРИЛОЖЕНИЕ II. *W*-ГРУППЫ ДЛЯ ЛОКАЛЬНЫХ ПОЛЕЙ

Чтобы сформулировать теорему Шафаревича (см. приложение III) и аналогичные результаты, удобно ввести видоизмененные группы Галуа (так называемые W-группы) [1]). Если K — коммутативное p-поле, то определим K_0 так же, как в гл. XII-2. Пусть $\mathfrak{K}$ — расширение Галуа поля K, содержащееся в K_{sep} и содержащее K_0, и пусть $\mathfrak{G}$, $\mathfrak{G}_0$ — группы Галуа поля $\mathfrak{K}$ соответственно над K и над K_0. Обозначим через φ автоморфизм поля K, индуцированный автоморфизмом Фробениуса поля K_{sep} над K. Положим

$$\mathfrak{W} = \bigcup_{\nu \in Z} \varphi^{\nu} \mathfrak{G}_0$$

и снабдим $\mathfrak{W}$ топологией, задаваемой полной системой окрестностей единицы в $\mathfrak{G}_0$. Тем самым $\mathfrak{W}$ превращается в квазикомпактную группу с максимальной компактной подгруппой $\mathfrak{G}_0$; при этом $\mathfrak{W}/\mathfrak{G}_0$ изоморфно Z. Группа $\mathfrak{W}$, снабженная этой топологией, называется *W-группой* поля $\mathfrak{K}$ над K. Существует очевидный

[1]) Именуемые обычно *группами Вейля.—Прим. перев.*

инъективный морфизм δ группы $\mathfrak{W}$ в $\mathfrak{G}$, отображающий ее на плотную подгруппу группы $\mathfrak{G}$. В применениях этой конструкции в качестве поля $\mathfrak{K}'$ берут обычно поле L_{ab}, где L — расширение Галуа конечной степени поля K. Если мы возьмем в частности $K = K_{ab}$, то из предложения 7 и следствия 2 теор. 3 гл. XII-3 сразу следует, что образ $\delta(\mathfrak{W}')$ W-группы поля K_{ab} в группе Галуа $\mathfrak{A}$ поля K_{ab} над K тот же самый, что и образ $\alpha(K^\times)$ группы $K^\times$ в группе $\mathfrak{A}$ относительно канонического изоморфизма α. В этом случае существует, следовательно, канонический изоморфизм $\mathfrak{w}$ группы $K^\times$ на $\mathfrak{w}$, такой, что $\alpha = \delta \circ \mathfrak{w}$.

Пусть K' — расширение конечной степени поля K; как всегда, предполагается, что K'_{sep} содержится в K'_{sep}. Пусть $\mathfrak{K}$, $\mathfrak{K}'$ — расширения Галуа соответственно полей K и K', такие, что $K_0 \subset \subset \mathfrak{K} \subset \mathfrak{K}' \subset K'_{sep}$, и пусть $\mathfrak{W}$, $\mathfrak{W}'$ суть W-группы поля $\mathfrak{K}$ над K и поля $\mathfrak{K}'$ над K' соответственно. Так же, как и для обычных групп Галуа, существует морфизм ограничения из $\mathfrak{W}'$ в $\mathfrak{W}$, обозначаемый снова через ρ. Так обстоит дело, например, в случае $\mathfrak{K} = K_{ab}$ и $\mathfrak{K}' = K'_{ab}$; в качестве немедленного следствия теоремы 2 гл. XII-2 (точно так же, как в следствии 1 этой теоремы) получаем, что $\rho \circ \mathfrak{w}' = \mathfrak{w} \circ N_{K'/K}$, где $\mathfrak{w}$, $\mathfrak{w}'$ — канонические изоморфизмы группы $K^\times$ на $\mathfrak{W}$ и группы $K'^\times$ на $\mathfrak{W}'$ соответственно.

С другой стороны, если $\mathfrak{K}$, $\mathfrak{K}'$ — два расширения Галуа поля K, $K_0 \subset \mathfrak{K} \subset \mathfrak{K}' \subset K_{sep}$ и $\mathfrak{W}$, $\mathfrak{W}'$ суть W-группы соответственно поля $\mathfrak{K}$ над K и поля $\mathfrak{K}'$ над K, то элементы группы $\mathfrak{W}$ суть ограничения элементов группы $\mathfrak{W}'$ на поле $\mathfrak{K}$ и мы можем отождествить $\mathfrak{W}$ с группой $\mathfrak{W}'/\Gamma$, где Γ — группа Галуа поля $\mathfrak{K}'$ над $\mathfrak{K}$. Возьмем в частности $\mathfrak{K} = K_{ab}$, $\mathfrak{K}' = K_{sep}$ и обозначим буквой Ω вместо $\mathfrak{W}'$ W-группу поля K_{sep} над K. Мы можем отождествить тогда $\mathfrak{W}$ с Ω/Γ, где Γ — группа Галуа поля K_{sep} над K_{ab} — есть не что иное, как замыкание $\Omega^{(1)}$ в Ω коммутанта группы Ω. Далее выберем (как в гл. XII-5) подполе K' поля K_{sep}, имеющее конечную степень n над K, и пусть Ω' есть W-группа поля K_{sep} над K'. Тогда Ω' будет открытой подгруппой индекса n в Ω, и W-группу $\mathfrak{W}'$ поля K'_{ab} над K можно отождествить с $\Omega'/\Omega'^{(1)}$. Это дает возможность, так же как в гл. XII-5, ввести гомоморфизм переноса t из $\mathfrak{W}$ в $\mathfrak{W}'$. Локальную теорему переноса (см. приложение I) можно поэтому выразить формулой $t \circ \mathfrak{w} = \mathfrak{w}' \circ j$, где j, как и в теореме 6 гл. XII-5,— естественное вложение группы $K^\times$ в $K'^\times$.

