MATHEMATICAL SURVEYS

NUMBER II

THE THEORY OF RINGS

by

NATHAN JACOBSON

1943

Н. ДЖЕКОБСОН

ТЕОРИЯ КОЛЕЦ

Перевод с английского

Н. Я. ВИЛЕНКИНА

1947

Государственное издательство

ИНОСТРАННОЙ ЛИТЕРАТУРЫ

Москва

Книга Н. Джекобсона является систематическим изложением теории колец, в первую очередь колец эндоморфизмов. Эта область абстрактной алгебры, возникшая в начале нашего столетия, получила дальнейшее развитие в работах Алберта, Артина, Э. Нетер и других, и в настоящее время продолжает быстро развиваться.

Книга рассчитана на научных работников-математиков, а также аспирантов и студентов старших курсов математических факультетов, специализирующихся по алгебре. Она может служить хорошим дополнением к работам советских ученых по современной алгебре, которые развивались по преимуществу в других смежных направлениях (см. книгу А. Г. Куроша „Теория групп" и работы И. М. Гельфанда по теории нормированных колец).

Заведующий Редакцией Математической Литературы
академик *А. Н. Колмогоров*.

ПРЕДИСЛОВИЕ

Теория, составляющая предмет этой книги, ведет свое начало с 1927 г., когда Артином была перенесена веддербарновская структурная теория алгебр на кольца, удовлетворяющие условиям обрыва цепей. В дальнейшем эта теория была значительно расширена и упрощена. Единственной книгой, посвященной этому вопросу, явился опубликованный в 1935 г. в серии «Ergebnisse» обзор Дейринга «Algebren» («Алгебры»). Новое изложение этой темы вполне оправдывается значительными успехами, достигнутыми с тех пор в этой области.

Чтение книги не требует почти никаких предварительных знаний. То, что это оказалось возможным в книге, посвященной результатам, относящимся к теореме Веддербарна, теории простых алгебр, развитой Албертом, Брауером и Нётер, и арифметической теории идеалов, еще раз показывает одно из наиболее замечательных свойств современной алгебры, а именно, простоту ее логической структуры.

Содержание книги распадается, в основном, на три части: структурную теорию, теорию представлений и арифметическую теорию идеалов. Первая из них возникла из структурной теории алгебр. Причиной ее возникновения было желание изучить и классифицировать «гиперкомплексные» расширения поля действительных чисел.

Наиболее известными именами, связанными с этим периодом развития теории, являются имена Молина, Дедекинда, Фробениуса и Картана. Структурная теория алгебр над любыми полями ведет свое начало с опубликования в 1907 г. диссертации Веддербарна; на кольца же она была перенесена Артином в 1927 г. Теория представлений первоначально была связана с проблемой представления групп матрицами. Эмми Нётер перенесла ее на кольца и сформулировала в виде теории модулей. Изучение модулей составляет также важную часть арифметической теории идеалов. Эта часть теории колец начинается с дедекиндовской теории идеалов алгебраических числовых полей, а более непосредственным образом — с аксиоматического обоснования этой теории, данного Эмми Нётер.

На протяжении всей книги мы делали особое ударение на изучении колец эндоморфизмов. Введение регулярных представлений дало возможность рассматривать теорию абстрактных колец как специальный случай более конкретной теории колец эндоморфизмов. Более того, теория модулей, а, следовательно, и теория представлений может рассматриваться как изучение совокупности колец эндоморфизмов, каждое из которых является гомоморфным образом фиксированного кольца o. Первая глава посвящена основам теории эндоморфизмов групп. Изложенные здесь понятия и результаты имеют фундаментальное значение для всех дальнейших рассмотрений. Во второй главе изучаются векторные пространства; она содержит результаты, некоторые из которых, по крайней мере для коммутативного случая, могли бы предполагаться уже известными, однако приведены здесь для полноты. Третья глава связана с арифметикой некоммутативных областей

главных идеалов. Многое в этой главе может рассматриваться как частный случай общей арифметической теории идеалов, развитой в шестой главе. Однако методы, используемые здесь, носят более элементарный характер, и это обстоятельство может представлять интерес для изучающих геометрию, так как результаты третьей главы имеют много приложений в этой области. Читатель, которого в первую очередь интересует структурная теория или теория представлений, может опустить эту главу, за исключением § 3. Эти теории и некоторые приложения к теории представлений групп проективными преобразованиями и к теории Галуа тел излагаются в четвертой главе. В пятой главе мы переходим к изучению алгебр. В первой ее части рассматривается теория простых алгебр над произвольным полем. Вторая часть посвящена характеристическому и минимальному полиномам алгебры и критерию сепарабельности алгебры, выражаемому при помощи ее следа.

В последнее время наблюдается большой интерес к изучению колец, не удовлетворяющих условиям обрыва цепей, вместо которых налагаются топологические или метрические условия. Упомянем исследования фон Неймана и Мэррея о кольцах преобразований гильбертова пространства, теорию регулярных колец построенную Нейманом, и теорию нормированных колец. И. М. Гельфанда. Эти теории находят много применений в анализе. Вследствие условий, которые мы накладываем на изучаемые в этой книге кольца, наши рассуждения не могут быть непосредственно приложены к проблемам топологической алгебры. Однако можно надеяться, что методы и результаты чисто алгебраической теории укажут путь для дальнейшего развития топологической алгебры.

Эта книга была начата во время 1940—1941 учебного года, когда я был приглашен читать лекции в университете Джона Гопкинса. Она служила основой прочитанного тогда курса и много выиграла от тщательного просмотра и критики д-ра Ирвинга Кохена, бывшего в то время одним из слушателей моих лекций. Я выражаю благодарность ему, а также профессорам Алберту, Шиллингу и Гуревичу за их поддержку и многие полезные советы.

Н. Джекобсон

7 марта, 1943 г

Глава I

ГРУППЫ И ЭНДОМОРФИЗМЫ

1. Кольца эндоморфизмов. С каждой коммутативной группой $\mathfrak{M}$ мы можем связать кольцо $\mathfrak{E}(\mathfrak{M})$, кольцо эндоморфизмов группы $\mathfrak{M}$ (гомоморфизмов группы $\mathfrak{M}$ в себя). С другой стороны, как мы увидим, каждое кольцо с единицей может быть получено, как подкольцо кольца эндоморфизмов его аддитивной группы. Поэтому мы можем воспользоваться теорией колец эндоморфизмов для построения теории абстрактных колец. Этот метод изучения колец является одним из наиболее важных среди тех, которыми мы будем пользоваться в этой книге. Поэтому целесообразно начать наше изложение кратким обзором той части теории групп и эндоморфизмов, которая нам позже понадобится.

В дальнейшем нас будут интересовать в основном коммутативные группы. Однако, так как большинство результатов этой главы справедливо для произвольной группы $\mathfrak{M}$, мы не будем предполагать сначала, что $\mathfrak{M}$ коммутативна. Тем не менее, удобнее употреблять аддитивную запись: групповая операция будет обозначаться знаком $+$, единичный элемент через 0, обратный к a через $-a$ и т. д.

Рассмотрим совокупность $\mathfrak{T}(\mathfrak{M})$ однозначных отображений множества $\mathfrak{M}$ в себя, т. е. на подмножество множества $\mathfrak{M}$. Как обычно, мы считаем, что отображения A и B равны, если образы xA и xB одинаковы для всех $x \in \mathfrak{M}$. Теперь мы превратим $\mathfrak{T}$ в алгебраическую систему, введя в ней две основные операции. Во-первых, если $A \in \mathfrak{T}$ и $B \in \mathfrak{T}$, то *сумма* $A+B$ определяется как

отображение, при котором образ каждого элемента $x \in \mathfrak{M}$ получается сложением образов xA и xB. Иными словами,

$$x(A+B) = xA + xB.$$

Произведение AB является результатом последовательного выполнения A и B:

$$x(AB) = (xA)B^{1}).$$

Легко проверяются следующие факты, относящиеся к системе $\mathfrak{T}$:

1) $\mathfrak{T}$ является группой относительно сложения. Единичным элементом этой группы является отображение 0, определенное равенством $x0 = 0$. Обратный элемент для $A, -A$, задается определяющим уравнением $x(-A) = -xA$.

2) $\mathfrak{T}$ является полугруппой с единицей относительно умножения, т. е. $(AB)C = A(BC)$, и единичным элементом в $\mathfrak{T}$ является тождественное отображение 1, $(x1 = x)$.

3) Имеет место дистрибутивный закон $A(B+C) = AB + AC$.

Таким образом, система $\mathfrak{T}$ весьма похожа на кольцо. Однако она не является им, так как соотношения $A+B = B+A$ и $(B+C)A = BA + CA$ не всегда справедливы. Мы можем удовлетворить первому из этих соотношений, предположив, что $\mathfrak{M}$ коммутативна, но даже в этом случае второе условие может не быть выполнено.

Пример. Пусть $\mathfrak{M}$ — циклическая группа порядка 2 с элементами 0, 1, где $1+1=0$. $\mathfrak{T}$ содержит четыре элемента:

$$0 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad 1 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

где всегда $\begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ обозначает отображение $0 \to a$, $1 \to b$.

[1]) Это равенство оправдывает наше обозначение xA. При его употреблении порядок записи соответствует порядку выполнения отображений.

Таблицами сложения и умножения для $\mathfrak{T}$ будут соответственно:

	0	1	A	B
0	0	1	A	B
1	1	0	B	A
A	A	B	0	1
B	B	A	1	0

	0	1	A	B
0	0	0	B	B
1	0	1	A	B
A	0	A	1	B
B	0	B	0	B

Так как $0A \neq 0$, то очевидно, что второй дистрибутивный закон не выполняется.

Мы рассмотрим теперь подмножество $\mathfrak{E}(\mathfrak{M})$ в $\mathfrak{T}$, состоящее из эндоморфизмов группы $\mathfrak{M}$, ($\mathfrak{M}$ — произвольная группа). Напомним определение:

Отображение A группы называется *эндоморфизмом*, если оно является гомоморфизмом группы в себя, т. е. если

$$(x+y)A = xA + yA.$$

Очевидно, что $\mathfrak{E}$ замкнуто относительно умножения, определенного в $\mathfrak{T}$. Кроме того, если B и C являются элементами из $\mathfrak{T}$ и $A \in \mathfrak{E}$, то

$$(B+C)A = BA + CA.$$

С нашей точки зрения система $\mathfrak{E}$ не является особенно интересной, когда $\mathfrak{M}$ будет произвольной группой, так как тогда $\mathfrak{E}$ незамкнуто относительно сложения, определенного в $\mathfrak{T}$. Однако положение совершенно изменяется, когда $\mathfrak{M}$ коммутативна. В этом случае легко видеть, что если A и B входят в $\mathfrak{E}$, то $A+B = B+A$, 0 и $-A$ принадлежат $\mathfrak{E}$. Так как дистрибутивный и коммутативный законы для умножения выполнены, то $\mathfrak{E}$ является кольцом. Таким образом, имеем основную теорему:

Теорема 1. *Если $\mathfrak{M}$ является коммутативной группой, то множество $\mathfrak{E}(\mathfrak{M})$ эндоморфизмов $\mathfrak{M}$ является кольцом относительно операций $A+B$ и AB, определенных уравнениями*

$$x(A+B) \equiv xA + xB, \quad x(AB) \equiv (xA)B.$$

Примеры: 1) Пусть $\mathfrak{M}$ — группа целых рациональных чисел с обычным сложением. Так как $\mathfrak{M}$ является циклической группой, образующей для которой будет 1, каждый эндоморфизм A определяется его действием на 1. Если $1A = a$ и $x = \underbrace{1 + \ldots + 1}_{x}$, то $xA = xa$, где xa — обычное произведение целых чисел x и a. Так как $(-x)A \equiv -xA$, то это равенство справедливо также для отрицательных x, а так как $0A = 0 = 0a$, оно справедливо и для 0. Таким образом, любой эндоморфизм A группы $\mathfrak{M}$ является отображением, при котором каждый элемент $x \in \mathfrak{M}$ умножается на фиксированный элемент a. A однозначно определяет элемент a, и очевидно, что каждое целое число a может быть получено таким образом из некоторого эндоморфизма. Следовательно, $\mathfrak{E}$ находится во взаимооднозначном соответствии с $\mathfrak{M}$. Если $A \to a$ и $B \to b$ в нашем соответствии, то

$$x(A+B) = xA + xB = xa + xb = x(a+b)$$

и таким же образом $x(AB) = x(ab)$. Следовательно, $A+B \to a+b$ и $AB \to ab$, т. е. $\mathfrak{E}$ изоморфно *кольцу* целых рациональных чисел $\mathfrak{M}$.

2) Обобщая пример 1, положим, что $\mathfrak{M}$ является прямой суммой n бесконечных циклических групп. Если образующими для $\mathfrak{M}$ являются $e_1, \ldots, e_n$, то каждый эндоморфизм A группы $\mathfrak{M}$ вполне определяется заданием образов $e_i A = f_i$. С другой стороны, мы можем выбрать элементы f_i произвольно в $\mathfrak{M}$ и определить $(\Sigma e_i x_i)A = \Sigma f_i x_i$, где x_i целые числа. Тогда A будет эндоморфизмом. Если

$$e_i A = e_i a_{i1} + \ldots + e_n a_{in} \quad (i = 1, \ldots, n),$$

где a_{ij} — целые рациональные числа, то соответствие $A \to (a_{ij})$ будет взаимооднозначным соответствием между $\mathfrak{E}$ и кольцом всех матриц порядка n с целыми рациональными элементами. Если $B \to (b_{ij})$, то можно проверить, что $A+B \to (a_{ij}) + (b_{ij})$ и $AB \to (b_{ij})(a_{ij})$. Следовательно, это соответствие является обратным изоморфизмом между $\mathfrak{E}$ и кольцом матриц с целыми рациональными элементами [1]). Можно заметить, что ассоциативный и коммутативный законы для этих матриц выводятся при помощи нашего соответствия из ассоциативного и дистрибутивного законов для эндоморфизмов.

3) Если $\mathfrak{M}$ является прямой суммой циклических групп порядка m, то подобное рассуждение показывает, что кольцо эндоморфизмов группы $\mathfrak{M}$ обратно-изоморфно кольцу матриц с элементами из кольца целых рациональных чисел, приведенных по модулю m.

Вернемся к рассмотрению произвольной группы $\mathfrak{M}$. Пусть $\mathfrak{G}(\mathfrak{M})$ является множеством взаимнооднозначных отображений $\mathfrak{M}$ на себя. Очевидно, что если $A \in \mathfrak{G}(\mathfrak{M})$, то определено обратное отображение A^{-1}. Отсюда следует, что $\mathfrak{G}(\mathfrak{M})$ является группой относительно умножения.

Если теперь A будет эндоморфизмом, то и A^{-1} — также эндоморфизм. Следовательно, пересечение $\mathfrak{A}(\mathfrak{M}) = \mathfrak{E}(\mathfrak{M}) \cap \mathfrak{G}(\mathfrak{M})$ также является группой относительно умножения. Элементы этой группы, взаимнооднозначные эндоморфизмы группы $\mathfrak{M}$ на себя, являются *автоморфизмами* группы $\mathfrak{M}$. Особенно интересными среди этих отображений являются *внутренние автоморфизмы*. Если $s \in \mathfrak{M}$, то внутренний автоморфизм, соответствующий элементу s, определяется равенством $xS = -s + x + s$. Если A является произвольным автоморфизмом, то $x(A^{-1}SA) = -sA + x + sA$, т. е. $A^{-1}SA$ будет внутренним автоморфизмом, соответствующим элементу sA. Это показывает, что совокупность внутренних автоморфизмов образует нормальный делитель во всей группе автоморфизмов.

Напомним, что в кольце с единицей элемент u называется *обратимым*, если он имеет как левый, так и правый обратные элементы. Непосредственно проверяется,

[1]) Если мы воспользуемся соответствием $A \to (a_{ij})^*$, где $(a_{ij})^*$ получается транспонированием матрицы (a_{ij}), то мы получим изоморфизм. Однако в дальнейшем мы встретимся с подобным положением, причем там будет невозможно сделать такой переход от обратного изоморфизма к изоморфизму. По этой причине мы предпочитаем употреблять соответствие $A \to (a_{ij})$.

что оба обратных элемента равны между собой и что никакой другой элемент кольца не может удовлетворять ни уравнению $ux = 1$, ни уравнению $xu = 1$. Как обычно, мы обозначаем обратный элемент для u через u^{-1}. Легко можно доказать, что множество обратимых элементов каждого кольца образует группу относительно умножения. Рассмотрим теперь коммутативную группу $\mathfrak{M}$, её кольцо эндоморфизмов $\mathfrak{E}$ и ее группу автоморфизмов $\mathfrak{A}$. Так как только взаимнооднозначные отображения множества имеют двусторонние обратные отображения, то очевидно, что $\mathfrak{A}$ будет группой обратимых элементов в $\mathfrak{E}$. Следствием этого факта является то, что группа автоморфизмов прямой суммы $\mathfrak{M}$ n бесконечных циклических групп изоморфна мультипликативной группе целочисленных матриц порядка n, детерминанты которых равны ± 1. Для этого заметим, что кольцо эндоморфизмов группы $\mathfrak{M}$ изоморфно кольцу целочисленных матриц порядка n, и используя мультипликативное свойство детерминанта, мы увидим, что обратимыми элементами последнего кольца являются матрицы с детерминантом, равным ± 1.

2. Группы с операторами. Часто бывает полезно рассматривать группы $\mathfrak{M}$ относительно фиксированного множества эндоморфизмов Ω, действующих в $\mathfrak{M}$. Мы особо отмечаем подгруппы, называемые Ω-*подгруппами* (или допустимыми), которые преобразуются в в себя при каждом эндоморфизме, принадлежащем Ω. Хотя в наших приложениях $\mathfrak{M}$ будет обычно бесконечной группой, следующие примеры показывают, что эта точка зрения полезна и при изучении конечных групп.

Примеры: 1) Ω пусто. Все подгруппы тогда будут допустимыми. 2) Ω состоит из внутренних автоморфизмов. Здесь Ω-подгруппы будут нормальными делителями. 3) Ω является множеством всех автоморфизмов. Ω-подгруппы являются характеристическими подгруппами группы $\mathfrak{M}$.

Пусть в дальнейшем $\mathfrak{M}$ и Ω фиксированы. Если $\mathfrak{N}_1$ и $\mathfrak{N}_2$ являются Ω-подгруппами, то, очевидно, пересечение $\mathfrak{N}_1 \cap \mathfrak{N}_2$ является также Ω-подгруппой. Объединение $(\mathfrak{N}_1, \mathfrak{N}_2)$, определяемое как наименьшая подгруппа, содержащая $\mathfrak{N}_1$ и $\mathfrak{N}_2$, может быть охарактеризовано как множество конечных сумм элементов из $\mathfrak{N}_1$ и $\mathfrak{N}_2$. Следовательно, $(\mathfrak{N}_1, \mathfrak{N}_2)$ является Ω-подгруппой. Если $\mathfrak{N}_1$ является нормальным делителем, то $(\mathfrak{N}_1, \mathfrak{N}_2) = \mathfrak{N}_1 + \mathfrak{N}_2 = \mathfrak{N}_2 + \mathfrak{N}_1$, где $\mathfrak{N}_1 + \mathfrak{N}_2$ обозначает множество элементов вида $x_1 + x_2$ при $x_i \in \mathfrak{N}_i$.

Если $\mathfrak{N}$ является Ω-подгруппой, то эндоморфизм $\alpha \in \Omega$ индуцирует в $\mathfrak{N}$ эндоморфизм, который мы также будем обозначать через α. Конечно, различные отображения α и β группы $\mathfrak{M}$ могут совпадать, если их рассматривать как отображения в $\mathfrak{N}$. Заметим, что если $\alpha\beta = \gamma \in \Omega$ или $\alpha + \beta = \delta \in \Omega$, то эти соотношения остаются справедливыми и для отображений, индуцированных в $\mathfrak{N}$.

Предположим теперь, что $\mathfrak{N}$ и $\mathfrak{P}$ являются Ω-подгруппами, причем $\mathfrak{P}$ нормальный делитель в $\mathfrak{N}$. Рассмотрим фактор-группу, состоящую из смежных классов $\mathfrak{P} + y$, где $y \in \mathfrak{N}$. Если $\alpha \in \Omega$, то α следующим образом определяет отображение в $\mathfrak{N}/\mathfrak{P}$. Если $\mathfrak{P} + y$ является некоторым смежным классом, то смежный класс $\mathfrak{P} + y\alpha$ не зависит от выбора представителя y и потому однозначно определяется смежным классом $\mathfrak{P} + y$ и эндоморфизмом α. Следовательно, соответствие $\mathfrak{P} + y \to \mathfrak{P} + y\alpha$ является однозначным отображением. Мы снова обозначим это отображение группы $\mathfrak{N}/\mathfrak{P}$ через α, т. е. $(\mathfrak{P} + y)\alpha = \mathfrak{P} + y\alpha$. Очевидно, что α будет эндоморфизмом группы $\mathfrak{N}/\mathfrak{P}$. Как и в случае подгруппы, соотношения $\alpha\beta = \gamma$ и $\alpha + \beta = \delta$ в $\mathfrak{N}$ влекут за собой те же соотношения для индуцированных отображений в $\mathfrak{N}/\mathfrak{P}$. Мы можем повторять эти процессы, беря фактор-группу для фактор-группы, подгруппу в фактор-группе и т. д. Таким образом порождается целая иерархия $\mathfrak{R}$ групп, в которых исходный эндоморфизм α индуцирует однозначно определенные эндоморфизмы. Мы будем называть члены множества $\mathfrak{R}$ Ω-*группами*.

Пусть $\mathfrak{N}$ и $\overline{\mathfrak{N}}$ будут любыми двумя Ω-группами. Отображение A группы $\mathfrak{N}$ на всю группу $\overline{\mathfrak{N}}$ называется Ω-*гомоморфизмом*, если оно является обыкновенным гомоморфизмом и $\alpha A = A\alpha$ для всех $\alpha \in \Omega$. Тогда $\overline{\mathfrak{N}}$ называется Ω-*гомоморф-*

ным образом группы $\mathfrak{N}$[1]). Если отображение A взаимнооднозначно,то оно является Ω-*изоморфизмом*, и тогда $\mathfrak{N}$ и $\overline{\mathfrak{N}}$ будут Ω-*изоморфны*. Если $\overline{\mathfrak{N}} \subseteq \mathfrak{N}$, то мы употребляем термин Ω-*эндоморфизм* для Ω-гомоморфизма, а если $\overline{\mathfrak{N}} = \mathfrak{N}$, то мы употребляем термин Ω-*автоморфизм* для Ω-изоморфизма.

3. Теоремы об изоморфизме. Пусть $\mathfrak{N}$ и $\mathfrak{P}$ являются Ω-группами, и $\mathfrak{P}$ - - нормальный делитель в $\mathfrak{N}$. Известно, что соответствие $x \to \mathfrak{P} + x$ будет гомоморфным отображением A группы $\mathfrak{N}$ на группу $\mathfrak{N}/\mathfrak{P}$. Так как $(\mathfrak{P} + x)\alpha = \mathfrak{P} + x\alpha$, то $A\alpha = \alpha A$, и потому A будет Ω-гомоморфизмом. Предположим теперь, что $\mathfrak{N}$ и $\overline{\mathfrak{N}}$ являются Ω-группами и что задан Ω-гомоморфизм $x \to \overline{x} = xA$ группы $\mathfrak{N}$ на группу $\overline{\mathfrak{N}}$. Если $\mathfrak{P}$ — множество элементов из $\mathfrak{N}$, отображающихся в 0, то $\mathfrak{P}$ будет нормальным делителем в $\mathfrak{N}$, и соответствие $\mathfrak{P} + x \to \overline{x} = xA$ будет изоморфизмом между $\mathfrak{N}/\mathfrak{P}$ и $\overline{\mathfrak{N}}$. Так как $(y\alpha)A = (yA)\alpha = 0\alpha = 0$ при $y \in \mathfrak{P}$, то $\mathfrak{P}$ является Ω-подгруппой, а так как $(\mathfrak{P} + x)\alpha = (\mathfrak{P} + x\alpha) \to (x\alpha)A = (xA)\alpha$, то упомянутый изоморфизм будет Ω-изоморфизмом между $\mathfrak{N}/\mathfrak{P}$ и $\overline{\mathfrak{N}}$. Этим доказана основная теорема о Ω-гомоморфизмах:

Теорема 2. *Если* $\mathfrak{N}$ *и* $\mathfrak{P}$ *являются* Ω-*группами, причем* $\mathfrak{P}$ — *нормальный делитель в* $\mathfrak{N}$, *то* $\mathfrak{N}$ Ω-*гомоморфно отображается на* $\mathfrak{N}/\mathfrak{P}$. *Обратно, если* $\mathfrak{N}$ Ω-*гомоморфно отображается на* Ω-*группу* $\overline{\mathfrak{N}}$ *и* $\mathfrak{P}$ *является множеством элементов, отображающихся в* 0 *при этом*

[1]) Если $\mathfrak{M}_i\,(i = 1, 2)$ будут группами и Ω_i — фиксированными множествами эндоморфизмов, мы можем говорить, что группа $\mathfrak{M}_1$ (Ω_1, Ω_2)-гомоморфно отображается на группу $\mathfrak{M}_2$, если существуют такие однозначные отображения $x_1 \to x_2$ группы $\mathfrak{M}_1$ на всю группу $\mathfrak{M}_2$ и однозначное отображение $\alpha_1 \to \alpha_2$ множества Ω_1 на все множество Ω_2, что $x_1 + y_1 \to x_2 + y_2$, $x_1\alpha_1 \to x_2\alpha_2$, если $x_1 \to x_2$, $y_1 \to y_2$ и $\alpha_1 \to \alpha_2$. Это отличается от определения Ω-гомоморфизма, так как для последнего соответствие отображений вполне определяется исходной группой $\mathfrak{M}$. Для наших целей важно только понятие Ω-гомоморфизма.

гомоморфизме, то $\mathfrak{P}$ *является* Ω-*нормальным делителем в* $\mathfrak{N}$, *и группы* $\overline{\mathfrak{N}}$ *и* $\mathfrak{N}/\mathfrak{P}$ *будут* Ω-*изоморфны.*

Если A является Ω-гомоморфизмом группы $\mathfrak{N}$ на группу $\overline{\mathfrak{N}}$ и $\mathfrak{R}$—Ω-подгруппа в $\mathfrak{N}$, то образ $\mathfrak{R}A$ подгруппы $\mathfrak{R}$ является Ω-подгруппой в $\overline{\mathfrak{N}}$. Если $\mathfrak{R}$ является нормальным делителем в $\mathfrak{N}$, то $\mathfrak{R}A$ будет нормальным делителем в $\mathfrak{R}A = \overline{\mathfrak{R}}$. С другой стороны, если $\overline{\mathfrak{R}}$ какая-либо Ω-подгруппа в $\overline{\mathfrak{N}}$ и $\mathfrak{R}$ — множество таких элементов y из $\mathfrak{N}$, что $yA \in \overline{\mathfrak{R}}$, то $\mathfrak{R}$ будет Ω-подгруппой в $\mathfrak{N}$, содержащей множество $\mathfrak{P}$ элементов, отображающихся в 0 при гомоморфизме A. При этом, если $\overline{\mathfrak{R}}$ будет нормальным делителем, то и $\mathfrak{R}$ также будет нормальным делителем. Если $\mathfrak{R}$ является Ω-подгруппой, содержащей $\mathfrak{P}$, то каждый элемент из $\mathfrak{N}$, отображающийся в элемент $\mathfrak{R}A$, лежит в $\mathfrak{R}$. В самом деле, если $xA = yA$, где $x \in \mathfrak{R}$ и $y \in \mathfrak{R}$, то $(x - y)A = 0$ и $x - y \in \mathfrak{P}$. Следовательно, $x = (x - y) + y \in \mathfrak{R}$. Эти результаты могут быть сформулированы следующим образом:

Теорема 3. *Пусть* A *является* Ω-*гомоморфизмом группы* $\mathfrak{N}$ *на группу* $\overline{\mathfrak{N}}$, *и пусть* $\mathfrak{P}$ — *множество элементов, отображающихся в* 0 *при гомоморфизме* A. *Тогда* $\mathfrak{R} \to \mathfrak{R}A = \overline{\mathfrak{R}}$ *будет взаимнооднозначным соответствием между* Ω-*подгруппами группы* $\mathfrak{N}$, *содержащими* $\mathfrak{P}$, *и* Ω-*подгруппами группы* $\overline{\mathfrak{N}}$. *Группа* $\mathfrak{R}$ *будет нормальным делителем в* $\mathfrak{N}$ *тогда и только тогда, если* $\overline{\mathfrak{R}}$ — *нормальный делитель в* $\overline{\mathfrak{N}}$.

Пусть теперь $\overline{\mathfrak{R}}$ будет Ω-нормальным делителем в $\overline{\mathfrak{N}}$. Если мы применим Ω-гомоморфизм группы $\overline{\mathfrak{N}}$ на группу $\overline{\mathfrak{N}}/\overline{\mathfrak{R}}$ после Ω-гомоморфизма группы $\mathfrak{N}$ на $\overline{\mathfrak{N}}$, мы получим Ω-гомоморфизм группы $\mathfrak{N}$ на группу $\overline{\mathfrak{N}}/\overline{\mathfrak{R}}$. В 0 группы $\overline{\mathfrak{N}}/\overline{\mathfrak{R}}$ будут отображаться элементы из $\mathfrak{R}$. Следовательно, нами получена

Первая теорема об изоморфизме. *Предположим, что* $\mathfrak{N}$ Ω-*гомоморфно отображается на* $\overline{\mathfrak{N}}$, $\overline{\mathfrak{R}}$ *пусть является* Ω-*нормальным делителем в* $\overline{\mathfrak{N}}$, *а* $\mathfrak{R}$ —

совокупностью элементов, отображающихся в $\overline{\mathfrak{R}}$. *Тогда* $\mathfrak{N}/\mathfrak{R}$ и $\overline{\mathfrak{N}}/\overline{\mathfrak{R}}$ *будут* Ω-*изоморфны.*

Очевидно, что отсюда вытекает

Следствие. *Если* $\mathfrak{R}$ *является* Ω-*подгруппой в* $\mathfrak{N}$, *содержащей* Ω-*нормальный делитель* $\mathfrak{P}$ *группы* $\mathfrak{N}$, *и* $\mathfrak{R}/\mathfrak{P}$ — *нормальный делитель в* $\mathfrak{N}/\mathfrak{P}$, *то* $\mathfrak{R}$ *будет нормальным делителем в* $\mathfrak{N}$ *и* $\mathfrak{N}/\mathfrak{R}$ *будет* Ω-*изоморфно группе* $\mathfrak{N}/\mathfrak{P}/\mathfrak{R}/\mathfrak{P}$.

Предположим, что $\mathfrak{N}_1$, $\mathfrak{N}_2$, $\mathfrak{M}_1$ являются Ω-группами, причем $\mathfrak{N}_i \subseteq \mathfrak{M}_1$ и $\mathfrak{N}_2$ — нормальный делитель в $\mathfrak{M}_1$. Тогда наименьшей подгруппой, содержащей $\mathfrak{N}_1$ и $\mathfrak{N}_2$, будет $\mathfrak{N} = \mathfrak{N}_1 + \mathfrak{N}_2 = \mathfrak{N}_2 + \mathfrak{N}_1$.

Группа $\mathfrak{N}_2$ будет нормальным делителем в $\mathfrak{N}$, и смежные классы в фактор-группе $\mathfrak{N}/\mathfrak{N}_2$ имеют вид $\mathfrak{N}_2 + x_1$, где $x_1 \in \mathfrak{N}_1$. Отсюда следует, что соответствие $x_1 \to \mathfrak{N}_2 + x_1$ является Ω-гомоморфизмом группы $\mathfrak{N}_1$ на группу $\mathfrak{N}/\mathfrak{N}_2$. Так как в 0 отображаются элементы из $\mathfrak{N}_1 \cap \mathfrak{N}_2$, то нами получена

Вторая теорема об изоморфизмах. *Если* $\mathfrak{N}_1$, $\mathfrak{N}_2$, $\mathfrak{M}_1$ *являются* Ω-*группами*, $\mathfrak{N}_i \subseteq \mathfrak{M}_1$ *и* $\mathfrak{N}_2$ — *нормальный делитель в* $\mathfrak{M}_1$, *то* 1) $\mathfrak{N}_1 + \mathfrak{N}_2 = \mathfrak{N}_2 + \mathfrak{N}_1$, 2) $\mathfrak{N}_1 \cap \mathfrak{N}_2$ *является нормальным делителем в* $\mathfrak{N}_1$ *и* 3) $\mathfrak{N}_1 + \mathfrak{N}_2/\mathfrak{N}_2$ Ω-*изоморфно группе* $\mathfrak{N}_1/\mathfrak{N}_1 \cap \mathfrak{N}_2$.

4. Теорема Жордана-Гельдера-Шрейера. Конечная цепь Ω-групп $\mathfrak{M}_1 \supseteq \mathfrak{M}_2 \supseteq \ldots \supseteq \mathfrak{M}_{s+1} = 0$ называется *нормальным рядом* в группе $\mathfrak{M}_1$, если каждая $\mathfrak{M}_i$ является нормальным делителем в $\mathfrak{M}_{i-1}$. Фактор-группы $\mathfrak{M}_{i-1}/\mathfrak{M}_i$ называются *факторами* этого ряда; одна цепь называется *уплотнением* другой, если она содержит все $\mathfrak{M}_i$, принадлежащие последней. Мы будем называть два нормальных ряда *изоморфными*, если существует такое взаимооднозначное соответствие между их факторами, что соответствующие факторы Ω-изоморфны.

Теорема 4 (Шрейер). *Любые два нормальных ряда группы* $\mathfrak{M}_1$ *обладают изоморфными уплотнениями.*

Пусть даны два нормальных ряда $\mathfrak{M}_1 \supseteq \ldots \supseteq \mathfrak{M}_{s+1} = 0$ и $\mathfrak{M}_1 = \mathfrak{N}_1 \supseteq \ldots \supseteq \mathfrak{N}_{t+1} = 0$. Положим $\mathfrak{M}_{ij} = \mathfrak{M}_{i+1} + (\mathfrak{M}_i \cap \mathfrak{N}_j)$ при $j = 1, 2, \ldots, t+1$ и $i = 1, 2, \ldots, s$

и $\mathfrak{M}_{s+1,\,1} = 0$. Тогда $\mathfrak{M}_{i,\,t+1} = \mathfrak{M}_{i+1,1}$ и $(\mathfrak{M}_1 =)\,\mathfrak{M}_{11} \supseteq \supseteq \ldots \supseteq \mathfrak{M}_{1t} \supseteq \mathfrak{M}_{21} \supseteq \ldots \supseteq \mathfrak{M}_{2\,t} \supseteq \ldots \supseteq \mathfrak{M}_{s,t} \supseteq 0$. Таким же образом полагаем $\mathfrak{N}_{ij} = \mathfrak{N}_{j+1} + (\mathfrak{N}_j \cap \mathfrak{M}_i)$ при $i = 1, 2, \ldots, s+1$ и $j = 1, 2, \ldots, t$, $\mathfrak{N}_{t+1,1} = 0$, и получаем, что $\mathfrak{N}_{j,\,s+1} = \mathfrak{N}_{j+1,1}$ и $(\mathfrak{N}_1 =)\,\mathfrak{N}_{11} \supseteq \ldots \supseteq \mathfrak{N}_{1s} \supseteq \mathfrak{N}_{21} \supseteq \ldots \supseteq \mathfrak{N}_{2s} \supseteq \ldots \supseteq \mathfrak{N}_{t,s} \supseteq 0$.

При этом каждая цепочка состоит из $st+1$ членов. Поставим $\mathfrak{M}_{ij}/\mathfrak{M}_{i,j+1}$ в соответствие с $\mathfrak{N}_{ji}/\mathfrak{N}_{j,i+1}$.

Тогда наша теорема является следствием леммы:

Лемма Цассенхауза. *Пусть* $\mathfrak{N}_1$, $\mathfrak{N}_1'$, $\mathfrak{N}_2$, $\mathfrak{N}_2'$, $\mathfrak{M}_1$ *являются* Ω-*группами, причем* $\mathfrak{N}_i \subseteq \mathfrak{M}_1$, $\mathfrak{N}_i' \subseteq \mathfrak{N}_i$ *и* $\mathfrak{N}_i'$ *является нормальным делителем в* $\mathfrak{N}_i$. *Тогда* $\mathfrak{N}_1' + (\mathfrak{N}_1 \cap \mathfrak{N}_2')$ *будет нормальным делителем в* $\mathfrak{N}_1 + (\mathfrak{N}_1 \cap \mathfrak{N}_2)$, $\mathfrak{N}_2' + (\mathfrak{N}_2 \cap \mathfrak{N}_1')$ *будет нормальным делителем в* $\mathfrak{N}_2' + (\mathfrak{N}_2 \cap \mathfrak{N}_1)$ *и соответствующие фактор-группы* Ω-*изоморфны.*

По второй теореме об изоморфизмах $\mathfrak{N}_2 \cap \mathfrak{N}_1' = (\mathfrak{N}_2 \cap \mathfrak{N}_1) \cap \mathfrak{N}_1'$ будет нормальным делителем в $\mathfrak{N}_1 \cap \mathfrak{N}_2$, а $\mathfrak{N}_1 \cap \mathfrak{N}_2/\mathfrak{N}_1' \cap \mathfrak{N}_2$ и $\mathfrak{N}_1' + (\mathfrak{N}_1 \cap \mathfrak{N}_2)/\mathfrak{N}_1'$ будут Ω-изоморфны. Таким же образом получаем, что $\mathfrak{N}_1 \cap \mathfrak{N}_2'$, а, следовательно, и $(\mathfrak{N}_1' \cap \mathfrak{N}_2) + (\mathfrak{N}_1 \cap \mathfrak{N}_2')$ также будут нормальными делителями в $\mathfrak{N}_1 \cap \mathfrak{N}_2$. При гомоморфном отображении группы $\mathfrak{N}_1 \cap \mathfrak{N}_2$ в $\mathfrak{N}_1' + (\mathfrak{N}_1 \cap \mathfrak{N}_2)/\mathfrak{N}_1'$ группа $(\mathfrak{N}_1' \cap \mathfrak{N}_2) + (\mathfrak{N}_1 \cap \mathfrak{N}_2')$ отображается в $(\mathfrak{N}_1' \cap \mathfrak{N}_2) + (\mathfrak{N}_1 \cap \mathfrak{N}_2') + \mathfrak{N}_1'/\mathfrak{N}_1' = (\mathfrak{N}_1 \cap \mathfrak{N}_2') + \mathfrak{N}_1'/\mathfrak{N}_1'$. Следовательно, по вышеприведенному следствию, $(\mathfrak{N}_1 \cap \mathfrak{N}_2') + \mathfrak{N}_1'$ будет нормальным делителем в $(\mathfrak{N}_1 \cap \mathfrak{N}_2) + \mathfrak{N}_1'$, а $\mathfrak{N}_1' + (\mathfrak{N}_1 \cap \mathfrak{N}_2)/\mathfrak{N}_1' + (\mathfrak{N}_1 \cap \mathfrak{N}_2')$ и $\mathfrak{N}_1 \cap \mathfrak{N}_2/(\mathfrak{N}_1 \cap \mathfrak{N}_2') + (\mathfrak{N}_1' \cap \mathfrak{N}_2)$ будут Ω-изоморфны.

По симметрии группа $\mathfrak{N}_1 \cap \mathfrak{N}_2/(\mathfrak{N}_1 \cap \mathfrak{N}_2') + (\mathfrak{N}_1' \cap \mathfrak{N}_2)$ Ω-изоморфна группе $\mathfrak{N}_2' + (\mathfrak{N}_1 \cap \mathfrak{N}_2)/\mathfrak{N}_2' + (\mathfrak{N}_2 \cap \mathfrak{N}_1')$.

Сравнивая вторые члены этих изоморфных пар, мы видим, что лемма доказана.

5. Условия обрыва цепей. Мы будем иногда предполагать, что в Ω-группе $\mathfrak{N}$ выполнено одно из следующих двух условий конечности:

Условие обрыва убывающих цепей. Если $\mathfrak{N} = \mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \supset \ldots$, где $\mathfrak{N}_i$ является Ω-нормальным делителем

в $\mathfrak{N}_{i-1}$, то эта последовательность может иметь лишь конечное число различных членов.

Условие обрыва возрастающих цепей. Если $\mathfrak{N} = \mathfrak{N}_1 \supset \supset \ldots \supset \mathfrak{N}_k = \mathfrak{P} \supset 0$ будет нормальным рядом в группе $\mathfrak{N}$, то всякая цепь Ω-подгрупп $0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2 \subset \ldots$, каждая из которых будет нормальным делителем в $\mathfrak{P}$, конечна.

Разумеется, оба эти условия выполнены, если группа $\mathfrak{N}$ конечна. С другой стороны, мы увидим, что эти условия могут быть использованы для замены предположения о конечности порядка при перенесении некоторых классических теорем о конечных группах на бесконечные Ω-группы. Следующие примеры показывают независимость наших условий.

Примеры. 1) *Аддитивная группа целых чисел.* Эта группа удовлетворяет условию обрыва возрастающих цепей, но не удовлетворяет условию обрыва убывающих цепей. Это справедливо также и для прямой суммы конечного числа бесконечных циклических групп (см. главу 3, § 3).

2) *Прямая сумма $\mathfrak{M}$ бесконечного числа циклических групп простого порядка p* [1]). Пусть элементы $x_1, x_2, \ldots$ образуют базис группы $\mathfrak{M}$ и пусть A будет эндоморфизмом, определенным равенствами $x_1 A = 0$, $x_i A = x_{i-1}$. Тогда группа $\mathfrak{M}$ удовлетворяет условию обрыва убывающих цепей относительно $\Omega = \{A\}$, но не удовлетворяет условию обрыва возрастающих цепей. Другим примером может служить группа, заданная образующими элементами $x_1, x_2, \ldots$ и соотношениями $px_1 = 0$, $px_i = x_{i-1}$. Здесь мы считаем, что множество Ω пусто.

Следует отметить, что если группа $\mathfrak{N}$ коммутативна, то условие обрыва возрастающих цепей может быть выражено в более простой форме: каждая цепь $0 \subset \mathfrak{P}_1 \subset \mathfrak{P}_2 \subset \ldots$ Ω-подгрупп имеет конечную длину. Если одно из условий обрыва цепей выполнено в (произвольной) группе $\mathfrak{N}$, то оно выполнено в каждом Ω-нормальном делителе $\mathfrak{P}$

[1]) Отметим, что относительно пустого множества эндоморфизмов эта группа не удовлетворяет ни одному из условий обрыва цепей.

и в каждой фактор-группе $\mathfrak{N}/\mathfrak{P}$. Если выполнены оба условия обрыва цепей, то $\mathfrak{N}$ обладает *композиционным рядом*, т. е. нормальным рядом $\mathfrak{N} = \mathfrak{N}_1 \supset \ldots \supset \mathfrak{N}_h \supset 0$, не имеющим собственного уплотнения. Заметим, что нормальный ряд является композиционным рядом, если все факторгруппы $\mathfrak{N}_{i-1}/\mathfrak{N}_i$ Ω-*простые*, т. е. не имеют собственных Ω-нормальных делителей. Для доказательства нашего утверждения предположим, что $\mathfrak{N}'$ является собственным Ω-нормальным делителем в $\mathfrak{N}$. Если $\mathfrak{N}/\mathfrak{N}'$ непростая группа, то существует такой нормальный делитель $\mathfrak{N}''$ в $\mathfrak{N}$, что $\mathfrak{N} \supset \mathfrak{N}'' \supset \mathfrak{N}' \supset 0$. Продолжая таким образом, мы получим после конечного числа шагов такой Ω-нормальный делитель $\mathfrak{N}_2$ группы $\mathfrak{N} = \mathfrak{N}_1$, что $\mathfrak{N}_1/\mathfrak{N}_2$ будет Ω-простой группой. Повторяя этот процесс для группы $\mathfrak{N}_2$, мы получим $\mathfrak{N}_3$ и т. д. Таким образом, мы будем иметь нормальный ряд $\mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \ldots$, который, в силу условия обрыва убывающих цепей, оборвется после конечного числа шагов и даст композиционный ряд для группы $\mathfrak{N}$.

Если Ω является множеством внутренних автоморфизмов, то композиционные *ряды для $\mathfrak{N}$ называются главными* рядами, а если Ω является множеством всех автоморфизмов, мы получаем *характеристические* ряды. Следующее обобщение теоремы Жордана-Гельдера показывает, в частности, единственность (с точностью до изоморфизма) факторов как у этих, так и у обычных композиционных рядов, для которых Ω пусто.

Теорема 5. *Каждые два композиционных ряда Ω-группы $\mathfrak{N}$ изоморфны.*

Доказательство непосредственно следует из теоремы Шрейера.

Теорема 6. *Для того, чтобы Ω-группа обладала композиционным рядом, необходимо и достаточно, чтобы в ней были выполнены оба условия обрыва цепей.*

Достаточность этих условий уже была доказана. Предположим теперь, что $\mathfrak{N}$ обладает композиционным рядом из h членов. Если $\mathfrak{N} = \mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \ldots$ является убывающей цепью Ω-подгрупп, то она имеет не более h членов, так как $\mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \ldots \supset \mathfrak{N}_k \supset 0$ является нормальной цепью

и может быть уплотнена в композиционный ряд, обладающий h членами. Аналогичные рассуждения применимы и к возрастающей цепи.

Если $\mathfrak{N}_1 \supset \ldots \supset \mathfrak{N}_h \supset 0$ является композиционным рядом для $\mathfrak{N}_1$, то h называется *длиной* группы $\mathfrak{N}_1$. Следовательно, группа Ω-проста тогда и только тогда, когда она имеет длину один.

Если $\mathfrak{N}'$ является Ω-нормальным делителем в $\mathfrak{N}_1$, мы можем предположить, что $\mathfrak{N}'$ — некоторый член композиционного ряда группы $\mathfrak{N}_1$, например, $\mathfrak{N}_{k+1}$. Тогда $\mathfrak{N}_{k+1}$ имеет длину $h-k$. По первой теореме об изоморфизме последовательность $\mathfrak{N}_1/\mathfrak{N}_{k+1} \supset \ldots \supset \mathfrak{N}_k/\mathfrak{N}_{k+1} \supset 0$ является композиционным рядом для $\mathfrak{N}_1/\mathfrak{N}_{k+1}$, и потому эта фактор-группа имеет длину k. Ω-эндоморфизм A группы $\mathfrak{N}$ называется *нормальным*, если он коммутирует со всеми внутренними автоморфизмами группы $\mathfrak{N}$. Тогда для любых a и x имеем: $-aA+xA+aA=-a+xA+a$. Таким образом, $aA=a+c(a)$, где $c(a)$ — элемент, коммутирующий с каждым элементом из $\mathfrak{N}A$. Если $\mathfrak{P}$ является Ω-нормальным делителем, то $\mathfrak{P}A$ при любом нормальном эндоморфизме A будет нормальным делителем в $\mathfrak{N}$. Отметим еще, что произведение нормальных эндоморфизмов также является нормальным эндоморфизмом.

Если A какой-либо Ω-эндоморфизм, то совокупность $\mathfrak{Z}_A$ таких элементов z, что $zA=0$, образует Ω-подгруппу. Очевидно, что $0 \subseteq \mathfrak{Z}_A \subseteq \mathfrak{Z}_{A^2} \subseteq \ldots$. Если $\mathfrak{Z}_{A^k} = \mathfrak{Z}_{A^{k+1}}$, то $\mathfrak{Z}_{A^{k+1}} = \mathfrak{Z}_{A^{k+2}} = \ldots$. Таким образом, в цепи $0 \subseteq \mathfrak{Z}_A \subseteq \mathfrak{Z}_{A^2} \subseteq \ldots$ мы либо все время имеем знак $\subset$, либо этот знак стоит перед $k\,(\geqslant 0)$ членами, а далее стоят знаки равенства. Предположим теперь, что $\mathfrak{N}A=\mathfrak{N}$ и $\mathfrak{Z}_A \neq 0$. Тогда $\mathfrak{Z}_{A^2} \supset \mathfrak{Z}_A$. Действительно, каждый элемент z из $\mathfrak{Z}_A$ имеет вид xA при некотором $x \in \mathfrak{N}$, и потому $zA = xA^2 = 0$. Следовательно, если $\mathfrak{Z}_{A^2} = \mathfrak{Z}_A$, то $xA=0$, т. е. каждое $z=0$. Таким же образом мы получим, что $0 \subset \mathfrak{Z}_A \subset \mathfrak{Z}_{A^2} \subset \ldots$. Итак, нами доказана

Теорема 7. *Если $\mathfrak{N}$ удовлетворяет условию обрыва возрастающих цепей, и если A — такой эндоморфизм, что $\mathfrak{N}A=\mathfrak{N}$, то $\mathfrak{Z}_A=0$.*

Если A является нормальным эндоморфизмом, то цепь $\mathfrak{N} \supseteq \mathfrak{N}A \supseteq \mathfrak{N}A^2 \supseteq \ldots$ будет нормальной цепью. Мы имеем либо $\mathfrak{N} \supset \mathfrak{N}A \supset \cdots$, либо $\mathfrak{N} \supset \mathfrak{N}A \supset \ldots \supset \mathfrak{N}A^k = \mathfrak{N}A^{k+1} = \ldots$. Первая из этих возможностей выполняется всегда при $\mathfrak{Z}_A=0$ и $\mathfrak{N} \supset \mathfrak{N}A$. В самом деле, если $\mathfrak{N}A^k = \mathfrak{N}A^{k+1}$, то $xA^{k+1} = yA^k$ для любого x и соответствующего y. Следовательно, $(xA^k - yA^{k-1})\,A=0$ и $xA^k = yA^{k-1}$, т. е. $\mathfrak{N}A^{k-1} = \mathfrak{N}A^k$. Таким образом, нами получена

Теорема 8. *Если в $\mathfrak{N}$ выполнено условие обрыва убывающих цепей и если A является таким нормальным эндоморфизмом, что $\mathfrak{Z}_A=0$, то $\mathfrak{N}=\mathfrak{N}A$.*

Комбинируя обе предыдущие теоремы, получаем:

Теорема 9. *Если в $\mathfrak{N}$ выполнены оба условия обрыва цепей и если A является Ω-нормальным эндоморфизмом, то либо A является автоморфизмом, либо $\mathfrak{N}A \subset \mathfrak{N}$ и $\mathfrak{Z}_A \neq 0$.*

Предположим снова, что в $\mathfrak{N}$ выполнено условие обрыва возрастающих цепей. Тогда для некоторого конечного k имеем $0 \subset \mathfrak{Z}_A \subset \ldots \subset \mathfrak{Z}_{A^k} = \mathfrak{Z}_{A^{k+1}} = \ldots$. Отсюда следует, что $\mathfrak{Z}_{A^k} \cap \mathfrak{N}A^k = 0$. В самом деле, если w лежит в этом пересечении, то $w = xA^k$ и $wA^k = 0$. Следовательно, $xA^{2k}=0$, и, так как $\mathfrak{Z}_{A^k} = \mathfrak{Z}_{A^{2k}}$, то $xA^k = w = 0$. Так как $\mathfrak{N}A^{k+1} \subseteq \mathfrak{N}A^k$, то A индуцирует в $\mathfrak{P} = \mathfrak{N}A^k$ Ω-эндоморфизм, а так как в $\mathfrak{P}$ нет таких отличных от нуля элементов z, что $zA=0$, то A будет изоморфизмом между $\mathfrak{P}$ и $\mathfrak{P}A$. Следовательно, если D является любым таким отображением в $\mathfrak{P}$, что $DA=0$, то $D=0$. Очевидно, что A индуцирует нильпотентный эндоморфизм ($A^k=0$) в $\mathfrak{Z}_{A^k}$.

Если A — нормальный эндоморфизм и в $\mathfrak{N}$ выполнено условие обрыва убывающих цепей, то $\mathfrak{N} \supset \ldots \supset \mathfrak{N}A^l = \mathfrak{N}A^{l+1} = \ldots$ Если x является любым элементом из $\mathfrak{N}$, то для некоторого y имеем $xA^l = yA^{2l}$, и потому

$$x = yA^l + (-yA^l + x) = x - yA^l + yA^l \in \mathfrak{N}A^l + \mathfrak{Z}_{A^l} = \mathfrak{Z}_{A^l} + \mathfrak{N}A^l.$$

Отображение, которое A индуцирует в $\mathfrak{Z}_{A^l}$, нильпотентно. Если D — любое такое преобразование в $\mathfrak{N}A^l$, что $AD=0$, где A — эндоморфизм, индуцированный в $\mathfrak{N}A^l$, то $D=0$.

Если в $\mathfrak{N}$ выполнены оба условия обрыва цепей, то целые числа k и l последних двух абзацев равны между собой. В самом деле, $\mathfrak{N}A^k \cap \mathfrak{Z}_A{}^k = 0$ и, следовательно, каждый элемент из $\mathfrak{N}A^k$, отображаемый в 0 эндоморфизмом A, равен нулю. Отсюда следует, что $\mathfrak{N}A^k = \mathfrak{N}A^{k+1}$, и потому $l \leqslant k$. С другой стороны, из $\mathfrak{N}A^l = (\mathfrak{N}A^l)A$ вытекает, что $\mathfrak{N}A^l \cap \mathfrak{Z}_A = 0$. Таким образом, если $yA^{l+1} = (yA^{l+1})A = 0$, то $yA^l = 0$, а потому $\mathfrak{Z}_{A^{l+1}} = \mathfrak{Z}_{A^l}$ и $k \leqslant l$. Итак, мы доказали важную лемму:

Лемма (Фиттинг). *Пусть в $\mathfrak{N}$ выполнены оба условия обрыва цепей и A является нормальным Ω-эндоморфизмом. Тогда для некоторого k мы имеем $\mathfrak{N} = \mathfrak{N}A^k + \mathfrak{Z}_A{}^k$, $\mathfrak{N}A^k \cap \mathfrak{Z}_{A^k} = 0$, причем эндоморфизм A нильпотентен в $\mathfrak{Z}_A{}^k$ и является автоморфизмом в $\mathfrak{N}A^k$.*

Замечание. Мы могли не предполагать в предыдущем рассуждении, что A является Ω-эндоморфизмом. Вместо этого предположим, что Ω содержит внутренние автоморфизмы, и пусть A удовлетворяет условию $A\Omega = \Omega A$, т. е. для каждого $\alpha \in \Omega$ найдутся $\alpha' \in \Omega$ и $\alpha'' \in \Omega$, такие, что $A\alpha = \alpha' A$ и $\alpha A = A\alpha''$. Так как Ω содержит внутренние автоморфизмы, то Ω-подгруппы являются нормальными делителями. Группы $\mathfrak{N}A$ и $\mathfrak{Z}_A$ будут Ω-подгруппами, и можно провести без изменений предыдущие рассуждения. Тем не менее, мы дадим эскиз более прямого доказательства последнего результата. Рассмотрим цепи $\mathfrak{N} \supseteq \mathfrak{N}A \supseteq \ldots$ и $0 \subseteq \mathfrak{Z}_A \subseteq \ldots$ Члены этих цепей являются Ω-подгруппами и потому, в силу условий обрыва цепей, найдется такое целое m, что $\mathfrak{N}A^m = \mathfrak{N}A^{m+1} = \ldots$ и $\mathfrak{Z}_{A^m} = \mathfrak{Z}_{A^{m+1}} = \ldots$ Положим $A^m = B$. Тогда $\mathfrak{N}B = \mathfrak{N}B^2$, $\mathfrak{Z}_B = \mathfrak{Z}_{B^2}$ и, следовательно, в силу условий обрыва цепей, $\mathfrak{N}B \cap \mathfrak{Z}_B = 0$.

Если x — произвольный элемент в $\mathfrak{N}$, то для некоторого y имеем $xB^2 = yB$, и потому

$$x = yB + (-yB + x) \in \mathfrak{N}B + \mathfrak{Z}_B.$$

6. Прямые суммы. В дальнейшем, на протяжении всей этой главы, мы будем предполагать, что Ω содержит все внутренние автоморфизмы группы $\mathfrak{N}$. Мы также будем предполагать, что в $\mathfrak{N}$ выполнены оба условия обрыва цепей. Из первого условия следует, что каждая Ω-подгруппа является нормальным делителем и что все Ω-эндоморфизмы нормальны. Условие обрыва возрастающих цепей может быть выражено поэтому в более простой форме: Каждая возрастающая цепь $0 \subset \mathfrak{N}_1 \subset \mathfrak{N}_2 \subset \ldots$ Ω-подгрупп $\mathfrak{N}_i$ обрывается после конечного числа членов.

Мы назовем $\mathfrak{N}$ *прямой суммой* Ω-подгрупп $\mathfrak{N}_i$, $i = 1, 2, \ldots, h$, если

$$\mathfrak{N} = \mathfrak{N}_1 + \mathfrak{N}_2 + \ldots + \mathfrak{N}_h$$

и

$$\mathfrak{N}_i \cap (\mathfrak{N}_1 + \mathfrak{N}_2 + \ldots + \mathfrak{N}_{i-1} + \mathfrak{N}_{i+1} + \ldots + \mathfrak{N}_h) = 0$$

для всех i. Разложение называется *собственным*, если все $\mathfrak{N}_i \neq 0$. Если не существует собственных разложений, отличных от $\mathfrak{N} = \mathfrak{N}$, то группа $\mathfrak{N}$ называется *неразложимой*. Для прямой суммы мы будем употреблять обозначение $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$. Так как $\mathfrak{N}_i$ являются нормальными делителями, то $\mathfrak{N}_i + \mathfrak{N}_j = \mathfrak{N}_j + \mathfrak{N}_i$, и мы можем также писать: $\mathfrak{N} = \mathfrak{N}_{1'} \oplus \ldots \oplus \mathfrak{N}_{h'}$ для любой перестановки $1', \ldots, h'$ индексов $1, \ldots, h$. Если $a \in \mathfrak{N}_i$ и $b \in \mathfrak{N}_j$, $j \neq i$, то коммутатор $-a-b+a+b \in \mathfrak{N}_i \cap \mathfrak{N}_j = 0$. Следовательно, $a+b = b+a$, и любой элемент из $\mathfrak{N}_i$ коммутирует с любым элементом из $\mathfrak{N}_j$.

Для того, чтобы $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$, где $\mathfrak{N}_i$ являются Ω-подгруппами, необходимо и достаточно, чтобы любой элемент x из $\mathfrak{N}$ мог быть единственным образом выражен в виде $x_1 + \ldots + x_h$, где $x_i \in \mathfrak{N}_i$. Отсюда непосредственно следует, что если $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$, то $\mathfrak{N}_1' = \mathfrak{N}_1 + \ldots + \mathfrak{N}_{k_1} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_{k_1}$, и если $\mathfrak{N}_2' = \mathfrak{N}_{k_1+1} + \ldots + \mathfrak{N}_{k_1+k_2}$, $\ldots$, $\mathfrak{N}_l' = \mathfrak{N}_{k_1+\ldots+k_{l-1}+1} + \ldots + \mathfrak{N}_{k_1+\ldots+k_l}$, то $\mathfrak{N} = \mathfrak{N}_1' \oplus \ldots \oplus \mathfrak{N}_l'$. Обратно, если $\mathfrak{N} = \mathfrak{N}'_1 \oplus \ldots \oplus \mathfrak{N}'_l$ и

$$\mathfrak{N}'_1 = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_{k_1}, \ldots, \mathfrak{N}_l' = \mathfrak{N}_{k_1+\ldots+k_{l-1}+1} \oplus \ldots \oplus \mathfrak{N}_{k_1+\ldots+k_l},$$

то

$$\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h, \quad h = k_1 + \ldots + k_l.$$

Если $\mathfrak{N} = \mathfrak{N}_1 \oplus \mathfrak{N}_2$, то из второй теоремы об изоморфизмах следует, что группа $\mathfrak{N}_2$ Ω-изоморфна $\mathfrak{N}/\mathfrak{N}_1$. Очевидно, что длина $\mathfrak{N}$ равна сумме длин $\mathfrak{N}_1$ и $\mathfrak{N}_2$. Если $\mathfrak{N}_1$ и $\mathfrak{N}_2$ являются такими Ω-подгруппами в $\mathfrak{N}$, что $\mathfrak{N} = \mathfrak{N}_1 + \mathfrak{N}_2$, и $\mathfrak{N}_3 = \mathfrak{N}_1 \cap \mathfrak{N}_2$, то $\mathfrak{N}/\mathfrak{N}_3 = (\mathfrak{N}_1/\mathfrak{N}_3) \oplus (\mathfrak{N}_2/\mathfrak{N}_3)$. Отсюда следует, что

$$\text{длина } \mathfrak{N} + \text{длина } (\mathfrak{N}_1 \cap \mathfrak{N}_2) = \text{длина } \mathfrak{N}_1 + \text{длина } \mathfrak{N}_2.$$

Мы можем, конечно, заменить $\mathfrak{N}$ через $\mathfrak{N}_1 + \mathfrak{N}_2$ и получить это соотношение для любых Ω-подгрупп в $\mathfrak{N}$.

Если $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$, так что для каждого x мы имеем $x = x_1 + \ldots + x_h$, где $x_i \in \mathfrak{N}_i$, то при помощи равенства $xE_i = x_i$ определяется отображение E_i. Так как x разлагается единственным образом, то отображение E_i однозначно. Если $y = y_1 + \ldots + y_h$, то $x + y = (x_1 + y_1) + \ldots + (x_h + y_h)$. Следовательно, $(x + y)\, E_i = xE_i + yE_i$. Если $\alpha \in \Omega$, то $x\alpha = x_1\alpha + \ldots + x_n\alpha$, так что $\alpha E_i = E_i\alpha$. E_i является, таким образом, Ω-эндоморфизмом. Очевидно, имеют место следующие соотношения:

$$E_i^2 = E_i, \quad E_iE_j = 0 \text{ при } i \neq j, \quad E_1 + \ldots + E_h = 1. \quad (1)$$

Отметим, что $E_i + E_j = E_j + E_i$ и что частичная сумма $E_{i_1} + \ldots + E_{i_n}$ также является эндоморфизмом.

Идемпотентный Ω-эндоморфизм E ($E^2 = E$) мы будем называть *проекцией*. Эндоморфизмы E_i, соответствующие прямому разложению, являются проекциями. Предположим, обратно, что E_i являются произвольными проекциями, удовлетворяющими соотношениям (1). Тогда $\mathfrak{N}E_i = \mathfrak{N}_i$ будут такими Ω-подгруппами, что $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$ и E_i будут проекциями, соответствующими этому разложению. Кроме того, если E является произвольной проекцией, а Z_E — множеством таких элементов z, что $zE = 0$, то, по лемме Фиттинга или непосредственным рассуждением, мы получаем, что $\mathfrak{N} = \mathfrak{N}E \oplus \mathfrak{Z}_E$. Следовательно, существует такая проекция E', что $E + E' = E' + E = 1$, $EE' = E'E = 0$.

Мы будем называть идемпотентный элемент E произвольного кольца *примитивным*, если его невозможно представить в виде $E = E' + E''$, где E' и E'' являются идемпотентными не равными нулю элементами, и $E'E'' = E''E' = 0$. Таким образом, группа $\mathfrak{N}$ неразложима тогда и только тогда, когда 1 является примитивной проекцией.

По лемме Фиттинга мы получаем:

Теорема 10. *Пусть $\mathfrak{N}$ — Ω-группа, причем Ω содержит все внутренние автоморфизмы группы $\mathfrak{N}$ и в $\mathfrak{N}$ выполнены оба условия обрыва цепей. Если $\mathfrak{N}$ неразложима, то любой Ω-эндоморфизм либо нильпотентен, либо является автоморфизмом.*

7. Теорема Крулля-Шмидта. Предположим, что группа $\mathfrak{N}$ разложима, т. е. что $\mathfrak{N} = \mathfrak{N}_1 \oplus \mathfrak{N}_2$, где $\mathfrak{N}_i \neq 0$. Если $\mathfrak{N}_1$ разложима: $\mathfrak{N}_1 = \mathfrak{N}_{11} \oplus \mathfrak{N}_{12}$, то $\mathfrak{N} = \mathfrak{N}_{11} \oplus \mathfrak{N}_{12} \oplus \mathfrak{N}_2$. Итак, $\mathfrak{N} \supset \mathfrak{N}_1 \supset \mathfrak{N}_{11} \neq 0$ и, продолжая подобным образом, мы получим такую неразложимую подгруппу $\mathfrak{N}_{1\ldots1}$, что $\mathfrak{N} = \mathfrak{N}_{1\ldots1} \oplus \mathfrak{N}_{1\ldots1}'$. Для упрощения обозначений напишем $\mathfrak{N} = \mathfrak{N}_1 \oplus \mathfrak{N}_1'$, где группа $\mathfrak{N}_1$ неразложима и не равна нулю. Если $\mathfrak{N}_1'$ разложима, то мы получаем: $\mathfrak{N}_1' = \mathfrak{N}_2 \oplus \mathfrak{N}_2'$, где $\mathfrak{N}_2$ неразложима и не равна нулю. Тогда $\mathfrak{N} = \mathfrak{N}_1 \oplus \mathfrak{N}_2 \oplus \mathfrak{N}_2'$. Этот процесс приводит к убывающей цепи подгрупп $\mathfrak{N}_1' \supset \mathfrak{N}_2' \supset \ldots$ Следовательно, он обрывается, и мы получаем $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$, где подгруппы $\mathfrak{N}_i$ неразложимы и не равны нулю.

Предположим теперь, что $\mathfrak{N} = \mathfrak{P}_1 \oplus \ldots \oplus \mathfrak{P}_k$ является вторым разложением, причем Ω-подгруппы $\mathfrak{P}_j$ неразложимы и не равны 0. Пусть E_i и F_j являются проекциями, соответствующими этим разложениям. Так как любая сумма вида $E_{i_1} + \ldots + E_{i_n}$, где все i_m различны, является эндоморфизмом, то, каков бы ни был эндоморфизм A, $AE_{i_1} + \ldots + AE_{i_n} = A(E_{i_1} + \ldots + E_{i_n})$ и $E_{i_1}A + \ldots + E_{i_n}A = (E_{i_1} + \ldots + E_{i_n})A$ являются также эндоморфизмами. Если мы применим эндоморфизм F_jE_1 к подгруппе $\mathfrak{N}_1$, то мы получим эндоморфизм этой группы, причем единичным эндоморфизмом в $\mathfrak{N}_1$ будет $E_1 = F_1E_1 + \ldots + F_kE_1$. Мы хотим показать, что хотя бы один из эндо-

морфизмов F_iE_1 является автоморфизмом в $\mathfrak{N}_1$. Это вытекает из следующей леммы.

Лемма. *Пусть $\mathfrak{N}$ является Ω-группой, причем Ω содержит все внутренние автоморфизмы группы $\mathfrak{N}$, и в группе $\mathfrak{N}$ выполнены оба условия обрыва цепей. Если группа $\mathfrak{N}$ неразложима, а A и B являются такими Ω-эндоморфизмами, что $A+B=1$, то либо A, либо B является автоморфизмом.*

Так как $A+B=1$ и A и B — эндоморфизмы, то $A^2+AB=A^2+BA$ и, следовательно, $AB=BA$. Если ни A, ни B не являются автоморфизмами, то оба они нильпотентны. Тогда $1=(A+B)^m$ будет суммой членов вида A^rB^s, где $r+s=m$. Для достаточо большого m либо $A^r=0$, либо $B^s=0$ и, следовательно, $1=0$, т. е. мы приходим к противоречию.

Применим эту лемму к эндоморфизмам $F_1E_1=A$ и $F_2E_1+\ldots+F_kE_1=B$, действующим в $\mathfrak{N}_1$. Если F_1E_1 не является автоморфизмом, то B является им и, следовательно, существует B^{-1}. Но тогда $F_2E_1B^{-1}+\ldots+F_kE_1B^{-1}=1$. Поэтому либо $F_2E_1B^{-1}$, либо $F_3E_1B^{-1}+\ldots+F_kE_1B^{-1}$ является автоморфизмом. Продолжая таким образом, мы получим, наконец, что для некоторого j $F_jE_1B^{-1}C^{-1}\ldots G^{-1}$ является автоморфизмом. Но так как B^{-1}, C^{-1}, ... — автоморфизмы в группе $\mathfrak{N}_1$, то отсюда следует, что F_jE_1 также является автоморфизмом в $\mathfrak{N}_1$. Для простоты предположим, что $j=1$.

Рассмотрим Ω-гомоморфное отображение F_1 группы $\mathfrak{N}_1$ в $\mathfrak{N}_1F_1\subseteq\mathfrak{P}_1$. Так как F_1E_1 — автоморфизм, то F_1 будет изоморфизмом. Итак, $\mathfrak{N}_1F_1$ является Ω-подгруппой в $\mathfrak{P}_1$ так же, как и подмножество $\overline{\mathfrak{P}}_1$ таких элементов $z\in\mathfrak{P}_1$, что $zE_1=0$. Если y является любым элементом из $\mathfrak{P}_1$, то $yE_1=wF_1E_1$ для некоторого $w\in\mathfrak{N}_1$. Следовательно, $y=(y-w)F_1+wF_1$, где $y-wF_1\in\overline{\mathfrak{P}}_1$. Так как $\overline{\mathfrak{P}}_1\cap\mathfrak{N}_1F_1=0$, то в силу неразложимости $\mathfrak{P}_1$, имеем $\overline{\mathfrak{P}}_1=0$ и $\mathfrak{N}_1F_1=\mathfrak{P}_1$. Таким образом $\mathfrak{N}_1F_1=\mathfrak{P}_1$ и, следовательно, F_1 является изоморфизмом между $\mathfrak{N}_1$ и $\mathfrak{P}_1$, а E_1 — изоморфизмом между $\mathfrak{P}_1$ и $\mathfrak{N}_1$. Покажем, что $H_1=E_1F_1+E_2+\ldots+E_h$ является Ω-эндоморфизмом.

Это вытекает из следующего общего замечания: Предположим, что $\mathfrak{N}=\mathfrak{N}_1\oplus\ldots\oplus\mathfrak{N}_h$ и что $\mathfrak{N}'=\mathfrak{N}_1'\oplus\ldots\oplus\mathfrak{N}_h'$ является Ω-подгруппой группы $\mathfrak{N}$. Если A_i — Ω-гомоморфизм группы $\mathfrak{N}_i$ на группу $\mathfrak{N}_i'$, то $E_1A_1+\ldots+E_hA_h$ будет Ω-эндоморфизмом в группе $\mathfrak{N}$. Зная, что $\mathfrak{P}_1\cap(\mathfrak{N}_2+\ldots+\mathfrak{N}_h)=0$, а, следовательно, $\mathfrak{N}'=\mathfrak{P}_1+\mathfrak{N}_2+\ldots+\mathfrak{N}_h=\mathfrak{P}_1\oplus\mathfrak{N}_2\oplus\ldots\oplus\mathfrak{N}_h$, мы получаем требуемый результат. Так как $zH_1=0$ влечет за собой $z=0$, то H_1 является автоморфизмом, т. е. $\mathfrak{N}'=\mathfrak{N}$.

Предположим теперь, что мы уже получили такое соответствие между $\mathfrak{P}_i$ и $\mathfrak{N}_i$ для $i=1, 2, \ldots, r$, что E_i является Ω-изоморфизмом между $\mathfrak{P}_i$ и $\mathfrak{N}_i$, а F_i является Ω-изоморфизмом между $\mathfrak{N}_i$ и $\mathfrak{P}_i$. Предположим также, что $\mathfrak{N}=\mathfrak{P}_1\oplus\ldots\oplus\mathfrak{P}_r\oplus\mathfrak{N}_{r+1}\oplus\ldots\oplus\mathfrak{N}_h$ и что $H_r=E_1F_1+\ldots+E_rF_r+E_{r+1}+\ldots+E_h$ является автоморфизмом. Так как внутренние автоморфизмы факторгруппы индуцируются внутренними автоморфизмами самой группы, то $\overline{\mathfrak{N}}=\mathfrak{N}/(\mathfrak{P}_1+\ldots+\mathfrak{P}_r)$ также удовлетворяет нашим условиям, и мы получаем, что

$$\overline{\mathfrak{N}}=\overline{\mathfrak{N}}_{r+1}\oplus\ldots\oplus\overline{\mathfrak{N}}_h=\overline{\mathfrak{P}}_{r+1}\oplus\ldots\oplus\overline{\mathfrak{P}}_k,$$

где группы $\overline{\mathfrak{N}}_l=(\mathfrak{P}_1+\ldots+\mathfrak{P}_r+\mathfrak{N}_l)/(\mathfrak{P}_1+\ldots+\mathfrak{P}_r)$ и $\overline{\mathfrak{P}}_j=(\mathfrak{P}_1+\ldots+\mathfrak{P}_r+\mathfrak{P}_j)/(\mathfrak{P}_1+\ldots+\mathfrak{P}_r)$ Ω-изоморфны соответственно группам $\mathfrak{N}_l$ и $\mathfrak{P}_j$. При помощи вышеприведенного рассуждения мы можем сопоставить $\overline{\mathfrak{P}}_{r+1}$, например, с $\overline{\mathfrak{N}}_{r+1}$, так, что соответствующие проекции $\bar{E}_{r+1}$ и $\bar{F}_{r+1}$ будут являться изоморфизмами между $\overline{\mathfrak{P}}_{r+1}$ и $\overline{\mathfrak{N}}_{r+1}$. Мы получили, таким образом, равенство $\mathfrak{N}=\overline{\mathfrak{P}}_{r+1}\oplus\overline{\mathfrak{N}}_{r+2}\oplus\ldots\oplus\overline{\mathfrak{N}}_h$. Если $x\in(\mathfrak{P}_1+\ldots+\mathfrak{P}_{r+1})\cap(\mathfrak{N}_{r+2}+\ldots+\mathfrak{N}_h)$, то смежный класс

$$\bar{x}=x+(\mathfrak{P}_1+\ldots+\mathfrak{P}_r)\in\overline{\mathfrak{P}}_{r+1}\cap(\overline{\mathfrak{N}}_{r+2}+\ldots+\overline{\mathfrak{N}}_h).$$

Следовательно, $\bar{x}=0$ и $x\in\mathfrak{P}_1+\ldots+\mathfrak{P}_r$. Так как $(\mathfrak{P}_1+\ldots+\mathfrak{P}_r)\cap(\mathfrak{N}_{r+1}+\ldots+\mathfrak{N}_h)=0$, то $x=0$. Таким образом

$$\mathfrak{P}_1+\ldots+\mathfrak{P}_{r+1}+\mathfrak{N}_{r+1}+\ldots+\mathfrak{N}_h=$$
$$=\mathfrak{P}_1\oplus\ldots\oplus\mathfrak{P}_{r+1}\oplus\mathfrak{N}_{r+2}\oplus\ldots\oplus\mathfrak{N}_h.$$

Следовательно, $H_{r+1} = E_1F_1 + \ldots + E_{r+1}F_{r+1} + E_{r+2} + \ldots + E_h$ является эндоморфизмом. Так как $\overline{F}_{r+1}$ является изоморфизмом между $\overline{\mathfrak{N}}_{r+1}$ и $\overline{\mathfrak{P}}_{r+1}$, то $z_{r+1}F_{r+1} \neq 0$, если $z_{r+1} \neq 0$ и $z_{r+1} \in \mathfrak{N}_{r+1}$. Следовательно, $zH_{r+1} = 0$ только тогда, когда $z = 0$; H_{r+1} является автоморфизмом, и $\mathfrak{N} = \mathfrak{P}_1 \oplus \ldots \oplus \mathfrak{P}_{r+1} \oplus \mathfrak{N}_{r+2} \oplus \ldots \oplus \mathfrak{N}_h$.

Этим доказаны следующие теоремы:

Теорема 11. (Крулль-Шмидт). *Пусть $\mathfrak{N}$ является Ω-группой, причем Ω содержит все внутренние автоморфизмы, и в $\mathfrak{N}$ выполнены оба условия обрыва цепей. Предположим, что $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h = \mathfrak{P}_1 \oplus \ldots \oplus \mathfrak{P}_k$ будут двумя разложениями группы $\mathfrak{N}$ в прямую сумму неразложимых не равных нулю групп. Тогда $h = k$, и существует такой Ω-автоморфизм H, что при соответствующей нумерации слагаемых $\mathfrak{P}_i$, $\mathfrak{N}_iH = \mathfrak{P}_i$ и $\mathfrak{N} = \mathfrak{P}_1 \oplus \ldots \oplus \mathfrak{P}_r \oplus \mathfrak{N}_{r+1} \oplus \ldots \oplus \mathfrak{N}_h$ для любого $r \leqslant h$.*

Теорема 11′. (Крулль-Шмидт, вторая формулировка). *Пусть при сделанных выше предположениях E_i и F_j будут такими примитивными проекциями, что*

$$E_1 + \ldots + E_h = 1, \quad E_iE_{i'} = 0, \text{ если } i \neq i',$$

$$F_1 + \ldots + F_k = 1, \quad F_jF_{j'} = 0, \text{ если } j \neq j'.$$

Тогда $h = k$, и мы можем так упорядочить эндоморфизмы F_i, чтобы существовал Ω-автоморфизм H, удовлетворяющий условию $F_i = H^{-1}E_iH$, и чтобы $H_r = E_1F_1 + \ldots + E_rF_r + E_{r+1} + \ldots + E_h$ являлся Ω-автоморфизмом.

В обеих теоремах мы берем $H = E_1F_1 + \ldots + E_hF_h$.

Если $\mathfrak{N} = \mathfrak{N}' \oplus \mathfrak{N}''$ является прямым разложением, то существует продолжение этого разложения до разложения в прямую сумму неразложимых групп. Отсюда следует, что если выше соответствующим образом упорядочить $\mathfrak{P}_i$, то существует такой Ω-автоморфизм H, что

$$\mathfrak{N}'H = \mathfrak{P}_1 \oplus \ldots \oplus \mathfrak{P}_t \text{ и } \mathfrak{N}''H = \mathfrak{P}_{t+1} \oplus \ldots \oplus \mathfrak{P}_h.$$

8. Полная приводимость. Если, как это имеет место в нашем случае, Ω-подгруппы группы $\mathfrak{N}$ являются нормальными делителями, то они образуют дедекиндову структуру $\mathfrak{L}$ относительно операций $\cap$ и $+$. В самом деле, дедекиндовский дистрибутивный закон

$$\mathfrak{N}_1 \cap (\mathfrak{N}_2 + \mathfrak{N}_3) = \mathfrak{N}_2 + \mathfrak{N}_1 \cap \mathfrak{N}_3, \quad \text{если } \mathfrak{N}_1 \supseteq \mathfrak{N}_2$$

имеет место. Понятия приводимости и разложимости являются структурными понятиями. Подобно этому, будем говорить, что $\mathfrak{N}$ *вполне приводимо*, если структура $\mathfrak{L}$ вполне приводима, т. е., если для каждой подгруппы $\mathfrak{N}' \subset \mathfrak{N}$ найдётся подгруппа $\mathfrak{N}'' \subset \mathfrak{N}$ такая, что $\mathfrak{N} = \mathfrak{N}' \oplus \mathfrak{N}''$. Элемент $\mathfrak{N}''$ называется *дополнением* $\mathfrak{N}'$ относительно $\mathfrak{N}$.

Пусть $\mathfrak{P}$, $\mathfrak{P}' \in \mathfrak{L}$ и $\mathfrak{P}' \subseteq \mathfrak{P}$ и пусть $\mathfrak{P}''$ является дополнением к элементу $\mathfrak{P}'$ относительно $\mathfrak{N}$. Из $\mathfrak{N} = \mathfrak{P}' + \mathfrak{P}''$ и из дедекиндова закона мы получаем, что $\mathfrak{P} = \mathfrak{P}' + (\mathfrak{P}'' \cap \mathfrak{P})$. Так как $\mathfrak{P}' \cap \mathfrak{P}'' = 0$, то $(\mathfrak{P} \cap \mathfrak{P}'')$ является дополнением $\mathfrak{P}'$ относительно $\mathfrak{P}$. Таким образом, всякая Ω-подгруппа $\mathfrak{P}$ вполне приводимой группы $\mathfrak{N}$ вполне приводима. Если $\mathfrak{N} = \mathfrak{N}_1 \supset \mathfrak{N}_2 \supset \ldots$ является бесконечной убывающей цепью элементов из $\mathfrak{L}$, то для $i = 2, 3, \ldots$ существуют такие элементы $\mathfrak{N}_i' \neq 0$, что $\mathfrak{N}_{i-1} = \mathfrak{N}_i \oplus \mathfrak{N}_i'$. Тогда

$$\mathfrak{N}_1 = \mathfrak{N}_2' \oplus \mathfrak{N}_2 = \ldots = \mathfrak{N}_2' \oplus \ldots \oplus \mathfrak{N}_i' \oplus \mathfrak{N}_i,$$

и $\mathfrak{N}_2' \subset \mathfrak{N}_2' \oplus \mathfrak{N}_3' \subset \mathfrak{N}_2' \oplus \mathfrak{N}_3' \oplus \mathfrak{N}_4' \subset \ldots$ является бесконечной возрастающей цепью. Следовательно, если во вполне приводимой группе выполнено условие обрыва возрастающих цепочек, то выполнено и условие обрыва убывающих цепочек. Предположим теперь, что $0 \subset \mathfrak{N}_1 \subset \mathfrak{N}_2 \subset \ldots$ является бесконечной возрастающей цепью. Определим $\mathfrak{N}_1'$ таким образом, что $\mathfrak{N} = \mathfrak{N}_1 \oplus \mathfrak{N}_1'$, и для $i > 1$ определим $\mathfrak{N}_i'$ так, чтобы $\mathfrak{N}_{i-1}' = (\mathfrak{N}_{i-1}' \cap \mathfrak{N}_i) \oplus \mathfrak{N}_i'$. Тогда $\mathfrak{N}_i + \mathfrak{N}_i' \supseteq \mathfrak{N}_{i-1}'$ и $\supseteq \mathfrak{N}_{i-1}$. Следовательно, $\mathfrak{N} = \mathfrak{N}_i + \mathfrak{N}_i'$. Так как $\mathfrak{N}_i' \cap (\mathfrak{N}_{i-1}' \cap \mathfrak{N}_i) = 0$, то $(\mathfrak{N}_i' \cap \mathfrak{N}_i) \cap \mathfrak{N}_{i-1}' = 0$, а так как $(\mathfrak{N}_i' \cap \mathfrak{N}_i) \subseteq \mathfrak{N}_{i-1}'$, то получаем, что $\mathfrak{N}_i' \cap \mathfrak{N}_i = 0$, и $\mathfrak{N} = \mathfrak{N}_i \oplus \mathfrak{N}_i'$. Отсюда и из соотношения $\mathfrak{N}_{i-1}' \supset \mathfrak{N}_i'$ вытекает, что $\mathfrak{N}_1' \supset \mathfrak{N}_2' \supset \ldots$ является бесконечной убывающей

цепью. Следовательно, условие обрыва убывающих цепей влечет за собой условие обрыва возрастающих цепей.

Теорема 12. *Если группа $\mathfrak{N}$ удовлетворяет обоим условиям обрыва цепей и вполне приводима, то* $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$, *где подгруппы $\mathfrak{N}_i$ простые. Обратно, если* $\mathfrak{N} = \mathfrak{N}_1 + \ldots + \mathfrak{N}_h$, *где $\mathfrak{N}_i$ — простые подгруппы, то $\mathfrak{N}$ вполне приводима и удовлетворяет обоим условиям обрыва цепей.*

Предположим сначала, что $\mathfrak{N}$ вполне приводима и что $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_h$, где подгруппы $\mathfrak{N}_i$ неразложимы. Если $\mathfrak{N}_i$ непростая группа, то она содержит $\mathfrak{N}_i' \neq 0$ и не равную $\mathfrak{N}_i$. Так как $\mathfrak{N}_i \subseteq \mathfrak{N}$, то $\mathfrak{N}_i$ также вполне приводима. Следовательно, при подходящем $\mathfrak{N}_i'' \neq 0$ имеем $\mathfrak{N}_i = \mathfrak{N}_i' \oplus \mathfrak{N}_i''$, вопреки предположению о неразложимости $\mathfrak{N}_i$. Пусть теперь $\mathfrak{N} = \mathfrak{N}_1 + \ldots + \mathfrak{N}_h$, где $\mathfrak{N}_i$ — простые подгруппы, и пусть $\mathfrak{P}_1$ является Ω-подгруппой в $\mathfrak{N}$. Тогда $\mathfrak{P}_1 \cap \mathfrak{N}_i \in \mathfrak{L}$ и, в силу простоты группы $\mathfrak{N}_i$, либо $\mathfrak{P}_1 \cap \mathfrak{N}_i = 0$, либо $\mathfrak{P}_1 \cap \mathfrak{N}_i = \mathfrak{N}_i$, так что $\mathfrak{P}_1 \supseteq \mathfrak{N}_i$. Если второе условие выполнено для всех i, то $\mathfrak{P}_1 = \mathfrak{N}$. В противном случае пусть i_1 такой индекс, что $\mathfrak{P}_1 \cap \mathfrak{N}_{i_1} = 0$. Тогда $\mathfrak{P}_2 = \mathfrak{P}_1 + \mathfrak{N}_{i_1} = \mathfrak{P}_1 \oplus \mathfrak{N}_{i_1}$. Если мы будем рассматривать $\mathfrak{P}_2$ вместо $\mathfrak{P}_1$, то получим, что либо $\mathfrak{P}_2 = \mathfrak{N}$, либо существует такое $\mathfrak{N}_{i_2}$ $(i_2 \neq i_1)$, для которого $\mathfrak{P}_2 \cap \mathfrak{N}_{i_2} = 0$. Тогда $\mathfrak{P}_3 = \mathfrak{P}_2 + \mathfrak{N}_{i_2} = \mathfrak{P}_2 \oplus \mathfrak{N}_{i_2}$. Продолжая таким образом, мы, наконец, дойдем до такого k, что $\mathfrak{N} = \mathfrak{P}_{k+1} = \mathfrak{P}_k \oplus \mathfrak{N}_{i_k} = \mathfrak{P}_1 \oplus \mathfrak{N}_{i_1} \oplus \ldots \oplus \mathfrak{N}_{i_k}$. Таким образом, $\mathfrak{N}_{i_1} \oplus \ldots \oplus \mathfrak{N}_{i_k}$ является дополнением к подгруппе $\mathfrak{P}_1$ относительно $\mathfrak{N}$. Если мы начнем с $\mathfrak{P}_1 = 0$, то получим разложение $\mathfrak{N} = \mathfrak{N}_{i_1} \oplus \ldots \oplus \mathfrak{N}_{i_k}$. Следовательно,

$$\mathfrak{N} = (\mathfrak{N}_{i_1} \oplus \ldots \oplus \mathfrak{N}_{i_k}) \supset (\mathfrak{N}_{i_2} \oplus \ldots \oplus \mathfrak{N}_{i_k}) \supset \ldots \supset \mathfrak{N}_{i_k} \supset 0$$

является композиционным рядом для $\mathfrak{N}$, и, по теореме 6, выполнены оба условия обрыва цепей.

9. $\mathfrak{o}$-модули. Введем теперь понятие модуля, имеющее особенно важное значение в теории представлений. *Представление* абстрактного кольца $\mathfrak{o}$ определим как гомоморфизм кольца $\mathfrak{o}$ в кольцо эндоморфизмов коммутативной группы $\mathfrak{M}$ и обозначим эндоморфизм, соответствующий элементу a из $\mathfrak{o}$, через A. Тем не менее, мы будем считать более удобным обозначать результат xA действия A через xa и рассматривать этот элемент как «произведение» $x \in \mathfrak{M}$ и $a \in \mathfrak{o}$. Очевидно, выполнены следующие соотношения:

$$\left.\begin{aligned} (x+y)\,a &= xa + ya, \\ x\,(a+b) &= xa + xb, \\ x\,(ab) &= (xa)\,b \end{aligned}\right\} \qquad (2)$$

для всех x, $y \in \mathfrak{M}$ и $a, b \in \mathfrak{o}$. Мы будем теперь называть коммутативную группу $\mathfrak{M}$ *$\mathfrak{o}$-модулем*, если для каждого элемента x из $\mathfrak{M}$ и для каждого элемента a из $\mathfrak{o}$ определено произведение $xa \in \mathfrak{M}$, причем выполнены соотношения (2). Таким образом мы получили, что группу $\mathfrak{M}$, в которой представляется кольцо $\mathfrak{o}$, можно рассматривать как $\mathfrak{o}$-модуль. С другой стороны, каждый $\mathfrak{o}$-модуль определяет представление. В самом деле, согласно первому равенству из системы (2), отображение $x \to xa$ является эндоморфизмом в $\mathfrak{M}$. Согласно второму и третьему равенствам, множество $\mathfrak{D}$ таких эндоморфизмов замкнуто относительно сложения и умножения. Кроме того, мы можем легко вывести, что $x\,0 = 0$ и что $x\,(-a) = -xa$, так что $\mathfrak{D}$ содержит нулевой эндоморфизм и обратный эндоморфизм для каждого эндоморфизма этого множества. Таким образом $\mathfrak{D}$ является кольцом. Теперь, согласно второму и третьему равенствам, соответствие между элементом a и эндоморфизмом $x \to xa$ является гомоморфным отображением кольца $\mathfrak{o}$ в $\mathfrak{D}$.

Так как кольцо $\mathfrak{o}$ существует независимо от $\mathfrak{M}$, то естественно сравнивать различные $\mathfrak{o}$-модули. Мы определяем *$\mathfrak{o}$-гомоморфизм* H $\mathfrak{o}$-модуля $\mathfrak{M}$ в $\mathfrak{o}$-модуль $\mathfrak{N}$ как такое гомоморфное отображение группы $\mathfrak{M}$ в $\mathfrak{N}$, при котором для всех $x \in \mathfrak{M}$ и $a \in \mathfrak{o}$ имеем $(xa)\,H = (xH)\,a$. Если гомоморфизм H взаимнооднозначен, то мы получаем *$\mathfrak{o}$-изоморфизм*. Сходным образом мы определяем *$\mathfrak{o}$-эндоморфизм* и *$\mathfrak{o}$-автоморфизм*. Если $\mathfrak{N}$ является такой под-

группой $\mathfrak{o}$-модуля, что для всех $y \in \mathfrak{N}$ и $a \in \mathfrak{o}$ имеем $ya \in \mathfrak{N}$, то $\mathfrak{N}$ является модулем относительно умножения ya. Тогда $\mathfrak{N}$ называется *подмодулем* в модуле $\mathfrak{M}$. Полагая $(x + \mathfrak{N})\, a = xa + \mathfrak{N}$, мы замечаем, что эта функция однозначна для пар $x + \mathfrak{N}$ из $\mathfrak{M}/\mathfrak{N}$ и a из $\mathfrak{o}$. Правила (2) выполнены, и потому $\mathfrak{M}/\mathfrak{N}$ является модулем, *фактор-модулем* модуля $\mathfrak{M}$ по подмодулю $\mathfrak{N}$. Модуль $\mathfrak{M}$ называется *приводимым*, если он содержит собственный $\mathfrak{o}$-подмодуль. Сходным образом определяется *разложимость* и *полная приводимость*.

Мы увидим в дальнейшем, что в теории колец основным является следующее представление. Рассмотрим $\mathfrak{o}$ как коммутативную группу относительно сложения, определенного в кольце $\mathfrak{o}$. Мы можем тогда превратить эту группу в $\mathfrak{o}$-модуль, полагая xa равным произведению x и a как элементов кольца. Тогда равенства (2) следуют из дистрибутивного и ассоциативного законов. Следовательно, группа $\mathfrak{o}$ является $\mathfrak{o}$-модулем. Отсюда следует, что соответствие между элементом кольца a и эндоморфизмом $x \to xa$ является представлением. Обозначим эндоморфизм $x \to xa$ через a_r и назовем это отображение *правым умножением*, определенным при помощи элемента a. Представление $a \to a_r$ является (правым) *регулярным представлением* кольца $\mathfrak{o}$. Если $\mathfrak{o}$ обладает единицей 1, то из $1a_r = 1b_r$ следует, что $a = b$; следовательно, регулярное представление взаимнооднозначно. $\mathfrak{o}$-подмодулями относительно регулярного представления будут правые идеалы в $\mathfrak{o}$.

Все теоремы, доказанные нами для Ω-групп, справедливы и для $\mathfrak{o}$-модулей. Изменения, которые нужно провести в утверждениях и доказательствах, очевидны. Например, если $\mathfrak{M}$ является $\mathfrak{o}$-модулем, гомоморфно отображаемым на $\mathfrak{o}$-модуль $\mathfrak{N}$, то множество $\mathfrak{P}$ элементов, отображающихся при этом в 0, является подмодулем в $\mathfrak{M}$, причем $\mathfrak{M}/\mathfrak{P}$ и $\mathfrak{N}$ будут $\mathfrak{o}$-изоморфны. Если $\mathfrak{o}$ содержит единицу, то следующий метод дает нам возможность привести теорию $\mathfrak{o}$-модулей к теории Ω-групп. Если $\mathfrak{M}$ и $\mathfrak{N}$ являются $\mathfrak{o}$-модулями, мы образуем прямую сумму $\mathfrak{S} = \mathfrak{M} \oplus \mathfrak{N} \oplus \mathfrak{o}$ и определим $(x + y + b)\, a = xa + ya + ba$, где $x \in \mathfrak{M}$, $y \in \mathfrak{N}$, $a \in \mathfrak{o}$ и $b \in \mathfrak{o}$. Таким образом мы получаем изоморфное $\mathfrak{o}$ кольцо эндоморфизмов Ω группы $\mathfrak{S}$. Теперь $\mathfrak{M}$ и $\mathfrak{N}$ являются $\mathfrak{O}$-подгруппами и $\mathfrak{O}$-гомоморфны ($\mathfrak{O}$-изоморфны) тогда и только тогда, когда они $\mathfrak{o}$-гомоморфны ($\mathfrak{o}$-изоморфны).

Наконец, мы можем заметить, что некоторые проблемы, касающиеся Ω-групп, могут быть приведены к вопросам, касающимся представлений. Для этого заменяют множество Ω содержащим его кольцом $\mathfrak{O}$, определенным как наименьшее подкольцо кольца эндоморфизмов, содержащее все преобразования из Ω. Тогда $\mathfrak{O}$ определяет свое собственное представление, или, более точно, представление кольца $\mathfrak{o}$, изоморфного $\mathfrak{O}$. Группа $\mathfrak{M}$, в которой действуют эндоморфизмы, будет, таким образом, $\mathfrak{o}$-модулем.

10. Левые модули. Так как мы интересуемся, в первую очередь, некоммутативными кольцами, то понятие обратного гомоморфизма почти столь же важно для нас, как понятие гомоморфизма. Напомним определение: Отображение $x \to x'$ кольца $\mathfrak{o}$ на кольцо $\mathfrak{o}'$ называется *обратным гомоморфизмом*, если для любых x, $y \in \mathfrak{o}$ выполняются следующие равенства:

$$(x + y)' = x' + y', \qquad (xy)' = y'x'.$$

Если при этом отображение взаимнооднозначно, то оно называется *обратным изоморфизмом*, а кольца $\mathfrak{o}$ и $\mathfrak{o}'$ обратно изоморфными. В том случае, когда $\mathfrak{o} = \mathfrak{o}'$, мы получаем понятие *обратного автоморфизма*. Например, ставя каждой матрице в соответствие транспонированную матрицу, мы получаем обратный изоморфизм в кольце матриц с целыми рациональными элементами.

Если $\mathfrak{o}$ является произвольным кольцом, то мы можем образовать множество $\mathfrak{o}'$, элементы которого стоят во взаимнооднозначном соответствии с элементами из $\mathfrak{o}$ ($x \to x'$) и определить $x' + y'$ как $(x + y)'$ и $x'y'$ как $(yx)'$. Получившаяся система является кольцом $\mathfrak{o}'$, обратно изоморфным кольцу $\mathfrak{o}$; соответствие $x \to x'$ будет обратным изоморфизмом.

Мы можем теперь сформулировать понятия, двойственные понятиям представления и $\mathfrak{o}$-модуля. Мы определяем *обратное представление* кольца $\mathfrak{o}$ как обратно гомоморфное отображение $a \to A'$ кольца $\mathfrak{o}$ в кольцо эндоморфизмов коммутативной группы $\mathfrak{M}$. В этом случае удобно обозначать величину xA', как функцию x и a, через ax. Тогда:

$$\left.\begin{aligned} a(x+y) &= ax+ay, \\ (a+b)x &= ax+bx, \\ (ab)x &= a(bx). \end{aligned}\right\} \qquad (3)$$

Мы приходим, таким образом, к определению левого *$\mathfrak{o}$-модуля* $\mathfrak{M}$, как коммутативной группы, для которой определено произведение элементов x из $\mathfrak{M}$ и a из $\mathfrak{o}$, значение которого ax лежит в $\mathfrak{M}$ и удовлетворяет соотношениям (3). Таким образом каждое обратное представление приводит к левому $\mathfrak{o}$-модулю, и, обратно, если задан левый $\mathfrak{o}$-модуль, то соответствие $a \to A'$, где $xA' = {}=dax$, является обратным представлением. Определения *изоморфизма*, *подмодуля* и т. д. такие же, как и для обычных модулей. Как естественно ожидать, „обратная" теория параллельна обычной теории. Мы можем, в самом деле, привести ее к обычной теории, замечая, что левый $\mathfrak{o}$-модуль может рассматриваться как $\mathfrak{o}'$-модуль, где $\mathfrak{o}'$ — кольцо, обратно изоморфное кольцу $\mathfrak{o}$. Тем не менее, во многих случаях нам будет удобнее непосредственно иметь дело с левыми модулями вместо того, чтобы проводить эту замену.

Как и ранее, аддитивная группа любого кольца $\mathfrak{o}$ является левым $\mathfrak{o}$-модулем относительно функции, значениями которой являются произведения ax, где x лежит в аддитивной группе $\mathfrak{o}$ и a в кольце $\mathfrak{o}$. Мы обозначим отображение $x \to ax$ через a_l и будем называть его *левым умножением*, определенным при помощи элемента a. Обратное представление $a \to a_l$ называется *левым регулярным представлением*. Очевидно, что подмодулями левого $\mathfrak{o}$-модуля $\mathfrak{o}$ являются левые идеалы кольца $\mathfrak{o}$.

Глава 2

ВЕКТОРНЫЕ ПРОСТРАНСТВА.

1. Определение. В этой главе мы будем изучать коммутативную группу $\mathfrak{R}$ относительно множества Φ эндоморфизмов, образующих тело (некоммутативное поле). Множество $\mathfrak{L}$ Φ-эндоморфизмов группы подобного типа является кольцом матриц над обратно изоморфным к Φ телом Φ'. Наше изучение эквивалентно, следовательно, изучению колец матриц. Один из основных результатов структурной теории колец (получаемый в главе 4) состоит в том, что всякое простое кольцо, удовлетворяющее некоторым условиям конечности, является кольцом матриц над телом. С помощью этой теоремы мы сможем показать, что наши кажущиеся весьма специальными рассмотрения занимают важное место в общей теории.

Уточним предположения, которые мы делаем относительно $\mathfrak{R}$ и Φ:

1. Если $\alpha, \beta \in \Phi$, то и $\alpha+\beta \in \Phi$ и $\alpha\beta \in \Phi$.
2. 0 и $1 \in \Phi$.
3. Если $\alpha \in \Phi$, то и $-\alpha \in \Phi$, и если $\alpha \neq 0$, то α является автоморфизмом, и $\alpha^{-1} \in \Phi$.

Таким образом, множество Φ является подтелом кольца эндоморфизмов группы $\mathfrak{R}$. Мы называем $\mathfrak{R}$ *векторным пространством* (линейным пространством) над Φ.

Так же, как и коммутативная группа относительно произвольного кольца эндоморфизмов, каждое векторное пространство $\mathfrak{R}$ над Φ может быть рассматриваемо как φ-модуль, где φ является произвольным кольцом, изоморфным с Φ. Определенное в модуле произ-

ведение $x1$, где 1 является единицей в φ, равно x для всех $x \in \mathfrak{R}$. С другой стороны, предположим, что φ является произвольным телом и что $\mathfrak{M}$ является φ-модулем, в котором $x\,1 = x$ для всех x. Пусть Φ обозначает кольцо эндоморфизмов $x \to x\alpha$, определенных при помощи элементов α из φ. Тогда Φ будет гомоморфным ненулевым образом тела φ. Отсюда следует, что Φ изоморфно φ. Следовательно, Φ является телом, и так как Φ содержит тождественное отображение, то Φ удовлетворяет условиям 1—3. Таким образом, мы можем определить векторное пространство, как такой φ-модуль, что φ является телом, и $x\,1 = x$ для всех x из модуля. Φ-подгруппа $\mathfrak{S}$ векторного пространства $\mathfrak{R}$ над Φ называется *подпространством* в $\mathfrak{R}$. Мы ограничимся рассмотрением *конечномерных* векторных пространств, т. е. таких пространств, которые удовлетворяют следующему условию:

4. Выполнено условие обрыва возрастающих цепей для подпространств.

Если x является некоторым вектором (элементом) из $\mathfrak{R}$, то множество (x) векторов вида $x\alpha$, где α — произвольный элемент из Φ, является неприводимым подпространством. В самом деле, если $x \neq 0$ и некоторое $y \neq 0$ лежит в подпространстве $\mathfrak{S}$ пространства (x), то $y = x\gamma$. Следовательно, $x\alpha = y\gamma^{-1}\alpha \in \mathfrak{S}$, так что $(x) = \mathfrak{S}$. Очевидно, что подпространства типа (x) являются единственными неприводимыми подпространствами, так как любое подпространство содержит подпространство такого вида.

Пусть $\mathfrak{S}$ является подпространством $\neq \mathfrak{R}$ и пусть y_1 — вектор, не лежащий в $\mathfrak{S}$. Тогда, так как (y_1) неприводимо, то $\mathfrak{S}_1 \equiv \mathfrak{S} + (y_1) = \mathfrak{S} \oplus (y_1)$. Если $\mathfrak{S}_1 \neq \mathfrak{R}$, то мы можем найти $y_2 \overline{\in} \mathfrak{S}_1$, и тогда $\mathfrak{S}_2 \equiv \mathfrak{S}_1 + (y_2) = \mathfrak{S}_1 \oplus (y_2) = \mathfrak{S} \oplus (y_1) \oplus (y_2)$. Продолжая таким образом, мы получим возрастающую цепь подпространств $\mathfrak{S}_i = \mathfrak{S} \oplus (y_1) \oplus \ldots \oplus (y_i)$. Следовательно, в силу условия обрыва возрастающих цепей, найдется такое целое r, что $\mathfrak{R} = \mathfrak{S} \oplus (y_1) \oplus \ldots \oplus (y_r)$. Положив $\mathfrak{S}' = (y_1) \oplus \ldots \oplus (y_r)$, мы получим разложение $\mathfrak{R} = \mathfrak{S} \oplus \mathfrak{S}'$. Следовательно, $\mathfrak{R}$ вполне приводимо. Если мы начнем с $\mathfrak{S} = 0$, то получим

множество таких векторов $x_1, x_2, \ldots, x_n \neq 0$, что $\mathfrak{R} = (x_1) \oplus \ldots \oplus (x_n)$ [1]). Каждый вектор x имеет единственное представление в виде $\Sigma x_i \xi_i$, где $\xi_i \in \Phi$; в самом деле, $x_i\xi_i$ определено элементом x, и $x_i\xi_i = x_i\eta_i$ влечет за собой $\xi_i = \eta_i$. Элементы x образуют *базис* пространства $\mathfrak{R}$ над Φ. По теореме Жордана-Гельдера, либо по теореме Крулля-Шмидта, их число n, *размерность* $\mathfrak{R}$ над Φ, инвариантно. В следующем параграфе мы получим непосредственное доказательство этого утверждения.

Из инвариантности размерности следует, что изоморфные φ-модули имеют одинаковую размерность. Обратно, пусть $\mathfrak{R}_1$ и $\mathfrak{R}_2$ являются φ-модулями, имеющими одинаковую размерность, и пусть $x_1^{(i)}, \ldots, x_n^{(i)}$ образуют базис для $\mathfrak{R}_i$. Тогда соответствие $\Sigma x_j^{(1)}\alpha_j \to \Sigma x_j^{(2)}\alpha_j$, где $\alpha_j \in \varphi$, является φ-изоморфизмом.

Если φ является произвольным телом, мы можем построить векторное пространство любой размерности n над кольцом эндоморфизмов Φ, изоморфным φ. В самом деле, пусть $\mathfrak{R}$ является пространством элементов

$$x = (\xi_1, \ldots, \xi_n), \quad \text{где} \quad \xi_i \in \varphi.$$

Мы будем считать, что $x = y = (\eta_1, \ldots, \eta_n)$, если $\xi_i = \eta_i$, и положим $x + y = (\xi_1 + \eta_1, \ldots, \xi_n + \eta_n)$, $x\alpha = (\xi_1\alpha_1, \ldots \xi_n\alpha)$ для $\alpha \in \varphi$. Тогда $\mathfrak{R}$ является φ-модулем, в котором $x\,1 = x$. Следовательно, $\mathfrak{R}$ является векторным пространством над

---

[1]) Если мы примем теорему о полном упорядочивании, то это утверждение может быть установлено без условия обрыва возрастающих цепей. В самом деле, пусть $[y_\alpha]$ является множеством векторов из $\mathfrak{R}$, где α пробегает отрезок множества порядковых чисел. Если $\mathfrak{S}$ является подпространством, мы определим все $\mathfrak{S}_\alpha$, как наименьшее подпространство, содержащее $\mathfrak{S}$ и все y_β при $\beta < \alpha$. Если $y_\alpha \notin \mathfrak{S}_\alpha$, то положим $y_\alpha = x_\alpha$. Тогда элементы x_α линейно независимы и порождают дополнение к $\mathfrak{S}$. Приведенное выше рассуждение показывает, что условие обрыва возрастающих цепей влечет за собой условие обрыва убывающих цепей. Итак, из полной приводимости $\mathfrak{R}$ вытекает, что условие обрыва возрастающих цепей следует из условия обрыва убывающих цепей. Это может быть также доказано непосредственно (глава 4, § 12).

кольцом Ф эндоморфизмов вида $x \to x\alpha$, и Ф изоморфно φ. Если мы положим $x_1 = (1, 0, \ldots, 0), \ldots, x_n = (0, \ldots, 0, 1)$, то получим прямое разложение $\mathfrak{R} = (x_1) \oplus \ldots \oplus (x_n)$. Следовательно, $\mathfrak{R}$ обладает композиционным рядом, и, таким образом, $\mathfrak{R}$ удовлетворяет обоим условиям обрыва цепей. Размерность $\mathfrak{R}$ равна n. Возможность построения векторного пространства над любым телом обеспечивает приложимость результатов, которые мы выведем для тел эндоморфизмов, к произвольным телам.

2. Изменение базиса. Векторы $y_1, \ldots, y_r$ из $\mathfrak{R}$ над Ф называются *линейно независимыми*, если $\mathfrak{S} \equiv (y_1) + \ldots + (y_r) = (y_1) \oplus \ldots \oplus (y_r)$, причем все $y_i \neq 0$. Эквивалентным этому условию является следующее: $\sum y_i \alpha_i = 0$ тогда и только тогда, когда все $\alpha_i = 0$. Предположим теперь, что элементы y_i линейно независимы, и $y_i = \sum x_j \beta_{ji}$ является выражением элементов y_i через базис $x_1, \ldots, x_n$. Если ρ является произвольным элементом из Ф, то элементы $y_1, y_2 + y_1\rho, y_3, \ldots, y_r$ линейно независимы. В противном случае $y_2 + y_1\rho \in (y_1) + (y_3) + \ldots + (y_r)$, и, следовательно, $y_2 \in (y_1) + (y_3) + \ldots + (y_r)$. Мы получаем, таким образом, что $\mathfrak{S} = (y_1) + (y_2 + y_1\rho) + (y_3) + \ldots + (y_r)$. Пусть $\beta_{n_1 1} \neq 0$, и положим $\rho = -\beta_{n_1 1}^{-1} \beta_{n_1 2}$. Тогда выражение для вектора $y_2^{(1)} = y_2 + y_1\rho$ не должно содержать x_{n_1}. Подобным же образом мы можем найти такие векторы

$$y_3^{(1)}, \ldots, y_r^{(1)} \text{ в } (x_1) + \ldots + (x_{n_1 - 1}) + (x_{n_1 + 1}) + \ldots + (x_n),$$

что $y_1, y_2^{(1)}, \ldots, y_r^{(1)}$ линейно независимы, и $\mathfrak{S} = (y_1) + (y_2^{(1)}) + \ldots + (y_r^{(1)})$. Пусть теперь $y_k^{(1)} = \sum x_i \beta_{ik}^{(1)}$, и предположим, что $\beta_{n_2 2}^{(1)} \neq 0$. Полагая $y_k^{(2)} = y_k^{(1)} - y_2^{(1)} \beta_{n_2 2}^{(1)-1} \beta_{n_2 k}^{(1)}$ для $k = 3, 4, \ldots$, мы замечаем, что $y_k^{(2)} \neq 0$ и что выражения для этих $y_k^{(2)}$ не содержат ни x_{n_1}, ни x_{n_2}. Кроме того, $\mathfrak{S} = (y_1) \oplus (y_2^{(1)}) \oplus (y_3^{(2)}) \oplus \ldots \oplus (y_r^{(2)})$. После несколь-

ких повторений этого процесса мы получаем $\mathfrak{S} = (y_1) \oplus \oplus (y_2^{(1)}) \oplus \ldots \oplus (y_r^{(r-1)})$, где

$$y_i^{(i-1)} = x_{n_i} \gamma_{n_i i} + \sum_{j \neq n_s} x_j \gamma_{ji} \neq 0, \quad \gamma_{n_i i} \neq 0, \quad s = 1, 2, \ldots, i$$

и все n_i различны. Соответствие между y_i и x_{n_i} ясно показывает, что $r \leqslant n$. Если $\mathfrak{S} = \mathfrak{R}$, то элементы y_i также образуют базис в $\mathfrak{R}$, и потому, по симметрии, $n \leqslant r$. Таким образом, еще раз доказано, что размерность $\mathfrak{R}$ инвариантна.

Немного усложняя приведенный выше метод, мы получим такой базис $z_1, \ldots, z_r$ для $\mathfrak{S}$, что

$$z_i = x_{n_i} \varepsilon_{n_i i} + \sum x_j \varepsilon_{ji}, \quad \varepsilon_{n_i i} \neq 0, \quad t = 1, \ldots, r.$$

Умножая эти векторы на $\varepsilon_{n_i i}^{-1}$ и переставляя их потом надлежащим образом, мы получим, наконец, такой базис $u_1, \ldots, u_r$ в $\mathfrak{S}$, что $u_i = x_{n_i} + \sum_{j \neq n_t} x_j \rho_{ji}$ и $n_1 < n_2 < \ldots$.

