Ю. А. ДРОЗД, В. В. КИРИЧЕНКО

# КОНЕЧНОМЕРНЫЕ АЛГЕБРЫ

*Допущено*
*Министерством высшего и среднего*
*специального образования УССР*
*в качестве учебного пособия для студентов*
*механико-математических факультетов*
*университетов*

КИЕВ
ИЗДАТЕЛЬСТВО ПРИ КИЕВСКОМ
ГОСУДАРСТВЕННОМ УНИВЕРСИТЕТЕ
ИЗДАТЕЛЬСКОГО ОБЪЕДИНЕНИЯ «ВИЩА ШКОЛА»
1980

УДК 519.48

**Конечномерные алгебры.** Дрозд Ю. А., Кириченко В. В. Киев, издательское объединение «Вища школа», 1980, 192 с.

В учебном пособии наряду с классическими вопросами (теория полупростых алгебр, радикал, центральные простые алгебры, теория Галуа, сепарабельные алгебры, представления групп) рассмотрены основы современной теории неполупростых алгебр (проективные модули, теорема Мориты, тензорные алгебры) и их применение к изучению квазифробениусовых однорядных и обобщенно однорядных алгебр.

Пособие соответствует программе специального курса по теории алгебр для студентов механико-математических факультетов. Изложение опирается только на стандартный курс алгебры.

Для студентов механико-математических факультетов университетов. Может быть использовано аспирантами и научными работниками соответствующих специальностей. Список лит.: 10 назв.

Печатается по постановлению Редакционно-издательского совета Киевского государственного университета

Рецензенты: доктора физ.-мат. наук П. М. ГУДИВОК, А. В. ЯКОВЛЕВ

Редакция естественной литературы
Зав. редакцией Б. Н. Фляшников

20203-076
Д——————111-80.1702030000
М224(04)-80

© Издательское объединение «Вища школа», 1980

## ПРЕДИСЛОВИЕ

Теория конечномерных алгебр — один из самых старых разделов современной алгебры. Его возникновение связано прежде всего с работами Гамильтона, открывшего знаменитое тело кватернионов, и Кэли, разработавшего теорию матриц. В дальнейшем строение конечномерных алгебр изучалось в работах целого ряда математиков, среди которых следует отметить Б. Пирса, К. С. Пирса, Клиффорда, Вейерштрасса, Дедекинда, Жордана, Фробениуса. В конце XIX в. Ф. Молин и Э. Картан описали полупростые алгебры над полями комплексных и действительных чисел и сделали первые шаги в изучении неполупростых алгебр.

Новый период в развитии теории конечномерных алгебр открывается работами Веддербёрна, которому принадлежат фундаментальные результаты этой теории: описание строения полупростых алгебр над произвольным полем, теорема о поднятии факторалгебры по радикалу, теорема о коммутативности конечных тел и др. В работах алгебраистов немецкой школы, возглавляемой Э. Нётер, Э. Артином, Р. Брауером, теория полупростых алгебр обрела современную форму, и бо́льшинство ее результатов было перенесено на кольца с условием минимальности (артиновы кольца). Кроме того, в этих работах была выявлена ведущая роль понятия модуля (или представления).

Дальнейшее развитие теории пошло в основном в двух направлениях. Первое из них привело к созданию теории бесконечномерных алгебр (и колец без условий обрыва); полученные здесь результаты отражены в монографии Н. Джекобсона «Строение колец». Второе направление — изучение строения неполупростых алгебр — столкнулось со значительными трудностями, большинство из которых не преодолено до сих пор. Поэтому здесь важное место занимают работы, связанные с выделением и описанием «естественных» классов алгебр. Это направление ведет свое начало от исследований Кёте, Асано, Накаямы по алгебрам главных идеалов и их обобщениям.

На протяжении всей своей истории теория конечномерных алгебр была тесно связана с различными разделами математики, черпая из них новые идеи и методы и в свою очередь оказывая существенное влияние на их развитие. На первых этапах наиболее глубокими были контакты с линейной алгеброй, теорией групп и их представлений, теорией Галуа. В последнее время, в особенности в связи с изучением неполупростых алгебр, важную роль начали играть методы гомологической алгебры, теории категорий, алгебраической геометрии.

Настоящая книга задумана как современный учебник по теории конечномерных алгебр. Основным инструментом исследования в ней являются методы теории модулей (представлений), которые, на наш взгляд, позволяют наиболее просто и ясно подойти как к классическим, так и к новым результатам. Естественно, мы не могли отразить в одинаковой степени все направления. Поэтому главное место в книге занимает структурная теория, т. е. изучение строения алгебр. В частности, почти не затронута общая теория представлений алгебр, которая в настоящее время переживает мощный подъем. Несомненно, специалисты заметят отсутствие и других разделов, возникших в последние годы. Тем не менее, мы надеемся, что эта книга даст возможность читателю изучить основные результаты классической теории алгебр и получить достаточную подготовку для знакомства с современными исследованиями.

Бóльшая часть книги опирается на стандартную программу курса высшей и линейной алгебры университетов и вполне доступна студентам второго — третьего курсов. В частности, мы не предполагаем наличие у читателя предварительных сведений по теории колец и модулей (более того, слово «кольцо» в книге почти не встречается). Главы, посвященные представлениям групп и теории Галуа, естественно, требуют знакомства с элементами теории групп (например, в объеме учебника А. И. Кострикина «Введение в алгебру»). В конце каждой главы приводятся упражнения различной сложности, которые содержат примеры, способствующие усвоению материала, а также фрагменты теорий, не нашедших отображения в основном тексте. Мы очень рекомендуем читателю (в особенности начинающему) прорабатывать большинство упражнений уже при первом чтении. Наиболее трудные из них сопровождаются довольно подробными указаниями.

Содержание книги распадается на три части. Первую из них составляют главы I—III, в которых содержатся основные понятия теории алгебр, излагается классическая теория полупростых алгебр и радикала. Последние параграфы главы III, посвященные схемам алгебр, можно рассматривать как введение в современные методы исследования. Вторую часть — главы IV—VI — можно назвать «тонкой теорией полупростых алгебр». Здесь на основе техники тензорных произведений и бимодулей излагается теория центральных простых алгебр, элементы теории Галуа полей, понятие группы Брауэра и теории сепарабельных алгебр. Наконец, третья часть — главы VIII—X — посвящена более современным результатам: теореме Мориты об эквивалентности категорий модулей, теории квазифробениусовых, однорядных, наследственных и обобщенно однорядных алгебр. Некоторые результаты этой части, по-видимому, можно найти только в журнальных статьях. Несколько особняком стоит глава VII, в которой на основании развитой теории полупростых алгебр излагается теория представлений групп, вплоть до теорем целочисленности и теоремы Бернсайда о разрешимости групп порядка $p^aq^b$.

Естественно, что мы нигде не стремились сформулировать и доказать теоремы в максимальной общности. Более того, специфика конечномерного случая использовалась всюду, где, по нашему мнению, это упрощало изложение. Искушенный читатель заметит, конечно, что многие результаты имеют место, например, для произвольных артиновых колец. Однако, как известно, очень часто такое обобщение выполняется почти автоматически. В тех же случаях, когда это не так, приходится привлекать достаточно сложные новые соображения, которые, на наш взгляд, могли существенно затруднить начинающему чтение книги.

Мы не приводим полного обзора литературы по теории конечномерных алгебр, так как даже по вопросам, затронутым в книге, он по объему был бы, вероятно, сравним с самой книгой. Назовем лишь несколько учебников и монографий на русском языке, по которым читатель может познакомиться с другими аспектами теории колец и алгебр [1, 3—9]. С вопросами арифметики полупростых алгебр можно познакомиться по книге [2] или по классическому учебнику Дойринга [10], к сожалению, до сих пор не переведенному на русский язык.

Мы придерживаемся общепринятых обозначений. В частности, символы $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ обозначают, соответственно, поля рациональных, действительных и комплексных чисел. Нумерация утверждений в книге дается по параграфам. Например, «теорема IV. 6.5» означает теорему с номером 6.5 (т. е. 5-ю в § 6) из гл. IV. Внутри главы IV та же теорема нумеруется как теорема 6.5.

# I

ГЛАВА

## ВВЕДЕНИЕ

**§ 1. Основные понятия. Примеры**

Алгебра над полем $K$, или $K$-алгебра,—это векторное пространство $A$ над этим полем, в котором задано билинейное ассоциативное умножение. Иными словами, любым двум элементам $a$ и $b$ из пространства $A$, взятым в определенном порядке, сопоставлен однозначно определенный элемент из $A$, который обычно называется их произведением и обозначается $ab$, причем выполняются следующие аксиомы:

$$1)\ a(b+c) = ab + ac;$$

$$2)\ (b+c)a = ba + ca;$$

$$3)\ (\alpha a)b = a(\alpha b) = \alpha(ab);$$

$$4)\ (ab)c = a(bc),$$

где $a$, $b$, $c$ — произвольные элементы из $A$, $\alpha$ — произвольный элемент (скаляр) поля $K$.

Алгебра $A$ называется конечномерной или бесконечномерной в зависимости от того, конечномерно или бесконечномерно пространство $A$. Мы в основном будем рассматривать конечномерные алгебры, хотя в некоторых главах нам придется иметь дело с бесконечномерными алгебрами.

Размерность векторного пространства $A$ называется размерностью алгебры $A$ и обозначается $[A : K]$.

Из билинейности умножения следует, что если в пространстве $A$ выбран базис $\{a_1, \ldots, a_n\}$, то умножение однозначно определяется заданием произведений базисных векторов $b_{ij} = a_i a_j$. Действительно, если $a = \sum_{i=1}^{n} \alpha_i a_i$, $b = \sum_{j=1}^{n} \beta_j a_j$, то

$$ab = \left(\sum_{i=1}^{n} \alpha_i a_i\right)\left(\sum_{j=1}^{n} \beta_j a_j\right) = \sum_{i,j=1}^{n} \alpha_i \beta_j (a_i a_j) = \sum_{i,j=1}^{n} \alpha_i \beta_j b_{ij}.$$

Разложим векторы $b_{ij}$ по базису $b_{ij} = \sum_{k=1}^{n} \gamma_{ij}^k a_k$. Мы видим, что структура алгебры на пространстве $A$ с фиксированным базисом однозначно задается набором $n^3$ элементов поля $K$ $\gamma_{ij}^k$ $(i, j, k = 1, \ldots, n)$. Эти элементы называются структурными константами алгебры $A$.

Конечно, векторы $b_{ij}$ (а потому и структурные константы $\gamma_{ij}^k$) нельзя задавать произвольно, хотя, определяя умножение формулой

$\left(\sum_{i=1}^{n}\alpha_i a_i\right)\left(\sum_{j=1}^{n}\beta_j b_j\right)=\sum_{i,j,k=1}^{n}\gamma_{ij}^{k}\alpha_i\beta_j a_k$, мы заведомо обеспечим его билинейность (т. е. выполнение аксиом 1)—3)), но этим вовсе не гарантируется ассоциативность. Уже ассоциативность умножения базисных элементов накладывает на структурные константы ограничения. Действительно,

$$(a_i a_j)\,a_k=\sum_{l=1}^{n}\gamma_{ij}^{l}a_l a_k=\sum_{l,m=1}^{n}\gamma_{ij}^{l}\gamma_{lk}^{m}a_m,$$

$$a_i\,(a_j a_k)=a_i\sum_{l=1}^{n}\gamma_{jk}^{l}a_l=\sum_{l,m=1}^{n}\gamma_{jk}^{l}\gamma_{il}^{m}a_m.$$

откуда следует, что для любых $i$, $j$, $k$

$$\sum_{l=1}^{n}\gamma_{ij}^{l}\gamma_{lk}^{m}=\sum_{l=1}^{n}\gamma_{jk}^{l}\gamma_{il}^{m}. \tag{1}$$

Наоборот, из соотношения (1) следует ассоциативность умножения для базисных векторов, а потому, как легко проверить, и для любых элементов алгебры.

Предположим, что $\{\tilde{a}_1, \ldots, \tilde{a}_n\}$ — новый базис пространства $A$, связанный с исходным матрицей перехода $S=(s_{ij})$. Тогда

$$\tilde{a}_i\tilde{a}_j=\left(\sum_{l=1}^{n}s_{il}a_l\right)\left(\sum_{r=1}^{n}s_{jr}a_r\right)=\sum_{l,r=1}^{n}s_{il}s_{jr}\,(a_l a_r)=\sum_{l,r,m=1}^{n}s_{il}s_{jr}\gamma_{lr}^{m}a_m=$$

$$=\sum_{k,l,r,m=1}^{n}s_{il}s_{jr}\gamma_{lr}^{m}s'_{mk}\tilde{a}_k,$$

где $s'_{mk}$ — коэффициенты обратной матрицы $S^{-1}$. Таким образом, структурные константы $\tilde{\gamma}_{ij}^{k}$, соответствующие новому базису, имеют вид

$$\tilde{\gamma}_{ij}^{k}=\sum_{l,r,m=1}^{n}s_{il}s_{jr}s'_{mk}\gamma_{lr}^{m},$$

т. е. набор элементов $\gamma_{ij}^{k}$ можно рассматривать как координаты трехвалентного тензора (дважды ковариантного и один раз контравариантного).

Элемент $e$ алгебры $A$ называется единицей алгебры, если для любого элемента $a\in A$ $ae=ea=a$. В дальнейшем мы всегда будем предполагать, что в алгебре $A$ есть единица. Заметим, что единица $e$ в алгебре единственна: если $e'$ — другая единица, то $e=ee'=e'$.

Существование единицы — это обычное и несущественное ограничение. Если $A$ — алгебра без единицы, то ее всегда можно «присоединить», рассмотрев алгебру $\tilde{A}$, состоящую из пар $(a, \alpha)$, где $a \in A$, $\alpha \in K$, с покоординатными сложением и умножением на скаляры и произведением, задаваемым формулой

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

Легко проверить, что $\tilde{A}$ является алгеброй, а элемент $(0, 1)$ — ее единицей. Практически все свойства алгебр $A$ и $\tilde{A}$ одинаковы, что мы попытаемся осветить в упражнениях.

**Примеры.** 1. Множество квадратных матриц $n$-го порядка с коэффициентами из поля $K$ образует алгебру относительно обычных действий над матрицами. Это — конечномерная алгебра размерности $n^2$, которую мы будем обозначать $M_n(K)$.

2. Многочлены от одной переменной над полем $K$ образуют бесконечномерную алгебру $K[x]$.

3. Если $V$ — векторное пространство над полем $K$, то линейные операторы в пространстве $V$ также образуют алгебру $E(V)$. Эта алгебра конечномерна или бесконечномерна в зависимости от того, конечномерно или бесконечномерно пространство $V$.

4. Рассмотрим четырехмерное векторное пространство над полем вещественных чисел $\mathbf{R}$ с базисом $\{e, i, j, k\}$. Определим в нем умножение с помощью такой таблицы:

| | $e$ | $i$ | $j$ | $k$ |
|---|---|---|---|---|
| $e$ | $e$ | $i$ | $j$ | $k$ |
| $i$ | $i$ | $-e$ | $k$ | $-j$ |
| $j$ | $j$ | $-k$ | $-e$ | $i$ |
| $k$ | $k$ | $j$ | $-i$ | $-e$ |

(Произведение $ab$ записано в строке с номером $a$ и столбце с номером $b$).

Легко проверить, что таким образом получается алгебра $\mathbf{H}$ над полем $\mathbf{R}$ с единицей $e$. Эта алгебра называется алгеброй кватернионов. Исторически это один из первых примеров алгебр.

5. Всякое расширение $L$ поля $K$, т. е. поле, содержащее $K$ в качестве подполя, можно рассматривать как алгебру над $K$. Если эта алгебра конечномерна, расширение называется конечным, в противном случае — бесконечным.

6. Пусть дана некоторая группа $G$. Примем элементы этой группы за базис векторного пространства, т. е. рассмотрим множество $KG$ формальных сумм вида $\sum_{g\in G}\alpha_g g$, где $\alpha_g$— элементы поля $K$, лишь конечное число которых отлично от нуля. Тогда умножение элементов группы (нашего базиса!) задает структуру алгебры в пространстве $KG$. Эта алгебра называется *групповой алгеброй* группы $G$ над полем $K$ и играет основную роль в теории представлений групп.

7. Рассмотрим $n$-мерное числовое пространство над полем $K$, т. е. множество наборов $(\alpha_1, \ldots, \alpha_n)$, $\alpha_i \in K$, с покоординатным сложением и умножением на скаляры. Определив умножение покоординатно

$$(\alpha_1, \ldots, \alpha_n)(\beta_1, \ldots, \beta_n) = (\alpha_1\beta_1, \ldots, \alpha_n\beta_n),$$

мы превратим его в алгебру над полем $K$, которую обозначим $K^n$.

8. Пусть $A_1, \ldots, A_n$ — алгебры над полем $K$. Рассмотрим их декартово произведение $A$, т. е. множество наборов $(a_1, \ldots, a_n)$, $a_i \in A_i$, и определим в нем операции покоординатно

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n),$$

$$\alpha(a_1, \ldots, a_n) = (\alpha a_1, \ldots, \alpha a_n),$$

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1b_1, \ldots, a_nb_n).$$

Очевидно, таким образом $A$ превращается в алгебру над $K$, которая называется *прямым произведением* алгебр $A_1, \ldots, A_n$ и обозначается $A_1 \times \ldots \times A_n$, или $\prod_{i=1}^{n} A_i$. Алгебры $A_1, \ldots, A_n$ называются *прямыми сомножителями* алгебры $A$. Конечно, предыдущий пример является частным случаем этого примера при $A_1 = \ldots = A_n = K$.

Алгебра $A$ называется *коммутативной*, если умножение в ней коммутативно, т. е. $ab = ba$ для всех $a, b \in A$. Алгебры из примеров 2, 3 и 6 коммутативны. Алгебра из примера 5 коммутативна, если коммутативна группа $G$. Алгебра из примера 7 коммутативна, если коммутативны все прямые сомножители $A_1, \ldots, A_n$. Остальные алгебры из приведенных выше примеров некоммутативны.

Подмножество $B$ алгебры $A$ называется *подалгеброй*, если $B$ само является алгеброй относительно тех же операций, что и $A$, и с той же единицей. Иными словами, $B$ должно быть подпространством в $A$, таким, что $e \in B$, и если $a, b \in B$, то и $ab \in B$.

**Примеры.** 1. Множество треугольных матриц, т. е. таких матриц $(a_{ij})$, что $a_{ij} = 0$ при $j < i$, образует подалгебру в алгебре всех матриц $M_n(K)$. Эту алгебру мы будем обозначать $T_n(K)$.

2. Диагональные матрицы также образуют подалгебру в $M_n(K)$, которую мы будем обозначать $D_n(K)$.

3. Множество матриц вида

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_{n-1} & \alpha_n \\ 0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-2} & \alpha_{n-1} \\ 0 & 0 & \alpha_1 & \dots & \alpha_{n-3} & \alpha_{n-2} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \alpha_1 & \alpha_2 \\ 0 & 0 & 0 & \dots & 0 & \alpha_1 \end{pmatrix},$$

как легко проверить, образует подалгебру в $M_n(K)$ размерности $n$. Эту алгебру мы будем называть ж о р д а н о в о й и обозначать $J_n(K)$.

4. Если $H$ — подгруппа группы $G$, то $KH$ есть подалгебра в $KG$.

5. Совокупность элементов $c$ алгебры $A$, перестановочных со всеми элементами алгебры, т. е. таких, что $ca = ac$ для всех $a \in A$, очевидно, образует в $A$ подалгебру, которая называется ц е н т р о м алгебры $A$ и обозначается $C(A)$.

6. Рассмотрим в алгебре $A$ совокупность скалярных кратных единице, т. е. элементов вида $\alpha e$, где $\alpha \in K$. Поскольку $(\alpha e)(\beta e) = \alpha\beta e$, они образуют подалгебру, которую обозначим $Ke$.

Естественное стремление любой теории — это классификация изучаемых объектов. Попытаемся классифицировать алгебры хотя бы малых размерностей. Если $[A : K] = 1$, то $A = Ke$, чем фактически полностью определяется строение этой алгебры, поэтому первый интересный случай — это $[A : K] = 2$.

Выберем в двумерной алгебре $A$ базис, принимая $e$ за первый базисный элемент: $\{e, a\}$, $a \notin Ke$. Тогда умножение однозначно определяется заданием произведения $aa = a^2$, причем, как легко видеть, ассоциативность обеспечивается автоматически. Кроме того, такая алгебра обязательно коммутативна. Пусть $a^2 = pa + qe$, где $p$ и $q$ — фиксированные элементы поля $K$. Рассмотрим многочлен $g(x) = x^2 - px - q$. Элемент $a$ — «корень» этого многочлена. Оказывается, строение алгебры $A$ в основном определяется тем, какие у $g(x)$ настоящие корни в поле $K$. Возможны три случая.

С л у ч а й 1. $g(x)$ имеет в $K$ два различных корня $x_1 \neq x_2$. Тогда $p = x_1 + x_2$, $q = -x_1x_2$. Положим $b = (a - x_1e)/(x_2 - x_1)$. Поскольку $b \notin Ke$, $\{e, b\}$ — базис $A$, причем

$$b^2 = (x_2 - x_1)^{-2}(a^2 - 2x_1a + x_1^2e) = (x_2 - x_1)^{-2}(pa + qe - 2x_1a + x_1^2e) =$$

$$= (x_2 - x_1)^{-2}[(x_2 - x_1)a - (x_2 - x_1)x_1e] = (x_2 - x_1)^{-1}(a - x_1e) = b.$$

С л у ч а й 2. $g(x)$ имеет в $K$ один корень (двукратный), т. е. $g(x) = (x - x_1)^2$, где $x_1 \in K$. Полагая $b = a - x_1e$, получаем базис $\{e, b\}$, для которого

$$b^2 = (a - x_1e)^2 = g(a) = 0.$$

Случай 3. $g(x)$ не имеет корней в $K$, т. е. он неприводим в этом поле. Покажем, что тогда $A$ есть поле, т. е. каждый ненулевой элемент $b$ имеет обратный $b^{-1}$, такой, что $bb^{-1} = e$. Проще всего это сделать обычным приемом «уничтожения иррациональности в знаменателе». Пусть $b = \alpha a + \beta e$. Тогда $g(x) = (\alpha x + \beta) f(x) + r$, где $r \in K$ — остаток от деления $g(x)$ на $\alpha x + \beta$, не равный нулю, а $f(x) = \alpha' x + \beta'$. Но отсюда следует, что $g(a) = 0 = (\alpha a + \beta e)(\alpha' a + \beta' e) + re$, т. е. элемент — $(\alpha' a + \beta' e)/r$ обратный к $b$.

Итак, мы получили следующий результат.

**Теорема 1.1.** *Двумерная алгебра $A$ над полем $K$ либо сама является полем, либо в ней можно выбрать базис $\{e, b\}$, такой, что $b^2 = b$ или $b^2 = 0$.*

Если поле $K$ алгебраически замкнуто (например, поле комплексных чисел), то случай 3 (поле) невозможен.

### § 2. Изоморфизм и гомоморфизм. Тела

При описании двумерных алгебр мы столкнулись с тем, что многие из них (например, все алгебры случая 1 или 2) «одинаково устроены» в том смысле, например, что в них можно выбрать базисы с одинаковыми таблицами умножения. Такие алгебры обладают совершенно одинаковыми свойствами и «внутренне неразличимы», хотя могут быть определены на разных векторных пространствах. Естественно отождествлять все такие алгебры и считать их просто разными копиями одной и той же алгебры. Это приводит к важнейшему понятию теории алгебр (и многих математических теорий) — изоморфизму.

Изоморфизм алгебры $A$ на алгебру $B$—это взаимно однозначное линейное отображение $f$ пространства $A$ на пространство $B$, сохраняющее умножение, т. е. такое, что $f(a_1 a_2) = f(a_1) f(a_2)$ для любых элементов $a_1$ и $a_2$ из алгебры $A$. Если существует изоморфизм из алгебры $A$ на алгебру $B$, то алгебры $A$ и $B$ называются изоморфными. Это обозначается $A \simeq B$ или, если надо явно указать изоморфизм $f$, $f : A \xrightarrow{\sim} B$.

Очевидно, существование изоморфизма $f : A \xrightarrow{\sim} B$ равносильно тому, что в $A$ и $B$ можно выбрать базисы с одинаковыми таблицами умножения. В частности, все двумерные алгебры над полем $K$ в случае 1 или 2 предыдущего параграфа будут изоморфны между собой.

В теории алгебр изоморфные алгебры, как правило, отождествляются. Говорят, что алгебры изучаются «с точностью до изоморфизма». Например, с точностью до изоморфизма, над алгебраически замкнутым полем $K$ есть две двумерные алгебры. Нетрудно убедиться, что это алгебры $K^2$ и $J_2(K)$.

Классический пример изоморфизма, важнейший для линейной алгебры,— это изоморфизм алгебры линейных операторов $E(V)$ в $n$-мерном пространстве $V$ и алгебры матриц $M_n(K)$, который получается, если сопоставить оператору его матрицу в фиксированном базисе.

Еще пример изоморфных алгебр — это алгебры $K^n$ и $D_n(K)$ (алгебра диагональных матриц).

Наконец, для любой алгебры $A$ с единицей $e$ подалгебра $Ke$ изоморфна основному полю $K$. Мы в дальнейшем всегда будем отождествлять элемент $\alpha$ поля $K$ с элементом $\alpha e \in A$ — его образом при этом изоморфизме — и рассматривать поле $K$ как подалгебру любой $K$-алгебры $A$. В частности, единицу алгебры $A$ мы часто будем обозначать просто 1.

Важную роль в теории алгебр играет также понятие гомоморфизма.

Гомоморфизм алгебры $A$ в алгебру $B$—это линейное отображение $f: A \to B$, сохраняющее умножение и единицу, т. е. такое, что $f(a_1a_2) = f(a_1)f(a_2)$ для любых $a_1, a_2 \in A$ и $f(e_A) = e_B$, где $e_A$ — единица алгебры $A$, $e_B$ — единица алгебры $B$.

Если гомоморфизм $f$ инъективен, т. е. из $a_1 \neq a_2$ следует $f(a_1) \neq f(a_2)$, он называется мономорфизмом. Если же $f$ сюръективен, т. е. для любого элемента $b \in B$ найдется такой $a \in A$, что $b = f(A)$, то он называется эпиморфизмом.

Очевидно, если $f$ одновременно является и мономорфизмом, и эпиморфизмом, то это изоморфизм. В этом случае (и только в этом) у $f$ есть обратное отображение $f^{-1}$, являющееся изоморфизмом $B$ на $A$.

Поскольку гомоморфизм $f$ — это линейное отображение, для его инъективности достаточно, чтобы из $f(a) = 0$ следовало $a = 0$. Действительно, если это так, то из $f(a_1) = f(a_2)$ следует, что $f(a_1 - a_2) = 0$, откуда $a_1 - a_2 = 0$, т. е. $a_1 = a_2$.

Как и для любых отображений, для гомоморфизмов определяется произведение, или суперпозиция: если $f: A \to B$ и $g: B \to C$ — гомоморфизмы алгебр, то можно определить отображение $gf: A \to C$ по правилу $gf(a) = g(f(a))$, и легко проверить, что $gf$ также является гомоморфизмом. Умножение гомоморфизмов ассоциативно: если одно из произведений $(gf)h$ и $g(fh)$ определено, то определено и другое, и они равны.

Можно привести такой пример гомоморфизма. Пусть $a$ — фиксированный элемент алгебры $A$. Рассмотрим отображение $K[x] \to A$, переводящее многочлен $f(x) = \alpha_0 x^n + \ldots + \alpha_n$ в элемент $f(a) = \alpha_0 a^n + \ldots + \alpha_n$. Очевидно, это гомоморфизм, а его образ состоит из всевозможных элементов вида $f(a)$. Этот образ обычно обозначается $K[a]$ и называется моногенной подалгеброй, порожденной элементом $a$. В частном случае, если $K[a] = A$, сама алгебра $A$ называется моногенной. Элемент $f(a)$ называется значением $f(x)$ при $x = a$.

Перейдем к изучению внутренних свойств алгебр и их элементов.

Элемент $a$ алгебры $A$ называется левым (правым) делителем нуля, если существует такой ненулевой элемент $b \in A$, что $ab = 0$ (соответственно $ba = 0$).

Аналогично $a$ называется левым (правым) делителем единицы, если существует такой элемент $b \in A$, что $ab = 1$ (соответственно $ba = 1$).

Заметим, что если $a$ одновременно является и левым, и правым делителем единицы, т. е. существуют $b$ и $b'$ такие, что $ab = b'a = 1$, то $b' = b'(ab) = (b'a)\,b = b$, и если $ac = 1$, то $b = b(ac) = (ba)\,c = c$. Таким образом, $b$ — единственный элемент, для которого $ab = 1$, и аналогично — единственный элемент, для которого $ba = 1$. В этом случае элемент $a$ называется обратимым, а $b$ — обратным к $a$ и обозначается: $b = a^{-1}$.

Вообще говоря, взаимосвязь между четырьмя сформулированными свойствами довольно сложная. Однако в конечномерных алгебрах положение существенно упрощается.

**Теорема 2.1.** *В конечномерной алгебре*

1) *всякий левый делитель нуля (единицы) является и правым делителем нуля (единицы) и наоборот;*

2) *всякий элемент является делителем нуля или единицы;*

3) *делитель нуля не может быть делителем единицы.*

Доказательство. а) Покажем вначале, что в любой алгебре левый (правый) делитель нуля не может быть правым (левым делителем единицы. Действительно, пусть $ab = 0$, но $b \neq 0$ и одновременно $ca = 1$. Тогда $0 = c(ab) = (ca)\,b = b$, что противоречит предположению $b \neq 0$.

б) Пусть теперь алгебра $A$ конечномерна, а $a \in A$ — элемент, не являющийся левым делителем нуля. Рассмотрим отображение $f$ векторного пространства $A$ в себя, задаваемое формулой $f(x) = ax$. Из аксиом алгебры следует, что $f$ — линейное отображение, причем, так как $a$ — не левый делитель нуля, из $f(x) = 0$ следует $x = 0$. Но тогда, ввиду конечномерности $A$, $f$ — невырожденное отображение и образ его совпадает со всем $A$. В частности, $1 = f(b) = ab$ для некоторого $b \in A$ и $a$ — левый делитель единицы.

Аналогично доказывается, что если $a$ — не правый делитель нуля, то он правый делитель единицы.

в) Теперь мы можем завершить доказательство теоремы. Если элемент $a \in A$ — левый делитель нуля, то ввиду а) он не может быть правым делителем единицы. Поэтому ввиду б) он обязан быть правым делителем нуля. Остальные утверждения п. 1) доказываются аналогично. После этого из а) следует 3), а из б) — 2).

Алгебра, каждый ненулевой элемент которой обратим, называется телом.

**Следствие 2.2.** *Конечномерная алгебра без делителей нуля есть тело.*

**Следствие 2.3.** *Подалгебра конечномерного тела есть тело. В частности, центр конечномерного тела — поле.*

Всякий элемент $a$ конечномерной $K$-алгебры $A$ является «корнем» некоторого ненулевого многочлена $f(x) \in K[x]$ (это означает, что $f(a) = 0$). Действительно, иначе подалгебра $K[a]$ была бы изоморфна $K[x]$, что невозможно, так как пространство $K[x]$ беско-

нечномерно. Многочлен наименьшей степени со старшим коэффициентом 1, корнем которого является $a$, называется м и н и м а л ь н ы м м н о г о ч л е н о м элемента $a$ и обозначается $m_a(x)$.

**Предложение 2.4.** *Всякий многочлен, корнем которого является $a$, делится на $m_a(x)$. В частности, минимальный многочлен определен однозначно.*

Д о к а з а т е л ь с т в о. Пусть $f(a) = 0$. Разделим $f(x)$ с остатком на $m_a(x)$: $f(x) = m_a(x)\,g(x) + r(x)$, причем либо $r(x) = 0$, либо его степень меньше степени $m_a(x)$. Но $f(a) = r(a) = 0$, поэтому вторая возможность исключена и $f(x)$ делится на $m_a(x)$.

**Предложение 2.5.** *Если $A$ — конечномерное тело над полем $K$, то для любого элемента $a \in A$ минимальный многочлен $m_a(x)$ неприводим.*

Д о к а з а т е л ь с т в о. Если $m_a(x) = f(x)\,g(x)$, где $f$ и $g$ — многочлены меньшей степени, то $0 = m_a(a) = f(a)\,g(a)$, но $f(a) \neq 0$, $g(a) \neq 0$, что невозможно.

**Следствие 2.6.** *Если поле $K$ алгебраически замкнуто, то единственное конечномерное тело над $K$ — это само $K$.*

Д о к а з а т е л ь с т в о. Если $A$ — такое тело и $a$ — любой его элемент, то $m_a(x)$ — неприводимый многочлен и, из-за алгебраической замкнутости $K$, он линеен: $m_a(x) = x - \alpha$, откуда $a = \alpha \in K$, так как $m_a(a) = 0$. Итак, $A = K$, что и требовалось доказать.

## § 3. Представления и модули

Определение алгебры, приведенное в самом начале главы, удобно и интересно именно своей общностью, благодаря которой оно охватывает весьма разнообразный и большой круг объектов. Однако при изучении строения и свойств алгебр часто существенную роль играют конкретные реализации данной алгебры, например, как некоторой алгебры матриц (или линейных операторов). Такие реализации изучает теория представлений, которая во многом будет нашим основным аппаратом исследования в этой книге.

П р е д с т а в л е н и е м $K$-алгебры $A$ называется ее гомоморфизм $T$ в алгебру $E(V)$ линейных операторов в некотором пространстве $V$. Иными словами, задать представление $T$ — значит сопоставить каждому элементу $a \in A$ линейный оператор $T(a)$ так, чтобы

$$T(a + b) = T(a) + T(b),$$

$$T(\alpha a) = \alpha T(a),$$

$$T(ab) = T(a)\,T(b),$$

$$T(1) = E \text{ (тождественный оператор)}$$

для любых $a, b \in A$, $\alpha \in K$. Если пространство $V$ конечномерно, то его размерность называется р а з м е р н о с т ь ю (или с т е п е н ь ю) представления $T$. Очевидно, образ представления $T$, т. е. совокупность всех операторов вида $T(a)$, образует подалгебру

в $E(V)$. Если $T$ — мономорфизм, эта подалгебра изоморфна алгебре $A$. В этом случае представление называется точным.

**Теорема 3.1** (Кэли). *Всякая алгебра имеет точное представление. Иными словами, всякая алгебра изоморфна подалгебре алгебры линейных операторов.*

Доказательство. Из аксиом алгебры следует, что для любого элемента $a \in A$ отображение $T(a) : x \to xa$, $x \in A$, является линейным оператором в пространстве $A$, причем $T(a+b) = T(a) + T(b)$, $T(\alpha a) = \alpha T(a)$, $T(ab) = T(a)\,T(b)$ и $T(1) = E$ (единичный оператор). Поэтому $T$ — представление алгебры $A$. Если $a \neq b$, то $1a \neq 1b$. Значит, операторы $T(a)$ и $T(b)$ различны и $T$ — точное представление, что и требовалось доказать.

Представление, построенное при доказательстве теоремы (Кэли), называется регулярным и играет важную роль в теории алгебр (этого можно ожидать уже потому, что оно дает сравнительно простую и стандартную реализацию данной алгебры). Размерность регулярного представления равна размерности алгебры.

Если представление $T$ конечномерно (а в дальнейшем мы будем рассматривать только такие представления), то мы можем выбрать в пространстве $V$ базис и сопоставить каждому оператору $T(a)$ его матрицу $[T(a)]$. Очевидно, соответствие $a \to [T(a)]$ является гомоморфизмом алгебры $A$ в алгебру матриц $M_n(K)$, где $n$ — размерность представления $T$. Такой гомоморфизм называется матричным представлением алгебры $A$. Если в пространстве $V$ выбрать новый базис, то каждая матрица $[T(a)]$ заменится на $C[T(a)]C^{-1}$, где $C$ — матрица перехода. Такие два матричных представления называются подобными.

Понятие подобия можно определить и для операторных представлений: два представления $T : A \to A(V)$ и $S : A \to E(W)$ называются подобными, если существует такой изоморфизм $f$ пространства $V$ на пространство $W$, что $T(a) = f\,S(a)\,f^{-1}$ для любого $a \in A$. Из сказанного выше, очевидно, следует, что в этом случае базисы в $V$ и $W$ можно выбрать таким образом, чтобы матрицы операторов $T(a)$ и $S(a)$ совпадали. Поэтому есть смысл изучать представления с точностью до подобия, т. е. отождествлять подобные представления.

В дальнейшем мы, как правило, не будем различать представление и соответствующее матричное представление. Заметим, что теорему 3.1 (теорему Кэли) можно сформулировать еще так: всякая конечномерная алгебра изоморфна подалгебре алгебры матриц (конечномерность, очевидно, нужна для того, чтобы регулярное представление было конечномерно).

Как правило, удобно бывает не рассматривать отдельно пространство $V$ и гомоморфизм $T : A \to E(V)$, а считать, что элементы алгебры сами являются операторами в $V$. Это приводит к понятию модуля.

Правым модулем над $K$-алгеброй $A$, или правым $A$-модулем, называется векторное пространство $M$ над полем $K$, для элементов которого задано умножение на элементы алгебры, т. е. каждой паре $(m, a)$, где $m \in M$, $a \in A$, сопоставлен однозначно определенный элемент $ma \in M$, причем выполняются следующие аксиомы:

1) $(m_1 + m_2)\, a = m_1 a + m_2 a$,

2) $m\,(a_1 + a_2) = ma_1 + ma_2$,

3) $(\alpha m)\, a = m\,(\alpha a) = \alpha\,(ma)$, где $\alpha \in K$,

4) $m\,(ab) = (ma)\, b$,

5) $m1 = m$.

Покажем, как по всякому представлению алгебры $A$ можно построить правый модуль над этой алгеброй, и наоборот: по всякому правому модулю можно построить представление.

Пусть $T : A \to E\,(V)$ — представление алгебры $A$. Определим умножение элементов $V$ на элементы алгебры, положив $va = vT\,(a)$ для любых $v \in V$, $a \in A$. Из определения представлений сразу следует, что таким образом $V$ превращается в правый $A$-модуль. Будем говорить, что этот модуль соответствует представлению $T$.

Наоборот, если $M$ — правый модуль над $A$, то из аксиом модуля следует, что при фиксированном $a \in A$ отображение $T\,(a) : m \to ma$ является линейным оператором в пространстве $M$. Сопоставляя $a$ оператор $T\,(a)$ (или его матрицу в некотором базисе), мы получаем представление алгебры $A$, соответствующее модулю $M$.

В частности, регулярному представлению соответствует регулярный модуль. Здесь $M = A$, а $ma$ есть произведение элементов $m$ и $a$ в алгебре $A$.

В дальнейшем, если не оговорено противное, все рассматриваемые модули будут предполагаться конечномерными (как векторные пространства над $K$).

Для модулей вводятся также понятия гомоморфизма и изоморфизма.

Гомоморфизм правого $A$-модуля $M$ в правый $A$-модуль $N$ — это линейное отображение $f : M \to N$, при котором $(ma)f = (mf)\, a$ для любых элементов $m \in M$ и $a \in A$.

Если $f$, кроме того, взаимно однозначно, то оно называется изоморфизмом, а модули $M$ и $N$ — изоморфными. В этом случае пишут $f : M \xrightarrow{\sim} N$, или просто $M \simeq N$. Очевидно, если $f : M \xrightarrow{\sim} N$, то $f^{-1} : N \xrightarrow{\sim} M$. Изоморфные модули обладают совершенно одинаковыми свойствами и отождествляются.

**Теорема 3.2.** *Представления, соответствующие изоморфным модулям, подобны, и наоборот, модули, соответствующие подобным представлениям, изоморфны.*

Доказательство. Пусть $T$ и $S$ — представления, соответствующие модулям $M$ и $N$, а $f : M \cong N$. Тогда для любого $m \in M$ и $a \in A$ имеет место равенство

$$mT(a)f = (ma)f = (mf)a = mfS(a),$$

т. е. $T(a)f = fS(a)$ или $T(a) = fS(a)f^{-1}$.

Наоборот, предположим, что представления $T$ и $S$ подобны, $T(a) = fS(a)f^{-1}$. Тогда, если $M$ и $N$ — соответствующие модули, $f$ является взаимно однозначным линейным отображением $M$ на $N$, причем

$$(ma)f = mT(a)f = mfS(a) = (mf)a$$

для любых $m \in M$ и $a \in A$, т. е. $f$ — изоморфизм модулей.

Таким образом, понятие изоморфизма модулей в точности соответствует понятию подобия представлений.

В дальнейшем нам будет удобно гомоморфизмы правых модулей записывать слева от элементов, т. е. писать $fa$ вместо $af$. Всюду, где не оговорено противное, мы будем придерживаться этой системы обозначений.

Гомоморфизмы модулей, как и гомоморфизмы алгебр, можно умножать, принимая за произведение гомоморфизмов $f : M \to N$ и $g : N \to L$ отображение $gf : M \to L$, такое, что $gf(m) = g(f(m))$ для всех $m \in M$ (легко проверить, что $gf$ также будет гомоморфизмом).

Однако для гомоморфизмов модулей определены и другие операции: сложение и умножение на скаляры. Если $f$ и $g$ — гомоморфизмы модуля $M$ в модуль $N$, то за $f + g$ принимают такое отображение $M \to N$, что $(f + g)(m) = f(m) + g(m)$, а за $\alpha f$, где $\alpha \in K$,— отображение $M \to N$, для которого $(\alpha f)(m) = \alpha f(m)$ для всех $m \in M$.

Нетрудно убедиться в том, что определенные таким образом $f + g$ и $\alpha f$ являются гомоморфизмами, а совокупность всех гомоморфизмов из $M$ в $N$ относительно этих операций есть векторное пространство над полем $K$. Это пространство мы будем обозначать $\mathrm{Hom}_A(M, N)$.

Умножение гомоморфизмов также обладает привычными свойствами: оно ассоциативно, т. е. $(gf)h = g(fh)$, как только эти произведения определены (очевидно, они определены одновременно), и билинейно $g(f + h) = gf + gh$; $(g + f)h = gh + fh$; $g(\alpha f) = (\alpha g)f = \alpha(gf)$, как только эти выражения имеют смысл. Несложную проверку этих свойств мы оставляем читателю.

Если гомоморфизм $f : M \to N$ инъективен, т. е. из $m_1 \neq m_2$ следует, что $f(m_1) \neq f(m_2)$, он называется мономорфизмом. Если же $f$ сюръективен, т. е. всякий элемент из $N$ имеет вид $f(m)$, то $f$ называется эпиморфизмом. Очевидно, если $f$ одновременно является моно- и эпиморфизмом, то это изоморфизм. Как и в случае алгебр, для мономорфности $f$, конечно, достаточно, чтобы из $f(m) = 0$ следовало $m = 0$.

Аналогично понятию правого модуля можно дать определение левого модуля над алгеброй $A$, как векторного пространства $L$, для элементов которого определено умножение $al$ ($a \in A$, $l \in L$, $al \in L$), удовлетворяющее таким аксиомам:

$$1)\ a(l_1 + l_2) = al_1 + al_2,$$

$$2)\ (a_1 + a_2)\, l = a_1 l + a_2 l,$$

$$3)\ a(\alpha l) = (\alpha a)\, l = \alpha (al), \qquad \alpha \in K,$$

$$4)\ (ab)\, l = a(bl),$$

$$5)\ 1l = l.$$

Левым модулям соответствуют антипредставления алгебры $A$, т. е. линейные отображения $T : A \to E(V)$, для которых $T(ab) = T(b)\, T(a)$; $T(1) = E$. Для антипредставлений и левых модулей понятия подобия, гомоморфизма и изоморфизма вводятся так же, как и для представлений и правых модулей. Имеют место и теоремы, аналогичные теоремам 3.1 и 3.2. В частности, рассматривая алгебру $A$ как левый модуль над собой, мы приходим к понятию регулярного левого модуля и регулярного антипредставления.

В дальнейшем мы будем рассматривать в основном правые модули, называя их просто модулями над алгеброй $A$, или $A$-модулями. Читатель легко может проследить, что все доказываемые результаты остаются в силе для левых модулей. Поэтому мы будем их использовать по мере надобности без особой оговорки.

**§ 4. Подмодули и фактормодули. Идеалы и факторалгебры**

Известно, какую важную роль в линейной алгебре играет понятие инвариантного подпространства некоторого оператора. Если задано представление $T : A \to E(V)$ алгебры $A$, то естественно рассматривать в $V$ подпространства, инвариантные относительно всех операторов представления. Это приводит нас к понятию подмодуля.

Подмодуль $A$-модуля $M$ — это подпространство $N \subset M$ такое, что $na \in N$ для любых элементов $n \in N$ и $a \in A$.

Выберем базис $\{e_1, \ldots, e_k\}$ в подпространстве $N$ и дополним его до базиса $M : \{e_1, \ldots, e_k, e_{k+1}, \ldots, e_m\}$. Тогда в этом базисе представление $T$, соответствующее модулю $M$, имеет вид

$$T(a) = \begin{pmatrix} T_1(a) & 0 \\ X(a) & T_2(a) \end{pmatrix}. \tag{1}$$

Такие представления (и все подобные ему) называются приводимыми. Очевидно, $T_1$ — это представление, соответствующее модулю $N$.

Наоборот, пусть представление $T$ приводимо, т. е. имеет вид (1), где $T_1$ — представление размерности $k$. Тогда подпространство $N$, натянутое на первые $k$ базисных векторов, будет инвариантно относительно всех операторов $T(a)$, т. е. будет подмодулем в $M$.

Из правил действий с клеточными матрицами следует, что отображение $a \to T_2(a)$ также является представлением алгебры $A$. Соответствующий ему модуль допускает следующую интерпретацию.

Пусть $m \in M$. Рассмотрим множество $m + N$, состоящее из элементов вида $m + n$, где $n$ пробегает все $N$. Такие множества называются *классами смежности* (или *смежными классами*) $M$ по $N$[1]. Если элемент $x$ лежит в классе $m + N$, то говорят, что $x$ *сравним с* $m$ *по модулю* $N$, и пишут $x \equiv m \pmod{N}$. Покажем, что любые два класса смежности либо совпадают, либо не пересекаются.

Действительно, если $(m_1 + N) \cap (m_2 + N) \neq \varnothing$, то в $N$ есть такие два элемента $n_1$ и $n_2$, что $m_1 + n_1 = m_2 + n_2$, откуда $m_1 - m_2 = n_2 - n_1 = n_0 \in N$ и для всякого элемента $n \in N$ $m_1 + n = m_2 + n_0 + n \in m_2 + N$, а $m_2 + n = m_1 + n - n_0 \in m_1 + N$, т. е. $m_1 + N = m_2 + N$.

Легко проверить, что если $x \in m + N$, $y \in m' + N$, то $x + y \in (m + m') + N$ и, кроме того, $\alpha x \in \alpha m + N$ и $xa \in ma + N$ для любых элементов $\alpha \in K$ и $a \in A$. Поэтому на множестве смежных классов можно определить структуру $A$-модуля, полагая

$$(m + N) + (m' + N) = (m + m') + N,$$

$$\alpha(m + N) = \alpha m + N, \tag{2}$$

$$(m + N)a = ma + N.$$

Справедливость всех аксиом очевидна, так как действия над классами определяются через их «представителей», т. е. через операции в модуле $M$.

Множество смежных классов $M$ по $N$ со структурой модуля, определенной формулами (2), называется *фактормодулем* модуля $M$ по подмодулю $N$ и обозначается так: $M/N$.

Заметим, что фактормодуль возникает вместе с естественным отображением $\pi : M \to M/N$, сопоставляющим элементу $m \in M$ класс $m + N$. Формулы (2) при этом обозначают, что $\pi$ является гомоморфизмом (и, очевидно, эпиморфизмом). Этот эпиморфизм мы будем называть *проекцией* $M$ *на фактормодуль* $M/N$.

Тривиальная проверка, которую мы оставляем читателю, показывает, что если $\{e_1, \ldots, e_k\}$ — базис $N$, а $\{e_{k+1}, \ldots, e_m\}$ — его дополнение до базиса $M$, то классы $\pi(e_{k+1}), \ldots, \pi(e_m)$ образуют базис $M/N$, причем соответствующее представление совпадает с $T_2$.

---

[1] Очевидно, класс смежности $m + N$ — это линейное многообразие с направляющим подпространством $N$, проходящее через вектор $m$.

Подмодули регулярного модуля называются правыми идеалами алгебры $A$. Таким образом, правый идеал — это пространство $I \subset A$, такое, что из $x \in I$ и $a \in A$ следует $xa \in I$. Подмодули левого регулярного модуля называются левыми идеалами. Отметим, что в термине «правый идеал» мы никогда не будем опускать прилагательное «правый», так как термин «идеал» употребляется совсем в другом смысле.

Важные примеры подмодулей и фактормодулей возникают при изучении гомоморфизмов.

Пусть $f : M_1 \to M_2$ — гомоморфизм $A$-модулей. Его ядром, $\operatorname{Ker} f$, называется совокупность всех элементов $m \in M_1$, для которых $f(m)=0$. Образом $\operatorname{Im} f$ гомоморфизма $f$ называется совокупность всех элементов из $M_2$, имеющих вид $f(m)$.

**Теорема 4.1** (о гомоморфизме). *Для любого гомоморфизма $f: M_1 \to M_2$ ядро и образ являются подмодулями соответственно в $M_1$ и $M_2$ и $\operatorname{Im} f \simeq M_1/\operatorname{Ker} f$.*

Доказательство. Если $f(m) = f(m') = 0$, то $f(m + m') = f(m) + f(m') = 0$, $f(\alpha m) = \alpha f(m) = 0$ и $f(ma) = f(m)a = 0$, т. е. $\operatorname{Ker} f = N_1$ — подмодуль в $M_1$. Аналогично, так как $f(m) + f(m') = f(m + m')$, $\alpha f(m) = f(\alpha m)$ и $f(m)a = f(ma)$, $\operatorname{Im} f = N_2 =$ подмодуль в $M_2$.

Пусть $m + N_1$ — какой-либо элемент $M_1/N_1$ и $x \in m + N_1$. Тогда $x = m + n$, где $f(n) = 0$, откуда следует, что $f(x) = f(m)$. Поэтому, полагая $g(m + N_1) = f(m)$, мы задаем отображение $g : M_1/N_1 \to N_2$, причем из того, что $f$ — гомоморфизм, и из определения операций (2) в фактормодуле следует, что $g$ — гомоморфизм.

Предположим, что $g(m + N_1) = 0$. Тогда $f(m) = 0$, т. е. $m \in N_1$ и $m + N_1 = 0 + N_1$ — нулевой класс фактормодуля $M/N_1$, а значит, $g$ — мономорфизм. Поскольку всякий элемент из $N_2$ имеет вид $f(m) = g(m + N_1)$, $g$ является эпиморфизмом и, следовательно, изоморфизмом $M_1/\operatorname{Ker} f$ на $\operatorname{Im} f$.

Несмотря на свою простоту, теорема о гомоморфизме играет важную роль при изучении модулей. Продемонстрируем это на одном примере.

Модуль $M$ называется циклическим, если в нем есть такой элемент $m_0$, что всякий элемент из $M$ имеет вид $m_0a$, где $a \in A$. Элемент $m_0$ называется образующим модуля $M$.

**Следствие 4.2.** *Всякий циклический модуль изоморфен фактормодулю регулярного модуля по некоторому правому идеалу.*

Доказательство. Пусть $M$ — циклический модуль с образующим $m_0$. Из аксиом модуля следует, что отображение $f : A \to M$, переводящее $a$ в $m_0a$, есть гомоморфизм модулей, причем, так как $m_0$ — образующий, $\operatorname{Im} f = M$. Но тогда $M \simeq A/\operatorname{Ker} f$, где $\operatorname{Ker} f$ — правый идеал.

Мы будем также часто пользоваться следующим результатом, уточняющим теорему о гомоморфизме.

**Теорема 4.3** (Нётер). *Пусть $N$ — подмодуль в $M$, $\pi$ — проекция $M$ на $\bar{M} = M/N$. Для любого подмодуля $L \subset M$ положим $\pi(L) = \{\pi(x) \mid x \in L\}$ и для любого подмодуля $\bar{L} \subset \bar{M}$ положим $\pi^{-1}(\bar{L}) = \{x \in M \mid \pi(x) \in \bar{L}\}$. Тогда*

1) *$\pi(L)$ — подмодуль в $\bar{M}$, а $\pi^{-1}(\bar{L})$ — подмодуль в $M$, содержащий $N$;*

2) *$\pi(\pi^{-1}(\bar{L})) = \bar{L}$, а если $L \supset N$, то $\pi^{-1}(\pi(L)) = L$;*

3) *если $L = \pi^{-1}(\bar{L})$, то $L/N \simeq \bar{L}$, а $M/L \simeq \bar{M}/\bar{L}$.*

Таким образом, мы получаем взаимно однозначное соответствие между подмодулями $\bar{M}$ и подмодулями $M$, содержащими $N$, причем это соответствие согласовано с операцией взятия фактормодулей.

Доказательство. Утверждение 1) тривиально. Далее, всякий элемент $\bar{x} \in \bar{L}$ имеет вид $\pi(x)$, где $x \in M$ и даже $x \in \pi^{-1}(\bar{L})$, так как $\pi(x) = \bar{x} \in \bar{L}$, что доказывает формулу $\bar{L} = \pi(\pi^{-1}(\bar{L}))$.

Пусть теперь $L$ — подмодуль в $M$, содержащий $N$. Ограничивая $\pi$ на $L$, мы получим гомоморфизм $\bar{\pi} : L \to \bar{M}$, ядром которого является $N$, а образом — $\pi(L) = \bar{L}$. Очевидно, $\pi^{-1}(\bar{L}) \supset L$. Докажем обратное включение. Если $m \in \pi^{-1}(\bar{L})$, то $\pi(m) \in \bar{L}$ и потому имеет вид $\pi(x)$, где $x \in L$. Из равенства $\pi(m) = \pi(x)$ следует, что $\pi(m - x) = 0$, т. е. $m - x = n \in N$. Но $N \subset L$, значит, и $m = x + n \in L$. Итак, мы показали, что $\pi^{-1}(\bar{L}) = L$ и $\bar{L} = \operatorname{Im} \bar{\pi} \simeq L/\operatorname{Ker} \bar{\pi} = L/N$.

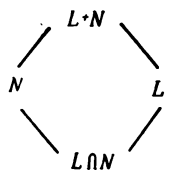
Обозначим через $\tau$ проекцию $\bar{M}$ на $\bar{M}/\bar{L}$ и рассмотрим гомоморфизм $\tau\pi : M \to \bar{M}/\bar{L}$. Поскольку $\tau$ и $\pi$— эпиморфизмы, $\tau\pi$ —также эпиморфизм.

Вычислим $\operatorname{Ker} \tau\pi$. $\tau\pi(m) = 0$ означает, что $\pi(m) \in \bar{L}$, т. е. $m \in \pi^{-1}(\bar{L}) = L$, поэтому $\operatorname{Ker} \tau\pi = L$ и по теореме о гомоморфизме $\bar{M}/\bar{L} \simeq M/L$.

Рассмотрим, что изменится, если $L$ — подмодуль в $M$, не содержащий $N$. По-прежнему можно рассмотреть $\bar{\pi} : L \to M/N$ — ограничение проекции $\pi : M \to M/N$. $\pi(x) = 0$ означает, что $x \in N$, откуда следует, что $\operatorname{Ker} \bar{\pi} = L \cap N$ и $\bar{L} = \operatorname{Im} \bar{\pi} \simeq L/L \cap N$. Но, как мы только что установили, $\bar{L} \simeq \pi^{-1}(\bar{L})/N$. В то же время $m \in \pi^{-1}(\bar{L})$ тогда и только тогда, когда $\pi(m) = \pi(x)$ для некоторого $x \in L$, т. е. $m = x + n$, где $n \in N$. Поэтому, обозначая через $L + N$, как обычно, подпространство в $M$, состоящее из всевозможных сумм $x + n$, мы видим, что $L + N = \pi^{-1}(\bar{L})$ — подмодуль в $M$ (это легко проверить и непосредственно) и $(L + N)/N \simeq \bar{L} \simeq L/L \cap N$. Нами доказана такая теорема.

**Теорема 4.4** (Нётер). *Для любых подмодулей $L$ и $N$ модуля $M$ $(L + N)/N \simeq L/L \cap N$.*

Если изобразить расположение подмодулей $L$, $N$, $L+N$ и $L \cap N$ в модуле $M$, то получим «параллелограмм»




Фактормодули $(L+N)/N$ и $L/L \cap N$ — это «противоположные стороны параллелограмма». Поэтому мы иногда будем называть вторую теорему Нётер «законом параллелограмма».

Естественное желание перенести полученные результаты на случай гомоморфизмов алгебр приводит к понятию идеала (или, как иногда говорят, двустороннего идеала).

Пусть $A$ и $B$ — две алгебры над полем $K$, $\varphi : A \to B$ — гомоморфизм $K$-алгебр. Его образ $\operatorname{Im}\varphi = \{\varphi(a) \mid a \in A\}$ есть, конечно, подалгебра в алгебре $B$. Но ядро $\operatorname{Ker}\varphi = \{a \in A \mid \varphi(a) = 0\}$ не является подалгеброй, поскольку в нем не лежит единица. Так как $\varphi$ — линейное отображение, $\operatorname{Ker}\varphi$ — подпространство в $A$. Кроме того, если $x \in \operatorname{Ker}\varphi$, то для любого $a \in A$ $\varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)\,0 = 0$ и аналогично $\varphi(xa) = 0$, т. е. $ax$ и $xa$ тоже лежат в $\operatorname{Ker}\varphi$. Иными словами, $\operatorname{Ker}\varphi$ одновременно является правым и левым идеалом.

Подпространство, являющееся одновременно правым и левым идеалом в алгебре, называется идеалом.

По всякому идеалу $I \subset A$ можно построить новую алгебру следующим образом.

Рассмотрим снова множество смежных классов $A$ по $I$. Если $a+I$ и $b+I$ — два таких класса, то для любых $x \in a+I$ и $y \in b+I$ элемент $xy$ лежит в классе $ab+I$. Поэтому множество смежных классов можно превратить в алгебру над полем $K$, полагая

$$(a+I)+(b+I) = (a+b)+I,$$

$$\alpha(a+I) = \alpha a + I, \quad \alpha \in K,$$

$$(a+I)(b+I) = ab+I.$$

Эта алгебра называется факторалгеброй алгебры $A$ по идеалу $I$ и обозначается $A/I$. Нулем этой алгебры служит класс $0+I=I$, а единицей — класс $1+I$.

Отображение $\pi : A \to A/I$, для которого $\pi(a) = a+I$, является эпиморфизмом алгебры $A$ на факторалгебру $A/I$. Оно называется проекцией $A$ на $A/I$.

Следующие результаты вполне аналогичны соответствующим теоремам, доказанным для модулей. Их доказательства, также ана-

логичные изложенным выше, мы оставляем читателю в качестве несложного упражнения.

**Теорема 4.5** (о гомоморфизме). *Для всякого гомоморфизма алгебр* $\varphi : A \to B$ $\operatorname{Im}\varphi \simeq A/\operatorname{Ker}\varphi$.

**Следствие 4.6.** *Если* $A = K[a]$ *— моногенная алгебра, то* $A \simeq K[x]/I$, *где* $I$ *— идеал, состоящий из кратных многочлена* $m_a(x)$.

**Теорема 4.7** (Нётер). *Пусть* $\pi$ *— проекция алгебры* $A$ *на факторалгебру* $\bar{A} = A/I$. *Для любого подмножества* $B \subset A$ *положим* $\pi(B) = \{\pi(b) \mid b \in B\}$, *а для любого подмножества* $\bar{B} \subset \bar{A}$ *положим* $\pi^{-1}(\bar{B}) = \{b \in A \mid \pi(b) \in \bar{B}\}$. *Тогда*

1) *если* $B$ *— идеал (подалгебра) в* $A$, *то* $\pi(B)$ *— идеал (подалгебра) в* $\bar{A}$; *если* $\bar{B}$ *— идеал (подалгебра) в* $\bar{A}$, *то* $\pi^{-1}(\bar{B})$ *— идеал (подалгебра) в* $A$;

2) *для любого идеала (подалгебры)* $\bar{B} \subset \bar{A}$ $\pi(\pi^{-1}(\bar{B})) = \bar{B}$; *для любого идеала (подалгебры)* $B \subset A$, *содержащего* $I$, $\pi^{-1}(\pi(B)) = B$;

3) *если* $\bar{B}$ *— идеал (подалгебра) в* $\bar{A}$, $B = \pi^{-1}(\bar{B})$, *то* $A/B \simeq \bar{A}/\bar{B}$ *(соответственно* $B/I \simeq \bar{B}$).

**Теорема 4.8** (Нётер). *Если* $I$ *— идеал, а* $B$ *— подалгебра в алгебре* $A$, *то* $(B + I)/I \simeq B/B \cap I$.

Если $N$ — подмодуль модуля $M$, а $I$ — правый идеал кольца $A$, определим $NI$ как множество сумм вида $\sum_i n_i a_i$, где $n_i \in N$, $a_i \in I$. Легко видеть, что $NI$ также является подмодулем в $M$. Может оказаться, что $NI = 0$, т. е. $na = 0$ для любых $n \in N$ и $a \in I$. В этом случае говорят, что $I$ а н н у л и р у е т подмодуль $N$. Для всякого модуля $M$ можно указать наибольший правый идеал в $A$, аннулирующий $M$. Положим $\operatorname{Ann} M = \{a \in A \mid ma = 0$ для любого $m \in M\}$. Очевидно, $\operatorname{Ann} M$ — правый идеал и даже идеал алгебры $A$. Он называется а н н у л я т о р о м модуля $M$.

Если идеал $I$ аннулирует модуль $M$, то $M$ можно рассматривать как модуль над факторалгеброй $A/I$, полагая $m(a + I) = ma$ (проверьте, что это определение не зависит от выбора представителя в классе $a + I$). Конечно, в этом случае $I$ аннулирует любой подмодуль и фактормодуль модуля $M$, и все «устройство» модуля $M$ не зависит от того, рассматривать ли его как $A$- или как $A/I$-модуль.

Наоборот, всякий $A/I$-модуль $M$ можно превратить в $A$-модуль, полагая $ma = m(a + I)$ (при этом автоматически $I$ аннулирует $M$).

В дальнейшем мы всегда будем отождествлять модули над $A/I$ и модули над $A$, которые аннулируются идеалом $I$. В частности, нам часто придется рассматривать регулярный $A/I$-модуль как $A$-модуль. Очевидно, его аннулятором будет именно идеал $I$.

Отметим еще, что для любого элемента $m$ модуля $M$ и любого правого идеала $I \subset A$ подмножество $mI = \{ma \mid a \in I\}$ есть подмодуль в $A$. Если $mI = 0$, говорят, что $I$ а н н у л и р у е т $m$. Среди правых идеалов, аннулирующих данный элемент, также есть

наибольший, который называется аннулятором $m$: $\operatorname{Ann} m = \{a \in A \mid ma = 0\}$. В отличие от аннулятора модуля, $\operatorname{Ann} m$ может не быть идеалом (см. упражнение 9 к этой главе).

**§ 5. Теорема Жордана—Гёльдера**

Во всяком ненулевом модуле $M$, очевидно, всегда есть по крайней мере два подмодуля: сам $M$ и нулевое подпространство (эти подмодули называют тривиальными). Если других подмодулей в $M$ нет, модуль $M$ называется простым. Соответствующее представление неприводимо, т. е. ни в каком базисе оно не приобретает вид (1) из § 4.

Предположим, что модуль $M$ не простой. Тогда в нем найдется нетривиальный подмодуль $N$, т. е. такой, что $N \neq 0$ и $N \neq M$ (т. е. $M/N \neq 0$). Говорят, что модуль $M$ является расширением модуля $L = M/N$ с ядром $N$. В силу теоремы о гомоморфизме это равносильно существованию некоторого эпиморфизма $M \twoheadrightarrow L$ с ядром $N$.

Если сами модули $L$ и $N$ не просты то в $L$ можно выбрать нетривиальный подмодуль $L_1$, а в $N$ — нетривиальный подмодуль $N_1$. В силу теоремы 4.3 $L_1 \simeq N_2/N$, где $N_2$ — подмодуль в $M$, содержащий $N$. В результате в $M$ возникает такая цепочка подмодулей: $M \supset N_2 \supset N \supset N_1 \supset 0$. Если в этой цепочке модуль $N_1$ или какой-либо из фактормодулей $M/N_2$, $N_2/N$, $N/N_1$ еще не просты, то в нее можно тем же способом вставить еще один подмодуль. Из-за конечномерности пространства $M$ этот процесс не может продолжаться неограниченно. Значит, в конце концов мы придем к такой цепочке: $M = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_{s-1} \supset M_s = 0$, у которой все фактормодули $M_i/M_{i+1}$ уже просты. Такая цепочка называется композиционным рядом модуля $M$. Фактормодули $M_i/M_{i+1}$ называются факторами этого ряда, а их число $s$ — длиной ряда.

Можно сказать, что факторы композиционного ряда — это «кирпичи», из которых модуль $M$ строится последовательными расширениями. Конечно, эти факторы не определяют, вообще говоря, модуль $M$, но они несут довольно большую информацию о его строении. Естественно возникает вопрос, насколько однозначно определяются они по модулю $M$. Ответ на него дает следующая важная теорема.

**Теорема 5.1** (Жордан — Гёльдер). *Если* $M = M_0 \supset M_1 \supset \ldots \supset M_s = 0$ *и* $M = N_0 \supset N_1 \supset \ldots \supset N_t = 0$ — *два композиционных ряда, то их длины равны и между факторами этих рядов можно установить взаимно однозначное соответствие так, что соответствующие факторы будут изоморфны.*

Доказательство будем проводить индукцией по $s$. Если $s = 1$, то модуль $M = M_0/M_1$ прост. Поэтому $t = 1$ и $N_0/N_1 = M = M_0/M_1$. Предположим, что $s > 1$ и для рядов длины $s - 1$ теорема уже доказана.

Если $M_1 = N_1$, то $M_0/M_1 = N_0/N_1$ и теорема сразу следует из индукционного предположения. Если же $M_1 \neq N_1$, то $M_1 + N_1 \neq$

$\neq M_1$ и, так как между $M$ и $M_1$ промежуточных подмодулей нет, $M_1 + N_1 = M$ и по закону параллелограмма

$$M_1/M_1 \cap N_1 \simeq M/M_1; \qquad M_1/M_1 \cap N_1 \simeq M/N_1.$$

Построим композиционный ряд в модуле $M_1 \cap N_1$

$$M_1 \cap N_1 = L_2 \supset L_3 \supset \ldots \supset L_k = 0.$$

Тогда $M_1 \supset L_2 \supset \ldots \supset L_k = 0$ — композиционный ряд в $M_1$. Сравнивая его с рядом $M_1 \supset M_2 \supset \ldots \supset M_s = 0$, получаем, по предположению индукции, что $s = k$ и что при некотором взаимно однозначном соответствии факторы этих рядов попарно изоморфны.