ПРИЛОЖЕНИЕ III. ТЕОРЕМА ШАФАРЕВИЧА

Эта теорема описывает структуру группы Галуа (или, точнее, W-группы, см. приложение II) поля L_{ab} над K, где K — коммутативное p-поле и L — его произвольное расширение Галуа конеч-

ной степени. Для формулировки и доказательства теоремы необходимы некоторые сведения о расширениях групп.

1. Примем предположения и обозначения гл. IX, так что K будет произвольным полем, $\mathfrak{G}$ — группой Галуа поля K_{sep} над K, а все алгебры над K такими, как указано в гл. IX-1. Пусть L — расширение Галуа поля K конечной степени n, содержащееся в K_{sep}; $\mathfrak{H}$ и $\mathfrak{g}$ — соответственно группы Галуа полей K_{sep} над L и L над K, так что мы можем отождествить $\mathfrak{g}$ с $\mathfrak{G}/\mathfrak{H}$. Если ρ — произвольный элемент из $\mathfrak{G}$, то его образ в $\mathfrak{g}$ будем обозначать $\bar{\rho}$.

Лемма А. *Пусть* φ — *морфизм группы* G *на* $\mathfrak{g}$, H — *его ядро*, ω — *морфизм из* H *в* $L^\times$, *и пусть для всех* $g \in G$ *и всех* $h \in H$

$$\omega(g^{-1}hg) = \omega(h)^{\varphi(g)}. \tag{1}$$

Тогда существует простая алгебра A размерности n^2 над K, содержащая L, такая, что ω распространяется до морфизма ω^* из G в $A^\times$, удовлетворяющего для всех $g \in G$ и $\xi \in L$ соотношению $\omega^*(g^{-1})\,\xi\omega^*(g) = \xi^{\varphi(g)}$. Кроме того эти условия определяют алгебру A и морфизм ω^* однозначно с точностью до изоморфизма, а $\omega^*(G)\cdot L^\times$ является нормализатором группы $L^\times$ в $A^\times$.

Выберем для каждого $\alpha \in \mathfrak{g}$ представителя g_α класса смежности $\varphi^{-1}(\{\alpha\})$ подгруппы H в G. Тогда для всех α, β из $\mathfrak{g}$ можно написать $g_\alpha g_\beta = g_{\alpha\beta} h(\alpha, \beta)$ с $h(\alpha, \beta) \in H$. Записывая $g_\alpha g_\beta g_\gamma$ сначала как $(g_\alpha g_\beta)\, g_\gamma$, а потом как $g_\alpha (g_\beta g_\gamma)$, получаем

$$h(\alpha\beta, \gamma)\, g_\gamma^{-1} h(\alpha, \beta)\, g_\gamma = h(\alpha, \beta\gamma)\, h(\beta, \gamma)$$

и, следовательно, в силу (1)

$$\omega[h(\alpha\beta, \gamma)]\,\omega[h(\alpha, \beta)]^\gamma = \omega[h(\alpha, \beta\gamma)]\,\omega[h(\beta, \gamma)]. \tag{2}$$

Рассмотрим теперь $\mathfrak{H}$-регулярное ковариантное отображение f из $\mathfrak{G}\times\mathfrak{G}\times\mathfrak{G}$ в $L^\times$, задаваемое формулой

$$f(\rho, \sigma, \tau) = \omega[h(\overline{\tau\sigma}^{-1}, \bar{\sigma}\bar{\rho}^{-1})]^\rho.$$

Из (2) следует, что это — множество факторов поля K. К нему можно, следовательно, применить конструкцию, описанную в доказательстве леммы 4 гл. IX-3, и получить простую алгебру A размерности n^2 над K. Как там было показано, положив $a = f(\varepsilon, \varepsilon, \varepsilon)$, мы получим изоморфизм θ поля L в A, если возьмем в качестве $\theta(\xi)$ для любого $\xi \in L$ элемент алгебры A, определяемый ковариантным отображением

$$(\rho, \sigma) \to (a^{-1}\xi)^\rho \delta_{\bar{\rho}\bar{\sigma}}$$

из $\mathfrak{G}\times\mathfrak{G}$ в L. Для каждого $\alpha \in \mathfrak{g}$ обозначим через e_α элемент алгебры A, определяемый отображением $(p, \sigma) \to \delta_{\bar{\rho}, \alpha\bar{\sigma}}$. Немед-

ленно проверяется, что формулы

$$\omega^*(g_\alpha) = e_\alpha \qquad \text{для всех } \alpha \in \mathfrak{g},$$
$$\omega^*(h) = \theta[\omega(h)] \quad \text{для всех } h \in H,$$