Если $\mathfrak{S} = \mathfrak{R}$, то из инвариантности размерности следует, что $r = n$. Тогда вектора u_i являются просто первоначальными векторами x_i. Предположим, обратно, что $r = n$, т. е. что элементы y_i линейно независимы, и их число равно размерности R. Тогда $u_i = x_i$, и потому элементы y_i, равно как и элементы x_i, образуют базис пространства $\mathfrak{R}$. Надо отметить, что переход от базиса $y_1, \ldots, y_n$ к базису $u_1 = x_1, \ldots, u_n = x_n$ был выполнен при помощи последовательных замен одного из следующих типов:

I. $y_i \to y_i$ для $i \neq r$ и $y_r \to y_r + y_s\rho$, $s \neq r$.

II. $y_i \to y_i$ для $i \neq r$ и $y_r \to y_r\sigma$, $\sigma \neq 0$.

III. $y_i \to y_i$ для $i \neq r, s$ и $y_r \to y_s$, $y_s \to y_r$.

Последний тип нужен для правильного упорядочивания элементов базисов.

Если $x_1, \ldots, x_n$ и $y_1, \ldots, y_n$ являются двумя произвольными базисами для $\mathfrak{R}$, мы можем предположить, что

$$y_i = \sum x_j \beta_{ji} \text{ и } x_j = \sum y_k \alpha_{kj}.$$

Эти выражения однозначны. Так как

$$y_i = \sum_{k,j} y_k \alpha_{kj} \beta_{ji}, \qquad x_j = \sum_{k,i} x_k \beta_{ki} \alpha_{ij},$$

то мы получаем:

$$\sum_j \alpha_{kj} \beta_{ji} = \delta_{ki}, \quad \sum_j \beta_{kj} \alpha_{ji} = \delta_{ki}$$

(δ_{ki} — символ Кронекера). Таким образом, если мы положим $B = (\beta_{ij})$, $A = (\alpha_{ij})$, то получаем $AB = 1 = BA$, где 1 обозначает единичную матрицу в кольце Φ_n всех матриц порядка n с элементами из тела Φ[1]).

С другой стороны, предположим, что $B = (\beta_{ij})$ является произвольной матрицей, имеющей правую обратную A ($BA = 1$). Положим $y_i = \sum x_j \beta_{ji}$, где $x_1, \ldots, x_n$ образуют базис $\mathfrak{R}$. Тогда

$$\sum y_k \alpha_{kj} = \sum x_i \beta_{ik} \alpha_{kj} = \sum x_i \delta_{ij} = x_j.$$

[1]) Если $\mathfrak{A}$ является кольцом, то $\mathfrak{A}_n$ обозначает множество всех элементов вида $\Sigma e_{ij} a_{ij}$, где $a_{ij} \in \mathfrak{A}$, причем $\Sigma e_{ij} a_{ij} = \Sigma e_{ij} b_{ij}$ тогда и только тогда, когда $a_{ij} = b_{ij}$. Мы положим $\Sigma e_{ij} a_{ij} + \Sigma e_{ij} b_{ij} = \Sigma e_{ij} (a_{ij} + b_{ij})$ и $(\Sigma e_{ij} a_{ij}) \times (\Sigma e_{ij} b_{ij}) = \Sigma e_{ij} (\Sigma a_{ik} b_{kj})$. Получающаяся система является кольцом. Подмножество элементов вида $\Sigma e_{ij} a$ является изоморфным с $\mathfrak{A}$ подкольцом $\overline{\mathfrak{A}}$. Мы индентифицируем $\overline{\mathfrak{A}}$ с $\mathfrak{A}$. Если $\mathfrak{A}$ содержит единицу 1, то $\mathfrak{A}_n$ содержит такие элементы $e_{ij} = e_{ij} 1$, что $e_{ij} e_{kl} = \delta_{jk} e_{il}$, и $e_{11} + \ldots + e_{nn}$ является единицей в кольце $\mathfrak{A}_n$. Каждый элемент a из $\mathfrak{A}_n$ может быть одним и только одним способом представлен в виде $\Sigma e_{ij} a_{ij}$, где $e_{ij} a_{ij}$ обозначает теперь произведение e_{ij} и a_{ij}, $a_{ij} \in \mathfrak{A}$. Элементы из $\mathfrak{A}$ коммутируют с e_{ij}. Обратно, пусть $\mathfrak{B}$ является произвольным кольцом с единицей 1 и элементы e_{ij} из $\mathfrak{B}$ удовлетворяют вышеприведенным условиям, причем $\Sigma e_{ii} = 1$; пусть, далее, $\mathfrak{B}$ содержит такое подкольцо $\mathfrak{A}$, что 1) $1 \in \mathfrak{A}$, 2) $a e_{ij} = e_{ij} a$ для всех a из $\mathfrak{A}$, и 3) каждый элемент из $\mathfrak{B}$ может быть одним и только одним образом записан в виде $\Sigma e_{ij} a_{ij}$. Тогда $\mathfrak{B} \cong \mathfrak{A}_n$.

Если элементы y_i линейно зависимы, мы можем выбрать из них такое линейное независимое подмножество $y_1, \ldots, y_r$, что $\mathfrak{S} \equiv (y_1) + \ldots + (y_n) = (y_1) \oplus \ldots \oplus (y_r)$ является надлежащим разложением. Так как $x_1, \ldots, x_n \in \mathfrak{S}$, то $\mathfrak{S} = \mathfrak{R}$, и мы получили противоречие с инвариантностью размерности. Следовательно, элементы y_i линейно независимы и потому они также образуют базис пространства $\mathfrak{R}$ и $AB = 1$.

Теорема 1. *Если Φ является телом, то $AB = 1$ в Φ_n тогда и только тогда, когда $BA = 1$.*

Если элементы y_i не образуют базиса, то они линейно зависимы и, следовательно, $\sum y_i \gamma_i = 0$, где не все $\gamma_i = 0$. Если $y_i = \sum x_j \beta_{ji}$, то $\sum \beta_{ji} \gamma_i = 0$, так что матрица

$$C = \begin{pmatrix} \gamma_1 & 0 & \ldots & 0 \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ \gamma_n & 0 & \ldots & 0 \end{pmatrix}$$

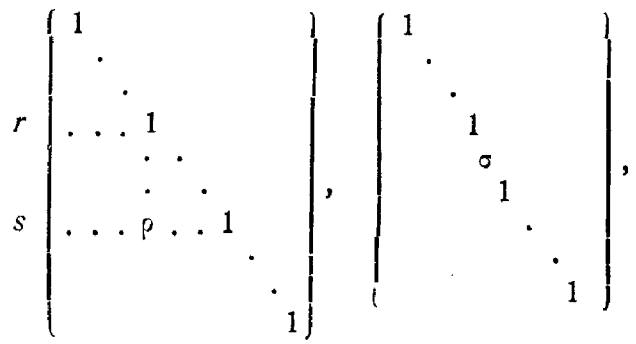
удовлетворяет условию $BC = 0$. Обратно, если $C \neq 0$ и $BC = 0$, то векторы $\sum x_j \beta_{ji}$ линейно зависимы. Таким образом, нами доказана

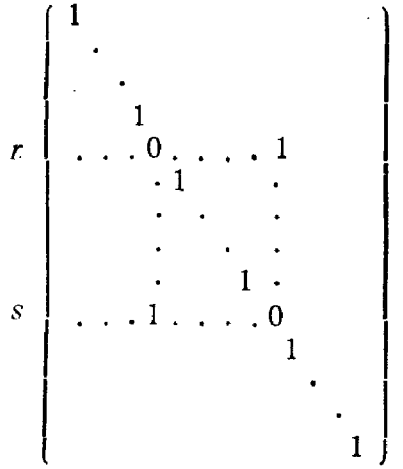
Теорема 2. *Если Φ является телом, то матрица из Φ_n тогда и только тогда обратима, если она не является левым делителем нуля.*

Пусть Φ' является телом, обратно изоморфным телу Φ, и $\alpha \to \alpha'$ будет обратным изоморфизмом между Φ и Φ'. Тогда отображение $(\alpha_{ij}) = A \to A^* = (\alpha^*_{ij})$, где $\alpha^*_{ij} = \alpha'_{ji}$, является обратным изоморфизмом между Φ_n и Φ_n'. Если $AB = 1$, то $B^*A^* = 1$ в Φ_n', и если $CB = 0$, то $B^*C^* = 0$. Отсюда следует, что мы можем в предыдущей теореме заменить слово «левый» словом «правый».

Мы видели, что можно было перейти от базиса $y_1, \ldots, y_n$ к $x_1, \ldots, x_n$ с помощью последовательности замен вышеописанных типов I, II и III. Матрицы, выра-

жающие новые элементы y_i через старые, имеют соответственно вид:





и называются *элементарными* матрицами. Если теперь $\{x_i\}$, $\{y_i\}$ и $\{z_i\}$ являются тремя различными базисами в $\mathfrak{R}$ и

$$y_j = \sum x_i \alpha_{ij}, \qquad z_k = \sum y_j \beta_{jk}, \quad \text{то } z_k = \sum x_i \gamma_{ik},$$

где $c = (\gamma_{ij}) = AB$. Итак, нами получена

Теорема 3. *Всякая обратимая матрица в* Φ_n *является произведением элементарных матриц.*

Следует отметить, что последний тип элементарных матриц излишен. Действительно, при $n = 2$ мы имеем:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

и соответствующие изменения для $n > 2$ очевидны.

3. Векторные пространства над различными телами. Один из типов векторных пространств, часто встречающихся в теории колец и алгебр, получается следующим образом. Пусть $\mathfrak{A}$ является кольцом с единицей и φ—подтелом кольца $\mathfrak{A}$, содержащим ту же единицу. Мы видели, что эндоморфизмы $x \to x\alpha$, где $x \in \mathfrak{A}$ и $\alpha \in \varphi$, образуют тело Φ, изоморфное φ. Так как Φ содержит тождественный эндоморфизм, то мы можем рассматривать $\mathfrak{A}$ как векторное пространство над Φ. Сходным образом мы можем использовать эндоморфизм $x \to \alpha x \equiv x\alpha'$ и получить тело эндоморфизмов Φ', обратно изоморфное φ.

Предположим теперь, что $\mathfrak{R}$ является некоторым векторным пространством над Φ и что Σ является подтелом в Φ. Мы обозначим множество эндоморфизмов $\xi \to \xi\alpha$ из Φ, где $\alpha \in \Sigma$, также через Σ. Предположим сначала, что размерность $(\mathfrak{R} : \Phi)$ равна n и что $(\Phi : \Sigma) = m$. Если тогда $x_1, \ldots, x_n$ является базисом модуля $\mathfrak{R}$ над Φ и $\xi_1, \ldots, \xi_m$ — базисом Φ над Σ, то каждый вектор из $\mathfrak{R}$ имеет одно и только одно представление в виде $\Sigma x_i \xi_j \alpha_{ij}$, где $a_{ij} \in \Sigma$. Следовательно, $x_i \xi_j$ образуют базис из mn элементов для $\mathfrak{R}$ над Σ. Обратно, если $\mathfrak{R}$ имеет конечную размерность над Σ, то очевидно, что, так как $\Phi \supseteq \Sigma$, $\mathfrak{R}$ также имеет конечную размерность над Φ. Кроме того, если x является некоторым вектором в $\mathfrak{R}$, $x \neq 0$, то множество $x\xi$, где ξ произвольно в Φ, является подпространством в $\mathfrak{R}$ над Σ. Если $x\xi_1, \ldots, x\xi_m$ образуют базис этого пространства, то $\xi_1, \ldots, \xi_m$ образуют базис тела Φ над Σ, и потому Φ имеет конечную размерность над Σ. Нами доказана таким образом

Теорема 4. *Если* $\mathfrak{R}$ *является векторным пространством, имеющим конечную размерность над* Φ,

и Σ *такое подтело в* Φ, *что* Φ *конечно над* Σ, *то* $(\mathfrak{R}:\Sigma)=(\mathfrak{R}:\Phi)(\Phi:\Sigma)$. *Обратно, если* $\mathfrak{R}$ *является любым векторным пространством над* Φ *и* $\mathfrak{R}$ *конечно над подтелом* Σ *тела* Φ, *то и* Φ *конечно над* Σ.

Этот же результат справедлив для множества Σ' эндоморфизмов вида $\xi\to\alpha\xi$. В дальнейшем на протяжении этой главы мы рассматриваем фиксированное векторное пространство $\mathfrak{R}$ над фиксированным телом Φ.

4. Кольцо линейных преобразований. Φ-эндоморфизм A пространства $\mathfrak{R}$ называется *линейным преобразованием* пространства $\mathfrak{R}$ над Φ. В произвольном кольце совокупность элементов, коммутирующих с элементами фиксированного подмножества кольца, образует подкольцо. Следовательно, совокупность линейных преобразований образует подкольцо $\mathfrak{L}$ в кольце всех эндоморфизмов.

Если A является линейным преобразованием и элементы $x_1,\ldots,x_n$ образуют базис пространства $\mathfrak{R}$ над Φ, то A вполне определяется заданием образов x_iA элементов x_i. В самом деле, если $x=\sum x_i\xi_i$, то мы имеем $xA=\sum(x_iA)\xi_i$. С другой стороны, мы можем произвольно выбрать n элементов y_i и проверить, что отображение $\sum x_i\xi_i\to\sum y_i\xi_i$ является таким линейным преобразованием A, что $x_iA=y_i$. В частности, для каждого $\alpha\in\Phi$ существует единственное линейное преобразование α' такое, что $x_i\alpha'=x_i\alpha$ для всех i. Разумеется, α' зависит как от выбора базиса, так и от α. Совокупность всех α' образует подкольцо Φ' в $\mathfrak{L}$, обратно изоморфное телу Φ; соответствие $\alpha\to\alpha'$ является обратным изоморфизмом.

Теперь мы можем рассматривать $\mathfrak{R}$ как векторное пространство над Φ'. Так как каждый элемент x может быть только одним способом представлен в виде $\sum x_i\xi_i$, то $x_1,\ldots,x_n$ образуют базис пространства $\mathfrak{R}$ над Φ', и потому $\mathfrak{R}$ имеет размерность n над Φ'. Эндоморфизмы α являются линейными преобразованиями в $\mathfrak{R}$ над Φ' и, так как $x_i\alpha=x_i\alpha'$, то α является эндоморфизмом, таким же

образом соответствующим эндоморфизму α' и базису x, каким α' соответствует α и базису x, т. е. $(\alpha')'=\alpha$.

Пусть E_{ij} обозначает такое линейное преобразование в $\mathfrak{R}$ над Φ, что $x_rE_{ij}=\delta_{ir}x_j$. Так как $x_r(E_{ij}\alpha')=x_r(\alpha'E_{ij})$, то $E_{ij}\alpha'=\alpha'E_{ij}$, и потому E_{ij} также линейно в $\mathfrak{R}$ над Φ'. Предположим теперь, что A является произвольным линейным преобразованием пространства $\mathfrak{R}$ над Φ и что $x_rA=\sum x_j\alpha_{rj}$. Тогда, как легко проверить, A и $\sum_{ij}E_{ij}\alpha'_{ij}$ имеют одинаковое действие на элементы x. Следовательно, $A=\sum E_{ij}\alpha'_{ij}$. Обратно, если $A=\sum E_{ij}\alpha'_{ij}$, то $A\in\mathfrak{L}$ и $x_rA=\sum x_j\alpha_{rj}$. Отсюда следует, что каждое A из $\mathfrak{L}$ может быть одним и только одним образом представлено в виде $\sum E_{ij}\alpha'_{ij}$, где $\alpha'\in\Phi'$. Так как

$$E_{ij}E_{kl}=\delta_{jk}E_{il},\quad \sum E_{ii}=1, \tag{1}$$

то $\mathfrak{L}=\Phi'_n$.

В силу (1), мы получаем:

$$\alpha'_{pq}=\sum_k E_{kp}\left(\sum E_{ij}\alpha'_{ij}\right)E_{qk}. \tag{2}$$

Следовательно, если $A=\sum E_{ij}\alpha'_{ij}$ коммутирует со всеми E_{kl}, то $\alpha'_{pq}=0$ при $p\neq q$ и $\alpha'_{pp}=A$, т. е. $A=\alpha'\in\Phi'$. Таким образом Φ' может быть охарактеризовано как множество элементов из $\mathfrak{L}$, коммутирующих со всеми E_{ij}. Мы можем также охарактеризовать Φ' как совокупность всех эндоморфизмов пространства $\mathfrak{R}$, коммутирующих со всеми эндоморфизмами α и со всеми E_{ij}, или, проще, со всеми эндоморфизмами $\sum E_{ij}\alpha_{ij}$. В самом деле, условием для того, чтобы A коммутировало с Φ, является $A\in\mathfrak{L}$. Таким же образом мы видим, что Φ будет совокупностью всех $\mathfrak{L}$-эндоморфизмов пространства $\mathfrak{R}$. В частности, центр[1]) $\mathfrak{C}$ кольца $\mathfrak{L}$ содержится в Φ. Так как $\mathfrak{C}\subseteq\mathfrak{L}$ и элементы из $\mathfrak{C}$ коммутируют со всеми E_{ij}, то $\mathfrak{C}\subseteq\Phi'$. Отсюда следует, что $\mathfrak{C}=\Phi\cap\Phi'$. Если тело Φ коммута-

[1]) Мы употребляем это название для совокупности элементов кольца, коммутирующих со всеми элементами этого кольца.

тивно, то преобразование $\alpha' = \alpha$ и, таким образом, α' не зависит от выбора базиса. Поле Ф будет в этом случае центром в $\mathfrak{L}$. Вернемся к общему случаю, где Ф является телом, и применим найденные нами свойства кольца $\mathfrak{L}$ для получения ряда структурных теорем.

Теорема 5. *Кольцо $\mathfrak{L}$ является простым.*

Напомним, что кольцо $\mathfrak{L}$ называется *простым*, если оно не содержит собственных двусторонних идеалов. Пусть $\mathfrak{B} \neq 0$ будет двусторонним идеалом в $\mathfrak{L} = \Phi_n'$. Если $\sum E_{ij}\beta'_{ij} = B$ является ненулевым элементом в $\mathfrak{B}$, то, в силу (2), мы получаем, что $\beta'_{ij} \in \mathfrak{B}$. По крайней мере одно из них, например $\beta'_{pq} \neq 0$. Но тогда $1 = \beta'_{pq}\beta'^{-1}_{pq} \in \mathfrak{B}$. Следовательно, $\mathfrak{B} = \mathfrak{L}$.

Теорема 6. *Кольцо $\mathfrak{L}$ является прямой суммой неприводимых правых (левых) идеалов.*

Совокупность $E_{kk}\mathfrak{L}$, состоящая из элементов $\sum_j E_{kj}\alpha'_{kj}$, является неприводимым правым идеалом. В самом деле, пусть $\mathfrak{J}$ — ненулевой правый идеал, содержащийся в $E_{kk}\mathfrak{L}$, и пусть $B = \sum_j E_{kj}\beta'_{kj} \in \mathfrak{J}$, где $\beta'_{kl} \neq 0$. Тогда $\mathfrak{J}$ содержит $BE_{lk}\beta'^{-1}_{kl} = E_{kk}$ и, следовательно, все элементы из $E_{kk}\mathfrak{L}$. Очевидно, что

$$\mathfrak{L} = E_{11}\mathfrak{L} \oplus \ldots \oplus E_{nn}\mathfrak{L}.$$

5. Автоморфизмы и обратные автоморфизмы в $\mathfrak{L}$. Пусть F_{ij} являются такими n^2-линейными преобразованиями, что

$$F_{ij}F_{kl} = \delta_{jk}F_{il}, \quad F_{11} + \ldots + F_{nn} = 1. \tag{3}$$

Если y — какой-либо ненулевой вектор, то найдется такое F_{pp}, что $yF_{pp} \neq 0$. Отсюда следует, что векторы $y_i = yF_{pi}$ образуют базис пространства $\mathfrak{N}$ над Ф. В самом деле, если $\sum y_i\beta_i = 0$, то

$$(\sum y_i\beta_i)F_{jp} = \sum y(F_{pi}F_{jp}) = (yF_{pp})\beta_j = 0$$

и, следовательно, $\beta_j = 0$ при $j = 1, \ldots, n$. Относительно y_i мы получаем, что

$$y_rF_{ij} = yF_{pr}F_{ij} = \delta_{ir}yF_{pj} = \delta_{ir}y_j. \tag{4}$$

Если S является таким линейным преобразованием, что $x_iS = y_i$, то S^{-1} определяется равенствами $y_iS^{-1} = x_i$. Из (4) и из определения E_{ij} мы получаем, что $F_{ij} = S^{-1}E_{ij}S$. Важным приложением этого результата является следующая теорема:

Теорема 7. *Каждый автоморфизм кольца $\mathfrak{L}$ имеет вид $\sum E_{ij}\alpha'_{ij} \to S^{-1}(\sum E_{ij}\alpha'^{s}_{ij})S$, где $\alpha' \to \alpha'^{s}$ является автоморфизмом в Φ'.*

Пусть G будет автоморфизмом кольца $\mathfrak{L} = \Phi'_n$. Тогда преобразования $F_{ij} = E^G_{ij}$ удовлетворяют условиям (3) и, следовательно, в $\mathfrak{L}$ найдется такое S, что $E^G_{ij} = S^{-1}E_{ij}S$. Отображение $A \to SA^GS^{-1} \equiv A^H$ является таким автоморфизмом в $\mathfrak{L}$, что $E^H_{ij} = E_{ij}$. Так как Φ' является совокупностью всех элементов, коммутирующих с E_{ij}, то H индуцирует автоморфизм s в Φ' и, следовательно, $(\sum E_{ij}\alpha'_{ij})^H = \sum E_{ij}\alpha'^{s}_{ij}$. Тогда

$$A^G = S^{-1}(\sum E_{ij}\alpha'^{s}_{ij})S.$$

Пусть теперь J — любой обратный автоморфизм в $\mathfrak{L}$. Так как преобразования $F_{ij} = E^J_{ji}$ удовлетворяют условиям (3), то в $\mathfrak{L}$ существует такое S, что $E^J_{ji} = S^{-1}E_{ij}S$. Соответствие $A \to SA^JS^{-1} \equiv A^K$ является обратным автоморфизмом, преобразующим E_{ij} в E_{ji}. Оно индуцирует, таким образом, обратный автоморфизм t в Φ', и

$$(\sum E_{ij}\alpha'_{ij})J = S^{-1}(\sum E_{ji}\alpha'^{t}_{ij})S.$$

Теорема 8. *Кольцо $\mathfrak{L}$ тогда и только тогда обладает обратным автоморфизмом, когда тело Ф обладает обратным автоморфизмом. При этом если $\mathfrak{L}$ обладает обратным автоморфизмом J, то $A^J =$*

$= S^{-1}(\sum E_{ji}\alpha'^{t}_{ij})S$, *где* $S \in \mathfrak{L}$, *и* $\alpha' \to \alpha'^{t}$ *является обратным автоморфизмом в* Φ' [1].

Если обратный автоморфизм J является *инволюцией*, т. е. если $J^2 = 1$, то $E_{ij} = E_{ij}^{J^2} = (S^J S^{-1}) E_{ij} S (S^J)^{-1}$. Следовательно, $S^J = \sigma' S$, где $\sigma' \in \Phi'$. Если $\sigma' \neq -1$, то $S^J + S = (\sigma' + 1) S \equiv T$, и $(\sigma' + 1)$ обладает обратным элементом в Φ'. Тогда $(\sum E_{ij}\alpha'_{ij})^J = T^{-1}(\sum E_{ji}\alpha'^{u}_{ij})\, T$, где $T^J = T$ и $\alpha'^{u} = (\sigma' + 1)\alpha'^{t}(\sigma' + 1)^{-1}$. Таким образом, мы можем предположить с самого начала, что $A^J = S^{-1}A^K S$, где $S^J = \pm S$ и $A^K = \sum E_{ji}\alpha'^{t}_{ij}$. Так как $A^{K^2} = S(SA^JS^{-1})^J S^{-1} = A$, то K — инволюция. Следовательно, t также является инволюцией. Заметим, наконец, что из $S^J = S^{-1}S^K S = \pm S$ следует $S^K = \pm S$.

Теорема 9. *Кольцо* $\mathfrak{L}$ *тогда и только тогда обладает инволюцией, когда тело* Φ *обладает инволюцией. Если* $\mathfrak{L}$ *обладает инволюцией* J, *то* $A^J = S^{-1}(\sum E_{ji}\alpha'^{t}_{ij})\, S$, *где* $\alpha' \to \alpha'^{t}$ *является инволюцией в* Φ', *а* $S \in \mathfrak{L}$ *и удовлетворяет равенству* $\sigma'_{ij} = \sigma'^{t}_{ji}$.

Рассмотрим теперь частный случай, когда Φ коммутативно. Как следствие предыдущих теорем получается следующая

Теорема 10. *Если* Φ *является полем, то всякий автоморфизм в* Φ_n, *оставляющий неподвижными элементы из* Φ, *является внутренним. Каждый обратный автоморфизм в* Φ_n, *оставляющий элементы из* Φ *неподвижными, имеет вид* $A \to S^{-1}A'S \equiv A^J$, *где* A' *является матрицей, получающейся транспонированием матрицы* A. *Обратный автоморфизм* J *будет инволюцией тогда и только тогда, когда* $S' = \pm S$.

6. Перестановочные кольца эндоморфизмов. Предположим, что $n = rs$ и определим

[1] Кольцо Φ тогда и только тогда обладает обратным автоморфизмом, когда им обладает Φ'.

$$G_{\alpha\beta} = \sum_{\mu=0}^{s-1} E_{\mu r+\alpha,\ \mu r+\beta}, \quad \alpha, \beta = 1,2, \ldots, r;$$

$$H_{\varkappa\lambda} = \sum_{\gamma=1}^{r} E_{(\varkappa-1)r+\gamma,\ (\lambda-1)r+\gamma}, \quad \varkappa, \lambda = 1,2, \ldots, s.$$

Легко проверить, что

$$G_{\alpha\beta}G_{\gamma\delta} = \delta_{\beta\gamma}G_{\alpha\delta}, \quad G_{11} + \ldots + G_{rr} = 1, \tag{5}$$

$$H_{\varkappa\lambda}H_{\mu\nu} = \delta_{\lambda\mu}H_{\varkappa\nu}, \quad H_{11} + \ldots + H_{ss} = 1, \tag{6}$$

$$G_{\alpha\beta}H_{\varkappa\lambda} = E_{(\varkappa-1)r+\alpha,\ (\lambda-1)r+\beta} = H_{\varkappa\lambda}G_{\alpha\beta}. \tag{7}$$

Из (7) следует, что каждый элемент в $\mathfrak{L}$ имеет вид $\sum G_{\alpha\beta}B_{\alpha\beta}$, где $B_{\alpha\beta}$ является суммой $\sum H_{\varkappa\lambda}\beta'_{\varkappa\lambda}$, $\beta'_{\varkappa\lambda} \in \Phi'$, и если $\sum G_{\alpha\beta}B_{\alpha\beta} = 0$, то $B_{\alpha\beta} = 0$. Отсюда следует, что $(\Phi_s')_r \cong \Phi'_{sr}$. Таким же образом, всякий элемент имеет одно и только одно выражение вида $\sum H_{\varkappa\lambda}C_{\varkappa\lambda}$, где $C_{\varkappa\lambda}$ имеет вид $\sum G_{\alpha\beta}\gamma'_{\alpha\beta}$, $\gamma'_{\alpha\beta} \in \Phi'$. Если $A = \sum G_{\alpha\beta}B_{\alpha\beta}$, то $B_{\alpha\beta} = \sum G_{\gamma\alpha}AG_{\beta\gamma}$. Следовательно, условием коммутирования A со всеми $G_{\alpha\beta}$ является равенство $A = B_{\alpha\alpha} = B_{\beta\beta} = \sum H_{\varkappa\lambda}\beta'_{\varkappa\lambda}$. Подобным же образом, для того, чтобы A коммутировало со всеми $H_{\varkappa\lambda}$, оно должно иметь вид $\sum G_{\alpha\beta}\gamma'_{\alpha\beta}$.

Пусть теперь Φ_r обозначает кольцо эндоморфизмов пространства $\mathfrak{R}$, имеющих вид $\sum G_{\alpha\beta}\rho_{\alpha\beta}$, где $\rho \in \Phi$. Φ_r-эндоморфизмами являются те Φ-эндоморфизмы, которые коммутируют со всеми $G_{\alpha\beta}$. Следовательно, они являются элементами из $\mathfrak{L}$, коммутирующими со всеми $G_{\alpha\beta}$. Они принадлежат, таким образом, множеству Φ_s' эндоморфизмов вида $\sum H_{\varkappa\lambda}\beta'_{\varkappa\lambda}$. По симметрии, Φ_r может быть охарактеризовано как множество всех Φ_s'-эндоморфизмов в $\mathfrak{R}$.

Предположим теперь, что $\mathfrak{R}$ является коммутативной группой, в которой определено кольцо эндоморфизмов типа Φ_r, где Φ является телом, содержащим тождественный эндоморфизм. Мы предполагаем, таким образом, что 1) существует r^2 эндоморфизмов $G_{\alpha\beta}$ в Φ_r, удовлетворяющих условию (5), 2) для любого ρ из Φ имеет место

$G_{\alpha\beta}\rho = \rho G_{\alpha\beta}$ и 3) каждый эндоморфизм из Φ_r имеет единственное представление в виде $\sum G_{\alpha\beta}\rho_{\alpha\beta}$. Мы предполагаем также, что для Φ_r-подгрупп выполнено условие обрыва возрастающих цепей. Так как $\Phi_r \supseteq \Phi \ni 1$, то $\mathfrak{R}$ является векторным пространством над Φ, хотя *a priori* не ясно, что $\mathfrak{R}$ имеет конечную размерность.

Пусть x будет ненулевым элементом из $\mathfrak{R}$. Так как $\sum G_{\alpha\alpha} = 1$, то существует такое $G_{\delta\delta}$, что $xG_{\delta\delta} \neq 0$. Положим $x_\alpha = xG_{\delta\alpha}$. Тогда эти элементы линейно независимы над Φ. Если $\mathfrak{R}_1$ обозначает множество элементов $\sum x_\alpha\rho_\alpha$, где $\rho \in \Phi$, то $\mathfrak{R}_1$ является Φ_r-подгруппой. Пусть $\mathfrak{R}_1 \neq \mathfrak{R}$ и пусть y является не лежащим в $\mathfrak{R}_1$ вектором. Как и ранее, найдется такое $G_{\varepsilon\varepsilon}$, что $yG_{\varepsilon\varepsilon} \notin \mathfrak{R}_1$, и если положить $x_{r+\alpha} = yG_{\varepsilon\alpha}$, то элементы вида $\sum x_{r+\alpha}\rho_\alpha$ образуют Φ_r-подгруппу $\mathfrak{R}_2$, независимую от $\mathfrak{R}_1$ в том смысле, что $\mathfrak{R}_1 \cap \mathfrak{R}_2 = 0$. Если $\mathfrak{R}_1 + \mathfrak{R}_2 \neq \mathfrak{R}$, то мы можем повторить этот процесс, получая таким образом цепь $\mathfrak{R}_1 \subset \mathfrak{R}_1 + \mathfrak{R}_2 \subset \ldots$. Согласно предположению о конечности таких цепей, она оборвется, и мы получим $\mathfrak{R} = \mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_s$. Следовательно, $\mathfrak{R}$ имеет конечную размерность $n = rs$ над Φ.

Теорема 11. *Пусть $\mathfrak{R}$ — коммутативная группа и Φ_r — матричное кольцо эндоморфизмов группы $\mathfrak{R}$, где Φ является телом. Если $\mathfrak{R}$ удовлетворяет условию обрыва возрастающих цепей для Φ_r-подгрупп, то она имеет конечную размерность $n = rs$ над Φ и $\mathfrak{R} = \mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_s$, где $\mathfrak{R}_i$ являются неприводимыми Φ_r-подгруппами.*

Неприводимость $\mathfrak{R}_i$ доказывается следующим образом: если z является некоторым ненулевым вектором в $\mathfrak{R}$, то существует такое ζ, что $zG_{\zeta 1}, \ldots, zG_{\zeta r}$ независимы над Φ. Следовательно, множество $z\Phi_r = \mathfrak{R}_i$ для любого $z \neq 0$ в $\mathfrak{R}_i$.

Если мы используем базис $x_1, \ldots, x_n$, определенный выше для $\mathfrak{R}$ над Φ, и определим линейные преобразования E_{ij} так же, как и выше, то получим: $G_{\alpha\beta} = \sum_{\mu=0}^{s-1} E_{\mu r+\alpha,\, \mu r+\beta}$. Итак, преобразование $G_{\alpha\beta}$ линейно в $\mathfrak{R}$ над Φ и производит то же действие на x_i, как и

$\sum_{\mu=0}^{s-1} E_{\mu r+\alpha,\, \mu r+\beta}$. Следовательно, мы можем использовать предыдущее рассуждение и получить следующую теорему.

Теорема 12. *Пусть Φ_r является таким матричным кольцом эндоморфизмов в коммутативной группе $\mathfrak{R}$, что в нем выполнены условия предыдущей теоремы. Тогда кольцо эндоморфизмов, коммутирующих с данными эндоморфизмами, имеет вид Φ_s', где Φ' является телом, обратно изоморфным телу Φ. Первоначальная совокупность эндоморфизмов Φ_r дудет полной совокупностью эндоморфизмов, коммутирующих с Φ_s'.*

7. Изоморфизм матричных колец. Предположим теперь, что мы имеем такое кольцо, которое может рассматриваться и как матричное кольцо Φ_n' и как Ψ_r', где Φ' и Ψ' являются телами. Тогда мы можем предположить, что Φ_n' является кольцом линейных преобразований n-мерного векторного пространства $\mathfrak{R}$ над Φ, где Φ обратно изоморфно Φ'. Пусть $G_{\alpha\beta}$ ($\alpha, \beta = 1, \ldots, r$) являются матричными единицами в Ψ_r'. Эндоморфизмы $\sum G_{\alpha\beta}\rho_{\alpha\beta}$, где $\rho_{\alpha\beta} \in \Phi$, образуют кольцо Φ_r, и мы видели, что размерность $\mathfrak{R}$ над Φ равна $rs = n$. Следовательно, $r \leqslant n$. Меняя местами Φ' и Ψ', мы получаем, что $n \leqslant r$ и, следовательно, $r = n$. Отсюда следует, что существует такое линейное преобразование S, что $G_{ij} = S^{-1}E_{ij}S$, где E_{ij} являются матричными единицами для Φ_n'. Так как элементы ψ' из Ψ' могут быть охарактеризованы как линейные преобразования, коммутирующие с G_{ij}, а элементы из Φ' — как линейные преобразования, коммутирующие с E_{ij}, то мы получаем, что $\Psi' = S^{-1}\Phi'S$.

Теорема 13. *Если $\Phi_n' = \Psi_r'$, где Φ' и Ψ' являются телами, то $r = n$, а Φ' и Ψ' изоморфны, причем в Φ_n' найдется такой элемент S, что $\Psi' = S^{-1}\Phi'S$ и $G_{ij} = S^{-1}E_{ij}S$ для соответствующих матричных единиц.*

8. Полулинейные преобразования. Мы рассмотрим сейчас один тип преобразований векторного пространства, впервые изучавшийся Сегре, который представляет собою

обобщение понятия линейного преобразования. Пусть S является автоморфизмом в теле Ф. Тогда преобразование T пространства $\mathfrak{R}$ называется *полулинейным преобразованием* $\mathfrak{R}$ над Ф, если

$$(x+y)\,T = xT + yT,\ (x\alpha)\,T = (xT)\alpha^S \qquad (8)$$

для всех x, y из $\mathfrak{R}$ и всех $\alpha \in \Phi$. Если $T \neq 0$, то S однозначно определяется преобразованием T. В самом деле, тогда существует такой вектор u, что $uT \neq 0$, и если S и S' являются такими автоморфизмами в Ф, для которых выполняется (8), то для всех α мы имеем $(uT)\alpha^S = (uT)\alpha^{S'}$. Следовательно, $\alpha^S = \alpha^{S'}$ и $S = S'$. Мы назовем S *автоморфизмом* преобразования T.

Из условия $\alpha T = T\alpha^S$ следует, очевидно, что эндоморфизм T коммутирует с множеством эндоморфизмов Ф. Если $S = 1$, то T, разумеется, коммутирует с каждым элементом из Ф, и T является линейным преобразованием. Из перестановочности T и Ф следует, что полулинейное преобразование отображает каждое подпространство $\mathfrak{S} \subset \mathfrak{R}$ в другое подпространство. Очевидно также, что если $\mathfrak{S}_1$ и $\mathfrak{S}_2$ являются такими подпространствами, что $\mathfrak{S}_1 \subseteq \mathfrak{S}_2$, то образ $\mathfrak{S}_1 T$ содержится в образе $\mathfrak{S}_2 T$. Так как для любых двух подпространств $\mathfrak{S}_1$, $\mathfrak{S}_2$ подпространство $\mathfrak{S}_1 + \mathfrak{S}_2$ может быть определено как наименьшее подпространство, содержащее $\mathfrak{S}_1$ и $\mathfrak{S}_2$, то если T является взаимнооднозначным полулинейным преобразованием, мы будем иметь $(\mathfrak{S}_1 + \mathfrak{S}_2)\,T = \mathfrak{S}_1 T + \mathfrak{S}_2 T$. Таким же образом получаем $(\mathfrak{S}_1 \cap \mathfrak{S}_2)\,T = \mathfrak{S}_1 T \cap \mathfrak{S}_2 T$. Поэтому всякое взаимнооднозначное полулинейное преобразование векторного пространства $\mathfrak{R}$ индуцирует структурный автоморфизм в структуре подпространств пространства $\mathfrak{R}$. По этой причине полулинейные преобразования применяются наравне с линейными преобразованиями в проективной геометрии.

Если T является произвольным полулинейным преобразованием, то мы обозначим через $\mathfrak{N} = \mathfrak{N}(T)$ пространство таких векторов z, что $zT = 0$, и предположим, что вектора $z_1, \ldots, z_r$ образуют базис этого пространства. Определим такое подпространство $\mathfrak{S}$, что $\mathfrak{R} = \mathfrak{N} \oplus \mathfrak{S}$, и пусть векторы $y_1, \ldots, y_{n-r}$ образуют базис в $\mathfrak{S}$. Из

этого непосредственно следует, что $y_1 T, \ldots, y_{n-r} T$ является базисом для $\mathfrak{R}T$. Следовательно, если мы назовем размерность $\mathfrak{R}T$ *рангом* T и размерность $\mathfrak{N}T$ *индексом дефекта* T, то получим следующее обобщение хорошо известной теоремы о линейных уравнениях:

$$\text{ранг } T + \text{индекс дефекта } T = n.$$

Если $x_1, \ldots, x_n$ образуют базис $\mathfrak{R}$ над Ф, то мы можем написать $x_i T = \sum x_j \tau_{ji}$ и назвать (τ_{ij}) *матрицей* преобразования T относительно этого базиса. Полулинейное преобразование T определяется своей *матрицей* и своим автоморфизмом, так как $\left(\sum x_i \xi_i\right) T = \sum x_j \tau_{ji} \xi_i^S$. С помощью координат $(\xi_1, \ldots, \xi_n)$ вектора x мы можем определить T как преобразование, переводящее $(\xi_1, \ldots, \xi_n)$ в $(\eta_1, \ldots, \eta_n)$, где $\eta_j = \sum \tau_{ji} \xi_i$. Если теперь (τ_{ij}) является некоторой матрицей и S некоторым автоморфизмом, то равенство $\left(\sum x_i \xi_i\right) T = \sum x_j \tau_{ji} \xi_i^S$ определяет полулинейное преобразование, имеющее автоморфизм S и, относительно базиса $x_1, \ldots, x_n$, матрицу (τ_{ij}).

Если $y_1, \ldots, y_n$ является другим базисом пространства $\mathfrak{R}$ над Ф и $y_i = \sum x_j \beta_{ji}$, то простое вычисление показывает, что матрицей полулинейного преобразования T относительно этого базиса будет $(\beta)^{-1}(\tau)(\beta^S)$, где (τ) является его матрицей относительно базиса $x_1, \ldots, x_n$. Следовательно, теория полулинейных преобразований соответствует теории матриц с элементами из тела, в которой две матрицы (τ) и (σ) считаются эквивалентными, если существует такая матрица (β), что $(\sigma) = (\beta)^{-1}(\tau)(\beta^S)$, где S некоторый фиксированный автоморфизм.

Предположим теперь, что Γ является некоторым множеством полулинейных преобразований. Если $\mathfrak{S}$ собственное подпространство в $\mathfrak{R}$, инвариантное относительно всех $T \in \Gamma$, то мы можем найти такой базис $y_1, \ldots, y_n$ для $\mathfrak{R}$, что элементы $y_1, \ldots, y_r$ образуют базис в $\mathfrak{S}$ $(0 < r < n)$. Тогда матрица T относительно этого базиса имеет вид $\begin{pmatrix} \tau_1 & * \\ 0 & \tau_2 \end{pmatrix}$, где (τ_1) является матрицей преобразования T в $\mathfrak{S}$ и (τ_2) матрицей преобразования T в фактор-пространстве $\mathfrak{R}/\mathfrak{S}$.

Обратно, при существовании базиса, относительно которого матрицы из Γ имеют эту „приведенную" форму, пространство $\mathfrak{R}$ будет приводимо, если рассматривать его как группу относительно множества операторов $\Omega = (\Gamma, \Phi)$ — теоретико-множественной суммы Γ и Φ. Принимая во внимание соотношение между матрицами полулинейного преобразования, мы можем сформулировать это условие также в следующей форме: если (τ) является матрицей для T относительно базиса $x_1, x_2, \ldots, x_n$ и S является автоморфизмом преобразования T, то существует такая не зависящая от T матрица (β), что $(\beta)^{-1}(\tau)\,(\beta^S) = \begin{pmatrix} \tau_1 & * \\ 0 & \tau_2 \end{pmatrix}$.

Пусть теперь $\mathfrak{R} = \mathfrak{R}_s \supset \mathfrak{R}_{s-1} \supset \ldots \supset \mathfrak{R}_1 \supset 0$ будет композиционным рядом в $\mathfrak{R}$ относительно Ω. Выберем такой базис $y_1, \ldots, y_n$ для $\mathfrak{R}$ над Φ, что $y_1, \ldots, y_{n_1}$ образуют базис для $\mathfrak{R}_1$, $y_{n_1+1}, \ldots, y_{n_1+n_2}$ базис для $\mathfrak{R}_2$ и т. д. Тогда если (β) является матрицей перехода от базиса $x_1, \ldots, x_n$ к базису $y_1, \ldots, y_n$, то матрицей преобразования T относительно элементов y будет

$$(\beta)^{-1}(\tau)\,(\beta^S) = \begin{pmatrix} \tau_1 & & & * \\ & \tau_2 & & \\ & & \ddots & \\ 0 & & & \tau_s \end{pmatrix}, \qquad (9)$$

где (τ_i) является матрицей полулинейного преобразования, индуцированного в $\mathfrak{R}_i/\mathfrak{R}_{i-1}$ преобразованием T, а ниже этих матриц стоят нули. Неприводимость $\mathfrak{R}_i/\mathfrak{R}_{i-1}$ равносильна следующим образом определенной неприводимости матрицы: невозможно найти такую не зависящую от T матрицу (β_i), чтобы $(\beta_i)^{-1}(\tau_i)\,(\beta_i^S)$ имело приведенную форму $\begin{pmatrix} \tau_{i1} & * \\ 0 & \tau_{i2} \end{pmatrix}$. Обратно, если (β) является матрицей, для которой имеет место (9), причем матрицы (τ_i) неприводимы, то $(\beta)^{-1}(\tau)\,(\beta^S)$ получается указанным путем из композиционного ряда.

Подобным же образом мы находим, что если $\mathfrak{R} = \mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_s$, где $\mathfrak{R}_j\,(\neq 0)$ являются Ω-подгруппами, то существует такая матрица (β), что

$$(\beta)^{-1}(\tau)\,(\beta^S) = \begin{pmatrix} \tau_1 & & & 0 \\ & \tau_2 & & \\ & & \ddots & \\ 0 & & & \tau_s \end{pmatrix}$$

для всех T, причем в этом случае нули стоят по обеим сторонам диагонали, а (τ_i) является матрицей преобразования, которое T индуцирует в $\mathfrak{R}_i$.

Отметим теперь следующие комбинаторные свойства множества полулинейных преобразований. Если T_1 и T_2 являются полулинейными преобразованиями с автоморфизмами S_1 и S_2, то $T_1 T_2$ будет полулинейным преобразованием с автоморфизмом $S_1 S_2$. Если $S_1 = S_2 = S$, то $T_1 + T_2$ является полулинейным преобразованием с автоморфизмом S, а если преобразование T_1 взаимнооднозначно, то T_1^{-1} будет полулинейным преобразованием с автоморфизмом S_1^{-1}.

Если теперь (τ_1) и (τ_2) — матрицы преобразований T_1 и T_2 относительно одного и того же базиса, то матрицей преобразования $T_1 T_2$ будет $(\tau_2)\,(\tau_1^{S_2})$. Таким образом, матрицей преобразования T^k будет $(\tau)\,(\tau^S)\ldots(\tau^{S^{k-1}})$. Если T взаимнооднозначно, то матрицей преобразования T^{-1} является $(\tau^{S^{-1}})^{-1}$. Если T_1 и T_2 обладают одним и тем же автоморфизмом, то матрицей преобразования $T_1 + T_2$ будет $(\tau_1) + (\tau_2)$. Из вышеизложенного следует, что соответствие между линейным преобразованием T и его матрицей (τ) является обратным автоморфизмом между кольцом линейных преобразований $\mathfrak{L}$ и кольцом матриц Φ_n. Так как Φ связано инвариантным образом с $\mathfrak{L}$, то это соответствие имеет известные преимущества по сравнению с ранее отмеченным соответствием между $\mathfrak{L}$ и Φ'_n.

Как приложения этих вычислений и результатов первой главы отметим следующие теоремы о матрицах из Φ_n.

Теорема 14. *Если* (ε_i) $(i = 1, \ldots, s)$ *являются такими ненулевыми матрицами из* Φ_n, *что*

$$(\varepsilon_i)^2 = (\varepsilon_i),\ (\varepsilon_i)(\varepsilon_j) = 0,\ \text{если } i \neq j \text{ и } \sum (\varepsilon_i) = 1,$$

то существует такая невырождающаяся матрица (β) *в* Φ_n, *что*

$$(\beta)^{-1}(\varepsilon_1)(\beta) = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & 0 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \begin{matrix} \\ \\ \} n_1 \\ \\ \\ \\ \end{matrix}, \quad (\beta)^{-1}(\varepsilon_2)(\beta) =$$

$$= \begin{pmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & 1 & \\ & & & & \ddots \\ & & & & & 0 \end{pmatrix} \begin{matrix} \\ \\ \} n_1 \\ \\ \\ \\ \end{matrix}, \ldots \qquad (10)$$

Это получается при рассмотрении (ε_i) как матрицы таких линейных преобразований E_i, что

$$E_i^2 = E_i \neq 0,\ E_i E_j = 0, \quad \text{если } i \neq j, \sum E_i = 1.$$

Тогда $\mathfrak{R} = \mathfrak{R}E_1 \oplus \ldots \oplus \mathfrak{R}E_s$, и потому относительно подходящего базиса мы получаем матрицы (10) для $E_1, E_2, \ldots$

Если T является полулинейным преобразованием, то мы можем применить замечание, следующее за леммой Фиттинга, и получим разложение $\mathfrak{R} = \mathfrak{N} \oplus \mathfrak{S}$, где $\mathfrak{N}$ и $\mathfrak{S}$ являются инвариантными относительно T подпространствами, причем преобразование T нильпотентно в $\mathfrak{N}$ и не вырождается в $\mathfrak{S}$. Отсюда вытекает следующая

Теорема 15. *Если* (τ) *является матрицей в* Φ_n, *а* S *— автоморфизм в* Φ, *то существует такая матрица* (β), *что*

$$(\beta)^{-1}(\tau)(\beta^S) = \begin{pmatrix} \nu & 0 \\ 0 & \sigma \end{pmatrix},$$

где $(\nu) \ldots (\nu^{S^k}) = 0$ *для достаточно больших* k *и матрица* (σ) *обратима.*

Глава 3

НЕКОММУТАТИВНЫЕ ОБЛАСТИ ГЛАВНЫХ ИДЕАЛОВ

1. Определения и примеры. При изучении линейного преобразования, или, более обще, полулинейного преобразования T с автоморфизмом S, мы обычно интересуемся кольцом преобразований $\Phi[T]$, порожденным преобразованием T и скалярными умножениями $x \to x\alpha$. Очевидно, что $\Phi[T]$ содержит преобразования $\alpha_0 + T\alpha_1 + T^2\alpha_2 + \ldots + T^m\alpha_m$. С другой стороны, $(T^k\alpha)(T^l\beta) = T^{k+l}\alpha^{S^l}\beta$, и потому множество полиномов от T замкнуто относительно умножения. Отсюда следует, что $\Phi[T]$ совпадает с совокупностью этих полиномов. Нам будет удобно теперь ввести некоторое кольцо $\Phi[t, S]$ полиномов от неизвестного t. Пусть сначала Φ является абстрактным телом, изоморфным кольцу эндоморфизмов Φ векторного пространства $\mathfrak{R}$ [1]), и пусть $\Phi[t, S]$ обозначает совокупность полиномов

$$\alpha_0 + t\alpha_1 + t^2\alpha_2 + \ldots + t^m\alpha_m,$$

где t является неизвестным, и коэффициенты α_i лежат в Φ. Мы будем считать, что $\alpha_0 + t\alpha_1 + \ldots + t^m\alpha_m = \beta_0 + t\beta_1 + \ldots + t^{m'}\beta_{m'}$ тогда и только тогда, когда $\alpha_0 = \beta_0$, $\alpha_1 = \beta_1, \ldots$. Сложение полиномов определим по правилу $(\alpha_0 + t\alpha_1 + \ldots) + (\beta_0 + t\beta_1 + \ldots) = (\alpha_0 + \beta_0) + t(\alpha_1 + \beta_1) + \ldots$. Умножение мы определим с помощью дистрибутивного закона и формулы

$$(t^k\alpha)(t^l\beta) = t^{k+l}\alpha^{S^l}\beta.$$

Легко проверить, что $\Phi[t, S]$ является кольцом.

Мы можем теперь поставить в соответствие полиному $\alpha_0 + t\alpha_1 + \ldots + t^m\alpha_m$ эндоморфизм $\alpha_0 + T\alpha_1 + \ldots + T^m\alpha_m \in \Phi[T]$. Наше соответствие будет тогда представлением $\Phi[t, S]$ в $\mathfrak{R}$, и $\mathfrak{R}$ будет $\Phi[t, S]$-модулем.

Если $\alpha(t) = \alpha_0 + \ldots + t^m\alpha_m$, $\alpha_m \neq 0$, то m называется *степенью* полинома $\alpha(t)$. Степенью нуля будем считать $-\infty$ и заметим, что тогда

$$\deg[\alpha(t) + \beta(t)] = \max(\deg\alpha(t), \deg\beta(t)),$$
$$\deg[\alpha(t)\beta(t)] = \deg\alpha(t) + \deg\beta(t).$$

Второе равенство показывает, что в $\Phi[t, S]$ отсутствуют делители нуля, т. е. что $\Phi[t, S]$ является областью целостности. Отметим также, что обратимыми элементами в этой области целостности будут лишь отличные от нуля элементы тела Φ. Пусть теперь $\beta(t) = \beta_0 + \ldots + t^{m'}\beta_{m'}$, где $\beta_{m'} \neq 0$, и $m' \leqslant m$. Тогда $\alpha(t) - \beta(t)\, t^{m-m'}(\beta_{m'}^{-1})^{S^{m-m'}}\alpha_m = \alpha_0' + t\alpha_1' + \ldots + t^{m-1}\alpha'_{m-1}$. Следовательно, если мы продолжим этот процесс деления, то получим такие полиномы $\gamma(t)$ и $\rho(t)$, что

$$\alpha(t) = \beta(t)\gamma(t) + \rho(t),$$

где $\deg\rho(t) < \deg\beta(t)$. Подобным же образом мы можем найти такие полиномы $\gamma_1(t)$ и $\rho_1(t)$, что $\alpha(t) = \gamma_1(t)\beta(t) + \rho_1(t)$, причем $\deg\rho_1(t) < \deg\beta(t)$.

Пусть теперь $\mathfrak{J}$ является ненулевым правым идеалом в $\Phi[t, S]$. Выберем в $\mathfrak{J}$ элемент $\beta(t) \neq 0$, имеющий наименьшую степень среди всех ненулевых элементов идеала $\mathfrak{J}$. Тогда, если $\alpha(t)$ является произвольным элементом из $\mathfrak{J}$, то $\alpha(t) = \beta(t)\gamma(t) + \rho(t)$, где $\deg\rho(t) < \deg\beta(t)$, а так как $\rho(t) = \alpha(t) - \beta(t)\gamma(t) \in \mathfrak{J}$, то $\rho(t) = 0$ в силу минимальности степени полинома $\beta(t)$. Таким образом, $\alpha(t) = \beta(t)\gamma(t)$, и потому $\mathfrak{J} = \beta(t)\Phi[t, S]$, где $\beta(t)\Phi[t, S]$ является идеалом, состоящим из правых крат-

[1]) Для наших целей нет необходимости делать различие в обозначениях между этими двумя совокупностями.

ных полинома $\beta(t)$. Идеал такого вида мы будем называть *главным правым идеалом*. Аналогично, всякий левый идеал является главным в том смысле, что он имеет вид $\Phi[t, S]\beta(t)$. Мы будем теперь называть область целостности $\mathfrak{o}$ *областью главных идеалов*, если каждый правый идеал является правым главным идеалом $a\mathfrak{o}$ и каждый левый идеал является главным левым идеалом $\mathfrak{o}a$. Таким образом, $\Phi[t, S]$ является примером области такого типа. Можно проверить, что следующие кольца также являются областями главных идеалов.

1) Кольцо целых чисел.

2) Любое тело.

3) Подкольцо гамильтоновской алгебры кватернионов, состоящее из элементов вида $1\alpha_0 + i\alpha_1 + j\alpha_2 + k\alpha_3$, где коэффициенты α_i либо все являются целыми рациональными числами, либо все они являются половинами нечетных целых чисел.

4) Кольцо $\Phi[t, ']$ дифференциальных полиномов. Кольцо этих полиномов определяется таким же образом, как и кольцо $\Phi[t, S]$, причем правило $\alpha t = t\alpha^S$ заменяется правилом $\alpha t = t\alpha + \alpha'$ и $(\alpha+\beta)' = \alpha' + \beta'$, $(\alpha\beta)' = \alpha\beta' + \alpha'\beta$.

В этой главе мы изучим детально теорию областей главных идеалов. Основные приложения, относящиеся к теории полулинейных преобразований, получаются при рассмотрении кольца $\Phi[t, S]$.

2. Элементарные свойства. Пусть $\mathfrak{o}$ является областью главных идеалов. Если $a\mathfrak{o}$ и $b\mathfrak{o}$ — ненулевые идеалы, причем $a\mathfrak{o} \supseteq b\mathfrak{o}$, то $b = ac$, или, иными словами, a является левым делителем элемента b. Если $a\mathfrak{o} = b\mathfrak{o}$, то $au = b$ и $bv = a$. Следовательно, $a = auv$ и $a(1 - uv) = 0$, а потому $uv = 1$. Подобно этому, $vu = 1$, и, таким образом, u и v являются обратимыми элементами в $\mathfrak{o}$.[1] Следовательно, a и b ассоциированы справа. Подобное же замечание справедливо и для левых идеалов. В этой главе мы будем

[1] Если $\mathfrak{o}$ является областью целостности и $uv = 1$ в кольце $\mathfrak{o}$, то $(1 - vu)v = 0$; следовательно, также и $vu = 1$.

иметь полный параллелизм между теорией правых и теорией левых идеалов, и поэтому все результаты будут выводиться и формулироваться лишь для правых идеалов.

Если $a_1\mathfrak{o} \subseteq a_2\mathfrak{o} \subseteq \ldots$ является цепью правых идеалов, то их теоретико-множественное объединение также является правым идеалом и, следовательно, имеет вид $a\mathfrak{o}$. Так как для некоторого N мы имеем $a \in a_N\mathfrak{o}$, то $a\mathfrak{o} = a_N\mathfrak{o} = a_{N+1}\mathfrak{o} = \ldots$. Предположим теперь, что $a_1\mathfrak{o} \supseteq a_2\mathfrak{o} \supseteq \ldots$ является убывающей цепью и что все $a_i\mathfrak{o}$ содержат фиксированный отличный от нуля элемент b. Тогда $b = a_ib_i$, $a_i = a_{i-1}c_{i-1}$ и, следовательно, $b = a_{i-1}(c_{i-1}b_i) = a_{i-1}b_{i-1}$. Отсюда вытекает, что $b_{i-1} = c_{i-1}b_i$ и $\mathfrak{o}\,b_1 \subseteq \mathfrak{o}\,b_2 \subseteq \ldots$, а потому для достаточно большого N имеем $\mathfrak{o}b_N = \mathfrak{o}b_{N+1} = \ldots$. Таким образом, элементы $c_N, c_{N+1}, \ldots$ обратимы, и $a_N\mathfrak{o} = a_{N+1}\mathfrak{o} = \ldots$. Отметим, что условие обрыва убывающих цепей справедливо лишь в том случае, когда $\mathfrak{o}$ является телом. В самом деле, предположим, что a является ненулевым элементом в $\mathfrak{o}$, и рассмотрим цепь $a\mathfrak{o} \supseteq a^2\mathfrak{o} \supseteq \ldots$. Пусть k является таким целым числом, что $a^k\mathfrak{o} = a^{k+1}\mathfrak{o}$. Тогда $a^{k+1} = a^ku$, где элемент u обратим, а поэтому и $a = u$ является обратимым элементом.

Теорема 1. *Для правых идеалов области главных идеалов $\mathfrak{o}$ имеет место условие обрыва возрастающих цепей. Убывающая цепь правых идеалов, пересечение которых отлично от нулевого элемента, содержит лишь конечное число различных идеалов. Если условие обрыва убывающих цепей выполнено без ограничений, то $\mathfrak{o}$ является телом.*

Пусть a и b будут отличными от нуля элементами; рассмотрим идеал $a\mathfrak{o} + b\mathfrak{o}$, состоящий из всех элементов вида $ax + by$, где x и y являются произвольными элементами кольца $\mathfrak{o}$. Этот идеал является наименьшим идеалом, содержащим $a\mathfrak{o}$ и $b\mathfrak{o}$. Пусть теперь $a\mathfrak{o} + b\mathfrak{o} = d\mathfrak{o}$. Тогда $d = ap + bq$ будет общим наибольшим левым делителем элементов a и b, т. е. d является левым делителем a и b, и всякий левый делитель элементов a и b будет левым делителем элемента d. Элемент d определен

с точностью до обратимого правого делителя. Каждый из определенных таким образом элементов d мы будем обозначать через (a, b). Пусть теперь $a = da_1$ и $b = db_1$. Тогда $a(1 - pa_1) = da_1 - apa_1 = bqa_1$, и аналогично $b(1 - qb_1) = apb_1$. Так как ни элемент p, ни элемент q не равны нулю, то тем самым доказано, что пересечение $a\mathfrak{o} \cap b\mathfrak{o} = m\mathfrak{o} \neq 0$. Элемент m является общим наименьшим правым кратным элементов a и b в обычном смысле слова: m является общим правым кратным элементов a и b, причем всякое другое общее правое кратное элементов a и b является правым кратным элемента m. Обозначим элемент m через $[a, b]$, заметив при этом, что он определен лишь с точностью до обратимого правого делителя.

Теорема 2. *Любые два ненулевые элемента a и b обладают общим наибольшим левым делителем (a, b) и общим наименьшим правым кратным $[a, b]$, которые определены с точностью до обратимого правого множителя.*

Существование общих правых кратных, отличных от нуля, дает нам возможность применить обычную конструкцию дробей для получения тела отношений области $\mathfrak{o}$. Для этой цели рассмотрим пары (a, b), где $b \neq 0$. Будем считать, что (a, b) эквивалентно (c, d), если при $m = bd_1 = db_1$, мы имеем $ad_1 = cb_1$. Это соотношение является симметричным, рефлексивным и транзитивным. Обозначим совокупность пар (c, d), эквивалентных паре (a, b), через a/b. Определим $a/b + c/d = (ad_1 + cb_1)/m$. Если $c \neq 0$ и $n = bc_2 = cb_2$, то положим $(a/b)(c/d) = ac_2/db_2$. Для $c = 0$ положим $(a/b)(0/d) = 0/d$. Легко видеть, что сумма и произведение определены таким образом однозначно и что совокупность всех a/b, называющихся (правыми) *дробями*, образует тело Φ относительно определенных таким образом сложения и умножения. Тело Φ содержит подкольцо $\bar{\mathfrak{o}}$, состоящее из элементов $a/1$, которые находятся в изоморфном соответствии с элементами кольца $\mathfrak{o}$. Таким образом, если мы заменим кольцо $\mathfrak{o}$ кольцом $\bar{\mathfrak{o}}$, то мы можем считать, что область $\mathfrak{o}$ является подкольцом тела Φ. Элемент a/b равен $(a/1)(b/1)^{-1}$, и потому Φ является наименьшим подтелом в Φ, содержащим кольцо $\mathfrak{o}$.

3. $\mathfrak{o}$-модуль с конечным числом образующих. Предположим, что $\mathfrak{o}$ является произвольным кольцом с единицей и что $\mathfrak{M}$ является $\mathfrak{o}$-модулем, в котором для всех x $x1 = x$. Напомним, что, по определению, для всех элементов x, y из $\mathfrak{M}$ и для всех элементов a, b из $\mathfrak{o}$ выполняются соотношения:

$$(x + y)a = xa + ya,$$
$$x(a + b) = xa + xb,$$
$$x(ab) = (xa)b.$$

Мы будем говорить, что модуль $\mathfrak{M}$ имеет *конечное число образующих*, если в $\mathfrak{M}$ существуют такие n элементов $x_1, x_2, \ldots, x_n$, называемых *образующими*, что любой элемент из $\mathfrak{M}$ может быть представлен в виде $\sum x_i a_i$, где $a_i \in \mathfrak{o}$. Если для подмодулей модуля $\mathfrak{M}$ выполнено условие обрыва возрастающих цепочек, то легко видеть, что модуль $\mathfrak{M}$ имеет конечное число образующих.

Предположим теперь, что $\mathfrak{N}$ является подмодулем модуля $\mathfrak{M}$, и пусть $\mathfrak{J}_i \equiv \mathfrak{J}_i(\mathfrak{N})$ обозначает совокупность элементов a_i, встречающихся в качестве коэффициентов при x_i в элементах подмодуля $\mathfrak{N}$, имеющих вид $x_i a_i + x_{i+1}a_{i+1} + \ldots + x_n a_n$. Тогда $\mathfrak{J}_i$ является правым идеалом. Очевидно, что если $\mathfrak{N}$ лежит во втором подмодуле $\mathfrak{P}$, то $\mathfrak{J}_i(\mathfrak{N}) \subseteq \mathfrak{J}_i(\mathfrak{P})$. С другой стороны, легко показать, что если $\mathfrak{N} \subseteq \mathfrak{P}$ и для всех $i = 1, \ldots, n$ имеем $\mathfrak{J}_i(\mathfrak{N}) = \mathfrak{J}_i(\mathfrak{P})$, то $\mathfrak{N} = \mathfrak{P}$. Это замечание позволяет нам доказать следующую теорему.

Теорема 3. *Если $\mathfrak{o}$ является кольцом, удовлетворяющим условию обрыва возрастающих (убывающих) цепей правых идеалов, то каждый $\mathfrak{o}$-модуль $\mathfrak{M}$ с конечным числом образующих удовлетворяет условию обрыва возрастающих (убывающих) цепей подмодулей.*

В самом деле, пусть $\mathfrak{M}_1 \subseteq \mathfrak{M}_2 \subseteq \ldots$ является возрастающей цепью подмодулей и пусть $\mathfrak{J}_i^{(k)} = \mathfrak{J}_i(\mathfrak{M}_k)$. Тогда $\mathfrak{J}_i^{(1)} \subseteq \mathfrak{J}_i^{(2)} \subseteq \ldots$, и, следовательно, найдется такое целое число N, что для всех i имеем $\mathfrak{J}_i^{(N)} = \mathfrak{J}_i^{(N+1)} = \ldots$. Отсюда

следует, что $\mathfrak{M}_N = \mathfrak{M}_{N+1} = \ldots$. Таким же образом рассматривается случай обрыва убывающих цепей.

Если элементы модуля $\mathfrak{M}$ могут быть одним и только одним образом представлены в виде $\sum x_i a_i$, то $\mathfrak{M}$ называется *свободным* модулем с *базисом* $x_1, \ldots, x_n$. Эквивалентным условием будет то, что элементы x_i являются образующими модуля $\mathfrak{M}$ и $\sum x_i d_i = 0$ только тогда, когда все $d_i = 0$. Так же как и для тел (см. главу 2), мы можем для любого кольца $\mathfrak{o}$ построить свободный модуль с заранее заданным числом элементов базиса. Но теорема инвариантности числа элементов базиса не будет справедливой, если на кольцо $\mathfrak{o}$ не наложить никаких ограничений. Таким образом, может случиться, что в модуле $\mathfrak{M}$ существуют элементы $y_1, \ldots, y_m$, порождающие все $\mathfrak{M}$, причем $m < n$. Мы покажем теперь, что теорема инвариантности справедлива при любом из следующих предположений:

1) $\mathfrak{o}$ является подкольцом некоторого тела;

2) Для правых идеалов кольца $\mathfrak{o}$ выполнено условие обрыва возрастающих цепей.

Предположим, в самом деле, что $\mathfrak{M}$ имеет $m < n$ образующих $y_k = \sum x_i a_{ik}$ [1]). Тогда каждый элемент $x_i = \sum y_k b_{ki}$, и, следовательно, $x_i = \sum x_j a_{jk} b_{ki}$. В силу единственности представления, имеем $\sum a_{jk} b_{ki} = \delta_{ji}$, так что

$$(a)(b) \equiv$$

$$\equiv \begin{pmatrix} a_{11} & \ldots a_{1m} & 0 \ldots 0 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_{m1} & \ldots a_{mm} & 0 \ldots 0 \\ a_{m+11} & \ldots a_{m+1m} & 0 \ldots 0 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ a_{n1} & \ldots a_{nm} & 0 \ldots 0 \end{pmatrix} \begin{pmatrix} b_{11} & \ldots b_{1m} & b_{1m+1} & \ldots b_{1n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ b_{m1} & \ldots b_{mm} & b_{mm+1} & \ldots b_{mn} \\ 0 & \ldots 0 & 0 & \ldots 0 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ 0 & \ldots 0 & 0 & \ldots 0 \end{pmatrix} = 1.$$

[1]) В силу симметрии достаточно рассмотреть только этот случай.

Так как $(b)(a) \neq 1$, то, в силу теоремы 1 из главы 2, это невозможно, если выполнено условие 1). Заметим далее, что отображение $\sum x_i a_i \to \sum y_k a_k$ является таким $\mathfrak{o}$-эндоморфизмом A, что $\mathfrak{M}A = \mathfrak{M}$. С другой стороны, множество $\mathfrak{Z}_A$ элементов, отображающихся в 0, при эндоморфизме A содержит элементы $x_{m+1}, \ldots, x_n$, а потому $\mathfrak{Z}_A \neq 0$. Но это невозможно в силу теоремы 7 из главы 1 [1]).

Пусть теперь $\mathfrak{F}$ является свободным $\mathfrak{o}$-модулем с базисом $e_1, \ldots, e_n$ и пусть $\mathfrak{M}$ является некоторым $\mathfrak{o}$-модулем с n образующими $x_1, \ldots, x_n$. Соответствие $\sum e_i a_i \to \sum x_i a_i$ будет $\mathfrak{o}$-гомоморфным отображением модуля $\mathfrak{F}$ на $\mathfrak{M}$. Следовательно, $\mathfrak{M}$ изоморфно фактор-модулю $\mathfrak{F}/\mathfrak{N}$, где $\mathfrak{N}$ является совокупностью элементов, отображающихся в 0 при этом гомоморфизме. Мы используем позже этот результат для изучения структуры $\mathfrak{o}$-модулей с конечным числом образующих над областью главных идеалов $\mathfrak{o}$. $\mathfrak{o}$-модуль, порожденный одним элементом, называется *циклическим*. Если мы рассмотрим кольцо $\mathfrak{o}$ как модуль относительно обычного умножения xa, то получим, что $\mathfrak{o}$ является свободным циклическим модулем, так как $a = 1a$. Правый идеал $\mathfrak{J}$ из $\mathfrak{o}$ будет $\mathfrak{o}$-подмодулем. Идеал $\mathfrak{J}$ будет циклическим модулем тогда и только тогда, когда он является главным идеалом, и $\mathfrak{J} = a\mathfrak{o}$ будет свободным модулем тогда и только тогда, когда a не является левым делителем нуля. Если теперь $\mathfrak{M}$ является циклическим $\mathfrak{o}$-модулем и x — образующим элементом модуля $\mathfrak{M}$, то соответствие между $a \in \mathfrak{o}$ и $xa \in \mathfrak{M}$ является $\mathfrak{o}$-гомоморфизмом. Таким образом, в этом случае $\mathfrak{M}$ изоморфно фактор-модулю $\mathfrak{o}/\mathfrak{J}$, где $\mathfrak{J}$ является правым идеалом, состоящим из таких элементов b, что $xb = 0$. Идеал $\mathfrak{J}$ называется *порядком* элемента x.

4. Циклические $\mathfrak{o}$-модули. В дальнейшем $\mathfrak{o}$ будет обозначать область главных идеалов. Если $\mathfrak{M}$ является $\mathfrak{o}$-модулем и x — элементом из $\mathfrak{M}$, то мы будем говорить, что x имеет *конечный порядок*, если $\mathfrak{J} \neq 0$. Предположим

[1]) Последний результат принадлежит C. J. Everett. Более полное рассмотрение этих вопросов содержится в его работе [3].

теперь, что элементы x и y имеют конечные порядки $\mathfrak{J}_1$ и $\mathfrak{J}_2$. Тогда $\mathfrak{J}_3 = \mathfrak{J}_1 \cap \mathfrak{J}_2 \neq 0$, и, так как для всех $b \in \mathfrak{J}_3$ имеем $(x+y)b = 0$, то элемент $x+y$ имеет также конечный порядок. Далее, если a является некоторым не равным нулю элементом из $\mathfrak{o}$, то $a\mathfrak{o} \cap \mathfrak{J}_1 = \mathfrak{J}_4 \neq 0$ и, если b является отличным от нуля элементом из $\mathfrak{J}_4$, то $b = ac$, где $c \neq 0$. Тогда $(xa)c = xb = 0$. Таким образом, совокупность элементов конечного порядка образует подмодуль модуля $\mathfrak{M}$.

Рассмотрим теперь циклический $\mathfrak{o}$-модуль $\mathfrak{M}$, образующий элемент которого имеет конечный порядок, благодаря чему, не теряя общности, мы можем считать, что $\mathfrak{M} = \mathfrak{o}/a\mathfrak{o}$, где $a \neq 0$. Каждый подмодуль модуля $\mathfrak{o}/a\mathfrak{o}$ имеет вид $b\mathfrak{o}/a\mathfrak{o}$, где $b\mathfrak{o} \supseteq a\mathfrak{o}$ и, следовательно, $a = bc$. Подмодуль $b\mathfrak{o}/a\mathfrak{o}$ является циклическим, так как он порождается смежным классом, к которому принадлежит элемент b. Так как порядком смежного класса $b + a\mathfrak{o}$ является $c\mathfrak{o}$, то модуль $b\mathfrak{o}/a\mathfrak{o}$ $\mathfrak{o}$-изоморфен модулю $\mathfrak{o}/c\mathfrak{o}$. По второй теореме об изоморфизме модуль $\mathfrak{o}/a\mathfrak{o}/b\mathfrak{o}/a\mathfrak{o}$ $\mathfrak{o}$-изоморфен модулю $\mathfrak{o}/b\mathfrak{o}$. Таким образом, с разложением $a = bc$ не равного нулю элемента a мы можем связать цепь $\mathfrak{o}$-модулей $\mathfrak{o}/a\mathfrak{o} \supseteq b\mathfrak{o}/a\mathfrak{o} \supseteq \supseteq a\mathfrak{o}/a\mathfrak{o} = 0$, для которой фактор-модулями являются соответственно $\mathfrak{o}/b\mathfrak{o}$ и $\mathfrak{o}/c\mathfrak{o}$, и обратно.

Найдем теперь условие, при котором для двух не равных нулю элементов a и b фактор-модули $\mathfrak{o}/a\mathfrak{o}$ и $\mathfrak{o}/b\mathfrak{o}$ будут $\mathfrak{o}$-изоморфны. Пусть 1_a является смежным классом в $\mathfrak{o}/a\mathfrak{o}$, содержащим элементу 1. При изоморфизме он отобразится в смежный класс u_b фактор-модуля $\mathfrak{o}/b\mathfrak{o}$. Тогда $1_a c$ соответствует $u_b c$. Так как при изоморфизме $0 \to 0$, то $u_b a = b\mathfrak{o}$. Если u является некоторым элементом из u_b, то $ua = b\mathfrak{v} = m$. Так как смежный класс 1_b, содержащий 1 в $\mathfrak{o}/b\mathfrak{o}$, имеет при некотором c вид $u_b c$, то мы получаем $uc = 1 + bq$. Следовательно, общим наибольшим левым делителем (u, b) элементов u и b является 1. Так как $ua_1 \in b\mathfrak{o}$ только тогда, когда $a_1 = ac_1$, то m является общим наименьшим правым кратным $[u, b]$ элементов u и b. Следуя Оре [Ore], мы будем называть элементы a и b *подобными справа*, если существует такой элемент $u \in \mathfrak{o}$, что $(u, b) = 1$ и $a = u^{-1}[u, b]$, или $ua\mathfrak{o} = u\mathfrak{o} \cap b\mathfrak{o}$ и $u\mathfrak{o} + b\mathfrak{o} = \mathfrak{o}$. Мы получили, таким образом, что фактор-модули $\mathfrak{o}/a\mathfrak{o}$ и $\mathfrak{o}/b\mathfrak{o}$ $\mathfrak{o}$-изоморфны лишь тогда, когда элементы a и b подобны справа. Обратное утверждение также справедливо, так как, повторяя предшествующие рассуждения, мы видим, что отображение $1_a c \to u_b c$ является изоморфизмом. Теперь условие $m = ua = b\mathfrak{v} = [u, b]$ влечет за собой отсутствие общего правого делителя у элементов a и v, т. е. $\mathfrak{o}a + \mathfrak{o}v = \mathfrak{o}$, а из $(u, b) = 1$ следует, что m является общим левым наименьшим кратным элементов a и v. Таким образом, элементы a и b подобны слева в очевидном смысле слова. В силу эквивалентности правого и левого подобия мы будем называть это свойство просто *подобием*. Если рассматривать $\mathfrak{o}$ как левый модуль относительно левого умножения, то получается

Теорема 4. *$\mathfrak{o}$-модули $\mathfrak{o}/a\mathfrak{o}$ и $\mathfrak{o}/b\mathfrak{o}$ $(a, b \neq 0)$ изоморфны тогда и только тогда, когда левые модули $\mathfrak{o}/\mathfrak{o}a$ и $\mathfrak{o}/\mathfrak{o}b$ изоморфны. Для того чтобы каждое из этих условий имело место, необходимо и достаточно, чтобы элементы a и b были подобны.*

Отметим, что элемент ua, а, следовательно, и элемент uav подобен элементу a, если u и v являются обратимыми элементами. Если кольцо $\mathfrak{o}$ коммутативно, и $m = ua = b\mathfrak{v}$, то $up + bq = 1$; тогда $aup + abq = b(\mathfrak{v}p + aq)$, и потому b является делителем элемента a. Таким же образом a является делителем b. Следовательно, в этом случае элементы a и b подобны тогда и только тогда, когда они отличаются обратимым множителем.

Пусть a является необратимым отличным от нуля элементом. Тогда $\mathfrak{o} \supset a\mathfrak{o} \supset 0$. Так как выполнены условия обрыва цепей, то $\mathfrak{o}$-модуль $\mathfrak{o}/a\mathfrak{o}$ обладает композиционным рядом. Этот ряд соответствует такой цепи идеалов $\mathfrak{o} = a_0\mathfrak{o} \supset \supset a_1\mathfrak{o} \supset a_2\mathfrak{o} \supset \ldots \supset a_n\mathfrak{o} = a\mathfrak{o}$, что $a_i\mathfrak{o}/a\mathfrak{o}/a_{i+1}\mathfrak{o}/a\mathfrak{o}$ и, следовательно, $a_i\mathfrak{o}/a_{i+1}\mathfrak{o}$ неприводимы. Если $a_{i+1} = a_i b_{i+1}$ и $a_0 = 1$, то кольцо $a_i\mathfrak{o}/a_{i+1}\mathfrak{o}$ изоморфно кольцу $\mathfrak{o}/b_{i+1}\mathfrak{o}$. Следовательно, имеем $a = b_1 b_2 \ldots b_n$, где элементы b_i неприводимы в том смысле, что они не являются ни нулями, ни обратимыми элементами и не имеют собственных делителей. Обратно, если $a = b_1 b_2 \ldots b_n$, где элементы b_i

неприводимы, то мы получаем композиционный ряд $\mathfrak{o}/a\mathfrak{o} \supset b_1\mathfrak{o}/a\mathfrak{o} \supset b_1b_2\mathfrak{o}/a\mathfrak{o} \supset \ldots \supset 0$. Таким образом, мы можем применить теорему Жордана-Гельдера и получить следующую теорему:

Теорема 5. *Каждый элемент a, отличный от нуля и не являющийся обратимым элементом, может быть представлен в виде $b_1 \ldots b_n$, где b_i являются неприводимыми элементами. Если $a = c_1 \ldots c_m$, где элементы c_j неприводимы, то $m = n$ и элементы b_i и c_j подобны при некотором, определенным образом установленном, однозначном соответствии между ними.*

Число n неприводимых множителей b_i в разложении $a = b_1 \ldots b_n$ называется *длиной* элемента a. Оно является также длиной композиционного ряда модуля $\mathfrak{o}/a\mathfrak{o}$. Пусть b является другим необратимым отличным от нуля элементом, и предположим сначала, что $(a, b) = 1$. Тогда элемент $a^{-1}[a, b] = b'$ подобен элементу b. Следовательно, длина $b' =$ длине b. Пусть теперь $(a, b) = d$ и $a = da$, $b = db_1$. Тогда $(a_1, b_1) = 1$, и длина $[a_1b_1] =$ длине $a_1 +$ + длина $a_1^{-1}[a_1, b_1] =$ длине $a_1 +$ длина b_1. Так как $[a, b] = d[a_1, b_1]$, то длина $[a, b] =$ длине $d +$ длина $a_1 +$ длина b_1 и длина $[a, b] +$ длина $d =$ длине $a_1 +$ длина $b_1 + 2$ длины $d =$ длине ab, и нами получена

Теорема 6. *Если a и b являются отличными от нуля необратимыми элементами, то длина $[a, b] +$ + длина $(a, b) =$ длине ab.*

Собственное прямое разложение кольца $\mathfrak{o}/a\mathfrak{o}$ связано с таким множеством идеалов $a_i\mathfrak{o}$, что $\mathfrak{o} \supset a_i\mathfrak{o} \supset a\mathfrak{o}$, $a_1\mathfrak{o} +$ $+ \ldots + a_n\mathfrak{o} = \mathfrak{o}$ и $a_i\mathfrak{o} \cap (a_1\mathfrak{o} + \ldots + a_{i-1}\mathfrak{o} + a_{i+1}\mathfrak{o} + \ldots +$ $+ a_n\mathfrak{o}) = a\mathfrak{o}$. Таким образом элементы a_i являются собственными делителями элемента a, общий наибольший левый делитель $(a_1, \ldots, a_n) = 1$ и общее наименьшее правое кратное $[a_i, (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)] = a$. Если $a = a_ib_i$, то кольцо $a_i\mathfrak{o}/a\mathfrak{o}$ $\mathfrak{o}$-изоморфно кольцу $\mathfrak{o}/b_i\mathfrak{o}$. Условием для неразложимости $a_i\mathfrak{o}/a\mathfrak{o}$ является отсутствие таких собственных делителей b_i' и b_i'' элемента b_i, что $[b_i', b_i''] = b_i$ и $(b_i', b_i'') = 1$, или отсутствие таких собственных делителей a_i' и a_i'' элемента a, что $[a_i', a_i''] = a$ и

$(a_i', a_i'') = a_i$. Нетрудно видеть, что это является интерпретацией теоремы Крулля-Шмидта. Более обычная интерпретация получается при помощи следующего теоретико-структурного рассуждения.

Пусть $\mathfrak{M}$ является группой относительно множества Ω эндоморфизмов, которое содержит все внутренние автоморфизмы. Предположим, что $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_n$, т. е. что

$$\mathfrak{M} = \mathfrak{M}_1 + \ldots + \mathfrak{M}_n,$$
$$\mathfrak{M}_i \cap (\mathfrak{M}_1 + \ldots + \mathfrak{M}_{i-1} + \mathfrak{M}_{i+1} + \ldots + \mathfrak{M}_n) = 0. \quad (1)$$

Положим $\mathfrak{N}_i = \mathfrak{M}_1 + \ldots + \mathfrak{M}_{i-1} + \mathfrak{M}_{i+1} + \ldots + \mathfrak{M}_n$.

Тогда при помощи повторного применения дедекиндова дистрибутивного закона мы получаем $(\mathfrak{N}_1 \cap \ldots \cap \mathfrak{N}_{i-1} \cap$ $\cap \mathfrak{N}_{i+1} \cap \ldots \cap \mathfrak{N}_n = \mathfrak{M}_i$. Следовательно,

$$0 = \mathfrak{N}_1 \cap \ldots \cap \mathfrak{N}_n,$$
$$\mathfrak{N}_i + (\mathfrak{N}_1 \cap \ldots \cap \mathfrak{N}_{i-1} \cap \mathfrak{N}_{i+1} \cap \ldots \cap \mathfrak{N}_n) = \mathfrak{M}. \quad (2)$$

Обратно, если мы имеем множество подгрупп $\mathfrak{N}_i$, удовлетворяющих этим условиям, то мы можем определить $\mathfrak{M}_i = (\mathfrak{N}_1 \cap \ldots \cap \mathfrak{N}_{i-1} \cap \mathfrak{N}_{i+1} \cap \ldots \cap \mathfrak{N}_n)$ и получить $\mathfrak{N}_i =$ $= \mathfrak{M}_1 + \ldots + \mathfrak{M}_{i-1} + \mathfrak{M}_{i+1} + \ldots + \mathfrak{M}_n$ и $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus$ $\oplus \mathfrak{M}_n$. Таким образом мы имеем полный дуализм между этими двумя типами разложений. Отметим также, что факторгруппа $\mathfrak{M}/\mathfrak{N}_i$ Ω-изоморфна $\mathfrak{M}_i$. Следовательно, мы получаем следующую теорему, дуальную теореме Крулля-Шмидта:

Теорема 7. *Пусть $\mathfrak{M}$ является такой Ω-группой, что Ω содержит все внутренние автоморфизмы, и в $\mathfrak{M}$ выполнены оба условия обрыва цепей. Предположим, что $\mathfrak{N}_1, \ldots, \mathfrak{N}_n$ и $\mathfrak{N}_1', \ldots, \mathfrak{N}_{n'}'$ являются двумя удовлетворяющими условию (2) множествами отличных от $\mathfrak{M}$ Ω-подгрупп, причем $\mathfrak{M}/\mathfrak{N}_i$ и $\mathfrak{M}/\mathfrak{N}_i'$ являются неразложимыми группами. Тогда $n = n'$, и существует такой Ω-автоморфизм H группы $\mathfrak{M}$ и соответствующее ему упорядочивание подгрупп $\mathfrak{N}_i'$, что $\mathfrak{N}_iH = \mathfrak{N}_i'$. В частности, группы $\mathfrak{M}/\mathfrak{N}_i$ и $\mathfrak{M}/\mathfrak{N}_i'$ будут Ω-изоморфны.*

Вернемся теперь к изучению области $\mathfrak{o}$ и назовем элемент a *неразложимым*, если a является таким отличным от нуля необратимым элементом, что модуль $\mathfrak{o}/a\mathfrak{o}$ неразложим. Последнее условие имеет место тогда и только тогда, когда не существует таких собственных делителей a' и a'' элемента a, что $a=[a', a'']$ и $(a', a'')=1$. Если a обладает таким разложением и $a=a'b''=a''b'$, то a является общим наименьшим левым кратным элементов b' и b'', и эти элементы не имеют необратимых общих правых делителей. Отсюда следует, что модуль $\mathfrak{o}/a\mathfrak{o}$ неразложим тогда и только тогда, когда модуль $\mathfrak{o}/\mathfrak{o}a$ неразложим. Из теоремы, дуальной к теореме Крулля-Шмидта, следует

Теорема 8. *Отличный от нуля необратимый элемент a может быть представлен в виде $[c_1, \ldots, c_n]$, где элементы c_i неразложимы, и $(c_i, [c_1, \ldots, c_{i-1}, c_{i+1}, \ldots c_n])=1$. Если мы имеем другое разложение $a=[d_1, \ldots, d_n]$ того же типа, то $n=m$ и элементы d_j могут быть так упорядочены, чтобы для всех i элемент c_i был подобен элементу d_i.*

Области полиномов. Пусть $\mathfrak{o}$ является областью полиномов $\Phi[t, S]$. Если $a=t^m+t^{m-1}\alpha_1+\ldots+\alpha_m$, где $m>0$, и d является некоторым элементом этой области, то $d=aq+r$, $\deg r<\deg a$. Следовательно, в каждом смежном классе по $a\Phi[t, S]$ существует элемент, степень которого меньше m. Как легко видеть, такой элемент однозначно определен. Отсюда следует, что всякий смежный класс по $a\Phi[t, S]$ может быть представлен в виде $\{1\}\xi_1+\{t\}\xi_2+\ldots+\{t^{m-1}\}\xi_m$, где $\{t^k\}$ является смежным классом, содержащим t^k, и $\xi_i\in\Phi$. Таким образом, рассматривая $\Phi[t, S]$-модуль $\Phi[t, S]/a\Phi[t, S]$ как Φ-модуль, мы получим, что размерность его равна степени элемента a.

Следствием этого является равенство степеней подобных полиномов. Степени полиномов, получающихся при разложении произвольного элемента a на множители, являются, таким образом, инвариантами a. Предположим, что элемент a подобен элементу b, т. е., что $a=u^{-1}[u, b]$, где $(u, b)=1$. Если $[u, b]=ua=bv$, то положим

$$u=bq_1+u_1, \quad v=q_2a+v_1,$$

где $\deg u_1<\deg b$ и $\deg v_1<\deg a$. Тогда

$$b(q_1-q_2)a=bv_1-u_1a.$$

Если $q_1\neq q_2$, то степень в левой части $\geqslant \deg a+\deg b$, в то время, как степень правой части $<\deg a+\deg b$. Следовательно, $q_1=q_2$ и $bv_1=u_1a$. Элементы b и u_1 не имеют необратимых общих левых делителей, а элементы v_1 и a не имеют необратимых общих правых делителей. Следовательно, $a=u_1^{-1}[u_1, b]$, где $\deg u_1<\deg b$. Например, если $b=t-\beta$, где $\beta\in\Phi$, то мы можем положить $u_1=\sigma$, $\sigma\in\Phi$, и $t-\beta=\sigma\sigma^{-1}(t-\beta)=[\sigma, t-\beta]$. Следовательно, подобные $t-\beta$ элементы ассоциированы справа с полиномами вида $\sigma^{-1}(t-\beta)$ или $t-\sigma^{-1}\beta\sigma^S$.

Пусть теперь $\Phi=R(i, j)$ является кватернионной алгеброй над действительно замкнутым полем: элементами Φ являются $\alpha_0+i\alpha_1+j\alpha_2+ij\alpha_3$, где $i^2=j^2=-1$ и $ij=-ji$. Положим $S=1$. Если $a(t)=a_0+ta_1+t^2a_2+\ldots+t^ma_m$, где $a_i\in\Phi$, то определим $\overline{a(t)}$ как $\bar{a}_0+t\bar{a}_1+t^2\bar{a}_2+\ldots+t^m\bar{a}_m$, где $\overline{\alpha_0+i\alpha_1+j\alpha_2+ij\alpha_3}=\alpha_0-i\alpha_1-j\alpha_2-ij\alpha_3$. Легко проверить, что

$$\overline{a(t)+b(t)}=\overline{a(t)}+\overline{b(t)}, \quad \overline{a(t)b(t)}=\overline{b(t)}\,\overline{a(t)} \tag{3}$$

и

$$a(t)+\overline{a(t)}, \quad a(t)\overline{a(t)}=\overline{a(t)}\,a(t) \tag{4}$$

имеют коэффициенты в R. Таким образом $a(t)\overline{a(t)}$ может быть разложено на линейные множители в $R(i)[t]$. Следовательно, неприводимые делители полинома $a(t)$ в $\Phi[t]$ линейны, и единственными неприводимыми полиномами в $\Phi[t]$ являются линейные полиномы. Как и в коммутативном случае, мы можем использовать тождество:

$$t^k-r^k=(t-r)(t^{k-1}+t^{k-2}r+\ldots+r^{k-1})$$

для доказательства того, что остаток при делении слева полинома $a(t)=a_0+ta_1+\ldots+t^ma_m$ на $t-r$ равен $a_0+ra_1+\ldots+r^ma_m$. Следовательно, $t-r$ является точным делителем полинома $a(t)$ тогда и только тогда, когда r является левосторонним корнем $a(t)$ в том смысле, что

$a_0 + ra_1 + \ldots + r^m a_m = 0$. Таким образом, мы доказали, что каждый полином, степень которого > 0, обладает левосторонним корнем, и таким же образом мы находим, что эти полиномы обладают правосторонними корнями ($a_0 + a_1 r + \ldots + a_m r^m = 0$), в этом смысле Φ *алгебраически замкнуто.*

Пусть далее $\Phi = R(i)$, где $i^2 = -1$ и R является действительно замкнутым полем. Предположим, что S является автоморфизмом $\alpha_0 + i\alpha_1 \to \alpha_0 - i\alpha_1$. Если полином $a(t) = a_0 + ta_1 + \ldots + t^m a_m$, где $a_i \in \Phi$, лежит в $\Phi[t, S]$, то мы определяем $\overline{a(t)} = \bar{a}_0 - ta_1 + t^2\bar{a}_2 - t^3 a_3 + \ldots$ (или $\bar{t} = -t$, $\overline{t^i a_i} = \bar{a}_i \bar{t}^i$). Тогда (3) выполнено, и $a(t)\overline{a(t)} = \overline{a(t)}\, a(t) = \alpha(t^2)$, где $\alpha(t^2)$ является полиномом от t^2 с коэффициентами из R. Мы можем разложить $\alpha(t^2)$ на множители вида $t^2 - a$, где $a \in \Phi$, причем эти множители неприводимы в $\Phi[t, S]$, когда $a \neq b\bar{b}$, т. е. когда a не является действительным и неотрицательным числом. Следовательно, всякое $a(t)$ обладает линейными и квадратичными множителями, и наш результат дает те специальные формы, которым подобен каждый неприводимый полином.

5. Двусторонние идеалы. Каждый двусторонний идеал $\mathfrak{J}$ имеет вид $a\mathfrak{o} = \mathfrak{o}a'$. Отсюда следует, что $a = ua'$, $a' = av$ и $a = uav$, $a' = ua'v$. Так как $ua \in \mathfrak{J}$, то $ua = au'$ и $a = au'v$, и потому $u'v = 1$. Следовательно, элемент v обратим. Аналогично, элемент u обратим, и $a\mathfrak{o} = \mathfrak{o}a$, $a'\mathfrak{o} = \mathfrak{o}a'$, т. е. каждый правый образующий элемент является левым образующим и обратно. Мы будем обозначать образующие двусторонних идеалов через a^*, b^*, ... Эти элементы характеризуются тем свойством, что для любого заданного элемента x найдется такой элемент x' ($\hat{x}$), что $xa^* = a^* x'$ ($a^* x = \hat{x} a^*$). Отсюда следует, конечно, что соответствие $x \to x'$ ($x \to x$) взаимно-однозначно и, следовательно, является автоморфизмом в $\mathfrak{o}$.

Если $\mathfrak{J}_1$ и $\mathfrak{J}_2$ являются двусторонними идеалами, то и $\mathfrak{J}_1 + \mathfrak{J}_2$ и $\mathfrak{J}_1 \cap \mathfrak{J}_2$ также будут двусторонними идеалами, равно как и произведение $\mathfrak{J}_1\mathfrak{J}_2$, определенное как совокупность сумм вида $\sum y_1 y_2$, где $y_i \in \mathfrak{J}_i$ [1]. Если $\mathfrak{J}_1 = a^*\mathfrak{o}$, $\mathfrak{J}_2 = b^*\mathfrak{o}$, то $\mathfrak{J}_1\mathfrak{J}_2 = (a^*\mathfrak{o})(b^*\mathfrak{o}) = a^*(\mathfrak{o}b^*)\mathfrak{o} = a^*(b^*\mathfrak{o})\mathfrak{o} = a^* b^* \mathfrak{o}$. Очевидно, что $\mathfrak{J}_1 \cap \mathfrak{J}_2 \supseteq \mathfrak{J}_1\mathfrak{J}_2$. Предположим теперь, что $\mathfrak{J}_2 \supseteq \mathfrak{J}_1 \neq 0$; тогда $a^* = b^* c$, и если $x \in \mathfrak{o}$, то найдутся такие элементы x' и $\bar{x}$, что $xa^* = a^* x'$ и $xb^* = b^* \bar{x}$. Следовательно, $b^* \bar{x} c = xa^* = a^* x' = b^* c x'$ и $\bar{x}c = cx'$. Так как элемент $\bar{x}$ произволен, то $c = c^*$ порождает такой двусторонний идеал $c^*\mathfrak{o}$, что $a^*\mathfrak{o} = (b^*\mathfrak{o})(c^*\mathfrak{o})$. Очевидно, что $c^*\mathfrak{o} \supseteq a^*\mathfrak{o}$.

Лемма 1. *Если $\mathfrak{J}_1$ и $\mathfrak{J}_2$ являются двусторонними отличными от нуля идеалами, то из $\mathfrak{J}_2 \supseteq \mathfrak{J}_1$ следует, что $\mathfrak{J}_1 = \mathfrak{J}_2\mathfrak{J}_3$, где $\mathfrak{J}_3$ — двусторонний идеал, содержащий $\mathfrak{J}_1$.*

Под максимальным двусторонним идеалом $p^*\mathfrak{o}$ мы будем понимать отличный от $\mathfrak{o}$ двусторонний идеал, который не содержится ни в одном двустороннем идеале, отличном от $\mathfrak{o}$ и $p^*\mathfrak{o}$. Таким же образом мы определяем максимальный правый идеал $p\mathfrak{o}$. Таким образом, идеал $p\mathfrak{o}$ максимален тогда и только тогда, когда элемент p неприводим.

Пусть теперь $p_1^*\mathfrak{o}$ является максимальным двусторонним идеалом, содержащим двусторонний идеал $a^*\mathfrak{o} \neq 0, \mathfrak{o}$. Такие идеалы существуют, так как $\mathfrak{o}/a^*\mathfrak{o}$ удовлетворяет условиям обрыва цепей. Мы получаем $a^*\mathfrak{o} = (p_1^*\mathfrak{o})(a_1^*\mathfrak{o})$, где $a_1^*\mathfrak{o} \neq a^*\mathfrak{o}$, так как $p_1^*\mathfrak{o} \neq 0$. Если $a_1^*\mathfrak{o} = \mathfrak{o}$, то $a^*\mathfrak{o} = p_1^*\mathfrak{o}$. В противном случае имеем $a_1^*\mathfrak{o} = (p_2^*\mathfrak{o})(a_2^*\mathfrak{o})$, где $\mathfrak{o} \supseteq a_2^*\mathfrak{o} \supset a_1^*\mathfrak{o}$. Продолжая этот процесс, мы получаем следующую лемму:

Лемма 2. *Каждый отличный от 0 и от $\mathfrak{o}$ двусторонний идеал $a^*\mathfrak{o}$ может быть разложен следующим образом: $(p_1^*\mathfrak{o})(p_2^*\mathfrak{o})\ldots(p_k^*\mathfrak{o})$, где $p_i^*\mathfrak{o}$ являются максимальными (или неразложимыми) двусторонними идеалами.*

---

[1]) Вообще если $\mathfrak{A}$ и $\mathfrak{B}$ являются подкольцами некоторого кольца, то $\mathfrak{AB}$ определяется как множество элементов вида Σab, где $a \in \mathfrak{A}$ и $b \in \mathfrak{B}$. Имеют место следующие правила: $\mathfrak{A}(\mathfrak{B}\mathfrak{C}) = (\mathfrak{A}\mathfrak{B})\mathfrak{C}$, $\mathfrak{A}(\mathfrak{B} + \mathfrak{C}) = \mathfrak{A}\mathfrak{B} + \mathfrak{A}\mathfrak{C}$, $(\mathfrak{B} + \mathfrak{C})\mathfrak{A} = \mathfrak{B}\mathfrak{A} + \mathfrak{C}\mathfrak{A}$,

Предположим, что идеал $p^*\mathfrak{o}$ является максимальным и содержит (или, что то же самое, является его делителем) идеал $(a^*\mathfrak{o})\,(b^*\mathfrak{o})$. Если $p^*\mathfrak{o} \not\supseteq a^*\mathfrak{o}$, то $p^*\mathfrak{o} + a^*\mathfrak{o} = \mathfrak{o}$ и, следовательно, $b^*\mathfrak{o} = \mathfrak{o}b^*\ \mathfrak{o} = (p^*\mathfrak{o} + a^*\mathfrak{o})\,b^*\mathfrak{o} = (p^*\mathfrak{o})\,(b^*\mathfrak{o}) + (a^*\mathfrak{o})\,(b^*\mathfrak{o}) \subseteq p^*\mathfrak{o}$.

Лемма 3. *Если максимальный идеал $p^*\mathfrak{o}$ является делителем идеала $(a^*\mathfrak{o})\,(b^*\mathfrak{o})$, то $p^*\mathfrak{o}$ будет либо делителем $a^*\mathfrak{o}$, либо делителем $b^*\mathfrak{o}$.*

Пусть $p^*\mathfrak{o}$ и $q^*\mathfrak{o}$ являются максимальными двусторонними идеалами. Если $p^*\mathfrak{o} = q^*\mathfrak{o}$, то, очевидно, $(p^*\mathfrak{o})\,(q^*\mathfrak{o}) = (q^*\mathfrak{o})\,(p^*\mathfrak{o})$. Предположим теперь, что $p^*\mathfrak{o} \neq q^*\mathfrak{o}$. Идеал $(p^*\mathfrak{o} \cap q^*\mathfrak{o}) \subseteq p^*\mathfrak{o}$, и потому $(p^*\mathfrak{o} \cap q^*\mathfrak{o}) = (p^*\mathfrak{o})\,(q_1^*\mathfrak{o})$. Но $q^*\mathfrak{o} \supseteq (p^*\mathfrak{o})\,(q_1^*\mathfrak{o})$ и, так как $q^*\mathfrak{o} \not\supseteq p^*\mathfrak{o}$, то $q^*\mathfrak{o} \supseteq q_1^*\mathfrak{o}$. Следовательно, $(p^*\mathfrak{o})\,(q^*\mathfrak{o}) \supseteq (p^*\mathfrak{o} \cap q^*\mathfrak{o})$. Так как обратное включение также справедливо, то $(p^*\mathfrak{o})\,(q^*\mathfrak{o}) = (p^*\mathfrak{o} \cap q^*\mathfrak{o})$. По симметрии мы получаем лемму:

Лемма 4. *Если $p^*\mathfrak{o}$ и $q^*\mathfrak{o}$ являются максимальными двусторонними идеалами, то $(p^*\mathfrak{o})\,(q^*\mathfrak{o}) = (q^*\mathfrak{o})\,(p^*\mathfrak{o})$.*

Из этих лемм вытекает, как и в коммутативном случае,

Теорема 9. *Двусторонние идеалы кольца $\mathfrak{o}$ образуют коммутативную систему относительно умножения. Всякий двусторонний идеал, отличный от 0 и $\mathfrak{o}$, обладает одним и только одним разложением в произведение максимальных двусторонних идеалов.*

Из этой теоремы следует, что если $a^*\mathfrak{o} = (p_1^*\mathfrak{o})^{e_1} \ldots (p_s^*\mathfrak{o})^{e_s}$, где идеалы $p_i^*\mathfrak{o}$ являются максимальными и $p_i^*\mathfrak{o} \neq p_j^*\mathfrak{o}$ при $i \neq j$, то всякий двусторонний идеал, содержащий $a^*\mathfrak{o}$, имеет вид $(p_1^*\mathfrak{o})^{f_1} \ldots (p_s^*\mathfrak{o})^{f_s}$, где $f_i \leqslant e_i$. Следовательно, если $a^*\mathfrak{o} = (p_1^*\mathfrak{o})^{e_1} \ldots (p_s^*\mathfrak{o})^{e_s}$ и $b^*\mathfrak{o} = (p_1^*\mathfrak{o})^{f_1} \ldots (p_s^*\mathfrak{o})^{f_s}$, где $e_i \geqslant 0$ и $f_i \geqslant 0$, то $a^*\mathfrak{o} + b^*\mathfrak{o} = (p_1^*\mathfrak{o})^{h_1} \ldots (p_s^*\mathfrak{o})^{h_s}$, где $h_i = \min(e_i, f_i)$, и $a^*\mathfrak{o} \cap b^*\mathfrak{o} = (p_1^*\mathfrak{o})^{g_1} \ldots (p_s^*\mathfrak{o})^{g_s}$, где $g_i = \max(e_i, f_i)$. Если $a^*\mathfrak{o} + b^*\mathfrak{o} = \mathfrak{o}$, то $a^*\mathfrak{o} \cap b^*\mathfrak{o} = (a^*\mathfrak{o})\,(b^*\mathfrak{o})$. Таким образом, для того, чтобы

$a^*\mathfrak{o} = (p^*\mathfrak{o})^e$, где $p^*\mathfrak{o}$ максимальный идеал, необходимо и достаточно, чтобы идеал $a^*\mathfrak{o}$ нельзя было представить в виде $b^*\mathfrak{o} \cap c^*\mathfrak{o}$, где $b^*\mathfrak{o}$ и $c^*\mathfrak{o}$ являются такими собственными делителями, что $b^*\mathfrak{o} + c^*\mathfrak{o} = \mathfrak{o}$.

Двусторонние идеалы в $\Phi[t, S]$. Пусть $a^* = t^n + t^{n-1}\alpha_1 + \ldots + t^{n-k}\alpha_k$, где $\alpha_k \neq 0$, порождает двусторонний идеал в $\Phi[t, S]$. Тогда, так как t^{n-k} порождает двусторонний идеал, то это справедливо и для $t^k + t^{k-1}\alpha_1 + \ldots + \alpha_k$. Следовательно, мы можем предположить, что $k = n$ и $\alpha_n \neq 0$. Если ξ является произвольным элементом из Φ, то существует такое ξ' в $\Phi[t, S]$, что

$$\xi(t^n + t^{n-1}\alpha_1 + \ldots + \alpha_n) = (t^n + t^{n-1}\alpha_1 + \ldots + \alpha_n)\xi'.$$

Следовательно, $\deg \xi' = 0$, т. е. $\xi' \in \Phi$. Тогда $\xi' = \alpha_n^{-1}\xi\alpha_n$. Если $n \neq 0$, то $\xi^{S^n} = \xi'$, и потому $\xi^{S^n} = \alpha_n^{-1}\xi\alpha_n$. Таким образом, мы видим, что если ни одна степень автоморфизма S, за исключением $S^0 = 1$, не является внутренним автоморфизмом, то единственными элементами a^* являются $t^k\alpha$, и двусторонними идеалами являются $t^k\mathfrak{o} = \mathfrak{o}t^k$, $k = 0, 1, 2, \ldots$.

Предположим теперь, что $S^r \in \mathfrak{R}$, $r > 0$, где через $\mathfrak{R}$ обозначена группа внутренних автоморфизмов тела Φ, и пусть S^r является наименьшей положительной степенью, обладающей этим свойством. Соответственно, пусть для всех ξ имеет место $\xi^{S^r} = \mu^{-1}\xi\mu$. Тогда, если $S^n \in \mathfrak{R}$, то n является кратным числа r. Если $a^* = t^n + t^{n_2}\beta_2 + t^{n_3}\beta_3 + \ldots + \beta_s$, причем $\beta_i \neq 0$, $n > n_2 > \ldots$ и $\xi a^* = a^*\xi'$, где по необходимости $\xi' = \beta_s^{-1}\xi\beta_s$, то автоморфизмы S^n, $S^{n_2}, \ldots$ являются внутренними. Следовательно, $a^* = t^{mr} + t^{(m-1)r}\gamma_1 + \ldots + \gamma_m$, где $\gamma_m \neq 0$, и для всех ξ имеем $\gamma_i\xi' = \mu^{-(m-i)}\xi\mu^{(m-i)}\gamma_i$. Так как $ta^* = a^*t'$, то $t' = t$ и, следовательно, $\gamma_i{}^S = \gamma_i$. Обратно, условия

$$\gamma_i\xi' = \mu^{-(m-i)}\xi\mu^{(m-i)}\gamma_i, \quad \gamma_i{}^S = \gamma_i \tag{5}$$

влекут за собой $xa^* = a^*x'$ для $x = \xi \in \Phi$ и $x = t$. Отсюда следует, что это справедливо для всех x из $\Phi[t, S]$. Общей формой образующего элемента для двустороннего

идеала является, следовательно, $t^k a^* \gamma$, где a^* имеет вышеуказанный вид.

6. Ограниченные идеалы Правый идеал $a\mathfrak{o}$ называется *ограниченным*, если он содержит отличный от нуля двусторонний идеал. Объединение двусторонних идеалов, содержащихся в $a\mathfrak{o}$, является двусторонним идеалом, называющимся *границей* $\mathfrak{J} = a^*\mathfrak{o} = \mathfrak{o}a^*$ идеала $a\mathfrak{o}$. Если $z \in \mathfrak{J}$, то для каждого $x \in \mathfrak{o}$ имеем $xz \in a\mathfrak{o}$ и, следовательно, $z \in \mathfrak{J}'$, где $\mathfrak{J}'$ обозначает идеал, состоящий из аннуляторов фактор-модуля $\mathfrak{o}/a\mathfrak{o}$. Следовательно, если идеал $a\mathfrak{o}$ ограничен, то $\mathfrak{J}' \neq 0$. Обратно, если $\mathfrak{J}' \neq 0$, то $1\mathfrak{J}' \subseteq a\mathfrak{o}$, и идеал $a\mathfrak{o}$ является ограниченным с границей $\mathfrak{J} \supseteq \mathfrak{J}'$. Таким образом, $\mathfrak{J} = \mathfrak{J}'$. Из этой характеристики границы следует, что если элементы a и b подобны, а идеал $a\mathfrak{o}$ ограничен, то идеал $b\mathfrak{o}$ также ограничен и имеет ту же самую границу. В частности, если $a\mathfrak{o} = a^*\mathfrak{o}$ является двусторонним идеалом, то $a\mathfrak{o} = b\mathfrak{o}$.

Другая характеристика ограниченности и границы получается следующим образом. Пусть элемент b подобен некоторому правому делителю элемента a и пусть $\mathfrak{J}' = \Delta b\mathfrak{o}$ является пересечением всех идеалов $b\mathfrak{o}$ такого вида. Предположим, что $\mathfrak{J}' \neq 0$. Если x является некоторым элементом из $\mathfrak{o}$, то положим $(x, a) = e$, $x = ex_1$, $a = ea_1$, так что $(x_1, a_1) = 1$. Пусть $m_1 = [x_1, a_1] = x_1 a_2 = a_1 x_2$. Тогда элемент a_2 подобен правому делителю a_1 элемента a. Следовательно, если $d \in \mathfrak{J}'$, то $d = a_2 d'$ и $xd = ex_1 a_2 d' = ea_1 x_2 d' = ax_2 d' \in a\mathfrak{o}$. Отсюда следует, что идеал $a\mathfrak{o}$ ограничен и имеет границу $\mathfrak{J} \supseteq \mathfrak{J}'$. С другой стороны, пусть $a\mathfrak{o}$ является ограниченным идеалом с границей $\mathfrak{J}$. Тогда если элемент b подобен правому делителю a, то $\mathfrak{o}/b\mathfrak{o}$ $\mathfrak{o}$-изоморфно подмодулю фактор-модуля $\mathfrak{o}/a\mathfrak{o}$, и, следовательно, если $d \in \mathfrak{J}$, то $d = 1d \in b\mathfrak{o}$. Так как идеал $b\mathfrak{o}$ произволен, то $d \in \Delta b\mathfrak{o} = \mathfrak{J}'$, и потому $\mathfrak{J} \subseteq \mathfrak{J}'$. Следовательно, $\mathfrak{J} = \mathfrak{J}'$.

Теорема 10. *Следующие условия эквивалентны*: 1) *идеал* $a\mathfrak{o}$ *ограничен*; 2) *существует такой элемент* $z \neq 0$, *что для всех* x $xz \in a\mathfrak{o}$; 3) *пересечение* $\Delta b\mathfrak{o}$ *всех*

идеалов $b\mathfrak{o}$, *где элемент* b *подобен некоторому правому делителю элемента* a, *отлично от нуля. Если эти условия выполнены, то границей* $a\mathfrak{o}$ *является совокупность элементов* z, *удовлетворяющих* 2), *или множество* $\Delta b\mathfrak{o}$ *из условия* 3).

Следствие. *Если элементы* a *и* b *подобны, и идеал* $a\mathfrak{o}$ *ограничен, то идеал* $b\mathfrak{o}$ *ограничен и имеет ту же границу, что и* $a\mathfrak{o}$.