Сравним теперь ряды $M \supset M_1 \supset L_2 \supset \ldots \supset L_s = 0$ и $M \supset N_1 \supset L_2 \supset \ldots \supset L_s = 0$. Начиная с третьего места, их факторы совпадают, а изоморфизмы $M/M_1 \simeq N_1/L_2$ и $M/N_1 \simeq M_1/L_2$ были установлены выше. Значит, все факторы этих рядов попарно изоморфны.

Наконец, сравнивая ряды $N_1 \supset L_2 \supset \ldots \supset L_s = 0$ и $N_1 \supset N_2 \supset \ldots \supset N_t = 0$, мы по предположению индукции получаем, что $s = t$ и факторы этих рядов попарно изоморфны. Значит, факторы исходных рядов также попарно изоморфны (при некотором взаимно однозначном соответствии). Теорема полностью доказана.

Длина композиционного ряда называется д л и н о й м о д у л я $M$ и обозначается $l(M)$, а факторы композиционного ряда называются п р о с т ы м и ф а к т о р а м и м о д у л я $M$. В силу теоремы Жордана—Гельдера, определение длины и простых факторов не зависит от выбора ряда.

Отметим, что порядок следования простых факторов в композиционном ряду определен, вообще говоря, неоднозначно. Например, для полупростых модулей, которые будут рассматриваться в следующей главе, он вообще произволен.

**Следствие** 5.2. *Если модуль $M$ является расширением модуля $L$ с ядром $N$, то $l(M) = l(N) + l(L)$.*

Д о к а з а т е л ь с т в о. Проведем композиционный ряд в модуле $L \simeq M/N : L = L_0 \supset L_1 \supset \ldots \supset L_k = 0$ и возьмем в $M$ прообразы $M_i$ модулей $L_i$. Тогда, по теореме 4.3, $M_i/M_{i+1} \simeq L_i/L_{i+1}$ — простые модули. Построим теперь композиционный ряд в модуле $N$ $N = N_0 \supset N_1 \supset \ldots \supset N_t = 0$. Тогда

$$M = M_0 \supset M_1 \supset \ldots \supset M_k = N = N_0 \supset N_1 \supset \ldots \supset N_t = 0$$

есть композиционной ряд в модуле $M$ длины $k + t$, что и доказывает утверждение.

**Следствие** 5.3 (формула Грассмана). *Если $L$ и $N$ — подмодули в $M$, то*

$$l(L + N) + l(L \cap N) = l(L) + l(N).$$

Д о к а з а т е л ь с т в о непосредственно вытекает из следствия 5.2 и закона параллелограмма.

Говорят, что подмодуль $N$ модуля $M$ максимален, если $N \neq M$ и не существует подмодуля $L$, отличного от $M$ и $N$, такого, что $M \supset L \supset N$. Очевидно, это равносильно тому, что фактормодуль $M/N$ прост. В композиционном ряду каждый следующий подмодуль максимален в предыдущем.

## § 6. Прямые суммы

Знание подмодуля и фактормодуля дает довольно большую информацию о строении всего модуля. Особенно понятным это становится, если посмотреть на матричную запись соответствующего представления (формула (1) § 4). Однако стоящая в левом нижнем углу матриц «склейка» $X(a)$, вообще говоря, не определяется подмодулем и фактормодулем и может быть устроена весьма сложно.

Наиболее приятен, конечно, случай, когда дополнительная информация, вносимая склейкой, отсутствует, т. е. $X(a) = 0$ и представление имеет вид

$$T(a) = \begin{pmatrix} T_1(a) & 0 \\ 0 & T_2(a) \end{pmatrix}. \tag{1}$$

Такие представления (и все им подобные) называются разложимыми.

На модульном языке понятие разложимого представления приводит к определению прямой суммы модулей.

Пусть $M_1, M_2, \ldots, M_n$ — модули над алгеброй $A$. Рассмотрим множество $M$ наборов $(m_1, \ldots, m_n)$, где $m_i \in M_i$, и введем в нем операции покоординатно

$$(m_1, \ldots, m_n) + (m_1', \ldots, m_n') = (m_1 + m_1', \ldots, m_n + m_n'),$$

$$\alpha(m_1, \ldots, m_n) = (\alpha m_1, \ldots, \alpha m_n), \quad \alpha \in K,$$

$$(m_1, \ldots, m_n)\, a = (m_1 a, \ldots, m_n a), \quad a \in A.$$

Очевидно, тем самым $M$ превращается в $A$-модуль, который называется прямой суммой модулей $M_1, \ldots, M_n$ и обозначается $M_1 \oplus \ldots \oplus M_n$ или $\bigoplus_{i=1}^{n} M_i$. Как векторное пространство $M$ — это прямая сумма пространств $M_1, \ldots, M_n$.

Если $n = 2$, а $\{e_1, \ldots, e_k\}$ и $\{f_1, \ldots f_l\}$ — базисы, соответственно, в $M_1$ и $M_2$, то легко проверить, что $\{(e_1, 0), \ldots, (e_k, 0), (0, f_1), \ldots, (0, f_l)\}$ — базис в $M_1 \oplus M_2$ и соответствующее представление имеет вид (1), где $T_1(a)$ и $T_2(a)$ — представления, соответствующие $M_1$ и $M_2$.

Модуль $M$, изоморфный $M_1 \oplus M_2$, где $M_1$ и $M_2$ — ненулевые модули, называется разложимым. Мы дадим внутреннюю характеристику разложимых модулей.

Пусть $N$ и $L$ — два подмодуля модуля $M$. Определим отображение $f: N \oplus L \to M$, положив $f(x, y) = x + y$, где $x \in N$, $y \in L$. Тривиально проверяется, что $f$ есть гомоморфизм, а $\operatorname{Im} f = L + N$. Вычислим $\operatorname{Ker} f$.

Если $(x, y) \in \operatorname{Ker} f$, то $x + y = 0$, т. е. $x = -y$. Поэтому $x \in N \cap L$. Наоборот, если $x \in N \cap L$, то элемент $(x, -x)$ модуля $N \oplus L$ лежит в $\operatorname{Ker} f$. Итак, $\operatorname{Ker} f \simeq N \cap L$, откуда следует такое предложение.

**Предложение 6.1.** *Гомоморфизм $f : N \oplus L \to M$ ($N$, $L$ — подмодули в $M$), определенный формулой $f(x, y) = x + y$, есть изоморфизм тогда и только тогда, когда $N + L = M$, а $N \cap L = 0$.*

Если эти условия выполнены, говорят, что $M$ разлагается в прямую сумму своих подмодулей $N$ и $L$, и пишут $M = N \oplus L$. Подмодуль $L$ в этом случае называется дополнением подмодуля $N$ (и наоборот). Говорят также, что подмодуль $N$ выделяется прямым слагаемым из модуля $M$.

Один и тот же подмодуль в $M$ может иметь различные дополнения (даже в простейшем случае, когда $A = K$, т. е. модули — это просто векторные пространства). Однако все дополнения изоморфны между собой: легко видеть, что каждое из них изоморфно фактормодулю $M/N$.

**Предложение 6.2.** *Следующие условия равносильны:*

1) *подмодуль $N$ модуля $M$ выделяется прямым слагаемым;*

2) *существует гомоморфизм $p : M \to N$, такой, что $p(x) = x$ для любого $x \in N$;*

3) *существует гомоморфизм $i : M/N \to M$, такой, что $i(y) \in y$ для любого класса $y \in M/N$.*

Доказательство. 1) $\Rightarrow$ 2). Если $M = N \oplus L$, то всякий элемент $m \in M$ однозначно представим в виде $m = x + y$, где $x \in N$, $y \in L$. Положим $p(m) = x$. Из однозначности сразу следует, что $p(m + m') = p(m) + p(m')$ для любого $m' \in M$, а $p(\alpha m) = \alpha p(m)$, $p(ma) = p(m)a$ для любых $\alpha \in K$, $a \in A$, т. е. $p$ — гомоморфизм. Если же $x \in N$, то $x = x + 0$, откуда $p(x) = x$.

2) $\Rightarrow$ 3). Определим значение $i$ на классе $\bar{m} = m + N$ по правилу $i(\bar{m}) = m - p(m)$. Если $m'$ — другой элемент из того же класса, то $m' = m + x$, где $x \in N$, откуда $m' - p(m') = m + x - p(m) - p(x) = m - p(m)$, т. е. наше определение не зависит от выбора представителя в классе $\bar{m}$. Легко проверить, что $i$ — гомоморфизм, причем, так как $p(m) \in N$, $i(\bar{m}) \in m + N = \bar{m}$.

3) $\Rightarrow$ 1). Обозначим $L = \operatorname{Im} i$. Поскольку $i(\bar{m}) \in \bar{m}$, где $\bar{m} = m + N$, $m - i(\bar{m}) \in N$, и запись $m = (m - i(\bar{m})) + i(\bar{m})$ показывает, что $N + L = M$. Если же $x \in N \cap L$, то $x = i(y)$, где $y = x + N = N$, т. е. $y = 0$ в $M/N$, и потому $x = 0$. Итак, $N \cap L = 0$ и $M = N \oplus L$.

Гомоморфизм $p$ часто называют проектором на подмодуль $N$. Как и дополнение, проектор определен неоднозначно.

Прямая сумма нескольких модулей также допускает внутреннюю трактовку.

**Теорема 6.3.** *Пусть $M_1, \ldots, M_k$ — подмодули модуля $M$, $f : M_1 \oplus \ldots \oplus M_k \to M$ — гомоморфизм, определенный формулой*

$f(m_1, \ldots, m_k) = m_1 + m_2 + \ldots + m_k$. *Тогда следующие условия равносильны:*

1) $f$ — *изоморфизм*;

2) $M_1 + \ldots + M_k = M$ *и* $M_i \cap \left(\sum_{j \neq i} M_j\right) = 0$ *для любого* $i$;

3) $M_1 + \ldots + M_k = M$ *и* $M_i \cap \left(\sum_{j<i} M_j\right) = 0$ *для любого* $i > 1$.

Доказательство. 1) $\Rightarrow$ 2). Эпиморфность $f$, очевидно, означает, что $M = M_1 + \ldots + M_k$. Далее, если $x \in M_i \cap \left(\sum_{j \neq i} M_j\right)$, то $x = \sum_{j \neq i} m_j$, где $m_j \in M_j$. Полагая $m_i = -x$, получаем $f(m_1, \ldots, m_k) = 0$, откуда ввиду мономорфности $f$ следует $m_1 = \ldots = m_k = 0$ и $x = 0$.

2) $\Rightarrow$ 3) очевидно.

3) $\Rightarrow$ 1). Из условия $M_1 + \ldots + M_k = M$ следует эпиморфность $f$. Далее, если $f(m_1, \ldots, m_k) = 0$ и $i$ — последний номер, для которого $m_i \neq 0$, то $m_i = -\sum_{j<i} m_j \in M_i \cap \left(\sum_{j<i} M_j\right)$, что невозможно. Поэтому $m_1 = \ldots = m_k = 0$ и $f$ — мономорфизм.

Если выполняются равносильные условия теоремы 6.3, то говорят, что модуль $M$ разлагается в прямую сумму подмодулей $M_1, \ldots, M_k$, и пишут $M = M_1 \oplus \ldots \oplus M_k$.

Внешнее и внутреннее определения прямой суммы равносильны: если $M = M_1 \oplus \ldots \oplus M_k$ — внешняя прямая сумма, то множество элементов $(0, \ldots, 0, m_i, 0, \ldots, 0)$ (все координаты, кроме $i$-й, равны 0) образует подмодуль $M_i'$ в модуле $M$, причем легко проверить, что $M_i' \simeq M_i$ и $M = M_1' \oplus \ldots \oplus M_k'$ (внутренняя прямая сумма).

Очевидно, всякий (конечномерный) модуль можно разложить в прямую сумму неразложимых модулей. В гл. III мы увидим, что такое разложение однозначно ( с точностью до изоморфизма и перестановки слагаемых). Поэтому если нам известны неразложимые модули над какой-либо алгеброй $A$, то мы можем описать все $A$-модули. Однако во многих случаях описание неразложимых модулей— это очень трудная задача, подчас недоступная известным в настоящее время методам.

### § 7. Эндоморфизмы. Пирсовское разложение

В этом параграфе мы докажем основные теоремы, устанавливающие связь теории представлений со структурной теорией алгебр. Эти результаты будут играть главную роль в последующих главах книги.

Напомним, что в § 2 мы определили действия над гомоморфизмами модулей и установили, что для любых двух $A$-модулей $M$ и $N$ множество $\mathrm{Hom}_A(M, N)$ можно рассматривать как векторное пространство над полем $K$. Особенно важным является тот случай, когда $M = N$. Гомоморфизмы из $\mathrm{Hom}_A(M, M)$ всегда можно пере-

множить. Значит, пространство $\mathrm{Hom}_A(M, M)$ превращается даже в $K$-алгебру. Эта алгебра называется алгеброй эндоморфизмов модуля $M$ и обозначается $E_A(M)$. Ее элементы (гомоморфизмы $M$ в себя) называются эндоморфизмами $M$. Обратимые элементы этой алгебры, т. е. изоморфизмы $M$ на $M$, называются автоморфизмами $M$.

Посмотрим, что дают введенные понятия в случае регулярного модуля. Пусть $f : A \to M$ — гомоморфизм регулярного модуля в произвольный модуль $M$. Тогда для любого элемента $a \in A$ $f(a) = f(1a) = f(1)\,a = m_0 a$, где $m_0 = f(1)$ — фиксированный элемент $M$. Наоборот, если зафиксировать произвольный элемент $m_0 \in M$ и положить $f(a) = m_0 a$, то, как легко проверить, мы получим гомоморфизм $f : A \to M$. Таким образом, мы установили взаимно однозначное соответствие между элементами $M$ и гомоморфизмами из $\mathrm{Hom}_A(A, M)$. Если $f$ и $g$ — два таких гомоморфизма, причем $f(1) = m_0$, $g(1) = m_1$, то $(f+g)(1) = m_0 + m_1$ и $(\alpha f)(1) = \alpha m_0$ для любого $K$. Следовательно, наше взаимно однозначное соответствие есть изоморфизм векторных пространств.

Пусть теперь $M = A$, $f$ и $g$ — эндоморфизмы $A$, причем $f(1) = a$, $g(1) = b$. Тогда $(fg)(1) = f(g(1)) = f(b) = f(1)\,b = ab$. Поэтому взаимно однозначное соответствие между $A$ и $E_A(A)$ есть изоморфизм алгебр.

Итак, мы доказали такую теорему.

**Теорема 7.1.** *Соответствие $f \to f(1)$ есть изоморфизм векторных пространств $\mathrm{Hom}_A(A, M)$ и $M$. Если $M = A$, это соответствие является изоморфизмом алгебр $E_A(A)$ и $A$.*

Алгебра эндоморфизмов — это подалгебра в алгебре всех линейных преобразований пространства $M$. Она состоит из тех преобразований, которые перестановочны со всеми преобразованиями $T(a)$, $a \in A$, где $T$ — представление, определенное модулем $M$. Таким образом, алгебра $E_A(M)$ возникает вместе с некоторым своим точным представлением (вернее, антипредставлением, поскольку эндоморфизмы мы договорились записывать слева от элементов, а линейные преобразования — справа). Соответствующий левый модуль естественно отождествить с векторным пространством $M$, на котором эндоморфизмы действуют по правилу: $fm = f(m)$ (значение $f$ на элементе $m \in M$).

Итак, каждый $A$-модуль $M$ можно рассматривать как левый модуль над алгеброй $E_A(M)$. Нетрудно проверить, что если $M = A$ — регулярный модуль, то соответствующий левый модуль над алгеброй $E_A(A) \simeq A$ есть просто левый регулярный модуль.

Аналогичные рассуждения справедливы и для левых модулей. При этом гомоморфизмы левых модулей удобно записывать справа от элементов. Образ $m$ при гомоморфизме $f$ будем обозначать через $mf$; соответственно, произведение $fg$ определим по правилу $m(fg) = (mf)g$. В таких обозначениях левый $A$-модуль превращается в правый модуль над своей алгеброй эндоморфизмов. Имеет место также аналог теоремы 7.1.

Как же связано строение алгебры эндоморфизмов со строением самого модуля, в частности с разложениями в прямую сумму?

Пусть $M$ разлагается в прямую сумму своих подмодулей $M = M_1 \oplus \ldots \oplus M_s$. Это означает, что всякий элемент $m \in M$ однозначно представим в виде суммы $m = m_1 + \ldots + m_s$, где $m_i \in M_i$. Обозначим $m_i = e_i m$. Из однозначности сразу следует, что $e_i(m + n) = e_i m + e_i n$, $e_i(\alpha m) = \alpha e_i(m)$ и $e_i(ma) = (e_i m)a$ для любых элементов $m, n \in M$; $\alpha \in K$; $a \in A$, т. е. $e_i$ — эндоморфизм $M$. Кроме того, если $m \in M_i$, то $e_i m = m$, а $e_j m = 0$ при $j \neq i$, откуда следует, что $e_j e_i = \delta_{ij} e_i$, где $\delta_{ij}$ — символ Кронекера ($\delta_{ij} = 1$ при $i = j$ и $\delta_{ij} = 0$ при $i \neq j$). Наконец, из определения $e_i$ вытекает, что $m = e_1 m + \ldots + e_s m$, т. е. $e_1 + \ldots + e_s = 1$.

Элемент $e$ алгебры $A$ называется идемпотентом, если $e^2 = e$. Два идемпотента $e$ и $f$, такие, что $ef = fe = 0$, называются ортогональными. Равенство $1 = e_1 + \ldots + e_s$, где $e_1, \ldots, e_s$ — попарно ортогональные идемпотенты, будем называть разложением единицы алгебры $A$.

**Теорема 7.2.** *Существует взаимно однозначное соответствие между разложениями $A$-модуля $M$ в прямую сумму подмодулей и разложениями единицы алгебры $E = E_A(M)$.*

Доказательство. Мы уже сопоставили всякому разложению модуля $M$ разложение единицы алгебры $E$. Пусть теперь $1 = e_1 + \ldots + e_s$ — разложение единицы алгебры $E$. Положим $M_i = \operatorname{Im} e_i$. Для любого элемента $m \in M$ тогда $m = (e_1 + \ldots + e_s)m = e_1 m + \ldots + e_s m$, причем $e_i m \in M_i$. Если $m = m_1 + \ldots + m_s$ — какое-нибудь представление элемента $m$ в виде суммы элементов $m_i \in M_i$, то $m_i = e_i x_i$ для некоторого $x_i \in M$. Поэтому

$$e_i m = \sum_{j=1}^{s} e_i m_j = \sum_{j=1}^{s} e_i e_j x_j = e_i x_i = m_i$$

(ввиду ортогональности идемпотентов $e_i$ и $e_j$ при $i \neq j$). Следовательно, такое представление однозначно, т. е. $M = M_1 \oplus \ldots \oplus M_s$.

**Следствие 7.3.** *Модуль $M$ неразложим тогда и только тогда, когда в алгебре $E_A(M)$ нет нетривиальных (т. е. отличных от 0 и 1) идемпотентов.*

Доказательство следует из того, что если $e$ — нетривиальный идемпотент, то $f = 1 - e$ — также нетривиальный идемпотент, ортогональный к $e$, а тогда $1 = e + f$ есть разложение единицы.

Сравнивая теоремы 7.1 и 7.2, получаем такое следствие.

**Следствие 7.4.** *Существует взаимно однозначное соответствие между разложениями модуля $M$ и разложениями регулярного модуля над алгеброй $E_A(M)$.*

Заметим, что если $1 = e_1 + \ldots + e_s$ — разложение единицы алгебры $A$, то соответствующее разложение регулярного $A$-модуля имеет вид $A = e_1 A \oplus \ldots \oplus e_s A$. Это разложение называется правым пирсовским разложением алгебры $A$. Анало-

гично определяется левое пирсовское разложение: $A = Ae_1 \oplus \ldots \oplus Ae_s$ (это есть разложение левого регулярного модуля).

Более того, если $M$ — произвольный $A$-модуль, то данное разложение единицы алгебры $A$ индуцирует разложение $M$ как векторного пространства $M = Me_1 \oplus \ldots \oplus Me_s$. Поскольку $f(me_i) = (fm)e_i$ для всякого эндоморфизма $f \in E_A(M)$, это разложение является даже разложением $M$ как левого $E_A(M)$-модуля (но, вообще говоря, оно не является разложением $M$ как $A$-модуля). Мы будем называть это разложение пирсовским разложением модуля $M$.

Слагаемые $e_iA$ правого пирсовского разложения алгебры $A$ являются правыми идеалами, т. е. $A$-модулями. Применяя к ним пирсовское разложение модулей, мы получаем такое разложение векторного пространства $A$:

$$A = \bigoplus_{i,j=1}^{s} e_iAe_j. \tag{1}$$

Это разложение называется двусторонним пирсовским разложением, или просто пирсовским разложением алгебры $A$. Компоненты пирсовского разложения $A_{ij} = e_iAe_j$, вообще говоря, уже не являются ни правыми, ни левыми идеалами. Тем не менее, это разложение дает удобную интерпретацию элементов алгебры $A$ в виде некоторых матриц.

Пусть $a$ и $b$ — два произвольных элемента алгебры $A$. Разложим их согласно пирсовскому разложению (1): $a = \sum_{i,j} a_{ij}$, $b = \sum_{i,j} b_{ij}$, где $a_{ij} = e_iae_j$, $b_{ij} = e_ibe_j$. Тогда $a + b = \sum_{i,j} (a_{ij} + b_{ij})$, а

$$ab = \sum_{i,k} \sum_{l,j} a_{ik}b_{lj} = \sum_{i,j} \left( \sum_{k} a_{ik}b_{kj} \right),$$

поскольку при $k \neq l$ $a_{ik}b_{lj} = e_iae_ke_lbe_j = 0$. Таким образом, $e_i(ab)e_j = \sum_k a_{ik}b_{kj}$. Это дает возможность записать элемент $a$ в виде матрицы из его пирсовских компонент

$$a = \begin{pmatrix} a_{11} & \ldots & a_{1s} \\ \ldots & \ldots & \ldots \\ a_{s1} & \ldots & a_{ss} \end{pmatrix}, \quad a_{ij} = e_iae_j \in A_{ij}. \tag{2}$$

Как мы только что видели, сложение и умножение элементов при этом перейдет в сложение и умножение матриц, определенные обычным образом. В дальнейшем мы часто будем пользоваться такой

записью. В частности, пирсовское разложение (1) мы будем записывать в виде

$$A=\begin{pmatrix} A_{11} & \dots & A_{1s} \\ \dots & \dots & \dots \\ A_{s1} & \dots & A_{ss} \end{pmatrix}.$$

Применим пирсовское разложение к алгебре эндоморфизмов модуля $M$, разложенного в прямую сумму $M = M_1 \oplus \dots \oplus M_s$. Пусть $1 = e_1 + \dots + e_s$ — соответствующее разложение единицы алгебры $E = E_A(M)$; $E_{ij} = e_i E e_j$. Пирсовское разложение элемента $f \in E$ имеет вид

$$f=\begin{pmatrix} f_{11} & \dots & f_{1s} \\ \dots & \dots & \dots \\ f_{s1} & \dots & f_{ss} \end{pmatrix}, \qquad f_{ij} = e_i f e_j.$$

Пусть $m = m_1 + \dots + m_s$ — произвольный элемент из $M$ ($m_i = e_i m$). Тогда

$$fm = \sum_{i,j} e_i f e_j m = \sum_{i,j} f_{ij} m_j,$$

т. е. если записать $m$ в виде столбца из элементов $m_1, \dots, m_s$, то

$$fm=\begin{pmatrix} f_{11} & \dots & f_{1s} \\ \dots & \dots & \dots \\ f_{s1} & \dots & f_{ss} \end{pmatrix}\begin{pmatrix} m_1 \\ \vdots \\ m_s \end{pmatrix},$$

где умножение будем понимать по-прежнему в обычном матричном смысле.

Заметим, что $f_{ij}m$ всегда лежит в $M_i$. Кроме того, значение $f_{ij}m$ однозначно определяется компонентой $m_j = e_j m$, так как $f_{ij}m = f_{ij}m_j$. Поэтому $f_{ij}$ естественно интерпретировать как гомоморфизм $M_j \to M_i$. Наоборот, если $g : M_j \to M_i$ — любой гомоморфизм, можно определить гомоморфизм $\bar{g} : M \to M$ по правилу $\bar{g}m = gm_j$ (где $m_j = e_j m$), и, очевидно, $\bar{g}$ будет лежать в $E_{ij}$. Следовательно, $E_{ij} \simeq \mathrm{Hom}_A(M_j, M_i)$, и мы всегда будем отождествлять $E_{ij}$ и $\mathrm{Hom}_A(M_j, M_i)$ при помощи этого изоморфизма.

В частности, возвращаясь к регулярному $A$-модулю, мы видим, что для любого разложения единицы $1 = e_1 + \dots + e_s$ алгебры $A$ компоненты пирсовского разложения $A_{ij} = e_i A e_j$ естественно отождествляются с $\mathrm{Hom}_A(e_j A, e_i A)$, причем это отождествление согласовано с матричной записью (2) элементов алгебры.

Наконец, интересный результат получается, если все слагаемые $M_1, \dots, M_s$ изоморфны между собой: $M_1 \simeq \dots \simeq M_s \simeq L$. В этом случае мы будем писать $M \simeq sL$. Очевидно, тогда $E_{ij} \simeq$

$\simeq E_A(L)$, и матричная запись эндоморфизмов приводит к такому выводу.

**Теорема 7.5.** *Если $M \simeq sL$, то алгебра $E_A(M)$ изоморфна алгебре матриц размерности $s$ с коэффициентами из $E_A(L)$.*

В дальнейшем алгебру матриц размерности $n$ с коэффициентами из некоторой алгебры $A$ мы будем обозначать $M_n(A)$.

**Следствие 7.6.** $M_n(A) \simeq E_A(nA)$.

В заключение рассмотрим связь идемпотентов с прямыми произведениями алгебр.

Пусть $A = A_1 \times \ldots \times A_k$. Положим $e_i = (0, \ldots, 1, \ldots, 0)$ (на $i$-м месте — единица алгебры $A_i$, на остальных — нули). Очевидно, $e_1, \ldots, e_k$ — попарно ортогональные идемпотенты и $1 = e_1 + \ldots + e_k$. Однако идемпотенты $e_i$ обладают дополнительным свойством — все они лежат в центре алгебры, т. е. $e_i a = ae_i$ для любого $a \in A$.

Идемпотенты, лежащие в центре, называются центральными. Если в разложении единицы все идемпотенты центральны, то само разложение называется центральным.

Для всякого центрального разложения единицы $1 = e_1 + \ldots + e_k$, конечно, $e_iA = Ae_i = e_iAe_i$, а $e_iAe_j = e_ie_jA = 0$ при $i \neq j$. Таким образом, правое, левое и двустороннее пирсовские разложения в этом случае совпадают, а их компоненты являются идеалами алгебры $A$.

**Теорема 7.7.** *Существует взаимно однозначное соответствие между:*

1) *разложениями алгебры $A$ в прямое произведение алгебр;*
2) *центральными разложениями единицы алгебры $A$;*
3) *разложениями $A$ в прямую сумму идеалов.*

Доказательство. Мы уже построили по всякому разложению в прямое произведение центральное разложение единицы, а по нему — разложение в прямую сумму идеалов.

Наоборот, пусть $A = I_1 \oplus \ldots \oplus I_k$, где $I_i$ — идеалы, и $1 = e_1 + \ldots + e_k$ — соответствующее разложение единицы. Тогда $I_i = e_iA$, поэтому $e_iae_j \in I_i \cap I_j$ для любого $a \in A$, откуда следует, что $e_iae_j = 0$, т. е. $e_iAe_j = 0$ при $i \neq j$, и пирсовское разложение имеет вид

$$A = \begin{pmatrix} A_1 & & & 0 \\ & A_2 & & \\ & & \ddots & \\ 0 & & & A_k \end{pmatrix},$$

где $A_i = e_iAe_i = e_iA$. Но тогда $A \simeq A_1 \times \ldots \times A_k$, что и требовалось доказать.

**Следствие 7.8.** *Существует взаимно однозначное соответствие между разложениями в прямое произведение алгебры $A$ и ее центра.*

Из доказательства теоремы 7.7 видно, что разложение единицы $1 = e_1 + \ldots + e_s$ центрально тогда и только тогда, когда $e_iAe_j =$

$= 0$ при $i \neq j$. Учитывая интерпретацию пирсовских компонент для алгебры эндоморфизмов, мы получаем такой результат.

**Следствие 7.9.** *Если* $M = M_1 \oplus \ldots \oplus M_s$, *причем* $\mathrm{Hom}_A(M_j, M_i) = 0$ *при* $i \neq j$, *то* $E_A(M) \simeq E_A(M_1) \times \ldots \times E_A(M_s)$.

## *Упражнения к главе I*

**1.** Вычислить регулярное матричное представление поля **C** комплексных чисел и алгебры **H** кватернионов (над полем вещественных чисел) в естественных базисах ($\{1, i\}$ для **C** и $\{1, i, j, k\}$ для **H**).

**2.** Используя регулярное представление, доказать, что алгебра кватернионов есть тело.

**3.** Пусть $A$ — алгебра над полем комплексных чисел с базисом $\{e, i, j, k\}$ и такой же таблицей умножения, как в алгебре кватернионов. Найти в алгебре $A$ делители нуля. Установить изоморфизм $A \simeq M_2(\mathbf{C})$.

**4.** Найти центр и идеалы алгебры $M_n(K)$.

**5.** Вычислить регулярное матричное представление жордановой алгебры $J_n(K)$, найти все ее идеалы.

**6.** Доказать, что всякая моногенная алгебра над алгебраически замкнутым полем изоморфна прямому произведению жордановых алгебр (Указание: использовать теорему Кэли и жорданову нормальную форму матриц.)

**7.** Пусть $M$ — числовое $n$-мерное пространство, рассматриваемое как модуль над алгеброй $A = T_n(K)$ треугольных матриц (в соответствующем представлении матрице $X$ сопоставляется она сама).

Найти подмодули модуля $M$ и соответствующие представления. Построить в $M$ композиционный ряд. Показать, что модуль $M$ неразложим. Вычислить $E_A(M)$.

**8.** Доказать, что если $M_1, \ldots, M_k$ — подмодули в $M$, $f$ — естественный гомоморфизм $M_1 \oplus \ldots \oplus M_k \to M$, определенный в § 6, то $\mathrm{Ker}\, f \simeq N_2 \oplus \ldots \oplus N_k$, где $N_i = M_i \cap \left(\sum_{j<i} M_j\right)$.

**9.** Пусть $M$ — циклический модуль над алгеброй $A$ с образующим $m$. Доказать, что $M \simeq A/\mathrm{Ann}\, m$. Проверить, что если $\mathrm{Ann}\, m$ — идеал в $A$ (например, если $A$ коммутативна), то $\mathrm{Ann}\, m = \mathrm{Ann}\, M$ и для любого образующего $m'$ $\mathrm{Ann}\, m' = \mathrm{Ann}\, m$.

Показать, что, если алгебра $A$ некоммутативна, $\mathrm{Ann}\, m$ может зависеть от выбора образующего $m$. (Указание: в качестве $A$ взять $M_n(K)$, а в качестве $M$ — числовое $n$-мерное пространство.)

**10** (пирсовское разложение идеала). Пусть $I$ — идеал в алгебре $A$, $1 = e_1 + \ldots + e_s$ — разложение единицы этой алгебры. Доказать, что элемент $a = \sum_{i,j} a_{ij}$ $(a_{ij} \in e_i A e_j)$ принадлежит $I$ тогда и только тогда, когда $a_{ij} \in e_i I e_j$.

**11.** Используя упражнение 10, описать идеалы алгебры треугольных матриц.

**12.** Пусть $A$ — алгебра, вообще говоря, без единицы, $\tilde{A}$ — алгебра, полученная присоединением единицы к $A$ (см. § 1)

$$\tilde{A} = \{(a, c) \mid a \in A, c \in K\}.$$

а) Доказать, что элементы вида $(a, 0)$ образуют в $\tilde{A}$ идеал, который изоморфен $A$ (как алгебра без единицы).

б) Отождествим $A$ с идеалом, построенным в п. а). Доказать, что всякий идеал алгебры $\tilde{A}$ содержится в $A$ (то же — для правых и левых идеалов).

в) Если в $A$ есть единица, показать, что $\tilde{A} \simeq A \times K$.

г) Доказать, что всякий гомоморфизм алгебр без единицы $f: A \to B$ однозначно продолжается для гомоморфизма $\tilde{f}: \tilde{A} \to \tilde{B}$ алгебр с единицей и всякий гомоморфизм алгебр с единицей $g: \tilde{A} \to \tilde{B}$ отображает $A$ в $B$. В частности, $A \simeq B$ тогда и только тогда, когда $\tilde{A} \simeq \tilde{B}$.

13. Определим представление алгебры без единицы $A$ как гомоморфизм $f: A \to E(V)$.

а) Дать определение модуля над алгеброй без единицы и установить связь между модулями и представлениями.

б) Пусть $M$ — модуль над алгеброй без единицы $A$. Положим $m(a, c) = ma + cm$ $(a \in A, c \in K)$. Показать, что тогда $M$ превращается в $\tilde{A}$-модуль.

в) Проверить, что для любых $A$-модулей $M$ и $N$ $\mathrm{Hom}_A(M, N) = \mathrm{Hom}_{\tilde{A}}(M, N)$, если $M$ и $N$ рассматривать как $\tilde{A}$-модули по правилу, определенному в п. б). В частности, $M = N$ как $A$-модули тогда и только тогда, когда $M \simeq N$ как $\tilde{A}$-модули.

# II

ГЛАВА

# ПОЛУПРОСТЫЕ АЛГЕБРЫ

Классическая теория полупростых алгебр — это, по-видимому, наиболее яркий пример того, как «модульные» методы дают возможность получать глубокие структурные результаты. В то же время полупростые алгебры и их представления играют важнейшую роль во многих разделах математики. В этой главе мы установим основные свойства полупростых алгебр и модулей над ними и докажем теорему Веддербёрна—Артина, которая дает полную классификацию таких алгебр. Основную роль при этом будут играть результаты гл. I (особенно § 7) и описание гомоморфизмов простых модулей — так называемая лемма Шура.

## § 1. Лемма Шура

Напомним, что ненулевой модуль $M$ называется простым, если в нем нет нетривиальных (т. е. отличных от 0 и $M$) подмодулей. Мы выяснили их значение в теории модулей: всякий модуль получается из простых последовательными расширениями. В то же время простые модули играют важную роль и в структурной теории, что во многом определяется следующими результатами.

**Теорема 1.1** (Шур). *Если $U$ и $V$ — простые $A$-модули, то всякий ненулевой гомоморфизм $f: U \to V$ есть изоморфизм.*

Доказательство следует из того, что $\mathrm{Ker}\, f$ и $\mathrm{Im}\, f$ — подмодули, соответственно, в $U$ и $V$, причем если $f \neq 0$, то $\mathrm{Ker}\, f \neq U$ и $\mathrm{Im} f \neq 0$, а потому $\mathrm{Ker}\, f = 0$ и $\mathrm{Im}\, f = V$, т. е. $f$ — моно- и эпиморфизм и, значит, изоморфизм.

**Следствие 1.2** (Шур). *Алгебра эндоморфизмов простого модуля есть тело.*

Действительно, всякий ненулевой элемент этой алгебры есть изоморфизм и потому обратим.

**Следствие 1.3.** *Регулярный $A$-модуль прост тогда и только тогда, когда алгебра $A$ есть тело.*

Доказательство следует из изоморфизма $A \simeq E_A(A)$ (теорема I.7.1) и того, что в теле нет нетривиальных правых идеалов.

Отметим, что обращение леммы Шура неверно: существуют непростые модули $M$, для которых $E_A(M)$ — тело (см. упражнение 7 гл. I).

## § 2. Полупростые модули и алгебры

Модуль $M$ называется полупростым, если он изоморфен прямой сумме простых модулей.

Полупростому модулю соответствует вполне приводимое представление, т. е. представление $T$ вида

$$T(a) = \begin{pmatrix} T_1(a) & & 0 \\ & T_2(a) & \\ & & \ddots \\ 0 & & T_n(a) \end{pmatrix},$$

где $T_i$ — неприводимые представления.

**Предложение 2.1.** *Следующие условия равносильны:*

1) *модуль $M$ полупрост;*

2) $M = \sum_{i=1}^{m} M_i$, *где $M_i$ — простые подмодули в $M$;*

3) *у всякого подмодуля $N \subset M$ есть дополнение;*

4) *у всякого простого подмодуля $N \subset M$ есть дополнение.*

Доказательство. 1) $\Rightarrow$ 2) по определению.

2) $\Rightarrow$ 3). Если $M = \sum_{i=1}^{m} M_i$, то тем более $M = N + \sum_{i=1}^{m} M_i$. Заметим теперь, что из простоты модуля $M_j$ следует, что либо $M_j \cap \left(N + \sum_{i=1}^{j-1} M_i\right) = 0$, либо $M_j \subset N + \sum_{i=1}^{j-1} M_j$. Опустив те $M_j$, для которых $M_j \subset N + \sum_{i=1}^{j-1} M_i$, мы получим такой набор подмодулей $N_k$, что $N + \sum_k N_k = M$ и $N_l \cap \left(N + \sum_{k<l} N_k\right) = 0$. Но тогда $M$ есть прямая сумма подмодулей $N$ и $N_k$ (теорема I.6.3) и $N' = \sum_k N_k$ — дополнение к $N$.

3) $\Rightarrow$ 4) очевидно.

4) $\Rightarrow$ 1) легко доказывается индукцией по длине $l(M)$ модуля $M$. Если $l(M) = 1$, то уже модуль $M$ прост. Пусть $l(M) > 1$ и $U$ —

простой подмодуль в $M$. Тогда $M = U \oplus U'$, где $U'$ — какое-нибудь дополнение к $U$ в $M$, а $l(M) = l(U) + l(U')$, т. е. $l(U') = l(M) - 1$. Если $N$ — простой подмодуль в $U'$ и $N'$ — его дополнение в $M$, то любой элемент $x \in U'$ представим в виде $x = n + n'$, где $n \in N$, $n' \in N'$, отсюда $n' = x - n \in N' \cap U'$. Таким образом, $U' = N \oplus (N' \cap U')$, т. е. в $U'$ всякий простой подмодуль имеет дополнение. По индукционному предположению $U' \simeq \simeq \bigoplus_{i=2}^{n} U_i$. Поэтому $M \simeq \bigoplus_{i=1}^{n} U_i$, где $U_1 = U$.

**Следствие 2.2.** *Всякий подмодуль и фактормодуль полупростого модуля полупрост.*

Доказательство. Пусть $N$ — подмодуль полупростого модуля $M$, $\pi : M \to M/N$ — проекция $M$ на фактормодуль. Если $M = \sum_{i=1}^{m} M_i$, где $M_i$ — простые модули, то $M/N = \sum_{i=1}^{m} \pi(M_i)$. Но $\pi(M_i)$ — фактормодуль $M_i$, поэтому либо $\pi(M_i) = 0$, либо $\pi(M_i) \simeq M_i$. Таким образом, $M/N$ — сумма простых подмодулей и потому полупрост.

Полупростота подмодуля $N$ следует из того, что если $N'$ — дополнение к $N$ в $M$, то $N \simeq M/N'$.

Если $M$ — полупростой модуль, $M = \bigoplus_{i=1}^{n} U_i$ — его разложение в прямую сумму простых подмодулей, то $M_j = \bigoplus_{i>j} U_i$ $(j = 0, 1, \ldots, n)$ — подмодули в $M$, причем $M_{j-1} \supset M_j$ и $M_{j-1}/M_j \simeq U_j$. Таким образом, $M = M_0 \supset M_1 \supset \ldots \supset M_n = 0$ — композиционный ряд в $M$, а $U_1, \ldots, U_n$ — его простые факторы. Тогда из теоремы Жордана — Гёльдера (I.5.1) следует такое предложение.

**Предложение 2.3.** *Если $M$ — полупростой модуль, $M \simeq U_1 \oplus \ldots \oplus U_n \simeq V_1 \oplus \ldots \oplus V_m$ — два разложения $M$ в прямую сумму простых модулей, то $n = m$ и при подходящей нумерации слагаемых $U_i \simeq V_i$ для всех $i$.*

Алгебра $A$ называется *полупростой*, если ее регулярный модуль полупрост. Простые подмодули регулярного правого (левого) $A$-модуля называются минимальными правыми (левыми) идеалами алгебры $A$.

Следующая лемма, вместе с предложением 2.1, дает возможность получить «внутреннюю» характеристику полупростых алгебр.

**Лемма 2.4** (Брауэр). *Если $I$ — минимальный правый идеал в алгебре $A$, то либо $I^2 = 0$, либо $I = eA$, где $e$ — идемпотент.*

Доказательство. Предположим, что $I^2 \neq 0$, т. е. в $I$ найдутся такие элементы, $x$ и $y$, что $xy \neq 0$. Тогда отображение $f : I \to I$, такое, что $f(a) = xa$, есть ненулевой гомоморфизм, и, поскольку $I$ — простой модуль, является изоморфизмом (теорема 1.1). Поэтому найдется элемент $e \in I$, для которого $x = xe$. Но в этом случае $xe = xe^2$, т. е. $f(e) = f(e^2)$, а значит, $e = e^2$, т. е.

$e$ — идемпотент. Наконец, $eA$ — ненулевой подмодуль в $I$, поэтому $I = eA$.

Правый (левый, двусторонний) идеал $I$ алгебры $A$ называется нильпотентным, если $I^m = 0$ для некоторого $m$.

**Следствие 2.5.** *Следующие условия равносильны:*

1) *алгебра $A$ полупроста;*

2) *всякий правый идеал в $A$ имеет вид $eA$, где $e$ — идемпотент*

3) *всякий ненулевой идеал в $A$ содержит ненулевой идемпотент;*

4) *в алгебре $A$ нет ненулевых нильпотентных идеалов;*

5) *в алгебре $A$ нет ненулевых нильпотентных правых идеалов.*

Доказательство. 1) $\Rightarrow$ 2). Если $I$ — правый идеал, то по предложению 2.1 $A = I \oplus I'$, где $I'$ — дополнение к $I$. Поэтому $I = eA$, где $1 = e + e'$ — соответствующее разложение единицы (теорема I.7.2).

2) $\Rightarrow$ 3) очевидно.

3) $\Rightarrow$ 4) следует из того, что если $e$ — ненулевой идемпотент, то $e^k = e \neq 0$ для любого $k$.

4) $\Rightarrow$ 5). Если $I \neq 0$ — нильпотентный правый идеал, то $AI$ — двусторонний идеал в $A$, причем $(AI)^m = AI^m$, поэтому и $AI$ нильпотентен.

5) $\Rightarrow$ 1). Если $I$ — простой подмодуль регулярного модуля, т. е. минимальный правый идеал алгебры $A$, то $I^2 \neq 0$ и по лемме 2.4 $I = eA$. Поэтому у $I$ есть дополнение $I' = (1 - e)A$ и по предложению 2.1 алгебра $A$ полупроста.

Заметим, что условия 3) и 4) следствия 2.5 симметричны относительно понятий «правый» и «левый». Поэтому «левая полупростота», т. е. полупростота левого регулярного модуля, эквивалентна полупростоте, и к условиям следствия 2.5 можно добавить все условия, которые получаются из них заменой слова «правый» на «левый».

Полученный критерий легко переформулировать в терминах элементов. Для этого сопоставим элементу $a \in A$ правый идеал $aA = \{ax | x \in A\}$ (правые идеалы такого вида называются главными) и выясним, что означает нильпотентность этого идеала. Всякий элемент из $(aA)^m$ есть сумма элементов вида $ax_1ax_2 \ldots ax_m$, где $x_1, \ldots, x_m$ — произвольные элементы алгебры. Поэтому $(aA)^m = 0$ тогда и только тогда, когда всякое произведение такого вида равно нулю. Иными словами, как только в произведении $a_1a_2 \ldots a_t$ элемент $a$ встречается $m$ раз, это произведение равно 0. Такие элементы называются существенно нильпотентными.

**Следствие 2.6.** *Алгебра $A$ полупроста тогда и только тогда, когда в ней нет ненулевых существенно нильпотентных элементов.*

**Следствие 2.7.** *Коммутативная алгебра полупроста тогда и только тогда, когда в ней нет нильпотентов (т. е. таких элементов $a \neq 0$, что $a^m = 0$).*

Действительно, в коммутативной алгебре всякий нильпотент, очевидно, существенно нильпотентен.

Заметим, что в некоммутативной алгебре могут быть нильпотенты, которые не существенно нильпотентны. Например, в матричной алгебре $M_2(K)$ матричная единица $e_{12}$ нильпотентна: $e_{12}^2 = 0$, но $e_{21}e_{12} = e_{22}$ — идемпотент, поэтому $e_{12}$ не существенно нильпотентен.

Нетрудно проверить, что в $M_2(K)$ существенно нильпотентных элементов, кроме нуля, нет (рекомендуем читателю убедиться в этом).

**Следствие 2.8.** *Центр полупростой алгебры полупрост.*

Доказательство следует из того, что для элементов центра нильпотентность, очевидно, равносильна существенной нильпотентности.

Наконец, из наших рассмотрений вытекает следующий важный критерий полупростоты, уже в терминах теории представлений.

**Теорема 2.9.** *Алгебра $A$ полупроста тогда и только тогда, когда у нее есть точный полупростой модуль* [2].

Доказательство. Необходимость нашего условия немедленно следует из того, что регулярный модуль точен. Покажем достаточность.

Пусть $M \oplus \overset{n}{\underset{i=1}{}} U_i$, где $U_i$ — простые $A$-модули, — точный модуль. Если $I \neq 0$ — идеал алгебры $A$, то из точности модуля $M$ следует, что $U_i I \neq 0$ для некоторого $i$. Но тогда $U_i I = U_i$, значит, $U_i I^m = U_i$. Поэтому $I^m \neq 0$ ни для какого $m$. По следствию 2.5 отсюда следует полупростота алгебры $A$.

## § 3. Векторные пространства и матрицы

Прежде чем переходить к общей теории полупростых алгебр и их представлений, мы рассмотрим векторные пространства и алгебры матриц над телами.

Пусть $D$ — (конечномерное) тело над $K$, $V$ — (конечномерный) левый $D$-модуль. $V$ называется (конечномерным) *векторным пространством* над телом $D$.

**Предложение 3.1.** *Векторное пространство — полупростой модуль. Всякий простой левый $D$-модуль изоморфен регулярному.*

Доказательство. Пусть $V$ — векторное пространство над $D$, $v_1$ — произвольный ненулевой элемент (вектор) из $V$. Гомоморфизм $f : D \to V$, переводящий $x \in D$ в $xv_1 \in V$, ненулевой, и потому $\operatorname{Ker} f = 0$ (поскольку регулярный левый $D$-модуль прост). Поэтому $Dv_1 = \operatorname{Im} f \simeq D$.

Если $V$ — простой модуль, то $V = Dv_1 \simeq D$. В противном случае найдется элемент $v_2 \notin Dv_1$. Тогда аналогично $Dv_2 \simeq D$, причем $Dv_1 + Dv_2$ строго содержит $Dv_1$. Продолжая этот процесс, мы в конце концов придем к равенству $V = \sum_{i=1}^{n} Dv_i$, где $Dv_i \simeq$

[2] Напомним, что модуль $M$ называется точным, если точно соответствующее представление, т. е. $\operatorname{Ann} M = 0$.

$\simeq D$ — простые модули. По предложению 2.1 $V$— полупростой модуль, что и требовалось доказать.

**Следствие 3.2.** *Всякое векторное пространство над телом $D$ изоморфно $nD$ (прямой сумме $n$ экземпляров регулярного модуля). Число $n$ при этом определено однозначно.*

Однозначность следует из того, что $n$ — это длина модуля $V$. Ее обычно называют р а з м е р н о с т ь ю векторного пространства $V$ и обозначают $[V : D]$. Очевидно, $[V : K] = [V : D]\,[D : K]$.

Согласно следствию I.7.6, алгебра эндоморфизмов $n$-мерного векторного пространства $V$ над телом $D$ изоморфна алгебре матриц $M_n(D)$ с коэффициентами из тела $D$. При этом само пространство $V$ естественно рассматривать как правый модуль над $M_n(D)$. В дальнейшем элементы $V$ мы будем отождествлять с «числовыми» векторами $(x_1, \ldots, x_n)$, $x_i \in D$. Тогда действие матриц на векторы — это обычное умножение вектора на матрицу.

**Предложение 3.3.** *Модуль $V$ над алгеброй $A = M_n(D)$ прост. Алгебра $M_n(D)$ полупроста.*

Д о к а з а т е л ь с т в о. Пусть $U$ — ненулевой $A$-подмодуль в $V$, $u = (u_1, \ldots, u_n)$ — ненулевой элемент из $U$. Предположим, для определенности, что $u_1 \neq 0$. Тогда всякий вектор $x = (x_1, \ldots, \ldots, x_n)$ можно представить в виде $x = uX$, где

$$X = \begin{pmatrix} u_1^{-1}x_1 & u_1^{-1}x_2 \ldots u_1^{-1}x_n \\ 0 & 0 \ldots 0 \\ \cdots & \cdots \\ 0 & 0 \ldots 0 \end{pmatrix}.$$

Поэтому $uA = V$, $A$-модуль $V$ прост и алгебра $M_n(D)$ полупроста по теореме 2.9.

Выпишем явное разложение регулярного $A$-модуля. Обозначим через $I_i$ правый идеал алгебры $M_n(D)$, состоящий из всех матриц вида

$$\begin{pmatrix} 0 & 0 \ldots 0 \\ \cdots & \cdots \\ x_1 & x_2 \ldots x_n \\ \cdots & \cdots \\ 0 & 0 \ldots 0 \end{pmatrix}$$

(ненулевой является $i$-я строка). Сопоставляя этой матрице элемент $(x_1, \ldots, x_n) \in V$, мы, очевидно, получим изоморфизм $I_i$ на $V$.

В дальнейшем мы будем обозначать через $e_{ij}$ м а т р и ч н ы е е д и н и ц ы, т. е. матрицы, у которых на $(ij)$-м месте стоит 1, а на остальных — 0. В частности, $1 = e_{11} + \ldots + e_{nn}$ — разложение единицы, причем $e_{ii}A = I_i$. Отсюда следует, что $E_A(V) \simeq \simeq e_{ii}Ae_{ii} \simeq D$.

**Предложение 3.4.** *Всякий модуль над алгеброй $A = M_n(D)$ полупрост. Всякий простой $A$-модуль изоморфен $V$, а регулярный $A$-модуль изоморфен $nV$.*

Доказательство. $A = I_1 \oplus \ldots \oplus I_n$ — разложение регулярного $A$-модуля, причем, как мы видели, $I_i \simeq V$. Если $M$ — произвольный $A$-модуль, $m$ — его ненулевой элемент, то $mI_i$ — либо нулевой модуль, либо изоморфен $I_i$, поскольку $I_i$ прост. Кроме того, $m = \sum_{i=1}^{n} me_{ii} \in \sum_{i=1}^{n} mI_i$, поэтому какой-то из модулей $mI_i$ ненулевой. Если сам модуль $M$ прост, то отсюда следует, что $M = mI_i \simeq V$. В противном случае аналогично доказательству предложения 3.1 мы представим $M$ в виде суммы простых подмодулей, что и завершает доказательство нашего утверждения.

**Следствие 3.5.** *Два модуля $M$ и $N$ над алгеброй $M_n(D)$ изоморфны тогда и только тогда, когда $[M : K] = [N : K]$.*

Доказательство. Если $M = mV$, а $N = kV$, то $[M : K] = m[V : K]$, а $[N : K] = k[V : K]$, т. е. $m = k$ тогда и только тогда, когда $[M : K] = [N : K]$.

**Предложение 3.6.** *В алгебре $A = M_n(D)$ нет идеалов, отличных от 0 и $A$.*

Доказательство. Пусть $I$ — ненулевой идеал в $A$, $X = (x_{ij})$ — ненулевая матрица из $I$, $x_{kl}$ — ненулевой элемент этой матрицы. Тогда $e_{ik}X \neq 0$ и лежит в $I_i \cap I$. Поэтому $I_i \cap I \neq 0$ и, ввиду простоты $I_i$, $I \supset I_i$ (для всех $i$!). Но тогда $I \supset \sum_{i=1}^{n} I_i = A$, что и требовалось доказать.

Алгебры, в которых нет идеалов, отличных от 0 и самой алгебры, называются простыми. Предложение 3.6 показывает, что алгебра $M_n(D)$ проста. В следующем параграфе мы увидим, что других (конечномерных) простых алгебр нет.

## § 4. Теорема Веддербёрна—Артина

Результаты § 7 гл. I и предыдущих параграфов гл. II дают возможность получить основные структурные теоремы полупростых алгебр.

Прежде всего из леммы Шура непосредственно следует описание коммутативных полупростых алгебр.

**Теорема 4.1** (Вейерштрасс—Дедекинд). *Коммутативная полупростая алгебра изоморфна прямому произведению полей. Наоборот, прямое произведение полей — полупростая алгебра.*

Доказательство. Пусть $A$ — коммутативная полупростая алгебра, $A = U_1 \oplus \ldots \oplus U_n$ — разложение регулярного $A$-модуля в прямую сумму простых, $1 = e_1 + \ldots + e_n$ — соответствующее разложение единицы. Из-за коммутативности все идемпотенты центральны. Тогда $A \simeq A_1 \times \ldots \times A_n$, где $A_i = e_iA \simeq E_A(U_i)$ (см. теорему I.7.7). По лемме Шура $A_i$ — тела, а поскольку они коммутативны — поля.

Наоборот, если $A \simeq A_1 \times \ldots \times A_n$, где $A_i$ — поля, то регулярный $A$-модуль имеет вид $A = U_1 \oplus \ldots \oplus U_n$, где $U_i$ — регулярный $A_i$-модуль, который прост.

**Следствие 4.2.** *Если поле $K$ алгебраически замкнуто, то всякая коммутативная полупростая $K$-алгебра изоморфна $K^n$.*

Общая структурная теорема получается комбинированием леммы Шура и матричной записи эндоморфизмов.

**Теорема 4.3** (Веддербёрн — Артин). *Всякая полупростая алгебра изоморфна прямому произведению матричных алгебр над телами. Наоборот, прямое произведение матричных алгебр над телами — полупростая алгебра.*

Доказательство. Пусть $A$ — полупростая алгебра, $A \simeq n_1U_1 \oplus \ldots \oplus n_sU_s$ — разложение регулярного $A$-модуля в прямую сумму простых, причем $U_i \not\simeq U_j$ при $i \neq j$. Полагая $n_iU_i = M_i$, мы получим разложение $A \simeq M_1 \oplus \ldots \oplus M_s$, причем $\mathrm{Hom}_A(U_i, U_j) = 0$ по теореме 1.1, а значит, и $\mathrm{Hom}_A(M_i, M_j) = 0$. Но тогда $A \simeq A_1 \times \ldots \times A_s$. где $A_i = E_A(M_i)$ (см. следствие I.7.9). Так как $M_i \simeq n_iU_i$, то из теоремы I.7.5 вытекает, что $A_i \simeq M_{n_i}(D_i)$, где $D_i = E_A(U_i)$ — тело (по лемме Шура).

Наоборот, если $A = A_1 \times \ldots \times A_s$, где $A_i = M_{n_i}(D_i)$, то регулярный $A$-модуль разлагается в прямую сумму $A = I_1 \oplus \ldots \oplus I_s$, где $I_i$ — регулярный $A_i$-модуль (см. теорему I.7.7). По предложению 3.4 $I_i$ — полупростые модули. Значит, и $A$ — полупростая алгебра.

**Следствие 4.4** (Молин). *Если поле $K$ алгебраически замкнуто, всякая полупростая $K$-алгебра изоморфна алгебре вида $M_{n_1}(K) \times \ldots \times M_{n_s}(K)$.*

**Следствие 4.5.** *Всякая простая $K$-алгебра изоморфна алгебре вида $M_n(D)$, где $D$ — тело.*

Доказательство. Мы уже видели, что $M_n(D)$ — простая алгебра. Наоборот, если алгебра $A$ проста, то единственный ненулевой идеал ее (сама $A$) содержит ненулевой идемпотент — 1, т. е алгебра полупроста (по следствию 2.5). Кроме того, $A$ должна быть неразложимой (в прямое произведение). Значит, $A \simeq M_n(D)$.

**Следствие 4.6.** *Всякая простая алгебра над алгебраически замкнутым полем $K$ изоморфна $M_n(K)$ для некоторого $n$.*

## § 5. Единственность разложения

Теорема Веддербёрна—Артина сопоставляет каждой полупростой алгебре $A$ набор $(D_1, \ldots, D_s; n_1, \ldots, n_s)$, где $D_i$ — тела, а $n_i$ — размерности матриц,

$$A \simeq M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s). \qquad (1)$$

Естественно возникает вопрос: однозначно ли определяются тела $D_i$ и размерности $n_i$? Мы покажем, что это так. Более того, само разложение (1) фактически однозначно.

Установим вначале общий результат, касающийся единственности разложения алгебр в прямые произведения.

**Теорема 5.1.** *Пусть $A \simeq A_1 \times \ldots \times A_s \simeq B_1 \times \ldots \times B_t$ — два разложения алгебры $A$ в прямое произведение неразложимых*

*алгебр,* $1 = e_1 + \ldots + e_s = f_1 + \ldots + f_t$ *— соответствующие центральные разложения единицы. Тогда* $s = t$ *и, при подходящей нумерации идемпотентов,* $e_i = f_i$ *и* $A_i \simeq B_i$ *для всех* $i$.

Доказательство. Ввиду теоремы 1.7.7 неразложимость $A_i \simeq e_iA$ и $B_i \simeq f_jB$ означает, что если $e_i = e_i' + e_i''$, $f_j = f_j' + f_j''$, где $e_i'$ и $e_i''$ (соответственно $f_j'$ и $f_j''$) — центральные ортогональные идемпотенты, то либо $e_i' = 0$, либо $e_i'' = 0$ (соответственно либо $f_j' = 0$, либо $f_j'' = 0$). Но, ввиду центральности $e_i$ и $f_j$, $e_if_j$ и $e_i - e_if_j$ — центральные ортогональные идемпотенты. Поэтому либо $e_if_j = 0$, либо $e_if_j = e_i$. Аналогично либо $e_if_j = 0$, либо $e_if_j = f_j$. Поскольку $e_i = e_i(f_1 + \ldots + f_t)$, найдется некоторый номер $j$, такой, что $e_if_j \neq 0$, т. е. $e_i = e_if_j = f_j$. Но такой номер может быть только один, так как при $k \neq j$ $e_if_k = f_jf_k = 0$. Отсюда, очевидно, следует, что $s = t$ и, при подходящей нумерации, $e_i = f_i$ для всех $i$. Тогда $A_i \simeq e_iA = f_iA \simeq B_i$.

Теперь мы можем установить единственность в теореме Веддербёрна — Артина.

**Теорема 5.2.** *Если* $A \simeq M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s) \simeq M_{k_1}(F_1) \times \ldots \times M_{k_t}(F_t)$, *где* $D_1, \ldots, D_s, F_1, \ldots, F_t$ *— тела, то* $s = t$ *и при подходящей нумерации* $n_i = k_i$ *и* $D_i \simeq F_i$ *для всех* $i$.

Доказательство. Поскольку в алгебре $M_n(D)$ нет идеалов, она неразложима. Поэтому из теоремы 5.1 сразу следует, что $s = t$ и при подходящей нумерации $M_{n_i}(D_i) \simeq M_{k_i}(F_i)$. Остается доказать, что если $A \simeq M_n(D) \simeq M_k(F)$, где $D$ и $F$ — тела, то $n = k$ и $D \simeq F$.

По предложению 3.4 у $A$ есть один простой модуль $V$, причем $A \simeq nV \simeq kV$, откуда $n = k$. Кроме того, $D \simeq E_A(V) \simeq F$, что завершает доказательство теоремы.

Простые алгебры $A_i = M_{n_i}(D_i)$ называются простыми компонентами полупростой алгебры $A$. В силу теоремы 5.2 они определены однозначно. Поэтому классификация полупростых алгебр полностью сводится к описанию конечномерных тел.

## § 6. Представления полупростых алгебр

Структурная теорема Веддербёрна — Артина вместе с результатами § 3 позволяет дать полное описание модулей над полупростыми алгебрами.

**Предложение 6.1.** *Пусть* $M$ *— модуль над алгеброй* $A = A_1 \times \ldots \times A_s$, $1 = e_1 + \ldots + e_s$ *— центральное разложение единицы алгебры* $A$. *Тогда* $M = \bigoplus_{i=1}^{s} Me_i$, *где* $Me_i$ *— модули над* $A_i$.

Доказательство. $Me_i$ — подмодуль в $M$, поскольку $e_i$ лежит в центре $A$. Далее $m = me_1 + \ldots + me_s$, и, кроме того, если $m = m_1 + \ldots + m_s$, где $m_i \in Me_i$, то $me_i = m_i$, т. е. это представление однозначно. Следовательно, $M = \bigoplus_{i=1}^{s} Me_i$. Но $Me_ie_j = 0$ при

$i \neq j$, поэтому $e_j A \subset \operatorname{Ann}(Me_i)$, т. е. $Me_i$ — модуль над $A/\bigoplus_{j \neq i} e_j A \simeq$ $\simeq A_i$, что и требовалось доказать.

**Теорема 6.2.** *Пусть $A$ — полупростая алгебра, $A_i \simeq M_{n_i}(D_i)$ — ее простые компоненты ($i = 1, \ldots, s$). Всякий $A$-модуль полупрост и однозначно представим в виде $\bigoplus_{i=1}^{s} k_i V_i$, где $V_i$ — простой $A_i$-модуль. В частности, простые $A$-модули находятся во взаимно однозначном соответствии с простыми компонентами алгебры $A$.*

Доказательство. В силу предложения 6.1 всякий $A$-модуль разлагается в прямую сумму $M_1 \oplus \ldots \oplus M_s$, где $M_i$ — уже $A_i$-модули. По предложению 3.4 $M_i \simeq k_i V_i$, что и доказывает теорему (единственность следует из предложения 2.3).

В теории представлений групп важную роль играет такое следствие из доказанной теоремы.

**Следствие 6.3.** *Пусть $T$ и $S$ — два представления полупростой алгебры $A$ над полем характеристики 0. Эти представления подобны тогда и только тогда, когда $\operatorname{tr} T(a) = \operatorname{tr} S(a)$ для любого $a \in A$*[3].

Доказательство. Если представления $T$ и $S$ подобны, то матрицы $T(a)$ и $S(a)$ подобны и потому имеют равные следы.

Наоборот, предположим, что $\operatorname{tr} T(a) = \operatorname{tr} S(a)$ для всех $a \in A$. Пусть $A = A_1 \times \ldots \times A_s$, где $A_i$ — простые компоненты $A$, $1 = e_1 + \ldots + e_s$ — центральное разложение единицы, $V_i$ — простые $A_i$-модули. Разложим модули $M$ и $N$, соответствующие представлениям $T$ и $S$: $M \simeq \bigoplus_{i=1}^{s} m_i V_i$; $N \simeq \bigoplus_{i=1}^{s} k_i V_i$. Если $v \in V_i$, то $ve_i = v$ и $ve_j = 0$ при $j \neq i$, откуда следует, что $\operatorname{tr} T(e_i) = m_i d_i$, а $\operatorname{tr} S(e_i) = k_i d_i$, где $d_i = [V_i : K]$. Поэтому из равенства следов вытекает $m_i = k_i$ для всех $i$, т. е. $M \simeq N$ и представления $T$ и $S$ подобны [4].

Теорема 6.2 дает возможность также вычислить алгебру эндоморфизмов модуля над полупростой алгеброй $A$. Для этого напомним, что если $V_i$ — простой модуль над алгеброй $A_i = M_{n_i}(D_i)$ (простой компонентой алгебры $A$), то $E_A(V_i) \simeq D_i$. Кроме того, по лемме Шура, $\operatorname{Hom}_A(V_i, V_j) = 0$ при $i \neq j$. Поэтому матричная запись эндоморфизмов дает и такой результат.

**Теорема 6.4.** *Если $M$ — модуль над полупростой алгеброй $A$, то алгебра $E_A(M)$ также полупроста. Точнее, если $M = \bigoplus_{i=1}^{s} k_i V_i$, где $V_i$ — простой модуль над простой компонентой $A_i = M_{n_i}(D_i)$ алгебры $A$, то $E_A(M) \simeq E_1 \times \ldots \times E_s$, где $E_i \simeq M_{k_i}(D_i)$.*

---

[3] $\operatorname{tr} X$ обозначает след матрицы $X$: если $X = (x_{ij})$, то $\operatorname{tr} X = x_{11} + \ldots + x_{nn}$.

[4] Как видно из доказательства, достаточно требовать совпадения следов только для элементов центра.

Полупростые алгебры $A$ и $B$ называются о д н о т и п н ы м и, если у них поровну простых компонент, а соответствующие тела изоморфны.

**Следствие 6.5.** *Алгебры $A$ и $B$ однотипны тогда и только тогда, когда $B \simeq E_A(M)$, где $M$ — точный $A$-модуль.*

Д о к а з а т е л ь с т в о следует из теоремы 6.4 и того факта, что точность модуля $M = \bigoplus_{i=1}^{s} k_i V_i$ означает, что $k_i > 0$ для всех $i$.

**Следствие 6.6.** *Если $M$ — полупростой модуль над произвольной алгеброй $A$, то $E_A(M)$ — полупростая алгебра.*

Действительно, $E_A(M) = E_{\bar{A}}(M)$, где $\bar{A} = A/\mathrm{Ann}\, M$. Но $M$ — точный $\bar{A}$-модуль, поэтому $\bar{A}$, а значит, и $E_{\bar{A}}(M)$ — полупростые алгебры (теорема 2.9).

В заключение выведем из полученных результатов так называемую т е о р е м у п л о т н о с т и для полупростых модулей.

**Теорема 6.7** (Бернсайд). *Пусть $M$ — полупростой модуль над некоторой алгеброй $A$, $B = E_A(M)$, $\bar{A} = E_B(M)$ (здесь $M$ рассматривается как левый $B$-модуль). Сопоставим каждому элементу $a \in A$ эндоморфизм $\bar{a} \in \bar{A}$, полагая $x\bar{a} = xa$. Тогда отображение $a \to \bar{a}$ есть эпиморфизм алгебр.*

Д о к а з а т е л ь с т в о. Не меняя алгебр $B$ и $\bar{A}$, мы можем заменить $A$ на $A/\mathrm{Ann}\, M$. Но если $a \in \mathrm{Ann}\, M$, то $\bar{a} = 0$. Поэтому можно считать, что $M$ — точный модуль. Тогда алгебра $A$ полупроста (по теореме 2.9). В этом случае из $a \neq 0$ следует $\bar{a} \neq 0$, и надо проверить, что так построенное отображение изоморфно.