задают морфизм ω^* из G в A. Отождествляя L с его образом $\theta(L)$ в A при помощи θ, мы видим, что все требуемые в лемме свойства выполняются. Пусть A', ω'^* имеют те же свойства, и пусть $e'_\alpha = \omega'^*(g_\alpha)$. Обозначим через $(\xi_1, \ldots, \xi_n)$ базис поля L над K; элементы $e_\alpha\xi_i$, $\alpha \in \mathfrak{g}$, $1 \leqslant i \leqslant n$, образуют базис алгебры A над K. В силу наших предположений элементы $e'_\alpha\xi_i$ алгебры A' имеют ту же таблицу умножения, что и элементы $e_\alpha\xi_i$ в A. А так как A' также размерности n^α над K, то K-линейное отображение из A в A', переводящее $e_\alpha\xi_i$ в $e'_\alpha\xi_i$ для всех α и i, является изоморфизмом алгебры A на A'. Ясно, что этот изоморфизм индуцирует тождественный морфизм на L и переводит ω^* в ω'^*. Этим доказано утверждение о единственности. Пусть наконец z принадлежит нормализатору группы $L^\times$ в $A^\times$; автоморфизм $x \to z^{-1}xz$ алгебры A должен индуцировать на L некоторый автоморфизм $\alpha \in \mathfrak{g}$, так что элемент ze_α^{-1} коммутирует в A со всеми элементами из L. Легко видеть, например из закона умножения в A, что тогда $ze_\alpha^{-1} \in L^\times$, т. е. $z = \xi e_\alpha = e_\alpha\xi^\alpha$ для некоторого $\xi \in L^\times$ и, следовательно, $z \in \omega^*(G) \cdot L^\times$. Поскольку $\omega^*(G)\, L^\times$ содержится, очевидно, в нормализаторе группы $L^\times$ в $A^\times$, этим и завершается доказательство.

Если ω в лемме A является изоморфизмом H на $L^\times$, то ω^* является, очевидно, изоморфизмом группы G с нормализатором $L^\times$ в $A^\times$.

2. Используем теперь лемму A в следующей ситуации. Пусть K, L, $\mathfrak{g}$ таковы, как выше, и пусть L' — расширение Галуа поля K, содержащееся в K_{sep}, содержащее L и конечной степени d над L. Обозначим через Γ, Δ группы Галуа поля L' соответственно над K и над L, так что группу $\mathfrak{g}$ можно отождествить с Γ/Δ. Пусть теперь G — некоторая группа, φ' — морфизм из G на Γ, H' — ядро φ' и ω' — морфизм из H' в $L'^\times$. Мы предположим, что G, H', φ', ω' удовлетворяют (1), будучи подставленными в (1) вместо соответственно G, H, φ, ω, так что лемму A можно применить к ним. Это дает нам алгебру A' размерности $[L'\colon K]^2$ над K и морфизм из G в $A'^\times$. Обозначим через ψ канонический морфизм группы Γ на $\mathfrak{g} = \Gamma/\Delta$ и положим $\varphi = \psi \circ \varphi'$, $H = \varphi'^{-1}(\Delta)$; φ является морфизмом группы G на $\mathfrak{g}$ с ядром H. Для простоты записи предположим, что группа H' коммутативна. Если H^c — коммутант группы H, то можно так же, как в гл. XII-5, определить гомоморфизм переноса t из H/H^c в H' и рассматривать его очевидным образом как морфизм из H в H'. Если теперь $\omega = \omega' \circ t$, то из условия (1) на ω'

следует, что $\omega(h)$ инвариантно относительно Δ для всех $h \in H$, так что ω отображает H в $L^\times$. Ясно, что в этой ситуации G, H, φ, ω удовлетворяют (1). Применяя лемму А, получаем алгебру A размерности $[L : K]^2$ над K и морфизм из G в $A^\times$.

Лемма В. В группе Брауэра $B(K)$ поля K выполнено соотношение $\mathrm{cl}(A) = \mathrm{cl}(A')^d$, *где* $d = [L' : L]$ *и* A, A' — *алгебры, определенные выше.*

Выберем для каждого $\xi \in \Gamma$ представителя g_ξ класса смежности $\varphi'^{-1}(\xi)$ подгруппы H' в G и положим для всех ξ, η из Γ

$$h'(\xi, \eta) = g_{\xi\eta}^{-1} g_\xi g_\eta.$$

Тогда так как объяснялось в доказательстве леммы А, можно построить множество факторов f' поля K, класс которого в $H(K)$ определяется классом алгебры A' в $B(K)$. При этом определение переноса показывает, что для каждого $h \in H$

$$t(h) = \prod_{\theta \in \Delta} (g_{\varphi'(h)\theta}^{-1} \cdot h \cdot g_\theta).$$

Пусть теперь M — полное множество представителей классов смежности подгруппы Δ в Γ. Элементы g_μ, $\mu \in M$, образуют полную систему представителей классов смежности подгруппы H в G. Для произвольного $\xi \in \Gamma$ запишем в виде $\mu(\xi)$ представителя из M класса $\xi\Delta$. Возьмем в Γ произвольные два элемента ξ, η и положим $\alpha = \mu(\xi)$, $\beta = \mu(\eta)$, $\gamma = \mu(\xi\eta)$, $\lambda = \gamma^{-1}\alpha\beta$. Чтобы построить множество факторов f поля K, принадлежащее $\mathrm{cl}(A)$, следует поступить так же, как в доказательстве леммы А, положив

$$h(\xi, \eta) = g_\gamma^{-1} g_\alpha g_\beta.$$

По определению ω имеем

$$\omega[h(\xi, \eta)] = \omega' \Big[\prod_{\theta \in \Delta} (g_{\lambda\theta}^{-1} g_\gamma^{-1} g_\alpha g_\beta g_\theta) \Big].$$

Для каждого $\theta \in \Delta$ пусть

$$\theta' = \beta\theta\eta^{-1}, \quad \theta'' = \alpha\theta'\xi^{-1},$$

где θ пробегает множество Δ, равно как и θ', θ'' и $\lambda\theta$. В группе G выполняется следующее (легко проверяемое) теоретико-групповое тождество:

$$g_{\lambda\theta}^{-1} g_\gamma^{-1} g_\alpha g_\beta g_\theta = h'(\gamma, \lambda\theta)^{-1} h'(\theta'', \xi\eta)\, h'(\xi, \eta)\, g_\eta^{-1} \cdot [h'(\theta'', \xi)^{-1}\, h'(\alpha, \theta')]\, g_\eta \cdot h'(\theta', \eta)^{-1} h'(\beta, \theta).$$