Такие же определения имеют место и для левых идеалов. Если теперь $a\mathfrak{o} \supseteq a^*\mathfrak{o}$, то рассмотрим идеал $\mathfrak{o}a$ и положим $\mathfrak{o}a + \mathfrak{o}a^* = \mathfrak{o}d$. Тогда $d = ka + la^*$. Так как $a^* = aa_1$, то мы получаем, что $da_1 = kaa_1 + la^*a_1 = kaa_1 + la_1'a^* = (ka + la_1'a)\,a_1$. Следовательно, $d = ua$, где $u = k + la_1'$. Тогда $\mathfrak{o}d \subseteq \mathfrak{o}a$, и $\mathfrak{o}a^* = a^*\mathfrak{o} \subseteq \mathfrak{o}a$. Таким образом, идеал $\mathfrak{o}a$ ограничен и имеет ту же границу, что и $a\mathfrak{o}$.

Теорема 11. *Если идеал* $a\mathfrak{o}$ *ограничен и имеет границу* $a^*\mathfrak{o} = \mathfrak{o}a^*$, *то и идеал* $\mathfrak{o}a$ *ограничен и имеет границу* $a^*\mathfrak{o}$.

Если идеалы $a\mathfrak{o}$ и $b\mathfrak{o}$ ограничены с границами соответственно $a^*\mathfrak{o}$ и $b^*\mathfrak{o}$, то $a^*\mathfrak{o} \cap b^*\mathfrak{o}$ является отличным от нуля двусторонним идеалом. Следовательно, идеал $a\mathfrak{o} \cap b\mathfrak{o}$ ограничен, и его границей является, очевидно, $a^*\mathfrak{o} \cap b^*\mathfrak{o}$. Из определения границы следует также, что если $b\mathfrak{o} \supseteq a\mathfrak{o}$ и $a = bc$, причем идеал $a\mathfrak{o}$ ограничен с границей $a^*\mathfrak{o}$, то и идеал $b\mathfrak{o}$ ограничен с границей $b^*\mathfrak{o} \supseteq a^*\mathfrak{o}$. Таким же образом идеал $\mathfrak{o}c$, а следовательно, и $c\mathfrak{o}$, ограничен, и его граница содержит $a^*\mathfrak{o}$. Если мы сопоставим эти утверждения, то получим, что если идеал $a\mathfrak{o} = bcd\mathfrak{o}$ ограничен, то и идеал $c\mathfrak{o}$ ограничен, и его граница содержит $a^*\mathfrak{o}$.

Теорема 12. *Если идеал* $a\mathfrak{o} = bcd\mathfrak{o}$ *ограничен и имеет границу* $a^*\mathfrak{o}$, *то и идеал* $c\mathfrak{o}$ *ограничен, и его граница* $c^*\mathfrak{o}$ *содержит* $a^*\mathfrak{o}$.

Пусть теперь элемент p неприводим. Тогда $p\mathfrak{o}$ является максимальным правым идеалом. Предположим, что $p\mathfrak{o} \supseteq (a^*\mathfrak{o})\,(b^*\mathfrak{o})$. Если $p\mathfrak{o} \not\supseteq a^*\mathfrak{o}$, то $p\mathfrak{o} + a^*\mathfrak{o} = \mathfrak{o}$ и, следовательно, $b^*\mathfrak{o} = (p\mathfrak{o})\,(b^*\mathfrak{o}) + (a^*\mathfrak{o})\,(b^*\mathfrak{o}) \subseteq p\mathfrak{o}$. Если идеал

$p\mathfrak{o}$ ограничен, то отсюда следует, что его граница $p^*\mathfrak{o}$ является максимальным двусторонним идеалом.

Пусть теперь элемент q неразложим, и пусть идеал $q\mathfrak{o}$ ограничен и имеет границу $q^*\mathfrak{o}$. Предположим, что $q^*\mathfrak{o} = q_1^*\mathfrak{o} \cap q_2^*\mathfrak{o}$, $q_1^*\mathfrak{o} + q_2^*\mathfrak{o} = \mathfrak{o}$. Положим $q_1\mathfrak{o} = q_1^*\mathfrak{o} + q\mathfrak{o}$, $q_2\mathfrak{o} = q_2^*\mathfrak{o} + q\mathfrak{o}$. Тогда $q_1\mathfrak{o} + q_2\mathfrak{o} = \mathfrak{o}$ и $q_1^*\mathfrak{o}q_2^*\mathfrak{o} = q_2^*\mathfrak{o}\, q_1^*\mathfrak{o} = q^*\mathfrak{o}$. Если $x \in q_1^*\mathfrak{o} + q\mathfrak{o}$, то $x\,(q_2^*\mathfrak{o}) \subseteq q\mathfrak{o}$, и также, если $x \in q_2^*\mathfrak{o} + q\mathfrak{o}$, то $x\,(q_1^*\mathfrak{o}) \subseteq q\mathfrak{o}$. Следовательно, $x\mathfrak{o} \subseteq q\mathfrak{o}$ и $x \in q\mathfrak{o}$. Таким образом, $q_1\mathfrak{o} \cap q_2\mathfrak{o} = q\mathfrak{o}$. В силу неразложимости идеала $q\mathfrak{o}$, мы получаем, что либо $q_1\mathfrak{o} = q\mathfrak{o}$, либо $q_2\mathfrak{o} = q\mathfrak{o}$. Соответственно, либо $q\mathfrak{o} \supseteq q_1^*\mathfrak{o}$, либо $q\mathfrak{o} \supseteq q_2^*\mathfrak{o}$. Так как $q^*\mathfrak{o}$ является границей идеала $q\mathfrak{o}$, то либо $q_1^*\mathfrak{o} = q^*\mathfrak{o}$, либо $q_2^*\mathfrak{o} = q^*\mathfrak{o}$. Отсюда следует, что $q^*\mathfrak{o}$ не может быть разложен в произведение собственных двусторонних взаимно простых множителей, т. е. $q^*\mathfrak{o}$ является степенью максимального двустороннего идеала.

Теорема 13. *Если элемент p неприводим и идеал $p\mathfrak{o}$ ограничен, то его граница $p^*\mathfrak{o}$ является максимальным двусторонним идеалом. Если элемент q неразложим и идеал $q\mathfrak{o}$ ограничен, то его граница $q^*\mathfrak{o}$ является степенью максимального двустороннего идеала.*

Элемент a называется *полным делителем* элемента $b \neq 0$, если существует такой двусторонний идеал $\mathfrak{J}$, что $a\mathfrak{o} \supseteq \mathfrak{J} \supseteq b\mathfrak{o}$. Таким образом, идеал $a\mathfrak{o}$ ограничен, и его граница $a^*\mathfrak{o}$ содержит $b\mathfrak{o}$. Так как мы видели, что $\mathfrak{o}a \supseteq a^*\mathfrak{o}$, и так как очевидно, что $\mathfrak{o}a^* = a^*\mathfrak{o} \supseteq \mathfrak{o}b$, то мы получаем также, что $\mathfrak{o}a \supseteq \mathfrak{o}a^* \supseteq \mathfrak{o}b$. Более симметричное условие, эквивалентное нашему, было дано Тейхмюллером, а именно: $(a\mathfrak{o} \cap \mathfrak{o}a) \supseteq \mathfrak{o}b\mathfrak{o}$. В самом деле, если $(a\mathfrak{o} \cap \mathfrak{o}a) \supseteq \mathfrak{o}b\mathfrak{o}$, то $a\mathfrak{o}$ содержит двусторонний идеал $\mathfrak{o}b\mathfrak{o}$, содержащий $b\mathfrak{o}$. Обратно, если $a\mathfrak{o} \supseteq a^*\mathfrak{o} \supseteq b\mathfrak{o}$, то $a^*\mathfrak{o} \supseteq \mathfrak{o}b\mathfrak{o}$ и $a\mathfrak{o} \supseteq \mathfrak{o}b\mathfrak{o}$. Подобным же образом получаем, что $\mathfrak{o}a \supseteq \mathfrak{o}b\mathfrak{o}$, и потому $(a\mathfrak{o} \cap \mathfrak{o}a) \supseteq \mathfrak{o}b\mathfrak{o}$. Как вытекает из следующей теоремы, понятие полной делимости инвариантно относительно подобия.

Теорема 14. *Если элемент a является полным делителем элемента b и a' подобно a, а b' подобно b, то a' является полным делителем элемента b'.*

Мы видели, что если идеал $a\mathfrak{o}$ ограничен, и элемент a' подобен элементу a, то идеал $a'\mathfrak{o}$ ограничен и имеет ту же самую границу $a^*\mathfrak{o}$, что и $a\mathfrak{o}$. Следовательно, если a является полным делителем элемента b, то a' также является полным делителем b. Предположим теперь, что $b' = u^{-1}[u, b]$, где $(u, b) = 1$. Тогда $u\mathfrak{o} + b\mathfrak{o} = \mathfrak{o}$, и если $a\mathfrak{o} \supseteq a^*\mathfrak{o} \supseteq b\mathfrak{o}$, то $u\mathfrak{o} + a^*\mathfrak{o} = \mathfrak{o}$. Таким образом, элемент $u^{-1}[u, a^*]$ подобен элементу a^*, и так как $a^*\mathfrak{o}$ является двусторонним идеалом, то $u^{-1}[u, a^*]\,\mathfrak{o} = a^*\mathfrak{o}$ и $ua^* = [u, a^*]$. Так как $(u\mathfrak{o} \cap a^*\mathfrak{o}) \supseteq (u\mathfrak{o} \cap b\mathfrak{o})$, то мы получаем, что $ub' = [u, b] = [u, a^*]\,c = ua^*c$. Следовательно, $b' = a^*c$ и $a^*\mathfrak{o} \supseteq b'\mathfrak{o}$, а потому a является полным делителем элемента b'. Отсюда следует, что a' является полным делителем b'.

Ограниченные элементы в $\Phi\,[t, S]$. Пусть Γ является центром тела Φ, и предположим, что $(\Phi : \Gamma) = m$ $(< \infty)$ и что существуют отличные от S^0 степени S, являющиеся внутренними автоморфизмами. Пусть S^r является наименьшей положительной степенью, обладающей этим свойством, причем для всех $\xi \in \Phi$ $\xi^{S^r} = \mu^{-1}\xi\mu$. Тогда S индуцирует автоморфизм в Γ и $S^r = 1$ в Γ. Если S^t является наименьшей степенью индуцированного автоморфизма, равной тождественному автоморфизму, то $t = r$. В самом деле, как мы докажем позже (глава 5, § 9), если автоморфизм S^t оставляет элементы Γ на месте, то S^t является внутренним автоморфизмом. Следовательно, $t \geqslant r$, и так как очевидно, что $t \leqslant r$, то $t = r$. Если Γ_0 является подполем, состоящим из элементов, остающихся на месте при автоморфизме S, то, в силу теории Галуа полей, имеем: $(\Gamma : \Gamma_0) = r$ [1]. Следовательно, $(\Phi : \Gamma_0) = mr$.

Так как автоморфизмы S и S^r коммутируют и $\xi^{S^r} = \mu^{-1}\xi\mu$, то $(\mu^S)^{-1}\xi\mu^S = \mu^{-1}\xi\mu$. Следовательно, $\mu^S = \delta\mu$, где $\delta \in \Gamma$. Отсюда следует, что $\delta\delta^S \ldots \delta^{S^{r-1}} = 1$. Тогда, как мы покажем в § 9, $\delta = \eta\,(\eta^S)^{-1}$, где $\eta \in \Gamma$. Заменяя μ через $\eta\mu$ и изменяя обозначения, мы можем считать, что $\mu^S = \mu$.

[1] См. главу 4 § 19.

Предположим теперь, что элемент $a^* = t^{mr}\gamma_0 + t^{(m-1)r}\gamma_1 + \ldots + \gamma_m$, где $\gamma_m = 1$ порождает двусторонний идеал. Тогда элемент a^* может быть записан в виде $u^m\delta_0 + u^{m-1}\delta_1 + \ldots + \delta_m$, где $\delta_m = 1$ и $u = t^r\mu^{-1}$, $u^2 = t^{2r}\mu^{-2}, \ldots$ Так как a^* порождает двусторонний идеал, то $\delta_i \in \Gamma_0$, и общей формой элемента, порождающего двусторонний идеал, является:

$$t^k (u^m\delta_0 + u^{m-1}\delta_1 + \ldots + \delta_m)\gamma, \quad \delta_i \in \Gamma_0.$$

Если $a(t)$ является полиномом степени h, то положим

$$u^i = a(t)\, q_i(t) + r_i(t), \quad i = 0, 1, \ldots, mrh,$$

где $\deg r_i(t) < h$. Так как полиномы степени $< h$ образуют пространство размерности $mrh = N$ над Γ_0, то в Γ_0 существуют такие элементы $\delta_0, \delta_1, \ldots, \delta_N$, что $\sum r_i(t)\delta_i = 0$. Следовательно, $\sum u^i\delta_i \equiv a^*(t) = a(t)\, q(t)$, где $q(t) = \sum q_i(t)\delta_i$ и $a(t)\,\Phi[t, S] \supseteq a^*(t)\,\Phi[t, S]$.

Теорема 15. *Если тело* Φ *имеет конечную размерность над своим центром и автоморфизм* S^r, $0 < r < \infty$, *является внутренним, то каждый идеал в* $\Phi[t, S]$ *ограничен.*

7. Матрицы с элементами из $\mathfrak{o}$. Если U и V входят в кольцо $\mathfrak{o}_n$ матриц порядка n с элементами из $\mathfrak{o}$ и $UV = 1$, то и $VU = 1$. Это является непосредственным следствием того, что кольцо $\mathfrak{o}$ может быть вложено в тело. Таким образом, U является обратимым элементом в $\mathfrak{o}_n$. Если A и B — некоторые $n \times r$ матрицы (n строк, r столбцов) с элементами из $\mathfrak{o}$ и $B = UAV$, где U и V являются обратимыми элементами соответственно в $\mathfrak{o}_n$ и $\mathfrak{o}_r$, то A и B называются *ассоциированными* матрицами. В этом параграфе мы рассмотрим проблему выбора канонической формы среди матриц, ассоциированных с данной. В следующем параграфе это будет применено для изучения структуры произвольного $\mathfrak{o}$-модуля.

Пусть a и b являются отличными от нуля элементами в $\mathfrak{o}$ и $a\mathfrak{o} + b\mathfrak{o} = d\mathfrak{o}$, $(a\mathfrak{o} \cap b\mathfrak{o}) = m\mathfrak{o}$. Тогда существуют

такие элементы p, q, r, s, что $ap + bq = d$, $ar + bs = 0$, где $m = ar = -bs \neq 0$ и $\mathfrak{o}r + \mathfrak{o}s = \mathfrak{o}$. Если $a = da_1$, $b = db_1$ и c_1, d_1 являются такими элементами, что $c_1r + d_1s = 1$, то мы полагаем $u = c_1p + d_1q$, и можно проверить, что

$$\begin{pmatrix} a_1 & b_1 \\ c_1 - ua_1 & d_1 - ub_1 \end{pmatrix} \begin{pmatrix} p & r \\ q & s \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Следовательно, матрица $\begin{pmatrix} p & r \\ q & s \end{pmatrix}$ обратима в $\mathfrak{o}_2$ и

$$V = \begin{array}{c} \\ 1 \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccccc} & & & i & & j & \\ \end{array} \\ \left\{\begin{array}{ccccccc} & & & \cdot & & \cdot & \\ & \cdot & & \cdot & & \cdot & \\ & & \cdot & \cdot & & \cdot & \\ & & & 1 & \cdot & \cdot & \\ \cdots & & & p & \cdots & r & \cdots \\ & & & \cdot & 1 & \cdot & \\ & & & \cdot & \cdot & \cdot & \\ & & & \cdot & & \cdot & \\ & & & & & 1 & \cdot \\ \cdots & & & q & & s & \cdots \\ & & & & & & 1 \\ & & & & & & \cdot \\ & & & & & & \cdot \\ & & & & & & 1 \end{array}\right\} \end{array} \begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \\ i \\ \\ \\ \\ \\ \\ \\ \\ \\ j \\ \\ \\ \\ \end{array}$$

является обратимым элементом в $\mathfrak{o}_r$. Если i-й строкой в A является $(c_1, \ldots, c_{i-1}, a, c_{i+1}, \ldots c_{j-1}, b, c_{j+1}, \ldots, c_r)$, то i-й строкой в AV будет $(c_1, \ldots, c_{i-1}, d, c_{i+1}, \ldots, c_{j-1}, 0, c_{j+1}, \ldots, c_r)$. Аналогичный результат имеет место для столбцов матрицы A.

Отметим далее, что следующие „элементарные“ преобразования могут быть выполнены при помощи умножения матрицы A справа и слева на обратимые матрицы:

I. Прибавление к i-му столбцу j-го столбца, умноженного справа на q $(i \neq j)$. Это делается при помощи умножения A справа на $(1 + e_{ji}q)$. Для того чтобы прибавить

к i-й строке j-ю строку, умноженную слева на q, надо умножить A слева на $(1+e_{ij}q)$.

II. Перестановка i-го и j-го столбцов (строк): надо образовать $A\ (1+e_{ij}+e_{ji}-e_{ii}-e_{jj})$ (или $(1+e_{ij}+e_{ji}-e_{ii}-e_{jj})\ A$).

III. Умножение i-го столбца (строки) справа (слева) на обратимый элемент u: надо образовать

$$A\ (1+(u-1)\ e_{ii}) \quad (\text{или } (1+(u-1)\ e_{ii})\ A).$$

Пусть $A\neq 0$ и $a_{pq}\neq 0$ является элементом матрицы A, имеющим наименьшую длину среди ненулевых элементов A. Произведя операции типа II, мы получаем ассоциированную с A матрицу $B=(b_{ij})$, для которой $b_{11}\neq 0$ имеет наименьшую длину. Если b_{11} не является левым делителем хотя бы одного из b_{1i}, то найдется соответствующая ассоциированная матрица BV, в которой на месте b_{11} стоит элемент $d\neq 0$, длина которого меньше, чем длина b_{11}. Таким же образом, если b_{11} не является правым делителем всех b_{i1}, то b_{11} может быть заменен элементом меньшей длины. После конечного числа таких замен мы получим ассоциированную с A матрицу C, в которой $c_{11}\neq 0$ и является левым делителем каждого элемента c_{1i} и правым делителем каждого элемента c_{i1}. Если $c_{1i}=c_{11}q_i$, то мы умножаем последовательно первый столбец справа на $-q_i$ и складываем с 2-м, 3-м, ..., r-м столбцом. При этом первый столбец остается неизменным, а элементы c_{1i}, $i>1$ заменяются нулем. Если мы применим подобную операцию к строкам, то получим ассоциированную с A матрицу D следующего вида:

$$D=\begin{pmatrix} d_1 & 0 & \dots 0 \\ 0 & d_{22}\dots d_{2r} \\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ 0 & d_{n2}\dots d_{nr} \end{pmatrix}, \qquad d_1\neq 0.$$

Этот процесс, примененный к матрице (d_{ij}) и повторенный для ее подматриц, показывает, что A обладает ассоциированной с ней матрицей, имеющей диагональную форму $\{d_1, \dots, d_s, 0, \dots, 0\}$, $d_i\neq 0$.

Можно предполагать, что каждый элемент d_i является полным делителем элементов d_j при $j>i$: если d_i для каждого элемента b является полным делителем bd_j, то $d_i\mathfrak{o}\supseteq\mathfrak{o}d_j\mathfrak{o}$ и, как мы видели, d_i является полным делителем элемента d_j. Пусть теперь существует такое $b\neq 0$, что d_1 не является левым делителем bd_2. Прибавим умноженную слева на b вторую строку к первой. Верхний угол получившейся матрицы имеет вид:

$$D_2=\begin{pmatrix} d_1 & bd_2 \\ 0 & d_2 \end{pmatrix};$$

D_2 обладает ассоциированной матрицей вида

$$D_2V_2=\begin{pmatrix} d'_{11} & 0 \\ d'_{12} & d'_{22} \end{pmatrix},$$

где d'_{11} является общим наибольшим левым делителем элементов d_1 и bd_2 и, следовательно, имеет меньшую длину, чем d_1. Эта матрица может быть приведена к диагональной форме, причем элемент, стоящий в первой строке и в первом столбце, будет иметь меньшую длину, чем d_1. Повторяя этот процесс, мы получим ассоциированную с A матрицу $\{e_1, \dots, e_s, 0, \dots, 0\}$, в которой каждый элемент e_i является левым делителем всех be_j при $j>i$. Следовательно,

Теорема 16. *Каждая прямоугольная матрица с элементами из $\mathfrak{o}$ имеет ассоциированную с ней диагональную матрицу $\{e_1, \dots, e_s, 0, \dots, 0\}$, в которой каждый элемент e_i является полным делителем e_j при $j>i$.*

Мы можем заменить e_i через $u_ie_iv_i$, где элементы u_i и v_i обратимы, и получить другую диагональную матрицу, имеющую те же свойства, что и $\{e_1, \dots, e_s, 0, \dots, 0\}$. Если $\mathfrak{o}$ является телом, то мы можем поэтому предполагать, что $e_i=1$. Таким образом мы получаем

Следствие. *Если $\mathfrak{o}$ является телом, то каждая прямоугольная матрица с элементами из $\mathfrak{o}$ обладает ассоциированной матрицей вида* $\{1, \dots, 1, 0, \dots, 0\}$.

Рассмотрим далее специально случай коммутативной области $\mathfrak{o}$. Пусть h_i обозначает общий наибольший делитель всех миноров матрицы A, имеющих i строк. Так как столбцы каждой матрицы AV являются линейными комбинациями столбцов матрицы A, то h_i является делителем i-строчных миноров матрицы AV. Таким же образом получаем, что h_i является делителем i-строчных миноров любой матрицы вида UA. Следовательно, если U и V являются обратными матрицами, то h_i является общим наибольшим делителем всех i-строчных миноров матрицы UAV. Если теперь U и V выбраны так, что $UAV = \{e_1, \ldots, e_s, 0, \ldots, 0\}$, где e_i является делителем e_j при $j > i$, то очевидно, что $h_i = e_1 \ldots e_i$, и потому $e_i = h_i h_{i-1}^{-1}$. Это позволяет нам непосредственно найти нормальную форму $\{e_1, \ldots, e_s, 0, \ldots, 0\}$ матрицы A. Можно также показать, что элементы e_i определены с точностью до обратимых делителей. В § 11 мы покажем, что в общем случае элементы e_i определяются матрицей A с точностью до подобия.

8. Структура $\mathfrak{o}$-модулей с конечным числом образующих. Мы видели, что любой $\mathfrak{o}$-модуль с конечным числом образующих имеет вид $\mathfrak{F}/\mathfrak{N}$, где $\mathfrak{F}$ является свободным модулем с базисом $x_1, \ldots, x_n$, а $\mathfrak{N}$ — его подмодулем. Мы рассмотрим сначала структуру $\mathfrak{N}$.

Теорема 17. *Если $\mathfrak{o}$ является кольцом главных идеалов, а $\mathfrak{F}$ — свободным $\mathfrak{o}$-модулем, то каждый подмодуль $\mathfrak{N}$ модуля $\mathfrak{F}$ свободен. Число элементов базиса модуля $\mathfrak{N}$ не превышает числа элементов базиса $\mathfrak{F}$.*

Пусть $\mathfrak{N}$ является подмодулем в $\mathfrak{F}$, и предположим, что $\mathfrak{N}$ содержится в модулях $(x_1, \ldots, x_n), \ldots, (x_{n_1}, \ldots, x_n)$, но не в модуле $(x_{n_1+1}, \ldots, x_n)$, где вообще $(y_1, \ldots, y_r)$ обозначает $\mathfrak{o}$-модуль, порожденный элементами y_i. Коэффициенты при x_{n_1} в элементах $y \in \mathfrak{N}$ образуют правый идеал $b_{n_1}\mathfrak{o} \neq 0$. Таким образом, существует элемент $y_1 = x_{n_1}b_{n_1} + \sum_{j>n_1} x_j b_j \in \mathfrak{N}$, и, если $z = x_{n_1}d_{n_1} + \sum_{j>n_1} x_j d_j$ является некоторым элементом из $\mathfrak{N}$, то мы имеем $d_{n_1} = b_{n_1}k$.

Следовательно, $z - y_1 k \in (x_{n_1+1}, \ldots, x_n)$. Рассмотрим далее $\mathfrak{o}$-модуль $\mathfrak{N}_1 = \mathfrak{N} \cap (x_{n_1+1}, \ldots, x_n)$. Применяя к нему те же рассуждения, мы найдем такое $n_2 > n_1$, что $\mathfrak{N}_1 \subseteq (x_j, \ldots, x_n)$ при $j \leqslant n_2$, но $\mathfrak{N}_1 \not\subseteq (x_{n_2+1}, \ldots, x_n)$. Следовательно, найдется такое $y_2 = x_{n_2}b_{n_2} + \sum_{j>n_2} x_j b_j$, что для любого $z \in \mathfrak{N}_1$ существует $k \in \mathfrak{o}$, при котором $z - y_2 k \in (x_{n_2+1}, \ldots, x_n)$. Если мы продолжим этот процесс, то получим $r \leqslant n$ таких элементов $y_1, \ldots, y_r \in \mathfrak{N}$, где $y_i = x_{ni}b_{ni} + \sum_{j>n_i} x_j b_{ji}$, $b_{ni} \neq 0$, $n_1 < n_2 < \ldots$, что любой элемент $z \in \mathfrak{N}$ имеет вид $\sum y_i k_i$. Элемент y можно представить в таком виде единственным образом, что легко следует из вида элементов y_i.

Далее, мы можем заменить базис x_i модуля $\mathfrak{F}$ базисом $\bar{x}_i = \sum x_j u_{ji}$, где матрица (u) является обратимым элементом в $\mathfrak{o}_n$. Также и элементы $y_k = \sum x_i b_{ik}$ могут быть заменены элементами $\bar{y}_k = \sum y_i v_{ik}$, где матрица (v) обратима в $\mathfrak{o}_r$. Тогда мы получим $y_k = \sum \bar{x}_i e_{ik}$, где матрица $(e) = (u)^{-1}(b)(v)$ ассоциирована с (b). Из теоремы 16 следует, что при подходящем выборе элементов $\bar{x}_i$ и $\bar{y}_i$ мы получим $\bar{y}_k = \bar{x}_k e_k$, где $e_k \neq 0$ при $k = 1, \ldots, s$, и $e_k = 0$ при $k > s$, причем каждый элемент e_k является полным делителем элемента e_l при $l > k$. Мы снова переходим к первоначальным обозначениям и будем писать x и y вместо $\bar{x}$ и $\bar{y}$.

Рассмотрим теперь фактор-модуль $\mathfrak{F}/\mathfrak{N}$. Он порождается смежными классами $\{x_i\}$, содержащими x_i. Если $\{x_1\}c_1 + \ldots + \{x_n\}c_n = 0$, то $x_1c_1 + \ldots + x_nc_n \in \mathfrak{N}$, и, следовательно, $c_j \in e_j\mathfrak{o}$ при $j = 1, \ldots, s$, и $c_j = 0$ при $j > s$. Так как $x_j e_j \in \mathfrak{N}$ при $j \leqslant s$, то $\mathfrak{F}/\mathfrak{N}$ является прямой суммой циклических модулей $\{x_i\}$. При этом циклические модули $\{x_1\}, \ldots, \{x_s\}$ конечны, а циклические модули $\{x_{s+1}\}, \ldots, \{x_n\}$ бесконечны. Модуль $\{x_j\}$ при $j \leqslant s$ изоморфен модулю $\mathfrak{o}/e_j\mathfrak{o}$, причем если элемент e_j обратим, то мы можем опустить соответствующее слагаемое $\{x_j\}$. Если $a_1, \ldots, a_s$ являются произвольными элементами из $\mathfrak{o}$, то существуют такие элементы k_i, что $a_i k_i = e_s b$ и,

если k является общим кратным элементов k_i, то $a_i k = e_s c_i$. Следовательно, $(\{x_1\} a_1 + \ldots + \{x_s\} a_s) k = 0$. Отсюда следует, что модуль $\mathfrak{P}/\mathfrak{N}$ смежных классов $\{x_1\} a_1 + \ldots + \{x_s\} a_s$ может быть охарактеризован как совокупность имеющих конечный порядок элементов из $\mathfrak{F}/\mathfrak{N}$. Фактор-модуль $\mathfrak{F}/\mathfrak{N}/\mathfrak{P}/\mathfrak{N}$ является свободным модулем размерности $n - s$. Очевидно, что это число есть инвариант модуля $\mathfrak{F}/\mathfrak{N}$. Если мы учтем, что всякий $\mathfrak{o}$-модуль с конечным числом образующих $\mathfrak{o}$-изоморфен фактор-модулю $\mathfrak{F}/\mathfrak{N}$, то получим следующие теоремы.

Теорема 18. *Каждый $\mathfrak{o}$-модуль с конечным числом образующих разлагается в прямую сумму свободного $\mathfrak{o}$-модуля и подмодуля, состоящего из элементов конечного порядка.*

Теорема 19. *Каждый $\mathfrak{o}$-модуль с конечным числом образующих разлагается в прямую сумму циклических $\mathfrak{o}$-модулей. Отличные от нуля порядки $e_i\mathfrak{o}$ могут быть выбраны так, что при $j > i$ элемент e_i является полным делителем элемента e_j.* [1)]

При дальнейшем изучении $\mathfrak{o}$-модулей с конечным числом образующих мы можем ограничиться случаем, когда все элементы модуля имеют конечный порядок. Таким образом, в принятых нами обозначениях $s = n$. Из теоремы 19 следует, что неразложимый $\mathfrak{o}$-модуль является циклическим порядка $q_i\mathfrak{o}$, где элемент q_i неразложим. Каждый модуль является прямой суммой модулей вида $\mathfrak{o}/q_i\mathfrak{o}$. По теореме Крулля-Шмидта элементы q_i определены с точностью до подобия. Мы назовем эти элементы *элементарными делителями* модуля.

9. Ограниченные неразложимые элементы. Мы видели, что если фактор-модуль $\mathfrak{o}/q\mathfrak{o}$ неразложим и идеал $q\mathfrak{o}$ ограничен, то его граница $q^*\mathfrak{o}$ является степенью $(p^*\mathfrak{o})^e$ максимального двустороннего идеала $(p^*\mathfrak{o})$. Если

[1)] Обычная теория коммутативных групп с конечным числом образующих получается из теорем 18 и 19, если положить кольцо $\mathfrak{o}$ равным кольцу целых рациональных чисел.

$q = p_1 \ldots p_t$ является разложением элемента q на неприводимые множители p_i, то идеалы $p_i\mathfrak{o}$ ограничены, причем их границы содержат идеал $q^*\mathfrak{o}$. Так как идеал $p_i\mathfrak{o}$ максимален, то его граница является максимальным двусторонним идеалом. Следовательно, его границей является идеал $p^*\mathfrak{o}$. Пусть теперь $p_1, \ldots, p_f$ — произвольные неприводимые элементы, имеющие то свойство, что границами идеалов $p_i\mathfrak{o}$ является $p^*\mathfrak{o}$. Предположим, что $p_{i+1} \ldots p_f\mathfrak{o} \supseteq (p^*\mathfrak{o})^{f-i}$. Тогда $p_i p_{i+1} \ldots p_f\mathfrak{o} \supseteq p_i (p^*\mathfrak{o})^{f-i} = (p_i\mathfrak{o})(p^*\mathfrak{o})^{f-i} \supseteq (p^*\mathfrak{o})(p^*\mathfrak{o})^{f-i} = (p^*\mathfrak{o})^{f-i+1}$. Таким образом, мы доказали, что идеал $p_1 \ldots p_f\mathfrak{o}$ ограничен и его границей является $(p^*\mathfrak{o})^e$, где $e \leqslant f$. Очевидно, отсюда следует, что границей идеала $p_1 \ldots p_k\mathfrak{o} \cap p_{k+1} \ldots p_f\mathfrak{o}$ является $(p^*\mathfrak{o})^e$, где $e \leqslant \min(k, f-k)$.

Образуем теперь прямую сумму $\mathfrak{N}_h$ h циклических модулей, каждый из которых $\mathfrak{o}$-изоморфен модулю $\mathfrak{o}/q\mathfrak{o}$, где элемент $q = p_1 \ldots p_f$ неразложим, и предположим, что модуль $\mathfrak{N}_h$ цикличен. Тогда модуль $\mathfrak{N}_h$ будет $\mathfrak{o}$-изоморфен модулю $\mathfrak{o}/q_h\mathfrak{o}$. Границей идеала $q_h\mathfrak{o}$ является $(p^*\mathfrak{a})^e$, и длина q_h равна fh. Таким образом, $fh \leqslant ek$, где через k обозначена длина элемента p^*. Рассмотрим теперь модуль $\mathfrak{N}_{h+1}$ — прямую сумму $h+1$ модулей, изоморфных модулю $\mathfrak{o}/q\mathfrak{o}$. Покажем, что либо модуль $\mathfrak{N}_{h+1}$ цикличен, либо $q_h\mathfrak{o} = (p^*\mathfrak{o})^e$. В самом деле, если модуль $\mathfrak{N}_{h+1}$ не является циклическим, то он разлагается в прямую сумму s (где $s > 1$) циклических модулей, порядками которых будут идеалы $e_i\mathfrak{o}$, причем элемент e_i является полным делителем элемента e_j при $j > i$. По теореме Крулля-Шмидта, неразложимые делители элементов e_i подобны элементу q и, следовательно, длина $e_1 \geqslant$ длины q, причем границей $e_1\mathfrak{o}$ является $(p^*\mathfrak{o})^e$. Тогда длина $e_2 \geqslant ek \geqslant fh =$ длине q_h. Так как

$$\text{длина } q_h + \text{длина } q \geqslant \text{длина } e_1 + \text{длина } e_2,$$

то мы видим, что длина $e_2 =$ длине $q_h =$ длине $(p^*)^e$. Следовательно, $q_h\mathfrak{o} = (p^*\mathfrak{o})^e$. Если модуль $\mathfrak{N}_{h+1}$ цикличен, то мы строим модуль $\mathfrak{N}_{h+2}$ и повторяем этот процесс далее. Так как длины элементов $q_h, q_{h+1}, \ldots$ образуют возрастающую последовательность, ограниченную длиной элемента

$(p^*)^e$, то мы найдем такое целое число k', что модуль $\mathfrak{N}_{k'}$ будет циклическим, в то время как модуль $\mathfrak{N}_{k'+1}$ не будет таковым. Тогда $q_{k'}\mathfrak{o} = (p^*\mathfrak{o})^e$, и фактор-модуль $\mathfrak{o}/(p^*\mathfrak{o})^e$ разложим в прямую сумму k' модулей, изморфных модулю $\mathfrak{o}/q\mathfrak{o}$. Тем самым доказана важная

Теорема 20. *Если модуль $\mathfrak{o}/q\mathfrak{o}$ неразложим и идеал $q\mathfrak{o}$ ограничен, причем его границей является идеал $(p^*\mathfrak{o})^e$, где идеал $p^*\mathfrak{o}$ максимален, то фактор-модуль $\mathfrak{o}/(p^*\mathfrak{o})^e$ разлагается в прямую сумму k' модулей, $\mathfrak{o}$-изоморфных модулю $\mathfrak{o}/q\mathfrak{o}$. Необходимым и достаточным условием для того, чтобы два неразложимых модуля $\mathfrak{o}/q\mathfrak{o}$ и $\mathfrak{o}/r\mathfrak{o}$, где идеалы $q\mathfrak{o}$ и $r\mathfrak{o}$ ограничены, были $\mathfrak{o}$-изоморфны, является совпадение границ идеалов $q\mathfrak{o}$ и $r\mathfrak{o}$.*

Следствие. *Если $p_1\mathfrak{o} \supseteq p^*\mathfrak{o}$ и $p_2\mathfrak{o} \supseteq p^*\mathfrak{o}$, причем элементы p_i неприводимы, то p_1 и p_2 подобны.*

В самом деле, $p_i\mathfrak{o}$ имеет границу $p^*\mathfrak{o}$, и модуль $\mathfrak{o}/p_i\mathfrak{o}$ неразложим. В частности, все делители p_i элемента q подобны.

Пусть $p^*\mathfrak{o}$ является произвольным не совпадающим с 0 и $\mathfrak{o}$ максимальным двусторонним идеалом, и $p\mathfrak{o} \neq \mathfrak{o}$ является максимальным содержащим $p^*\mathfrak{o}$ правым идеалом. Если элементы $p_1, \ldots, p_h$ подобны p, то, как и выше, показываем, что идеал $p_1 \ldots p_h\mathfrak{o}$ имеет границу $(p^*\mathfrak{o})^{h'}$, где $h' \leqslant h$. Предположим, что мы уже определили такие элементы $p_1, \ldots, p_h$, что границей идеала $p_1 \ldots p_h\mathfrak{o}$ является $(p^*\mathfrak{o})^h$. Тогда существует такой элемент p_{h+1}, что границей идеала $p_1 \ldots p_{h+1}\mathfrak{o}$ является $(p^*\mathfrak{o})^{h+1}$. В противном случае для каждого p', подобного p, мы имели бы $p_1 \ldots p_h p'\mathfrak{o} \supseteq (p^*\mathfrak{o})^h$. Так как пересечение $\Delta p'\mathfrak{o} = p^*\mathfrak{o}$, то $\Delta p_1 \ldots p_h p'\mathfrak{o} = p_1 \ldots p_h(p^*\mathfrak{o})$ и содержит $(p^*\mathfrak{o})^h$. Отсюда следует, что $p_1 \ldots p_h\mathfrak{o} \supseteq (p^*\mathfrak{o})^{h-1}$ вопреки выбору элементов $p_1, \ldots, p_h$. Таким образом, для каждого целого числа e существуют такие элементы p_i, $i = 1, \ldots, e$, что границей $p_1 \ldots p_e\mathfrak{o}$ является $(p^*\mathfrak{o})^e$. Тогда идеал $p_1 \ldots p_e\mathfrak{o}$ неразложим, так как в противном случае его границей был бы идеал $(p^*\mathfrak{o})^{e'}$, где $e' < e$. Из предыдущей теоремы вытекает теперь

Теорема 21. *Пусть $q = p_1 \ldots p_e$, где элементы p_i неприводимы, и идеал $p_i\mathfrak{o}$ имеет границу $p^*\mathfrak{o}$. Тогда для того, чтобы элемент q был неразложим, необходимо и достаточно, чтобы границей идеала $q\mathfrak{o}$ был идеал $(p^*\mathfrak{o})^e$.*

Сравнение длин показывает, что число k' неразложимых компонент в прямом разложении модуля $\mathfrak{o}/(p^*\mathfrak{o})^e$ равно длине k элемента p^*. Мы будем называть это число *емкостью* идеала $p^*\mathfrak{o}$. Отметим теперь некоторые важные следствия нашего критерия неразложимости.

Теорема 22. *Если элемент $q = rst$ неразложим и идеал $q\mathfrak{o}$ ограничен, то элемент s неразложим*, т. е. *каждый подмодуль и каждый фактор-модуль неразложимого модуля $\mathfrak{o}/q\mathfrak{o}$, где идеал $q\mathfrak{o}$ ограничен, неразложим.*

Предположим, что $r = p_1 \ldots p_k$, $s = p_{k+1} \ldots p_l$, $t = p_{l+1} \ldots p_e$, причем элементы p_i неприводимы. Пусть $p^*\mathfrak{o}$ является границей $p_i\mathfrak{o}$. Тогда границей $q\mathfrak{o}$ является $(p^*\mathfrak{o})^e$. Если идеал $s\mathfrak{o}$ разложим, то $(s\mathfrak{o}) \supseteq (p^*\mathfrak{o})^{l-k-1}$. Мы видели, что $t\mathfrak{o} \supseteq (p^*\mathfrak{o})^{e-l}$, и поэтому $st\mathfrak{o} \supseteq s(p^*\mathfrak{o})^{e-l} = (s\mathfrak{o})(p^*\mathfrak{o})^{e-l} \supseteq (p^*\mathfrak{o})^{e-k-1}$. Таким же образом получаем, что $rst\mathfrak{o} \supseteq (p^*\mathfrak{o})^{e-1}$, вопреки тому факту, что границей $rst\mathfrak{o}$ является $(p^*\mathfrak{o})^e$.

Теорема 23. *Если идеалы $q_1\mathfrak{o}$ и $q_2\mathfrak{o}$ содержат ограниченный идеал $q\mathfrak{o}$ и элемент q неразложим, то либо $q_1\mathfrak{o} \supseteq q_2\mathfrak{o}$, либо $q_2\mathfrak{o} \supseteq q_1\mathfrak{o}$.*

Если $q_1\mathfrak{o} \cap q_2\mathfrak{o} = q_3\mathfrak{o}$, то $q_3\mathfrak{o} \supseteq q\mathfrak{o}$ и, следовательно, элемент q_3 неразложим. Если границей идеала $q_i\mathfrak{o}$ является $(p^*\mathfrak{o})^{e_i}$, $i = 1, 2$, то границей идеала $q_3\mathfrak{o}$ будет $(p^*\mathfrak{o})^{e_3}$, где $e_3 = \max(e_1, e_2)$. Следовательно, длина элемента q_3 равна наибольшей из длин элементов q_1, q_2, например длине q_1. Тогда $q_3\mathfrak{o} = q_1\mathfrak{o} \subseteq q_2\mathfrak{o}$.

Из этой теоремы легко вытекает следующая

Теорема 24. *Если элемент q неразложим и идеал $q\mathfrak{o}$ ограничен, то модуль $\mathfrak{o}/q\mathfrak{o}$ обладает лишь одним композиционным рядом.*

Пусть теперь $b\mathfrak{o}$ является ограниченным идеалом, граница которого имеет вид $(p^*\mathfrak{o})^e$, где идеал $p^*\mathfrak{o}$ максимален. Предположим, что $b = [q_1, \ldots q_\lambda]$ является прямым разложением b на неразложимые элементы, причем границей $q_i\mathfrak{o}$

является $(p^*\mathfrak{o})^{e_i}$, и $e_1 \geqslant \ldots \geqslant e_\lambda \geqslant 1$. Очевидно, что $e = e_1$. Покажем, что $\lambda \leqslant k$, где k обозначает емкость идеала $p^*\mathfrak{o}$. Предположим, что $\lambda > k$. Если $q_i'\mathfrak{o} \supseteq q_i\mathfrak{o}$, то $[q_1', q_2', \ldots] = q'$ будет являться прямым разложением элемента q', так как мы имеем, очевидно, $q_i'\mathfrak{o} + (q_1'\mathfrak{o} \cap \ldots \cap q'_{i-1}\mathfrak{o} \cap \cap q'_{i+1}\mathfrak{o} \cap \ldots) = \mathfrak{o}$. Выберем делители $q_i'\mathfrak{o}$ идеалов $q_i\mathfrak{o}$ так, чтобы они имели длину e_k при $i = 1, \ldots, k$, и образуем элемент $q' = [q_1', \ldots, q_k']$ или идеал $q_1'\mathfrak{o} \cap \ldots \cap q_k'\mathfrak{o} = q'\mathfrak{o}$. Так как $q'\mathfrak{o} \supseteq (p^*\mathfrak{o})^{e_k}$ и последний идеал разложим на k неразложимых идеалов длины e_k, то мы получаем, что $q'\mathfrak{o} = (p^*\mathfrak{o})^{e_k}$. Таким образом $(p^*\mathfrak{o})^{e_k} \supseteq (q_1\mathfrak{o} \cap \ldots \cap q_k\mathfrak{o})$. С другой стороны, все идеалы $q_{k+1}\mathfrak{o}, \ldots, q_\lambda\mathfrak{o}$ содержат $(p^*\mathfrak{o})^{e_k}$, и мы приходим к противоречию с тем, что $(q_1\mathfrak{o} \cap \ldots \cap q_k\mathfrak{o}) + q_{k+1}\mathfrak{o} = \mathfrak{o}$.

Теорема 25. *Если идеал $b\mathfrak{o}$ имеет границу $(p^*\mathfrak{o})^e$, где $p^*\mathfrak{o}$ является максимальным идеалом емкости k, то прямое разложение элемента b имеет не более k членов.*

Приложения к случаю полиноминальных колец. Предположим, что $\mathfrak{o} = \Phi[t]$, т. е., что $S = 1$. Двусторонние идеалы этой области порождаются полиномами, коэффициенты которых лежат в центре Γ тела Φ. Пусть ρ является элементом из Φ, алгебраическим над Γ в том смысле, что он является корнем полинома $\alpha(t)$ из $\Gamma[t]$. Тогда $\alpha(t)$ делится на $t - \rho$. Если $\alpha(t)$ имеет наименьшую степень среди полиномов, для которых ρ является корнем, то $\alpha(t)$ неприводим в $\Gamma[t]$. Следовательно, если σ является другим таким элементом из Φ, что $\alpha(\sigma) = 0$, то из следствия к теореме 20 следует, что $t - \rho$ и $t - \sigma$ подобны, поэтому $\sigma = \beta^{-1}\rho\beta$. Так как наше предположение о том, что элементы ρ и σ удовлетворяют одному и тому же неприводимому уравнению, эквивалентно предположению, что отображение $\xi(\rho) \to \xi(\sigma)$, где $\xi(t) \subset \Gamma[t]$, является изоморфизмом между $\Gamma(\rho)$ и $\Gamma(\sigma)$ над Γ[1], то нами доказана

Теорема 26. *Пусть Φ является телом с центром Γ и пусть $\Gamma(\rho)$ и $\Gamma(\sigma)$ являются изоморфными алгебраическими над Γ подполями тела Φ. Тогда всякий изоморфизм между $\Gamma(\rho)$ и $\Gamma(\sigma)$ может быть продолжен до внутреннего автоморфизма тела Φ.*

[1] т. е. изоморфизмом, оставляющим на месте элементы из Γ.

Рассмотрим далее $\Phi[t, S]$, где $S^r = 1$ для некоторого $r > 0$, причем ни одна меньшая степень S не является внутренним автоморфизмом. Если мы используем определенную на стр. 77 форму элементов, которые порождают двусторонние идеалы, то увидим, что полином $t^r - \gamma$ порождает максимальный двусторонний идеал в том случае, когда γ является произвольным отличным от нуля элементом, принадлежащим центру Γ, причем $\gamma^S = \gamma$. Для того чтобы полином $t^r - \gamma$ делился на $t - \rho$, необходимо и достаточно, чтобы $\gamma = N(\rho) \equiv \rho\rho^S \ldots \rho^{S^{r-1}}$. В самом деле, если γ коммутирует с ρ, то из $\gamma = \rho\rho^S \ldots \rho^{S^{r-1}}$ следует, что $\gamma = \rho^S \ldots \rho^{S^{r-1}}\rho = N(\rho^S)$ и обратно.

Так как

$$(t^r - \gamma) = (t - \rho)(t^{r-1} + t^{r-2}\rho^{S^{r-1}} + \ldots + \rho^S \ldots \rho^{S^{r-1}}) + (N(\rho) - \gamma) = (t^{r-1} + t^{r-2}\rho^{S^{r-1}} + \ldots + \rho^S \ldots \rho^{S^{r-1}})(t - \rho) + (N(\rho^S) - \gamma),$$

то наше утверждение очевидно. Так как $t^r - \gamma$ порождает максимальный идеал, то любые два неприводимые множителя полинома $t^r - \gamma$ подобны. Кроме того, $t - \rho$ и $t - \sigma$ подобны тогда и только тогда, когда $\sigma = \beta^{-1}\rho\beta^S$. Следовательно, нами получена

Теорема 27. *Пусть Φ является телом и S — таким автоморфизмом в Φ, что $S^r = 1$, $0 < r < \infty$, и ни одна меньшая степень автоморфизма S не является внутренним автоморфизмом. Если элемент γ лежит в центре тела Φ, $\gamma^S = \gamma$ и ρ и σ являются такими элементами тела Φ, что $N(\rho) = \gamma = N(\sigma)$, то существует такой элемент $\beta \in \Phi$, что $\sigma = \beta^{-1}\rho\beta^S$.*

Следствие. *Для того чтобы $N(\sigma) = 1$, необходимо и достаточно, чтобы $\sigma = \beta^{-1}\beta^S$.*

Отметим, что условия, наложенные на S, равносильны утверждению, что S порождает конечную группу $\mathfrak{G}$ внешних автоморфизмов, т. е. что все нетождественные автоморфизмы, входящие в $\mathfrak{G}$, являются внешними. Предпо-

ложим теперь снова, что $\gamma \in \Gamma$, $\gamma^S = \gamma$, и пусть $r = r_1 r_2$. Пусть $\gamma^{r_1} = N(\rho)$, где $\rho \in \Phi$. Тогда полином $t^r - \gamma^{r_1} = (t^{r_1} - \gamma)\, q(t)$ делится на $t - \rho$. Вследствие подобия всех неприводимых делителей полинома $t^r - \gamma^{r_1}$ полином $t^{r_2} - \gamma$ будет делиться слева на некоторое подходящее $t - \sigma$. Так как

$$t^{r_2} - \gamma = (t - \sigma)\,(t^{r_2-1} + \ldots + \sigma^S \ldots \sigma^{S^{r_2-1}}) + \\ + (\sigma\sigma^S \ldots \sigma^{S^{r_2-1}} - \gamma),$$

то $\gamma = \sigma\sigma^S \ldots \sigma^{S^{r_2-1}}$. Но $\gamma \in \Gamma$, и, следовательно, $\gamma = \sigma^S \ldots \sigma^{S^{r_2-1}}\sigma$, а так как $\gamma^S = \gamma$, то $\gamma = \sigma^S \ldots \sigma^{S^{r_2-1}}\sigma^{S^{r_2}}$. Таким образом, $\sigma^{S^{r_2}} = \sigma$.

Теорема 28. *Предположим, что* Φ, S *и* γ *имеют тот же смысл, что и в предыдущей теореме. Если* $r = r_1 r_2$ *и* γ^{r_1} *является нормой некоторого элемента из* Φ, *то* $\gamma = \sigma\sigma^S \ldots \sigma^{S^{r_2-1}}$, где $\sigma^{S^{r_2}} = \sigma$.

10. Ограниченные $\mathfrak{o}$-модули. $\mathfrak{o}$-модуль $\mathfrak{M}$ называется *ограниченным*, если существует такой элемент $b \neq 0$ кольца $\mathfrak{o}$, что $xb = 0$ для всех $x \in \mathfrak{M}$. Совокупность всех таких b образует двусторонний идеал $\mathfrak{B} \neq 0$, который мы назовем *границей* модуля $\mathfrak{M}$. Это согласуется с определением, данным ранее для циклического случая. Легко видеть, что для того чтобы модуль $\mathfrak{M}$ был ограниченным, необходимо и достаточно, чтобы порядки любого множества образующих y_i были ограниченными правыми идеалами. Граница порядка любого $x \in \mathfrak{M}$ является делителем идеала $\mathfrak{B}$.

Если $q_1, \ldots, q_u$ являются элементарными делителями модуля $\mathfrak{M}$, то мы видели, что эти элементы определены с точностью до подобия модулем $\mathfrak{M}$. С другой стороны, любые два неразложимые элемента q подобны тогда и только тогда, когда они имеют одинаковую границу. Следовательно, нами получена основная

Теорема 29. *Границы элементарных делителей ограниченного* $\mathfrak{o}$*-модуля являются инвариантами модуля; они не зависят от различных разложений модуля.*

Пусть $\mathfrak{B} = (p_1{}^*\mathfrak{o})^{f_1} \ldots (p_r{}^*\mathfrak{o})^{f_r}$ будет разложением границы модуля $\mathfrak{M}$, причем максимальные идеалы $p_i{}^*\mathfrak{o}$ различны. Положим $\mathfrak{B}_i = \mathfrak{B}\,(p_i{}^*\mathfrak{o})^{-f_i}$ и обозначим через $\mathfrak{M}^{(i)}$ подмножество $\mathfrak{M}\mathfrak{B}_i$ конечных сумм элементов вида xb_i, где $b_i \in \mathfrak{B}_i$. Так как $\mathfrak{B}_i$ является правым идеалом, то $\mathfrak{M}^{(i)}$ является подмодулем, и так как $\mathfrak{B}_1 + \ldots + \mathfrak{B}_r = \mathfrak{o}$, то $\mathfrak{M} = \mathfrak{M}^{(1)} + \ldots + \mathfrak{M}^{(r)}$. Элементы из $\mathfrak{M}^{(i)}$ удовлетворяют уравнению $x_i (p_i{}^*\mathfrak{o})^{f_i} = 0$, и потому границей $\mathfrak{M}^{(i)}$ является идеал $(p^*\mathfrak{o})^{f_i'}$, где $f_i' \leqslant f_i$. Отсюда следует, что $\mathfrak{M}^{(i)} \cap (\mathfrak{M}^{(1)} + \ldots + \mathfrak{M}^{(i-1)} + \mathfrak{M}^{(i+1)} + \ldots + \mathfrak{M}^{(r)}) = 0$, и, следовательно, $\mathfrak{M} = \mathfrak{M}^{(1)} \oplus \ldots \oplus \mathfrak{M}^{(r)}$. Кроме того, так как для любого x имеем $x p_1{}^{*f_1'} \ldots p_r{}^{*f_r'} = 0$, то $f_i' = f_i$. Предположим, что элемент y из $\mathfrak{M}$ удовлетворяет при некотором k уравнению $y\,(p_j{}^*\mathfrak{o})^k = 0$. Тогда, если мы представим y как $y = y_1 + \ldots + y_r$, $y_i \in \mathfrak{M}^{(i)}$, то получим $y_i\,(p_j{}^*\mathfrak{o})^k = 0$, и так как $(p_j{}^*\mathfrak{o})^k + (p_i{}^*\mathfrak{o})^{f_i} = \mathfrak{o}$, то $y_i = 0$ при $i \neq j$. Таким образом, подмодуль $\mathfrak{M}^{(j)}$ может быть охарактеризован как совокупность таких элементов y_j, для которых $y_j\,(p_j\mathfrak{o})^k = 0$ при некотором k. Отметим также, что если $\mathfrak{N}$ является произвольным подмодулем модуля $\mathfrak{M}$, то $\mathfrak{N} = \mathfrak{N}^{(1)} \oplus \ldots \oplus \mathfrak{N}^{(r)}$, где $\mathfrak{N}^{(i)} = \mathfrak{M}^{(i)} \cap \mathfrak{N}$.

Остановимся теперь на случае, когда $r = 1$, т. е. $\mathfrak{B} = (p^*\mathfrak{o})^f$. Пусть в этом случае $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$ является разложением $\mathfrak{M}$ на неразложимые $\mathfrak{o}$-модули и пусть $(p^*\mathfrak{o})^{e_i}$ является границей циклического модуля $\mathfrak{M}_i$, причем $e_1 \geqslant \ldots \geqslant e_u$. Очевидно, что $e_1 = f$.

Рассмотрим сначала неразложимый $\mathfrak{o}$-модуль $\mathfrak{N}$ с границей $(p^*\mathfrak{o})^g$. Если x является образующим элементом в $\mathfrak{N}$ и $q\mathfrak{o}$ является его порядком, причем $q = p_1 \ldots p_g$, где элементы p_i неприводимы, то $x p_1 \ldots p_{g-1} = y$ не равно нулю, и $y(p^*\mathfrak{o}) = 0$. Таким образом, подмодуль $\mathfrak{N}_0$, состоящий из таких элементов y_0, что $y_0(p^*\mathfrak{o}) = 0$, отличен от нуля. Так как $\mathfrak{N}_0 \subseteq \mathfrak{N}$, то он неразложим, а так как его границей является $p^*\mathfrak{o}$, то подмодуль $\mathfrak{N}_0$ неприводим. Отметим также, что подмодуль $\mathfrak{N}(p^*\mathfrak{o})^j$ неразложим и его элементарный делитель имеет длину, равную $\max(0,\ g - j)$.

В общем случае, когда $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, из $y(p^*\mathfrak{o}) = 0$ и $y = y_1 + \ldots + y_u$, где $y_i \in \mathfrak{M}_i$, следует, что $y_i(p^*\mathfrak{o}) = 0$. Следовательно, u может быть охарактеризовано как длина подмодуля $\mathfrak{M}_0$, состоящего из таких элементов y_0, что $y_0(p^*\mathfrak{o}) = 0$. Мы имеем также $\mathfrak{M}(p^*\mathfrak{o})^j = \mathfrak{M}_1(p^*\mathfrak{o})^j \oplus \ldots \oplus \mathfrak{M}_u(p^*\mathfrak{o})^j$, и, следовательно, число $\delta(j, \mathfrak{M})$ тех границ $(p^*\mathfrak{o})^{e_i}$, показатели которых e_i больше чем j, является длиной пересечения $\mathfrak{M}(p^*\mathfrak{o})^j \cap \mathfrak{M}_0$.

Если $\mathfrak{N}$ является подмодулем модуля $\mathfrak{M}$, то $\mathfrak{N}(p^*\mathfrak{o})^j \subseteq \mathfrak{M}(p^*\mathfrak{o})^j$ и, следовательно, $\mathfrak{N}(p^*\mathfrak{o})^j \cap \mathfrak{N}_0 = \mathfrak{N}(p^*\mathfrak{o})^j \cap \mathfrak{M}_0 \subseteq \mathfrak{M}(p^*\mathfrak{o})^j \cap \mathfrak{M}_0$. Отсюда следует, что $\delta(j, \mathfrak{N}) \leqslant \delta(j, \mathfrak{M})$, и поэтому, если $(p^*\mathfrak{o})^{g_1}$, $(p^*\mathfrak{o})^{g_2}$, ... являются границами элементарных делителей модуля $\mathfrak{N}$ и $g_1 \geqslant g_2 \geqslant \ldots$, то мы получаем, что $e_i \geqslant g_i$. Если мы применим этот факт и отмеченное выше разложение $\mathfrak{M} = \mathfrak{M}^{(1)} \oplus \ldots \oplus \mathfrak{M}^{(r)}$ к тому случаю, когда модуль $\mathfrak{M}$ цикличен, то получим доказательство необходимости в следующей теореме.

Теорема 30. *Предположим, что* $a = [q_{11}, \ldots, q_{1u_1}; \ldots; \ldots, q_{ru_r}]$ *является прямым разложением элемента* a *на неразложимые элементы* q_{ij}, *причем границей идеала* $q_{ij}\mathfrak{o}$ *является* $(p^*_i\mathfrak{o})^{e_{ij}}$ и $e_{i1} \geqslant e_{i2} \geqslant \ldots$ *Пусть также* $b = [s_{11}, \ldots, s_{1u_1}; \ldots; \ldots, s_{ru_r}]$, *где границей* $s_{ij}\mathfrak{o}$ *является* $(p_i^*\mathfrak{o})^{g_{ij}}$, *и* $g_{i1} \geqslant g_{i2} \geqslant \ldots \geqslant 0$. *Тогда для того чтобы* b *было подобно некоторому делителю элемента* a, *необходимо и достаточно, чтобы* $e_{ij} \geqslant g_{ij}$.

Для доказательства достаточности заметим, что существует делитель q'_{ij} элемента q_{ij}, границей которого является $(p_i^*\mathfrak{o})^{g_{ij}}$. В самом деле, мы получим такой элемент, образовав произведение первых g_{ij} неприводимых делителей элемента q_{ij}. Отсюда следует, что $a' = [q'_{11}, \ldots, q'_{1u_1}; \ldots; \ldots, q'_{ru_r}]$ является делителем элемента a. Так как по теоремам 20 и 21 элемент q'_{ij} подобен элементу s_{ij}, то элемент a' подобен элементу b.

11. Инвариантные множители. Пусть $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_s$ является разложением конечного $\mathfrak{o}$-модуля $\mathfrak{M}$ в прямую сумму модулей, $\mathfrak{o}$-изоморфных модулям $\mathfrak{o}/e_i\mathfrak{o}$, причем e_i является полным делителем элемента e_j при $j > i$. Мы хотим показать, что элементы e_i с точностью до подобия являются инвариантами модуля $\mathfrak{M}$.

Предположим сначала, что модуль $\mathfrak{M}$ ограничен. Разлагая элементы e_i на неразложимые элементы q_{ijl}, где границей идеала $q_{ijl}\mathfrak{o}$ является $(p_j^*\mathfrak{o})^{h_{ijl}}$ ($p_j^*\mathfrak{o}$ — максимальный двусторонний идеал), мы получим разложение модуля $\mathfrak{M}$ на неразложимые $\mathfrak{o}$-модули. Пусть $p^*\mathfrak{o}$ является одним из идеалов $p_j^*\mathfrak{o}$, k — его емкостью и элементы $q_1, \ldots q_u$ — теми неразложимыми частями элементов e_i, для которых границы идеалов $q_i\mathfrak{o}$ имеют вид $(p^*\mathfrak{o})^{h_i}$. Напомним, что если границей идеала $q_i\mathfrak{o}$ является $(p^*\mathfrak{o})^{h_i}$, то длина элемента q_i равна h_i. Если q является одним из элементов q_i, и q — неразложимая часть элемента e_r, то e_{r+1} делится на $(p^*)^h$. Следовательно, по теореме 30, элемент e_{r+1} содержит не менее, чем k элементов q_i, длины h_i которых больше или равны h. Так как k является емкостью идеала $p^*\mathfrak{o}$, то этими элементами исчерпываются те из q_i, которые входят в разложение элемента e_{r+1} и соответствуют элементу p^*. Таким образом, мы можем так упорядочить элементы q_i, чтобы в последовательности $q_1, \ldots, q_k; q_{k+1}, \ldots, q_{2k}; \ldots; q_{tk+1}, \ldots, q_{tk+m}$ длины элементов q_i образовывали невозрастающую последовательность, причем элементы $q_1, \ldots, q_k$ являлись неразложимыми частями элемента e_s, $q_{k+1}, \ldots, q_{2k}$ — неразложимыми частями элемента e_{s-1} и т. д.

Если мы имеем второе разложение $\mathfrak{M}_1' \oplus \ldots \oplus \mathfrak{M}_{s'}'$ модуля $\mathfrak{M}$ и модуль $\mathfrak{M}_i'$ $\mathfrak{o}$-изоморфен модулю $\mathfrak{o}/e_i'\mathfrak{o}$, а элемент e_i' является полным делителем элемента e_j' при $j > i$, то мы можем таким же образом упорядочить неразложимые элементы q', соответствующие элементу p^*. По теореме Крулля-Шмидта, элементы q_i и q_i' подобны, и число их одинаково. Таким образом, неразложимые части элементов e_{s-j} и e'_{s-j} могут быть так поставлены во

взаимно однозначное соответствие, чтобы соответствующие части были подобны. Тогда и элементы e_{s-j} и e'_{s-j} подобны, и $s = s'$.

Пусть теперь $\mathfrak{M}$ является произвольным модулем, $\mathfrak{A} = a^*\mathfrak{o}$ — границей идеала $e_{s-1}\mathfrak{o}$, $\mathfrak{B} = b^*\mathfrak{o}$ — границей идеала $e'_{s'-1}\mathfrak{o}$. Пусть $\mathfrak{N}_s$ является подмодулем модуля $\mathfrak{M}_s$, состоящим из таких элементов y, что $y\mathfrak{A}\mathfrak{B} = y\mathfrak{B}\mathfrak{A} = 0$. Если $e_s = ca^*$, и y_s является образующим элементом модуля $\mathfrak{M}_s$ порядка $e_s\mathfrak{o}$, то $y_s c \in \mathfrak{N}_s$ и его порядок равен $a^*\mathfrak{o}$. Следовательно, если z_s — образующий элемент модуля $\mathfrak{N}_s$, то его порядок равен $d_s\bar{a}\mathfrak{o}$, где элемент $\bar{a}$ подобен a^*. Так как $a^*\mathfrak{o}$ является двусторонним идеалом, то $\bar{a}$ отличается от a^* обратимым множителем, и потому порядок элемента z_s равен $d_s a^*\mathfrak{o} = a^* d_s\mathfrak{o}$. Предположим теперь, что $\mathfrak{N}$ является подмодулем модуля $\mathfrak{M}$, состоящим из таких элементов y, что $y\mathfrak{A}\mathfrak{B} = 0$. Очевидно, что подмодуль $\mathfrak{N}$ ограничен, и $\mathfrak{N} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_{s-1} \oplus \mathfrak{N}_s$ является разложением модуля $\mathfrak{N}$ на циклические модули, порядки которых ограничены, причем граница каждого порядка делит следующий порядок. Подобным образом мы получаем, что

$$\mathfrak{N} = \mathfrak{M}_1' \oplus \ldots \oplus \mathfrak{M}'_{s'-1} \oplus \mathfrak{N}'_{s'},$$

где $\mathfrak{N}'_{s'} \subseteq \mathfrak{M}'_{s'}$. Следовательно, в силу результата, полученного для ограниченных модулей, $s' = s$ и элементы e_i и e_i' подобны при $i = 1, \ldots, s-1$. Отсюда, применяя к модулю $\mathfrak{M}$ теорему Крулля-Шмидта, мы получаем, что элементы e_s и e'_s подобны. Мы будем называть элементы e_i инвариантными множителями модуля. Итак, нами получена

Теорема 31 (Накаяма). *Инвариантные множители $\mathfrak{o}$-модуля $\mathfrak{M}$ однозначно определены с точностью до подобия.*

12. Теория отдельно взятого полулинейного преобразования. Мы видели, что если T является полулинейным преобразованием с автоморфизмом S, которое действует в векторном пространстве $\mathfrak{N}$ над телом Φ, то мы можем

рассматривать $\mathfrak{N}$ как $\mathfrak{o} = \Phi[t, S]$-модуль, полагая $x\alpha(t) = x\alpha(T)$. Если T_1 и T_2 являются полулинейными преобразованиями в $\mathfrak{N}$, имеющими одинаковый автоморфизм S, то определенные ими $\Phi[t, S]$-модули изоморфны тогда и только тогда, когда существует такое линейное преобразование A, что $T_2 = A^{-1}T_1A$. В самом деле, если A является $\Phi[t, S]$-изоморфизмом, то A линейно, так как $\xi A = A\xi$ при всех $\xi \in \Phi$, и $T_1A = AT_2$, а потому $T_2 = A^{-1}T_1A$. Обратно, если это условие выполнено для некоторого автоморфизма A, то $\alpha(T_1)A = A\alpha(T_2)$ при всех $\alpha(t)$, и A является изоморфизмом. Если матрицами преобразований T_1, T_2 и A относительно базиса $x_1, \ldots, x_n$ будут соответственно (τ_1), (τ_2) и (α), то условие $T_2 = A^{-1}T_1A$ эквивалентно условию $(\tau_2) = (\alpha)(\tau_1)(\alpha^S)^{-1}$ (или $(\tau_2) = (\beta)^{-1}(\tau_1)(\beta^S)$, где $(\beta) = (\alpha)^{-1}$).

Рассмотрим теперь фиксированное преобразование T. Тогда, каков бы ни был вектор x, в последовательности векторов x, xT, ... найдется вектор xT^m, который является линейной комбинацией векторов xT^i, $i < m$, например, $xT^m = x\beta_m + \ldots + xT^{m-1}\beta_1$. Тогда $x(T^m - T^{m-1}\beta_1 - \ldots - \beta_m) = 0$, и потому каждый элемент $\Phi[t, S]$-модуля $\mathfrak{N}$ имеет конечный порядок. Из общей теории следует тогда, что $\mathfrak{N} = \mathfrak{N}_1 \oplus \ldots \oplus \mathfrak{N}_s$, где $\mathfrak{N}_i$ являются циклическими модулями, образующие элементы u_i которых имеют порядок $e_i\Phi[t, S]$. При этом $e_i = e_i(t)$ является полным делителем $e_j(t)$ при $j > i$. Если степень инвариантного множителя $e_i(t)$ равна n_i, то векторы $u_i, \ldots, u_iT^{n_i-1}$ образуют базис модуля $\mathfrak{N}_i$ над Φ. Следовательно, $u_1, \ldots, u_1T^{n_1-1}; \ldots; \ldots, u_sT^{n_s-1}$ является базисом модуля $\mathfrak{N}$ над Φ, и относительно этого базиса матрицей преобразования T будет

$$\begin{pmatrix} \tau^{(1)} & & & \\ & \tau^{(2)} & & \\ & & \ddots & \\ & & & \tau^{(s)} \end{pmatrix},$$

где

$$\tau^{(i)} = \begin{pmatrix} 0 & . & . & . & \beta_{n_i}^{(i)} \\ 1 & 0 & . & . & \beta_{n_i-1}^{(i)} \\ 0 & 1 & . & . & . \\ . & . & . & . & . \\ . & . & . & 0 & . \\ 0 & . & 0 & 1 & \beta_1^{(i)} \end{pmatrix},$$

если $e_i(t) = t^{n_i} - t^{n_i-1}\beta_1^{(i)} - \ldots - \beta_{n_i}^{(i)}$. Если (α) является произвольной матрицей из Φ_n, то существует такая матрица (ρ), что матрица $(\rho)^{-1}(\alpha)(\rho^S)$ будет иметь указанный вид. Подобным образом мы можем получить каноническую форму матрицы (α), соответствующую разложению $\mathfrak{R}$ на неразложимые $\mathfrak{o}$-модули.

Рассмотрим в качестве примера случай, когда T является линейным преобразованием, действующим в модуле $\mathfrak{R}$ над Φ, где $\Phi = R(i, j)$ является кватернионной алгеброй над действительно замкнутым полем. Мы видели, что в $\mathfrak{o} = \Phi[t]$ неприводимыми являются лишь линейные полиномы. Границей $p^*(t)$ идеала $p(t) = (t-\alpha)$ является $t - \alpha$, если $\alpha \in R$. С другой стороны, имеем $N(t-\alpha) = (t-\alpha)(t-\bar{\alpha})$. Мы получаем таким образом все неприводимые полиномы (со старшим коэффициентом 1) в $R[t]$. Рассмотрим теперь идеал $(t-\alpha)^e\mathfrak{o}$. Его границей является $(p^*)^e\mathfrak{o}$. В самом деле, в противном случае $(t-\alpha)^e$ являлось бы делителем полинома $(p^*)^f$, где $f < e$. Но это, очевидно, невозможно, если $p^* = (t-\alpha)$. Если же $p^* \neq (t-\alpha)$, то мы имеем

$$(t-\alpha)^e q(t) = N(t)^f = (t-\alpha)^f (t-\bar{\alpha})^f.$$

Так как $\bar{\alpha} \in R(\alpha)$, то коэффициенты полинома $q(t)$ лежат в $R(\alpha)$, и так как это кольцо коммутативно, то мы приходим к противоречию с теоремой о единственности разложения в $\mathfrak{R}(\alpha)[t]$. Отсюда следует теперь, что полином $(t-\alpha)^e$ неразложим и что каждый неразложимый элемент подобен элементу такого вида. Следовательно, если $\mathfrak{S}$ является неразложимым подпространством в $\mathfrak{R}$, то оно порождается вектором y порядка $(t-\alpha)^e\mathfrak{o}$. Если мы рассмотрим в $\mathfrak{S}$ базис $y_k = y(T-\alpha)^{k-1}$, $k = 1, \ldots, e$, то получим матрицу

$$\begin{pmatrix} \alpha & & & \\ 1 & \alpha & & \\ & \ddots & \ddots & \\ & & \ddots & \ddots \\ & & & 1 \quad \alpha \end{pmatrix}. \tag{6}$$

Две такие матрицы подобны тогда и только тогда, когда их диагональные элементы α_1 и α_2 подобны; если α_1 и α_2 подобны, то они являются корнями одного и того же неприводимого в $R[t]$ полинома, и обратно. Любая матрица подобна матрице, имеющей вдоль главной диагонали «ящички» вида (6) и на остальных местах нули.

Вернемся к общему случаю и рассмотрим разложение $\mathfrak{R} = \mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_s$, где $\mathfrak{R}_i$ — циклические модули, порядки которых $e_i(t)$ являются инвариантными множителями. Для того, чтобы определить полиномы $e_i(t)$, выберем базис $x_1, \ldots, x_f$ модуля $\mathfrak{R}$ над Φ и положим $x_i T = \sum x_j \tau_{ji}$. Тогда модуль $\mathfrak{R}$ $\Phi[t, S]$-изоморфен фактор-модулю свободного $\Phi[t, S]$-модуля $\mathfrak{F}$, базис которого образуют $e_1, \ldots, e_n$, по подмодулю $\mathfrak{N}$, содержащему элементы $f_i = e_i t - \sum e_j \tau_{ji}$. Покажем, что элементы f_i образуют базис подмодуля $\mathfrak{N}$. В самом деле, если f является произвольным элементом из $\mathfrak{N}$, то мы можем выбрать полиномы $\varphi_1(t), \ldots, \varphi_f(t)$ таким образом, что $f - \sum f_i \varphi_i(t) = \sum e_i \beta_i$, где $\beta_i \in \Phi$. Тогда $\sum x_i \beta_i = 0$, и потому $\beta_i = 0$. Таким образом $f = \sum f_i \varphi_i(t)$. Предположим теперь, что $\sum f_i \varphi_i(t) = 0$. Тогда $\sum e_i [t\varphi_i(t) - \sum \tau_{ij}\varphi_j(t)] = 0$, и $t\varphi_i(t) = \sum \tau_{ij}\varphi_j(t)$, $i = 1, \ldots, n$. Если некоторое $\varphi_i(t) \neq 0$, и $\varphi_k(t)$ является одним из таких полиномов, имеющим среди них максимальную степень, то равенство $t\varphi_k(t) = \sum \tau_{kj}\varphi_j(t)$ невозможно. Следовательно, для всех i имеем $\varphi_i(t) = 0$. Отсюда мы получим, что $e_i(t)$ являются диагональными элементами в нормальной форме матрицы $1 \cdot t - (\tau)$, которая выражает элементы f_i через e_i.

В случае, когда тело Φ коммутативно и преобразование T линейно, кольцо $\Phi[t]$ коммутативно и $e_i(t) = h_i(t)\,h_{i-1}(t)^{-1}$, где $h_0(t) = 1$ и $h_i(t)$ является общим наибольшим делителем всех миноров i-го порядка матрицы $1\cdot t - (\tau)$. Последний инвариантный множитель $e_s(t) = \mu(t)$ обладает тем свойством, что для всех x имеет место $x\mu(T) = 0$. В самом деле, мы имеем $u_i\mu(T) = 0$, где u_i является образующим элементом модуля $\mathfrak{R}_i$, и, так как каждый элемент x имеет вид $\sum u_i\xi_i(T)$, то $x\mu(T) = 0$. Так как $\mu(t)\,\Phi[t, S]$ является порядком элемента u_s, то $\mu(t)$ является полиномом наименьшей степени со старшим коэффициентом 1, для которого T, или, что то же самое, матрица (τ) преобразования T является корнем. Так как другие инвариантные множители являются делителями полинома $\mu(t)$ и характеристический полином $f(t) = \det(1t - (\tau)) = \Pi e_i(t)$, то $f(t)$ и $\mu(t)$ обладают одними и теми же неприводимыми множителями в $\Phi[t]$ и могут отличаться лишь кратностями этих множителей. Это хорошо известная

Теорема 32. (Фробениус). *Пусть* (τ) *— матрица из* Φ_n, *где* Φ *— поле, и пусть* $\mu(t)$ *— последний инвариантный множитель матрицы* $1t - (\tau)$ *из* $(\Phi[t])_n$. *Тогда* 1) $\mu((\tau)) = 0$; 2) $\mu(t)$ *является делителем любого полинома* $\gamma(t)$, *имеющего то свойство, что* $\gamma((\tau)) = 0$, и 3) $\mu(t)$ *и характеристический полином, равный* $\det(1t - (\tau))$, *имеют в* $\Phi[t]$ *одни и те же неприводимые множители.*

Пусть теперь Φ такое тело, что $(\Phi : \Gamma) = m < \infty$, где через Γ обозначен центр тела Φ, и пусть S такой автоморфизм в Φ, что S^r, $0 < r < \infty$, является внутренним автоморфизмом, в то время как ни одна меньшая положительная степень S внутренним автоморфизмом не является. Если Γ_0 — подполе поля Γ, состоящее из элементов, остающихся инвариантными при автоморфизме S, то $(\Gamma : \Gamma_0) = r$, и, следовательно, $(\Phi : \Gamma_0) = mr$. Мы видели, что $\xi^{S^r} = \mu^{-1}\xi\mu$, где $\mu^S = \mu$. Двусторонние идеалы кольца $\mathfrak{o} = \Phi[t, S]$ порождаются элементами вида $t^j(u^h + u^{h-1}\gamma_1 + \ldots + \gamma_h)$, где $u = t^r\mu^{-1}$ и $\gamma_i \in \Gamma_0$. Каждый идеал кольца $\mathfrak{o}$ ограничен.

Если $\mathfrak{o}_1 = \Gamma_0[u]$, то очевидно, что любой $\mathfrak{o}$-модуль является $\mathfrak{o}_1$-модулем, и если два $\mathfrak{o}$-модуля $\mathfrak{o}$-изоморфны, то они и $\mathfrak{o}_1$-изоморфны. Мы хотим доказать для модулей, не содержащих элементов порядка $t\mathfrak{o}$, утверждение, обратное последнему результату. Для этой цели рассмотрим сначала неразложимый модуль $\mathfrak{R}_1$ такого типа. Тогда $\mathfrak{R}_1$ обладает границей $(p^*)^e\mathfrak{o}$, где $p^* = u^h + u^{h-1}\gamma_1 + \ldots + \gamma_h$, $\gamma_i \in \Gamma_0$ и $\gamma_h \neq 0$. Мы видели, что модуль $\mathfrak{R}_1$ может быть вложен в циклический модуль $\mathfrak{R}$, образующий элемент которого имеет порядок $(p^*)^e\mathfrak{o}$, и что $\mathfrak{R} = \mathfrak{R}_1 \oplus \ldots \oplus \mathfrak{R}_k$, где модули $\mathfrak{R}_i$ $\mathfrak{o}$-изоморфны неразложимым $\mathfrak{o}$-модулям и k является емкостью идеала $p^*\mathfrak{o}$. Мы можем получить разложение модуля $\mathfrak{R}$ на неразложимые $\mathfrak{o}$-модули, разлагая модули $\mathfrak{R}_i$. Это дает kl неразложимых $\mathfrak{o}_1$-компонент модуля $\mathfrak{R}$. С другой стороны, мы можем применить также следующий способ. Пусть элементы $\rho_1, \ldots, \rho_{mr}$ образуют базис тела Φ над Γ_0. Так как векторы zt^ju^l, $j = 0, \ldots, r-1$, $l = 0, \ldots, h-1$, образуют базис модуля $\mathfrak{R}$ над Φ, то векторы $zt^ju^l\rho_i$, $i = 1, \ldots, mr$ образуют базис модуля $\mathfrak{R}$ над Γ_0. Следовательно, $\mathfrak{R}$ является прямой суммой mr^2 циклических $\mathfrak{o}_1$-модулей, образующими элементами которых являются $zt^j\rho_i$. Порядками этих модулей будут $(p^*)^e\mathfrak{o}_1$, и так как идеал $p^*\mathfrak{o}_1$ максимален в коммутативном кольце $\mathfrak{o}_1$, то эти модули неразложимы. Отсюда следует, что $mr^2 = kl$ и что $\mathfrak{R}_1$ является прямой суммой $\frac{mr^2}{k}$ неразложимых $\mathfrak{o}_1$-модулей, порядками которых являются идеалы $(p^*)^e\mathfrak{o}_1$.

Пусть теперь $\mathfrak{R}_1$ и $\bar{\mathfrak{R}}_1$ являются двумя неразложимыми модулями, не содержащими элементов порядка $t\mathfrak{o}$, и предположим, что $\mathfrak{R}_1$ и $\bar{\mathfrak{R}}_1$ $\mathfrak{o}_1$-изоморфны. Тогда, если $\bar{p}^*$, $\bar{e}$, $\bar{k}$ имеют для модуля $\bar{\mathfrak{R}}_1$ тот же смысл, что и p^*, e, k для модуля $\mathfrak{R}_1$, то мы, очевидно, будем иметь $k = \bar{k}$, и $(p^*)^e = (\bar{p}^*)^{\bar{e}}$. Таким образом, модули $\mathfrak{R}_1$ и $\bar{\mathfrak{R}}_1$ имеют одинаковую границу, и потому они $\mathfrak{o}$-изоморфны. Если мы применим теорему Крулля-Шмидта, то получим из этого специального случая следующую теорему:

Теорема 33. *Предположим, что* $\mathfrak{R}$ *и* $\bar{\mathfrak{R}}$ *являются* $\Phi[t, S]$*-модулями, содержащими лишь элементы конеч-*

ного порядка, причем в них нет элементов порядка $t\Phi[t, S]$. *Тогда для того, чтобы модули* $\mathfrak{R}$ *и* $\bar{\mathfrak{R}}$ *были* $\Phi[t, S]$*-изоморфны, необходимо и достаточно, чтобы они были* $\Gamma_0[u]$*-изоморфны.*

Следствие. *При предположениях теоремы, модули* $\mathfrak{R}$ *и* $\bar{\mathfrak{R}}$ $\Phi[t, S]$*-изоморфны тогда и только тогда, когда они* $\Phi[u]$*-изоморфны.*

Пусть теперь T является полулинейным преобразованием в $\mathfrak{R}$ над Φ, где Φ и S имеют прежний смысл. Условие отсутствия в $\mathfrak{R}$ векторов порядка $t\Phi[t, S]$ совпадает с предположением, что преобразование T взаимнооднозначно. Наши результаты дают поэтому условия для подобия двух взаимнооднозначных преобразований T_1 и T_2, обладающих одним и тем же автоморфизмом S. Таким образом, следствие устанавливает, что преобразования T_1 и T_2 подобны тогда и только тогда, когда линейные преобразования $U_1 = T_1{}^r\mu^{-1}$ и $U_2 = T_2{}^r\mu^{-1}$ подобны. Если мы вспомним о связи преобразований и матриц, то получим теорему:

Теорема 34. *Пусть* Φ *такое тело, что* $(\Phi : \Gamma) = m < \infty$, *где через* Γ *обозначен центр тела, и пусть* S *такой автоморфизм в* Φ, *что* $\xi^{S^r} = \mu^{-1}\xi\mu$, $0 < r < \infty$, $\mu^S = \mu$ *и ни одна меньшая степень* S *не является внутренним автоморфизмом. Если* (τ_1) *и* (τ_2) *являются невырождающимися (т. е. обратимыми) матрицами в* Φ_n, *то для того, чтобы существовала такая невырождающаяся матрица* (β), *что* $(\tau_2) = (\beta)^{-1}(\tau_1)(\beta^S)$, *необходимо и достаточно, чтобы матрицы* $N(\tau_1)\mu^{-1} = (\tau_1)(\tau_1^S)\ldots(\tau_1^{S^{r-1}})\mu^{-1}$ *и* $N(\tau_2)\mu^{-1}$ *были подобны в обычном смысле слова.*

Другой интересный случай приведенной выше теоремы мы получим, если положим $r = 1$ и $\mu = 1$: два линейных преобразования модуля $\mathfrak{R}$ над телом Φ подобны тогда и только тогда, когда они подобны, как преобразования модуля $\mathfrak{R}$ над центром Γ тела Φ. Как легко видеть, в этом случае нет необходимости предполагать, что преобразования T_1 и T_2 взаимооднозначны.

Глава 4

СТРУКТУРА КОЛЕЦ ЭНДОМОРФИЗМОВ И АБСТРАКТНЫХ КОЛЕЦ

1. Общая проблема. Специальные случаи. Рассмотрим произвольную коммутативную группу $\mathfrak{M}$ и фиксированное множество Ω эндоморфизмов $\alpha, \beta, \ldots$, действующих в группе $\mathfrak{M}$. Пусть $\mathfrak{A}$ является множеством Ω-эндоморфизмов, т. е. эндоморфизмов, коммутирующих с каждым эндоморфизмом из множества Ω. $\mathfrak{A}$ есть содержащее тождественный эндоморфизм подкольцо кольца эндоморфизмов группы $\mathfrak{M}$. В этой главе мы наложим различные условия на структуру Ω-подгрупп группы $\mathfrak{M}$ и исследуем получающиеся от этого ограничения для кольца $\mathfrak{A}$. Эти результаты будут применены к изучению структуры абстрактных колец. Наконец, мы дадим некоторые приложения к теории проективных представлений групп и к теории Галуа тел.

Примеры. 1) $\mathfrak{M}$ — конечная коммутативная группа; множество Ω пусто.

2) $\mathfrak{M}$ — векторное пространство над телом $\Omega = \Phi$. Здесь $\mathfrak{A}$ — кольцо линейных преобразований. Мы видели, что $\mathfrak{A} = \Phi_n'$, где Φ' обратно изоморфно телу Φ, или $\mathfrak{A}$ обратно изоморфно кольцу Φ_n. Напомним, что $\mathfrak{A}$ — простое кольцо.

3) $\mathfrak{M}$ — векторное пространство над телом Φ, и Ω — теоретико-множественная сумма Φ и некоторого множества преобразований $T_1, T_2, \ldots$. В этом случае $\mathfrak{A}$ состоит из всех коммутирующих с $T_1, T_2, \ldots$ линейных преобразований. Отсюда следует, что, если $(\tau_1), (\tau_2), \ldots$; $S_1, S_2, \ldots$

являются соответственно матрицами преобразований T_1, T_2, ... относительно некоторого фиксированного базиса и их автоморфизмами, то $\mathfrak{A}$ обратно изоморфно подкольцу кольца Φ_n, состоящему из таких матриц (α), что $(\alpha)(\tau_i) = (\tau_i)(\alpha^{\sigma_i})$.

Мы хотим показать, что любое кольцо $\mathfrak{A}$ с единицей можно рассматривать, как кольцо Ω-эндоморфизмов некоторой коммутативной группы $\mathfrak{M}$. В качестве группы $\mathfrak{M}$ выберем аддитивную группу кольца $\mathfrak{A}$. Мы видели, что правое умножение $x \to xa = xa_r$ является эндоморфизмом в $\mathfrak{M}$ и что совокупность этих эндоморфизмов образует подкольцо $\mathfrak{A}_r$ кольца эндоморфизмов группы $\mathfrak{M}$. Кольцо $\mathfrak{A}_r$ изоморфно кольцу $\mathfrak{A}$. Подобным же образом мы определили левое умножение a_l с помощью равенства $xa_l = ax$ и показали, что совокупность этих умножений образует кольцо $\mathfrak{A}_l$, обратно изоморфное кольцу $\mathfrak{A}$.

Из ассоциативного закона вытекает, что если $a_r \in \mathfrak{A}_r$ и $b_l \in \mathfrak{A}_l$, то $a_r b_l = b_l a_r$. С другой стороны, предположим, что B является однозначным преобразованием в группе $\mathfrak{M}$, коммутирующим со всеми a_r, и положим $1B = b$. Тогда $xB = (1x)B = (1B)x_r = bx_r = bx$. Таким образом $B = b_l$, и $\mathfrak{A}_l$ является множеством всех $\mathfrak{A}_r$-эндоморфизмов. Таким же образом $\mathfrak{A}_r$ есть множество $\mathfrak{A}_l$-эндоморфизмов. Изоморфизм между $\mathfrak{A}_r$ и $\mathfrak{A}$ позволит нам поэтому применить теорию колец Ω-эндоморфизмов к теории абстрактных колец. Сформулируем этот фундаментальный результат в следующей теореме.

Теорема 1. *Любое кольцо $\mathfrak{A}$ с единицей изоморфно кольцу $\mathfrak{A}_r$ своих правых умножений и обратно изоморфно кольцу $\mathfrak{A}_l$ своих левых умножений. $\mathfrak{A}_r$ является кольцом всех $\mathfrak{A}_l$-эндоморфизмов, действующих в аддитивной группе $\mathfrak{M}$ кольца $\mathfrak{A}$, а $\mathfrak{A}_l$ — кольцом $\mathfrak{A}_r$-эндоморфизмов группы $\mathfrak{M}$.*

$\mathfrak{A}_l$-($\mathfrak{A}_r$-) подгруппы аддитивной группы кольца $\mathfrak{A}$ являются его левыми (правыми) идеалами. ($\mathfrak{A}_l$, $\mathfrak{A}_r$)-подгруппы являются двусторонними идеалами. Отметим также, что $\mathfrak{A}_r \cap \mathfrak{A}_l$ состоит из эндоморфизмов $c_r = c_l$, где c входит в центр $\mathfrak{C}$ кольца $\mathfrak{A}$. В самом деле, если $a_r = b_l$, то $1a_r = 1b_l$ и $a = b$. Тогда при всех x имеем $ax = xa$, и потому $a = c \in \mathfrak{C}$.

2. Алгебры над полем. Таким же образом наши результаты применяются к теории алгебр (гиперкомплексных систем). Алгебра определяется следующим образом: пусть Φ является некоторым абстрактным полем; множество $\mathfrak{A}$ называется *алгеброй* над полем Φ, если

1. $\mathfrak{A}$ кольцо.

2. Аддитивная группа кольца $\mathfrak{A}$ представляет собою Φ-модуль, причем для всех $x \in \mathfrak{A}$ имеем $x1 = x$, где через 1 обозначена единица поля Φ.

3. $a_r\alpha = \alpha a_r$, $a_l\alpha = \alpha a_l$ для всех $a \in \mathfrak{A}$ и $\alpha \in \Phi$.

Последнее условие может быть также записано в таком виде: для всех $a, b \in \mathfrak{A}$ и $\alpha \in \Phi$ имеем $(ab)\alpha = (a\alpha)b = a(b\alpha)$. Так как Φ является полем, то кольцо эндоморфизмов, соответствующих элементам этого поля, изоморфно полю Φ. Следовательно, если мы хотим изучать некоторую алгебру, то мы можем принять точку зрения главы 2 и рассматривать в качестве основного понятия не абстрактное поле, а множество эндоморфизмов. В настоящей главе мы будем придерживаться этой точки зрения. Свойства, Φ, как поля, не будут играть никакой роли. Таким образом, мы можем изучать кольцо $\mathfrak{A}$ относительно произвольного множества Φ эндоморфизмов $\alpha, \beta, \ldots$, которые коммутируют как с левыми, так и с правыми умножениями. Если мы предположим, что множество Φ пусто, то получим обычные кольца; если же предположить, что Φ является полем, то получаются алгебры над этим полем. $\mathfrak{A}$ будет называться Φ-*кольцом*. Мы будем также изучать Φ-подкольца и Φ-идеалы кольца $\mathfrak{A}$.

Если кольцо $\mathfrak{A}$ обладает единицей 1, то $x\alpha = x(1\alpha) = (1\alpha)x$, и потому эндоморфизм α является как правым, так и левым умножением на элемент α. Отсюда следует, что элемент 1α лежит в центре кольца $\mathfrak{A}$. Любой идеал кольца $\mathfrak{A}$ является поэтому Φ-идеалом. Следовательно, в формулировках многих важных структурных теорем мы можем, не теряя общности, опускать упоминание о множестве операторов Φ.

Если мы хотим сравнивать две различные алгебры $\mathfrak{A}_1$ и $\mathfrak{A}_2$, то естественно предполагать, что поле Φ является одним и тем же для обеих алгебр. Таким образом, мы будем называть алгебры $\mathfrak{A}_1$ и $\mathfrak{A}_2$ *изоморфными*, если между ними существует взаимнооднозначное соответствие $a_1 \to a_2$, являющееся одновременно изоморфизмом колец $\mathfrak{A}_1$ и $\mathfrak{A}_2$ и Φ-изоморфизмом из аддитивных групп: если $a_1 \to a_2$ и $b_1 \to b_2$, то

$$a_1 + b_1 \to a_2 + b_2,\ a_1\alpha \to a_2\alpha,\ a_1 b_1 \to a_2 b_2.$$

Это соответствие называется *изоморфизмом*. Аналогично определяются *гомоморфизмы*, *автоморфизмы*, *обратные автоморфизмы* и т. д.

Рассмотрим теперь некоторые методы конструирования алгебр конечной размерности. Очевидно, что Φ_n является такой алгеброй, если определить $a\alpha$, как произведение a на диагональную матрицу $\{\alpha, \ldots, \alpha\}$. Кольцо $\mathfrak{L}$ линейных преобразований n-мерного векторного пространства $\mathfrak{M}$ над Φ также является алгеброй, если определить $A\alpha$, как произведение A на скалярное умножение α. Как мы видели, если $x_1, \ldots, x_n$ образуют базис пространства $\mathfrak{M}$ над Φ и $x_i A = \sum x_j \alpha_{ji}$, то соответствие между A и матрицей (α_{ij}) будет обратным изоморфизмом между алгебрами $\mathfrak{L}$ и Φ_n. Пусть теперь $\mathfrak{A}$ — произвольная алгебра. Тогда умножения $x \to xa$ и $x \to ax$ будут линейными преобразованиями в алгебре $\mathfrak{A}$, рассматриваемой, как векторное пространство над Φ. Так как $x(a\alpha) = (xa)\alpha$, и $(a\alpha)x = (ax)\alpha$, то $(a\alpha)_r = a_r\alpha$ и $(a\alpha)_l = a_l\alpha$. Из этих равенств следует, что, если $\mathfrak{A}$ обладает единицей, то соответствие $a \to a_r$ является изоморфизмом между алгеброй $\mathfrak{A}$ и подалгеброй $\mathfrak{A}_r$ алгебры $\mathfrak{L}$. Если мы скомбинируем это соответствие с одним из обратных изоморфизмов между $\mathfrak{L}$ и Φ_n, то получим обратный изоморфизм между $\mathfrak{A}$ и подалгеброй алгебры Φ_n. Подобным же образом, комбинируя соответствие $a \to a_l$ с одним из обратных изоморфизмов между $\mathfrak{L}$ и Φ_n, мы получаем изоморфизм между $\mathfrak{A}$ и подалгеброй алгебры Φ_n. Более точно, пусть $x_1, \ldots, x_n$ — базис алгебры $\mathfrak{A}$ над Φ, и пусть $x_i a = \sum x_j \rho_{ji}(a)$ и $ax_i = \sum x_j \lambda_{ji}(a)$. Тогда, если обозначить $(\rho_{ij}(a))$ через $R(a)$ и $(\lambda_{ji}(a))$ — через $L(a)$, то соответствие $a \to R(a)$ представляет собою обратный изоморфизм, а соответствие $a \to L(a)$ — изоморфизм между $\mathfrak{A}$ и подалгебрами алгебры Φ_n. Следует отметить, что мы можем также комбинировать обратный изоморфизм $a \to R(a)$ с обратным изоморфизмом $(\alpha) \to (\alpha)'$, где через $(\alpha)'$ обозначена транспонированная матрица (α), и получить второй изоморфизм между $\mathfrak{A}$ и подалгеброй алгебры Φ_n.

Если в $\mathfrak{A}$ отсутствует единица, то мы образуем векторное пространство $\mathfrak{B} = \mathfrak{A} + (x_0)$ и определим

$$(x_0\alpha + a)(x_0\beta + b) = x_0(\alpha\beta) + a\beta + b\alpha + ab,$$

где $a, b \in \mathfrak{A}$.

Тогда $\mathfrak{B}$ будет алгеброй с единицей x_0, и $\mathfrak{A}$ содержится в $\mathfrak{B}$ в качестве подалгебры. Следовательно, $\mathfrak{B}$, и тем более $\mathfrak{A}$, изоморфна некоторой алгебре матриц. Таким образом нами доказана

Теорема 2. *Любая алгебра с конечным базисом изоморфна подалгебре матричной алгебры.*

Эта теорема дает общий метод для получения алгебр конечной размерности. Существует также второй общий метод. Пусть $\mathfrak{A}$ — векторное пространство над Φ с базисом $x_1, \ldots, x_n$. Выберем в Φ n^3 элементов γ_{ijk} и положим $x_i x_j = \sum_a x_a \gamma_{aij}$. Для того, чтобы это определение приводило к ассоциативной алгебре, необходимо, чтобы для элементов γ_{ijk} было выполнено условие $\sum_a \gamma_{lak}\gamma_{aij} = \sum_a \gamma_{lia}\gamma_{ajk}$. Тогда, если мы определим $\left(\sum x_i\xi_i\right)\left(\sum x_j\eta_j\right) = \sum x_a\gamma_{aij}\xi_i\eta_j$, то получим $(x_i x_j)x_k = x_i(x_j x_k)$ и, следовательно, для всех x, y, z имеем $(xy)z = x(yz)$. Очевидно, что $(xy)\alpha = (x\alpha)y = x(y\alpha)$ и что выполнен дистрибутивный закон. Следовательно, $\mathfrak{A}$ — алгебра.

Примеры. 1) В качестве базиса выберем элементы x_1, x_2, x_3, x_4, положив

$$x_1x_i = x_i = x_ix_1,\ x_2^2 = 1\alpha,$$
$$x_3^2 = 1\beta,\ x_4^2 = -1\alpha\beta,\ x_2x_3 = -x_3x_2 = x_4,$$
$$x_3x_4 = -x_4x_3 = -x_2\beta,\ x_4x_2 = -x_2x_4 = -x_3\alpha.$$

2) Пусть $\mathfrak{G}$ — конечная группа с элементами $1, s, \ldots, u$. Поставим их во взаимнооднозначное соответствие с элементами базиса некоторого векторного пространства и обозначим вектор, соответствующий элементу s, через x_s. Тогда, если мы положим $x_sx_t = x_{st}$, то условие ассоциативности будет выполнено. Следовательно, мы получаем алгебру, которая называется *групповым кольцом* группы $\mathfrak{G}$ над Φ.

3) Пусть $\mathfrak{A}$ является фактор-алгеброй $\Phi[t]/(\nu(t))$, где $\Phi[t]$ — обычная область полиномов, и $(\nu(t))$ является главным идеалом, порожденным полиномом $\nu(t) = t^n - t^{n-1}\beta_1 - \ldots - \beta_n$. Тогда $\mathfrak{A}$ обладает базисом, состоящим из элементов 1, $x = \{t\}$, где $\{t\}$ обозначает смежный класс, содержащий t, и $x^2, \ldots, x^{n-1}$. Таблица умножения выводится из соотношения $x^n = x^{n-1}\beta_1 + \ldots + 1\beta_n$ и из ассоциативного закона.

3. Предварительные результаты. Перейдем теперь к рассмотрению общей проблемы, сформулированной в § 1: даны коммутативная группа $\mathfrak{M}$ и множество Ω ее эндоморфизмов; что можно сказать относительно структуры кольца $\mathfrak{A}$ всех Ω-эндоморфизмов группы $\mathfrak{M}$?

Мы видели, что если $\mathfrak{N}$ является Ω-подгруппой группы $\mathfrak{M}$ и $A \in \mathfrak{A}$, то $\mathfrak{N}A$ является некоторой Ω-подгруппой. Множество элементов, отображающихся в подгруппу $\mathfrak{N}$ при эндоморфизме A, также будет Ω-подгруппой. С прямым разложением группы $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, где $\mathfrak{M}_i$ — некоторые Ω-подгруппы, связано разложение

$$1 = E_1 + \ldots + E_u,\ E_iE_j = 0,\ \text{если } i \neq j,\ E_i^2 = E_i, \quad (1)$$

где E_i являются проекциями на $\mathfrak{M}_i$. Обратно, если даны такие эндоморфизмы E_i, для которых выполнены условия (1), то $\mathfrak{M} = \mathfrak{M}E_1 \oplus \ldots \oplus \mathfrak{M}E_u$. Ω-группа неразложима тогда и только тогда, когда 1 является примитивным идемпотентным элементом кольца $\mathfrak{A}$.

Под *вполне примарным кольцом* $\mathfrak{A}$ мы будем понимать кольцо, содержащее такой ниль-идеал $\mathfrak{R}$ (т. е. идеал, все элементы которого нильпотентны), что $\mathfrak{A}/\mathfrak{R}$ является телом. Если b — любой не лежащий в $\mathfrak{R}$ элемент, то найдется такое c, что $bc \equiv 1 \pmod{\mathfrak{R}}$, или $bc = 1 + z$, где $z \in \mathfrak{R}$. Если $z^m = 0$, то мы имеем $(1+z)(1 - z + z^2 - \ldots \pm z^{m-1}) = 1$, и, следовательно, элемент b обладает обратным элементом $c(1 - z + z^2 - \ldots)$. Таким образом, $\mathfrak{R}$ может быть определено как совокупность всех вырождающихся (необратимых) элементов кольца $\mathfrak{A}$, и потому $\mathfrak{R}$ определяется однозначно. Из леммы Фиттинга (глава 1, § 5) вытекает следующая

Теорема 3. *Если $\mathfrak{M}$ является неразложимой группой и удовлетворяет обоим условиям обрыва цепей, то кольцо $\mathfrak{A}$ ее Ω-эндоморфизмов вполне примарно.*

По лемме Фиттинга, любой элемент $A \in \mathfrak{A}$ либо является автоморфизмом, либо нильпотентен. Последний случай может иметь место либо когда $\mathfrak{M}A \subset \mathfrak{M}$, либо когда существует такой элемент $z \neq 0$, что $zA = 0$ (эти два условия эквивалентны). Пусть $\mathfrak{R}$ является совокупностью всех эндоморфизмов, не являющихся автоморфизмами. Если $B \in \mathfrak{R}$ и A — произвольный эндоморфизм, то AB и BA лежат в $\mathfrak{R}$. Предположим, что $B_1 + B_2 = A$ является автоморфизмом. Тогда $C_1 + C_2 = 1$, где $C_i = B_iA^{-1} \in \mathfrak{R}$. Так как эндоморфизм C_2 нильпотентен, то для некоторого r имеем $C_2^r = 0$, и, следовательно, $C_1(1 + C_2 + C_2^2 + \ldots + C_2^{r-1}) = 1 = (1 + C_2 + \ldots + C_2^{r-1})C_1$, и поэтому $C_1 \notin \mathfrak{R}$. Полученное противоречие показывает, что $\mathfrak{R}$ является идеалом. Если $A + \mathfrak{R}$ — смежный класс, не совпадающий с идеалом $\mathfrak{R}$, то A — автоморфизм и, следовательно, $(A + \mathfrak{R})(A^{-1} + \mathfrak{R}) = 1 + \mathfrak{R}$. Таким образом, $\mathfrak{A}/\mathfrak{R}$ является телом. Сюда относится также следующий важный результат:

Теорема 4. (Лемма Шура). *Если $\mathfrak{M}$ является неприводимой Ω-группой, то $\mathfrak{A}$ тело.*

Если $A \neq 0$ и $A \in \mathfrak{A}$, то $\mathfrak{M}A = \mathfrak{M}$, и множество таких элементов z, что $zA = 0$, состоит лишь из элемента 0. Таким образом, A является автоморфизмом и, следовательно, обладает в $\mathfrak{A}$ обратным элементом.

4. Кольца матриц.

Лемма. *Пусть $\mathfrak{A}$ будет произвольным кольцом с единицей и e_{ij}, $i,j = 1, \ldots, u$, — множеством элементов из $\mathfrak{A}$, удовлетворяющих соотношениям:*

$$1 = e_{11} + \ldots + e_{uu}, \quad e_{ij}\, e_{kl} = \delta_{jk} e_{il}. \tag{2}$$

Тогда $\mathfrak{A} = \mathfrak{B}_u$, где $\mathfrak{B}$ является подкольцом кольца $\mathfrak{A}$, состоящим из элементов, коммутирующих со всеми e_{ij}. Кольцо $\mathfrak{B}$ изоморфно кольцу $e_{ii}\mathfrak{A}e_{ii}$.

Если $a \in \mathfrak{A}$, то легко проверить, что $a_{ij} = \sum e_{pi} a e_{jp}$ лежит в $\mathfrak{B}$, и $a = \sum e_{ij} a_{ij}$. С другой стороны, если a_{ij} являются произвольными элементами из $\mathfrak{B}$ и $\sum e_{ij} a_{ij} = 0$, то $a_{ij} = \sum e_{pi} (\sum e_{ij} a_{ij}) e_{jp} = 0$. Следовательно, $\mathfrak{A} = \mathfrak{B}_u$. Если $a = \sum e_{ij} a_{ij}$ является произвольным элементом из $\mathfrak{A}$, то $e_{ii} a e_{ii} = e_{ii} a_{ii}$. Соответствие между $e_{ii} a e_{ii}$ и $a_{ii} \in \mathfrak{B}$ будет изоморфизмом.

Лемма. *Если $\mathfrak{M} = \mathfrak{M}_1 \oplus \mathfrak{M}_2$ и $1 = E_1 + E_2$, где E_i — проекция $\mathfrak{M}$ на $\mathfrak{M}_i$, то кольцо $\mathfrak{A}_1$ Ω-эндоморфизмов группы $\mathfrak{M}_1$ изоморфно $E_1 \mathfrak{A} E_1$, где $\mathfrak{A}$ — кольцо Ω-эндоморфизмов группы $\mathfrak{M}$.*

Если $A \in \mathfrak{A}$, то $E_1 A E_1$ индуцирует Ω-эндоморфизм B в группе $\mathfrak{M}_1$ и отображает $\mathfrak{M}_2$ в 0. Следовательно, если $B = 0$, то $E_1 A E_1 = 0$, и соответствие между $E_1 A E_1$ и B будет изоморфизмом между $E_1 \mathfrak{A} E_1$ и подкольцом $\overline{\mathfrak{A}}_1$ кольца $\mathfrak{A}_1$. С другой стороны, если $B \in \mathfrak{A}_1$, то $E_1 B E_1 = E_1 B$ является элементом $E_1 (E_1 B E_1) E_1$ из $E_1 \mathfrak{A} E_1$, индуцирующим в $\mathfrak{M}_1$ эндоморфизм B. Следовательно, $\overline{\mathfrak{A}}_1 = \mathfrak{A}_1$.

Теорема 5. *Если $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, где подгруппы $\mathfrak{M}_i$ Ω-изоморфны, то $\mathfrak{A} = \mathfrak{B}_u$, где $\mathfrak{B}$ изоморфно кольцу Ω-эндоморфизмов одной из подгрупп $\mathfrak{M}_i$.*

Пусть E_i является проекцией, определенной этим разложением, а B_{1i} — фиксированным Ω-изоморфизмом между

$\mathfrak{M}_1$ и $\mathfrak{M}_i$, $i \neq 1$. Положим $E_{ii} = E_i$, $E_{1i} = E_{11} B_{1i} E_{ii}$, $E_{i1} = E_{ii} B_{1i}^{-1} E_{11}$ и $E_{ij} = E_{i1} E_{1j}$ при $i \neq j$, $i \neq 1$, $j \neq 1$. Тогда легко проверить, что $E_{ij} E_{kl} = \delta_{jk} E_{il}$ при всех i, k, l. Поэтому наша теорема является непосредственным следствием предыдущих лемм.

5. Вполне приводимые группы. Предположим, что $\mathfrak{M}$ является вполне приводимой Ω-группой, удовлетворяющей одному (и тем самым обоим) условию обрыва цепей. Тогда $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, где подгруппы $\mathfrak{M}_i$ неприводимы. Перенумеруем эти подгруппы так, чтобы $\mathfrak{M}_1, \ldots, \mathfrak{M}_{n_1}$ были Ω-изоморфны, $\mathfrak{M}_{n_1+1}, \ldots, \mathfrak{M}_{n_1+n_2}$ были Ω-изоморфны между собой, но не Ω-изоморфны $\mathfrak{M}_1$ и т. д.

Если теперь $\mathfrak{N}_1$ и $\mathfrak{N}_2$ — произвольные неприводимые Ω-подгруппы группы $\mathfrak{M}$ и B является Ω-гомоморфным отображением $\mathfrak{N}_1$ на некоторую подгруппу группы $\mathfrak{N}_2$, то очевидно, что либо $B = 0$, либо B является Ω-изоморфизмом между $\mathfrak{N}_1$ и всей подгруппой $\mathfrak{N}_2$. Если $1 = E_1 + E_2 + \ldots + E_u$ является разложением 1 на проекции, соответствующие разложению $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, и A является любым Ω-эндоморфизмом, то $E_i A E_j$ индуцирует Ω-гомоморфное отображение $\mathfrak{M}_i$ на некоторую подгруппу, лежащую в $\mathfrak{M}_j$. Следовательно, если i пробегает значения $n_1 + \ldots + n_{p-1} + 1, \ldots, n_1 + \ldots + n_p$ и j пробегает значения $n_1 + \ldots + n_{q-1} + 1, \ldots, n_1 + \ldots + n_q$, причем $p \neq q$, то $E_i A E_j$ отображает подгруппу $\mathfrak{M}_1$ в 0. Так как $E_i A E_j$ отображает и все остальные подгруппы $\mathfrak{M}_k$ в 0, то мы получаем $E_i A E_j = 0$. Таким образом, если мы положим $E^{(1)} = E_1 + \ldots + E_{n_1}$, $E^{(2)} = E_{n_1+1} + \ldots + E_{n_1+n_2}, \ldots$, $E^{(t)} = E_{n_1 + \ldots + n_{t-1}+1} + \ldots + E_{n_1 + \ldots + n_t}$, то получим $A = \sum E_i A E_j = E^{(1)} A E^{(1)} + \ldots + E^{(t)} A E^{(t)}$. Так как $(E^{(p)} A E^{(p)})(E^{(q)} B E^{(q)}) = 0$ при $p \neq q$, то $E^{(p)} \mathfrak{A} E^{(p)}$ является двусторонним идеалом в кольце $\mathfrak{A}$ и последнее является прямой суммой таких идеалов. Мы видели, что кольцо $E^{(p)} \mathfrak{A} E^{(p)}$ изоморфно кольцу $\mathfrak{A}_p$ Ω-эндоморфизмов группы $\mathfrak{M} E^{(p)}$. Так как неразложимые части $\mathfrak{M} E^{(p)}$ неприводимы и Ω-изоморфны, то, по предыдущей теореме и по лемме Шура, $\mathfrak{A}_p = \Phi_{n_p}^{(p)}$, где $\Phi_{n_p}^{(p)}$ является кольцом

матриц над телом $\Phi^{(p)}$, изоморфным кольцу Ω-эндоморфизмов группы $\mathfrak{M}_{n_1+\cdots+n_{p-1}+1}$.

Теорема 6. *Кольцо Ω-эндоморфизмов вполне приводимой группы, удовлетворяющей условию обрыва возрастающих (убывающих) цепей, является прямой суммой своих двусторонних идеалов, каждый из которых изоморфен кольцу матриц над некоторым телом.*

6. Нильпотентные эндоморфизмы. Предположим, что $\mathfrak{M}$ является Ω-группой, для которой выполнены оба условия обрыва цепей, а $\mathfrak{B}$ — замкнутым относительно умножения множеством нильпотентных Ω-эндоморфизмов. Мы хотим доказать следующую теорему.

Теорема 7. *Если s является длиной композиционного ряда группы $\mathfrak{M}$, и $B_1, \ldots, B_s$ лежат в $\mathfrak{B}$, то* $B_s \ldots B_1 = 0$.

Пусть $\mathfrak{N}$ является такой Ω-подгруппой, что $\mathfrak{N}B_i \subseteq \mathfrak{N}$, и предположим, что $\mathfrak{N}B_s \ldots B_1 \neq 0$.