Пусть $A = A_1 \times \ldots \times A_s$, где $A_i \simeq M_{n_i}(D_i)$, а $M = \bigoplus_{i=1}^{s} k_i V_i$, где $V_i$ — простой $A_i$-модуль. Тогда $B = B_1 \times \ldots \times B_s$, где $B_i \simeq M_{k_i}(D_i)$, причем соответствующее разложение единицы $1 = e_1 + \ldots + e_s$ таково, что $e_i M = k_i V_i$. Обозначим простой $B_i$-модуль через $U_i$. Тогда $e_i M \simeq m_i U_i$ (как $B$-модуль). Но $[V_i : K] = n_i d_i$, где $d_i = [D_i : K]$, а $[U_i : K] = k_i d_i$. Поэтому $[e_i M : K] = k_i n_i d_i = m_i k_i d_i$, откуда $m_i = n_i$, $\bar{A} = E_B(M) \simeq A$ и мономорфизм $A \to \bar{A}$ обязан быть изоморфным.

**Следствие 6.8.** *Если $U$ простой $A$-модуль, $D = E_A(U)$ — его тело эндоморфизмов и $[U : D] = n$, то у $A$ есть факторалгебра, изоморфная $M_n(D)$.*

Д о к а з а т е л ь с т в о непосредственно вытекает из теоремы 6.7 и теоремы о гомоморфизме.

## *Упражнения к главе II*

1. Доказать, что неприводимое представление коммутативной алгебры над алгебраически замкнутым полем одномерно.

2. Пусть $A$ — коммутативная полупростая подалгебра алгебры $M_n(K)$, где $K$ — алгебраически замкнутое поле. Доказать, что найдется такая матрица $S$, что для любой матрицы $X \in A$ $SXS^{-1}$ — диагональная матрица. (Две подалгебры, $A$ и $A'$, алгебры $B$ называются *сопряженными*, если в $B$ найдется обратимый элемент $b$, такой, что $bab^{-1} \in A'$ для любого $a \in A$, и любой элемент $a' \in A'$ имеет такой вид. Упражнение 2 означает, что подалгебра $A \subset M_n(K)$ сопряжена с некоторой подалгеброй алгебры диагональных матриц.)

3. При каких условиях моногенная алгебра полупроста?

4. Доказать, что матрица $X \in M_n(K)$, где $K$ — алгебраически замкнутое поле, сопряжена с некоторой диагональной матрицей тогда и только тогда, когда моногенная подалгебра, порожденная матрицей $X$, полупроста.

5. Пусть $G$ — циклическая группа порядка $n$. Доказать, что групповая алгебра $KG$ полупроста тогда и только тогда, когда характеристика поля $K$ не делит $n$.

6. Доказать, что коммутативная алгебра полупроста тогда и только тогда, когда любая ее моногенная подалгебра полупроста.

7. Описать те алгебры, у которых любая моногенная подалгебра полупроста.

8. Описать алгебры без нильпотентных элементов.

9. Доказать, что всякий ненулевой идемпотент в алгебре $M_n(D)$ сопряжен с $\sum_{i=1}^{k} e_{ii}$ для некоторого $k$ $(1 \leqslant k \leqslant n)$.

10. Пусть $X$ и $Y$ — две матрицы из алгебры $A = M_n(K)$, $XA = \{XS \mid S \in A\}$, $YA = \{YS \mid S \in A\}$. Очевидно, $XA$ и $YA$ — правые идеалы. Когда они изоморфны как $A$-модули?

11. Доказать, что изоморфные простые подалгебры в алгебре $M_n(K)$ сопряжены.

12. Показать, что если алгебра $A$ полупроста, то длина левого регулярного модуля равна длине регулярного модуля (для неполупростых алгебр это, вообще говоря, неверно).

13. Пусть $A$ — полупростая алгебра над полем $K$ характеристики 0, $T$ и $S$ — ее представления одинаковой размерности, причем для любого элемента $a \in A$ найдется такая матрица $C_a$, что $C_a T(a) C_a^{-1} = S(a)$. Доказать, что представления $T$ и $S$ подобны[5].

# III

ГЛАВА

# РАДИКАЛ

Теоремы II.4.3 (Веддербёрна — Артина) и II.6.2 дают полное описание полупростых алгебр и их представлений. В то же время о строении неполупростых алгебр и модулей над ними известно гораздо меньше, даже если поле $K$ алгебраически замкнуто. Основное место здесь занимает понятие *радикала* — наименьшего идеала, факторалгебра по которому полупроста. Существенным свойством радикала является его нильпотентность. Она

[5] Это упражнение предложено А. В. Ройтером.

дает возможность «поднимать идемпотенты по модулю радикала». При этом естественно возникает важный класс модулей — *проективные модули*, находящиеся во взаимно однозначном соответствии с полупростыми, что дает возможность доказать для них однозначность разложения на неразложимые, а с помощью алгебры эндоморфизмов перенести этот результат и на произвольные модули. Наконец, в последних параграфах этой главы мы введем понятие *схемы алгебры* и *универсальной алгебры схемы* и с их помощью получим некоторое (правда, далеко не полное) описание алгебр, по крайней мере, в алгебраически замкнутом случае [6]. В частности, отсюда получается классификация так называемых *наследственных алгебр* (по-прежнему над алгебраически замкнутым полем).

Напомним, что, если не оговорено противное, все алгебры предполагаются конечномерными (бесконечномерные алгебры встретятся в § 6 как универсальные алгебры схем).

**§ 1. Радикал модуля и алгебры**

Пусть $M$—полупростой модуль: $M = \bigoplus_{i=1}^{s} U_i$, где $U_i$ — простые модули, $\pi_i$ — проекция $M$ на $U_i$. Тогда для любого ненулевого элемента $m \in M$ $\pi_i(m) \neq 0$ хотя бы для одного номера $i$. Можно сказать, что гомоморфизмы из $M$ во всевозможные простые модули «различают» элементы модуля $M$. Нетрудно проверить, что и наоборот, если гомоморфизмы из $M$ в простые модули различают элементы, то $M$ полупрост. Действительно, если $N$ — минимальный подмодуль в $M$, $n \in N$ — ненулевой элемент, то $f(n) \neq 0$ для некоторого гомоморфизма $f : M \to U$, где $U$ — простой модуль. Но тогда $N \cap \operatorname{Ker} f = 0$ ввиду минимальности $N$. Кроме того, $\operatorname{Im} f = U$, т. е. $M/\operatorname{Ker} f \simeq U$ и $\operatorname{Ker} f$ — максимальный подмодуль в $M$. Поэтому $N + \operatorname{Ker} f = M$ и $\operatorname{Ker} f$ — дополнение в $M$ к $N$. Следовательно, $M$ — полупростой модуль (см. предложение II.2.1).

Для произвольного модуля $M$ введем «меру его неполупростоты»: совокупность всех элементов $m \in M$, таких, что $f(m) = 0$ для любого гомоморфизма $f$ из $M$ в простой модуль. Очевидно, что эти элементы образуют в $M$ подмодуль, который называется *радикалом модуля* $M$ и обозначается $\operatorname{rad} M$.

Поскольку для любого ненулевого гомоморфизма $f : M \to U$, где $U$ — простой модуль, $\operatorname{Ker} f$ — максимальный подмодуль в $M$ и наоборот, всякий максимальный подмодуль $M' \subset M$ есть ядро проекции $\pi : M \to M/M'$, а модуль $M/M'$ прост, радикал есть пересечение всех максимальных подмодулей модуля $M$.

**Теорема 1.1.** *Модуль $M$ полупрост тогда и только тогда, когда* $\operatorname{rad} M = 0$. *Фактормодуль* $M/\operatorname{rad} M$ *всегда полупрост.*

*Доказательство.* Первое утверждение мы уже доказали выше. Поэтому достаточно проверить, что $\operatorname{rad}(M/\operatorname{rad} M) = 0$.

[6] В гл. VIII эти понятия будут обобщены на произвольные алгебры с сепарабельной факторалгеброй по радикалу.

Но по теореме 1.4.3 максимальные подмодули в $M/\operatorname{rad} M$ имеют вид $M'/\operatorname{rad} M$, где $M'$ — максимальный подмодуль в $M$ (поскольку всегда $M' \supset \operatorname{rad} M$). Очевидно, $\bigcap (M'/\operatorname{rad} M) = (\bigcap M')/\operatorname{rad} M = 0$, т. е. $\operatorname{rad}(M/\operatorname{rad} M) = 0$, и теорема доказана.

**Предложение 1.2.** $\operatorname{rad}\left(\bigoplus_{i=1}^{s} M_i\right) = \bigoplus_{i=1}^{s} \operatorname{rad} M_i$.

Доказательство. Всякий гомоморфизм $f: M \to U$, где $M = \bigoplus_{i=1}^{s} M_i$, однозначно определяется набором гомоморфизмов $f_i: M_i \to U$ по формуле $f(m_1, \ldots, m_s) = \sum_{i=1}^{s} f(m_i)$ (см. § 7 гл. I). Поэтому если $m_i \in \operatorname{rad} M_i$ для всех $i$, то $f(m_1, \ldots, m_s) = 0$ и $(m_1, \ldots, m_s) \in \operatorname{rad} M$.

Наоборот, если $(m_1, \ldots, m_s) \in \operatorname{rad} M$, то, рассматривая гомоморфизмы $f: M \to U$, для которых $f_j = 0$ при $j \neq i$, мы видим, что $f_i(m_i) = 0$ для любого гомоморфизма $f_i: M_i \to U$. Следовательно, $m_i \in \operatorname{rad} M_i$, что и требовалось доказать.

**Предложение 1.3.** *$f(\operatorname{rad} M) \subset \operatorname{rad} N$ для всякого гомоморфизма модулей $f: M \to N$.*

Доказательство. Если $m \in \operatorname{rad} M$, то для любого гомоморфизма $g: N \to U$, где $U$ — простой модуль, $gf(m) = 0$, т. е. $f(m) \in \operatorname{rad} N$.

Этот результат позволяет по любому гомоморфизму $f: M \to N$ построить индуцированный гомоморфизм $\tilde{f}: M/\operatorname{rad} M \to N/\operatorname{rad} N$, положив $\tilde{f}(m + \operatorname{rad} M) = f(m) + \operatorname{rad} N$.

**Лемма 1.4** (Накаяма). *Гомоморфизм $f: M \to N$ эпиморфен тогда и только тогда, когда эпиморфен индуцированный им гомоморфизм $\tilde{f}: M/\operatorname{rad} M \to N/\operatorname{rad} N$.*

Доказательство. Если $f$ — эпиморфизм, то, конечно, и $\tilde{f}$ есть эпиморфизм. Наоборот, эпиморфность $\tilde{f}$ означает, что $\operatorname{Im} f + \operatorname{rad} N = N$. Но если $\operatorname{Im} f \neq N$, то $\operatorname{Im} f$ содержится в некотором максимальном подмодуле $N'$. Поскольку и $\operatorname{rad} N \subset N'$, $\operatorname{Im} f + \operatorname{rad} N \subset N'$ и не совпадает с $N$. Следовательно, $\operatorname{Im} f = N$, т. е. $f$ — эпиморфизм.

Таким образом, эпиморфность достаточно проверять «по модулю радикала». Иногда полезна несколько другая форма этого результата:

**Следствие 1.5.** *Если $N$ и $L$ — такие подмодули в $M$, что $N + L = M$ и $N \subset \operatorname{rad} M$, то $L = M$.*

Доказательство представляется читателю.

Радикал регулярного модуля алгебры $A$ называется радикалом алгебры. По определению $\operatorname{rad} A$ — это правый идеал. Из теоремы 1.1 следует, что полупростота алгебры $A$ равносильна равенству $\operatorname{rad} A = 0$.

**Теорема 1.6.** *Для любого $A$-модуля $M$* $\operatorname{rad} M = MR$, *где* $R = \operatorname{rad} A$. *В частности, радикал алгебры — двусторонний идеал и факторалгебра по нему полупроста.*

Доказательство. Рассмотрим гомоморфизм $A \to M$, переводящий всякий элемент $a \in A$ в $ma$, где $m$ — фиксированный элемент из $M$ (см. теорему I.7.1). По предложению 1.3 он переводит радикал в радикал, т. е. $mR \subset \operatorname{rad} M$. Поэтому $MR \subset \operatorname{rad} M$.

В частности, $AR \subset R$, т. е. $R$ — двусторонний идеал, а факторалгебра $A/R = \overline{A}$ полупроста по теореме 1.1.

Рассмотрим фактормодуль $\overline{M} = M/MR$. Он аннулируется радикалом $R$, поэтому его можно рассматривать как $\overline{A}$-модуль, полупростой по теореме II.6.2. Следовательно, для любого ненулевого класса $\overline{m} = m + MR$ найдется гомоморфизм $f : \overline{M} \to U$, где $U$ — простой модуль, такой, что $f(\overline{m}) \neq 0$. Комбинируя $f$ с проекцией $\pi : M \to \overline{M}$, мы получим гомоморфизм $f\pi : M \to U$, для которого $f\pi(m) \neq 0$, т. е. $m \notin \operatorname{rad} M$. Отсюда следует включение $\operatorname{rad} M \subset MR$, что и завершает доказательство теоремы.

Заметим, что фактически мы установили, что $MR = \operatorname{rad} M$ — наименьший подмодуль в $M$, фактормодуль по которому полупрост.

**Следствие 1.7.** *Всякий полупростой $A$-модуль является модулем над полупростой факторалгеброй $\overline{A} = A/\operatorname{rad} A$. В частности, число простых $A$-модулей равно числу простых компонент алгебры $\overline{A}$.*

**Следствие 1.8.** *Радикал алгебры есть пересечение всех максимальных идеалов.*

Доказательство. Если $I$ — максимальный идеал алгебры $A$, то $A/I$ — простая алгебра, в частности полупростой $A$-модуль, поэтому $(A/I)R = 0$, т. е. $R \subset I$ и $I/R$ — максимальный идеал факторалгебры $\overline{A} = A/R$ (теорема I.4.7). Обозначим через $J$ пересечение всех максимальных идеалов алгебры $A$. Тогда $J \supset R$ и $J/R$ есть пересечение максимальных идеалов алгебры $\overline{A}$. Но $\overline{A}$ — полупростая алгебра, поэтому $J/R = 0$, т. е. $J = R$.

**Следствие 1.8** дает симметричную характеристику радикала (свободную от понятий «правый» и «левый»). Поэтому из него вытекает, что радикал левого регулярного модуля совпадает с радикалом алгебры.

**Предложение 1.9.** *Радикал $R$ алгебры $A$ — это нильпотентный идеал, содержащий все нильпотентные правые идеалы.*

Доказательство. Из теоремы 1.6 и леммы Накаямы (следствие 1.5) следует, что $R^2 = \operatorname{rad} R \neq R$ и вообще $R^{m+1} = \operatorname{rad} R^m \neq R^m$, если только $R^m \neq 0$. Но цепочка подпространств $R \supset R^2 \supset \ldots \supset R^m \supset R^{m+1} \supset \ldots$ должна оборваться, поэтому $R^m = 0$ для какого-то $m$.

Наоборот, если $I$ — нильпотентный правый идеал, то $(I + R)/R$ — нильпотентный правый идеал в полупростой алгебре $A/R$. Тогда по следствию II.2.5 $(I + R)/R = 0$, т. е. $I + R = R$.

**Следствие 1.10.** *Радикал алгебры есть множество всех существенно нильпотентных элементов.*

Важное свойство радикала связано со следующим понятием. Правый (левый) идеал $I$ алгебры $A$ называется квазирегулярным, если любой элемент $1 - x$, где $x \in I$, обратим.

**Предложение 1.11.** *Радикал — это квазирегулярный идеал, содержащий все правые и левые квазирегулярные идеалы.*

Доказательство. Если $x \in R$, то $x^k = 0$ для некоторого $k$, а тогда $(1 - x)(1 + x + x^2 + \ldots + x^{k-1}) = 1 - x^k = 1$, т. е. $1 - x$ обратим. Наоборот, пусть $I \not\subset R$, где $I$ — какой-либо правый идеал. Тогда $I \not\subset M$ для некоторого максимального правого идеала $M$. Поэтому $I + M = A$. В частности, $1 = x + m$, где $x \in I$, а $m \in M$. Но $m = 1 - x$ — необратимый элемент, так как $mA \neq A$. Значит, $I$ не квазирегулярен.

Таким образом, в конечномерных алгебрах нильпотентность и квазирегулярность совпадают.

**Следствие 1.12.** *Всякий правый (левый) ниль-идеал (т. е. такой, все элементы которого нильпотентны) содержится в радикале и потому нильпотентен.*

Доказательство следует из того, что если $I$ — правый ниль-идеал, то все элементы $1 - x$ ($x \in I$) обратимы: если $x^m = 0$, то $(1 - x)(1 + x + \ldots + x^{m-1}) = 1$.

В дальнейшем мы будем часто использовать еще такую характеристику радикала.

**Предложение 1.13.** *Радикал $R$ алгебры $A$ — это единственный ниль-идеал, факторалгебра по которому полупроста.*

Доказательство. Радикал обладает этими свойствами, как было показано выше. Наоборот, из того, что алгебра $A/I$ полупроста, следует, что $I \supset \operatorname{rad} A$, а из того, что $I$ — ниль-идеал, следует, что $I \subset \operatorname{rad} A$.

**Следствие 1.14.** $\operatorname{rad}(A/I) = (R + I)/I$, *где* $R = \operatorname{rad} A$.

Доказательство. Из нильпотентности $R$ следует нильпотентность $(R + I)/I$. В то же время $(A/I)/((R + I)/I) \simeq A/(R + I) \simeq (A/R)((R + I)/I)$. Но $A/R$ — полупростая алгебра, поэтому всякая ее факторалгебра тоже полупроста. Значит, $(R+I)/I = \operatorname{rad}(A/I)$.

## § 2. Подъем идемпотентов. Главные модули

Нильпотентность радикала дает мощный метод исследования неполупростых алгебр: подъем идемпотентов по модулю радикала.

**Лемма 2.1.** *Пусть $I$ — ниль-идеал алгебры $A$, $u$ — такой элемент алгебры, что $u^2 \equiv u \pmod I$. Тогда в $A$ существует такой идемпотент $e$, что $e \equiv u \pmod I$.*

Доказательство. Положим $v = u + r - 2ur$, где $r = u^2 - u$. Тогда $ur = ru$, $r^2 \in I^2$, поэтому $v^2 \equiv u^2 + 2ur - 4u^2r \equiv u + r + 2ur - 4ur \equiv v \pmod{I^2}$. Кроме того, очевидно, $v \equiv u \pmod I$. Поступая таким же образом с элементом $v$, мы построим элемент $v_1$, такой, что $v_1^2 \equiv v_1 \pmod{I^4}$ и $v_1 \equiv v \pmod{I^2}$.

Значит, $v_1 \equiv u \pmod{I}$. Продолжая этот процесс и учитывая нильпотентность идеала $I$, мы и построим требуемый идемпотент $e$.

Из леммы 2.1 легко выводится характеристика тех алгебр, у которых регулярный модуль неразложим.

**Теорема 2.2.** *Следующие условия равносильны:*

1) *регулярный $A$-модуль неразложим;*

2) *$A/R$ — тело ($R = \operatorname{rad} A$);*

3) *в алгебре $A$ есть единственный максимальный правый идеал;*

4) *необратимые элементы алгебры $A$ образуют правый идеал*[7].

Доказательство. 1) $\Rightarrow$ 2). Условие 1) означает, что в алгебре $E_A(A) = A$ нет нетривиальных идемпотентов (следствие I.7.3). Но тогда в силу леммы 2.1 их не может быть и в полупростой алгебре $A/R$, а тогда, очевидно, $A/R$ есть тело.

2) $\Rightarrow$ 4). Если $A/R$ — тело и элемент $a \in A$ не лежит в $R$, то класс $a + R$ обратим в $A/R$, т. е. существует такой элемент $b \in A$, что $ab \equiv 1 \pmod{R}$. Но тогда по предложению 1.11 элемент $ab$, а значит и $a$, обратим. Так как все элементы радикала необратимы, то $R$ — это в точности множество всех необратимых элементов, что и доказывает 4).

4) $\Rightarrow$ 3). Пусть $I$ — идеал, состоящий из всех необратимых элементов алгебры $A$. Тогда любой правый идеал $J \neq A$ содержится в $I$, так как обратимых элементов в $J$ быть не может, и $I$ — единственный максимальный правый идеал.

3) $\Rightarrow$ 1) следует из того, что если модуль $M$ разложим $M = N \oplus L$, где $N \neq 0$, $L \neq 0$, то в нем есть по крайней мере два максимальных подмодуля $N' \oplus L$ и $N \oplus L'$, где $N'$ и $L'$ — максимальные подмодули соответственно в $N$ и $L$.

Алгебры, удовлетворяющие условиям теоремы 2.2, называются локальными.

Из следствия I.7.4 вытекает такое утверждение.

**Следствие 2.3** (Фиттинг). *Модуль неразложим тогда и только тогда, когда его алгебра эндоморфизмов локальна.*

Применим полученные результаты к прямым слагаемым регулярного модуля. Модули, изоморфные неразложимым прямым слагаемым регулярного, называются главными неразложимыми, или просто главными. Иными словами, главный $A$-модуль имеет вид $eA$, где $e$ — минимальный идемпотент, который нельзя представить в виде $e = e' + e''$, где $e'$, $e''$ — ненулевые ортогональные идемпотенты. По следствию 2.3 это равносильно локальности алгебры $E_A(eA) \simeq eAe$.

**Предложение 2.4.** $\operatorname{rad}(eAe) = eRe$. *Идемпотент $e \in A$ минимален тогда и только тогда, когда минимален идемпотент $\bar{e} = e + R$ алгебры $\bar{A} = A/R$ ($R = \operatorname{rad} A$).*

Доказательство. Очевидно, $eRe$ — идеал в $eAe$, нильпотентный ввиду нильпотентности $R$. С другой стороны, $eAe/eRe \simeq$

[7] Поскольку условие 2) симметрично, в условиях 1), 3), 4) можно всюду правые модули и идеалы заменить левыми.

$\simeq \bar{e}\bar{A}\bar{e}$ — полупростые алгебры. По предложению 1.13 $eRe = \mathrm{rad}\,(eAe)$. Второе утверждение следует теперь из теоремы 2.2, поскольку $\bar{e}$ минимален тогда и только тогда, когда $\bar{e}\bar{A}\bar{e}$ — тело.

**Следствие 2.5.** *Главный модуль содержит единственный максимальный подмодуль.*

Доказательство. Если $eA$ — главный модуль, то $\bar{e} = e + R$ — минимальный идемпотент, а тогда $\bar{e}\bar{A} \simeq eA/eR$ — простой модуль и $eR$ — максимальный подмодуль в $eA$. Но по теореме 1.6 $eR = \mathrm{rad}\,(eA)$ содержится во всех максимальных подмодулях, поэтому он является единственным максимальным подмодулем в $eA$.

**Предложение 2.6.** *Если* $f : eA \to M$ *— гомоморфизм* $A$*-модулей, то* $f(e) \in Me$*, и, сопоставляя гомоморфизму* $f$ *элемент* $f(e)$*, мы устанавливаем изоморфизм векторных пространств* $\mathrm{Hom}_A(eA, M) \simeq Me$.

Доказательство. $f(e) = f(e^2) = f(e)\,e \in Me$, и если $f(e) = g(e)$, то $f(ea) = f(e)\,a = g(e)\,a = g(ea)$ для любого $a \in A$, т. е. $f = g$ и отображение $\mathrm{Hom}_A(eA, M) \to Me$ есть мономорфизм. С другой стороны, ограничивая на $eA$ гомоморфизм $A \to M$, переводящий $a$ в $ma$, мы получим гомоморфизм $f : eA \to M$, переводящий $e$ в $me$, т. е. отображение $\mathrm{Hom}_A(eA, M) \to Me$ и эпиморфно.

**Следствие 2.7.** *Для любого гомоморфизма* $f : eA \to M$ *и любого эпиморфизма* $g : N \to M$ *существует гомоморфизм* $\varphi : eA \to N$*, такой, что* $f = g\varphi$.

Доказательство. Пусть $f(e) = me$ и $n$ — прообраз $m$ в $N$. Тогда за $\varphi$ можно принять гомоморфизм $eA \to N$, переводящий $e$ в $ne$.

**Следствие 2.8.** *Если в модуле* $M$ *есть всего один максимальный подмодуль, то* $M$ *изоморфен фактормодулю главного модуля.*

Доказательство. Пусть $M'$ — единственный максимальный подмодуль в $M$. Тогда $M' = MR$ и $M/MR$ — простой модуль, т. е. $M/MR \simeq \bar{e}\bar{A}$ для некоторого минимального идемпотента $\bar{e}$ алгебры $\bar{A} = A/R$. Но по лемме 2.1 $\bar{e} = e + R$, где $e$ — идемпотент в $A$, минимальный по предложению 2.4, и $\bar{e}\bar{A} \simeq eA/eR$. Обозначим через $\pi$ проекцию $M$ на $\bar{e}\bar{A}$, а через $f$ — проекцию $eA$ на $\bar{e}\bar{A}$. По следствию 2.7 существует гомоморфизм $\varphi : eA \to M$, такой, что $\pi\varphi = f$, причем индуцированный гомоморфизм $\tilde{\varphi} : eA/eR \to M/MR$ есть изоморфизм. По лемме Накаямы (лемма 1.4) $\varphi$ — эпиморфизм и $M \simeq eA/\mathrm{Ker}\varphi$.

**Следствие 2.9.** *Главные модули* $eA$ *и* $fA$ *изоморфны тогда и только тогда, когда изоморфны простые модули* $\bar{e}\bar{A}$ *и* $\bar{f}\bar{A}$ ($\bar{A} = A/R$, $\bar{a} = a + R$).

Доказательство. Если $eA \simeq fA$, то $\bar{e}\bar{A} \simeq eA/eR \simeq fA/fR \simeq \bar{f}\bar{A}$. Наоборот, пусть $\bar{e}\bar{A} \simeq \bar{f}\bar{A}$. Комбинируя этот изоформизм с проекцией $eA \to \bar{e}\bar{A}$, мы получим эпиморфизм $g : eA \to$

$\to \bar{f}\bar{A}$. По следствию 2.7 $g = \pi\varphi$, где $\varphi : eA \to fA$, а $\pi$ — проекция $fA \to \bar{f}\bar{A}$. Поскольку $\varphi$ индуцирует изоморфизм $\bar{e}\bar{A} \simeq \bar{f}\bar{A}$, он является эпиморфизмом (по лемме 1.4). Аналогично строится эпиморфизм $\psi : fA \to eA$. Но тогда $\varphi\psi$ и $\psi\varphi$ — эпиморфизмы и поэтому изоморфизмы (так как $eA$ и $fA$ — конечномерные пространства). Поэтому $\varphi$ и $\psi$ — также изоморфизмы, что и завершает доказательство следствия.

Итак, между главными и простыми модулями устанавливается естественное взаимно однозначное соответствие. Заметим, что аналогичные результаты верны и для левых модулей. Но в полупростой алгебре $\bar{A}$, как легко видеть, $\bar{e}\bar{A} \simeq \bar{f}\bar{A}$ тогда и только тогда, когда $\bar{A}\bar{e} \simeq \bar{A}\bar{f}$ (и то, и другое означает просто, что $\bar{e}$ и $\bar{f}$ принадлежат одной простой компоненте). Поэтому мы получаем такой результат.

**Следствие 2.10.** *Левые главные модули $Ae$ и $Af$ изоморфны тогда и только тогда, когда изоморфны модули $eA$ и $fA$.*

### § 3. Проективные модули. Проективные накрытия

Следствие 2.7 выражает важнейшее свойство главных модулей — их проективность.

Модуль $P$ над алгеброй $A$ называется п р о е к т и в н ы м, если для любого эпиморфизма $g : M \to N$ и любого гомоморфизма $f : P \to N$ существует такой гомоморфизм $\varphi : P \to M$, что $f = g\varphi$. Говорят, что $f$ м о ж н о п о д н я т ь до $\varphi$, или что $\varphi$ — это п о д ъ е м $f$ на $M$.

**Предложение 3.1.** *Проективные модули $P$ и $Q$ изоморфны тогда и только тогда, когда изоморфны полупростые модули $\bar{P} = P/PR$ и $\bar{Q} = Q/QR$ ($R = \operatorname{rad} A$).*

Д о к а з а т е л ь с т в о. Всякий изоморфизм $P \xrightarrow{\sim} Q$ индуцирует изоморфизм $\bar{P} \simeq \bar{Q}$. Наоборот, если $\bar{P} \simeq \bar{Q}$, то существует эпиморфизм $f : P \to \bar{Q}$, который можно поднять до гомоморфизма $\varphi : P \to Q$ (так как $P$ — проективный модуль), причем $\varphi$ будет эпиморфизмом по лемме Накаямы. Аналогично строится эпиморфизм $\psi : Q \to P$. Но тогда из сравнения размерностей сразу следует, что $\varphi$ и $\psi$ изоморфизмы.

**Предложение 3.2.** *Прямая сумма модулей проективна тогда и только тогда, когда проективно каждое слагаемое.*

Д о к а з а т е л ь с т в о. Всякий гомоморфизм $f : P \oplus Q \to N$ однозначно задается парой гомоморфизмов $f_1 : P \to N$ и $f_2 : Q \to N$ : $f(p, q) = f_1(p) + f_2(q)$ и, очевидно, решением уравнения $f = g\varphi$, где $g$ — эпиморфизм $M \to N$, а $\varphi$ — искомый гомоморфизм $P \to M$, будет такая пара $\varphi_1 : P \to M$ и $\varphi_2 : Q \to N$, что $f_1 = g\varphi_1$ и $f_2 = g\varphi_2$. Таким образом, $f$ можно поднять тогда и только тогда, когда можно поднять каждый гомоморфизм $f_1$, $f_2$, что и доказывает утверждение.

Одним из основных примеров проективных модулей являются свободные модули. С в о б о д н ы й м о д у л ь — это модуль, изоморфный прямой сумме регулярных, т. е. имеющий вид $nA$ для некоторого $n$. Элементы свободного модуля можно рассматривать

как «векторы» $(a_1, \ldots, a_n)$ с коэффициентами из $A$ и покоординатными операциями. Число $n$ называется р а н г о м свободного модуля.

**Предложение 3.3.** *Всякий гомоморфизм $f : nA \to M$ однозначно задается произвольным набором элементов $\{m_1, \ldots, m_n\}$ модуля $M$ по формуле*

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{n} m_i a_i. \qquad (1)$$

Таким образом, $\mathrm{Hom}_A(nA, M) \simeq nM$.

Д о к а з а т е л ь с т в о. Тривиально проверяется, что отображение $f : nA \to M$, определенное формулой (1), при любых $m_1, \ldots, m_n$ является гомоморфизмом. Наоборот, если $f$ — гомоморфизм $nA \to M$, положим $m_i = f(u_i)$, где $u_i = (0, \ldots, 1, \ldots, 0)$ (1 на $i$-м месте). Поскольку $(a_1, \ldots, a_n) = \sum_{i=1}^{n} u_i a_i$, $f(a_1, \ldots, a_n) = \sum_{i=1}^{n} f(u_i) a_i = \sum_{i=1}^{n} m_i a_i$ и предложение доказано.

Множество элементов $\{m_1, \ldots, m_n\}$ модуля $M$ называется с и с т е м о й о б р а з у ю щ и х, если всякий элемент $m \in M$ можно представить в виде $m = \sum_{i=1}^{n} m_i a_i$ для некоторых $a_i \in A$. Иными словами, это означает, что гомоморфизм $f : nA \to M$, определенный формулой (1), есть эпиморфизм. Из теоремы о гомоморфизме тогда вытекает

**Следствие 3.4.** *Если в модуле $M$ есть система образующих, состоящая из $n$ элементов, то $M$ изоморфен фактормодулю свободного модуля ранга $n$.*

Заметим, что в конечномерном модуле $M$ всегда есть конечная система образующих (например, любой базис). Наименьшее число элементов во всевозможных системах образующих называется ч и с л о м о б р а з у ю щ и х модуля $M$ и обозначается $\mu_A(A)$.

Свободные модули, как и главные, проективны (по предложению 3.2). Следующая теорема устанавливает связь между свободными, главными и проективными модулями.

**Теорема 3.5.** *Следующие условия равносильны:*

1) *модуль $P$ проективен;*

2) *$P$ изоморфен прямой сумме главных модулей;*

3) *$P$ изоморфен прямому слагаемому свободного модуля;*

4) *ядро любого эпиморфизма $f : M \to P$ дополнимо в $M$ (очевидно, тогда $M \simeq P \oplus \mathrm{Ker}\, f$).*

Д о к а з а т е л ь с т в о. 2) $\Rightarrow$ 1) и 3) $\Rightarrow$ 1) по предложению 3.2.

4) $\Rightarrow$ 3) по следствию 3.4.

1) $\Rightarrow$ 4). Существует гомоморфизм $\varphi : P \to M$, такой, что $f\varphi = 1$, а по предложению I.6.2 это равносильно дополнимости $\mathrm{Ker}\, f$.

1) $\Rightarrow$ 2). Разложим полупростой модуль $\overline{P} = P/PR$ в прямую сумму простых $\overline{P} = U_1 \oplus \ldots \oplus U_t$ и для каждого $U_i$ выберем главный модуль $P_i$, такой, что $P_i/P_iR \simeq U_i$. Обозначим $Q = \bigoplus_{i=1}^{t} P_i$. Тогда $Q$ — проективный модуль и $Q/QR \simeq P/PR$. Следовательно, $P \simeq Q$ (по предложению 3.1), что и требовалось доказать.

Оказывается, проективные модули находятся во взаимно однозначном соответствии с полупростыми, подобно тому, как это имеет место для главных и простых модулей.

**Теорема 3.6.** *Сопоставляя проективному модулю $P$ полупростой модуль $\overline{P} = P/PR$, мы устанавливаем взаимно однозначное соответствие между проективными и полупростыми модулями. Если $P = P_1 \oplus \ldots \oplus P_n = Q_1 \oplus \ldots \oplus Q_m$ — два разложения проективного модуля $P$ в прямую сумму главных, то $n = m$ и, при подходящей нумерации слагаемых, $P_i \simeq Q_i$ для всех $i$.*

Доказательство. В силу предложения 3.1, нужно проверить только, что всякий полупростой модуль $M$ изоморфен $P/PR$, где $P$ — проективный модуль. Но для этого достаточно разложить $M$ в прямую сумму простых $M = U_1 \oplus \ldots \oplus U_n$ и положить $P = P_1 \oplus \ldots \oplus P_n$, где $P_i$ — такой главный модуль, что $U_i \simeq P_i/P_iR$.

Если же $P_1 \oplus \ldots \oplus P_n \simeq Q_1 \oplus \ldots \oplus Q_m$, где $P_i$ и $Q_i$ —главные модули, то, факторизуя по радикалу, мы получим изоморфизм $\overline{P}_1 \oplus \ldots \oplus \overline{P}_n \simeq \overline{Q}_1 \oplus \ldots \oplus \overline{Q}_m$ ($\overline{P}_i = P_i/P_iR$, $\overline{Q}_j = Q_j/Q_jR$), причем $P_i$ и $Q_j$ — простые модули. По предложению II.2.3, $n = m$ и $\overline{P}_i \simeq \overline{Q}_i$ для всех $i$ (при подходящей нумерации), а тогда по следствию 2.9 и $P_i \simeq Q_i$.

Из следствия 3.4 вытекает, что всякий модуль изоморфен фактормодулю проективного. Конечно, данный модуль $M$ можно представить в виде $P/N$, где $P$ проективен, многими разными способами. Однако, как мы сейчас покажем, существует в некотором смысле минимальное такое представление, и оно единственно.

Проективный модуль $P$ называется проективным накрытием модуля $M$ и обозначается $P(M)$, если существует эпиморфизм $f: P \to M$, индуцирующий изоморфизм $P/\operatorname{rad} P \rightrightarrows M/\operatorname{rad} M$. Очевидно, это равносильно тому, что $M \simeq P/N$, где $N \subset \operatorname{rad} P$.

**Теорема 3.7.** 1) *Для всякого модуля $M$ существует проективное накрытие, единственное с точностью до изоморфизма.*

2) $P(M) \simeq P(\overline{M})$, *где* $\overline{M} = M/\operatorname{rad} M$.

3) *Если $g$ — эпиморфизм проективного модуля $Q$ на модуль $M$, то $Q \simeq P_1 \oplus P_2$, где $P_1 \simeq P(M)$, ограничение $g$ на $P_1$ — эпиморфизм, а $P_2 \subset \operatorname{Ker} g$. Более того, изоморфизм $P(M) \rightrightarrows P_1$ можно выбрать так, чтобы его композиция с эпиморфизмом $g$ давала фиксированный эпиморфизм $f: P(M) \to M$.*

Доказательство. По теореме 3.6 $\overline{M} \simeq P/\operatorname{rad} P$ для некоторого проективного модуля $P$. Но тогда эпиморфизм $P \to \overline{M}$ продолжается до гомоморфизма $f: P \to M$, причем по лемме Накаямы $f$ — эпиморфизм, т. е $P$ — проективное накрытие $M$, что доказывает утверждение 1) и 2) (однозначность следует из предложения 3.1).

Пусть теперь $Q$ — какой-нибудь проективный модуль и $g: Q \to M$ — эпиморфизм. Поднимем $g$ до гомоморфизма $\varphi: Q \to P$, такого, что $f\varphi = g$. Тогда индуцированное отображение $\overline{\varphi}: Q/\operatorname{rad} Q \to P/\operatorname{rad} P$ есть эпиморфизм и по лемме Накаямы $\varphi$ — эпиморфизм. По теореме 3.5, $Q = P_1 \oplus \operatorname{Ker} \varphi$, где $P_1 \simeq P$. Поскольку $P_2 = \operatorname{Ker} \varphi \subset \operatorname{Ker} g$, то это доказывает и утверждение 3).

**Следствие 3.8.** $P(M \oplus N) \simeq P(M) \oplus P(N)$.

Доказательство очевидно.

**Следствие 3.9.** *Пусть* $R = \operatorname{rad} A$, $\overline{A} = A/R$, $1 = \overline{e_1} + \ldots + \overline{e_n}$ — *разложение единицы алгебры* $\overline{A}$. *Тогда существует такое разложение единицы* $1 = e_1 + \ldots + e_n$ *алгебры* $A$, *что* $\overline{e_i} = e_i + R$.

Доказательство. Очевидно, $A = P(\overline{A})$. С другой стороны, если $U_i = \overline{e_i}\overline{A}$, а $P_i = P(U_i)$, то $P(\overline{A}) \simeq P_1 \oplus \ldots \oplus P_n$. Следовательно, $A \simeq P_1 \oplus \ldots \oplus P_n$, причем этот изоморфизм можно выбрать так, чтобы его композиция с естественным эпиморфизмом $P_1 \oplus \ldots \oplus P_n \to U_1 \oplus \ldots \oplus U_n = \overline{A}$ давала проекцию $\pi: A \to \overline{A}$. Пусть $1 = e_1 + \ldots + e_n$ — разложение единицы алгебры $A$, соответствующее разложению $A \simeq P_1 \oplus \ldots \oplus P_n$ регулярного модуля. Тогда $e_iA/e_iR = \overline{e_i}\overline{A}$, т. е. идемпотенты $e_i + R$ дают разложение единицы, соответствующее разложению $\overline{A} = \overline{e_1}\overline{A} \oplus \ldots \oplus \overline{e_n}\overline{A}$. Ввиду взаимно однозначного соответствия между разложениями единицы и разложениями модуля (теорема I.7.2), $e_i + R = \overline{e_i}$, что и требовалось доказать.

В заключение этого параграфа мы применим полученные результаты к изучению одного класса алгебр.

Алгебра $A$ называется примарной, если $A/\operatorname{rad} A$ — простая алгебра.

**Теорема 3.10.** *Следующие условия равносильны*:

1) *алгебра* $A$ *примарна*;
2) *в* $A$ *есть один максимальный идеал*;
3) *всякий собственный идеал алгебры* $A$ *нильпотентен*;
4) *у алгебры* $A$ *есть один простой модуль*;
5) *у алгебры* $A$ *есть один главный модуль*;
6) $A \simeq M_n(B)$, *где* $B$ — *локальная алгебра*.

Доказательство проведем по схеме

3) $\Rightarrow$ 2) $\Rightarrow$ 1) $\Rightarrow$ 4) $\Rightarrow$ 5) $\Rightarrow$ 6) $\Rightarrow$ 1) $\Rightarrow$ 3).

3) $\Rightarrow$ 2). Если все идеалы нильпотентны, то все они содержатся в $R = \operatorname{rad} A$ (предложение 1.9) и потому $R$ — единственный максимальный идеал.

2) $\Rightarrow$ 1) вытекает из следствия 1.8. 1) $\Rightarrow$ 4) по следствию 1.7. 4) $\Rightarrow$ 5) по следствию 2.9.

5) $\Rightarrow$ 6). Регулярный модуль $A$ изоморфен $nP$, где $P$ — единственный главный модуль, откуда $A \simeq E_A(A) \simeq M_n(B)$, где $B = E_A(P)$ — локальная алгебра (по следствию 2.3).

6) $\simeq$ 1). Пусть $A = M_n(B)$. Покажем, что $\operatorname{rad} A = M_n(J)$, где $J = \operatorname{rad} B$. Действительно, $M_n(J)$ — нильпотентный идеал в $A$, а $A/M_n(J) \simeq M_n(B/J)$ — простая алгебра, так как $B/J$ — тело. Поэтому $M_n(J) = \operatorname{rad} A$ (по предложению 1.13) и $A$ — примарная алгебра.

1) $\Rightarrow$ 3). Если $I$ — идеал примарной алгебры $A$, то $(I + R)/R$ — идеал простой алгебры $A/R$, откуда либо $(I + R)/R = 0$, т. е. $I \subset R$, либо $(I + R)/R = A/R$, т. е. $I + R = A$ и, по лемме Накаямы, $I = A$. Итак, если $I \neq A$, то $I \subset R$ и потому нильпотентен.

Заметим, что при доказательстве импликации 6) $\Rightarrow$ 1) мы фактически попутно доказали

**Предложение 3.11.** $\operatorname{rad} M_n(B) = M_n(\operatorname{rad} B)$.

## § 4. Теорема Крулля — Шмидта

Из теоремы 3.6, в частности, следует однозначность разложения регулярного модуля в прямую сумму неразложимых. В этом параграфе, используя результаты § 7 гл. I, мы перенесем этот факт на произвольные модули. Прежде всего переведем его на язык идемпотентов.

**Теорема 4.1.** *Пусть* $1 = e_1 + \ldots + e_n = f_1 + \ldots + f_m$ — *два разложения единицы алгебры* $A$, *причем идемпотенты* $e_i$ и $f_j$ *минимальны. Тогда* $n = m$ *и в алгебре* $A$ *есть такой обратимый элемент* $a$, *что при подходящей нумерации* $f_i = ae_ia^{-1}$ *для всех* $i$.

Доказательство. $A = e_1A \oplus \ldots \oplus e_nA = f_1A \oplus \ldots \oplus f_mA$ — два разложения регулярного модуля в прямую сумму главных. По теореме 3.6 $n = m$ и $e_iA \simeq f_iA$ для всех $i$ (при подходящей нумерации). Но изоморфизм $e_iA \simeq f_iA$ осуществляется некоторым элементом $a_i \in f_iAe_i$ так, что $f_ia_i = a_ie_i = a_i$. Положим $a = a_1 + \ldots + a_n$. Тогда $ae_i = a_ie_i = a_i$ и $f_ia = f_ia_i = a_i$ для всех $i$. Покажем, что $a$ обратим. Для этого выберем элементы $b_i \in e_iAf_i$, осуществляющие обратные к $a_i$ изоморфизмы $f_iA \simeq e_iA$, и положим $b = b_1 + \ldots + b_n$. Поскольку $a_ib_i = f_i$, а $e_ib = b_i = bf_i$, то $ab = \sum_{i=1}^{n} a_ib_i = \sum_{i=1}^{n} f_i = 1$ и $b = a^{-1}$. Следовательно, из равенства $ae_i = f_ia$ следует, что $f_i = ae_ia^{-1}$. Теорема доказана.

Теперь для доказательства однозначности разложения остается применить теорему 4.1 к алгебре эндоморфизмов.

**Теорема 4.2.** (Крулль—Шмидт). *Если* $M = M_1 \oplus \ldots \oplus M_n = N_1 \oplus \ldots \oplus N_m$ — *два разложения модуля* $M$ *в прямую сумму неразложимых модулей, то* $n = m$ *и при подходящей нумерации* $M_i \simeq N_i$ *для всех* $i$.

Доказательство. По теореме I.7.2 данным двум разложениям $M$ в прямую сумму неразложимых соответствуют два раз-

ложения единицы алгебры $E = E_A(M)$ : $1 = e_1 + \ldots + e_n = f_1 + \ldots + f_m$, причем $e_i$ и $f_j$ — минимальные идемпотенты; $M_i = e_iM$, а $N_j = f_jM$. По теореме 4.1 $n = m$ и при подходящей нумерации $f_i = ae_ia^{-1}$, где $a$ — обратимый элемент алгебры $E$, т. е. автоморфизм модуля $M$. Пусть $a_i$ — ограничение $a$ на $M_i$. Так как $ae_i = f_ia$, то $ae_i(m) \in f_iM = N_i$, т. е. $a_i$ отображает $M_i$ в $N_i$. Поскольку $a$ — мономорфизм, $a_i$ — также мономорфизм. С другой стороны, $a$ — эпиморфизм, поэтому любой элемент из $N_i$ имеет вид $y = a(x)$. Но тогда $f_i(y) = y = f_ia(x) = ae_i(x)$ и $e_i(x) \in M_i$, т. е. $a_i$ — эпиморфизм $M_i$ на $N_i$ и потому изоморфизм. Теорема доказана.

## § 5. Радикал алгебры эндоморфизмов

Применим полученные результаты для выяснения поведения радикала при пирсовском разложении.

**Лемма 5.1.** *Пусть $f : M \to N$ — гомоморфизм неразложимых $A$-модулей. Тогда либо $f$—изоморфизм, либо для любого гомоморфизма $g : N \to M$ $fg \in \operatorname{rad} E_A(N)$ и $gf \in \operatorname{rad} E_A(M)$.*

Доказательство. Пусть $g \in \operatorname{Hom}_A(N, M)$ и $gf \notin \operatorname{rad} E_A(N)$. Тогда, поскольку алгебра $E_A(N)$ локальна (следствие 2.3), $fg$ — обратимый элемент, т. е. автоморфизм $N$, и потому $f$ — эпиморфизм. Если $\varphi = (fg)^{-1}$, то $f(g\varphi) = 1$ и по предложению 1.6.2 $M \simeq N \oplus \operatorname{Ker} f$. Ввиду неразложимости $M$, $\operatorname{Ker} f = 0$, т. е. $f$ — мономорфизм и, значит, изоморфизм. Аналогично доказывается, что если $gf \notin \operatorname{rad} E_A(M)$, то $f$ — изоморфизм.

**Теорема 5.2.** *Пусть $M = M_1 \oplus \ldots \oplus M_s$, где $M_i \simeq n_iN_i$, а модули $N_i$ неразложимы и $N_i \not\simeq N_j$ при $i \neq j$. Обозначим $\operatorname{Hom}_A(M_i, M_j) = E_{ij}$ и рассмотрим двустороннее пирсовское разложение алгебры $E = E_A(M)$*

$$E = \begin{pmatrix} E_{11} & E_{12} & \ldots & E_{1s} \\ E_{21} & E_{22} & \ldots & E_{2s} \\ \ldots & \ldots & \ldots & \ldots \\ E_{s1} & E_{s2} & \ldots & E_{ss} \end{pmatrix}.$$

*Тогда радикал алгебры $E$ имеет вид*

$$R = \begin{pmatrix} R_{11} & E_{12} & \ldots & E_{1s} \\ E_{21} & R_{22} & \ldots & E_{2s} \\ \ldots & \ldots & \ldots & \ldots \\ E_{s1} & E_{s2} & \ldots & R_{ss} \end{pmatrix}, \qquad (1)$$

*где $R_{ii} = \operatorname{rad} E_{ii}$. Иными словами, если $1 = e_1 + \ldots + e_s$ — соответствующее разложение единицы алгебры $E$, то $e_iRe_j = e_iEe_j$ при $i \neq j$ и $e_iRe_i = \operatorname{rad} e_iEe_i$.*

Доказательство. Согласно § 7 гл. I, элементы $E_{ij}$ можно рассматривать как матрицы размера $n_i \times n_j$ с коэффициентами из $H_{ij} = \mathrm{Hom}_A(N_i, N_j)$. Поэтому $R_{ii} = M_{n_i}(R_i)$, где $R_i = \mathrm{rad}\, E_A(N_i)$ (см. предложение 3.11). А из леммы 5.1 следует, что $E_{ij}E_{jl} \subset R_{ii}$ при $i \neq j$. Следовательно, множество $R$, определенное формулой (1), есть идеал в $E$, причем $E/R \simeq E_{11}/R_{11} \times \ldots \ldots \times E_{ss}/R_{ss}$ — полупростая алгебра, а потому $R \supset \mathrm{rad}\, E$.

С другой стороны, рассмотрим правый идеал

$$I_i = \begin{pmatrix} 0 & 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ E_{i1} & E_{i2} & \ldots & R_{ii} & \ldots & E_{is} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}$$

($i$-я строка $R$). Установим его нильпотентность. Действительно,

$$I_i^2 = \begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ R_{ii}E_{i1} & \ldots & R_{ii}^2 & \ldots & R_{ii}E_{is} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix}$$

и вообще

$$I_i^{k+1} = \begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ R_{ii}^k E_{i1} & \ldots & R_{ii}^{k+1} & \ldots & R_{ii}^k E_{is} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix},$$

а $R_{ii}^k = 0$ при некотором $k$. Значит, $I_i^{k+1} = 0$. Поэтому $I_i \subset \mathrm{rad}\, E$. Следовательно, $R = I_1 + \ldots + I_s \subset \mathrm{rad}\, E$, что и доказывает теорему.

Применяя теорему 5.2 к алгебре $A \simeq E_A(A)$, получаем такой результат.

**Теорема 5.3.** *Пусть* $1 = e_1 + \ldots + e_s$ *— такое разложение единицы алгебры* $A$, *что идемпотенты* $\bar{e}_i = e_i + R$ *центральны в факторалгебре* $\bar{A} = A/R$, *где* $R = \mathrm{rad}\, A$. *Тогда* $e_iRe_j = e_iAe_j$ *при* $i \neq j$; $e_iRe_i = \mathrm{rad}\,(e_iAe_i)$.

Доказательство. Поскольку $\bar{e}_i$ — центральные идемпотенты, $A$-модули $\bar{e}_i\bar{A}$ и $\bar{e}_j\bar{A}$ при $i \neq j$ не имеют изоморфных прос-

тых слагаемых. Но тогда, по следствию 2.9, в $e_iA$ и $e_jA$ нет изоморфных главных слагаемых и из теоремы 5.2 следует, что $e_iAe_j = \mathrm{Hom}_A(e_jA, e_iA) \subset \mathrm{rad}\, A$. Поскольку $\mathrm{rad}\,(e_iAe_i) = e_iRe_i$ по предложению 2.4, отсюда и следует утверждение теоремы.

Введем теперь один класс алгебр, играющий основную роль в теории конечномерных алгебр.

**Теорема 5.4.** *Следующие условия равносильны:*

1) *факторалгебра* $\bar{A} = A/R$, *где* $R = \mathrm{rad}\, A$, *изоморфна прямому произведению тел;*

2) *если* $A = P_1 \oplus \ldots \oplus P_s$ *— разложение регулярного модуля в прямую сумму главных, то* $P_i \not\simeq P_j$ *при* $i \neq j$;

3) *существует такая алгебра* $B$ *и такой* $B$*-модуль* $M$, *что* $A \simeq E_B(M)$ *и* $M = M_1 \oplus \ldots \oplus M_s$, *где* $M_i$ *— неразложимые модули и* $M_i \not\simeq M_j$, *при* $i \neq j$.

Доказательство. 1) $\Rightarrow$ 2). Если $\bar{A} \simeq D_1 \times \ldots \times D_s$, где $D_i$ — тела, то по следствию 3.9 $A \simeq P_1 \oplus \ldots \oplus P_s$, причем $P_i/P_iR \simeq U_i$, где $U_i$ — простой $D_i$-модуль. $P_i$ — главные модули и $P_i \not\simeq P_j$ при $i \neq j$, поскольку $U_i \not\simeq U_j$ при $i \neq j$.

2) $\Rightarrow$ 3) следует из теоремы I.7.1: достаточно положить $B = A$, а за $M$ принять регулярный $A$-модуль.

3) $\Rightarrow$ 1) непосредственно следует из теоремы 5.2.

Алгебра $A$, удовлетворяющая условиям теоремы 5.4, называется приведенной.

Пусть $A$ — произвольная алгебра, $A \simeq n_1P_1 \oplus \ldots \oplus n_sP_s$ — разложение регулярного $A$-модуля в прямую сумму главных, причем $P_i \not\simeq P_j$ при $i \neq j$. Обозначим $P = P_1 \oplus \ldots \oplus P_s$ и $B = E_A(P)$. Тогда $B$ — приведенная алгебра, которая называется базисной алгеброй алгебры $A$. Если $1 = e_1 + \ldots + e_s$ — разложение единицы алгебры $B$, соответствующее данному разложению модуля $P$, то будем говорить, что главный $B$-модуль $Q_i = e_iB$ соответствует главному $A$-модулю $P_i$, а проективный $B$-модуль $Q = k_1Q_1 \oplus \ldots \oplus k_sQ_s$ соответствует проективному $A$-модулю $P = k_1P_1 \oplus \ldots \oplus k_sP_s$.

**Лемма 5.5.** *Если* $B$ *— базисная алгебра алгебры* $A$, $Q_1$, $Q_2$ *— проективные* $B$*-модули, соответствующие проективным* $A$*-модулям* $P_1$, $P_2$, *то* $\mathrm{Hom}_B(Q_1, Q_2) \simeq \mathrm{Hom}_A(P_1, P_2)$.

Доказательство, ввиду матричной записи эндоморфизмов, введенной в § 7 гл. I, сводится к проверке изоморфизма $\mathrm{Hom}_B(Q_j, Q_i) \simeq \mathrm{Hom}_A(P_j, P_i)$, где $Q_i$ — главные $B$-модули, соответствующие главным $A$-модулям $P_i$. Но и $\mathrm{Hom}_B(Q_j, Q_i)$ и $\mathrm{Hom}_A(P_j, P_i)$ отождествляется с $e_iBe_j$, что и доказывает лемму.

**Теорема 5.6.** *Следующие условия равносильны:*

1) *базисные алгебры алгебр* $A_1$ и $A_2$ *изоморфны;*

2) $A_2 \simeq E_{A_1}(P)$, *где* $P$ *— проективный* $A_1$*-модуль, в который входят прямыми слагаемыми все главные* $A_1$*-модули;*

3) $A_2 \simeq E_{A_1}(P_1)$ и $A_1 \simeq E_{A_2}(P_2)$, *где* $P_i$ *— проективные* $A_i$*-модули* $(i = 1, 2)$.

Доказательство. 1) $\Rightarrow$ 2). Пусть $B$ — общая базисная алгебра алгебр $A_1$ и $A_2$, $Q$ — проективный $B$-модуль, соответствующий регулярному $A_2$-модулю, $P$ — проективный $A_1$-модуль, соответствующий $Q$. Тогда в $Q$ входят прямыми слагаемыми все главные $B$-модули. Значит, в $P$ входят все главные $A_1$-модули и по лемме 5.5 $A_2 \simeq E_{A_2}(A_2) \simeq E_B(Q) \simeq E_{A_1}(P)$.

Заметим, что, поскольку условие 1) симметрично, мы заодно доказали и импликацию 1) $\Rightarrow$ 3).

2) $\Rightarrow$ 1). Пусть $P = k_1P_1 \oplus \ldots \oplus k_sP_s$, где $P_1, \ldots, P_s$ — все попарно неизоморфные главные $A_1$-модули, $A_2 = E_{A_1}(P)$. Из теоремы 5.2 вытекает, что $A_2/\operatorname{rad} A_2 \simeq M_{k_1}(D_1) \times \ldots \times M_{k_s}(D_s)$, где $D_i = B_i/\operatorname{rad} B_i$, а $B_i = E_{A_1}(P_i)$. Поэтому у $A_2$ есть $s$ простых модулей, а значит, и $s$ главных $P'_1, \ldots, P'_s$ (следствие 2.9), причем, как и в лемме 5.5, легко установить, что $\operatorname{Hom}_{A_2}(P'_j, P'_i) \simeq \operatorname{Hom}_{A_1}(P_j, P_i)$. Но тогда $E_{A_2}(P'_1 \oplus \ldots \oplus P'_s) \simeq E_{A_1}(P_1 \oplus \ldots \oplus P_s)$, что и требовалось доказать.

3) $\Rightarrow$ 2). Если $A_2 \simeq E_{A_1}(P_1)$, где $P_1 = k_1Q_1 \oplus \ldots \oplus k_sQ_s$, а $Q_i$ — попарно неизоморфные главные $A_1$-модули, то из теоремы 5.2 следует, что у $A_2$ есть $s$ простых, а потому и $s$ главных модулей. Аналогично, если $A_1 \simeq E_{A_2}(P_2)$, где $P_2 = m_1Q'_1 \oplus \ldots \oplus m_tQ'_t$, а $Q'_i$ — попарно неизоморфные главные $A_2$-модули, то у $A_1$ есть $t$ главных модулей. Отсюда следует, что $s \leqslant t$ и $t \leqslant s$, т. е. $s = t$ и $Q_1, \ldots, Q_s$ — все главные $A_1$-модули.

Алгебры, удовлетворяющие условия теоремы 5.6, называются *однотипными*. Очевидно, для полупростых алгебр это понятие совпадает с введенным в § 6 гл. II.

**Следствие 5.7.** *Всякая алгебра $A$ изоморфна алгебре эндоморфизмов проективного модуля $P$ над приведенной алгеброй $B$. Алгебра $B$ определена однозначно (с точностью до изоморфизма) и изоморфна базисной алгебре алгебры $A$.*

Отметим, что модуль $P$, вообще говоря, определен неоднозначно (см. упражнение 16 этой главы).

## § 6. Схема алгебры

Полученные результаты позволяют наметить некоторый подход к исследованию строения неполупростых алгебр. При этом, учитывая следствие 5.7, можно ограничиться приведенными алгебрами.

Пусть $P_1, \ldots, P_s$ — все попарно неизоморфные главные модули над алгеброй $A$ (по следствию 2.9, их число равно числу простых компонент алгебры $\bar{A} = A/R$, где $R = \operatorname{rad} A$). Обозначим $R_i = P_iR$ и $V_i = R_i/R_iR$. $V_i$ — полупростой модуль, так что $V_i \simeq \simeq \bigoplus_{j=1}^{s} t_{ij}U_j$, где $U_j = P_j/R_j$ —простые модули (ввиду теоремы 3.7, это равносильно изоморфизму $P(R_i) \simeq \bigoplus_{j=1}^{s} t_{ij}P_j$). Сопоставим каждому модулю $P_i$ точку на плоскости, которую будем обозначать номером $i$, и соединим точку $i$ с точкой $j$ $t_{ij}$ стрелками. Полученный на-

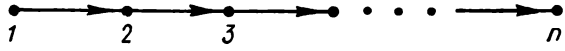
бор точек и стрелок назовем *схемой алгебры* $A$ и будем обозначать $S(A)$.

Рассматривая левые модули, можно аналогичным образом определить *левую схему алгебры* $S'(A)$.

Заметим, что однотипные алгебры имеют одинаковые схемы. Кроме того, так как $V_i = P_iR/P_iR^2$, схемы алгебр $A$ и $A/R^2$ совпадают.

**Примеры.** 1. Если алгебра $A$ полупроста, то $R_i = 0$ и $S(A)$ — это просто набор точек без стрелок.

2. Пусть $A = T_n(K)$ — алгебра треугольных матриц размерности $n$. Матричные единицы $e_{ii}$ являются ее минимальными идемпотентами, а $1 = e_{11} + \ldots + e_{nn}$ — разложением единицы. Поскольку, как легко видеть, $[e_{ii}A : K] = n - i + 1$, $P_i = e_{ii}A$ — попарно неизоморфные главные $A$-модули. Из теоремы 5.3 непосредственно следует, что $R_i = e_{i(i+1)}K + \ldots + e_{in}K \simeq P_{i+1}$. Поэтому $S(A)$ имеет вид




3. Жорданова алгебра $J_n(K)$ локальна, и ее радикал цикличен (проверьте это). Поэтому единственный главный модуль — это регулярный, и он является проективным накрытием своего радикала. Следовательно, схема алгебры $J_n(K)$ имеет вид

Вообще *схемой* $S$ мы будем называть произвольный конечный набор точек, соединенных между собой стрелками. Обычно точки мы будем обозначать номерами 1, 2, ..., $s$. Тогда схема $S$ задается своей *матрицей инцидентности*

$$[S] = \begin{pmatrix} t_{11}\, t_{12} \ldots t_{1s} \\ t_{21}\, t_{22} \ldots t_{2s} \\ \ldots\ldots\ldots \\ t_{s1}\, t_{s2} \ldots t_{ss} \end{pmatrix},$$

где $t_{ij}$ — число стрелок, ведущих из точки $i$ в точку $j$. Если стрелка $\sigma$ схемы $S$ соединяет точку $i$ с точкой $j$, то $i$ называется *началом*, а $j$ — *концом* стрелки $\sigma$. Это обозначается так: $\sigma: i \to j$.

Две схемы, $S$ и $T$, называются *изоморфными*, если между их точками и стрелками можно установить взаимно однозначное соответствие, при котором начала и концы соответствующих стрелок переходят друг в друга. Нетрудно убедиться в том, что $S \simeq T$ тогда и только тогда, когда матрицы инцидентности $[S]$ и $[T]$ можно перевести друг в друга одновременными перестановками одноименных строк и столбцов. В частности, схема алгебры, конечно, определена однозначно с точностью до изоморфизма.

*Путь* схемы $S$ — это упорядоченный набор стрелок $\{\sigma_1, \ldots, \sigma_k\}$, такой, что конец стрелки $\sigma_i$ совпадает с началом стрелки $\sigma_{i+1}$ $(i = 1, \ldots, k-1)$. Число стрелок $k$ называется *длиной* пу-

т и. Начало стрелки $\sigma_1$ называется **началом пути**, а конец стрелки $\sigma_k$ — **концом пути**. Мы будем говорить, что путь **соединяет** точку $i$ с точкой $j$, и писать $\sigma_1 \dots \sigma_k : i \to j$.

Будем считать алгебру $A$ приведенной. Тогда $\bar{A} \simeq D_1 \times \dots \times D_s$, где $D_i = E_A(U_i)$, а $U_i$ можно рассматривать как регулярный $D_i$-модуль. Пусть $1 = \bar{e}_1 + \dots + \bar{e}_s$ — разложение единицы алгебры $\bar{A}$, такое, что $\bar{e}_i\bar{A} \simeq D_i$, $1 = e_1 + \dots + e_s$ — соответствующее разложение единицы алгебры $A$ (см. следствие 3.9). В этом случае $P_i = e_iA$; $R_i = e_iR$, а $V_i = e_iV$, где $V = R/R^2$. Обозначим $V_{ij} = e_iVe_j$. $V_{ij}$ есть правый $D_i$-модуль, причем $V_{ij} \simeq t_{ij}U_j$. Поэтому $\mu_{D_j}(V_j) = t_{ij}$. Выберем в $V_{ij}$ систему образующих из $t_{ij}$ элементов и занумеруем их стрелками схемы $S(A)$, ведущими из $i$ в $j$ (их также $t_{ij}$ штук). Пусть $v_\sigma$ — образующий, соответствующий стрелке $\sigma : i \to j$, а $r_\sigma$ — его прообраз в $R_{ij} = e_iRe_j$. Совокупность всех элементов $\{v_\sigma\}$ (по всем стрелкам схемы $S$) — это система образующих модуля $V$. По лемме Накаямы (следствие 1.5) $\{r_\sigma\}$ — система образующих $R$ (как правого идеала). Заметим, что если $\sigma : i \to j$, то $e_ir_\sigma = r_\sigma e_j = r_\sigma$, а $r_\sigma r_\tau = 0$, если конец стрелки $\sigma$ не совпадает с началом $\tau$.

**Лемма 6.1.** *Если никакой путь схемы $S(A)$ не ведет из точки $i$ в точку $j$ ($i \neq j$), то $\mathrm{Hom}_A(P_j, P_i) = 0$. Если алгебра $A$ приведенная, то всякий элемент $r \in R_{ij}$ представим в виде $r = \Sigma r_{\sigma_1} r_{\sigma_2} \dots r_{\sigma_k} a_{\sigma_1\sigma_2} \dots$ $\dots \sigma_k$, где сумма берется по всем путям $\sigma_1\sigma_2 \dots \sigma_k : i \to j$, а $a_{\sigma_1\sigma_2} \dots$ $\dots \sigma_k \in A_{jj} = e_jAe_j$.*

Доказательство. По лемме 5.5 алгебру $A$ можно считать приведенной, а тогда по теореме 5.3 $\mathrm{Hom}_A(P_j, P_i) \simeq e_iAe_j = R_{ij}$ (при $i \neq j$). Поэтому достаточно доказать второе утверждение. Рассуждения, приведенные выше, показывают, что если $r \in R_{ij}$, то $r \equiv \Sigma r_\sigma a_\sigma \pmod{R^2}$, где $a_\sigma \in A_{ij}$, а сумма берется по всем стрелкам $\sigma : i \to j$. Тогда элемент $r' = r - \Sigma r_\sigma a_\sigma$ лежит в $e_iR^2e_j$. Но $R = \sum_{i,j} R_{ij}$, откуда следует, что $e_iR^2e_j = \sum_k R_{ik}R_{kj}$, т.е. $r' = \sum_k x_k y_k$, где $x_k \in R_{ik}$, $y_k \in R_{kj}$. Снова $x_k \equiv \sum_\tau r_\tau a_\tau \pmod{R^2}$, где $\tau : i \to k$, $a_\tau \in A_{kk}$, а $a_\tau y_k \equiv \sum_p r_p a_{\tau p} \pmod{R^2}$, где $p : k \to j$, $a_{\tau p} \in A_{jj}$. Поэтому $r' \equiv \Sigma r_\tau r_p a_{\tau p} \pmod{R^3}$, где $\tau p : i \to j$. Продолжая этот процесс и учитывая нильпотентность радикала, мы и получим искомое выражение для $r$. Отметим, что возможно $\mathrm{Hom}_A(P_j, P_i) = 0$, даже если из $i$ в $j$ ведет путь (см. упражнение 12).