Положим для каждого $\xi \in \Gamma$

$$c(\xi) = \omega' \left[\prod_{\theta \in \Delta} h'(\mu(\xi), \theta) h'(\theta, \xi)^{-1} \right].$$

Принимая во внимание тот факт, что ω' удовлетворяет условию (1), получаем

$$\omega [h(\xi, \eta)] = c(\xi)^{\eta} c(\eta) c(\xi\eta)^{-1} \omega' [h'(\xi, \eta)]^d.$$

Мы видим, что в силу формул из доказательства леммы A множество факторов f, определяющее алгебру A, отличается от f'^d на кограницу отображения $(\rho, \sigma) \to c(\sigma\rho^{-1})^{\rho}$. Этим доказана лемма B.

3. Возьмем теперь в качестве K коммутативное p-поле, L пусть будет такое же, как в § 1, а в качестве групп G и H возьмем W-группы поля L_{ab} соответственно над K и над L. Как объяснялось в приложении II, можно отождествить $\mathfrak{g}$ с G/H и взять в качестве φ канонический морфизм группы G на $\mathfrak{g} = G/H$. В качестве ω можно, как там объяснялось, выбрать морфизм, обратный к каноническому морфизму $\mathfrak{w}_L$ из $L^{\times}$ на H. Лемма A утверждает тогда, что ω можно продолжить (в существенном единственным образом) до изоморфизма группы G с нормализатором группы $L^{\times}$ в мультипликативной группе $A^{\times}$ некоторой простой алгебры A над K. В силу результатов гл. IX и XII отсюда следует, что структура группы G полностью определяется инвариантом Хассе $h(A)$ алгебры A. Его значение дается следующей теоремой Шафаревича.

Т е о р е м а. *В указанных предположениях A является алгеброй с делением размерности n^2 над K и с инвариантом Хассе $h(A) = e(1/n)$, где $n = [L : K]$.*

Поскольку A определяется однозначно (с точностью до изоморфизма) полями K и L, вместо $h(A)$ можно писать (L/K). Доказательство будет проведено в три шага.

(a) Пусть K такое же, как и выше, а поля L, L' таковы, как в § 2. Обозначим через G, H, H' W-группы поля L'_{ab} соответственно над K, L, L'. Выберем ω' обратным к каноническому изоморфизму $\mathfrak{w}_{L'}$, из $L'^{\times}$ на H'. Если снова t — гомоморфизм переноса из H/H^c в H' и если снова положить $\omega = \omega' \circ t$, то теорема переноса (см. приложения I, II), примененная к полям L, L' и W-группам H и H', немедленно показывает, что ω является обратным к каноническому изоморфизму $\mathfrak{w}_L$ группы $L^{\times}$ на группу H/H^c, если последнюю отождествить с W-группой поля L_{ab} над L. Мы можем, следовательно, применить лемму B к алгебрам A и A', если A определить так же, как и выше, а A' — с помощью полей K и L' вместо полей

K и L, участвующих в определении алгебры A. Это дает $(L/K) = (L'/K)^d$, где $d = [L' : L]$.

(b) Рассмотрим теперь случай циклического расширения L поля K. Пусть α, в обозначениях гл. IX-4,— образующая группы Галуа $\mathfrak{g}$ поля L над K, а χ — характер группы $\mathfrak{g}$, задаваемый формулой $\chi(\alpha) = \mathbf{e}(1/n)$. Снова отождествляя $\mathfrak{g}$ с G/H, обозначим через a представителя элемента α в G. Пусть t_0 — гомоморфизм переноса из G в H. Поскольку a^i образуют полную систему представителей классов смежности группы G по H, $0 \leqslant i < n$, имеем $t_0(a) = a^n$. Положим $\theta = \omega(a^n)$, где ω так же, как выше,— изоморфизм, обратный к каноническому изоморфизму $\mathfrak{w}_L$ группы $L^\times$ на H. Так как a^n инвариантен относительно автоморфизма $h \to a^{-1}ha$ группы H, то имеем $\theta^\alpha = \theta$, т. е. $\theta \in K^\times$. Пусть G^c — замыкание коммутанта группы G; G/G^c можно отождествить с W-группой поля K_{ab} над K (см. приложение II). Поэтому группа $K^\times$ отображается каноническим морфизмом $\mathfrak{w}_K$ на G/G^c. Если обозначить через ω_0 обратный к нему изоморфизм и рассматривать его как очевидный морфизм из G в $K^\times$, то теорема переноса, примененная к K, L, G, H, показывает, что $\omega_0 = \omega \circ t_0$ и, следовательно, $\theta = \omega_0(a)$. Теперь становится ясным, что алгебра A, определенная выше с помощью полей K и L, является не чем иным, как циклической алгеброй $[L/K; \chi, \theta]$, построенной в предложении 11 гл. IX-4. Точнее, если обозначить на время последнюю алгебру через A_0, то, положив $\omega^*(h) = \omega(h)\, u_0$, $h \in H$, $\omega^*(a) = u_1$, мы определим морфизм ω^* из G в A_0, обладающий всеми предписываемыми леммой A свойствами. Это дает

$$(L/K) = (\chi, \theta)_K = \chi(\mathfrak{w}_K(\theta)) = \chi(\alpha) = e(1/n).$$

(c) Пусть теперь L — произвольное расширение Галуа степени n поля K. Выберем циклическое расширение K' степени n поля K (например неразветвленное) и обозначим через L' композит полей K' и L в K_{sep}. Пусть $K_1 = K' \cap L$ и $d = [L : K_1]$. Тогда L' имеет степень d как над L, так и над K'. Из (a) вытекает, следовательно, что

$$(L'/K)^d = (L/K) = (K'/K).$$

Применяя (b) к K и K', находим, что $(L/K) = \mathbf{e}(1/n)$. В силу следствия 1 теор. 1 гл. XII-2 A должна быть алгеброй с делением; в самом деле, в обозначениях этого следствия она изоморфна циклической алгебре с делением $[K_n/K; \chi_n, \pi]$, где χ_n — неразветвленный характер порядка n, такой, что $\chi_n(\varphi) = e(1/n)$, где φ — автоморфизм Фробениуса поля K_{sep} над K.