Так как $\mathfrak{N} \supseteq \mathfrak{N}B_i \supseteq \mathfrak{N}B_jB_i \supseteq \ldots$ и каждое $\mathfrak{N}B_s \ldots B_1$ является Ω-подгруппой, то мы получаем следующую убывающую цепь Ω-подгрупп:

$$\mathfrak{N} \supseteq \Sigma\mathfrak{N}B_i \supseteq \Sigma\mathfrak{N}B_iB_j \supseteq \ldots$$

Если между двумя членами этой цепи стоит знак равенства, то то же самое имеет место для всех последующих членов. Так как $\mathfrak{N}$ имеет длину $\leqslant s$ и $\mathfrak{N}B_s \ldots B_1 \neq 0$, то знак равенства должен иметь место между подгруппами $\Sigma\mathfrak{N}B_{i_1} \ldots B_{i_r} \equiv \mathfrak{N}'$ и $\Sigma\mathfrak{N}B_{i_1} \ldots B_{i_{r+1}}$ при $r < s$. Так как $\mathfrak{N}B_s \ldots B_1 \neq 0$, то $\mathfrak{N}' \neq 0$ и $\mathfrak{N}' = \sum\mathfrak{N}'B_j = \ldots$. Тогда существует такая бесконечная последовательность эндоморфизмов $B_{i_1}, B_{i_2}, \ldots$, что $\mathfrak{N}'B_{i_p} \ldots B_{i_1} \neq 0$. В самом деле, предположим, что уже найдены такие p членов $B_{i_1}, \ldots, B_{i_p}$ этой последовательности, что $\mathfrak{N}'B_{i_p} \ldots B_{i_1} \neq 0$. Тогда $\mathfrak{N}'B_{i_p} \ldots B_{i_1} = \mathfrak{N}'B_1B_{i_p} \ldots B_{i_1} + \ldots + \mathfrak{N}'B_sB_{i_p} \ldots B_{i_1}$, и так как $\mathfrak{N}'B_{i_p} \ldots B_{i_1} \neq 0$, то найдется такое i_{p+1}, что $\mathfrak{N}'B_{i_{p+1}} \ldots$

$\ldots B_{i_1} \neq 0$. Пусть k будет одним из индексов, бесконечное число раз встречающихся в последовательности $B_{i_1}, B_{i_2}, \ldots$ Опуская достаточное число членов, мы можем предположить, что $i_1 = k$. Таким образом, существует s таких эндоморфизмов $C_1, \ldots, C_s \in \mathfrak{B}$, где $C_i = B_i'B_k$ и B_i' являются произведениями эндоморфизмов B_j, что $\mathfrak{N}'C_s \ldots C_1 \neq 0$. Так как эндоморфизм B_k нильпотентен, то $\mathfrak{N}'B_k \subset \mathfrak{N}'$, и, так как $\Sigma\mathfrak{N}'C_i \subseteq \mathfrak{N}'B_k$, то $\Sigma\mathfrak{N}'C_i \subset \mathfrak{N}'$. В силу сказанного в первой части доказательства, мы можем найти такую Ω-подгруппу $\overline{\mathfrak{N}}$, причем $\overline{\mathfrak{N}} \neq 0$ и $\overline{\mathfrak{N}} \subset \mathfrak{N}' \subset \mathfrak{N}$, что $\overline{\mathfrak{N}} = \sum\overline{\mathfrak{N}}C_i$. Если мы повторим это рассуждение, то получим такую подгруппу $\overline{\overline{\mathfrak{N}}}$, отличную от нуля и содержащуюся внутри $\overline{\mathfrak{N}}$, и такие эндоморфизмы D_i из $\mathfrak{B}$, что $\overline{\overline{\mathfrak{N}}} = \sum\overline{\overline{\mathfrak{N}}}D_i$. Таким образом, этот процесс приводит к бесконечной убывающей цепи Ω-подгрупп, и, следовательно, предположение, что $\mathfrak{N}B_s \ldots \ldots B_1 \neq 0$, неприемлемо. Если мы применим это к $\mathfrak{N} = \mathfrak{M}$, то получим, что $B_s \ldots B_1 = 0$.

В качестве первого следствия этого результата отметим, что в случае неразложимости группы $\mathfrak{M}$, удовлетворяющей обоим условиям обрыва цепей, множество $\mathfrak{R}$ всех невзаимнооднозначных Ω-эндоморфизмов является нильпотентным идеалом: имеет место $\mathfrak{R}^s = 0$, где s является длиной группы $\mathfrak{M}$.

7. Радикал кольца эндоморфизмов. В этом и следующем параграфах сохраняется предположение об обрыве возрастающих и убывающих цепей в группе $\mathfrak{M}$. Пусть $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, где подгруппы $\mathfrak{M}_i$ отличны от нуля и неразложимы; пусть, далее, $1 = E_1 + \ldots + E_u$, где E_i являются проекциями на подгруппы $\mathfrak{M}_i$. Любой эндоморфизм A из $\mathfrak{A}$ может быть одним и только одним способом представлен в виде ΣA_{ij}, где A_{ij} лежит в $E_i\mathfrak{A}E_j$. Эндоморфизм A_{ij} отображает каждую подгруппу $\mathfrak{M}_k$, $k \neq i$, в 0 и индуцирует Ω-гомоморфное отображение $\mathfrak{M}_i$ на некоторую Ω-подгруппу, лежащую в $\mathfrak{M}_j$.

Пусть $\mathfrak{R}$ обозначает множество эндоморфизмов вида $B = \Sigma B_{ij}$, где ни одно из B_{ij} не индуцирует Ω-изомор-

физма между $\mathfrak{M}_i$ и $\mathfrak{M}_j$. Таким образом, либо в $\mathfrak{M}_i$ существуют такие элементы $z_i \neq 0$, что $z_i B_{ij} = 0$, либо $\mathfrak{M}_i B_{ij} \subset \mathfrak{M}_j$. Мы хотим показать, что $\mathfrak{N}$ является нильпотентным идеалом. Если $j \neq k$, то, так как $E_j E_k = 0$, мы будем иметь $A_{ij}B_{kl} = 0$ и $B_{ij}A_{kl} = 0$. Если $z_i B_{ij} = 0$, то $z_i B_{ij} A_{jl} = 0$. Предположим теперь, что $\mathfrak{M}_j \neq \neq \mathfrak{M}_i B_{ij} \equiv \mathfrak{M}_j'$, но что $B_{ij}A_{jl}$ индуцирует Ω-изоморфизм между $\mathfrak{M}_i$ и $\mathfrak{M}_l$. Тогда A_{jl} индуцирует Ω-изоморфизм между $\mathfrak{M}_j'$ и $\mathfrak{M}_l$. Отсюда следует, что $\mathfrak{M}_j = \mathfrak{M}_j' \oplus \mathfrak{M}_j''$, где $\mathfrak{M}_j''$ является подмножеством в $\mathfrak{M}_j$, отображающимся в 0 при эндоморфизме A_{jl}[1]). Но это противоречит предположению о неразложимости группы $\mathfrak{M}_j$. Таким образом, мы получили, что если $B_{ij} \in \mathfrak{N}$ и A является произвольным Ω-эндоморфизмом, то $B_{ij}A \in \mathfrak{N}$. Кроме того, если $A_{ki}B_{ij}$ индуцирует Ω-изоморфизм между $\mathfrak{M}_k$ и $\mathfrak{M}_j$, то A_{ki} индуцирует Ω-изоморфизм между $\mathfrak{M}_k$ и $\mathfrak{M}_i$ и, следовательно, B_{ij} индуцирует Ω-изоморфизм между $\mathfrak{M}_i$ и $\mathfrak{M}_j$, вопреки сделанному предположению. Таким образом, $AB_{ij} \in \mathfrak{N}$.

Пусть теперь B_{ij}, $C_{ij} \in \mathfrak{N}$. Рассмотрим эндоморфизм $A_{ij} = B_{ij} + C_{ij}$. Если A_{ij} индуцирует Ω-изоморфизм $\bar{A}_{ij}$ между $\mathfrak{M}_i$ и $\mathfrak{M}_j$, то положим $A_{ji} = E_j \bar{A}_{ij}^{-1} E_i$. Тогда $E_i = B_{ij}A_{ji} + C_{ij}A_{ji}$, причем эндоморфизмы $B_{ij}A_{ji}$ и $C_{ij}A_{ji}$ не будут автоморфизмами в $\mathfrak{M}_i$. Так как подгруппа $\mathfrak{M}_i$ неразложима, то это невозможно, и потому $A_{ij} \in \mathfrak{N}$. Если мы сопоставим эти результаты, то получим, что $\mathfrak{N}$ является двусторонним идеалом в кольце $\mathfrak{A}$.

Если $B \in \mathfrak{N}$, то рассмотрим такое разложение $\mathfrak{M} = \mathfrak{M}' \oplus \mathfrak{M}''$, что B является нильпотентным эндоморфизмом в $\mathfrak{M}'$ и автоморфизмом в $\mathfrak{M}''$ (лемма Фиттинга). По теореме Крулля-Шмидта существует такой Ω-автоморфизм U, что $\mathfrak{M}'U = \mathfrak{M}^*$, $\mathfrak{M}''U = \mathfrak{M}^{**}$, где, при соответствующем упорядочивании подгрупп $\mathfrak{M}_i$, $\mathfrak{M}^* = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_t$, $\mathfrak{M}^{**} = \mathfrak{M}_{t+1} \oplus \ldots \oplus \mathfrak{M}_u$. Таким образом $U^{-1}BU = C$ лежит в $\mathfrak{N}$, и этот эндоморфизм индуцирует в $\mathfrak{M}^{**}$ автоморфизм $\bar{C}$. Следовательно, если $E^{**} = E_{t+1} + \ldots + E_u$, то $E^{**}CE^{**}\bar{C}^{-1}E^{**} = E^{**}$ лежит в $\mathfrak{N}$, что невозможно, так как при $t \neq u$ E_{t+1}, E_{t+2}, ... лежат в $E_{t+1}\mathfrak{A}E_{t+1}$, ... Таким образом, $\mathfrak{M}^{**} = 0 = \mathfrak{M}''$, и потому эндоморфизм B нильпотентен. Так как каждый элемент из $\mathfrak{N}$ нильпотентен, то по теореме, доказанной в предыдущем параграфе, идеал $\mathfrak{N}$ нильпотентен. Если теперь $\mathfrak{N}$ является произвольным нильпотентным двусторонним идеалом в $\mathfrak{A}$ и $N = \sum N_{ij}$ лежит в $\mathfrak{N}$, то и каждый эндоморфизм $N_{ij} = E_i N E_j$ лежит в $\mathfrak{N}$. Отсюда следует, что N_{ij} лежит в $\mathfrak{N}$, так как в противном случае мы могли бы показать с помощью соответствующего умножения, что $E_j \in \mathfrak{N}$. Следовательно, $\mathfrak{N} \subseteq \mathfrak{N}$.

[1]) См. доказательство теоремы Крулля-Шмидта, глава 1.

Теорема 8. *Пусть $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$ является разложением удовлетворяющей обоим условиям обрыва цепей Ω-группы $\mathfrak{M}$ на неразложимые отличные от нуля подгруппы $\mathfrak{M}_i$ и пусть E_i являются соответствующими проекциями. Тогда множество эндоморфизмов вида ΣB_{ij}, где $B_{ij} \in E_i \mathfrak{A} E_j$, и B_j не является взаимнооднозначным отображением $\mathfrak{M}_i$ на $\mathfrak{M}_j$, будет нильпотентным двусторонним идеалом $\mathfrak{N}$ в кольце $\mathfrak{A}$ всех Ω-эндоморфизмов. $\mathfrak{N}$ содержит каждый нильпотентный двусторонний идеал кольца $\mathfrak{A}$.*

Идеал $\mathfrak{N}$ называется *радикалом* кольца $\mathfrak{A}$.

8. Структура кольца эндоморфизмов произвольной группы. Упорядочим компоненты $\mathfrak{M}_i$ таким образом, чтобы $\mathfrak{M}_1, \ldots, \mathfrak{M}_{n_1}$ были Ω-изоморфны, $\mathfrak{M}_{n_1+1}, \ldots, \mathfrak{M}_{n_1+n_2}$ были Ω-изоморфны между собой, но не Ω-изоморфны $\mathfrak{M}_1$ и т. д. Положим:

$$\mathfrak{M}^{(1)} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_{n_1}, \quad \mathfrak{M}^{(2)} = \mathfrak{M}_{n_1+1} \oplus \ldots \oplus \mathfrak{M}_{n_1+n_2}, \ldots$$

$$E^{(1)} = E_1 + \ldots + E_{n_1}, \quad E^{(2)} = E_{n_1+1} + \ldots + E_{n_1+n_2}, \ldots$$

Тогда $\mathfrak{M} = \mathfrak{M}^{(1)} \oplus \ldots \oplus \mathfrak{M}^{(q)}$. Если i и j принадлежат различным последовательностям $n_1 + \ldots + n_{p-1} + 1, \ldots, n_1 + \ldots + n_p$ и $n_1 + \ldots + n_{q-1} + 1, \ldots, n_1 + \ldots + n_q$, то $E_i \mathfrak{A} E_j$ входит в радикал $\mathfrak{N}$. Следовательно, $E^{(p)}\mathfrak{A}E^{(q)} \subseteq \mathfrak{N}$

при $p \neq q$ и $E^{(p)}\mathfrak{A}E^{(p)} + \mathfrak{R}$ является двусторонним идеалом в кольце $\mathfrak{A}$, которому соответствует двусторонний идеал $\bar{\mathfrak{A}}_p$ в $\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{R}$. Так как $E^{(p)}\mathfrak{A}E^{p}$ содержит $E^{(p)}$, то $\bar{\mathfrak{A}}_p \neq 0$. Очевидно, что $\bar{\mathfrak{A}} = \bar{\mathfrak{A}}_1 \oplus \ldots \oplus \bar{\mathfrak{A}}_t$. Мы видели, что соответствие между $A_p \subset E^{(p)}\mathfrak{A}E^{(p)}$ и индуцированным им эндоморфизмом подгруппы $\mathfrak{M}^{(p)}$ является изоморфизмом между $E^{(p)}\mathfrak{A}E^{(p)}$ и кольцом Ω-эндоморфизмов группы $\mathfrak{M}^{(p)}$. Отсюда следует, что радикал кольца $E^{(p)}\mathfrak{A}E^{(p)}$ состоит из элементов $\sum B_{ij}$, где $i, j = n_1 + \ldots + n_{p-1} + 1, \ldots, n_1 + \ldots n_p$, и B_{ij} не является взаимно-однозначным соответствием между $\mathfrak{M}_i$ и $\mathfrak{M}_j$. Таким образом, радикалом кольца $E^{(p)}\mathfrak{A}E^{(p)}$ является $(E^{(p)}\mathfrak{A}E^{(p)} \cap \cap \mathfrak{R}) = E^{(p)}\mathfrak{R}E^{(p)}$ и $\bar{\mathfrak{A}}_p \cong E^{(p)}\mathfrak{A}E^{(p)}/E^{(p)}\mathfrak{R}E^{(p)}$ [1]).

Предположим теперь, что группа $\mathfrak{M}$ *однородна* в том смысле, что все ее неразложимые компоненты $\mathfrak{M}_i$ Ω-изоморфны. Мы видели, что $\mathfrak{A} = \mathfrak{B}_u$, где $\mathfrak{B}$ изоморфно кольцу Ω-эндоморфизмов подгруппы $\mathfrak{M}_i$. Мы видели также, что $\mathfrak{B}/\mathfrak{S}$ является телом, если $\mathfrak{S}$ обозначает радикал кольца $\mathfrak{B}$. Если $\mathfrak{R}$ обозначает радикал кольца $\mathfrak{A}$, то $\mathfrak{R} \cap \mathfrak{B}$ является нильпотентным двусторонним идеалом кольца $\mathfrak{B}$ и потому содержится в $\mathfrak{S}$. С другой стороны, если E_{ij} являются матричными единицами в $\mathfrak{A}$ и $S_{ij} \in \mathfrak{S}$, то множество элементов вида $\sum E_{ij}S_{ij}$ является нильпотентным идеалом кольца $\mathfrak{A}$ и, следовательно, содержится в $\mathfrak{R}$. В частности, $\sum E_{ii}S \in \mathfrak{R}$ и $\mathfrak{R} \cap \mathfrak{B} = \mathfrak{S}$. Если $B = \sum E_{ij}B_{ij}$ является произвольным элементом из $\mathfrak{R}$, то $B_{ij} = \sum E_{ki}BE_{jk}$ лежит в $\mathfrak{R} \cap \mathfrak{B} = \mathfrak{S}$. Таким образом, $\mathfrak{R} = \mathfrak{S}_u$ и фактор-кольцо $\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{R}$ изоморфно кольцу $(\mathfrak{B}/\mathfrak{S})_u$ матриц над телом. Так как кольца такого вида всегда будут простыми, то мы показали, что кольцо $\bar{\mathfrak{A}}$ просто. С другой стороны, мы видели, что $\bar{\mathfrak{A}} = \bar{\mathfrak{A}}_1 \oplus \ldots \oplus \bar{\mathfrak{A}}_t$, и потому, если кольцо $\bar{\mathfrak{A}}$ просто, то $t = 1$ и группа $\mathfrak{M}$ однородна. Таким образом, нами установлены следующие связи:

[1]) Мы применяем теорему об изоморфизме: если $\mathfrak{A} \supseteq \mathfrak{B}$ и $\mathfrak{N}$ является идеалом в $\mathfrak{A}$, то $(\mathfrak{B} + \mathfrak{N})/\mathfrak{N} \cong \mathfrak{B}/\mathfrak{B} \cap \mathfrak{N}$.

Группа $\mathfrak{M}$ однородна $\rightarrow$ $\mathfrak{A} = \mathfrak{B}_u$ и $\mathfrak{B}$ вполне примарно $\rightarrow$ кольцо $\mathfrak{A}/\mathfrak{R}$ просто $\rightarrow$ группа $\mathfrak{M}$ однородна. Следовательно, нами получена

Теорема 9. *Следующие условия эквивалентны между собой:*

1. *Группа* $\mathfrak{M}$ *однородна.*
2. $\mathfrak{A} = \mathfrak{B}_u$, *где* $\mathfrak{B}$ *вполне примарно.*
3. *Кольцо* $\mathfrak{A}/\mathfrak{R}$ *просто.*

Вопрос о единственности представления кольца $\mathfrak{A}$ в виде $\mathfrak{B}_u$ решается следующей теоремой.

Теорема 10. *Пусть выполнены условия предыдущей теоремы. Тогда, если* $\mathfrak{A} = \mathfrak{B}'_{u'}$, *где* $\mathfrak{B}'$ *вполне примарно, то* $u = u'$ *и* $\mathfrak{B} \cong \mathfrak{B}'$.

Пусть E'_{ij} является новым множеством матричных единиц. Так как $E'_{ii}\mathfrak{A}E'_{ii} \cong \mathfrak{B}'$, то E'_{ii} является единственным идемпотентным элементом в $E'_{ii}\mathfrak{A}E'_{ii}$. Следовательно, E'_{ii} является примитивным идемпотентным элементом и компоненты разложения $\mathfrak{M} = \mathfrak{M}E'_{11} \oplus \ldots \oplus \mathfrak{M}E'_{u'u'}$ неразложимы. По теореме Крулля-Шмидта $u = u'$, и существует такой Ω-автоморфизм A, что при соответствующем упорядочивании элементов E_{ii} и E'_{jj} имеем $A^{-1}E_{ii}A = E'_{i'i'}$.

Так как группа $\mathfrak{M}$ однородна, то существует такой Ω-автоморфизм P, что $\mathfrak{M}_i P = \mathfrak{M}_i$. Следовательно, если $B = PA$, то мы получаем $B^{-1}E_{ii}B = E'_{ii}$. Тогда эндоморфизм $B^{-1}E_{ij}B$ индуцирует Ω-изоморфизм между $\mathfrak{M}_i'$ и $\mathfrak{M}_j'$, и потому $\sum_1^u B^{-1}E_{j1}BE'_{1j}$, а также и $C = \sum E_{j1}BE'_{1j}$ являются Ω-автоморфизмами. Очевидно, что $E_{ij}C = CE'_{ij}$ и $E_{ij} = CE'_{ij}C^{-1}$. Так как $\mathfrak{B}$ и $\mathfrak{B}'$ являются соответственно множествами эндоморфизмов, коммутирующих с E_{ij} и E'_{ij}, то мы получаем, что $\mathfrak{B} = C\mathfrak{B}'C^{-1}$.

9. Прямые суммы. Рассмотрим теперь теорию абстрактных колец. Для того, чтобы включить в наши рассмотрения и случай алгебр, предположим, что $\mathfrak{A}$

является кольцом и Ф является множеством эндоморфизмов аддитивной группы кольца $\mathfrak{A}$, которые коммутируют с элементами из $\mathfrak{A}_r$ и из $\mathfrak{A}_l$. Начнем с некоторых элементарных замечаний относительно разложения кольца $\mathfrak{A}$ в прямую сумму Ф-идеалов. Первым из них будет специальный случай теоремы, связывающей прямые разложения и проекции, а именно:

Лемма. *Если $\mathfrak{A}$ является Ф-кольцом с единицей и $\mathfrak{A}=\mathfrak{J}_1\oplus\ldots\oplus\mathfrak{J}_u$ — прямое разложение кольца $\mathfrak{A}$ на левые Ф-идеалы, отличные от нуля, то $1=e_1+\ldots+e_u$, где $e_j^2=e_j\neq 0$, $e_je_k=0$ при $j\neq k$ и $\mathfrak{J}_j=\mathfrak{A}e_j$.*

Дадим прямое доказательство этой леммы. Пусть $1=e_1+\ldots+e_u$, где $e_j\in\mathfrak{J}_j$. Тогда любой элемент $a=ae_1+\ldots+ae_u$ и $ae_j\in\mathfrak{J}_j$. Если $a=a_j\in\mathfrak{J}_j$, то $a_j=a_je_1+\ldots+a_je_u$. Так как идеалы $\mathfrak{J}_j$ независимы, то все $a_je_k=0$ за исключением $a_je_j=a_j$. Следовательно, $\mathfrak{J}_j=\mathfrak{A}e_j$ и $e_j^2=e_j\neq 0$, $e_je_k=0$ при $j\neq k$.

Предположим теперь, что кольцо $\mathfrak{A}=\mathfrak{A}_1\oplus\ldots\oplus\mathfrak{A}_t$ является прямой суммой двусторонних Ф-идеалов. Если $j\neq k$, то $\mathfrak{A}_j\mathfrak{A}_k\subseteq\mathfrak{A}_j\cap\mathfrak{A}_k=0$. Следовательно, любой Ф-идеал (левый, правый или двусторонний) кольца $\mathfrak{A}_j$ является Ф-идеалом кольца $\mathfrak{A}$. С другой стороны, пусть $\mathfrak{J}$ является левым Ф-идеалом в $\mathfrak{A}$. Тогда $\mathfrak{J}_j=\mathfrak{A}_j\mathfrak{J}\subseteq\mathfrak{J}\cap\mathfrak{A}_j$ является левым идеалом в $\mathfrak{A}_j$. Так как

$$\mathfrak{J}=1\cdot\mathfrak{J}=\mathfrak{A}\mathfrak{J}=\mathfrak{J}_1\oplus\ldots\oplus\mathfrak{J}_t, \tag{3}$$

то $\mathfrak{J}\cap\mathfrak{A}_j\subseteq\mathfrak{J}_j$ и, следовательно, $\mathfrak{J}\cap\mathfrak{A}_j=\mathfrak{J}_j$. Разложение (3) показывает в частности, что $\mathfrak{J}$ удовлетворяет условию возрастающих (убывающих) цепей для одно- или двусторонних идеалов тогда и только тогда, когда эти условия выполнены в каждом из $\mathfrak{A}_j$.

Предположим, что $\mathfrak{A}_j$ являются неразложимыми двусторонними отличными от нуля Ф-идеалами, т. е. пусть $\mathfrak{A}_j=\mathfrak{A}_j'\oplus\mathfrak{A}_j''$ влечет за собой, что либо $\mathfrak{A}_j'$, либо $\mathfrak{A}_j''$ равен нулю. Тогда идеалы $\mathfrak{A}_j$ однозначно определены. В самом деле, если $\mathfrak{A}=\mathfrak{B}_1\oplus\ldots\oplus\mathfrak{B}_u$ является разложением $\mathfrak{A}$ на неразложимые отличные от нуля двусторонние

Ф-идеалы, то $\mathfrak{A}_i\cap\mathfrak{B}_j=0$ для всех j, кроме одного, так как $\mathfrak{A}_1=(\mathfrak{A}_1\cap\mathfrak{B}_1)\oplus\ldots\oplus(\mathfrak{A}_1\cap\mathfrak{B}_u)$; считая $j=1$, мы получим, что $\mathfrak{A}_1=\mathfrak{A}_1\cap\mathfrak{B}_1$ и, по симметрии, $\mathfrak{B}_1=\mathfrak{A}_1\cap\mathfrak{B}_1=\mathfrak{A}_1$. Подобным образом, при соответствующем упорядочивании, находим, что $\mathfrak{A}_2=\mathfrak{B}_2,\ldots$ и $t=u$.

Теорема 11. *Если $\mathfrak{A}$ является Ф-кольцом с единицей и $\mathfrak{A}=\mathfrak{A}_1\oplus\ldots\oplus\mathfrak{A}_t$ является разложением $\mathfrak{A}$ в прямую сумму неразложимых отличных от нуля двусторонних Ф-идеалов, то любое разложение $\mathfrak{A}$ в прямую сумму неразложимых отличных от нуля Ф-идеалов имеет те же компоненты, что и данное разложение.*

10. Радикал. Напомним, что *ниль-кольцом* называется кольцо, содержащее лишь нильпотентные элементы, и *нильпотентным кольцом* — кольцо, конечная степень которого равна нулю. Таким образом, утверждение, что кольцо $\mathfrak{A}$ нильпотентно, означает, что для некоторого числа s любое произведение $a_1a_2\ldots a_s$ равно нулю при произвольных $a_i\in\mathfrak{A}$. В частности, $a^s=0$ при всех a, и потому $\mathfrak{A}$ является ниль-кольцом. Замечательно, что утверждение, обратное этому почти тривиальному факту, имеет место, если в кольце $\mathfrak{A}$ выполнено условие обрыва убывающих цепей для Ф-идеалов. Прежде чем проводить доказательство, отметим следующие леммы.

Лемма 1. *Если $\mathfrak{J}_1$ и $\mathfrak{J}_2$ являются нильпотентными Ф-идеалами кольца $\mathfrak{A}$, то и идеал $\mathfrak{J}_1+\mathfrak{J}_2$ нильпотентен.*

Пусть $\mathfrak{J}_1^r=0$ и $\mathfrak{J}_2^s=0$. Имеем $(\mathfrak{J}_1+\mathfrak{J}_2)^k=\sum\mathfrak{J}_{i_1}\mathfrak{J}_{i_2}\ldots\mathfrak{J}_{i_k}$, где $i_j=1,2$. Если $k=r+s-1$, то каждое произведение содержит не менее r раз идеал $\mathfrak{J}_1$ или не менее s раз идеал $\mathfrak{J}_2$. В первом случае заменим любое $\mathfrak{J}_2\mathfrak{J}_1$ в произведении на $\mathfrak{J}_1$. После конечного числа таких замен мы получим $\mathfrak{J}_{i_1}\ldots\mathfrak{J}_{i_k}\subseteq\mathfrak{J}_1^r\mathfrak{J}_2^t=0$. Подобным же образом, если существует не менее s идеалов $\mathfrak{J}_2$, мы получаем $\mathfrak{J}_{i_1}\ldots\mathfrak{J}_{i_k}\subseteq\mathfrak{J}_2^s\mathfrak{J}_1^{t'}$, и потому во всех случаях $\mathfrak{J}_{i_1}\ldots\mathfrak{J}_{i_k}=0$ и $(\mathfrak{J}_1+\mathfrak{J}_2)^k=0$.

Лемма 2. *Если* $\mathfrak{J}$ *является нильпотентным левым* Ф*-идеалом кольца* $\mathfrak{A}$, *то* $\mathfrak{J}$ *содержится в нильпотентном двустороннем* Ф*-идеале.*

Так как $\mathfrak{A}\mathfrak{J} \subseteq \mathfrak{J}$, то мы имеем $(\mathfrak{J} + \mathfrak{J}\mathfrak{A})^k \subseteq \mathfrak{J}^k + \mathfrak{J}^k\mathfrak{A}$. Следовательно, если $\mathfrak{J}^r = 0$, то $(\mathfrak{J} + \mathfrak{J}\mathfrak{A})^r = 0$. Очевидно, что $\mathfrak{J} + \mathfrak{J}\mathfrak{A}$ будет двусторонним Ф-идеалом.

Из этих лемм вытекает следующая

Теорема 12. *Пусть* $\mathfrak{R}$ *является объединением всех нильпотентных левых* Ф*-идеалов* Ф*-кольца. Тогда* $\mathfrak{R}$ *будет двусторонним* Ф*-ниль-идеалом.*

Под объединением мы понимаем наименьшую подгруппу, содержащую все нильпотентные левые Ф-идеалы. Если $b \in \mathfrak{R}$, то $b \in \mathfrak{J}_1 + \ldots + \mathfrak{J}_m = \mathfrak{J}$ для некоторых нильпотеитных левых Ф-идеалов $\mathfrak{J}_j$. По лемме 1, идеал $\mathfrak{J}$ нильпотентен и, следовательно, элемент b нильпотентен. По лемме 2 $\mathfrak{J} \subseteq \mathfrak{S}$, где $\mathfrak{S}$ является нильпотентным двусторонним Ф-идеалом. Следовательно, при любом a имеем $ba \in \mathfrak{S} \subseteq \mathfrak{R}$, и потому $\mathfrak{R}$ является как правым, так и левым идеалом.

Предположим теперь (и на протяжении всей главы сохраним это ограничение), что $\mathfrak{A}$ является Ф-кольцом, удовлетворяющим условию обрыва убывающих цепей для левых Ф-идеалов. Пусть $\mathfrak{N}$ является левым Ф-ниль-идеалом кольца $\mathfrak{A}$. Так как произведение Ф-идеалов снова будет Ф-идеалом и $\mathfrak{N} \supseteq \mathfrak{N}^2 \supseteq \ldots$, то найдется такое целое число k, что $\mathfrak{N}^k = \mathfrak{N}^{k+1}$, и, следовательно, $\mathfrak{N}^k = \mathfrak{N}^{k+1} = \mathfrak{N}^{k+2} = \ldots$ Теперь мы покажем, что $\mathfrak{M} = \mathfrak{N}^k = 0$. Очевидно, $\mathfrak{M} = \mathfrak{M}^2$ является левым Ф-ниль-идеалом. Если $\mathfrak{M} \neq 0$, то пусть $\mathfrak{J}$ будет минимальным левым Ф-идеалом, содержащимся в $\mathfrak{M}$ и обладающим тем свойством, что $\mathfrak{M}\mathfrak{J} \neq 0$ (существование такого идеала следует из условия обрыва убывающих цепей). Тогда найдется в $\mathfrak{J}$ такой элемент b, что $\mathfrak{M}b \neq 0$. Так как $\mathfrak{M}b$ является левым Ф-идеалом, содержащимся в $\mathfrak{J}$, и $\mathfrak{M}(\mathfrak{M}b) = \mathfrak{M}b$, то мы получаем, что $\mathfrak{M}b = \mathfrak{J}$. Отсюда следует существование такого элемента $m \in \mathfrak{M}$, что $mb = b$. Но это невозможно, так как в этом случае мы имели бы при достаточно большом r $b = mb = m^2b = \ldots = m^rb = 0$. Это противоречие показывает, что $\mathfrak{M} = 0$, и мы получим, таким образом, следующую теорему.

Теорема 13. *Если в* Ф*-кольце* $\mathfrak{A}$ *выполнено условие обрыва убывающих цепей для левых* Ф*-идеалов, то любой левый* Ф*-ниль-идеал кольца* $\mathfrak{A}$ *нильпотентен.* [1])

В качестве следствия получаем, что определенный в теореме 12 идеал $\mathfrak{R}$ нильпотентен. Если $\mathfrak{J}$ является любым левым ниль-идеалом в кольце $\mathfrak{A}$, то $\mathfrak{J} \subseteq \mathfrak{R}$. Это следует из того, что идеал $\mathfrak{J}$ нильпотентен. Кроме того, $\mathfrak{R}$ содержит каждый нильпотентный правый Ф-идеал. В самом деле, как и выше, показываем, что каждый такой идеал содержится в двустороннем нильпотентном Ф-идеале и что этот последний содержится в $\mathfrak{R}$. Мы будем называть $\mathfrak{R}$ (левым) *радикалом* кольца $\mathfrak{A}$. Таким же образом, если в $\mathfrak{A}$ выполнено условие обрыва цепей для правых Ф-идеалов, то $\mathfrak{A}$ обладает правым радикалом $\mathfrak{R}'$, который содержит все правые Ф-ниль-идеалы. Если выполнены оба условия обрыва убывающих цепей, то $\mathfrak{R} = \mathfrak{R}'$. Докажем теперь следующую теорему.

Теорема 14. *Если* Ф*-кольцо* $\mathfrak{A}$ *удовлетворяет обоим условиям обрыва цепей для левых* Ф*-идеалов, то каждый левый* Ф*-идеал* $\mathfrak{J}$, *содержащий ненильпотентный элемент, содержит отличный от нуля идемпотентный элемент.*

Предположим, что $\mathfrak{J} = \mathfrak{J}_1 \oplus \mathfrak{J}_2$, где $\mathfrak{J}_j$ являются левыми Ф-идеалами. Если $\mathfrak{J}_1$ и $\mathfrak{J}_2$ ниль-идеалы, то они нильпотентны, и, следовательно, идеал $\mathfrak{J}$ нильпотентен. Таким образом, хотя бы один из идеалов $\mathfrak{J}_j$ не является ниль-идеалом, и потому мы можем предположить с самого начала, что идеал $\mathfrak{J}$ неразложим, если его рассматривать как группу относительно множества Ω эндоморфизмов, являющегося теоретико-множественным объединением $\mathfrak{A}_l$ и Ф. Отображение $y \to yb \equiv yB$, где y и b лежат в $\mathfrak{J}$, является Ω-эндоморфизмом. Следовательно, по лемме Фиттинга, либо эндоморфизм B нильпотентен, либо он является автоморфизмом. Если эндоморфизм B нильпотентен, то b является нильпотентным элементом, а так как, по предположению, $\mathfrak{J}$ не является ниль-идеалом, то

[1]) Эта теорема принадлежит Гопкинсу. Я благодарен профессору Р. Брауеру за приведенное выше доказательство.

найдется такой элемент b, что соответствующее ему преобразование B является автоморфизмом. Тогда $\mathfrak{J}B = \mathfrak{J}$, и, следовательно, существует такой элемент $e \in \mathfrak{J}$, что $eB = b$. Тогда $eb = b$ и $(e^2 - e)\,b = (e^2 - e)\,B = 0$ и потому $e^2 = e \neq 0$ является идемпотентным элементом, лежащим в $\mathfrak{J}$.

Таким же образом мы можем применить лемму Шура для доказательства следующей теоремы.

Теорема 15. *Если $\mathfrak{J}$ является неприводимым левым Ф-идеалом, то либо $\mathfrak{J}^2 = 0$, либо $\mathfrak{J} = \mathfrak{A}e$, где e — некоторый идемпотентный элемент.*

Мы рассматриваем снова отображение $y \to y' = yB$, где y и b лежат в $\mathfrak{J}$. Либо $B = 0$, либо B является автоморфизом. Как и ранее, из второго предположения следует, что $\mathfrak{J}$ содержит идемпотентный элемент e. Тогда $\mathfrak{J} = \mathfrak{A}e$.

11. Структура полупростых колец. Мы будем называть Ф-кольцо $\mathfrak{A}$ *полупростым*, если 1) в нем выполнено условие обрыва убывающих цепей левых Ф-идеалов, и 2) оно не содержит нильпотентных левых Ф-идеалов. Из предыдущего параграфа следует, что $\mathfrak{A}$ не содержит тогда отличных от нуля левых Ф-ниль-идеалов и нильпотентных правых Ф-идеалов. Если $\mathfrak{A}$ является кольцом, удовлетворяющим условию 1), и $\mathfrak{R}$ — его радикал, то фактор-кольцо $\overline{\mathfrak{A}} = \mathfrak{A}/\mathfrak{R}$ полупросто. В самом деле, если $\overline{\mathfrak{J}}$ является нильпотентным левым Ф-идеалом кольца $\overline{\mathfrak{A}}$, то $\overline{\mathfrak{J}} = \mathfrak{J}/\mathfrak{R}$, где $\mathfrak{J}$ является левым Ф-идеалом кольца $\mathfrak{A}$, и при некотором k имеем $\mathfrak{J}^k \subseteq \mathfrak{R}$. Тогда при достаточно большом s получим $\mathfrak{J}^{ks} \subset \mathfrak{R}^s = 0$. Следовательно, $\mathfrak{J} \subseteq \mathfrak{R}$ и $\overline{\mathfrak{J}} = 0$. Следующая теорема имеет фундаментальное значение при определении структуры полупростых колец.

Теорема 16. *Любое полупростое Ф-кольцо обладает единицей, и структура его левых Ф-идеалов вполне приводима. Обратно, если $\mathfrak{A}$ является Ф-кольцом, которое обладает следующими свойствами*: 1) *$\mathfrak{A}$ обладает единицей*, 2) *структура его левых Ф-идеалов вполне приводима и в ней выполнено условие обрыва убывающих цепей, то кольцо $\mathfrak{A}$ полупросто.*

Предположим, что кольцо $\mathfrak{A}$ полупросто. Мы хотим показать сначала, что любой неприводимый отличный от нуля левый Ф-идеал $\mathfrak{J}$ обладает дополнением. Так как $\mathfrak{J}^2 \neq 0$, то $\mathfrak{J} = \mathfrak{A}e$, где e — идемпотентный элемент, лежащий в $\mathfrak{J}$. Пусть $\mathfrak{J}'$ является множеством таких элементов $b' \in \mathfrak{A}$, что $b'e = 0$. Тогда $\mathfrak{J}'$ будет левым Ф-идеалом и $\mathfrak{J} \cap \mathfrak{J}' = 0$. Так как $a = ae + (a - ae) = b + b'$, где $b \in \mathfrak{J}$, $b' \in \mathfrak{J}'$, то $\mathfrak{J}'$ является дополнением идеала $\mathfrak{J}$.

Положим $\mathfrak{J} = \mathfrak{J}_1$, $e = e_1$. Если идеал $\mathfrak{J}'$ не минимален, то пусть $\mathfrak{J}_2 = \mathfrak{A}e_2$, где ${e_2}^2 = e_2$, будет неприводимым, отличным от нуля, левым идеалом, содержащимся в $\mathfrak{J}'$. Тогда $\mathfrak{A} = \mathfrak{J}_2 \oplus \mathfrak{J}_2'$, где $\mathfrak{J}_2'$ является левым Ф-идеалом, состоящим из таких элементов c', что $c'e_2 = 0$. Отсюда следует, что $\mathfrak{J}' = \mathfrak{J}_2 \oplus \mathfrak{J}''$, где идеал $\mathfrak{J}'' = \mathfrak{J}_2' \cap \mathfrak{J}'$ может быть определен как совокупность таких элементов b'', что $b''e_1 = b''e_2 = 0$. Следовательно, $\mathfrak{A} = \mathfrak{J}_1 \oplus \mathfrak{J}_2 \oplus \mathfrak{J}''$, где $\mathfrak{J}'' \subset \mathfrak{J}'$. Если идеал $\mathfrak{J}''$ не является неприводимым, то мы повторяем наше рассуждение и получаем $\mathfrak{A} = \mathfrak{J}_1 \oplus \mathfrak{J}_2 \oplus \mathfrak{J}_3 \oplus \mathfrak{J}'''$, где идеал $\mathfrak{J}_j = \mathfrak{A}e_j \neq 0$ неприводим, $e_j e_i = 0$ при $i < j$, ${e_i}^2 = e_i \neq 0$, и $\mathfrak{J}'''$ является лежащим в $\mathfrak{J}''$ левым Ф-идеалом. Продолжая таким образом, мы получим, наконец, $\mathfrak{A} = \mathfrak{J}_1 \oplus \mathfrak{J}_2 \oplus \ldots \oplus \mathfrak{J}_u$, где идеал $\mathfrak{J}_i = \mathfrak{A}e_j$ неприводим, ${e_i}^2 = e_i$ и $e_j e_i = 0$ при $i < j$. Следовательно, мы показали полную приводимость структуры.

Если мы образуем элемент $v = \sum e_i - \sum_{i<j} e_i e_j + \ldots + (-1)^{u-1} e_1 e_2 \ldots e_u$, то можно проверить, что $e_k v = e_k$ при $k = 1, \ldots, u$. Так как любой элемент $a = \sum a_k e_k$, то при всех a имеем $av = a$. В частности, $v^2 = v$. Множество таких элементов z, что $vz = 0$, является правым Ф-идеалом, который мы обозначим через $\mathfrak{B}$. Так как $z_1 z_2 = (z_1 v)\, z_2 = z_1 (v z_2) = 0$ при $z_1, z_2 \in \mathfrak{B}$, то $\mathfrak{B}^2 = 0$ и, следовательно, $\mathfrak{B} = 0$. В силу того, что $v(a - va) = 0$, мы получим, что при любом a $a - va = 0$, и потому $a = va$. Таким образом, v является также и левой единицей, и мы можем положить $v = 1$.

Обратно, если кольцо $\mathfrak{A}$ обладает единицей и структура его левых Ф-идеалов вполне приводима, то любой левый отличный от нуля Ф-идеал $\mathfrak{J}$ имеет вид $\mathfrak{A}e$, где $e^2 = e$. В самом деле, $\mathfrak{A} = \mathfrak{J} \oplus \mathfrak{J}'$ и, следовательно, $1 = e + e'$, где $e \in \mathfrak{J}$, $e' \in \mathfrak{J}'$, $e^2 = e \neq 0$, $e'^2 = e'$ и $ee' = e'e = 0$. Тогда $\mathfrak{J} = \mathfrak{A}e$. Так как идеал $\mathfrak{J}$ содержит отличный от нуля идемпотентный элемент e, то он не может быть нильпотентным. Если в кольце $\mathfrak{A}$ выполнено условие обрыва убывающих цепей, то из доказанного следует, что оно полупросто. Поэтому наша теорема доказана, равно как и ее

Следствие. *Любой левый Ф-идеал полупростого Ф-кольца является главным и порождается идемпотентным элементом.*

Если мы вспомним общие теоретико-структурные рассуждения из главы 3 § 4, то получим следующую теорему, дуальную теореме 16.

Теорема 17. *Если $\mathfrak{A}$ является полупростым Ф-кольцом, то существуют такие максимальные левые Ф-идеалы $\mathfrak{M}_1, \ldots, \mathfrak{M}_u$ кольца $\mathfrak{A}$, что* $0 = \mathfrak{M}_1 \cap \ldots \cap \mathfrak{M}_u$, $\mathfrak{M}_i + (\mathfrak{M}_1 \cap \ldots \cap \mathfrak{M}_{i-1} \cap \mathfrak{M}_{i+1} \cap \ldots \cap \mathfrak{M}_u) = \mathfrak{A}$.

В самом деле, если $\mathfrak{A} = \mathfrak{J}_1 \oplus \ldots \oplus \mathfrak{J}_u$, где идеалы $\mathfrak{J}_j$ неприводимы, то идеалы $\mathfrak{M}_i = \mathfrak{J}_1 + \ldots + \mathfrak{J}_{i-1} + \mathfrak{J}_{i+1} + \ldots + \mathfrak{J}_u$ удовлетворяют условиям нашей теоремы.

Этот результат приводит к интересной «арифметической» характеристике радикала, а именно:

Теорема 18. *Пусть $\mathfrak{A}$ является Ф-кольцом с единицей, в котором выполнено условие обрыва убывающих цепей левых Ф-идеалов. Тогда радикал $\mathfrak{R}$ кольца $\mathfrak{A}$ совпадает с пересечением всех максимальных левых Ф-идеалов кольца $\mathfrak{A}$.*

Так как фактор-кольцо $\overline{\mathfrak{A}} = \mathfrak{A}/\mathfrak{R}$ полупросто, то $\overline{0} = \overline{\mathfrak{M}}_1 \cap \ldots \cap \overline{\mathfrak{M}}_u$ для подходяще выбранных максимальных левых Ф-идеалов $\overline{\mathfrak{M}}_i$ кольца $\overline{\mathfrak{A}}$. Следовательно, если $\mathfrak{M}_i$ является левым Ф-идеалом кольца $\mathfrak{A}$, состоящим из элементов, отображающихся в $\overline{\mathfrak{M}}_i$, то $\mathfrak{M}_1 \cap \ldots \cap \mathfrak{M}_u = \mathfrak{R}$.

По первой теореме об изоморфизмах $\mathfrak{A}_l$-группы [1]) $\overline{\mathfrak{A}}/\overline{\mathfrak{M}}_i$ и $\mathfrak{A}/\mathfrak{M}_i$ изоморфны. Следовательно, группа $\mathfrak{A}/\mathfrak{M}_i$ неприводима, и $\mathfrak{M}_i$ является максимальным левым Ф-идеалом. Если мы обозначим пересечение всех максимальных левых Ф-идеалов через $\mathfrak{S}$, то мы доказали, таким образом, что $\mathfrak{S} \subseteq \mathfrak{R}$. С другой стороны, пусть $\mathfrak{M}$ является произвольным максимальным левым Ф-идеалом. Тогда либо $\mathfrak{M} + \mathfrak{R} = \mathfrak{M}$, либо $\mathfrak{M} + \mathfrak{R} = \mathfrak{A}$. В последнем случае $1 = m + r$, где $m \in \mathfrak{M}$ и $r \in \mathfrak{R} \ldots$, и потому $1 = (1 + r + r^2 + \ldots)(1 - r) = (1 + r + r^2 + \ldots)m \in \mathfrak{M}$. Это противоречит максимальности идеала $\mathfrak{M}$ и доказывает, что $\mathfrak{M} + \mathfrak{R} = \mathfrak{M}$, т. е. что $\mathfrak{R} \subseteq \mathfrak{M}$. Таким образом, $\mathfrak{R} \subseteq \mathfrak{S}$, и теорема доказана.

Мы переходим теперь к основной теореме о полупростых Ф-кольцах. Мы основываем доказательство на двух фактах: 1) $\mathfrak{A}$ изоморфно $\mathfrak{A}_r$ и 2) $\mathfrak{A}_r$ является совокупностью всех $\mathfrak{A}_l$-эндоморфизмов. Оба эти факта являются следствиями того, что кольцо $\mathfrak{A}$ обладает единицей. Но мы видели, что $\mathfrak{A} = \mathfrak{J}_1 \oplus \ldots \oplus \mathfrak{J}_u$, где $\mathfrak{J}_j$ — неприводимые $\mathfrak{A}$-группы. Следовательно, в силу общей теории, данной в § 5, $\mathfrak{A}_r$ будет прямой суммой двусторонних идеалов, каждый из которых представляет собою кольцо матриц над телом. Таким образом, мы получили, что $\mathfrak{A} = P_{n_1}^{(1)} \oplus \ldots \oplus P_{n_t}^{(t)}$, где $P^{(i)}$ являются телами. Но двусторонние идеалы $\mathfrak{A}_i = P_{ni}^{(i)}$ будут Ф-идеалами, так как элементы, принадлежащие Ф, являются умножениями на элементы из центра $\mathfrak{C}$ кольца $\mathfrak{A}$. Если 1_i является единицей в кольце $\mathfrak{A}_i$, то эндоморфизм, индуцированный в $\mathfrak{A}_i$ эндоморфизмом α, также будет умножением на элемент $1_i\alpha$, принадлежащий центру $\mathfrak{C}_i$ кольца $\mathfrak{A}_i$. Так как $P^{(i)} \supseteq \mathfrak{C}_i$, то $P^{(i)}$ является Ф-подкольцом кольца $\mathfrak{A}$. Тем самым доказана первая часть структурной теоремы:

Теорема 19. ***Каждое полупростое Ф-кольцо является прямой суммой своих двусторонних идеалов, каждое из которых представляет собою кольцо матриц над Ф-телом, и обратно.***

[1]) Нам не нужно упоминать здесь Ф, так как $\mathfrak{A}_l \supseteq \Phi$.

Для того, чтобы доказать вторую часть теоремы, достаточно, в силу сказанного в § 9, доказать, что кольцо матриц над телом полупросто. Мы видели в главе 2, что кольцо такого типа будет прямой суммой неприводимых левых идеалов. Они являются Ф-идеалами. Следовательно, кольцо $\mathfrak{A}$ полупросто в силу предшествовавшей теоремы.

Из теории колец матриц получаем также

Следствие. *Полупростое Ф-кольцо удовлетворяет обоим условиям обрыва цепей для левых (правых) Ф-идеалов.*

Это следствие показывает, в частности, что условия, наложенные в определении полупростого кольца на левые идеалы, выполняются также и для правых идеалов. Мы можем также начинать с условий, наложенных на правые идеалы. Тогда мы получим, что $\mathfrak{A}_i$ является прямой суммой колец матриц над телами. Следовательно, кольцо $\mathfrak{A}$ обратно изоморфно кольцу, имеющему описанную структуру; а так как кольцо, обратно изоморфное кольцу матриц над телом, является также кольцом матриц над телом, то мы получаем, что кольцо $\mathfrak{A}$ полупросто. Любой теореме, справедливой для левых (правых) идеалов полупростого кольца, соответствует дуальная теорема о правых (левых) идеалах. Например, из вышеприведенного следствия получаем, что правые идеалы кольца $\mathfrak{A}$ являются главными.

Если $\mathfrak{A}$ является простым Ф-кольцом, удовлетворяющим условию обрыва убывающих цепей для левых Ф-идеалов, и кольцо $\mathfrak{A}$ не полупросто, то $\mathfrak{A}$ нильпотентно. Так как $\mathfrak{A}^2 \subset \mathfrak{A}$ является двусторонним Ф-идеалом, то мы получаем, что $\mathfrak{A}^2 = 0$. Таким образом, любой элемент $b \neq 0$ порождает двусторонний идеал, и, следовательно, все кольцо $\mathfrak{A}$, т. е., каков бы ни был отличный от нуля элемент b, $\mathfrak{A} = \{b\}$, где через $\{b\}$ обозначено множество элементов вида $\sum b\alpha_1\alpha_2 \ldots \alpha_m$, причем $\alpha_i \in \Phi$ или $\alpha_i = \pm 1$, и $b^2 = 0$. Кольцо такого вида называется *Ф-нуль-кольцом*. Следовательно, если простое кольцо $\mathfrak{A}$ удовлетворяет условию обрыва убывающих цепей и не является Ф-нуль-кольцом, то оно полупросто. Применяя вышеприведенную теорему, находим, что имеет место

Теорема 20. *Простое Ф-кольцо, в котором выполнено условие обрыва убывающих цепей для левых Ф-идеалов, является либо Ф-нуль-кольцом, либо кольцом матриц P_n над Ф-телом P, и обратно. Если $\mathfrak{A} = P_n = \Psi_m$, где Ψ — также тело, то $n = m$, и тела P и Ψ изоморфны.*

«Прямая» часть этой теоремы является непосредственным следствием теоремы о полупростых кольцах. «Обратная» часть и единственность n и P с точностью до изоморфизма были доказаны в главе 2.

Любопытно отметить, что соответствующее утверждение для колец, удовлетворяющих условию обрыва возрастающих цепей левых идеалов, не имеет места. В самом деле, пусть $P = P_0(\xi)$ является полем рациональных функций одного неизвестного над полем P_0 характеристики 0 и $\mathfrak{A} = P[t, ']$ — кольцом дифференциальных полиномов над P, т. е. полиномов по t, где $\alpha t = t\alpha + \alpha'$, причем α' является обычной производной функции α. $\mathfrak{A}$ является кольцом главных идеалов и, следовательно, удовлетворяет условию обрыва возрастающих цепей. Легко показать, что в $\mathfrak{A}$ нет собственных двусторонних идеалов и потому кольцо $\mathfrak{A}$ просто. Тем не менее, так как $\mathfrak{A}$ не является телом, оно не имеет вида Ψ_n, где Ψ — тело.

Если мы используем результаты § 9 и предыдущих теорем, то получим следующую теорему.

Теорема 21. *Структура двусторонних Ф-идеалов полупростого Ф-кольца $\mathfrak{A}$ вполне приводима. Если $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t = \mathfrak{B}_1 \oplus \ldots \oplus \mathfrak{B}_s$ являются разложениями кольца $\mathfrak{A}$ на неприводимые двусторонние Ф-идеалы, то $s = t$, и при подходящем упорядочивании идеалов $\mathfrak{B}_i$ имеем $\mathfrak{A}_i = \mathfrak{B}_i$.*

Предположим, что $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$, где $\mathfrak{A}_i$ являются неприводимыми двусторонними Ф-идеалами. Тогда для любого двустороннего Ф-идеала $\mathfrak{B}$ кольца $\mathfrak{A}$ будет иметь место разложение $\mathfrak{B} = \mathfrak{B}_1 \oplus \ldots \oplus \mathfrak{B}_t$, где $\mathfrak{B}_i = \mathfrak{B} \cap \mathfrak{A}_i$ являются двусторонними Ф-идеалами кольца $\mathfrak{A}$. Следова-

тельно, либо $\mathfrak{B}_i = \mathfrak{A}_i$, либо $\mathfrak{B}_i = 0$. Таким образом, $\mathfrak{B} = \mathfrak{A}_{i_1} \oplus \ldots \oplus \mathfrak{A}_{i_r}$, и потому существует 2^t двусторонних Ф-идеалов кольца $\mathfrak{A}$.

Рассмотрим теперь связь между разложениями кольца $\mathfrak{A}$ в прямую сумму левых Ф-идеалов и прямую сумму двусторонних Ф-идеалов. Если $\mathfrak{J}$ является неприводимым левым Ф-идеалом, то мы видели, что $\mathfrak{J}$ содержится в одном из $\mathfrak{A}_i$, например, в $\mathfrak{A}_1$. Если $\mathfrak{J}'$ — другой левый Ф-идеал и $\mathfrak{J}' \subseteq \mathfrak{A}_2$, то $\mathfrak{J}$ и $\mathfrak{J}'$ не будут $\mathfrak{A}_l$-изоморфны, так как для 1_1, единицы кольца $\mathfrak{A}_1$, мы имеем $1_1 \mathfrak{J} = \mathfrak{J}$, в то время как $1_1 \mathfrak{J}' = 0$. Таким образом, если $\mathfrak{B}$ является объединением всех неприводимых левых Ф-идеалов, $\mathfrak{A}_l$-изоморфных с $\mathfrak{J}$, то $\mathfrak{B} \subseteq \mathfrak{A}_1$. Покажем, что $\mathfrak{B}$ будет двусторонним идеалом. В самом деле, если $b \in \mathfrak{B}$, то $b = y_1 + \ldots + y_r$, где y_i лежат в неприводимых изоморфных с $\mathfrak{J}$ Ф-идеалах $\mathfrak{J}_i$. Тогда для произвольного элемента a идеал $\mathfrak{J}_i a$ либо равен нулю, либо $\mathfrak{A}_e$-изоморфен идеалу $\mathfrak{J}$. Следовательно, $y_i a \in \mathfrak{B}$ и $ba \in \mathfrak{B}$, и потому $\mathfrak{B}$ является как правым, так и левым идеалом. Так как идеал $\mathfrak{A}_1$ неприводим, то $\mathfrak{B} = \mathfrak{A}_1$. Итак, нами получена

Теорема 22. *Если кольцо $\mathfrak{A}$ полупросто и $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$ — его разложение на неприводимые двусторонние Ф-идеалы, то каждый идеал $\mathfrak{A}_i$ является объединением неприводимых левых (правых) Ф-идеалов, $\mathfrak{A}_l$-($\mathfrak{A}_r$-) изоморфных данному неприводимому левому (правому) Ф-идеалу.*

Следствие. *Число t неприводимых двусторонних компонент равно числу $\mathfrak{A}_l$-неизоморфных (соответственно $\mathfrak{A}_r$-неизоморфных) классов левых (правых) идеалов.*

Для произвольного левого Ф-идеала $\mathfrak{J}$ кольца $\mathfrak{A}$ определим $\mathfrak{Z}_r(\mathfrak{J})$, как множество таких элементов $b \in \mathfrak{A}$, что $\mathfrak{J}b = 0$. $\mathfrak{Z}_r(\mathfrak{J})$ является правым Ф-идеалом. Подобным же образом для правого Ф-идеала $\mathfrak{J}'$ мы можем получить левый Ф-идеал $\mathfrak{Z}_l(\mathfrak{J}')$, состоящий из таких элементов c, что $c\mathfrak{J}' = 0$. Если кольцо $\mathfrak{A}$ полупросто, то мы можем считать, что $\mathfrak{J} = \mathfrak{A}e$, и тогда $\mathfrak{A} = \mathfrak{A}e \oplus \mathfrak{A}e'$, где $e^2 = e$, $e'^2 = e'$, $ee' = e'e = 0$. Тогда мы имеем также $\mathfrak{A} = e\mathfrak{A} \oplus e'\mathfrak{A}$.

Покажем, что $\mathfrak{Z}_r(\mathfrak{A}e) = e'\mathfrak{A}$. В самом деле, $e'\mathfrak{A} \subseteq \mathfrak{Z}_r(\mathfrak{A}e)$ и если $b \in \mathfrak{Z}_r(\mathfrak{A}e)$, то $eb = 0$ и, следовательно, $b = (e + e')\, b = e'b \in e'\mathfrak{A}$. По симметрии имеем $\mathfrak{Z}_l(e'\mathfrak{A}) = \mathfrak{A}e$. Таким образом, $\mathfrak{Z}_l(\mathfrak{Z}_r(\mathfrak{J})) = \mathfrak{J}$ и, подобным же образом, $\mathfrak{Z}_r(\mathfrak{Z}_l(\mathfrak{J}')) = \mathfrak{J}'$. Соответствия $\mathfrak{J} \to \mathfrak{Z}_r(\mathfrak{J})$ и $\mathfrak{J}' \to \mathfrak{Z}_l(\mathfrak{J}')$ взаимно обратны и являются взаимно-однозначными отображениями структуры левых Ф-идеалов на структуру правых Ф-идеалов, и обратно. Очевидно, что если $\mathfrak{J}_1 \subseteq \mathfrak{J}_2$, то $\mathfrak{Z}_r(\mathfrak{J}_1) \supseteq \mathfrak{Z}_r(\mathfrak{J}_2)$. Этот результат выражается следующей теоремой.

Теорема 23. *Если $\mathfrak{A}$ является полупростым кольцом, то соответствие $\mathfrak{J} \to \mathfrak{Z}_r(\mathfrak{J})$ является обратным изоморфизмом между структурой левых Ф-идеалов и структурной правых Ф-идеалов кольца $\mathfrak{A}$.*

Пусть $\mathfrak{C}$ будет центром полупростого кольца $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$. Мы видели, что $\mathfrak{C}$ является Ф-подкольцом. Если $c \in \mathfrak{C}$, то $c = c_1 + \ldots + c_t$, где $c_i \in \mathfrak{A}_i$. Так как $a = \sum a_i$, где $a_i \in \mathfrak{A}_i$ и $ac = ca$, то мы имеем $a_i c_i = c_i a_i$. Кроме того, $a_j c_i = c_i a_j = 0$ при $j \neq i$. Следовательно $c_i \in \mathfrak{C}$ и $\mathfrak{C} = \mathfrak{C}_1 \oplus \ldots \oplus \mathfrak{C}_t$, где $\mathfrak{C}_i = \mathfrak{C} \cap \mathfrak{A}_i$. $\mathfrak{C}_i$ является центром кольца $\mathfrak{A}_i$. В самом деле, если $d_i \in \mathfrak{C}_i$ и $d_i a_i = a_i d_i$, то $d_i \in \mathfrak{C}$ и, следовательно, $d_i \in \mathfrak{C}_i$. Так как $\mathfrak{A}_i = P^{(i)}{}_{n_i}$, где $P^{(i)}$ — тело, то центр кольца $\mathfrak{A}_i$ содержится в $P^{(i)}$ и является поэтому полем.

Теорема 24. *Если $\mathfrak{A}$ является полупростым Ф-кольцом и $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$, где $\mathfrak{A}_i$ — простые двусторонние идеалы кольца $\mathfrak{A}$, то его центр $\mathfrak{Z}$ будет Ф-кольцом и $\mathfrak{C} = \mathfrak{C}_1 \oplus \ldots \oplus \mathfrak{C}_t$, где $\mathfrak{C}_i = \mathfrak{C} \cap \mathfrak{A}_i$ будет полем.*

12. Представления полупростых колец. Предположим сначала, что $\mathfrak{A}$ является произвольным кольцом, а $\mathfrak{M}$ — $\mathfrak{A}$-модулем. Если $\mathfrak{J}$ — правый идеал в $\mathfrak{A}$, то множество $x\mathfrak{J}$ элементов вида xb, где x фиксировано и b пробегает идеал $\mathfrak{J}$, будет $\mathfrak{A}$-подмодулем модуля $\mathfrak{M}$. Соответствие $b \to xb$ является $\mathfrak{A}$-гомоморфизмом между $\mathfrak{J}$ и $x\mathfrak{J}$. Следовательно, если идеал $\mathfrak{J}$ неприводим, то либо $\mathfrak{J}$

$\mathfrak{A}$-изоморфен $x\mathfrak{J}$, либо $x\mathfrak{J}=0$. Если модуль $\mathfrak{M}$ неприводим, то $x\mathfrak{J}$ при любом элементе x и любом правом идеале $\mathfrak{J}$ либо равно нулю, либо совпадает с $\mathfrak{M}$. Если теперь $\mathfrak{A}$ является полупростым кольцом, то $\mathfrak{A}=\mathfrak{J}_1\oplus\ldots\oplus\mathfrak{J}_u$, где $\mathfrak{J}_j$ — неприводимые правые Ф-идеалы. Тогда, если модуль $\mathfrak{M}$ неприводим и $\mathfrak{M}\mathfrak{A}\neq 0$, то существуют такой элемент $x\in\mathfrak{M}$ и такой идеал $\mathfrak{J}_j$, что $x\mathfrak{J}_j\neq 0$. Отсюда следует, что $\mathfrak{M}=x\mathfrak{J}_j$ и потому $\mathfrak{A}$-изоморфно идеалу $\mathfrak{J}_j$. Предположим теперь, что кольцо $\mathfrak{A}$ полупросто и что $x1=x$ для всех элементов x из $\mathfrak{M}$. Тогда каждый элемент $x=x1\in x\mathfrak{A}=x\mathfrak{J}_1+\ldots+x\mathfrak{J}_u$. Так как подмодули $x\mathfrak{J}_j$ либо неприводимы, либо равны 0, то $\mathfrak{M}$ является объединением своих неприводимых подмодулей. Если в $\mathfrak{M}$ выполнено условие обрыва возрастающих цепей или, что эквивалентно этому, если модуль $\mathfrak{M}$ обладает конечным числом образующих, то $\mathfrak{M}=\mathfrak{M}_1+\ldots+\mathfrak{M}_t$ для соответствующих неприводимых подмодулей $\mathfrak{M}_i\neq 0$. Отсюда следует, что $\mathfrak{M}=\mathfrak{M}_{i_1}\oplus\ldots\oplus\mathfrak{M}_{i_t}$. В самом деле, если $\mathfrak{M}\neq\mathfrak{M}_1\equiv\mathfrak{M}_{i_1}$, то найдется такой наименьший индекс $j=i_2$, что $\mathfrak{M}_j\neq\mathfrak{M}_{i_1}$. Тогда $\mathfrak{M}_{i_1}\cap\mathfrak{M}_{i_2}=0$ и $\mathfrak{M}'=\mathfrak{M}_1+\ldots+\mathfrak{M}_{i_2}=\mathfrak{M}_{i_1}\oplus\mathfrak{M}_{i_2}$. Если $\mathfrak{M}'\neq\mathfrak{M}$, то пусть i_3 является таким наименьшим индексом, что $\mathfrak{M}_{i_3}\neq\mathfrak{M}'$. Тогда $\mathfrak{M}''=\mathfrak{M}_1+\ldots+\mathfrak{M}_{i_3}=\mathfrak{M}_{i_1}\oplus\mathfrak{M}_{i_2}\oplus\mathfrak{M}_{i_3}$. Этот процесс приводит, как легко видеть, к желаемому разложению. Таким образом, мы показали, что $\mathfrak{A}$-модуль $\mathfrak{M}$ вполне приводим и удовлетворяет условию обрыва убывающих цепей.

С другой стороны, предположим, что выполнено условие обрыва убывающих цепей, и пусть $\mathfrak{M}_1\subset\mathfrak{M}_2\subset\ldots$ является возрастающей цепью $\mathfrak{A}$-подмодулей. Если x_i является элементом из $\mathfrak{M}_{i+1}$, не лежащим в $\mathfrak{M}_i$, то $x_i\mathfrak{A}\subseteq\mathfrak{M}_{i+1}$. Так как $x_i\in x_i\mathfrak{A}=x_i\mathfrak{J}_1+\ldots+x_i\mathfrak{J}_u$, то хотя бы один из неприводимых подмодулей $x_i\mathfrak{J}_j$ отличен от нуля и лежит в $\mathfrak{M}_{i+1}$, но не лежит в $\mathfrak{M}_i$. Выберем один из таких подмодулей $x_i\mathfrak{J}_j$ и обозначим его через $\mathfrak{N}_i$. Рассмотрим цепь $(\mathfrak{N}_1+\mathfrak{N}_2+\ldots)\supseteq(\mathfrak{N}_2+\mathfrak{N}_3+\ldots)\supseteq\ldots$, где $(\mathfrak{N}_k+\mathfrak{N}_{k+1}+\ldots)$ обозначает объединение всех $\mathfrak{N}_i$ при $i\geqslant k$. Покажем, что $(\mathfrak{N}_1+\mathfrak{N}_2+\ldots)\supset(\mathfrak{N}_2+\mathfrak{N}_3+\ldots)$. В самом деле, если $(\mathfrak{N}_1+\mathfrak{N}_2+\ldots)=(\mathfrak{N}_2+\mathfrak{N}_3+\ldots)$, то для любого элемента $y_1\in\mathfrak{N}_1$ имеем $y_1=y_2+\ldots+y_m$, где $y_i\in\mathfrak{N}_i$, причем мы можем считать, что $y_m\neq 0$. Таким образом $y_m=y_1-y_2-\ldots-y_{m-1}\in(\mathfrak{N}_1+\ldots+\mathfrak{N}_{m-1})\subseteq\mathfrak{M}_m$. Следовательно, $y_m\mathfrak{A}\subseteq\mathfrak{M}_m$, что невозможно, так как $y_m\mathfrak{A}$ является отличным от нуля $\mathfrak{A}$-модулем в $\mathfrak{N}_m$, и потому $y_m\mathfrak{A}=\mathfrak{N}_m$. Таким образом, мы получаем включения

$$(\mathfrak{N}_1+\mathfrak{N}_2+\ldots)\supset(\mathfrak{N}_2+\mathfrak{N}_3+\ldots)\supset\ldots$$

В силу условия обрыва убывающих цепей, эта цепь имеет конечную длину, и, следовательно, первоначальная возрастающая цепь $\mathfrak{M}_1\subset\mathfrak{M}_2\subset\ldots$ также конечна.

Теорема 25. *Пусть $\mathfrak{A}$ является полупростым Ф-кольцом, а $\mathfrak{M}$ — таким $\mathfrak{A}$-модулем, что при всех $x\in\mathfrak{M}$ имеем $x1=x$. Тогда, если в $\mathfrak{M}$ выполнено какое-либо из условий обрыва цепей для $\mathfrak{A}$-подмодулей, то модуль $\mathfrak{M}$ вполне приводим, и в нем выполнено и другое условие обрыва цепей. Каждый неприводимый модуль $\mathfrak{M}$ $\mathfrak{A}$-изоморфен неприводимому правому идеалу кольца $\mathfrak{A}$. Число неизоморфных между собою $\mathfrak{A}$-модулей равно числу неприводимых двусторонних идеалов $\mathfrak{A}_i$ в разложении $\mathfrak{A}=\mathfrak{A}_1\oplus\ldots\oplus\mathfrak{A}_t$.*

Имеет место частичное обращение этой теоремы. Для того чтобы это доказать, нам нужно сделать следующие общие замечания. Предположим, что $\mathfrak{M}$ является $\mathfrak{A}$-модулем и что $\mathfrak{B}$ является двусторонним идеалом в $\mathfrak{A}$, аннулирующим $\mathfrak{M}$ в том смысле, что $xb=0$ для всех $x\in\mathfrak{M}$ и всех $b\in\mathfrak{B}$. Если мы обозначим смежный класс $a+\mathfrak{B}$ через $\bar{a}$, то очевидно, что функция $x\bar{a}\equiv xa$ является однозначной функцией элементов x и $\bar{a}\in\bar{\mathfrak{A}}=\mathfrak{A}/\mathfrak{B}$. Отсюда следует, что $\mathfrak{M}$ является $\bar{\mathfrak{A}}$-модулем относительно этого умножения. Очевидно, что $\mathfrak{A}$-подмодули модуля $\mathfrak{M}$ являются $\bar{\mathfrak{A}}$-подмодулями, и обратно, и что $\mathfrak{A}$-приводимость, $\mathfrak{A}$-разложимость и т. д. эквивалентны $\bar{\mathfrak{A}}$-приводимости, $\bar{\mathfrak{A}}$-разложимости и т. д.; нетрудно также видеть, что если $\mathfrak{M}$ и $\mathfrak{N}$ являются двумя аннулирующимися идеалом $\mathfrak{B}$ $\mathfrak{A}$-моду-

лями, то $\mathfrak{A}$-гомоморфизмы и $\mathfrak{A}$-изоморфизмы между ними являются в то же время $\overline{\mathfrak{A}}$-гомоморфизмами и $\overline{\mathfrak{A}}$-изоморфизмами, и обратно.

Пусть теперь $\mathfrak{A}$ является Ф-кольцом, удовлетворяющим условию обрыва убывающих цепей для левых Ф-идеалов, а $\mathfrak{R}$ — радикалом кольца $\mathfrak{A}$. Тогда для любого элемента x неприводимого $\mathfrak{A}$-модуля $\mathfrak{M}$ $x\mathfrak{R}$ будет подмодулем, и потому либо $x\mathfrak{R}=0$, либо $x\mathfrak{R}=\mathfrak{M}$. Если $x\mathfrak{R}=\mathfrak{M}$, то $\mathfrak{M}=x\mathfrak{R}=x\mathfrak{R}^2=\ldots=0$. Следовательно, $\mathfrak{R}$ аннулирует модуль $\mathfrak{M}$, и $\mathfrak{M}$ является $\overline{\mathfrak{A}}$-модулем, где $\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{R}$. Если $\overline{\mathfrak{A}}=\overline{\mathfrak{A}}_1\oplus\ldots\oplus\overline{\mathfrak{A}}_t$, то либо $\mathfrak{M}\mathfrak{A}=0$, либо $\mathfrak{M}$ изоморфно некоторому правому идеалу, содержащемуся в одном из $\overline{\mathfrak{A}}_i$. Отсюда следует, что $\mathfrak{M}$ будет $\overline{\mathfrak{A}}_i$-модулем. Подобным же образом, если $\mathfrak{M}$ является объединением неприводимых подмодулей, то $x\mathfrak{R}=0$ для всех x, и $\mathfrak{M}$ будет $\overline{\mathfrak{A}}$-модулем.

Теорема 26. *Пусть $\mathfrak{A}$ является Ф-кольцом, удовлетворяющим условию обрыва убывающих цепей для левых Ф-идеалов и пусть $\mathfrak{M}$ является таким $\mathfrak{A}$-модулем, что $\mathfrak{M}\mathfrak{A}\neq 0$. Если модуль $\mathfrak{M}$ неприводим, то $\mathfrak{M}$ будет $\overline{\mathfrak{A}}_i$-модулем, где через $\overline{\mathfrak{A}}_i$ обозначен один из неприводимых двусторонних идеалов фактор-кольца $\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{R}$. Если $\mathfrak{M}$ является объединением неприводимых $\mathfrak{A}$-модулей, то $\mathfrak{M}$ будет $\overline{\mathfrak{A}}$-модулем.*

Другой формой этого результата является следующая

Теорема 27. *Пусть $\mathfrak{A}$ является отличным от нуля Ф-кольцом эндоморфизмов группы $\mathfrak{M}$, причем в $\mathfrak{A}$ выполнено условие обрыва убывающих цепей левых Ф-идеалов. Тогда, если группа $\mathfrak{M}$ неприводима, то кольцо $\mathfrak{A}$ просто, а если $\mathfrak{M}$ является объединением неприводимых $\mathfrak{A}$-групп, то кольцо $\mathfrak{A}$ полупросто.*

В самом деле, в этом случае $\mathfrak{M}$ будет $\mathfrak{A}$-модулем, и представление кольца $\mathfrak{A}$ в самом кольце $\mathfrak{A}$ будет, очевидно, взаимооднозначным.

Предположим теперь, что $\mathfrak{A}$ является любым кольцом эндоморфизмов группы $\mathfrak{M}$, содержащим единичный эндоморфизм, и пусть $\mathfrak{A}=\mathfrak{A}_1\oplus\ldots\oplus\mathfrak{A}_t$ будет разложением

кольца $\mathfrak{A}$ на двусторонние идеалы. Тогда $\mathfrak{M}=\mathfrak{M}\mathfrak{A}_1+\ldots+\mathfrak{M}\mathfrak{A}_t$, где $\mathfrak{M}\mathfrak{A}_i$ обозначает наименьший подмодуль, содержащий все элементы вида xa_i при $a_i\in\mathfrak{A}_i$. Если $1=1_1+\ldots+1_t$, где $1_i\in\mathfrak{A}_i$, то 1_i является единицей в кольце $\mathfrak{A}_i$, так как $\mathfrak{A}_i=\mathfrak{A}1_i=1_i\mathfrak{A}$. Следовательно, если $x_i\in\mathfrak{M}\mathfrak{A}_i$, то $x_i1_i=x_i$, и так как $1_i1_j=0$, то $x_i1_j=0$ при $i\neq j$. Если $x_1+\ldots+x_t=0$, где $x_i\in\mathfrak{M}\mathfrak{A}_i$, то $(x_1+\ldots+x_t)\,1_i=x_i1_i=x_i=0$. Таким образом,

$$\mathfrak{M}=\mathfrak{M}\mathfrak{A}_1\oplus\ldots\oplus\mathfrak{M}\mathfrak{A}_t.$$

Предположим снова, что кольцо $\mathfrak{A}$ полупросто, и пусть в модуле $\mathfrak{M}$ выполнены оба условия обрыва цепей. Тогда $\mathfrak{M}\mathfrak{A}_i$ является объединением неприводимых подмодулей, каждый из которых изоморфен правым идеалам кольца $\mathfrak{A}_i$. Как мы видели в § 5, кольцо $\mathfrak{A}$-эндоморфизмов модуля $\mathfrak{M}$ имеет вид $\mathfrak{B}=\mathfrak{B}_1\oplus\ldots\oplus\mathfrak{B}_t$, где $\mathfrak{B}_1$ состоит из эндоморфизмов, получаемых из $\mathfrak{A}$-эндоморфизмов b_i подмодуля $\mathfrak{M}_i\equiv\mathfrak{M}\mathfrak{A}_i$ при помощи такого распространения их на весь модуль $\mathfrak{M}$, что $\mathfrak{M}_ib_j=0$ при $j\neq i$. Таким образом, $\mathfrak{M}_i=\mathfrak{M}\mathfrak{B}_i$. Если подкольцо $\mathfrak{A}_i$ является кольцом матриц над телом, то и кольцо эндоморфизмов, индуцированных эндоморфизмами из $\mathfrak{A}$ в $\mathfrak{M}_i$, имеет ту же структуру. Из наших результатов о кольцах матриц [1] следует тогда, что если $\mathfrak{A}_i=P_{n_i}^{(i)}$, то $\mathfrak{B}_i=\overline{P}_{m_i}^{(i)}$, где через $\overline{P}^{(i)}$ обозначено тело, обратно изоморфное телу $P^{(i)}$, и $\mathfrak{A}$ является совокупностью всех $\mathfrak{B}$-эндоморфизмов модуля $\mathfrak{M}$.

Теорема 28. *Пусть $\mathfrak{A}$ является полупростым Ф-кольцом эндоморфизмов модуля $\mathfrak{M}$, содержащим единичный эндоморфизм, и пусть в $\mathfrak{M}$ выполнено одно из условий обрыва цепей для $\mathfrak{A}$-подмодулей. Если $\mathfrak{A}=P_{n_1}^{(1)}\oplus\ldots\oplus P_{n_t}^{(t)}$, где $P_{n_i}^{(i)}$ является двусторонним идеалом и $P^{(i)}$ — телом, то кольцо $\mathfrak{A}$-эндоморфизмов $\mathfrak{B}$ имеет вид $\mathfrak{B}=\overline{P}_{n_1}^{(1)}\oplus\ldots\oplus\overline{P}_{n_t}^{(t)}$, где $\overline{P}_{n_i}^{(i)}$ является двусторонним идеалом и тело $\overline{P}^{(i)}$ обратно изоморфно телу $P^{(i)}$. $\mathfrak{A}$ будет кольцом $\mathfrak{B}$-эндоморфизмов модуля $\mathfrak{M}$.*

[1] См. главу 2, § 6.

13. Кольца, удовлетворяющие условию обрыва убывающих цепей. Из результатов предыдущего отдела вытекает интересная

Теорема 29. *Если* $\mathfrak{A}$ *является Ф-кольцом с единицей, удовлетворяющим условию обрыва убывающих цепей для правых (левых) Ф-идеалов, то* $\mathfrak{A}$ *удовлетворяет также условию обрыва возрастающих цепей для правых (левых) Ф-идеалов.*

Пусть $\mathfrak{R}$ является радикалом кольца $\mathfrak{A}$ и $\mathfrak{R}^{s+1}=0$, $\mathfrak{R}^s\neq 0$. Тогда $\mathfrak{A}\supset\mathfrak{R}\supset\ldots\supset\mathfrak{R}^s\supset 0$ является убывающей цепью $\mathfrak{A}$-модулей ($\mathfrak{A}_r$-групп). Фактор-модули $\mathfrak{A}/\mathfrak{R}$, $\mathfrak{R}/\mathfrak{R}^2$, ... отображаются в нуль элементами из $\mathfrak{R}$ и, следовательно, могут рассматриваться как $(\mathfrak{A}/\mathfrak{R})$-модули. Так как кольцо $\mathfrak{A}$ удовлетворяет условию обрыва убывающих цепей, то и фактор-модули $\mathfrak{A}/\mathfrak{R}$, $\mathfrak{R}/\mathfrak{R}^2$, ... также должны удовлетворять этому условию. Так как кольцо $\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{R}$ полупросто, и его единица является единичным эндоморфизмом в $\mathfrak{A}/\mathfrak{R}$, $\mathfrak{R}/\mathfrak{R}^2$, ..., то эти модули удовлетворяют условию обрыва возрастающих цепей и, следовательно, обладают композиционным рядом. Например, $\mathfrak{A}/\mathfrak{R}=\overline{\mathfrak{I}}_1\supset\overline{\mathfrak{I}}_2\supset\ldots\supset\overline{\mathfrak{I}}_m=0$, где фактор-модули $\overline{\mathfrak{I}}_j/\overline{\mathfrak{I}}_{j+1}$ $\mathfrak{A}$-неприводимы. Следовательно, $\mathfrak{A}=\mathfrak{I}_1\supset\mathfrak{I}_2\supset\ldots\supset\mathfrak{I}_m=\mathfrak{R}$, где $\mathfrak{I}_j$ является правым Ф-идеалом, отображающимся в 0 при гомоморфизме кольца $\mathfrak{A}$ на $\mathfrak{A}/\mathfrak{R}$. По первой теореме об изоморфизме, модуль $\mathfrak{I}_j/\mathfrak{I}_{j+1}$ $\mathfrak{A}$-изоморфен модулю $\overline{\mathfrak{I}}_j/\overline{\mathfrak{I}}_{j+1}$ и, следовательно, он $\mathfrak{A}$-неприводим. Таким же образом получаем $\mathfrak{R}=\mathfrak{I}_m\supset\ldots\supset\mathfrak{I}_{m+p}=\mathfrak{R}^2$, где $\mathfrak{I}_k$ являются правыми Ф-идеалами, и факторы $\mathfrak{I}_k/\mathfrak{I}_{k+1}$ неприводимы, и т. д. Следовательно, $\mathfrak{A}$ обладает композиционным рядом, и поэтому для правых Ф-идеалов кольца $\mathfrak{A}$ имеют место оба условия обрыва цепей.

Эта теорема позволяет непосредственно применять наши результаты о кольцах эндоморфизмов к абстрактным кольцам. Таким образом, следствием доказанного в § 6 является следующая теорема.

Теорема 30. *Если* $\mathfrak{A}$ *является Ф-кольцом с единицей, удовлетворяющим условию обрыва убывающих цепей для левых (правых) Ф-идеалов, то любое его нильподкольцо* $\mathfrak{B}$ *нильпотентно.*

Рассмотрим кольцо $\overline{\mathfrak{B}}$ тех правых умножений в $\mathfrak{A}$, которые соответствуют элементам из $\mathfrak{B}$. Элементы из $\overline{\mathfrak{B}}$ будут $\mathfrak{A}_l$-эндоморфизмами. Следовательно, если s — длина композиционного ряда для $\mathfrak{A}_l$-группы $\mathfrak{A}$, то $\overline{b}_1\ldots\overline{b}_s=0$ для любых элементов $\overline{b}_i$ из $\overline{\mathfrak{B}}$. Таким образом, $xb_1\ldots b_s=0$ для любого $x\in\mathfrak{A}$ и $b_i\in\mathfrak{B}$. Следовательно, $\mathfrak{B}^{s+1}=0$.

Отметим также следующую теорему, непосредственно вытекающую из результатов § 8.

Теорема 31. *Если* $\mathfrak{A}$ *является Ф-кольцом, удовлетворяющим условию обрыва убывающих цепей для левых (правых) Ф-идеалов, то следующие свойства кольца* $\mathfrak{A}$ *эквивалентны между собой:*

1. $\mathfrak{A}$ *является прямой суммой* $\mathfrak{A}_l$-($\mathfrak{A}_r$-) *изоморфных между собой неразложимых левых (правых) Ф-идеалов.*
2. *Фактор-кольцо* $\mathfrak{A}/\mathfrak{R}$, *где* $\mathfrak{R}$ *является радикалом кольца* $\mathfrak{A}$, *просто.*
3. $\mathfrak{A}=\mathfrak{B}_u$, *где* $\mathfrak{B}$ *является вполне примарным кольцом.*

Если какое-либо из этих условий выполнено, то $\mathfrak{A}$ является *примарным* кольцом.

14. Регулярные представления. Пусть $\mathfrak{A}$ является произвольным Ф-кольцом с единицей, удовлетворяющим условиям обрыва убывающих цепей для односторонних идеалов. Предположим, что $\mathfrak{A}=e_1\mathfrak{A}\oplus\ldots\oplus e_u\mathfrak{A}$ является разложением $\mathfrak{A}$ в прямую сумму отличных от нуля правых идеалов, причем

$$1=\sum e_i,\quad e_i^2=e_i\neq 0,\quad e_ie_j=0,\ \text{если}\ i\neq j. \tag{4}$$

Если $\mathfrak{N}$ — какой-либо нильпотентный двусторонний идеал кольца $\mathfrak{A}$ и $\overline{e}_i=e_i+\mathfrak{N}$, то в кольце $\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{N}$ имеем

$$1=\sum\overline{e}_i,\quad \overline{e}_i^2=\overline{e}_i\neq 0,\quad \overline{e}_i\overline{e}_j=0,\ \text{если}\ i\neq j, \tag{5}$$

и потому $\overline{\mathfrak{A}}=\overline{e}_1\overline{\mathfrak{A}}\oplus\ldots\oplus\overline{e}_u\overline{\mathfrak{A}}$ является разложением кольца $\overline{\mathfrak{A}}$ в прямую сумму правых идеалов. Так как $\overline{e}_i\neq 0$,

то $\bar{e}_i\bar{\mathfrak{A}} \neq 0$. Мы хотим показать, что любое разложение $\bar{\mathfrak{A}}$ в прямую сумму правых идеалов может быть получено таким образом. Для этого нам нужна

Лемма. *Если $\bar{e}_1, \ldots, \bar{e}_v$ являются отличными от нуля идемпотентными элементами кольца $\bar{\mathfrak{A}}$, для которых $\bar{e}_i\bar{e}_j = 0$ при $i \neq j$, то возможно выбрать в смежных классах $\bar{e}_i$ такие элементы e_i, что $e_i^2 = e_i$ и $e_ie_j = 0$.*

Предположим, что для $j = 1, \ldots, m$ уже определены элементы e_j с требуемыми свойствами. Выберем в $\bar{e}_{m+1}$ любой элемент u и образуем элемент $v = u - eu - ue + eue$, где $e = \sum_1^m e_i$. Тогда при $i = 1, \ldots, m$ имеем $e_iv = ve_i = 0$ и $v \equiv u \pmod{\mathfrak{R}}$. Следовательно, $v^2 = v + z$, где z является нильпотентным элементом, например, $z^s = 0$. Очевидно, что $zv = vz$. Постараемся теперь определить элемент $w = f(z)\,v + g(z)$ таким образом, чтобы $w^2 = w$ и $f(z)$ и $g(z)$ являлись полиномами от z с целыми коэффициентами. Это приводит к рассмотрению уравнений

$$f^2 + 2fg = f,\quad g^2 + f^2z = g. \tag{6}$$

Мы решим сначала эти уравнения при помощи степенных рядов от неизвестного t. Исключая g, мы получаем $f(t) = (1+4t)^{-\frac{1}{2}}$ и $g(t) = \frac{1}{2}[1 - f(t)]$. Рассмотрим теперь разложение функции $f(t) = (1+4t)^{-\frac{1}{2}}$. Нетрудно видеть, что

$$f(t) = 1 + \sum (-1)^n \binom{2n-1}{n} 2t^n,$$

и таким образом все коэффициенты в разложениях для $f(t)$ и $g(t)$ являются целыми числами. Формальные тождества

$$[f(t)]^2 + 2f(t)\,g(t) = f(t),\quad [g(t)]^2 + [f(t)]^2 t = g(t)$$

выполнены. Отсюда следует, что если $f_s(t)$ и $g_s(t)$ являются s-ми частными суммами рядов соответственно для $f(t)$ и $g(t)$, то функции $f = f_s(z)$ и $g = g_s(z)$ удовлетворяют уравнениям (6). Следовательно, $w = fv + g$ является идемпотентным элементом. Так как $e_iv = ve_i = 0$, то $we_i = e_iw = 0$. Формула, полученная нами для w, показывает, что $w \equiv v \pmod{\mathfrak{R}}$ и, следовательно, $w \equiv u \pmod{\mathfrak{R}}$. Таким образом, w может служить элементом e_{m+1}, и по индукции лемма доказана.

Замечание. Вышеприведенное доказательство сохраняет силу и в случае, когда алгебра $\mathfrak{A}$ не содержит единицы. В самом деле, мы можем присоединить к $\mathfrak{A}$ единицу и строить вышеуказанным образом идемпотентный элемент e_{m+1}, начав с элемента $u \in \mathfrak{A}$. Нетрудно видеть, что тогда и $e_{m+1} \in \mathfrak{A}$.

Если в лемме $\sum \bar{e}_i = \bar{1}$, то $\sum e_i = 1 + y$, где $y \in \mathfrak{R}$. Так как $\sum e_i$ является идемпотентным элементом, то $(1+y)^2 = 1 + y$. Следовательно, $y^2 + y = 0$. Таким образом $y = -y^2 = y^3 = \ldots = 0$ и потому $\sum e_i = 1$. Отсюда следует, что если $\bar{\mathfrak{A}} = \bar{e}_1\bar{\mathfrak{A}} \oplus \ldots \oplus \bar{e}_v\bar{\mathfrak{A}}$ является разложением $\bar{\mathfrak{A}}$ в прямую сумму отличных от нуля правых идеалов, причем элементы $\bar{e}_i$ удовлетворяют условиям (5), то $\mathfrak{A} = e_1\mathfrak{A} \oplus \ldots \oplus e_v\mathfrak{A}$, где элементы $e_i \in \bar{e}_i$ удовлетворяют условиям (4). Из леммы и из теоремы Крулля-Шмидта следует также, что идемпотентные элементы e_i примитивны тогда и только тогда, когда примитивны элементы $\bar{e}_i$. Таким образом, идеал $e_i\mathfrak{A}$ неразложим тогда и только тогда, когда неразложим идеал $\bar{e}_i\bar{\mathfrak{A}}$. Если $\mathfrak{R}$ является радикалом кольца $\mathfrak{A}$, то фактор-кольцо $\bar{\mathfrak{A}}$ полупросто, и, следовательно, идеал $\bar{e}_i\bar{\mathfrak{A}}$ неразложим тогда и только тогда, когда он неприводим. Нами доказана тем самым

Теорема 32. *Пусть $\mathfrak{A}$ является Ф-кольцом с единицей, удовлетворяющим условиям обрыва убывающих цепей для односторонних идеалов, и пусть $\mathfrak{R}$ — его радикал. Если $\mathfrak{A} = e_1\mathfrak{A} \oplus \ldots \oplus e_u\mathfrak{A}$, где элементы e_i удовлетворяют условиям* (4), *то $\bar{\mathfrak{A}} \equiv \mathfrak{A}/\mathfrak{R} = \bar{e}_1\bar{\mathfrak{A}} \oplus \ldots \oplus \bar{e}_u\bar{\mathfrak{A}}$.*

Идеал $e_i\mathfrak{A}$ неразложим тогда и только тогда, когда идеал $\bar{e}_i\bar{\mathfrak{A}}$ неприводим.

Рассмотрим модуль $\mathfrak{M} = e_i\mathfrak{A} \oplus e_j\mathfrak{A} = e\mathfrak{A}$, $e = e_i + e_j$. Так как $\mathfrak{A} = \mathfrak{M} \oplus (1-e)\mathfrak{A}$, то определенные этим разложением проекции E и E' являются левыми умножениями соответственно на элементы e и $e' = 1 - e$. Так как $\mathfrak{A}_l$ является кольцом $\mathfrak{A}_r$-эндоморфизмов аддитивной группы кольца $\mathfrak{A}$ (см. § 4), то $E\mathfrak{A}_lE$ является кольцом $\mathfrak{A}_r$-эндоморфизмов $\mathfrak{M}$. Таким образом кольцо $\mathfrak{A}_r$-эндоморфизмов модуля $\mathfrak{M}$ обратно изоморфно кольцу $e\mathfrak{A}e$. Следовательно, согласно § 8, $e_i\mathfrak{A}$ и $e_j\mathfrak{A}$ $\mathfrak{A}$-изоморфны тогда и только тогда, когда кольцо $e\mathfrak{A}e$ примарно. Но

$$e\mathfrak{A}e/(\mathfrak{R} \cap e\mathfrak{A}e) \cong (e\mathfrak{A}e + \mathfrak{R})/\mathfrak{R} = \bar{e}\,\bar{\mathfrak{A}}\,\bar{e}\,,$$

и кольцо $\bar{e}\,\bar{\mathfrak{A}}\,\bar{e}$ обратно изоморфно кольцу $\bar{\mathfrak{A}}_r$-эндоморфизмов модуля $\bar{\mathfrak{M}} = \bar{e}\,\bar{\mathfrak{A}}$. Так как модуль $\bar{\mathfrak{M}}$ вполне приводим, то кольцо $\bar{e}\bar{\mathfrak{A}}\bar{e}$ полупросто. Отсюда следует, что $\mathfrak{R} \cap e\mathfrak{A}e = e\mathfrak{R}e$ и $e\mathfrak{R}e$, которое, очевидно, содержится в радикале кольца $e\mathfrak{A}e$, совпадает с этим радикалом. Следовательно, кольцо $e\mathfrak{A}e$ примарно тогда и только тогда, когда кольцо $\bar{e}\bar{\mathfrak{A}}\bar{e}$ просто, и нами получена поэтому следующая

Теорема 33. *Пусть $\mathfrak{A}$, $\bar{\mathfrak{A}}$ и т. д. имеют тот же смысл, что и в предыдущей теореме, и идемпотентные элементы e_i примитивны. $\mathfrak{A}$-модули $e_i\mathfrak{A}$ и $e_j\mathfrak{A}$ $\mathfrak{A}$-изоморфны тогда и только тогда, когда $\bar{e}_i\bar{\mathfrak{A}}$ и $\bar{e}_j\bar{\mathfrak{A}}$ $\bar{\mathfrak{A}}$-изоморфны.*

Так как $e_i\mathfrak{R} = e_i\mathfrak{A} \cap \mathfrak{R}$, то $\mathfrak{A}$-модуль $e_i\mathfrak{A}/e_i\mathfrak{R}$ изоморфен модулю $(e_i\mathfrak{A} + \mathfrak{R})/\mathfrak{R}$. Этот последний является, в сущности, $\bar{\mathfrak{A}}$-модулем $\bar{e}_i\bar{\mathfrak{A}}$. Следовательно, модуль $e_i\mathfrak{A}/e_i\mathfrak{R}$ неприводим, и потому $e_i\mathfrak{R}$ является максимальным подмодулем модуля $e_i\mathfrak{A}$, а $\bar{e}_i\bar{\mathfrak{A}}$ будет первым композиционным фактором модуля $e_i\mathfrak{A}$. С другой стороны, если $\mathfrak{M}$ — максимальный подмодуль модуля $e_i\mathfrak{A}$, то фактор-модуль $e_i\mathfrak{A}/\mathfrak{M}$ неприводим, и потому этот модуль аннулируется радикалом $\mathfrak{R}$. Отсюда вытекает, что $e_i\mathfrak{R} \subseteq \mathfrak{M}$ и, следовательно,

$e_i\mathfrak{R} = \mathfrak{M}$. Таким образом, $e_i\mathfrak{R}$ будет единственным максимальным подмодулем $\mathfrak{A}$-модуля $e_i\mathfrak{A}$. Это составляет первую часть следующей теоремы.

Теорема 34. *Если $\mathfrak{J}$ является неразложимым правым идеалом, встречающимся в прямом разложении кольца $\mathfrak{A}$, то существует только один максимальный в $\mathfrak{J}$ правый идеал кольца $\mathfrak{A}$. Если $\mathfrak{J}$ и $\mathfrak{J}'$ — неразложимые правые идеалы, встречающиеся в прямых разложениях кольца $\mathfrak{A}$, то для того, чтобы идеалы $\mathfrak{J}$ и $\mathfrak{J}'$ были $\mathfrak{A}$-изоморфны, необходимо и достаточно, чтобы их первые композиционные факторы были $\mathfrak{A}$-изоморфны.*

Вторая часть этой теоремы следует из теоремы Крулля-Шмидта и из теоремы 33. В самом деле, по первой из них идеал $\mathfrak{J}$ $\mathfrak{A}$-изоморфен одному из правых идеалов $\mathfrak{J}_1$, встречающихся в том прямом разложении $\mathfrak{A}$, в которое входит $\mathfrak{J}'$. По теореме 33 идеалы $\mathfrak{J}_1$ и $\mathfrak{J}'$ изоморфны тогда и только тогда, когда их первые композиционные факторы изоморфны. Следовательно, это же имеет место и для идеалов $\mathfrak{J}$ и $\mathfrak{J}'$.

Для того, чтобы получить связь между разложением кольца $\mathfrak{A}$ в прямую сумму неразложимых правых идеалов и разложением его в прямую сумму неразложимых двусторонних идеалов, нам нужна следующая

Лемма. *Пусть $\mathfrak{N}$ и $\mathfrak{N}'$ являются $\mathfrak{A}$-модулями, обладающими композиционными рядами. Предположим, что $\mathfrak{N}$ обладает только одним максимальным подмодулем $\mathfrak{M}$ и что $\mathfrak{N}$ $\mathfrak{A}$-гомоморфно отображается на подмодуль $\mathfrak{N}^*$ модуля $\mathfrak{N}'$. Тогда любой композиционный ряд модуля $\mathfrak{N}'$ содержит $\mathfrak{A}$-изоморфный модулю $\mathfrak{N}/\mathfrak{M}$ фактор.*

Отметим сначала, что любой истинный подмодуль $\mathfrak{Z}$ модуля $\mathfrak{N}$ содержится в $\mathfrak{M}$. В самом деле, фактор-модуль $\mathfrak{N}/\mathfrak{Z}$ содержит максимальный подмодуль $\bar{\mathfrak{M}}_1$, и соответствующий ему подмодуль $\mathfrak{M}_1$ модуля $\mathfrak{N}$ является максимальным и содержит $\mathfrak{Z}$. Так как $\mathfrak{M}$ — единственный максимальный подмодуль модуля $\mathfrak{N}$, то $\mathfrak{M} = \mathfrak{M}_1$. Пусть теперь $\mathfrak{Z}$ будет подмодулем, состоящим из элементов, отображающихся

в 0 при гомоморфном отображении модуля $\mathfrak{N}$ на $\mathfrak{N}^*$. Тогда модуль $\mathfrak{N}^*$ $\mathfrak{A}$-изоморфен фактор-модулю $\mathfrak{N}/\mathfrak{Z}$. Так как $(\mathfrak{N}/\mathfrak{Z}) \supset (\mathfrak{M}/\mathfrak{Z}) \supseteq 0$, то $\mathfrak{N}/\mathfrak{Z}$ обладает композиционным фактором $(\mathfrak{N}/\mathfrak{Z})/(\mathfrak{M}/\mathfrak{Z})$, который $\mathfrak{A}$-изоморфен фактор-модулю $\mathfrak{N}/\mathfrak{M}$. Следовательно, $\mathfrak{N}^*$, а тогда и $\mathfrak{N}'$, обладает композиционным фактором, $\mathfrak{A}$-изоморфным $\mathfrak{N}/\mathfrak{M}$.

Ограничимся теперь только такими неразложимыми идеалами кольца $\mathfrak{A}$, которые встречаются в прямых разложениях кольца $\mathfrak{A}$. Они имеют всегда вид $e\mathfrak{A}$, где e является примитивным идемпотентным элементом. Наоборот, всякий идеал такого вида неразложим и принадлежит некоторому прямому разложению кольца $\mathfrak{A}$. Мы будем говорить, что два таких идеала $e\mathfrak{A}$ и $e'\mathfrak{A}$ принадлежат одному и тому же *блоку*, если существует последовательность таких неразложимых идеалов $e\mathfrak{A} = e_1\mathfrak{A}, e_2\mathfrak{A}, \ldots, e_h\mathfrak{A} = e'\mathfrak{A}$, что $e_i^2 = e_i$ и каждый идеал $e_i\mathfrak{A}$ обладает композиционным фактором, $\mathfrak{A}$-изоморфным одному из композиционных факторов идеала $e_{i+1}\mathfrak{A}$. Это отношение между идеалами $e\mathfrak{A}$ и $e'\mathfrak{A}$ обладает, очевидно, всеми свойствами эквивалентности. Последовательность идеалов $\{e_i\mathfrak{A}\}$ называется последовательностью, *связывающей* идеалы $e\mathfrak{A}$ и $e'\mathfrak{A}$. При этих определениях мы имеем следующую теорему.

Теорема 35. *Пусть* $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$ *является разложением кольца* $\mathfrak{A}$ *в прямую сумму неразложимых двусторонних идеалов. Два неразложимые идеала* $e\mathfrak{A}$ *и* $e'\mathfrak{A}$ *принадлежат одному и тому же блоку тогда и только тогда, когда они содержатся в одной и той же компоненте* $\mathfrak{A}_i$. *Следовательно,* $\mathfrak{A}_i$ *является объединением множества неразложимых идеалов* $e\mathfrak{A}$, *принадлежащих к одному и тому же блоку.*

Мы видели в § 9, что любой неразложимый идеал содержится в одном и только одном идеале $\mathfrak{A}_i$. Если идеалы $e\mathfrak{A}$ и $e'\mathfrak{A}$ принадлежат одному и тому же блоку, то они содержатся в одной и той же двусторонней компоненте. В самом деле, предположим, что $e\mathfrak{A}$ и $e'\mathfrak{A}$ лежат в различных компонентах, скажем, соответственно в $\mathfrak{A}_1$ и $\mathfrak{A}_2$. Если 1_1 является единицей в $\mathfrak{A}_1$, то $(e\mathfrak{A})\, 1_1 = e\mathfrak{A}$ и $(e'\mathfrak{A})\, 1_1 = 0$, а потому $e\mathfrak{A}$ не обладает композиционными факторами, $\mathfrak{A}$-изоморфными какому-либо из композиционных факторов $e'\mathfrak{A}$. Таким образом, если $\{e_i\mathfrak{A}\}$ является последовательностью, связывающей идеалы $e\mathfrak{A}$ и $e'\mathfrak{A}$, то каждая пара $e_i\mathfrak{A}$, и $e_{i+1}\mathfrak{A}$, содержится в одной и той же компоненте, что остается поэтому справедливым и для идеалов $e\mathfrak{A}$ и $e'\mathfrak{A}$. Если идеалы $e\mathfrak{A}$ и $e'\mathfrak{A}$ принадлежат различным блокам, то $e\mathfrak{A}e'\mathfrak{A} = 0$. В противном случае, найдется элемент $b = eae' \neq 0$, и тогда левое умножение, определенное элементом b, будет $\mathfrak{A}$-гомоморфизмом между $e'\mathfrak{A}$ и отличным от нуля подмодулем модуля $e\mathfrak{A}$. Следовательно, в силу леммы, как $e'\mathfrak{A}$, так и $e\mathfrak{A}$ обладают, вопреки предположению, композиционными факторами, изоморфными $\overline{e'\mathfrak{A}}$. Пусть теперь $\mathfrak{A} = e_1\mathfrak{A} \oplus \ldots \oplus e_u\mathfrak{A}$ является разложением кольца $\mathfrak{A}$ в прямую сумму отличных от нуля неразложимых правых идеалов. Предположим, что элементы e_i удовлетворяют условиям (4). Пусть идеалы $e_1\mathfrak{A}, \ldots, e_{n_1}\mathfrak{A}$ принадлежат к одному блоку, идеалы $e_{n_1+1}\mathfrak{A}, \ldots, e_{n_1+n_2}\mathfrak{A}$ принадлежат также к одному блоку, но отличному от блока, содержащего идеал $e_1\mathfrak{A}$, и т. д. Положим $\mathfrak{B}_1 = e_1\mathfrak{A} \oplus \ldots \oplus e_{n_1}\mathfrak{A}$, $\mathfrak{B}_2 = e_{n_1+1}\mathfrak{A} \oplus \ldots \oplus e_{n_1+n_2}\mathfrak{A}, \ldots$ Тогда $e_j\mathfrak{A}e_i\mathfrak{A} = 0$ при $i \leqslant n_1$ и $j > n_1$. Следовательно, $\mathfrak{A}(e_i\mathfrak{A}) \subseteq \mathfrak{B}_1(e_i\mathfrak{A}) \subseteq \mathfrak{B}_1$, и $\mathfrak{B}_1$ является двусторонним идеалом. Подобно этому каждый из идеалов $\mathfrak{B}_i$ будет двусторонним и, так как $\mathfrak{B}_i$ представляет собою объединение идеалов одного и того же блока, то он содержится в одном из $\mathfrak{A}_s$. Следовательно, мы можем считать, что $\mathfrak{B}_1 = \mathfrak{A}_1, \ldots, \mathfrak{B}_t = \mathfrak{A}_t$. Предположим теперь, что идеалы $e\mathfrak{A}$ и $e'\mathfrak{A}$ принадлежат к различным блокам. Мы можем считать, что $e\mathfrak{A} = e_1\mathfrak{A} \subseteq \mathfrak{A}_1$. Как мы видели, $e_i\mathfrak{A}e'\mathfrak{A} = 0$ при $i \leqslant n_1$. Следовательно, найдется такое $j > n_1$, что $e_j\mathfrak{A}e'\mathfrak{A} \neq 0$, и потому $e_j\mathfrak{A}$ и $e'\mathfrak{A}$ лежат в одной и той же компоненте, т. е. $e\mathfrak{A}$ и $e'\mathfrak{A}$ принадлежат разным компонентам.

Полученный выше результат справедлив, конечно, и для левых идеалов. Следующая теорема дает связь между прямыми разложениями на правые и на левые идеалы.

Теорема 36. *Если* $\mathfrak{A} = e_1\mathfrak{A} \oplus \ldots \oplus e_u\mathfrak{A}$, *где элементы* e_i *удовлетворяют условиям* (4), *то* $\mathfrak{A} = \mathfrak{A}e_1 \oplus$

$\oplus \ldots \oplus \mathfrak{A}e_u$. *Идеал* $\mathfrak{A}e_i$ *неразложим тогда и только тогда, когда неразложим идеал* $e_i\mathfrak{A}$. *Если идеалы* $e_i\mathfrak{A}$ *и* $e_j\mathfrak{A}$ *неразложимы, то они* $\mathfrak{A}$*-изоморфны тогда и только тогда, когда идеалы* $\mathfrak{A}e_i$ *и* $\mathfrak{A}e_j$ $\mathfrak{A}$*-изоморфны.*

Первая часть этой теоремы очевидна, так как условием неразложимости в обоих случаях является примитивность идемпотента e_i. Для того, чтобы доказать вторую часть, предположим сначала, что кольцо $\mathfrak{A}$ полупросто. Тогда для того, чтобы идеалы $e_i\mathfrak{A}$ и $e_j\mathfrak{A}$ были изоморфны, они должны лежать в одном неприводимом двустороннем идеале $\mathfrak{B}$ кольца $\mathfrak{A}$. Так как $e_i\mathfrak{A} \subseteq \mathfrak{B}$ тогда и только тогда, когда $\mathfrak{A}e_i \subseteq \mathfrak{B}$, то теорема в рассматриваемом случае справедлива. В общем же случае она вытекает из теоремы 33.

Отметим, что нам удалось получить обобщение всех основных теорем о структуре полупростых колец, за исключением теоремы, устанавливающей обратный изоморфизм между структурой левых идеалов и структурой правых идеалов. Класс колец, в которых имеет место эта теорема, явился объектом весьма интересных исследований Накаямы. Мы отсылаем читателя к его работам ([10], [14]) по этим вопросам.

15. Кольца главных идеалов. В этом и следующем параграфах мы покажем, следуя Асано, что основные результаты главы 3 справедливы для колец главных идеалов, в которых выполнены условия обрыва убывающих цепей для односторонних идеалов. Эти результаты будут играть важную роль в мультипликативной теории идеалов, которую мы рассмотрим в главе 6.

Под кольцом главных идеалов мы понимаем здесь кольцо с единицей, в котором каждый левый идеал является главным левым идеалом и каждый правый идеал является главным правым идеалом. Ради простоты предположим, что множество Ф эндоморфизмов пусто. Докажем сначала следующую теорему.

Теорема 37. *Если в кольце с единицей* $\mathfrak{A}$, *удовлетворяющем условиям обрыва убывающих цепей для односторонних идеалов, каждый двусторонний идеал является главным правым и главным левым идеалом то кольцо* $\mathfrak{A}$ *будет прямой суммой двусторонних идеалов, каждый из которых является примарным кольцом обладающим теми же свойствами, что и кольцо* $\mathfrak{A}$.

Пусть $\mathfrak{A}_1$ будет минимальным ненильпотентным двусторонним идеалом кольца $\mathfrak{A}$. Тогда при соответствующих элементах c и c' $\mathfrak{A}_1 = \mathfrak{A}c = c'\mathfrak{A}$ и $\mathfrak{A}c^2 = (c')^2\mathfrak{A}$ является содержащимся в $\mathfrak{A}_1$ двусторонним идеалом кольца $\mathfrak{A}$. Так как $(\mathfrak{A}c)^2 = \mathfrak{A}(c\mathfrak{A})c \subseteq \mathfrak{A}(\mathfrak{A}c)c = \mathfrak{A}c^2$, то идеал $\mathfrak{A}c^2$ не является нильпотентным. Следовательно, в силу минимальности $\mathfrak{A}_1$, имеем $\mathfrak{A}c^2 = \mathfrak{A}c = c'\mathfrak{A} = (c')^2\mathfrak{A}$. Так как условие обрыва возрастающих цепей имеет место в $\mathfrak{A}_1$, если рассматривать его как $\mathfrak{A}_l$-группу, то $\mathfrak{A}_l$-эндоморфизм $x \to xc$ взаимооднозначен в $\mathfrak{A}_1$. Следовательно, единственным элементом z из $\mathfrak{A}_1$, для которого $zc = 0$, является $z = 0$ Таким образом, если обозначить через $\mathfrak{A}^*$ совокупность таких элементов $a^* \in \mathfrak{A}$, что $a^*c = 0$, то $\mathfrak{A}^*$ будет левым идеалом, причем $\mathfrak{A}^* \cap \mathfrak{A}_1 = 0$. Для любого элемента x кольца $\mathfrak{A}$ найдется такой элемент y, что $xc = yc^2$. Следовательно, $x = (x - yc) + yc \in \mathfrak{A}^* + \mathfrak{A}_1$, и потому $\mathfrak{A} = \mathfrak{A}_1 \oplus \mathfrak{A}^*$. Таким же образом получим, что $\mathfrak{A} = \mathfrak{A}_1 \oplus \mathfrak{A}''$, где $\mathfrak{A}''$ будет правым идеалом, состоящим из таких элементов a'', что $c'a'' = 0$. Если a'' является произвольным элементом из $\mathfrak{A}''$, то $a'' = a_1 + a^*$, где $a_1 \in \mathfrak{A}_1$ и $a^* \in \mathfrak{A}^*$. Тогда $0 = c'a'' = c'a_1 + c'a^* \in \mathfrak{A}_1 \oplus \mathfrak{A}^*$ и $c'a_1 = 0$. Следовательно, $a_1 = 0$ и $a'' = a^* \in \mathfrak{A}^*$. Таким же образом, если $a^* \in \mathfrak{A}^*$, то $a^* \in \mathfrak{A}''$, и потому $\mathfrak{A}^* = \mathfrak{A}''$ является двусторонним идеалом. Отсюда следует, что идеал $\mathfrak{A}_1$ примарен. В противном случае в $\mathfrak{A}_1$ найдется ненильпотентный двусторонний отличный от $\mathfrak{A}_1$ идеал $\mathfrak{B}_1$, что противоречит минимальности идеала $\mathfrak{A}_1$. Для того, чтобы закончить доказательство, нам понадобится

Лемма. *Пусть* $\mathfrak{A}$ *является кольцом с единицей, а* $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$ *— разложением его на двусторонние идеалы. Для того, чтобы каждый правый (левый, двусторонний) идеал кольца* $\mathfrak{A}$ *был главным правым (левым, левым и правым) идеалом, необходимо и достаточно, чтобы это имело место в каждом из идеалов* $\mathfrak{A}_i$.