Схема $S$ называется **связной**, если ее нельзя разбить на два непустых непересекающихся подмножества, не соединенных между собой стрелками.

**Теорема 6.2.** *Алгебра $A$ неразложима в прямое произведение тогда и только тогда, когда схема $S(A)$ связна.*

Доказательство. Пусть схема $S = S(A)$ несвязна, $S = S_1 \cup S_2$, причем $S_1 \cap S_2 = \varnothing$, $S_1 \neq \varnothing$, $S_2 \neq \varnothing$ и точки из $S_1$ и $S_2$ не соединены стрелками. Тогда по лемме 6.1, если $i \in S_1$, $j \in S_2$, то $\mathrm{Hom}_A(P_i, P_j) = 0$ и $\mathrm{Hom}_A(P_j, P_i) = 0$. По следствию I.7.9 алгебра $A$ разложима. Наоборот, если алгебра $A$ разложима $A = A_1 \times A_2$, то для любого главного $A_1$-модуля $P_i$ и любого главного $A_2$-модуля $P_j$ $\mathrm{Hom}_A(P_i, P_j) = 0$ и $\mathrm{Hom}_A(P_j, P_i) = 0$, поэтому точки $i$ и $j$ не соединены и схема $S(A)$ несвязна.

**Следствие 6.3.** *Алгебры $A$ и $A/R^2$ разложимы или неразложимы одновременно.*

Кроме схемы $S(A)$, у алгебры $A$ есть еще ряд важных инвариантов. Это прежде всего тела $D_i = E_A(U_i)$ и кратности $n_i$, с которыми $P_i$ входит в разложение регулярного модуля. Для приведенной алгебры $n_i = 1$, но тела $D_i$ могут быть произвольными. Если поле $K$ алгебраически замкнуто, положение значительно упрощается: все $D_i$ совпадают с основным полем $K$.

Алгебру $A$ над полем $K$ назовем расщепимой, если $A/R \simeq M_{n_1}(K) \times \ldots \times M_{n_s}(K)$. Над алгебраически замкнутым полем все алгебры расщепимы.

Для расщепимых алгебр лемму 6.1 можно несколько усилить.

**Лемма 6.4.** *Пусть $A$ — приведенная расщепимая алгебра. Тогда всякий элемент $r \in R_{ij}$ можно представить в виде $r = \Sigma r_{\sigma_1} r_{\sigma_2} \ldots r_{\sigma_k} c_{\sigma_1 \sigma_2 \ldots \sigma_k}$, где $c_{\sigma_1 \sigma_2 \ldots \sigma_k} \in K$, а сумма берется по всем путям $\sigma_1 \sigma_2 \ldots \sigma_k : i \to j$* (отметим, что здесь возможно и $i = j$).

Доказательство. Дословно повторяется доказательство леммы 6.1, если заметить, что в данном случае $A_{jj}/R_{jj} = K$, т. е. всякий элемент алгебры $A_{jj}$ представим в виде $c + x$, где $c \in K$, $x \in R_{jj}$.

Циклом схемы $S$ называется путь, у которого начало и конец совпадают.

**Следствие 6.5.** *Если в схеме приведенной расщепимой алгебры $A$ нет циклов, то $E_A(P) = K$ для любого главного $A$-модуля $P$.*

Лемма 6.4 дает возможность по всякой схеме $S$ построить $K$-алгебру $K(S)$, вообще говоря, бесконечномерную, такую, что всякая приведенная расщепимая алгебра с данной схемой является ее факторалгеброй.

Базис пространства $K(S)$ будут образовывать всевозможные пути схемы $S$ и набор символов $\{\varepsilon_i\}$ (по одному для каждой точки $i$). Таким образом, всякий элемент $K(S)$ однозначно записывается в виде $\sum_{i=1}^{s} c_i \varepsilon_i + \sum c_{\sigma_1 \ldots \sigma_k} \sigma_1 \ldots \sigma_k$ (вторая сумма берется по всем путям схемы $S$), где $c_i \in K$, $c_{\sigma_1 \ldots \sigma_k} \in K$. Символ $\varepsilon_i$ нам будет удобно рассматривать как путь длины 0 с началом и концом в точке $i$.

Определим произведение путей $\alpha$ и $\beta$ как путь $\alpha\beta$, если конец $\alpha$ совпадает с началом $\beta$, и как 0 — в противном случае. Иными словами,

$$(\sigma_1 \dots \sigma_k)(\tau_1, \dots \tau_l) = \begin{cases} \sigma_1 \dots \sigma_k \tau_1 \dots \tau_l, \text{ если конец } \sigma_k \text{ совпадает с} \\ \text{началом } \tau_1, \\ 0 \text{ — в противном случае;} \end{cases}$$

$$\varepsilon_i \sigma_1 \dots \sigma_k = \begin{cases} \sigma_1 \dots \sigma_k, \text{ если } i \text{ — начало } \sigma_1, \\ 0 \text{ — в противном случае;} \end{cases}$$

$$\sigma_1 \dots \sigma_k \varepsilon_i = \begin{cases} \sigma_1 \dots \sigma_k, \text{ если } i \text{ — конец } \sigma_k, \\ 0 \text{ — в противном случае;} \end{cases}$$

$$\varepsilon_i \varepsilon_j = \begin{cases} \varepsilon_i \text{ при } i = j, \\ 0 \text{ при } i \neq j. \end{cases}$$

Распространим это определение на все пространство $K(S)$ «по линейности», положив $\left(\sum_\alpha c_\alpha \alpha\right)\left(\sum_\beta c'_\beta \beta\right) = \sum_{\alpha,\beta} c_\alpha c'_\beta (\alpha\beta)$, где $\alpha, \beta$ — пути схемы $S$, а $c_\alpha$, $c'_\beta$ — элементы поля $K$. Тривиальная проверка показывает, что таким образом $K(S)$ превращается в алгебру над полем $K$ с единицей $1 = \varepsilon_1 + \dots + \varepsilon_s$.

Обозначим через $J$ совокупность тех элементов алгебры $K(S)$, у которых коэффициенты при $\varepsilon_i$ равны 0 для всех $i$. Очевидно, $J$ — идеал в $K(S)$. Идеал $I \subset K(S)$ назовем правильным, если $J^2 \supset I \supset J^n$ для некоторого $n \geqslant 2$.

**Теорема 6.6.** *Для любого правильного идеала $I \subset K(S)$ факторалгебра $K(S)/I$ есть расщепимая приведенная алгебра со схемой $S$. Наоборот, всякая расщепимая приведенная алгебра со схемой $S$ изоморфна факторалгебре алгебры $K(S)$ по некоторому правильному идеалу $I$.*

Доказательство. Обозначим $A_n = K(S)/J^{n+1}$ $(n \geqslant 1)$. Базис алгебры $A_n$ образуют классы $\bar{\alpha} = \alpha + J^{n+1}$, где $\alpha$ — произвольный путь схемы $S$ длины не более $n$. $\bar{J} = J/J^{n+1}$ — нильпотентный идеал в $A_n$, причем $A_n/\bar{J} \simeq K(S)/J \simeq K^s$ (базис этой алгебры образуют классы $\bar{\varepsilon}_i = \varepsilon_i + J$, а $\varepsilon_i \varepsilon_j = \delta_{ij}\varepsilon_i$). По предложению 1.13 $\bar{J} = \operatorname{rad} A_n$. Таким образом, $A_n$ — приведенная расщепимая алгебра, причем $A_n/J^2 \simeq A_1$, т. е. $S(A_n) = S(A_1)$. Но в алгебре $A_1$ $\bar{\varepsilon}_i \bar{J} \bar{\varepsilon}_j$ — это векторное пространство над $K$ с базисом $\{\bar{\sigma}\}$, где $\sigma$ — стрелки, ведущие из $i$ в $j$. Поэтому если $[S] = (t_{ij})$ — матрица инцидентности схемы $S$, то $\bar{\varepsilon}_i \bar{J} \bar{\varepsilon}_j \simeq t_{ij} U_j$, где $U_j = \varepsilon_j A_1 / \bar{\varepsilon}_j \bar{J}$, и $S(A_1) = S$. Отсюда следует первое утверждение теоремы (с учетом следствия 1.14).

Пусть теперь $A$ — произвольная приведенная расщепимая алгебра со схемой $S$, $1 = e_1 + \ldots + e_s$ — разложение единицы на минимальные идемпотенты, $\{r_\sigma\}$— система образующих радикала, построенная выше (перед леммой 6.1).

Для всякого пути $\alpha = \sigma_1 \ldots \sigma_k$ схемы $S$ обозначим $r_\alpha = r_{\sigma_1} \ldots r_{\sigma_k}$, $r_{e_i} = e_i$ и положим $f\left(\sum_\alpha c_\alpha \alpha\right) = \sum_\alpha c_\alpha r_\alpha$. Из соотношений между $r_\sigma$ и $e_i$ следует, что $f$ — гомоморфизм алгебры $K(S)$ в алгебру $A$, а ввиду леммы 6.4 и эпиморфизм. Поэтому $A \simeq K(S)/I$, где $I = \operatorname{Ker} f$. Но, как легко видеть, $f(J) = R$, где $R = \operatorname{rad} A$. Поскольку $R^n = 0$ для некоторого $n$, $J^n \subset I$. Наконец, элементы $v_\sigma = r_\sigma + R^2$ линейно независимы в $R/R^2$, поэтому гомоморфизм $A_1 \to A/R^2$ есть изоморфизм, т. е. $I \subset J^2$. Теорема полностью доказана.

Алгебра $K(S)$ называется алгеброй путей, или универсальной алгеброй схемы $S$.

Аналогичную конструкцию, конечно, можно дать и для левых схем. Однако имеет место такое предложение.

**Предложение 6.7.** *Если $A$ — расщепимая алгебра, то схема $S'(A)$ получается из схемы $S(A)$ переворотом всех стрелок, или транспонированием матрицы инцидентности.*

Доказательство. Алгебру $A$ можно считать приведенной. Тогда, как мы уже видели, $[S(A)] = (t_{ij})$, где $t_{ij}$— размерность пространства $e_i V e_j$ ($V = R/R^2$, а $1 = e_1 + \ldots + e_s$ — разложение единицы на минимальные идемпотенты). Аналогично $[S'(A)] = (t'_{ij})$, где $t'_{ij}$ — размерность $e_j V e_i$, т. е. $t_{ij} = t'_{ji}$, что и требовалось доказать.

## § 7. Наследственные алгебры

Конструкция универсальной алгебры позволяет дать описание одного интересного класса алгебр — наследственных.

Алгебра $A$ называется наследственной, если в ней любой правый идеал проективен[8].

**Теорема 7.1.** *Следующие условия равносильны:*

1) *алгебра $A$ наследственна;*

2) *всякий подмодуль главного $A$-модуля проективен;*

3) *всякий подмодуль проективного $A$-модуля проективен;*

4) $\operatorname{rad} A$ *проективен (как правый $A$-модуль).*

Доказательство. 1) $\Rightarrow$ 2) и 3) $\Rightarrow$ 1) как частный случай.

2) $\Rightarrow$ 4). Если $A = P_1 \oplus \ldots \oplus P_n$, где $P_i$ — главные модули, то $\operatorname{rad} A = R = R_1 \oplus \ldots \oplus R_n$, где $R_i = \operatorname{rad} P_i$. Поэтому из проективности всех $R_i$ следует проективность $R$.

4) $\Rightarrow$ 3) Пусть $M$ — подмодуль проективного $A$-модуля $P$. Проективность $M$ будем доказывать индукцией по $l(P) = l$. База ин-

[8] Аналогично можно ввести наследственные слева алгебры. Однако в гл. VIII мы увидим, что для конечномерных алгебр эти два понятия совпадают.

дукции, $l = 1$, тривиальна, так что можно считать, что если $l(P) < l$, то предложение доказано.

У модуля $P$ есть главное прямое слагаемое $P_1 : P = P_1 \oplus P_2$ (возможно, $P_2 = 0$). Обозначим через $\pi$ проекцию $P$ на $P_1$. Если $\pi(M) = P_1$, то по теореме 3.5 $M \simeq P_1 \oplus N$, где $N = M \cap P_2$ — подмодуль в $P_2$. Поскольку $l(P_2) < l$, $N$ (а вместе с ним и $M$) проективен.

Если же $\pi(M) \neq P_1$, то $M \subset R_1 \oplus P_2$, где $R_1 = P_1 R$ — прямое слагаемое радикала и потому проективный модуль. Но снова $l(R_1 \oplus P_2) < l$, потому $M$ проективен. Теорема доказана.

**Лемма 7.2.** *Если алгебра $A$ наследственна, то любой ненулевой гомоморфизм главных $A$-модулей $f : P_i \to P_j$ есть мономорфизм.*

Доказательство следует из того, что в данном случае $\operatorname{Im} f$ — проективный модуль и по теореме 3.5 $P_i \simeq \operatorname{Im} f \oplus \operatorname{Ker} f$. Значит, если $\operatorname{Im} f \neq 0$, обязательно $\operatorname{Ker} f = 0$.

**Следствие 7.3.** *Если алгебра $A$ наследственна, то в схеме $S(A)$ нет циклов.*

Доказательство. Если в $S(A)$ есть стрелка $\sigma$ с началом $i$ и концом $j$, то существует ненулевой гомоморфизм $f_\sigma : P_j \to P_j$, причем $\operatorname{Im} f_\sigma \subset \operatorname{rad} P_i$. Пусть $A$ — наследственная алгебра и $\sigma_1 \dots \sigma_k$ — путь с началом и концом в точке $i$. Тогда $f = f_{\sigma_1} \dots f_{\sigma_k}$ — мономорфизм $P_i \to P_i$, так как $f_{\sigma_1}, \dots, f_{\sigma_k}$ — мономорфизмы, и $\operatorname{Im} f \subset \operatorname{rad} P_i$, что невозможно из соотношения между размерностями.

Дадим теперь описание наследственных приведенных расщепимых алгебр.

**Теорема 7.4.** *Если $S$ — схема без циклов, то $K(S)$ — наследственная алгебра. Наоборот, наследственная приведенная расщепимая алгебра $A$ изоморфна алгебре $K(S)$, где $S = S(A)$. Таким образом, между схемами без циклов и приведенными расщепимыми наследственными алгебрами существует взаимно однозначное соответствие.*

Доказательство. Очевидно, в схеме без циклов длины путей ограничены, поэтому $A = K(S)$ — конечномерная алгебра. Обозначим $P_i = \varepsilon_i A$. Элементы $P_i$ — это линейные комбинации $\sum_\alpha c_\alpha \alpha$, где $\alpha$ — пути с началом $i$ (включая $\varepsilon_i$). Тогда $\operatorname{rad} P_i = P_i J$ состоит из линейных комбинаций $\sum_\alpha c_\alpha \alpha$, где $\alpha$ — пути ненулевой длины с началом в $i$. Поэтому $P_i J = \bigoplus_\sigma \sigma A$, где $\sigma$ пробегает все стрелки с началом в точке $i$. Но если $\sigma : i \to j$, то, сопоставляя всякой линейной комбинации $\sum_\beta c_\beta \beta$, где $\beta$ — пути с началом $j$ (включая $\varepsilon_j$), элемент $\sum_\beta c_\beta \sigma \beta$, мы получим, как легко видеть, изоморфизм $P_j \simeq \sigma A$. Следовательно, $P_i J$ — проективные модули, а потому

и $J = \bigoplus_{i=1}^{s} P_i J$ — проективный модуль, а $A$ — наследственная алгебра по теореме 7.1.

Остается проверить, что если $I \subset J^2$ и $\widetilde{A} = A/I$ — наследственная алгебра, то $I = 0$. Обозначим $R = J/I$, $\widetilde{P}_i = P_i/P_i I$. Тогда $R = \operatorname{rad} \widetilde{A}$, а $\widetilde{P}_i$ — главные $\widetilde{A}$-модули. Кроме того, $\widetilde{A}/R \simeq A/J$, а $R/R^2 \simeq J/J^2$. Покажем, что и вообще $R^k/R^{k+1} \simeq J^k/J^{k+1}$ (индукцией по $k$). Предположим, что $R^{k-1}/R^k \simeq J^{k-1}/J^k$, и пусть $\widetilde{P} = P(R^{k-1}/R^k) = \bigoplus_{i=1}^{s} m_i \widetilde{P}_i$. Тогда $\widetilde{P} = P(R^{k-1})$ (теорема 3.7), а так как $R^{k-1}$ проективен, $\widetilde{P} \simeq R^{k-1}$. Поэтому $R^k \simeq \widetilde{P}R$, а $R^k/R^{k+1} \simeq \widetilde{P}R/\widetilde{P}R^2$, и, так как $\widetilde{P}_i R/\widetilde{P}_i R^2 \simeq P_i J/P_i J^2$, отсюда следует, что $R^k/R^{k+1} \simeq J^k/J^{k+1}$. Но из этого изоморфизма, очевидно, вытекает, что $I \subset J^k$ для всех $k$, т. е. $I = 0$, что и требовалось доказать.

## *Упражнения к главе III*

1. Найти радикал алгебры $T_n(K)$.

2. Найти радикал моногенной алгебры $K[x]/f(x)K[x]$.

3. Доказать, что если алгебра $A$ не проста, то в ней найдется максимальный идеал с ненулевым аннулятором.

4. Доказать, что минимальный правый идеал либо содержится в радикале, либо является главным модулем.

5. Пусть $M$ — модуль над алгеброй $A$, $R = \operatorname{rad} A$, $\overline{A} = A/R$, $\overline{A} = n_1 U_1 \oplus \ldots \oplus n_s U_s$ — разложение $\overline{A}$ в прямую сумму простых модулей, $\overline{M} = M/MR \simeq t_1 U_1 \oplus \ldots \oplus t_s U_s$. Доказать, что $\mu_A(M) = \mu_A(\overline{M})$. Показать, что $\mu_A(M) = \max_i \left\{ \left[ \frac{t_i - 1}{n_i} \right] + 1 \right\}$ ($[t/n]$ — целая часть числа $t/n$).

6. Обозначим через $I(M)$ множество эндоморфизмов модуля $M$, образы которых лежат в $\operatorname{rad} M$.

а) Проверить, что $I(M)$ — нильпотентный идеал в $E_A(M)$.

б) Доказать, что для проективного модуля $PI(P) = \operatorname{rad} E_A(P)$.

в) Построить пример модуля $M$, для которого $I(M) \neq \operatorname{rad} E_A(M)$.

7. Доказать, что алгебра является приведенной тогда и только тогда, когда ее нильпотентные элементы образуют идеал.

8. Пусть $1 = e_1 + \ldots + e_n$ — разложение единицы алгебры $A$, в котором все идемпотенты минимальны.

а) Доказать, что размерность точного представления алгебры $A$ не меньше $n$.

Если у $A$ есть точное представление размерности $n$, $A$ назовем минимальной алгеброй степени $n$.

б) Пусть $A$ — минимальная алгебра. Будем писать $i \to j$, если $e_i A e_j \neq 0$. Доказать, что $\to$ есть отношение квазипорядка на множестве $S = \{1, 2, \ldots, n\}$, т. е. $i \to i$, и из $i \to j$ и $j \to k$ следует $i \to k$.

в) Доказать, что минимальная алгебра всегда расщепима, а приведена тогда и только тогда, когда $\to$ есть отношение порядка, т. е. из $i \to j$ и $j \to i$ следует $i = j$.

9. Предположим, что на множестве $S = \{1, 2, \ldots, n\}$ задано отношение квазипорядка $\to$. Построить минимальную алгебру $A$ степени $n$, такую, что $i \to j$ тогда и только тогда, когда $e_i A e_j \neq 0$. (Указание: рассмотреть подалгебру в $M_n(K)$ с базисом, состоящим из тех матричных единиц $e_{ij}$, для которых $i \to j$.)

10. Доказать, что две минимальные алгебры степени $n$, задающие на $S$ одно и то же отношение квазипорядка, изоморфны.

11. Найти радикал, схему и базисную алгебру минимальной алгебры. Доказать, что алгебра минимальна тогда и только тогда, когда минимальна ее базисная алгебра.

12. Пусть $R^2 = 0$, где $R = \operatorname{rad} A$; $P_1, \ldots, P_s$ — главные $A$-модули. Доказать, что $\operatorname{Hom}_A(P_j, P_i) \neq 0$, $i \neq j$, тогда и только тогда, когда в схеме $S(A)$ из $i$ в $j$ ведет стрелка.

13. Показать, что расщепимая приведенная алгебра $A$, у которой $R^2 = 0$, однозначно (с точностью до изоморфизма) определяется своей схемой.

14. Пусть $A$ — алгебра над полем вещественных чисел $\mathbf{R}$, состоящая из комплексных матриц второго порядка вида

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

где $a \in \mathbf{R}$; $b, c \in \mathbf{C}$. Найти $S(A)$ и $S'(A)$.

15. Описать трехмерные алгебры над алгебраически замкнутым полем.

16. Пусть $\varphi$ — эндоморфизм алгебры $A$, $T : A \to M_n(K)$ — представление этой алгебры, $M$ — соответствующий модуль. Обозначим через $M\varphi$ модуль, соответствующий представлению $T\varphi : A \to M_n(K)$.

а) Дать внутреннее описание модуля $M\varphi$ и проверить, что $M(\varphi\psi) \simeq (M\varphi)\psi$ а $(M \oplus N)\varphi \simeq M\varphi \oplus N\varphi$.

б) Доказать, что если $\varphi$ — автоморфизм, то модуль $P\varphi$ проективен тогда и только тогда, когда проективен модуль $P$. (Указание: проверить, что $A\varphi \simeq A$.)

в) Доказать, что если $A$ — приведенная алгебра, $P$ и $Q$ — проективные $A$-модули, то $E_A(P) \simeq E_A(Q)$ тогда и только тогда, когда $Q \simeq P\varphi$ для некоторого автоморфизма $\varphi$ алгебры $A$. (Указание: воспользоваться матричной записью эндоморфизмов.)

г) Привести пример проективного модуля $P$ над приведенной алгеброй $A$, для которого $P \not\simeq P\varphi$ при некотором автоморфизме $\varphi$ алгебры $A$.

17. Схемой с кратностями называется схема $S$, каждой точке $i$ которой сопоставлено натуральное число $n_i$. Обозначим $A = K(S)$, $P_i = \varepsilon_i A$, $P = n_1 P_1 \oplus \ldots \oplus n_s P_s$, $\widetilde{A} = E_A(P)$. Доказать для алгебры $\widetilde{A}$ аналог теоремы 6.6 с заменой приведенной расщепимой алгебры на произвольную расщепимую и схемы на схему с кратностями.

18. Доказать, что если в схеме $S$ нет циклов, то алгебра из упражнения 17 наследственна и всякая расщепимая наследственная (конечномерная) алгебра имеет такой вид.

19. Цоколем, $\operatorname{soc} M$, модуля $M$ называется сумма всех его минимальных подмодулей.

а) Показать, что $\operatorname{soc} M = M$ тогда и только тогда, когда $M$ полупрост.

б) Доказать, что при любом гомоморфизме $f : M \to N$ $f(\operatorname{soc} M) \subseteq \operatorname{soc} N$ и $f$ есть мономорфизм тогда и только тогда, когда индуцированное отображение $\operatorname{soc} M \to \operatorname{soc} N$ есть мономорфизм.

в) Доказать, что цоколи правого и левого регулярного $A$-модуля — идеалы в $A$. Они называются, соответственно, правым и левым цоколями алгебры $A$ и обозначаются $r.\operatorname{soc} A$ и $l.\operatorname{soc} A$.

г) Проверить, что $r.\operatorname{soc} A = \{a \in A \mid aR = 0\}$ $(R = \operatorname{rad} A)$, а $l.\operatorname{soc} A = \{a \in A \mid Ra = 0\}$.

д) Вычислить правый и левый цоколи алгебры $A = T_n(K)$, показать, что $r.\operatorname{soc} A \neq l.\operatorname{soc} A$.

20. Пусть $P_1, \ldots, P_s$ — все попарно неизоморфные главные $A$-модули. Проведем в $P_i$ композиционный ряд и предположим, что среди простых факторов этого ряда простой модуль $U_j = P_j/\operatorname{rad} P_j$ встречается $c_{ij}$ раз. Числа $c_{ij}$ называются числами Картана, а матрица $c(A) = (c_{ij})$ — матрицей Картана алгебры $A$.

а) Доказать, что $c(A) = c(B)$, где $B$ — базисная алгебра алгебры $A$.

б) Проверить, что если $(\operatorname{rad} A)^2 = 0$, то $c(A) = E + [S]$ ($E$ — единичная матрица, $[S]$ — матрица инцидентности схемы $S = S(A)$).

в) Обозначим $A_n = K(S)/J^{n+1}$. Доказать, что $c(A_n) = E + [S] + [S]^2 + \ldots + [S]^n$.

г) Доказать, что для наследственной алгебры $A$ матрица $[S]$, где $S = S(A)$, всегда нильпотентна, а $C(A) = \sum_{m=0}^{\infty} [S]^m$, и число Картана $c_{ij}$ совпадает с числом путей схемы $S$ с началом $i$ и концом $j$ ($i \neq j$), а $c_{ii} = 1$. (Указание: в этом случае $c_{ij} = \sum_k t_{ik} c_{kj}$ при $i \neq j$, т. е. $c(A) = [S]\, c(A) + E$, где $[S] = (t_{ij})$.)

# IV

ГЛАВА

# ЦЕНТРАЛЬНЫЕ ПРОСТЫЕ АЛГЕБРЫ

Теорема Веддербёрна—Артина сводит изучение полупростых алгебр к описанию тел над полем $K$. Если $D$ — конечномерное тело над $K$, $C$ — его центр, то $C$ — поле (расширение поля $K$), а $D$ можно рассматривать как алгебру над полем $C$. Таким образом, исследование разбивается на два этапа: изучение расширений поля $K$ и изучение центральных тел, т. е. таких тел, центр которых совпадает с основным полем. Оказывается, эти две задачи весьма непохожи друг на друга. Однако здесь удается применить единые методы исследования, основанные на понятиях бимодуля и тензорного произведения алгебр.

Настоящая глава и посвящена изложению этих методов и их применению к изучению центральных тел. Главную роль здесь будет играть, по-видимому, теорема 3.1, из которой уже сравнительно просто выводятся основные теоремы тел (теорема Сколема—Нётер и теорема о централизаторе).

## § 1. Бимодули

Пусть $A$ и $B$ — две алгебры над полем $K$, $A$-$B$-бимодулем называется векторное пространство $M$, на котором заданы структуры левого $A$-модуля и правого $B$-модуля, связанные законом ассоциативности, т. е.

$$(am)\, b = a\, (mb)$$

для любых $a \in A$, $b \in B$, $m \in M$.

Если $A = B$, то $M$ называется просто $A$-бимодулем.

Для бимодулей вводятся все те понятия, которые мы ввели в гл. I для модулей: гомоморфизм, изоморфизм, подбимодуль, факторбимодуль, прямая сумма и т. д. При этом читатель легко может убедиться, что такие основные результаты гл. I, как теорема о гомоморфизме, закон параллелограмма, теорема Жордана—Гёльдера и т. п., дословно переносятся на случай бимодулей. Впрочем, в следующем параграфе мы увидим, что изучение $A$-$B$-бимодулей на самом деле равносильно изучению модулей над некоторой новой алгеброй — тензорным произведением алгебр $A$ и $B^\circ$.

Рассмотрим ряд примеров, которые будут играть важную роль в дальнейшем и которые демонстрируют важность понятия бимодуля для структурной теории алгебр.

**Примеры.** 1. Очевидно, всякую алгебру $A$ можно рассматривать как бимодуль над собой. Этот бимодуль называется регулярным. Подбимодули регулярного бимодуля — это подпространства $I \subset A$, замкнутые относительно умножения на произвольные элементы $a \in A$ и слева, и справа, т. е. идеалы алгебры $A$. С этой точки зрения, простые алгебры — это такие, для которых регулярный бимодуль прост.

Выясним, как устроены эндоморфизмы регулярного бимодуля. Если $f : A \to A$ — такой эндоморфизм, то $f$ является, в частности, эндоморфизмом регулярного модуля, и, как было показано в теореме I.7.1, он имеет вид $f(x) = ax$, где $a$ — фиксированный элемент из $A$. Но $f$ должен быть и эндоморфизмом левого регулярного модуля, а это означает, что $f(bx) = bf(x)$ для любого $b \in A$, т. е. $abx = bax$ для всех $b$, $x \in A$, откуда следует, что $a \in C(A)$. Наоборот, если $a$ — элемент центра, то то же самое рассуждение показывает, что умножение на $a$ есть эндоморфизм регулярного бимодуля. Итак, мы установили следующее.

**Предложение 1.1.** *Подбимодули регулярного бимодуля — это идеалы алгебры. Алгебра эндоморфизмов регулярного бимодуля изоморфна центру алгебры.*

2. Пусть $f : B \to A$ — гомоморфизм алгебр. Свяжем с ним $B$-$A$-бимодуль, который будем обозначать ${}_fA$. Для этого рассмотрим регулярный $A$-модуль и определим на нем структуру левого $B$-модуля по правилу $ba = f(b)\,a$. Ассоциативность очевидна, и $A$ превращается в $B$-$A$-бимодуль, который обозначим ${}_fA$. Предыдущий пример получается из этого, если положить $B = A$, а $f$ — тождественный эндоморфизм.

3. Будем рассматривать $D$-бимодули, где $D$ — конечномерное тело над $K$. Если $M$ — такой бимодуль, то он является, в частности, векторным пространством над телом $D$. Отображение $m \to md$ при фиксированном $d \in D$ является тогда эндоморфизмом векторного пространства $M$, и при фиксированном изоморфизме $M \simeq nD$, где $n = [M : D]$, ему соответствует матрица $T(d) \in M_n(D)$, причем легко проверить, что $T(d + d') = T(d) + T(d')$; $T(\alpha d) = \alpha T(d)$ $(\alpha \in K)$; $T(dd') = T(d)\,T(d')$ и $T(1) = 1$. Говорят, что соответ-

ствие $d \to T(d)$ есть самопредставление тела $D$ размерности $n$.

Особенно интересен случай $n = 1$. Тогда $T(d) \in D$ и $T : D \to D$ есть автоморфизм тела $D$.

Наоборот, со всяким самопредставлением размерности $n$ можно связать $D$-бимодуль, рассмотрев векторное пространство $nD$ и положив $xd = xT(d)$, $x \in nD$. В частности, со всяким автоморфизмом связывается $D$-бимодуль $M$, такой, что $[M : D] = 1$.

## § 2. Тензорные произведения

С понятием модуля мы связали в гл. I понятие представления, т. е. линейного отображения, согласованного с умножением. Попытаемся осуществить подобную конструкцию для бимодулей.

Пусть $M$ является $A$-$B$-бимодулем. Тогда всякой паре элементов $(a, b)$, $a \in A$, $b \in B$ сопоставляется эндоморфизм $M$ как векторного пространства: $m \to amb$. Таким образом, мы получаем отображение $A \times B \to E(M)$, причем легко убедиться, что оно билинейно (т. е. при фиксированном $a$ линейно по $b$ и наоборот). Итак, забывая на время об умножении, мы приходим к необходимости классифицировать билинейные отображения $U \times V \to W$, где $U$, $V$, $W$ — векторные пространства над полем $K$.

Выберем базисы $\{u_1, \ldots, u_n\}$ и $\{v_1, \ldots, v_m\}$ в пространствах $U$ и $V$. Тогда билинейное отображение $F$: $U \times V \to W$ однозначно определяется значениями $F(u_i, v_j) = w_{ij}$, причем $w_{ij}$ можно задавать произвольно. Это приводит к следующему определению.

Тензорным произведением пространства $U$ с базисом $\{u_1, \ldots, u_n\}$ и пространства $V$ с базисом $\{v_1, \ldots, v_m\}$ называется векторное пространство $U \otimes V$ с базисом $\{u_i \otimes v_j\}$, $i = 1, \ldots, n$; $j = 1, \ldots, m$, и фиксированным билинейным отображением $\otimes : U \times V \to U \otimes V$, определенным по правилу $\otimes(u_i, v_j) = u_i \otimes v_j$. Образ пары $(u\ v)$ при отображении $\otimes$ обозначается $u \otimes v$.

Приведенные выше рассуждения устанавливают универсальное свойство тензорного произведения.

**Теорема 2.1.** *Для всякого билинейного отображения $F$: $U \times V \to W$ существует единственное линейное отображение $\tilde{F} : U \otimes V \to W$, такое, что $F = \tilde{F} \otimes$ (т. е. $F(u, v) = \tilde{F}(u \otimes v)$).*

**Следствие 2.2.** *Если $\Phi : U \times V \to W_0$ — такое билинейное отображение, что для всякого билинейного отображения $F : U \times V \to W$ существует единственное отображение $\tilde{F} : W_0 \to W$, такое, что $\tilde{F}\Phi = F$, то существует единственный изоморфизм $\varphi : W_0 \rightleftarrows U \otimes V$, такой, что $u \otimes v = \varphi\Phi(u, v)$ для всех элементов $u \in U$, $v \in V$.*

Доказательство. Из условия теоремы следует существование и единственность гомоморфизма $\varphi : W_0 \to U \otimes V$, для которого $u \otimes v = \varphi\Phi(u, v)$. С другой стороны, из теоремы 2.1 следует, что существует гомоморфизм $\tilde{\Phi} : U \otimes V \to W_0$, для кото-

рого $\tilde{\Phi}(u \otimes v) = \Phi(u, v)$. Но тогда $\varphi\tilde{\Phi}(u \otimes v) = \varphi\Phi(u, v) = u \otimes v$, откуда по теореме 2.1 следует, что $\varphi\tilde{\Phi} = 1$. Аналогично $\tilde{\Phi}\varphi\Phi(u, v) = \tilde{\Phi}(u \otimes v) = \Phi(u, v)$, откуда следует, что $\tilde{\Phi}\varphi = 1$, т. е. $\tilde{\Phi}$ — обратное отображение к $\varphi$.

Существование и единственность изомофизма $\varphi$ позволяет отождествлять всякое пространство $W_0$, удовлетворяющее условию следствия 2.2, с тензорным произведением $U \otimes V$. При этом, в частности, отождествляются все тензорные произведения, получающиеся при различном выборе базисов в $U$ и $V$.

Кроме того, теорема 2.1 позволяет установить основные свойства тензорного произведения.

**Предложение 2.3.** *Для любых пространств $U$, $V$, $W$ существует единственный изоморфизм $f: U \otimes V \simeq V \otimes U$, такой, что $f(u \otimes v) = v \otimes u$, и единственный изоморфизм $g: (u \otimes V) \otimes W \simeq U \otimes (V \otimes W)$, такой, что $g((u \otimes v) \otimes w) = u \otimes (v \otimes w)$.*

Доказательство. Поскольку $(u, v) \to v \otimes u$ есть, очевидно, билинейное отображение, существует единственный гомоморфизм $f: U \otimes V \to V \otimes U$, для которого $f(u \otimes v) = v \otimes u$. Но, аналогично, существует гомоморфизм $f': V \otimes U \to U \otimes V$, для которого $f'(v \otimes u) = u \otimes v$, и из теоремы 2.1 сразу следует, что $f$ и $f'$ — взаимно обратные изоморфизмы.

Пусть теперь $F$ — билинейное отображение $(U \otimes V) \times W \to Z$. При фиксированном $w \in W$ оно превращается в линейное отображение $F_w: U \otimes V \to Z$, т. е. в билинейное отображение $U \times V \to Z$, причем, очевидно, $F_w$ зависит от $w$ линейно. Поэтому при фиксированном $u \in U$ отображение $V \times W \to Z$, сопоставляющее паре $(v, w)$ вектор $F_w(u, v)$, билинейно и потому определяет линейное отображение $V \otimes W \to Z$, линейно зависящее от $u$. Тем самым определяется билинейное отображение $U \times (V \otimes W) \to Z$. Переходя к тензорным произведениям, мы всякому линейному отображению $(U \otimes V) \otimes W \to Z$ сопоставим отображение $U \otimes (V \otimes W) \to Z$ (очевидно, единственное). Наоборот, всякому отображению $U \otimes (V \otimes W) \to Z$ сопоставляется единственное отображение $(U \otimes V) \otimes W \to Z$. Полагая вначале $Z = (U \otimes V) \otimes W$, а затем $Z = U \otimes (V \otimes W)$, мы получим требуемый изоморфизм $g$ и обратный к нему.

В дальнейшем мы будем отождествлять $U \otimes V$ и $V \otimes U$, а также $(U \otimes V) \otimes W$ и $U \otimes (V \otimes W)$ (и писать без скобок $U \otimes V \otimes W$).

Всякий элемент из $U \otimes V$, по определению, однозначно представим в виде $\sum_{i,j} \alpha_{ij}(u_i \otimes v_j)$. Полагая $\sum_{i=1}^{n} \alpha_{ij} u_i = x_j$, мы можем этот элемент записать в виде $\sum_{j=1}^{m} x_j \otimes v_j$, причем легко проверить, что

эта запись однозначна. Аналогично, всякий элемент из $U \otimes V$ однозначно записывается в виде $\sum_{i=1}^{n} u_i \otimes y_i$, $y_i \in V$.

Если $U'$ — подпространство в $U$, то $(u', v) \to u \otimes v$ есть билинейное отображение $U' \times V \to U \otimes V$, которое определяет гомоморфизм $f: U' \otimes V \to U \otimes V$. Очевидно, если базис в $U$ выбран так, что $\{u_1, \ldots, u_k\}$ $(k \leqslant n)$ — базис $U'$, то образ $f$ состоит из элементов вида $\sum_{i=1}^{k} u_i \otimes y_i$ и $f$ есть мономорфизм, позволяющий рассматривать $U' \otimes V$ как подпространство в $U \otimes V$. При этом легко видеть, что если $U = U' \otimes U''$, то $U \otimes V = U' \otimes V \oplus U'' \otimes V$. Аналогичные утверждения верны и для подпространств пространства $V$.

Пусть теперь $A$ и $B$ — алгебры над полем $K$. Тогда при фиксированных $a_0 \in A$ и $b_0 \in B$ отображение $A \times B \to A \otimes B$, сопоставляющее паре $(a, b)$ элемент $aa_0 \otimes bb_0$, билинейно и потому продолжается до линейного отображения $F: A \otimes B \to A \otimes B$, при котором $a \otimes b \to aa_0 \otimes bb_0$. С другой стороны, $F$ билинейно зависит от $(a_0, b_0)$, поэтому мы можем любому элементу $x \in A \otimes B$ сопоставить линейное отображение $F_x$, линейно зависящее от $x$ и такое, что $F_{a_0 \otimes b_0}(a \otimes b) = aa_0 \otimes bb_0$.

Обозначив $F_x(y) = yx$, мы определим тогда в $A \otimes B$ билинейное умножение, такое, что $(a \otimes b)(a_0 \otimes b_0) = aa_0 \otimes bb_0$ для любых $a$, $a_0 \in A$, $b$, $b_0 \in B$. Поскольку $[(a \otimes b)(a' \otimes b')](a'' \otimes b'') = (aa'' \otimes bb')(a'' \otimes b'') = aa'a'' \otimes bb'b'' = (a \otimes b)[(a' \otimes b')(a'' \otimes b'')]$, а $(a \otimes b) \times (1 \otimes 1) = (1 \otimes 1)(a \otimes b) = a \otimes b$, пространство $A \otimes B$ тем самым превращается в алгебру над полем $K$, которая называется тензорным произведением алгебр $A$ и $B$.

Из предложения 2.3 вытекает, что $A \otimes B \simeq B \otimes A$ и $(A \otimes B) \otimes C \simeq A \otimes (B \otimes C)$ как алгебры.

Тензорные произведения дают возможность свести изучение бимодулей к изучению модулей.

Пусть $M$ — некоторый $A$-$B$-бимодуль. Обозначим через $A^\circ$ алгебру, обратную к $A$, т. е. состоящую из тех же элементов, но с умножением: $a^\circ b^\circ = (ba)^\circ$ (здесь $a^\circ$ обозначает элемент $a \in A$, рассматриваемый как элемент алгебры $A^\circ$). Введем на $M$ структуру модуля над алгеброй $B \otimes A^\circ$, полагая $m(b \otimes a^\circ) = amb$. Корректность этого определения и аксиомы модуля проверяются непосредственно.

Наоборот, всякий $B \otimes A^\circ$-модуль $N$ можно рассматривать как $A$-$B$-бимодуль, если положить $an = n(1 \otimes a^\circ)$, $nb = n(b \otimes 1)$. Таким образом, понятия $A$-$B$-бимодуля и $B \otimes A^\circ$-модуля фактически совпадают.

В заключение вычислим центр тензорного произведения алгебр.

**Теорема 2.4.** $C(A \otimes B) = C(A) \otimes C(B)$.

Доказательство. Выберем в $A$ подпространство $A'$, дополнительное к $C(A)$, т. е. такое, что $A = A' \oplus C(A)$ как век-

торное пространство. Тогда $A \otimes B = A' \otimes B \oplus C(A) \otimes B$. Покажем, что $C(A \otimes B) \subset C(A) \otimes B$. Действительно, пусть $c \in C(A \otimes B)$, $c = x + y$, где $x \in A' \otimes B$, $y \in C(A) \otimes B$. Тогда $c(a \otimes 1) = (a \otimes 1)c$, откуда следует, что $x(a \otimes 1) = (a \otimes 1)x$, так как $y(a \otimes 1) = (a \otimes 1)y$ автоматически.

Выберем базис $\{b_1, \ldots, b_m\}$ в $B$ и запишем $x = \sum_{i=1}^{m} x_i \otimes b_i$. Из однозначности такой записи следует, что $x_i a = a x_i$ для любого $a$, т. е. $x_i \in C(A)$. Так как $x_i \in A'$, то $x_i = 0$ и $x = 0$.

Аналогично, выбирая базис в $C(A)$ и раскладывая $C(A) \otimes B = C(A) \otimes C(B) \oplus C(A) \otimes B'$, где $B'$ — дополнение к $C(B)$, мы покажем, что $C(A \otimes B) \subset C(A) \otimes C(B)$. Но обратное включение очевидно, что и доказывает теорему.

## § 3. Центральные простые алгебры

Алгебра $A$ над полем $K$ называется центральной, если $C(A) = K$.

Мы поставили задачу изучить в этой главе центральные тела (конечномерные над $K$). Однако, как будет видно из дальнейшего, удобнее рассматривать сразу все центральные простые алгебры, т. е. алгебры вида $M_n(D)$, где $D$ — центральное тело.

Из предложения 1.1 следует, что алгебра является центральной простой тогда и только тогда, когда ее регулярный бимодуль прост, а его алгебра эндоморфизмов совпадает с $K$. Это дает возможность охарактеризовать алгебру $A \otimes A^\circ$.

Определим гомоморфизм $T$ алгебры $A \otimes A^\circ$ в алгебру эндоморфизмов $E(A)$ векторного пространства $A$, приняв за $T(a \otimes b^\circ)$ линейный оператор, переводящий $x \in A$ в $axb$.

**Теорема 3.1.** *Алгебра $A$ является простой центральной алгеброй над полем $K$ тогда и только тогда, когда гомоморфизм $T : A \otimes A^\circ \to E(A)$, определенный выше, есть изоморфизм.*

Доказательство. Если $A$ — простая центральная алгебра, то $A$ можно рассматривать как простой модуль над алгеброй $A \otimes A^\circ$ с телом эндоморфизмов $K$. Но тогда по теореме 2.6.7 гомоморфизм $T : A \otimes A^\circ \to E(A)$ есть эпиморфизм, и, так как $[A \otimes A^\circ : K] = n^2 = [E(A) : K]$, где $n = [A : K]$, $T$ является изоморфизмом.

Наоборот, если $T$ — изоморфизм, то, отождествляя $A \otimes A^\circ$ с $E(A)$, мы видим, что $A$ — простой $A \otimes A^\circ$-модуль, т. е. простой $A$-бимодуль, и его алгебра эндоморфизмов есть $K$. Иными словами, $A$ — центральная простая алгебра.

Мы применим теорему 3.1 для изучения строения алгебры $A \otimes B$, где $A$ — центральная простая, а $B$ — произвольная $K$-алгебра.

**Теорема 3.2.** *Всякий идеал алгебры $A \otimes B$, где $A$ — простая центральная алгебра, имеет вид $A \otimes I$, где $I$ — идеал алгебры $B$.*

Доказательство. Очевидно, если $I$ — идеал в $B$, то $A \otimes I$ — идеал в $A \otimes B$. Наоборот, пусть $J$ — идеал алгебры $A \otimes B$.

Выбирая базис $\{a_1, \ldots, a_n\}$ в $A$, мы можем каждый элемент из $A \otimes B$ однозначно записать в виде $\sum_{i=1}^{n} a_i \otimes b_i$, где $b_i \in B$. Рассмотрим линейный оператор $T_k$ в пространстве $A$, переводящий $a_k$ в 1, а остальные элементы базиса — в 0. По теореме 3.1 $T_k = T(y_k)$, где $y_k \in A \otimes A^\circ$: $y_k = \sum_{j=1}^{n} a_j \otimes x_j^0$, $x_j \in A$. Но тогда $\sum_{j=1}^{n} (a_j \otimes 1) \times \left(\sum_{i=1}^{n} a_i \otimes b_i\right)(x_j \otimes 1) = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_j a_i x_j \otimes b_i\right) = \sum_{i=1}^{n} (a_i T_k) \otimes b_i = 1 \otimes b_k$. Поэтому если элемент $\sum_{i=1}^{n} a_i \otimes b_i$ лежит в идеале $J$, то $(1 \otimes b_k) \in J$ для любого $k$. Пусть $I = \{b \in B \mid 1 \otimes b \in J\}$. Очевидно, $I$ — идеал в алгебре $B$, и, как мы только что показали, всякий элемент из $J$ имеет вид $\sum_{i=1}^{n} a_i \otimes b_i$, где $b_i \in I$, т. е. $J = A \otimes I$, что и требовалось доказать.

**Следствие 3.3.** *Если $A$ — центральная простая алгебра, то алгебра $A \otimes B$ проста тогда и только тогда, когда $B$ проста.*

**Следствие 3.4.** *Если $A$ — центральная простая алгебра, то* $\operatorname{rad}(A \otimes B) = A \otimes \operatorname{rad} B$ *для любой алгебры $B$.*

Доказательство следует из характеристики радикала как пересечения максимальных двусторонних идеалов.

**Следствие 3.5.** *Если $A$ — центральная простая алгебра, то алгебра $A \otimes B$ полупроста тогда и только тогда, когда алгебра $B$ полупроста.*

Комбинируя теорему 3.2 с теоремой 2.4, описывающей центр тензорного произведения, мы получаем еще такое следствие.

**Следствие 3.6.** *Если $A$ — центральная простая алгебра, то алгебра $A \otimes B$ является центральной простой тогда и только тогда, когда $B$ — центральная простая алгебра.*

## § 4. Основные теоремы теории тел

**Теорема 4.1** (Сколема—Нётер). *Если $f$ и $g$ — два гомоморфизма простой алгебры $B$ в центральную простую алгебру $A$, то в $A$ существует такой обратимый элемент $a$, что $g(b) = af(b)a^{-1}$ для всех $b \in B$.*

Доказательство. Рассмотрим $B$-$A$-бимодули ${}_fA$ и ${}_gA$ (см. § 1, пример 2). Это — модули над алгеброй $A \otimes B^\circ$, которая проста по следствию 3.4. Но поскольку размерности этих модулей совпадают (это есть $[A : K]$), по следствию 2.3.5, ${}_fA \simeq {}_gA$.

Пусть $\varphi$—изоморфизм ${}_fA$ в ${}_gA$. Тогда $\varphi$ является автоморфизмом регулярного $A$-модуля и потому имеет вид $\varphi(x) = ax$, где $a$ — фиксированный обратимый элемент из $A$. Кроме того, $\varphi$ является гомоморфизмом левых $B$-модулей, т. е. $\varphi(bx) = b\varphi(x)$. Если учесть определение ${}_fA$ и ${}_gA$, то $\varphi(f(b)x) = g(b)\varphi(x)$. Полагая $x = 1$, мы

получаем, что $af(b) = \varphi(f(b)) = g(b)\varphi(1) = g(b)a$ для любого $b \in B$, т. е. $g(b) = af(b)a^{-1}$.

Отображение $x \to axa^{-1}$, очевидно, является автоморфизмом алгебры $A$. Этот автоморфизм называется внутренним. Если $B$ — подалгебра в $A$, то $aBa^{-1} = \{aba^{-1} | b \in B\}$ также является подалгеброй. Говорят, что $B$ и $aBa^{-1}$ сопряжены в $A$.

**Следствие 4.2.** *Изоморфные простые подалгебры $B$ и $B'$ центральной простой алгебры $A$ сопряжены. Более того, всякий изоморфизм $g: B \xrightarrow{\sim} B'$ продолжается до внутреннего автоморфизма алгебры $A$, т. е. имеет вид $g(b) = aba^{-1}$, где $a$ — обратимый элемент из $A$.*

Доказательство следует из теоремы Сколема—Нётер, если наряду с $g$ рассмотреть тождественное вложение $f$ алгебры $B$ в алгебру $A$.

**Следствие 4.3.** *Всякий автоморфизм центральной простой алгебры является внутренним. В частности, всякий автоморфизм алгебры $M_n(K)$ — внутренний.*

Заметим, что в доказательстве теоремы Сколема—Нётер алгебры $A$ и $B$ по сути равноправны: мы пользовались только простотой тензорного произведения $A \otimes B^0$, для чего достаточно, чтобы одна (любая) из этих алгебр была центральной простой, а вторая — простой. Поэтому можно сформулировать «двойственную» теорему, доказательство которой предоставляется читателю.

**Теорема 4.4.** *Если $f$ и $g$ — два гомоморфизма центральной простой алгебры $B$ в простую алгебру $A$, то в $A$ существует такой обратимый элемент $a$, что $g(b) = af(b)a^{-1}$ для всех $b \in B$.*

**Следствие 4.5.** *Изоморфные центральные простые подалгебры $B$ и $B'$ простой алгебры $A$ сопряжены. Более того, всякий изоморфизм $g: B \xrightarrow{\sim} B'$ продолжается до внутреннего автоморфизма алгебры $A$, т. е. имеет вид $g(b) = aba^{-1}$, где $a$ — обратимый элемент из $A$.*

Конечно, аналог следствия 4.3 для нецентральных простых алгебр неверен. Простейший пример — это комплексное сопряжение, являющееся невнутренним автоморфизмом поля комплексных чисел как алгебры над полем вещественных чисел.

Теорема Сколема-Нётер часто называется первой основной теоремой теории тел. Вторая основная теорема связана с понятием централизатора.

Централизатором подмножества $X$ алгебры $A$ называется совокупность всех таких элементов $a \in A$, что $ax = xa$ для любого $x \in X$. Централизатор подмножества $X$ — это подалгебра в $A$, которую обозначим так: $C_A(X)$. В частном случае, когда $X = A$, $C_A(A) = C(A)$—центр алгебры.

**Теорема 4.6.** *Пусть $A$ — центральная простая алгебра, $B$ — ее простая подалгебра, $B' = C_A(B)$. Тогда:*

1) *$B'$ — простая алгебра;*
2) $C_A(B') = B$;
3) $[B : K][B' : K] = [A : K]$;
4) *если $B' \simeq M_m(D)$, то $A \otimes B^0 \simeq M_n(D)$, причем $m$ делит $n$,*

Доказательство. Рассмотрим $B$-$A$-бимодуль ${}_fA$, где $f$ — тождественное вложение $B$ в $A$. По следствию 3.4 алгебра $A \otimes B^\circ$ проста. Значит, $A \otimes B^\circ \simeq M_n(D)$, а ${}_fA \simeq mU$, где $U$ — простой модуль над $A \otimes B^\circ$. Поэтому $E_{A\otimes B^\circ}({}_fA) \simeq M_m(D)$.

Пусть $\varphi$ — эндоморфизм ${}_fA$. Тогда это эндоморфизм регулярного $A$-модуля, т. е. $\varphi$ имеет вид $\varphi(x) = ax$. Кроме того, $\varphi(bx) = b\varphi(x)$, откуда, полагая $x = 1$, получаем, что $ab = ba$ для всех $b \in B$, т. е. $a \in B'$. Наоборот, если $a \in B'$, то отображение $x \to ax$, очевидно, есть эндоморфизм ${}_fA$. Поэтому $B' \simeq E({}_fA) \simeq M_m(D)$, т. е. мы доказали утверждения 1) и 4) (кроме утверждения о делимости).

Обозначим $d = [D : K]$. Тогда $U \simeq nD$, откуда $[U : K] = nd$ и $[A : K] = mnd$. С другой стороны, $[A : K][B : K] = [A \otimes B^\circ : K] = n^2d$, а $[B' : K] = m^2d$. Отсюда следует, что $[B : K] = \dfrac{n^2d}{mnd} = \dfrac{n}{m}$, т. е. $m$ делит $n$ и $[A : K] = [B : K][B' : K]$, что доказывает 3) и 4).

Пусть, наконец, $B'' = C_A(B')$. Очевидно, $B \subset B''$. Но алгебра $B'$ проста, поэтому для нее также верно утверждение 3), откуда $[B'' : K] = [A : K]/[B' : K] = [B : K]$. Следовательно, $B'' = B$, что завершает доказательство теоремы.

**§ 5. Подполя тел. Поля расщепления**

Применим результаты предыдущего параграфа к изучению подполей центральных тел. Нас будут интересовать максимальные подполя, т. е. такие, которые не содержатся ни в каком большем подполе.

**Теорема 5.1.** *Подполе $L$ тела $G$ максимально тогда и только тогда, когда $L = C_D(L)$. Если тело $G$ центрально, то в этом случае $[D : K] = [L : K]^2$ и $D \otimes L \simeq M_n(L)$, где $n = [L : K]$.*

Доказательство. Очевидно, всякое подполе, содержащее $L$, содержится в $C_D(L)$. Поэтому если $L = C_D(L)$, то оно максимально. С другой стороны, если элемент $a$ лежит в $C_D(L)$, но не лежит в $L$, то совокупность элементов вида $f(a)$, где $f(x)$ — многочлен над полем $L$, образует коммутативную подалгебру в $D$, т. е. подполе, строго большее чем $L$. Это доказывает первое утверждение.

Пусть теперь $D$ — центральное тело, $L$ — его максимальное подполе. Тогда $L = C_D(L)$, откуда по теореме 4.6 следует, что $[D : K] = [L : K]^2$ и $D \otimes L \simeq M_n(L)$ (ввиду коммутативности $L$ $L^\circ \simeq L$). Наконец, подсчет размерностей сразу дает равенство $n = [L : K]$.

**Следствие 5.2.** *Размерность центральной простой алгебры всегда является квадратом целого числа.*

Для любой $K$-алгебры $A$ и расширения $L$ поля $K$ алгебру $A \otimes L$ можно рассматривать как $L$-алгебру, полагая $\alpha x = x(1 \otimes \alpha)$, где $x \in A \otimes L$, $\alpha \in L$. Эту $L$-алгебру мы будем обозначать $A_L$. Говорят, что $A_L$ получается из $A$ расширением поля скаляров. Очевидно, $[A_L : L] = [A : K]$.

Теорема 5.1 показывает, что если $L$ — максимальное подполе центрального тела $D$, то $D_L \simeq M_n(L)$. Очевидно, тогда $M_k(D) \otimes L \simeq M_{nk}(L)$.

Если $K$-алгебра $A$ центральна, то теорема 2.4 показывает, что $L$-алгебра $A_L$ также является центральной. В частности, если $A$ — центральная простая $K$-алгебра, то $A_L$ — центральная простая $L$-алгебра.

Поле $L$ называется п о л е м р а с щ е п л е н и я центральной простой алгебры $A$, если $A_L \simeq M_n(L)$. Из теоремы 5.1 следует, что поле расщепления всегда существует.

Однако поле расщепления, конечно, не единственно, хотя бы потому, что всякое его расширение также является полем расщепления. В самом деле, даже минимальное поле расщепления (не содержащее других полей расщепления) определяется неоднозначно (см. упражнение 6 этой главы).

Следующая теорема дает некоторую характеристику полей расщепления, которая будет полезна в дальнейшем.

**Теорема 5.3.** *Поле $L$ является полем расщепления центрального тела $D$ размерности $d^2$ тогда и только тогда, когда $[L : K] = md$ и $L$ изоморфно подалгебре алгебры $M_m(D)$.*

Д о к а з а т е л ь с т в о. Пусть $D \otimes L \simeq M_d(L)$. Рассмотрим простой $D_L$-модуль, или, что то же, простой $L$-$D$-бимодуль $U$. $U$ является правым векторным пространством над $D$, а умножение на элемент $\alpha \in L$ определяет эндоморфизм этого векторного пространства. Обозначая через $T(\alpha)$ матрицу этого эндоморфизма, мы получаем гомоморфизм (и даже мономорфизм, поскольку $L$ поле) $T : L \to M_m(D)$, где $m = [U : D]$.

С другой стороны, так как $D_L \simeq M_d(L)$, то $U \simeq dL$ и $[U : K] = d[L : K]$. Но в то же время $[U : K] = md^2$, откуда $[L : K] = md$.

Наоборот, пусть $L$ — подполе в алгебре $A = M_m(D)$ размерности $md$, $L'$ — централизатор $L$. Тогда $L' \supset L$ и по теореме 4.6 $[L : K][L' : K] = [A : K] = m^2d^2$, откуда $(L' : K] = md = [L : K]$, т. е. $L' = L$, и потому $A \otimes L \simeq M_n(L)$, т. е. $L$ — поле расщепления для $A$, а значит, и для тела $D$.

## § 6. Группа Брауэра. Теорема Фробениуса

В § 3 мы отметили, что класс центральных простых алгебр замкнут относительно тензорного умножения. Основное поле $K$ играет при этом роль единицы, поскольку $A \otimes K \simeq A$ для любой алгебры $A$. Наконец, теорема 3.1 показывает, что обратная алгебра $A^\circ$, действительно, «с точностью до матриц» является обратной к алгебре $A$ в смысле этой операции Все это позволяет определить на множестве классов изоморфизма центральных тел структуру группы следующим образом.

Зафиксируем по одному представителю в каждом классе изоморфизма центральных тел. Если $D_1$ и $D_2$ — два таких представителя, то $D_1 \otimes D_2$ — центральная простая алгебра, поэтому она изоморфна какой-то алгебре вида $M_n(D)$, где $D$ — центральное тело.

Положим $D = D_1D_2$. Из § 2 следует, что $D_1D_2 = D_2D_1$ и $D_1(D_2D_3) = (D_1D_2)D_3$. Далее $DK = KD = D$, и по теореме 3.2 $DD^\circ = D^\circ D = K$. Таким образом, наше множество центральных тел превращается в коммутативную группу. Эта группа называется группой Брауэра поля $K$ и обозначается $\mathrm{Br}(K)$.

Если $L$ — расширение поля $K$, то для всякого центрального тела $D$ $L$-алгебра $D_L$ — центральная простая, поэтому она изоморфна $M_n(D')$, где $D'$ — центральное тело над $L$. Легко проверить, что, сопоставляя $D$ тело $D'$, мы получаем гомоморфизм групп $\mathrm{Br}(K) \to \mathrm{Br}(L)$. Ядро этого гомоморфизма состоит из тех тел, для которых $L$ является полем расщепления. Эта подгруппа группы Брауэра обозначается $\mathrm{Br}(L/K)$. Теорема 5.1 показывает, что всякий элемент группы Брауэра лежит в какой-то подгруппе вида $\mathrm{Br}(L/K)$, т. е. $\mathrm{Br}(K) = \bigcup \mathrm{Br}(L/K)$.

Фактическое вычисление группы Брауэра, как правило, весьма сложно, а строение этой группы известно лишь для некоторых полей $K$. Мы ограничимся простейшими случаями: полем вещественных чисел и конечными полями (см. гл. V).

Конечно, если $K$ — алгебраически замкнутое поле, над ним нет центральных (и вообще никаких) тел, отличных от самого $K$, т. е. его группа Брауэра тривиальна.

Над полем $\mathbf{R}$ вещественных чисел есть по крайней мере одно центральное тело — тело кватернионов $\mathbf{H}$. Замечательный результат состоит в том, что это — единственное центральное тело над полем $\mathbf{R}$.

**Теорема 6.1** (Фробениус). *Единственные конечномерные тела над полем* $\mathbf{R}$ *вещественных чисел — это само поле* $\mathbf{R}$, *поле* $\mathbf{C}$ *комплексных чисел и тело кватернионов* $\mathbf{H}$.

Доказательство. Пусть вначале $L$ — конечное расширение поля $\mathbf{R}$, $a$ — произвольный элемент $L$, $m_a(x)$ — минимальный многочлен элемента $a$ над полем $\mathbf{R}$ (см. § 2 гл. I). Он неприводим и потому является либо линейным (в этом случае $a \in \mathbf{R}$), либо квадратным вида $x^2 + 2px + q$, где $p^2 < q$. Во втором случае элемент $a + p$ — корень многочлена $x^2 + (q - p^2)$. Наконец, $(a + p)/\sqrt{q - p^2}$ — корень многочлена $x^2 + 1$. Поэтому подполе $\mathbf{R}[a]$ изоморфно полю $\mathbf{C}$. Поскольку поле $\mathbf{C}$ алгебраически замкнуто, $L \simeq \mathbf{C}$.

Итак, конечные расширения поля $R$ — это само $\mathbf{R}$ и $\mathbf{C}$. Поэтому $\mathbf{C}$ является полем расщепления любого центрального тела $D$ над $\mathbf{R}$. Пусть $D \neq \mathbf{R}$, $d^2 = [D : \mathbf{R}]$, $L$ — максимальное подполе в $D$. Так как $L \neq \mathbf{R}$, то $L \simeq \mathbf{C}$, откуда по теореме 5.1 $d = [\mathbf{C} : \mathbf{R}] = 2$, т. е. $[D : \mathbf{R}] = 4$.

Обозначим через $i$ элемент подполя $L$, такой, что $i^2 = -1$ (образ элемента $i \in \mathbf{C}$ при изоморфизме $\mathbf{C} \simeq L$). Комплексное сопряжение дает автоморфизм поля $L$, при котором $i$ переходит в $-i$. По следствию 4.2 в $D$ найдется ненулевой элемент $j$, такой, что $jij^{-1} = -i$, т. е. $ji = -ij$.

Поскольку $j$ и $i$ неперестановочны, $j \notin L$, т. е. 1, $i$, $j$ линейно независимы. Кроме того, $j^2 i = -jij = ij^2$, т. е. $j^2 \in C_D(L) = L$. Итак, $j^2 = \alpha + \beta i$, где $\alpha, \beta \in \mathbf{R}$. Но $j^2$ обязано коммутировать с $j$, поэтому $j(\alpha + \beta i) = \alpha j + \beta ji = (\alpha + \beta i) j = \alpha j - \beta ij$ и $\beta = 0$. Значит, $j^2 = \alpha \in \mathbf{R}$. Очевидно, $\alpha < 0$ (иначе $\alpha = \gamma^2$ и $(j - \gamma)(j + \gamma) = 0$, что невозможно). Заменяя, если нужно, $j$ на $j/\sqrt{-\alpha}$, можно считать, что $j^2 = -1$.

Итак, мы уже выбрали элементы $i$ и $j$, такие, что $i^2 = j^2 = -1$, $ji = -ij$. Обозначим $k = ij$. Тогда $k^2 = ijij = -i^2 j^2 = -1$; $ik = i^2 j = -j$; $ki = iji = -i^2 j = j$. Аналогично $jk = -kj = i$. Иными словами, элементы $i$, $j$, $k$ множатся так же, как одноименные элементы тела кватернионов. Поэтому можно задать гомоморфизм $f : \mathbf{H} \to D$, являющийся мономорфизмом, поскольку $\mathbf{H}$ — тело. Но $[\mathbf{H} : \mathbf{R}] = [D : \mathbf{R}]$. Значит, $f$ — изоморфизм, что и требовалось доказать.

**Следствие 6.2.** $\mathrm{Br}(\mathbf{R}) = \mathrm{Br}(\mathbf{C}/\mathbf{R})$ *есть циклическая группа второго порядка.*

## *Упражнения к главе IV*

1. Пусть $D$ — конечномерное тело над $K$. Показать, что два $D$-бимодуля изоморфны тогда и только тогда, когда соответствующие самопредставления подобны (т. е. отличаются на внутренний автоморфизм алгебры $M_n(D)$).

2. Пусть $S$ и $T$ — конечные множества, на которых задан квазипорядок $\to$, $A$ и $B$ — соответствующие минимальные алгебры над полем $K$ (см. упражнения 8—10 к гл. III). Введем квазипорядок на декартовом произведении $S \times T$, полагая $(s, t) \to (s', t')$, если $s \to s'$ и $t \to t'$. Доказать, что $A \otimes B$ есть минимальная алгебра, соответствующая так определенному квазипорядку на декартовом произведении $A \times B$.

3. Доказать, что $\mathbf{C} \otimes \mathbf{C} \simeq \mathbf{C} \oplus \mathbf{C}$ ($\mathbf{C}$ рассматривается как алгебра над $\mathbf{R}$). Этот пример показывает, что тензорное произведение простых алгебр не обязано быть простой алгеброй.

4. Линейное отображение $\partial : A \to A$ называется *дифференцированием алгебры* $A$, если для любых элементов $a, b \in A$ $\partial(ab) = a(\partial b) + (\partial a) b$.

а) Доказать, что при фиксированном $x \in A$ отображение $\partial_x$, определенное формулой $\partial_x a = ax - xa$, является дифференцированием алгебры $A$. Это дифференцирование называется в н у т р е н н и м.

б) Доказать, что если $\partial$ — дифференцирование алгебры $A$, то отображение $T : A \to M_2(A)$, определяемое формулой

$$T(a) = \begin{pmatrix} a & \partial a \\ 0 & a \end{pmatrix},$$

есть гомоморфизм алгебр.

в) Доказать, что всякое дифференцирование центральной простой алгебры является внутренним. (У к а з а н и е: воспользоваться утверждением б) и теоремой Сколема—Нётер.)

5. Пусть $A$ — простая алгебра, $B$ — ее центральная простая подалгебра, $B' = C_A(B)$. Доказать, что: а) $B'$ — простая алгебра; б) $[B : K][B' : K] = [A : K]$; в) если $B' \simeq M_m(D)$, то $A \otimes B^\circ \simeq M_n(D)$, причем $m$ делит $n$.

Привести пример, в котором $C_A(B') \neq B$.

**6.** Рассмотрим алгебру $D$ над полем $\mathbf{Q}$ рациональных чисел с базисом $\{1, i, j, k\}$ и таблицей умножения

| | $i$ | $j$ | $k$ |
|---|---|---|---|
| $i$ | $-1$ | $k$ | $-j$ |
| $j$ | $-k$ | $2$ | $-2i$ |
| $k$ | $j$ | $2i$ | $2$ |

(проверьте, что это действительно алгебра).

а) Доказать, что $D$ — центральное тело.