4. В заключение делаем несколько замечаний, которые помогут уяснить описанную выше ситуацию.

Возьмем прежде всего, как и в гл. IX, алгебру A размерности n^2 над произвольным полем K, расширение L степени n поля K и K-линейный изоморфизм f из L в A. Обозначим через V векторное пространство размерности n над L, такое, что алгебра A, рассматриваемая как векторное пространство над K с умножением $(\xi, x) \to xf(\xi)$, $\xi \in L$, $x \in A$, совпадает с V. Для каждого $a \in A$ отображение $x \to ax$ является эндоморфизмом $F(a)$ пространства V; F определяет тем самым представление алгебры A в $\mathrm{End}_L V$, и в силу следствия 5 предл. 3 гл. IX-1 его L-линейное расширение F_L является изоморфизмом A_L на $\mathrm{End}_L V$. Пусть $z \in A$ таково, что $zf(\xi) = f(\xi)z$ при всех $\xi \in L$. Тогда отображение $x \to xz$ принадлежит $\mathrm{End}_L V$, коммутирует с $F(a)$ для всех $a \in A$, т. е. со всеми элементами из $\mathrm{End}_L V$, и следовательно, имеет вид $x \to xf(\zeta)$ при некотором $\zeta \in L$. Это означает, что $z = f(\zeta)$. Иначе говоря, $f(L)$ является своим собственным «коммутантом» в A, а $f(L)$ — своим централизатором в $A^\times$. Пусть теперь f' — другое вложение поля L в A. Построим V', F' по f' так же, как мы определили V, F по f. Как отмечалось в гл. IX-2, из предложения 4 гл. IX-1 следует, что существует L-линейный изоморфизм Y из V на V', такой, что $F' = Y^{-1}FY$. В силу наших определений это означает, что Y является биекцией алгебры A на себя, такой, что $Y(xf(\xi)) = Y(x)f'(\xi)$ и $Y(ax) = aY(x)$ для всех $\xi \in L$ и всех x, a из A. Положим $x = 1_A$ и $b = Y(1_A)$. Мы видим, что $b \in A^\times$ и $f' = b^{-1}fb$. Иначе говоря, два вложения поля L в A отличаются лишь на внутренний автоморфизм алгебры A, причем все автоморфизмы поля L над K индуцированы такими автоморфизмами алгебры A.

Напомнив эти хорошо известные факты, вернемся к коммутативному p-полю K и его расширению Галуа L степени n с группой Галуа $\mathfrak{g}$. Пусть A — алгебра с делением размерности n^2 над K с инвариантом $h(A) = \mathbf{e}(1/n)$. По следствию 2 теор. 2 гл. XII-2 алгебра A_L тривиальна; по следствию 3 теор. 3 гл. IX-3 можно, следовательно, вложить поле L в A, и в силу сделанных выше замечаний это вложение в существенном единственно. При этом $L^\times$ является своим собственным централизатором в $A^\times$. Если N — нормализатор этой группы в $A^\times$, то для каждого $\nu \in N$ автоморфизм $x \to \nu^{-1}x\nu$ алгебры A индуцирует автоморфизм α поля L над K, и отображение $\nu \to \alpha$ является морфизмом φ из N на группу $\mathfrak{g}$ с ядром $L^\times$. Пусть G, H суть W-группы поля L_{ab} над полями K и L соответственно, а $\mathfrak{w}_L$ —канонический изоморфизм $L^\times$ на H, описанный в приложении II. Теорема Шафаревича (в сочетании с леммой A) утверждает, что $\mathfrak{w}_L$ можно продолжить до изоморфизма $\mathfrak{w}$ группы N на G, такого, что $\mathfrak{w}(\nu)$ для всех $\nu \in N$ индуцирует

на L автоморфизм φ (ν). Это продолжение единственно с точностью до автоморфизма алгебры A вида $x \to \xi^{-1}x\xi$, где $\xi \in L$.

Пусть, наконец, K' — поле, промежуточное между K и L и соответствующее подгруппе $\mathfrak{g}'$ группы $\mathfrak{g}$. Пусть $n' = [L : K']$. Положим $N' = \varphi^{-1}(\mathfrak{g}')$; w изоморфно отображает группу N' на W-группу G' поля L_{ab} над K'. Сразу видно, что элементы группы N' порождают подалгебру A' в A, центр которой равен K'. Эта подалгебра имеет размерность n'^2 над K, и N' является нормализатором группы L в A'. Следовательно, алгебра A' связана с полями K' и L так же, как алгебра A связана с полями K и L, и имеет инвариант $h'(A') = \mathbf{e}(1/n')$.

ПРИЛОЖЕНИЕ IV. РАСПРЕДЕЛЕНИЕ ХЕРБРАНДА ДЛЯ НЕАБЕЛЕВЫХ РАСШИРЕНИЙ

1. Начнем с нескольких общих замечаний о распределениях Хербранда (см. гл. VIII-3). Пусть K—снова коммутативное p-поле.