Если $\mathfrak{J}_i$ является правым идеалом в $\mathfrak{A}_i$, то он будет и правым идеалом в $\mathfrak{A}$, так как $\mathfrak{A}_i\mathfrak{A}_j = 0$ при $i \neq j$. Следовательно, так как $c_i \in \mathfrak{A}_i$, то $\mathfrak{J}_i = c_i\mathfrak{A} = c_i\mathfrak{A}_i$. С другой стороны, любой правый идеал $\mathfrak{J}$ кольца $\mathfrak{A}$ имеет вид $\mathfrak{J} = \mathfrak{J}_1 \oplus \ldots \oplus \mathfrak{J}_t$, где $\mathfrak{J}_i = \mathfrak{A}_i \cap \mathfrak{J}$ является правым идеалом кольца $\mathfrak{A}_i$. Если $\mathfrak{J}_i = c_i\mathfrak{A}_i$, где $c_i \in \mathfrak{J}_i$, то $\mathfrak{J} = c_1\mathfrak{A}_1 + \ldots + c_t\mathfrak{A}_t = c\mathfrak{A}$, причем элемент $c = c_1 + \ldots + c_t$ лежит в $\mathfrak{J}$.

Из этой леммы вытекает, что определенные выше кольца $\mathfrak{A}_1$ и $\mathfrak{A}^*$ удовлетворяют тем же самым условиям, что и кольцо $\mathfrak{A}$. Если кольцо $\mathfrak{A}^*$ не примарно, то мы можем повторить этот процесс и получить разложение $\mathfrak{A}^* = \mathfrak{A}_2 \oplus \mathfrak{A}''$, где $\mathfrak{A}_2$ и $\mathfrak{A}''$ являются двусторонними идеалами кольца $\mathfrak{A}'$ и, следовательно, кольца $\mathfrak{A}$, причем идеал $\mathfrak{A}_2$ примарен. После конечного числа повторений этого процесса мы получим $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$, где идеалы $\mathfrak{A}_i$ примарны и удовлетворяют условиям теоремы.

Теорема 38. *Пусть $\mathfrak{A} = \mathfrak{B}_u$, где $\mathfrak{B}$ — вполне примарное кольцо, и $\mathfrak{A}$ удовлетворяет условиям обрыва цепей для односторонних идеалов. Предположим, что радикал $\mathfrak{R}$ кольца $\mathfrak{A}$ является главным правым идеалом и главным левым идеалом. Тогда для любого элемента w, принадлежащего $\mathfrak{R} \cap \mathfrak{B}$, но не принадлежащего $\mathfrak{R}^2 \cap \mathfrak{B}$, имеем $\mathfrak{R} = w\mathfrak{A} = \mathfrak{A}w$.*

Если $\mathfrak{R} \cap \mathfrak{B} = \mathfrak{S}$ и e_{ij} являются такими матричными единицами, что $\mathfrak{A} = \sum e_{ij}\mathfrak{B}$ и $e_{ij}b = be_{ij}$ для $b \in \mathfrak{B}$, то $\mathfrak{R} = \sum e_{ij}\mathfrak{S}$. Тогда $\mathfrak{R}^k = \sum e_{ij}\mathfrak{S}^k$ и $\mathfrak{S}^k = \mathfrak{R}^k \cap \mathfrak{B}$. Отметим далее, что если u и v являются такими элементами кольца $\mathfrak{A}$, что $\bar{uv} \equiv 1 \pmod{\mathfrak{R}}$, то $\bar{uv} = 1 - r$, где $r \in \mathfrak{R}$, и, следовательно, если $r^s = 0$, то $\bar{uv}(1 + r + r^2 + \ldots + r^{s-1}) = \bar{uv} = 1$. Очевидно, что $v \equiv \bar{v} \pmod{\mathfrak{R}}$. Так как $\mathfrak{A}/\mathfrak{R}$ является кольцом матриц над телом, то и $\bar{vu} \equiv 1 \pmod{\mathfrak{R}}$. Следовательно, найдется такой элемент v', что $v'u = 1$ и $v' \equiv \bar{v} \pmod{\mathfrak{R}}$. Отсюда следует, что $v' = v$, и u является обратимым элементом, обратным для которого будет элемент v.

После этих предварительных замечаний мы можем перейти к доказательству теоремы. Пусть $w \in \mathfrak{S}$, но $w \notin \mathfrak{S}^2$. Тогда $w = zu$, где $\mathfrak{R} = z\mathfrak{A}$. Будем рассматривать элемент u по модулю $\mathfrak{R}$. Так как $\mathfrak{A}/\mathfrak{R}$ является кольцом матриц над телом, то существуют такие обратимые по модулю $\mathfrak{R}$ элементы v_1 и v_2, что $u \equiv v_1 e_s v_2 \pmod{\mathfrak{R}}$, где $e_s = \sum_1^s e_{ii}$. Мы можем считать, что элементы v_1 и v_2 обратимы в самом кольце $\mathfrak{A}$. Таким образом, $u = v_1 e_s v_2 + r$, где $r \in \mathfrak{R}$ и $w = z(v_1 e_s v_2 + r)$, $wv_2^{-1} = (zv_1)e_s + zrv_2^{-1}$. Следовательно, $wv_2^{-1} \equiv (zv_1)e_s \pmod{\mathfrak{R}^2}$. Если мы представим wv_2^{-1} как $\sum e_{ij}w_{ij}$, где $w_{ij} \in \mathfrak{B}$, то из доказанного следует, что при $j > s$ элементы w_{ij} лежат в $\mathfrak{S}^2$. Если $v_2^{-1} = \sum e_{ij}v_{ij}$, где $v_{ij} \in \mathfrak{B}$, то при $j > s$ каждый из элементов v_{ij} лежит в $\mathfrak{S}$. В противном случае элемент v_{ij} был бы обратим, и так как $w_{ij} = wv_{ij}$, то мы получили бы, что, вопреки нашему предположению, $w \in \mathfrak{S}^2$. Мы доказали поэтому, что $v_{ij} \equiv 0 \pmod{\mathfrak{S}}$ при $j > s$. Так как элемент v обратим по модулю $\mathfrak{R}$, то это невозможно, за исключением того случая, когда $s = n$, т. е. когда $u \equiv v_1 v_2 \pmod{\mathfrak{R}}$. Так как элементы v_1 и v_2 обратимы, то отсюда следует, что и элемент u также обратим, и $\mathfrak{R} = z\mathfrak{A} = w\mathfrak{A}$. Подобно этому показываем, что $\mathfrak{R} = \mathfrak{A}w$.

Теорема 39. *При предположениях предыдущей теоремы идеалы $\mathfrak{S}^k$, $k = 0, 1, \ldots$, $(\mathfrak{S}^0 = \mathfrak{B})$ являются единственными правыми (левыми) идеалами в кольце $\mathfrak{B}$, идеалы $\mathfrak{R}^k$ — единственными двусторонними идеалами кольца $\mathfrak{A}$, и $\mathfrak{S}^k$ будет главным правым (левым) идеалом.*

Пусть b является любым отличным от нуля элементом кольца $\mathfrak{B}$. Если $b \notin \mathfrak{S}$, то элемент b обратим. Предположим теперь, что $b \in \mathfrak{S}^k$, но $b \notin \mathfrak{S}^{k+1}, k > 0$. Тогда $b \in \mathfrak{R}^k$, но $b \notin \mathfrak{R}^{k+1}$ и, следовательно, $b = w^k u$, где $w \in \mathfrak{S}$, но $w \notin \mathfrak{S}^2$. Если мы представим u в виде $u = \sum e_{ij}u_{ij}$, то получим, что $b = w^k u_{ii}$ и $w^k u_{ij} = 0$. Следовательно, мы можем заменить элемент u элементом $u_1 = u_{11}$ и получить,

что $b = w^k u_1$, где $u_1 \in \mathfrak{B}$. Тогда элемент u_1 обратим. Рассуждая подобным же образом, мы можем доказать, что $b = \bar{u}_1 w^k$, где элемент $\bar{u}_1$ обратим в $\mathfrak{B}$. Если теперь b является произвольным элементом из $\mathfrak{S}^k$, то найдется такое $l \geqslant k$, что $b \in \mathfrak{S}^l$, но $b \notin \mathfrak{S}^{l+1}$, и потому $b = w^l u_2 = w^k c$, где $c \in \mathfrak{B}$ и, подобно этому, $b = \bar{c} w^k$, где $\bar{c} \in \mathfrak{B}$. Итак, мы доказали, что $\mathfrak{S}^k = w^k \mathfrak{B} = \mathfrak{B} w^k$. Пусть теперь $\mathfrak{J}$ является правым идеалом в кольце $\mathfrak{B}$. Предположим, что $\mathfrak{J} \subseteq \mathfrak{S}^k$, но $\mathfrak{J} \not\subseteq \mathfrak{S}^{k+1}$, и пусть b является элементом из идеала $\mathfrak{J}$, не лежащим в $\mathfrak{S}^{k+1}$. Тогда $b = w^k u_1$, где элемент u_1 обратим. Следовательно, $w^k \in \mathfrak{J}$ и $\mathfrak{S}^k = \mathfrak{J}$. Так как любой двусторонний идеал $\mathfrak{B}_1$ кольца $\mathfrak{A}$ имеет вид $\sum e_{ij} \mathfrak{J}$, где $\mathfrak{J}$ является двусторонним идеалом кольца $\mathfrak{B}$, то $\mathfrak{B}_1$ должен быть одним из идеалов $\sum e_{ij} \mathfrak{S}^k = \mathfrak{N}^k$.

Докажем теперь следующую теорему.

Теорема 40. *Если $\mathfrak{B}$ является кольцом главных идеалов, то и $\mathfrak{A} = \mathfrak{B}_u$, кольцо матриц над $\mathfrak{B}$, также является кольцом главных идеалов.*

Пусть $\mathfrak{F}$ обозначает свободный $\mathfrak{B}$-модуль с u образующими. Элементами модуля $\mathfrak{F}$ являются последовательности из u элементов $(b_1, \ldots, b_u)$, где $b_i \in \mathfrak{B}$. Сопоставим с любым правым идеалом $\mathfrak{J}$ кольца $\mathfrak{A}$ множество $\mathfrak{F}(\mathfrak{J})$ элементов модуля $\mathfrak{F}$, которое состоит из столбцов матриц, входящих в идеал $\mathfrak{J}$. Очевидно, что $\mathfrak{F}(\mathfrak{J})$ является подмодулем модуля $\mathfrak{F}$ и потому, в силу доказанного на стр. 86, $\mathfrak{F}(\mathfrak{J})$ имеет $m (\leqslant u)$ образующих. Пусть этими образующими являются элементы $(b_{1j}, b_{2j}, \ldots, b_{uj})$, $j = 1, \ldots m$, и пусть b является матрицей (b_{ij}), где $b_{ij} = 0$ при $j > m$. Докажем, что $\mathfrak{J} = b\mathfrak{A}$. Заметим для этого, что если $c = \sum e_{ij} c_{ij}$ является элементом идеала $\mathfrak{J}$, то и ce_{pq} также лежит в $\mathfrak{J}$, причем q-ым столбцом матрицы ce_{pq} будет p-ый столбец матрицы c, а все остальные ее столбцы состоят из нулей. Так как столбцы матрицы b встречаются в матрицах из $\mathfrak{J}$, то матрицы $\sum_i e_{ij} b_{ij}$ входят в $\mathfrak{J}$ при $j = 1, \ldots, u$ и, следовательно,

$b = \sum_{i,j} e_{ij} b_{ij}$ также лежит в $\mathfrak{J}$. u^2 матриц be_{pq} содержат столбцы матрицы b на всех возможных местах, и, так как эти столбцы образуют базис модуля $\mathfrak{F}(\mathfrak{J})$, то любой элемент из $\mathfrak{J}$ имеет вид bv при подходящем выборе элемента $v \in \mathfrak{A}$. Подобные же рассуждения справедливы и для левых идеалов.

Пусть теперь $\mathfrak{A}$ — любое примарное кольцо с единицей, в котором выполнены условия обрыва убывающих цепей для односторонних идеалов. Предположим, что радикал кольца $\mathfrak{A}$ является главным правым и главным левым идеалом. Тогда, по теореме 39, $\mathfrak{A} = \mathfrak{B}_u$, где $\mathfrak{B}$ — вполне примарное кольцо главных идеалов. Следовательно, по теореме 40, кольцо $\mathfrak{A}$ само будет кольцом главных идеалов.

Теорема 41. *Если в примарном кольце $\mathfrak{A}$, удовлетворяющем условиям обрыва убывающих цепей односторонних идеалов, радикал $\mathfrak{N}$ является главным левым и главным правым идеалом, то $\mathfrak{A}$ является кольцом главных идеалов.*

Из этой теоремы и из теоремы 37 вытекает

Теорема 42. *Если в кольце с единицей $\mathfrak{A}$, удовлетворяющем условиям обрыва убывающих цепей односторонних идеалов, каждый двусторонний идеал является главным левым и главным правым идеалом, то $\mathfrak{A}$ является кольцом главных идеалов.*

16. Модули над кольцом главных идеалов. Мы хотим определить структуру $\mathfrak{A}$-модулей с конечным числом образующих, если кольцо $\mathfrak{A}$ имеет вид, описанный в § 15. Как обычно, мы предполагаем, что $x1 = x$ для всех x из модуля $\mathfrak{M}$, где через 1 обозначена единица кольца $\mathfrak{A}$. Так как $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$, то $\mathfrak{M} = \mathfrak{M}\mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{M}\mathfrak{A}_t$. Далее, $\mathfrak{A}_i \mathfrak{A}_j = 0$ при $i \neq j$, и, следовательно, $\mathfrak{A}_i$-подмодуль из $\mathfrak{M}\mathfrak{A}_i$ является $\mathfrak{A}$-подмодулем и $\mathfrak{A}_i$-изоморфизм подмодулей из подмодуля $\mathfrak{M}\mathfrak{A}_i$ влечет за собой их $\mathfrak{A}$-изоморфизм. Следовательно, мы можем считать, что $t = 1$, т. е., что кольцо $\mathfrak{A}$ примарно. Рассмотрим сначала случай, когда кольцо

$\mathfrak{A} = \mathfrak{B}$ вполне примарно. Тогда, если $\mathfrak{S}$ является его радикалом, и $w \in \mathfrak{S}$, но $w \notin \mathfrak{S}^2$, то, как мы видели, каждый элемент из $\mathfrak{B}$ имеет вид $uw^k = w^k u'$, где элементы u и u' обратимы. Следовательно, если (a_{ij}) является матрицей из $\mathfrak{B}_m$, то мы можем при помощи элементарных преобразований (стр. 83—84) привести ее к диагональной форме. Таким образом, существуют такие обратимые элементы u_1 и u_2 из $\mathfrak{B}_m$, что

$$u_1 (a_{ij}) u_2 = \begin{pmatrix} w^{k_1} & & & & & \\ & w^{k_2} & & & & \\ & & \cdot & & & \\ & & & \cdot & & \\ & & & & w^{k_s} & \\ & & & & & 0 \\ & & & & & & \cdot \\ & & & & & & & \cdot \\ & & & & & & & & 0 \end{pmatrix}, \qquad (7)$$

где $0 \leqslant k_1 \leqslant k_2 \leqslant \ldots < l$, если $\mathfrak{S}^l = 0$, и $\mathfrak{S}^{l-1} \neq 0$. Как мы видели в главе 3, отсюда следует, что любой $\mathfrak{B}$-модуль с конечным числом образующих разлагается в прямую сумму циклических $\mathfrak{B}$-модулей, изоморфных $\mathfrak{B}$-модулям $\mathfrak{B}/w^k\mathfrak{B} = \mathfrak{B}/\mathfrak{S}^k$. Так как отображение $x \to w^{l-k}x$ является $\mathfrak{B}$-гомоморфизмом между $\mathfrak{B}$ и $\mathfrak{S}^{l-k}$, отображающим элементы из $\mathfrak{S}^k$, и только их, в нуль, то $\mathfrak{S}^{l-k}$ и $\mathfrak{B}/\mathfrak{S}^k$ изоморфны. Но кольцо $\mathfrak{S}^{l-k}$ неразложимо, ибо в противном случае мы имели бы $\mathfrak{S}^{l-k} = \mathfrak{J}_1 \oplus \mathfrak{J}_2$, где $\mathfrak{J}_j$ были бы правыми отличными от нуля идеалами из $\mathfrak{B}$, что невозможно, так как каждый из идеалов $\mathfrak{J}_j$ является степенью идеала $\mathfrak{S}$. Таким образом, и циклические модули $\mathfrak{B}/w^k\mathfrak{B}$ неразложимы.

Пусть теперь $\mathfrak{A} = \mathfrak{B}_u = \sum e_{ij}\mathfrak{B}$, где $\mathfrak{B}$ — вполне примарное кольцо главных идеалов. Если $\mathfrak{M}$ является некоторым $\mathfrak{A}$-модулем, с образующими $x_1, x_2, \ldots, x_n$, то образующими элементами $\mathfrak{M}$, рассматриваемого как $\mathfrak{B}$-модуль, будут элементы $x_i e_{jk}$. Таким образом $\mathfrak{M}$ имеет конечное число образующих относительно $\mathfrak{B}$. Множества

$\mathfrak{M}e_{ii}$ являются $\mathfrak{B}$-модулями, так как $e_{ii}b = be_{ii}$ для всех $b \in \mathfrak{B}$, и эти модули $\mathfrak{B}$-изоморфны, ибо, как легко проверить, соответствие $x \to xe_{1i}$ является $\mathfrak{B}$-изоморфизмом между $\mathfrak{M}e_{11}$ и $\mathfrak{M}e_{ii}$. Очевидно, что $\mathfrak{M} = \mathfrak{M}e_{11} \oplus \ldots \oplus \mathfrak{M}e_{uu}$. Рассмотрим подмодуль $\mathfrak{M}e_{11}$. Так как $\mathfrak{B}$ является кольцом главных идеалов, то $\mathfrak{M}e_{11}$ является $\mathfrak{B}$-модулем с конечным числом образующих. Следовательно, по нашему предположению, мы можем написать: $\mathfrak{M}e_{11} = \mathfrak{M}^{(1)} \oplus \ldots \oplus \mathfrak{M}^{(g)}$, где $\mathfrak{M}^{(j)}$ является $\mathfrak{B}$-модулем, порожденным элементом y_j. В силу отмеченного изоморфизма, мы имеем $\mathfrak{M}e_{ii} = \mathfrak{M}^{(1)}e_{1i} \oplus \ldots \oplus \mathfrak{M}^{(g)}e_{1i}$, где модуль $\mathfrak{M}^{(j)}e_{1i}$ цикличен и порождается элементом $y_j e_{1i}$. Отсюда следует, что элементы y_j являются образующими элементами модуля $\mathfrak{M}$ относительно $\mathfrak{A}$. Предположим теперь, что $y_1a_1 + \ldots + y_ra_r = 0$ при $a_j = \sum e_{ik}b_{ik}^{(j)}$. Так как $y_j e_{11} = y_j$, то мы имеем:

$$0 = (y_1 e_{11} a_1 + \ldots + y_g e_{11} a_g)\, e_{pp} =$$
$$= (y_1 b_{1p}^{(1)} + \ldots + y_g b_{1p}^{(g)})\, e_{1p}, \quad p = 1, 2, \ldots$$

Отсюда следует, что $b_{1p}^{(j)} = 0$ и, следовательно, $y_g a_g = 0$. Таким образом, $\mathfrak{M} = (y_1) \oplus \ldots \oplus (y_g)$, где через (y_j) обозначен циклический $\mathfrak{A}$-модуль, порожденный элементом y_j. Тем самым доказана

Теорема 43. *Если $\mathfrak{A}$ является кольцом главных идеалов, удовлетворяющим условиям обрыва убывающих цепей односторонних идеалов, то каждый $\mathfrak{A}$-модуль с конечным числом образующих является прямой суммой циклических $\mathfrak{A}$-модулей.*

Наши рассуждения показывают также, что если $\mathfrak{M}$ является неразложимым $\mathfrak{A}$-модулем, то $\mathfrak{M}e_{11}$ является неразложимым $\mathfrak{B}$-модулем. В самом деле, если $\mathfrak{M}e_{11} = \mathfrak{M}' \oplus \mathfrak{M}''$, то мы можем разложить $\mathfrak{M}'$ и $\mathfrak{M}''$ на циклические модули $\mathfrak{M}^{(j)}$, $j = 1, 2, \ldots, g$, $g \geqslant 2$, и тогда получится разложение $\mathfrak{M}$ на g циклических $\mathfrak{A}$-модулей. С другой стороны, предположим, что $\mathfrak{M}e_{11}$ является неразложимым $\mathfrak{B}$-модулем. Если $\mathfrak{M} = \mathfrak{M}' \oplus \mathfrak{M}''$, то мы можем записать, что $\mathfrak{M}' = \mathfrak{M}'e_{11} \oplus \ldots \oplus \mathfrak{M}'e_{uu}$, $\mathfrak{M}'' = \mathfrak{M}''e_{11} \oplus \ldots \oplus \mathfrak{M}''e_{uu}$

и получить прямое разложение модуля $\mathfrak{M}$ на $2u$ компонент. Однако, так как $\mathfrak{M} = \mathfrak{M}e_{11} \oplus \ldots \oplus \mathfrak{M}e_{uu}$, и модули $\mathfrak{M}e_{ii}$ неразложимы, то мы приходим к противоречию с теорией Крулля-Шмидта.

Если $\mathfrak{M} = (y_1)$ является неразложимым $\mathfrak{B}_u$-модулем, то можно предположить, что $y_1 e_{11} = y_1$ и что y_1 порождает неразложимый $\mathfrak{B}$-модуль. Тогда, рассматривая множество элементов a из $\mathfrak{A} = \mathfrak{B}_u$, аннулирующих элемент y_1, получаем, что (y_1) $\mathfrak{A}$-изоморфен $\mathfrak{A}/\mathfrak{J}$, где $\mathfrak{J}$ обозначает правый идеал, порожденный элементами e_{ij} при $i > 1$ и элементами $e_{ij}w^k$. Если мы применим $\mathfrak{A}$-гомоморфизм $x \to e_{11}w^{l-k}x$, то сможем доказать, что модуль $\mathfrak{A}/\mathfrak{J}$ и, следовательно, (y_1) изоморфен идеалу $e_{11}\mathfrak{R}^{l-k}$. Теперь так же, как и в главе 3, назовем *границей* некоторого $\mathfrak{A}$-модуля $\mathfrak{M}$ двусторонний идеал кольца $\mathfrak{A}$, состоящий из таких элементов d, что $xd = 0$ для всех $x \in \mathfrak{M}$. Для модулей граница может обращаться в нулевой идеал. Легко видеть, что границей (y_1) (или $e_{11}\mathfrak{R}^{l-k}$) является $\mathfrak{R}^k$. Следовательно, если кольцо $\mathfrak{A}$ примарно, то для того, чтобы два неразложимых $\mathfrak{A}$-модуля были изоморфны, необходимо и достаточно, чтобы они обладали одинаковыми границами. Из разложения $\mathfrak{M} = \mathfrak{M}\mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{M}\mathfrak{A}_t$ видно, однако, что этот результат справедлив для произвольных колец главных идеалов $\mathfrak{A}$ и, наконец, по теореме Крулля-Шмидта, мы получаем следующий общий критерий:

Теорема 44. *Если $\mathfrak{A}$ является кольцом главных идеалов, то для $\mathfrak{A}$-изоморфизма двух $\mathfrak{A}$-модулей с конечным числом образующих необходимо и достаточно, чтобы совокупность границ неразложимых компонент, которые встречаются в разложении одного из модулей, совпадала с совокупностью границ, встречающихся при разложении другого модуля.*

Большинство результатов главы 3 может теперь быть доказано для рассматриваемых здесь колец. Упомянем, например, следующую теорему, которая нам позже понадобится.

Теорема 45. *Если $\mathfrak{M}$ является неразложимым $\mathfrak{A}$-модулем и $\mathfrak{Q}$ — его границей, то $\mathfrak{A} = \mathfrak{A}/\mathfrak{Q}$ является примарным кольцом. Если e является показателем радикала кольца $\overline{\mathfrak{A}}$, то $\mathfrak{M}$ имеет длину e. Неразложимый $\mathfrak{A}$-модуль обладает только одним композиционным рядом.*

Доказательство предоставляется читателю.

Отметим, что если $\mathfrak{o}$ является произвольной областью главных идеалов, а $\mathfrak{J}$ — отличным от нуля двусторонним идеалом кольца $\mathfrak{o}$, то $\mathfrak{o}/\mathfrak{J}$ будет кольцом главных идеалов, в котором выполнены оба условия обрыва цепей односторонних идеалов. Следовательно, если $\mathfrak{M}$ — ограниченный $\mathfrak{o}$-модуль в смысле главы 3 и $\mathfrak{J}$ — граница для $\mathfrak{M}$, то $\mathfrak{M}$ будет $(\mathfrak{o}/\mathfrak{J})$-модулем, и потому результаты, касающиеся ограниченных $\mathfrak{o}$-модулей, являются следствиями развитой нами сейчас теории. Впрочем, проще обратиться к результатам главы 3.

17. Проективные и аффинные представления группы. В заключение этой главы мы рассмотрим некоторые приложения развиваемой до сих пор теории. Мы начнем с проблемы представлений групп.

Хорошо известно, что проективное пространство $\mathfrak{P}$ размерности $(n-1) \geqslant 3$ может рассматриваться как система одномерных подпространств $\{x\alpha\}$ соответствующим образом выбранного n-мерного векторного пространства $\mathfrak{M}$ над телом Φ. k-мерные подпространства в $\mathfrak{M}$ соответствуют $(k-1)$-подпространствам в $\mathfrak{P}$. Известно также, что коллинеации, или, как их иначе называют, проективные преобразования пространства $\mathfrak{P}$, т. е. сохраняющие инцидентности взаимнооднозначные преобразования пространства $\mathfrak{P}$, индуцируются невырождающимися полулинейными преобразованиями пространства $\mathfrak{M}$ над Φ. Два полулинейных преобразования T_1 и T_2 дают один и тот же результат в $\mathfrak{P}$ тогда и только тогда, когда $T_1 = T_2\mu$, где $\mu \in \Phi$. Полная проективная группа изоморфна поэтому $\mathfrak{S}/\Phi^*$, где через $\mathfrak{S}$ обозначена группа невырождающихся полулинейных преобразований, а через Φ^* — совокупность отображений вида $x \to x\mu$, где $\mu \neq 0$ и лежит в Φ [1]).

[1]) Так как здесь групповая операция обозначается как умножение, то мы будем употреблять термины произведение, степень и т. д.

Напомним также, что коллинеации, которые порождаются перспективами, являются единственными коллинеациями, для которых соответствующие полулинейные преобразования индуцируют внутренние автоморфизмы в Ф. Мы будем называть такие коллинеации *специальными*.

Рассмотрим следующую проблему: Даны группа $\mathfrak{g} = (1, s, t, \ldots)$ и проективное пространство $\mathfrak{P}$; определить гомоморфные отображения $\mathfrak{g}$ в группу коллинеаций пространства $\mathfrak{P}$. Такие гомоморфизмы называются *проективными представлениями* группы $\mathfrak{g}$. Два представления $s \to c_s$ и $s \to d_s$ называются *эквивалентными* (*строго эквивалентными*), если существует такая коллинеация (специальная коллинеация) $u \to u'$, что $(uc_s)' = u'd_s$, или, если обозначить $u \to u'$ через f, $d_s = f^{-1}c_s f$.

Если перенести это на пространство $\mathfrak{M}$, то мы получим следующую формулировку: Проективное представление группы $\mathfrak{g}$ соответствует такому отображению $s \to T_s$, где T_s является невырожденным полулинейным преобразованием в $\mathfrak{M}$, что

$$T_s T_t = T_{st}\rho_{s,t}, \quad \rho_{s,t} \in \Phi.$$

Если $\bar{s}$ обозначает автоморфизм тела Ф, определенный преобразованием T_s, то

$$\xi^{\bar{s}\,\bar{t}} = \rho_{s,t}^{-1}\,\xi^{\overline{st}}\rho_{s,t} \tag{8}$$

для всех $\xi \in \Phi$. Таким образом, (называя фактор-группу группы всех автоморфизмов тела Ф по нормальному делителю, состоящему из внутренних автоморфизмов, *группой внешних автоморфизмов* тела Ф), мы видим, что соответствие $s \to \bar{s}$ определяет гомоморфное отображение группы $\mathfrak{g}$ на подгруппу группы внешних автоморфизмов тела Ф. Отсюда следует, что подмножество $\mathfrak{h}$, состоящее из тех элементов h группы $\mathfrak{g}$, для которых T_h является специальной коллинеацией, является нормальным делителем группы $\mathfrak{g}$. Множество $\mathfrak{p} = \{\rho_{s,t}\}$ мы будем называть *системой факторов* представления. Из ассоциативного закона вытекают условия:

$$\rho_{s,\,tu}\rho_{t,\,u} = \rho_{st,\,u}\rho_{s,t}^{\bar{u}}. \tag{9}$$

Проективные представления $s \to T_s$ и $s \to U_s$ эквивалентны, если существует такое невырождающееся полулинейное преобразование A, автоморфизмом которого является $\bar{a}$, и элементы μ_s, что

$$U_s = A^{-1}T_s A\mu_s = A^{-1}\left(T_s \mu_s^{\bar{a}^{-1}}\right)A.$$

Мы получим строгую эквивалентность, если преобразование A может быть выбрано линейным. Если s' является автоморфизмом, определенным преобразованием U_s, $\sigma_{s,t}$ — —системой факторов представления $s \to U_s$, то мы получаем необходимые условия для эквивалентности:

$$s' = \bar{a}^{-1}\bar{s}\bar{a}\mu_s, \quad \sigma_{s,t} = \mu_{s,t}^{-1}\rho_{s,t}^{\bar{a}}\mu_s^{\bar{a}^{-1}\bar{t}\,\bar{a}}\mu_t, \tag{10}$$

где в первом равенстве μ_s обозначает внутренний автоморфизм $\xi \to \mu_s^{-1}\xi\mu_s$. Необходимыми условиями для строгой эквивалентности являются

$$s' = \bar{s}\mu_s, \quad \sigma_{s,t} = \mu_{st}^{-1}\rho_{s,t}\mu_s^{\bar{t}}\mu_t. \tag{11}$$

Если тело Ф коммутативно, то единственным внутренним автоморфизмом является тождественное отображение. Следовательно, соответствие $s \to \bar{s}$ будет гомоморфным отображением группы $\mathfrak{g}$ на подгруппу группы автоморфизмов поля Ф. Строго эквивалентные представления обладают одинаковыми автоморфизмами в Ф.

Важный класс проективных отображений образуют отображения, для которых система факторов имеет вид $\rho_{s,t} = 1$. В этом случае мы имеем $T_{st} = T_s T_t$, и соответствие $s \to \bar{s}$ является гомоморфизмом. Мы назовем представления такого типа *аффинными представлениями* и будем определять эквивалентность двух таких представлений условием $U_s = A^{-1}T_s A$, где A является линейным преобразованием (т. е $\mu_s = 1$). Наконец, мы можем наложить добавочное условие, предположив, что $\bar{s}$ является тождественным автоморфизмом для всех s. Тогда T_s будет линейным преобразованием. Если при

этом тело Ф коммутативно, то мы получаем классический случай, которому посвящена весьма обширная литература.

В дальнейшем будем предполагать, что группа $\mathfrak{g}$ конечна. Пусть r является ее порядком и p характеристикой Ф. Мы хотим доказать следующую теорему.

Теорема 46. *Если* $p \nmid r$ **), то любое проективное представление группы* $\mathfrak{g}$ *вполне приводимо.*

Под полной приводимостью мы понимаем полную приводимость $\mathfrak{M}$ относительно множества эндоморфизмов $\{\Phi, T_1, T_s, \ldots\}$. Пусть $\mathfrak{N}$ является подпространством пространства $\mathfrak{M}$, инвариантным относительно всех преобразований T_s, и пусть $\mathfrak{N}^*$ — его любое дополнительное подпространство, т. е. пусть $\mathfrak{M} = \mathfrak{N} \oplus \mathfrak{N}^*$. Мы хотим показать, что можно выбрать $\mathfrak{N}^*$ таким образом, чтобы оно также было инвариантно относительно всех преобразований T_s. Если $x \in \mathfrak{M}$, то мы можем представить его в виде $x = y + y^*$, где $y \in \mathfrak{N}$ и $y^* \in \mathfrak{N}^*$. Отображение $x \to y = xD$, определенное этим разложением, является тогда таким идемпотентным линейным преобразованием, что $\mathfrak{M}D = \mathfrak{N}$. Но любое линейное преобразование, отображающее $\mathfrak{M}$ в $\mathfrak{N}$ и являющееся тождественным преобразованием в $\mathfrak{N}$, идемпотентно. Следовательно, если преобразования $D_1, \ldots, D_m$ обладают этим свойством, и $p \nmid m$, то и $\frac{1}{m}(D_1 + \ldots + D_m)$ обладает этим свойством. Таким образом, и $E = \frac{1}{r}\left(\sum_{s \in \mathfrak{g}} T_s^{-1} D T_s\right)$ обладает этим же свойством, так как отображения $T_s^{-1} D T_s$ линейны, $\mathfrak{M} T_s^{-1} D T_s \subseteq \mathfrak{N} T_s = \mathfrak{N}$ и $y T_s^{-1} D T_s = y$ при всех $y \in \mathfrak{N}$. Но

$$T_t^{-1} E T_t = \frac{1}{r} \sum_s T_t^{-1} T_s^{-1} D T_s T_t = \frac{1}{r} \sum_s \rho_{s,t}^{-1} T_{st}^{-1} D T_{st} \rho_{s,t} = E,$$

*) p не делит r. (*Прим. пер.*)

так как $T_{s^{-1}}^{-1} D T_{s^{-1}}$ коммутирует с $\rho_{s,t}$, и st пробегает всю группу $\mathfrak{g}$, когда s пробегает ее. Таким образом, E, а, следовательно, и $1 - E$ коммутирует со всеми T_s. Тогда $\mathfrak{M} = \mathfrak{M}E \oplus \mathfrak{M}(1-E) = \mathfrak{N} \oplus \mathfrak{N}'$, и $\mathfrak{N}'$ остается инвариантным относительно всех T_s.

18. Скрещенные произведения. Предыдущая теорема может быть усилена, если заменить предположение $p \nmid r$ более слабым $p \nmid q$, где q обозначает порядок нормального делителя $\mathfrak{h}$, состоящего из таких элементов h, для которых автоморфизм $\bar{h}$ является внутренним. Для того, чтобы доказать это, а также и для других целей, введем некоторое кольцо $\mathfrak{A}$, определенное при помощи $\mathfrak{g}$, Ф, соответствия $s \to \bar{s} = s^H$ и системы факторов ρ. Нам нет необходимости предполагать, что $\bar{s}$ и ρ получаются из проективного представления, а достаточно лишь считать, что они удовлетворяют условиям (8) и (9), что $\rho_{s,t} \neq 0$. Элементами кольца $\mathfrak{A} = \Phi(\mathfrak{g}, H, \rho)$ будут выражения вида $\sum_{s \in \mathfrak{g}} t_s \xi_s$, где ξ_s пробегают Ф. Мы считаем, что $\sum t_s \xi_s = \sum t_s \eta_s$ тогда и только тогда, когда для всех s $\xi_s = \eta_s$, и определяем

$$\sum t_s \xi_s + \sum t_s \eta_s = \sum t_s (\xi_s + \eta_s),$$
$$\left(\sum t_s \xi_s\right)\left(\sum t_t \eta_t\right) = \sum_{s,t} t_{st} \rho_{s,t} \xi^{\bar{s}} \eta_t.$$

Легко проверить, что $\mathfrak{A}$ действительно будет кольцом. Мы будем называть его *скрещенным произведением* тела Ф и группы $\mathfrak{g}$ при соответствии H и системе факторов ρ.

Из условий, наложенных на ρ, следует, в частности, что $\rho_{s,1}\rho_{1,1} = \rho_{s,1}\rho_{s,1}^{\bar{1}}$. Следовательно, $\rho_{s,1}^{\bar{1}} = \rho_{1,1}$, $\rho_{1,1}^{\bar{1}} = \rho_{1,1}$ и $\rho_{s,1} = \rho_{1,1}$. Таким же образом получаем, что $\rho_{1,s} = \rho_{1,1}^{\bar{s}}$. Отметим также, что $\xi^{\bar{1}} = \rho_{1,1}^{-1} \xi \rho_{1,1}$. Отсюда следует, что элемент $t_1 \rho_{1,1}^{-1}$ является единицей 1 в кольце $\mathfrak{A}$ и что элементы 1ξ образуют подтело кольца $\mathfrak{A}$, кото-

рое мы можем идентифицировать с телом Ф. Можно считать, что $t_s \equiv t_s 1$, где 1 является единицей тела Ф. Тогда любой элемент кольца $\mathfrak{A}$ имеет вид $\sum t_s \xi_s$, где теперь $t_s \xi_s$ обозначает произведение t_s на элемент ξ_s из Ф. Кольцо $\mathfrak{A}$ является векторным пространством над Ф относительно эндоморфизмов $x \to x\xi$. Так как каждый элемент кольца $\mathfrak{A}$ может быть единственным образом представлен в виде $\sum t_s \xi_s$, то $(\mathfrak{A} : \Phi) = r$. Отметим, что

$$\xi t_s = t_s \overline{\xi^s}, \qquad t_s t_t = t_{st} \rho_{s,t}.$$

Подобно этому, эндоморфизмы $x \to \xi x \equiv x\xi'$ образуют обратно изоморфное телу Ф тело Ф′, и мы имеет также $(\mathfrak{A} : \Phi') = r$. Так как правые (левые) идеалы кольца $\mathfrak{A}$ являются подпространствами над Ф (Ф′), то в кольце $\mathfrak{A}$ выполнены оба условия обрыва цепей правых (левых) идеалов.

Если $s \to T_s$ является проективным представлением группы $\mathfrak{g}$ в пространстве $\mathfrak{M}$ над Ф с соответствием $s \to \bar{s}$ и системой факторов ρ, то соответствие $\sum t_s \xi_s \to \sum T_s \xi_s$ является представлением кольца $\mathfrak{A}$ при помощи эндоморфизмов модуля $\mathfrak{M}$, при котором 1 отображается в единичный эндоморфизм. Если два $\mathfrak{A}$-модуля, определенных таким образом, будут $\mathfrak{A}$-изоморфны, то соответствующие проективные представления строго эквивалентны. Обратно, если мы имеем такое представление кольца $\mathfrak{A}$ эндоморфизмами в $\mathfrak{M}$, что $1 \to 1$, то $\mathfrak{M}$ может рассматриваться как векторное пространство относительно эндоморфизмов из $\Phi \subseteq \mathfrak{A}$. Если $(\mathfrak{M} : \Phi)$ конечно и элементу t_s соответствует преобразование T_s, то мы получим проективное представление $s \to T_s$ группы $\mathfrak{g}$, имеющее то же самое соответствие и ту же систему факторов, что и $\mathfrak{A}$. Таким образом, теория представлений кольца $\mathfrak{A}$ тесно связана с теорией проективных представлений группы $\mathfrak{g}$, обладающих тем же соответствием и той же системой факторов.

Пусть $\mathfrak{B}$ обозначает подкольцо кольца $\mathfrak{A}$, состоящее из элементов вида $\sum_{h \in \mathfrak{h}} t_h \xi_h$. Тогда $\mathfrak{B}$ является скрещенным произведением тела Ф и группы $\mathfrak{h}$ с системой факторов $\rho_{h,k}$ и соответствием $h \to \bar{h}$. Пусть элементы $1, u, \ldots, w$ будут представителями смежных классов из $\mathfrak{g}/\mathfrak{h}$. Тогда, если $s \in \mathfrak{g}$, то $s = uh$, где $h \in \mathfrak{h}$. Следовательно, $t_s = t_u t_h \rho_{u,h}^{-1} = t_u b$, где $b \in \mathfrak{B}$. Отсюда следует, что элементы кольца $\mathfrak{A}$ могут быть представлены в виде $\sum t_u b_u$, где $b_u \in \mathfrak{B}$ и суммирование производится по представителям $1, u, \ldots$. Это представление единственно. В самом деле, если $\sum t_u b_u = 0$, то мы подставим $b_u = \sum t_h \xi_{h,u}$ и получим $\sum t_{uh} \rho_{u,h} \xi_{h,u} = 0$. Так как r элементов uh различны между собою, то $\rho_{u,h} \xi_{h,u} = 0$, $\xi_{h,u} = 0$ и, следовательно, $b_u = 0$. Теперь, $t_s^{-1} = (\rho_{1,1} \rho_{s^{-1},s})^{-1} t_{s^{-1}}$ и потому

$$t_s^{-1} t_h t_s = (\rho_{1,1} \rho_{s^{-1},s})^{-1} t_{s^{-1}} t_h t_s =$$
$$= (\rho_{1,1} \rho_{s^{-1},s})^{-1} t_{s^{-1} h s} \rho_{s^{-1}, hs} \overline{\rho^{s}_{s^{-1},h}} =$$
$$= t_{s^{-1} h s} \left(\rho_{1,1}^{\overline{s^{-1} h s}} \rho_{s^{-1},s}^{\overline{s^{-1} h s}} \right)^{-1} \rho_{s^{-1}h,\,s} \rho^{s}_{s^{-1},\,h}$$

лежит в $\mathfrak{B}$. Следовательно, отображение $b \to t_s^{-1} b t_s \equiv b^s$ является автоморфизмом в $\mathfrak{B}$. Используя этот автоморфизм, мы можем написать:

$$(t_u b_u)(t_v b_v) = t_{uv} \rho_{u,v} b_u^{v'} b_v.$$

Мы можем теперь доказать следующую теорему.

Теорема 47. *Для того, чтобы $\mathfrak{A}$ было полупростым кольцом, необходимо и достаточно, чтобы кольцо $\mathfrak{B}$ было полупростым.*

Пусть $\mathfrak{S}$ является радикалом кольца $\mathfrak{B}$. Так как автоморфизм $b \to t_s^{-1} b t_s$ отображает нильпотентный идеал в нильпотентный идеал, то $t_s^{-1} \mathfrak{S} t_s \subseteq \mathfrak{S}$. Отсюда следует, что совокупность $\mathfrak{N}$ элементов вида $\Sigma t_u s_u$, где $s_u \in \mathfrak{S}$, образует двусторонний идеал в $\mathfrak{A}$. Так как $\mathfrak{N} \supseteq \mathfrak{S}$, то он содержит и $\mathfrak{A}\mathfrak{S}\mathfrak{A}$. С другой стороны, по определению, $\mathfrak{N} \subseteq \mathfrak{A}\mathfrak{S}$. Следовательно, $\mathfrak{N} = \mathfrak{A}\mathfrak{S} = \mathfrak{A}\mathfrak{S}\mathfrak{A}$. Тогда $\mathfrak{N}^k = \mathfrak{A}\mathfrak{S}^k$, и потому идеал $\mathfrak{N}$ нильпотентен. Следовательно, если $\mathfrak{S} \neq 0$, то радикал $\mathfrak{N}$ кольца $\mathfrak{A}$ отличен от нуля. Предпо-

ложим теперь, что $\mathfrak{S}=0$. Мы хотим показать, что если $\mathfrak{J}$ является любым отличным от нуля двусторонним идеалом кольца $\mathfrak{A}$, то $(\mathfrak{B}\cap\mathfrak{J})\neq 0$. Пусть $z=t_u b_u+\dots$ является отличным от нуля элементом идеала $\mathfrak{J}$, который имеет наименьшее число не равных нулю коэффициентов b_u. Если $b\in\mathfrak{B}$, то элементы $zb=t_u b_u b+\dots$ и $bz=t_u b^{u'} b_u+\dots$ лежат в $\mathfrak{J}$. Отметим какой-либо индекс u, для которого $b_u\neq 0$. Так как элементы $b^{u'}$ пробегают все кольцо $\mathfrak{B}$, то коэффициенты c_u элементов $t_u c_u+\dots$ идеала $\mathfrak{J}$, имеющих тот же вид, что и z[1]), образуют двусторонний отличный от нуля идеал $\mathfrak{J}_u$. Так как кольцо $\mathfrak{B}$ полупростое, то идеал $\mathfrak{J}_u$ обладает единицей e_u, и e_u лежит в центре кольца $\mathfrak{B}$. Мы можем теперь предположить, что $z=t_u e_u+\dots$. Покажем, что $z=t_u e_u$. В самом деле, предположим, что $z=t_u e_u+t_v b_v+\dots$, где $b_v\neq 0$. Для любого ξ из Φ элемент $\xi z-z\xi^{\bar u}=t_v(\xi^{\bar v}b_v-b_v\xi^{\bar u})+\dots$ лежит в $\mathfrak{B}$ и обладает меньшим числом отличных от нуля членов, чем z. Этот элемент отличен от нуля, когда $\xi^{\bar v}b_v\neq b_v\xi^{\bar u}$. Теперь, если $b_v=\sum t_h\beta_h$, то

$$\xi^{\bar v}b_v-b_v\xi^{\bar u}=\sum t_h(\xi^{\bar v\bar h}\beta_h-\beta_h\xi^{\bar u}).$$

Так как $b_v\neq 0$, то найдется $\beta_h\neq 0$, и потому $\xi^{\bar u}=\beta_h^{-1}\xi^{\bar v\bar h}\beta_h$. Это справедливо для всех ξ, и отсюда вытекает, что u получается из v умножением на внутренний автоморфизм, вопреки нашему предположению, что u и v принадлежат различным смежным классам по $\mathfrak{h}$ в группе $\mathfrak{g}$. Следовательно, $z=t_u e_u$ и $t_u^{-1}z=e_u$ является отличным от нуля элементом из $\mathfrak{B}\cap\mathfrak{J}$. Если положить $\mathfrak{J}=\mathfrak{N}$, то мы получаем, что $\mathfrak{N}=0$, так как $(\mathfrak{B}\cap\mathfrak{N})$ является нильпотентным идеалом в $\mathfrak{B}$.

Мы видели, что если $p\nmid q$, где q является порядком $\mathfrak{h}$, то любое представление кольца $\mathfrak{B}$, при котором $1\to 1$, вполне приводимо. Если мы применим это к регулярному представлению в $\mathfrak{B}_r$, то увидим, что структура правых идеалов кольца $\mathfrak{B}$ вполне приводима. Следовательно, кольцо $\mathfrak{B}$ полупросто, и мы доказали следующие теоремы.

[1]) Т. е. такие, что $c_v=0$, если $b_v=0$.

Теорема 48. *Скрещенное произведение $\mathfrak{A}$ полупросто, если $p\nmid q$, где q является порядком $\mathfrak{h}$.*

Теорема 49. *Проективное представление $s\to T_s$ конечной группы вполне приводимо, если $p\nmid q$, где q обозначает порядок подгруппы, состоящей из таких элементов h, для которых T_h является специальной коллинеацией.*

Из доказательства главной теоремы следует также

Теорема 50. *Если $\mathfrak{h}=(1)$, то кольцо $\mathfrak{A}$ просто.*

В самом деле, в этом случае $\mathfrak{B}=\Phi$, и потому $\mathfrak{S}=0$. Тогда, если $\mathfrak{J}$ является отличным от нуля двусторонним идеалом кольца $\mathfrak{A}$, то $\Phi\cap\mathfrak{J}$ является отличным от нуля идеалом тела Φ, и потому $\Phi\cap\mathfrak{J}=\Phi$. Таким образом, $\mathfrak{J}$ содержит 1, и потому $\mathfrak{J}=\mathfrak{A}$.

Предположим, что $\mathfrak{h}=(1)$. Тогда, если для всех ξ имеем $(\sum t_s\beta_s)\xi=\xi(\sum t_s\beta_s)$, то $\xi^{\bar s}\beta_s=\beta_s\xi$. Следовательно, если $\beta_s\neq 0$, то $\xi^{\bar s}=\beta_s\xi\beta_s^{-1}$. Таким образом, $s=1$, и мы доказали, что все элементы кольца $\mathfrak{A}$, коммутирующие со всеми элементами тела Φ, лежат в Φ. Следовательно, центр кольца $\mathfrak{A}$ лежит в центре Γ тела Φ. Если $\gamma\in\Gamma$, то из того, что для всех s $\gamma t_s=t_s\gamma$, вытекает, что $\gamma\in\Gamma_0$, где через Γ_0 обозначено подполе поля Γ, состоящее из элементов, остающихся инвариантными при всех автоморфизмах $\bar s$. Отсюда следует, что Γ_0 является центром кольца $\mathfrak{A}$. Если $\Phi=\Gamma$, т. е., если Φ является полем, то как известно, $(\Gamma:\Gamma_0)=r$[1]). Следовательно, $(\mathfrak{A}:\Gamma_0)=r^2$.

Предположим теперь, что не только $\mathfrak{h}=(1)$, но и $\rho_{s,t}=1$. Так как кольцо $\mathfrak{A}$ просто, то $\mathfrak{A}=\mathfrak{J}_1\oplus\dots\oplus\mathfrak{J}_n$, где $\mathfrak{J}_i$ являются между собой $\mathfrak{A}$-изоморфными неприводимыми правыми идеалами. $\mathfrak{A}$-изоморфизм между правыми идеалами будет, в частности, взаимнооднозначным линейным отображением этих идеалов друг на друга, если рассматривать их как подпространства векторного пространства $\mathfrak{A}$ над Φ. Следовательно, $(\mathfrak{J}_j:\Phi)=(\mathfrak{J}_k:\Phi)=m$ и $r=(\mathfrak{A}:\Phi)=um$. Пусть теперь $\mathfrak{J}$ будет правым идеалом,

[1]) Это будет доказано в следующем отделе.

состоящим из кратных ea элемента $e=\sum t_s$. Так как $et_s=a_s$ то $ea=e\alpha$ при соответствующем $\alpha\in\Phi$. Следовательно $(\mathfrak{J}:\Phi)=1$, и потому идеал $\mathfrak{J}$ неприводим. Тогда $(\mathfrak{J}_j:\Phi)=(\mathfrak{J}:\Phi)=1$, и $r=u$. Отсюда следует, что $\mathfrak{A}=\Psi_r$, где Ψ является телом. Тело Ψ содержит центр Γ_0 кольца $\mathfrak{A}$, и так как $(\mathfrak{A}:\Psi)=r^2$, то отсюда следует, что если $\Phi=\Gamma$, то $\Psi=\Gamma_0$.

Теорема 51. *Если* $\mathfrak{A}=\Phi(\mathfrak{g},H,1)$ *и* $\mathfrak{h}=1$, *то* $\mathfrak{A}=\Psi_r$, *где* Ψ *является телом, и степень* r *равна порядку группы* $\mathfrak{g}$. *Если при этом тело* $\Phi=\Gamma$ *коммутативно, то* $\mathfrak{A}=\Gamma_{0r}$, *где через* Γ_0 *обозначен центр кольца* $\mathfrak{A}$.

19. Теория Галуа тел. Пусть Φ является произвольным телом, а $\mathfrak{G}=(1,S,\ldots,U)$ — конечной группой, состоящей из r внешних автоморфизмов тела Φ. Подмножество инвариантных элементов (т. е. таких элементов, что $\alpha^S=\alpha$) образует подтело Φ_0 тела Φ. Обозначим множество левых (правых) умножений в Φ, соответствующих элементам из Φ_0, через Φ_0' (Φ_0), а множество эндоморфизмов вида $\sum S\xi_S$, ($\sum S\xi_S'$), где ξ_S (ξ_S') является правым (левым) умножением на элемент ξ_S из Φ, через $(\Phi,\mathfrak{G})$ $((\Phi',\mathfrak{G}))$. Отметим, что $\xi S=S\xi^S$. Следовательно, если $\mathfrak{A}$ является скрещенным произведением тела Φ и абстрактной группы $\mathfrak{g}$, изоморфной группе $\mathfrak{G}$, определенным при помощи изоморфизма $s\to S$ и системы факторов $\rho_{s,t}=1$, то соответствие $\sum t_s\xi_s\to\sum S\xi_s$ будет представлением кольца $\mathfrak{A}$ эндоморфизмами аддитивной группы тела Φ. Так как кольцо $\mathfrak{A}$ просто, то это представление взаимно однозначно. Следовательно, в силу последней теоремы, кольцо $(\Phi,\mathfrak{G})=\Psi_r$, где Ψ является телом.

Если $\alpha\neq0$ и β лежат в Φ, то найдется такой элемент ξ из Φ, что $\alpha\xi=\beta$. Отсюда следует, что $(\Phi,\mathfrak{G})=\Psi_r$ является неприводимым множеством эндоморфизмов и, следовательно, в силу $\mathfrak{A}$-изоморфизма любых двух неприводимых $\mathfrak{A}$-групп, существуют r таких элементов $\alpha_1,\ldots,\alpha_r$ тела Φ, что каждый элемент из Φ может быть представлен одним и только одним образом в виде $\alpha_1\psi_1+\ldots+\alpha_r\psi_r$, где

$\psi\in\Psi$. Для того, чтобы доказать это еще раз непосредственно, предположим, что E_{ij} образуют матричный базис в Ψ_r, и выберем E_{pp} и α таким образом, чтобы $\alpha E_{pp}\neq0$. Тогда нетрудно видеть, что элементы $\alpha_1=\alpha E_{p1},\ldots,\alpha_r=\alpha E_{pr}$ независимы над Ψ. Так как любой элемент β представим в виде $\beta=(\alpha E_{pp})\sum E_{ij}\psi_{ij}$ при соответственно выбранных ψ_{ij}, то мы имеем $\beta=\alpha_1\psi_{p1}+\ldots+\alpha_r\psi_{pr}$.

Пусть Ψ' будет кольцом линейных преобразований ψ' аддитивной группы тела Φ над Ψ, определенных равенствами $\alpha_i\psi'\equiv\alpha_i\psi$. Мы видели в главе 2, что Φ является r-мерным пространством над Ψ', Ψ' — совокупностью всех эндоморфизмов, коммутирующих с эндоморфизмами из Ψ_r, и Ψ_r — совокупностью всех линейных преобразований Φ над Ψ'.

Напомним теперь, что $\Psi_r=(\Phi,\mathfrak{G})$. Если A является эндоморфизмом, коммутирующим со всеми эндоморфизмами из Φ, то A будет левым умножением, например, $\xi\to\alpha\xi\equiv\xi\alpha'$. Если при этом A коммутирует со всеми элементами из $\mathfrak{G}$, то $(\alpha\xi)^S=\alpha^S\xi^S=\alpha\xi^S$ и $\alpha'\in\Phi_0'$. Подобным же образом мы можем рассмотреть Φ_0 и $(\Phi',\mathfrak{G})$ и получить следующую теорему.

Теорема 52. *Пусть* Φ *является произвольным телом,* $\mathfrak{G}$ *— конечной группой, состоящей из* r *внешних автоморфизмов тела* Φ, *и* Φ_0 *— подтелом, состоящим из инвариантных элементов. Тогда размерность* Φ *над* Φ_0' (Φ *над* Φ_0) *равна* r, *и* $(\Phi,\mathfrak{G})$ $((\Phi',\mathfrak{G}))$ *будет полной совокупностью линейных преобразований* Φ *над* Φ_0' (Φ *над* Φ_0).

Предположим, что V является любым автоморфизмом в Φ, оставляющим неизменными элементы из Φ_0. Тогда V будет линейным преобразованием пространства Φ над Φ_0' и, следовательно, $V=\sum S\xi_S$. Для каждого эндоморфизма η мы имеем $\eta V-V\eta^V=0$. Тогда, $\sum S(\eta^S\xi_S-\xi_S\eta^V)=0$ и, если $\xi_S\neq0$, то $\eta^V=\xi_S^{-1}\eta^S\xi_S$. Так как ни один из автоморфизмов $S\neq1$ не является внутренним, это может иметь место только для одного S, и потому $V=S\xi$. Так

как V является автоморфизмом, то $\xi = 1$, и $V = S \in \mathfrak{G}$. В частности, для любого элемента γ из Φ, коммутирующего со всеми элементами из Φ_0, внутренний автоморфизм $\eta \longrightarrow \gamma^{-1}\eta\gamma$ лежит в $\mathfrak{G}$ и, следовательно, является тождественным отображением. Таким образом, γ лежит в центре тела Φ.

Если $\mathfrak{H}$ является подгруппой группы $\mathfrak{G}$, то мы обозначим подтело, состоящее из элементов, остающихся инвариантными при преобразованиях из $\mathfrak{H}$, через $\Phi(\mathfrak{H})$, а, если Σ — подтело, лежащее между Φ_0 и Φ, то мы обозначим подгруппу группы $\mathfrak{G}$, оставляющую элементы из Σ неподвижными, через $\mathfrak{G}(\Sigma)$. Отметим, что $\Phi_0 \subseteq \Phi(\mathfrak{H})$, $\Phi(\mathfrak{G}) = \Phi_0$, $\Phi(1) = \Phi$. Следующая теорема является фундаментальной в теории Галуа.

Теорема 53. *Соответствия* $\mathfrak{H} \longrightarrow \Phi(\mathfrak{H})$ *и* $\Sigma \longrightarrow \mathfrak{G}(\Sigma)$ *являются взаимно обратными. Каждое из них является взаимнооднозначным соответствием между подгруппами группы* $\mathfrak{G}$ *и телами* Σ, *лежащими между* Φ_0 *и* Φ. *Размерность* $(\Phi : \Sigma) = (\Phi : \Sigma')$ *равна порядку группы* $\mathfrak{G}(\Sigma)$, *и* $(\Sigma : \Phi_0) = (\Sigma : \Phi_0')$ *равна индексу* $\mathfrak{G}(\Sigma)$.

Пусть $\mathfrak{H}$ является подгруппой группы $\mathfrak{G}$ и $\Phi(\mathfrak{H})$ — множеством инвариантных элементов. Если автоморфизм $S \in \mathfrak{G}$ оставляет неподвижными элементы из $\Phi(\mathfrak{H})$, то, как мы видели, $S \in \mathfrak{H}$. Таким образом, $\mathfrak{G}(\Phi(\mathfrak{H})) = \mathfrak{H}$. Предположим теперь, что задано тело Σ, $\Phi_0 \subseteq \Sigma \subseteq \Phi$, и пусть Δ является множеством линейных преобразований в Φ над Σ'. Тогда $\Delta \subseteq (\Phi, \mathfrak{G})$. Если $\sum S\xi_S \in \Delta$, и μ' является любым элементом из Σ', то

$$\sum S\mu'^S\xi_S = \mu' \sum S\xi_S = (\sum S\xi_S)\mu' = \sum S\mu'\xi_S,$$

где μ'^S обозначает левое умножение, соответствующее элементу μ^S. Следовательно, $\sum S(\mu'^S - \mu')\xi_S = 0$. Если $S \in \mathfrak{G}(\Sigma) = \mathfrak{H}$, то $\mu'^S = \mu'$. Предположим теперь, что $S \notin \mathfrak{H}$. Мы утверждаем, что тогда $\xi_S = 0$. В самом деле,

пусть $\xi_S \neq 0$. Так как $S \notin \mathfrak{H}$, то найдется такой элемент μ, что $\mu^S \neq \mu$. С другой стороны,

$$S(\mu'^S - \mu')\xi_S + T(\mu'^T - \mu')\xi^T + \ldots = 0.$$

Очевидно, что это соотношение не может быть приведено к $S(\mu'^S - \mu')\xi_S = 0$, и поэтому мы можем предположить, что $\xi_T \neq 0$ и $\mu'^T - \mu' \neq 0$, так что T также не лежит в $\mathfrak{H}$. Тогда, умножая слева на эндоморфизм η и справа на $\xi_S^{-1}\eta^S\xi_S$ и вычитая, мы получаем

$$T(\mu'^T - \mu')(\eta^T\xi_T - \xi_T\xi_S^{-1}\eta^S\xi_S) + \ldots = 0.$$

Так как автоморфизм TS^{-1} не является внутренним, то мы можем выбрать η таким образом, чтобы $\eta^T\xi_T - \xi_T\xi_S^{-1}\eta^S\xi_S$ не равнялось нулю. Если мы продолжим этот процесс, то получим, наконец, один член $U(\mu'^U - \mu')\zeta_U = 0$, причем $U \notin \mathfrak{H}$, и $\zeta_U \neq 0$. Так как это исключено, то мы доказали, что $\xi_S = 0$ при всех S, не входящих в $\mathfrak{H}$. Следовательно, Δ состоит из преобразований вида $\sum_{S \in \mathfrak{H}} S\xi_S$, и Σ' является совокупностью всех эндоморфизмов, коммутирующих с эндоморфизмами из Δ. С другой стороны, форма элементов, входящих в Δ, показывает, что эти преобразования являются в точности такими ζ', что $\zeta \in \Phi(\mathfrak{H})$. Следовательно, $\Phi(\mathfrak{G}(\Sigma)) = \Sigma$. Соотношения, касающиеся размерностей, следуют из теоремы 1.

Если $\Sigma = \Phi(\mathfrak{H})$, то $\Sigma^S = \Phi(S^{-1}\mathfrak{H}S)$. Следовательно, $\mathfrak{H}$ будет нормальным делителем тогда и только тогда, когда Σ преобразуется в себя всеми элементами из $\mathfrak{G}$. Если $1, S, \ldots$ являются представителями смежных классов по $\mathfrak{H}$, то преобразования, индуцированные в Σ этими элементами, различны между собой и зависят лишь от смежных классов. Их совокупность образует группу $\overline{\mathfrak{G}} \cong \mathfrak{G}/\mathfrak{H}$. Элементы S, не лежащие в $\mathfrak{H}$, индуцируют внешние автоморфизмы в Σ. В самом деле, если S является внутренним автоморфизмом тела Σ, то существует такой внут-

ренний автоморфизм A тела Φ, что SA оставляет элементы тела Σ инвариантными. Тогда $SA = H \in \mathfrak{G}(\Sigma) = \mathfrak{H}$ и $S^{-1}H = A$ является внутренним автоморфизмом, вопреки нашему предположению.

Если тело Φ коммутативно и $\xi \in \Phi$, то пусть $\xi, \ldots, \xi^T$ являются всеми сопряженными с ξ элементами поля Φ. Коэффициенты при степенях t элемента

$$(t-\xi)\ldots(t-\xi^T)$$

остаются инвариантными при автоморфизмах из $\mathfrak{G}$ и потому принадлежат подполю Φ_0. Таким образом, каждый элемент из Φ удовлетворяет сепарабельному уравнению * с коэффициентами из Φ_0. Так как, $\xi, \ldots, \xi^T$ лежат в Φ, то отсюда следует, что Φ является нормальным сепарабельным полем над Φ_0. Для того, чтобы дополнить теорию Галуа конечных расширений полей в этом направлении, было бы необходимо доказать обратную теорему: если Φ является конечным нормальным сепарабельным расширением поля Φ_0, то элементы из Φ_0 будут единственными элементами, остающимися инвариантными при автоморфизмах из группы Галуа поля Φ над Φ_0.

20. Конечные группы полулинейных преобразований. Рассмотрим такое проективное представление конечной группы, что $\rho = 1$ и группа $\mathfrak{h} = (1)$. Таким образом, кольцо $\Phi(\mathfrak{g}, H, 1) = \Psi_r$ полулинейных преобразований T_s образует группу, и автоморфизмы $\bar{s} \in \Phi$, связанные с преобразованиями T_s, различны между собой и являются внешними. Пусть $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \bigoplus \mathfrak{M}_m$ будет разложением векторного пространства на неприводимые Ψ_r-модули. В каждом из $\mathfrak{M}_i$ мы можем выбрать такой вектор x_i, что $y_i = x_i(\sum t_s) = x_i(\sum T_s) \neq 0$. Тогда $y_i T_s = y_i$, и так как каждый элемент из $\mathfrak{M}_i$ имеет вид $y_i(\sum T_s \xi_s) = y_i \xi$, то $\mathfrak{M}_i$ имеет размерность 1 над Φ. Следовательно, элементы $y_1, \ldots, y_m$ образуют базис модуля $\mathfrak{M}$ над Φ.

* = уравнению первого рода. *(Прим. пер.)*

Пусть $\mathfrak{M}_0$ является множеством векторов из $\mathfrak{M}$, остающихся инвариантными при всех преобразованиях T_s. $\mathfrak{M}_0$ будет векторным пространством над Φ_0, где через Φ_0 обозначено подтело тела Φ, состоящее из элементов, остающихся инвариантными при всех автоморфизмах $\bar{s}$. Если $y = \sum y_i \xi_i \in \mathfrak{M}_0$, то $\xi_i^{\bar{s}} = \xi_i \in \Phi_0$ и, следовательно, элементы $y_1, \ldots, y_m$ образуют также базис $\mathfrak{M}_0$ над Φ_0.

Теорема 54. *Пусть $\mathfrak{M}$ является m-мерным векторным пространством над телом Φ, и $T_1 = 1$, $T_s, \ldots, T_u$ — конечной группой полулинейных преобразований, причем индуцированные ими автоморфизмы $\bar{1}, \bar{s}, \ldots, \bar{u}$ различны между собой и являются внешними автоморфизмами. Если $\mathfrak{M}_0$ состоит из множества векторов, остающихся инвариантными при всех преобразованиях T_s, а Φ_0 является подтелом, инвариантным относительно всех $\bar{s}$, то $\mathfrak{M}_0$ будет векторным пространством размерности m над Φ_0, и расширение $\mathfrak{M}_0\Phi = \mathfrak{M}$.*

Если мы применим соответствие между полулинейными преобразованиями и матрицами, то можем сформулировать эту теорему также следующим образом:

Теорема 55. *Если $\mathfrak{G}$ является конечной группой внешних автоморфизмов $\bar{1}, \bar{s}, \ldots, \bar{u}$ тела Φ, а τ_s — такими матрицами с элементами из Φ, что $\tau_1 = 1$ и $\tau_t \tau_s^{\bar{t}} = \tau_{ts}$, то существует такая невырождающаяся матрица α, что $\tau_s = \alpha^{-1}\alpha^{\bar{s}}$ для всех $\bar{s}$.*

Глава 5

АЛГЕБРЫ НАД ПОЛЕМ

1. Прямое произведение алгебр. В предыдущей главе мы интересовались главным образом абсолютными свойствами колец. Роль множества эндоморфизмов Ф была скорее второстепенной, его единственной функцией было ослаблять предположение, что в совокупности идеалов кольца выполнены условия обрыва цепей. Полученные результаты применялись, в частности, к алгебрам. С другой стороны, большая часть теории алгебр посвящена их «относительным» свойствам — существенно зависящим от того поля Ф, над которым определена алгебра. Эта часть теории является предметом настоящей главы. Мы рассмотрим сначала теорию простых алгебр, а позже снова займемся изучением произвольных алгебр.

Рассмотрения главы 4 были в значительной мере посвящены аддитивным разложениям кольца в прямую сумму его идеалов. В теории простых алгебр основную роль играет один тип мультипликативных разложений — прямое произведение. Пусть $\mathfrak{A}$ является алгеброй над полем Ф, и $(\mathfrak{A}:\Phi)=n<\infty$ [1]. Мы будем говорить, что $\mathfrak{A}$ является *прямым произведением* $\mathfrak{A}_1\times\mathfrak{A}_2$ подалгебр $\mathfrak{A}_1$ и $\mathfrak{A}_2$, если выполнены следующие условия:

1. Элементы из $\mathfrak{A}_1$ коммутируют с элементами из $\mathfrak{A}_2$.
2. $\mathfrak{A}=\mathfrak{A}_1\mathfrak{A}_2=\mathfrak{A}_2\mathfrak{A}_1$.
3. $(\mathfrak{A}:\Phi)=(\mathfrak{A}_1:\Phi)(\mathfrak{A}_2:\Phi)$.

[1] В этой главе мы предполагаем, что наши алгебры имеют конечную размерность. Некоторые из результатов справедливы и при менее ограничительных условиях, но, ради простоты, мы не будем указывать на эти обобщения теории.

Очевидно, что в этих условиях можно поменять местами $\mathfrak{A}_1$ и $\mathfrak{A}_2$, так что если $\mathfrak{A}=\mathfrak{A}_1\times\mathfrak{A}_2$, то и $\mathfrak{A}=\mathfrak{A}_2\times\mathfrak{A}_1$. Ввиду условия 3, ясно, что это понятие существенно зависит от поля Ф. Так, например, если Σ является собственным подполем поля Ф, и $\mathfrak{A}=\mathfrak{A}_1\times\mathfrak{A}_2$, если рассматривать их как алгебры над Ф, то $\mathfrak{A}\neq\mathfrak{A}_1\times\mathfrak{A}_2$, если рассматривать их как алгебры над Σ. В самом деле, тогда $(\mathfrak{A}:\Sigma)(\Phi:\Sigma)=(\mathfrak{A}_1:\Sigma)(\mathfrak{A}_2:\Sigma)$.

Пусть элементы $y_1,\ldots,y_{n_1}$ образуют базис алгебры $\mathfrak{A}_1$ над полем Ф с таблицей умножения $y_iy_{i'}=\sum y_p\gamma_{pii'}^{(1)}$, и элементы $z_1,\ldots,z_{n_2}$ образуют базис алгебры $\mathfrak{A}_2$ над Ф с таблицей умножения $z_jz_{j'}=\sum z_q\gamma_{qjj'}^{(2)}$, где $\gamma_{pii'}^{(1)}$ и $\gamma_{qjj'}^{(2)}$ лежат в Ф. Тогда каждый элемент b из $\mathfrak{A}_1$ имеет вид $\sum y_i\varphi_i$, и каждый элемент c из $\mathfrak{A}_2$ имеет вид $\sum z_j\varphi_j$. В силу условия 2, каждый элемент a кольца $\mathfrak{A}$ является суммой вида $\sum a_k^{(1)}a_k^{(2)}$, где $a_k^{(i)}\in\mathfrak{A}_i$. Следовательно, $a=\sum y_iz_j\varphi_{ij}$. В силу условия 3, элементы $x_{ij}=y_iz_j$, $i=1,\ldots,n_1$; $j=1,\ldots,n_2$, линейно независимы и потому образуют базис алгебры $\mathfrak{A}$ над полем Ф. Таблица умножения $x_{ij}x_{i'j'}=\sum x_{pq}\gamma_{pii'}^{(1)}\gamma_{qjj'}^{(2)}$ этого базиса определяется выбором базисов y_i и z_j подалгебр $\mathfrak{A}_1$ и $\mathfrak{A}_2$. Следовательно, если $\mathfrak{B}$ является второй алгеброй над Ф, $\mathfrak{B}=\mathfrak{B}_1\times\mathfrak{B}_2$ и $a_1\to a_1^S$, $a_2\to a_2^S$ являются изоморфизмами над Ф, соответственно, между алгебрами $\mathfrak{A}_1$ и $\mathfrak{B}_1$, $\mathfrak{A}_2$ и $\mathfrak{B}_2$, то $\sum x_{ij}\varphi_{ij}\to\sum x_{ij}^S\varphi_{ij}$, где $x_{ij}=y_iz_j$, $x_{ij}^S=y_i^Sz_j^S$ будет изоморфизмом между алгебрами $\mathfrak{A}$ и $\mathfrak{B}$ над полем Ф. В этом смысле алгебра $\mathfrak{A}=\mathfrak{A}_1\times\mathfrak{A}_2$ определяется своими компонентами $\mathfrak{A}_1$ и $\mathfrak{A}_2$. Более обще, если $\mathfrak{B}$ является некоторой алгеброй, содержащей такие две подалгебры $\mathfrak{B}_1$ и $\mathfrak{B}_2$, что $b_1b_2=b_2b_1$ для $b_i\in\mathfrak{B}_i$, и если $a_i\to a_i^S$ является гомоморфным отображением $\mathfrak{A}_i$ на $\mathfrak{B}_i$, то $\sum x_{ij}\varphi_{ij}\to\sum x_{ij}^S\varphi_{ij}$, $x_{ij}^S=y_i^Sz_j^S$, будет гомоморфным отображением $\mathfrak{A}_1\times\mathfrak{A}_2$ на $\mathfrak{B}_1\mathfrak{B}_2=\mathfrak{B}_2\mathfrak{B}_1$.

Если $a=\sum y_iz_j\varphi_{ij}$, то $a=y_1a_1^{(2)}+\ldots+y_{n_1}a_{n_1}^{(2)}$, где $a_l^{(2)}\in\mathfrak{A}_2$, и так как элементы y_iz_j линейно независимы,

то из $a=0$ вытекает, что все $a_i^{(2)}=0$. Теперь, если $y_1, \ldots, y_r$ является любым множеством линейно независимых элементов из $\mathfrak{A}_1$, мы можем добавить к ним элементы $y_{r+1}, \ldots, y_{n_1}$ так, чтобы получить базис алгебры $\mathfrak{A}_1$ над Ф. Таким же образом, если элементы $z_1, \ldots, z_s$ из $\mathfrak{A}_2$ линейно независимы, то мы можем присоединить к ним еще элементы и получить базис алгебры $\mathfrak{A}_2$. Отсюда следует, что элементы $y_i z_j$, $i=1, \ldots, r$; $j=1, \ldots, s$ линейно независимы. Как частный случай этого мы получаем, что если $\mathfrak{B}_i$ является подалгеброй в $\mathfrak{A}_i$, то $\mathfrak{B}_1\mathfrak{B}_2=\mathfrak{B}_2\mathfrak{B}_1=\mathfrak{B}_1 \times \mathfrak{B}_2$. Если $\mathfrak{A}_1=\mathfrak{A}_{11} \times \mathfrak{A}_{12}$, то $\mathfrak{A}=(\mathfrak{A}_{11} \times \mathfrak{A}_{12}) \times \mathfrak{A}_2=\mathfrak{A}_{11} \times (\mathfrak{A}_{12} \times \mathfrak{A}_2)$. Таким образом, для прямого умножения имеет место ассоциативный закон. Отметим также, что размерность пересечения $\mathfrak{A}_1 \cap \mathfrak{A}_2$ над полем Ф не больше 1. В самом деле, если a и b являются элементами из $\mathfrak{A}_1 \cap \mathfrak{A}_2$, то элементы a^2, ab, ba и b^2 линейно зависимы, так как $ab=ba$. Если подалгебры $\mathfrak{A}_1$ и $\mathfrak{A}_2$ обладают единицами 1_1 и 1_2 соответственно, то $1=1_1 1_2$ будет единицей алгебры $\mathfrak{A}$. Но $1_1=1_1(1_1 1_2)=1_1 1_2=1$ и также $1_2=1$. Следовательно, $\mathfrak{A}_1 \cap \mathfrak{A}_2$ состоит из кратных 1α, где $\alpha \in \Phi$.

Пусть теперь $\mathfrak{A}_1$ и $\mathfrak{A}_2$ являются произвольными алгебрами с единицами. Предположим, что $y_1=1_1, y_2, \ldots, y_{n_1}$ и $z_1=1_2, z_2, \ldots, z_{n_2}$ являются базисами этих алгебр, а $y_i y_{i'}=\sum y_p \gamma_{pii'}^{(1)}$ и $z_j z_{j'}=\sum z_q \gamma_{qjj'}^{(2)}$ — таблицами умножения этих базисов. Определим алгебру $\mathfrak{A}$, воспользовавшись базисом x_{ij}, $i=1, \ldots, n_1$, $j=1, \ldots, n_2$, подчиненным таблице умножения $x_{ij}x_{i'j'}=\sum x_{pq}\gamma_{pii'}^{(1)}\gamma_{qjj'}^{(2)}$. Легко проверить, что подмножество элементов алгебры $\mathfrak{A}$ вида $\sum x_{i1}\varphi_i$, где $\varphi_i \in \Phi$, образует подалгебру $\bar{\mathfrak{A}}_1 \subseteq \mathfrak{A}$, изоморфную $\mathfrak{A}_1$, а подмножество элементов вида $\sum x_{1j}\varphi_j$ образует подалгебру $\bar{\mathfrak{A}}_2$, изоморфную алгебре $\mathfrak{A}_2$. Из таблицы умножения мы получаем, что $x_{i1}x_{1j}=x_{ij}=x_{1j}x_{i1}$ и $(x_{i1}x_{1j})(x_{i'1}x_{1j'})=(x_{i1}x_{i'1})(x_{1j}x_{1j'})$. Из последнего соотношения и из выполнения ассоциативного закона в алгебрах $\bar{\mathfrak{A}}_1$ и $\bar{\mathfrak{A}}_2$ следует, что в алгебре $\mathfrak{A}$ также выполнен ассоциативный закон. Очевидно, что $\mathfrak{A}=\bar{\mathfrak{A}}_1 \times \bar{\mathfrak{A}}_2$. Мы сконструировали, таким образом, алгебру $\mathfrak{A}$, которая является прямым произведением алгебр, изоморфных данным алгебрам $\mathfrak{A}_1$ и $\mathfrak{A}_2$. Как мы видели выше, $\mathfrak{A}$ является единственной с точностью до изоморфизма алгеброй, обладающей этим свойством. Мы будем идентифицировать алгебры $\mathfrak{A}_i$ и $\bar{\mathfrak{A}}_i$ и называть $\mathfrak{A}$ прямым произведением ($\mathfrak{A}=\mathfrak{A}_1 \times \mathfrak{A}_2$) алгебр $\mathfrak{A}_1$ и $\mathfrak{A}_2$. В этом рассуждении не является существенным сделанное нами ограничение, что алгебры $\mathfrak{A}_i$ обладают единицами. В самом деле, мы можем присоединить единицу 1_i к алгебре $\mathfrak{A}_i$, получая при этом алгебру $\mathfrak{B}_i$. Мы образуем $\mathfrak{B}_1 \times \mathfrak{B}_2$ и будем считать подалгебру $\mathfrak{A}_1 \times \mathfrak{A}_2$ прямым произведением алгебр $\mathfrak{A}_1$ и $\mathfrak{A}_2$.

2. Расширение поля. Алгебра, тесно связанная с прямым произведением, получается следующим образом. Пусть $\mathfrak{A}$ является алгеброй с базисом $x_1, \ldots, x_n$ над полем Ф, а $\mathfrak{B}$ — алгеброй с единицей над Ф. Рассмотрим множество выражений вида $x_1 b_1 + \ldots + x_n b_n$, где $b_i \in \mathfrak{B}$. Два таких выражения $\sum x_i b_i$ и $\sum x_i b_i'$ будем считать равными тогда и только тогда, когда $b_i=b_i'$. Определим

$$\sum x_i b_i + \sum x_i b_i' = \sum x_i (b_i + b_i'),$$
$$\left(\sum x_i b_i\right)\left(\sum x_j b_j'\right) = \sum x_k \sum b_i b_j' \gamma_{kij},$$

если $x_i x_j = \sum x_k \gamma_{kij}$, где $\gamma_{kij} \in \Phi$. Нетрудно видеть, что определенная таким образом система является кольцом. Оно не зависит от выбора базиса x_i в том смысле, что кольца, определенные при помощи различных базисов, изоморфны между собой. Следовательно, мы можем обозначить это кольцо через $\mathfrak{A}_\mathfrak{B}$.

Так как кольцо $\mathfrak{B}$ содержит единицу, то оно содержит изоморфное с Ф подполе 1Φ, состоящее из элементов вида 1α. Кольцо $\mathfrak{A}_\mathfrak{B}$ содержит подмножество элементов вида $\sum x_i (1\alpha_i)$, которые образуют подкольцо, изоморфное кольцу $\mathfrak{A}$. Мы идентифицируем это кольцо с $\mathfrak{A}$. Теперь определение $\sum (x_i b_i) b = \sum x_i (b_i b)$ превращает кольцо $\mathfrak{A}_\mathfrak{B}$

в $\mathfrak{B}$-модуль. Из этого определения мы получаем, что

$$u1 = u, \quad (uv)b = u(vb), \quad (ub)x = (ux)b$$

для всех u, v из $\mathfrak{A}_\mathfrak{B}$, всех x из $\mathfrak{A}$ и всех b из $\mathfrak{B}$. Таким образом, операция в модуле коммутирует с левыми и с правыми умножениями на элементы из $\mathfrak{A}$. Так как $\mathfrak{A}_\mathfrak{B}$ является $\mathfrak{B}$-модулем, и $\mathfrak{B} \supseteq 1\Phi$, то $\mathfrak{A}_\mathfrak{B}$ является Φ-модулем (мы полагаем $u\alpha = u(1\alpha)$). Если $\alpha \in \Phi$ и элементы u и v произвольны, то $(uv)\alpha = u(v\alpha) = (u\alpha)v$. Следовательно, $\mathfrak{A}_\mathfrak{B}$ является алгеброй над Φ. Если элементы $y_1, \ldots, y_m$ образуют базис алгебры $\mathfrak{B}$ над полем Φ, то mn элементов $x_i y_j$ образуют базис алгебры $\mathfrak{A}_\mathfrak{B}$ над Φ.

Эти свойства характеризуют $\mathfrak{A}_\mathfrak{B}$. В самом деле, предположим, что $\mathfrak{K}$ является такой алгеброй, что

1. $\mathfrak{K}$ содержит $\mathfrak{A}$.

2. $\mathfrak{K}$ является $\mathfrak{B}$-модулем, где $\mathfrak{B}$ — алгебра с единицей 1, и $ua = u(1a)$ для всех $u \in \mathfrak{K}$ и всех $a \in \Phi$. $\mathfrak{K}$ порождается алгеброй $\mathfrak{A}$ в том смысле, что наименьший $\mathfrak{B}$-подмодуль модуля $\mathfrak{K}$, содержащий $\mathfrak{A}$, совпадает с самим $\mathfrak{K}$.

3. $(uv)b = u(vb)$, $(ub)x = (ux)b$ для всех u, $v \in \mathfrak{K}$, всех $x \in \mathfrak{A}$ и всех $b \in \mathfrak{B}$.

4. $(\mathfrak{K} : \Phi) = (\mathfrak{A} : \Phi)(\mathfrak{B} : \Phi)$.

Тогда, если $x_1, \ldots, x_n$ образуют базис алгебры $\mathfrak{A}$ над Φ, то элементы из $\mathfrak{K}$ могут быть одним и только одним образом представлены в виде $\sum x_i b_i$, где $b_i \in \mathfrak{B}$. Если $x_i x_j = \sum x_k \gamma_{kij}$, то

$$(\sum x_i b_i)(\sum x_j b_j') = \sum (x_i b_i)(x_j b_j') = \sum ((x_i b_i) x_j) b_j' =$$
$$= \sum ((x_i x_j) b_i) b_j' = \sum x_k \gamma_{kij} b_i b_j' = \sum x_k b_i b_i' \gamma_{kij}.$$

Следовательно, $\mathfrak{K}$ изоморфно $\mathfrak{A}_\mathfrak{B}$.

Если кольцо $\mathfrak{A}$ обладает единицей 1, то $(\sum x_i b_i)1 = \sum (x_i b_i)1 = \sum (x_i 1) b_i = \sum x_i b_i$, и, подобно этому, $1(\sum x_i b_i) = \sum x_i b_i$. Следовательно, 1 является единицей алгебры $\mathfrak{A}_\mathfrak{B}$. Множество элементов вида $1b$ образует подалгебру, изоморфную $\mathfrak{B}$. Отметим, что $u(1b) = ub$ и что $(1b)x = xb = x(1b)$, если $u \in \mathfrak{A}_\mathfrak{B}$ и $x \in \mathfrak{A}$. Следовательно, если идентифицировать алгебру, состоящую из элементов вида $1b$ с $\mathfrak{B}$, то мы можем написать, что $\mathfrak{A}_\mathfrak{B} = \mathfrak{A} \times \mathfrak{B}$.

Если $\mathfrak{A}_1$ является подалгеброй алгебры $\mathfrak{A}$, то можно предположить, что элементы $x_1, \ldots, x_r$ образуют базис алгебры $\mathfrak{A}_1$, причем $x_1, \ldots, x_n$ образуют базис алгебры $\mathfrak{A}$. Элементы $\sum_1^r x_i b_i$ образуют алгебру, и множество таких элементов является наименьшим $\mathfrak{B}$-модулем, содержащим $\mathfrak{A}_1$. Ясно, что эта алгебра изоморфна алгебре $\mathfrak{A}_{1\mathfrak{B}}$ и поэтому может быть обозначена через $\mathfrak{A}_{1\mathfrak{B}}$. Если $\mathfrak{A}_1$ является идеалом (нильпотентным идеалом) в $\mathfrak{A}$, то и $\mathfrak{A}_{1\mathfrak{B}}$ будет идеалом (нильпотентным идеалом) в $\mathfrak{A}_\mathfrak{B}$. Следовательно, если кольцо $\mathfrak{A}_\mathfrak{B}$ просто (полупросто), то и кольцо $\mathfrak{A}$ просто (полупросто).

Предположим теперь, что $\mathfrak{B} = \mathrm{P}$ является полем [1]. Тогда $(uv)\rho = u(v\rho) = (u\rho)v$ для всех u, v из $\mathfrak{A}_\mathrm{P}$ и всех ρ из P. Следовательно, мы можем рассматривать $\mathfrak{A}_\mathrm{P}$ как алгебру над полем P. Если не оговорено другое, то мы и будем на самом деле рассматривать $\mathfrak{A}_\mathrm{P}$ таким образом. Очевидно, что $(\mathfrak{A}_\mathrm{P} : \mathrm{P}) = (\mathfrak{A} : \Phi)$. Могут быть отмечены следующие правила:

$$(\mathfrak{A}_1 \oplus \mathfrak{A}_2)_\mathrm{P} = \mathfrak{A}_{1\mathrm{P}} \oplus \mathfrak{A}_{2\mathrm{P}},$$
$$(\mathfrak{A}_1 \oplus \mathfrak{A}_2)_\mathrm{P} = \mathfrak{A}_{1\mathrm{P}} \times \mathfrak{A}_{2\mathrm{P}},$$
$$(\mathfrak{A}_\mathrm{P})_\Sigma = \mathfrak{A}_\Sigma,$$

если Σ является содержащим P полем.

3. Представления матрицами и пространства представлений. Вторым важным средством в нашем изучении алгебр является теория представлений алгебры $\mathfrak{A}$ матрицами. В обычной теории мы интересовались представлениями алгебры матрицами с элементами из поля Φ. Для исследования простых алгебр нам понадобится обобщение,

[1] Следует отметить, что в определении $\mathfrak{A}_\mathfrak{B}$ не используется сделанное нами предположение о конечности базиса алгебры $\mathfrak{A}_\mathfrak{B}$. Абстрактная характеристика дается в общем случае условиями 1., 2., 3., и 4': если элементы $x_1, \ldots, x_r$ линейно независимы в $\mathfrak{A}$ и $y_1, \ldots, y_s$ линейно независимы в $\mathfrak{B}$, то rs элементов $x_i y_j$ линейно независимы в $\mathfrak{A}_\mathfrak{B}$. Расширения $\mathfrak{A}_\mathrm{P}$, когда поле P является бесконечным расширением, имеют много важных приложений.

при котором элементы матриц берутся в независимой от $\mathfrak{A}$ простой алгебре $\mathfrak{B}$. Тем не менее, прежде, чем рассмотреть этот общий случай, мы хотим подробнее исследовать более простой.

Как и в случае представления эндоморфизмами, существуют два типа представления матрицами. Во-первых, определим (обычное) *представление матрицами* алгебры $\mathfrak{A}$ над Φ, как гомоморфное отображение $a \to A$ алгебры $\mathfrak{A}$ на подалгебру алгебры матриц Φ_N: если $a \to A$ и $b \to B$, то

$$a + b \to A + B, \quad a\alpha \to A\alpha, \quad ab \to AB.$$

Таким же образом определим *обратное представление матрицами*, как обратно гомоморфное отображение $\mathfrak{A}$ на подалгебру алгебры матриц. Предположим теперь, что $\mathfrak{R}$ является коммутативной группой, удовлетворяющей следующим условиям:

1. $\mathfrak{R}$ является таким Φ-модулем, что для всех $x \in \mathfrak{R}$ и для единицы 1 из Φ имеем $x1 = x$, и кроме того, $(\mathfrak{R} : \Phi) = N$.

2. $\mathfrak{R}$ является левым $\mathfrak{A}$-модулем.

3. $(a\alpha)x = (ax)\alpha = a(x\alpha)$ для всех $a \in \mathfrak{A}$, всех $\alpha \in \Phi$ и всех $x \in \mathfrak{R}$.

Тогда $\mathfrak{R}$ будет N-мерным векторным пространством над Φ, и эндоморфизмы, соответствующие элементам a, будут линейными преобразованиями. Так как $\mathfrak{R}$ является левым $\mathfrak{A}$-модулем, то соответствие между элементом a и преобразованием a будет обратно гомоморфным отображением кольца $\mathfrak{A}$ в кольцо линейных преобразований. В силу условия 3, линейное преобразование, соответствующее $a\alpha$, является произведением линейного преобразования a и умножения на скаляр α. Следовательно, это соответствие будет обратно гомоморфным отображением алгебры $\mathfrak{A}$ на подалгебру алгебры линейных преобразований. Напомним, что соответствие между линейными преобразованиями векторного пространства и матрицами, которые они определяют относительно некоторого фиксированного базиса, является обратным изоморфизмом между этими алгебрами. Отсюда следует, что если $x_1, \ldots, x_N$ является этим базисом и $ax_i = \sum x_j \alpha_{ji}$, то соответствие между a и матрицей $A = (\alpha_{ij})$ будет представлением алгебры $\mathfrak{A}$ матрицами из Φ_N. Мы

можем также обратить порядок рассуждения и ассоциировать, таким образом, с каждым представлением алгебры $\mathfrak{A}$ матрицами группу $\mathfrak{R}$, удовлетворяющую условиям 1., 2. и 3. Будем называть такую группу *пространством представления* алгебры $\mathfrak{A}$. Подобные рассуждения справедливы и для обратных представлений. В этом случае модули должны удовлетворять условию 1. и условиям:

2′. $\mathfrak{R}$ является $\mathfrak{A}$-модулем;

3′. $x(a\alpha) = (xa)\alpha = (x\alpha)a$, где $a \in \mathfrak{A}$, $\alpha \in \Phi$, $x \in \mathfrak{R}$.

Будем называть $\mathfrak{R}$ *пространством обратного представления алгебры* $\mathfrak{A}$. Мы ограничимся только случаем обычных представлений, так как изменения, необходимые для рассмотрения обратных представлений, будут очевидны.

Напомним, что если элементы $y_1, \ldots, y_N$ образуют второй базис пространства представления $\mathfrak{R}$ и $y_i = \sum x_j \mu_{ji}$, то матрицей для a относительно этого базиса будет $M^{-1}AM$, $M = (\mu_{ij})$. Представление $a \to M^{-1}AM$ называется *подобным* представлению $a \to A$. Таким образом, пространство представления определяет класс подобных представлений матрицами. Мы будем называть два пространства представлений матрицами $\mathfrak{R}_1$ и $\mathfrak{R}_2$ *изоморфными*, если между ними существует взаимнооднозначное соответствие, являющееся в одно и то же время Φ-изоморфизмом и $\mathfrak{A}$-изоморфизмом. Если U является таким изоморфизмом и элементы $x_1, \ldots, x_N$ образуют базис $\mathfrak{R}_1$ над Φ, то элементы $z_1 = x_1U, \ldots, z_N = x_NU$ образуют базис $\mathfrak{R}_2$ над Φ. Кроме того, если $ax_i = \sum x_j \alpha_{ji}$, то и $az_i = \sum z_j \alpha_{ji}$. Таким образом, изоморфные пространства представления определяют одинаковые классы подобных представлений матрицами. Обратное также справедливо.

Будем называть представление *приводимым*, *разложимым*, *вполне приводимым*, если группа $\mathfrak{R}$ относительно эндоморфизмов из Φ и из $\mathfrak{A}$ является соответственно приводимой, разложимой, вполне приводимой. Из рассуждений § 8 главы 2 ясно, что представление приводимо тогда и только тогда, когда оно подобно представлению вида

$$\begin{pmatrix} A_1 & * \\ 0 & A_2 \end{pmatrix}. \qquad (1)$$

Представление $a \to A_1$ соответствует истинному подпространству $\mathfrak{S}$, остающемуся инвариантным относительно эндоморфизмов a. Условием для того, чтобы $\mathfrak{R}$ разлагалось в прямую сумму $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2$, где $\mathfrak{R}_i$ — инвариантные отличные от нуля подпространства, является подобие представления, определенного пространством $\mathfrak{R}$, представлению вида

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}. \tag{2}$$

Здесь $a \to A_i$ является представлением, определенным пространством представления $\mathfrak{R}_i$. Напомним также, что если $\mathfrak{R} = \mathfrak{R}_s \supset \mathfrak{R}_{s-1} \supset \ldots \supset \mathfrak{R}_1 \supset 0$ является цепью инвариантных относительно преобразований a подпространств, то наше представление подобно следующему

$$\begin{pmatrix} A_1 & & & * \\ & A_2 & & \\ & & \ddots & \\ & & & \ddots \\ 0 & & & A_s \end{pmatrix}, \tag{3}$$

где представления $a \to A_i$ связаны с пространствами $\mathfrak{R}_i/\mathfrak{R}_{i-1}$. Цепь подпространств будет композиционным рядом тогда и только тогда, когда все представления $a \to A_i$ неприводимы. Условием полной приводимости является подобие представления представлению вида (3), в котором ящички * выше «диагонали» состоят из нулей и представления $a \to A_i$ неприводимы.

Наши рассуждения приобретают гораздо более простую форму, если алгебра $\mathfrak{A}$ обладает единицей 1 и 1 отображается в единичную матрицу. Отсюда, разумеется, следует, что $1x = x$ для всех $x \in \mathfrak{R}$. Тогда $(1\alpha)x = x\alpha$. Таким образом, в этом случае достаточно рассматривать $\mathfrak{R}$ как левый $\mathfrak{A}$-модуль. С другой стороны, если $\mathfrak{R}$ является произвольным левым $\mathfrak{A}$-модулем, в котором для всех x $1x = x$, то $\mathfrak{R}$ будет левым Φ-модулем относительно операции $\alpha x \equiv (1\alpha)x$. Так как Φ коммутативно, то $\mathfrak{R}$ может также

рассматриваться как Φ-модуль, если положить $x\alpha \equiv \alpha x$. Кроме того, если размерность $(\mathfrak{R} : \Phi)$ конечна, то $\mathfrak{R}$ является пространством представления. Отметим, что условие конечности $(\mathfrak{R} : \Phi)$ эквивалентно требованию существования конечного числа образующих в $\mathfrak{R}$ над $\mathfrak{A}$. В самом деле, если элементы $y_1, \ldots, y_r$ являются образующими модуля $\mathfrak{R}$ над $\mathfrak{A}$, а элементы $a_1, \ldots, a_n$ — образующими в $\mathfrak{A}$ относительно Φ, то nr элементов $a_i y_j$ будут образующими в $\mathfrak{R}$ относительно Φ. Следовательно, конечность $(\mathfrak{R} : \Phi)$ доказана.

Если $\mathfrak{A}$ обладает единицей 1, но 1 не отображается в единичное преобразование, то мы представляем $\mathfrak{R}$ в виде $\mathfrak{R} = \mathfrak{S} \oplus \mathfrak{Z}$, где $\mathfrak{S}$ является совокупностью элементов вида $1x$, а $\mathfrak{Z}$ — совокупностью элементов вида $x - 1x$, которые аннулируются единицей. Если мы выберем базис $y_1, \ldots, y_N$ для $\mathfrak{R}$ таким образом, чтобы элементы $y_1, \ldots, y_r$ образовывали базис для $\mathfrak{S}$, а элементы $y_{r+1}, \ldots, y_N$ — базис для $\mathfrak{Z}$, то матрицей, соответствующей элементу a из $\mathfrak{A}$ относительно этого базиса, будет

$$\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}.$$

В представлении $a \to A$, связанном с пространством $\mathfrak{S}$, мы имеем $1 \to 1$, что позволяет нам и в этом случае свести исследование к исследованию левых Φ-модулей.

4. Приложение теории $\mathfrak{A}$-модулей. Пусть $\mathfrak{R}$ будет каким-либо пространством представления алгебры $\mathfrak{A}$. Множество $\mathfrak{J}x$ векторов вида bx, где x — фиксированный элемент из $\mathfrak{R}$, а b пробегает левый Φ-идеал $\mathfrak{J}$, является инвариантным подпространством в $\mathfrak{R}$. Подобно этому, пространство $\mathfrak{J}\mathfrak{S}$ векторов $b_1x_1 + \ldots + b_rx_r$, где x_i пробегают множество $\mathfrak{S}$ и b_i пробегают идеал $\mathfrak{J}$, является инвариантным подпространством. Принимая во внимание рассуждения § 12 главы 4, мы можем доказать, что, если пространство $\mathfrak{R}$ неприводимо и $\mathfrak{N}$ является радикалом алгебры $\mathfrak{A}$, то $\mathfrak{N}\mathfrak{R} = 0$. Следовательно, в этом случае $\mathfrak{R}$ будет пространством представления полупростой алгебры $\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{N}$.

Кроме того, ввиду неприводимости пространства $\mathfrak{R}$, либо $\mathfrak{A}\mathfrak{R}=0$, либо единица алгебры $\overline{\mathfrak{A}}$ является тождественным преобразованием в $\mathfrak{R}$. В первом случае пространство $\mathfrak{R}$ одномерно, а во втором (глава 4, § 12) пространство $\mathfrak{R}$ $\mathfrak{A}$-изоморфно неприводимому левому идеалу алгебры $\overline{\mathfrak{A}}$. Если $\overline{\mathfrak{A}}=\overline{\mathfrak{A}}_1\oplus\ldots\oplus\overline{\mathfrak{A}}_t$, где $\overline{\mathfrak{A}}_i$ — неприводимые двусторонние идеалы, то $\mathfrak{R}$ аннулируется всеми идеалами $\overline{\mathfrak{A}}_i$, за исключением, скажем, идеала $\overline{\mathfrak{A}}_1$. Таким образом, $\mathfrak{R}$ является левым $\overline{\mathfrak{A}}_1$-модулем. Но число таких неприводимых $\mathfrak{A}$-модулей $\mathfrak{R}$, что $\mathfrak{A}\mathfrak{R}\neq 0$, равно числу t компонент $\overline{\mathfrak{A}}_i$ алгебры $\overline{\mathfrak{A}}$, и мы можем сформулировать следующую теорему.

Теорема 1. Пусть $\mathfrak{N}$ *является радикалом алгебры* $\mathfrak{A}$, и $\overline{\mathfrak{A}}=\mathfrak{A}/\mathfrak{N}=\overline{\mathfrak{A}}_1\oplus\ldots\oplus\overline{\mathfrak{A}}_t$, *где* $\overline{\mathfrak{A}}_i$ — *простые идеалы. Тогда любое неприводимое представление* $a\to A$ *или является нулевым представлением* ($a\to 0$), *или подобно представлению, получаемому при использовании одного из неприводимых левых идеалов алгебры* $\overline{\mathfrak{A}}$ *в качестве пространства представления. Число классов подобных отличных от нуля неприводимых представлений равно числу компонент* $\overline{\mathfrak{A}}_i$.

Напомним также, что если алгебра $\mathfrak{A}$ полупроста, то любой $\mathfrak{A}$-модуль, в котором для всех x $1x=x$, вполне приводим. Если теперь $\mathfrak{R}$ является произвольным пространством представления алгебры $\mathfrak{A}$, то мы можем представить $\mathfrak{R}$ в виде $\mathfrak{R}=\mathfrak{S}\oplus\mathfrak{Z}$, где $1y=y$ для всех $y\in\mathfrak{S}$ и $1z=0$ для всех $z\in\mathfrak{Z}$. Так как $\mathfrak{S}$ является левым $\mathfrak{A}$-модулем, в котором $1y=y$, то $\mathfrak{S}$ вполне приводимо. Кроме того, $\mathfrak{Z}$ мы можем разложить на одномерные подпространства. Тем самым доказана

Теорема 2. *Каждое представление полупростой алгебры вполне приводимо.*

Специальным случаем этой теоремы является полная приводимость представления матрицами любой простой ненулевой алгебры $\mathfrak{A}$. Все неприводимые отличные от нуля представления такой алгебры подобны между собой.

Если, в частности, $\mathfrak{A}=\Phi_r$, то все отличные от нуля неприводимые представления подобны первоначальному представлению $A\to A$. Это может быть также получено, если отметить, что $\Phi_r e_{11}$ является неприводимым левым идеалом (через e_{ij} обозначены матричные единицы). Ф-базисом для этого идеала будет $x_1=e_{11},\ldots,x_r=e_{r1}$, и если $A=\sum e_{ij}\alpha_{ij}$, то $Ax_i=\sum x_j\alpha_{ji}$. Следовательно, представление, определенное этим идеалом, является первоначальным представлением $A\to A$.

5. Представление алгебры матрицами с элементами из простой алгебры. Если $\mathfrak{B}$ является произвольной алгеброй, то мы определим *представление* (*обратное представление*) алгебры $\mathfrak{A}$ *матрицами с элементами из* $\mathfrak{B}$, как гомоморфное (обратно гомоморфное) отображение алгебры $\mathfrak{A}$ на подалгебру алгебры матриц $\mathfrak{B}_N$. Как и в том специальном случае, когда $\mathfrak{B}=\Phi$, мы называем представления $a\to A_1$ и $a\to A_2$ *подобными*, если существует такая независимая от a матрица M, что $A_2=M^{-1}A_1M$. Представление $a\to A$ *приводимо*, если оно подобно представлению вида (1), и *разложимо*, если оно подобно представлению вида (2). Оно *вполне приводимо*, если оно подобно представлению вида (3), где ящички * равны нулю и представления $a\to A_i$ неприводимы. Мы ограничимся изучением представлений алгебр с единицей матрицами с элементами также из алгебры с единицей. Кроме того, мы предположим, что единица алгебры $\mathfrak{A}$ отображается в единичную матрицу. Как мы увидим, в этом случае теория обратных представлений в некотором отношении более естественна, чем теория обычных представлений. Поэтому мы будем иметь в виду главным образом первую из них, указывая лишь там, где это нужно, изменения, необходимые для обычной теории.

Мы хотим сформулировать при помощи модулей проблему представлений. Для этой цели необходимо вспомнить теорию свободных модулей, рассмотренную в главе 3, § 3. Мы будем теперь называть $\mathfrak{B}$-модуль $\mathfrak{R}$ $\mathfrak{B}$-*пространством*, если $\mathfrak{R}$ является прямой суммой конечного числа свободных модулей. Так как $\mathfrak{B}$ удовлетворяет усло-

вию обрыва возрастающих цепей идеалов, то ранг N пространства $\mathfrak{R}$ является инвариантом. Если $x_1, \ldots, x_N$ и $y_1, \ldots, y_N$ являются двумя базисами для $\mathfrak{R}$, то $y_i = \sum x_j b_{ji}$ $x_j = \sum y_i c_{ij}$, где матрицы $B = (b_{ij})$ и $C = (c_{ij})$ лежат в $\mathfrak{B}_N$. Тогда $BC = CB = 1$, так что $C = B^{-1}$. Обратно, если элементы $x_1, \ldots, x_N$ образуют базис и матрица B обратима в $\mathfrak{B}_N$, то элементы $y_i = \sum x_j b_{ji}$ образуют второй базис.

Пусть теперь a является $\mathfrak{B}$-эндоморфизмом в $\mathfrak{R}$, $x_i a = \sum x_j a_{ji}$, и $A = (a_{ij})$ лежит в $\mathfrak{B}_N$. Тогда матрица A единственным образом определяется эндоморфизмом a. Таким образом, мы получаем однозначное соответствие между алгеброй $\mathfrak{L}$ $\mathfrak{B}$-эндоморфизмов пространства $\mathfrak{R}$ и множеством матриц из $\mathfrak{B}_N$. Как и в том случае, когда $\mathfrak{B}$ является телом, мы можем показать, что это соответствие является обратным изоморфизмом между алгеброй $\mathfrak{B}$-эндоморфизмов и алгеброй $\mathfrak{B}_N$.

Определим теперь $\mathfrak{B}$-*пространство обратного представления* алгебры $\mathfrak{A}$ как коммутативную группу $\mathfrak{R}$, удовлетворяющую следующим условиям:

1. $\mathfrak{R}$ является $\mathfrak{B}$-пространством.
2. $\mathfrak{R}$ является таким $\mathfrak{A}$-модулем, что для всех $x \in \mathfrak{R}$ и для единицы 1 алгебры $\mathfrak{A}$ имеем $x\,1 = x$.
3. $(xa)\,b = (xb)\,a$, если $x \in \mathfrak{R}$, $a \in \mathfrak{A}$ и $b \in \mathfrak{B}$.
4. $1\,\alpha$ из $\mathfrak{A}$ отображается в тот же эндоморфизм, что и $1\,\alpha$ из $\mathfrak{B}$.

Теперь, в силу условия 3., эндоморфизм, соответствующий элементу a, является $\mathfrak{B}$-эндоморфизмом. Следовательно, если элементы $x_1 \ldots, x_N$ образуют $\mathfrak{B}$-базис для $\mathfrak{R}$ и $ax_i = \sum x_j a_{ji}$, то соответствие между a и матрицей $A = (a_{ij})$ из $\mathfrak{B}_N$ является кольцевым обратным гомоморфизмом. В силу условия 4., элементу $a\alpha = a(1\,\alpha)$ соответствует матрица $A(1\,\alpha) = A\alpha$, и потому мы получаем обратно гомоморфное отображение алгебры $\mathfrak{A}$ на подалгебру алгебры $\mathfrak{B}_N$. Отсюда следует, что каждое $\mathfrak{B}$-пространство обратного представления алгебры $\mathfrak{A}$ определяет обратное представление, и обратно. Снова,

как и в случае, когда $\mathfrak{B} = \Phi$, другой базис пространства $\mathfrak{R}$ определяет обратное представление, подобное обратному представлению $a \to A$. Пространства обратных представлений $\mathfrak{R}_1$ и $\mathfrak{R}_2$ будут $(\mathfrak{A},\mathfrak{B})$-изоморфны тогда и только тогда, когда они определяют одинаковые классы подобных обратных представлений.

Рассмотрим теперь алгебру $\mathfrak{A}_{\mathfrak{B}} = \mathfrak{A} \times \mathfrak{B}$. Мы видели, что если элементы $x_1 \ldots, x_n$ образуют базис пространства $\mathfrak{A}$ над Φ, то каждый элемент из $\mathfrak{A}_{\mathfrak{B}}$ может быть единственным образом представлен в виде $x_1 b_1 + \ldots + x_n b_n$, где $b_i \in \mathfrak{B}$. Таким образом, $\mathfrak{A}_{\mathfrak{B}}$ является $\mathfrak{B}$-пространством ранга n относительно правого умножения $x \to xb$, как операции модуля. Алгебра $\mathfrak{A}_{\mathfrak{B}}$ является также $\mathfrak{A}$-модулем относительно правого умножения. Следовательно, $\mathfrak{A}_{\mathfrak{B}}$ является $\mathfrak{B}$-пространством обратного представления алгебры $\mathfrak{A}$. Покажем далее, что любое $\mathfrak{B}$-пространство $\mathfrak{R}$ обратного представления будет $\mathfrak{A}_{\mathfrak{B}}$-модулем. В самом деле, пусть $\overline{\mathfrak{A}}$ обозначает совокупность эндоморфизмов, соответствующих элементам из $\mathfrak{A}$, и $\overline{\mathfrak{B}}$ — совокупность эндоморфизмов, соответствующих элементам из $\mathfrak{B}$. Так как соответствия $a \to a \in \overline{\mathfrak{A}}$ и $b \to b \in \overline{\mathfrak{B}}$ являются гомоморфизмами, то соответствие, отображающее элемент $\sum a_i b_i$ алгебры $\mathfrak{A}_{\mathfrak{B}}$ на эндоморфизм $\sum a_i b_i$ из $\overline{\mathfrak{A}}\,\overline{\mathfrak{B}} = \overline{\mathfrak{B}}\,\overline{\mathfrak{A}}$, будет гомоморфным отображением. Таким образом, $\mathfrak{R}$ является $\mathfrak{A}_{\mathfrak{B}}$-модулем. С другой стороны, каждый $\mathfrak{A}_{\mathfrak{B}}$-модуль, являющийся, если его рассматривать относительно $\mathfrak{B}$, $\mathfrak{B}$-пространством, будет $\mathfrak{B}$-пространством обратного представления алгебры $\mathfrak{A}$.

Подобным же образом можно показать, что теория обычных представлений эквивалентна теории $\mathfrak{B}$-пространств представлений, которые определяются условиями 1., 4., и

2′. $\mathfrak{R}$ является таким левым $\mathfrak{A}$-модулем, что для всех x и для единицы 1 алгебры $\mathfrak{A}$ имеем $1\,x = x$.

3′. $(ax)\,b = a\,(xb)$, если $x \in \mathfrak{R}$, $a \in \mathfrak{A}$ и $b \in \mathfrak{B}$.

Введем обратно изоморфную с $\mathfrak{A}$ алгебру $\mathfrak{A}'$. Тогда мы можем рассматривать $\mathfrak{R}$ как $\mathfrak{A}'$-модуль относительно

произведения $xa' \equiv ax$ ($a \longleftrightarrow a'$ является обратным изоморфизмом). Таким образом $\mathfrak{R}$ является $\mathfrak{B}$-пространством обратного представления алгебры $\mathfrak{A}'$ и потому будет $\mathfrak{A}'_{\mathfrak{B}}$-модулем. Обратно, любой $\mathfrak{A}'_{\mathfrak{B}}$-модуль, являющийся $\mathfrak{B}$-пространством, будет $\mathfrak{B}$-пространством представления алгебры $\mathfrak{A}$.