б) Проверить, что $L_1 = \mathbf{Q}[i]$ и $L_2 = \mathbf{Q}[j]$ — неизоморфные максимальные подполя в $D$.

**7.** Доказать, что если $D_1$ и $D_2$ — такие центральные тела над $K$, что $[D_1 : K]$ и $[D_2 : K]$ взаимно просты, то $D_1 \otimes D_2$ есть тело. (Указание: предполагая, что $D_1 \otimes D_2 = M_n(D)$, вычислить двумя способами $D_1 \otimes D_2 \otimes D_2^{\circ}$ и вывести отсюда, что $n$ делит $[D_2 : K]$.)

**8** (теорема Диксона). Доказать, что два элемента центрального тела сопряжены тогда и только тогда, когда у них совпадают минимальные многочлены.

**9** (тело Гильберта). Пусть $L$ — некоторое поле, $\varphi$ — автоморфизм поля $L$. Рассмотрим «степенные ряды» вида $\sum\limits_{i \gg -\infty}^{\infty} a_i t^i$, где $a_i \in L$, $t$ — некоторый символ («переменное»), а обозначение $i \gg -\infty$ показывает, как обычно, что в этот ряд входит лишь конечное число членов с отрицательными номерами. Сложение рядов определяется как обычно: $\sum\limits_{i \gg -\infty}^{\infty} a_i t^i + \sum\limits_{i \gg -\infty}^{\infty} b_i t^i = \sum\limits_{i \gg -\infty}^{\infty} (a_i + b_i) t^i$, а умножение — исходя из правил $ta = \varphi(a) t$ $(a \in L)$ и $a \sum\limits_{i \gg -\infty}^{\infty} a_i t^i = \sum\limits_{i \gg -\infty}^{\infty} (a a_i) t^i$.

а) Проверить, что множество рядов с так определенными операциями образует тело $L[[t, \varphi]]$. Это тело называется телом Гильберта.

б) Пусть $K = \{a \in L \mid \varphi(a) = a\}$, $n$ — порядок автоморфизма $\varphi$, т. е. наименьшее натуральное число, такое, что $\varphi^n$ есть тождественный автоморфизм (или $\infty$, если такого натурального числа не существует). Доказать, что центр тела Гильберта есть $K[[t^n]]$, если $n \neq \infty$, и $K$, если $n = \infty$.

в) Построить пример центрального бесконечномерного тела. (Указание: принять за $L$ поле рациональных функций $K(x)$.)

# V

ГЛАВА

# ТЕОРИЯ ГАЛУА

В этой главе мы применим аппарат бимодулей и тензорных произведений к изучению расширений поля $K$, т. е. к теории Галуа.

## § 1. Элементы теории полей

Далее нам понадобятся некоторые известные результаты о строении полей и их расширений.

Пусть $K$ — произвольное поле. Напомним, что характеристикой поля $K$ называется наименьшее натуральное число $p$, для которого

$$p1 = \underbrace{1 + 1 + \ldots + 1}_{p \text{ раз}} = 0 \quad \text{(если такое число существует)}.$$

Если такого числа нет, т. е. $m1 \neq 0$ ни для какого $m$, говорят, что $K$ — поле характеристики 0. Поскольку из равенства $p = mn$, очевидно, следует, что $p1 = (m1)(n1)$, характеристика поля — всегда простое число (или 0).

Предположим, что $K$ — поле характеристики 0. Тогда из $n \neq m$ следует, что $n1 \neq m1$, и мы можем, отождествляя элемент $n1$ с числом $n$, считать, что $K$ содержит множество натуральных чисел. Обозначая далее $(-n)1 = -n1$ и отождествляя $-n1$ с числом $-n$, мы можем рассматривать и совокупность целых чисел как подмножество (подкольцо) поля $K$. Наконец, рассматривая отношения $n1/m1$, мы можем вложить в $K$ все поле рациональных чисел $\mathbf{Q}$.

Если поле $K$ — простой характеристики $p$, положение еще проще: легко видеть, что в этом случае элементы вида $n1$, где $0 \leqslant n < p$, сами образуют подполе, изоморфное полю $\mathbf{F}(p)$ вычетов по модулю $p$.

Очевидно, поля $\mathbf{Q}$ и $\mathbf{F}(p)$ уже не содержат собственных подполей. Поля, обладающие этим свойством, называются простыми. Итогом наших рассуждений является следующая теорема.

**Теорема 1.1.** *Всякое поле $K$ содержит простое подполе, изоморфное либо $\mathbf{Q}$ (если $K$ — характеристики 0), либо $\mathbf{F}(p)$ (если $K$ — характеристики $p > 0$).*

**Следствие 1.2.** *Если поле $K$ конечно, то число элементов в нем равно $p^n$, где $p$ — простое число.*

Доказательство. Характеристика конечного поля всегда отлична от нуля, т. е. $K \supset \mathbf{F}(p)$ для некоторого простого $p$. Но тогда $K$ — конечное расширение $\mathbf{F}(p)$. Выбирая в нем базис, мы сразу получаем, что $K$ состоит из $p^n$ элементов, где $n = [K : F(p)]$.

Нас будут интересовать в основном конечные расширения фиксированного поля $K$. Важнейшую роль при построении и исследовании таких расширений играет следующий результат.

**Теорема 1.3** (Кронекер). *Пусть $p(x)$ — неприводимый многочлен над полем $K$, $(p(x))$ — идеал в $K[x]$, состоящий из многочленов, кратных $p(x)$: $(p(x)) = \{p(x)\,g(x) \mid g(x) \in K[x]\}$. Тогда $K[x]/(p(x))$ есть поле, в котором многочлен $p(x)$ имеет корень. Наоборот, если $L$ — расширение поля $K$, в котором $p(x)$ имеет корень $a$, то $K[a] \simeq K[x]/(p(x))$.*

Доказательство. Обозначим $I = (p(x))$ и рассмотрим в факторалгебре $K[x]/I$ класс $\bar{x} = x + I$. Из определения действий в факторалгебре следует, что $p(\bar{x}) = p(x) + I = 0$, т. е. $\bar{x}$ — корень $p(x)$. Остается проверить, что $K[x]/I$ есть поле.

Пусть $\bar{f} = f(x) + I$ — ненулевой класс $K[x]/I$, т. е. $f(x) \not\in I$. Тогда многочлены $f(x)$ и $p(x)$ взаимно просты. Потому $1 = f(x)\,h(x) + p(x)\,g(x)$, где $h(x)$ и $g(x)$ — некоторые многочлены. Обозначим $\bar{h} = h(x) + I$, получаем, что $\bar{f}\bar{h} = 1$ в факторалгебре $K[x]/I$.

Наоборот, пусть $L$ — расширение поля $K$, $a \in L$ — корень $p(x)$. Тогда $p(x) = m_a(x)$. Определяя гомоморфизм $\varphi : K[x] \to L$ формулой $\varphi(f(x)) = f(a)$, из теоремы о гомоморфизме находим, что $K[a] \simeq K[x]/I$.

Заметим, что расширение $K[x]/I$ — конечное: если степень $p(x)$ равна $n$, то легко проверить, что $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1}$ — базис $K[x]/I$.

Из теоремы Кронекера можно получить такое важное следствие. Пусть $f(x)$ — произвольный многочлен над полем $K$, $p(x)$ — его неприводимый множитель. Тогда в поле $K_1 = K[x]/(p(x))$ многочлен $p(x)$, а потому и $f(x)$ имеет корень $a_1$, откуда по теореме Безу $f(x) = (x - a_1)\,f_1(x)$. Продолжая этот процесс, мы построим цепочку конечных расширений [9] $K \subset K_1 \subset K_2 \subset \ldots$, такую, что в $K_i$ многочлен $f(x)$ имеет $i$ корней (с учетом кратности). Отсюда следует, что если $f(x)$ — степени $n$, то в поле $K_n$ он разложится на линейные множители.

Говорят, что $L$ — поле разложения многочлена $f(x)$, если в нем $f(x)$ разлагается на линейные множители, но ни в каком его собственном подполе $f(x)$ не разлагается на линейные множители.

**Теорема 1.4.** *Для любого многочлена $f(x) \in K[x]$ существует поле разложения $L$ и любые два поля разложения изоморфны.*

Доказательство. Существование поля разложения следует из изложенного выше. Его единственность мы будем доказывать индукцией по степени $n$ многочлена $f(x)$. База индукции, $n = 1$, тривиальна: здесь автоматически $L = K$.

Пусть $f(x)$ — многочлен степени $n$, $L$ и $L'$ — его поля разложения, $p(x)$ — неприводимый (над $K$) множитель $f(x)$. Тогда $p(x)$ имеет корень $a$ в поле $L$ и корень $a'$ в поле $L'$. Из теоремы Кронекера следует, что поля $K[a]$ и $K[a']$ изоморфны. Отождествляя их, можно считать, что $L$ и $L'$ содержат общее подполе $K_1 = K[a]$.

[9] Заметим, что в этой цепочке включения не обязаны быть строгими. Например, если $p(x)$ — линейный многочлен, то уже $K_1 = K$.

Но тогда $L$ и $L'$ — расширения поля $K_1$. Более того, это поля разложения над $K_1$ многочлена $f_1(x) = f(x)/(x-a)$ степени $n-1$. По индукционному предположению $L \simeq L'$, что и требовалось доказать.

Покажем, что поле разложения $L$ — также конечное расширение основного поля $K$. Поскольку $L$ — подполе поля $K_n$, получающегося из $K$ цепочкой конечных расширений, наше утверждение является частным случаем следующего результата.

**Теорема 1.5.** *Если $K = K_0 \subset K_1 \subset \ldots \subset K_{n-1} \subset K_n$ — цепочка полей, в которой $K_{i+1}$ — конечное расширение $K_i$ для любого $i$, то $K_n$ — конечное расширение $K$ и $[K_n : K] = \prod_{i=1}^{n} [K_i : K_{i-1}]$.*

Доказательство, очевидно, достаточно провести для случая $n = 2$: общий результат получается отсюда по индукции.

Итак, пусть $K \subset F \subset L$, причем $[F:K] = n$ и $[L:F] = m$. Выберем базис $\{a_1, \ldots, a_n\}$ поля $F$ над $K$ и базис $\{b_1, \ldots, b_m\}$ поля $L$ над $F$. Тогда всякий элемент $F$ имеет вид $\sum_{i=1}^{n} \alpha_i a_i$, где $\alpha_i \in K$, а всякий элемент поля $L$ — вид $\sum_{j=1}^{m} \beta_j b_j$, где $\beta_j \in F$. Но, расписывая $\beta_j = \sum_{i=1}^{n} \alpha_{ij} a_i$, $\alpha_{ij} \in K$, мы получим $\sum_{j=1}^{m} \beta_j b_j = \sum_{i,j} \alpha_{ij} a_i b_j$, $\alpha_{ij} \in K$, т. е. $\{a_i b_j\}$ — система образующих векторного пространства $L$ над полем $K$.

С другой стороны, если $\sum_{i,j} \alpha_{ij} a_i \beta_j = 0$, то из линейной независимости $\{b_j\}$ над $F$ следует, что $\sum_{i=1}^{n} \alpha_{ij} a_i = 0$ для любого $j$, откуда, ввиду линейной независимости $a_i$ над $K$, $\alpha_{ij} = 0$ для всех $i$, $j$, т. е. элементы $a_i b_j$ линейно независимы над $K$. Итак, мы построим базис $\{a_i b_j\}$ поля $L$ над $K$, состоящий из $nm$ элементов, что и доказывает теорему.

## § 2. Конечные поля. Теорема Веддербёрна

Применим полученные ранее результаты для описания конечных полей (и даже всех конечных тел!). Докажем вначале одну лемму о коммутативных группах.

**Лемма 2.1.** *Если в коммутативной группе $G$ есть элементы порядков $m$ и $n$, то в $G$ есть и элемент порядка $k$, где $k$ — наименьшее общее кратное $m$ и $n$.*

Доказательство. Пусть $x$ — элемент порядка $m$, $y$ — элемент порядка $n$. Если $m$ и $n$ взаимно просты, то $k = mn$ и $(xy)^k = x^k y^k = 1$. Наоборот, если $(xy)^l = 1$, то $x^l = y^{-l}$ и элементы $x^l$ и $y^l$ имеют одинаковый порядок. Но порядок элемента $x^l$

делит $m$, а порядок $y^l$ делит $n$, откуда следует, что $x^l = y^l = 1$, т. е. $l$ делится на $m$ и $n$, а потому и на $k$.

В общем случае разложим $m$ и $n$ на простые множители и для каждого простого числа $p$ выберем в $m$ или в $n$ сомножитель вида $p^t$, где $t$ — степень, с которой $p$ входит в $k$. Тогда $m$ и $n$ разложатся в произведения $m = m_0m'$ и $n = n_0n'$ так, что $k = m_0n_0$, причем $m_0$ и $n_0$ взаимно просты.

Но элементы $x' = x^{m'}$ и $y' = y^{n'}$ имеют порядки, соответственно, $m_0$ и $n_0$, поэтому порядок элемента $x'y'$ есть $m_0n_0 = k$, что и требовалось доказать.

Непосредственным следствием этой леммы является такая теорема.

**Теорема 2.2.** *Конечная подгруппа мультипликативной группы поля циклична. В частности, мультипликативная группа конечного поля всегда циклична.*

Доказательство. Пусть $G$ — подгруппа мультипликативной группы поля $K$, состоящая из $n$ элементов. Из леммы 2.1 следует, что в $G$ есть элемент $g$ такого порядка $m$, что порядок любого элемента из $G$ делит $m$. Поэтому $a^m = 1$ для любого $a \in G$, т. е. все элементы $G$ — корни уравнения $x^m - 1 = 0$. Значит, $n \leqslant m$. Отсюда сразу вытекает, что $n = m$ и $g$ — образующий группы $G$.

**Теорема 2.3.** *Для любого простого числа $p$ и любого натурального $n$ существует единственное, с точностью до изоморфизма, поле из $p^n$ элементов.*

Доказательство. Положим $K = \mathbf{F}(p)$ и рассмотрим над $K$ многочлен $f(x) = x^{p^n} - x$. Пусть $L$ — его поле разложения, $S$ — множество корней $f(x)$ в поле $L$. Поскольку $f'(x) = -1$, $f(x)$ не имеет кратных корней, т. е. $S$ состоит из $p^n$ элементов. Но $a \in S$ тогда и только тогда, когда $a^{p^n} = a$. Применяя формулу для бинома Ньютона, легко замечаем, что в любом поле характеристики $p$ $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. Поскольку еще и $(ab)^{p^n} = a^{p^n}b^{p^n}$ и $(a^{-1})^{p^n} = (a^{p^n})^{-1}$, то отсюда следует, что $S$ — подполе в $L$, и потому $S = L$, т. е. $L$ состоит из $p^n$ элементов.

Пусть теперь $L'$ — произвольное поле из $p^n$ элементов, $G$ — мультипликативная группа поля $L'$. $G$ состоит из $p^n - 1$ элементов, поэтому для любого $a \in G$ $a^{p^n-1} = 1$ и $a^{p^n} = a$. Но последнее равенство верно и при $a = 0$, т. е. все элементы $L'$ — корни уравнения $x^{p^n} - x = 0$. Поскольку их как раз $p^n$, $L'$ — поле разложения $f(x)$ и по теореме 1.3 $L' \simeq L$.

Из теоремы 2.3 следует, в частности, что конечные поля с одинаковым числом элементов изоморфны. В сочетании с теоремой Сколема—Нётер это приводит к следующему замечательному результату.

**Теорема 2.4** (Веддербёрн). *Всякое конечное тело коммутативно, т. е. является полем.*

Доказательство. Если $D$ — конечное тело, то его центр $K$ — это некоторое конечное поле. Пусть $[D : K] = d^2$. Для любого максимального подполя $L$ тела $D$ $[L : K] = d$. Значит, все они состоят из одинакового числа элементов и потому изоморфны. Из теоремы Сколема—Нётер следует, что тогда все они сопряжены. С другой стороны, очевидно, всякий элемент $a \in D$ лежит в каком-то максимальном подполе. Поэтому если $G$ — мультипликативная группа тела $D$, а $H$ — мультипликативная группа какого-то максимального подполя $L$, то $G = \bigcup_g gHg^{-1}$, где $g$ пробегает все $G$. Покажем, что это невозможно при $H \neq G$.

Обозначим порядок $G$ через $n$, а порядок $H$ — через $m$. Из того, что $G = \bigcup gHg^{-1}$, следует, что $n < mk$, где $k$ — число различных подгрупп вида $gHg^{-1}$ (поскольку все они содержат единицу). Но если $g_1 = gh$, где $h \in H$, то $g_1Hg_1^{-1} = gHg^{-1}$, откуда следует, что $k$ не превосходит $i$ — индекса $H$ в $G$. Мы приходим к противоречию с теоремой Лагранжа, утверждающей, что $n = mi$.

Итак, обязательно $H = G$, т. е. $L = D$, что и доказывает теорему.

## § 3. Сепарабельные расширения

Вернемся к изучению конечных расширений произвольных полей. Как и в предыдущей главе, важную роль при этом будет играть алгебра $L \otimes L$ (заметим, что здесь $L^\circ = L$). Поэтому нам понадобится информация о строении тензорных произведений полей.

Далее нам придется пользоваться тензорными произведениями над различными полями (как над основным полем $K$, так и над его расширениями). Тензорное произведение векторных пространств (или алгебр) над полем $L \supset K$ мы будем обозначать знаком $\otimes_L$. При этом нетрудно убедиться, что «формула ассоциативности» из предложения IV.2.3 имеет место и в этой более общей ситуации. Именно, если $L \subset M$ — два расширения поля $K$, $U$ — векторное пространство над $L$, а $V$ и $W$ — над $M$, то $(U \otimes_L V) \otimes_M W \simeq U \otimes_L (V \otimes_M W)$. Доказательство этой формулы мы оставляем читателю. Заметим, что $\otimes_K$ — это просто $\otimes$.

Рассмотрим простейший случай, когда один из сомножителей является моногенным, т. е. имеет вид $K[a]$.

**Предложение 3.1.** *Пусть $L$ и $F$ — конечные расширения поля $K$, причем $F = K[a]$, и минимальный многочлен элемента $a$ над $K$ есть $p(x)$. Тогда $L \otimes F \simeq L[x]/(p(x))$.*

Доказательство. Очевидно, $L \otimes F$, как $L$-алгебра, моногенна: $L \otimes F = L[1 \otimes a]$. Поэтому, сопоставляя $f(x) \in L[x]$ элемент $f(1 \otimes a) \in L \otimes F$, мы получаем эпиморфизм $L[x]$ на $L \otimes F$.

Поэтому $L \otimes F \simeq L[x]/(m(x))$, где $m(x)$ — минимальный многочлен элемента $1 \otimes a$ над $L$. Но, очевидно, $p(1 \otimes a) = 1 \otimes p(a) = 0$ и в то же время элементы $1, 1 \otimes a, \ldots, 1 \otimes a^{n-1}$,

где $n$ — степень $p(x)$, линейно независимы над $L$. Отсюда следует, что $m(x) = p(x)$. Предложение доказано.

Выясним строение факторалгебры $K[x]/(f(x))$ для произвольного многочлена $f(x)$.

**Лемма 3.2.** *Если* $f(x) = f_1(x) \ldots f_t(x)$, *где многочлены* $f_1(x), \ldots, f_t(x)$ *попарно взаимно просты, то* $K[x]/(f(x)) \simeq \prod_{i=1}^{t} K[x]/(f_i(x))$.

Доказательство. Обозначим $I = (f(x))$, $I_i = (f_i(x))$. Сопоставим каждому классу $g(x) + I$ факторалгебры $K[x]/(f(x))$ набор $(g(x) + I_1, g(x) + I_2, \ldots, g(x) + I_t) \in \prod_{i=1}^{t} K[x]/I_i$. Очевидно, это будет гомоморфизм алгебр, и даже мономорфизм, так как если $g(x)$ делится на все $f_i(x)$, то из их взаимной простоты следует, что $g(x)$ делится на их произведение, т. е. на $f(x)$. Но размерность алгебры $K[x]/I$ равна $n$, где $n$ — степень $f(x)$, а размерность алгебры $K[x]/I_i$ равна $n_i$, где $n_i$ — степень $f_i(x)$. Поэтому размерности $K[x]/I$ и $\prod_{i=1}^{t} K[x]/I_i$ одинаковы, и наш мономорфизм обязан быть изоморфизмом.

**Следствие 3.3.** *Алгебра* $K[x]/(f(x))$ *полупроста тогда и только тогда, когда многочлен* $f(x)$ *не имеет кратных неприводимых множителей.*

Доказательство. Если $f(x) = p_1(x) \ldots p_s(x)$, где $p_1(x), \ldots, p_s(x)$ — попарно различные неприводимые многочлены, то $K[x]/(f(x)) \simeq \prod_{i=1}^{t} K[x]/(p_i(x))$, а $K[x]/(p_i(x))$ — поля (по теореме Кронекера), т. е. эта алгебра полупроста. Если же $f(x) = p^2(x)\, g(x)$, то класс многочлена $p(x)\, g(x)$, как легко видеть, является ненулевым нильпотентным элементом в $K[x]/(f(x))$.

**Следствие 3.4.** *В условиях предложения 3.1 алгебра* $L \otimes F$ *полупроста тогда и только тогда, когда многочлен* $p(x)$ *не имеет в поле* $L$ *кратных неприводимых множителей.*

**Следствие 3.5.** *Пусть* $F = K[a]$ *— моногенное расширение, причем* $a$ *— простой корень своего минимального многочлена* $p(x)$. *Тогда для любой коммутативной полупростой алгебры* $A$ *алгебра* $A \otimes F$ *полупроста.*

Доказательство. Разлагая $A$ по теореме Вейерштрасса — Дедекинда в прямое произведение полей, мы видим, что достаточно проверить полупростоту алгебр вида $L \otimes F$, где $L$ — поле. По следствию 3.4 нужно показать, что $p(x)$ не имеет в $L$ кратных неприводимых множителей.

Предположим, что $g(x)$ — кратный неприводимый множитель $p(x)$ над полем $L$, $L'$ — расширение $L$, в котором $g(x)$ имеет корень

$b$. Тогда $b$ — кратный корень $p(x)$. Но $K[b] \simeq K[a]$ по теореме Кронекера, откуда следует, что $a$ — кратный корень $p(x)$, что противоречит предположению.

Неприводимый многочлен $p(x)$ называется сепарабельным, если ни в каком расширении поля $K$ он не имеет кратных корней. Рассуждение, проведенное при доказательстве следствия 3.5, показывает, что для этого достаточно, чтобы в каком-то расширении $p(x)$ имел простой корень.

Элемент $a$ конечномерного тела называется сепарабельным, если сепарабелен его минимальный многочлен.

**Теорема 3.6.** *Для любого конечного расширения $L$ поля $K$ равносильны следующие условия:*

*1) $L \otimes L$ — полупростая алгебра;*

*2) для любой полупростой коммутативной алгебры $A$ алгебра $A \otimes L$ полупроста;*

*3) всякий элемент поля $L$ сепарабелен;*

4) *$L = K[a_1, \ldots, a_t]$, где все элементы $a_i$ сепарабельны.*

Доказательство. Очевидно, 2) $\Rightarrow$ 1) и 3) $\Rightarrow$ 4).

1) $\Rightarrow$ 3). Пусть $a$ — несепарабельный элемент из $L$, $F = K[a]$. Тогда $a$ — кратный корень своего минимального многочлена, и по следствию 3.4 $L \otimes F$ — неполупростая алгебра, а тогда и алгебра $L \otimes L \supset L \otimes F$ неполупроста.

4) $\Rightarrow$ 2) будем доказывать индукцией по $t$. База индукции, $t = 1$,— следствие 3.4. Обозначим $F = K[a_t]$. Тогда $F$-алгебра $A_F = A \otimes F$ полупроста. Но $A \otimes L \simeq A_F \otimes_F L$, а $L = F[a_1, \ldots, a_{t-1}]$ и по предложению индукции алгебра $A \otimes L$ полупроста, что и завершает доказательство теоремы.

Расширение, удовлетворяющее равносильным условиям теоремы 3.6, называется сепарабельным.

**Следствие 3.7.** *Если дана цепочка полей $K = K_0 \subset K_1 \subset \ldots \subset K_n = L$, где $K_i$ — конечное расширение $K_{i-1}$, то $L$ сепарабельно над $K$ тогда и только тогда, когда каждое $K_i$ сепарабельно над $K_{i-1}$.*

Доказательство снова достаточно провести при $n = 2$. Если $K_1$ сепарабельно над $K$, а $L$ сепарабельно над $K_1$, то $L \otimes L \simeq L \otimes (K_1 \otimes_{K_1} L) \simeq A \otimes_{K_1} L$, где $A = L \otimes K_1$ — полупростая алгебра. Поэтому $L \otimes L$ — полупростая алгебра, т. е. $L$ сепарабельно над $K$.

С другой стороны, $K_1 \otimes K_1$ — подалгебра в $L \otimes L$, поэтому из полупростоты $L \otimes L$ следует полупростота $K_1 \otimes K_1$. Рассмотрим алгебру $L \otimes_{K_1} L$ и зададим отображение $f: L \otimes L \to L \otimes_{K_1} L$, переводящее $a \otimes b$ в $a \otimes_{K_1} b$. Легко проверяется, что $f$ — эпиморфизм алгебр. Значит, $L \otimes_{K_1} L$ изоморфна факторалгебре $L \otimes L$. Но факторалгебра полупростой алгебры полупроста, поэтому из сепарабельности $L$ над $K$ следует его сепарабельность над $K_1$.

Поле $K$ называется совершенным, если любое его конечное расширение сепарабельно или, что то же, сепарабелен всякий

неприводимый многочлен из $K[x]$. Нетрудно установить следующий критерий совершенности.

**Теорема 3.8.** *Любое поле характеристики 0 совершенно. Поле $K$ характеристики $p$ совершенно тогда и только тогда, когда для любого $\alpha \in K$ разрешимо уравнение $x^p = \alpha$.*

Доказательство. Если $f(x)$ — неприводимый многочлен, $f'(x)$ — его производная, то либо $f$ и $f'$ взаимно просты, либо $f$ делит $f'$, что возможно, очевидно, лишь, если $f'(x) = 0$. Пусть $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n$, $\alpha_0 \neq 0$, тогда $f'(x) = n\alpha_0 x^{n-1} + (n-1)\alpha_1 x^{n-2} + \ldots + \alpha_{n-1}$. Если $K$ — поле характеристики 0, то $n\alpha_0 \neq 0$, т. е. $f'(x) \neq 0$ и $f$ и $f'$ взаимно просты. Поэтому $f(x)$ не имеет кратных корней ни в каком расширении поля $K$, т. е. сепарабелен. Если же $K$ — поле характеристики $p$, то $f'(x) = 0$ тогда и только тогда, когда $f(x)$ имеет вид $\beta_0 x^{p^k} + \beta_1 x^{p^{k-1}} + \ldots + \beta_k$. Предположим, что уравнение $x^p = \beta_i$ имеет решение $\gamma_i \in K$. Тогда, как легко заметить, $f(x) = (\gamma_0 x^k + \gamma_1 x^{k-1} + \ldots + \gamma_k)^p$, т. е. $f(x)$ не неприводим. Если же уравнение $x^p = \alpha$ для некоторого $\alpha \in K$ не имеет решения, то в поле разложения многочлена $f(x) = x^p - \alpha$ имеет место равенство $f(x) = (x - \beta)^p$, где $\beta^p = \alpha$, из которого вытекает несепарабельность многочлена $f(x)$. Теорема доказана

**Следствие 3.9.** *Конечное поле совершенно.*

Доказательство вытекает из того, что отображение $\varphi : K \to K$ ($K$ — конечное поле характеристики $p$), переводящее $\alpha$ в $\alpha^p$, инъективно, т. е. из $\alpha^p = \beta^p$ следует $\alpha = \beta$, поскольку $\alpha^p - \beta^p = (\alpha - \beta)^p$. Из-за конечности $K$ $\varphi$ тогда взаимно однозначно, что и требовалось доказать.

## § 4. Нормальные расширения. Группа Галуа

Перейдем к основной теме этой главы — изучению автоморфизмов конечных расширений. Напомним связь между автоморфизмами и бимодулями, установленную в гл. IV (§ 1, примеры 2, 3). Пусть $L$ — конечное расширение поля $K$, $\sigma$ — автоморфизм $L$. Тогда ${}_\sigma L$ есть $L$-бимодуль, в котором операторы из $L$ действуют справа как в регулярном $L$-модуле, а слева по правилу $ax = x\sigma(a)$. Наоборот, если $M$ — такой $L$-бимодуль, что[10] $[M : L] = 1$, то $M \simeq L$ как правый $L$-модуль. Сопоставляя элементу $a \in L$ эндоморфизм $x \to ax$ правого $L$-модуля $M$, мы получим гомоморфизм $L \to E_L(M) \simeq L$, т. е. автоморфизм поля $L$. Поэтому $M \simeq {}_\sigma L$ для некоторого автоморфизма $\sigma$. Легко проверяется, что ${}_\sigma L \simeq {}_\tau L$ тогда и только тогда, когда $\sigma = \tau$.

Итак, мы установили взаимно однозначное соответствие между множеством автоморфизмов поля $L$ и классами изоморфизма одно-

[10] В принципе следовало бы различать левую и правую размерности $M$ над $L$, однако из-за конечномерности они совпадают: каждая из них равна $[M : K]/[L : K]$.

мерных (над $L$) $L$-бимодулей. Поскольку одномерный бимодуль, очевидно, прост, то, рассматривая его как модуль над $L \otimes L$, мы получаем следующий результат.

**Теорема 4.1.** *Существует взаимно однозначное соответствие между автоморфизмами поля $L$ и теми простыми компонентами алгебры $(L \otimes L)/\mathrm{rad}\,(L \otimes L)$, которые изоморфны $L$.*

Отсюда простым подсчетом размерностей мы получаем такое следствие.

**Следствие 4.2.** *Число различных автоморфизмов поля $L$ не превосходит $[L : K]$ и может равняться $[L : K]$ только в том случае, если $L$ сепарабельно.*

Если расширение $L$ имеет точно $[L : K]$ различных автоморфизмов, оно называется нормальным. В силу теоремы 4.1 это равносильно изоморфизму $L \otimes L \approx L^n$. Нормальное расширение всегда сепарабельно.

**Следствие 4.3.** *Если расширение $L$ поля $K$ нормально и $K \subset K_1 \subset L$, то расширение $L$ поля $K_1$ также нормально.*

Доказательство следует из того, что $L \otimes_{K_1} L$ есть факторалгебра алгебры $L \otimes L$ (см. доказательство следствия 3.7), а всякая факторалгебра $L^n$ сама имеет вид $L^m$ для некоторого $m \leqslant n$.

Автоморфизмы расширения $L$ поля $K$, очевидно, образуют группу, которую мы будем обозначать $G\,(L/K)$. Если расширение нормально, $G\,(L/K)$ называется его группой Галуа.

Элемент $a$ поля $L$ называется инвариантом автоморфизма $\sigma$, если $\sigma\,(a) = a$. Это равносильно тому, что в бимодуле ${}_\sigma L$ $ax = xa$ для любого $x \in {}_\sigma L$. Если $H$ — подмножество в $G\,(L/K)$, то инвариантом $H$ называется элемент $a \in L$, являющийся инвариантом любого элемента $\sigma \in H$. Инварианты подмножества $H$ образуют подполе в $L$. Это подполе называется полем инвариантов $H$ и обозначается $\mathrm{Inv}\,H$.

**Теорема 4.4.** *Следующие условия равносильны:*

*1) расширение $L$ поля $K$ нормально;*

*2) $\mathrm{Inv}\,G\,(L/K) = K$;*

*3) $L$ есть поле разложения некоторого сепарабельного многочлена $f(x) \in K[x]$.* (Произвольный многочлен называется сепарабельным, если сепарабельны все его неприводимые множители.)

Доказательство. 1) $\Rightarrow$ 2). Обозначим $K_1 = \mathrm{Inv}\,G\,(L/K)$. Тогда $L$ — расширение $K_1$ и $G\,(L/K) = G\,(L/K_1)$, что невозможно при $K_1 \neq K$, поскольку порядок группы $G\,(L/K)$ равен $[L : K]$.

2) $\Rightarrow$ 3). Пусть $a$ — произвольный элемент поля $L$. Применим к $a$ все автоморфизмы из $G\,(L/K)$ и выпишем все те из полученных элементов, которые попарно различны: $a = a_1, a_2, \ldots, a_k$. Рассмотрим многочлен $f(x) = (x - a_1) \ldots (x - a_k)$. Он переходит в себя

при любом автоморфизме $\sigma \in G(L/K)$. Поэтому $f(x) \in K[x]$. Итак, $a$ — корень сепарабельного многочлена из $K[x]$, который разлагается в поле $L$ на линейные множители.

Выберем в $L$ некоторую систему образующих (например, базис) $L = K[\omega_1, \ldots, \omega_t]$ и для каждого $\omega_i$ построим сепарабельный многочлен $f_i(x)$, корнем которого является $\omega_i$ и который разлагается в $L$ на линейные множители. Тогда $L$ — поле разложения многочлена $f(x) = f_1(x) \ldots f_t(x)$, который является сепарабельным над полем $K$.

3) $\Rightarrow$ 1) будем доказывать индукцией по степени $d$ многочлена $f(x)$. База индукции, $d = 1$, тривиальна ($L = K$). Предположим, что для многочленов степени $d - 1$ теорема уже доказана.

Пусть $L = K[\omega_1, \ldots, \omega_t]$, где $\omega_i$ — корни $f(x)$. Обозначим $K_1 = K[\omega_1]$. $L$ есть поле разложения (над $K_1$) сепарабельного многочлена $f(x)/(x - \omega_1)$ степени $d - 1$, поэтому $L$ нормально над $K$: $L \otimes_{K_1} L \simeq L^m$. Но $L \otimes L \simeq (L \otimes K_1) \otimes_{K_1} L$. Выясним, как устроено $L \otimes K_1$. Пусть $p(x)$ — минимальный многочлен элемента $\omega_1$. Он сепарабелен и разлагается в $L$ на линейные множители: $p(x) = (x - a_1) \ldots (x - a_s)$ ($a_1 = \omega_1, a_1, \ldots, a_s$ попарно различны). Но тогда $K[a_i] \simeq K_1$, что дает $s$ различных гомоморфизмов $\sigma_i : K_1 \to L$, причем $s = [K_1 : K]$. Соответственно можно построить $s$ $K_1$-$L$-бимодулей ${}_{\sigma_i}L$, одномерных над $L$. Поэтому у $L \otimes K_1$ есть факторалгебра, изоморфная $L^s$. Но простой подсчет размерностей показывает, что тогда $L \otimes K_1 \simeq L^s$ и $L \otimes L \simeq L^s \otimes_{K_1} L \simeq L^{ms}$. Теорема полностью доказана.

**Следствие 4.5.** *Для всякого сепарабельного расширения $L$ поля $K$ существует нормальное расширение $L'$, содержащее $L$.*

Доказательство. Пусть $L = K[\omega_1, \ldots, \omega_t]$, где $\omega_i$ — корень сепарабельного многочлена $f_i(x)$. Тогда за $L'$ можно принять поле разложения многочлена $f(x) = f_1(x) \ldots f_t(x)$.

## § 5. Основная теорема теории Галуа

В этом параграфе мы докажем центральные теоремы теории полей: теорему о нормальном базисе и основную теорему теории Галуа. Предварительно сделаем следующее полезное замечание.

**Лемма 5.1.** *Пусть $A$ — алгебра над полем $K$, $M$ и $N$ — некоторые $A$-модули, $L$ — конечное расширение поля $K$, $A_L = L \otimes A$, $M_L = L \otimes M$, $N_L = L \otimes N$ ($M_L$ и $N_L$, очевидно, можно рассматривать как $A_L$-модули). Если $M_L \simeq N_L$ как $A_L$-модули, то $M \simeq N$ как $A$-модули.*

Доказательство. Рассмотрим $M_L$ и $N_L$ как $A$-модули. Поскольку $L$ есть $n$-мерное векторное пространство над $K$, $M_L \simeq nM$ и $N_L \simeq nN$. Но из изоморфизма $nM \simeq nN$ в силу теоремы Крулля—Шмидта следует, что $M \simeq N$.

Пусть $L$ — расширение поля $K$, $G = G(L/K)$, $KG$ — групповая алгебра группы $G$ над полем $K$ (см. § 1 гл. I, пример 6). Тогда $L$

можно превратить в левый $KG$-модуль, полагая $\left(\sum_{g\in G}\alpha_g g\right)\cdot a = \sum_{g\in G}\alpha_g g(a)$ для любого $a\in L$.

**Теорема 5.2.** *Расширение $L$ нормально тогда и только тогда, когда $L$, как левый $KG$-модуль, изоморфен левому регулярному $KG$-модулю.*

Доказательство. Если $L\simeq KG$ как левый $KG$-модуль, то $[KG:K]=[L:K]$. Но $[KG:K]=(G:1)$ (порядку группы $G$). Значит, $L$ нормально.

Наоборот, пусть $L$ — нормальное расширение. Будем рассматривать $L\otimes L$ как левый модуль над алгеброй $L\otimes KG\simeq LG$. В силу леммы 5.1 нам достаточно показать, что $L\otimes L\simeq LG$.

Но $L\otimes L$, как модуль над собой (или бимодуль над $L$), разлагается в прямую сумму $L\otimes L\simeq\bigoplus_{\sigma\in G}{}_\sigma L$. Пусть $1=\sum_{\sigma\in G}e_\sigma$—соответствующее разложение единицы. Легко проверить, что отображение $x\to gx$ есть автоморфизм алгебры $L\otimes L$. Поэтому $ge_\sigma$ — минимальный идемпотент этой алгебры, и по теореме II. 5. 1 $ge_\tau=e_\tau$ для некоторого $\tau\in G$. По определению бимодуля ${}_\tau L$ это означает, что $age_\sigma=ge_\sigma\tau(a)$ для любого $a\in L$.

Поскольку для $x=\Sigma a_i\otimes b_i\in L\otimes L$ $gx=\Sigma a_i\otimes gb_i$, а $ax=\Sigma aa_i\otimes b_i$, $agx=gax$ для любого $a\in L$. Следовательно, $age_\sigma=gae_\sigma=g(e_\sigma\sigma(a))=ge_\sigma(g\sigma(a))$, т. е. $\tau=g\sigma$.

Итак, $ge_\sigma=e_{g\sigma}$. Сопоставляя элементу $\sigma\in LG$ элемент $e_\sigma$, мы получаем изоморфизм $LG$-модулей $LG\simeq L\otimes L$, что и требовалось доказать.

Отметим, что изоморфизм $Kg$-модулей $L\simeq KG$ означает существование такого элемента $\omega\in L$, что элементы $\sigma(\omega)$, где $\sigma$ пробегает группу $G$, образуют базис $L$. Базис такого вида называется нормальным, а теорема 5.2 — теоремой о нормальном базисе.

**Следствие 5.3.** *Нормальное расширение моногенно.*

Доказательство. Если $\omega$ — элемент, для которого $\sigma(\omega)$ образуют базис, то, поскольку $\sigma(\omega)$ — корни многочлена $m_\omega(x)$, его степень равна размерности расширения $L$, откуда следует, что $L=K[\omega]$.

Из теоремы о нормальном базисе немедленно следует основная теорема теории Галуа.

**Теорема 5.4.** *Пусть $L$ — нормальное расширение поля $K$, $G=G(L/K)$. Для любого подполя $F$ поля $L$ обозначим* Inv $F$ *подгруппу в $G$, состоящую из всех элементов $\sigma$, таких, что $\sigma(a)=a$ для всех $a\in F$. Тогда:*

*1) для любой подгруппы $H\subset G$* Inv (Inv $H$) $=H$, *а для любого подполя $F\subset L$* Inv (Inv $F$) $=F$;

*2) сопоставляя подгруппе $H$ подполе* $\operatorname{Inv} H$, *мы получаем взаимно однозначное соответствие между подгруппами группы Галуа и подполями поля $L$, причем $H \supset H_1$ тогда и только тогда когда* $\operatorname{Inv} H \subset \operatorname{Inv} H_1$;

3) $\operatorname{Inv} F \simeq G(L/F)$ *для любого подполя $F$*;

4) *подполе $F$ нормально тогда и только тогда, когда нормальна подгруппа* $\operatorname{Inv} F$, *в этом случае* $G(F/K) \simeq G/\operatorname{Inv} F$.

Доказательство. Очевидно, $\operatorname{Inv}(\operatorname{Inv} H) \supset H$ и $\operatorname{Inv}(\operatorname{Inv} F) \supset F$. Вычислим размерность поля $\operatorname{Inv} H$. Для этого воспользуемся изоморфизмом левых $KG$-модулей $L \simeq KG$. При этом изоморфизме $\operatorname{Inv} H$ переходит в подпространство $V \subset KG$, состоящее из таких элементов $x$, что $\sigma x = x$ для всех $\sigma \in H$. Запишем $x$ в виде $x = \sum_{g \in G} \alpha_g g$. Тогда $\sigma x = \sum_{g \in G} \alpha_g (\sigma g)$, откуда следует, что $\alpha_g = \alpha_{\sigma g}$ для любого $\sigma \in H$ и базис $V$ образуют элементы вида $\sum_{\sigma \in H} \sigma g$, где $g$ — фиксированный элемент из $G$. Различных элементов такого вида столько, сколько есть классов смежности $G$ по $H$, т. е. $(G : H)$. Итак, $[\operatorname{Inv} H : K] = (G : H)$.

С другой стороны, поле $L$ нормально над любым подполем $F$ (по следствию 4.3). Следовательно, существует $[L : F]$ различных автоморфизмов $L$, оставляющих все элементы $F$ неподвижными, т. е. порядок группы $\operatorname{Inv} F$ равен $[L : F]$.

В частности, порядок группы $\operatorname{Inv}(\operatorname{Inv} H)$ равен

$$[L : \operatorname{Inv} H] = [L : K]/[\operatorname{Inv} H : K] = (G : 1)/(G : H) = (H : 1),$$

откуда $\operatorname{Inv}(\operatorname{Inv} H) = H$. Аналогично размерность поля $\operatorname{Inv}(\operatorname{Inv} F)$ равна

$$(G : \operatorname{Inv} F) = (G : 1)/(\operatorname{Inv} F : 1) = [L : K]/[L : F] = [F : K]$$

и $\operatorname{Inv}(\operatorname{Inv} F) = F$, что завершает доказательство утверждений 1) и 2). Заметим, что попутно мы установили и изоморфизм $G(L/F) \simeq \simeq \operatorname{Inv} F$.

Вычислим теперь $\operatorname{Inv}(g(F))$, где $g$ — произвольный автоморфизм из $G$. Если $\sigma \in \operatorname{Inv}(g(F))$, то $\sigma g(a) = g(a)$ для любого $a \in F$, т. е. $g^{-1}\sigma g(a) = a$ и $g^{-1}\sigma g \in \operatorname{Inv} F$. Следовательно, $\operatorname{Inv}(g(F)) = g(\operatorname{Inv} F)g^{-1}$, и если $\operatorname{Inv} F$ — нормальная подгруппа, то $\operatorname{Inv}(g(F)) = \operatorname{Inv} F$, откуда $g(F) = F$ для любого $g \in G$. Таким образом, всякий автоморфизм поля $L$ в этом случае индуцирует автоморфизм поля $F$, причем легко проверить, что $g$ и $h$ индуцируют один и тот же автоморфизм $F$ тогда и только тогда, когда они лежат в одном классе смежности по $\operatorname{Inv} F$. Всего мы получаем $(G : \operatorname{Inv} F)$ автоморфизмов $F$ над $K$. Поскольку $(G : \operatorname{Inv} F) = = [S : K]$, отсюда следует, что поле $F$ нормально и $G(F/K) \simeq G/\operatorname{Inv} F$.

Наоборот, если $F$ нормально, то по теореме 4.4 $F$ есть поле разложения сепарабельного многочлена $f(x) \in K[x]$. Поскольку любой автоморфизм $g$ поля $L$ переводит корень $f(x)$ снова в некоторый ко-

рень $f(x)$, $g(F) = F$ и $g(\mathrm{Inv}\, F)\, g^{-1} = \mathrm{Inv}\, F$, т. е. $\mathrm{Inv}\, F$ — нормальная подгруппа, что завершает доказательство теоремы.

**Следствие 5.5.** *В сепарабельном расширении $L$ поля $K$ содержится только конечное число подполей.*

Доказательство. Если $L$ нормально, это следует сразу из основной теоремы теории Галуа, так как конечная группа имеет конечное число подгрупп. В общем же случае достаточно погрузить $L$ в некоторое нормальное расширение (это можно сделать по следствию 4.5).

**Следствие 5.6.** *Сепарабельное расширение моногенно.*

Доказательство. Всякое расширение конечного поля нормально по теоремам 2.3 и 4.4 и потому моногенно (см. следствие 5.3). Поэтому основное поле $K$ можно считать бесконечным.

Сепарабельное расширение $L$ поля $K$ содержит конечное число подполей. Если $a$ — элемент $L$, не лежащий ни в каком собственном подполе, то, очевидно, $L = K[a]$. Поэтому доказательство сводится к такому факту из линейной алгебры.

**Лемма 5.7.** *Векторное пространство над бесконечным полем нельзя представить в виде объединения конечного числа собственных подпространств.*

Доказательство. Очевидно, что пространство $V$ нельзя представить в виде объединения двух собственных подпространств $V_1$ и $V_2$: если $x_1 \in V_1 / V_2$, а $x_2 \in V_2 / V_1$, то $x_1 + x_2$ не лежит ни в $V_1$, ни в $V_2$. Пусть теперь $V = \bigcup_{i=1}^{m} V_i$, где $V_i$ — собственные подпространства. Покажем, что хотя бы одно из них содержится в объединении остальных.

Действительно, пусть $x_1$ лежит только в $V_1$, а $x_2$ лежит только в $V_2$. Тогда для любого ненулевого $\alpha \in K$ $x_1 + \alpha x_2$ не лежит в $V_1 \cup \cup V_2$, поэтому $x_1 + \alpha x_2 \in V_i$, где $i > 2$. Поскольку $\alpha$ может принимать бесконечно много значений, найдутся два различных элемента $\alpha$ и $\beta$ поля $K$, такие, что $x_1 + \alpha x_2 \in V_i$ и $x_1 + \beta x_2 \in V_i$ (для одного и того же $i$). Но тогда $x_2 \in V_i$, что противоречит предположению.

Итак, мы можем выбросить одно из подпространств и получить представление $V$ в виде объединения $m - 1$ подпространств. Применяя эту процедуру, мы в конце концов придем к случаю двух подпространств, что невозможно.

## § 6. Скрещенные произведения

Теория Галуа дает новый подход к изучению центральных простых алгебр. В этом параграфе мы дадим конструкцию, позволяющую описать группу Брауэра в терминах нормальных расширений и построить для всякого центрального тела $D$ некоторую алгебру вида $M_n(D)$.

Прежде всего установим следующий важный результат.

**Лемма 6.1** (Нётер). *Пусть $D$ — конечномерное центральное тело над $K$. Существует максимальное подполе $L \subset D$, сепарабельное над $K$.*

Доказательство. Если характеристика $K$ равна 0, то всякое подполе в $D$ сепарабельно. Поэтому можно считать, что $K$—поле характеристики $p > 0$. Покажем, что в этом случае в $D$ обязательно найдется сепарабельный над $K$ элемент, не лежащий в $K$.

Возьмем произвольный элемент $a \in D \setminus K$. Пусть $f(x) = m_a(x)$. Если элемент $a$ несепарабелен, то он является кратным корнем (в $K[a]$) неприводимого многочлена $f(x)$, откуда следует, что $f'(x) = 0$, а тогда $f(x) = g(x^p)$ для некоторого $g(x) \in K[x]$. Элемент $a^p$ является тогда корнем многочлена $g(x)$. Если он несепарабелен, то вновь $g(x) = h(x^p)$ для какого-то $h(x) \in K[x]$. Продолжая этот процесс, мы прийдем к элементу $b$, который несепарабелен над $K$, но $b^p$ уже сепарабелен.

Предположим, что $b^p \in K$, и рассмотрим отображение $\delta : D \to D$, переводящее $d \in D$ в $db - bd$. Поскольку $b \notin K$, найдется $d_0 \in D$, такое, что $\delta(d_0) \neq 0$. В то же время $\delta^p(d_0) = d_0 b^p - b^p d_0 = 0$, так как $b^p \in K$. Пусть $m$ — наименьшее натуральное число, такое, что $\delta^m(d_0) = 0$, $t = \delta^{m-1}(d_0)$, $w = \delta^{m-2}(d_0)$ и $u = b^{-1}t$. Тогда $t = \delta w = wb - bw$, а $\delta t = 0$, т. е. $tb = bt$, и потому $ub = bu$. Но отсюда $b = tu^{-1} = (wb - bw)u^{-1} = wbu^{-1} - bwu^{-1} = (wu^{-1})b - b(wu^{-1})$, т. е. $b = cb - bc$, где $c = wu^{-1}$. Домножая на $b^{-1}$, получаем $c = 1 + bcb^{-1}$.

Как и для $a$, для $c$ найдется показатель $p^n = q$, такой, что элемент $c^q$ сепарабелен над $K$. Но из равенства $c = 1 + bcb^{-1}$ следует, что $c^q = 1 + bc^q b^{-1}$, и если $c^q \in K$, то $c^q = 1 + c^q$, что невозможно. Итак, $c^q \notin K$, что и требовалось доказать.

Теперь мы уже можем легко доказать лемму индукцией по размерности $[D : K]$. База индукции, $[D : K] = 1$, тривиальна. Предположим, что для тел меньшей размерности над центром лемма уже доказана.

Выберем в $D$ элемент $a \in D \setminus K$, сепарабельный над $K$, и положим $F = K[a]$, $D_1 = C_D(F)$. По теореме IV.4.6 $F = C_D(D)$, т. е., поскольку $F \subset D_1$, $F = C(D_1)$. Но $[D_1 : F] < [D : K]$. Значит, в $D_1$ есть максимальное подполе $L$, сепарабельное над $F$. Тогда $[D_1 : F] = [L : F]^2$, а $[D : K] = [D_1 : K][F : K] = [D_1 : F] \times [F : K]^2 = [L : F]^2 [F : K]^2 = [L : F]^2$, т. е. $L$ — максимальное подполе в $D$ (по теореме IV.5.1). Поскольку $F$ сепарабельно над $K$, по следствию 3.7 $L$ также сепарабельно над $K$, что и требовалось доказать.

**Следствие 6.2.** *У всякой простой центральной алгебры есть нормальное поле расщепления.*

Для доказательства достаточно воспользоваться теоремой IV.5.1 и следствием 4.5.

В терминах группы Брауэра следствие 6.2 означает, что

$$\mathrm{Br}\, K = \bigcup_L \mathrm{Br}\,(L/K),$$

где $L$ пробегает нормальные расширения поля $K$.

Пусть теперь $D$ — центральное тело с нормальным полем расщепления $L$. По теореме IV.5.3 для некоторого $m$ $L$ вкладывается в алгебру $A = M_m(D)$, причем $[A : K] = [L : K]^2$. Если $\sigma \in G(L/K)$, то по теореме Сколема—Нётер (точнее, по следствию IV.4.2) $\sigma$ продолжается до внутреннего автоморфизма алгебры $A$. Иными словами, в $A$ найдется такой обратимый элемент $a_\sigma$, что для любого $x \in L$ $\sigma(x) = a_\sigma x a_\sigma^{-1}$, или $a_\sigma x = \sigma(x) a_\sigma$. При этом элемент $a_\sigma$, очевидно, определен с точностью до множителя, перестановочного со всеми $x \in L$, т. е., поскольку $L = C_A(L)$, с точностью до множителя из $L$.

Но если $\tau$ — другой элемент группы $G = G(L/K)$, то $\sigma\tau(x) = a_{\sigma\tau} x a_{\sigma\tau}^{-1}$, и в то же время

$$\sigma\tau(x) = \sigma(a_\tau x a_\tau^{-1}) = a_\sigma a_\tau x a_\tau^{-1} a_\sigma^{-1} = (a_\sigma a_\tau)\, x\, (a_\sigma a_\tau)^{-1},$$

откуда $a_\sigma a_\tau = \gamma_{\sigma,\tau} a_{\sigma\tau}$ для некоторого $\gamma_{\sigma,\tau} \in L$. Итак, получаем функцию $\gamma_{\sigma,\tau}$ от двух переменных $\sigma, \tau \in G$ со значениями в мультипликативной группе $L^*$ поля $L$. Вычисляя двумя способами $a_\sigma a_\tau a_\rho$, получаем

$$(a_\sigma a_\tau)\, a_\rho = \gamma_{\sigma,\tau} a_{\sigma\tau} a_\rho = \gamma_{\sigma,\tau}\gamma_{\sigma\tau,\rho} a_{\sigma\tau\rho},$$

$$a_\sigma\, (a_\tau a_\rho) = a_\sigma \gamma_{\tau,\rho} a_{\tau\rho} = \sigma(\gamma_{\tau,\rho})\, a_\sigma a_{\tau\rho} = \sigma(\gamma_{\tau,\rho})\, \gamma_{\sigma,\tau\rho} a_{\sigma\tau\rho},$$

откуда

$$\gamma_{\sigma,\tau}\gamma_{\sigma\tau,\rho} = \sigma(\gamma_{\tau,\rho})\, \gamma_{\sigma,\tau\rho}. \tag{1}$$

Функция $\gamma$, удовлетворяющая этому уравнению, называется *коциклом* группы $G$ со значениями в $L^*$ (точнее, двумерным коциклом). Легко проверить, что произведение коциклов также есть коцикл. Поэтому можно говорить о *группе коциклов* $Z(G, L^*)$.

Наоборот, пусть $\gamma \in Z(G, L^*)$. Построим алгебру $A = A(G, L, \gamma)$, которая называется *скрещенным произведением* группы $G$ на поле $L$, определенным коциклом $\gamma$.

Элементами алгебры $A(G, L, \gamma)$ будут формальные линейные комбинации $\sum_{\sigma \in G} a_\sigma e_\sigma$, где $a_\sigma$ — элементы поля $L$, а $e_\sigma$ — некоторые символы.

Структура векторного пространства на $A$ определяется обычным «покоординатным образом», а умножение определяется правилами

$$e_\sigma x = \sigma(x)\, e_\sigma, \quad x \in L; \qquad e_\sigma e_\tau = \gamma_{\sigma,\tau} e_{\sigma\tau}$$

(элементы же из $L$ умножаются обычным образом). Ассоциативность введенного так умножения следует непосредственно из уравнения (1) для коцикла.

**Теорема 6.3.** *$A = A(G, L, \gamma)$ есть простая центральная алгебра над полем $K$, а $L$ — ее поле расщепления.*

Доказательство. Если элемент $\sum_\sigma a_\sigma e_\sigma$ лежит в центре $A$, то он, в частности, перестановочен со всеми элементами из $L$, откуда

$$a\sum_\sigma a_\sigma e_\sigma = \sum_\sigma (aa_\sigma)\, e_\sigma = \Big(\sum_\sigma a_\sigma e_\sigma\Big)\, a = \sum_\sigma a_\sigma e_\sigma a = \sum_\sigma a_\sigma \sigma(a)\, e_\sigma,$$

т. е., как только $a_\sigma \neq 0$, $a = \sigma(a)$ для всех $a \in L$, откуда $\sigma = 1$. Итак, $C_A(L) = L$, а тогда $C(A) \subset L$. Но если элемент $a \in L$ лежит в $C(A)$, то $ae_\sigma = e_\sigma a = \sigma(a) e_\sigma$ для всех $\sigma \in G$, т. е. $a \in \operatorname{Inv} G = K$. Следовательно, алгебра $A$ центральна.

Пусть теперь $I$ — идеал в $A$. Выберем в $I$ ненулевой элемент $x = \sum_\sigma a_\sigma e_\sigma$ с наименьшим числом ненулевых коэффициентов $a_\sigma$. Домножая $x$ на $e_\sigma^{-1}$, можно считать, что $a_1 \neq 0$. Возьмем произвольный элемент $a \in L$. Тогда $ax - xa \in I$. Но

$$ax - xa = \sum_\sigma aa_\sigma e_\sigma - \sum_\sigma a_\sigma e_\sigma a = \sum_\sigma aa_\sigma e_\sigma - \sum_\sigma a_\sigma \sigma(a)\, e_\sigma =$$

$$= \sum_\sigma (aa_\sigma - \sigma(a)\, a_\sigma)\, e_\sigma,$$

причем $aa_1 - 1(a)\, a_1 = 0$, т. е. в $ax - xa$ меньше ненулевых координат. Значит, $ax - xa = 0$ и $x \in C_A(L) = L$. Но тогда $x$ обратим и $I = A$.

Осталось проверить, что $L$ — это поле расщепления $A$. Но это сразу следует из того, что $C_A(L) = L$ и теоремы IV.4.6.

**Следствие 6.4.** *Пусть $D$ — центральное тело, $L$ — его нормальное поле расщепления. Тогда для некоторого $m$ и некоторого коцикла $\gamma \in Z(G, L^*)$ $M_m(D) \simeq A(G, L, \gamma)$.*

Доказательство. Выше мы уже построили в $M_m(D)$ элементы $e_\sigma$, которые перемножаются между собой и с элементами из $L$ в точности так же, как одноименные элементы из $A = A(G, L, \gamma)$. Это дает возможность определить гомоморфизм алгебр $f: A \to M_m(D)$. Поскольку алгебра $A$ проста, $f$ есть мономорфизм. Но так как $(G : 1) = [L : K]$, $[A : K] = [L : K]^2 = [M_m(D) : K]$ (см. теорему IV.5.3), то $f$ — изоморфизм, что и требовалось доказать.

Коцикл $\delta \in Z(G, L^*)$ называется кограницей, если существует функция $\mu_\sigma$, определенная на $G$ и со значениями в $L^*$, такая, что

$$\delta_{\sigma,\tau} = \mu_\sigma \sigma(\mu_\tau)\, \mu_{\sigma\tau}^{-1}$$

для любых $\sigma, \tau \in G$.

**Теорема 6.5.** *Пусть $\gamma$ и $\eta$ — два коцикла из $Z(G, L^*)$. Алгебры $A = A(G, L, \gamma)$ и $B = A(G, L, \eta)$ изоморфны тогда и только тогда, когда $\gamma = \delta\eta$ для некоторой кограницы $\delta$.*

Доказательство. Предположим, что $f: A \xrightarrow{\sim} B$. Тогда $f(L)$ — подполе в $B$, изоморфное $L$. Применяя следствие IV.4.2 из теоремы Сколема—Нётер, можно считать, что $f(a) = a$ для всех $a \in L$. Обозначим $f_\sigma = f(e_\sigma) \in B$. Тогда

$$f(e_\sigma a) = f_\sigma a = f(\sigma(a) e_\sigma) = \sigma(a) f_\sigma,$$

откуда следует, что $f_\sigma = \mu_\sigma e_\sigma$ для некоторого $\mu_\sigma \in C_B(L) = L$. Но тогда

$$f(e_\sigma e_\tau) = f_\sigma f_\tau = \mu_\sigma e_\sigma \mu_\tau e_\tau = \mu_\sigma \sigma(\mu_\tau) e_\sigma e_\tau = \mu_\sigma \sigma(\mu_\tau) \eta_{\sigma,\tau} e_{\sigma\tau} :=$$

$$= f(\gamma_{\sigma,\tau} e_{\sigma\tau}) = \gamma_{\sigma,\tau} f_{\sigma\tau} = \gamma_{\sigma,\tau} \mu_{\sigma\tau} e_{\sigma\tau},$$

т. е. $\gamma_{\sigma,\tau} = \mu_\sigma \sigma(\mu_\tau) \mu_{\sigma\tau}^{-1} \eta_{\sigma,\tau}$.

Наоборот, пусть $\gamma = \delta\eta$, где $\delta_{\sigma,\tau} = \mu_\sigma \sigma(\mu_\tau) \mu_{\sigma\tau}^{-1}$. Определим отображение $f: A \to B$, положив $f\left(\sum_\sigma a_\sigma e_\sigma\right) = \sum_\sigma a_\sigma \mu_\sigma e_\sigma$. Нетрудно убедиться, что $f$ является гомоморфизмом алгебр. Но из-за простоты $A$ и равенства размерностей $A$ и $B$ $f$ будет изоморфизмом, что и требовалось доказать.

Когранницы образуют подгруппу $B(G, L^*)$ в группе $Z(G, L^*)$, а теорема 6.5 вместе со следствием 6.4 означает, что элементы группы $\mathrm{Br}(L/K)$ находятся во взаимно однозначном соответствии с элементами факторгруппы

$$H(G, L^*) = Z(G, L^*)/B(G, L^*).$$

**Теорема 6.6.** $\mathrm{Br}(L/K) \simeq H(G, L^*)$.

Доказательство основывается на следующей лемме.

**Лемма 6.7.** *$A(G, L, \gamma) \otimes A(G, L, \eta) \simeq M_n(A(G, L, \gamma\eta))$, где $n = [L : K]$.*

Доказательство. Обозначим $A = A(G, L, \gamma)$; $B = A(G, L, \eta)$. Поскольку поле $L$ вкладывается и в $A$, и в $B$, в $A \otimes B$ содержится подалгебра $L \otimes L$. Как показано в доказательстве теоремы 5.2, в $L \otimes L$ лежит единственный ненулевой идемпотент $f$, такой, что $(x \otimes 1) f = f(1 \otimes x)$ для всех $x \in L$. Покажем, что для любого $\sigma \in G$ $f(e_\sigma \otimes e_\sigma) = (e_\sigma \otimes e_\sigma) f$. Действительно, $(e_\sigma \otimes e_\sigma)^{-1} \times$ $\times f(e_\sigma \otimes e_\sigma)$ — также идемпотент в $L \otimes L$, причем

$$(x \otimes 1)(e_\sigma \otimes e_\sigma)^{-1} f(e_\sigma \otimes e_\sigma) = (e_\sigma \otimes e_\sigma)^{-1} (\sigma(x) \otimes 1) f(e_\sigma \otimes e_\sigma) =$$

$$= (e_\sigma \otimes e_\sigma)^{-1} f(1 \otimes \sigma(x))(e_\sigma \otimes e_\sigma) = (e_\sigma \otimes e_\sigma)^{-1} f(e_\sigma \otimes e_\sigma)(1 \otimes x),$$

поскольку $e_\sigma x = \sigma(x) e_\sigma$, т. е. $x e_\sigma^{-1} = e_\sigma^{-1} \sigma(x)$. Значит, $(e_\sigma \otimes e_\sigma)^{-1} \times$ $\times f(e_\sigma \otimes e_\sigma) = f$, что и требовалось проверить.

Рассмотрим теперь алгебру $T = f(A \otimes B) f$. Сопоставляя элементу $a \in L$ элемент $\bar{a} = f(1 \otimes a) = (a \otimes 1) f$, мы получим вложе-

ние поля $L$ в алгебру $T$. Обозначим также $\bar{e}_\sigma = f(e_\sigma \otimes e_\sigma) = (e_\sigma \otimes e_\sigma) f$. Тогда

$$\bar{a}\bar{b} = \overline{ab}, \quad \bar{e}_\sigma \bar{a} = (e_\sigma \otimes e_\sigma) f (1 \otimes a) = (e_\sigma \otimes e_\sigma)(a \otimes 1) f =$$

$$= (\sigma(a) \otimes 1)(e_\sigma \otimes e_\sigma) f = \overline{\sigma(a)}\,\bar{e}_\sigma,$$

$$\bar{\gamma}_{\sigma,\tau}\bar{e}_\tau = f(e_\sigma \otimes e_\sigma)(e_\tau \otimes e_\tau) = f(e_\sigma e_\tau \otimes e_\sigma e_\tau) = f(\gamma_{\sigma,\tau} e_{\sigma\tau} \otimes \eta_{\sigma,\tau} e_{\sigma\tau}) =$$

$$= f(\gamma_{\sigma,\tau} \otimes 1)(1 \otimes \eta_{\sigma,\tau})(e_{\sigma\tau} \otimes e_{\sigma\tau}) = (\gamma_{\sigma,\tau}\eta_{\sigma,\tau} \otimes 1) f(e_{\sigma\tau} \otimes e_{\sigma\tau}) =$$

$$= \bar{\gamma}_{\sigma,\tau}\bar{\eta}_{\sigma,\tau}\bar{e}_{\sigma\tau}.$$

Поэтому отображение $\sum_\sigma a_\sigma e_\sigma \to \sum_\sigma \bar{a}_\sigma \bar{e}_\sigma$ есть гомоморфизм (а, значит, мономорфизм) $A(G, L, \gamma\eta) \to T$.

С другой стороны, $T \simeq E_{A \otimes B}(f(A \otimes B))$. Но разложение единицы в $L \otimes L$ имеет вид $1 = \sum_{\sigma \in G} f_\sigma$, где $f_\sigma$ — такой (единственный) идемпотент, что $xf_\sigma = f_\sigma \sigma(x)$ для всех $x \in L$. Кроме того, $(1 \otimes e_\tau) \times f_\sigma (1 \otimes e_\tau)^{-1} = f_{\tau\sigma}$ (см. доказательство теоремы 5.2). Поэтому все модули $f_\sigma(A \otimes B)$ изоморфны между собой, и в частности, изоморфны $f(A \otimes B)$, $f = f_1$. Следовательно, $A \otimes B \simeq M_n(T)$, откуда $[T : K] = n^2 = [A(G, L, \gamma\eta) : K]$, т. е. $T \simeq A(G, L, \gamma\eta)$, что и завершает доказательство.

Доказательство теоремы 6.6 следует теперь из того, что отображение $Z(G, L^*) \to \mathrm{Br}(L/K)$ есть гомоморфизм (по лемме 6.7), его ядро есть $B(G, L^*)$ (по теореме 6.5), и это отображение эпиморфно (по следствию 6.4).

**Следствие** 6.8. *Алгебра $A(G, L, \gamma)$ изоморфна $M_n(K)$ тогда и только тогда, когда $\gamma \in B(G, L^*)$.*

## *Упражнения к главе V*

1. Пусть $K$ — поле характеристики $p > 0$. Доказать, что отображение $\varphi$, переводящее элемент $a \in K$ в $a^p$, является эндоморфизмом поля $K$. Это отображение называется эндоморфизмом Фробениуса. Доказать, что если поле $K$ конечно, то $\varphi$ — автоморфизм. Вычислить $\mathrm{Im}\,\varphi$, если $K = F(t)$ — поле рациональных функций над некоторым полем $F$.

2. Доказать, что группа автоморфизмов конечного поля — циклическая, а автоморфизм Фробениуса является ее образующим.

3. Предположим, что характеристика поля $K$ не равна 2. Показать, что всякое квадратичное расширение $L$ поля $K$, т. е. такое поле, что $[L:K] = 2$, является полем разложения некоторого многочлена вида $x^2 - a$, где $a$ — неквадрат в $K$. Обычно пишут $L = K[\sqrt{a}]$. Проверить, что $K[\sqrt{a}] \simeq K[\sqrt{b}]$ тогда и только тогда, когда $ab^{-1}$ — квадрат в $K$.