Лемма А. *Пусть* $\mathfrak{K}$, $\mathfrak{K}'$—*два расширения Галуа* (*конечные или нет*) *поля* K, *такие, что* $K \subset \mathfrak{K} \subset \mathfrak{K}'$, *и пусть* $\mathfrak{G}$, $\mathfrak{G}'$, $\mathfrak{H}$— *группы Галуа соответственно поля* $\mathfrak{K}$ *над* K, *поля* $\mathfrak{K}'$ *над* K *и поля* $\mathfrak{K}'$ *над* $\mathfrak{K}$. *Обозначим через* φ *канонический морфизм группы* $\mathfrak{G}'$ *на* $\mathfrak{G} = \mathfrak{G}'/\mathfrak{H}$. *Пусть* $\mathbf{H}$, $\mathbf{H}'$ — *распределения Хербранда соответственно на* $\mathfrak{G}$ *и* $\mathfrak{G}'$. *Тогда* $\mathbf{H}(f) = \mathbf{H}'(f \circ \varphi)$ *для каждой локально постоянной функции* f *на* $\mathfrak{G}$.

Это очевидно. Как обычно, утверждение можно выразить, сказав, что $\mathbf{H}$ является образом (точнее, «прямым образом») распределения $\mathbf{H}'$ относительно φ.

Лемма В. *Пусть* K' — *расширение конечной степени поля* K; $\mathfrak{K}$ — *расширение Галуа* (*конечное или нет*) *поля* K, *такое, что* $K \subset K' \subset \mathfrak{K}$; $\mathfrak{G}$, $\mathfrak{G}'$ — *группы Галуа поля* $\mathfrak{K}$ *соответственно над* K *и над* K'; $\mathbf{H}$, $\mathbf{H}'$ — *распределения Хербранда на* $\mathfrak{G}$ *и* $\mathfrak{G}'$. *Тогда для каждой локально постоянной функции* f *на* $\mathfrak{G}$, *равной* 0 *вне* $\mathfrak{G}'$, *имеем* $\mathbf{H}'(f) = e\mathbf{H}(f) - df(\varepsilon)$, *где* e, d — *соответственно порядок ветвления и дифференциальная экспонента поля* K' *над* K, *а* ε — *единичный элемент в* $\mathfrak{G}$.

Это, также очевидное, утверждение можно выразить, сказав, что $\mathbf{H}'$ совпадает с $e\mathbf{H}$ на открытых и компактных подмножествах в $\mathfrak{G}'$, не содержащих ε, или, короче, совпадает с $e\mathbf{H}$ всюду на $\mathfrak{G}'$ вне ε. Этого, с учетом соотношения $\mathbf{H}'(1) = 0$, т. е. $\mathbf{H}'(\mathfrak{G}') = 0$, достаточно для того, чтобы полностью определить $\mathbf{H}'$ по $\mathbf{H}$.

Обозначим снова через K_0 максимальное неразветвленное расширение поля K в K_{sep}. Пусть $\mathfrak{K}$ — произвольное расширение Галуа поля K, промежуточное между K_0 и K_{sep}. Обозначим через $\mathfrak{G}$, $\mathfrak{G}_0$ группы Галуа поля $\mathfrak{K}$ соответственно над K и K_0 и через $\mathfrak{W}$ его W-группу над K. Согласно определениям приложения II, максимальная компактная подгруппа $\mathfrak{W}_0$ группы $\mathfrak{W}$ есть не что иное, как $\mathfrak{G}_0$. Пусть теперь $\mathbf{H}$ — распределение Хербранда на $\mathfrak{G}$. Как было показано в лемме 3 гл. XII-4 (см. замечание в конце доказательства этой леммы), $\mathbf{H}$ равно 0 вне $\mathfrak{G}_0$. Его можно, следовательно, рассматривать как распределение на $\mathfrak{W}$, которое равно 0 вне $\mathfrak{W}_0$. Полученное таким образом распределение будем называть распределением Хербранда на $\mathfrak{W}$.

2. Формула для распределения Хербранда на W-группе поля K_{ab} над K была получена в теореме 5 гл. XII-4. То же самое теперь будет сделано для W-группы поля L_{ab} над K, где L — произвольное расширение Галуа конечной степени поля K. Обозначим эту группу через G. В конце приложения III мы построили алгебру с делением A, содержащую L, и канонический изоморфизм $\mathfrak{w}$ нормализатора N группы $L^\times$ в $A^\times$ на G. С помощью $\mathfrak{w}^{-1}$ перенесем на N распределение Хербранда на G и назовем полученное распределение распределением Хербранда на N. Чтобы описать его явно, нам понадобится еще одна лемма.

Лемма C. *Пусть* τ, *в обозначениях* п. 4 *приложения* III,— *гомоморфизм переноса из* N *в* $L^\times$. *Тогда* $\tau(N) = K^\times$, *и ядро* τ *является замыканием в* N *коммутанта* N^c *группы* N. *Распределение Хербранда на* $K^\times$ *является образом относительно* τ *распределения Хербранда на* N.