Предположим теперь, что алгебра $\mathfrak{B}$ простая. Напомним, что в этом случае $\mathfrak{B}$ будет прямой суммой, например, m $\mathfrak{B}$-изоморфных неприводимых правых идеалов $\mathfrak{J}$, и что $\mathfrak{B} = \mathfrak{D}_m$, где $\mathfrak{D}$ — некоторое тело. Само $\mathfrak{B}$ будет свободным циклическим модулем, базисом которого будет 1. Любой $\mathfrak{B}$-модуль $\mathfrak{N}$, в котором $x1 = x$ для всех x, будет прямой суммой неприводимых модулей, $\mathfrak{B}$-изоморфных неприводимым правым идеалам $\mathfrak{J}$. Следовательно, $\mathfrak{N}$ будет свободным циклическим модулем тогда и только тогда, когда он является прямой суммой m неприводимых подмодулей, и $\mathfrak{N}$ будет $\mathfrak{B}$-пространством тогда и только тогда, когда он является прямой суммой $h = Nm$ неприводимых $\mathfrak{B}$-модулей. Тогда, если $\mathfrak{S}$ является произвольным подпространством в $\mathfrak{N}$, то $\mathfrak{N} = \mathfrak{S} \oplus \mathfrak{S}'$, где $\mathfrak{S}'$ также является подпространством. Таким образом, если элементы $y_1, \ldots, y_u$ образуют базис для $\mathfrak{S}$, то найдется базис пространства $\mathfrak{N}$, включающий элементы y_i. Применяя этот результат, мы можем доказать, что, как и в случае, когда $\mathfrak{B} = \Phi$, условием приводимости обратного представления является существование в пространстве $\mathfrak{N}$ обратного представления истинного $\mathfrak{B}$-подпространства, инвариантного относительно эндоморфизмов a. Условием разложимости обратного представления является возможность представить $\mathfrak{N}$ в виде $\mathfrak{N} = \mathfrak{N}_1 \oplus \mathfrak{N}_2$, где $\mathfrak{N}_i$ будут подпространствами обратного представления в пространстве $\mathfrak{N}$. Для полной приводимости представления достаточно, чтобы $\mathfrak{N}$ было вполне приводимым $\mathfrak{A}_{\mathfrak{B}}$-модулем. Как мы видели в главе 4, если алгебра $\mathfrak{A}_{\mathfrak{B}}$ полупроста, то любой $\mathfrak{A}_{\mathfrak{B}}$-модуль, в котором $x1 = x$ для всех x, будет вполне приводим. Следовательно, если алгебра $\mathfrak{A}_{\mathfrak{B}}$ полупроста, то любое обратное представление алгебры $\mathfrak{A}$ матрицами с элементами из $\mathfrak{B}$ вполне приводимо.

Если $\mathfrak{B} = \mathfrak{D}$ является телом,* то любой такой неприводимый $\mathfrak{D}$-модуль, что $\mathfrak{N}\mathfrak{D} \neq 0$, будет свободным циклическим модулем. $\mathfrak{D}$-пространства, определенные в этом параграфе, будут просто векторными пространствами над $\mathfrak{D}$, которые мы рассматривали ранее. Следовательно, в этом случае любой $\mathfrak{A}_{\mathfrak{D}}$-модуль $\mathfrak{N}$, в котором $x1 = x$ для всех x и $(\mathfrak{N} : \mathfrak{D})$ конечно, является $\mathfrak{D}$-пространством обратного представления алгебры $\mathfrak{A}$. Как и выше, условие конечности $(\mathfrak{N} : \mathfrak{D})$ эквивалентно условию существования конечного числа образующих для $\mathfrak{N}$ относительно $\mathfrak{A}_{\mathfrak{D}}$. В частности, неприводимые $\mathfrak{A}_{\mathfrak{D}}$-модули являются $\mathfrak{D}$-пространствами обратных представлений. Эти модули будут поэтому неприводимыми $\mathfrak{D}$-пространствами обратных представлений алгебры $\mathfrak{A}$. Как мы видели, любой неприводимый $\mathfrak{A}_{\mathfrak{D}}$-модуль $\mathfrak{A}_{\mathfrak{D}}$-изоморфен неприводимому правому идеалу $\mathfrak{J}$ алгебры $\mathfrak{A}_{\mathfrak{D}}/\mathfrak{N}$, где $\mathfrak{N}$—радикал алгебры $\mathfrak{A}_{\mathfrak{D}}$. Порядок матриц, определенных идеалом $\mathfrak{J}$, равен размерности (или рангу) идеала $\mathfrak{J}$ над $\mathfrak{D}$. Число неизоморфных неприводимых $\mathfrak{A}_{\mathfrak{D}}$-модулей, в которых $x1 = x$ для всех x, и, следовательно, число классов неприводимых отличных от нуля обратных представлений равно числу простых двусторонних идеалов в алгебре $\mathfrak{A}_{\mathfrak{D}}/\mathfrak{N}$.

6. Прямые произведения и композиты полей. В качестве приложения развитой выше теории изучим теперь структуру $\mathfrak{A}_{\mathfrak{B}}$ для того случая, когда $\mathfrak{A}$ является сепарабельным полем, а $\mathfrak{B}$ — произвольным полем над Φ. Предположим сначала, что $\mathfrak{B}$ содержит подполе, изоморфное наименьшему нормальному расширению поля Φ, содержащему $\mathfrak{A}$. Тогда, если $(\mathfrak{A} : \Phi) = n$, то, как хорошо известно, существует в точности n различных изоморфизмов $a \to a^{(i)}, i = 1, \ldots, n$, между $\mathfrak{A}$ и подполями поля $\mathfrak{B}$ [1]). Таким образом, мы получили n обратных гомоморфных отображений $\mathfrak{A}$ в алгебру матриц с коэффициентами из $\mathfrak{B}$,

* На протяжении этой главы мы понимаем под телом *алгебру* с делением. (*Прим. пер.*)

[1]) См. Ван-дер-Варден, Современная алгебра, том 1, стр. 116.

и, так как эти матрицы имеют порядок 1, то все обратные гомоморфизмы неприводимы и не подобны между собой. Из общей теории следует, что $\mathfrak{A}_{\mathfrak{B}}/\mathfrak{N}$, где через $\mathfrak{N}$ обозначен радикал, является в этом случае прямой суммой, по меньшей мере, n идеалов. Так как размерность этих идеалов над $\mathfrak{B} \geqslant 1$ и $(\mathfrak{A}_{\mathfrak{B}} : \mathfrak{B}) = n$, то отсюда следует, что $\mathfrak{N} = 0$ и что существует в точности n простых идеалов в $\mathfrak{A}_{\mathfrak{B}}$, каждый из которых имеет над $\mathfrak{B}$ размерность 1. Если теперь поле $\mathfrak{B}$ произвольно, то мы берем поле $\mathfrak{C}$, содержащее как $\mathfrak{B}$, так и наименьшее нормальное расширение поля $\mathfrak{A}$ над Φ. Так как $(\mathfrak{A}_{\mathfrak{B}})_{\mathfrak{C}} = \mathfrak{A}_{\mathfrak{C}}$, то алгебра $\mathfrak{A}_{\mathfrak{B}}$ полупроста.

Теорема 3. *Если поле $\mathfrak{A}$ является сепарабельным расширением поля Φ, причем $(\mathfrak{A} : \Phi) = n$, и поле $\mathfrak{B}$ является произвольным расширением поля Φ, то алгебра $\mathfrak{A}_{\mathfrak{B}}$ полупроста. Если $\mathfrak{B}$ содержит подполе, изоморфное наименьшему нормальному полю, содержащему $\mathfrak{A}$, то все неприводимые представления поля $\mathfrak{A}$ матрицами с элементами из $\mathfrak{B}$ имеют порядок 1.*

По структурной теории полупростых колец, $\mathfrak{A}_{\mathfrak{B}}$ является прямой суммой полей, например $\mathfrak{F}_1 \oplus \ldots \oplus \mathfrak{F}_t$. Если $1 = e_1 + \ldots + e_t$ является соответствующим разложением единицы алгебры $\mathfrak{A}_{\mathfrak{B}}$ на единицы полей $\mathfrak{F}_i$, то множество $e_i\mathfrak{A}$ элементов вида $e_i a$, где $a \in \mathfrak{A}$, будет подполем поля $\mathfrak{F}_i$, изоморфным полю $\mathfrak{A}$. Подобным же образом, $\mathfrak{F}_i$ содержит подполе $e_i\mathfrak{B}$, изоморфное полю $\mathfrak{B}$. Так как $(e_i\mathfrak{A})(e_i\mathfrak{B}) = e_i\mathfrak{A}\mathfrak{B}e_i = \mathfrak{F}_i$, то поле $\mathfrak{F}_i$ порождается этими двумя полями.

Предположим теперь, что мы имеем произвольные два поля $\mathfrak{A}$ и $\mathfrak{B}$ над Φ и два изоморфных отображения $a \to a^S$ и $b \to b^T$ полей $\mathfrak{A}$ и $\mathfrak{B}$ соответственно в подполя $\mathfrak{A}^S$ и $\mathfrak{B}^T$ третьего поля $\mathfrak{F}$. Тогда мы назовем систему $(\mathfrak{F}, S, T)$ *композитом* полей $\mathfrak{A}$ и $\mathfrak{B}$, если только $\mathfrak{F} = [\mathfrak{A}^S, \mathfrak{B}^T]$, где через $[\mathfrak{A}^S, \mathfrak{B}^T]$ обозначено наименьшее подполе поля $\mathfrak{F}$, содержащее $\mathfrak{A}^S$ и $\mathfrak{B}^T$[1]). Мы будем

рассматривать два композита $(\mathfrak{F}, S, T)$ и $(\mathfrak{F}', S', T')$ как *эквивалентные*, если изоморфизмы $a^S \to a^{S'}$ и $b^T \to b^{T'}$ могут быть продолжены до изоморфизма между $\mathfrak{F}$ и $\mathfrak{F}'$. Очевидно, что такое продолжение, если оно возможно, однозначно определено.

Мы видели, что если $\mathfrak{A}$ является сепарабельным полем, то $\mathfrak{A}_{\mathfrak{B}} = \mathfrak{F}_1 \oplus \ldots \oplus \mathfrak{F}_s$. Отображения $a \to a^{S_i} \equiv ae_i$, где $a \in \mathfrak{A}$, являются изоморфизмами между $\mathfrak{A}$ и подполями $\mathfrak{A}^{S_i}$ полей $\mathfrak{F}_i$. Подобно этому, $b \to b^{T_i} \equiv be_i$ будет изоморфизмом между $\mathfrak{B}$ и $\mathfrak{B}^{T_i}$. Кроме того, $\mathfrak{F}_i = (\mathfrak{A}^{S_i})(\mathfrak{B}^{T_i}) = [\mathfrak{A}^{S_i}, \mathfrak{B}^{T_i}]$, и поэтому $(\mathfrak{F}_i, S_i, T_i)$ является композитом полей $\mathfrak{A}$ и $\mathfrak{B}$.

Мы хотим доказать следующую теорему.

Теорема 4. *Композиты $(\mathfrak{F}_i, S_i, T_i)$ $i = 1, \ldots, t$ не эквивалентны между собой. Любой композит сепарабельного поля $\mathfrak{A}$ и поля $\mathfrak{B}$ эквивалентен одному из $(\mathfrak{F}_i, S_i, T_i)$.*

Для того, чтобы доказать, что $(\mathfrak{F}_i, S_i, T_i)$ и $(\mathfrak{F}_j, S_j, T_j)$ не эквивалентны при $i \neq j$, заметим, что e имеет вид $a_1b_1 + \ldots + a_rb_r$, где $a_k \in \mathfrak{A}$ и $b_k \in \mathfrak{B}$ и, так как $e_i^2 = e_i$, то $e_i = (a_1e_i)(b_1e_i) + \ldots + (a_re_i)(b_re_i) = a_1^{S_i}b_1^{T_i} + \ldots + a_r^{S_i}b_r^{T_i}$. Если бы $(\mathfrak{F}_i, S_i, T_i)$ было эквивалентно $(\mathfrak{F}_j, S_j, T_j)$, то требуемый изоморфизм отображал бы e_i в $a_1^{S_j}b_1^{T_j} + \ldots + a_r^{S_j}b_r^{T_j} = (a_1b_1 + \ldots a_rb_r)e_j = e_ie_j = 0$, что невозможно. Предположим теперь, что $(\mathfrak{F}, S, T)$ является любым композитом полей $\mathfrak{A}$ и $\mathfrak{B}$. Тогда отображение $\sum ab \to \sum a^S b^T$ будет гомоморфным отображением $\mathfrak{A}_{\mathfrak{B}}$ на подалгебру $\mathfrak{A}^S\mathfrak{B}^T$ поля $\mathfrak{F}$. Так как единственными идеалами алгебры $\mathfrak{A}_{\mathfrak{B}}$ являются идеалы вида $\mathfrak{F}_{i_1} \oplus \ldots \oplus \mathfrak{F}_{i_r}$, и так как поле $\mathfrak{F}$ не имеет делителей нуля, то идеалом, отображающимся при этом гомомофизме в нуль, будет идеал вида $\mathfrak{F}_1 \oplus \ldots \oplus \mathfrak{F}_{i-1} \oplus \mathfrak{F}_{i+1} \oplus \ldots \oplus \mathfrak{F}_t = \mathfrak{L}_i$. Следовательно, алгебра $\mathfrak{A}^S\mathfrak{B}^T$ изоморфна $\mathfrak{F}/\mathfrak{L}_i$, и потому она

---

[1]) Если оба поля $\mathfrak{A}$ и $\mathfrak{B}$ содержат трансцендентные элементы, то это определение требует некоторого изменения. См. Chevalley [9].

изоморфна $\mathfrak{F}_i$. Отсюда вытекает, что $\mathfrak{A}^S\mathfrak{B}^T$ является полем и потому $\mathfrak{A}^S\mathfrak{B}^T = [\mathfrak{A}^S, \mathfrak{B}^T] = \mathfrak{F}$. Кроме того, изоморфизм, определенный нашим гомоморфным отображением, является соответствием $\sum a^S b^T \to \sum (a^{S_i})(b^{T_i})$. Следовательно, композиты $(\mathfrak{F}, S, T)$ и $(\mathfrak{F}_i, S_i, T_i)$ эквивалентны.

Мы видели, что если $\mathfrak{B}$ содержит поле, эквивалентное наименьшему нормальному расширению поля $\mathfrak{A}$, то $t = n$, и каждое из полей $\mathfrak{F}_i$ одномерно над $\mathfrak{B}$. Следовательно, поле $\mathfrak{F}_i = \mathfrak{B}^{S_i}$ изоморфно полю $\mathfrak{B}$.

Теорема 5. *Если поле $\mathfrak{A}$ является сепарабельным расширением поля Φ, $(\mathfrak{A} : \Phi) = n$ и $\mathfrak{B}$ содержит поле, изоморфное наименьшему нормальному расширению поля $\mathfrak{A}$ над Φ, то $\mathfrak{A}_\mathfrak{B} = \mathfrak{B}_1 \oplus \ldots \oplus \mathfrak{B}_n$, где $\mathfrak{B}_i \cong \mathfrak{B}$.*

Из следующего примера видно, что эта теорема перестает быть справедливой для случая несепарабельных полей. Пусть $\mathfrak{A} = \Phi(x)$, где Φ является полем характеристики p, и $x^p = \xi$ лежит в Φ, причем x не лежит в Φ. Предположим, что $\mathfrak{B}$ является полем $\Phi(y)$, где $y^p = \xi$. Тогда $\mathfrak{A}_\mathfrak{B}$ содержит отличный от нуля нильпотентный элемент $z = x - y$. Так как алгебра $\mathfrak{A}_\mathfrak{B}$ коммутативна, то z порождает нильпотентный идеал, и потому алгебра $\mathfrak{A}_\mathfrak{B}$ не будет полупростой.

7. Центральные простые алгебры. Вернемся теперь к основной теме этой главы, а именно к теории простых алгебр. Во всех наших рассуждениях мы будем исключать из рассмотрения тривиальные нуль-алгебры. При этом условии мы можем следующим образом сформулировать фундаментальную структурную теорему.

Теорема 6. (Веддербарн [Wedderburn]). *Любая простая алгебра $\mathfrak{A}$ над Φ является прямым произведением $\Phi_m \times \mathfrak{D}$, где $\mathfrak{D}$—тело, и обратно, любая алгебра такого вида простая. Если $\mathfrak{A} = \Phi_m \times \mathfrak{D} = \Phi_{m'} \times \mathfrak{F}$, где $\mathfrak{F}$ является также телом, то $m = m'$ и тела $\mathfrak{D}$ и $\mathfrak{F}$ изоморфны.*

Нам понадобится также

Теорема 7. $\Phi_{rs} = \Phi_r \times \Phi_s$.

Она является непосредственным следствием вычислений, проделанных в § 6 главы 2.

Простая алгебра $\mathfrak{A}$ называется *центральной*, если ее центр совпадает с совокупностью элементов вида 1α, где $\alpha \in \Phi$ [1]). Например, Φ_m будет простой центральной алгеброй. Понятие центральной алгебры является в известном смысле противоположным понятию коммутативной алгебры, и мы увидим, что теория прямых произведений таких алгебр значительно проще, чем изложенная в предыдущем отделе теория прямых произведений коммутативных алгебр.

Если $\mathfrak{A} = \Phi_m \times \mathfrak{D} = \mathfrak{D}_m$, где $\mathfrak{D}$ является телом, то центр $\mathfrak{C}$ алгебры $\mathfrak{A}$ содержится в $\mathfrak{D}$. Следовательно, алгебра $\mathfrak{A}$ будет центральной тогда и только тогда, когда тело $\mathfrak{D}$ центрально. Если $\mathfrak{A}$ является любой простой алгеброй, то ее центр $\mathfrak{C}$ будет полем, и алгебру $\mathfrak{A}$ можно рассматривать как алгебру над этим полем $\mathfrak{C}$. Очевидно, что $\mathfrak{A}$ центральна над $\mathfrak{C}$.

Предположим теперь, что $\mathfrak{A}$—произвольная алгебра с единицей, а $\mathfrak{B}$—центральная простая алгебра. Мы хотим показать, что двусторонние идеалы алгебры $\mathfrak{A}_\mathfrak{B}$ могут быть поставлены во взаимооднозначное соответствие с двусторонними идеалами алгебры $\mathfrak{A}$. Пусть $\mathfrak{J}_0$ является двусторонним идеалом алгебры $\mathfrak{A}$. Тогда $\mathfrak{J} = \mathfrak{J}_0\mathfrak{B} = \mathfrak{J}_{0\mathfrak{B}}$ будет двусторонним идеалом в $\mathfrak{A}_\mathfrak{B}$. Пусть элементы $x_1, \ldots, x_n$ образуют такой базис алгебры $\mathfrak{A}$ над Φ, что $x_1, \ldots, x_r$ является базисом идеала $\mathfrak{J}_0$ над Φ. Тогда, если $\sum_1^n x_i b_i \in \mathfrak{A}$, то $b_i = \beta_i$, где β_i лежит в Φ. Если $\sum_1^n x_i b_i \in \mathfrak{J}$, то $b_{r+1} = \ldots = b_n = 0$. Следовательно, $\mathfrak{A} \cap \mathfrak{J}$ состоит из эле-

[1]) Я обязан профессору Алберту за предложение этого термина, вместо имеющего слишком много значений термина «нормальный», употреблявшегося ранее в этом смысле. Термин «централизатор», которым мы будем далее пользоваться, также принадлежит Алберту.

ментов вида $\sum_1^r x_i\beta_i$ и $\mathfrak{A}\cap\mathfrak{J}=\mathfrak{J}_0$. Отсюда следует, что $\mathfrak{J}_{0\mathfrak{B}}=\overline{\mathfrak{J}}_{0\mathfrak{B}}$ тогда и только тогда, когда $\mathfrak{J}_0=\overline{\mathfrak{J}}_0$.

Пусть теперь $\mathfrak{J}$ является произвольным двусторонним идеалом в $\mathfrak{A}\times\mathfrak{B}$, $\mathfrak{J}_0=\mathfrak{A}\cap\mathfrak{J}$, и пусть элементы $x_1, \ldots, x_n$ образуют такой базис алгебры $\mathfrak{A}$, что $x_1, \ldots, x_r$ образуют базис для $\mathfrak{J}_0$. Очевидно, что $\mathfrak{J}_0$ будет двусторонним идеалом алгебры $\mathfrak{A}$ и $\mathfrak{J}_{0\mathfrak{B}}\subseteq\mathfrak{J}$. Предположим, что $\mathfrak{J}_{0\mathfrak{B}}\subset\mathfrak{J}$, и пусть $x_1b_1+\ldots x_nb_n$ будет не содержащимся в $\mathfrak{J}_{0\mathfrak{B}}$ элементом из $\mathfrak{J}$. Тогда и элемент $x_{r+1}b_{r+1}+\ldots, +x_nb_n$ также обладает этим свойством, и потому, по крайней мере, один из элементов b_j, $j=r+1, \ldots, n$ отличен от нуля. Пусть теперь $x_{i_1}b_{i_1}+\ldots+x_{i_s}b_{i_s}$, $b_{i_j}\neq 0$, $i_j=r+1, \ldots, n$, будет элементом из $\mathfrak{J}$, для которого s имеет наименьшее положительное значение. Элементы

$$b(x_{i_1}b_{i_1}+\ldots+x_{i_s}b_{i_s}),\quad (x_{i_1}b_{i_1}+\ldots+x_{i_s}b_{i_s})b$$

лежат в $\mathfrak{J}$ для любого элемента b алгебры $\mathfrak{B}$. Отсюда следует, что первые компоненты b_{i_1} этих элементов, включая и нуль, образуют отличный от нуля двусторонний идеал алгебры $\mathfrak{B}$, и, следовательно, так как алгебра $\mathfrak{B}$ является простой, b_{i_1} может быть любым элементом из $\mathfrak{B}$. Таким образом, идеал $\mathfrak{J}$ содержит элемент $x_{i_1}+x_{i_2}b_2'+\ldots+x_{i_s}b_s'$ и, следовательно, он содержит элемент

$$b(x_{i_1}+x_{i_2}b_2'+\ldots+x_{i_s}b_s')-(x_{i_1}+x_{i_2}b_2'+\ldots+$$

$$+x_{i_s}b_s')b=\sum_{j=2}^{s}x_{i_j}(b_j'b-b_j'b).$$

Так как индекс s минимален, то все $bb'_j=b_j'b$, и потому, в силу центральности алгебры $\mathfrak{B}$, $b_j'=\beta_j\in\Phi$. Таким образом, идеал $\mathfrak{J}$ содержит элемент $x_{i_1}+x_{i_2}\beta_2+\ldots+x_{i_s}\beta_s$, который, очевидно, лежит в $\mathfrak{A}$. Это противоречит тому, что элементы $x_1, \ldots, x_r$ образуют базис идеала $\mathfrak{J}_0=(\mathfrak{A}\cap\mathfrak{J})$. Следовательно, нами доказана

Теорема 8. *Если $\mathfrak{A}$ является алгеброй с единицей, а $\mathfrak{B}$ — центральной простой алгеброй, то соответствие $\mathfrak{J}_0\to\mathfrak{J}_{0\mathfrak{B}}$ будет взаимооднозначным соответствием между двусторонними идеалами алгебры $\mathfrak{A}$ и двусторонними идеалами алгебры $\mathfrak{A}_{\mathfrak{B}}$.*

Следствие 1. *Если алгебра $\mathfrak{A}$ простая, а алгебра $\mathfrak{B}$ центральная простая, то и алгебра $\mathfrak{A}_{\mathfrak{B}}$ простая.*

Если $\mathfrak{N}$ является радикалом алгебры $\mathfrak{A}_{\mathfrak{B}}$, то $\mathfrak{N}_0=\mathfrak{A}\cap\mathfrak{N}$ будет нильпотентным идеалом алгебры $\mathfrak{A}$ и потому содержится в радикале $\mathfrak{N}_0'$ алгебры $\mathfrak{A}$. С другой стороны, $\mathfrak{N}'_{0\mathfrak{B}}$ будет нильпотентным идеалом в $\mathfrak{A}_{\mathfrak{B}}$, и потому $\mathfrak{N}'_{0\mathfrak{B}}\subseteq\mathfrak{N}$. Следовательно, $\mathfrak{N}_0'=\mathfrak{N}_0$. Отсюда вытекает, в частности,

Следствие 2. *Если алгебра $\mathfrak{A}$ полупроста и алгебра $\mathfrak{B}$ является центральной и простой, то алгебра $\mathfrak{A}_{\mathfrak{B}}$ полупроста.*

Пусть теперь $c=x_1b_1+\ldots+x_nb_n$ является элементом алгебры $\mathfrak{A}_{\mathfrak{B}}=\mathfrak{A}\times\mathfrak{B}$, коммутирующим со всеми элементами b из $\mathfrak{B}$. Тогда $\sum x_i(bb_i-b_ib)=0$, и $bb_i=b_ib$. Следовательно, $b_i\in\Phi$ и $c\in\mathfrak{A}$. Отсюда следует, что центр алгебры $\mathfrak{A}\times\mathfrak{B}$ совпадает с центром алгебры $\mathfrak{A}$. Если $\mathfrak{A}$ является центральной простой алгеброй, то и алгебра $\mathfrak{A}\times\mathfrak{B}$ также является центральной и простой.

Теорема 9. *Элементами прямого произведения $\mathfrak{A}\times\mathfrak{B}$ алгебры с единицей $\mathfrak{A}$ и центральной простой алгебры $\mathfrak{B}$, коммутирующими со всеми элементами из $\mathfrak{B}$, могут быть лишь элементы алгебры $\mathfrak{A}$. Если алгебра $\mathfrak{A}$ центральная простая, то и алгебра $\mathfrak{A}\times\mathfrak{B}$ центральная простая.*

8. Представление полупростой алгебры матрицами с элементами из центральной простой алгебры. Как и ранее, мы ограничиваемся такими представлениями алгебры $\mathfrak{A}$, при которых единица алгебры $\mathfrak{A}$ отображается в единичную матрицу. Если $\mathfrak{A}$ — полупростая алгебра и $\mathfrak{B}$ —

центральная простая алгебра, то алгебра $\mathfrak{A}_{\mathfrak{B}}$ полупроста. Как мы видели в § 5, отсюда вытекает следующая

Теорема 10. *Если $\mathfrak{A}$ является полупростой алгеброй, то любое обратное представление (обычное представление) алгебры $\mathfrak{A}$ матрицами с элементами из центральной простой алгебры вполне приводимо.*

Предположим теперь, что алгебра $\mathfrak{A}$ простая. Пусть $\mathfrak{B}$ будет прямой суммой m изоморфных неприводимых правых идеалов. Таким образом, $\mathfrak{B} = \mathfrak{D}_m$, где $\mathfrak{D}$ является телом. Мы видели, что алгебра $\mathfrak{A}_{\mathfrak{B}}$ проста. Следовательно, $\mathfrak{A}_{\mathfrak{B}}$ будет прямой суммой r изоморфных неприводимых правых идеалов, и $\mathfrak{A}_{\mathfrak{B}} = \mathfrak{E}_r$, где $\mathfrak{E}$ является телом. Любой неприводимый правый идеал алгебры $\mathfrak{A}_{\mathfrak{B}}$ является $\mathfrak{B}$-модулем и поэтому будет прямой суммой, например, h $\mathfrak{B}$-изоморфных неприводимых $\mathfrak{B}$-модулей. Отсюда следует, что $\mathfrak{A}_{\mathfrak{B}}$ разлагается в прямую сумму rh неприводимых $\mathfrak{B}$-модулей. С другой стороны, если $(\mathfrak{A} : \Phi) = n$, то $\mathfrak{A}_{\mathfrak{B}}$ будет $\mathfrak{B}$-пространством ранга n. Так как любое $\mathfrak{B}$-пространство ранга 1 является суммой m $\mathfrak{B}$-изоморфных неприводимых $\mathfrak{B}$-модулей, то $\mathfrak{A}_{\mathfrak{B}}$ будет прямой суммой mn неприводимых $\mathfrak{B}$-модулей. Таким образом, $rh = mn$.

Пусть теперь $\mathfrak{R}$ является произвольным неприводимым $\mathfrak{B}$-пространством обратного представления алгебры $\mathfrak{A}$. Тогда $\mathfrak{R} = \mathfrak{S}_1 \oplus \ldots \oplus \mathfrak{S}_{\overline{m}}$, где $\mathfrak{S}_i$ будут изоморфными неприводимыми $\mathfrak{A}_{\mathfrak{B}}$-модулями. Каждый из модулей $\mathfrak{S}_i$ разлагается в прямую сумму h изоморфных неприводимых $\mathfrak{B}$-модулей. Следовательно, $\mathfrak{R}$ разлагается в прямую сумму $\overline{m}h$ неприводимых $\mathfrak{B}$-модулей. Так как $\mathfrak{R}$ является $\mathfrak{B}$-пространством, то отсюда следует, что $h\overline{m} \equiv 0 \pmod{m}$. Если теперь m'' будет таким меньшим чем $\overline{m}$ целым числом, что $hm'' \equiv 0 \pmod{m}$, то прямая сумма m'' модулей $\mathfrak{S}_i$ будет $\mathfrak{B}$-пространством. Она совпадает поэтому с $\mathfrak{R}$. Отсюда следует, что $m'' = \overline{m}$, так что $h\overline{m} = m\overline{h}$ является общим наименьшим кратным h и m. Равенство $h\overline{m} = m\overline{h}$ показывает, что ранг $\mathfrak{R}$ над $\mathfrak{B}$ равен $\overline{h}$. Следовательно, порядок матриц, определенных пространством $\mathfrak{R}$, равен $\overline{h}$. Если $\mathfrak{R}'$ является другим неприводимым $\mathfrak{B}$-пространством обратного представления алгебры $\mathfrak{A}$, то $\mathfrak{R}'$ также будет прямой суммой $\overline{m} = h^{-1}[h, m]$ неприводимых $\mathfrak{A}_{\mathfrak{B}}$-модулей. Отсюда следует, что пространства $\mathfrak{R}'$ и $\mathfrak{R}$ $\mathfrak{A}_{\mathfrak{B}}$-изоморфны. Таким образом, все неприводимые обратные представления алгебры $\mathfrak{A}$ матрицами подобны между собой. Любое обратное представление алгебры $\mathfrak{A}$ вполне приводится на неприводимые части, каждая из которых подобна представлению, определенному пространством $\mathfrak{R}$. Эти результаты могут быть сформулированы в виде следующей теоремы:

Теорема 11. *Пусть $\mathfrak{A}$ является простой алгеброй, а $\mathfrak{B}$ — центральной простой алгеброй. Пусть $(\mathfrak{A} : \Phi) = n$, $\mathfrak{B} = \mathfrak{D}_m$ и $\mathfrak{A}_{\mathfrak{B}} = \mathfrak{E}_r$, где $\mathfrak{D}$ и $\mathfrak{E}$ являются телами. Тогда $r|mn$, и если $mn = hr$ и $[h, m] = \overline{hm} = h\overline{m}$, то алгебра $\mathfrak{A}$ обладает обратным представлением в $\mathfrak{B}_N$ тогда и только тогда, когда $\overline{h}|N$. Любые два представления алгебры $\mathfrak{A}$ в одной и той же алгебре матриц $\mathfrak{B}_N$ подобны между собой.*

Подобным же образом мы можем доказать следующую теорему.

Теорема 11′. *Пусть $\mathfrak{A}$ и $\mathfrak{B}$ имеют тот же смысл, что и в теореме 11, и пусть $\mathfrak{A}'_{\mathfrak{B}} = \mathfrak{E}'_{r'}$, где алгебра $\mathfrak{A}'$ обратно изоморфна алгебре $\mathfrak{A}$, и $\mathfrak{E}'$ является телом. Тогда $r'|mn$, и если $mn = h'r'$ и $[h', m] = h'\overline{m}' = \overline{h}'m$, то алгебра $\mathfrak{A}$ обладает обратным представлением в $\mathfrak{B}_N$ тогда и только тогда, когда $\overline{h}'|N$. Любые два представления алгебры $\mathfrak{A}$ в одной и той же алгебре матриц $\mathfrak{B}_N$ подобны между собой.*

Мы можем получить несколько более точную форму теоремы 11, рассматривая сначала ее специальный случай, когда $\mathfrak{B} = \mathfrak{D}$ является телом, и распространяя потом полученный таким образом результат на общий случай, когда $\mathfrak{B} = \mathfrak{D}_m$. Если $\mathfrak{B} = \mathfrak{D}$, то $m = 1$ и $[h, m] = h$. Мы получаем

Следствие. *Пусть $\mathfrak{A}$ является простой алгеброй и $\mathfrak{D}$ — центральным телом. Положим $(\mathfrak{A} : \Phi) = n$ и*

$\mathfrak{A}_{\mathfrak{D}} = \mathfrak{E}_s$. *Тогда* $n = hs$, *и* $\mathfrak{A}$ *тогда и только тогда обладает обратным представлением в* $\mathfrak{D}_N$, *когда* $h|N$.

Если теперь $\mathfrak{A}_{\mathfrak{D}} = \mathfrak{E}_s$, то $\mathfrak{A}_{\mathfrak{B}} = \mathfrak{E}_{sm}$ для $\mathfrak{B} = \mathfrak{D}_m$. Следовательно, целое число r из теоремы 11 равно sm и $n = hs$. Этим доказана

Теорема 12. *Пусть* $\mathfrak{A}$ *и* $\mathfrak{B}$ *имеют тот же смысл, что и в теореме 11, и пусть* $\mathfrak{A}_{\mathfrak{D}} = \mathfrak{E}_s$, *где* $\mathfrak{E}$ *является телом. Тогда* $s|n$, *и если* $n = sh$ *и* $[h, m] = h\overline{m} = \overline{h}m$, *то алгебра* $\mathfrak{A}$ *обладает обратным представлением в* $\mathfrak{B}_N$ *тогда и только тогда, когда* $\overline{h}\,|\,N$.

Теорема 12′. *Пусть* $\mathfrak{A}$ *и* $\mathfrak{B}$ *имеют тот же смысл, что и в теореме 11, и пусть* $\mathfrak{A}_{\mathfrak{D}} = \mathfrak{E}'_{s'}$ *где* $\mathfrak{E}$ *является телом. Тогда* $s'|n$, *и если* $n = s'h'$ *и* $[h', m] = h'\overline{m}' = \overline{h}'m$, *то алгебра* $\mathfrak{A}$ *обладает представлением в* $\mathfrak{B}_N$ *тогда и только тогда, когда* $\overline{h}'|N$.

Предположим теперь, что $\mathfrak{A}$ является телом, и $\mathfrak{B} = \mathfrak{D}$ является центральным телом. Мы можем рассматривать $\mathfrak{A} \times \mathfrak{D} = \mathfrak{E}_s$ как $\mathfrak{A}$-пространство. Тогда, повторяя рассуждения, приведшие нас к теореме 11, мы можем доказать, что $s|d$, где $d = (\mathfrak{D} : \Phi)$. Проведение детального доказательства предоставим читателю.

Теорема 13. *Пусть* $\mathfrak{A}$ *является телом и* $\mathfrak{D}$ *— центральным телом. Тогда, если* $\mathfrak{A} \times \mathfrak{D} = \mathfrak{E}_s$, *где* $\mathfrak{E}$ *является телом, то* s *будет общим делителем чисел* $n = (\mathfrak{A} : \Phi)$ *и* $d = (\mathfrak{D} : \Phi)$. *Если* $(d, n) = 1$, *то* $\mathfrak{A} \times \mathfrak{D}$ *будет телом.*

9. Простые подалгебры центральной простой алгебры. Теория представлений может быть применена к изучению подалгебр простой центральной алгебры $\mathfrak{A}$. В самом деле, если $\mathfrak{B}$ является подалгеброй, то отображение $b \to b$ будет представлением алгебры $\mathfrak{B}$ матрицами первого порядка с элементами из $\mathfrak{A}$. Если $\mathfrak{B}$ является простой алгеброй с единицей, то мы можем применить теорему 12′.[1] Пусть $\mathfrak{A} = \mathfrak{D}_m$, где $\mathfrak{D}$ является центральным телом, $(\mathfrak{B} : \Phi) = q$ и $\mathfrak{B}' \times \mathfrak{D} = \mathfrak{B}_{\mathfrak{D}} = \mathfrak{E}'_{s'}$, где $\mathfrak{E}'$ является телом. Тогда $q = s'h'$ и, если $\overline{h}' = m^{-1}\,[h', m]$, то $\mathfrak{B}$ обладает представлением лишь в таких $\mathfrak{A}_N$, для которых $\overline{h}'|N$. Так как $\mathfrak{B}$ обладает представлением матрицами первого порядка с элементами из $\mathfrak{A}$, то $\overline{h}' = 1$. Следовательно, $h'|m$, и если положить $m = h'l$, то мы получим, что $ms' = ql$. Таким образом, $q|ms'$.

Теорема 14. *Если* $\mathfrak{B}$ *является простой содержащей единицу подалгеброй центральной простой алгебры* $\mathfrak{A} = \mathfrak{D}_m$, *где* $\mathfrak{D}$ *— тело, то* $\mathfrak{B}' \times \mathfrak{D} = \mathfrak{E}'_{s'}$, *где* $\mathfrak{E}'$ *является телом, причем* $s'|q$ *и* $q|ms'$.

Следствие. *Если* $\mathfrak{B}$ *является содержащей единицу подалгеброй центрального тела* $\mathfrak{D}$, *то* $\mathfrak{B}' \times \mathfrak{D} = \mathfrak{E}'_q$, *где* $\mathfrak{E}'$ *является телом и* $q = (\mathfrak{B} : \Phi)$

Если $\mathfrak{B}_1$ и $\mathfrak{B}_2$ являются изоморфными подалгебрами алгебры $\mathfrak{A}$, то мы можем рассматривать их как изоморфные образы одной и той же алгебры $\mathfrak{B}$. Если отображение $b_1 \to b_2$ является изоморфизмом между $\mathfrak{B}_1$ и $\mathfrak{B}_2$, то отображения $b \to b_1$ и $b \to b_2$ будут представлениями алгебры $\mathfrak{B}$ матрицами первого порядка с элементами из $\mathfrak{A}$. Эти представления подобны. Итак, нами получена следующая

Теорема 15. *Если* $\mathfrak{B}_1$ *и* $\mathfrak{B}_2$ *являются изоморфными содержащими единицу простыми подалгебрами центральной простой алгебры* $\mathfrak{A}$, *то любой изоморфизм между ними может быть продолжен до внутреннего автоморфизма алгебры* $\mathfrak{A}$.

Отсюда, очевидно, следует

Теорема 16. *Любой автоморфизм центральной простой алгебры является внутренним.*

[1]) Следует отметить, что начиная с этих пор мы будем применять обозначения, отличные от употреблявшихся в § 8. Здесь $\mathfrak{A}$ обозначает центральную простую алгебру, а $\mathfrak{B}$ — простую алгебру, которая может не быть центральной. Это представляется желательным, так как в наших приложениях $\mathfrak{B}$ будет обычно подалгеброй алгебры $\mathfrak{A}$.

422—Б

10. Дифференцирования. В теории дифференцирований алгебры существуют теоремы, весьма похожие на теоремы § 9. Если $\mathfrak{B}$ является подалгеброй алгебры $\mathfrak{A}$, то *дифференцированием* D подалгебры $\mathfrak{B}$ *в* $\mathfrak{A}$ называется отображение $\mathfrak{B}$ на часть алгебры $\mathfrak{A}$, удовлетворяющее следующим условиям:

$$(b_1 + b_2) D = b_1 D + b_2 D, \quad (b\alpha) D = (bD)\alpha,$$
$$(b_1 b_2) D = b_1 (b_2 D) + (b_1 D) b_2.$$

Если $\mathfrak{B} = \mathfrak{A}$, то мы просто говорим о *дифференцировании в алгебре* $\mathfrak{A}$. Нетрудно видеть, что если D_1, $D_2 \in \mathfrak{H}$, где $\mathfrak{H}$ обозначает совокупность дифференцирований в алгебре $\mathfrak{A}$, то $D\alpha$ и $D_1 \pm D_2 \in \mathfrak{H}$. Так как

$$(b_1 b_2) D_1 D_2 = (b_1 D_2)(b_2 D_1) + b_1 (b_2 D_1 D_2) + (b_1 D_1 D_2) b_2 + (b_1 D_1)(b_2 D_2),$$

то $D_1 D_2$ не будет, вообще говоря, дифференцированием. Однако,

$$(b_1 b_2)(D_1 D_2 - D_2 D_1) = b_1 (b_2 (D_1 D_2 - D_2 D_1)) + (b_1 (D_1 D_2 - D_2 D_1)) b_2,$$

так что $[D_1, D_2] = D_1 D_2 - D_2 D_1$ является дифференцированием. Для любого элемента d из $\mathfrak{A}$ мы можем определить дифференцирование при помощи соответствия $x \to [x, d] = xd - dx$. Дифференцирования подобного типа называются внутренними. Как и для обычного дифференцирования справедливо правило Лейбница:

$$(b_1 b_2) D^k = b_1 (b_2 D^k) + \binom{k}{1} (b_1 D)(b_2 D^{k-1}) + \ldots + (b_1 D^k) b_2.$$

Следовательно, если поле Φ имеет отличную от нуля характеристику p, то

$$(b_1 b_2) D^p = b_1 (b_2 D^p) + (b_1 D^p) b_2,$$

так что D^p является дифференцированием. Таким же образом мы доказываем при помощи индукции, что

$$b d^k = d^k b + \binom{k}{1} d^{k-1} b' + \ldots + b^{(k)},$$

где $b' = [b, d]$, $b'' = [[b, d], d]$ и т. д. Таким образом, для полей Φ характеристики $p \neq 0$ мы имеем:

$$[b, d^p] = b^{(p)} = [\ldots [[b, \overbrace{d], d], \ldots, d}^{p}].$$

Теория дифференцирований обладает далеко идущим параллелизмом с теорией изоморфизмов. Например, справедлива следующая теорема:

Теорема 17. *Если $\mathfrak{B}$ является полупростой содержащей единицу подалгеброй центральной простой алгебры $\mathfrak{A}$, то любое дифференцирование $\mathfrak{B}$ в $\mathfrak{A}$ может быть продолжено до внутреннего дифференцирования всей алгебры $\mathfrak{A}$.*

Рассмотрим множество матриц из $\mathfrak{A}_2$, имеющих вид

$$\begin{pmatrix} b & bD \\ 0 & b \end{pmatrix},$$

где b пробегает $\mathfrak{B}$. Это множество образует алгебру, изоморфную алгебре $\mathfrak{B}$, и, следовательно, определяет представление $\mathfrak{B}$ матрицами с элементами из $\mathfrak{A}$. Пусть $\mathfrak{R}$ будет соответствующим $\mathfrak{A}$-пространством этого представления. Соответственно форме матриц, $\mathfrak{R}$ обладает таким базисом x_1, x_2, что $\mathfrak{A}$-пространство $\mathfrak{R}_1 = x_1 \mathfrak{A}$ инвариантно относительно эндоморфизмов b из $\mathfrak{B}$. Так как $\mathfrak{B}_{\mathfrak{R}}$-модуль $\mathfrak{R}$ вполне приводим, то существует второе пространство $\mathfrak{R}_2 = y\mathfrak{A}$, также инвариантное относительно эндоморфизмов b и такое, что $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2$. Пусть $y = x_1 a_1 + x_2 a_2$, где $a_i \in \mathfrak{A}$. Так как при соответствующих элементах a_1' и a_2' из $\mathfrak{A}$ $x_2 = x_1 a_1' + y a_2'$, то a_2 обладает в $\mathfrak{A}$ обратным элементом a_2'. Мы можем заменить y элементом $y a_2'$. Следовательно, можно предположить, что $x_2 = x_1 d + y$ и $y = x_2 - x_1 d$. Матрицей, переводящей

$\mathfrak{A}$-базис x_1, y в $\mathfrak{A}$-базис x_1, x_2, будет $\begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix}$. Обратной для этой матрицы будет $\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}$. Так как $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2$, то матрицей эндоморфизма b относительно базиса x_1, y будет $\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$. Следовательно,

$$\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}\begin{pmatrix} b & bD \\ 0 & b \end{pmatrix}\begin{pmatrix} 1 & -d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}.$$

Простое вычисление показывает что $b_1 = b_2 = b$ и $bD = [b, D]$ для всех b.

Как следствие теоремы 17 получаем следующую теорему.

Теорема 18. *Каждое дифференцирование простой центральной алгебры является внутренним.*

11. Перестановочные подалгебры. Если $\mathfrak{B}$ является подалгеброй алгебры $\mathfrak{A}$, то мы назовем подалгебру алгебры $\mathfrak{A}$, состоящую из элементов, перестановочных с элементами из $\mathfrak{B}$, *централизатором* $\mathfrak{A}(\mathfrak{B})$ подалгебры $\mathfrak{B}$ в $\mathfrak{A}$. Как обычно, мы обозначаем алгебру правых умножений в $\mathfrak{A}$ через $\mathfrak{A}_r$ и алгебру левых умножений в $\mathfrak{A}$ — через $\mathfrak{A}_l$. Пусть $\overline{\mathfrak{B}}_r(\overline{\mathfrak{B}}_l)$ будет алгеброй правых (левых) умножений $b_r(b_l)$ в $\mathfrak{A}$, определенных элементами b из $\mathfrak{B}$. Напомним, что если алгебра $\mathfrak{A}$ обладает единицей, то $\mathfrak{A}_l$ является алгеброй $\mathfrak{A}_r$-эндоморфизмов и $\mathfrak{A}_r$ является алгеброй $\mathfrak{A}_l$-эндоморфизмов. Тогда алгеброй эндоморфизмов, перестановочных с эндоморфизмами из $\mathfrak{A}_l$ и из $\overline{\mathfrak{B}}_r$, будет $\overline{\mathfrak{A}(\mathfrak{B})}_r$. В самом деле, если C является таким эндоморфизмом, то $C = c_r$ будет правым умножением. Так как $\mathfrak{A}_r$ изоморфно алгебре $\mathfrak{A}$ при изоморфизме $a \to a_r$, отображающем элементы из $\mathfrak{B}$ на элементы из $\overline{\mathfrak{B}}_r$, то отсюда следует, что $c \in \mathfrak{A}(\mathfrak{B})$. Если подалгебра $\mathfrak{B}$ содержит единицу, то алгебра эндоморфизмов $\mathfrak{A}_l\overline{\mathfrak{B}}_r = \overline{\mathfrak{B}}_r\mathfrak{A}_l$ содержит $\mathfrak{A}_l$ и $\overline{\mathfrak{B}}_r$.

Следовательно, в этом случае $\overline{\mathfrak{A}(\mathfrak{B})}_r$ может быть охарактеризована как алгебра действующих в $\mathfrak{A}$ $\mathfrak{A}\overline{\mathfrak{B}}_r$-эндоморфизмов.

Предположим теперь, что $\mathfrak{A}$ является центральной простой алгеброй, а $\mathfrak{B}$ — простой подалгеброй, содержащей единицу алгебры $\mathfrak{A}$. Алгебра $\mathfrak{A}_l\overline{\mathfrak{B}}_r$ будет гомоморфным образом алгебры $\mathfrak{A}' \times \mathfrak{B}$, где алгебра $\mathfrak{A}'$ обратно изоморфна алгебре $\mathfrak{A}$. Мы видели, что алгебра $\mathfrak{A}' \times \mathfrak{B}$ проста. Следовательно, эта алгебра имеет вид $\mathfrak{E}_r$, где $\mathfrak{E}$ — тело. Отсюда следует, что алгебра $\mathfrak{A}_l\overline{\mathfrak{B}}_r$ изоморфна $\mathfrak{E}_r$ и $\mathfrak{A}_l\overline{\mathfrak{B}}_r = \mathfrak{A}_l \times \overline{\mathfrak{B}}_r = \overline{\mathfrak{E}}_r$, где тело $\overline{\mathfrak{E}}$ изоморфно телу $\mathfrak{E}$. Так как $1\mathfrak{A}_l = \mathfrak{A}$, то $\mathfrak{A}$ обладает конечным числом образующих относительно $\overline{\mathfrak{E}}_r$. Следовательно, в силу доказанного в § 6 главы 2, алгебра $\overline{\mathfrak{E}}_r$-эндоморфизмов имеет вид $\overline{\mathfrak{E}}_s'$, где $\overline{\mathfrak{E}}'$ обратно изоморфно $\mathfrak{E}$, и размерность алгебры $\mathfrak{A}$ над $\mathfrak{E}$ равна rs. Таким образом, $\overline{\mathfrak{A}(\mathfrak{B})}_r = \overline{\mathfrak{E}}_s'$ и $\mathfrak{A}(\mathfrak{B}) = \mathfrak{E}_s'$, где $\mathfrak{E}' \cong \overline{\mathfrak{E}}'$.

Определим теперь $\mathfrak{A}(\mathfrak{A}(\mathfrak{B}))$. Очевидно, что $\mathfrak{B} \subset \mathfrak{A}(\mathfrak{A}(\mathfrak{B}))$. С другой стороны, если $c \in \mathfrak{A}(\mathfrak{A}(\mathfrak{B}))$, то c_r является $\overline{\mathfrak{E}}_s'$-эндоморфизмом. Так как $\overline{\mathfrak{E}}_s'$-эндоморфизмы принадлежат $\overline{\mathfrak{E}}_r = \mathfrak{A}_l\mathfrak{B}_r$, то $c_r \in \mathfrak{A}_l \times \overline{\mathfrak{B}}_r$. Так как c_r коммутирует с элементами из $\mathfrak{A}_l$, то, по теореме 9, $c_r \in \overline{\mathfrak{B}}_r$. Следовательно, $c \in \mathfrak{B}$, и потому $\mathfrak{A}(\mathfrak{A}(\mathfrak{B})) = \mathfrak{B}$. Из этого равенства следует, что $\mathfrak{B} \cap \mathfrak{A}(\mathfrak{B})$ будет как центром алгебры $\mathfrak{B}$, так и центром алгебры $\mathfrak{A}(\mathfrak{B})$.

Пусть $(\mathfrak{A} : \Phi) = n$, $(\mathfrak{E} : \Phi) = e$. Тогда $n = (\mathfrak{A} : \overline{\mathfrak{E}})(\mathfrak{E} : \Phi) = rse$. Так как $\mathfrak{A}(\mathfrak{B}) = \mathfrak{E}_s'$, то $(\mathfrak{A}(\mathfrak{B}) : \Phi) = es^2$. Кроме того, $\mathfrak{A}' \times \mathfrak{B} = \mathfrak{E}_r$, так что $(\mathfrak{A}' \times \mathfrak{B} : \Phi) = n(\mathfrak{B} : \Phi) = er^2$. Следовательно, $n(\mathfrak{B} : \Phi)(\mathfrak{A}(\mathfrak{B}) : \Phi) = e^2r^2s^2 = n^2 = (\mathfrak{A} : \Phi)^2$ и $(\mathfrak{B} : \Phi)(\mathfrak{A}(\mathfrak{B}) : \Phi) = (\mathfrak{A} : \Phi)$.

Теорема 19. *Пусть $\mathfrak{A}$ является центральной простой алгеброй и $\mathfrak{B}$ — простой подалгеброй, содержащей единицу. Тогда, если $\mathfrak{A}(\mathfrak{B})$ является централизатором подалгебры $\mathfrak{B}$ и $\mathfrak{A}'$ — алгеброй, обратно изоморфной алгебре $\mathfrak{A}$, имеют место следующие утверждения:*

1. *Подалгебра* $\mathfrak{A}(\mathfrak{B})$ *проста и содержит единицу.*
2. $\mathfrak{A}(\mathfrak{A}(\mathfrak{B})) = \mathfrak{B}$.
3. *Если* $\mathfrak{B} \times \mathfrak{A}' = \mathfrak{E}_r$, *где* $\mathfrak{E}$ *— тело, то* $\mathfrak{A}(\mathfrak{B}) = \mathfrak{E}_s'$, *где* $\mathfrak{E}'$ *является телом, обратно изоморфным телу* $\mathfrak{E}$.
4. $(\mathfrak{A} : \Phi) = (\mathfrak{B} : \Phi)(\mathfrak{A}(\mathfrak{B}) : \Phi)$.

12. Подполя и поля расщепления. Предположим, что в предыдущей теореме $\mathfrak{B} = \mathfrak{F}$ является полем. Тогда $\mathfrak{A}(\mathfrak{F}) \supseteq \mathfrak{F}$, так что $(\mathfrak{A} : \Phi) = (\mathfrak{F} : \Phi)(\mathfrak{A}(\mathfrak{F}) : \Phi) \geqslant (\mathfrak{F} : \Phi)^2$. Предположим далее, что $\mathfrak{A} = \mathfrak{D}$ является центральным телом. Тогда мы можем включить $\mathfrak{F}$ в такое поле $\overline{\mathfrak{F}}$, что $\mathfrak{D}(\overline{\mathfrak{F}}) = \overline{\mathfrak{F}}$. В самом деле, если $\mathfrak{D}(\mathfrak{F}) \supset \mathfrak{F}$, то мы можем выбрать элемент b, лежащий в $\mathfrak{D}(\mathfrak{F})$, но не в $\mathfrak{F}$, и получить поле $\mathfrak{F}_1 = \mathfrak{F}(b)$, содержащее $\mathfrak{F}$ как правильную часть. Если $\mathfrak{D}(\mathfrak{F}_1) \supset \mathfrak{F}_1$, то мы повторяем этот процесс. В конце концов, мы получим поле $\overline{\mathfrak{F}}$ с искомым свойством. Наши рассуждения показывают также, что если $\mathfrak{D}(\mathfrak{F}) \supset \mathfrak{F}$, то $\mathfrak{F}$ не будет максимальным подполем в $\mathfrak{D}$. Обратно, если поле $\mathfrak{F}$ не является максимальным, то $\mathfrak{F}$ лежит в большем поле $\mathfrak{F}_1$ и, следовательно, $\mathfrak{D}(\mathfrak{F}) \supset \mathfrak{F}$. Так как $\mathfrak{D}(\overline{\mathfrak{F}}) = \overline{\mathfrak{F}}$, то $(\mathfrak{D} : \Phi) = (\overline{\mathfrak{F}} : \Phi)^2$. Тем самым доказана

Теорема 20. *Размерность любого центрального тела* $\mathfrak{D}$ *является квадратом. Если* $(\mathfrak{D} : \Phi) = \delta^2$, *то* δ *будет размерностью любого максимального подполя тела* $\mathfrak{D}$.

Если $(\mathfrak{D} : \Phi) = \delta^2$, то δ называется *степенью* или индексом тела $\mathfrak{D}$, и если $\mathfrak{A} = \mathfrak{D}_m$, то δ называется *индексом* алгебры $\mathfrak{A}$. Очевидно, что размерность алгебры $\mathfrak{A}$ является квадратом $n = (\delta m)^2$. Если теперь $\mathfrak{F}$ является таким содержащим 1 подполем алгебры $\mathfrak{A}$, что $(\mathfrak{F} : \Phi) = \delta m$, то $\mathfrak{A}(\mathfrak{F}) = \mathfrak{F}$, и потому $\mathfrak{F}$ будет максимальным подполем алгебры $\mathfrak{A}$.

Применим теперь теорему 14 к $\mathfrak{B} = \mathfrak{F}$. Согласно этой теореме, $\mathfrak{F}' \times \mathfrak{D} = \mathfrak{E}_{s'}'$, где $\mathfrak{E}'$ является телом и $q = \delta m$ является делителем ms'. Таким образом, δ / s' и $\mathfrak{F}' \times \mathfrak{A} = \mathfrak{E}_{s'm}'$, где $\delta m / s'm$. Мы видели, что центром

алгебры $\mathfrak{F}' \times \mathfrak{A}$ будет $\mathfrak{F}'$ и что $\mathfrak{F}' \subseteq \mathfrak{E}'$. Следовательно,

$$((\mathfrak{F}' \times \mathfrak{A}) : \Phi) = (\mathfrak{F} : \Phi)(\delta m)^2 = (\mathfrak{E}' : \Phi)(s'm)^2.$$

Так как $s' \geqslant \delta$ и $(\mathfrak{E}' : \Phi) \geqslant (\mathfrak{F} : \Phi)$, то из предыдущего равенства следует, что $s' = \delta$ и $(\mathfrak{E}' : \Phi) = (\mathfrak{F} : \Phi)$. Следовательно, $\mathfrak{E}' = \mathfrak{F}'$ и $\mathfrak{F}' \times \mathfrak{A} = \mathfrak{F}_n'$. Так как $\mathfrak{F}$ является полем, то мы можем также написать, что $\mathfrak{F} \times \mathfrak{A} = \mathfrak{A}_{\mathfrak{F}} = \mathfrak{F}_n$.

Будем называть поле $\mathfrak{F}$ *полем расщепления* центральной простой алгебры $\mathfrak{A} = \mathfrak{D}_m$, если $\mathfrak{A}_{\mathfrak{F}} = \mathfrak{F}_n$. Так как $(\mathfrak{F}_n)_{\mathfrak{K}} = \mathfrak{K}_n$, если $\mathfrak{K} \supseteq \mathfrak{F}$, то любое поле, являющееся расширением поля расщепления, само будет полем расщепления. Если $\mathfrak{D}_{\mathfrak{F}} = \mathfrak{E}_s$, то $\mathfrak{A}_{\mathfrak{F}} = (\mathfrak{D}_m)_{\mathfrak{F}} = \mathfrak{E}_{sm}$. Следовательно, в силу той части теоремы Веддербарна, в которой говорится об однозначности, мы получаем, что если $\mathfrak{F}$ является полем расщепления для $\mathfrak{A}$, то оно будет им и для $\mathfrak{D}$. Очевидно, что и обратно, поле $\mathfrak{F}$ расщепляет $\mathfrak{A}$, если оно расщепляет $\mathfrak{D}$. В самом деле, если $\mathfrak{D}_{\mathfrak{F}} = \mathfrak{F}_\delta$, то $\mathfrak{A}_{\mathfrak{F}} = \mathfrak{F}_{\delta m}$. Результаты, полученные нами в предыдущем абзаце, доказывают достаточность условий следующей теоремы:

Теорема 21. *Для того чтобы поле* $\mathfrak{F}$ *было полем расщепления центрального тела* $\mathfrak{D}$ *степени* δ, *необходимо и достаточно, чтобы* $f = (\mathfrak{F} : \Phi)$ *было кратным* $m\delta$ *числа* δ *и чтобы* $\mathfrak{F}$ *было изоморфно содержащей единицу подалгебре алгебры* $\mathfrak{D}_m$.

Для доказательства необходимости этих условий применим следствие теоремы 11. Так как $\mathfrak{D}_{\mathfrak{F}} = \mathfrak{F} \times \mathfrak{D} = \mathfrak{F}_{\mathfrak{D}} = \mathfrak{F}_\delta$, то $f = m\delta$ и $\mathfrak{F}$ обладает обратным представлением в $\mathfrak{D}_m$. Так как $\mathfrak{F}$ является полем, то $\mathfrak{F}$ изоморфно содержащему единицу подполю алгебры $\mathfrak{D}_m$.

Из существования поля расщепления центральной простой алгебры вытекает

Теорема 22. *Если* $\mathfrak{A}$ *— центральная простая алгебра и поле* Γ *— любое расширение поля* Φ *(не обязательно конечной размерности), то алгебра* $\mathfrak{A}_\Gamma$ *будет центральной и простой.*

В самом деле, пусть $\mathfrak{F}$ является полем расщепления конечной размерности. Тогда существует поле Σ, содержащее поля $\mathfrak{F}$ и Γ[1]), и $\mathfrak{A}_\Sigma = (\mathfrak{A}_\mathfrak{F})_\Sigma = \Sigma_n$. Следовательно, $(\mathfrak{A}_\Gamma)_\Sigma = \Sigma_n$. Так как расширение любого идеала алгебры $\mathfrak{A}_\Gamma$ будет идеалом в $(\mathfrak{A}_\Gamma)_\Sigma$, то алгебра $\mathfrak{A}_\Gamma$ проста. Подобным же образом доказываем, что алгебра $\mathfrak{A}_\Gamma$ центральна.

13. Группа Брауера. Мы видели, что прямое произведение любых двух центральных простых алгебр является центральной простой алгеброй. Рассмотрим структуру прямого произведения $\mathfrak{A}' \times \mathfrak{A}$, где $\mathfrak{A}$ является центральной простой алгеброй и алгебра $\mathfrak{A}'$ обратно изоморфна алгебре $\mathfrak{A}$. Для этой цели применим теорему 14 к случаю, когда $\mathfrak{B} = \mathfrak{A}$. Мы получим тогда, что $\mathfrak{A}' \times \mathfrak{A} = \mathfrak{E}_{s'm}$, причем $n = (\mathfrak{A} : \Phi)$ является делителем числа $s'm$. Из сравнения размерностей над Φ мы получаем, что $s'm = n$ и $\mathfrak{E}' = \Phi$. Следовательно, нами доказана

Теорема 23. *Если $\mathfrak{A}$ является центральной простой алгеброй и $\mathfrak{A}'$ является алгеброй, обратно изоморфной алгебре $\mathfrak{A}$, то $\mathfrak{A}' \times \mathfrak{A} = \Phi_n$.*

Второе, более прямое доказательство этой теоремы проводится следующим образом: пусть $\mathfrak{A}_r$ и $\mathfrak{A}_l$ обозначают, соответственно, алгебры правых и левых умножений в $\mathfrak{A}$. Рассмотрим $\mathfrak{A}_r\mathfrak{A}_l = \mathfrak{A}_l\mathfrak{A}_r$. Элементами этой алгебры будут линейные преобразования алгебры $\mathfrak{A}$, рассматриваемой как n-мерное векторное пространство над Φ. Отметим также, что алгебра $\mathfrak{A}' \times \mathfrak{A}$ гомоморфно отображается на $\mathfrak{A}_l\mathfrak{A}_r$, и так как алгебра $\mathfrak{A}' \times \mathfrak{A}$ проста, то эти алгебры изоморфны. Отсюда следует, что алгебра $\mathfrak{A}_l\mathfrak{A}_r$ содержит n^2 линейно независимых элементов. Следовательно, $\mathfrak{A}_l\mathfrak{A}_r$ изоморфна Φ_n, и это же справедливо для $\mathfrak{A}' \times \mathfrak{A}$.

Этот результат позволяет нам определить замечательную группу, открытую впервые Р. Брауером. Рассмотрим совокупность $\mathfrak{S}$ центральных простых алгебр над фиксированным полем Φ. Два элемента $\mathfrak{A}$ и $\mathfrak{B}$ множества $\mathfrak{S}$ называются *подобными* ($\mathfrak{A} \sim \mathfrak{B}$), если в их представлениях $\mathfrak{A} = \mathfrak{D}_m$, $\mathfrak{B} = \overline{\mathfrak{D}}_{\overline{m}}$ тела $\mathfrak{D}$ и $\overline{\mathfrak{D}}$ изоморфны. Так как тело $\mathfrak{D}$ определяется алгеброй $\mathfrak{A}$ с точностью до изоморфизма, то отношение подобия вполне определено. Очевидно, что это отношение обладает свойствами эквивалентности и, следовательно, определяет разложение $\mathfrak{S}$ на непересекающиеся множества $\{\mathfrak{A}\}$, $\{\mathfrak{B}\}$, ... ($\{\mathfrak{A}\}$ обозначает совокупность алгебр, подобных данной алгебре $\mathfrak{A}$). Элементами группы Брауера $\mathfrak{G}(\Phi)$ являются множества $\{\mathfrak{A}\}$. Умножение определяется следующим образом: $\{\mathfrak{A}\}\{\mathfrak{B}\} = \{\mathfrak{A} \times \mathfrak{B}\}$. Это определение однозначно. В самом деле, если $\mathfrak{A} = \mathfrak{D}_{n_1}^{(1)} \sim \overline{\mathfrak{A}} = \overline{\mathfrak{D}}_{\overline{m}_1}^{(1)}$ и $\mathfrak{B} = \mathfrak{D}_{n_2}^{(2)} \sim \overline{\mathfrak{B}} = \overline{\mathfrak{D}}_{\overline{m}_2}^{(2)}$, то $\mathfrak{A} \times \mathfrak{B} = (\mathfrak{D}^{(1)} \times \mathfrak{D}^{(2)})_{n_1 n_2}$ и $\overline{\mathfrak{A}} \times \overline{\mathfrak{B}} = (\overline{\mathfrak{D}}^{(1)} \times \overline{\mathfrak{D}}^{(2)})_{m_1 m_2}$. Центральные простые алгебры $\mathfrak{D}^{(1)} \times \mathfrak{D}^{(2)}$ и $\overline{\mathfrak{D}}^{(1)} \times \mathfrak{D}^{(2)}$ изоморфны, и, следовательно, соответствующие им тела также изоморфны. Класс алгебр матриц ($\mathfrak{A} \sim 1$) является единицей в группе $\mathfrak{G}$. В силу предшествующей теоремы, $\{\mathfrak{A}\}\{\mathfrak{A}'\} = \{1\}$, и потому $\{\mathfrak{A}'\} = \{\mathfrak{A}\}^{-1}$. Так как прямое умножение коммутативно и ассоциативно, то $\mathfrak{G}(\Phi)$ будет коммутативной группой.

Если P является полем над Φ, то отображение $\{\mathfrak{A}\} \to \{\mathfrak{A}_P\}$ будет гомоморфным отображением $\mathfrak{G}(\Phi)$ на подгруппу группы $\mathfrak{G}(P)$. В самом деле, $(\mathfrak{A} \times \mathfrak{B})_P = \mathfrak{A}_P \times \mathfrak{B}_P$.

Нашей главной целью в §§ 14 — 16 будет доказательство теоремы о конечности порядка каждого элемента группы $\mathfrak{G}(\Phi)$. До сих пор нам приходилось ссылаться лишь на результаты, полученные в этой книге. Теперь, однако, мы должны изложить часть теории коммутативных полей. В частности, нами будут использованы результаты § 6, которые до сих пор служили лишь иллюстрацией к теории прямых произведений.

14. Сепарабельные подполя. Предположим, что поле Φ имеет характеристику $p \neq 0$ и что $\mathfrak{D}$ является центральным телом степени p. Если a является любым элементом тела $\mathfrak{D}$, не лежащим в Φ, то $\Phi(a)$ будет под-

[1]) Точнее говоря, содержащее подполя, изоморфные полям $\mathfrak{F}$ и Γ.

полем тела $\mathfrak{D}$, имеющим размерность p над Φ, и если b является не лежащим в $\Phi(a)$ элементом из $\mathfrak{D}$, то алгебра, порожденная элементами a и b, будет совпадать с $\mathfrak{D}$. Предположим теперь, что элемент a не будет сепарабельным элементом над Φ, так что $a^p = \alpha \in \Phi$. Рассмотрим дифференцирование $x \to x' = [x, a]$. Если $x \notin \Phi(a)$, то $x' \neq 0$. Однако, $x^{(p)} = [x, a^{(p)}] = 0$. Следовательно, существует такое целое число $k \geqslant 1$, что $x^{(k)} \neq 0$, но $x^{(k+1)} = 0$. Если мы положим $b = x^{(k-1)}(x^{(k)})^{-1}$ и $c = ab$, то получим, что $b' = 1$ и $c' = a$. Таким образом

$$[c^p, a] = [c \underbrace{[\ldots [c, a] \ldots]}_{p}] = a.$$

Следовательно, $[c^p - c, a] = 0$ и $c^p = c + g(a)$, где $g(a) \in \Phi(a)$. Очевидно, что $g(a)$ коммутирует с элементами c и a и, следовательно, $g(a) = \gamma \in \Phi$, и c является сепарабельным элементом.

Лемма. *Если центральное тело $\mathfrak{D}$ степени p и характеристики p содержит элемент, несепарабельный над Φ, то $\mathfrak{D}$ содержит также и сепарабельный элемент, не входящий в Φ.*

Отметим, что элемент b удовлетворяет уравнению вида $b^p = \beta$, так как $[b^p, a] = 0$. Элементы $b^i a^j$, $i, j = 0, \ldots, p-1$, образуют базис тела $\mathfrak{D}$, и умножение определяется следующими соотношениями:

$$a^p = \alpha, \quad b^p = \beta, \quad ba - ab = 1.$$

Таким же образом мы можем использовать в качестве образующих элементы a и c, связанные следующими соотношениями:

$$a^p = \alpha, \quad c^p = c + \gamma, \quad a^{-1}ca = c + 1.$$

Так как элементы $c+1$, $c+2, \ldots, c+(p-1)$ удовлетворяют уравнению $t^p = t + \gamma$, то $\Phi(c)$ будет циклическим полем над Φ с образующим автоморфизмом $c \to c + 1$.

Предыдущая лемма может быть применена при доказательстве следующей теоремы:

Теорема 24. *Любое центральное над полем Φ тело $\mathfrak{D}$ содержит максимальное сепарабельное подполе.*

Если Φ имеет характеристику нуль, то теорема очевидна. Предположим, что характеристика p поля Φ не равна нулю. Пусть a_1 является сепарабельным элементом из $\mathfrak{D}$ и $(\Phi(a_1) : \Phi) = r_1 > 0$. Если $\mathfrak{B}$ является алгеброй, состоящей из элементов, коммутирующих с элементами из $\Phi(a_1)$, то $(\mathfrak{D} : \Phi) = \delta^2 = (\Phi(a_1) : \Phi)(\mathfrak{B} : \Phi) = r_1 b$, где $b = (\mathfrak{B} : \Phi)$. Поле $\Phi(a_1)$ будет центром алгебры $\mathfrak{B}$. Если $\mathfrak{B}$ содержит сепарабельный над $\Phi(a_1)$ элемент a_2 и $(\Phi(a_1, a_2) : \Phi(a_1)) = r_2 > 0$, то $\Phi(a_1, a_2)$ будет сепарабельным полем размерности $r_1 r_2$ над Φ. Этот процесс приводит или к максимальному сепарабельному подполю над Φ, или к центральному телу, все подполя которого, содержащие центр как собственное подмножество, чисто несепарабельны. Пусть $\mathfrak{D}$ будет таким телом и Φ — его центром. Если $\mathfrak{F} = \Phi(a_1, a_2, \ldots, a_k)$ является максимальным подполем тела $\mathfrak{D}$, то каждый из элементов a_i удовлетворяет уравнению вида $a_i^{p^{m_i}} = \alpha_i$. Следовательно, $\mathfrak{F}$ содержит такое подполе $\mathfrak{F}_0$, что $(\mathfrak{F} : \mathfrak{F}_0) = p$ и $\mathfrak{F} = \mathfrak{F}_0(a)$, где $a^p \in \mathfrak{F}_0$. Элементы, коммутирующие с элементами из $\mathfrak{F}_0$, образуют центральное тело $\mathfrak{B}$ степени p над $\mathfrak{F}_0$. Так как $\mathfrak{B}$ содержит такой элемент a, что $a \notin \mathfrak{F}_0$, но $a^p \in \mathfrak{F}_0$, то $\mathfrak{B}$ содержит такой элемент c, что $c^p - c = g(a) \in \mathfrak{F}_0$, но $c \notin \mathfrak{F}_0$. Тогда элемент

$$(c^p - c)^{p^m} = c^{p^{m+1}} - c^{p^m} = (c^{p^m})^p - (c^{p^m}) = g(a)^{p^m}$$

лежит в Φ, если m достаточно велико. Следовательно, c^{p^m} будет сепарабельным элементом над Φ, причем $c^{p^m} \notin \Phi$, так как из $c^{p^m} = c^{p^{m-1}} + g(a)^{p^{m-1}}$, $c^{p^{m-1}} = c^{p^{m-2}} + g(a)^{p^{m-2}}, \ldots$ следует, что $\Phi(c^{p^m}, \mathfrak{F}_0) = \Phi(c, \mathfrak{F}_0) \supset \mathfrak{F}_0$. Таким образом, предположение, что $\mathfrak{D}$ содержит лишь чисто несепарабельные подполя, приводит к противоречию, и, следовательно, теорема доказана.

15. Скрещенные произведения. Пусть $\mathfrak{D}$ является центральным телом степени δ; обозначим через $\mathfrak{F}$ максимальное сепарабельное подполе тела $\mathfrak{D}$. Тогда $\mathfrak{F}$ может быть расширено до нормального сепарабельного поля $\mathfrak{K}$ размерности $\nu = \delta m$ над Φ. Мы видели, что $\mathfrak{K}$ является полем расщепления и, следовательно, содержится в центральной простой алгебре $\mathfrak{D}_m$, подобной телу $\mathfrak{D}$. Кроме того, $\mathfrak{K}$ будет максимальным подполем алгебры $\mathfrak{D}_m$. Пусть $1, S, \ldots, V$ являются элементами группы Галуа $\mathfrak{G}$ поля $\mathfrak{K}$ над Φ. Так как автоморфизм $k \to k^S$ поля $\mathfrak{K}$ может быть продолжен до внутреннего автоморфизма алгебры $\mathfrak{D}_m$, то существует такой обратимый элемент $u_S \in \mathfrak{D}_m$, что $u_S^{-1} k u_S = k^S$ или, иначе, $k u_S = u_S k^S$ для всех $k \in \mathfrak{K}$. Элемент $u_{ST}^{-1} u_S u_T$ перестановочен со всеми элементами k и, следовательно, $u_S u_T = u_{ST} \rho_{S,T}$, где $\rho \in \mathfrak{K}$. В силу ассоциативного закона получаем

$$\rho_{S,T,U} \rho_{T,U} = \rho_{ST,U} \rho_{S,T}^{U},$$

и потому $\rho = \{\rho_{S,T}\}$ образуют систему факторов. Рассмотрим теперь скрещенное произведение $\mathfrak{K}(\mathfrak{G}, \rho)$ поля $\mathfrak{K}$ с его группой Галуа $\mathfrak{G}$, имеющее в качестве системы факторов $\{\rho_{S,T}\}$ [1]. Очевидно, что оно гомоморфно отображается на подалгебру $\mathfrak{B}$ алгебры $\mathfrak{D}_m$, состоящую из элементов вида $\sum u_S k_S$. Так как алгебра $\mathfrak{K}(\mathfrak{G}, \rho)$ проста, то она изоморфна алгебре $\mathfrak{B}$, и так как $(\mathfrak{K}(\mathfrak{G}, \rho) : \Phi) = \nu^2$, то $\mathfrak{B} = \mathfrak{D}_m$.

Теорема 25. *Любая центральная простая алгебра подобна некоторому скрещенному произведению* $\mathfrak{K}(\mathfrak{G}, \rho)$.

Эта теорема позволяет нам применить теорию скрещенных произведений к центральным простым алгебрам. Напомним, что, по определению, системы факторов $\rho_{S,T}$ и $\sigma_{S,T}$ ассоциированы, если существуют такие элементы $\mu_S \in \mathfrak{K}$, что $\rho_{S,T} = \sigma_{S,T} \frac{\mu_{ST}}{\mu_S^T \mu_T}$. Следовательно, если v_S

[1] Так как соответствие здесь является тождественным, то мы можем применить это упрощение обозначений главы 4.

является другим множеством таких элементов из $\mathfrak{D}_m = \mathfrak{K}(\mathfrak{G}, \rho)$, что $v_S^{-1} k v_S = k^S$, то $u_S^{-1} v_S \in \mathfrak{K}$ и $v_S = u_S \mu_S$. Тогда, если $v_S v_T = v_{ST} \sigma_{S,T}$, то системы ρ и σ ассоциированы ($\rho \infty \sigma$). При этих определениях мы имеем следующую теорему.

Теорема 26. $\mathfrak{K}(\mathfrak{G}, \rho) \infty 1$ *тогда и только тогда, когда* $\rho \infty 1$.

Если $\rho \infty 1$, то мы заменяем элементы u_S элементами $v_S = u_S \mu_S$ и получаем $v_S v_T = v_{ST}$. Из § 18 главы 4 следует, что $\mathfrak{K}(\mathfrak{G}, \rho)$ изоморфно Φ_ν. Обратно, предположим, что $\mathfrak{K}(\mathfrak{G}, \rho) \infty 1$. Тогда $\mathfrak{K}(\mathfrak{G}, \rho)$ изоморфно $\mathfrak{K}(\overline{\mathfrak{G}}, 1)$ и, следовательно, $\mathfrak{K}(\mathfrak{G}, \rho)$ содержит такое поле $\mathfrak{K}_1$, изоморфное полю $\mathfrak{K}$, и такие элементы v_{S_1}, что каждый его элемент имеет вид $\sum v_{S_1} k_{S_1}^{(1)}$, где $k^{(1)} \in \mathfrak{K}_1$, и

$$k^{(1)} v_{S_1} = v_{S_1} k^{(1)S_1}, \quad v_{S_1} v_{T_1} = v_{S_1 T_1}, \tag{4}$$

где S_1 лежит в группе Галуа поля $\mathfrak{K}_1$. Мы можем предположить, что S_1 является автоморфизмом $k_1 \to (k^S)_1$, где $k \to k_1$ — некоторый заданный изоморфизм между $\mathfrak{K}$ и $\mathfrak{K}_1$. Этот изоморфизм может быть продолжен до некоторого автоморфизма $a \to a_1$ алгебры $\mathfrak{K}(\mathfrak{G}, \rho)$. Если $u_{S_1} = (u_S)_1$, то мы имеем

$$k^{(1)} u_{S_1} = u_{S_1} k^{(1)S_1}, \quad u_{S_1} u_{T_1} = u_{S_1 T_1} \rho_{S,T}^{(1)}.$$

Если мы сравним это с (4), то получим, что $\rho^{(1)} \infty 1$ и, следовательно, $\rho \infty 1$.

Рассмотрим теперь скрещенные произведения $\mathfrak{K}_1(\mathfrak{G}_1, \rho_1)$ и $\mathfrak{K}_2(\mathfrak{G}_2, \sigma_2)$, где $\mathfrak{K}_1 \cong \mathfrak{K}_2$ и изоморфизмом между $\mathfrak{K}_1$ и $\mathfrak{K}_2$ является соответствие $k_1 \to k_2$. Пусть S_1 и S_2 будут соответствующими автоморфизмами из групп Галуа $\mathfrak{G}_1$ и $\mathfrak{G}_2$ в том смысле, что $k_1^{S_1} \to k_2^{S_2}$. Мы хотим найти, чему равно $\mathfrak{K}_1(\mathfrak{G}_1, \rho_1) \times \mathfrak{K}_2(\mathfrak{G}_2, \sigma_2)$.

Очевидно, что $\mathfrak{K}_1(\mathfrak{G}_1, \rho_1) \times \mathfrak{K}_2(\mathfrak{G}_2, \sigma_2)$ содержит $\mathfrak{K}_1 \times \mathfrak{K}_2$. Последнее произведение является прямой суммой ν полей, изоморфных полю $\mathfrak{K}_1$. Если e_i будет единицей одной из его компонент, то элементы этой компоненты имеют вид $e_i k_2$, где $k_2 \in \mathfrak{K}_2$, т. е. $\mathfrak{K}_1 \times \mathfrak{K}_2 =$

$= e_1\mathfrak{K}_2 \oplus \ldots \oplus e_\nu\mathfrak{K}_2$. Подобно этому $e_i\mathfrak{K}_2 = e_i\mathfrak{K}_1$. Соответствие $k_1 \to k_2^{(i)}$, получающееся из равенства $e_i k_1 = e_i k_2^{(i)}$, является (обратным) представлением $\mathfrak{K}_1$ в $\mathfrak{K}_2$, и мы видели, что таким образом получаются все (с точностью до подобия, которое в этом случае совпадает с идентичностью) неприводимые представления $\mathfrak{K}_1$ в $\mathfrak{K}_2$. С другой стороны, мы имеем ν различных представлений $k_1 \to k_2^{S_2}$, где S_2 пробегает группу $\mathfrak{G}_2$. Следовательно, $k_2^{(i)} = k_2^{S_2}$ и идемпотентные элементы стоят во взаимно-однозначном соответствии с элементами группы $\mathfrak{G}_2$. Мы можем поэтому обозначить e_i через e_{S_2}; тогда

$$\sum e_{S_2} = 1, \quad e_{S_2} e_{T_2} = 0, \quad \text{если} \quad S_2 \neq T_2,$$
$$e_{S_2}^2 = e_{S_2}, \quad e_{S_2}(k_1 - k_2^{S_2}) = 0.$$

Отображения $x \to v_{T_2}^{-1} x v_{T_2}$ и $x \to u_{T_1}^{-1} x u_{T_1}$ являются автоморфизмами в $\mathfrak{K}_1 \times \mathfrak{K}_2$. Так как простые компоненты полупростой алгебры однозначно определены, то элементы $v_{T_2}^{-1} e_{S_2} v_{T_2}$ и $u_{T_1}^{-1} e_{S_2} u_{T_1}$ снова являются элементами e_i. Так как v_{T_2} коммутирует с k_1 и $v_{T_2}^{-1} k_2 v_{T_2} = k_2^{T_2}$, то

$$v_{T_2}^{-1} e_{S_2} v_{T_2} (k_1 - k_2^{S_2 T_2}) = 0.$$

Следовательно, $v_{T_2}^{-1} e_{S_2} v_{T_2} = e_{S_2 T_2}$ и подобно этому

$$u_{T_1}^{-1} e_{S_2} u_{T_1} = e_{T_2^{-1} S_2}.$$

Мы определяем теперь $e_{S,T} = v_{S_2}^{-1} v_{T_2} e_{T_2}$ и проверяем, что

$$e_{S,T} e_{U,V} = \delta_{T,U} e_{S,V}, \quad \sum e_{S,S} = 1.$$

Эти матричные единицы могут быть использованы для представления $\mathfrak{K}_1(\mathfrak{G}_1, \rho_1) \times \mathfrak{K}_2(\mathfrak{G}_2, \sigma_2)$ в виде $\mathfrak{K}_1(\mathfrak{G}_1, \rho_1) \times \mathfrak{K}_2(\mathfrak{G}_2, \sigma_2) = \mathfrak{B}_\nu$, где $\mathfrak{B}$ является совокупностью элементов, коммутирующих со всеми элементами $e_{S,T}$, и изоморфна с $e_{1,1}(\mathfrak{K}_1 \mathfrak{G}_1, \rho_1) \times \mathfrak{K}_2(\mathfrak{G}_2, \sigma_2)) e_{1,1} = \overline{\mathfrak{B}}$. В силу

отмеченных выше соотношений, имеем $e_{1,1} u_{S_1} v_{S_2} = u_{S_1} v_{S_2} e_{1,1} = w_S \in \overline{\mathfrak{B}}$ и $\overline{k}_1 \equiv k_1 e_{1,1} = k_2 e_{1,1} \equiv \overline{k}_2 \in \overline{\mathfrak{B}}$. Тогда

$$\overline{w}_S \overline{w}_T = \overline{w}_{ST} \overline{\rho}_{1S_1, T_1} \overline{\sigma}_{2S_2, T_2}, \quad \overline{k}\overline{w}_S = \overline{w}_S \overline{k}^S,$$

где $k \equiv \overline{k}_1$ и $\overline{k}^S = \overline{k}_1^{S_1}$. Мы показали, что $\overline{\mathfrak{B}}$ содержит скрещенное произведение $\overline{\mathfrak{K}}(\overline{\mathfrak{G}}, \overline{\rho}_1 \overline{\sigma}_2)$, а так как его размерность над Φ равна ν^2, то $\overline{\mathfrak{B}}$ совпадает с этим скрещенным произведением. Следовательно, нами доказана следующая

Теорема 27. *Пусть поля $\mathfrak{K}_1$ и $\mathfrak{K}_2$ являются изоморфными сепарабельными нормальными расширениями поля Φ и $k_1 \to k_2$ — изоморфизмом между ними. Тогда $\mathfrak{K}_1(\mathfrak{G}_1, \rho_1) \times \mathfrak{K}_2(\mathfrak{G}_2, \sigma_2) \infty \overline{\mathfrak{K}}(\overline{\mathfrak{G}}, \overline{\rho}_1, \overline{\sigma}_2)$, где $\overline{\mathfrak{K}}$ изоморфно $\mathfrak{K}_i$ и $k_i \to \overline{k}_i$ является таким изоморфизмом между $\mathfrak{K}_i$ и $\overline{\mathfrak{K}}$, что $\overline{k}_1 = \overline{k}_2$.*

Эта теорема имеет следующее значение: пусть $\rho_{S,T}$ и $\sigma_{S,T}$ являются системами факторов. Произведением их назовем систему факторов $\tau_{S,T} = \rho_{S,T} \sigma_{S,T}$. Множество систем факторов образует относительно этого умножения коммутативную группу. Системы факторов вида $\rho_{S,T} = \frac{\mu_{ST}}{\mu_S^T \mu_T}$ образуют подгруппу, и две системы факторов, принадлежащие одному и тому же смежному классу по этой подгруппе, ассоциированы между собой. Если $\mathfrak{H}_\mathfrak{K}$ является фактор-группой, элементами которой будут классы ассоциированных систем факторов, и $\mathfrak{G}_\mathfrak{K}(\Phi)$ — подгруппой группы Брауера поля Φ, состоящей из таких классов центральных простых алгебр, которые имеют $\mathfrak{K}$ полем расщепления, то, по нашей теореме, группы $\mathfrak{H}_\mathfrak{K}$ и $\mathfrak{G}_\mathfrak{K}(\Phi)$ изоморфны.

Теорема 28. *Если алгебра $\mathfrak{K}(\mathfrak{G}, \rho)$ имеет индекс δ, то $\rho^\delta \infty 1$.*

Пусть $\mathfrak{K}(\mathfrak{G}, \rho) = \mathfrak{D}_m$, где $\mathfrak{D}$ — центральное тело. Тогда $\mathfrak{D}_m = \mathfrak{J}_1 \oplus \ldots \oplus \mathfrak{J}_m$, где $\mathfrak{J}_i$ являются изоморфными неприводимыми правыми идеалами, имеющими, следова-

тельно, одну и ту же размерность, если рассматривать их как векторные пространства над $\mathfrak{K}$. Так как $(\mathfrak{D}_m : \mathfrak{K}) = \nu$ и $(\mathfrak{D}_m : \Phi) = \nu^2 = \delta^2 m^2$, то $(\mathfrak{J}_i : \mathfrak{K})\, m = \nu$ и $(\mathfrak{J}_i : \mathfrak{K}) = \delta$. Элементы u_S определяют полулинейные преобразования пространства $\mathfrak{J}_i$ над $\mathfrak{K}$. Следовательно, если элементы $x_1, \ldots, x_\delta$ образуют базис пространства $\mathfrak{J}_i$ над $\mathfrak{K}$ и $x_i u_S = \sum x_j \mu_{jiS}$, где $\mu \in \mathfrak{K}$, то матрицы $M_S = (\mu_{jiS})$ удовлетворяют уравнениям $M_T M_S^T = M_{ST} \rho_{S,T}$. Если мы положим $\det M_S = \mu_S$, то получим, что $\rho_{S,T}^\delta \mu_{S,T} = \mu_S^T \mu_T$. Следовательно, $\rho^\delta \infty 1$.

16. Экспонент центральной простой алгебры. Из результатов предыдущего параграфа вытекает

Теорема 29. *Если $\mathfrak{A}$ является центральной простой алгеброй индекса δ, то $\{\mathfrak{A}\}^\delta = 1$, т. е. прямое произведение δ алгебр, изоморфных алгебре $\mathfrak{A}$, имеет вид $\Phi_{m\delta}$.*

В самом деле, мы видели, что $\mathfrak{A} \infty \mathfrak{K}(\mathfrak{G}, \rho)$ и $\mathfrak{A}_1 \times \ldots \times \mathfrak{A}_\delta \infty \mathfrak{K}(\mathfrak{G}, \rho^\delta)$, если $\mathfrak{A}_i \cong \mathfrak{A}$. Так как $\rho^\delta \infty 1$, то $\mathfrak{A}_1 \times \ldots \times \mathfrak{A}_\delta \infty 1$. Таким образом, порядок каждого элемента группы Брауера конечен. Порядок e класса алгебр $\{\mathfrak{A}\}$ назовем *экспонентом* центральной простой алгебры $\mathfrak{A}$. Предыдущая теорема показывает, что экспонент является делителем индекса алгебры $\mathfrak{A}$.

Теорема 30. *Каждый простой делитель p индекса алгебры $\mathfrak{A}$ является делителем экспонента этой алгебры.*

Если $\mathfrak{F}$ является полем, содержащим поле Φ, то, как мы видели, соответствие между $\{\mathfrak{A}\}$ и $\{\mathfrak{A}_\mathfrak{F}\}$ будет гомоморфным отображением группы Брауера над Φ на подгруппу группы Брауера над $\mathfrak{F}$. Следовательно, экспонент $e_\mathfrak{F}$ алгебры $\mathfrak{A}_\mathfrak{F}$ является делителем экспонента алгебры $\mathfrak{A}$. Пусть теперь $\mathfrak{A} \infty \mathfrak{K}(\mathfrak{G}, \rho) = \mathfrak{D}_m$, где $(\mathfrak{K} : \Phi) = \nu = \delta m$. Пусть p^s будет наибольшей степенью простого числа p, делящей ν, и $\mathfrak{G}_p$ силовской подгруппой порядка p^s группы $\mathfrak{G}$. Для соответствующего группе $\mathfrak{G}_p$ подполя $\mathfrak{F}$ поля $\mathfrak{K}$ имеем $(\mathfrak{K} : \mathfrak{F}) = p^s$. Рассмотрим $\mathfrak{K}(\mathfrak{G}, \rho)_{\mathfrak{F}_1}$, где $\mathfrak{F}_1 \cong \mathfrak{F}$.

Так как полем расщепления для $\mathfrak{K}(\mathfrak{G}, \rho)\mathfrak{F}$ будет $\mathfrak{K}_1 \cong \mathfrak{K}$, и $(\mathfrak{K}_1 : \mathfrak{F}_1) = p^s$, то степенью $\mathfrak{K}(\mathfrak{G}, \rho)_{\mathfrak{F}_1}$ будет p^t, где $t \leqslant s$ и, следовательно, $e_{\mathfrak{F}_1} = p^u$, где $u \leqslant t$. Таким образом, $e \equiv 0 \pmod{e_{\mathfrak{F}_1}}$, $e \equiv 0 \pmod{p}$, за исключением того случая, когда $u = 0$. Если же $u = 0$, то $\mathfrak{K}(\mathfrak{G}, \rho)_{\mathfrak{F}_1} \infty 1$ и, следовательно, $(\mathfrak{F}_1 : \Phi)$ делится на δ. Так как $(\mathfrak{F}_1 : \Phi) = \frac{\nu}{p^s}$ и $\left(\frac{\nu}{p^s}, p\right) = 1$, то это невозможно.

Докажем, наконец, следующую теорему, позволяющую во многих исследованиях о центральных телах сводить проблему к случаю степени вида p^h, где p — простое число.

Теорема 31. *Если $\mathfrak{D}$ является центральным телом степени $\delta = p_1^{s_1} \ldots p_l^{s_l}$, где p_i — различные простые числа, то $\mathfrak{D} = \mathfrak{D}_1 \times \ldots \times \mathfrak{D}_l$, где алгебра $\mathfrak{D}_i$ имеет степень $p_i^{s_i}$ и определена алгеброй $\mathfrak{D}$ с точностью до изоморфизма.*

Пусть $e = p_i^{t_1} \ldots p_l^{t_l}$, $0 < t_i \leqslant s_i$ является экспонентом $\mathfrak{D}$. В силу обычных теоретико-групповых рассуждений, имеем $\{\mathfrak{D}\} = \{\mathfrak{D}_1\} \ldots \{\mathfrak{D}_l\}$, где $\{\mathfrak{D}_i\}^{p^{t_i}} = 1$. Мы можем предполагать, что $\mathfrak{D}_i$ является телом. Тогда его степень равна $p_i^{s_i'}$, где $s_i' \geqslant t_i$. Так как степени тел $\mathfrak{D}_i$ взаимно просты, то их прямое произведение $\mathfrak{D}_1 \times \ldots \times \mathfrak{D}_l$ будет телом, и так как оно подобно телу $\mathfrak{D}$, то $\mathfrak{D} \cong \mathfrak{D}_1 \times \ldots \times \mathfrak{D}_l$ и $s_i' = s_i$. Если теперь $\mathfrak{D} = \mathfrak{D}_1 \times \ldots \times \mathfrak{D}_l = \mathfrak{C}_1 \times \ldots \times \mathfrak{C}_l$, где $\mathfrak{C}_i$ имеет степень $p_i^{s_i}$, то $\mathfrak{D}_i^{q_i} \infty \mathfrak{C}_i^{q_i}$, если $q^i = e p_i^{-t_i}$. Так как $(q_i, p_i^{t_i}) = 1$, то существуют такие целые числа a_i, b_i, что $q_i a_i + p_i^{t_i} b_i = 1$. Тогда $(\mathfrak{D}_i^{q_i})^{a_i} \infty (\mathfrak{C}_i^{q_i})^{a_i}$, $\mathfrak{D}_i \infty \mathfrak{C}_i$, и так как обе эти алгебры являются телами, то $\mathfrak{D}_i \cong \mathfrak{C}_i$.

17. Центральные тела над специальными полями. Любой элемент a алгебры $\mathfrak{A}$ удовлетворяет некоторому уравнению $\varphi(a) = 0$, где $\varphi(t)$ является отличным от нуля полиномом из $\Phi[t]$. В самом деле, положим $a^0 = 1$, если $\mathfrak{A}$ обладает единицей, и $a^0 = 0$ в противном случае,

и рассмотрим последовательность $a^0, a^1, a^2, \ldots$ Она содержит лишь конечное число линейно независимых элементов. Следовательно, найдется такое m, $0 < m \leqslant n$, где через n обозначена размерность алгебры $\mathfrak{A}$, что $a^m = a^{m-1}\alpha_1 + \ldots + a^0\alpha_m$. Таким образом, $\varphi(a) = 0$ для $\varphi(t) = t^m - t^{m-1}\alpha_1 - \ldots - t^0\alpha_m$, где $t^0 = 1$ или 0 соответственно тому, равно ли $a^0 = 1$ или 0. Пусть теперь m минимально. Тогда элементы a^i при $i < m$ линейно независимы, и потому элементы α_i, необходимые для выражения a^m через a^i, $i < m$, однозначно определены. Отсюда следует, что соответствующий полином $\varphi(t) \equiv \mu_a(t)$ является единственным полиномом степени m со старшим коэффициентом 1, для которого a будет корнем. Кроме того, ясно, что m является наименьшей степенью всех таких полиномом $\varphi(t) \neq 0$, что $\varphi(a) = 0$. При помощи деления мы можем показать также, что $\mu_a(t)$ является делителем любого такого полинома $\varphi(t)$, что $\varphi(a) = 0$. Назовем полином $\mu_a(t)$ *минимальным полиномом* элемента a.

Если $\mathfrak{A}$ является телом, то полином $\mu_a(t)$ неприводим. В самом деле, если $\mu_a(t) = \mu^{(1)}(t)\mu^{(2)}(t)$, то $\mu^{(1)}(a)\mu^{(2)}(a) = 0$, и потому либо $\mu^{(1)}(a) = 0$, либо $\mu^{(2)}(a) = 0$. В силу минимальности степени полинома $\mu_a(t)$, либо $\mu^{(1)}(t)$, либо $\mu^{(2)}(t)$ имеет степень нуль. Если теперь поле Ф алгебраически замкнуто, то все неприводимые полиномы линейны, и потому для любого элемента a имеем $a - 1\alpha = 0$ или $a = 1\alpha$. Итак, доказана

Теорема 32. *Единственным телом над алгебраически замкнутым полем* Ф *будет само поле* Ф.

Предположим, что Ф является действительно замкнутым полем. Хорошо известно, что единственными алгебраическими расширениями поля Ф являются само Ф и $\Phi(i)$, где $i^2 = -1$. [1] Пусть $\mathfrak{A} \neq \Phi$ будет центральным телом над Ф. Если $(\mathfrak{A} : \Phi) = m^2$, где $m > 1$, то существует такое максимальное подполе Σ тела $\mathfrak{A}$, что $(\Sigma : \Phi) = m$. Следовательно, $\Sigma = \Phi(i)$ и $m = 2$. Так как поле $\Phi(i)$

[1] См. Ван-дер-Варден, Современная алгебра, том 1, стр. 224.

нормально, то $\mathfrak{A}$ является скрещенным произведением, и потому существует такой второй элемент j тела $\mathfrak{A}$, что $j^{-1}ij = -i$, $j^2 = 1\beta$. Элемент β отрицателен, и j может быть нормирован таким образом, чтобы $j^2 = -1$. Следовательно, тело $\mathfrak{A}$ обладает базисом, состоящим из элементов 1, i, j, $k = ij$, причем

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji,$$

и $\mathfrak{A}$ будет кватернионной алгеброй Гамильтона. Как известно, алгебра $\mathfrak{A}$ такого вида является телом. Если $\mathfrak{A}$ — нецентральное тело над Ф, то центром алгебры $\mathfrak{A}$ будет алгебраически замкнутое поле $\Phi(i)$. Следовательно, в силу теоремы 32, $\mathfrak{A} = \Phi(i)$.

Теорема 33 (Фробениус). *Единственными телами над действительно замкнутым полем* Ф *являются* Ф, $\Phi(i)$ *и алгебра кватернионов* $\Phi(i, j)$.

Пусть теперь Ф является конечным полем и $\mathfrak{A}$ — центральным телом над Ф. Обозначим мультипликативную группу отличных от нуля элементов тела $\mathfrak{A}$ через $\mathfrak{A}'$. Если Σ является максимальным подполем, то совокупность Σ' отличных от нуля элементов из Σ будет подгруппой группы $\mathfrak{A}'$. Любой элемент $b \neq 0$ может быть включен в максимальное подполе, и так как любое максимальное подполе имеет вид $u^{-1}\Sigma u$, то $b \in u^{-1}\Sigma' u$ при соответствующем элементе u. Таким образом $\mathfrak{A}'$ является теоретико-множественным объединением сопряженных с Σ' подгрупп. Но объединение всех подгрупп конечной группы, сопряженных с данной подгруппой, может совпадать со всей группой лишь тогда, когда эта подгруппа совпадает со всей группой. Следовательно, $\Sigma' = \mathfrak{A}'$, и тело $\mathfrak{A}$ коммутативно. Таким образом, $\mathfrak{A} = \Phi$.

Теорема 34. (Веддербарн). *Единственным центральным телом над конечным полем* Ф *является само поле* Ф.

Этим также доказано, что любое тело над конечным полем коммутативно. Кроме того, так как любое тело может рассматриваться как алгебра над своим центром, то эта теорема справедлива для произвольных конечных тел.

18. Минимальный полином алгебры. В дальнейшем в этой главе мы будем рассматривать алгебры, которые могут не быть простыми. Мы определим специальный класс полупростых алгебр, называемых сепарабельными, и дадим конструктивный критерий принадлежности алгебры к этому классу. Если поле Φ имеет характеристику нуль, то каждая полупростая алгебра сепарабельна, так что в этом случае критерий сепарабельности совпадает с критерием полупростоты. Мы получим также, следуя Веддербарну, структурную теорему, которая в некотором смысле сводит изучение произвольных алгебр к изучению полупростых и нильпотентных алгебр.

Рассмотрим сначала теорию минимального полинома элемента a произвольной алгебры $\mathfrak{A}$. Предположим, что мы имеем взаимнооднозначное представление $x \to X$ алгебры $\mathfrak{A}$ матрицами из алгебры матриц Φ_N, причем, если алгебра $\mathfrak{A}$ обладает единицей, то эта единица отображается в единицу алгебры Φ_N [1]). Пусть $\mathfrak{A}$ обозначает совокупность матриц, представляющих $\mathfrak{A}$, и пусть A является матрицей, соответствующей элементу a. Мы утверждаем, что тогда минимальный полином $\mu_a(t)$ элемента a будет также и минимальным полиномом матрицы A, рассматриваемой как элемент алгебры Φ_N. В самом деле, очевидно, что $\mu_a(t)$ является минимальным полиномом матрицы A, рассматриваемой как элемент алгебры $\bar{\mathfrak{A}}$. Из наших предположений следует, что если $\bar{\mathfrak{A}}$ обладает единицей, то эта единица является единицей алгебры Φ_N. Следовательно, в этом случае минимальный полином матрицы A в $\bar{\mathfrak{A}}$ совпадает с минимальным полиномом в Φ_N. Предположим теперь, что $\bar{\mathfrak{A}}$ не обладает единицей, и пусть $\mu_A(t) = t^m - t^{m-1}\alpha_1 - \ldots - 1\alpha_{m-1}$ будет минимальным полиномом A в Φ_N. Тогда элемент $1\alpha_m = A^m - A^{m-1}\alpha_1 - \ldots - A\alpha_{m-1}$ принадлежит к $\bar{\mathfrak{A}}$ и поэтому должен равняться нулю. Таким образом, постоянный член в $\mu_A(t)$ равен нулю и, следовательно, $\mu_A(t)$ будет минимальным полиномом

[1]) В этом рассуждении мы можем употреблять вместо обычных представлений обратные представления алгебры $\mathfrak{A}$.

элемента A в $\bar{\mathfrak{A}}$. Напомним теперь, что минимальный полином матрицы A равен последнему инвариантному множителю лежащей в $\Phi[t]_N$ матрицы $(1t - A)$. Следовательно, и $\mu_a(t)$ равен последнему инвариантному множителю матрицы $(1t - A)$, и если $f(t)$ является характеристическим полиномом, равным $\det(1t - A)$, то $\mu_a(t)$ будет делителем полинома $f(t)$. Так как $f(t)$ равен произведению всех инвариантных множителей, а каждый инвариантный множитель является делителем последнего из них, то каждый неприводимый делитель полинома $f(t)$ будет делителем полинома $\mu_a(t)$.

Пусть элементы $x_1, \ldots, x_n$ образуют базис алгебры $\mathfrak{A}$ над полем Φ и пусть $P = \Phi(\xi_1, \ldots, \xi_n)$ будет полем, полученным из Φ присоединением неизвестных ξ_i. Образуем алгебру $\mathfrak{A}_P$ и назовем элемент $x_1\xi_1 + \ldots + x_n\xi_n$ этой алгебры общим элементом алгебры $\mathfrak{A}$. Предположим теперь, что $x_i \to X_i$ является взаимнооднозначным представлением алгебры $\mathfrak{A}$ в Φ_N. Тогда $\sum x_i\gamma_i \to \sum X_i\gamma_i$, где $\gamma_i \in P$, будет взаимнооднозначным представлением $\mathfrak{A}_P$ в P_N, удовлетворяющим условию $1 \to 1$, если $\mathfrak{A}_P$ обладает единицей[1]). Поэтому можно применить вышеприведенные рассуждения к $\sum x_i\xi_i$. Мы видим, что $m(t, \xi)$ — последний инвариантный множитель матрицы $(1t - \sum X_i\xi_i)$ — является минимальным полиномом элемента $\sum x_i\xi_i$ и делителем характеристического полинома

$$f(t, \xi) = \det(t - \sum X_i\xi) = \\ = t^N - t^{N-1}\varphi_1(\xi) + \ldots + (-1)^N\varphi_N(\xi).$$

Так как коэффициенты полинома $f(t, \xi)$ являются полиномами от ξ_i, то из леммы Гаусса следует, что коэффициенты полинома $m(t, \xi)$ также будут полиномами от

[1]) Если некоторое расширение $\mathfrak{A}_P$ алгебры $\mathfrak{A}$ обладает единицей, то и $\mathfrak{A}$ обладает единицей. Это следует из известной теоремы о том, что система линейных уравнений с коэффициентами из Φ имеет решение в поле расширения P тогда и только тогда, когда она имеет решение в Φ. Детали доказательства предоставляются читателю.

ξ_i [1]. Мы показывали также, что полиномы $m(t, \xi)$ и $f(t, \xi)$ обладают одинаковыми неприводимыми множителями в $P[t]$, отличаясь самое большее кратностями этих множителей. Из определения $m(t, \xi)$ как минимального полинома для $\sum x_i \xi_i$ в $\mathfrak{A}_P$ следует, что $m(t, \xi)$ зависит лишь от $\sum x_i \xi_i$, а не от использованного частного представления. Мы будем называть этот полином *минимальным полиномом алгебры* $\mathfrak{A}$.

Пусть элементы $y_1, \ldots, y_n$, где $y_i = \sum x_j \mu_{ji}$, образуют второй базис алгебры $\mathfrak{A}$ и пусть $m'(t, \eta)$ будут минимальным полиномом, определенным общим элементом $\sum y_i \eta_i$. Если мы используем поле $\Sigma = \Phi(\xi, \eta)$, то мы можем сравнить $m(t, \xi)$ и $m'(t, \eta)$. Напомним теперь, что если элементы $a_1, \ldots, a_r$ линейно независимы в алгебре $\mathfrak{A}$, то они остаются линейно независимыми в любом расширении $\mathfrak{A}_\Sigma$ этой алгебры. Из этого следует, что минимальный полином элемента алгебры не изменяется, если расширить поле, над которым определена алгебра. Следовательно, $m(t, \xi)$ и $m'(t, \eta)$ будут минимальными полиномами соответственно элементов $\sum x_i \xi_i$ и $\sum y_i \eta_i$ в алгебре $\mathfrak{A}_\Sigma$. Так так $y_i = \sum x_j \mu_{ji}$, то $\sum y_i \eta_i = \sum x_j \xi'_j$, где $\xi'_j = \sum \mu_{ji} \eta_i$. Следовательно, $m(t, \xi') = m'(t, \eta)$. В этом смысле полином $m(t, \xi)$ является инвариантом алгебры $\mathfrak{A}$. Мы пишем

$$m(t, \xi) = t^r - t^{r-1} T(\xi) + \ldots + (-1)^r N(\xi).$$

Если ξ_i заменить некоторыми элементами из Φ, например, $\xi_i = \alpha_i$, то мы получим полином $m_a(t) = m(t, \alpha)$, называемый *главным полиномом*, связанным с элементом $a = \sum x_i \alpha_i$ алгебры $\mathfrak{A}$. Применяя соотношение $m(t, \xi') = m'(t, \eta)$, мы видим, что полином $m_a(t)$ не зависит от выбора базиса. Следовательно, это же имеет место и для функций $T(a) \equiv T(\alpha)$ и $N(a) \equiv N(\alpha)$, называемых соответственно *главным следом и главной нормой* элемента a. Равенство $m(x(\xi), \xi) = 0$ эквивалентно n

[1] См. Albert, Modern Higher Algebra, стр. 37.

полиноминальным тождествам $\rho_i(\xi) = 0$, получающимся при представлении $m(x(\xi), \xi)$ в виде $\sum x_i \rho_i(\xi)$. Таким образом, мы имеем $m(a, \alpha) = 0$. Отсюда следует, что $m_a(t)$ делится на $\mu_a(t)$. Так как полиномы $f(t, \alpha)$ и $\mu_a(t)$ имеют одинаковые неприводимые множители, то и полиномы $m_a(t)$ и $\mu_a(t)$ имеют одинаковые неприводимые множители.

Матрица $(T(x_i x_j))$ называется *дискриминантной матрицей* алгебры $\mathfrak{A}$. При изменении базиса эта матрица заменяется коградиентной ($M'TM$, где матрица M невырождающаяся). $\det(T(x_i x_j))$ называется *дискриминантом* алгебры $\mathfrak{A}$. Дискриминанты алгебры $\mathfrak{A}$ отличаются друг от друга не равными нулю множителями, являющимися квадратами элементов из Φ.

Рассмотрим теперь вопрос о вычислении минимального полинома $m(t, \xi)$. Предположим сначала, что $\mathfrak{A} = \Phi_r$. Применим здесь представление $\mathfrak{A}$ в самом себе. Если ξ_{ij} являются неизвестными, то полином $f(t, \xi) = \det(1t - (\xi_{ij}))$ неприводим в $P[t]$, где $P = \Phi(\xi_{ij})$ [1]. Следовательно, $m(t, \xi) = f(t, \xi)$. Подобным же образом изучается алгебра $\mathfrak{A} = \Phi^{(1)}_{r_1} \oplus \ldots \oplus \Phi^{(s)}_{r_s}$, где $\Phi^{(i)} \cong \Phi$. Общим элементом алгебры $\mathfrak{A}$ будет

$$\begin{pmatrix} \xi^{(1)}_{ij} & & \\ & \ddots & \\ & & \xi^{(s)}_{ij} \end{pmatrix}.$$

Применяя это представление, мы получаем, что $m(t, \xi) = \prod f_h(t, \xi^{(h)})$, где f_h является характеристическим полиномом элемента $(1t - (\xi^{(h)}))$.

Пусть теперь $\mathfrak{A}$ является произвольной алгеброй. Заметим, что $m(t, \xi)$ не изменится, если заменить алгебру $\mathfrak{A}$ алгеброй $\mathfrak{A}_\Gamma$, где Γ — расширение поля Φ; в самом деле, $\sum x_i \xi_i$ будет также общим элементом для $\mathfrak{A}_\Gamma$. Следовательно, достаточно определить $m(t, \xi)$ для $\mathfrak{A}_\Gamma$, где поле Γ

[1] См. L. E. Dickson, Algebras and Their Arithmetics, стр. 115.

является алгебраическим замыканием поля Ф. Предположим, что $x \to X$ является таким взаимнооднозначным представлением алгебры $\mathfrak{A}_\Gamma$, что $1 \to 1$, если алгебра $\mathfrak{A}_\Gamma$ обладает единицей. Мы можем считать, что это представление имеет вид

$$\begin{pmatrix} X^{(1)} & & * \\ & \ddots & \\ 0 & & X^{(s)} \end{pmatrix}, \tag{5}$$

где $x \to X^{(h)}$ являются неприводимыми представлениями, из которых некоторые могут быть нулевыми. Если $\mathfrak{N}$—радикал кольца $\mathfrak{A}_\Gamma$, то $\mathfrak{A}_\Gamma/\mathfrak{N} = \Gamma^{(1)}_{r_1} \oplus \ldots \oplus \Gamma^{(s)}_{r_s}$, где $\Gamma^{(i)}$ являются телами. Так как поле Γ алгебраически замкнуто, то из теоремы 32 следует, что $\Gamma^{(i)} \cong \Gamma$. Представление $x \to X^{(h)}$ будет представлением одного из Γ_{r_i}. Следовательно, если это представление не является нулевым, то множество матриц $X^{(h)}$ будет совокупностью всех матриц, имеющих то же число строк и столбцов, что и матрица $X^{(h)}$. Следовательно, возможно выразить матричные единицы $e^{(h)}_{ij}$ h-го «ящичка» в виде линейной комбинации матриц $X^{(h)}$. Отсюда вытекает, что характеристический полином $f_h(t, \xi)$ элемента $(1t - \sum X^{(h)}_i \xi_i)$ неприводим и, следовательно, $m(t, \xi) = \prod f_{hj}(t, \xi)$ — произведению некоторых из полиномов f_{hj}. Так как $m(t, \xi)$ является последним инвариантным множителем элемента $(1t - X)$, то $m(t, \xi)$ делится на каждый из полиномов f_{hj}. Мы хотим теперь показать, что представления $x \to X^{(h)}$ содержат все неприводимые ненулевые представления алгебры $\mathfrak{A}_\Gamma$. Для этой цели напомним, что если $\mathfrak{J}^{(k)}$ является некоторым неприводимым левым идеалом в $\Gamma^{(k)}_{rk}$, то представления алгебры $\mathfrak{A}_\Gamma$, определенные при помощи s идеалов $\mathfrak{J}^{(k)}$, $k = 1, \ldots, s$, образуют полную систему неэквивалентных неприводимых отличных от нулевого представлений алгебры $\mathfrak{A}_\Gamma$. Если $\mathfrak{A}^{(k)}$ обозначает двусторонний идеал алгебры $\mathfrak{A}_\Gamma$, отображающийся в $\Gamma^{(k)}_{r_k}$, то представление идеала $\mathfrak{A}^{(k)}$,

определенное при помощи идеала $\mathfrak{J}^{(l)}$, где $l \neq k$, является нулевым представлением. Следовательно, если определенное идеалом $\mathfrak{J}^{(k)}$ представление не встречается среди составляющих представлений $x \to X^{(h)}$, то элементы идеала $\mathfrak{A}^{(k)}$ представляются в (5) матрицами, все диагональные «ящички» которых состоят из нулей. Очевидно, что такие матрицы образуют нильпотентную алгебру, и так как представление идеала $\mathfrak{A}^{(k)}$ взаимнооднозначно, то идеал $\mathfrak{A}^{(k)}$ нильпотентен, вопреки соотношению, $\mathfrak{A}^{(k)}/\mathfrak{N} \cap \mathfrak{A}^{(k)} \cong \Gamma^{(k)}_{rk}$. Отметим наконец, что если алгебра $\mathfrak{A}$ обладает единицей, то ни одно из представлений $x \to X^{(h)}$ не может быть нулевым. Следовательно, $m(t, \xi)$ делится на t тогда и только тогда, когда $\mathfrak{A}$ не обладает единицей.