4. Найти поле разложения многочлена $x^3 - 2$ над полем рациональных чисел. Вычислить его группу Галуа над полем рациональных чисел.

5.а) Пусть $K$ — конечное поле из $q$ элементов, $f(x)$ — неприводимый многочлен степени $d$ над полем $K$. Доказать, что $f(x)$ делит $x^{q^d} - x$, и, наоборот, если $f(x)$ делит $x^{q^d} - x$, то $d$ делит $n$.

б) Обозначим через $\psi(d)$ число неприводимых многочленов степени $d$ со старшим коэффициентом 1 над полем $K$. Доказать, что тогда $q^n = \sum_{d/n} d\psi(d)$.

в) Используя формулу обращения Мёбиуса (см., например, И. М. Виноградов «Основы теории чисел». М., 1965), доказать, что

$$\psi(n) = \frac{1}{n} \sum_{d/n} \mu\left(\frac{n}{d}\right) q^d,$$

где $\mu$ — функция Мёбиуса.

6. Пусть $K$ — поле характеристики $p > 0$, $F = K[a]$ — его конечное моногенное расширение, $m(x)$ — минимальный многочлен элемента $a$ над $K$. Доказать, что алгебра $F \otimes F$ локальна тогда и только тогда, когда $m(x) = x^{p^k} - \alpha$ для некоторого целого $k$ и некоторого $\alpha \in K$. В этом случае неприводимый многочлен $m(x)$ и элемент $a$ называются чисто несепарабельными, а показатель $k$ — высотой элемента $a$.

7. Пусть $L$ — конечное расширение поля $K$. Доказать равносильность следующих условий:

1) $L \otimes L$ — локальная алгебра;
2) для любой локальной коммутативной алгебры $A$ алгебра $A \otimes L$ локальна;
3) всякий элемент поля $L$ чисто несепарабелен;
4) $L = K[a_1, \ldots, a_t]$, где все элементы $a_i$ чисто несепарабельны.

Показать, что в последнем случае высота любого элемента поля $L$ не превосходит наибольшую из высот элементов $a_1, \ldots, a_t$.

8. Пусть $K = K_0 \subset K_1 \subset \ldots \subset K_n = L$ — цепочка конечных расширений. Доказать, что $L$ чисто несепарабельно над $K$ тогда и только тогда, когда каждое $K_i$ чисто несепарабельно над $K_{i-1}$.

9. Для всякого конечного расширения $L$ поля $K$ обозначим $L_s$ совокупность всех сепарабельных, а $L_i$ — совокупность всех чисто несепарабельных элементов поля $L$. Доказать, что: а) $L_s$ и $L_i$ — подполя поля $L$, причем $L_s \cap L_i = K$; б) $L$ чисто несепарабельно над $L_s$.

Предположим теперь, что $L_s$ нормально. Доказать, что: в) $L$ сепарабельно над $L_i$; г) если $\{a_1, \ldots, a_n\}$ — базис $L_s$, а $\{b_1, \ldots, b_m\}$—базис $L_i$, то $\{a_k b_j\}$ ($k = 1, \ldots, n$; $j = 1, \ldots, m$) — базис поля $L$.

В частности, $[L : K] = [L_s : K][L_i : K]$ и $L$ — наименьшее поле, содержащее $L_s$ и $L_i$. Подполя $L_s$ и $L_i$ называются соответственно сепарабельной и чисто несепарабельной частью расширения $L$.

10. Доказать, что если $L$ — конечное расширение поля $K$, то следующие условия равносильны; 1) $L$ моногенно; 2) $L$ содержит лишь конечное число подполей. (Указание к доказательству 1) $\Rightarrow$ 2): показать, что если $L = K[a]$, $F$ — подполе в $L$, а $x^m + b_1 x^{m-1} + \ldots + b_m$ — минимальный многочлен $a$ над $F$, то $F = K[b_1, \ldots, b_m]$.) Построить пример немоногенного расширения. (Указание: положить $K = F(x, y)$ — поле рациональных функций от двух переменных над полем характеристики $p > 0$.)

11. Пусть $F$ — подполе конечного расширения $L$ поля $K$, $d = [F : K]$ Доказать, что число различных гомоморфизмов $F \to L$ (считая тождественный) не превосходит $d$ и равно $d$ тогда и только тогда, когда $F$ сепарабельно, а $L$ содержит подполе $F' \supset F$, нормальное над $K$.

12. Доказать, что наименьшее нормальное расширение, содержащее данное сепарабельное, определено однозначно с точностью до изоморфизма.

13. Предположим, что конечное расширение $L$ поля $K$ является композитом своих подполей $L_1$ и $L_2$ (т. е. наименьшим полем, содержащим $L_1$ и $L_2$), причем $L_2$ нормально над $K$. Доказать, что тогда $L$ нормально над $L_1$, причем $G(L/L_1) \simeq \mathrm{Inv}(L_1 \cap L_2) \subset G(L_2/K)$.

Следующий цикл упражнений (с 14 по 22) посвящен решению уравнений в радикалах. Для простоты характеристика основного поля $K$ в этих упражнениях предполагается равной 0, кроме упражнения 22, в котором указывается, какие изменения должны быть внесены для полей положительной характеристики.

**14.** Пусть $L$ — поле разложения многочлена $x^n - 1$. Доказать, что в $L$ содержится «первообразный корень степени $n$ из 1», т. е. такой корень $\zeta$ данного многочлена, что все остальные являются его степенями; более того, число таких корней равно $\varphi(n)$, где $\varphi$ — функция Эйлера. Используя это, показать, что $G(L/K)$ — циклическая группа, порядок которой делит $\varphi(n)$.

**15.** Предполагая, что $K$ содержит первообразный корень степени $n$ из 1, доказать, что если $L = K[a]$, где $a$ — корень многочлена $x^n - \alpha$, $\alpha \in K$, то $L$ — нормальное расширение, $G(L/K)$ циклична, а ее порядок делит $n$. В частности, если $p$ — простое число, то многочлен $x^p - \alpha$ либо неприводим, либо разлагается в поле на линейные множители.

**16.** Наоборот, пусть по-прежнему $K$ содержит первообразный корень $\zeta$ степени $n$ из 1, а $L$ — нормальное расширение $K$ с циклической группой Галуа порядка $n$. Доказать, что тогда $L = K[a]$, где минимальный многочлен элемента $a$ имеет вид $x^n - \alpha$. (Указание: за $a$ можно принять $\omega + \zeta\sigma(\omega) + \zeta^2\sigma^2(\omega) + \ldots + \zeta^{n-1}\sigma^{n-1}(\omega)$, где $\sigma$ — образующий $G(L/K)$, а $\omega$ — образующий $KG$-модуля $L$.)

**17.** Говорят, что $L$ — радикальное расширение поля $K$, если в нем есть цепочка подполей $K = L_0 \subset L_1 \subset \ldots \subset L_m = L$, такая, что $L_i = L_{i-1}[a_i]$, где минимальный многочлен элемента $a_i$ над полем $L_{i-1}$ имеет вид $x^{n_i} - \alpha_i$ (очевидно, уплотняя эту цепочку, можно добиться, чтобы все степени $n_i$ были простыми числами). Предполагая, что $K$ содержит первообразные корни всех степеней $n_i$ из 1, показать, что всякое радикальное расширение вкладывается в нормальное радикальное расширение.

**18.** Расширение $L$ назовем разрешимым, если его можно вложить в радикальное расширение. Доказать, что поле разложения многочлена $x^n - 1$ разрешимо для любого $n$. (Указание: доказывать по индукции, с использованием результатов упражнений 14—16.)

**19.** Доказать, что расширение $L$ и наименьшее нормальное расширение, содержащее $L$ (упражнение 12), разрешимы одновременно. (Указание: использовать результаты упражнений 17 и 18.)

**20.** Доказать, что нормальное расширение $L$ разрешимо тогда и только тогда, когда разрешима его группа Галуа $G$, т. е. в ней есть такой ряд подгрупп $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{1\}$, что $G_i$ нормальна в $G_{i-1}$ и факторгруппа $G_i/G_{i-1}$ абелева для всех номеров $i$. (Указание: можно считать, что $G_i/G_{i-1}$ циклична, а $L$ радикально и воспользоваться результатами упражнений 15 и 16; упражнение 18 позволяет присоединить корни из 1, а упражнение 13 — проследить, как при этом изменяется группа Галуа.)

**21.** Неприводимое уравнение $f(x) = 0$, где $f(x) \in K[x]$, называется разрешимым в радикалах, если оно имеет корень в некотором радикальном расширении. Доказать, что для этого необходимо и достаточно, чтобы поле разложения многочлена $f(x)$ было разрешимым.

**22.** Разработать аналогичную теорию для полей характеристики $p > 0$. При этом в определении радикального расширения нужно допустить еще многочлены вида $x^p - x - \alpha$. Соответственно, нужно модифицировать упражнение 16 (при $n = p$, $\alpha \in K$). Учесть также, что чисто несепарабельное расширение всегда радикально.

Упражнения 23—27 посвящены важному примеру скрещенных произведений — циклическим алгебрам. Известный результат Брауэра, Нётер и Хассе говорит о том, что если $K$ — поле алгебраических чисел (т. е. конечное расширение поля $\mathbf{Q}$), то эта конструкция дает все центральные тела над $K$. Во всех этих упражнениях предполагается, что $L$ — нормальное расширение поля $K$ с циклической группой Галуа $G$ порядка $n$; образующий этой группы обозначается $\sigma$.

23. Пусть $\gamma \in Z(G, L^*)$ — коцикл группы $G$ со значениями в $L^*$. Доказать, что он лежит в одном классе смежности по подгруппе кограниц $B(G, L^*)$ с некоторым коциклом $\eta$ вида

$$\eta_{\sigma^i, \sigma^j} = \begin{cases} 1, & \text{если } i + j < n, \\ \alpha, & \text{если } i + j \geqslant n, \end{cases}$$

где $\alpha \in K^*$. Соответствующую алгебру $A(G, L, \gamma)$ обозначим $A(L, \sigma, \alpha)$ (она зависит, вообще говоря, от выбора образующего $\sigma$). (Указание: в алгебре $A(G, L, \gamma)$ элемент $e_{\sigma^i}$ можно заменить на $e_{\sigma}^i$.)

24. Доказать, что $A(L, \sigma, \alpha) \simeq A(L, \sigma, \beta)$ тогда и только тогда, когда в $L^*$ найдется такой элемент $\lambda$, что $\beta = \alpha N(\lambda)$, где $N(\lambda) = \lambda\sigma(\lambda)\sigma^2(\lambda) \ldots \sigma^{n-1}(\lambda)$. Проверить, что $N$ — гомоморфизм группы $L^*$ в группу $K^*$, и вывести отсюда, что $\mathrm{Br}(L/K) \simeq K^*/\mathrm{Im}\, N$. Гомоморфизм $N$ называется нормой.

25. Пусть $K$ — конечное поле, $L$ — его конечное расширение. Доказать, что в этом случае норма $N : L^* \to K^*$ является эпиморфизмом. (Указание: применить теорему Веддерберна о конечных телах.)

26. Обозначим $K = F(t)$ поле рациональных функций над полем $F$ из двух элементов. Доказать, что многочлен $x^2 + x + 1$ неприводим над полем $K$. (Возможно, это упражнение будет легче, если за $K$ принять поле $F((t))$ формальных степенных рядов над полем $F$.)

27. В обозначениях предыдущего упражнения пусть $L = K[a]$, где $a$ — корень многочлена $x^2 + x + 1$. Доказать, что если $N : L^* \to K^*$ — норма (см. упражнение 24), то $t \notin \mathrm{Im}\, N$. Используя результат упражнения 24, построить четырехмерное тело $D$ над $K$, содержащее подполе, изоморфное $K[\sqrt{t}]$, что дает пример чисто несепарабельного поля расщепления центрального тела.

28. Доказать «теорему о независимости автоморфизмов»: если $L$ — нормальное расширение поля $K$, $G = G(L/K)$, то для любой функции $f : G \to L$ найдется такой элемент $a \in L$, что $\sum_{\sigma \in G} f(\sigma)\sigma(a) \neq 0$. (Указание: воспользоваться теоремой 6.3, рассмотрев $L$ как модуль над алгеброй $A(G, L, 1)$, где 1 — единичный коцикл.)

# VI

ГЛАВА

## СЕПАРАБЕЛЬНЫЕ АЛГЕБРЫ

Среди полупростых алгебр особое место занимают такие, которые остаются полупростыми при любом расширении основного поля. Эти алгебры называются сепарабельными. Примерами сепарабельных алгебр являются, с одной стороны, центральные простые ал-

гебры, а с другой стороны — сепарабельные поля. Оказывается, общий случай представляет собой в некотором смысле комбинацию этих двух примеров. Мы установим также следующие основные свойства сепарабельных алгебр: полупростота всех бимодулей; теорема Веддербёрна—Мальцева о подъеме сепарабельной факторалгебры (этот результат мы используем в гл. VIII для обобщения конструкций «универсальной алгебры» из § 6 гл. III); невырожденность формы главного следа (играющая важную роль в теории чисел при изучении арифметических свойств сепарабельных алгебр).

## § 1. Бимодули над сепарабельными алгебрами

Алгебра $A$ над полем $K$ называется сепарабельной, если для любого расширения $L$ поля $K$ алгебра $A_L = A \otimes L$ полупроста.

В частности, сепарабельная алгебра полупроста, однако обратное, вообще говоря, неверно: если $L$ — несепарабельное расширение поля $K$, то $L$ — полупростая $K$-алгебра, но $L \otimes L$ — неполупростая алгебра, как следует из теоремы V.3.6.

Мы дадим описание сепарабельных алгебр и критерий сепарабельности, обобщающий теорему V.3.6.

Прежде всего установим следующий простой результат.

**Лемма 1.1.** *Для любой $K$-алгебры $A$ существует такое расширение $L$ поля $K$, что $L$-алгебра $A_L$ расщепима, т. е.*

$$A_L/\operatorname{rad} A_L \simeq M_{n_1}(L) \times \ldots \times M_{n_s}(L).$$

Доказательство. Пусть $\bar{A} = A/\operatorname{rad} A \simeq \prod_{i=1} M_{k_i}(D_i)$, где $D_i$ — тела, причем, например, $[D_1 : K] = d > 1$.

Поскольку $(\operatorname{rad} A) \otimes L$, очевидно,—нильпотентный идеал, он содержится в $\operatorname{rad} A_L$ для любого поля $L$. Следовательно, $A_L/\operatorname{rad} A_L$— факторалгебра алгебры $\bar{A}_L$. Выберем в $D_1$ элемент $a \notin K$. Пусть $p(x)$ — его минимальный многочлен, $F = K[a]$. Поскольку $p(x)$ имеет корень в $F$, $D_1 \otimes F$ — не тело. Следовательно, если обозначить $B = M_{k_1}(D_1)$, то тела, входящие в разложение алгебры $B_F/\operatorname{rad} B_F$, имеют размерности над $F$ меньшие, чем размерность $[D_1 : K]$. Продолжая это «понижение размерностей», мы получим в конце концов такое поле $L$, что $A_L$— расщепимая алгебра.

Поле $L$, существование которого утверждает лемма 1.1, называется полем расщепления алгебры $A$. Заметим, что оно определяется далеко не однозначно. Даже минимальное поле расщепления, т. е. такое, подполя которого уже не являются полями расщепления, определяется не однозначно (см. упражнение 6 к гл. IV).

**Теорема 1.2.** *Следующие условия равносильны:*

*1) алгебра $A$ сепарабельна;*

*2) алгебра $A \otimes A^\circ$ полупроста;*

*3)* $A \simeq A_1 \times A_2 \times \ldots \times A_s$, *где* $A_i$ — *простые алгебры с сепарабельными центрами.*

Доказательство. 1) $\Rightarrow$ 2). Пусть $L$ — поле расщепления алгебры $A$. Поскольку $A_L$ — полупростая алгебра, $A_L \simeq \simeq M_{n_1}(L) \times \ldots \times M_{n_t}(L)$. Тогда $(A_L) \otimes_L (A_L^\circ)$ — прямое произведение алгебр вида $M_k(L) \otimes_L M_m(L) \simeq M_{km}(L)$, т. е. полупростая алгебра. Остается заметить, что $(A_L) \otimes_L (A_L^\circ) = (A \otimes L) \otimes_L (L \otimes \otimes A^\circ) \simeq A \otimes (L \otimes_L L) \otimes A^\circ \simeq A \otimes L \otimes A^\circ \simeq (A \otimes A^\circ)_L$. А из полупростоты алгебры $(A \otimes A^\circ)_L$ следует полупростота $A \otimes A^\circ$.

2) $\Rightarrow$ 3). Если $A \otimes A^\circ$ полупроста, то и $A$ полупроста, т. е. $A = A_1 \times \ldots \times A_s$, где $A_i$ — простые алгебры, причем $A_i \otimes A_i^\circ$ — полупростые. Следовательно, центр алгебры $A_i \otimes A_i^\circ$ полупрост. Но $C(A_i \otimes A_i^\circ) = C(A_i) \otimes C(A_i^\circ) = C(A_i) \otimes C(A_i)$, откуда по теореме V.3.6. $C(A_i)$ — сепарабельное поле.

3) $\Rightarrow$ 1). Пусть $A = A_1 \times \ldots \times A_s$, где $A_i$ — простые алгебры, причем все центры $C_i = C(A_i)$ сепарабельны. По следствию V.6.2 существует сепарабельное расширение $F$ поля $C_i$, такое, что $A_i \otimes_{C_i} F \simeq M_k(F)$. Если $L$ — произвольное расширение поля $K$, то $(A_{i_L}) \otimes_{C_i} F \simeq L \otimes (A_i \otimes_{C_i} F) \simeq M_k(L \otimes F)$. Но из следствия V.3.7 вытекает, что $F$ сепарабельно над $K$. Значит, $L \otimes F$, а потому и $(A_{i_L}) \otimes_{C_i} F$ — полупростые алгебры. Отсюда, очевидно, следует полупростота $A_{i_L}$ и всей $A_L$ для любого поля $L$, т. е. сепарабельность $A$.

Заметим, что попутно мы установили такое следствие.

**Следствие 1.3.** *Алгебра* $A$ *сепарабельна тогда и только тогда, когда* $A_L \simeq M_{n_1}(L) \times \ldots \times M_{n_s}(L)$ *для некоторого расширения* $L$ *поля* $K$. *Кроме того, поле* $L$ *можно считать сепарабельным.*

**Следствие 1.4.** *Если поле* $K$ *совершенно (например, поле характеристики* 0 *или конечное поле), то всякая полупростая* $K$*-алгебра сепарабельна.*

Из полупростоты алгебры $A \otimes A^\circ$ мы получаем еще и такой результат.

**Следствие 1.5.** *Алгебра* $A$ *сепарабельна тогда и только тогда, когда всякий* $A$*-бимодуль полупрост.*

Очевидно, последнее утверждение можно переформулировать следующим образом: алгебра $A$ сепарабельна тогда и только тогда, когда всякий $A$-бимодуль (или, что то же, всякий $A \otimes A^\circ$-модуль) проективен. Замечательное обстоятельство состоит в том, что достаточно проверять проективность только регулярного бимодуля, т. е. самой алгебры $A$, рассматриваемой как $A \otimes A^\circ$-модуль.

**Теорема 1.6.** *Алгебра* $A$ *сепарабельна тогда и только тогда, когда регулярный* $A$*-бимодуль проективен.*

Доказательство. Предположим, что регулярный $A$-бимодуль проективен. Выберем некоторое поле расщепления $L$ алгебры $A$. Тогда $A_L/\operatorname{rad} A_L \simeq M_{n_1}(L) \times \ldots \times M_{n_s}(L)$. По теореме

III.3.5 $A$ является прямым слагаемым свободного $A \otimes A^\circ$-модуля $F$. Но тогда $A_L$ является прямым слагаемым свободного модуля $F_L$ над алгеброй $(A \otimes A^\circ)_L \simeq (A_L) \otimes_L (A_L^\circ)$, т. е. проективным $A_L$-бимодулем. В силу следствия III.1.8 радикал регулярного бимодуля совпадает с радикалом алгебры. Разложение факторалгебры $A_L/\operatorname{rad} A_L$ в прямое произведение простых алгебр дает разложение $A_L$-бимодуля $A_L/\operatorname{rad} A_L$ в прямую сумму простых бимодулей (минимальных идеалов этой факторалгебры).

В силу соответствия между проективными и полупростыми модулями (теорема III.3.6), ему соответствует разложение $A_L$ в прямую сумму идеалов, или, что то же, в прямое произведение алгебр $A_L = A_1 \times \ldots \times A_s$, причем $A_i/\operatorname{rad} A_i \simeq M_n(L)$, где $n = n_i$.

Тогда по теореме III.3.4 $A_i \simeq M_n(B)$, где $B/\operatorname{rad} B \simeq L$ ($B$, вообще говоря, зависит от номера $i$). Кроме того, так как $A_i$ — проективный $A_L$-бимодуль, а компоненты $A_j$ при $j \neq i$ действуют на нем нулевым образом, $A_i$ — проективный $A_i$-бимодуль. Заметим теперь, что если $R = \operatorname{rad} B$, то $I = (R \otimes_L B^\circ) \otimes (B \otimes_L R^\circ)$ — нильидеал в $B \otimes_L B^\circ$, причем $(B \otimes_L B^\circ)/I \simeq L \otimes_L L \simeq L$. Следовательно, по предложению III.1.3 $I = \operatorname{rad}(B \otimes_L B^\circ)$ и $B \otimes_L \otimes_L B^\circ$ — локальная алгебра, а $A_i \otimes A_i^\circ \simeq M_{n^2}(B \otimes_L B^\circ)$ — примарная алгебра. По теореме III.3.10 у нее есть ровно один главный модуль (очевидно, это $A_i$), причем $A_i \otimes_L A_i^\circ \simeq n^2 A_i$ как $A_i$-бимодуль. Но $[A_i : L] = n^2 b$, где $b = [B : L]$, $[A_i \otimes_L A_i^\circ : L] = n^4 b^2$, откуда $b = 1$, т. е. $B \simeq L$, $A_i \simeq M_n(L)$ и $A$ сепарабельна по следствию 1.3.

Отметим, наконец, что если $(A_L) \otimes_L (A_L^\circ)$ полупроста, то полупроста и алгебра $A \otimes A^\circ$, откуда получаем такое следствие.

**Следствие 1.7.** *Если $L$-алгебра $A_L$ сепарабельна для некоторого расширения $L$ поля $K$, то и $K$-алгебра $A$ сепарабельна.*

## § 2. Теорема Веддербёрна—Мальцева

Пусть $A$ — произвольная, вообще говоря, неполупростая алгебра, $R$ — ее радикал, $\bar{A} = A/R$, $\pi$ — проекция алгебры $A$ на факторалгебру $\bar{A}$. Во многих вопросах теории алгебр бывает важно «поднять» факторалгебру $\bar{A}$ до изоморфной ей подалгебры в $A$. Дадим точное определение.

Подъемом факторалгебры $\bar{A}$ назовем такой гомоморфизм алгебр $\varepsilon : \bar{A} \to A$, что $\pi\varepsilon = 1$. Очевидно, подъем $\varepsilon$ всегда является мономорфизмом, а $\operatorname{Im}\varepsilon = A_0$ — подалгебра в $A$, изоморфная $\bar{A}$, причем $A = A_0 \oplus R$ (прямая сумма векторных пространств).

Наоборот, если $A_0$ — подалгебра в $A$, изоморфная $\bar{A}$, то $A_0 \cap R = 0$ (так как $A_0$ полупроста). Следовательно, $A = A_0 \oplus R$ (так как $[A : K] = [A_0 : K] + [R : K]$). Тогда ограничение проекции $\pi$ на подалгебру $A_0$ дает изоморфизм $\bar{\pi} : A_0 \xrightarrow{\sim} \bar{A}$. Полагая

$\varepsilon = \bar{\pi}^{-1}$, мы получим подъем факторалгебры $A$. Итак, существование подъема равносильно дополнимости радикала.

Два подъема, $\varepsilon : \bar{A} \to A$ и $\eta : \bar{A} \to A$, назовем *сопряженными*, если в алгебре $A$ есть такой обратимый элемент $a$, что $\eta(x) = a\varepsilon(x)a^{-1}$ для всех $x \in \bar{A}$. Если, кроме того, $a = 1 + r$, где $r \in R$ (такие элементы называются *унипотентными*), то говорят, что $\varepsilon$ и $\eta$ *унипотентно сопряжены*.

Настоящий параграф будет посвящен доказательству следующего основного результата.

**Теорема 2.1** (Веддербёрн—Мальцев). *Если факторалгебра $\bar{A}$ сепарабельна, то подъем всегда существует и любые два подъема унипотентно сопряжены.*

Отметим, что без предположения сепарабельности оба утверждения теоремы перестают быть верными: подъем может не существовать (см. упражнение 4), а два различных подъема могут быть не сопряжены (см. упражнение 5).

*Доказательство* существования подъема проведем «поэтапно», постепенно расширяя класс алгебр, для которых устанавливается этот результат.

1) Предположим вначале, что алгебра $A$ расщепима, т. е. $\bar{A} \simeq M_{n_1}(K) \times \ldots \times M_{n_s}(K)$. Обозначим через $U_i$ простой $A$-модуль, принадлежащий $i$-й компоненте алгебры $\bar{A}$, $P_i$ — соответствующий главный $A$-модуль (см. следствие III.2.9). Тогда $\bar{A} = n_1U_1 \oplus \ldots \oplus n_sU_s$. Следовательно, $A \simeq n_1P_1 \oplus \ldots \oplus n_sP_s$ (теорема III.3.6).

Используя изоморфизм $A \simeq E_A(A)$ и матричную запись эндоморфизмов прямой суммы (см. § 7 гл. I), мы находим, что $A$ изоморфна алгебре матриц вида

$$\begin{pmatrix} x_{11} & x_{12} \ldots x_{1s} \\ x_{21} & x_{22} \ldots x_{2s} \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ x_{s1} & x_{s2} \ldots x_{ss} \end{pmatrix},$$

где $x_{ij} \in \mathrm{Hom}_A(n_jP_j, n_iP_i)$. В частности, $A$ содержит подалгебру «диагональных матриц», изоморфную $E_A(n_1P_1) \times \ldots \times E_A(n_sP_s) \simeq \simeq M_{n_1}(A_1) \times \ldots \times M_{n_s}(A_s)$, где $A_i = E_A(P_i)$, а потому и подалгебру, изоморфную $\bar{A}$, откуда, как мы видим, следует существование подъема.

2) Пусть теперь $\bar{A}$ — произвольная сепарабельная алгебра, но $R^2 = 0$. Выберем базис $\{a_1, \ldots, a_n\}$ в алгебре $A$ так, чтобы элементы $\{\bar{a}_1, \ldots, \bar{a}_m\}$, где $\bar{a}_i = \pi(a_i)$, образовывали базис факторалгебры $\bar{A}$, а элементы $\{a_{m+1}, \ldots, a_n\}$ — базис радикала $A$. Обозначим через $\{\alpha_{ij}^k\}$ структурные константы алгебры $A$. Иными словами, $a_ia_j =$

$= \sum_{k=1}^{n} \alpha_{ij}^{k} a_k$, а тогда $\bar{a}_i \bar{a}_j = \sum_{k=1}^{m} \alpha_{ij}^{k} \bar{a}_k$. Подъем $\varepsilon$, как линейное отображение, достаточно задавать на базисных элементах. Условие $\pi\varepsilon = 1$ означает, что $\varepsilon(\bar{a}_i)$ должен иметь вид $a_i + \sum_{j=m+1}^{n} x_{ij} a_j$, где $x_{ij} \in K$. Наконец, $\varepsilon$ будет гомоморфизмом тогда и только тогда, когда выполняется соотношение $\varepsilon(\bar{a}_i \bar{a}_j) = \varepsilon(\bar{a}_i)\,\varepsilon(\bar{a}_j)$. Но

$$\varepsilon(\bar{a}_i \bar{a}_j) = \varepsilon\Big(\sum_{k=1}^{m} \alpha_{ij}^{k} \bar{a}_k\Big) = \sum_{k=1}^{m} \alpha_{ij}^{k} \Big(a_k + \sum_{l=m+1}^{n} x_{kl} a_l\Big) =$$

$$= \sum_{l=1}^{m} \alpha_{ij}^{l} a_l + \sum_{k=1}^{m} \sum_{l=m+1}^{n} \alpha_{ij}^{k} x_{kl} a_l;$$

$$\varepsilon(\bar{a}_i)\,\varepsilon(\bar{a}_j) = \Big(a_i + \sum_{k=m+1}^{n} x_{ik} a_k\Big)\Big(a_j + \sum_{k=m+1}^{n} x_{jk} a_k\Big) =$$

$$= \sum_{l=1}^{n} \alpha_{ij}^{l} a_l + \sum_{k,l=m+1}^{n} x_{jk} \alpha_{ik}^{l} a_l + \sum_{k,l=m+1}^{n} x_{ik} \alpha_{kj}^{l} a_l.$$

Мы учли здесь, что произведение элементов радикала равно 0, а произведение любого элемента на элемент радикала вновь лежит в радикале. Приравнивая коэффициенты при базисных векторах $a_l$, мы получаем систему линейных уравнений для $x_{kl}$

$$\sum_{k=1}^{m} \alpha_{ij}^{k} x_{kl} = \alpha_{ij}^{l} + \sum_{k=m+1}^{n} \alpha_{ik}^{l} x_{jk} + \sum_{k=m+1}^{k} \alpha_{kj}^{l} x_{ik}, \quad i, j = 1, \ldots, n;$$

$$l = m + 1, \ldots, n.$$

Итак, в данном случае существование подъема равносильно разрешимости системы линейных уравнений, коэффициенты которой — структурные константы — не меняются при расширении основного поля. Но если $L$ — поле расщепления алгебры $A$, то $\bar{A}_L$ — расщепимая полупростая алгебра. Тогда ввиду 1) существует подъем $\bar{A}_L \to A_L$. Следовательно, наша система линейных уравнений (с коэффициентами из поля $K$) имеет решение в поле $L$. Но имеет место такой простой факт.

**Лемма 2.2.** *Если система линейных уравнений с коэффициентами из поля $K$ имеет решение в расширении этого поля, то она имеет решение и в $K$.*

Доказательство немедленно следует из теоремы Кронекера—Капелли.

Таким образом, существование подъема над $L$ влечет существование подъема и для исходной алгебры (в случае $R^2 = 0$).

3) Общий случай теперь легко получается индукцией по размерности радикала.

Пусть $R^2 \neq 0$ и $B = A/R^2$. В силу предыдущего пункта существует подъем $\bar{\varepsilon} : \bar{A} \to B$. Обозначим через $A'$ прообраз $\operatorname{Im} \bar{\varepsilon}$ в алгебре $A$. Тогда $A' \supset R^2$ и $A'/R^2 \simeq \operatorname{Im} \varepsilon \simeq \bar{A}$ — полупростая алгебра. Из предложения III.1.13 следует, что $R^2 = \operatorname{rad} A'$. Поскольку $\dim R^2 < \dim R$, к алгебре $A'$ применимо индукционное предположение и существует подъем $\varepsilon : \bar{A} \to A'$. Но тогда $\varepsilon$ будет и подъемом $\bar{A}$ в $A$.

Доказательству сопряженности мы предпошлем следующую теорему, обобщающую теорему IV.4.4 («двойственную» к теореме Сколема—Нётер). Этот результат представляет и самостоятельный интерес.

**Теорема 2.3.** *Если $f$ и $g$ — гомоморфизмы центральной простой алгебры $B$ в некоторую алгебру $A$, то в $A$ существует такой обратимый элемент $a$, что $g(b) = af(b)a^{-1}$ для всех $b \in B$.*

**Следствие 2.4.** *Изоморфные центральные простые подалгебры $B$ и $B'$ любой алгебры $A$ сопряжены. Более того, всякий изоморфизм $g : B \xrightarrow{\sim} B'$ продолжается до внутреннего автоморфизма алгебры $A$, т. е. имеет вид $g(b) = aba^{-1}$, где $a$ — обратимый элемент из $A$.*

Для доказательства, как и в теореме Сколема — Нётер, достаточно установить изоморфизм $B$-$A$-бимодулей ${}_fA$ и ${}_gA$ (см. гл. IV, § 1, пример 2). Но как правые $A$-модули оба они совпадают с регулярным модулем. Поэтому утверждение теоремы сводится к следующей лемме.

**Лемма 2.5.** *Пусть $A$ — произвольная, $B$ — центральная простая алгебра, $M$ и $N$ — некоторые $B$-$A$-бимодули. Тогда если $M$ и $N$ изоморфны как $A$-модули, то они изоморфны и как $B$-$A$-бимодули.*

Доказательство. Пусть $L$ — поле расщепления алгебры $B$. Так как $(A_L) \otimes_L (B^\circ_L) \simeq (A \otimes B^\circ)_L$, нам ввиду леммы V.5.1 достаточно доказать, что если $M_L$ и $N_L$ изоморфны как $A_L$-модули, то они изоморфны и как $B_L$-$A_L$-бимодули. Поэтому можно считать, что с самого начала $B = M_n(K)$. Тогда $A \otimes B^\circ \simeq M_n(A)$, и нам нужно проверить, что если два $M_n(A)$-модуля $M$ и $N$ изоморфны как $A$-модули, то они изоморфны и как $M_n(A)$-модули.

Обозначим $M_i = Me_{ii}$. Очевидно, $M_i$ есть $A$-подмодуль в $M$, причем $M = \bigoplus_{i=1}^{n} M_i$. Кроме того, $M_i e_{ij} \subset M_j$ и умножения на $e_{ij}$ и $e_{ji}$ — это взаимно обратные $A$-гомоморфизмы. Следовательно, $M_i \simeq M_j$ и $M \simeq nM_1$ как $A$-модуль. Ввиду теоремы Крулля — Шмидта, из изоморфизма $A$-модулей $M$ и $N$ следует изоморфизм $M_1$ и $N_1$. Пусть $\varphi$ — этот изоморфизм. Заметим, что всякий элемент $x \in M$ однозначно записывается в виде $x = x_1 + x_2 e_{12} + \ldots + x_n e_{1n}$, где $x_i \in M_1$.

Определим отображение $\psi : M \to N$, полагая

$$\psi(x) = \varphi(x_1) + \varphi(x_2) e_{12} + \ldots + \varphi(x_n) e_{1n}.$$

Легко проверить, что $\psi$ — гомоморфизм $M_n(A)$-модулей, причем, поскольку $\varphi$ взаимно однозначен, $\psi$ также взаимно однозначен что и требовалось доказать.

Вернемся к доказательству сопряженности в теореме Веддербёрна—Мальцева. Пусть $\varepsilon$ и $\eta$ — два подъема $\bar{A}$ в $A$. Нам нужно найти такой элемент $a = 1 + r$, $r \in R$, что $a\varepsilon(x)a^{-1} = \eta(x)$ для всех $x \in \bar{A}$, или $r\varepsilon(x) = \eta(x)r$. Вновь выбирая базисы в $\bar{A}$ и $A_n$ и записывая $r$ с «неопределенными коэффициентами» $r = \sum_{i=m+1}^{n} x_i a_i$, мы превратим это равенство в систему линейных уравнений относительно $x_i$. Ввиду леммы 2.2 достаточно показать существование решения этой системы, т. е. унитарную сопряженность $\varepsilon$ и $\eta$, в каком-нибудь расширении $L$ поля $K$. Конечно, за $L$ следует принять поле расщепления, что сводит задачу к случаю расщепимых алгебр.

Итак, мы можем считать, что $\bar{A} = M_{n_1}(K) \times \ldots \times M_{n_s}(K)$.

Обозначим через $\bar{e}_{ij}^k$ матричные единицы $k$-й компоненты алгебры $\bar{A}$, $k = 1, \ldots, s$; $i, j = 1, \ldots, n_k$, и положим $e_{ij}^k = \varepsilon(\bar{e}_{ij}^k)$, $f_{ij}^k = \eta(\bar{e}_{ij}^k)$. Тогда $1 = \sum_{k=1}^{s}\sum_{i=1}^{n_k} e_{ii}^k = \sum_{k=1}^{s}\sum_{i=1}^{n_k} f_{ii}^k$ — два разложения единицы алгебры $A$, причем $e_{ii}^k A \simeq f_{ii}^k A$. По теореме III.5.1 в алгебре $A$ найдется такой обратимый элемент $a$, что $f_{ii}^k = ae_{ii}^k a^{-1}$ для всех $k = 1, \ldots, s$; $i = 1, \ldots, n_k$.

Переходя в $\bar{A}$ с помощью проекции $\pi$, мы получаем $\bar{e}_{ii}^k = \bar{a}\bar{e}_{ii}^k\bar{a}^{-1}$, где $\bar{a} = \pi(a)$, откуда легко следует, что $\bar{a} = \sum_{i,k} \alpha_{ik}\bar{e}_{ii}^k$, причем $\alpha_{ik} \neq 0$ для всех $i$, $k$. Положим $b = \sum_{i,k} \alpha_{ik}e_{ii}^k$. Тогда $b$ — обратимый элемент, перестановочный со всеми $e_{ii}^k$, откуда следует, что $ab^{-1}$ — унипотентный элемент, причем $f_{ii}^k = (ab^{-1})e_{ii}^k(ab^{-1})^{-1}$. Поэтому в дальнейшем можно считать, что $e_{ii}^k = f_{ii}^k$ для всех $i$, $k$.

Обозначим $e^k = \sum_{i=1}^{n_k} e_{ii}^k$. Тогда $\bar{e}^k = \sum_{i=1}^{n_k} \bar{e}_{ii}^k$ — центральные идемпотенты факторалгебры $\bar{A}$. Учитывая, что $e_{ij}^k = e_{ii}^k e_{ij}^k e_{jj}^k$ и $f_{ij}^k = e_{ii}^k f_{ij}^k e_{jj}^k$, т. е. $e_{ij}^k$ и $f_{ij}^k$ лежат в $A_k = e^k A e^k$, мы видим, что, ограничивая $\varepsilon$ и $\eta$ на $\bar{A}_k = \bar{e}^k\bar{A}\bar{e}^k$, мы получаем гомоморфизмы $\varepsilon_k : \bar{A}_k \to A_k$; $\eta_k : \bar{A}_k \to A_k$.

Поскольку $\bar{A}_k$ — центральная простая алгебра, из теоремы 2.3 следует, что найдутся такие обратимые элементы $a_k \in A_k$, что $\eta_k(x) = a_k\varepsilon_k(x)a_k^{-1}$ для всех $k$. Вновь применяя отображение $\pi$, мы видим, что $y = \bar{a}_k y\bar{a}_k^{-1}$ для любого $y \in \bar{A}_k$, где $\bar{a}_k = \pi(a_k)$, откуда

следует, что $\bar{a}_k = \alpha_k e_k$ для некоторого $\alpha_k \in K$. Заменяя $a_k$ на $\alpha_k^{-1} a_k$, мы можем считать, что $a_k = r_k + e_k$, где $r_k \in R$. Но тогда, полагая $a = \sum_{k=1}^{s} a_k$, мы получаем, что $\eta(x) = a\varepsilon(x)a^{-1}$, причем $a = 1 + r$, где $r \in R$, что и требовалось доказать.

**§ 3. След, норма, дискриминант**

Пусть $T$ — представление некоторой алгебры $A$. Рассмотрим характеристический многочлен $\det(xE - T(a))$ матрицы $T(a)$. Поскольку характеристические многочлены подобных матриц совпадают, он не меняется при замене представления $T$ подобным, т. е. фактически определяется соответствующим $A$-модулем $M$. Этот многочлен называется характеристическим многочленом элемента $a$ относительно модуля $M$ (или представления $T$) и обозначается $X_{M,a}(x)$.

Аналогично, следом и нормой элемента $a$ относительно модуля $M$ называются, соответственно, след и определитель матрицы $T(a)$. След и норма обозначаются, соответственно, $\mathrm{Tr}_M(a)$ и $N_M(a)$.

Из определения непосредственно вытекает, что след — это линейное отображение $A \to K$, т. е.

$$\mathrm{Tr}_M(a+b) = \mathrm{Tr}_M(a) + \mathrm{Tr}_M(b);\ \mathrm{Tr}_M(\alpha a) = \alpha\,\mathrm{Tr}_M(a), \qquad \alpha \in K.$$

Кроме того, $\mathrm{Tr}_M(ab) = \mathrm{Tr}_M(ba)$, $N_M(ab) = N_M(a)N_M(b)$, и для любого $\alpha \in K$

$$X_{M,\alpha}(x) = (x-\alpha)^d;\ \mathrm{Tr}_M(\alpha) = d\alpha;\ N_M(\alpha) = \alpha^d,$$

где $d = [M : K]$.

Следующее простое предложение сводит вычисление характеристических многочленов, следов и норм к случаю простых модулей.

**Предложение 3.1.** *Пусть $M = M_0 \supset M_1 \supset \ldots \supset M_s = 0$ — композиционный ряд модуля $M$, $U_i = M_i/M_{i-1}$ — его простые факторы. Тогда для любого элемента $a \in A$*

$$X_{M,a}(x) = \prod_{i=1}^{s} X_{U_i,a}(x);\quad N_M(a) = \prod_{i=1}^{s} N_{U_i}(a);\quad \mathrm{Tr}_M(a) = \sum_{i=1}^{s} \mathrm{Tr}_{U_i}(a).$$

Доказательство немедленно следует из того, что представление $T$, соответствующее модулю $M$, приводится к виду

$$T(a) = \begin{pmatrix} T_1(a) & & 0 \\ & T_2(a) & \\ * & & \ddots \\ & & T_s(a) \end{pmatrix},$$

где $T_i$ — представление, соответствующее модулю $U_i$.

**Следствие 3.2.** *Если элемент $a$ лежит в* $\operatorname{rad} A$, *то* $X_{M,a}(x) = x^d$, $N_M(a) = \operatorname{Tr}_M(a) = 0$, *где* $d = [M : K]$.

Действительно, если $U$ — простой модуль, то $ua = 0$ для всех $u \in U$, т. е. в соответствующем представлении $a$ переходит в нулевую матрицу.

**Предложение 3.3.** *Для любого расширения $L$ поля $K$*

$$X_{M_L, a\otimes 1}(x) = X_{M,a}(x),\quad N_{M_L}(a\otimes 1) = N_M(a),\quad \operatorname{Tr}_{M_L}(a\otimes 1) = \operatorname{Tr}_M(a).$$

Доказательство следует из того, что если $\{m_1, \ldots, m_d\}$ — базис $M$ над $K$, то $\{m_1 \otimes 1, \ldots, m_d \otimes 1\}$ — базис $M_L$ над $L$ и в этих базисах элементам $a$ и $a \otimes 1$ соответствует одна и та же матрица.

Как мы увидим в дальнейшем, иногда наряду с представлениями алгебры $A$ над основным полем $K$ удобно рассматривать ее представления над некоторым расширением $L$ поля $K$, или, что то же, представления $L$-алгебры $A_L$, т. е. $A_L$-модули. В дальнейшем мы будем отождествлять элемент $a \in A$ с элементом $a \otimes 1 \in A_L$ и писать $X_{M,a}(x)$, $\operatorname{Tr}_M(a)$, $N_M(a)$ вместо $X_{M,a\otimes 1}(x)$, $\operatorname{Tr}_M(a \otimes 1)$, $N_M(a \otimes 1)$, где $M$ — некоторый $A_L$-модуль.

Вообще говоря, коэффициенты $X_{M,a}(x)$, в частности, $\operatorname{Tr}_M(a)$, $N_M(a)$ — это элементы поля $L$. Если они лежат в $K$ для любого элемента $a \in A$, назовем $A_L$-модуль $M$ правильным (этот термин будет использован только в данном параграфе).

Формой следа на алгебре $A$, соответствующей $A$-модулю $M$, называется функция $B_M(a, b) = \operatorname{Tr}_M(ab)$, где $a, b \in A$. В силу свойств следа, $B_M$ — симметрическая билинейная форма на пространстве $A$. Дискриминант формы $B_M$, т. е. элемент

$$\Delta_M = \begin{vmatrix} \operatorname{Tr}_M(a_1a_1) & \operatorname{Tr}_M(a_1a_2) \ldots \operatorname{Tr}_M(a_1a_n) \\ \operatorname{Tr}_M(a_2a_1) & \operatorname{Tr}_M(a_2a_2) \ldots \operatorname{Tr}_M(a_2a_n) \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \operatorname{Tr}_M(a_na_1) & \operatorname{Tr}_M(a_na_2) \ldots \operatorname{Tr}_M(a_na_n) \end{vmatrix},$$

где $\{a_1, \ldots, a_n\}$ — базис $A$, называется дискриминантом модуля $M$. Очевидно, $\Delta_M$ определен с точностью до квадрата ненулевого элемента поля $K$. Если форма $B_M$ невырождена, т. е. $\Delta_M \neq 0$, назовем модуль $M$ невырожденным.

С этими определениями связан следующий критерий сепарабельности.

**Теорема 3.4.** *Алгебра $A$ сепарабельна тогда и только тогда, когда для некоторого расширения $L$ поля $K$ существует невырожденный $A_L$-модуль $M$. Более того, поле $L$ всегда можно выбрать сепарабельным, а модуль $M$ — правильным.*

Доказательство. Если $a \in \operatorname{rad} A_L$, то по следствию 3.2 $B_M(a, b) = \operatorname{Tr}_M(ab) = 0$ для любого $b \in A_L$ и форма $B_M$ вырождена. Поэтому если $M$ — невырожденный $A_L$-модуль, то алгебра $A_L$ полупроста. Но из предложения 3.3 следует, что для любого расширения $F$ поля $L$ дискриминант $A_F$-модуля $M_F$ равен $\Delta_M$. Значит, $M_F$ — невырожденный $A_F$-модуль и алгебра $A_F$ полупроста. Поэтому $A_L$, а тогда по следствию 1.7 и алгебра $A$ сепарабельны.

Наоборот, пусть алгебра $A$ сепарабельна, $L$ — ее поле расщепления. Тогда $A_L \simeq A_1 \times \ldots \times A_s$, где $A_k = M_{n_k}(L)$. Пусть $U_k$ — простой $A_k$-модуль. Тогда для любой матрицы $a_k \in A_k$ многочлен $X_{U_k, a_k}(x)$ — это просто характеристический многочлен матрицы $a_k$. Обозначим $M = U_1 \oplus \ldots \oplus U_s$. Тогда по предложению 3.3 для любого элемента $b = (a_1, \ldots, a_s)$ из $A_1 \times \ldots \times A_s$ многочлен $X_{M,b}(x)$ — это произведение характеристических многочленов матриц $a_k$. В частности, $\operatorname{Tr}_M(b) = \sum_{k=1}^{s} \operatorname{tr} a_k$, $N_M(b) = \prod_{k=1}^{s} \det a_k$. Базис алгебры $A_L$ состоит из матричных единиц $e_{ij}^k$ ($k$ указывает номер компоненты, $k = 1, \ldots, s$; $i, j = 1, \ldots, n_k$), причем, очевидно, $\operatorname{Tr}_M(e_{ii}^k) = 1$, а $\operatorname{Tr}_M(e_{ij}^k) = 0$ при $i \neq j$. Отсюда получаем

$$\operatorname{Tr}_M(e_{ij}^k e_{rt}^l) = \begin{cases} 1, & \text{если } k = l,\ i = t,\ j = r, \\ 0 & \text{— в противном случае.} \end{cases}$$

Поэтому в определителе $\Delta_M$ в каждой строке и каждом столбце стоит ровно одна 1, а остальные элементы равны 0, откуда $\Delta_M = \pm 1 \neq 0$, т. е. модуль $M$ невырожден.

Поле $L$ можно выбрать сепарабельным по следствию 1.3. Докажем, что модуль $M$ правильный, т. е. при $a \in A$ коэффициенты многочлена $X_{M,a}(x)$ лежат в поле $K$. Заметим вначале, что $X_{M,a}(x)$ не зависит от выбора поля расщепления $L$: для любого поля, содержащего $L$, это вытекает из предложения 3.3, а если $F$ — какое-нибудь поле расщепления, то всегда можно построить поле, содержащее как $F$, так и $L$. Поэтому ввиду следствия V 4.5 поле $L$ можно считать нормальным. Обозначим $G = G(L/K)$.

Группа $G$ действует на алгебре $A_L$ по правилу $\sigma(a \otimes \lambda) = a \otimes \sigma(\lambda)$, где $a \in A$, $\lambda \in L$. Покажем, что для любого элемента $b \in A_L$ имеет место равенство $X_{M,\sigma(b)}(x) = \sigma(X_{M,b}(x))$, где $\sigma(f(x))$ обозначает многочлен, полученный применением $\sigma$ ко всем коэффициентам многочлена $f(x)$. Если эта формула будет установлена, то для любого $a \in A$ получим $\sigma(X_{M,a}(x)) = X_{M,\sigma(a)}(x) = X_{M,a}(x)$, и по теореме V 4.4 все коэффициенты $X_{M,a}(x)$ лежат в поле $K$, т. е. $M$ — правильный модуль.

Заметим прежде всего, что если $b=(a_1, \ldots, a_s) \in A_L$, то $X_{M,b}(x)= = X_{M,b'}(x)$, где $b'=(a_{t_1}, \ldots, a_{t_s})$ для любой перестановки $(t_1, t_2, \ldots \ldots, t_s)$ номеров $1, 2, \ldots, s$. Поскольку $A_L \simeq \sigma(A_1) \times \ldots \times \sigma(A_s)$, из теоремы II.5.2 следует, что $\sigma(A_k)=A_{t_k}$ для некоторой перестановки индексов $(t_1, \ldots, t_s)$. В частности, тогда $n_k = n_{t_k}$. Обозначим через $\sigma_k$ ограничение $\sigma$ на $A_k$ и рассмотрим изоморфизм $\bar{\sigma}_k : A_k \to A_{t_k}$, переводящий матрицу $(\lambda_{ij})$ в матрицу $(\sigma(\lambda_{ij}))$. Композиция $\bar{\sigma}_k^{-1}\sigma_k$ — это автоморфизм алгебры $A_k$, тождественный на ее центре $L$. По теореме Сколема — Нётер (точнее, по следствию IV.4.3) этот автоморфизм внутренний, т. е. $\bar{\sigma}_k^{-1}\sigma_k(a)=u_k a u_k^{-1}$ для некоторого $u_k \in \in A_k$, откуда $\sigma_k(a)=v_k\bar{\sigma}_k(a)v_k^{-1}$, где $v_k=\bar{\sigma}_k(u_k)$ и $\sigma$ имеет вид, с точностью до перестановки компонент,

$$(a_1, \ldots, a_s) \to (v_1\bar{\sigma}_1(a_1)v_1^{-1}, \ldots, v_s\bar{\sigma}_s(a_s)v_s^{-1}).$$

Но, очевидно, характеристический многочлен матрицы $\bar{\sigma}_k(a_k)$, а потому и матрицы $v_k\bar{\sigma}_k(a_k)v_k^{-1}$ получается применением $\sigma$ ко всем коэффициентам характеристического многочлена матрицы $a_k$, откуда и следует требуемая формула $X_{M,\sigma(b)}(x) = \sigma(X_{M,b}(x))$. Теорема полностью доказана.

Отметим, что использование расширений основного поля в теореме 3.5. существенно: в упражнении 9 дан такой пример сепарабельной алгебры $A$, что всякий $A$-модуль вырожден. Невырожденный $A$-модуль всегда существует, если характеристика поля $K$ равна 0 (см. упражнение 6) или если алгебра $A$ коммутативна (см. ниже пример 1).

Многочлен $X_{M,a}(x)$, где $M$ — модуль, построенный выше, называется главным многочленом элемента $a \in A$ и обозначается $P_a(x)$. Норма и след $\mathrm{Tr}_M(a)$ и $N_M(a)$ называются, соответственно, главным следом и главной нормой элемента $a$ и обозначаются $\mathrm{Tr}(a)$, $N(a)$. Если нужно явно указать, о какой алгебре идет речь, пишут $P_{A/K,a}(x)$, $\mathrm{Tr}_{A/K}(a)$ и $N_{A/K}(a)$. Билинейная форма $B(a, b) = \mathrm{Tr}(ab)$ называется формой главного следа, а ее дискриминант $\Delta(A/K)$ — дискриминантом сепарабельной алгебры $A$ (напомним, что он определен с точностью до множителя, являющегося квадратом ненулевого элемента из $K$). В процессе доказательства теоремы 2.4 мы установили следующий факт.

**Теорема 3.5.** *Коэффициенты главного многочлена, в частности главный след и главная норма, лежат в поле $K$. Форма главного следа сепарабельной алгебры всегда невырождена, т. е. $\Delta(A/K) \neq 0$.*

Кроме того, поскольку модуль $M$ точный, а всякая матрица является корнем своего характеристического многочлена, имеет место такое предложение.

**Предложение 3.6.** *Всякий элемент сепарабельной алгебры является корнем своего главного многочлена.*

Отметим еще, что из построения модуля $M$ и формулы $(A \otimes F) \otimes_F L \simeq A \otimes L$, где $L \supset F$, непосредственно вытекает и такое предложение.

**Предложение 3.7.** *Для любого элемента $a \in A$ и любого расширения $F$ поля $K$*

$$P_{A_F/F,a}(x) = P_{A/K,a}(x),\ \mathrm{Tr}_{A_F/F}(a) = \mathrm{Tr}_{A/K}(a),\ N_{A_F/F}(a) = N_{A/K}(a).$$

Ниже приведены примеры вычисления главного многочлена.

**Примеры. 1.** Пусть $F$ — сепарабельное расширение поля $K$. Тогда для всякого поля расщепления $L$ $F \otimes L \simeq L^n$, где $n = [F : K]$, и главный многочлен совпадает с характеристическим многочленом регулярного модуля. Очевидно, то же имеет место и для любой коммутативной сепарабельной алгебры $A$.

**2.** Пусть теперь $A$ — центральная простая алгебра размерности $d^2$, $L$ — его максимальное подполе. Тогда $A \otimes L \simeq M_d(L)$ и $P_a(x)$ — это характеристический многочлен матрицы, соответствующей элементу $a \otimes 1$. Если $\mathrm{X}_a(x)$ обозначает характеристический многочлен регулярного модуля, то, поскольку регулярный $A_L$-модуль — прямая сумма $d$ простых модулей, $\mathrm{X}_a(x) = (P_a(x))^d$. В частности, $\mathrm{N}_A(a) = (\mathrm{N}(a))^d$, $\mathrm{Tr}_A(a) = d\mathrm{Tr}(a)$.

## *Упражнения к главе VI*

**1.** Доказать, что для любых модулей $M$ и $N$ над алгеброй $A$ и любого расширения $L$ основного поля $\mathrm{Hom}_{A_L}(M_L, N_L) \simeq \mathrm{Hom}_A(M, N) \otimes L$. (Указания: можно воспользоваться теоремой о строении решений однородной системы линейных уравнений.)

**2.** Назовем $A$-модуль $M$ сепарабельным, если $A_L$-модуль $M_L$ полупрост для любого $L$. Доказать, что $M$ сепарабелен тогда и только тогда, когда он полупрост, а алгебра $E_A(M)$ сепарабельна.

**3.** Найти необходимые и достаточные условия того, чтобы:

а) алгебра $A_L$ была простой для любого $L$;

б) $A_L$-модуль $M_L$ был простым для любого $L$ (такой модуль называют абсолютно простым, а соответствующее представление — абсолютно неприводимым).

**4.** Пусть $F$ — поле характеристики 2, $K = F(t)$ — поле рациональных функций над $F$, $A = K[x]/(x^4 - t^2)$. Найти $R = \mathrm{rad}\, A$ и $A/R$. Проверить, что в $A$ нет подалгебры, изоморфной $A/R$. Построить аналогичный пример для поля любой характеристики $p > 0$.

**5.** Пусть поля $F$ и $K$ определены так же, как и в предыдущем упражнении, $L = K[x]/(x^2 - t)$, $A$ — $L$-алгебра с базисом $\{1, r\}$, где $r^2 = 0$. Рассматривая $A$ как $K$-алгебру, установить, что $A/\mathrm{rad}\, A \simeq L$, и найти в $A$ две различные подалгебры, изоморфные $L$ (поскольку $A$ коммутативна, эти подалгебры не сопряжены в $A$). Построить аналогичный пример для поля любой характеристики $p > 0$.

**6.** Доказать, что алгебра $A$ над полем характеристики 0 полупроста тогда и только тогда, когда регулярный $A$-модуль невырожден.

**7.** Вывести из результата предыдущего упражнения, что существует многочлен $F(x_{ij}^k)$ с целыми коэффициентами от $n^3$ переменных $x_{ij}^k$, $i, j, k = 1, \ldots, n$,

такой, что алгебра $A$ над полем характеристики 0 со структурными константами $\gamma_{ij}^k$ полупроста тогда и только тогда, когда $F(\gamma_{ij}^k) \neq 0$.

8. Пусть $K$ — поле характеристики $p$, $A = M_p(K)$. Проверить, что регулярный $A$-модуль вырожден. Перенести этот результат на произвольную центральную простую $K$-алгебру размерности $p^2$.

9. Доказать, что если $D$ — центральное тело размерности $p^2$ над полем характеристики $p$, то всякий $D$-модуль вырожден (пример такого тела см. в упражнении 27 к гл. V). Таким образом, в теореме 3. 4 действительно нужно рассматривать $A_L$-модули, а не только $A$-модули.

10. Пусть $A$ — алгебра над полем $K$ с базисом $\{a_1, ..., a_n\}$ и структурными константами $\gamma_{ij}^k$. Рассмотрим алгебру $\tilde{A}$ над полем $F = K(t_1, ..., t_n)$ рациональных функций $n$ переменных с тем же базисом и теми же структурными константами[11]. Обозначим $\tilde{a} = \sum_{i=1}^{n} t_i a_i$, $P(x, t_1, ..., t_n) = m_{\tilde{a}}(x)$—минимальный многочлен элемента $\tilde{a}$ (очевидно, это есть многочлен от $(n+1)$-й переменной $x, t_1, ..., t_n$).

Если $a = \sum_{i=1}^{n} \alpha_i a_i$—произвольный элемент алгебры $A$, то многочлен $P_{A,a}(x) = P(x, \alpha_1, ..., \alpha_n)$ называется главным многочленом элемента $a$.

а) Доказать, что $P_{A,a}(x)$ не зависит от выбора базиса в алгебре $A$.

б) Проверить, что $P_{A_L, a\otimes 1}(x) = P_{A,a}(x)$ для любого расширения $L$ поля $K$.

в) Установить, что если $A$ — сепарабельная алгебра, то это определение главного многочлена совпадает с данными в § 3.

11. Мы сохраняем определения и обозначения предыдущего упражнения. Если $P_{A,a}(x) = x^m + \beta_1 x^{m-1} + ... + \beta_m$, $\beta_i \in K$, положим $\mathrm{Tr}_{A/K}(a) = -\beta_1$ $\mathrm{N}_{A/K}(a) = (-1)^m \beta_m$ и будем их называть соответственно главным следом и главной нормой.

а) Проверить, что главный след — линейная форма на пространстве $A$, причем $\mathrm{Tr}_{A/K}(ab) = \mathrm{Tr}_{A/K}(ba)$, а $\mathrm{N}_{A/K}(ab) = \mathrm{N}_{A/K}(a)\,\mathrm{N}_{A/K}(b)$.

б) Доказать, что алгебра $A$ сепарабельна тогда и только тогда, когда билинейная форма $\mathrm{Tr}_{A/K}(ab)$ на пространстве $A$ невырождена.

12. Пусть $L$ — конечное расширение поля $K$. Доказать, что если $a$ — элемент $L$-алгебры $A$, то

$$P_{A/K,a}(x) = \mathrm{N}_{L(x)/K(x)}(P_{A/L,a}(x)), \quad \mathrm{Tr}_{A/K}(a) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{A/L}(a)),$$

$$\mathrm{N}_{A/K}(a) = \mathrm{N}_{L/K}(\mathrm{N}_{A/L}(a)).$$

13. Доказать, что если у идеала $I$ алгебры $A$ есть базис, состоящий из нильпотентных элементов, то $I \subset \mathrm{rad}\, A$. (Указание: воспользоваться тем, что след нильпотентной матрицы равен 0.)

---

[11] Если определить тензорное произведение бесконечномерных алгебр, то легко видеть, что $\tilde{A} = A \otimes F$.

# VII

ГЛАВА

# ПРЕДСТАВЛЕНИЯ КОНЕЧНЫХ ГРУПП

В этой главе мы воспользуемся общей теорией полупростых алгебр и их представлений для получения основных результатов классической теории представлений конечных групп.

## § 1. Теорема Машке

Представлением группы $G$ над полем $K$ называется гомоморфизм этой группы в группу $GL(V)$ обратимых линейных операторов в векторном пространстве $V$ над полем $K$. Иными словами, задать представление $T$ — это значит сопоставить каждому элементу $g \in G$ обратимый линейный оператор $T(g) \in GL(V)$ так, что $T(gh) = T(g)\,T(h)$ для всех $g, h \in G$. Для представлений групп, как и для представлений алгебр, определяются понятия подобия, приводимости, разложимости и т. п. Однако оказывается, что изучать представления группы $G$ — это то же самое, что изучать представления ее групповой алгебры (см. гл. I, § 1, пример 6).

Напомним, что базис групповой алгебры $KG$ составляют элементы группы $G$, которые перемножаются, как в группе. Если $T : KG \to E(V)$ — представление групповой алгебры, а $g \in G$, то $T(g)\,T(g^{-1}) = T(gg^{-1}) = T(1) = 1$. Поэтому $T(g)$ — обратимый оператор, так что, ограничивая $T$ на $G$, получаем представление группы $G$. Наоборот, пусть $T : G \to GL(V)$ — представление группы $G$. Распространим его на алгебру $KG$ «по линейности», полагая $T\left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} \alpha_g T(g)\Big)$. Очевидно, получится представление $T : KG \to E(V)$, ограничение которого на $G$ совпадает с исходным представлением. Итак, представления группы и групповой алгебры — это, по сути, одно и то же.

В этой главе все рассматриваемые группы предполагаются конечными. Решающую роль в теории представлений конечных групп играет следующий замечательный результат, известный как «теорема Машке».

**Теорема 1.1.** *Если характеристика поля $K$ не делит порядок группы $G$, то групповая алгебра $KG$ сепарабельна.*

Доказательство. В силу теоремы VI.3.4 достаточно указать какой-нибудь невырожденный $KG$-модуль. Оказывается, в нашем случае уже регулярный $KG$-модуль невырожден. Действительно, возьмем в качестве базиса алгебры $KG$ множество $\{g_1, \ldots, g_n\}$ всех элементов группы $G$ (здесь $n$ — порядок $G$). Если $g \neq 1$, то $g_i g \neq g_i$ для всех $i = 1, \ldots, n$, следовательно, $\mathrm{Tr}(g) = 0$ ($\mathrm{Tr}$ здесь означает след регулярного представления). С другой стороны, $\mathrm{Tr}(1) = [KG : K] = n$. Поэтому $\mathrm{Tr}(g_i g_j) = 0$, если $g_j \neq g_i^{-1}$ и $\mathrm{Tr}(g_i g_j) = n$ при $g_i = g_j^{-1}$. Таким образом, в каждой строке и каждом столбце дискриминанта $\Delta$ регулярного представления стоит

ровно один ненулевой элемент (заметим, что $n = n1 \neq 0$, так как характеристика $K$ не делит $n$). Следовательно, $\Delta \neq 0$ (точнее, $\Delta = \pm n^n$) и алгебра $KG$ сепарабельна.

**Следствие 1.2.** *Если характеристика поля $K$ не делит порядок группы $G$, то всякое представление группы $G$ над полем $K$ вполне приводимо.*

Оказывается, имеет место и теорема, обратная к теореме Машке.

**Теорема 1.3.** *Если характеристика поля $K$ делит порядок группы $G$, то алгебра $KG$ не полупроста.*

Доказательство. Рассмотрим в алгебре $KG$ элемент $s = \sum_{x \in G} x$. Очевидно, для любого $g \in G$ имеет место равенство $gs = sg = s$. Поэтому $s$ лежит в центре алгебры $KG$. С другой стороны, $s^2 = \sum_{x \in G} xs = ns = 0$ (так как порядок $n$ группы $G$ делится на характеристику поля $K$). По следствию II.2.8 алгебра $KG$ не полупроста.

Таким образом, теория представлений групп фактически распадается на две существенно различные теории: классическую (когда порядок группы не делится на характеристику поля) и модулярную (когда порядок группы делится на характеристику поля). В этой главе (кроме некоторых упражнений) мы будем рассматривать только классическую теорию представлений. Поэтому всюду в дальнейшем мы будем предполагать, что порядок $n$ группы $G$ не делится на характеристику поля $K$.

## § 2. Число и размерности неприводимых представлений

Из теоремы Машке и теории полупростых алгебр и их представлений сравнительно просто вытекают следующие важные результаты о числе и размерностях неприводимых представлений.

**Теорема 2.1.** *Если $d_1, \ldots, d_s$ — размерности всех (попарно неизоморфных) представлений группы $G$ над алгебраически замкнутым полем $K$, то $d_1^2 + \ldots + d_s^2 = n$, где $n = (G : 1)$.*

Доказательство. По теореме Веддербёрна — Артина (точнее, по следствию II.4.4) и по теореме II.6.2, если $d_1, \ldots, d_s$ — размерности всех неприводимых представлений алгебры $KG$, то $KG \simeq \simeq \prod_{i=1}^{s} \cdot M_{d_i}(K)$, откуда $n = [KG : K] = \sum_{i=1}^{s} d_i^2$.

Пусть по-прежнему поле $K$ алгебраически замкнуто. Тогда центр алгебры $KG$ по следствию II.4.2 изоморфен $K^s$, где $s$ — число простых компонент $KG$, или, что то же, число неизоморфных неприводимых представлений. Поэтому число неприводимых представлений равно размерности центра алгебры $KG$. Но элемент $a = \sum_{x \in G} \alpha_x x$ лежит в центре $KG$ тогда и только тогда, когда $ga = ag$ для любого $g \in G$, или, что то же, $gag^{-1} = a$. Поскольку $gag^{-1} = \sum_{x \in G} \alpha_x (gxg^{-1})$,

это означает, что коэффициенты при $x$ и $gxg^{-1}$ элемента $a$ одинаковы.

Напомним, что элементы $x$ и $gxg^{-1}$ называются сопряженными в группе $G$. Вся группа $G$ распадается на попарно непересекающиеся классы сопряженных элементов $C_1, C_2, \ldots, C_s$. Из приведенных выше рассуждений следует, что базис центра групповой алгебры $KG$ образуют элементы $c_i = \sum_{x \in C_i} x$, $i = 1, \ldots, s$. Отсюда вытекает такая теорема.