Если G^c — замыкание в G коммутанта группы G, то W-группа поля K_{ab} над K равна G/G^c. Обозначим через $\mathfrak{w}_K$ канонический изоморфизм $K^\times$ на эту группу и через γ — канонический морфизм группы G на G/G^c. По лемме A распределение Хербранда на G/G^c является образом относительно γ распределения Хербранда на G. Обозначим через t гомоморфизм переноса из G/G^c в H, рассматриваемый как морфизм из G в H. Из теоремы переноса (см. приложения I и II) следует, что t имеет ядро G^c, а $t(G)$ является образом группы $K^\times$ в H относительно $\mathfrak{w}_L$. Выберем произвольное $v \in N$ и положим $g = \mathfrak{w}(v)$ и $\xi = \mathfrak{w}_k^{-1}[\gamma(g)]$. По теореме переноса $t(g) = \mathfrak{w}_L(\xi)$. Поскольку $\mathfrak{w}$ — изоморфизм группы N на G, индуцирующий $\mathfrak{w}_L$ на $L^\times$, мы видим, что $\tau(v) = \xi$. Лемма становится теперь очевидной.

3. Пусть обозначения снова те же, что и в п. 4 приложения III. Алгебра с делением A является p-полем (некоммутативным при $n > 1$), структура которого описана в гл. I. Пусть R_A — его максимальное компактное подкольцо. Максимальными компактными подкольцами полей L и K будут тогда $R_L = L \cap R_A$ и $R_K = K \cap R_A$. Обозначим через q модуль p-поля K. Модуль A равен по предложению 5 гл. I-4 q^n, а модуль L равен q^f, где f — модулярная степень поля L над K. Приведенную норму в алгебре A над K будем записывать в виде $v_{A/K}$. Для каждого $x \in A$ положим $\| x \| = \mathrm{mod}_K\, |v_{A/K}(x)|$. В силу следствия 1 предл. 6 гл. IX-2 и следствия 3 теор. 3 гл. I-2 имеем $\mathrm{mod}_A(x) = \| x \|^n$. Следовательно, отображение $x \to \| x \|$ отображает $A^\times$ на подгруппу $\mathbf{Q}$ группы $\mathbf{R}_+$, порожденной q. Рассматривая A как левое векторное пространство над L (размерности n), видим также, что для всех $\xi \in L$ $\mathrm{mod}_A(\xi) = \mathrm{mod}_L(\xi)^n$ и, следовательно, $\| \xi \| = \mathrm{mod}_L(\xi)$, так что отображение $x \to \| x \|$ отображает $L^\times$ на подгруппу Q_f группы Q, порожденную q^f. Поэтому оно должно отображать N на подгруппу Q' конечного индекса в Q, так что ядро $N_0 = N \cap R_A^\times$ этого морфизма есть максимальная компактная подгруппа в N, а w отображает его на группу Галуа поля L_{ab} над K_0. Максимальное неразветвленное расширение поля K, содержащееся в L, равно $K_1 = L \cap K_0$ и имеет степень f над K. Поскольку w отображает группы N, $L^\times$, $N_0 L^\times$ на W-группы поля L_{ab} соответственно над полями K, L, K_1, то мы заключаем, что $N_0 L^\times$ имеет в N индекс f, в силу чего Q_f имеет в Q' индекс f. Таким образом, $Q' = Q$. По аналогичным причинам индекс группы $R_L^\times$ в N_0 равен порядку ветвления $e = n/f$ поля L над K.

4. Пусть dv — мера Хаара на N, нормированная так, что мера N_0 равна 1. Следующая теорема принадлежит по существу Тэйту и Шанкар Сену (*J. Ind. Math. Soc.*, **27** (1964)).

Т е о р е м а. *Пусть* $\mathbf{H}$ *— распределение Хербранда на* N. *Тогда для всех локально постоянных функций* f *на* N

$$H(f) = -\int_{N_0} [f(v) - f(1_A)] \cdot \| 1_A - v \|^{-1} dv. \qquad (1)$$

В абелевом случае, когда $n = 1$, $K = L = A$, $N = K^\times$, это — переформулировка теоремы 5 гл. XII-4. Отсюда с учетом леммы B сразу следует, что $\mathbf{H}(f)$ совпадает с правой частью (1), если f равна 0 вне $L^\times$. Иначе говоря, если правую часть (1) обозначить через $\mathbf{H}_1(f)$, то $\mathbf{H}$ совпадает с $\mathbf{H}_1$ на $L^\times$, и теорема будет доказана, если мы покажем, что $\mathbf{H} = \mathbf{H}_1$ на каждом классе смежности подгруппы

N в $L^\times$, отличном от $L^\times$. Пусть a — элемент такого класса, α — его образ в группе Галуа $\mathfrak{g}$ поля L над K. Обозначим через $\mathfrak{g}'$ циклическую подгруппу группы g, порожденную α, и через K' — поле, промежуточное между K и L и соответствующее $\mathfrak{g}'$. Как мы видели в конце приложения III, a и L порождают подполе A' алгебры A с центром K', связанное с K' и L так, как алгебра A связана с K и L. Нормализатор N' подгруппы $L^\times$ в $A'^\times$ является подгруппой в N, порожденной a и $L^\times$. Рассматривая A как левое векторное пространство над A' (размерности n/n', если $n' = [L: K']$), получаем $\mathrm{mod}_A(x') = \mathrm{mod}_{A'}(x)^{n/n'}$ для $x' \in A'$, т. е. $\mathrm{mod}_{A'}(x') = \| x' \|^{n'}$. Применяя лемму B к K, K', L, т. е. к распределениям Хербранда на W-группах поля L_{ab} над K и K', находим, что достаточно проверить (1) для K', L, A', N', если отождествить эти группы с помощью канонических изоморфизмов соответственно с N и N'. Иначе говоря, доказывая теорему, можно предполагать, что L — циклическое расширение поля K. Точнее, если a и α такие же, как и выше, то можно предполагать, что α имеет порядок, $n > 1$ и порождает $\mathfrak{g}$, и надо доказать, что $\mathbf{H}$ совпадает с $\mathbf{H}_1$ на классе $aL^\times$.