Если $f_h(t, \xi) = t^{n_h} - t^{n_h - 1} T^{(h)}(\xi) + \ldots + (-1)^{n_h} N^{(h)}(\xi)$, то $T^{(h)}(\xi)$ является следом матрицы $\sum X^{(h)}_i \xi_i$, а $N^{(h)}(\xi)$ — детерминантом этой матрицы. Очевидно, что $T(\xi) = \sum_j T^{(h_j)}(\xi)$ и $N(\xi) = \prod N^{(h_j)}(\xi)$. Используя свойства $T^{(h)}$ и $N^{(h)}$ и тот факт, что отображение $\sum x_i \alpha_i \to \sum X^{(h)}_i \alpha_i$ гомоморфно, мы получаем следующие важные соотношения для главного следа и главной нормы:

$$T(a + b) = T(a) + T(b), \quad T(a\alpha) = T(a)\alpha, \; T(ab) = T(ba),$$
$$N(ab) = N(a)N(b), \quad N(a\alpha) = N(a)\,\alpha^r.$$

Конечно, если алгебра $\mathfrak{A}$ не обладает единицей, то $N(a) = 0$.

Примеры. 1) Пусть $\mathfrak{A}$ является сепарабельным полем и поле P — наименьшим нормальным расширением поля $\mathfrak{A}$. Тогда $\mathfrak{A}_P = P^{(1)} \oplus \ldots \oplus P^{(n)}$, где $n = (\mathfrak{A} : \Phi)$. Следовательно, полином $m(t, \xi)$ имеет степень n и поэтому совпадает с характеристическим полиномом матрицы общего элемента в регулярном представлении.

2) Пусть $\mathfrak{A}$ будет чисто несепарабельным полем характеристики $p \neq 0$ вида $\Phi(x_1, \ldots, x_m)$, где $x_i^p = \gamma_i \in \Phi$ и $(\mathfrak{A} : \Phi) = p^m$. Тогда элементы $x_1^{k_1} \ldots x_m^{k_m}$, $0 \leqslant k_i < p$, образуют базис поля $\mathfrak{A}$, и если $x = \sum x_1^{k_1} \ldots x_m^{k_m} \xi_{k_1 \ldots k_m}$, то $m(t, \xi) = t^p - \sum \gamma_1^{k_1} \ldots \gamma_m^{k_m} \xi^p_{k_1 \ldots k_m}$.

19. Сепарабельные алгебры. Если $\mathfrak{A}$ является конечным сепарабельным расширением поля Φ, то, как мы видели, алгебра $\mathfrak{A}_\Gamma$ будет полупростой для любого поля расширения Γ поля Φ. Пусть теперь поле $\mathfrak{A}$ несепарабельно и имеет характеристику p, a — несепарабельный элемент и $\varphi(t) = (t^p)^r + (t^p)^{r-1}\beta_1 + \ldots + \beta_r$ — его минимальный полином. Так как элементы $1, a, \ldots, a^{p^r-1}$ линейно независимы в $\mathfrak{A}$, то они будут линейно независимы в $\mathfrak{A}_\Gamma$. Следовательно, при любых элементах γ_i из Γ $b = a^r + a^{r-1}\gamma_1 + \ldots + \gamma_r \neq 0$. Предположим, что поле Γ алгебраически замкнуто, и выберем в качестве γ_i элементы $\beta_i^{\frac{1}{p}}$. Тогда $b^p = 0$, и потому алгебра $\mathfrak{A}_\Gamma$ не будет полупростой. Этот факт приводит нас к определению *сепарабельной алгебры* над полем Φ как такой алгебры $\mathfrak{A}$ над Φ, для которой алгебра $\mathfrak{A}_\Gamma$ будет полупростой, каково бы ни было поле расширения Γ поля Φ. Обобщением нашего результата о полях будет следующая

Теорема 35. *Для того, чтобы алгебра $\mathfrak{A}$ была сепарабельной над полем Φ, необходимо и достаточно, чтобы $\mathfrak{A} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_t$, где алгебра $\mathfrak{A}_i$ проста и обладает центром $\mathfrak{C}_i$, сепарабельным над Φ.*

Необходимость. По определению, если алгебра $\mathfrak{A}$ сепарабельна, то она полупроста и, следовательно, $\mathfrak{A} = \mathfrak{A}_1 \oplus, \ldots \oplus \mathfrak{A}_t$, где каждая алгебра $\mathfrak{A}_i$ проста. Центр $\mathfrak{C}_i$ алгебры $\mathfrak{A}_i$ сепарабелен. В самом деле, в противном случае одно из полей $\mathfrak{C}_i$, например $\mathfrak{C}_1$, содержало бы несепарабельный элемент, и, следовательно, если Γ является алгебраическим замыканием поля Φ, алгебра $\mathfrak{C}_{1\Gamma}$ содержала бы нильпотентный элемент $b \neq 0$. Так как элемент b лежит в центре алгебры $\mathfrak{A}_\Gamma$, то главный идеал $b\mathfrak{A}_\Gamma$ был бы нильпотентным вопреки предположению.

Достаточность. Так как $\mathfrak{A}_\Gamma = \mathfrak{A}_{1\Gamma} \oplus \ldots \oplus \mathfrak{A}_{t\Gamma}$, то достаточно рассмотреть случай, когда алгебра $\mathfrak{A} = \mathfrak{A}_1$ проста и ее центр сепарабелен. Пусть поле P изоморфно наименьшему нормальному расширению поля $\mathfrak{C}$. Мы видели, что $\mathfrak{C} \times \mathrm{P} = \mathrm{P}^{(1)} \oplus \ldots \oplus \mathrm{P}^{(r)}$, где $\mathrm{P}^{(j)}$ является полем, изоморфным полю P, и $r = (\mathfrak{C} : \Phi)$. Пусть

$1 = e_1 + \ldots + e_r$, где $e_j \in \mathrm{P}^{(j)}$. Тогда $\mathrm{P}^{(j)} = e_j\mathrm{P}$, и потому для любого элемента c из $\mathfrak{C}$ мы будем иметь $e_i c = e_i \rho^{(i)}$, где $\rho^{(i)} \in \mathrm{P}$ и где соответствия $c \to \rho^{(i)}$ являются различными неприводимыми (обратными) представлениями поля $\mathfrak{C}$ в P. Пусть теперь элементы $x_1, \ldots, x_n$ $(n = \nu^2)$ образуют базис алгебры $\mathfrak{A}$ над $\mathfrak{C}$ и

$$x_i x_{i'} = \sum x_k c_{kii'}, \tag{6}$$

где $c_{kii'} \in \mathfrak{C}$. Тогда, если элементы $c_1, \ldots, c_r$ образуют базис поля $\mathfrak{C}$ над Φ, то элементы $x_i c_j$ образуют базис алгебры $\mathfrak{A}$ над Φ. Таким образом, каждый элемент из $\mathfrak{A} \times \mathrm{P}$ имеет вид $\sum x_i c_j \gamma_{ij}$, где $\gamma_{ij} \in \mathrm{P}$. Если мы выразим элементы c_j через e_j, то получим однозначное представление вида $\sum x_i e_j \gamma_{ij}$ для каждого элемента из $\mathfrak{A} \times \mathrm{P}$. Так как $e_j e_k = 0$ при $j \neq k$, то $\mathfrak{A} \times \mathrm{P} = \mathfrak{A}_1 \oplus \ldots \oplus \mathfrak{A}_r$, где $\mathfrak{A}_j$ является двусторонним идеалом с базисом $x_1^{(j)} = x_1 e_j, \ldots, x_n^{(j)} = x_n e_j$ над P. В силу (6), имеем $x_i^{(j)} x_{i'}^{(j)} = \sum x_k^{(j)} \gamma_{kii'}^{(j)}$. Таким образом, $\mathfrak{A}_i$ является центральной простой алгеброй над P, изоморфной, как алгебра над Φ, алгебре $(\mathfrak{A}$ над $\mathfrak{C})_\mathrm{P}$. Если теперь Γ — любое расширение поля Φ, то образуем расширение Σ, содержащее поля P и Γ. Тогда $\mathfrak{A}_\Sigma = (\mathfrak{A}_\mathrm{P})_\Sigma = \mathfrak{A}_{1\Sigma} \oplus \ldots \oplus \mathfrak{A}_{r\Sigma}$, где алгебры $\mathfrak{A}_{j\Sigma}$ простые и центральные. Так как $\mathfrak{A}_\Sigma = (\mathfrak{A}_\Gamma)_\Sigma$, то алгебра $\mathfrak{A}_\Gamma$ полупростая.

Второй критерий сепарабельности алгебры дается следующей теоремой.

Теорема 36. *Для того чтобы алгебра $\mathfrak{A}$ была сепарабельной, необходимо и достаточно, чтобы ее дискриминант Δ был отличен от нуля.*

Отметим сначала, что $\Delta = \det(T(x_i x_j)) = 0$ тогда и только тогда, когда существует такой отличный от нуля элемент $z \in \mathfrak{A}$, что $T(za) = 0$ для всех a. В самом деле, если $\Delta = 0$, то система уравнений $\sum T(x_i x_j)\xi_j = 0$ обладает решением $(\xi_1, \ldots, \xi_n)$, отличным от $(0, \ldots, 0)$, и, следовательно, элемент $z = \sum x_i \xi_i \neq 0$ удовлетворяет уравнениям $T(x_i z) = T(z x_i) = 0$ для $i = 1, \ldots, n$. Отсюда следует, что $T(za) = 0$ для всех a. Обратное очевидно:

если $T(za)=0$ для всех a, то $T(x_iz)=0$, и поэтому система уравнений $\sum T(x_ix_j)\xi_j=0$ обладает нетривиальным решением. Тогда $\Delta=0$. Предположим теперь, что алгебра $\mathfrak{A}$ несепарабельна. Тогда существует такое поле Γ, что алгебра $\mathfrak{A}_\Gamma$ обладает радикалом $\mathfrak{N}$. Если $z\in\mathfrak{N}$, то $za\in\mathfrak{N}$ для всех a из $\mathfrak{A}_\Gamma$. Пусть теперь $x\to X$ будет взаимнооднозначным представлением алгебры $\mathfrak{A}_\Gamma$ матрицами. Тогда если $z\to Z$ и $a\to A$, то матрица $ZA=X$ нильпотентна. Если мы применим матрицы вида (5), то увидим, что каждая матрица X_i нильпотентна, и, следовательно, все $T^{(i)}(X)=0$. Тогда и $T(X)=\sum T^{h_i}(X)=0$, а поэтому $T(za)=0$ для всех a и $\Delta=0$. Пусть теперь алгебра $\mathfrak{A}$ сепарабельна, и пусть поле Γ является алгебраическим замыканием поля Φ. Тогда $\mathfrak{A}_\Gamma=\Gamma_{n_1}^{(1)}\oplus\ldots\oplus\Gamma_{n_t}^{(t)}$, где $\Gamma^{(i)}\cong\Gamma$, и потому $\mathfrak{A}_\Gamma$ является алгеброй матриц вида

$$X=\begin{pmatrix}(\xi_{ij}^{(1)}) & & \\ & \ddots & \\ & & (\xi_{kl}^{(t)})\end{pmatrix},$$

где элементы ξ произвольны; как мы видели, $T(X)$ будет обычным следом элемента x. Если мы используем базис $e_{i_kj_k}^{(k)}$; $i_k, j_k=1,\ldots,n_k$; $k=1,\ldots,t$, для алгебры $\mathfrak{A}_\Gamma$, где $e_{i_kj_k}^{(k)}$ является матричным базисом для $\Gamma_{n_k}^{(k)}$, то получим простым вычислением, что $\det(T(e_{i_kj_k}^{(k)}e_{i_lj_l}^{(l)}))=\pm 1$.

20. Теорема Веддербарна

Теорема 37. *Пусть $\mathfrak{A}$ является алгеброй с радикалом $\mathfrak{N}$. Тогда если алгебра $\mathfrak{A}=\mathfrak{A}/\mathfrak{N}$ сепарабельна, то существует такая подалгебра $\mathfrak{S}$ алгебры $\mathfrak{A}$, что $\mathfrak{A}=\mathfrak{N}+\mathfrak{S}$, $\mathfrak{N}\cap\mathfrak{S}=0$* [1].

[1]) Эта теорема дана Веддербарном для полей Φ характеристики 0; доказательство в общем случае является тривиальным изменением рассуждений Wederburn'a [8] или Dickson [2].

Предположим сначала, что $\mathfrak{N}^2\neq 0$. Тогда $(\mathfrak{A}/\mathfrak{N}^2:\Phi)<(\mathfrak{A}:\Phi)$. Так как $\mathfrak{A}/\mathfrak{N}^2/\mathfrak{N}/\mathfrak{N}^2\cong\overline{\mathfrak{A}}$, то $\mathfrak{N}/\mathfrak{N}^2$ будет радикалом алгебры $\mathfrak{A}/\mathfrak{N}^2$, и эта алгебра удовлетворяет условиям теоремы. Мы можем предположить, что теорема уже установлена для алгебр размерности меньшей, чем $(\mathfrak{A}:\Phi)$. Следовательно, существует такая содержащая $\mathfrak{N}^2$ подалгебра $\mathfrak{S}_1$ алгебры $\mathfrak{A}$, что

$$\mathfrak{A}/\mathfrak{N}^2=\mathfrak{S}_1/\mathfrak{N}^2+\mathfrak{N}/\mathfrak{N}^2,\ (\mathfrak{S}_1/\mathfrak{N}^2)\cap(\mathfrak{N}/\mathfrak{N}^2)=0.$$

Эти равенства эквивалентны следующим:

$$\mathfrak{A}=\mathfrak{S}_1+\mathfrak{N},\ \mathfrak{S}_1\cap\mathfrak{N}=\mathfrak{N}^2. \tag{7}$$

Так как $\mathfrak{A}/\mathfrak{N}=(\mathfrak{S}_1+\mathfrak{N})/\mathfrak{N}\cong\mathfrak{S}_1/\mathfrak{S}_1\cap\mathfrak{N}=\mathfrak{S}_1/\mathfrak{N}^2$, то радикалом алгебры $\mathfrak{S}_1$ будет $\mathfrak{N}^2$, и $\mathfrak{S}_1$ удовлетворяет условиям теоремы. Так как $\mathfrak{S}_1\cap\mathfrak{N}=\mathfrak{N}^2$, то $(\mathfrak{S}_1:\Phi)<(\mathfrak{A}:\Phi)$, и потому существует такая подалгебра $\mathfrak{S}$ алгебры $\mathfrak{S}_1$, что $\mathfrak{S}_1=\mathfrak{S}+\mathfrak{N}^2$ и $\mathfrak{S}\cap\mathfrak{N}^2=0$. Тогда, в силу соотношений (7), $\mathfrak{A}=\mathfrak{S}+\mathfrak{N}$ и $\mathfrak{S}\cap\mathfrak{N}=0$.

Предположим далее, что $\overline{\mathfrak{A}}=\overline{\Phi}_{n_1}^{(1)}\oplus\ldots\oplus\overline{\Phi}_{n_t}^{(t)}$, где $\overline{\Phi}^{(i)}\cong\Phi$, и пусть $\overline{u}_k$ является единицей в $\overline{\Phi}_{n_k}^{(k)}$. Мы можем выбрать идемпотентные элементы u_k в $\overline{u}_k$ так, чтобы $u_ku_l=0$ при $k\neq l$. Тогда $u_k\mathfrak{A}u_k/(u_k\mathfrak{A}u_k\cap\mathfrak{N})\cong(u_k\mathfrak{A}u_k+\mathfrak{N})/\mathfrak{N}=\Phi_{n_k}^{(k)}$. Следовательно, алгебра $u_k\mathfrak{A}u_k$ примарна, и ее радикалом является $u_k\mathfrak{A}u_k\cap\mathfrak{N}=u_k\mathfrak{N}u_k$. Отсюда следует, что $u_k\mathfrak{A}u_k$ содержит подалгебру $\mathfrak{S}_k\cong\overline{\Phi}_{n_k}^{(k)}$. Так как $u_ku_l=0$ при $k\neq l$, то $\mathfrak{S}_k\mathfrak{S}_l=0$, и потому алгебра $\mathfrak{S}=\mathfrak{S}_1+\ldots+\mathfrak{S}_t=\mathfrak{S}_1\oplus\ldots\oplus\mathfrak{S}_t$ полупроста, и ее размерность равна Σn_k^2. Следовательно, $\mathfrak{S}\cap\mathfrak{N}=0$, и, сравнивая размерности, мы видим, что $\mathfrak{S}+\mathfrak{N}=\mathfrak{A}$.

Наконец, пусть $\mathfrak{A}$ будет любой алгеброй, удовлетворяющей условиям теоремы, причем $\mathfrak{N}^2=0$. Если поле Γ является любым расширением поля Φ, то $\mathfrak{A}_\Gamma/\mathfrak{N}_\Gamma\cong(\overline{\mathfrak{A}})_\Gamma$ и последняя алгебра полупроста. Следовательно, $\mathfrak{N}_\Gamma$ будет радикалом алгебры $\mathfrak{A}_\Gamma$. Если поле Γ является алгебраическим замыканием поля Φ, то $\mathfrak{A}_\Gamma/\mathfrak{N}_\Gamma=\overline{\Gamma}_{n_1}^{(1)}\oplus\ldots\oplus\overline{\Gamma}_{n_r}^{(r)}$,

где $\bar{\Gamma}^{(k)} \cong \Gamma$. Матричные единицы простых компонент алгебры $\bar{\mathfrak{A}}_\Gamma$ могут быть выражены при помощи базиса $\bar{y}_1, \ldots, \bar{y}_r$ алгебры $\bar{\mathfrak{A}}$ в виде $\Sigma \bar{y}_i w_i$, где $w_i \in \Gamma$. Так как существует лишь конечное число элементов w_i, входящих в эти выражения, и каждый из элементов w алгебраичен над Φ, то они порождают конечное расширение P поля Φ. Очевидно, что $\bar{\mathfrak{A}}_P$ будет представлять собою прямую сумму алгебр матриц над P и $\mathfrak{A}_P/\mathfrak{N}_P = \bar{P}_{n_1}^{(1)} \oplus \ldots \oplus \bar{P}_{n_t}^{(t)}$, а тогда, как мы уже показали, $\bar{\mathfrak{A}}_P = \bar{\mathfrak{N}}_P + \tilde{\mathfrak{S}}$ и $\tilde{\mathfrak{S}} \cap \bar{\mathfrak{N}}_P = 0$, где $\tilde{\mathfrak{S}}$ является подалгеброй $\mathfrak{A}_P$. Пусть элементы $\rho_0 = 1, \rho_1, \ldots, \rho_s$ образуют базис поля P над Φ, и элементы $x_1, \ldots, x_n$ образуют такой базис алгебры $\mathfrak{A}$ над $\Phi(P)$, что элементы $x_{r+1}, \ldots, x_n$ будут базисом радикала $\mathfrak{N}$ над $\Phi(P)$. Тогда $x_i = y_i - z_i$, где $y_i \in \tilde{\mathfrak{S}}$ и $z_i \in \mathfrak{N}_P$. Элементы $y_1, \ldots, y_r$ образуют базис алгебры $\tilde{\mathfrak{S}}$ и $y_i = x_i + \Sigma z_{ij}\rho_j$, где $z_{ij} \in \mathfrak{N}$. Положим $x_i' = x_i + z_{i0}$. Тогда элементы $x_1', \ldots, x_r', x_{r+1}, \ldots, x_n$ образуют базис алгебры $\mathfrak{A}$ над Φ и $y_i = x_i' + z_i'$, где $z_i' = \sum_{k=1}^{s} z_{ik}\rho_k$. Следовательно, $x_i'x_j' = \sum x'_k \gamma_{kij} + v_{ij}$, где $\gamma_{ijk} \in \Phi$ и $v_{ij} \in \mathfrak{N}$. Отсюда следует, что $y_i y_j = \sum y_k \gamma_{kij} + u_{ij}$, где $u_{ij} \in \mathfrak{N}_P$, и так как $y_i \in \tilde{\mathfrak{S}}$, то $u_{ij} = 0$. Если мы подставим в эти соотношения вместо элементов y_i их выражения $x_i' + z_i'$, то они примут вид:

$$x_i'x_j' + x_i'z_j' + z_i'x_j' = \sum (x_k' + z_k')\,\gamma_{kij}.$$

Если мы представим каждый член в виде $\Sigma a_i\rho_i$ и сравним коэффициенты при $\rho_0 = 1$, то получим, что $x_i'x_j' = \sum x_k' \gamma_{kij}$. Следовательно, совокупность всех элементов вида $\Sigma x_i' \alpha_i$, где $\alpha \in \Phi$, образует искомую алгебру $\mathfrak{S}$.

Глава 6

МУЛЬТИПЛИКАТИВНАЯ ТЕОРИЯ ИДЕАЛОВ

1. Кольца отношений. Эмми Нётер показала, что основная теорема разложения для идеалов максимальной области алгебраических чисел может быть выведена из некоторых весьма простых свойств этой области. Эти требования содержатся в теореме: Если $\mathfrak{o}$ является коммутативной областью целостности, то отличные от нуля и от $\mathfrak{o}$ идеалы разлагаются одним и только одним способом на произведение простых идеалов тогда и только тогда, когда область $\mathfrak{o}$ удовлетворяет следующим условиям:

N 1. $\mathfrak{o}$ целозамкнута (в своем поле отношений).

N 2. Выполнено условие обрыва убывающих цепей для идеалов, содержащих любой фиксированный, отличный от нуля, идеал.

N 3. Для всех идеалов выполнено условие обрыва возрастающих цепей.

В настоящей главе мы рассмотрим обобщение этого результата на некоммутативные кольца. Теория эта принадлежит главным образом Шпайзеру, Брандту, Артину, Хассе и Дейрингу; аксиоматическое же обоснование ее — Асано. Многие из результатов этой главы были уже изложены в наших исследованиях об областях главных идеалов. Нам понадобятся также ссылки на теорию колец главных идеалов, развитую нами в §§ 15—16 главы 4.

Начнем с колец, обладающих единицей. Элемент a кольца $\mathfrak{o}$ называется *регулярным*, если он не является

ни правым, ни левым делителем нуля. Первое ограничение, которое мы наложим на кольцо, состоит в том, что кольцо $\mathfrak{o}$ обладает (правым) *кольцом отношений*, т. е. таким содержащим $\mathfrak{o}$ кольцом $\mathfrak{A}$, что 1) каждый регулярный элемент кольца $\mathfrak{o}$ обладает в $\mathfrak{A}$ обратным элементом, и 2) каждый элемент кольца $\mathfrak{A}$ имеет вид ab^{-1}, где a и b лежат в $\mathfrak{o}$. Весьма просто получить условия, при которых для $\mathfrak{o}$ существовало бы подобное кольцо $\mathfrak{A}$. Для этой цели рассмотрим любую пару элементов a и b кольца $\mathfrak{o}$, причем элемент b регулярен. Тогда b^{-1} лежит в $\mathfrak{A}$ и, следовательно, $b^{-1}a$ имеет вид $a_1b_1^{-1}$, где a_1 и b_1 лежат в $\mathfrak{o}$. Тогда $ba_1 = ab_1$. Поэтому для существования кольца $\mathfrak{A}$ необходимо, чтобы для любой пары элементов a и b кольца $\mathfrak{o}$, где элемент b регулярен, существовало общее правое кратное $m = ab_1 = ba_1$ с регулярным элементом b_1.

Обратно, предположим, что это условие выполнено. Как и в главе 3, рассмотрим такие пары (a, b) элементов a и b кольца $\mathfrak{o}$, что элемент b регулярен. Если (c, d) является другой парой этого вида и m — любым таким кратным вида $db_1 = bd_1$, что элемент b_1 (а, следовательно, и элемент d_1) регулярен, то мы будем считать пары (a, b) и (c, d) эквивалентными ($(a, b) \sim (c, d)$), если $ad_1 = cb_1$. Отметим, что если это условие выполнено для какого-либо m, то оно выполнено и для любого $n = db_2 = bd_2$, для которого элементы b_2 и d_2 регулярны. В самом деле, мы можем найти такие регулярные элементы e_2 и e_1, что $b_1e_2 = b_2e_1$. Тогда $d_1e_2 = d_2e_1$ и $ad_2 = cb_2$. Отсюда непосредственно следует, что соотношение $\sim$ симметрично, рефлексивно и транзитивно. Как обычно, мы обозначаем совокупность пар, эквивалентных паре (a, b), через a/b.

Если $m = db_1 = bd_1$ и элементы b_1 и d_1 регулярны, то определим $a/b + c/d$ как $(ad_1 + cd_1)/m$ и, если $n = bc_1 = cb_1$, где элемент b_1 регулярен, то определим $(a/b)(c/d) = ac_1/db_1$. Определенные таким образом функции однозначны и превращают множество $\mathfrak{A}$ «дробей» a/b в кольцо. Предоставляем проверку этих фактов читателю. Кольцо $\mathfrak{A}$ обладает единицей $1/1$ и содержит

изоморфное кольцу $\mathfrak{o}$ подкольцо, состоящее из элементов $a/1$. Идентифицируем это подкольцо с $\mathfrak{o}$ и будем писать a вместо $a/1$. Тогда если элемент a не является делителем нуля, то он обладает в кольце $\mathfrak{A}$ обратным элементом $a^{-1} = 1/a$. Так как любой элемент кольца $\mathfrak{A}$ имеет вид $(a/1)(1/b) = ab^{-1}$, то $\mathfrak{A}$ является правым кольцом отношений кольца $\mathfrak{o}$.

Отметим далее, что кольцо отношений определено однозначно с точностью до изоморфизма. В самом деле, легко проверить, что если кольца $\mathfrak{o}$ и $\mathfrak{o}'$ изоморфны, причем $a \to a'$ является изоморфизмом между ними, то их кольца отношений $\mathfrak{A}$ и $\mathfrak{A}'$ также изоморфны, причем изоморфным соответствием для них будет $ab^{-1} \to a'(b')^{-1}$. Наконец, заметим, что если $\mathfrak{A}$ является кольцом отношений кольца $\mathfrak{o}$, то всякий регулярный элемент из $\mathfrak{A}$ обладает в кольце $\mathfrak{A}$ обратным элементом.

2. Порядки и идеалы. Поскольку условия для того, чтобы кольцо $\mathfrak{o}$ обладало кольцом отношений, уже установлены, более удобно изучать вместо кольца $\mathfrak{o}$ его кольцо отношений $\mathfrak{A}$. Таким образом, предположим, что $\mathfrak{A}$ задано как любое кольцо с единицей, в котором каждый регулярный элемент обладает обратным. Например, $\mathfrak{A}$ может быть любым кольцом, удовлетворяющим условию обрыва убывающих цепей правых и левых идеалов[1]. Рассмотрим подкольца $\mathfrak{o}$ кольца $\mathfrak{A}$, определяемые следующим образом.

Определение 1. *Порядком* $\mathfrak{o}$ кольца $\mathfrak{A}$ называется содержащее 1 подкольцо, обладающее тем свойством, что каждый элемент из $\mathfrak{A}$ имеет вид ab^{-1} при некоторых элементах a и b из $\mathfrak{o}$.

---

[1]) В самом деле, в этом случае если a не является левым делителем нуля, то отображение $x \to ax$ будет $\mathfrak{A}$,-изоморфизмом между $\mathfrak{A}$ и правым идеалом $a\mathfrak{A}$. В силу условия обрыва убывающих цепей для правых идеалов, $a\mathfrak{A} = \mathfrak{A}$. Следовательно, существует такой элемент b, что $ab = 1$. Подобно этому, существует такой элемент b', что $b'a = 1$. Отсюда следует, что $b = b'$.

Следует отметить, что это определение имеет односторонний смысл, и мы не должны предполагать, что элементы кольца $\mathfrak{A}$ представимы в виде $b^{-1}a$, где b и a лежат в $\mathfrak{o}$. Последнее условие будет, однако, выполнено в порядках, с которыми мы будем главным образом иметь дело в дальнейшем.

Порядки $\mathfrak{o}_1$ и $\mathfrak{o}_2$ называются *эквивалентными*, если существуют такие регулярные элементы a_1, b_1, a_2, b_2 кольца $\mathfrak{A}$, что $a_1\mathfrak{o}_1 b_1 \subseteq \mathfrak{o}_2$ и $a_2\mathfrak{o}_2 b_2 \subseteq \mathfrak{o}_1$. Очевидно, что это соотношение симметрично, рефлексивно и транзитивно. *Ограничимся рассмотрением лишь таких порядков, которые эквивалентны фиксированному порядку* $\mathfrak{o}_0$, и для простоты будем употреблять термин «порядок» вместо «порядок, эквивалентный порядку $\mathfrak{o}_0$». Для доказательства того, что подкольцо $\mathfrak{o}'$, содержащее единицу, является порядком, достаточно показать существование такого порядка $\mathfrak{o}$ и таких регулярных элементов a, b, a' и b', что $a\mathfrak{o}b \subseteq \mathfrak{o}'$ и $a'\mathfrak{o}'b' \subseteq \mathfrak{o}$. В самом деле, если z является любым элементом кольца $\mathfrak{A}$, то существуют такие элементы p, q из $\mathfrak{o}$, что $a^{-1}za = pq^{-1}$ и потому $z = (apb)(aqb)^{-1}$.

Определение 2. Подмножество $\mathfrak{a}$ кольца $\mathfrak{A}$ называется (дробным) *правым* $\mathfrak{o}$*-идеалом*, если 1) $\mathfrak{a}\mathfrak{o} \subseteq \mathfrak{a}$, 2) $\mathfrak{a}$ содержит регулярный элемент и 3) в кольце $\mathfrak{A}$ существует такой регулярный элемент a, что $a\mathfrak{a} \subseteq \mathfrak{o}$.

Левый $\mathfrak{o}$*-идеал* определяется подобным же образом. Если $\mathfrak{a}$ является одновременно правым $\mathfrak{o}$-идеалом и левым $\mathfrak{o}$-идеалом, то $\mathfrak{a}$ называется *двусторонним* $\mathfrak{o}$*-идеалом*. Если a — любой регулярный элемент, то множество $\mathfrak{a} = a\mathfrak{o}$ будет правым $\mathfrak{o}$-идеалом. В самом деле, выполнение условий 1) и 2) очевидно, а условие 3) выполнено, так как $a^{-1}\mathfrak{a} = \mathfrak{o}$. Идеал такого вида называется *главным*. В этих терминах условия 2) и 3) могут быть заменены соответственно условиями:

2′) $\mathfrak{a}$ содержит главный правый $\mathfrak{o}$-идеал и

3′) $\mathfrak{a}$ содержится в главном правом $\mathfrak{o}$-идеале.

Пусть теперь $\mathfrak{o}$ будет некоторым порядком, а $\mathfrak{a}$ — правым $\mathfrak{o}$-идеалом. Рассмотрим множество $\mathfrak{o}_l$ таких

элементов x, что $x\mathfrak{a} \subseteq \mathfrak{a}$ [1]). Очевидно, что $\mathfrak{o}_l$ является содержащим единицу подкольцом кольца $\mathfrak{A}$. Так как существуют такие регулярные элементы a и b, что $b\mathfrak{o} \subseteq \mathfrak{a} \subseteq a\mathfrak{o}$, то $b\mathfrak{o}a^{-1} \subset \mathfrak{o}_l$, и так как $\mathfrak{o}_l(b\mathfrak{o}) \subseteq a\mathfrak{o}$, то $\mathfrak{o}_l b \subseteq a\mathfrak{o}$ и $\mathfrak{o}_l \subseteq a\mathfrak{o}b^{-1}$. Таким образом, $\mathfrak{o}_l$ является порядком. Так как $a^{-1}\mathfrak{a} \subseteq \mathfrak{o}$, то $\mathfrak{a}a^{-1}\mathfrak{a} \subseteq \mathfrak{a}$, и потому $\mathfrak{a}a^{-1} \subseteq \mathfrak{o}_l$, $\mathfrak{a} \subseteq \mathfrak{o}_l a$. Наконец, b лежит в $\mathfrak{a}$, так что $\mathfrak{o}_l b \subseteq \mathfrak{a}$. Это показывает, что $\mathfrak{a}$ является левым $\mathfrak{o}_l$-идеалом.

Подобным же образом, если $\mathfrak{a}$ является левым $\mathfrak{o}$-идеалом, то совокупность $\mathfrak{o}_r$ таких элементов y, что $\mathfrak{a}y \subseteq \mathfrak{a}$, является порядком, и $\mathfrak{a}$ будет $\mathfrak{o}_r$-идеалом. Следовательно, начиная с правого $\mathfrak{o}$-идеала, мы можем определить сначала $\mathfrak{o}_l$ и потом, рассматривая $\mathfrak{a}$ как левый $\mathfrak{o}_l$-идеал, доказать, что множество $\mathfrak{o}_r$ таких элементов y, что $\mathfrak{a}y \subseteq \mathfrak{a}$, является порядком, а $\mathfrak{a}$ — правым $\mathfrak{o}_r$-идеалом. Очевидно, $\mathfrak{o} \subseteq \mathfrak{o}_r$.

Теорема 1. *Если* $\mathfrak{a}$ *является правым (левым)* $\mathfrak{o}$*-идеалом, то совокупность таких элементов* x, *что* $x\mathfrak{a} \subseteq \mathfrak{a}$, *будет порядком* $\mathfrak{o}_l$, *а совокупность таких элементов* y, *что* $\mathfrak{a}y \subseteq \mathfrak{a}$, — *порядком* $\mathfrak{o}_r$. *Множество* $\mathfrak{a}$ *является левым* $\mathfrak{o}_l$*-идеалом и правым* $\mathfrak{o}_r$*-идеалом.*

Порядки $\mathfrak{o}_l$ и $\mathfrak{o}_r$ называются соответственно *левым порядком* и *правым порядком* идеала $\mathfrak{a}$. Если $\mathfrak{a} \subseteq \mathfrak{o}_r$, то $\mathfrak{a} \subseteq \mathfrak{o}_l$ и обратно. В этом случае идеал $\mathfrak{a}$ называется *целым*. Если $\mathfrak{a}$ является главным $\mathfrak{o}$-идеалом $a\mathfrak{o}$, то $a\mathfrak{o}_r \subseteq a\mathfrak{o}$ и потому $\mathfrak{o}_r = \mathfrak{o}$. Подобно этому $\mathfrak{o}_l = a\mathfrak{o}a^{-1}$.

Если $\mathfrak{a}$ — правый идеал с правым порядком $\mathfrak{o}_r$ и левым порядком $\mathfrak{o}_l$, то пусть $\mathfrak{a}^{-1}$ обозначает совокупность таких элементов z кольца $\mathfrak{A}$, что $az\mathfrak{a} \subseteq \mathfrak{a}$. Очевидно, что элементы z могут быть также охарактеризованы либо соотношением $az \subseteq \mathfrak{o}_l$, либо соотношением $z\mathfrak{a} \subseteq \mathfrak{o}_r$. Если c и d — такие регулярные элементы, что $d\mathfrak{o}_r \subseteq \mathfrak{a} \subseteq c\mathfrak{o}_r$, то $\mathfrak{a}(\mathfrak{o}_r c^{-1})\mathfrak{a} = (\mathfrak{a}\mathfrak{o}_r)(c^{-1}\mathfrak{a}) \subseteq (\mathfrak{a}\mathfrak{o}_r)\mathfrak{o}_r = \mathfrak{a}$ и $\mathfrak{a}^{-1}d \subseteq \mathfrak{o}_r$. Тогда $\mathfrak{o}_r c^{-1} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{o}_r d^{-1}$, и так как $\mathfrak{a}^{-1}$

[1]) К сожалению, наше обозначение совпадает здесь с обозначением для кольца левых умножений. Поэтому мы не будем в этой главе употреблять старое обозначение для этого кольца.

является левым $\mathfrak{o}$-модулем, то $\mathfrak{a}^{-1}$ будет левым $\mathfrak{o}_r$-идеалом. Подобно этому, $\mathfrak{a}^{-1}$ будет правым $\mathfrak{o}_l$-идеалом.

Теорема 2. *Если $\mathfrak{a}$ является идеалом с правым порядком $\mathfrak{o}_r$ и левым порядком $\mathfrak{o}_l$, то совокупность таких элементов z кольца $\mathfrak{a}$, что $\mathfrak{a}z\mathfrak{a} \subseteq \mathfrak{a}$, будет левым $\mathfrak{o}_r$-идеалом и правым $\mathfrak{o}_l$-идеалом.*

Идеал $\mathfrak{a}^{-1}$ называется *обратным* идеалу $\mathfrak{a}$. Так как $\mathfrak{a}^{-1}$ представляет собой совокупность таких элементов z, что $z\mathfrak{a} \subseteq \mathfrak{o}_r$, то для любого другого идеала $\mathfrak{b} \subset \mathfrak{a}$ с правым порядком $\mathfrak{o}_r$ (левым порядком $\mathfrak{o}_l$) мы будем иметь $\mathfrak{a}^{-1} \subset \mathfrak{b}^{-1}$. Если $\mathfrak{a} = a\mathfrak{o}$, то $\mathfrak{o}_r = \mathfrak{o}$, и если z лежит в $\mathfrak{a}^{-1}$, то $za = b$ лежит в $\mathfrak{o}$. Следовательно, $z = ba^{-1}$ и и $\mathfrak{a}^{-1} = \mathfrak{o}a^{-1}$.

3. Ограниченные порядки. Мы увидим далее, что основным понятием излагаемой теории является, как и для областей главных идеалов, понятие ограниченного идеала. Правый (левый) $\mathfrak{o}$-идеал $\mathfrak{a}$ называется *ограниченным*, если он содержит двусторонний $\mathfrak{o}$-идеал. Следует отметить, что это определение применимо к любому идеалу, как целому, так и к нецелому, и что нет необходимости оговаривать, что двусторонний идеал отличен от нуля, так как это требование содержится в нашем новом определении идеала: Если все идеалы порядка $\mathfrak{o}$ ограничены, то мы назовем сам порядок $\mathfrak{o}$ *ограниченным*. В этом параграфе мы исследуем некоторые свойства ограниченных порядков.

Так как любой идеал содержит главный идеал, то для того чтобы порядок $\mathfrak{o}$ был ограниченным, достаточно, разумеется, чтобы каждый главный $\mathfrak{o}$-идеал содержал двусторонний $\mathfrak{o}$-идеал. Предположим, что порядок $\mathfrak{o}$ является *максимальным* в том смысле, что не существует порядка (эквивалентного $\mathfrak{o}$), содержащего $\mathfrak{o}$ как собственное подмножество[1]). Тогда мы имеем следующую теорему.

[1]) Примеры ограниченных максимальных порядков будут даны далее.

Теорема 3 *Следующие условия, налагаемые на максимальный порядок $\mathfrak{o}$, эквивалентны*: 1) *порядок $\mathfrak{o}$ ограничен*, 2) *каждый целый правый (или левый) $\mathfrak{o}$-идеал содержит двусторонний $\mathfrak{o}$-идеал*, 3) *для любого регулярного элемента c из $\mathfrak{o}$ $c\mathfrak{o}$ является двусторонним $\mathfrak{o}$-идеалом и* 4) *для каждого регулярного элемента a существует такой регулярный элемент b, что $\mathfrak{o}b \subseteq a\mathfrak{o}$ (или $b\mathfrak{o} \subseteq a\mathfrak{o}$).*

Предположим, что для любого регулярного элемента a из $\mathfrak{o}$ идеал $a\mathfrak{o}$ содержит двусторонний $\mathfrak{o}$-идеал $\mathfrak{a}$. Так как порядок $\mathfrak{o}$ максимален, то оба порядка идеала $\mathfrak{a}$ совпадают с $\mathfrak{o}$. Следовательно, $(a\mathfrak{o})^{-1} = \mathfrak{o}a^{-1} \subseteq \mathfrak{a}^{-1}$ и $\mathfrak{o}a^{-1}\mathfrak{o} \subseteq \mathfrak{a}^{-1}$. Отсюда следует, что $\mathfrak{o}a^{-1}\mathfrak{o}$ содержится в правом (левом) главном $\mathfrak{o}$-идеале и потому $\mathfrak{o}a^{-1}\mathfrak{o}$ является двусторонним $\mathfrak{o}$-идеалом. Если c — произвольный регулярный элемент, то c имеет вид ba^{-1}, где b и a лежат в $\mathfrak{o}$. Тогда $\mathfrak{o}c\mathfrak{o} = \mathfrak{o}ba^{-1}\mathfrak{o} \subseteq \mathfrak{o}a^{-1}\mathfrak{o}$ и $\mathfrak{o}c\mathfrak{o}$ является двусторонним $\mathfrak{o}$-идеалом. Мы доказали, что из условия 2) следует условие 3). Предположим теперь, что выполнено условие 3). Если a является произвольным регулярным элементом, то двусторонний $\mathfrak{o}$-идеал $\mathfrak{a} = \mathfrak{o}a^{-1}\mathfrak{o}$ содержит как $\mathfrak{o}a^{-1}$, так и $a^{-1}\mathfrak{o}$. Следовательно, $\mathfrak{a}^{-1} \subseteq (\mathfrak{o}\mathfrak{a}^{-1})^{-1} = a\mathfrak{o}$. Так как $\mathfrak{a}^{-1}$ является двусторонним $\mathfrak{o}$-идеалом, то он содержит главный левый $\mathfrak{o}$-идеал $\mathfrak{o}b$. Подобно этому, $\mathfrak{o}a$ содержит $\mathfrak{a}^{-1}$, а также соответствующий идеал $b'\mathfrak{o}$, где элемент b' регулярен. Таким образом из условия 3) следуют условия 1) и 4). Так как условие 2) является очевидным следствием условия 1), то условия 1), 2) и 3) эквивалентны. Докажем, наконец, что из условия 4) следует условие 1). Пусть $a\mathfrak{o}$ будет произвольным главным идеалом и b таким регулярным элементом, что $a\mathfrak{o} \supseteq \mathfrak{o}b$. Тогда $a\mathfrak{o} \supseteq \mathfrak{o}b\mathfrak{o}$ и $\mathfrak{o}b\mathfrak{o}$ будет правым $\mathfrak{o}$-идеалом. Так как порядок $\mathfrak{o}$ максимален, то левый порядок идеала $\mathfrak{o}b\mathfrak{o}$ совпадает с $\mathfrak{o}$ и потому $\mathfrak{o}b\mathfrak{o}$ является также и левым $\mathfrak{o}$-идеалом. Это показывает, что условие 1) выполнено, и теорема доказана полностью.

Следующая теорема показывает, что если $\mathfrak{o}$ является ограниченным максимальным порядком, то условие, что каждый элемент x кольца $\mathfrak{A}$, имеет вид ab^{-1}, может быть

заменено дуальным требованием, что каждый x имеет вид $c^{-1}d$, где c и d лежат в $\mathfrak{o}$.

Теорема 4. *Если $\mathfrak{o}$ — ограниченный максимальный порядок, то каждый элемент x из $\mathfrak{A}$ имеет вид $c^{-1}d$, где c и d лежат в $\mathfrak{o}$.*

Мы знаем, что каждый элемент x из $\mathfrak{A}$ может быть записан в виде ab^{-1}, где a и b лежат в $\mathfrak{o}$. Так как элемент b регулярен, то $b\mathfrak{o} \supseteq \mathfrak{a} \supseteq \mathfrak{o}c$, где $\mathfrak{a}$ является двусторонним $\mathfrak{o}$-идеалом и элемент c регулярен. Так как порядок $\mathfrak{o}$ максимален, то левый и правый порядки идеала $\mathfrak{a}$ совпадают с $\mathfrak{o}$ и, следовательно, $\mathfrak{o}b^{-1} \subseteq \mathfrak{a}^{-1} \subseteq c^{-1}\mathfrak{o}$. Таким образом, $ab^{-1} = c^{-1}d$ для соответствующего d из $\mathfrak{o}$.

Теорема 5. *Предположим, что $\mathfrak{o}$ является максимальным ограниченным порядком, $\mathfrak{o}'$ — любым порядком и $\mathfrak{M}$ — таким множеством, что $a'\mathfrak{M}b' \subseteq \mathfrak{o}'$ для соответствующих регулярных элементов a', b'. Тогда существуют такие регулярные элементы c и d, что $c\mathfrak{M} \subseteq \mathfrak{o}$ и $\mathfrak{M}d \subseteq \mathfrak{o}$.*

Так как порядок $\mathfrak{o}'$ эквивалентен порядку $\mathfrak{o}$, то существуют такие регулярные элементы a и b, что $a\mathfrak{M}b \subseteq \mathfrak{o}$. Следовательно, $a\mathfrak{M} \subseteq \mathfrak{o}b^{-1} \subseteq \mathfrak{o}b^{-1}\mathfrak{o} \subseteq c'\mathfrak{o}$. Таким образом, $\mathfrak{M} \subseteq c\mathfrak{o}$ для $c = a^{-1}c'$. Подобно этому, $\mathfrak{M} \subseteq \mathfrak{o}d$ для подходящего регулярного элемента d.

Мы применим этот результат для доказательства следующей теоремы.

Теорема 6. *Каждый максимальный порядок $\mathfrak{o}'$, эквивалентный ограниченному максимальному порядку $\mathfrak{o}$, сам ограничен.*

Пусть a является любым регулярным элементом из $\mathfrak{o}'$, а b и c такими регулярными элементами, что $boc \subseteq \mathfrak{o}'$. Тогда $a\mathfrak{o}' \supseteq (ab)\mathfrak{o}c$ и $(ab)\mathfrak{o} \supseteq \mathfrak{o}b'$ для некоторого регулярного элемента b'. Следовательно, $a\mathfrak{o}' \supseteq \mathfrak{o}b'c$. Если мы применим предыдущую теорему к $\mathfrak{M} = \mathfrak{o}'$, то получим существование такого регулярного элемента c', что $\mathfrak{o}'c' \subseteq \mathfrak{o}$. Тогда $a\mathfrak{o}' \supseteq \mathfrak{o}'c'b'c$ и, вследствие теоремы 3, порядок $\mathfrak{o}'$ ограничен.

4. Аксиомы. Наложим теперь следующие условия на наш порядок $\mathfrak{o}$.

I. Порядок $\mathfrak{o}$ максимален.

II. Условие обрыва убывающих цепей выполнено для целых односторонних $\mathfrak{o}$-идеалов, содержащих любой фиксированный целый двусторонний $\mathfrak{o}$-идеал.

III. Для целых двусторонних $\mathfrak{o}$-идеалов выполнено условие обрыва возрастающих цепей.

IV. Порядок $\mathfrak{o}$ ограничен.

Если $\mathfrak{A}$ является полем, то любой отличный от нуля идеал в старом смысле будет идеалом и в том смысле, который мы придали ему в этой главе. Следовательно, условия II и III эквивалентны соответственно нётеровским условиям N 2 и N 3. Напомним теперь смысл условия N 1. Предположим, что $\mathfrak{A}$ является алгеброй с единицей, конечной размерности над лежащим в ней полем Φ, и пусть $\mathfrak{g}$ будет некоторым порядком в Φ. Тогда $\mathfrak{g}$ будет некоторым содержащим единицу подкольцом поля Φ, имеющим поле Φ своим полем отношений. Элемент a из $\mathfrak{A}$ называется *$\mathfrak{g}$-целым*, если он является корнем полинома из $\mathfrak{g}[t]$ со старшим коэффициентом 1. При $\mathfrak{A} = \Phi$ порядок $\mathfrak{o} = \mathfrak{g}$ называется *целозамкнутым*, если любой $\mathfrak{o}$-целый элемент из $\mathfrak{A}$ лежит в $\mathfrak{o}$. Для того, чтобы изучить связь между этим свойством и условием I, мы нуждаемся в следующем общем условии.

Теорема 7. *Если в порядке $\mathfrak{g}$ выполнено условие обрыва возрастающих цепей идеалов, то для того чтобы элемент a из $\mathfrak{A}$ был $\mathfrak{g}$-целым, необходимо и достаточно, чтобы все степени a^k содержались в одном $\mathfrak{g}$-модуле из $\mathfrak{A}$ с конечным числом образующих.*

Если элемент a целый, то $a^m = a^{m-1}\gamma_1 + \ldots + 1\gamma_m$, где γ_i лежат в $\mathfrak{g}$. Отсюда следует, что все a^k принадлежат $\mathfrak{g}$-модулю $(1, a, \ldots, a^{m-1})$ с образующими элементами a^i, $0 \leqslant i \leqslant m-1$. Обратно, пусть $\mathfrak{M}$ является $\mathfrak{g}$-модулем с конечным числом образующих, содержащим все элементы a^k. Так как для идеалов из $\mathfrak{g}$ выполнено условие обрыва возрастающих цепей, то $\mathfrak{M}$ удовлетворяет условию обрыва возрастающих цепей для $\mathfrak{g}$-модулей.

Следовательно, для цепи $(1)\subseteq(1,\ a)\subseteq(1,\ a,\ a^2)\subseteq\ldots$ существует такое целое число m, что $(1,\ a,\ \ldots,\ a^{m-1})=(1,\ a,\ \ldots,\ a^m)$. Тогда $a^m=a^{m-1}\gamma_1+\ldots+1\gamma_m$ для некоторых элементов γ_i из $\mathfrak{o}$.

Мы можем теперь показать, что если в порядке $\mathfrak{o}$ поля $\mathfrak{A}=\Phi$ выполнено условие III, то условия I и N 1 эквивалентны. В самом деле, пусть элемент a целый. Тогда все степени a и, следовательно, множество $\mathfrak{o}[a]$ полиномов от a с коэффициентами из $\mathfrak{o}$ принадлежат некоторому $\mathfrak{o}$-модулю $(a_1,\ \ldots,\ a_r)$, порожденному элементами a_i из $\mathfrak{A}$. Мы можем представить их в виде $a_i=b_id^{-1}$, где b_i и d лежат в $\mathfrak{o}$. Следовательно, $\mathfrak{o}[a]\subseteq\mathfrak{o}d^{-1}$ и потому $\mathfrak{o}[a]$ является порядком (эквивалентным порядку $\mathfrak{o}$). Так как $\mathfrak{o}[a]\supseteq\mathfrak{o}$, то из условия I следует, что $\mathfrak{o}[a]=\mathfrak{o}$, т. е. $a\in\mathfrak{o}$. Таким образом, порядок $\mathfrak{o}$ целозамкнут. Обратно, предположим, что порядок $\mathfrak{o}$ целозамкнут. Тогда для любого порядка $\mathfrak{o}'$ найдется такой элемент $b\in\mathfrak{A}$, что $\mathfrak{o}'\subseteq\mathfrak{o}b$. Следовательно, элементы из $\mathfrak{o}'$ $\mathfrak{o}$-целые и потому $\mathfrak{o}'\subseteq\mathfrak{o}$. Мы доказали поэтому, что порядок $\mathfrak{o}$ максимальный. Таким образом, если $\mathfrak{A}$ является полем, то условия I, II и III эквивалентны условиям N 1, N 2 и N 3.

Вернемся к общему случаю произвольного кольца $\mathfrak{A}$ и рассмотрим некоторые следствия наших аксиом. Заметим сначала, что любой идеал из $\mathfrak{o}$ в старом смысле, содержащий двусторонний $\mathfrak{o}$-идеал $\mathfrak{a}$, является целым $\mathfrak{o}$-идеалом. Так как эти идеалы находятся во взаимнооднозначном соответствии с идеалами фактор-кольца $\mathfrak{o}/\mathfrak{a}$, то условие II эквивалентно условию II′: В фактор-кольце $\mathfrak{o}/\mathfrak{a}$ кольца $\mathfrak{o}$ по целому двустороннему $\mathfrak{o}$-идеалу $\mathfrak{a}$ выполнено условие обрыва убывающих цепей для (обычных) односторонних идеалов.

Напомним, что для любого кольца с единицей условия обрыва возрастающих цепей односторонних идеалов являются следствием условий обрыва убывающих цепей. Следовательно, первые из них выполнены в $\mathfrak{o}$, и, таким образом, мы имеем:

V. Условия обрыва возрастающих цепей выполнены для целых односторонних $\mathfrak{o}$-идеалов, содержащих любой фиксированный целый двусторонний $\mathfrak{o}$-идеал.

Очевидно, что отсюда следует условие III. Тем не менее мы предпочли выделить III, как отдельное предположение, так как во многих важных случаях оно выполнено, в то время как условие II не выполняется.

Если $\mathfrak{a}$ и $\mathfrak{b}$ являются целыми правыми (левыми, двусторонними) $\mathfrak{o}$-идеалами, то, очевидно, что $\mathfrak{a}+\mathfrak{b}$ будет идеалом того же типа. Если $\mathfrak{a}$ и $\mathfrak{b}$ являются целыми двусторонними $\mathfrak{o}$-идеалами, то $\mathfrak{ab}$ содержит регулярный элемент, и потому $\mathfrak{ab}$ будет целым двусторонним $\mathfrak{o}$-идеалом. Так как пересечение $\mathfrak{a}\cap\mathfrak{b}$ содержит $\mathfrak{ab}$, то $\mathfrak{a}\cap\mathfrak{b}$ — также целый двусторонний $\mathfrak{o}$-идеал.

Определение 3. Целый двусторонний отличный от $\mathfrak{o}$ $\mathfrak{o}$-идеал $\mathfrak{p}$ называется *простым идеалом*, если для любой пары таких целых двусторонних $\mathfrak{o}$-идеалов $\mathfrak{a}$, $\mathfrak{b}$, что $\mathfrak{ab}\equiv 0(\mathrm{mod}\,\mathfrak{p})$, мы имеем либо $\mathfrak{a}\equiv 0\,(\mathfrak{p})$, либо $\mathfrak{b}\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$.

Если $\mathfrak{ab}\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$, то $\mathfrak{a}'\mathfrak{b}'\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$ для $\mathfrak{a}'=\mathfrak{a}+\mathfrak{p}$ и $\mathfrak{b}'=\mathfrak{b}+\mathfrak{p}$. Так как из $\mathfrak{a}'\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$ следует $\mathfrak{a}\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$, то для того, чтобы установить, является ли идеал $\mathfrak{p}$ простым, достаточно проверить целые идеалы $\mathfrak{a}'$, $\mathfrak{b}'$, содержащие $\mathfrak{p}$. Таким образом, если идеал $\mathfrak{p}$ *максимален* в том смысле, что не существует отличного от $\mathfrak{o}$ двустороннего $\mathfrak{o}$-идеала, лежащего между $\mathfrak{o}$ и $\mathfrak{p}$, то идеал $\mathfrak{p}$ простой. Это замечание составляет тривиальную часть следующей важной теоремы:

VI. Целый двусторонний отличный от $\mathfrak{o}$ $\mathfrak{o}$-идеал $\mathfrak{p}$ будет простым тогда и только тогда, когда он максимален. Если это условие выполнено, то $\mathfrak{o}/\mathfrak{p}$ является кольцом матриц над полем.

Свойство максимальности эквивалентно свойству простоты фактор-кольца $\bar{\mathfrak{o}}=\mathfrak{o}/\mathfrak{p}$. Предположим теперь, что $\mathfrak{p}$ — простой идеал. Так как в $\mathfrak{o}$ выполнено условие обрыва убывающих цепей левых идеалов, то оно обладает радикалом $\bar{\mathfrak{r}}$, и потому существует такой двусторонний $\mathfrak{o}$-идеал $\mathfrak{r}$ кольца $\mathfrak{o}$, что $\bar{\mathfrak{r}}=\mathfrak{r}/\mathfrak{p}$. Кольцо $\mathfrak{o}/\mathfrak{r}$ изоморфно кольцу $\bar{\mathfrak{o}}/\bar{\mathfrak{r}}$. Следовательно, кольцо $\mathfrak{o}/\mathfrak{r}$ полупросто. Тогда при соответствующем s $\bar{\mathfrak{r}}^s=0$. Следовательно, $\mathfrak{r}^s\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$, и, так как идеал $\mathfrak{p}$ простой, то $\mathfrak{r}\equiv 0\,(\mathrm{mod}\,\mathfrak{p})$. Это

показывает, что кольцо $\bar{\mathfrak{o}}$ полупросто. Если $\bar{\mathfrak{o}}$ — непростое кольцо, то существуют такие два двусторонних отличных от нуля идеала $\bar{\mathfrak{a}}$ и $\bar{\mathfrak{b}}$ кольца $\bar{\mathfrak{o}}$, что $\bar{\mathfrak{a}}\bar{\mathfrak{b}} = 0$. Но в этом случае существовали бы такие лежащие в $\mathfrak{o}$ двусторонние $\mathfrak{o}$-идеалы $\mathfrak{a}$, $\mathfrak{b}$, что $\mathfrak{ab} \equiv 0 \pmod{\mathfrak{p}}$, но ни $\mathfrak{a}$, ни $\mathfrak{b}$ не лежат в $\mathfrak{p}$. Следовательно, кольцо $\mathfrak{o}$ простое, и идеал $\mathfrak{p}$ максимальный. Вторая часть теоремы является следствием фундаментальной структурной теоремы теории простых колец.

Если $\mathfrak{o}/\mathfrak{p} = \mathfrak{d}_k$, где $\mathfrak{d}$ — тело, то k называется *емкостью* простого идеала $\mathfrak{p}$.

5. Порядки в алгебре. Пусть $\mathfrak{A}$ является сепарабельной алгеброй над Φ, $(\mathfrak{A} : \Phi) = n$, и пусть $\mathfrak{g}$ — порядок в Φ. Рассмотрим вопрос о включении $\mathfrak{g}$ в порядок $\mathfrak{o}$ алгебры $\mathfrak{A}$ [1]). Если $\mathfrak{o}$ — какой-либо из этих порядков, то пусть $\mathfrak{B} = \mathfrak{o}\Phi$ будет наименьшей содержащей $\mathfrak{o}$ подалгеброй алгебры $\mathfrak{A}$. Тогда, если b является некоторым регулярным в $\mathfrak{A}$ элементом из $\mathfrak{o}$, то b будет регулярным в $\mathfrak{B}$, и потому его обратный элемент лежит в $\mathfrak{B}$. Из определения порядка следует, что $\mathfrak{B} = \mathfrak{A}$, и потому $\mathfrak{o}$ содержит базис $u_1, \ldots, u_n$ алгебры $\mathfrak{A}$ над Φ. С другой стороны, если $\mathfrak{o}$ является любым содержащим $\mathfrak{g}$ и базис $u_1, \ldots, u_n$ алгебры $\mathfrak{A}$ подкольцом в $\mathfrak{A}$, то $\mathfrak{o}$ будет порядком. В самом деле, любой элемент из $\mathfrak{A}$ имеет вид $(\sum u_i\gamma_i)\gamma^{-1}$, где γ_i, γ лежат в $\mathfrak{g}$, и так как $\sum u_i\gamma_i$ лежит в $\mathfrak{o}$, то этот элемент имеет вид $b\gamma^{-1}$, где γ и b лежат в $\mathfrak{o}$.

Теорема 8. *Для того чтобы содержащее порядок $\mathfrak{g}$ подкольцо алгебры $\mathfrak{A}$ являлось порядком, необходимо и достаточно, чтобы оно содержало базис алгебры $\mathfrak{A}$ над Φ.*

Мы можем, очевидно, считать $u_1 = 1$ одним из элементов базиса. Допустим теперь, что порядок $\mathfrak{g}$ удовлетворяет условиям I и III (или N 1 и N 3), и предположим,

[1]) Здесь слово „порядок" понимается в первоначальном смысле. Выбор эквивалентных классов порядков будет сделан позже.

что $\mathfrak{o}$ является порядком, состоящим лишь из $\mathfrak{g}$-целых элементов. Для того, чтобы изучить порядки такого типа нам понадобятся следующие теоремы.

Теорема 9. *Сумма $a+b$ и произведение ab коммутирующих ($ab = ba$) $\mathfrak{g}$-целых элементов будут также $\mathfrak{g}$-целыми элементами.*

В самом деле, если $a^m = \sum_0^{m-1} a^i\gamma_i$ и $b^{m'} = \sum_0^{m'-1} b^j\eta_j$, где элементы γ_i и η_i лежат в $\mathfrak{g}$, то все степени $(a+b)^k$ содержатся в $\mathfrak{g}$-модуле с образующими a^ib^j, $0 \leqslant i \leqslant m-1$, $0 \leqslant j \leqslant m'-1$. Следовательно, по теореме 7, элемент $(a+b)$ целый. Подобные же рассуждения применимы к ab.

В качестве непосредственного следствия получаем, что в коммутативной алгебре $\mathfrak{A}$ совокупность $\mathfrak{g}$-целых элементов образует подкольцо. Это замечание может быть применено для доказательства следующей теоремы.

Теорема 10. *Если порядок $\mathfrak{g}$ удовлетворяет условиям* I *и* III, *то минимальный полином $\mu_a(t)$, главный полином $m_a(t)$ и характеристический полином $f_a(t)$ $\mathfrak{g}$-целого элемента a при любом взаимнооднозначном представлении алгебры $\mathfrak{A}$ лежат в $\mathfrak{g}[t]$.*

Пусть старший коэффициент лежащего в $\mathfrak{g}[t]$ полинома $\varphi(t)$ равен 1, a является корнем $\varphi(t)$ и $\mathfrak{B}$ — полем разложения над Φ полинома $\varphi(t)$ [1]). Тогда в $\mathfrak{B}[t]$ полином $\varphi(t) = \Pi(t - a_i)$, и так как $\mu_a(t)$ является делителем $\varphi(t)$, то $\mu_a(t) = \Pi'(t - a_j)$ будет произведением некоторых из множителей $(t - a_j)$. Элементы a_j будут $\mathfrak{g}$-целыми в $\mathfrak{B}$ и, следовательно, коэффициенты полинома $\mu_a(t)$ будут $\mathfrak{g}$-целыми. Так как порядок $\mathfrak{g}$ целозамкнут, то $\mu_a(t)$ лежит в $\mathfrak{g}[t]$. Утверждение относительно $m_a(t)$ и $f_a(t)$ следует из того, что корни этих полиномов совпадают, с точностью до кратности, с корнями $\mu_a(t)$.

Предположим, как и ранее, что $\mathfrak{o}$ является содержащим $\mathfrak{g}$ порядком, состоящим из $\mathfrak{g}$-целых элементов. Пусть

[1]) $\mathfrak{B}' = \Phi(a_1, \ldots, a_n)$, где $\varphi(t) = \Pi(t - a_i)$ в $\mathfrak{B}[t]$. См. Ван-дер-Варден. **Современная алгебра**, ч. I, стр. 101.

элементы $u_1 = 1, u_2, \ldots, u_n$ образуют содержащийся в $\mathfrak{o}$ базис алгебры $\mathfrak{A}$. Тогда, заменив элементы u_i, $i > 1$, их некоторыми кратными $u_i\gamma_i$, где $\gamma_i \in \mathfrak{g}$, и вернувшись к первоначальным обозначениям, мы можем предположить, что константы умножения γ_{kij} в $u_iu_j = \sum u_k\gamma_{kij}$ лежат в $\mathfrak{g}$. Отсюда следует, что совокупность элементов $\sum u_i\mu_i$, где $\mu_i \in \mathfrak{g}$, является порядком $\mathfrak{o}_0 \subseteq \mathfrak{o}$ [1]). Предположим, что $d = \sum u_i\delta_i$ лежит в $\mathfrak{o}$. Тогда, по предыдущей теореме, главные следы $T(u_id)$ и $T(u_iu_j)$ лежат в $\mathfrak{g}$. Уравнения

$$T(u_id) = \sum T(u_iu_j)\,\delta_j$$

показывают, что, так как $\Delta = \det(T(u_iu_j)) \neq 0$, элементы δ_j содержатся в $\mathfrak{g}\Delta^{-1}$. Таким образом, $\mathfrak{o}$ является подмодулем $\mathfrak{g}$-модуля $\mathfrak{o}_0\Delta^{-1}$ с конечным числом образующих. Так как для идеалов порядка $\mathfrak{g}$ выполнено условие обрыва возрастающих цепей, то любой подмодуль $\mathfrak{g}$-модуля с конечным числом образующих имеет конечное число образующих [2]). В частности, это имеет место для $\mathfrak{o}$. Обратно, если $\mathfrak{o}$ является любым содержащим $\mathfrak{g}$ порядком и $\mathfrak{o}$ имеет конечное число образующих над $\mathfrak{g}$, то, по теореме 7, все элементы порядка $\mathfrak{o}$ будут $\mathfrak{g}$-целыми.

Теорема 11. *Для того чтобы порядок $\mathfrak{o}$ ($\supseteq \mathfrak{g}$) состоял лишь из $\mathfrak{g}$-целых элементов, необходимо и достаточно, чтобы $\mathfrak{o}$ был $\mathfrak{g}$-модулем с конечным числом образующих.*

Если теперь $\mathfrak{M}$ является любым $\mathfrak{g}$-модулем, порожденным конечным числом элементов $v_1, \ldots, v_r$, то мы можем написать $v_j = (\sum u_i\nu_{ij})\nu^{-1}$, где ν_{ij} и ν лежат в $\mathfrak{g}$. Тогда $\mathfrak{M} \subseteq \mathfrak{o}_0\nu^{-1} \subseteq \mathfrak{o}\nu^{-1}$. В частности, если $\mathfrak{o}'$ будет любым порядком, состоящим из $\mathfrak{g}$-целых элементов и содержащим порядок $\mathfrak{g}$, то $\mathfrak{o}' \subseteq \mathfrak{o}\nu^{-1}$ при подходящем элементе ν. По

[1]) Одновременно это рассуждение показывает, что порядки рассматриваемого здесь типа существуют. В самом деле, мы можем начать рассуждение с любого базиса u_i, $u_1 = 1$, для которого константы умножения лежат в $\mathfrak{g}$, и взять совокупность $\mathfrak{o}_0$ элементов вида $\sum u_i\mu_i$, где $\mu_i \in \mathfrak{g}$. Тогда $\mathfrak{o}_0$ является порядком.

[2]) Глава 3, теорема 3.

симметрии, существует такой элемент μ из $\mathfrak{g}$, что $\mathfrak{o}'\mu^{-1} \supseteq \mathfrak{o}$, и, таким образом, нами доказана следующая

Теорема 12. *Если два порядка $\mathfrak{o}$ и $\mathfrak{o}'$ состоят из $\mathfrak{g}$-целых элементов и содержат порядок $\mathfrak{g}$, то они эквивалентны.*

Если мы вернемся к доказательству теоремы 11, то увидим, что элемент Δ зависит не от порядка $\mathfrak{o}$, а только от базиса $u_1, \ldots, u_n$. Следовательно, наши рассуждения показывают, что если $\mathfrak{o}'$ является любым порядком, содержащим порядок $\mathfrak{o}$ и состоящим лишь из $\mathfrak{g}$-целых элементов, то $\mathfrak{o}' \subseteq \mathfrak{o}_0\Delta^{-1}$. Кроме того, если $\mathfrak{o}'$ — любой порядок, эквивалентный порядку $\mathfrak{o}$, то $\mathfrak{o}' \subseteq a\mathfrak{o}b$, причем $\mathfrak{g}$-модуль $a\mathfrak{o}b$ обладает конечным числом образующих, и потому все элементы порядка $\mathfrak{o}'$ будут $\mathfrak{g}$-целыми. Таким образом, любой порядок $\mathfrak{o}'$, содержащий порядок $\mathfrak{o}$ и эквивалентный ему, содержится в $\mathfrak{o}_0\Delta^{-1}$; отсюда следует, что существует максимальный порядок $\mathfrak{o}'$, эквивалентный порядку $\mathfrak{o}$ и содержащий его.

Теорема 13. *Если $\mathfrak{o}$ имеет то же значение, что в предыдущей теореме, то $\mathfrak{o}$ можно включить в максимальный порядок $\mathfrak{o}'$, эквивалентный порядку $\mathfrak{o}$.*

Пусть $\mathfrak{S}$ обозначает кольцо $\mathfrak{g}$-целых элементов центра $\mathfrak{C}$ алгебры $\mathfrak{A}$. Тогда, если $\mathfrak{o}$ является порядком, состоящим лишь из $\mathfrak{g}$-целых элементов, то, по теореме 9, $\mathfrak{o}\mathfrak{S}$ будет содержащим кольцо $\mathfrak{S}$ (а, следовательно, и $\mathfrak{g}$) порядком, состоящим лишь из $\mathfrak{g}$-целых элементов. Если сам порядок $\mathfrak{o}$ содержит $\mathfrak{g}$, то, как мы видели, порядки $\mathfrak{o}$ и $\mathfrak{o}\mathfrak{S}$ эквивалентны. Следовательно, если при этом порядок $\mathfrak{o}$, максимален, то $\mathfrak{o} = \mathfrak{o}\mathfrak{S}$ и $\mathfrak{o}$ содержит $\mathfrak{S}$.

Теорема 14. *Любой максимальный порядок $\mathfrak{o}$, содержащий $\mathfrak{g}$ и состоящий лишь из $\mathfrak{g}$-целых элементов, содержит все $\mathfrak{g}$-целые элементы, лежащие в центре кольца $\mathfrak{A}$.*

Пусть порядок $\mathfrak{o}'$, эквивалентный порядку $\mathfrak{o}$, содержит $\mathfrak{g}$ и состоит лишь из $\mathfrak{g}$-целых элементов. Тогда, как мы видели, $\mathfrak{o}'$ содержится в $\mathfrak{g}$-модуле $a\mathfrak{o}b$ с конечным числом образующих, и, следовательно, все элементы порядка $\mathfrak{o}'$

будут $\mathfrak{g}$-целыми. Предположим теперь, что алгебра $\mathfrak{A}$ коммутативна, и $\mathfrak{o}$ является совокупностью всех $\mathfrak{g}$-целых элементов. Тогда $\mathfrak{o}$ будет порядком; все элементы любого порядка $\mathfrak{o}'$, эквивалентного порядку $\mathfrak{o}$, будут $\mathfrak{g}$-целыми, и потому $\mathfrak{o}' \subseteq \mathfrak{o}$.

Теорема 15. *Если алгебра $\mathfrak{A}$ коммутативна, то совокупность $\mathfrak{o}$ всех $\mathfrak{g}$-целых элементов алгебры $\mathfrak{A}$ является максимальным порядком. Любой порядок, эквивалентный порядку $\mathfrak{o}$, содержится в $\mathfrak{o}$.*

Если $\mathfrak{o}' \subseteq a\mathfrak{o}b$ и $\mathfrak{o}$ является порядком, содержащим $\mathfrak{g}$, то также и $\mathfrak{o}'\mathfrak{g} \subseteq a\mathfrak{o}b$. Следовательно, если порядок $\mathfrak{o}'$ эквивалентен порядку $\mathfrak{o}$, то и порядок $\mathfrak{o}'\mathfrak{g}$ эквивалентен $\mathfrak{o}$, а если порядок $\mathfrak{o}'$ максимален, то $\mathfrak{o}' = \mathfrak{o}'\mathfrak{g}$. Подведем итог: если порядок $\mathfrak{g}$ удовлетворяет условиям I и III, то порядки $\mathfrak{o}$, обладающие свойствами 1) $\mathfrak{o}$ содержит $\mathfrak{g}$ и 2) $\mathfrak{o}$ содержит лишь $\mathfrak{g}$-целые элементы, принадлежат к одному классу эквивалентных порядков; все порядки этого класса обладают свойством 2), а все максимальные порядки этого класса обладают обоими свойствами. Далее на протяжении этого параграфа мы будем предполагать, что $\mathfrak{g}$ удовлетворяет условиям I и III и $\mathfrak{o}$ удовлетворяет условиям 1) и 2).

Любой правый идеал $\mathfrak{a}$ лежит в главном $\mathfrak{o}$-идеале $a\mathfrak{o}$, и потому $\mathfrak{a}$ является $\mathfrak{g}$-модулем с конечным числом образующих. Так как идеал $\mathfrak{a}$ содержит регулярный элемент b, то он содержит базис $v_1 = bu_1, \ldots, v_n = bu_n$ алгебры $\mathfrak{A}$. Единица $1 = \sum v_i \rho_i$, где $\rho_i \in \Phi$, и, следовательно, существует соотношение вида $\eta = \sum v_i \eta_i$, где η и η_i лежат в $\mathfrak{g}$. Таким образом, η лежит в пересечении $\mathfrak{a} \cap \mathfrak{g}$, и $\mathfrak{a} \cap \mathfrak{g} \neq 0$. Очевидно, что $\mathfrak{a} \cap \mathfrak{g}$ является $\mathfrak{g}$-идеалом. Отметим также, что идеал $\eta\mathfrak{o} = \mathfrak{o}\eta$ является двусторонним $\mathfrak{o}$-идеалом, содержащимся в $\mathfrak{a}$, и потому идеал $\mathfrak{a}$ ограничен.

Теорема 16. *Любой порядок $\mathfrak{o}$ алгебры $\mathfrak{A}$ ограничен.*

Предположим далее, что $\mathfrak{a}$ — целый двусторонний $\mathfrak{o}$-идеал. Рассмотрим $\mathfrak{g}$-фактор-модуль $\mathfrak{o}/\mathfrak{a}$ и отметим, что он имеет конечное число образующих. Так как он аннулируется идеалом $\mathfrak{a}_0 = \mathfrak{a} \cap \mathfrak{g}$, то его можно рассматривать как $(\mathfrak{g}/\mathfrak{a}_0)$-модуль. Мы видели, что $\mathfrak{a}_0 \neq 0$. Следовательно, если $\mathfrak{g}$ удовлетворяет условию II, то в $\mathfrak{g}/\mathfrak{a}_0$ выполнено условие обрыва убывающих цепей идеалов, и потому в $\mathfrak{o}/\mathfrak{a}$ выполнено условие обрыва убывающих цепей $(\mathfrak{g}/\mathfrak{a}_0)$-подмодулей. Отсюда следует, что для целых $\mathfrak{o}$-идеалов, содержащих идеал $\mathfrak{a}$, выполнено условие обрыва убывающих цепей.

Теорема 17. *Если порядок $\mathfrak{g}$ удовлетворяет условию* II, *то любой порядок $\mathfrak{o}$ алгебры $\mathfrak{A}$ также удовлетворяет этому условию.*

Специальным типом областей $\mathfrak{g}$, в которых выполнены наши условия, являются области главных идеалов. В самом деле, мы видели в главе 3, что для этих областей выполнены условия N 2 и N 3, а выполнение условия N 1 может быть доказано, как и в случае целых чисел, при помощи теоремы об однозначном разложении на простые множители. Пусть $\mathfrak{o}$ является порядком алгебры $\mathfrak{A}$, содержащим порядок $\mathfrak{g}$ и состоящим лишь из $\mathfrak{g}$-целых элементов. Тогда, если элементы $u_1, \ldots, u_n$ образуют содержащийся в $\mathfrak{o}$ базис алгебры $\mathfrak{A}$, таблица умножения для которого имеет лишь целые коэффициенты, то мы видели, что $\mathfrak{o}$ содержит свободный $\mathfrak{g}$-модуль с базисом u_i, и $\mathfrak{o}$ содержится в свободном $\mathfrak{g}$-модуле, базисом которого является $u_i\Delta^{-1}$, где $\Delta = \det\left(T(u_iu_j)\right)$. Отсюда следует, что $\mathfrak{o}$ будет свободным $\mathfrak{g}$-модулем с базисом из n элементов.

Теорема 18. *Если $\mathfrak{g}$ является областью главных идеалов, то любой порядок $\mathfrak{o}$ обладает свободным базисом, состоящим из $n = (\mathfrak{A} : \Phi)$ элементов.*

6. Разложения двусторонних идеалов. Вернемся теперь к общему случаю произвольного кольца $\mathfrak{A}$ и некоторого порядка $\mathfrak{o}$ из $\mathfrak{A}$, удовлетворяющего условиям I—IV [1]). Нашей ближайшей целью является доказательство существования и единственности разложения любого двусторон-

[1]) На самом деле, нам понадобятся в этом параграфе лишь условия I, III, IV и VII: любой простой $\mathfrak{o}$-идеал максимален.

него целого идеала в произведение простых идеалов. Если мы рассмотрим рассуждения § 5 главы 3, то увидим, что решающим шагом являлась теорема о том, что двусторонний $\mathfrak{o}$-идеал $\mathfrak{a}$ содержится в двустороннем $\mathfrak{o}$-идеале $\mathfrak{b}$ тогда и только тогда, когда существует такой двусторонний целый $\mathfrak{o}$-идеал $\mathfrak{c}$, что $\mathfrak{a} = \mathfrak{cb}$. Этот факт вытекает из нижеследующей теоремы.

Теорема 19. *Если $\mathfrak{a}$ является двусторонним $\mathfrak{o}$-идеалом и $\mathfrak{a} \subset \mathfrak{o}$, то $\mathfrak{a}^{-1} \supset \mathfrak{o}$.*

Нам понадобятся две леммы.

Лемма 1. *Любой двусторонний целый $\mathfrak{o}$-идеал $\mathfrak{a}$ содержится в простом идеале.*

Это следует из условия обрыва возрастающих цепей и критерия VI.

Лемма 2. *Любой двусторонний целый $\mathfrak{o}$-идеал $\mathfrak{a}$ содержит произведение простых идеалов.*

Если идеал $\mathfrak{a}$ простой, то лемма справедлива. В противном случае существуют такие два содержащих $\mathfrak{a}$ двусторонних целых $\mathfrak{o}$-идеала $\mathfrak{a}'$ и $\mathfrak{a}''$, что $\mathfrak{a}'\mathfrak{a}'' \equiv 0 \pmod{\mathfrak{a}}$, но $\mathfrak{a}' \not\equiv 0$ и $\mathfrak{a}'' \not\equiv 0 \pmod{\mathfrak{a}}$. Тогда $\mathfrak{a}' \supset \mathfrak{a}$, $\mathfrak{a}'' \supset \mathfrak{a}$. Если мы повторим этот процесс с идеалами $\mathfrak{a}'$ и $\mathfrak{a}''$ и с идеалами, получающимися из них, то получим нашу лемму в качестве следствия условия обрыва возрастающих цепей.

Доказательство теоремы. Пусть $\mathfrak{p}$ является простым идеалом, содержащим $\mathfrak{a}$. Тогда, если $\mathfrak{a}^{-1} = \mathfrak{o}$, то $\mathfrak{p}^{-1} = \mathfrak{o}$. Пусть a будет регулярным элементом из $\mathfrak{p}$, и рассмотрим содержащийся в $\mathfrak{p}$ правый $\mathfrak{o}$-идеал $a\mathfrak{o}$. В силу условия ограниченности, $a\mathfrak{o}$ содержит двусторонний $\mathfrak{o}$-идеал, и потому, по лемме 2, $a\mathfrak{o}$ содержит произведение $\mathfrak{p}_1 \dots \mathfrak{p}_r$ простых идеалов $\mathfrak{p}_i$. Предположим, что идеалы $\mathfrak{p}_i$ выбраны таким образом, что их число r минимальное, т. е. идеал $a\mathfrak{o}$ не содержит произведения $r-1$ простых идеалов. Так как $\mathfrak{p} \supseteq a\mathfrak{o} \supseteq \mathfrak{p}_1 \dots \mathfrak{p}_r$, то один из идеалов $\mathfrak{p}_i$ равен $\mathfrak{p}$ и $\mathfrak{p}_1 \dots \mathfrak{p}_r = \mathfrak{b}\mathfrak{p}\mathfrak{c}$. Тогда $a^{-1}\mathfrak{b}\mathfrak{p}\mathfrak{c} \subset \mathfrak{o}$ и $a^{-1}\mathfrak{b} \subseteq (\mathfrak{pc})^{-1}$. Так как $(\mathfrak{pc})(\mathfrak{pc})^{-1} \subseteq \mathfrak{o}$, то $\mathfrak{p}(\mathfrak{c}(\mathfrak{pc})^{-1}) \subseteq \mathfrak{o}$ и $\mathfrak{c}(\mathfrak{pc})^{-1} \subseteq \mathfrak{p}^{-1} = \mathfrak{o}$. Таким образом, $(\mathfrak{pc})^{-1} \subseteq \mathfrak{c}^{-1}$, а так как $(\mathfrak{pc})^{-1} \supseteq \mathfrak{c}^{-1}$, то мы имеем $(\mathfrak{pc})^{-1} = \mathfrak{c}^{-1}$. Отсюда следует, что $a^{-1}\mathfrak{b} \subseteq \mathfrak{c}^{-1}$, $a^{-1}\mathfrak{bc} \subseteq \mathfrak{o}$ и $\mathfrak{bc} \subseteq a\mathfrak{o}$. Так как $\mathfrak{bc}$ является произведением $r-1$ простого идеала, то мы получаем противоречие с минимальностью r. Важным следствием из этой теоремы является следующая

Теорема 20. *Если $\mathfrak{a}$ — правый (левый) $\mathfrak{o}$-идеал, то $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$ ($\mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}$).*

Множество $\mathfrak{a}^{-1}\mathfrak{a}$ содержится в $\mathfrak{o}$ и потому является целым двусторонним $\mathfrak{o}$-идеалом. Так как порядок $\mathfrak{o}$ максимальный, то порядки идеала $\mathfrak{a}^{-1}\mathfrak{a}$ совпадают с $\mathfrak{o}$. Теперь $(\mathfrak{a}^{-1}\mathfrak{a})^{-1}(\mathfrak{a}^{-1}\mathfrak{a}) \subseteq \mathfrak{o}$, и потому $(\mathfrak{a}^{-1}\mathfrak{a})^{-1}\mathfrak{a}^{-1} \subseteq \mathfrak{a}^{-1}$. Следовательно, $(\mathfrak{a}^{-1}\mathfrak{a})^{-1} \subseteq \mathfrak{o}$ и, в силу предыдущей теоремы, $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$.

Теперь может быть доказана важная

Теорема 21. *Если правый $\mathfrak{o}$-идеал $\mathfrak{a}$ содержится в двустороннем $\mathfrak{o}$-идеале $\mathfrak{b}$, то существует такой целый правый $\mathfrak{o}$-идеал $\mathfrak{c}$, что $\mathfrak{a} = \mathfrak{cb}$.*

Так как $\mathfrak{a} \subseteq \mathfrak{b}$, то $\mathfrak{c} \equiv \mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{o}$, и $\mathfrak{c}$ является целым правым $\mathfrak{o}$-идеалом. Так как $\mathfrak{b}^{-1}\mathfrak{b} = \mathfrak{o}$, то $\mathfrak{cb} = \mathfrak{a}\mathfrak{b}^{-1}\mathfrak{b} = \mathfrak{a}$.

Мы можем теперь повторить рассуждения § 5 главы 3 и получим тогда: 1) коммутативность умножения целых двусторонних $\mathfrak{o}$-идеалов и 2) однозначное разложение любого целого двустороннего идеала в произведение простых идеалов. По теореме 20 двусторонние $\mathfrak{o}$-идеалы образуют относительно умножения группу $G(\mathfrak{o})$ с единицей $\mathfrak{o}$, причем обратным элементом для $\mathfrak{a}$ будет $\mathfrak{a}^{-1}$. Если теперь $\mathfrak{a}$ — любой двусторонний $\mathfrak{o}$-идеал, то в $\mathfrak{o}$ найдется такой регулярный элемент a, что $a\mathfrak{a} \subseteq \mathfrak{o}$, или $(a\mathfrak{o})\mathfrak{a} \subseteq \mathfrak{o}$ [1]. Идеал $a\mathfrak{o}$ содержит некоторый целый двусторонний $\mathfrak{o}$-идеал $\mathfrak{b}$, и потому $\mathfrak{ba} = \mathfrak{c} \subseteq \mathfrak{o}$. Таким образом, $\mathfrak{a} = \mathfrak{b}^{-1}\mathfrak{c}$, где идеалы $\mathfrak{b}$ и $\mathfrak{c}$ целые, и группа $G(\mathfrak{o})$ порождается содержащимися в ней целыми идеалами. Отсюда следует, конечно, что группа $G(\mathfrak{o})$ коммутативна. Каждый элемент $\mathfrak{a}$ из $G(\mathfrak{o})$ имеет единственное представление

[1] В самом деле, существует такой регулярный элемент $b = a^{-1}c$, где a и c лежат в $\mathfrak{o}$, что $\mathfrak{a} \subseteq b\mathfrak{o}$. Следовательно, $\mathfrak{a} \subseteq a^{-1}c\mathfrak{o} \subseteq a^{-1}\mathfrak{o}$ и $a\mathfrak{a} \subseteq \mathfrak{o}$.

в виде $\mathfrak{p}_1^{g_1} \dots \mathfrak{p}_s^{g_s}$, где $g_i \geqq 0$ и $\mathfrak{p}_i$ — различные простые идеалы. Следовательно, нами доказана фундаментальная

Теорема 22. *Двусторонние $\mathfrak{o}$-идеалы образуют группу $G(\mathfrak{o})$ относительно умножения. $G(\mathfrak{o})$ является прямым произведением бесконечных циклических групп, порожденных простыми идеалами порядка $\mathfrak{o}$.*

7. Структура фактор-кольца $\mathfrak{o}/\mathfrak{a}$. *Пусть* $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$, где $\mathfrak{p}_i$ — различные простые идеалы, и все $e_i > 0$. Тогда, положив $\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_i^{-e_i}$, мы получим, что $\mathfrak{o} = \mathfrak{a}_1 + \dots + \mathfrak{a}_s$ и $\mathfrak{a}_i \cap (\mathfrak{a}_1 + \dots + \mathfrak{a}_{i-1} + \mathfrak{a}_{i+1} + \dots + \mathfrak{a}_s) = \mathfrak{a}$. Это непосредственно следует из теоремы 21 и из однозначности разложения на простые множители. Следовательно, $\mathfrak{o}/\mathfrak{a} = \bar{\mathfrak{a}}_1 \oplus \dots \oplus \bar{\mathfrak{a}}_s$, где $\bar{\mathfrak{a}}_i = \mathfrak{a}_i/\mathfrak{a}$. Очевидно, что $\mathfrak{o}/\mathfrak{p}_i^{e_i} = (\mathfrak{a}_i + \mathfrak{p}_i^{e_i})/\mathfrak{p}_i^{e_i} \cong \mathfrak{a}_i/(\mathfrak{a}_i \cap \mathfrak{p}_i^{e_i}) = \bar{\mathfrak{a}}_i$. Отметим также, что если $\mathfrak{a} = \mathfrak{p}^e$, где $\mathfrak{p}$ — простой идеал, то $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a}$ содержит нильпотентный идеал $\bar{\mathfrak{p}} = \mathfrak{p}/\mathfrak{p}^e$, и фактор-кольцо $\bar{\mathfrak{o}}/\bar{\mathfrak{p}}$ изоморфно простому кольцу $\mathfrak{o}/\mathfrak{p}$. Отсюда следует, что $\bar{\mathfrak{p}}$ является радикалом кольца $\bar{\mathfrak{o}}$ и $\bar{\mathfrak{o}}$ — примарное кольцо.

Мы хотим доказать, что для любого идеала $\mathfrak{a}$ фактор-кольцо $\mathfrak{o}/\mathfrak{a}$ будет кольцом главных идеалов. В силу полученного нами прямого разложения кольца $\mathfrak{o}/\mathfrak{a}$, нам достаточно рассмотреть случай $\mathfrak{a} = \mathfrak{p}^e$, и, по теореме 41 из главы 4, наша теорема будет доказана, если мы покажем, что радикал $\bar{\mathfrak{p}} = \mathfrak{p}/\mathfrak{p}^e$ кольца $\mathfrak{o}/\mathfrak{p}^e$ будет главным правым и главным левым идеалом. Но идеалы кольца $\bar{\mathfrak{o}}$ имеют вид $\bar{\mathfrak{b}} = \mathfrak{b}/\mathfrak{p}^e$, где $\mathfrak{b}$ — целый $\mathfrak{o}$-идеал, содержащий $\mathfrak{p}^e$. Следовательно, по теореме 21, любой правый (левый) идеал $\bar{\mathfrak{b}}$ кольца $\bar{\mathfrak{o}}$, содержащийся в идеале $\bar{\mathfrak{p}}$, имеет вид $\bar{\mathfrak{c}}\bar{\mathfrak{p}}$ ($\bar{\mathfrak{p}}\bar{\mathfrak{c}}$), где $\bar{\mathfrak{c}}$ является правым (левым) идеалом. Наша теорема следует поэтому из следующей теоремы.

Теорема 23. *Если каждый содержащийся в радикале $\mathfrak{P}$ правый (левый) идеал примарного кольца $\mathfrak{O}$ может быть представлен в виде $\mathfrak{C}\mathfrak{P}$ ($\mathfrak{P}\mathfrak{C}$), где $\mathfrak{C}$ — правый (левый) идеал, то радикал $\mathfrak{P}$ является главным правым (левым) идеалом.*

Напомним, что $\mathfrak{O}$ является матричным кольцом $\mathfrak{O}_{0k}$ над вполне примарным кольцом $\mathfrak{O}_0$. Радикалом кольца $\mathfrak{O}_0$ будет $\mathfrak{O}_0 \cap \mathfrak{P} = \mathfrak{P}_0$, и $\mathfrak{P} = \sum e_{ij}\mathfrak{P}_0$, где элементы e_{ij} образуют матричный базис кольца $\mathfrak{O} = \sum e_{ij}\mathfrak{O}_0$. Предположим сначала, что $\mathfrak{P}^2 = 0$. Возьмем в $\mathfrak{P}_0$ отличный от нуля элемент w и рассмотрим правый идеал $w\mathfrak{O}$. Очевидно, что $w\mathfrak{O} \subseteq \mathfrak{P}$, и потому $w\mathfrak{O} = \mathfrak{C}\mathfrak{P}$, где $\mathfrak{C}$ — некоторый правый идеал. Так как $(\mathfrak{C} + \mathfrak{P})\mathfrak{P} = \mathfrak{C}\mathfrak{P}$, то мы можем предположить, что $\mathfrak{C} \supset \mathfrak{P}$. Рассмотрим простое кольцо $\bar{\mathfrak{O}} = \mathfrak{O}/\mathfrak{P}$ и в нем правый идеал $\bar{\mathfrak{C}} = \mathfrak{C}/\mathfrak{P}$. Мы знаем, что $\bar{\mathfrak{C}}$ имеет вид $\bar{u}\bar{\mathfrak{O}}$, где $\bar{u}$ является отличным от нуля идемпотентным элементом. Но смежные классы $\bar{e}_{ij} = e_{ij} + \mathfrak{P}$ образуют матричный базис кольца $\bar{\mathfrak{O}}$, и $\bar{\mathfrak{O}} = \sum \bar{e}_{ij}\bar{\mathfrak{O}}_0$, где $\bar{\mathfrak{O}}_0 = (\mathfrak{O}_0 + \mathfrak{P})/\mathfrak{P}$ является телом, изоморфным телу $\mathfrak{O}_0/\mathfrak{P}_0$. Отсюда следует существование такого регулярного элемента $\bar{q}$ из $\bar{\mathfrak{O}}$, что $\bar{u} = \bar{q}^{-1}\sum_1^t \bar{e}_{ii}\bar{q}$. Любой элемент q из смежного класса $\bar{q}$ регулярен в $\mathfrak{O}$, и, вследствие вида идеала $\bar{\mathfrak{C}}$, идеал $\mathfrak{C}$ состоит из элементов вида $(q^{-1}e_t q)x + z$, где $x \in \mathfrak{O}$, $z \in \mathfrak{P}$ и $e_t = \sum_1^t e_{ii}$. Следовательно, $w = \sum_j q^{-1}e_t y_j$, где $y_j \in \mathfrak{P}$, и $qw = \sum e_t y_j$. Если мы представим q в виде $q = \sum e_{ij}q_{ij}$, где $q_{ij} \in \mathfrak{O}_0$, то из этого равенства будет следовать, что $q_{ij}w = 0$ при $i = t+1, \dots, n$. Так как каждый необратимый элемент кольца $\mathfrak{O}_0$ содержится в $\mathfrak{P}_0$, то эти элементы q_{ij} лежат в $\mathfrak{P}_0$. При $t \neq n$ это противоречит регулярности элемента q; отсюда следует, что $\bar{u} = \bar{1}$. Тогда $\bar{\mathfrak{C}} = \bar{\mathfrak{O}}$, $\mathfrak{C} = \mathfrak{O}$ и $\mathfrak{P} = w\mathfrak{O}$ является главным правым идеалом. Если $\mathfrak{P}^2 \neq 0$, то рассматривается фактор-кольцо $\mathfrak{O}/\mathfrak{P}^2$. Оно удовлетворяет условиям теоремы, и, кроме того, квадрат его радикала $\mathfrak{P}^* = \mathfrak{P}/\mathfrak{P}^2$ равен нулю. Следовательно, идеал $\mathfrak{P}/\mathfrak{P}^2$

является главным, т. е. $\mathfrak{P} = w\mathfrak{O} + \mathfrak{P}^2$. Тогда $\mathfrak{P}^2 = w\mathfrak{P} + \mathfrak{P}^3$, $\mathfrak{P}^3 = w\mathfrak{P}^2 + \mathfrak{P}^4, \ldots$, и потому $\mathfrak{P} = w\mathfrak{O}$. Таким же образом доказываем, что $\mathfrak{P}$ является главным левым идеалом.

Отсюда следует

Теорема 24. *Фактор-кольцо* $\mathfrak{o}/\mathfrak{a}$ *кольца* $\mathfrak{o}$ *по целому двустороннему* $\mathfrak{o}$*-идеалу* $\mathfrak{a}$ *является кольцом главных идеалов.*

8. Ограниченные $\mathfrak{o}$-модули. Предыдущая теорема позволяет нам получить структуру $\mathfrak{o}$-модуля $\mathfrak{M}$ с конечным числом образующих, *ограниченного* в том смысле, что аннулирующий его идеал содержит регулярный элемент. Аннулирующий идеал $\mathfrak{a}$ будет тогда целым двусторонним $\mathfrak{o}$-идеалом, и $\mathfrak{M}$ может рассматриваться как $\bar{\mathfrak{o}}$-модуль, где $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a}$. Так как в кольце главных идеалов $\mathfrak{o}$ выполнено условие обрыва убывающих цепей, то к нему непосредственно приложимы результаты §§ 15—16 главы 4. Мы получаем, таким образом, что $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \ldots \oplus \mathfrak{M}_u$, где $\mathfrak{M}_i$ являются неразложимыми циклическими $\mathfrak{o}$-модулями (или $\bar{\mathfrak{o}}$-модулями).

Назовем аннулирующий идеал $\mathfrak{a}$ *границей* модуля $\mathfrak{M}$. Для того чтобы модуль $\mathfrak{M}$ был неразложим, необходимо, чтобы его граница была степенью простого идеала. Это непосредственно следует из разложения $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a} = \bar{\mathfrak{a}}_1 \oplus \oplus \ldots \oplus \bar{\mathfrak{a}}_s$, где $\bar{\mathfrak{a}}_i = \mathfrak{a}\mathfrak{p}_i^{-e_i}/\mathfrak{a}$, и $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ является разложением идела $\mathfrak{a}$ в произведение степеней различных простых идеалов. Очевидно, что если модули $\mathfrak{M}$ и $\mathfrak{N}$ ограничены и $\mathfrak{o}$-изоморфны, то они имеют одну и ту же границу. С другой стороны, если модули $\mathfrak{M}$ и $\mathfrak{N}$ неразложимы и имеют одинаковую границу $\mathfrak{p}^e$, то оба эти модуля можно рассматривать как $(\mathfrak{o}/\mathfrak{p}^e)$-модули. Следовательно, в силу результатов § 16 главы 4, модули $\mathfrak{M}$ и $\mathfrak{N}$ $(\mathfrak{o}/\mathfrak{p}^e)$-изоморфны, а тогда они и $\mathfrak{o}$-изоморфны. Напомним также, что неразложимый ограниченный $\mathfrak{o}$-модуль $\mathfrak{M}$ обладает лишь одним композиционным рядом, и его длина равна показателю e простого идеала $\mathfrak{p}$ в границе $\mathfrak{p}^e$ модуля $\mathfrak{M}$. Любой подмодуль и фактор-модуль модуля $\mathfrak{M}$ неразложимы [1].

Пусть теперь $\mathfrak{M}$ будет произвольным модулем, и пусть $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, где модули $\mathfrak{M}_i$ неразложимы и отличны от нуля. Если границей модуля $\mathfrak{M}_i$ является $\mathfrak{p}_i^{e_i}$, где $\mathfrak{p}_i$ — простой идеал, то из теоремы Крулля-Шмидта видно, что идеалы $\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_u^{e_u}$ будут инвариантами модуля $\mathfrak{M}$. Инварианты двух $\mathfrak{o}$-изоморфных ограниченных модулей $\mathfrak{M}$ и $\mathfrak{N}$ совпадают. Обратно, если $\mathfrak{M}$ и $\mathfrak{N}$ имеют одинаковые инварианты, то мы можем предположить, что индексы их неразложимых компонент выбраны таким образом, чтобы модули $\mathfrak{M}_i$ и $\mathfrak{N}_i$ имели одинаковую границу. Тогда $\mathfrak{M}_i$ и $\mathfrak{N}_i$, а, следовательно, и $\mathfrak{M}$ и $\mathfrak{N}$ $\mathfrak{o}$-изоморфны.

Для приложений к теории идеалов более удобно иметь дело с дуальным разложением нуля в прямое пересечение. Здесь мы рассматриваем такие отличные от $\mathfrak{M}$ подмодули $\mathfrak{M}_i'$, что $0 = \mathfrak{M}_1' \cap \ldots \cap \mathfrak{M}_u'$, $\mathfrak{M}_i' + (\mathfrak{M}_1' \cap \ldots \cap \mathfrak{M}_{i-1}' \cap \mathfrak{M}_{i+1}' \cap \ldots \cap \mathfrak{M}_u') = \mathfrak{M}$ и модули $\mathfrak{M}/\mathfrak{M}_i'$ неразложимы. Напомним, что если $\mathfrak{M} = \mathfrak{M}_1 \oplus \ldots \oplus \mathfrak{M}_u$, где модули $\mathfrak{M}_i$ неразложимы, то мы получаем дуальное разложение нуля, полагая $\mathfrak{M}_i' = \mathfrak{M}_1 + \ldots + \mathfrak{M}_{i-1} + \mathfrak{M}_{i+1} + \ldots + \mathfrak{M}_u$. Обратно, любое множество подмодулей $\mathfrak{M}_i'$ описанного типа приводит к множеству подмодулей $\mathfrak{M}_i$, если положить $\mathfrak{M}_i = \mathfrak{M}_1' \cap \ldots \cap \mathfrak{M}_{i-1}' \cap \mathfrak{M}_{i+1}' \cap \ldots \cap \mathfrak{M}_u'$. Из доказанного следует, что модуль $\mathfrak{M}$ вполне определяется с точностью до $\mathfrak{o}$-изоморфизма границами модулей $\mathfrak{M}/\mathfrak{M}_i'$ ($\mathfrak{o}$-изоморфных модулям $\mathfrak{M}_i$), где $\mathfrak{M}_i'$ являются компонентами дуального разложения.

9. Разложение целых $\mathfrak{o}$-идеалов. Теперь нетрудно увидеть важность предположения об ограниченности целых правых (левых) идеалов. Из ограниченности целого правого $\mathfrak{o}$-идеала $\mathfrak{b}$ вытекает, что $\mathfrak{o}$-модуль $\mathfrak{M} = \mathfrak{o}/\mathfrak{b}$ огра-

[1] Вообще любой подмодуль (фактор-модуль) ограниченного $\mathfrak{o}$-модуля $\mathfrak{M}$ ограничен. Его граница является делителем границы модуля $\mathfrak{M}$.

ничен. В самом деле, если $\mathfrak{a}$ является содержащимся в $\mathfrak{b}$ двусторонним $\mathfrak{o}$-идеалом, то $\mathfrak{a}$ содержится в аннуляторе модуля $\mathfrak{M}$. Граница модуля $\mathfrak{M}$ будет объединением всех содержащихся в $\mathfrak{b}$ двусторонних $\mathfrak{o}$-идеалов. Мы будем называть этот $\mathfrak{o}$-идеал также (правой) *границей* идеала $\mathfrak{b}$. Таким же образом определяется левая граница целого левого $\mathfrak{o}$-идеала.

Соответственно дуальному разложению модуля $\mathfrak{M} = \mathfrak{o}/\mathfrak{b}$ мы получаем такие правые $\mathfrak{o}$-идеалы $\mathfrak{q}_i$ $(i = 1, \ldots, u)$, что

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_u = \mathfrak{b}, \quad \mathfrak{q}_i + (\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{i-1} \cap \mathfrak{q}_{i+1} \cap \ldots \cap \mathfrak{q}_u) = \mathfrak{o}$$

или, если применять обычное обозначение $[\,,]$ для пересечения и $(\,,)$ для объединения, то

$$[\mathfrak{q}_1, \ldots, \mathfrak{q}_u] = \mathfrak{b}, \quad (\mathfrak{q}_i, [\mathfrak{q}_1, \ldots, \mathfrak{q}_{i-1}, \mathfrak{q}_{i+1}, \ldots, \mathfrak{q}_u]) = \mathfrak{o}. \quad (1)$$

Дуальными компонентами модуля $\mathfrak{M}$ будут модули $\mathfrak{M}_i' = \mathfrak{q}_i/\mathfrak{b}$. Так как модуль $\mathfrak{M}/\mathfrak{M}_i'$ неразложим, то и модуль $\mathfrak{o}/\mathfrak{q}_i$, $\mathfrak{o}$-изоморфный модулю $\mathfrak{o}/\mathfrak{b}/\mathfrak{b}/\mathfrak{q}_i = \mathfrak{M}/\mathfrak{M}_i'$, неразложим. Граница модуля $\mathfrak{M}/\mathfrak{M}_i'$ является границей идеала $\mathfrak{q}_i$. Очевидно, что справедливо также и обратное утверждение: любое разложение идеала $\mathfrak{b}$ в прямое пересечение (в смысле равенства (1)) таких идеалов, что $\mathfrak{o}/\mathfrak{q}_i$ являются неразложимыми $\mathfrak{o}$-модулями, приводит к разложению нуля в $\mathfrak{M} = \mathfrak{o}/\mathfrak{b}$ в прямое пересечение таких подмодулей $\mathfrak{M}_i'$, что модули $\mathfrak{M}/\mathfrak{M}_i'$ неразложимы. Из общей теории следует, что если $\overline{\mathfrak{b}}$ является вторым целым правым $\mathfrak{o}$-идеалом и $\overline{\mathfrak{b}} = [\overline{\mathfrak{q}}_1, \overline{\mathfrak{q}}_2, \ldots]$ — таким его разложением в прямое пересечение, что модули $\mathfrak{o}/\overline{\mathfrak{q}}_i$ неразложимы, то для того чтобы модули $\mathfrak{o}/\mathfrak{b}$ и $\mathfrak{o}/\overline{\mathfrak{b}}$ были $\mathfrak{o}$-изоморфны, необходимо и достаточно, чтобы границы $\overline{\mathfrak{p}}_1^{f_1}$, $\overline{\mathfrak{p}}_2^{f_2}, \ldots$ идеалов $\overline{\mathfrak{q}}_1, \overline{\mathfrak{q}}_2, \ldots$ совпадали с точностью до порядка с границами идеалов $\mathfrak{q}_1, \mathfrak{q}_2, \ldots$ Как и в случае областей главных идеалов, мы называем идеалы $\mathfrak{b}$ и $\overline{\mathfrak{b}}$ *подобными* (справа), если модули $\mathfrak{o}/\mathfrak{b}$ и $\mathfrak{o}/\overline{\mathfrak{b}}$ $\mathfrak{o}$-изоморфны. Тогда мы имеем следующую теорему.

Теорема 25. *Если* $\mathfrak{b} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots]$ *и* $\overline{\mathfrak{b}} = [\overline{\mathfrak{q}}_1, \overline{\mathfrak{q}}_2, \ldots]$ *являются разложениями целых правых* $\mathfrak{o}$*-идеалов* $\mathfrak{b}$ *и* $\overline{\mathfrak{b}}$ *в прямое пересечение таких идеалов* $\mathfrak{q}_i$ *и* $\overline{\mathfrak{q}}_i$, *что модули* $\mathfrak{o}/\mathfrak{q}_i$ *и* $\mathfrak{o}/\overline{\mathfrak{q}}_i$ *неразложимы, то для того чтобы идеалы* $\mathfrak{b}$ *и* $\overline{\mathfrak{b}}$ *были подобны, необходимо и достаточно, чтобы совокупности границ у идеалов* $\mathfrak{q}_i$ *и* $\overline{\mathfrak{q}}_i$ *совпадали.*

Если $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ — целый двусторонний $\mathfrak{o}$-идеал и $\mathfrak{p}_i$ — различные простые идеалы, то $\mathfrak{a} = [\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s}]$ и $(\mathfrak{p}_i^{e_i}, [\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_{i-1}^{e_{i-1}}, \mathfrak{p}_{i+1}^{e_{i+1}}, \ldots]) = \mathfrak{o}$. Кроме того, $\overline{\mathfrak{o}} = \mathfrak{o}/\mathfrak{p}^e$, где $\mathfrak{p}$ — простой идеал, будет примарным кольцом с радикалом $\overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{p}^e$. Так как $\mathfrak{o}/\overline{\mathfrak{p}} = \mathfrak{d}_k$, где $\mathfrak{d}$ является телом и k — емкостью идеала $\mathfrak{p}$, то $\overline{\mathfrak{o}}$ будет прямой суммой k изоморфных между собой неразложимых правых идеалов. Отсюда следует, что в любом разложении идеала $\mathfrak{p}^e$ в прямое пересечение $[\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_k]$, где модули $\mathfrak{o}/\mathfrak{q}_i$ неразложимы, содержится точно k идеалов, и все идеалы $\mathfrak{q}_i$ подобны между собой. Таким образом, все идеалы $\mathfrak{q}_i$ имеют одну и ту же границу, которой будет поэтому идеал $\mathfrak{p}^e$. В общем случае произвольного целого двустороннего $\mathfrak{o}$-идеала $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ мы получаем разложение $\mathfrak{a} = [\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s}]$ в прямое пересечение, разлагая описанным образом идеалы $\mathfrak{p}_i^{e_i}$.

Теорема 26. *Пусть* $\mathfrak{a} = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_s^{e_s}$ *является целым двусторонним* $\mathfrak{o}$*-идеалом и* $\mathfrak{p}_i$ *— простым идеалом емкости* k_i, *причем* $\mathfrak{p}_i \neq \mathfrak{p}_j$, *если* $i \neq j$. *Тогда* $\mathfrak{a}$ *будет прямым пересечением* $[\mathfrak{q}_{11}, \ldots, \mathfrak{q}_{k_11}; \ldots; \mathfrak{q}_{1s}, \ldots, \mathfrak{q}_{k_ss}]$, *где модули* $\mathfrak{o}/\mathfrak{q}_{ij}$ *неразложимы, и при фиксированном* j *любые два идеала* $\mathfrak{q}_{ij}$ *и* $\mathfrak{q}_{i'j}$ *подобны и имеют границу* $\mathfrak{p}_j^{e_j}$.

Непосредственным следствием теории модулей является также следующая

Теорема 27. *Если* $\mathfrak{q}$ *— такой целый правый* $\mathfrak{o}$*-идеал, что модуль* $\mathfrak{o}/\mathfrak{q}$ *неразложим, то* $\mathfrak{o}/\mathfrak{q}$ *имеет лишь один композиционный ряд, и его длина равна* e, *если границей идеала* $\mathfrak{q}$ *будет* $\mathfrak{p}^e$, *где* $\mathfrak{p}$ *— простой идеал. Все компози-*

ционные факторы модуля $\mathfrak{o}/\mathfrak{q}$ $\mathfrak{o}$*-изоморфны между собой. Если* $\mathfrak{q}'$ *— любой содержащий* $\mathfrak{q}$ *целый правый* $\mathfrak{o}$*-идеал, то модуль* $\mathfrak{o}/\mathfrak{q}'$ *также неразложим.*

Из теорем 26 и 27 мы получаем

Следствие: *Простой идеал* $\mathfrak{p}$ *емкости* k *представим в виде прямого пересечения* $[\mathfrak{q}_1, \ldots, \mathfrak{q}_k]$ *максимальных правых подобных между собой* $\mathfrak{o}$*-идеалов* $\mathfrak{q}_i$ *и будет границей этих идеалов.*

10. Нормальные идеалы. Для того чтобы получить удовлетворительную теорию разложения односторонних идеалов, необходимо рассматривать одновременно все максимальные порядки $\mathfrak{o}$, эквивалентные фиксированному порядку. Это важное замечание было впервые сделано Брандтом для порядков в алгебрах. В дальнейшем мы будем предполагать, что все максимальные порядки удовлетворяют условиям II, III и IV. Следует отметить, что условие IV справедливо для всех максимальных порядков, если оно выполнено для одного из них.

Определение 4. Идеал $\mathfrak{a}_{ik}$ называется *нормальным*, если как его левый порядок $\mathfrak{o}_i$, так и его правый порядок $\mathfrak{o}_k$ максимальны.

В следующих двух параграфах мы изложим теорию разложений нормальных идеалов. Здесь же мы установим нормальность любых правых (левых) $\mathfrak{o}$-идеалов максимального порядка $\mathfrak{o}$, для которых развиваемая ниже теория будет поэтому иметь место.

Лемма 1. *Для любого целого правого отличного от* $\mathfrak{o}$ $\mathfrak{o}$*-идеала* $\mathfrak{b}$*, границей которого является простой идеал* $\mathfrak{p}$*, существует такой целый левый* $\mathfrak{o}$*-идеал* $\mathfrak{c}$ *с (левой) границей* $\mathfrak{p}$*, что* $\mathfrak{p} = \mathfrak{c}\mathfrak{b}$.