**Теорема 2.2.** *Число неизоморфных неприводимых представлений конечной группы $G$ над алгебраически замкнутым полем $K$ равно числу классов сопряженных элементов в группе $G$.*

**Следствие 2.3.** *Группа $G$ абелева тогда и только тогда, когда все ее неприводимые представления над алгебраически замкнутым полем одномерны.*

Доказательства достаточно заметить, что группа абелева тогда и только тогда, когда каждый класс сопряженных элементов состоит из одного элемента, т. е. ввиду теоремы 2.2 число ее неприводимых представлений равно порядку группы. Учитывая соотношение между размерностями этих представлений и порядком $G$ (теорема 2.1), мы видим, что так будет в том и только том случае, когда все эти представления одномерны.

**Следствие 2.4.** *Если $G$ и $H$ — абелевы группы одинакового порядка, а поле $K$ алгебраически замкнуто, то групповые алгебры $KG$ и $KH$ изоморфны.*

## § 3. Характеры

Пусть $T$ — представление группы $G$ над полем $K$, $M$ — соответствующий $KG$-модуль. Для любого элемента $a \in KG$ определен тогда его след $\mathrm{Tr}_M(a)$ относительно модуля $M$ (§ 3 гл. VI) — это след матрицы $T(a)$ (в любом базисе). В частности, для любого элемента $x \in G$ определен элемент $\chi(x) = \mathrm{Tr}_M(x)$ поля $K$. Функцию $\chi : G \to K$ называют характером представления $T$. Если $T$ неприводимо, то $\chi$ называют неприводимым характером. Характер регулярного представления называется регулярным характером и обозначается $\chi_{\mathrm{reg}}$.

**Предложение 3.1.**

$$\chi_{\mathrm{reg}}(x) = \begin{cases} n & \text{при } x = 1, \\ 0 & \text{при } x \neq 1. \end{cases}$$

Доказательство очевидно.

**Предложение 3.2.** *Для любого характера $\chi(gxg^{-1}) = \chi(x)$. Иными словами, характер постоянен на каждом классе сопряженных элементов.*

Доказательство следует из того, что для любого представления $T$ $T(gxg^{-1}) = T(g)\,T(x)\,T(g)^{-1}$, т. е. матрицы $T(gxg^{-1})$ и $T(x)$ подобны и, в частности, имеют одинаковый след.

Заметим еще, что из следствия II.6.3. немедленно вытекает такая теорема.

**Теорема 3.3.** *Пусть $K$ — поле характеристики 0. Тогда представление однозначно определяется своим характером, т. е. из равенства характеров следует подобие представлений.*

Пусть теперь поле $K$ алгебраически замкнуто, $\chi_1, \ldots, \chi_s$ — все неприводимые характеры группы $G$ над полем $K$. Обозначим $\chi_{ij} = \chi_i(g_j)$, где $g_j \in C_j$ ($C_1, \ldots, C_s$ — классы сопряженных элементов группы $G$). Квадратная матрица $X = (\chi_{ij})$ называется таблицей характеров группы $G$ над полем $K$. Заметим, что если $M_i$ — модуль $i$-го неприводимого представления, то $KG \simeq \bigotimes_{i=1}^{s} d_i M_i$, где $d_i = [M_i : K]$, откуда $\chi_{\text{reg}} = \sum_{i=1}^{s} d_i \chi_i$.

Как мы уже заметили, элементы $c_i = \sum_{x \in C_i} x$, $i = 1, \ldots, s$, образуют базис центра $C$ групповой алгебры группы $G$. С другой стороны, $C \simeq K^s$, поэтому если $1 = e_1 + \ldots + e_s$ — разложение единицы алгебры $C$, то элементы $\{e_1, \ldots, e_s\}$ также образуют базис $C$. Следовательно, в поле $K$ найдутся такие элементы $\alpha_{ij}$ и $\beta_{ij}$, что $c_i = \sum_{j=1}^{s} \alpha_{ij} e_j$, $e_i = \sum_{j=1}^{s} \beta_{ij} c_j$, причем матрицы $A = (\alpha_{ij})$ и $B = (\beta_{ij})$ взаимно обратны. Оказывается, коэффициенты $\alpha_{ij}$ и $\beta_{ij}$ тесно связаны с таблицей характеров.

**Предложение 3.4.** *Обозначим через $d_i$ размерность неприводимого представления с характером $\chi_i$, $h_j$ — число элементов в классе $C_j$. Тогда*

$$\alpha_{ij} = \frac{h_i}{d_i} \chi_{ji}; \quad \beta_{ij} = \frac{d_i}{n} \chi_i(g_j^{-1}),$$

*где $g_j \in C_j$.*

Доказательство. Заметим, что в $j$-м неприводимом представлении элемент $e_j$ действует тождественным образом, а элементы $e_k$ ($k \neq j$) — нулевым. Поэтому $\chi_j(e_k) = 0$ при $k \neq j$, а $\chi_j(e_j) = d_j$. Отсюда

$$\chi_j(c_i) = \chi_j\Big(\sum_{k=1}^{s} \alpha_{ik} e_k\Big) = \sum_{k=1}^{s} \alpha_{ik} \chi_j(e_k) = d_j \alpha_{ij}.$$

С другой стороны, очевидно, $\chi_j(c_i) = h_i \chi_{ji}$, откуда и получаем выражение для $\alpha_{ij}$.

Для нахождения $\beta_{ij}$ воспользуемся тем, что $\chi_{\text{reg}} = \sum_{i=1}^{s} d_i \chi_i$. Заметим, что $\chi_{\text{reg}}(c_k g) = 0$, если $g^{-1} \notin C_k$, и $\chi_{\text{reg}}(c_k g) = n$, если $g^{-1} \in C_k$ (это следует из предложения 3.1). Поэтому если $g_j \in C_j$, то

$\chi_{reg}(e_i g_j^{-1}) = \chi_{reg}\left(\sum_{k=1}^{s} \beta_{ik} c_k g_j^{-1}\right) = n\beta_{ij}$. С другой стороны, $\chi_{reg}(e_i g_j^{-1}) =$

$= \sum_{k=1}^{s} d_k \chi_k (e_i g_j^{-1}) = d_i \chi_i (g_j^{-1})$, поскольку $\chi_k (e_i g) = 0$ при $k \neq i$, а $\chi_i (e_i g) = \chi_i (g)$. Отсюда получаем формулу для $\beta_{ij}$.

Учитывая, что матрицы $A$ и $B$ взаимно обратны, мы немедленно получаем следующие «соотношения ортогональности» для характеров.

**Теорема** 3.5.

$$\frac{1}{n} \sum_{k=1}^{s} h_k \chi_i (g_k) \chi_j (g_k^{-1}) = \begin{cases} 0 & \text{при } i \neq j, \\ 1 & \text{при } i = j; \end{cases}$$

$$\frac{1}{n} \sum_{k=1}^{s} \chi_k (g_i) \chi_k (g_j^{-1}) = \begin{cases} 0 & \text{при } i \neq j, \\ 1/h_i & \text{при } i = j. \end{cases}$$

**Следствие** 3.6. *Представление $T$ группы $G$ над алгебраически замкнутым полем характеристики 0 неприводимо тогда и только тогда, когда его характер $\chi$ удовлетворяет равенству*

$$\frac{1}{n} \sum_{k=1}^{s} h_k \chi (g_k) \chi (g_k^{-1}) = 1.$$

Доказательство. Разложим представление $T$ в прямую сумму неприводимых. Соответственно, характер $\chi$ представится в виде $\chi = \sum_{i=1}^{s} m_i \chi_i$, где $\chi_1, \ldots, \chi_s$ — неприводимые характеры. Но тогда

$$\frac{1}{n} \sum_{k=1}^{s} h_k \chi (g_k) \chi (g_k^{-1}) =$$

$$= \frac{1}{n} \sum_{i,j} m_i m_j \sum_{k=1}^{s} h_k \chi_i (g_k) \chi_j (g_k^{-1}) = \sum_{i-1}^{s} m_i^2,$$

и это выражение равно 1 тогда и только тогда, когда $\chi = \chi_i$ для некоторого $i$, т. е. ввиду теоремы 3.3 $T$ — неприводимое представление.

Если $K = C$ — поле комплексных чисел, то соотношениям ортогональности можно придать несколько иной вид. Для этого воспользуемся следующей леммой.

**Лемма 3.7.** *Если $\chi$ — характер представления $T$ размерности $d$ группы $G$ над полем комплексных чисел, то для любого элемента $g \in G$ $\chi(g)$ есть сумма $d$ корней степени $n$ из 1 и $\chi(g^{-1}) = \overline{\chi(g)}$, где, как обычно, $\bar{z}$ — число, комплексно-сопряженное к $z$.*

Доказательство. Как известно, $g^n = e$, откуда $T(g)^n = E$ для любого $g \in G$. Поскольку многочлен $x^n - 1$ не имеет кратных корней, отсюда следует, что матрица $T(g)$ подобна диагональной

$$T(g) \sim \begin{pmatrix} \varepsilon_1 & & 0 \\ & \varepsilon_2 & \\ & & \ddots \\ 0 & & \varepsilon_d \end{pmatrix},$$

где $\varepsilon_i^n = 1$. Отсюда $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_d$,

$$T(g^{-1}) \sim \begin{pmatrix} \varepsilon_1^{-1} & & 0 \\ & \varepsilon_2^{-1} & \\ & & \ddots \\ 0 & & \varepsilon_d^{-1} \end{pmatrix}.$$

Значит,

$$\chi(g^{-1}) = \varepsilon_1^{-1} + \ldots + \varepsilon_d^{-1} = \bar{\varepsilon}_1 + \ldots + \bar{\varepsilon}_d = \overline{\chi(g)}.$$

В частности, $\chi_i(g_j^{-1}) = \bar{\chi}_{ij}$, и соотношения ортогональности из теоремы 3.5. можно переписать в виде

$$\frac{1}{n} \sum_{k=1}^{s} h_k \chi_{ik} \bar{\chi}_{jk} = \begin{cases} 0 & \text{при } i \neq j, \\ 1 & \text{при } i = j; \end{cases}$$

$$\frac{1}{n} \sum_{k=1}^{s} \chi_{ki} \bar{\chi}_{kj} = \begin{cases} 0 & \text{при } i \neq j, \\ 1/h_i & \text{при } i = j. \end{cases}$$

## § 4. Теоремы целочисленности

В этом параграфе нам понадобятся некоторые свойства целых алгебраических чисел. Напомним, что комплексное число $z$ называется целым алгебраическим, если оно является корнем уравнения $x^m + a_1 x^{m-1} + \ldots + a_m = 0$ с целыми коэффициентами $a_i$.

**Предложение 4.1.** *Если рациональное число является целым алгебраическим, то оно целое.*

Доказательство. Пусть $z = p/q$, где $p$ и $q$ — взаимно простые целые числа, является корнем уравнения $x^m + a_1 x^{m-1} + \ldots + a_m = 0$, где все $a_i$ — целые. Приводя к общему знаменателю, получаем $p^m = -a_1 q p^{m-1} - \ldots - a_m q^m$, что невозможно, так как $p$ и $q$ взаимно просты.

Следующая лемма дает удобный критерий того, что некоторое число $z$ является целым алгебраическим.

**Лемма 4.2.** *Для того чтобы число $z$ было целым алгебраическим, необходимо и достаточно, чтобы нашлись такие комплексные числа $y_1, \ldots, y_t$, не все равные нулю, что $zy_i = \sum_{j=1}^{t} a_{ij}y_j$, где все $a_{ij}$ — целые числа.*

Доказательство. Если $z$ — корень целочисленного уравнения $x^m + a_1x^{m-1} + \ldots + a_m = 0$, то, очевидно, достаточно положить $y_1 = 1$, $y_2 = z, \ldots, y_m = z^{m-1}$.

Наоборот, пусть существуют $y_1, \ldots, y_t$ с указанным свойством. Обозначим через $A$ матрицу $(a_{ij})$, а через $Y$ — вектор-столбец с координатами $y_1, \ldots, y_t$. Тогда $(zE - A)Y = 0$, откуда следует, что $\det(zE - A) = 0$. Но $\det(zE - A) = z^t + a_1z^{t-1} + \ldots + a_t$, где $a_i$ — целочисленные линейные комбинации произведений элементов матрицы $A$, т. е. целые числа. Следовательно, $z$ — целое алгебраическое число.

**Следствие 4.3.** *Сумма и произведение целых алгебраических чисел суть целые алгебраические числа. Иными словами, целые алгебраические числа образуют кольцо.*

Доказательство. Пусть $y_1, \ldots, y_t$ — такие числа, что $zy_i = \sum_j a_{ij}y_j$ ($a_{ij}$—целые), а $y'_1, \ldots, y'_r$—такие числа, что $z'y' = \sum_j a'_{ij}y'_j$ ($a'_{ij}$ — целые). Тогда, как легко видеть, набор чисел $\{y_iy'_j\}$, $i = 1, \ldots, t$; $j = 1, \ldots, r$, будет обладать тем же свойством относительно чисел $z + z'$ и $zz'$, что и требовалось доказать.

Поскольку корни из единицы, конечно, суть целые алгебраические числа, из леммы 3.7 мы получаем такое следствие.

**Следствие 4.4.** *Если $\chi$ — характер группы $G$ над полем комплексных чисел, то $\chi(x)$ — целое алгебраическое число для любого $x \in G$.*

Воспользуемся теперь обозначениями предыдущего параграфа. В частности, пусть $X = (\chi_{ij})$ — таблица характеров группы $G$ над полем комплексных чисел.

**Теорема 4.5.** *Все числа $\alpha_{ij} = (h_i/d_j)\,\chi_{ji}$ — целые алгебраические.*

Доказательство. Заметим, что $c_ic_j$ для любых $i$ и $j$ — элемент центра алгебры $\mathbf{C}G$. С другой стороны, $c_ic_j$— целочисленная линейная комбинация элементов группы $G$. Отсюда следует, что $c_ic_j = \sum_k \gamma_{ijk}c_k$, где все $\gamma_{ijk}$— целые числа. В то же время

$$c_ic_j = \Big(\sum_p \alpha_{ip}e_p\Big)\Big(\sum_q \alpha_{jq}e_q\Big) = \sum_p \alpha_{ip}\alpha_{jp}e_p,$$

а $c_k = \sum_p \alpha_{kp}e_p$, откуда $c_ic_j = \sum_{p,k} \gamma_{ijk}\alpha_{kp}e_p$ и $\alpha_{ij}\alpha_{jp} = \sum_k \gamma_{ijk}\alpha_{kp}$. Полагая $z = \alpha_{ip}$, $y_j = \alpha_{jp}$ ($p$ — фиксированное), мы можем воспользо-

ваться леммой 4.2, из которой следует, что $\alpha_{ip}$ — целое алгебраическое число.

**Следствие 4.6.** *Размерности $d_i$ неприводимых комплексных представлений делят порядок группы.*

Для доказательства перепишем первое из соотношений ортогональности (теорема 3.5)

$$\sum_{k=1}^{s} \frac{h_k \chi_{ik}}{d_i} \chi_i (g_k^{-1}) = \frac{n}{d_i} .$$

Поскольку $(h_k\chi_{ik})/d_i = \alpha_{ki}$ и $\chi_i (g_k^{-1})$ — целые алгебраические числа, число $n/d_i$ — также целое алгебраическое. А поскольку оно рациональное, то является целым, что и требовалось доказать.

## § 5. Тензорное произведение представлений

Для представлений групп, наряду с обычными теоретико-модульными конструкциями можно определить еще одну операцию — тензорное (или кронекеровское) произведение.

Пусть $M$ и $N$ — два модуля над групповой алгеброй $KG$. Тогда их тензорное произведение (как векторных пространств) можно превратить в $KG$-модуль, полагая для любого элемента $g \in G$ $(m \otimes n)\, g = mg \otimes ng$. Так построенный модуль и называется тензорным произведением $KG$-модулей $M$ и $N$, а соответствующее представление группы $G$ — тензорным произведением представлений, соответствующих модулям $M$ и $N$.

Вычислим характер тензорного произведения представлений. Пусть представление $T$, соответствующее модулю $M$, в некотором базисе $\{u_1, \ldots, u_m\}$ имеет вид

$$T(g) = \begin{pmatrix} \varphi_{11}(g) \ldots \varphi_{1n}(g) \\ \cdots\cdots\cdots \\ \varphi_{m1}(g) \ldots \varphi_{mm}(g) \end{pmatrix},$$

а представление $S$, соответствующее модулю $N$, в некотором базисе $\{v_1, \ldots, v_n\}$ имеет вид

$$S(g) = \begin{pmatrix} \psi_{11}(g) \ldots \psi_{1m}(g) \\ \cdots\cdots\cdots \\ \psi_{m1}(g) \ldots \psi_{nn}(g) \end{pmatrix}.$$

Тензорные произведения $u_i \otimes v_j$, $i = 1, \ldots, m$; $j = 1, \ldots, n$, образуют базис $M \otimes N$, причем

$$(u_i \otimes v_j)\, g = u_i g \otimes v_j g = \Big(\sum_k \varphi_{ik}(g)\, u_k\Big) \otimes \Big(\sum_l \psi_{jl}(g)\, v_l\Big) =$$

$$= \sum_{k,l} \varphi_{ik}(g)\, \psi_{jl}(g)\, (u_k \otimes v_l).$$

Таким образом, элементы матрицы $(T \otimes S)(g)$, соответствующей $g$ в этом представлении,— это всевозможные произведения элементов матриц [12] $T(g)$ и $S(g)$. В частности,

$$\operatorname{Tr}(T \otimes S)(g) = \sum_{i=1}^{m} \sum_{j=1}^{n} \varphi_{ii}(g)\, \psi_{jj}(g) = (\operatorname{Tr} T(g))(\operatorname{Tr} S(g)).$$

Итак, мы доказали такое предложение.

**Предложение 5.1.** *Характер тензорного произведения равен произведению характеров.*

**Следствие 5.2.** *Пусть* $\chi_1, \ldots, \chi_s$ *— неприводимые характеры группы* $G$. *Существуют такие натуральные числа* $n_{ijk}$, *что* $\chi_i \chi_j = \sum_{k=1}^{s} n_{ijk} \chi_k$ *для любых* $i, j$.

Доказательство. Пусть $M_1, \ldots, M_s$ — все простые $KG$-модули. Тогда $M_i \otimes M_j \simeq \oplus_k n_{ijk} M_k$ для некоторых натуральных $n_{ijk}$, откуда и следует наше утверждение.

Пусть теперь $G = G_1 \times G_2$. Всякое представление $T$ одного из прямых сомножителей (например, $G_1$) можно рассматривать как представление всей группы $G$, полагая $T(g_1, g_2) = T(g_1)$. В частности, если $T$ — представление $G_1$, а $S$ — представление $G_2$, можно построить их тензорное произведение $T \otimes S$, которое есть представление группы $G$. При этом имеет место теорема.

**Теорема 5.3.** *Пусть поле* $K$ *алгебраически замкнуто. Если представление* $T$ *группы* $G_1$ *и представление* $S$ *группы* $G_2$ *неприводимы, то и представление* $T \otimes S$ *группы* $G = G_1 \times G_2$ *неприводимо и всякое неприводимое представление группы* $G$ *однозначно представляется в таком виде.*

Доказательство. Пусть $M(N)$ — $KG_1$-модуль ($KG_2$-модуль), соответствующий представлению $T(S)$. Поскольку $K$ алгебраически замкнуто, $E_{KG_1}(M) = E_{KG_2}(N) = K$ и по теореме II. 6. 7, сопоставляя элементу $a \in KG_1$ линейное отображение $m \to ma$, мы получим эпиморфизм алгебр $KG_1 \to E(M)$.

Выберем базис $\{u_1, \ldots, u_m\}$ в модуле $M$ и пусть $x = \sum_{i=1}^{m} u_i \otimes n_i$, $n_i \in N$ — ненулевой элемент из $M \otimes N$. Для определенности будем считать, что $n_1 \neq 0$. Возьмем в алгебре $KG_1$ такой элемент $a = \sum_j \alpha_j g_j$, $\alpha_j \in K$, $g_j \in G_1$, что соответствующее линейное отображение $M \to M$ переводит $u_1$ в произвольный элемент $m \in M$, а $u_2, \ldots, u_m$ — в 0. Тогда

$$x \sum_j \alpha_j (g_j, 1) = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_j u_j g_j \otimes n_i = \sum_{i=1}^{m} u_i a \otimes n_i = m \otimes n_1.$$

[12] Эта матрица называется кронекеровским или тензорным произведением матриц $T(g)$ и $S(g)$ и обозначается $T(g) \otimes S(g)$.

Аналогично можно подобрать такой элемент $b \in KG$, что $(m \otimes n_1)\, b = m \otimes n$ для любого $n \in N$. Следовательно, подмодуль, порожденный элементом $x$, совпадает с $M \otimes L$, т. е. $M \otimes N$ — простой модуль.

Заметим теперь, что элементы $(g_1, g_2)$ и $(g_1', g_2')$ сопряжены в группе $G = G_1 \times G_2$ тогда и только тогда, когда $g_1$ и $g_1'$ сопряжены в $G_1$, а $g_2$ и $g_2'$ — в $G_2$. Поэтому если $C_1, \ldots, C_s$ — классы сопряженных элементов в $G_1$, а $D_1, \ldots, D_t$— в $G_2$, то $C_i \times D_j$, $i = 1, \ldots, s$; $j = 1, \ldots, t$ — классы сопряженных элементов в $G_1 \times G_2$. В частности, их число равно $st$, поэтому ввиду теоремы 2.2, если мы установим, что для простых модулей из $M \otimes N \simeq M' \otimes N'$ следует $M \simeq M'$ и $N \simeq N'$, то всякий простой $KG$-модуль будет иметь вид $M \otimes N$.

Обозначим через $\chi$ характер, соответствующий модулю $M$, $\chi'$ — модулю $M'$, $\xi$ — характер, соответствующий $N$, и $\xi'$—$N'$, и пусть для определенности $M \simeq M'$. Выберем представителя $g_i$ в классе $C_i$, $f_j$ — в классе $D_j$ и пусть число элементов в группе $G_i$ есть $n_i$, в классе $C_i$ — $h_i$ и в классе $D_j$ — $k_j$. Тогда число элементов в $G$ равно $n_1 n_2$, в классе $C_i \times D_j$ — $h_i k_j$, а $(g_i, f_j)$ — представитель этого класса. Характер, соответствующий $M \otimes N$, есть $\chi\xi$, а характер, соответствующий $M' \otimes N'$,— $\chi'\xi'$. Тогда

$$\frac{1}{n_1 n_2} \sum_{ij} h_i k_j \chi\xi (g_i, f_j)\, \chi'\xi' (g_i^{-1}, f_j^{-1}) =$$

$$= \frac{1}{n_1 n_2} \sum_{i,j} h_i k_j \chi (g_i)\, \xi (f_j)\, \chi' (g_i^{-1})\, \xi' (f_j^{-1}) =$$

$$= \frac{1}{n_1} \sum_{i} h_i \chi (g_i)\, \chi' (g_i^{-1}) \cdot \frac{1}{n_2} \sum_{j} k_j \xi (f_j)\, \xi' (f_j^{-1}) = 0,$$

откуда ввиду теоремы 3.5 (и неприводимости характеров $\chi\xi$ и $\chi'\xi'$) $\chi\xi \neq \chi'\xi'$ и $M \otimes N \not\simeq M' \otimes N'$. Теорема доказана.

Таким образом, зная представления групп $G_1$ и $G_2$, мы можем построить все представления их прямого произведения.

Применим конструкцию тензорного произведения представлений для доказательства следующего результата, усиливающего следствие 4.6.

**Теорема 5.4.** Пусть $C$ — *центр группы* $G$. *Размерность любого неприводимого представления* $G$ *над полем комплексных чисел делит индекс* $(G : C)$.

Доказательство. Пусть $d$ — размерность неприводимого представления, $T$, $M$ — соответствующий модуль.

Если $g \in C$, то матрица $T(g)$ коммутирует со всеми матрицами представления $T$, и по лемме Шура она скалярна: $T(g) = \lambda(g) E$. Рассмотрим представление $M \otimes \ldots \otimes M$ ($m$ раз) группы $G \times \ldots$

$\ldots \times G$. Если элементы $g_i$ лежат в $C$, то в этом представлении $(g_1, \ldots, g_m)$ действует как умножение на число $\lambda(g_1) \ldots \lambda(g_m) = \lambda(g_1 \ldots g_m)$. В частности, если $g_1 \ldots g_m = 1$, то этот элемент действует тождественным образом. Но наборы $(g_1, \ldots, g_m)$ такие, что $g_i \in C$ и $g_1 \ldots g_m = 1$ образуют подгруппу $H$ в $G \times \ldots \times G$. Следовательно, $M \otimes \ldots \otimes M$ — это фактически представление факторгруппы $(G \times \ldots \times G)/H$, порядок которой есть $n^m/c^{m-1}$, $(n = (G : 1)$, $c = (C : 1)$, тогда $(H : 1) = c^{m-1})$. По следствию 4.6 размерность этого представления (равная $d^m$) делит $n^m/c^{m-1}$, т. е. $n^m/c^{m-1}\, d^m$ — целое число.

Обозначим $q = n/cd$. Это рациональное число, причем $cq^m$ — целое для любого $m$. Очевидно, это возможно только, если $q$ — целое, что и требовалось доказать.

## § 6. Теорема Бернсайда

В этом параграфе мы покажем, как теория представлений используется для отыскания нормальных подгрупп и, следовательно, доказательства непростоты и разрешимости тех или иных классов групп. Всюду в этом параграфе представления рассматриваются над полем комплексных чисел.

Пусть $T$ — неприводимое представление размерности $d$ группы $G$, $\chi$ — его характер. По лемме 3.7 для любого $g \in G$ число $\chi(g)$ есть сумма $d$ корней степени $n$ из 1, где $n = (G : 1)$. Кроме того, если матрица $T(g)$ не скалярная, эти корни различны, а тогда

$$|\chi(d)| = \varepsilon_1 + \ldots + \varepsilon_d | < |\varepsilon_1| + \ldots + |\varepsilon_d| = d.$$

Обозначим через $\mathbf{Q}$ поле рациональных чисел, $\varepsilon$ — первообразный корень степени $n$ из 1, $L = \mathbf{Q}[\varepsilon]$. Тогда $L$ есть поле разложения многочлена $x^n - 1$, т. е. по теореме V.4.4 — нормальное расширение поля $\mathbf{Q}$. Обозначим через $\Gamma$ его группу Галуа. Заметим, что для любого элемента $\sigma \in \Gamma$ и любого корня $\varepsilon_i$ из 1 $\sigma(\varepsilon_i)$ — также корень из 1. В частности, $\sigma(\chi(g))$ — также сумма $d$ корней из 1, откуда $|\sigma(\chi(g))| \leqslant d$. Из этих соображений выведем следующий результат.

**Теорема 6.1.** *Пусть $C$ — такой класс сопряженных элементов в группе $G$, что число элементов $h$ в классе $C$ взаимно просто с размерностью $d$ неприводимого представления $T$. Тогда либо все матрицы $T(g)$ $(g \in C)$ скалярные, либо $\chi(g) = 0$ для всех $g \in C$, где $\chi$ = характер представления $T$.*

Доказательство. По теореме 4.5 $(h/d)\,\chi(g)$, где $g \in C$ — целое алгебраическое число. В то же время и $\chi(g)$ — целое алгебраическое число. Пользуясь взаимной простотой $d$ и $h$, подберем целые числа $x$ и $y$ так, чтобы $xd + yh = 1$. Тогда

$$z = y\frac{h}{d}\chi(g) + x\chi(g) = \frac{yh + xd}{d}\chi(g) = \frac{\chi(g)}{d}$$

— целое алгебраическое число. Если $T(g)$ — не скалярная матрица, то, как мы видели, $|z| < 1$. С другой стороны, для любого

$\sigma \in \Gamma$ число $\sigma(z)$ — целое алгебраическое (оно удовлетворяет всем тем же уравнениям, что и $z$), причем $|\sigma(z)| < 1$. Следовательно, и число $q = \prod_{\sigma \in \Gamma} \sigma(z)$ — целое алгебраическое, причем $|q| < 1$. Но, очевидно, $\sigma(q) = q$ для всех $\sigma \in \Gamma$, т. е. $q \in Q$ (по теореме V.4.4). Ввиду предложения 4.1 $q$ — целое число, откуда $q = 0$, а потому и $z = 0$, что и требовалось доказать.

Заметим, что скалярные матрицы образуют нормальную подгруппу в группе невырожденных матриц. Поэтому те элементы $g \in G$, для которых матрицы $T(g)$ скалярные, образуют нормальную подгруппу $N(T)$ в $G$. Если $T$ неприводимое и не одномерное, то $N(T) \neq G$. Эти соображения позволяют применять теорему 6.1 для отыскания нормальных подгрупп. Мы докажем таким способом следующие две теоремы Бернсайда.

**Теорема 6.2.** *Если в группе $G$ есть такой класс сопряженных элементов $C \neq \{1\}$, что число элементов в нем $h = p^l$, где $p$ — простое число, то группа $G$ не простая, т. е. в ней есть нетривиальная нормальная подгруппа.*

Доказательство. Пусть $T_1, \ldots, T_s$ — все неприводимые представления $G$, $d_1, \ldots, d_s$ — их размерности и $\chi_1, \ldots, \chi_s$ — характеры. Будем считать, что $T_1$ — одномерное представление, такое, что $T_1(g) = 1$ для всех $g$. Тогда $\chi_1(g) = 1$ для всех $g$. Если еще хотя бы одно из $T_i$ — одномерное, то его ядро — нетривиальная нормальная подгруппа в $G$. Следовательно, можно считать $d_i > 1$ при $i \neq 1$.

Пусть $g \in C$. Если $T_i(g)$ — скалярная матрица, то вновь в $G$ есть нетривиальная нормальная подгруппа. В противном случае, если $d_i$ не делится на $p$, то $\chi_i(g) = 0$ по теореме 6.1. Воспользуемся теперь формулой $\chi_{\text{red}} = \sum_{i=1}^{s} d_i \chi_i$ и предложением 3.1. Получаем

$$\chi_{\text{red}}(g) = 0 = 1 + \sum_{i=2}^{s} d_i \chi_i(g) = 1 + pz,$$

где $z$ — целое алгебраическое число, откуда $z = -1/p$, что невозможно ввиду предложения 4.1. Теорема доказана.

**Теорема 6.3.** *Если $(G : 1) = p^a q^b$, где $p$ и $q$ — простые числа, то группа $G$ разрешима*[13] .

Доказательство будем вести индукцией по порядку группы $G$. При этом используем следующие известные результаты из теории конечных групп:

а) если порядок группы $G$ — степень простого числа, то группа $G$ имеет нетривиальный центр;

---

[13] Напомним, что группа $G$ называется разрешимой, если в ней есть такой ряд подгрупп $G \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{1\}$, что $G_{i+1}$ — нормальная подгруппа в $G_i$ и факторгруппа $G_i/G_{i+1}$ абелева для всех $i = 0, 1, \ldots, m-1$ ($G_0 = G$).

б) если порядок группы $G$ делится на $p^a$, где $p$ простое, то в $G$ есть подгруппа порядка $p^a$ (теорема Силова).

Выберем в $G$ подгруппу $H$ порядка $p^a$, и пусть элемент $g \neq 1$ лежит в центре $H$. Обозначим $\overline{H} = \{x \in G \mid xg = gx\}$ (нормализатор элемента $g$). Очевидно, $\overline{H} \supset H$, поэтому $(G : \overline{H})$ делит $(G : H) = q^b$. Но число элементов, сопряженных с $g$, как легко видеть, равно $(G : \overline{H})$, т. е. является степенью $q$. По теореме 6.2 в $G$ есть нетривиальная нормальная подгруппа $N$. По предположению индукции группы $N$ и $G/N$ разрешимы, а тогда, очевидно, и группа $G$ разрешима, что и требовалось доказать.

## *Упражнения к главе VII*

Во всех упражнениях, кроме упражнений 18—22, предполагается, что $K$ — поле, характеристика которого не делит порядок группы $G$.

1. Пусть $G = \{g_1, \ldots, g_n\}$ — конечная группа, $M$ и $N$ — два $KG$-модуля, $f: M \to N$ — произвольное линейное отображение. Доказать, что отображение $\bar{f}: M \to N$, задаваемое формулой $\bar{f}(m) = \frac{1}{n} \sum_{i=1}^{n} f(mg_i^{-1})\, g_i$, является гомоморфизмом $KG$-модулей.

2. Вывести из упражнения 1, что в описанной ситуации всякий подмодуль $N \subset M$ выделяется прямым слагаемым. (Указание. применить указанную конструкцию к произвольному проектору пространства $M$ на подпространство $N$ и воспользоваться предложением I.6.2.) Этот результат дает новое доказательство теоремы Машке, не зависящее от результатов гл. VI.

3. Установить изоморфизм $KG \simeq KG_1 \otimes KG_2$, если $G = G_1 \times G_2$.

В упражнениях 4—6 предполагается, что поле $K$ содержит первообразный корень степени $n = (G : 1)$ из 1 (или, что то же, является полем разложения многочлена $x^n - 1$). Группа $G$ во всех этих упражнениях предполагается абелевой.

4. Доказать, что групповая алгебра $KG$ в указанных предположениях расщепима, а группа $G$ имеет $n$ различных неприводимых представлений, которые все одномерны (т. е. являются гомоморфизмами $G \to K^*$, где $K^*$ — мультипликативная группа поля $K$).

5. Обозначим через $\widehat{G}$ множество всех неприводимых представлений группы $G$ над полем $K$ (они называются характерами $G$ над $K$). Для любых двух характеров $f_1$ и $f_2$ положим $(f_1 f_2)(g) = f_1(g) f_2(g)$, где $g \in G$.

а) Проверить, что $f_1 f_2$ — также характер $G$ над $K$ и относительно так определенной операции $\widehat{G}$ является абелевой группой порядка $n$.

б) Доказать, что для фиксированного элемента $g \in G$ отображение $\tilde{g}: \widehat{G} \to K$, определенное формулой $\tilde{g}(f) = f(g)$, является характером группы $\widehat{G}$.

в) Доказать, что отображение $\delta: G \to \widehat{\widehat{G}}$, переводящее $g$ в $\tilde{g}$, является гомоморфизмом групп.

г) Установить, что $\operatorname{Ker} \delta = \{1\}$, т. е. $\delta$ — мономорфизм и, поскольку $(G : 1) = (\widehat{\widehat{G}} : 1)$, изоморфизм групп.

6. Используя тот факт, что всякая абелева группа $G$ разлагается в прямое произведение циклических, вычислить явно все ее характеры и показать, что $\hat{G} \simeq G$ (в отличие от изоморфизма $\delta$ из предыдущего упражнения этот изоморфизм существенно зависит от явного вида разложения группы $G$ в произведение циклических).

7. Группой кватернионов называется подмножество $\{e, i, j, k, -e, -i, -j, -k\}$ алгебры кватернионов (см. § 1 гл. I, пример 4). Проверить, что эти восемь элементов действительно образуют группу относительно умножения. Найти все неприводимые представления этой группы над полями действительных и комплексных чисел. (Указание: в последнем случае можно воспользоваться результатом упражнения 3 гл. I.)

8. Группой диэдра $D_n$ называется группа с образующими $a$, $b$ и определяющими соотношениями $a^n = b^2 = 1$, $ba = a^{-1}b$.

а) Доказать, что $D_n$ — конечная группа порядка $2n$.

б) Проверить, что соответствие

$$a \to \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}, \quad b \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

($k$ — целое число) задает представление $T_k$ группы диэдра $D_n$, причем при различных $k$, удовлетворяющих неравенству $0 < k < n/2$, представления $T_k$ неприводимы и неподобны.

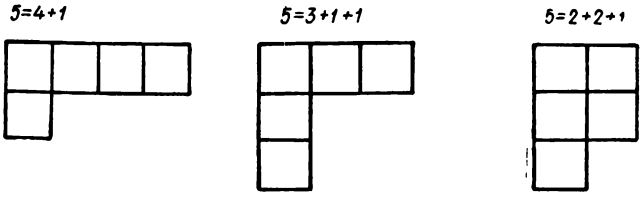
в) Найти одномерные представления группы $D_n$ и доказать, что эти представления и представления $T_k$, $0 < k < n/2$, из пункта б) составляют все неприводимые представления $D_n$ над полем комплексных или действительных чисел. (Указание: использовать теорему 2.1.).

Следующие упражнения (9—13) посвящены описанию представлений симметрической группы $S_n$, т. е. группы всех подстановок на множестве $\{1, 2, \ldots, n\}$. Напомним некоторые факты о строении этой группы. Циклом длины $k$ $(i_1, i_2, \ldots, i_k)$ называется подстановка, которая переводит $i_1$ в $i_2$, $i_2$ в $i_3$, ..., $i_k$ в $i_1$, а все остальные элементы оставляет на месте. Все числа $i_1, \ldots, i_k$ предполагаются различными. Возможен случай $k = 1$. Очевидно, такой цикл — это тождественная подстановка. Циклы $(i_1, \ldots, i_k)$ и $(j_1, \ldots, j_l)$ называются независимыми, если множества $\{i_1, \ldots, i_k\}$ и $\{j_1, \ldots, j_l\}$ не пересекаются. Всякая подстановка $\sigma$ раскладывается в произведение непересекающихся циклов $\sigma = (i_{11} \ldots i_{1k_1})(i_{21} \ldots i_{2k_2}) \ldots (i_{t1} \ldots i_{tk_t})$, где $k_1 + \ldots + k_t = n$, причем это разложение однозначно (с точностью до порядка сомножителей, так как независимые циклы, очевидно, перестановочны). Набор длин $(k_1, \ldots, k_t)$ называют цикленным типом подстановки $\sigma$.

9. Доказать, что две подстановки сопряжены в $S_n$ тогда и только тогда, когда они имеют одинаковый цикленный тип. Таким образом, класс сопряженных элементов в $S_n$ однозначно определяется разбиением числа $n$ в сумму натуральных слагаемых $n = k_1 + k_2 + \ldots + k_t$.

Далее мы будем всегда считать, что $k_1 \geqslant k_2 \geqslant \ldots \geqslant k_t$. Такой цикленный тип удобно задавать так называемой диаграммой Юнга — расположением $n$ клеточек в $t$ строк, по $k_i$ в $i$-й строке.

Примеры (для $n = 5$):




Позицией на диаграмме Юнга называется произвольное расположение чисел $\{1, 2, \ldots, n\}$ в клетках этой диаграммы. Говорят, что диаграмма Юнга, соответствующая разбиению $(k_1, \ldots, k_s)$, выше диаграммы, соответствующей $(l_1, \ldots, l_t)$, если $k_1 > l_1$, или $k_1 = l_1$, но $k_2 > l_2$, или $k_1 = l_1$, $k_2 = l_2$, но $k_3 > l_3$ и т. д. (лексикографический порядок).

10. Пусть $D_1$ и $D_2$ — позиции на двух диаграммах Юнга, первая из которых выше второй.

а) Доказать, что для любых позиций на диаграммах $D_1$ и $D_2$ найдутся два числа $i \neq j$, которые стоят в одной строке диаграммы $D_1$ и в одном столбце диаграммы $D_2$.

б) Доказать, что для любой подстановки $\sigma$ найдутся такие транспозиции (т. е. циклы длины 2) $\tau_1 = (i_1 i_2)$ и $\tau_2 = (j_1 j_2)$, что $\tau_1\sigma = \sigma\tau_2$, причем числа $i_1$, $i_2$ стоят в одной строке диаграммы $D_1$, а числа $j_1$, $j_2$ — в одном столбце диаграммы $D_2$.

11. Для любой позиции $D$ на диаграмме Юнга обозначим через $P_D$ множество подстановок, переставляющих числа только внутри строк этой диаграммы, а через $Q_D$ — множество подстановок, переставляющих числа только внутри столбцов.

а) Проверить, что $P_D$ и $Q_D$ — подгруппы в $S_n$, причем $P_D \cap Q_D = \{1\}$.

б) Доказать, что если $D_1$ и $D_2$ — две позиции на одной и той же диаграмме Юнга, то либо найдется пара чисел $i \neq j$, которые стоят в одной строке $D_1$ и в одном столбце $D_2$, либо, переставляя числа в строках $D_1$ и столбцах $D_2$, можно получить одну и ту же позицию.

в) Доказать, что для любой позиции $D$ и любой подстановки $\sigma$ либо найдутся транспозиции $\tau_1 \in P_D$ и $\tau_2 \in Q_D$, такие, что $\tau_1\sigma = \sigma\tau_2$, либо $\sigma = \xi\eta$, где $\xi \in P_D$, а $\eta \in Q_D$, причем такое представление однозначно.

12. Симметризатором Юнга, соответствующим позиции $D$ на некоторой диаграмме, называется элемент $c_D$ групповой алгебры $A = KS_n$, определенный формулой

$$c_D = \sum_{\substack{\xi \in P_D \\ \eta \in Q_D}} \operatorname{sgn}(\eta)\, \xi\eta,$$

где $\operatorname{sgn}(\eta)$ — знак подстановки $\eta$, равный 1 для четных и $-1$ для нечетных подстановок.

Доказать, что если $\sigma \in P_D$, то $\sigma c_D = c_D$, а если $\sigma \in Q_D$, то $c_D\sigma = \operatorname{sgn}(\sigma) c_D$. Наоборот, если $a \in A$ — любой элемент, удовлетворяющий этим условиям, то $a = \alpha c_D$ для некоторого $\alpha \in K$. (Указание: воспользоваться результатом упражнения 11, в).)

13. Обозначим $M_D = c_D A$, где $c_D$ — симметризатор Юнга, $A = KS_n$.

а) Доказать, что $E_D(M_D) = K$. (Указание: воспользоваться результатом предыдущего упражнения.)

б) В предположениях упражнения 10 доказать, что $\operatorname{Hom}_A(M_{D_1}, M_{D_2}) = 0$.

в) Вывести отсюда, что, когда $D$ пробегает все позиции на диаграммах Юнга, $M_D$ пробегает все простые $A$-модули (с точностью до изоморфизма), причем $M_{D_1} \simeq M_{D_2}$ тогда и только тогда, когда $D_1$ и $D_2$ — позиции на одной и той же диаграмме.

14. Пусть $A = KG$, $M$ и $N$ — два произвольных $A$-модуля, $\chi$ и $\psi$ — характеры соответствующих представлений. В обозначениях теоремы 3.5 доказать, что

$$\frac{1}{n}\sum_{k=1}^{s} h_k \chi(g_k)\psi(g_k^{-1}) = \dim \operatorname{Hom}_A(M, N).$$

15. Вывести из следствия 2.3 и 4.6, что всякая группа порядка $p^2$, где $p$ — простое число, абелева.

16. Пусть $M$ — модуль над групповой алгеброй $KG$, $M^*$ — пространство линейных форм на $M$, т. е. $M^* = \operatorname{Hom}_K(M, K)$. Проверить, что, полагая $(fg)\times$ $\times (m) = f(mg^{-1})$ для любых $f \in M^*$, $m \in M$, $g \in G$, мы превращаем $M^*$ в $KG$-модуль, причем если $T$ — представление, соответствующее $M$, то представление $T^*$ соответствующее $M^*$, имеет вид $T^*(g) = T(g^{-1})'$ (штрих означает переход к транспонированной матрице). В частности, если $\chi$ — характер представления $T$, $\chi^*$ — представления $T^*$, то $\chi^*(g) = \chi(g^{-1})$, а если $K = \mathbf{C}$, то $\chi^*(g) = \overline{\chi(g)}$.

17. Представление $T$ группы $G$ над полем комплексных (или действительных) чисел называется унитарным, если все матрицы $T(g)$ унитарны.

а) Доказать, что всякое комплексное (действительное) представление конечной группы $G = \{g_1, \ldots, g_n\}$ подобно унитарному. (Указание: выбрать каким-нибудь образом скалярное произведение $(u, v)$ в соответствующем модуле $M$, превращающее $M$ в унитарное (эвклидово) пространство, и положить $\langle u, v\rangle = \sum_{i=1}^{n} (ug_i, vg_i)$. Тогда скалярное произведение $\langle u, v\rangle$ по-прежнему превращает $M$ в унитарное пространство и $\langle ug, vg\rangle = \langle u, v\rangle$ для всех $g \in G$.)

б) Вывести отсюда еще одно доказательство того, что всякое представление $G$ над $\mathbf{R}$ или $\mathbf{C}$ вполне приводимо.

в) На примере бесконечной циклической группы показать, что для бесконечных групп утверждение пункта а) неверно.

В последующих упражнениях предполагается, что характеристика $p$ поля $K$ делит порядок $n$ группы $G$.

18. Пусть $H$ — такая подгруппа группы $G$, что индекс $(G : H)$ взаимно прост $p$, $N$ — подмодуль $KG$-модуля $M$, дополняемый как $KH$-модуль. Доказать, что тогда $N$ дополняем и как $KG$-модуль. (Указание: выбрать по представителю в смежных классах $G$ по $H$ и поступить, как в упражнениях 1 и 2.)

19. Предположим, что $G$ — $p$-группа, т. е. $n = p^k$. Обозначим $I = \left\{\sum_{g\in G} \alpha_g g \;\middle|\; \sum_g \alpha_g = 0\right\}$. Доказать, что $I = \operatorname{rad} KG$, причем $KG/I \simeq K$. (Указание: воспользоваться результатом упражнения 13 к гл. VI.)

20. а) Пусть $M$ — неприводимое представление $p$-группы $G$. Доказать, что $[M : K] = 1$ и $mg = m$ для всех $m \in M$, $g \in G$.

б) Доказать, что всякое представление $G$ над $K$ подобно специальному треугольному, т. е. представлению вида

$$T(g) = \begin{pmatrix} 1 & & * \\ & 1 & \\ & & \ddots \\ 0 & & & 1 \end{pmatrix}.$$

в) Вывести из пункта б), что всякая конечная $p$-группа $G$ изоморфна подгруппе группы верхних специальных треугольных матриц над полем вычетов по модулю $p$.

г) Доказать, что всякая конечная $p$-группа $G$ нильпотентна, т. е. в ней существует ряд нормальных подгрупп. $G = G_0 \supset G_1 \supset \ldots \supset G_k = \{1\}$, таких, что для любого $i = 1, \ldots, k$ факторгруппа $G_{i+1}/G_i$ содержится в центре $G/G_i$.

21. Описать неразложимые представления циклической $p$-группы над полем характеристики $p$; убедиться, что их число равно порядку группы.

22. Пусть $G$ — нециклическая группа порядка $p^2$ (т. е. прямое произведение двух циклических групп порядка $p$). Построить для любого четного $d$ неразложимое представление группы $G$ размерности $d$. (Указание: если $a$ и $b$ — образующие циклических сомножителей $G$, положить

$$T(a) = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix}, \qquad T(b) = \begin{pmatrix} E & X \\ 0 & E \end{pmatrix},$$

где $E$ — единичная, $X$ — произвольная матрица.) Проверить, что если поле $K$ бесконечно, то существует бесконечно много неподобных представлений группы $G$ размерности $d$. Перенести этот результат на произвольную нециклическую $p$-группу.

23. Пусть $G$ — прямое произведение трех циклических групп порядка $p$ с образующими $a$, $b$ и $c$. Проверить, что, полагая

$$T(a) = \begin{pmatrix} E & E \\ 0 & E \end{pmatrix}, \qquad T(b) = \begin{pmatrix} E & X \\ 0 & E \end{pmatrix}, \qquad T(c) = \begin{pmatrix} E & Y \\ 0 & E \end{pmatrix},$$

где $X$ и $Y$ — произвольные квадратные матрицы, мы получаем представление $T = T_{X,Y}$ группы $G$, причем представления $T_{X,Y}$ и $T_{X',Y'}$ подобны тогда и только тогда, когда подобны пары матриц $X, Y$ и $X', Y'$, т. е. существует матрица $C$, такая, что $X' = CXC^{-1}$ и $Y' = CYC^{-1}$. Отметим, что С. А. Кругляк построил, при $p > 2$, для любой нециклической $p$-группы $G$ представление $S_{X,Y}$, зависящее от пары матриц $X, Y$, и такое, что $S_{X,Y}$ и $S_{X',Y'}$ подобны тогда и только тогда, когда подобны пары матриц $X, Y$ и $X', Y'$. Классификация пар матриц с точностью до подобия является одной из труднейших задач линейной алгебры и до настоящего временн не решена.

# VIII

ГЛАВА

## ТЕОРЕМА МОРИТЫ

В § 3 гл. II мы отмечали, что модули над телом $D$ и над простой алгеброй $M_n(D)$ «устроены одинаково». Результаты § 6 той же главы показывают, что и вообще модули над однотипными полупростыми алгебрами обладают одинаковыми свойствами: у таких модулей изоморфны кольца эндоморфизмов и т. п. В § 5 гл. III эти результаты были перенесены на проективные модули уже над любыми однотипными алгебрами (лемма III.5.5). Оказывается, здесь можно избавиться от требования проективности: над однотипными алгеб-

рами все модули устроены одинаково. Однако, чтобы придать этому утверждению точный смысл, нужно ввести ряд понятий, играющих в настоящее время важную роль в различных разделах математики. Это прежде всего понятия категории и функтора, а также понятие эквивалентности категорий, которое является математической интерпретацией выражения «устроены одинаково».

Теорема Мориты, которую мы докажем в этой главе, как раз и утверждает, что алгебры однотипны тогда и только тогда, когда категории модулей над ними эквивалентны. Техника, которая применяется при доказательстве этой теоремы (тензорные произведения, точные последовательности), оказывается полезной и во многих других вопросах. В частности, в § 5 мы построим тензорную алгебру бимодуля, обобщающую понятие алгебры путей схемы и играющую аналогичную роль при описании неполупростых алгебр (не обязательно расщепимых).

## § 1. Категории и функторы

Говорят, что задана **категория** $C$, если определены:

1) множество $\mathrm{Ob}\, C$, элементы которого называются **объектами** категории $C$;

2) множество $\mathrm{Mor}\, C$, элементы которого называются **морфизмами** категории $C$;

3) каждому морфизму $f \in \mathrm{Mor}\, C$ сопоставлена упорядоченная пара объектов $(X, Y)$ категории $C$ (мы будем называть $X$ **началом**, а $Y$ — **концом** морфизма $f$, писать $f : X \to Y$ и говорить, что $f$ — морфизм из объекта $X$ в объект $Y$; множество всех морфизмов из $X$ в $Y$ обозначается $\mathrm{Hom}\,(X, Y)$ или, если нужно явно указать категорию, $\mathrm{Hom}_C\,(X, Y)$);

4) для любой тройки объектов $X, Y, Z \in \mathrm{Ob}\, C$ и любой пары морфизмов $f : X \to Y$ и $g : Y \to Z$ однозначно определен морфизм $gf : X \to Z$, который называется **композицией** или **произведением** морфизмов $f$ и $g$;

5) умножение морфизмов ассоциативно, т. е. для любой тройки морфизмов $f, g, h$ $h(gf) = (hg)f$, если эти произведения определены[14];

6) для каждого объекта $X \in \mathrm{Ob}\, C$ существует морфизм $1_X \in \mathrm{Hom}\,(X, X)$, такой, что для любых морфизмов $f : X \to Y$ и $g : Z \to X$ $f1_X = f$ и $1_X g = g$.

Тривиально проверяется, что морфизм $1_X$ с указанными свойствами единствен. Он называется **единичным**, или **тождественным** морфизмом объекта $X$.

**Примеры** категорий. 1. **Категория множеств** Sets. Объектами этой категории являются множества, а морфизмами $f : X \to Y$ — отображения множества $X$ во множество $Y$. Компози-

[14] Легко видеть, что если определена левая часть этого равенства, то определена и правая, и наоборот,— это будет тогда и только тогда, когда конец морфизма $g$ совпадает с началом морфизма $g$, а конец $g$ — с началом $h$.

ция морфизмов — это просто последовательное выполнение отображений. Выполнение всех аксиом категории очевидно[15].

2. Категория групп Gr. Объекты этой категории — это группы, морфизмы $f: X \to Y$ — это гомоморфизмы группы $X$ в группу $Y$, а композиция определяется как обычное умножение гомоморфизмов.

3. Аналогично определяются категория векторных пространств над некоторым полем $K$ (обозначим ее Vect, или $\mathrm{Vect}_K$, если нужно явно указать поле), категория $K$-алгебр Alg (или $\mathrm{Alg}_K$), категория mod-$A$ правых и категория $A$-mod левых модулей над алгеброй $A$ и т. п. Во всех этих примерах морфизмами служат некоторые отображения множеств, а композиция морфизмов — это их последовательное применение. Однако следующие примеры показывают, что встречаются категории и другого типа.

4. Всякую полугруппу $P$ (с единицей) можно рассматривать как множество морфизмов некоторой категории, содержащей всего один объект. При этом за композицию морфизмов естественно принимается их произведение в полугруппе $P$.

5. Категория матриц Mat. Объектами этой категории служат натуральные числа, а множество морфизмов $\mathrm{Hom}(m, n)$ определяется как множество всех матриц размера $n \times m$ с коэффициентами из некоторого поля $K$. Композиция морфизмов — это обычное произведение матриц. Здесь проверка всех аксиом также тривиальна.

6. Пусть $M$ — некоторое частично упорядоченное множество. Будем рассматривать его как множество объектов категории, в которой $\mathrm{Hom}(x, y)$ состоит из одного элемента при $x \leqslant y$ и $\mathrm{Hom}(x, y) = \varnothing$ в противном случае. Композиция морфизмов определяется здесь, очевидно, естественным образом.

7. Категория путей. Пусть $S$ — некоторая схема (см. § 6 гл. III). С ней можно связать категорию $C_S$ следующим образом. Положим $\mathrm{Ob}\, C_S = S$, а $\mathrm{Hom}(i, j)$. где $i, j \in S$ — множество путей с началом $i$ и концом $j$. Произведение путей определяется, как и в гл. III, приписыванием одного пути к другому, а за $1_i$ можно принять «пустой» путь с началом и концом $i$ (см. гл. III). Вновь тривиально проверяется, что получается категория, которую назовем категорией путей схемы $S$.

8. Дуальная категория. По произвольной категории $C$ можно построить новую категорию $C^\circ$ следующим образом. Положим $\mathrm{Ob}\, C^\circ = \mathrm{Ob}\, C$, $\mathrm{Mor}\, C^\circ = \mathrm{Mor}\, C$, но началом (концом) морфизма $f$ в категории $C^\circ$ объявим его конец (начало) в категории $C$. За произведение $gf$ в категории $C^\circ$ примем произведение $fg$, опреде-

---

[15] Конечно, при таком определении Ob (Sets) и Mor (Sets) множествами не являются. Однако для всех практических целей это не существенно: всегда можно ограничиться подмножествами некоторого фиксированного множества (и их отображениями). Это замечание относится и к другим аналогичным примерам.

ленное в категории $C$. Категория $C^\circ$ называется дуальной по отношению к категории $C$. Очевидно, $C^{\circ\circ} = C$.

Для того чтобы избежать путаницы, обычно объекты и морфизмы категории $C^\circ$ также помечают кружочком: $X^\circ$, $f^\circ$ и т. п. Тогда приведенные выше определения можно записать в виде формул $\mathrm{Ob}\ C^\circ = (\mathrm{Ob}\ C)^\circ$, $\mathrm{Mor}\ C^\circ = (\mathrm{Mor}\ C)^\circ$, $\mathrm{Hom}_{C^\circ}(X^\circ, Y^\circ) = \mathrm{Hom}_C(Y, X)^\circ$ и $g^\circ f^\circ = (gf)^\circ$.

В произвольной категории имеет смысл понятие изоморфизма. Именно, морфизм $f: X \to Y$ называется изоморфизмом тогда и только тогда, когда существует морфизм $f^{-1}: Y \to X$, такой, что $f^{-1}f = 1_X$, а $ff^{-1} = 1_Y$. Очевидно, этими условиями морфизм $f^{-1}$ определяется однозначно. Он называется морфизмом, обратным к $f$. Конечно, $f^{-1}$ также является изоморфизмом и $(f^{-1})^{-1} = f$. Легко проверить также, что композиция изоморфизмов $f$ и $g$ (если она определена) снова является изоморфизмом, причем $(gf)^{-1} = f^{-1}g^{-1}$.

Так же, как при изучении групп, алгебр и модулей, важную роль играет понятие гомоморфизма, в теории категорий центральное место занимает понятие функтора.

Функтором $F$ из категории $C$ в категорию $D$ называется пара отображений $F_{\mathrm{ob}}: \mathrm{Ob}\ C \to \mathrm{Ob}\ D$ и $F_{\mathrm{mor}}: \mathrm{Mor}\ C \to \mathrm{Mor}\ D$, удовлетворяющая следующим условиям:

1) если $f: X \to Y$, то $F_{\mathrm{mor}}(f): F_{\mathrm{ob}}(X) \to F_{\mathrm{ob}}(Y)$;

2) $F_{\mathrm{mor}}(1_X) = 1_{F_{\mathrm{ob}}(X)}$;

3) если определено произведение $gf$, то $F_{\mathrm{mor}}(gf) = F_{\mathrm{mor}}(g)\,F_{\mathrm{mor}}(f)$.

Обычно вместо $F_{\mathrm{mor}}(f)$ и $F_{\mathrm{ob}}(X)$ пишут просто $F(f)$ и $F(X)$.

**Примеры** функторов. 1. Пусть $C$ — произвольная категория. Фиксируем произвольный объект $X \in \mathrm{Ob}\ C$ и построим функтор $h_X: C \to \mathrm{Sets}$ следующим образом. Если $Y \in \mathrm{Ob}\ C$, положим $h_X(Y) = \mathrm{Hom}(X, Y)$. Если $f: Y \to Z$, то за $h_X(f)$ примем отображение множеств $\mathrm{Hom}(X, Y) \to \mathrm{Hom}(X, Z)$, переводящее произвольный морфизм $g: X \to Y$ в морфизм $fg: X \to Z$. Выполнение условий 1) и 2) очевидно, а условие 3) вытекает из ассоциативности умножения морфизмов [16].

Если $C = \mathrm{mod}\text{-}A$ (или $A\text{-mod}$), где $A$ — алгебра над полем $K$, то все множества $\mathrm{Hom}(X, Y)$ являются векторными пространствами над $K$ и легко видеть, что для любого $f$ отображение $h_X(f)$ является гомоморфизмом. Поэтому $h_X$ в данном случае можно рассматривать как функтор в категорию Vect векторных пространств над полем $K$.

2. Пренебрегающие функторы. Пусть $C = \mathrm{Gr}$, $D = \mathrm{Sets}$. Определим функтор $F: C \to D$, полагая $F(X) = X$ и $F(f) = f$ для любых $X \in \mathrm{Ob}\ C$ и $f \in \mathrm{Mor}\ C$. Иными словами, мы «забываем» о структуре группы на $X$ и рассматриваем $X$ просто как множество, а гомоморфизм — как отображения множеств.

---

[16] Читателям, неискушенным в категорной технике, рекомендуем проверить это.

Этот функтор называется пренебрегающим функтором из категории групп в категорию множеств.

Аналогично можно построить целую серию примеров пренебрегающих функторов, принимая за $C$ «категорию множеств с более богатой структурой», а за $D$ — «категорию множеств с более бедной структурой».

Например: а) $C = \mathrm{Alg}_K$, $D = \mathrm{Vect}_K$; б) $C = \text{mod-}A$, $D = \mathrm{Vect}$; в) $C = \mathrm{Alg}_L$, $D = \mathrm{Alg}_K$, где $L$ — расширение поля $K$, и т. п.

3. Пусть $A$ — некоторая алгебра, $B = M_n(A)$. Построим функтор $G : \text{mod-}A \to \text{mod-}B$ следующим образом. Для всякого $A$-модуля $M$ положим $G(M) = nM$. Наделим $G(M)$ структурой $B$-модуля естественным образом: рассматривая элемент $x \in G(M)$ как $n$-мерный вектор с координатами из $M$, определим $xb$, где $b \in B$, по обычному правилу умножения матриц. Если $f : M \to N$ — гомоморфизм $A$-модулей, определим $G(f) : G(M) \to G(N)$ «покоординатно»: для $x = (x_1, \ldots, x_n)$ положим $G(f)\, x = (fx_1, \ldots, fx_n)$. Легко проверить, что $G(f)$ — это гомоморфизм $B$-модулей и что приведенная конструкция действительно определяет функтор.

4. Если $L$ — расширение поля $K$, то можно построить функтор $F : \mathrm{Alg}_K \to \mathrm{Alg}_L$, принимая за $F(A)$ $L$-алгебру $A_L = A \otimes L$, а за $F(f)$, где $f : A \to B$,— гомоморфизм $L$-алгебр $f \otimes 1 : A_L \to B_L$.

5. Пусть $C$ — полугруппа с единицей, рассматриваемая как категория с одним объектом (пример 4 категорий). Выясним, что такое функтор $F$ из категории $C$ в категорию $\mathrm{Vect}_K$. Поскольку $\mathrm{Ob}\, C$ состоит из одного элемента, то для задания $F_{\mathrm{ob}}$ достаточно фиксировать одно векторное пространство $V$. Тогда для всякого элемента $a$ полугруппы $F(a) \in E(V)$, причем $F(1) = 1_V$, а $F(ab) = F(a)\, F(b)$. Иными словами, $F_{\mathrm{mor}}$ — это представление полугруппы $C$ в векторном пространстве $V$.

6. Если $C^\circ$ — категория, дуальная к категории $C$, то функторы $F : C^\circ \to D$ часто называются **контравариантными функторами** из категории $C$ в категорию $D$ (в этом случае обычные функторы из $C$ в $D$ называются **ковариантными функторами**). Поскольку между множествами $\mathrm{Ob}\, C^\circ$ и $\mathrm{Ob}\, C$, а также $\mathrm{Mor}\, C^\circ$ и $\mathrm{Mor}\, C$ имеется взаимно однозначное соответствие, для контравариантного функтора $F$ отображения $F_{\mathrm{ob}}$ и $F_{\mathrm{mor}}$ можно рассматривать и как отображения, соответственно, $\mathrm{Ob}\, C \to \mathrm{Ob}\, D$ и $\mathrm{Mor}\, C \to \mathrm{Mor}\, D$. Однако при этом аксиомы 1)—3) из определения функтора принимают следующий вид:

1°), если $f : X \to Y$, то $F(f) : F(Y) \to F(X)$ ($F$ «переворачивает стрелки»);

2°) $F(1_X) = 1_{F(X)}$;

3°) $F(gf) = F(f)\, F(g)$ ($F$ «меняет порядок стрелок»).

Важный пример контравариантного функтора получается аналогично примеру 1. Фиксируя объект $X \in \mathrm{Ob}\, C$, можно построить функтор $h_X^\circ : C^\circ \to \mathrm{Sets}$, полагая $h_X^\circ(Y^\circ) = \mathrm{Hom}(Y, X)$, а $h_X^\circ(f^\circ)$, где

$f: Y \to Z$ — отображение $\mathrm{Hom}(Z, X) \to \mathrm{Hom}(Y, X)$, переводящее морфизм $g: Z \to X$ в морфизм $gf: Y \to X$. Если $C = \mathrm{mod}\text{-}A$ (или $A\text{-mod}$), то $h_X^\circ$ также можно рассматривать как функтор $C^\circ \to \mathrm{Vect}$.

## § 2. Точные последовательности

В дальнейшем часто будут встречаться ситуации, в которых приходится одновременно рассматривать довольно много модулей и их гомоморфизмов, связанных различными соотношениями. Для описания таких ситуаций очень удобен «язык диаграмм и точных последовательностей». Пусть, например, заданы модули $M_i$ и $N_i$ $(i = 1, 2, 3)$ и гомоморфизмы $f_i: M_i \to N_i$ $(i = 1, 2, 3)$, $g: M_1 \to M_2$, $h: M_2 \to M_3$, $g': N_1 \to N_2$ и $h': N_2 \to N_3$. В этом случае говорят, что дана диаграмма модулей

$$\begin{array}{ccccc} M_1 & \xrightarrow{g} & M_2 & \xrightarrow{h} & M_3 \\ \downarrow{\scriptstyle f_1} & & \downarrow{\scriptstyle f_2} & & \downarrow{\scriptstyle f_3} \\ N_1 & \xrightarrow{g'} & N_2 & \xrightarrow{h'} & N_3 \end{array} \qquad (1)$$

Диаграмма (1) называется коммутативной, если $f_2 g = g' f_1$ и $f_3 h = h' f_2$. Иными словами, если в диаграмме есть два пути, соединяющие некоторую пару модулей, то произведения гомоморфизмов, взятые вдоль каждого из этих путей, должны совпадать. Аналогичный смысл вкладывается в понятие коммутативной диаграммы и в произвольном случае. Понятно, что такая терминология позволяет кратко описывать довольно сложные ситуации.

Пусть дана последовательность модулей и гомоморфизмов (конечная или бесконечная).

$$\ldots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots \qquad (2)$$

Говорят, что эта последовательность точна в члене $M_i$, если $\mathrm{Ker}\, f_i = \mathrm{Im}\, f_{i-1}$. Если последовательность (2) точна во всех своих членах, то говорят, что она точна.

Приведем примеры, иллюстрирующие введенную терминологию.

1. Последовательность $0 \to N \xrightarrow{f} M$ (первое отображение, очевидно, нулевое) точна тогда и только тогда, когда $\mathrm{Ker}\, f = 0$, т. е. $f$ — мономорфизм. Аналогично последовательность $M \xrightarrow{g} N \to 0$ точна тогда и только тогда, когда $g$ — эпиморфизм.

2. Выясним, что означает точность последовательности $0 \to N \xrightarrow{f} M \xrightarrow{g} L$. Точность в члене $N$, как и выше, означает мономорфность $f$. Иными словами, $N$ можно рассматривать (отождествляя его с $\mathrm{Im}\, f$) как подмодуль в $M$. Точность же в члене $M$ означает, что $\mathrm{Im}\, f = \mathrm{Ker}\, g$, т. е. $N$ можно отождествить с ядром гомоморфизма $g$.

Аналогично точность последовательности $N \xrightarrow{f} M \xrightarrow{g} L \to 0$ означает, что $g$ есть эпиморфизм, при помощи которого $L$ можно отождествить с фактормодулем $M/\operatorname{Im} f$ (этот фактормодуль называется к о я д р о м гомоморфизма $f$ и обозначается $\operatorname{Coker} f$).

3. Наконец, точность последовательности

$$0 \to N \xrightarrow{f} M \xrightarrow{g} L \to 0$$

означает, что $f$ есть мономорфизм, а $g$ — эпиморфизм, причем если отождествить $N$ с подмодулем $M$ (при помощи мономорфизма $f$), то $L$ отождествляется с фактормодулем $M/N$.

4. Переформулируем на языке диаграмм и точных последовательностей одно из определений проективного модуля (см. теорему III.3.5): модуль $P$ проективен тогда и только тогда, когда любую диаграмму вида

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow{g} & N & \to & 0 \end{array}$$

с точной строкой можно дополнить до коммутативной диаграммы

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle \bar{f}} & \downarrow{\scriptstyle f} & & \\ M & \xrightarrow[g]{} & N & \longrightarrow & 0 \end{array}$$

(напомним, что точность в данном случае означает эпиморфность $g$, а коммутативность выражается равенством $f = g\bar{f}$).