В этой ситуации применим лемму C. Как нетрудно видеть, заключение этой леммы в сочетании с инвариантностью распределения Хербранда относительно внутренних автоморфизмов дает возможность полностью определить $\mathbf{H}$ на $aL^\times$. В самом деле обозначим снова через τ перенос из N в $L^\times$, рассматриваемый как морфизм из N в $L^\times$. Более точно, в силу леммы C это — морфизм из N на $K^\times$ и его ядро Γ есть замыкание коммутанта группы N. Так как N порождается a и $L^\times$ и $a^{-1}\xi a = \xi^\alpha$ для всех $\xi \in L^\times$, то последняя группа является подгруппой в $L^\times$, порожденной элементами $\xi^\alpha\xi^{-1}$. По теореме Гильберта она совпадает с ядром морфизма $N_{L/K}$ из $L^\times$ в $K^\times$, а так как это компактная подгруппа в $R_L^\times$, то τ имеет то же ядро, Γ, что и $N_{L/K}$ в $L^\times$. Для каждого $\nu \in aL^\times$ можно взять $1_A, \nu, \ldots, \nu^{n-1}$ в качестве представителей классов смежности подгруппы N в $L^\times$; это дает $\tau(\nu) = \nu^n$. Положим в частности $\theta = \tau(a) = a^n$. Беря $1_A, a, \ldots, a^{n-1}$ в качестве представителей тех же самых классов, видим, что $\tau(\xi) = N_{L/K}(\xi)$ для всех $\xi \in L^\times$. Следовательно, для всех $0 \leqslant i < n$ τ отображает $a^iL^\times$ на $\theta^i N_{L/K}(L^\times)$. Поскольку ядро τ есть Γ, то (как вытекает из теории полей классов) $K^\times$ должно быть дизъюнктным объединением классов смежности подгруппы $N_{L/K}(L^\times)$ в $K^\times$. Возьмем теперь какую-нибудь локально постоянную функцию f на N, равную 0 вне $aL^\times \cap N_0$. Для каждого γ из ядра отображения τ можно представить γ в виде $\gamma = \xi^\alpha\xi^{-1}$ с $\xi \in L^\times$ так, чтобы внутренний автоморфизм $x \to \xi^{-1}x\xi$, переводящий каждый класс $a^iL^\times$ в себя, индуцировал

на $aL^\times$ отображение $\nu \to \nu\gamma^{-1}$. Поскольку $\mathbf{H}$ очевидно инвариантно относительно таких автоморфизмов, получаем $\mathbf{H}(f_\gamma) = \mathbf{H}(f)$ для функций $f_\gamma\colon \nu \to f(\nu\gamma^{-1})$ на N. Обозначим через $d\gamma$ меру Хаара на Γ, нормированную так, чтобы мера Γ равнялась 1, и положим

$$\bar{f}(\nu) = \int_\Gamma f(\nu\gamma^{-1})\, d\gamma.$$

Тогда $\mathbf{H}(f) = \mathbf{H}(\bar{f})$, и $\bar{f}$ инвариантна относительно сдвига на ядро морфизма τ, так что можно записать ее в виде $f' \circ \tau$, где f' — функция на $K^\times$, равная 0 вне $R_K^\times \cap \theta N_{L/K}(L^\times)$. Так как образ распределения $\mathbf{H}$ относительно τ является распределением Хербранда на $K^\times$, которое задается формулой из нашей теоремы, получаем

$$\mathbf{H}(f) = -\int_{R_K^\times} f'(\xi)\, \mathrm{mod}_K(1-\xi)^{-1} d^\times\xi,$$

где $d^\times\xi$ — «мультипликативная» мера Хаара на $K^\times$, нормированная так, чтобы мера $R_K^\times$ равнялась 1.

Для $\nu \in aL^\times$ положим $\xi = \tau(\nu) = \nu^n$. Выбрав базис $\eta_0, \ldots, \eta_{n-1}$ поля L над K и используя базис $(\nu^i\eta_j)_{0\leqslant i,\, j<n}$ алгебры A над K, сразу находим (по следствию 3 теор. 3 гл. I-2), что отображения $x \to \nu x$ и $x \to (1_A - \nu)x$ алгебры A в себя имеют модули

$$\mathrm{mod}_A(\nu) = \mathrm{mod}_K(\xi)^n, \qquad \mathrm{mod}_A(1_A - \nu) = \mathrm{mod}_K(1-\xi)^n.$$

Это дает

$$\|\nu\| = \mathrm{mod}_K[\tau(\nu)], \qquad \|1_A - \nu\| = \mathrm{mod}_K[1 - \tau(\nu)]; \tag{2}$$

более того, поскольку группа N порождается элементами $aL^\times$, первая формула (2) остается справедливой для всех $\nu \in N$; отсюда следует, что $\tau^{-1}(R_K^\times) = N_0$. А так как образ относительно τ меры Хаара dv на N должен быть мерой Хаара на $K^\times$, мы видим, что этот образ равен $d^\times\xi$. Следовательно, полученная выше формула для $\mathbf{H}(f)$ может быть записана в виде

$$\mathbf{H}(f) = -\int_{N_0} \bar{f}(\nu)\, \|1_A - \nu\|^{-1} d\nu.$$

В силу определения $\bar{f}$ и того очевидного факта, что мера $\|1_A - \nu\|^{-1} d\nu$ сама инвариантна относительно всех внутренних автоморфизмов, этим и завершается доказательство.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

В этот указатель включены все понятия и термины, определение которых дается или упоминается в тексте, даже если это не было сделано в виде формального определения.

ОГЛАВЛЕНИЕ