Рассмотрим правый идеал $\mathfrak{b}/\mathfrak{p} = \overline{\mathfrak{b}}$ простого кольца $\overline{\mathfrak{o}} = \mathfrak{o}/\mathfrak{p}$. Так как $\overline{\mathfrak{b}} \neq \overline{\mathfrak{o}}$, то левый идеал $\overline{\mathfrak{c}}$, состоящий из левых аннуляторов элементов идеала $\overline{\mathfrak{b}}$, отличен от нуля. Пусть идеалу $\overline{\mathfrak{c}}$ соответствует целый левый $\mathfrak{o}$-идеал $\mathfrak{c}$, тогда $\mathfrak{c} \neq \mathfrak{p}$, и $\mathfrak{p}^2 \subseteq \mathfrak{c}\mathfrak{b} \subseteq \mathfrak{p}$. Так как $\mathfrak{c}\mathfrak{b}$ является двусторонним $\mathfrak{o}$-идеалом, то либо $\mathfrak{c}\mathfrak{b} = \mathfrak{p}^2$, либо $\mathfrak{c}\mathfrak{b} = \mathfrak{p}$. Если бы было справедливо первое равенство, то для каждого элемента y из $\mathfrak{c}$ мы имели бы $y\mathfrak{p} \subseteq \mathfrak{p}^2$, и, умножая на $\mathfrak{p}^{-1}$, получили бы $y\mathfrak{o} \subseteq \mathfrak{p}$. Это противоречит тому, что в идеале $\mathfrak{c}$ существуют элементы y, не лежащие в $\mathfrak{p}$. Следовательно, $\mathfrak{c}\mathfrak{b} = \mathfrak{p}$.

Лемма 2. *Если целый правый* $\mathfrak{o}$*-идеал* $\mathfrak{b}$ *строго содержится в* $\mathfrak{o}$*, то* $\mathfrak{b}^{-1} \supset \mathfrak{o}$.

Пусть $\mathfrak{q}$ является таким максимальным правым $\mathfrak{o}$-идеалом, что $\mathfrak{o} \supset \mathfrak{q} \supset \mathfrak{b}$. Тогда граница $\mathfrak{p}$ идеала $\mathfrak{q}$ будет простым идеалом. Если a — регулярный элемент из $\mathfrak{p}$, то $a\mathfrak{o} = \mathfrak{c}\mathfrak{p}$, где $\mathfrak{c}$ — правый $\mathfrak{o}$-идеал. По предыдущей лемме $\mathfrak{p} = \mathfrak{b}\mathfrak{q}$, где $\mathfrak{b}$ — некоторый левый $\mathfrak{o}$-идеал, содержащий $\mathfrak{p}$, но отличный от него. Следовательно, $a\mathfrak{o} = \mathfrak{c}\mathfrak{b}\mathfrak{q}$, $\mathfrak{o} = a^{-1}\mathfrak{c}\mathfrak{b}\mathfrak{q}$, и потому $a^{-1}\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{q}^{-1}$. Если $\mathfrak{q}^{-1} = \mathfrak{o}$, то $a^{-1}\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{o}$, $\mathfrak{c}\mathfrak{b} \subseteq a\mathfrak{o} = \mathfrak{c}\mathfrak{p}$ и $\mathfrak{c}\mathfrak{b}\mathfrak{p}^{-1} \subseteq \mathfrak{c}$. Таким образом, $\mathfrak{b}\mathfrak{p}^{-1}$ содержится в максимальном порядке $\mathfrak{o}$. Отсюда следует, что $\mathfrak{b} \subseteq (\mathfrak{p}^{-1})^{-1} = \mathfrak{p}$. Это противоречие показывает, что $\mathfrak{q}^{-1} \supset \mathfrak{o}$ и, следовательно, $\mathfrak{b}^{-1} \supset \mathfrak{o}$.

Лемма 3. *Если* $\mathfrak{b}$ *является правым* $\mathfrak{o}$*-идеалом, причем порядок* $\mathfrak{o}$ *максимален, то* $\mathfrak{b}^{-1}$ *будет нормальным идеалом.*

Пусть $\mathfrak{o}'$ является левым порядком идеала $\mathfrak{b}$, $\mathfrak{o}''$ — правым порядком идеала $\mathfrak{b}^{-1}$ и $\mathfrak{o}^*$ — любым порядком, содержащим $\mathfrak{o}''$. Очевидно, что $\mathfrak{o}^* \supseteq \mathfrak{o}'' \supseteq \mathfrak{o}'$. Рассмотрим множество $\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}$. Так как $(\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b})(\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}) \subseteq \mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{o}'\mathfrak{o}^*\mathfrak{b} = \mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}$, то $\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}$ будет подкольцом кольца $\mathfrak{A}$. Оно содержит $\mathfrak{o}$, так как $\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b} \supseteq \mathfrak{b}^{-1}\mathfrak{b} = \mathfrak{o}$. Если теперь a и b являются регулярными элементами соответственно из идеалов $\mathfrak{b}^{-1}$ и $\mathfrak{b}$, то $a\mathfrak{o}^*b \subseteq \mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}$ и $b(\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b})a \subseteq \mathfrak{b}\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}\mathfrak{b}^{-1} \subseteq \mathfrak{o}'\mathfrak{o}^*\mathfrak{o}' = \mathfrak{o}^*$. Это показывает, что $\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b}$ будет порядком, и потому, в силу максимальности порядка $\mathfrak{o}$, $\mathfrak{b}^{-1}\mathfrak{o}^*\mathfrak{b} = \mathfrak{o}$. Отсюда следует, что $\mathfrak{b}^{-1}\mathfrak{o}^* \subseteq \mathfrak{b}^{-1}$, и так как $\mathfrak{o}''$ является правым порядком идеала $\mathfrak{b}^{-1}$, то $\mathfrak{o}^* = \mathfrak{o}''$. Это доказывает максимальность порядка $\mathfrak{o}''$ и нормальность идеала $\mathfrak{b}^{-1}$.

Теорема 28. *Если порядок* $\mathfrak{o}$ *максимален, то любой правый (левый)* $\mathfrak{o}$*-идеал* $\mathfrak{b}$ *будет нормальным идеалом.*

Пусть сначала $\mathfrak{b}$ будет целым идеалом и пусть $\mathfrak{o} \supset \mathfrak{b}_1 \supset \mathfrak{b}_2 \supset \ldots \supset \mathfrak{b}_m = \mathfrak{b}$ будет цепочкой правых $\mathfrak{o}$-идеалов, соответствующих композиционному ряду модуля $\mathfrak{o}/\mathfrak{b}$. Тогда $\mathfrak{b}^{-1} \supset \mathfrak{o}$ и, следовательно, $(\mathfrak{b}^{-1})^{-1} \subset \mathfrak{o}$. Так как $\mathfrak{b}^{-1}\mathfrak{b}\mathfrak{b}^{-1} = \mathfrak{o}\mathfrak{b}^{-1} = \mathfrak{b}^{-1}$, то $\mathfrak{b} \subseteq (\mathfrak{b}^{-1})^{-1}$. Следовательно, если $m = 1$, то $\mathfrak{b} = (\mathfrak{b}^{-1})^{-1}$, в силу максимальности $\mathfrak{b}$. Тогда теорема следует из Леммы 3. Допустим теперь, что теорема доказана для целых идеалов $\mathfrak{b}'$, длина модуля $\mathfrak{o}/\mathfrak{b}'$ которых меньше m. Тогда $\mathfrak{b}_{m-1}$ будет нормальным идеалом, а левый порядок $\mathfrak{o}'$ идеала $\mathfrak{b}_{m-1}$ — максимальным порядком и $\mathfrak{b}_{m-1}\mathfrak{b}_{m-1}^{-1} = \mathfrak{o}'$. Мы хотим доказать, что $\mathfrak{o}' \supset \mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$ и что идеал $\mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$ максимален в $\mathfrak{o}'$. Очевидно, что $\mathfrak{o}' = \mathfrak{b}_{m-1}\mathfrak{b}_{m-1}^{-1} \supseteq \mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$ и, если $\mathfrak{o}' = \mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$, то $\mathfrak{o}'\mathfrak{b}_{m-1} = \mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}\mathfrak{b}_{m-1} = \mathfrak{b}_m\mathfrak{o} = \mathfrak{b}_m$ вопреки неравенству $\mathfrak{b}_{m-1} \supset \mathfrak{b}_m$. Далее, пусть $\mathfrak{c}$ будет таким правым $\mathfrak{o}'$-идеалом, что $\mathfrak{o}' \supset \mathfrak{c} \supseteq \mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$. Тогда $\mathfrak{o}'\mathfrak{b}_{m-1} = \mathfrak{b}_{m-1} \supseteq \mathfrak{c}\mathfrak{b}_{m-1} \supseteq \mathfrak{b}_m$, и либо $\mathfrak{b}_{m-1} = \mathfrak{c}\mathfrak{b}_{m-1}$, либо $\mathfrak{c}\mathfrak{b}_{m-1} = \mathfrak{b}_m$. Если $\mathfrak{b}_{m-1} = \mathfrak{c}\mathfrak{b}_{m-1}$, то $\mathfrak{o}' = \mathfrak{c}\mathfrak{o}' = \mathfrak{c}$. Следовательно, $\mathfrak{c}\mathfrak{b}_{m-1} = \mathfrak{b}_m$ и $\mathfrak{c} = \mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$. Это доказывает, что $\mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$ является максимальным правым $\mathfrak{o}'$-идеалом, содержашимся в $\mathfrak{o}'$, и, согласно ранее доказанному, идеал $\mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$ будет нормальным. Как легко видеть, левый порядок идеала $\mathfrak{b}_m\mathfrak{b}_{m-1}^{-1}$ совпадает с левым порядком идеала $\mathfrak{b}_m$, и потому идеал $\mathfrak{b}_m = \mathfrak{b}$ нормален. Если идеал $\mathfrak{b}$ не является целым, то существует такой регулярный элемент a, что $a\mathfrak{b} \subseteq \mathfrak{o}$. Так как правый $\mathfrak{o}$-идеал $a\mathfrak{b}$ целый, то его левый порядок максимален. Если теперь $\mathfrak{o}^*$ будет левым порядком идеала $\mathfrak{b}$, то $a\mathfrak{o}^*a^{-1}$ будет левым порядком идеала $a\mathfrak{b}$. Так как $a\mathfrak{o}^*a^{-1}$ является максимальным порядком, то и порядок $\mathfrak{o}^*$ максимальный.

11. Группоид Брандта. Для того чтобы получить обобщение теоремы 22, применимое к односторонним идеалам, нам понадобится понятие группоида, которое мы теперь и определим. Система G называется *группоидом*, если для некоторых пар элементов этой системы определено умножение, удовлетворяющее следующим условиям:

1. Для каждого элемента a_{ij} существуют такие однозначно определенные элементы e_i и e_j системы G, что произведения e_ia_{ij} и $a_{ij}e_j$ определены, и $e_ia_{ij} = a_{ij}e_j = a_{ij}$. Эти элементы называются соответственно *правой* и *левой единицами* элемента a_{ij}.

2. Если e является единицей для любого элемента из G, то e является своей собственной левой единицей и своей собственной правой единицей.

3. Произведение ab определено тогда и только тогда, когда правая единица элемента a совпадает с левой единицей элемента b.

4. Если произведения ab и bc определены, то и произведения $(ab)c$ и $a(bc)$ определены, причем $(ab)c = a(bc)$.

5. Для любого элемента a_{ij} с левой единицей e_i и правой единицей e_j найдется такой элемент a_{ij}^{-1} с левой единицей e_j и правой единицей e_i, что $a_{ij}a_{ij}^{-1} = e_i$ и $a_{ij}^{-1}a_{ij} = e_j$. Мы назовем элемент a_{ij}^{-1} *обратным* элементу a_{ij}.

6. Для любой пары единиц e_i и e_j найдется элемент a_{ij}, для которого e_i будет левой, а e_j — правой единицей [1].

Пример. Пусть G_0 будет произвольной группой и G — совокупностью матриц порядка n (где n — конечное число или бесконечность), один из элементов которых лежит в группе G_0, а остальные являются нулями. Обозначим матрицу, в которой элемент a из G_0 стоит в i-й строке и j-м столбце, через a_{ij} и положим $a_{ij}b_{jk} = (ab)_{ik}$. Легко проверить, что G является группоидом. Единицами группоида G будут элементы $e_i = 1_{ii}$, и обратным элементу a будет элемент $(a^{-1})_{ji}$.

Нетрудно видеть, что в произвольном группоиде G элемент a^{-1}, обратный элементу a, определен однозначно. Отметим также, что $(a^{-1})^{-1} = a$ и что, если ab определено, то и $b^{-1}a^{-1}$ определено, причем $(ab)^{-1} = b^{-1}a^{-1}$.

[1] Следует отметить, что к любому группоиду G можно присоединить элемент 0, определив $0a = 0 = a0$ и $ab = 0$, если ab не определено в G. Расширенная система будет специальным типом полугруппы, называемой вполне простой (см A. H. Clifford [3]). Для нужных нам приложений данное в тексте определение представляется более удобным.

Если ab определено и e является левой единицей элемента a, то e будет левой единицей элемента ab. В самом деле, $e(ab) = (ea)\,b = ab$.

Обозначим через $G(e)$ совокупность элементов из G, для которых e является левой и правой единицей. Легко проверить, что $G(e)$ будет группой относительно умножения, определенного в G. Если e и e' являются единицами и c — элементом, для которого они будут соответственно левой единицей и правой единицей, то отображение $x \to c^{-1}xc$ будет изоморфным отображением $G(e)$ на $G(e')$. Если группа $G(e)$ коммутативна, то этот изоморфизм не зависит от выбора элемента c. В самом деле, если d будет другим элементом с левой единицей e и правой единицей e', то cd^{-1} лежит в $G(e)$. Следовательно, $(cd^{-1})\,x = x\,(cd^{-1})$ при любом элементе x из $G(e)$, и потому $c^{-1}xc = d^{-1}xd$. В этом случае мы назовем элементы x из $G(e)$ и $x' = c^{-1}xc$ из $G(e')$ *сопряженными*.

Рассмотрим теперь совокупность G нормальных идеалов. Пусть $\mathfrak{a}$ и $\mathfrak{b}$ лежат в G и пусть $\mathfrak{o}'$ будет левым порядком идеала $\mathfrak{a}$, а $\mathfrak{o}$ — правым порядком идеала $\mathfrak{b}$. Тогда найдутся такие регулярные элементы a и b, что $\mathfrak{a} \subseteq \mathfrak{o}'a$ и $\mathfrak{b} \subseteq b\mathfrak{o}$. Следовательно, $\mathfrak{ab} \subseteq \mathfrak{o}'ab\mathfrak{o}$, и так как по теореме 5 существует такой регулярный элемент c, что $\mathfrak{o}' \subseteq \mathfrak{o}c$, то $\mathfrak{ab} \subseteq \mathfrak{o}cab\mathfrak{o}$. Мы видели, что $\mathfrak{o}cab\mathfrak{o}$ является двусторонним $\mathfrak{o}$-идеалом, и потому существует такой регулярный элемент d, что $d\mathfrak{o} \supseteq \mathfrak{o}cab\mathfrak{o} \supseteq \mathfrak{ab}$. Этим показано, что $\mathfrak{ab}$ является правым $\mathfrak{o}$-идеалом. Подобным же образом доказывается, что $\mathfrak{ab}$ левый $\mathfrak{o}'$-идеал. Так как порядки $\mathfrak{o}$ и $\mathfrak{o}'$ максимальны, то они будут порядками для $\mathfrak{ab}$, и, следовательно, $\mathfrak{ab}$ нормальный идеал.

Назовем произведение $\mathfrak{ab}$ нормальных идеалов $\mathfrak{a}$ и $\mathfrak{b}$ *собственным*, если для любых двух таких идеалов $\mathfrak{a}'$ и $\mathfrak{b}'$, что $\mathfrak{a}' \supseteq \mathfrak{a}$, $\mathfrak{b}' \supseteq \mathfrak{b}$ и либо $\mathfrak{a}' \supset \mathfrak{a}$, либо $\mathfrak{b}' \supset \mathfrak{b}$, имеет место строгое включение $\mathfrak{a}'\mathfrak{b}' \supset \mathfrak{ab}$. Мы хотим показать, что множество G нормальных идеалов образует группоид относительно собственного умножения. Условие 1 выполнено для любого нормального идеала $\mathfrak{a}_{ij}$ и его левого и правого порядков $\mathfrak{o}_i$ и $\mathfrak{o}_j$. Выполнение условия 2 очевидно. Выполнение условия 3 показывает следующая

Лемма. *Произведение* $\mathfrak{ab}$ *двух нормальных идеалов* $\mathfrak{a}$ *и* $\mathfrak{b}$ *будет собственным тогда и только тогда, когда правый порядок идеала* $\mathfrak{a}$ *совпадает с левым порядком идеала* $\mathfrak{b}$.

Пусть $\mathfrak{o}$ будет правым порядком идеала $\mathfrak{a}$ и $\mathfrak{o}'$ — левым порядком идеала $\mathfrak{b}$. Если $\mathfrak{o}' \neq \mathfrak{o}$, то $\mathfrak{ao}'$ — нормальный идеал, причем $\mathfrak{a} \subset \mathfrak{ao}'$. Так как $(\mathfrak{ao}')\,\mathfrak{b} = \mathfrak{a}\,(\mathfrak{o}'\mathfrak{b}) = \mathfrak{ab}$, то $\mathfrak{ab}$ не будет собственным произведением. Обратно, предположим, что $\mathfrak{o} = \mathfrak{o}'$, и пусть $\mathfrak{a}'$ будет нормальным идеалом, содержащим $\mathfrak{a}$, причем $\mathfrak{ab} = \mathfrak{a}'\mathfrak{b}$. Тогда $\mathfrak{a}'\mathfrak{bb}^{-1} = \mathfrak{abb}^{-1}$ или $\mathfrak{a}'\mathfrak{o} = \mathfrak{ao} = \mathfrak{a}$. Таким образом, $\mathfrak{a} \supseteq \mathfrak{a}'$, и потому $\mathfrak{a}' = \mathfrak{a}$.

Выполнение условия 4 теперь очевидно.

Для нормального идеала $\mathfrak{a}_{ij}$ положим $\mathfrak{a}_{ji} = \mathfrak{a}_{ij}^{-1}$, и тогда, в силу теоремы 20, выполняется условие 5. Произведение $\mathfrak{o}'\mathfrak{o}$ двух произвольных порядков $\mathfrak{o}$ и $\mathfrak{o}'$ будет нормальным идеалом, для которого $\mathfrak{o}'$ и $\mathfrak{o}$ будут его порядками. Тем самым доказано, что условие 6 выполняется, и, следовательно, справедлива следующая

Теорема 29. *Нормальные идеалы образуют группоид* G *относительно операции собственного умножения. Максимальные порядки будут единицами, а идеал* $\mathfrak{a}^{-1}$ *обратным элементом для* $\mathfrak{a}$ *в группоиде* G.

Докажем далее справедливость следующего усиления условия 6.

Теорема 30. *Если* $\mathfrak{o}$ *и* $\mathfrak{o}'$ *являются максимальными порядками, то* $(\mathfrak{oo}')^{-1}$ *будет целым идеалом с правым порядком* $\mathfrak{o}$ *и левым порядком* $\mathfrak{o}'$. *Идеал* $(\mathfrak{oo}')^{-1}$ *содержит любой целый идеал* $\mathfrak{a}$, *для которого* $\mathfrak{o}$ *является правым порядком и* $\mathfrak{o}'$ *— левым порядком.*

Так как $\mathfrak{oo}'$ — нормальный идеал, то $(\mathfrak{oo}')^{-1}$ будет нормальным идеалом с левым порядком $\mathfrak{o}'$ и правым порядком $\mathfrak{o}$. Так как $\mathfrak{o} \supseteq (\mathfrak{oo}')\,(\mathfrak{oo}')^{-1} \supseteq (\mathfrak{oo}')^{-1}$, то $(\mathfrak{oo}')^{-1}$ — целый идеал. Пусть теперь $\mathfrak{a}$ является любым целым идеалом с правым порядком $\mathfrak{o}$ и левым порядком $\mathfrak{o}'$. Тогда $\mathfrak{oo}'\mathfrak{a} \subseteq \mathfrak{oa} \subseteq \mathfrak{o}$, и потому $\mathfrak{a} \subseteq (\mathfrak{oo}')^{-1}$.

Идеал $(\mathfrak{oo}')^{-1}$ называется *идеалом расстояния от* $\mathfrak{o}$ *до* $\mathfrak{o}'$.

Напомним, что группа $G(\mathfrak{o})$ двусторонних $\mathfrak{o}$-идеалов коммутативна. Следовательно, если $\mathfrak{c}$ является идеалом с левым порядком $\mathfrak{o}$ и правым порядком $\mathfrak{o}'$, то отображение $\mathfrak{a} \to \mathfrak{c}^{-1}\mathfrak{a}\mathfrak{c} = \mathfrak{a}'$ будет изоморфизмом между $G(\mathfrak{o})$ и $G(\mathfrak{o}')$, причем этот изоморфизм не зависит от $\mathfrak{c}$. Как и в случае абстрактного группоида, мы будем называть идеалы $\mathfrak{a}$ и $\mathfrak{a}'$ *сопряженными*. Очевидно, что $\mathfrak{a}$ будем простым идеалом $\mathfrak{p}$ или степенью простого идеала $\mathfrak{p}^e$ тогда и только тогда, когда $\mathfrak{a}' = \mathfrak{p}'$ или $\mathfrak{p}'^e$, где $\mathfrak{p}'$ — простой идеал порядка $\mathfrak{o}'$.

12. Необходимость условий I—IV. Пусть $\mathfrak{A}$ будет кольцом с единицей, в котором всякий регулярный элемент обладает обратным. Пусть далее G будет множеством аддитивных подгрупп $\mathfrak{a}, \mathfrak{b}\ldots$ кольца $\mathfrak{A}$, образующих группоид относительно композиции, совпадающей с обычным умножением аддитивных подгрупп, если оно определено [1]. Мы предполагаем, что выполнены следующие условия:

1. Каждая подгруппа $\mathfrak{a}$ из G содержит регулярный элемент.

2. Каждая единица $\mathfrak{o}$ из G является порядком в $\mathfrak{A}$.

3. Для любой единицы $\mathfrak{o}$ из G каждый правый (левый) целый $\mathfrak{o}$-идеал принадлежит G, причем $\mathfrak{o}$ будет его правой (левой) единицей.

4. Для любой пары единиц $\mathfrak{o}$ и $\mathfrak{o}'$ найдется содержащаяся в $\mathfrak{o} \cap \mathfrak{o}'$ подгруппа $\mathfrak{a}$, для которой $\mathfrak{o}$ будет правой, а $\mathfrak{o}'$ левой единицей.

Отметим, что если подгруппа $\mathfrak{a}$ принадлежит G и $\mathfrak{o}$ является ее правой (левой) единицей, то $\mathfrak{a}$ будет правым (левым) $\mathfrak{o}$-идеалом. В самом деле, $\mathfrak{a}$ является правым $\mathfrak{o}$-модулем, и если a — регулярный элемент из $\mathfrak{a}$, то $\mathfrak{a}$ содержит $a\mathfrak{o}$. Так как $\mathfrak{a}^{-1}\mathfrak{a} = \mathfrak{o}$, то $b^{-1}\mathfrak{a} \subseteq \mathfrak{o}$ для регулярного элемента b^{-1} из $\mathfrak{a}^{-1}$, и потому $\mathfrak{a} \subseteq b\mathfrak{o}$.

Теорема 31 (Асано). *Если выполнены вышеприведенные условия* 1—4, *то единицы группоида G образуют совокупность эквивалентных порядков, удовлетворяющих условиям* I—IV. *Множество единиц группоида G содержит все максимальные порядки, эквивалентные этим порядкам. Группоид G состоит из нормальных идеалов, относящихся к этим порядкам, причем композицией в группоиде является собственное умножение.*

Эквивалентность. Пусть $\mathfrak{o}$ и $\mathfrak{o}'$ являются двумя единицами в G, $\mathfrak{a}$ — идеалом, для которого $\mathfrak{o}$ будет правой, а $\mathfrak{o}'$ — левой единицей. Тогда, если a будет регулярным элементом в $\mathfrak{a}$ и b — регулярным элементом в $\mathfrak{a}^{-1}$, то $\mathfrak{o}' = a\mathfrak{o}a^{-1} \supseteq a\mathfrak{o}b$. Подобно этому $\mathfrak{o} \supseteq c\mathfrak{o}'d$ при соответствующих элементах c и d.

Ограниченность целых идеалов. Если a лежит в $\mathfrak{o}$, то идеал $a\mathfrak{o}$ целый и, следовательно, принадлежит G. Пусть $\mathfrak{o}'$ будет левой единицей для идеала $a\mathfrak{o}$ в G и пусть $\mathfrak{a}$ является содержащимся в $\mathfrak{o} \cap \mathfrak{o}'$ идеалом, для которого $\mathfrak{o}$ будет левой, а $\mathfrak{o}'$ — правой единицей. Тогда $a\mathfrak{o} = \mathfrak{o}'(a\mathfrak{o}) \supseteq \mathfrak{a}(a\mathfrak{o})$, причем $\mathfrak{a}(a\mathfrak{o})$ будет двусторонним принадлежащим G $\mathfrak{o}$-идеалом.

Максимальность. Предположим, что $\mathfrak{o}$ является единицей в G, и пусть порядок $\mathfrak{o}^*$ эквивалентен порядку $\mathfrak{o}$ и содержит его. Тогда существуют такие элементы a и b, что $\mathfrak{o}^* \subseteq a\mathfrak{o}b$. Если $b = dc^{-1}$, где d и c лежат в $\mathfrak{o}$, то $\mathfrak{o}^* \subseteq a\mathfrak{o}c^{-1}$. Мы видели, что $\mathfrak{o}c$ содержит некоторый целый правый идеал $g\mathfrak{o}$, и потому $g^{-1}\mathfrak{o}c \supseteq \mathfrak{o}$ и $g^{-1}\mathfrak{o} \supseteq \mathfrak{o}c^{-1}$. Следовательно, $\mathfrak{o}^* \subseteq a\mathfrak{o}c^{-1} \subseteq ag^{-1}\mathfrak{o}$. Таким образом, если $h^{-1} = ag^{-1}$, то $h\mathfrak{o}^*$ содержится в $\mathfrak{o}$ и потому является целым правым $\mathfrak{o}$-идеалом. В силу условия 3, $h\mathfrak{o}^*$ принадлежит G, и $\mathfrak{o}$ является его правой единицей. Если $\mathfrak{a}$ обозначает элемент группоида G, обратный элементу $h\mathfrak{o}^*$, то $\mathfrak{a}h\mathfrak{o}^* = \mathfrak{o}$. Так как $(\mathfrak{o}^*)^2 = \mathfrak{o}^*$, то отсюда следует, что $\mathfrak{o}\mathfrak{o}^* = \mathfrak{o}$ и $\mathfrak{o}^* \subseteq \mathfrak{o}$. Следовательно, $\mathfrak{o}^* = \mathfrak{o}$.

Условие обрыва возрастающих цепей. Пусть $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots$ является возрастающей последовательностью целых правых $\mathfrak{o}$-идеалов. Объединение $\mathfrak{a}$ идеалов $\mathfrak{a}_i$ будет целым правым $\mathfrak{o}$-идеалом и, следовательно, принадлежит G. Мы имеем тогда $\mathfrak{a}_1\mathfrak{a}^{-1} \subseteq \mathfrak{a}_2\mathfrak{a}^{-1} \subseteq \ldots \subseteq \mathfrak{a}\mathfrak{a}^{-1} = \mathfrak{o}'$, где $\mathfrak{o}'$ — левая единица идеала $\mathfrak{a}$. $\mathfrak{o}'$ будет объединением идеалов $\mathfrak{a}_i\mathfrak{a}^{-1}$. Так как 1 лежит в $\mathfrak{o}'$, то она лежит в одном из идеалов $\mathfrak{a}_i\mathfrak{a}^{-1}$, например, в $\mathfrak{a}_m\mathfrak{a}^{-1}$. Тогда $\mathfrak{o}' = \mathfrak{a}_m\mathfrak{a}^{-1} =$

[1] Напомним, что произведением $\mathfrak{a}\mathfrak{b}$ двух аддитивных подгрупп $\mathfrak{a}$ и $\mathfrak{b}$ будет наименьшая аддитивная подгруппа, содержащая все элементы ab, где $a \in \mathfrak{a}$ и $b \in \mathfrak{b}$.

$= \mathfrak{a}_{m+1}\mathfrak{a}^{-1} = \ldots$ Умножая на $\mathfrak{a}$, получаем, что $\mathfrak{a}_m = \mathfrak{a}_{m+1} = \ldots$

Ослабленное условие обрыва убывающих цепей. Пусть $\mathfrak{b}_1 \supseteq \mathfrak{b}_2 \supseteq \ldots$ будет убывающей цепью целых правых $\mathfrak{o}$-идеалов, каждый из которых содержит двусторонний $\mathfrak{o}$-идеал $\mathfrak{a}$. Идеалы $\mathfrak{b}_i$ и $\mathfrak{a}$ принадлежат группоиду G, и мы имеем соотношение $\mathfrak{o} \supseteq \mathfrak{b}_1^{-1}\mathfrak{b}_2$. Следовательно, $\mathfrak{b}_2^{-1} = \mathfrak{o}\mathfrak{b}_2^{-1} \supseteq \mathfrak{b}_1^{-1}\mathfrak{o}' \supseteq \mathfrak{b}_1^{-1}$, где через $\mathfrak{o}'$ обозначена левая единица для $\mathfrak{b}_2$. Таким образом, $\mathfrak{b}_1^{-1} \subseteq \mathfrak{b}_2^{-1} \subseteq \ldots \subseteq \mathfrak{a}^{-1}$ и $\mathfrak{a}\mathfrak{b}_1^{-1} \subseteq \mathfrak{a}\mathfrak{b}_2^{-1} \subseteq \ldots$ будет возрастающей цепью целых левых $\mathfrak{o}$-идеалов. Отсюда следует, что при некотором индексе m $\mathfrak{a}\mathfrak{b}_m^{-1} = \mathfrak{a}\mathfrak{b}_{m+1}^{-1} = \ldots$, а тогда $\mathfrak{b}_m^{-1} = \mathfrak{b}_{m+1}^{-1} = \ldots$ и $\mathfrak{b}_m = \mathfrak{b}_{m+1} = \ldots$. Так как любой целый $\mathfrak{o}$-идеал ограничен и порядок $\mathfrak{o}$ максимален, то любой $\mathfrak{o}$-идеал ограничен. Следовательно, каждая единица $\mathfrak{o}$ удовлетворяет условиям I—IV. Любой элемент $\mathfrak{a}$ группоида G будет идеалом относительно своих единиц, а так как эти единицы максимальны, то они будут порядками идеала $\mathfrak{a}$. Отсюда следует, что элемент, обратный $\mathfrak{a}$ в группоиде G, будет обычным обратным идеалу $\mathfrak{a}$ идеалом. Следовательно, операция в группоиде G совпадает с ранее определенной. Остается показать, что каждый максимальный порядок $\mathfrak{o}'$, эквивалентный какому-либо порядку $\mathfrak{o}$ из G, принадлежит G и каждый нормальный идеал, порядки которого принадлежат G, сам принадлежит G. Пусть порядок $\mathfrak{o}'$ максимален и $\mathfrak{o}' \subseteq a\mathfrak{o}b$. Тогда $\mathfrak{o}\mathfrak{o}' \subseteq \mathfrak{o}a\mathfrak{o}b \subseteq \mathfrak{o}c$ при соответствующем элементе c, и потому $\mathfrak{o}\mathfrak{o}'$ будет левым $\mathfrak{o}$-идеалом. Его порядками будут, очевидно, максимальные порядки $\mathfrak{o}$ и $\mathfrak{o}'$. Так как обратный идеал $(\mathfrak{o}\mathfrak{o}')^{-1}$ состоит из таких элементов x, что $(\mathfrak{o}\mathfrak{o}')x \subseteq \mathfrak{o}$, то $(\mathfrak{o}\mathfrak{o}')^{-1}$ лежит в $\mathfrak{o}$. Отсюда следует, что $(\mathfrak{o}\mathfrak{o}')^{-1}$ принадлежит G, и так как его левая единица в группоиде G является его левым порядком, то $\mathfrak{o}' \in G$. Наконец, пусть $\mathfrak{b}$ будет любым правым $\mathfrak{o}$-идеалом ($\mathfrak{o}$ принадлежит G), а $\mathfrak{a}$ — содержащимся в $\mathfrak{b}$ двусторонним $\mathfrak{o}$-идеалом. Так как $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2$, где $\mathfrak{a}_1$ и $\mathfrak{a}_2$ являются целыми двусторонними $\mathfrak{o}$-идеалами, то $\mathfrak{a}$ принадлежит G. Тогда $\mathfrak{c} = \mathfrak{b}^{-1}\mathfrak{a}$ содержится в $\mathfrak{o}$ и, следовательно,

принадлежит G. Следовательно, $\mathfrak{b}^{-1} = \mathfrak{c}\mathfrak{a}^{-1} \in G$ и $\mathfrak{b} = (\mathfrak{b}^{-1})^{-1} \in G$.

Пример. Пусть $\mathfrak{o}$ является областью главных идеалов и $\mathfrak{A}$ — ее кольцом отношений. Рассмотрим множество G аддитивных подгрупп вида $a\mathfrak{o}b$, где элементы a и b отличны от нуля. Если x является таким элементом из $\mathfrak{A}$, что $(a\mathfrak{o}b)x = a\mathfrak{o}b$, то $(\mathfrak{o}b)x \subseteq \mathfrak{o}b$ и $bx = yb$, где $y \in \mathfrak{o}$. Следовательно, $x \in b^{-1}\mathfrak{o}b$, и, обратно, если x будет любым элементом из $b^{-1}\mathfrak{o}b$, то $(a\mathfrak{o}b)x \subseteq a\mathfrak{o}b$. Отсюда следует, что, если $a\mathfrak{o}b = a'\mathfrak{o}b'$, то $b^{-1}\mathfrak{o}b = (b')^{-1}\mathfrak{o}b'$. Следовательно, „правая единица“ $b^{-1}\mathfrak{o}b$ элемента $a\mathfrak{o}b$ однозначно определена в группоиде G. Подобным же образом „левая единица“ $a\mathfrak{o}a^{-1}$ элемента $\mathfrak{a} = a\mathfrak{o}b$ не зависит от выбора a в представлении идеала $\mathfrak{a}$. Мы будем рассматривать лишь такие произведения $(a\mathfrak{o}b)(c\mathfrak{o}d)$, для которых правый порядок $b^{-1}\mathfrak{o}b$ элемента $a\mathfrak{o}b$ совпадает с левым порядком $c\mathfrak{o}c^{-1}$ элемента $c\mathfrak{o}d$. Тогда $tc\mathfrak{o} = \mathfrak{o}bc$, и $(a\mathfrak{o}b)(c\mathfrak{o}d) = abc\mathfrak{o}d$ лежит в G. Множество $b^{-1}\mathfrak{o}a^{-1}$ может быть охарактеризовано как совокупность таких элементов x, что $(a\mathfrak{o}b)x$ лежит в левом порядке $a\mathfrak{o}a^{-1}$. Следовательно, если мы определим $(a\mathfrak{o}b)^{-1}$ как $b^{-1}\mathfrak{o}a^{-1}$, то $(a\mathfrak{o}b)^{-1}$ однозначно определяется элементом $a\mathfrak{o}b$ и удовлетворяет равенствам $(a\mathfrak{o}b)(a\mathfrak{o}b)^{-1} = a\mathfrak{o}a^{-1}$, $(a\mathfrak{o}b)^{-1}(a\mathfrak{o}b) = b^{-1}\mathfrak{o}b$. Каждый правый или левый $a^{-1}\mathfrak{o}a$-идеал (как целый, так и дробный) будет главным идеалом и, следовательно, лежит в G. Наконец, для любой пары единиц $a^{-1}\mathfrak{o}a$ и $b^{-1}\mathfrak{o}b$ множества G найдется элемент $b^{-1}\mathfrak{o}a$, для которого они будут соответственно правой и левой единицами. Таким образом, G является группоидом, удовлетворяющим условиям 1, 2 и 3. Покажем теперь, что если каждый целый $\mathfrak{o}$-идеал ограничен, то и условие 4 выполняется. В этом случае, если $a = bc^{-1}$, где b и c лежат в $\mathfrak{o}$, будет любым элементом из $\mathfrak{A}$, то в $\mathfrak{o}$ найдется такой элемент c^*, что $c^*\mathfrak{o} = \mathfrak{o}c^*$ и $c^{-1}c^*$ лежит в $\mathfrak{o}$. Это очевидно, так как $c\mathfrak{o}$ содержит двусторонний $\mathfrak{o}$-идеал $c^*\mathfrak{o} = \mathfrak{o}c^*$, и потому $c^* = cc'$, где $c' \in \mathfrak{o}$ и $c^{-1}c^* = c'$. Отсюда следует, что $a\mathfrak{o}c^* = ac^*\mathfrak{o}$ будет целым идеалом с левым порядком $a\mathfrak{o}a^{-1}$ и правым порядком $\mathfrak{o}$. Так как порядок $b^{-1}\mathfrak{o}b$ изоморфен порядку $\mathfrak{o}$, то в нем выполнены те же условия, что и в $\mathfrak{o}$,

и потому подобными же рассуждениями мы можем показать, что для любой пары порядков $a^{-1}\mathfrak{o}a$ и $b^{-1}\mathfrak{o}b$ найдется $a^{-1}\mathfrak{o}a$-левый, $b^{-1}\mathfrak{o}b$-правый идеал, содержащийся в их пересечении. Это показывает, что наши рассуждения непосредственно применимы к областям главных идеалов, в которых каждый целый идеал ограничен.

13. Разложение нормальных идеалов. Рассмотрим теперь вопрос о разложении целых элементов группоида G. Будем обозначать через $\mathfrak{a}_{ij}, \mathfrak{b}_{ij}, \ldots$ нормальные идеалы, для которых максимальные порядки $\mathfrak{o}_i$ и $\mathfrak{o}_j$ из G являются соответственно левым и правым порядками. Следующая лемма будет основной в дальнейших рассмотрениях.

Лемма. *Для того чтобы* $\mathfrak{b}_{kj} \supseteq \mathfrak{a}_{ij}$ ($\mathfrak{b}_{jk} \supseteq \mathfrak{a}_{ji}$), *необходимо и достаточно, чтобы* $\mathfrak{a}_{ij} = \mathfrak{c}_{ik}\mathfrak{b}_{kj}$ ($\mathfrak{a}_{ji} = \mathfrak{b}_{jk}\mathfrak{c}_{ki}$), *где идеал* $\mathfrak{c}_{ik}$ ($\mathfrak{c}_{ki}$) *целый. Равенство имеет место тогда и только тогда, когда* $\mathfrak{c}_{ik} = \mathfrak{o}_i$ ($\mathfrak{c}_{ki} = \mathfrak{o}_k$).

Если $\mathfrak{a}_{ij} = \mathfrak{c}_{ik}\mathfrak{b}_{kj}$, где $\mathfrak{c}_{ik} \subseteq \mathfrak{o}_k$, то $\mathfrak{a}_{ij} \subseteq \mathfrak{b}_{kj}$. В силу предыдущей леммы, $\mathfrak{a}_{ij} = \mathfrak{b}_{ki}$ лишь в том случае, когда $k = i$ и $\mathfrak{c}_{ik} = \mathfrak{o}_i$. Обратно, если $\mathfrak{b}_{kj} \supseteq \mathfrak{a}_{ij}$, то $\mathfrak{a}_{ij} = \mathfrak{a}_{ij}\mathfrak{b}_{kj}^{-1}\mathfrak{b}_{kj} = \mathfrak{c}_{ik}\mathfrak{b}_{kj}$, где $\mathfrak{c}_{ik} = \mathfrak{a}_{ij}\mathfrak{b}_{kj}^{-1}$. Тогда $\mathfrak{c}_{ik} \subseteq \mathfrak{a}_{ij}\mathfrak{a}_{kj}^{-1} = \mathfrak{o}_i$, и потому идеал $\mathfrak{c}_{ik}$ **целый** [1].

Предположим, что $\mathfrak{a}_{ij}$ — целый идеал и $\mathfrak{a}_{ij} \subset \mathfrak{a}_j$. Пусть последовательность $\mathfrak{o}_j \supset \mathfrak{a}_{i_1 j} \supset \mathfrak{a}_{i_2 j} \supset \ldots \supset \mathfrak{a}_{i_m j} = \mathfrak{a}_{ij}$ состоит из целых правых $\mathfrak{o}_j$-идеалов, соответствующих членам композиционного ряда модуля $\mathfrak{o}_j/\mathfrak{a}_{ij}$. Композиционные факторы этого ряда будут тогда $\mathfrak{o}_j$-изоморфны модулям $\mathfrak{a}_{i_{k-1}j}/\mathfrak{a}_{i_k j}$. По лемме мы получаем, что $\mathfrak{a}_{i_k j} = \mathfrak{p}_{i_k i_{k-1}}\mathfrak{a}_{i_{k-1}j}$, и, следовательно, $\mathfrak{a}_{ij} = \mathfrak{p}_{i i_{m-1}}\mathfrak{p}_{i_{m-1} i_{m-2}} \ldots \mathfrak{p}_{i_1 j}$ ($\mathfrak{p}_{i_1 j} = \mathfrak{a}_{i_1 j}$). Целые идеалы $\mathfrak{p}_{i_k i_{k-1}}$ будут максимальными в своих порядках. В противном случае, мы имели бы $\mathfrak{p}_{i_k i_{k-1}} = \mathfrak{r}_{i_k l}\mathfrak{s}_{l i_{k-1}}$, где $\mathfrak{r}_{i_k l}$ — целый идеал, отличный от $\mathfrak{o}_{i_k}$ и $\mathfrak{s}_{l i_{k-1}}$ — целый идеал, отличный от $\mathfrak{o}_{i_{k-1}}$. Тогда мы

[1] Вообще, если $\mathfrak{b}_{kl} \supseteq \mathfrak{a}_{ij}$, то мы имеем $\mathfrak{a}_{ij} = \mathfrak{c}_{ik}\mathfrak{b}_{kl}\mathfrak{b}_{lj}$, где идеалы $\mathfrak{c}_{ik} = \mathfrak{a}_{ij}(\mathfrak{o}_k\mathfrak{a}_{ij})^{-1}$ и $\mathfrak{b}_{lj} = \mathfrak{b}_{kl}^{-1}\mathfrak{a}_{ij}$ целые.

получили бы, что $\mathfrak{a}_{i_{k-1}j} \supset \mathfrak{s}_{l i_{k-1}}\mathfrak{a}_{i_{k-1}j} \supset \mathfrak{a}_{i_k j}$, вопреки предположению о неприводимости модуля $\mathfrak{a}_{i_{k-1}j}/\mathfrak{a}_{i_k j}$. Отсюда следует, что граница идеала $\mathfrak{p}_{i_k i_{k-1}}$ в $\mathfrak{o}_{i_{k-1}}$, а также его левая граница в $\mathfrak{o}_{i_k}$, являются простыми идеалами. Очевидно также, что мы можем обратить порядок вышеприведенных рассуждений: Если $\mathfrak{a}_{ij} = \mathfrak{p}_{i i_{m-1}}\mathfrak{p}_{i_{m-1} i_{m-2}} \ldots \mathfrak{p}_{i_1 j}$ является разложением идеала $\mathfrak{a}_{ij}$ в произведение максимальных целых идеалов $\mathfrak{p}_{i_k i_{k-1}}$, то цепь $\mathfrak{o}_j \supset \mathfrak{p}_{i_1 j} \supset \mathfrak{p}_{i_2 i_1}\mathfrak{p}_{i_1 j} \supset \ldots \supset \mathfrak{a}_{ij}$ соответствует композиционному ряду модуля $\mathfrak{o}_j/\mathfrak{a}_{ij}$.

Для того чтобы изучить связь между различными разложениями идеала $\mathfrak{a}_{ij}$, нам понадобится одно обобщение понятия изоморфизма, применимое к модулям относительно различных порядков кольца $\mathfrak{A}$. Пусть $\mathfrak{M}_j$ и $\mathfrak{M}_k$ будут соответственно $\mathfrak{o}_j$- и $\mathfrak{o}_k$-модулями, каждый из которых имеет конечное число образующих и ограничен. Мы будем говорить, что модули $\mathfrak{M}_j$ и $\mathfrak{M}_k$ *сопряжены*, если инварианты этих модулей можно таким образом поставить в соответствие друг с другом, чтобы соответствующие инварианты были сопряжены. Если $j = k$, то, в силу доказанного в § 8, сопряженность эквивалентна обычному изоморфизму.

Теорема 32. *Если* $\mathfrak{c}_{ij}$ — *целый, а* $\mathfrak{b}_{jk}$ — *любой идеал, то модули* $\mathfrak{M}_j = \mathfrak{o}_j/\mathfrak{c}_{ij}$ *и* $\mathfrak{M}_k = \mathfrak{b}_{jk}/\mathfrak{c}_{ij}\mathfrak{b}_{jk}$ *сопряжены.*

Заметим сначала, что эти модули структурно изоморфны. В самом деле, любой подмодуль модуля $\mathfrak{M}_j$ соответствует такому идеалу $\mathfrak{d}_{lj}$, что $\mathfrak{o}_j \supseteq \mathfrak{d}_{lj} \supseteq \mathfrak{c}_{ij}$. Тогда $\mathfrak{b}_{jk} \supseteq \mathfrak{d}_{lj}\mathfrak{b}_{jk} \supseteq \mathfrak{c}_{ij}\mathfrak{b}_{jk}$, и, умножая на $\mathfrak{b}^{-1}{}_{jk}$, мы получаем, что равенство может иметь место во второй совокупности соотношений лишь тогда, когда оно имеет место в первой. Кроме того, любой подмодуль модуля $\mathfrak{M}_k$ имеет вид $\mathfrak{u}_{lk}/\mathfrak{c}_{ij}\mathfrak{b}_{jk}$, где $\mathfrak{u}_{lk}$ является содержащимся в $\mathfrak{b}_{jk}$ $\mathfrak{o}_k$-модулем. Но тогда $\mathfrak{u}_{lk}$ будет правым $\mathfrak{o}_k$-идеалом, и потому $\mathfrak{u}_{lk}$ будет нормальным идеалом. Следовательно, по лемме, $\mathfrak{u}_{lk} = \mathfrak{d}_{lj}\mathfrak{b}_{jk}$, где $\mathfrak{d}_{lj}$ — целый идеал. Таким образом, наше соответствие между подмодулями модулей $\mathfrak{M}_j$ и $\mathfrak{M}_k$ взаимно-однозначно, а так как оно сохраняет порядок, то оно бу-

дет структурным изоморфизмом. Если c_{jj} является границей $\mathfrak{M}_j$, то легко видеть, что границей $\mathfrak{M}_k$ будет сопряженный идеал $c_{kk} = b_{jk}^{-1} c_{jj} b_{jk}$. Следовательно, если мы представим c_{ij} как прямое пересечение таких o_j-правых идеалов $c_{i_1 j}, \ldots, c_{i_s j}$, что модули $o_j/c_{i_k j}$ неразложимы, то границы модулей $o_j/c_{i_r j}$ будут сопряжены с границами модулей $b_{jk}/c_{i_r j} b_{jk}$. Напомним, что границы модулей $o_j/c_{i_r j}$ являются инвариантами модуля $\mathfrak{M}_j$. С другой стороны, в силу структурного изоморфизма, нуль модуля $\mathfrak{M}_k$ будет прямым пересечением модулей $\mathfrak{M}_k^{(r)} = c_{i_r j} b_{jk}/c_{ij} b_{jk}$, причем фактор-модули $\mathfrak{M}_k/\mathfrak{M}_k^{(r)}$ неразложимы. Так как модуль $\mathfrak{M}_k/\mathfrak{M}_k^{(r)}$ изоморфен модулю $b_{jk}/c_{i_r j} b_{jk}$, то его граница сопряжена с границей модуля $o_j/c_{i_r j}$, и потому инварианты модуля $\mathfrak{M}_j$ сопряжены с инвариантами модуля $\mathfrak{M}_k$.

Разумеется, такое же рассуждение может быть проведено для левых модулей. Назовем теперь целые идеалы b_{ij} и c_{kl} *подобными справа* (*подобными слева*), если модуль o_j/b_{ij} (левый модуль o_i/b_{ij}) сопряжен с модулем o_l/c_{kl} (левым модулем o_k/c_{kl}). В следующем параграфе мы покажем, что два идеала подобны справа тогда и только тогда, когда они подобны слева. Мы можем поэтому опускать определения «правый» и «левый» в этих терминах. Сформулируем теперь основную теорему о разложениях.

Теорема 33. *Любой целый идеал a_{ij} может быть разложен в произведение $\mathfrak{p}_{i i_{m-1}} \mathfrak{p}_{i_{m-1} i_{m-2}} \ldots \mathfrak{p}_{i_1 j}$ максимальных целых идеалов. Если $a_{ij} = \mathfrak{p}'_{i k_{n-1}} \mathfrak{p}'_{k_{n-1} k_{n-2}} \ldots \mathfrak{p}'_{k_1 j}$ является другим разложением такого типа, то число сомножителей в обоих произведениях равно, и они могут быть поставлены в соответствие друг другу таким образом, что соответствующие сомножители подобны.*

Мы видели, что разложение $\mathfrak{p}_{i i_{m-1}} \ldots \mathfrak{p}_{i_1 j}$ идеала a_{ij} соответствует композиционному ряду модуля o_j/a_{ij}, причем композиционные факторы этого ряда изоморфны модулям $a_{i_{k-1} j} / \mathfrak{p}_{i_k i_{k-1}} a_{i_{k-1} j}$. По предыдущей теореме, эти модули сопряжены с модулями $o_{i_{k-1}}/\mathfrak{p}_{i_k i_{k-1}}$. Наша теорема является поэтому непосредственным следствием теоремы Жордана-Гельдера.

Теорема 34. *Для того чтобы модуль o_j/q_{ij} был неразложим, необходимо и достаточно, чтобы идеал q_{ij} единственным образом разлагался в произведение максимальных целых идеалов. Если это условие выполнено, то все максимальные множители идеала q_{ij} подобны между собой.*

Необходимость условия непосредственно вытекает из теоремы 27. Для того чтобы доказать достаточность, предположим, что $q_{ij} = [q_{i_1 j}, q_{i_2 j}]$ и $(q_{i_1 j}, q_{i_2 j}) = o_j$. Тогда $q_{ij} = r_{i i_1} q_{i_1 j} = r_{i i_2} q_{i_2 j}$, где $r_{i i_k}$ являются целыми идеалами. Следовательно, если $q_{i_1 j} \neq q_{ij}$ и $q_{i_2 j} \neq q_{ij}$, то мы получим два различных разложения идеала q_{ij}.

Отсюда вытекают очевидные следствия.

Следствие 1. *Если модуль o_j/q_{ij} неразложим и идеал q_{kl} является делителем q_{ij}, то модуль o_l/q_{kl} неразложим.*

Следствие 2. *Модуль o_j/q_{ij} неразложим тогда и только тогда, когда неразложим левый модуль o_i/q_{ij}.*

Напомним, что если модуль o_i/q_{ij} неразложим, то его (правая) граница имеет вид $\mathfrak{p}_{jj}^e$, где идеал $\mathfrak{p}_{jj}$ простой, и e равно длине композиционного ряда модуля o_i/q_{ij}. Очевидно, что e может быть охарактеризовано как число максимальных множителей в разложении идеала q_{ij}. Отсюда и из соответствующего результата относительно левых модулей вытекает

Следствие 3. *Если модуль o_j/q_{ij} неразложим и границей идеала q_{ij} является $\mathfrak{p}_{jj}^e$, где $\mathfrak{p}_{jj}$ — простой идеал, то левая граница идеала q_{ij} имеет вид $\mathfrak{p}_{ii}^e$, где $\mathfrak{p}_{ii}$ — также простой идеал.*

Если $\mathfrak{p}_{jj}$ является простым идеалом, то $o_j/\mathfrak{p}_{jj}$ будет простым кольцом, и, следовательно, все композиционные факторы модуля $o_j/\mathfrak{p}_{jj}$ изоморфны между собой. Отсюда вытекает следующая

Теорема 35. *Все максимальные множители простого идеала* $\mathfrak{p}_{jj}$ *подобны между собой.*

Покажем, наконец, что порядок классов подобия максимальных идеалов, появляющихся при разложении любого целого идеала, может быть выбран произвольно, т. е. если $\mathfrak{a}_{ij} = \mathfrak{p}_{ii_{m-1}}\mathfrak{p}_{i_{m-1}i_{m-2}}\cdots\mathfrak{p}_{i_1 j}$, где $\mathfrak{p}$ — максимальные идеалы, и если $\mathfrak{p}_{i_k i_{k-1}}$ принадлежит к классу подобия C_k, то найдется такое разложение $\mathfrak{a}_{ij} = \mathfrak{p}'_{ik_{m-1}}\cdots$ $\cdots\mathfrak{p}'_{k_1 j}$, что соответствующие классы подобия $C'_1, \ldots, C'_m$ образуют любую перестановку классов $C_1, \ldots, C_m$. Очевидно, что для доказательства этого достаточно показать справедливость следующей теоремы:

Теорема 36. *Если* $\mathfrak{p}_{ij}$ *и* $\mathfrak{p}_{jk}$ *являются максимальными целыми идеалами, то* $\mathfrak{p}_{ij}\mathfrak{p}_{jk} = \mathfrak{p}'_{il}\mathfrak{p}'_{lk}$, *где идеалы* $\mathfrak{p}_{ij}$ *и* $\mathfrak{p}'_{lk}$, *а также и идеалы* $\mathfrak{p}_{jk}$ *и* $\mathfrak{p}'_{il}$ *подобны между собой.*

Если модуль $\mathfrak{o}_k/\mathfrak{p}_{ij}\mathfrak{p}_{jk}$ неразложим, то идеалы $\mathfrak{p}_{ij}$ и $\mathfrak{p}_{jk}$ подобны справа. Следовательно, мы можем положить $\mathfrak{p}'_{il} = \mathfrak{p}_{ij}$ и $\mathfrak{p}'_{lk} = \mathfrak{p}_{jk}$. Если же этот модуль разложим, то мы имеем

$$\mathfrak{p}_{ij}\mathfrak{p}_{jk} = [\mathfrak{p}'_{i_1 k}, \mathfrak{p}'_{i_2 k}], \quad (\mathfrak{p}'_{i_1 k}, \mathfrak{p}'_{i_2 k}) = \mathfrak{o}_k.$$

Тогда мы можем предположить, что идеал $\mathfrak{p}'_{i_1 k}$ подобен идеалу $\mathfrak{p}_{ij}$, а идеал $\mathfrak{p}'_{i_2 k}$ подобен идеалу $\mathfrak{p}_{jk}$. Так как $\mathfrak{p}_{ij}\mathfrak{p}_{jk} = \mathfrak{r}_{ii_1}\mathfrak{p}'_{i_1 k} = \mathfrak{r}_{ii_2}\mathfrak{p}'_{i_2 k}$, то мы можем положить $\mathfrak{p}'_{lk} = \mathfrak{p}'_{i_1 k}$ и $\mathfrak{p}'_{il} = \mathfrak{r}_{ii_1}$.

14. Подобие нормальных идеалов. Граница $\mathfrak{a}_{jj}$ любого целого идеала $\mathfrak{a}_{ij}$ будет $\mathfrak{o}_j$-идеалом вида $\mathfrak{b}_{ji}\mathfrak{a}_{ij}$, где $\mathfrak{b}_{ji}$ — целый идеал, являющийся делителем любого идеала такого вида. Таким же образом можно охарактеризовать левую границу $\mathfrak{a}_{ii}$. Таким образом $\mathfrak{a}_{ii}$ будет делителем идеала $\mathfrak{a}_{ij}\mathfrak{b}_{ji}$, и число максимальных множителей идеала $\mathfrak{a}_{ii}$ не должно превосходить числа максимальных множителей идеала $\mathfrak{a}_{ij}\mathfrak{b}_{ji}$, а тем самым и числа максимальных множителей идеала $\mathfrak{a}_{jj}$. По симметрии, число максимальных множителей идеалов $\mathfrak{a}_{ii}$ и $\mathfrak{a}_{jj}$ одинаково, и потому $\mathfrak{a}_{ii} = \mathfrak{a}_{ij}\mathfrak{b}_{ji}$. Тогда идеал $\mathfrak{a}_{ii} = \mathfrak{a}_{ij}\mathfrak{a}_{jj}\mathfrak{a}_{ij}^{-1}$ сопряжен с идеалом $\mathfrak{a}_{jj}$. Мы можем использовать этот факт для доказательства следующей леммы.

Лемма. *Если идеалы* $\mathfrak{a}_{ij}$ *и* $\mathfrak{b}_{kl}$ *подобны справа и модуль* $\mathfrak{o}_j/\mathfrak{a}_{ij}$ *неразложим, то эти идеалы подобны слева.*

Так как $\mathfrak{o}_i/\mathfrak{a}_{ij}$ и $\mathfrak{o}_k/\mathfrak{b}_{kl}$ неразложимы, то достаточно показать, что эти левые модули имеют сопряженные границы, т. е. что левая граница идеала $\mathfrak{a}_{ij}$ сопряжена с левой границей идеала $\mathfrak{b}_{kl}$. По предположению, правые границы идеалов $\mathfrak{a}_{ij}$ и $\mathfrak{b}_{kl}$ сопряжены между собой. Так как обе границы любого идеала сопряжены, то наше утверждение доказано.

Предположим теперь, что левый модуль $\mathfrak{o}_j/\mathfrak{a}_{ij}$ разложим, и пусть $\mathfrak{a}_{ij} = [\mathfrak{a}_{i_1 j}, \mathfrak{a}_{i_2 j}]$, $(\mathfrak{a}_{i_1 j}, \mathfrak{a}_{i_2 j}) = \mathfrak{o}_j$. Тогда $\mathfrak{a}_{ij} = \mathfrak{a}'_{ii_1}\mathfrak{a}_{i_1 j} = \mathfrak{a}'_{ii_2}\mathfrak{a}_{i_2 j}$. Пересечение $\mathfrak{a}_{ik} = [\mathfrak{a}_{ii_1}, \mathfrak{a}_{ii_2}]$ содержит $\mathfrak{a}_{ij}$, и потому $\mathfrak{a}_{ij} = \mathfrak{a}_{ik}\mathfrak{c}_{kj}$. Так как $\mathfrak{c}_{kj} = \mathfrak{a}_{ik}^{-1}\mathfrak{a}_{ij} \supseteq$ $\supseteq \mathfrak{a}'^{-1}_{ii_1}\mathfrak{a}_{ij} = \mathfrak{a}_{i_1 j}$, и подобно этому $\mathfrak{c}_{kj} \supseteq \mathfrak{a}_{i_2 j}$, то мы получаем, что $\mathfrak{c}_{kj} = \mathfrak{o}_j$, т. е. что $\mathfrak{a}_{ij} = [\mathfrak{a}'_{ii_1}, \mathfrak{a}'_{ii_2}]$. Пусть, далее, $(\mathfrak{a}'_{ii_1}, \mathfrak{a}'_{ii_2}) = \mathfrak{c}_{il}$. Тогда $\mathfrak{c}_{il}^{-1}\mathfrak{a}_{ij} \subseteq \mathfrak{a}'^{-1}_{ii_1}\mathfrak{a}_{ij} = \mathfrak{a}_{i_1 j}$ и $\mathfrak{c}_{il}^{-1}\mathfrak{a}_{ij} \subseteq \mathfrak{a}_{i_2 j}$, откуда вытекает, что $\mathfrak{c}_{il} = \mathfrak{o}_i$. Таким образом, $\mathfrak{a}_{ij}$ совпадает с прямым пересечением $\mathfrak{o}_i$-левых идеалов $\mathfrak{a}'_{ii_1}$ и $\mathfrak{a}'_{ii_2}$.

Мы видели, что модули $\mathfrak{a}_{i_2 j}/\mathfrak{a}'_{ii_2}$ и $\mathfrak{a}_{i_2 j}/\mathfrak{a}'_{ii_2}\mathfrak{a}_{i_2 j} = \mathfrak{a}_{i_2 j}/\mathfrak{a}_{ij}$ сопряжены. Так как модуль $\mathfrak{o}_j/\mathfrak{a}_{i_1 j} = (\mathfrak{a}_{i_1 j}, \mathfrak{a}_{i_2 j})/\mathfrak{a}_{i_1 j}$ $\mathfrak{o}_j$-изоморфен модулю $\mathfrak{a}_{i_2 j}/[\mathfrak{a}_{i_1 j}, \mathfrak{a}_{i_2 j}] = \mathfrak{a}_{i_2 j}/\mathfrak{a}_{ij}$, то отсюда следует, что модули $\mathfrak{o}_{i_2}/\mathfrak{a}'_{ii_2}$ и $\mathfrak{o}_j/\mathfrak{a}_{i_1 j}$ сопряжены. Следовательно, идеалы $\mathfrak{a}_{i_1 j}$ и $\mathfrak{a}'_{ii_2} = \mathfrak{a}_{ij}\mathfrak{a}_{i_2 j}^{-1}$ подобны справа и, по симметрии, эти идеалы подобны также и слева. Аналогично доказывается подобие идеалов $\mathfrak{a}_{i_2 j}$ и $\mathfrak{a}'_{ii_1}$.

Рассмотрим теперь общий случай, когда $\mathfrak{a}_{ij} = [\mathfrak{a}_{i_1 j}, \ldots,$ $\ldots, \mathfrak{a}_{i_s j}]$, причем, если обозначить $[\mathfrak{a}_{i_1 j}, \ldots, \mathfrak{a}_{i_{r-1} j}, \mathfrak{a}_{i_{r+1} j}, \ldots,$ $\ldots, \mathfrak{a}_{i_s j}]$ через $\mathfrak{b}_{k_r j}$, то $(\mathfrak{a}_{i_r j}, \mathfrak{b}_{k_r j}) = \mathfrak{o}_j$. Напишем $\mathfrak{a}_{ij} = \mathfrak{a}_{ik_r}\mathfrak{b}_{k_r j} =$ $= \mathfrak{b}'_{ii_r}\mathfrak{a}_{i_r j}$ и покажем, что $\mathfrak{a}_{ij}$ будет прямым пересечением $\mathfrak{o}_i$-левых идеалов $\mathfrak{a}'_{ik_r}$. Это было доказано выше для слу-

чая $s = 2$. Следовательно, мы можем предположить, что утверждение справедливо для разложений, состоящих из $s - 1$ компонент. Нетрудно видеть, что $\mathfrak{b}'_{ii_r} = \mathfrak{a}_{ij}\mathfrak{a}_{i_rj}^{-1} = [\mathfrak{a}_{i_1j}, \ldots, \mathfrak{a}_{i_sj}]\,\mathfrak{a}_{i_rj}^{-1} = [[\mathfrak{a}_{i_1j}, \mathfrak{a}_{i_rj}]\,\mathfrak{a}_{i_rj}^{-1}, \ldots, [\mathfrak{a}_{i_sj}, \mathfrak{a}_{i_rj}]\,\mathfrak{a}_{i_rj}^{-1}]$, и, если мы опустим в последнем выражении член $(\mathfrak{a}_{i_qj} \cap \mathfrak{a}_{i_rj})\,\mathfrak{a}_{i_rj}^{-1}$, $q \neq r$, то получим $\mathfrak{b}_{k_qj}\mathfrak{a}_{i_rj}^{-1}$. Так как, в силу дистрибутивного закона Дедекинда, $(\mathfrak{b}_{k_qj}, [\mathfrak{a}_{i_qj}, \mathfrak{a}_{i_rj}]) = [(\mathfrak{b}_{k_qj}, \mathfrak{a}_{i_qj}), \mathfrak{a}_{i_rj}]$ и $(\mathfrak{b}_{k_qj}, \mathfrak{a}_{i_qj}) = \mathfrak{o}_j$, то мы получаем, что $(\mathfrak{b}_{k_qj}, [\mathfrak{a}_{i_qj}, \mathfrak{a}_{i_rj}]) = \mathfrak{a}_{i_rj}$. Следовательно, $(\mathfrak{b}_{k_qj}\mathfrak{a}_{i_rj}^{-1}, [\mathfrak{a}_{i_qj}, \mathfrak{a}_{i_rj}]\,\mathfrak{a}_{i_rj}^{-1}) = \mathfrak{o}_j$, и потому разложение $\mathfrak{b}'_{ii_r}$ на идеалы $[\mathfrak{a}_{i_qj}, \mathfrak{a}_{i_rj}]\,\mathfrak{a}_{i_rj}^{-1}$, $q \neq r$, будет прямым разложением. Так как $\mathfrak{b}'_{ii_r} = \mathfrak{a}'_{ik_r}(\mathfrak{b}_{k_rj}\mathfrak{a}_{i_rj}^{-1})$, то мы выводим из индуктивного предположения, что $\mathfrak{b}'_{ii_r}$ является прямым пересечением $\mathfrak{o}_i$-левых идеалов $\mathfrak{a}'_{ik_q}$. Так как $\mathfrak{a}_{ij}$ является прямым пересечением идеалов $\mathfrak{a}'_{ik_r}$ и $\mathfrak{b}'_{ii_r}$, то $\mathfrak{a}_{ij}$ будет прямым пересечением всех идеалов $\mathfrak{a}'_{ik_r}$. Сформулируем полученный результат в виде теоремы.

Теорема 37. *Если идеал $\mathfrak{a}_{ij}$ является прямым пересечением правых $\mathfrak{o}_j$-идеалов $\mathfrak{a}_{i_rj}$ и $\mathfrak{b}_{k_rj} = [\mathfrak{a}_{i_1j}, \ldots, \mathfrak{a}_{i_{r-1}j}, \mathfrak{a}_{i_{r+1}j}, \ldots, \mathfrak{a}_{i_sj}]$, то $\mathfrak{a}_{ij}$ будет прямым пересечением $\mathfrak{o}_i$-левых идеалов $\mathfrak{a}_{ij}\mathfrak{b}_{k_rj}^{-1} = \mathfrak{a}'_{ik_r}$.*

Так как $\mathfrak{a}_{ij} = [\mathfrak{a}_{i_rj}, \mathfrak{b}_{k_rj}]$, $(\mathfrak{a}_{i_rj}, \mathfrak{b}_{k_rj}) = \mathfrak{o}_j$, то идеал $\mathfrak{a}_{i_rj}$ подобен идеалу $\mathfrak{a}'_{ik_r} = \mathfrak{a}_{ij}\mathfrak{b}_{k_rj}^{-1}$. Отсюда и из леммы вытекает

Теорема 38. *Если $\mathfrak{a}_{ij} = [\mathfrak{a}_{i_1j}, \ldots, \mathfrak{a}_{i_rj}] = [\mathfrak{a}_{ij_1}, \ldots, \mathfrak{a}_{ij_r}]$ являются прямыми разложениями идеала $\mathfrak{a}_{ij}$ на такие $\mathfrak{o}_j$-правые идеалы и $\mathfrak{o}_j$-левые идеалы, что модули $\mathfrak{o}_j/\mathfrak{a}_{ikj}$ и $\mathfrak{o}_i/\mathfrak{a}_{ijk}$ неразложимы, то делители $\mathfrak{a}_{ikj}$ и $\mathfrak{a}_{ijk}$ могут быть упорядочены таким образом, что соответствующие члены будут подобны справа и слева.*

Очевидно, что отсюда следует

Теорема 39. *Если два идеала подобны справа (слева), то они подобны и слева (справа).*

Докажем, наконец, что два двусторонних идеала сопряжены между собой тогда и только тогда, когда они подобны. Для этой цели нам понадобится

Лемма. *Емкости любых двух сопряженных простых идеалов $\mathfrak{p}_{ii}$ и $\mathfrak{p}_{jj}$ равны.*

Разложим идеал $\mathfrak{p}_{ii}$ следующим образом: $\mathfrak{p}_{ii} = \mathfrak{p}_{ii_{k-1}}\mathfrak{p}_{i_{k-1}i_{k-2}}\ldots\mathfrak{p}_{i_1i}$, где $\mathfrak{p}_{i_ri_{r-1}}$ — максимальные идеалы. Тогда, так как k является длиной композиционного ряда модуля $\mathfrak{o}_i/\mathfrak{p}_{ii}$, то k будет емкостью идеала $\mathfrak{p}_{ii}$. Мы можем считать, что $\mathfrak{p}_{jj} = \mathfrak{q}_{ji}\mathfrak{p}_{ii}\mathfrak{q}_{ji}^{-1}$, где $\mathfrak{q}_{ji}$ является максимальным целым идеалом. Рассмотрим теперь идеал $\mathfrak{p}_{i_1i}\mathfrak{q}_{ji}^{-1}$. Если $\mathfrak{p}_{i_1i} = \mathfrak{q}_{ji}$, то мы имеем, очевидно, $\mathfrak{p}_{i_1i}\mathfrak{q}_{ji}^{-1} = \mathfrak{o}_j = \mathfrak{q}'^{-1}_{j_1j}\mathfrak{p}'_{j_1j}$, где $\mathfrak{p}'_{j_1j} = \mathfrak{q}'_{j_1j}$ — максимальный целый идеал. С другой стороны, если $\mathfrak{p}_{i_1i} \neq \mathfrak{q}'_{j_1j}$, то $(\mathfrak{p}_{i_1i}, \mathfrak{q}_{ji}) = \mathfrak{o}_i$, и потому $[\mathfrak{p}_{i_1i}, \mathfrak{q}_{ji}]$ будет прямым пересечением идеалов $\mathfrak{p}_{i_1i}$ и $\mathfrak{q}_{ji}$. Тогда $[\mathfrak{p}_{i_1i}, \mathfrak{q}_{ji}] = \mathfrak{q}'_{j_1i_1}\mathfrak{p}_{i_1i} = \mathfrak{p}'_{j_1j}\mathfrak{q}_{ji}$, и потому опять $\mathfrak{p}_{i_1i}\mathfrak{q}_{ji}^{-1} = \mathfrak{q}'^{-1}_{j_1i_1}\mathfrak{p}'_{j_1j}$, где $\mathfrak{p}'$ и $\mathfrak{q}'$ — максимальные идеалы. Таким образом, $\mathfrak{p}_{jj} = \mathfrak{q}_{ji}\mathfrak{p}_{ii_{k-1}}\ldots\mathfrak{p}_{i_2i_1}\mathfrak{q}'^{-1}_{j_1i_1}\mathfrak{p}'_{j_1j} = \mathfrak{q}_{ji}\mathfrak{p}_{ii_{k-1}}\ldots\mathfrak{p}_{i_3i_2}\mathfrak{q}'^{-1}_{j_2i_2}\mathfrak{p}'_{j_2j_1}\mathfrak{p}'_{j_1j} = \ldots = \mathfrak{q}_{ji}\mathfrak{q}'^{-1}_{j_ki}\mathfrak{p}'_{j_kj_{k-1}}\ldots\mathfrak{p}'_{j_1j} = \mathfrak{q}'^{-1}_{lj}\mathfrak{q}''_{lj_k}\mathfrak{p}'_{j_kj_{k-1}}\ldots\mathfrak{p}'_{j_1j} = \mathfrak{q}'^{-1}_{lj}\mathfrak{r}_{lj}$. Так как идеал $\mathfrak{q}'_{lj}$ максимален, то $\mathfrak{r}_{lj} = \mathfrak{q}'_{lj}\mathfrak{p}_{jj}$ имеет $k' + 1$ максимальный множитель, если емкость идеала $\mathfrak{p}_{jj}$ равна k'. С другой стороны, разложение $\mathfrak{r}_{lj} = \mathfrak{q}''_{ljk}\mathfrak{p}'_{j_kj_{k-1}}\ldots\mathfrak{p}'_{j_1j}$ показывает, что $\mathfrak{r}_{lj}$ имеет $k + 1$ максимальный множитель, и потому мы доказали, что $k' = k$.

Теорема 40. *Для того чтобы идеалы $\mathfrak{a}_{ii}$ и $\mathfrak{a}_{jj}$ были подобны, необходимо и достаточно, чтобы они были сопряжены.*

Очевидно, что пересечение $\mathfrak{a}_{ii}$ правых $\mathfrak{o}_i$-идеалов будет также и пересечением границ этих идеалов. Следовательно, непосредственно из определения (правого) подо-

бия следует, что если идеалы $\mathfrak{a}_{ii}$ и $\mathfrak{a}_{jj}$ подобны, то они сопряжены. Обратно, предположим, что идеалы $\mathfrak{a}_{ii}$ и $\mathfrak{a}_{jj}$ сопряжены. Тогда входящие в эти идеалы степени $\mathfrak{p}_{ii}^e$ и $\mathfrak{p}_{jj}^e$ простых идеалов могут быть сопоставлены таким образом, чтобы соответствующие друг другу $\mathfrak{p}_{ii}^e$ и $\mathfrak{p}_{jj}^e$ были сопряжены. Но модуль $\mathfrak{o}_i/\mathfrak{p}_{ii}^e$ разлагается в прямую сумму k изоморфных неразложимых модулей, где k является емкостью идеала $\mathfrak{p}_{ii}$, причем границей каждого из этих подмодулей будет $\mathfrak{p}_{ii}^e$. Следовательно, в силу предыдущей леммы, модуль $\mathfrak{o}_j/\mathfrak{p}_{jj}^e$ будет прямой суммой k неразложимых модулей, границей каждого из которых служит $\mathfrak{p}_{jj}^e$. Таким образом, идеалы $\mathfrak{p}_{ii}^e$ и $\mathfrak{p}_{jj}^e$, а следовательно, и идеалы $\mathfrak{a}_{ii}$ и $\mathfrak{a}_{jj}$ подобны.

БИБЛИОГРАФИЯ

Albert, A. A. [1]: *On the rank equation of any normal division algebra*, Bull. Amer. Math., Soc. **35** (1929), 335—338; [2]: *The rank function of any simple algebra*, Proc. Nat. Acad. Sci., **15** (1929), 372—375; [3]: *On direct products*, Trans. Amer. Math. Soc. **33** (1931); 690—711; [4]: *On the construction of cyclic algebras with a given exponent*, Amer. J. Math. **54** (1932), 1—13; [5]: *On normal simple algebras*, Trans. Amer. Math. Soc. **34** (1932), 620—625; [6]: *A note on normal division algebras of order sixteen*, Bull. Amer. Math. Soc. **38** (1932), 703—706; [7]; *Normal division algebras over a modular field*, Trans. Amer. Math. Soc. **36** (1934), 388—394; [8]: *On normal Kummer fields over a non-modular field*, Trans. Amer. Math. Soc. **36** (1934), 885—892; [9]: *Involutorial simple algebras and real Riemann matrices*, Ann. of Math. **36** (1935), 886—964; [10]: *Normal division algebras of degree p^e over F of characteristic p*, Trans. Amer. Math, Soc. **39** (1936), 183—188; [11]: *Simple algebpas of degree p^e over a centrum of characteristic p*, Trans. Amer. Math. Soc. **40** (1936), 112—126; [12]: *Modern Higher Algebra*, Chicago, 1937; [13]: *On cyclic algebras*, Ann. of Math. **39** (1938), 669—682; [14]: *Non-cyclic algebras with pure maximal subfields*, Bull. Amer. Math. Soc. **44** (1938), 576—579; [15]: *A note on normal division algebras of prime degree*, Bull. Amer. Math. Soc. **44** (1938), 649—652; [16]: *Structure of Algebras*, New York, 1939; [17]: *On p-adic fields and rational division algebras*, Ann. of Math. **41** (1940), 674—692; [18]: *Non-associative algebras, I. Fundamental concepts and isotopy*, Ann. of Math. **43** (1942), 685—707; [19]: *Non-associative algebras, II. New simple algebras*, Ann. of Math. **43** (1942), 708—723.

Albert, A. A., and Hasse, H. [1]: *A determination of all normal division algebras over an algebraic number field*, Trans. Amer. Math. Soc. **34** (1932), 722—726.

Artin, E. [1]: *Über einen Satz von Herrn J. H. Maclagan Wedderburn*, Abh. Math. Sem Univ. Hamburg **5** (1927),

245—250; [2]: *Zur Theorie der hyperkomplexen Zahlen*, Abh. Math. Sem. Univ. Hamburg. **5** (1927), 251—260; [3]: *Zur Arithmetik hyperkomplexer Zahlen*, Abh. Math. Sem. Univ. Hamburg **5** (1927), 261—239; [4]: *Galois Theory*, Notre Dame, 1942.

Artin, E., and Whaples, G. [1]: *The theory of simple rings*, Amer. J. Math. **65** (1943), 87—107.

Asano, K. [1]: *Über die Darstellungen einer endlichen Gruppe durch reele Kollineationen*, Proc. Imp. Acad. Tokyo **9** (1933), 574—576; [2]: *Nichtkommutative Hauptidealringe. I*, Act. Sci. Ind., No. 696, Paris, 1938; [3]: *Arithmetische Idealtheorie in nichtkommutativen Ringen*, Jap. J. Math. **15** (1939), 1—36; [4]: *Über verallgemeinerte Abelsche Gruppe mit hyperkomplexem Operatorenring und ihre Anwendungen*, Jap. J. Math. **15** (1939), 231—253; [5]: *Über Ringe mit Vielfachenkettensatz*, Proc. Imp. Acad. Tokyo **15** (1939), 288—291.

Asano, K., und Nakayama, T. [1]: *Über halblineare Transformationen*, Math. Ann. **115** (1937), 87—114.

Asano, K., und Shoda, K. [1]: *Zur Theorie der Darstellungen einer endlichen Gruppe durch Kollineationen*, Compositio Math. **2** (1935), 230—240.

Baer, R. [1]: *A Galois theory of linear systems over commutative fields*, Amer. J. Math. **62** (1940), 551—588; [2]: *Inverses and zero-divisors*, Bull. Amer. Math. Soc. **48** (1942), 630—638.

Birkhoff, G. [1]: *On the representability of Lie algebras and Lie groups by matrices*, Ann. of Math. **38** (1937), 526—532; [2]: *Lattice Theory*, New York, 1940.

Birkhoff, G., and MacLane, S., [1]: *A Survey of Modern Algebra*, New York, 1941.

Brandt, H. [1]: *Idealtheorie in einer Dedekindschen Algebra*. Jber. Deutsch. Math. Verein **37** (1928), 5—7; [2]: *Primidealzerlegung in einer Dedekindschen Algebra*, Schweizerische Naturforschende Gesellschaft. Verhandlungen **28** (1929), 288—290; [3]: *Zur Idealtheorie Dedekindscher Algebren*, Comment. Math. Helv. **2** (1930), 13—17; [4]: *Über die Axiome des Gruppoids*, Vierteljschr. Naturforsch. Ges. Zürich. **85** (1940), 95—104.

Brauer, R. [1]: *Untersuchungen über der arithmetischen Eigenschaften von Gruppen linearer Substitutionen,, I*, Math. Z. **28** (1928), 677—696; [2]: *ibid., II* **31** (1930), 733—747; [3]: *Über Systeme hyperkomplexer Zahlen*, Math. Z. **30** (1929), 79—107; [4]: *Über die algebraische Struktur von Schiefkörpern*, J. Reine Angew. Math. **166** (1932), 241—252; [5]: *Über die Konstruktion der Schiefkörper, die von endlichen Rang in bezug auf ein gegebenes Zentrum sind*, J. Reine Angew. Math. 168 (1932), 44—64; [6]: *Über den Index und den Exponenten von Divisionsalgebren*, Tôhoku Math. J. **37** (1933), 77—87; [7]: *Über die Kleinsche Theorie der algebraischen Gleichungen*, Math. Ann. **110** (1934), 473—500; [8]; *Eine Bedingung für vollständige Reduzibilität von Darstellungen gewöhnlicher und infintesimaler Gruppen*, Math. Z. **41** (1936), 330—339; [9]: *On algebras which are connected with the semi-simple continuous groups*, Ann. of Math. **38** (1937), 857—872; [10]: *On normal division algebras of index five*, Proc. Nat. Acad. Sci. **24** (1938), 243—246; [11]: *On modular and p-adic representations of algebras*, Proc. Nat. Acad. Sci. **25** (1939), 252—258; [12]; *Investigations on group characters*, Ann. of Math. **42** (1941) 936—958; [13]: *On sets of matrices with coefficients in a division ring*, Trans. Amer. Math. Soc. **49** (1941), 502—548; [14]: *On the nilpotency of the radical of a ring*, Bull. Amer. Math. Soc. **48** (1942), 752—758.

Brauer, R., Hasse, H., und Noether, E. [1]: *Beweis eines Hauptsatzes in der Theorie der Algebren*, J. Reine Angew. Math. **167** (1932), 399—404.

Brauer, R., und Nesbitt, C. [1]: *On the regular representations of algebras*, Proc. Nat. Acad. Sci. **23** (1937), 236—240; [2]: *On the modular representations of groups of finite order. I*, Toronto Studies, 1937; [3]: *On the modular characters of groups*, Ann. of Math. **42** (1941), 556—590.

Brauer, R. und Noether, E. [1]: *Über minimale Zerfällungskörper irreduzibler Darstellungen*, S. B. Preuss. Akad. Wiss. 32 (1927), 221—228.

Brauer, R., und Weyl, H. [1]; *Spinors in n dimensions*, Amer. J. Math. **57** (1935), 425—449.

Casimir, H., und van der Waerden, B. L. [1]: *Algebraischer Beweis der vollständigen Reduzibilität der Darstellungen halbeinfacher Liescher Gruppen*, Math. Ann. **111** (1935), 1—12.

Chevalley, C. [1]: *Sur la théorie du corps de classes dans les corps finis et les corps locaux*, J. Fac. Sci. Imp. Univ. Tokyo **9** (1933), 366—476; [2]: *La théorie du symbole de restes normiques*, J. Reine Angew. Math. **169** (1933), 140—156; [3]: *Sur certains idéaux d'une algèbre simple*, Abh. Math. Sem. Univ. Hamburg. **10** (1934), 83—105; [4]: *Demonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg. **11** (1936), 73—75; [5] *Généralisation de la théorie du corps de classes pour les extensions infinies*, J. Math.

Pures Appl, Cép. 9, **15** (1936), 359—371; [6]: *L'arithmétique dans les algèbres de matrices*, Act. Sci. Ind. No. 323, Paris. 1936; [7]: *La théorie du corps de classes*, Ann. of Math. 41 (1940), 394—418; [8]; *An algebraic proof of a property of Lie groups*, Amer. J. Math. **63** (1941), 785—793; [9]: *On the composition of fields*, Bull. Amer. Math., Soc, **48** (1942) 482—487.

Clifford, A. H. [1]: *Representations induced in an invariant subgroup*, Ann. of Math. **38** (1937), 533—550; [2]: *Semigroups admitting relative inverses*, Ann. of Math. **42** (1941), 1037—1049; [3]: *Matrix representations of completely simple semigroups*, Amer. J. Math. 64 (1942), 327—342.

Deuring, M. [1]: *Galoissche Theorie und Darstelungstheorie*, Math. Ann. **107** (1932), 140—144; [2] *Algebren*, Ergebnisse der Math. **4**, Berlin, 1935.

Dickson, L. E. [1]: *Linear Algebras*, Cambridge, 1914; [2]; *Algebras and their Arithmetics*, Chicago, 1923; [3]: *Algebren und ihre Zahlentheorie*, Zurich, 1927.

Dorroh, J. L. [1]: *Concerning adjunctions to algebras*, Bull. Amer. Math, Soc. **38** (1932), 85—88; [2]; *Concerning the direct product of algebras*. Ann. of Math. **36** (1935), 882—885.

Eichler, M. [1]: *Bestimmung der Idealklassenzahl in gewissen normalen einfachen Algebren*, J. Reine Angew. Math. **176** (1937), 192—202; [2]: *Über die Einheiten der Divisionsalgebren*, Math. Ann. **114** (1937), 635—654; [3]: *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörpern und inre L-Reihen*, J. Reine Angew. Math. **179** (1938), 227—251; [4]: *Über die Idealklassenzahl hyperkomplexer Systeme*, Math. Z. **43** (1938), 481—494; [5] *Zur Einheitentheorie der einfachen Algebren*, Comment. Math. Helv. 11 (1939), 253—272.

Etherington, I. M. H. [1]: *Genetic algebras*, Proc. Roy. Soc. Edinburgh 59 (1939), 242—258.

Everett, C. J., Jr. [1]: *Rings as groups with operators*, Bull. Amer. Math. Soc. **45** (1939) 274—279; [2]: *Annihilator ideals and representation iteration for abstract rings*, Duke Math. J. 5 (1939), 623—627; [3]; *Vector spaces over rings*, Bull. Amer Math. Soc. **48** (1942), 312—316; [4]: *An extension theory for rings*, Amer. J. Math. **64** (1942), 363—370.

Fitting, H. [1]: *Die Theorie der Automorphismenringe Abelscher Gruppen und ihr Analogon bei nicht kommutativen Gruppen*, Math. Ann. 107 (1932), 514—542; [2]: *Über die direkten Produktzerlegungen einer Gruppe in direkt unzerlegbar. Faktoren*, Math. Z. **39** (1935), 16—30; [3]: *Primärkomponentenzerlegung in nichtkommutativen Ringen*, Math. Ann. **111** (1935), 19—41; [4]: *Über die Existenz gemeinsamer Verfeinerungen bei direkten Produktzerlegungen einer Gruppe*, Math. Z, v. 41 (1936), 380—395; [5]: *Die Determinantenideale eines Moduls*, Jber. Deutsch. Math. Verein, v. 46 (1936), 195—228; [6]: *Über der Zusammenhang zwischen dem Begriff der Gleichartigkeit zweier Ideale und dem Äquivalenzbegriff der Elementarteilertheorie*, Math. Ann. **112** (1936), 572—582; [7]: *Der Normenbegriff für Ideale eines Ringes beliebiger Struktur*, J. Reine Angew. Math. **178** (1937), 107—122.

Гельфанд, И. М. [1]: *Normierte Ringe*, Матем. сборник, новая серия. **9** (1941), 3—23; [2]: *Ideale und primäre Ideale in normierten Ringen*, Матем. сборник, новая серия. **9** (1941), 41—48.

Головин, О. Н. [1]: *Множители без центра в прямых разложения, групп*, Матем. сборник, новая серия. **6** (1939), 423—426.

Haantjes, J. [1]: *Halblineare Transformationen*, Math. Ann. **111** (1937), 293—304.

Hall, M. [1]: *A type of algebraic closure*, Ann. of Math. **40** (1939), 360—369; [2]: *The position of the radical in an algebra*, Trans. Amer. Math. Soc. **48** (1940), 391—404.

Harrison, G. [1]: *The structure of algebraic moduls*, Proc. Nat. Acad. Sci. **28** (1942), 410—413.

Hasse, H. [1]: *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924) 113—130; [2]: *Äquivalenz quadratischer Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 158—162; [3]: *Über p-adische Schiefkörper und ihre Bedeutung fur die Arithmetik hyperkomplexer Zahlsysteme*, Math. Ann. **104** (1931), 495—534; [4]: *The theory of cyclic algebras over an algebraic number field*, Trans. Amer. Math. Soc. **34** (1932), 171—214; and *Additional note to the author's «Theory of cyclic algebras over an algebraic number field»*, Trans. Amer. Math. Soc. **34** (1932), 727—730; [5]: *Die Struktur der R. Brauerschen Algebrenklassengruppe über einem algebraischen Zahlkörper*, Math. Ann. **107** (1932), 731—760; [6]: *Über gewisse Ideale in einer einfachen Algebra*, Act. Sci. Ind. No. 109, Paris, 1934.

, und Schilling, O. F. G. [1]: *Die Normen aus r normalen Divisionsalgebra über einem algebraischen ılkörper*, J. Reine Angew. Math. **174** (1936) 248—252.

.ns, C. [1]: *Nilrings with minimal condition for admis-sible left ideals*, Duke Math. J. **4** (1938), 664—667; [2]: *Rings with minimal conditions for left ideals*, Ann. of Math. **40** (1939), 712—730.

Henke, K. [1]: *Zur arithmetischen Idealtheorie hyperkomplexer Zahlen*, Abh. Math. Sem. Univ. Hamburg. **11** (1936), 311—332

Higman, G. [1]: *The units of group-ringe*, Proc. London, Math. Soc. **46** (1940), 231—240.

Hochschild, G. P. [1]: *Semi-simple algebras and generalized derivations*, Amer. J. Math. **64** (1941), 677—694.

Ingraham, H. H., and Wolf, M. C. [1]: *Relative linear sets and similarity of matrices whose elements belong to a division algebra*, Trans. Amer. Math. Soc. **42** (1937), 16—31.

Jacobson, N. [1]: *Non-commutative polynomials and cyclic algebras*, Ann. of Math. **35** (1934), 197—208; [2]: *Totally disconnected locally compact rings*, Amer. J. Math. **58** (1936), 433—449; [3]: *Pseudo-linear transformations*, Ann. of Math. v. **38** (1937), 484—507; [4]: *Abstract derivations and Lie algebras*, Trans. Amer, Math. Soc. **42** (1937), 206—224; [5]: *p-algebras of exponent p.*, Bull. Amer. Math. Soc. **43** (1937), 667—670; [6]: *A note on topological fields*, Amer. J. Math. **59** (1937), 889—894; [7]: *A note on non-associative algebras*, Duke Math. J. **3** (1937), 544—548; [8]: *Simple Lie algebras over a field of characteristic zero*, Duke Math. J. **4** (1938), 534—551; [9]: *Normal semi-linear transformations*, Amer. J. Math. **61** (1939), 45—58; [10]: *The fundamental theorem of the Galois theory for quasi-fields*, Ann. of Math. **41** (1940), 1—7; [11]: *Restricted Lie algebras of characteristic p*, Trans. amer. Math. Soc. **50** (1941), 15—25; [12]: *Classes of restricted Lie algebras of characteristic p. I*, Amer. J. Math. **63** (1941), 481—515; [13]: *ibid.*, II. Duke Math. J. **10** (1943), 107—121.

Jacobson, N., and Taussky, O. [1]: *Locally compact rings*, Proc. Nat. Acad. Sci. 21 (1935), 106—108.

Jennings, S. A. [1]: *The structure of the group ring of a p-group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175—185; [2]: *Central chains of ideals in an associative ring*, Duke Math. J. **9** (1942), 341—355.

Jordan, P., von Neumann, J., and Wigner, E. [1]: *On an algebraic generalization of the quantum mechanical formalism*, Ann. of Math. **35** (1934), 29—64.

Kalisch, G. K. [1]: *On special Jordan algebras*, Dissertation University of Chicago, Chicago, 1942.

Kawada, Y. und Kondô, K. [1]: *Idealtheorie in nichtkommutativen Halbgruppen*, Jap. J. Math. **16** (1939), 31—45.

Kiokemeister, F. [1]: *The parastrophic criterion for the factorization of primes*, Trans. Amer. Math. Soc. **50** (1941), 140—159.

Kořínek, V. [1]: *Maximale kommutative Körper in einfachen Systemen hyperkomplexer Zahlen*, Mém. Soc. Sci. Bohème, 1932, No. 1. (1933), 1—24; [2]: *Une remarque concernant l'arithmétique des nombres hypercomplexes*, Mém. Soc. Roy. Sci. Bohème, 1932, No. 4 (1933), 1—8; [3]: *Sur la décomposition d'un groupe en produit direct des sous-groupes*, Casopis Pěst. Mat. Fys. **66** (1937), 261—286; исправления **67** (1938), 209—210.

Koethe, G. [1]: *Schiefkörper unendlichen Ranges über dem Zentrum*, Math. Ann. **105** (1931), 15—39; [2]: *Verallgemeinerte Abelsche Gruppen mit hyperkomplexen Operatorenring*, Math. Z., **39** (1934), 29—44.

Krull, W. [1]: *Über verallgemeinerte endliche Abelsche Gruppen*, Math. Z. **23** (1925), 161—196.

Курош, А. Г. [1]: *Проблемы теории колец, связанные с проблемой Бернсайда о периодических группах*, Известия Академии наук СССР, Серия математическая **5** (1941), 233—240.

Landherr, W. [1]: *Über einfache Liesche Ringe*, Abh. Math. Sem. Univ. Hamburg. **11** (1934), 41—64; [2]: *Liesche Ringe vom Typus A über einem algebraischen Zahlkörper (Die lineare Gruppe) und hermitesche Formen über einem Schiefkörper*, Abh. Math. Sem. Hansischen Univ. **12** (1938), 200—241.

Levitzki, J. [1]: *Über nilpotente Subringe*, Math. Ann. **105** (1931), 620—627; [2]: *On the equivalence of the nilpotent elements of a semi-simple ring*, Compositio Math. **5** (1938), 392—402; [3]: *On rings which satisfy the minimum condition for the right-hand ideals*, Compositio Math. **7** (1939), 214—222.

MacDuffee, C. C. [1]: *The Theory of Matrices*, Erg. der Math. **2**, Berlin, 1933; [2]: *Matrices with elements in a principal ideal ring*, Bull. Amer Math. Soc. **39** (1933), 564—584; [3]: *Modules and ideals in a Frobenius algebra*, Monatsh. Math. Phys. **48** (1939), 292—313; [4]: *An Introduction to Abstract Algebra*, New York, 1940.

MacLane, S. and Schilling, O. F. G., [1]: *A formula for the direct product of crossed product algebras*, Bull. Amer. Math. Soc. **48** (1942), 108–114; [2]: *Groups of algebras over an algebraic number field*, Amer. J. Math. **65** (1943), 299—308.

Maeda, F. [1]: *Ring-decomposition without chain condition*, J. Sci. Hirosima Univ., Ser. A, **8** (1938), 145—167.

Мальцев, А. И. [1]: *On the immersion of an algebraic ring into a field*, Math., Ann. **113** (1936), 686—691.

McCoy, N. H. [1]: *On the characteristic roots of matric polynomials*, Bull. Amer. Math. Soc. **42** (1936), 592—600; [2]: *Quasi-commutative rings and differential ideals*, Trans. Amer. Math. Soc. **39** (1936), 101 116; [3]: *Subrings of direct sums*, Amer. J. Math. **60** (1938), 374—382; [4]: *Subrings of infinite direct sums*, Duke Math. J. **4** (1938), 486—494; [5]: *Generalized regular rings*, Bull. Amer. Math. Soc. 45 (1939), 175—178; [6] *Algebraic properties of certain matrices over a ring*, Duke Math. J. **9** (1942), 322—340.

McCoy, N. H. and Montgomery, D. [1]: *A representation of generalized Boolean rings*, Duke Math. J. **3** (1937), 455—459.

Moriya, M. [1]: *Zur Bewertung der einfache Algebren*, Proc. Imp. Acad. Japan **13** (1937), 392–395.

Murray, F. J. and von Neumann, J. [1]: *On rings of operators*, Ann. of Math. **37** (1936), 116—229; [2]: *ibid.*, II, Trans. Amer. Math. Soc. **41** (1937), 208—248.

Nakayma, T. [1]: *Über die Beziehungen zwischen den Faktorensystemen und der Normklassengruppe eines galoisschen Erweiterungskörpers*, Math. Ann. **112** (1935), 85—91; [2]: *Über die direkte Zerlegung einer Divisionsalgebra*, Jap. J. Math. **12** (1935), 65—70; [3]: *Über die Algebren über einem Körper von der Primzahlcharakteristik*, Proc. Imp. Acad. Tokyo **11** (1935), 305–306; [4]: *Ibid II* **12** (1936), 113–114; [5]: *Eine Bemerkung über die Summe und den Durchschnitt von zwei Idealen in einer Algebra*, Proc. Imp. Acad. Tokyo **12** (1936), 179—182; [6]: *Über die Klassifikation halblinearer Transformationen*, Proc. Phys. Math. Soc. Japan **19** (1937), 99—107; [7]: *Divisionsalgebren über diskret bewerteten perfekten Körpern*, J. Reine. Angew. Math. **178** (1937), 11—13; [8]: *A note on the elementary divisor theory in non-commutative domains*, Bull. Amer. Math. Soc. **44** (1938), 719—723; [9]: *Some studies on regular representations, induced representations and modular representations*, Ann. of Math. **39** (1938), 361—369; [10]: *On Frobeniusean Algebras. I*, Ann of Math. **40** (1939), 611—633; [11]: *A remark on the sum and the intersection of two normal ideals of an algebra*, Bull. Amer. Math. Soc. **46** (1940), 460–472; исправления, v. 47 (1941), 332; [12]: *Note on uniserial and generalized uni-serial rings*, Proc. Imp. Acad. Tokyo **16** (1940), 285 289; [13]: *Normal basis of a quasi-field*, Proc. Imp. Acad. Tokyo. **16** (1940); 532—536; [14]: *On Frobeniusean algebras, II*, Ann. of Math. **42** (1941), 1—21 [5]: *Algebras with anti-isomorphic left and right ideal lattices*, Proc. Imp. Acad. Tokyo **17** (1941), 53—56.

Nakayama, T. and Nesbitt, C. [1]: *Note on symmetric algebras*, Ann. of Math. **39** (1938), 659—668.

Nakayama, T. und Shoda, K. [1] *Über die Darstellung einer endlichen Gruppe durch halblineare Transformationen*, Jap. J. Math. **12** (1936), 109—122.

Nehrkorn, H. [1]: *Über absolute Idealklassengruppen und Einheiten in algebraischen Zahlkorpern*, Abh. Math. Sem. Univ. Hamburg **9** (1933), 318—334.

Nesbitt, C. [1]: *On the regular representations of algebras*, Ann. of Math. **39** (1938), 634—658.

Neuhaus, A. [1]: *Products of normal semi-fields*, Trans. Amer. Math. Soc. **49** (1941), 106—121.

von Neumann, J. [1]: *On regular rings*, Proc. Nat. Acad, Sci. **22** (1936), 707—713; [2]: *Algebraic theory of continuous geometries*, Proc. Nat. Acad. Sci. **23** (1937), 16—22; [3]: *Continuous rings and their arithmetics*, Proc. Nat. Acad. Sci. **23** (1937), 341–349; [ ]: *On rings of operators, III*, Ann. of Math. **41** (1940), 94—161.

Niven, I. [1]: *Equations in quaternions*, Amer. Math. Monthly, v. 48 (1941), 654 661; [2]: *The roots of a quaternion*, Amer. Math. Monthly 49 (1942), 386—388.

Noether, E. [1]: *Der Diskriminantensatz für die Ordnungen eines algebraischen Zahl oder Funktionenkörpers*, J. Reine Angew. Math. **157** (1927), 82—1 4; [2]: *Hyperkomplexe Grössen und Darstellungstheorie*, Math. Z. 30 (1929), 641—692; [3]: *Hyperkomplexe Systeme in ihre Beziehungen zur kommutativen Algebra und Zahlentheorie*, Zurich Congress Proceedings, (1932), 189–194; [4]: *Der Hauptgeschlechtsatz für relativ-galiossche Zahlkörper*, Math. Ann. **108** (1933), 411—419; [5]: *Nichtkommutativ Algebren*, Math. Z. **37** (1933), 514–541; [6]: *Zerfallende verschränkte Produkte und inre Maximalordnungen*, Act. Sci. Ind., Paris, 1934.

Noether, E. und Schmeidler, W. [1]: *Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrucken*, Math. Z. **8** (1920), 1—35.

Ore, O. [1]: *Linear equations in non-commutative fields*, Ann. of Math. **32** (1931), 463—477; [2]: *Theory of non-commutative polynomials*, Ann. of Math. **34** (1933), 480—508.

Osima, M. [1]: *Über die Darstellung einer Gruppe durch halblineare Transformationen*, Proc.-Phys. Math. Soc. Japan **20** (1938), 1—5.

Perlis, S. [1]: *A characterization of the radical of an algebra*. Bull. Amer. Math. Soc. **48** (1942), 128—132.

Pickert, G. [1]: *Neue Methoden in der Strukturtheorie der kommutativ-assoziativen Algebren*, Math. Ann. **116** (1938), 217—280.

Rees, D. [1]: *On semi-groups*, Proc. Cambridge Philos. Soc. **36** (1940), 387—400; [2]: *Note on semi-groups*, Proc. Cambridge Philos. Soc. **37** (1941), 434—435.

Rinehart, R. F. [1]: *Some properties of the discriminant matrices of a linear associative algebra*, Bull. Amer. Math. Soc. **42** (1936), 570—576; [2]: *Commutative algebras which are polynomial algebras*, Duke Math. J. **4** (1938), 725—736; [3]: *An interpretation of the index of inertia of the discriminant matrices of a linear associative algebra*, Trans. Amer. Math. Soc. **46** (1939), 307—327.

Schiffman, M. [1]: *The ring of automorphisms of an Abelian group*, Duke Math. J. **6** (1940), 579—597.

Schilling, O. F. G. [1]: *Über gewisse Beziehungen zwischen der Arithmetik hyperkomplexer Zahlsysteme und algebraischer Zahlkörper*, Math. Ann. **111** (1935), 372—398; [2]: *Einheitentheorie in rationalen hyperkomplexen Systemen*, J. Reine Angew. Math., **175** (1936), 246—251; [3]: *Über die Darstellungen endlicher Gruppen*, J. Reine Angew. Math. **174** (1936), 188; [4]: *The structure of certain rational infinite algebras*, Duke Math. J. **3** (1937), 303—310; [5]: *Arithmetic in a special class of algebras*, Ann. of Math. **38** (1937), 116—119; [6]: *Units in p-adic algebras*, Amer. J. Math. **61** (1939), 883—896.

Schreier, O. [1]: *Über den Jordan-Hölderschen Satz*, Abh. Math. Sem. Univ. Hamburg **6** (1928), 300—302.

Шмидт, О. Ю. [1]: *Über unendliche Gruppen mit endlicher Kette*, Math. Z. **29** (1928), 34—41.

Шнейдмюллер, В. И. [1]: *О кольцах с конечными убывающими цепями подколец*, Доклады Академии Наук СССР, **28** (1940), 579—581.

Schur, I. [1]: *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. 127 (1904), 20—50; [2]: *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn A. Speiser*, Mat. Z. **5** (1919), 7—10.

Scorza, G. [1]: *Corpi Numericie Algebre*, Messina, 1921.

Scott, W. M. [1]: *On matrix algebras over an algebraically closed field*, Ann. of Math. **43** (1942), 147—160.

Segre, C. [1]: *Un nuovo campo di ricerche geometriche*, Atti Accad. Sci. Torino **25** (1889), 276—301.

Serbin, H. [1]: *Factorization in principal ideal rings*, Duke Math., J. **4** (1938), 656—663.

Shoda K. [1]: *Über die Automorphismen einer endlichen Abelschen Gruppe*, Math. Ann. **100** (1928), 674—686; [2]: *Über die mit einer Matrix vertauschbaren Matrizen*, Math. Z. **29** (1929), 696—712; [3]: *Über die Galoissche Theorie der Halbeinfachen hyperkomplexen Systeme*, Math. Ann. **107** (1932), 252—258; [4]: *Über die Äquivalenz der Darstellungen endlicher Gruppen durch halblineare Transformationen*, Proc. Imp. Acad. Japan. **14** (1938), 278—280; [5]: *Über die Invarianten der endlichen Gruppen halblinearer Transformationen*, Proc. Imp. Acad. Japan **14** (1938), 281—285

Skolem, T. [1]: *Zur Theorie der associativen Zahlensysteme* Oslo, 1927.

Speiser, A. [1]: *Zahlentheoretische Sätze aus der Gruppentheorie*, Math. Z. **5** (1919), 1—6; [2]: *Idealtheorie in rationalen Algebren, Dickson's Algebren*, Chapter 13, Zurich, 1927; [3]: *Zahlentheorie in rationalen Algebren*, Comment. Math. Helv. 8 (1936), 391—406.

Stauffer, R. [1]: *The construction of a normal basis in a separable normal extension field*, Amer. J. Math. **58** (1936), 585—597.

Stone, M. H., [1]: *The theory of representations of Boolean algebras*, Trans. Amer. Math. Soc. **40** (1936), 37—111.

Teichmüller, O. [1]: *Verschränkte Produkte mit Normalringen*, Deutsche Math. *I* (1936), 92—102; [2]: *Multiplikation zyklischer Normalringe*, Deutsche Math. **1** (1936) 197—238; [3]: *p-Algebren*, Deutsche Math. 1 (1936), 362—388; [4]: *Zerfällende zyklische p-Algebren*, J. Reine Angew. Math. **176** (1937), 157—160; [5]: *Der Elementarteilersatz für nichtkommutative Ringe*, S.—B. Preuss. Akad. Wiss., 1937;

[6]: *Über die sogennante nichtkommutative Galoissche Theorie und die Relationen* $\xi_{\lambda,\mu,\nu}\xi_{\lambda,\mu,\nu,\pi}\xi^{\lambda}_{\mu\nu,\pi} = \xi_{\lambda,\mu,\nu\pi}\xi_{\lambda\mu,\nu,\pi}$ Deutsche Math. **5** (1940), 138—149.

Tsen, C. C. [1]: *Divisionsalgebren über Funktionenkörpern*, Nach Ges. Wiss. Göttingen, 1933, 335—339; [2]: *Algebren über Funktionenkörpern*, Göttingen Dissertation, 1934; [3]: *Zur Stufentheorie der quasialgebraisch-Algeschlossenheit kommutativer Körper*, J. Chinese Math. Soc. *I* (1936), 81—92.

Узков, А. И. [1]: *Абстрактное обоснование брандтовой теории идеалов*. Матем. сборник. Новая серия. **6** (1939), 263—281.

Van der Waerden, B. L. [1]: *Moderne Algebra*, **1** and 2, Berlin 1931; 2 und edition **1**, 1937, 2, 1940; [2]: *Die Klassifikation der einfachen Lieschen Gruppen*, Math. Z. **37** (1933), 446—462; [3]: *Gruppen von linearen Transformationen*, Erg. der Math. **4**, Berlin, 1935.

Warning E. [1]: *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Univ. Hamburg. **11** (1936), 76—83.

Wedderburn, J. H. N. [1]: *A theorem on finite algebras*, Trans. Amer. Math. Soc **6** (1905) 349—352; [2]: *On hypercomplex numbers*, Proc. London Math. Soc., Ser. 2, **6** (1908), 77—118; [3]: *A type of primitive algebra*, Trans. Amer. Meth. Soc. **15** (1914), 162—166; [4]: *On division algebras*, Trans. Amer. Math. Soc. **22** (1921), 129—135; [5]: *Algebras which do not possess a finite basis*. Trans. Amer. Math. Soc. **26** (1924), 395—426; [6]: *A theorem on simple algebras*, Bull. Amer. Math. Soc. **31** (1925), 11—13; [7]: *Noncommutative domains of integrity*, J. Reine Angew. Math. **167** (1932), 129—141; [8]: *Lectures on Matrices*, New York, 1934; [9]: *Note on algebras*, Ann. of Math. **38** (1937), 854—856.

Weyl, H [1]: *Note on matric algebras*. Ann. of Math. **38** (1937), 477—483; [2]: *Commutator algebra of a finite group of collineations*, Duke Math. J. **3** (1937), 209—212; [3]: *The Classical Groups*, Princeton, 1939.

Whaples, G [1]: *Non-analytic class field theory and Grunwald's theorem*, Duke Math. J. **9** (1942), 455—473.

Whitehead, J. H. C. [1]: *On the decomposition of an infinitesimal group*, Proc. Cambridge Philos. Soc. v. 32 (1936), 229—237; [2]: *Certan equations in the algebra of a semisimple infinites mal group*, Quart, J. Math., Oxford Ser. 8 (1937), 220—237; [3]: *Note on linear associative algebras*, J. London, Math. Soc. **16** (1941), 118—125.

Whitney, H. [1]: *Tensor products of abelian groups*, Duke Math., J. **4** (1938), 495—528.

Witt, E. [1]: *Über die Kommutativität endlicher Schiefkörper*, Abh. Math. Sem. Univ. Hamburg **8** (1930), 413; [2]: *Zerlegung reeler algebraischer Funktionen in Quadrate. Schiefkörper über reelen Funktionenkörper*, J. Reine Angew. Math. **171** (1934), 4—11; [3]: *Riemann-Rochscher Satz und ζ-Funktion in Hyperkomplexen*, Math. Ann. **110** (1934), 12—28; [4]: *Zwei Regeln über verschränkte Producte*, J. Reine Angew. Math. **173** (1935), 191—192; [5]: *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31—44; [6]: *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. Reine Angew. Math. **176** (1937), 126—140; [7]: *Schiefkörper über diskret bewerteten Körpern*, J. Reine Angew. Math. **176** (1937), 153—156; [8]: *Treue Darstellung Liescher Ringe*, J. Reine Angew. Math. **177** (1937), 152—160.

Wolf, L. A. [1]: *Similarity of matrices in which the elements are real quaternions*, Bull. Amer. Math. Soc. **42** (1936), 737—743.

Zassenhaus, H. [1]: *Zum Satz von Jordan-Hölder-Schreir*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 106—108; [2]: *Lehrbuch der Gruppentheorie*, Leipzig, 1937; [3]: *Über Liesche Ringe mit Primzahlcharakteristik*, Abb. Math. Sem. Univ. Hamburg **13** (1939), 1—100; [4]: *Darstellungstheorie nilpotenter Lie-Ringe bei Charakteristik $p>0$*, J. Reine Angew. Math. **182** 1940, 150—155.

Zorn, M. [1]: *Theorie der alternativen Ringe*, Abh. Math. Sem. Univ. Hamburg **8** (1930), 123—147; [2]: *Note zur analytischen hyperkomplexen Zahlentheorie*, Abh. Math. Sem. Univ. Hamburg **9** (1933), 197—201; [3]: *Alternativkörper und quadratische Systeme*, Abh. Math. Sem. Univ, Hamburg **9** (1933), 395—402; [4]: *On a theorem of Engel*, Bull. Amer. Math. Soc. **43** (1937), 401—404; [5]: *Alternative rings and related questions, I: Existence of the radical*, Ann. of Math. **42** (1941), 676—686.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ

Глава 1

Группы и эндоморфизмы

Глава 2

Векторные пространства

Глава 3

Некоммутативные области главных идеалов

Глава 4

Структура колец эндоморфизмов и абстрактных колец

Глава 5

Алгебры над полем

Глава 6

Мультипликативная теория идеалов

ОПЕЧАТКИ

Страница	Строка	Напечатано	Должно быть
18	8 св.	$\mathfrak{N}/\mathfrak{R} \mid \mathfrak{R}/\mathfrak{P}$	$\mathfrak{N}/\mathfrak{P} \mid \mathfrak{R}/\mathfrak{P}$
55	1 сн.	$\mathfrak{R}/\mathfrak{G}$	$\mathfrak{N}/\mathfrak{S}$
56	9 св.	$\mathfrak{S}$	S
139	3 »	$g=g_s(t)$	$g=g_s(z)$
162	2 »	$et_s=t_s$	$et_s=e$
219	11 »	$\mathfrak{A}\times\Gamma$	$\mathfrak{A}\times\mathrm{P}$

Зак. 748. Джекобсон