Точная последовательность

$$0 \to N \xrightarrow{f} M \xrightarrow{g} L \to 0$$

называется р а с щ е п л я ю щ е й с я, если существуют такие гомоморфизмы $\bar{f}: M \to N$ и $\bar{g}: L \to M$, что $\bar{f}f = 1_N$, а $g\bar{g} = 1_L$. В силу предложения I.6.2, достаточно проверить существование только $\bar{f}$ (или только $\bar{g}$): в этом случае $M$ отождествляется с прямой суммой $N \oplus L$, причем $f$ — это естественное вложение $N \to N \oplus L$ (переводящее элемент $x \in N$ в пару $(x, 0)$), а $g$ — проекция $N \oplus L$ на второе слагаемое.

Сформулируем, наконец, одну диаграммную лемму, которую мы часто будем употреблять в дальнейшем.

**Лемма 2.1** (лемма о пяти гомоморфизмах). *Пусть в коммутативной диаграмме*

$$\begin{array}{ccccccccc} M_1 & \xrightarrow{f_1} & M_2 & \xrightarrow{f_2} & M_3 & \xrightarrow{f_3} & M_4 & \xrightarrow{f_4} & M_5 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow{\scriptstyle \varphi_4} & & \downarrow{\scriptstyle \varphi_5} \\ N_1 & \xrightarrow{g_1} & N_2 & \xrightarrow{g_2} & N_3 & \xrightarrow{g_3} & N_4 & \xrightarrow{g_4} & N_5 \end{array} \qquad (3)$$

*обе строки точны, а гомоморфизмы* $\varphi_i$, $i = 1, 2, 4, 5$, *суть изоморфизмы. Тогда и* $\varphi_3$ — *изоморфизм.*

Доказательство. Пусть элемент $x \in M_3$ лежит в ядре $\varphi_3$, т. е. $\varphi_3 x = 0$. Тогда $\varphi_4 f_3 x = g_3 \varphi_3 x = 0$ и, так как $\varphi_4$ — изоморфизм, $f_3 x = 0$, т. е. $x \in \operatorname{Ker} f_3$. Но, ввиду точности, $\operatorname{Ker} f_3 = \operatorname{Im} f_2$. Значит, найдется элемент $y \in M_2$, такой, что $x = f_2 y$. Кроме того, $g_2 \varphi_2 y = \varphi_3 f_2 y = \varphi_3 x = 0$. Значит, $\varphi_2 y \in \operatorname{Ker} g_2 = \operatorname{Im} g_1$, т. е. $\varphi_2 y = g_1 z$ для некоторого $z \in N_1$. Но $\varphi_1$ — также изоморфизм, поэтому $z = \varphi_1 u$, где $u \in M_1$ и $\varphi_2 f_1 u = g_1 \varphi_1 u = g_1 z = \varphi_2 y$, откуда $f_1 u = y$ и $x = f_2 y = f_2 f_1 u = 0$ (снова из-за точности). Итак, $\operatorname{Ker} \varphi_3 = 0$, т. е. $\varphi_3$ — мономорфизм.

Выберем теперь произвольный элемент $a \in N_3$. Поскольку $\varphi_4$ — изоморфизм, найдется $b \in M_4$, такой, что $\varphi_4 b = g_3 a$. Кроме того, $\varphi_5 f_4 b = g_4 \varphi_4 b = g_4 g_3 a = 0$, значит, $f_4 b = 0$ и $b \in \operatorname{Ker} f_4 = \operatorname{Im} f_3$, т. е. $b = f_3 c$, где $c \in M_3$. Положим $\bar{a} = a - \varphi_3 c$. Так как $g_3 \varphi_3 c = \varphi_4 f_3 c = \varphi_4 b = g_3 a$, $g_3 \bar{a} = 0$, т. е. $\bar{a} \in \operatorname{Ker} g_3 = \operatorname{Im} g_2$. Пусть $\bar{a} = g_2 d$, где $d \in N_2$. Выберем $\bar{c} \in M_2$ так, чтобы $d = \varphi_2 \bar{c}$. Тогда $\varphi_3 f_2 \bar{c} = g_2 \varphi_2 \bar{c} = g_2 d = \bar{a}$, откуда $a = \bar{a} + \varphi_3 c = \varphi_3 (f_2 \bar{c} + c) \in \operatorname{Im} \varphi_3$. Итак, $\varphi_3$ — эпиморфизм, а потому и изоморфизм.

Чаще всего встречаются такие случаи применения леммы о пяти гомоморфизмах.

1) Дана коммутативная диаграмма

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

с точными строками, причем $\varphi_1$ и $\varphi_3$ — изоморфизмы. Тогда и $\varphi_2$ — изоморфизм (это следует из леммы 2.1, если дополнить нашу диаграмму тождественными отображениями нулевых модулей до диаграммы вида (3)).

2) Дана коммутативная диаграмма

$$\begin{array}{ccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 \end{array}$$

с точными строками, причем $\varphi_1$ и $\varphi_2$ — изоморфизмы. Тогда и $\varphi_3$ — изоморфизм (нужно дополнить нашу диаграмму до диаграммы

$$\begin{array}{ccccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \downarrow & & \downarrow \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

тождественными отображениями).

3) Аналогично, если в коммутативной диаграмме с точными строками

$$\begin{array}{ccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 \\ & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} \\ 0 & \longrightarrow & N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 \end{array}$$

$\varphi_2$ и $\varphi_3$ — изоморфизмы, то и $\varphi_1$ — изоморфизм.

## § 3. Тензорные произведения

В этом параграфе мы введем новый важный функтор на категории модулей — тензорное произведение модулей.

Пусть $A$ — некоторая алгебра, $M$ — правый и $N$ — левый $A$-модули. В векторном пространстве $M \otimes N$ рассмотрим подпространство $T$, порожденное всеми элементами вида $xa \otimes y - x \otimes ay$, где $x \in M$, $y \in N$, $a \in A$. Факторпространство $(M \otimes N)/T$ называется тензорным произведением модулей $M$ и $N$ над алгеброй $A$ и обозначается $M \otimes_A N$. Обозначим через $\pi$ естественную проекцию $M \otimes N \to M \otimes_A N$. Композиция $\pi$ с билинейным отображением $\otimes : M \times N \to M \otimes N$ (переводящим $(x, y)$ в $x \otimes y$) дает билинейное отображение $\otimes_A : M \times N \to M \otimes_A N$. Образом $(x, y)$ при этом отображении является $x \otimes_A y = \pi(x \otimes y)$.

Отображение $\otimes_A$ обладает дополнительным свойством, которое мы будем называть «внутренней $A$-билинейностью»: $xa \otimes_A y = x \otimes_A ay$. Более того, так же как $\otimes$ является универсальным билинейным отображением, $\otimes_A$ является универсальным внутренне $A$-билинейным отображением в смысле следующего утверждения.

**Теорема 3.1.** *Пусть $F : M \times N \to V$ — внутренне $A$-билинейное отображение в произвольное векторное пространство $V$. Тогда существует единственное линейное отображение $f : M \otimes_A N \to V$, такое, что $F(x, y) = f(x \otimes_A y)$ для любых $x \in M$ и $y \in N$.*

Доказательство. Поскольку $F$ билинейно, найдется единственное линейное отображение $\varphi : M \otimes N \to V$, такое, что $F(x, y) = \varphi(x \otimes y)$ для любых $x \in M$, $y \in N$ (теорема IV.2.1). Но $\varphi(xa \otimes y - x \otimes ay) = \varphi(xa \otimes y) - \varphi(x \otimes ay) = F(xa, y) -$

$= F(x, ay) = 0$ ввиду внутренней $A$-билинейности $F$. Поэтому $T \subset \operatorname{Ker} \varphi$ и $\varphi$ индуцирует единственное отображение $f: M \otimes_A N \to V$, такое, что $\varphi = f\pi$, или, что то же, $f(x \otimes_A y) = f\pi(x \otimes y) = \varphi(x \otimes y) = F(x, y)$.

Очевидно, универсальное внутренне $A$-билинейное отображение единственно с точностью до канонического изоморфизма. Универсальность позволяет сравнительно просто установить основные свойства тензорного умножения.

**Предложение 3.2.** *Для любой пары гомоморфизмов $A$-модулей $f: M \to M'$ и $g: N \to N'$ существует единственное линейное отображение $f \otimes_A g: M \otimes_A N \to M' \otimes_A N'$, такое, что $(f \otimes_A g)(x \otimes_A y) = fx \otimes_A gy$. Если $f': M' \to M''$ и $g': N' \to N''$ — другая пара гомоморфизмов, то $(f' \otimes_A g')(f \otimes_A g) = f'f \otimes_A g'g$.*

Доказательство. Рассмотрим отображение $F: M \times N \to M' \otimes_A N'$, такое, что $F(x, y) = fx \otimes_A gy$. Легко проверить, что $F$ — это внутренне $A$-билинейное отображение. Поэтому существует единственное отображение $f \otimes_A g: M \otimes_A N \to M' \otimes_A N'$, такое, что $(f \otimes_A g)(x \otimes_A y) = F(x, y) = fx \otimes_A gy$. Второе утверждение тривиально.

Указанное свойство позволяет рассматривать тензорное произведение как функтор в категории модулей. Точнее, зафиксируем левый $A$-модуль $N$ и построим функтор $\otimes_A N: \text{mod-}A \to \text{Vect}$, сопоставляя всякому правому $A$-модулю $M$ векторное пространство $M \otimes_A N$, а всякому гомоморфизму $f: M \to M'$ — линейное отображение $f \otimes_A 1: M \otimes_A N \to M' \otimes_A N$. Выполнение аксиом функтора тогда следует из предложения 3.2. Аналогично можно построить функтор $M \otimes_A: A\text{-mod} \to \text{Vect}$ (при фиксированном правом $A$-модуле $M$).

Функториальность тензорного произведения позволяет иногда превратить $M \otimes_A N$ снова в модуль. Пусть, например, $N$ является $A$-$B$-бимодулем (или, как часто говорят, дана ситуация ${}_AM_A$, ${}_AN_B$). Тогда каждый элемент $b \in B$ индуцирует гомоморфизм $A$-модулей $N \to N$, переводящий элемент $y \in N$ в $yb$, и, следовательно, гомоморфизм векторных пространств $M \otimes_A N \to M \otimes_A N$, переводящий $x \otimes_A y$ в $x \otimes_A yb$. Очевидно, тем самым $M \otimes_A N$ превращается в $B$-модуль. Аналогично в ситуации ${}_BM_A$, ${}_AN$ (т. е. $M$ есть $B$-$A$-бимодуль, $N$ — левый $A$-модуль) $M \otimes_A N$ превращается в левый $B$-модуль, если положить $b(x \otimes_A y) = bx \otimes_A y$. Наконец, в ситуации ${}_BM_A$, ${}_AN_C$ тензорное произведение $M \otimes_A N$ превращается в $B$-$C$-бимодуль. Это позволяет итерировать операцию тензорного умножения, рассматривая произведения трех и более модулей (в подходящей ситуации). При этом, как показывает следующее утверждение, порядок, в котором выполняется перемножение, не существен.

**Предложение 3.3.** *В ситуации* $M_A$, ${}_AN_B$, ${}_BL$ *существует единственный изоморфизм*

$$(M \otimes_A N) \otimes_B L \xrightarrow{\sim} M \otimes_A (N \otimes_B L),$$

*переводящий* $(x \otimes_A y) \otimes_B z$ *в* $x \otimes_A (y \otimes_B z)$.

Доказательство. Фиксируем элемент $z \in L$ и определим отображение $F_z : M \times N \to M \otimes_A (N \otimes_B L)$, полагая $F_z(x, y) = x \otimes_A (y \otimes_B z)$. Очевидно, оно будет внутренне $A$-билинейным, и потому существует однозначно определенное линейное отображение $f_z : M \otimes_A N \to M \otimes_A (N \otimes_B L)$, переводящее $x \otimes_A y$ в $x \otimes_A (y \otimes_B z)$. Меняя $z$, получаем внутренне $B$-билинейное отображение $F : (M \otimes_A N) \times L \to M \otimes_A (N \otimes_B L)$, переводящее пару $(x \otimes_A y, z)$ в $x \otimes_A (y \otimes_B z)$. Оно однозначно пропускается через линейное отображение $f : (M \otimes_A N) \otimes_B L \to M \otimes_A (N \otimes_B L)$, такое, что $f(x \otimes_A y) \otimes_B z = x \otimes_A (y \otimes_B z)$. Аналогично строится линейное отображение $g : M \otimes_A (N \otimes_B L) \to (M \otimes_A N) \otimes_B L$, переводящее $x \otimes_A (y \otimes_B z)$ в $(x \otimes_A y) \otimes_B z$. Поскольку, очевидно, всевозможные элементы вида $x \otimes_A (y \otimes_B z)$ (соответственно, $(x \otimes_A y) \otimes_B z$) порождают пространство $M \otimes_A (N \otimes_B L)$ (соответственно, $(M \otimes_A N) \otimes_B L$), $f$ и $g$ — взаимно обратные отображения, что и требовалось доказать.

Легко видеть, что в ситуации ${}_CM_A$, ${}_AN_B$, ${}_BL_D$ построенный изоморфизм будет также изоморфизмом $C$-$D$-бимодулей.

Аналогично доказывается утверждение, устанавливающее связь между функторами $\otimes$ и Hom.

Заметим, что, например, в ситуации ${}_BM_A$, $N_A$ пространство $\mathrm{Hom}_A(M, N)$ превращается в правый $B$-модуль, если положить $(fb)(m) = f(bm)$. Аналогично в ситуации $M_A$, ${}_BN_A$ $\mathrm{Hom}_A(M, N)$ превращается в левый $B$-модуль, а в ситуации ${}_BM_A$, ${}_CN_A$ — в $C$-$B$-бимодуль. При этом имеет место

**Предложение 3.4** («формула сопряженности»). *В ситуации* $M_A$, ${}_AN_B$, $L_B$ *существует единственный изоморфизм*

$$\mathrm{Hom}_B(M \otimes_A N, L) \xrightarrow{\sim} \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, L)),$$

*переводящий гомоморфизм* $\varphi : M \otimes_A N \to L$ *в гомоморфизм* $\bar{\varphi} : M \to \mathrm{Hom}_B(N, L)$, *такой, что* $\bar{\varphi}(x)(y) = \varphi(x \otimes_A y)$.

Доказательство. То, что $\bar{\varphi}$ есть гомоморфизм $A$-модулей, проверяется тривиально. Построим обратное отображение. Пусть $\psi : M \to \mathrm{Hom}_B(N, L)$ есть гомоморфизм $A$-модулей. Тогда, как нетрудно убедиться, отображение $M \times N \to L$, переводящее $(x, y)$ в $\psi(x)(y)$, внутренне $A$-билинейно и потому определяет отображение $\bar{\psi} : M \otimes_A N \to L$, такое, что $\bar{\psi}(x \otimes_A y) = \psi(x)(y)$. Легко проверить,

что $\bar{\psi}$ — гомоморфизм $B$-модулей и так построенные отображения $\mathrm{Hom}_B(M \otimes_A N, L) \rightleftarrows \mathrm{Hom}_A(M, \mathrm{Hom}_B(N, L))$ взаимно обратны.

Важными свойствами функторов $\otimes$ и Hom являются так называемые «свойства точности».

**Предложение 3.5.** (а) *Последовательность $A$-модулей*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \tag{1}$$

*точна тогда и только тогда, когда для любого $A$-модуля $N$ точна последовательность*

$$0 \to \mathrm{Hom}_A(N, M_1) \xrightarrow{h_N(f)} \mathrm{Hom}_A(N, M_2) \xrightarrow{h_N(g)} \mathrm{Hom}_A(N, M_3). \tag{2}$$

(б) *Последовательность $A$-модулей*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0 \tag{1'}$$

*точна тогда и только тогда, когда для любого $A$-модуля $N$ точна последовательность*

$$0 \to \mathrm{Hom}_A(M_3, N) \xrightarrow{h^0_N(g)} \mathrm{Hom}_A(M_2, N) \xrightarrow{h^0_N(f)} \mathrm{Hom}_A(M_1, N). \tag{2'}$$

Доказательство. Предположим, что последовательность (1) точна. Тогда $f$ — мономорфизм, и если $h_N(f)(\varphi) = f\varphi = 0$, где $\varphi : N \to M_1$, то и $\varphi = 0$, т. е. $h_N(f)$ — мономорфизм и последовательность (2) точна в члене $\mathrm{Hom}_A(N, M_1)$. Поскольку $\mathrm{Im}\, f = \mathrm{Ker}\, g$, $gf = 0$, а потому $h_N(g)\, h_N(f) = h_N(gf) = 0$. Значит, $\mathrm{Im}\, h_N(f) \subset \mathrm{Ker}\, h_N(g)$. Пусть теперь $\varphi \in \mathrm{Ker}\, h_N(g)$, где $\varphi : N \to M_2$. Иными словами, $h_N(g)(\varphi) = g\varphi = 0$. Тогда $\mathrm{Im}\, \varphi \subset \mathrm{Ker}\, g = \mathrm{Im}\, f$. Но гомоморфизм устанавливает изоморфизм $M_1 \simeq \mathrm{Im}\, f$, потому $\varphi$ можно представить как композицию $f\psi$, где $\psi : N \to M_1$, т. е. $\varphi = h_N(f)(\psi) \in \mathrm{Im} h_N(f)$ и последовательность (2) точна в члене $\mathrm{Hom}_A(N, M_2)$.

Наоборот, пусть последовательность (2) точна для любого $N$. Подставляя в качестве $N$ $\mathrm{Ker}\, f$, мы видим, что отображение $\mathrm{Hom}_A(\mathrm{Ker}\, f, M_1) \to \mathrm{Hom}_A(\mathrm{Ker}\, f, M_2)$ мономорфно. Но если $\varphi$ — вложение $\mathrm{Ker}\, f$ в $M_1$, то $f\varphi = 0$, откуда $\varphi = 0$, т. е. $\mathrm{Ker}\, f = 0$ и $f$ — мономорфизм.

Пусть теперь $N = M_1$. Тогда $f = f1_N = h_N(f)(1_N) \in \mathrm{Im}\, h_N(f) = \mathrm{Ker}\, h_N(g)$ и потому $gf = h_N(g)(f) = 0$, т. е. $\mathrm{Im}\, f \subset \mathrm{Ker}\, g$. Наконец, положим $N = \mathrm{Ker}\, g$, $\varphi$—вложение $N$ в $M_2$. Тогда $h_N(g)(\varphi) = g\varphi = 0$, значит, $\varphi \in \mathrm{Ker}\, h_N(g) = \mathrm{Im}\, h_N(f)$, т. е. $\varphi = f\psi$, откуда $\mathrm{Ker}\, g = \mathrm{Im}\, \varphi \subset \mathrm{Im}\, f$ и последовательность (1) точна.

Аналогично доказывается и утверждение (б).

Используя формулу сопряженности, можно перенести свойства точности и на тензорное произведение.

**Предложение 3.6.** *Если последовательность правых $A$-модулей*

$$M_1 \to M_2 \to M_3 \to 0 \tag{3}$$

*точна, то точна и последовательность $B$-модулей*

$$M_1 \otimes_A N \to M_2 \otimes_A N \to M_3 \otimes_A N \to 0 \tag{4}$$

*для любого $A$-$B$-бимодуля $N$.*

Доказательство. По предложению 3.5 нам нужно проверить точность последовательности

$$0 \to \mathrm{Hom}_B(M_3 \otimes_A N, L) \to \mathrm{Hom}_B(M_2 \otimes_A N, L) \to \mathrm{Hom}_B(M_1 \otimes_A N, L)$$

для любого $B$-модуля $L$. Но по предложению 3.4 эту последовательность можно переписать так:

$$0 \to \mathrm{Hom}_A(M_3, \mathrm{Hom}_B(N, L)) \to \mathrm{Hom}_A(M_2, \mathrm{Hom}_B(N, L)) \to$$

$$\to \mathrm{Hom}_A(M_1, \mathrm{Hom}_B(N, L)),$$

после чего ее точность сразу следует из предложения 3.5.

Указанные свойства часто выражают словами: «функтор Hom точен слева, а $\otimes$ — справа», или, вернее, функторы $h_N$ и $h_N^0$ точны слева, а функторы $\otimes_A N$ — справа. Конечно, и функтор $M \otimes_A$ точен справа (доказательство аналогично предложению 3.6).

Отметим в заключение следующий простой факт.

**Предложение 3.7.** *Отображение $M \to M \otimes_A A$, переводящее элемент $m$ в $m \otimes_A 1$, является изоморфизмом правых $A$-модулей. Отображение $N \to A \otimes_A N$, переводящее $n$ в $1 \otimes_A n$, является изоморфизмом левых $A$-модулей.*

Для доказательства достаточно заметить, что отображение $M \times A \to M$, переводящее $(m, a)$ в $ma$, очевидно, внутренне билинейно и индуцированное им отображение $M \otimes_A A \to M$ является гомоморфизмом, обратным к указанному отображению $M \to M \otimes_A A$.

## § 4. Теорема Мориты

В этом параграфе мы установим, для каких алгебр $A$ и $B$ категории модулей mod-$A$ и mod-$B$ «одинаково устроены». Для этого прежде всего нужно придать словам «одинаково устроены» точный смысл, т. е. указать, какие категории мы будем считать одинаковыми. Попытка определить изоморфизм категорий $C$ и $C'$ как такой функтор $F : C \to C'$, для которого существует обратный $G : C' \to C$, т. е. $GF = 1_C$, $FG = 1_{C'}$, оказывается неудачной. Во-первых, среди естественно возникающих функторов таковых, как правило, не имеется, а во-вторых, некоторые категории, «одинаковые» с интуитивной точки зрения, оказываются в этом смысле неизоморфными. Примером могут служить ка-

тегории матриц Mat и векторных пространств Vect. Причина такого явления ясна: категория матриц описывает векторные пространства «с точностью до изоморфизма», в то время как в категории Vect у каждого пространства существует много «изоморфных копий». Поэтому между ними никак нельзя установить взаимно однозначное соответствие.

Более естественным оказывается подход, использующий не равенство, а изоморфизм функторов. Дадим точные определения.

Пусть $F$ и $G$ — два функтора из категории $C$ в категорию $C'$. Морфизмом функтора $F$ в функтор $G$ называется отображение $\varphi$, сопоставляющее каждому объекту $X \in \mathrm{Ob}\, C$ морфизм $\varphi(X) : F(X) \to G(X)$ (категории $C'$!), причем так, что для любого морфизма $f : X \to Y$ категории $C$ коммутативна следующая диаграмма:

$$\begin{array}{ccc} F(X) & \xrightarrow{\varphi(X)} & G(X) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(Y) & \xrightarrow{\varphi(Y)} & G(Y) \end{array}$$

Мы будем писать $\varphi : F \to C$.

Если задан еще функтор $H : C \to C'$ и морфизм функторов $\psi : D \to H$, то можно определить композицию $\psi\varphi$: $F \to H$, полагая $(\psi\varphi)(X) = \psi(X)\,\varphi(X)$. Легко видеть, что при таком определении множество функторов из категории $C$ в категорию $C'$ и их морфизмов образуют категорию функторов $\mathrm{Func}(C, C')$. Кроме того, морфизм $\varphi$: $F \to G$ является изоморфизмом в этой категории тогда и только тогда, когда для любого объекта $X \in \mathrm{Ob}\, C$ морфизм $\varphi(X)$ является изоморфизмом. В этом случае говорят, что $\varphi$ — изоморфизм функторов, и пишут $\varphi : F \xrightarrow{\sim} G$, или $F \simeq G$.

Так, нетрудно убедиться, что построенные в предложениях 3.3 и 3.4 изоморфизмы являются на самом деле изоморфизмами соответствующих функторов.

Эквивалентностью категорий $C$ и $C'$ называется пара функторов $F : C \to C'$ и $G : C' \to C$, таких, что $GF \simeq 1_C$, $FG \simeq 1_{C'}$. Если такая эквивалентность существует, категории $C$ и $C'$ называются эквивалентными.

В дальнейшем нам понадобятся следующие очевидные свойства эквивалентностей категорий.

**Предложение 4.1.** *Если пара функторов $F : C \to C'$ и $G : C' \to C$ является эквивалентностью категорий, то:*

(1) *отображение* $\mathrm{Hom}_C(X, Y) \to \mathrm{Hom}_{C'}(F(X), F(Y))$, *переводящее $f$ в $F(f)$, взаимно однозначно;*

(1′) *отображение* $\mathrm{Hom}_{C'}(U, V) \to \mathrm{Hom}_C(G(U), G(V))$, *переводящее $g$ в $G(g)$, взаимно однозначно;*

(2) *морфизм $f \in \mathrm{Mor}\, C$ является изоморфизмом тогда и только тогда, когда $F(f)$ изоморфизм;*

(2′) *морфизм* $g \in \mathrm{Mor}\, C'$ *является изоморфизмом тогда и только тогда, когда* $G(g)$ *изоморфизм*;

(3) *каждый объект* $X \in \mathrm{Ob}\, C$ *изоморфен объекту вида* $G(U)$, *где* $U \in \mathrm{Ob}\, C'$;

(3′) *каждый объект* $U \in \mathrm{Ob}\, C'$ *изоморфен объекту вида* $F(X)$, *где* $X \in \mathrm{Ob}\, C$.

Мы докажем утверждения (1) и (1′), оставляя прочие читателю в качестве легкого упражнения.

Пусть $f : X \to Y$ — морфизм категории $C$. Обозначим через $\varphi$ изоморфизм функторов $GF \xrightarrow{\sim} 1_C$ и рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} GE(X) & \xrightarrow{\varphi(X)} & X \\ {\scriptstyle GF(f)}\downarrow & & \downarrow{\scriptstyle f} \\ GF(Y) & \xrightarrow{\varphi(Y)} & Y \end{array}$$

Поскольку $\varphi(X)$ — изоморфизм, то $f = \varphi(Y) GF(f) \varphi(X)^{-1}$. Значит, из того, что $F(f) = F(f')$, следует $f = f'$, т. е. отображение $\mathrm{Hom}_C(X, Y) \to \mathrm{Hom}_{C'}(F(X), F(Y))$ инъективно. Аналогично инъективно и отображение $\mathrm{Hom}_{C'}(U, V) \to \mathrm{Hom}_C(G(U), G(V))$.

Рассмотрим теперь произвольный морфизм $g : F(X) \to F(Y)$. Пусть $f = \varphi(Y)\, G(g)\, \varphi(X)^{-1}$, $g' = F(f)$. Тогда, как и выше, $f = \varphi(Y)\, G(g')\, \varphi(X)^{-1}$, откуда, ввиду изоморфности $\varphi(X)$ и $\varphi(Y)$, $G(g) = G(g')$. Следовательно, $g = g' = F(f)$, т. е. отображение $\mathrm{Hom}_C(X, Y) \to \mathrm{Hom}_{C'}(F(X), F(Y))$ взаимно однозначно.

Перейдем к категориям модулей. Пусть пара функторов $F$, $G$ является эквивалентностью категорий mod-$A$ и mod-$B$. Объединяя предложение 4.1 с критерием точности (предложение 3.5), мы получим следующее предложение.

**Предложение 4.2.** (а) *Последовательность* $A$*-модулей*

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$$

*точна тогда и только тогда, когда точна последовательность* $B$*-модулей*

$$0 \to F(M_1) \xrightarrow{F(f)} F(M_2) \xrightarrow{F(g)} F(M_3).$$

(б) *Последовательность* $A$*-модулей*

$$M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

*точна тогда и только тогда, когда точна последовательность* $B$*-модулей*

$$F(M_1) \xrightarrow{F(f)} F(M_2) \xrightarrow{F(g)} F(M_3) \to 0.$$

(в) $A$*-модуль* $P$ *проективен тогда и только тогда, когда проективен* $B$*-модуль* $F(P)$.

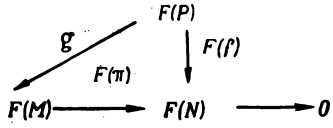
Доказательство. Мы докажем утверждение (в), оставляя (а) и (б) читателю. Для этого мы воспользуемся «диаграммным» определением проективности (см. § 2, пример 4). Предположим, что $F(P)$ проективен и пусть дана диаграмма $A$-модулей

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow f & & \\ M & \xrightarrow{\pi} & N & \to & 0 \end{array}$$

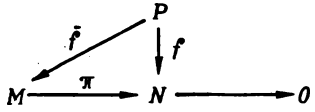
с точной строкой. Применяя функтор $F$, получим диаграмму $B$-модулей

$$\begin{array}{ccccc} & & F(P) & & \\ & & \downarrow F(f) & & \\ F(M) & \xrightarrow{F(\pi)} & F(N) & \to & 0 \end{array}$$

с точной (ввиду утверждения (б)) строкой. Ее можно дополнить до коммутативной диаграммы




причем ввиду предложения 4.1 $g = F(\bar{f})$ для некоторого морфизма $\bar{f} : P \to M$. Но тогда $F(\pi\bar{f}) = F(\pi)\,F(\bar{f}) = F(\pi)g = F(f)$, откуда $\pi\bar{f} = f$, т. е. диаграмма




коммутативна и $P$ проективен.

Наоборот, если $P$ проективен, то проективен и изоморфный ему модуль $GF(P)$, а тогда по уже доказанному проективен и $F(P)$.

**Следствие 4.3.** *Пусть $F$, $G$ — эквивалетность категорий* mod-$A$ *и* mod-$B$, $P = G(B)$. *Тогда $P$ — проективный $A$-модуль, причем $E_A(P) \simeq B$, и для любого $A$-модуля $M$ существует эпиморфизм $nP \to M$ (для некоторого $n$).*

В этом случае говорят, что $P$ — образующий $A$-модуль.

Доказательство. Проективность $P$ следует из проективности $B$-модуля $B$ и предложения 4.2. Далее, по предложению 4.1 $E_A(P) \simeq E_B(B) \simeq B$. Наконец, всякий $A$-модуль $M$ изоморфен модулю вида $G(N)$ для некоторого $B$-модуля $N$. Но существует эпи-

морфизм $nB \to N$, который индуцирует эпиморфизм $G(nB) \simeq nP \to$ $\to G(N) \simeq M$, что и требовалось доказать.

Пусть теперь дан проективный $A$-модуль $P$ и $B = E_A(P)$. В этом случае мы будем говорить, что $B$—минор алгебры $A$. Тогда можно построить функторы $F$: mod-$A \to$ mod-$B$ и $G$: mod-$B \to$ mod-$A$, полагая $F(M) = \mathrm{Hom}_A(P, M)$ и $G(N) = N \otimes_B P$ ($P$ рассматривается как левый $B$-модуль). Определим также функторные морфизмы $\varphi : 1_{\text{mod-}B} \to FG$ и $\psi : GF \to 1_{\text{mod-}A}$ следующим образом. Для всякого $B$-модуля $N$ за $\varphi(N)$ примем гомоморфизм $N \to \mathrm{Hom}_A(P, N \otimes_B P)$, переводящий элемент $x \in N$ в отображение $\bar{x} : P \to N \otimes_B P$, такое, что $\bar{x}(p) = p \otimes_B x$. Для всякого $A$-модуля $M$ за $\psi(M)$ примем гомоморфизм $\mathrm{Hom}_A(P, M) \otimes_B P \to M$, переводящий $f \otimes_B p$ (где $f \in$ $\in \mathrm{Hom}_A(P, M)$, $p \in P$) в $f(p) \in M$. Легко проверяется, что $\varphi$ и $\psi$ действительно являются морфизмами функторов.

Заметим, что, вообще говоря, не всякий $A$-модуль изоморфен модулю вида $G(N)$. Действительно, всегда существует эпиморфизм $f : nB \to N$. Пусть $N' = \mathrm{Ker}\, f$, $g$ — эпиморфизм $mB \to N'$. Тогда точна последовательность

$$mB \xrightarrow{g} nB \xrightarrow{f} N \to 0.$$

Следовательно, точна последовательность

$$G(mB) \xrightarrow{G(g)} G(nB) \xrightarrow{G(f)} G(N) \to 0.$$

Но $G(nB) \simeq nP$, $G(mB) \simeq mP$, т. е. если $M \simeq G(N)$, то существует точная последовательность вида

$$mP \to nP \to M \to 0. \tag{1}$$

Поэтому естественно рассматривать категорию mod-$P$, объектами которой являются те $A$-модули, для которых существуют точные последовательности вида (1), а морфизмами — всевозможные гомоморфизмы таких модулей.

**Теорема 4.4.** *Пара функторов $F = h_P$ и $G = \otimes_B P$ является эквивалентностью категорий* mod-$P$ *и* mod-$B$.

Доказательство. Покажем, что $\varphi : 1_{\text{mod-}B} \xrightarrow{\sim} FG$, а $\psi : GF \xrightarrow{\sim}$ $\xrightarrow{\sim} 1_{\text{mod-}P}$. Действительно, $\varphi(B)$ — это естественный изоморфизм $B =$ $= \mathrm{Hom}_A(P, P) \xrightarrow{\sim} \mathrm{Hom}_A(P, B \otimes_B P) = FG(B)$. Тогда $\varphi(nB)$, очевидно, также изоморфизм. Но, как мы уже видели, для любого $B$-модуля $N$ можно построить точную последовательность

$$mB \xrightarrow{g} nB \xrightarrow{f} N \to 0.$$

Применим к ней функтор $FG$. Поскольку $G$ — точный справа функтор, а $F$ точен (так как $P$ проективен), получим коммутативную диаграмму с точными строками

$$\begin{array}{ccccccc} & & mB & \xrightarrow{g} & nB & \xrightarrow{f} & N \to 0 \\ & & \varphi(mB)\downarrow & & \varphi(nB)\downarrow & & \varphi(N)\downarrow \\ FG(mB) & \xrightarrow[FG(g)]{} & FG(nB) & \xrightarrow[FG(f)]{} & FG(N) & \to 0 & \end{array}$$

Поскольку $\varphi(mB)$ и $\varphi(nB)$ — изоморфизмы, из леммы о пяти гомоморфизмах (лемма 2.1) следует, что и $\varphi(N)$ — изоморфизм, что и требовалось доказать.

Аналогично можно показать, что для любого модуля $M \in \mathrm{mod}\text{-}P$ гомоморфизм $\psi(M)$ также является изоморфизмом.

Из теоремы 4.4 и следствия 4.3 вытекает следующий результат.

**Следствие 4.5** (теорема Мориты). *Категории* mod-$A$ *и* mod-$B$ *эквивалентны тогда и только тогда, когда существует такой проективный образующий $A$-модуль $P$, что $E_A(P) \simeq B$. В этом случае эквивалентность категорий осуществляет пара функторов $F = h_P$ и $G = \otimes_B P$.*

Как показал Морита, на самом деле всякая эквивалентность категорий имеет вид, указанный в этом следствии.

Условие эквивалентности категорий имеет такой простой смысл. Пусть $A \simeq k_1P_1 \oplus \ldots \oplus k_tP_t$ — разложение регулярного $A$-модуля в прямую сумму главных, причем $P_i \not\simeq P_j$ при $i \neq j$. Если $P$ — проективный образующий $A$-модуль, то существует эпиморфизм $nP \to A$, откуда $nP \simeq A \oplus M$. Тогда по теореме Крулля—Шмидта в $P$ обязаны входить прямыми слагаемыми все модули $P_1, \ldots, P_t$. Поскольку всякий проективный модуль есть прямая сумма главных, мы видим, что проективные образующие — это такие проективные модули, в которые входят прямыми слагаемыми все главные $A$-модули. Учитывая теорему III.5.6, мы видим, что категории mod-$A$ и mod-$B$ эквивалентны тогда и только тогда, когда алгебры $A$ и $B$ однотипны, т. е. их базисные алгебры изоморфны. В частности, теорема Мориты дает возможность при изучении модулей ограничиться случаем, когда $A$ — приведенная алгебра. Кроме того, результаты § 5 гл. III позволяют обозреть все алгебры, категории модулей над которыми эквивалентны.

## § 5. Тензорные и наследственные алгебры

В этом параграфе мы дадим обобщение конструкции «алгебры путей» (§ 6 гл. III). Таким обобщением является тензорная алгебра бимодуля.

Пусть $B$ — некоторая алгебра, $V$ — бимодуль над $B$. Тогда $V^{\otimes 2} = V \otimes_B V$ также можно рассматривать как $B$-бимодуль. Итерируя эту процедуру, построим $B$-бимодуль $V^{\otimes k}$ для всех $k \geqslant 2$, полагая $V^{\otimes k} = V^{\otimes(k-1)} \otimes_B V$. Кроме того, удобно считать, что $V^{\otimes 0} =$

$= B$, а $V^{\otimes 1} = V$. Из ассоциативности тензорного умножения непосредственно следует, что $V^{\otimes k} \otimes_B V^{\otimes m} \simeq V^{\otimes (k+m)}$. В дальнейшем мы будем отождествлять $V^{\otimes k} \otimes_B V^{\otimes m}$ и $V^{\otimes (k+m)}$ при помощи этого изоморфизма.

Рассмотрим теперь прямую сумму $T(V) = \bigoplus_{k=0}^{\infty} V^{\otimes k}$. Элементы $T(V)$ — конечные суммы $\sum_k t_k$, где $t_k \in V^{\otimes k}$. Построенный выше изоморфизм дает возможность для элементов $t_k \in V^{\otimes k}$ и $t_m \in V^{\otimes m}$ определить умножение, полагая $t_k t_m = t_k \otimes_B t_m \in V^{\otimes (k+m)}$. Это умножение по линейности можно распространить на все $T(V)$, которые таким образом превращаются в алгебру (вообще говоря, бесконечномерную). Она называется тензорной алгеброй $B$-бимодуля $V$.

По построению $T(V)$ содержит подалгебру $B = V^{\otimes 0}$ и $B$-подбимодуль $V = V^{\otimes 1}$. Более того, как показывает следующая теорема, $T(V)$ является универсальной алгеброй с этим свойством.

**Теорема 5.1.** *Пусть* $\varphi : B \to A$ *— гомоморфизм алгебр, а* $f : V \to A$ *— гомоморфизм* $B$*-бимодулей*[17]. *Тогда существует единственный гомоморфизм алгебр* $F : T(V) \to A$, *ограничение которого на* $B$ *совпадает с* $\varphi$, *а на* $V$ *— с* $f$.

Доказательство. Гомоморфизм $f$ индуцирует гомоморфизмы $B$-бимодулей $f^{\otimes k} : V^{\otimes k} \to A^{\otimes k}$. Но умножение в алгебре $A$ индуцирует гомоморфизм бимодулей $A^{\otimes k} \to A$, при котором образом $a_1 \otimes_B a_2 \otimes_B \ldots \otimes_B a_k$ является $a_1 a_2 \ldots a_k$. Итак, мы получаем набор гомоморфизмов $f_k : V^{\otimes k} \to A$, таких, что $f_k(v_1 \otimes_B \ldots \otimes_B v_k) = f(v_1) f(v_2) \ldots f(v_k)$. Очевидно, тем самым мы получаем гомоморфизм алгебр $F : T(V) \to A$ (нужно еще положить $f_0 = \varphi$, $f_1 = f$). Единственность $F$ непосредственно следует из того, что $T(V)$ порождается (как алгебра) элементами из $B$ и $V$.

Как обычно, универсальное свойство, сформулированное в теореме 5.1, определяет алгебру $T(V)$ с точностью до изоморфизма.

В алгебре $T(V)$ естественно выделяется идеал $J = J(V) = \bigoplus_{k=1}^{\infty} V^{\otimes k}$. Мы будем называть его фундаментальным идеалом тензорной алгебры.

Идеалы $I \subset T(V)$, такие, что $J^2 \supset I \supset J^k$ для некоторого $k$, мы будем называть правильными.

Наиболее важным для нас будет случай, когда алгебра $B$ полупроста (и даже сепарабельна). Оказывается, в этом случае тензорные алгебры $B$-бимодулей играют роль «универсальных накрывающих», аналогично тому, что имеет место в расщепимом случае для алгебр путей (см. теорему III.6.6).

[17] $A$ становится B-бимодулем, если положить $b_1 a b_2 = \varphi(b_1)\, a \varphi(b_2)$ для любых $a \in A$, $b_1, b_2 \in B$.

**Теорема 5.2.** *Пусть $A$ — конечномерная алгебра, $R = \operatorname{rad} A$, $B = A/R$. Предположим, что алгебра $B$ сепарабельна. Тогда алгебра $A$ изоморфна факторалгебре алгебры $T(V)$, где $V = R/R^2$, по некоторому правильному идеалу.*

Доказательство. По теореме Веддербёрна—Мальцева (теореме VI.2.1) в $A$ содержится подалгебра $\overline{A} \simeq B$. Это дает возможность определить мономорфизм алгебр $\varphi : B \to A$ и рассматривать $A$ как $B$-бимодуль, Кроме того, $A = \overline{A} \oplus R$ (как $B$-бимодуль). Поскольку $B \otimes B^\circ$ — полупростая алгебра (теорема VI.1.1), всякий $B$-бимодуль полупрост. В частности, в $R$ содержится такой $B$-подбимодуль $\overline{R}$, что $R = \overline{R} \oplus R^2$. Очевидно, тогда $\overline{R} \simeq V$ и этим изоморфизмом можно воспользоваться для определения мономорфизма $B$-бимодулей $f : V \to R$.

По теореме 5.1 существует гомоморфизм $F : T(V) \to A$, который на $B$ совпадает с $\varphi$, а на $V$ — с $f$. Тогда $F$ индуцирует изоморфизм алгебр $T(V)/J^2 \simeq A/R^2$. Значит, $I = \operatorname{Ker} F \subset J^2$. С другой стороны, $F(J) \subset R$. Значит, $F(J^k) \subset R^k$ и, поскольку $R$ нильпотентен, $F(J^k) = 0$ для некоторого $k$, т. е. $J^k \subset I$ и $I$ — правильный идеал.

Заметим теперь, что $F(B) = \varphi(B) = \overline{A}$, а $F(V) = f(V) = \overline{R}$. Следовательно, всякий элемент $r \in R$ имеет вид $r = F(x) + r'$, где $x \in J$, $r' \in R^2$. Отсюда, очевидно, следует, что всякий элемент $r \in R^i$ имеет вид $F(x) + r'$, где $x \in J^i$, а $r' \in R^{i+1}$. Ввиду нильпотентности радикала мы получаем равенство $F(J) = R$. Значит, $F$— эпиморфизм и $A \simeq T(V)/I$, что и требовалось доказать.

Пару $(B, V)$, где $B = A/R$, $V = R/R^2$, мы будем называть типом алгебры $A$. Если $B$ — сепарабельная алгебра, будем говорить, что $A$ — алгебра сепарабельного типа. Очевидно, тип определяет схему $S(A)$ алгебры $A$ (см. § 6 гл. III). Эту схему мы будем поэтому называть схемой типа $(B, V)$.

Очевидно, если $B$ — полупростая алгебра, $V$ — конечномерный $B$-бимодуль, то всякая факторалгебра $T(V)/I$, где $I$ — правильный идеал, конечномерна и имеет тип $(B, V)$. В частности, факторалгебра $T(V)/J^2$ — это наименьшая (по размерности) алгебра данного типа.

Как мы уже говорили, алгебра $T(V)$, вообще говоря, бесконечномерна. Нетрудно указать условия, при которых она будет конечномерной.

**Предложение 5.3.** *Пусть $B$ — полупростая алгебра, $V$ — конечномерный $B$-бимодуль. Для того, чтобы алгебра $T(V)$ была конечномерной, необходимо и достаточно, чтобы схема типа $(B, V)$ не имела циклов.*

Доказательство. Очевидно, $T(V)$ конечномерна тогда и только тогда, когда $V^{\otimes m} = 0$ для некоторого $m$. Разложим $B$ в прямое произведение простых алгебр: $B = B_1 \times \ldots \times B_n$. Пусть $1 = e_1 + \ldots + e_n$ — соответствующее центральное разложение

единицы, $V_{ij} = e_i V e_j$. В схеме $S$ типа $(B, V)$ из точки $i$ в точку $j$ ведет стрелка тогда и только тогда, когда $V_{ij} \neq 0$. Заметим, что $V = \bigoplus_{i,j} V_{ij}$ (как $B$-бимодуль), причем $V_{ij} \otimes_B V_{kl} \neq 0$ тогда и только тогда, когда $V_{ij} \neq 0$, $V_{kl} \neq 0$, $j = k$. Поэтому $e_i V^{\otimes 2} e_j \neq 0$ тогда и только тогда, когда из точки $i$ в точку $j$ ведет путь длины 2. Аналогично $e_i V^{\otimes m} e_j \neq 0$ тогда и только тогда, когда из $i$ в $j$ ведет путь длины $m$, откуда и следует наше утверждение.

Применим развитую технику для описания наследственных алгебр, т. е. алгебр, все правые идеалы которых проективны (см. § 7 гл. III).

**Теорема 5.4.** *Конечномерная наследственная алгебра $A$ сепарабельного типа $(B, V)$ изоморфна $T(V)$. Наоборот, если в схеме типа $(B, V)$ нет циклов, то $T(V)$ — конечномерная наследственная алгебра.*

Доказательство. Проверим вначале, что $T = T(V)$ — наследственная алгебра. Заметим, что поскольку $T(V)/J \simeq B$ — полупростая алгебра, а $J^m = 0$ для некоторого $m$ (предложение 5.3), $J = \operatorname{rad} T$ (предложение III.1.13). Пусть $1 = e_1 + \ldots + e_n$ — минимальное разложение единицы алгебры $B$ (очевидно, оно будет и минимальным разложением единицы алгебры $T$).

Если $P_i = e_i T = \bigoplus_{k=0}^{\infty} e_i V^{\otimes k}$, то $P_i J = e_i J = \bigoplus_{k=1}^{\infty} e_i V^{\otimes k} = e_i V \otimes_B T$.

Но $e_i V \simeq \bigoplus_{j=1}^{n} s_j U_j$, где $U_j$ — простые $B$-модули, а тогда $P_i J \simeq \bigoplus_{j=1}^{n} s_j \times$ $\times (U_j \otimes_B T) \simeq \bigoplus_{j=1}^{n} s_j P_j$ — проективный модуль. Следовательно, $J = \bigoplus_{i=1}^{n} e_i J$ — проективный модуль и $T$ — наследственная алгебра (теорема III.7.1).

Ввиду теоремы 5.2 осталось показать, что если $A = T/I$ — наследственная алгебра, где $I$ — правильный идеал, то $I = 0$ (заметим, что по следствию III.7.3 в схеме наследственной алгебры нет циклов). Обозначим $R = J/I = \operatorname{rad} A$, $\tilde{P}_i = P_i/P_i I$ — главные $A$-модули. Индукцией по $k$ установим, что $R^k/R^{k+1} \simeq J^k/J^{k+1}$. База индукции $k = 1$ следует из того, что $I \subset J^2$.

Предположим, что $R^{k-1}/R^k \simeq J^{k-1}/J^k$, $k \geqslant 2$, и рассмотрим $\tilde{P} = P(R^{k-1}/R^k)$. Пусть $\tilde{P} \simeq \bigoplus_{i=1}^{n} s_i \tilde{P}_i$. По теореме III.3.7 $\tilde{P} = P(R^{k-1})$. Поскольку $R^{k-1}$ — проективный модуль, $\tilde{P} \simeq R^{k-1}$. Тогда $R^k \simeq \tilde{P}R$, а $R^k/R^{k+1} \simeq \tilde{P}R/\tilde{P}R^2$. Но, поскольку $R/R^2 \simeq J/J^2$, а $P = P(J^{k-1}/J^k) \simeq$ $\simeq \bigoplus_{i=1}^{n} s_i P_i$, отсюда вытекает, что $R^k/R^{k+1} \simeq PR/PR^2 \simeq J^k/J^{k+1}$, что

и требовалось доказать. Следовательно, $I \subset J^k$ для любого $k \geqslant 2$, откуда, ввиду нильпотентности $J$, $I = 0$. Теорема полностью доказана.

## *Упражнения к главе VIII*

**1.** Доказать, что каждая из следующих категорий эквивалентна своей дуальной категории:

а) категория конечномерных векторных пространств;

б) категория конечных абелевых групп. (У к а з а н и е: воспользоваться упражнением 5 к гл. VII.)

**2.** Пусть дана коммутативная диаграмма с точными строками

$$\begin{array}{ccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & M_4 \\ \downarrow{\scriptstyle \alpha_1} & & \downarrow{\scriptstyle \alpha_2} & & \downarrow{\scriptstyle \alpha_3} & & \downarrow{\scriptstyle \alpha_4} \\ N_1 & \longrightarrow & N_2 & \longrightarrow & N_3 & \longrightarrow & N_4 \end{array}$$

Доказать, что:

а) если $\alpha_1$ — эпиморфизм, а $\alpha_2$ и $\alpha_4$ — мономорфизмы, то и $\alpha_3$ — мономорфизм;

б) если $\alpha_4$ — мономорфизм, а $\alpha_1$ и $\alpha_3$ — эпиморфизмы, то и $\alpha_2$ — эпиморфизм.

**3. Лемма 3 × 3.** Доказать, что если в коммутативной диаграмме

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M_1 & \to & N_1 & \to & L_1 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M_2 & \to & N_2 & \to & L_2 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & M_3 & \to & N_3 & \to & L_3 & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

все столбцы и две какие-нибудь строки точны, то и третья строка точна.

**4.** Коммутативная диаграмма

$$\begin{array}{ccc} X & \xrightarrow{\bar{f}} & L \\ {\scriptstyle \bar{g}}\downarrow & & \downarrow{\scriptstyle g} \\ M & \xrightarrow{f} & N \end{array}$$

называется **декартовым квадратом**, если для любой коммутативной диаграммы

$$\begin{array}{ccc} Y & \xrightarrow{\xi} & L \\ {\scriptstyle \eta}\downarrow & & \downarrow{\scriptstyle g} \\ M & \xrightarrow{f} & N \end{array}$$

существует единственный гомоморфизм $\varphi : Y \to X$, такой, что $\xi = \bar{f}\varphi$, а $\eta = \bar{g}\varphi$.

Доказать, что любую пару гомоморфизмов $f : M \to L$ и $g : L \to N$ можно включить в декартов квадрат. (У к а з а н и е: рассмотреть в $M \oplus L$ подмодуль $\{(x, y) | f(x) = g(y)\}$.) Насколько единственный такой квадрат?

**5.** Пусть дана точная последовательность

$$0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$$

и произвольный гомоморфизм $\varphi : N' \to N$. Рассмотрим диаграмму

$$\begin{array}{ccccccccc} 0 & \to & L & \xrightarrow{f'} & M' & \xrightarrow{g'} & N' & \to & 0 \\ & & {\scriptstyle 1_L}\downarrow & & {\scriptstyle \varphi'}\downarrow & & {\scriptstyle \varphi}\downarrow & & \\ 0 & \to & L & \xrightarrow{f} & M & \xrightarrow{g} & N & \to & 0 \end{array}$$

где правый квадрат декартов, а $f'$ определяется равенствами $f = \varphi' f'$, $g' f' = 0$ (ввиду определения декартова квадрата эти равенства однозначно определяют $f'$). Доказать, что верхняя строка этой диаграммы точна (ее называют подъемом исходной точной последовательности вдоль $\varphi$).

6 (лемма Шануэля). Доказать, что если даны две точные последовательности

$$0 \to N_1 \to P_1 \xrightarrow{f_1} M \to 0,$$

$$0 \to N_2 \to P_2 \xrightarrow{f_2} M \to 0$$

с проективными модулями $P_1$ и $P_2$, то $P_1 \oplus N_2 \simeq P_2 \oplus N_1$. (Указание: рассмотреть подъем первой последовательности вдоль $f_2$, а второй — вдоль $f_1$.)

7. Доказать, что категория левых проективных $A$-модулей эквивалентна категории, дуальной к категории правых проективных $A$-модулей. (Указание: воспользоваться функтором $h^0_A = \mathrm{Hom}_A(\cdot, A)$.)

8. Доказать, что для любого $A$-модуля $M$ существует точная последовательность

$$P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \to 0$$

с проективными модулями $P_1$ и $P_0$, такая, что $\mathrm{Ker}\, f_0 \subset \mathrm{rad}\, P_0$, а $\mathrm{Ker}\, f_1 \subset \mathrm{rad}\, P_1$, причем если

$$Q_1 \xrightarrow{g_1} Q_0 \xrightarrow{g_0} M \to 0$$

— другая последовательность с теми же свойствами, то существует коммутативная диаграмма

$$\begin{array}{ccccccc} P_1 & \xrightarrow{f_1} & P_0 & \xrightarrow{f_0} & M & \to & 0 \\ {\scriptstyle \varphi_1}\downarrow & & {\scriptstyle \varphi_0}\downarrow & & \downarrow{\scriptstyle 1_M} & & \\ Q_1 & \xrightarrow{g_1} & Q_0 & \xrightarrow{g_0} & M & \to & 0 \end{array}$$

в которой $\varphi_0$ и $\varphi_1$ — изоморфизмы.

9 (М. Ауслендер). Пусть для $A$-модуля $M$ построена точная последовательность

$$P_1 \xrightarrow{f_1} P_0 \xrightarrow{f_0} M \to 0,$$

обладающая свойствами, перечисленными в предыдущем упражнении. Обозначим $\mathrm{Tr}\,(M) = \mathrm{Coker}\, h^0_A(f_1)$ (см. пример 6 функторов из § 1 и упражнение 7).

а) Доказать, что $\mathrm{Tr}\,(M)$ с точностью до изоморфизма не зависит от выбора точной последовательности с указанными свойствами.

б) Проверить, что точная последовательность

$$h^0_A(P_0) \xrightarrow{h^0_A(f_1)} h^0_A(P_1) \longrightarrow \mathrm{Tr}\,(M) \longrightarrow 0$$

также обладает свойствами, перечисленными в упражнении 8.

в) Доказать, что $\mathrm{Tr}\,(M)$ не содержит проективных прямых слагаемых.

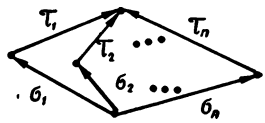
г) Установить, что если $M = P \oplus N$, где $P$ проективен, а $N$ не содержит проективных прямых слагаемых, то $\mathrm{Tr}\,(\mathrm{Tr}\,(M)) \simeq N$.

10. В обозначениях теоремы 4.4 доказать, что если $F(U) \neq 0$, где $U$ — простой $A$-модуль, то $F(U)$ — также простой $B$-модуль, причем если $U'$ — простой модуль, неизоморфный $U$, то $F(U') \not\simeq F(U)$.

11. Пусть $1 = e_1 + \ldots + e_n$ — минимальное разложение единицы алгебры $A$, $n \geqslant 2$. Доказать, что алгебра $A$ полупроста (сепарабельна) тогда и только тогда, когда для любой пары индексов $i \neq j$ полупроста (сепарабельна) алгебра $eAe$, где $e = e_i + e_j$.

12. Доказать, что если алгебра $A$ наследственна, $P$ — проективный $A$-модуль, а $B = E_A(P)$, то и алгебра $B$ наследственна.

13. Обозначим через $S$ схему вида




и пусть $A$ — факторалгебра алгебры путей $K(S)$ по идеалу, порожденному элементом $\sum_{i=1}^{n} \sigma_i \tau_i$. Доказать, что алгебра $A$ ненаследственна, но для любого неединичного идемпотента $e \in A$ алгебра $eAe$ наследственна. (Указание: если $S'$ — схема, содержащая часть (но не все) вершин схемы $S$ и все стрелки, их соединяющие, а $e$ — сумма путей длины 0 схемы $S'$, то $eAe \simeq K(S')$.)

Следующая группа упражнений (14—19) посвящена одному применению тензорных произведений — теории индуцированных представлений групп. Пусть $H$ — подгруппа группы $G$, $N$ — некоторый $KH$-модуль. Тогда **индуцированный $KG$-модуль** $\mathrm{Ind}_H^G(N)$ определяется как $N \otimes_{KN} KG$. Если $T$ — представление группы $H$, соответствующее модулю $N$, а $\chi$ — его характер, то представление группы $G$, соответствующее модулю $\mathrm{Ind}_H^G(N)$, называется **представлением, индуцированным** $T$, а его характер $\mathrm{Ind}_H^G \chi$ — **характером, индуцированным** $\chi$. Всякий $KG$-модуль $M$ можно, конечно, рассматривать и как $KH$-модуль, который обозначается $\mathrm{Res}_H^G(M)$ и называется **ограничением** $M$ на подгруппу $H$.

14 (закон взаимности Фробениуса). Пусть $M$ — некоторый $KG$-модуль, $\chi$ — его характер, $N$ — некоторый $KH$-модуль, $\psi$ — его характер.

а) Доказать, что $\mathrm{Hom}_{KG}(\mathrm{Ind}_H^G(N), M) \simeq \mathrm{Hom}_{KH}(N, \mathrm{Res}_H^G(M))$.

б) Доказать, что если $n = (G : 1)$, $m = (H : 1)$, то

$$\frac{1}{n} \sum_{g \in G} \mathrm{Ind}_H^G \psi(g) \chi(g^{-1}) = \frac{1}{m} \sum_{h \in H} \psi(h) \mathrm{Res}_H^G \chi(h^{-1}).$$

(Указание: воспользоваться упражнением 14 к гл. VII.)

в) Вывести из а), что если характеристика поля $K$ не делит порядок группы $G$, $M$ — простой $KG$-модуль и $N$ — простой $KH$-модуль, то кратность вхождения $M$ в $\mathrm{Ind}_H^G(N)$ равна кратности вхождения $N$ в $\mathrm{Res}_H^G(M)$.

15. Пусть $F \supset H$ — две подгруппы $G$. Доказать, что $\mathrm{Ind}_H^G(N) \simeq \mathrm{Ind}_F^G \times$ $\times (\mathrm{Ind}_H^F(N))$ для любого $KH$-модуля $N$.

**16** (формула Макки). Пусть $F$ и $H$ — две подгруппы $G$, $\sigma_1, \ldots, \sigma_s$ — система представителей двойных смежных классов $G$ по $H$ и $F$ (т. е. $G = \bigcup_{i=1}^{s} H\sigma_i F$, причем эти классы попарно не пересекаются). Обозначим $H_i = (\sigma_i^{-1} H \sigma_i) \cap F$. Всякий $KH$-модуль $N$ можно превратить в $KH_i$-модуль, полагая $x(\sigma_i^{-1} h \sigma_i) = xh$ для любого $h$. Этот $KH_i$-модуль обозначим $N_i$. Доказать, что

$$\mathrm{Res}_F^G(\mathrm{Ind}_H^G(N)) \simeq \bigoplus_{i=1}^{s} \mathrm{Ind}_{H_i}^F(N_i)$$

для любого $KH$-модуля $N$. (Указание: $KG$ как $KH$-$KF$-бимодуль разлагается в прямую сумму $\bigoplus_{i=1}^{s} V_i$, где $V_i$ — подпространство с базисом $\{h\sigma_i f \mid h \in H, f \in F\}$. Проверить, что $V_i \simeq \mathrm{Ind}_{H_i}^F(KH_i)$ как $KF$-модуль, и распространить этот изоморфизм на все $KH$-модули, например, по аналогии с доказательством теоремы 4.4.)

**17**. а) Используя результат упражнений 14 и 16, доказать, что если $K$ — поле характеристики 0, то для простоты $KG$-модуля $\mathrm{Ind}_H^G(N)$ необходимо и достаточно, чтобы $KH$-модуль $N$ был прост и для любого $i$ $KH_i$-модули $N_i$ и $\mathrm{Res}_{H_i}^H(N)$ не имели изоморфных прямых слагаемых (здесь $H_i$, $N_i$ определяются как и в упражнении 16, при $F = H$).

б) Вывести отсюда, что если подгруппа $H$ нормальна, то представление $\mathrm{Ind}_H^G(T)$ неприводимо тогда и только тогда, когда $T$ неприводимо и неизоморфно представлению $T_\sigma$, где $T_\sigma(h) = T(\sigma^{-1} h \sigma)$, ни для какого $\sigma \notin H$.

**18**. а) Доказать, что всякое неразложимое представление подгруппы $H$ группы $G$ изоморфно прямому слагаемому некоторого представления вида $\mathrm{Res}_H^G(T)$, где $T$ — неразложимое представление $G$.

б) В случае, когда характеристика $p$ поля $K$ не делит индекс $(G : H)$, доказать, что всякое неразложимое представление группы $G$ изоморфно прямому слагаемому некоторого представления вида $\mathrm{Ind}_H^G(T)$, где $T$ — неразложимое представление $H$. (Указание: для любого $KG$-модуля $M$ построить эпиформизм $KG$-модулей $\tau : M \otimes_{KH} KG \to M$, который расщепляется как эпиморфизм $KH$-модулей, и воспользоваться упражнением 18 к гл. VII.)

**19**. Используя результаты предыдущего упражнения, а также упражнений 21 и 22 к гл. VII, доказать, что группа $G$ имеет конечное число неразложимых представлений над полем характеристики $p$ тогда и только тогда, когда ее силовская $p$-подгруппа циклична (теорема Хигмана).

# IX

ГЛАВА

## КВАЗИФРОБЕНИУСОВЫ АЛГЕБРЫ

Важную роль в теории конечномерных алгебр играет двойственность, которая существует между категориями правых и левых модулей. В настоящей главе мы построим эту двойственность, ис-

следуем ее свойства и применим полученные результаты к изучению двух классов алгебр: квазифробениусовых алгебр, введенных в рассмотрение Накаямой, а также однорядных алгебр, или алгебр главных идеалов, которые впервые изучил Асано.

## § 1. Двойственность. Инъективные модули

Сначала установим двойственность между категориями левых и правых модулей над некоторой конечномерной алгеброй $A$. Такую двойственность можно определить следующим образом.

Всякому (конечномерному) правому $A$-модулю $M$ сопоставим левый $A$-модуль $M^*$, построенный по такому правилу. В качестве векторного пространства $M^*$ возьмем пространство $\mathrm{Hom}(M, K)$ линейных функционалов на $M$ (сопряженное пространство), а действие операторов из $A$ на $M^*$ определим формулой $(af)(m) = f(ma)$ для любых $a \in A$, $f \in M^*$, $m \in M$. Легко проверяется, что таким образом $M^*$ превращается в левый $A$-модуль.

Аналогично, если $M$ — левый $A$-модуль, то сопряженное пространство $M^*$ превращается в правый $A$-модуль.

Всякое линейное отображение $\varphi : M \to N$ индуцирует сопряженное отображение $\varphi^* : N^* \to M^*$

$$(\varphi^* f)(m) = f(\varphi m).$$

Нетрудно убедиться в том, что если $\varphi$ — гомоморфизм $A$-модулей, то и $\varphi^*$ является гомоморфизмом $A$-модулей. При этом $(\varphi\psi)^* = \psi^*\varphi^*$, а $1^* = 1$.

Следовательно, сопоставляя модулю $M$ модуль $M^*$, а гомоморфизму $\varphi$ — гомоморфизм $\varphi^*$, мы получим контравариантный функтор (см. § 1 гл. VIII). Точнее, мы получаем два контравариантных функтора: из категории mod-$A$ правых $A$-модулей в категорию $A$-mod левых $A$-модулей и наоборот. Мы их будем называть функторами двойственности.

Напомним, что существует естественное отображение $\delta_M : M \to M^{**}$, сопоставляющее вектору $m \in M$ линейный функционал $\delta(m) : M^* \to K$ по правилу $\delta(m)(f) = f(m)$. Очевидно, $\delta_M$ определяет морфизм тождественного функтора в композицию функторов двойственности, построенных выше. Но из элементарной линейной алгебры известно, что для любого конечномерного пространства $M$ отображение $\delta_M$ является изоморфизмом. Поэтому наши рассуждения можно подытожить в такой теореме.

**Теорема 1.1.** *Функторы двойственности устанавливают эквивалентность категорий* mod-$A$ *и* $(A\text{-mod})^\circ$. *В частности, эти функторы точны и из* $M^* = 0$ *следует, что* $M = 0$.

**Следствие 1.2.** *Модуль $M$ прост тогда и только тогда, когда прост модуль $M^*$. При этом если $M \simeq e\overline{A}$, где $\overline{A} = A/\mathrm{rad}A$, а $e$ — минимальный идемпотент $\overline{A}$, то $M^* \simeq \overline{A}e$.*

Доказательство. Поскольку $M \simeq M^{**}$, достаточно проверить, что если $M$ не прост, то и $M^*$ не прост. Но если $N$ —

нетривиальный подмодуль в $M$, то можно рассмотреть точную последовательность

$$0 \to N \to M \to M/N \to 0.$$

Применяя к ней функтор двойственности, получим точную последовательность

$$0 \to (M/N)^* \to M^* \to N^* \to 0,$$

в которой $(M/N)^*$ и $N^*$ — ненулевые модули, т. е. $M^*$ не прост.

Пусть теперь $M \simeq \bar{eA}$, где $e$ — минимальный идемпотент. Тогда $Me \neq 0$ и найдется функционал $f \in M^*$, такой, что $f(Me) \neq 0$. Но $f(me) = (ef)(m)$. Значит, $eM^* \neq 0$. Следовательно, $M^* \simeq \bar{Ae}$.

**Следствие 1.3.** *Между подмодулями модулей $M$ и $M^*$ существует взаимно однозначное соответствие, обращающее включение.*

Для доказательства достаточно заметить, что всякий подмодуль $N \subset M$ определяет эпиморфизм $\pi : M \to M/N$, а следовательно, мономорфизм $\pi^* : (M/N)^* \to M^*$, т. е. подмодуль в $M^*$. Этот подмодуль имеет простой смысл: он совпадает с «ортогональным дополнением» $N^\perp = \{f \in M^* \mid f(N) = 0\}$. Кроме того, $M^*/N^\perp \simeq N^*$.

Отметим такие очевидные формулы:

$$(N_1 + N_2)^\perp = N_1^\perp \cap N_2^\perp, \quad (N_1 \cap N_2)^\perp = N_1^\perp + N_2^\perp. \tag{1}$$

Соответствие, удовлетворяющее формулам (1), называется антиизоморфизмом структур.

В дальнейшем нам часто придется иметь дело с подмодулем $(\operatorname{rad} M)^\perp \subset M^*$. Поскольку $\operatorname{rad} M$ — это пересечение максимальных подмодулей, $(\operatorname{rad} M)^\perp$ — это сумма минимальных подмодулей модуля $M^*$. Она называется цоколем модуля $M^*$ и обозначается $\operatorname{soc} M^*$. Заметим, что цоколь модуля можно также определить формулой

$$\operatorname{soc} M = \{m \in M \mid m(\operatorname{rad} A) = 0\}.$$

Кроме того, из вышесказанного следует, что $\operatorname{soc} M^* \simeq (M/\operatorname{rad} M)^*$.

Мы видели, какую роль играют при изучении строения алгебр проективные и особенно главные модули. Естественно ожидать, что двойственные к ним модули также окажутся полезны при более тонких рассмотрениях. «Переворачивая стрелки» в известных теоремах о проективных модулях (теорема III.3.5 и пример 4 из § 2 гл. VIII), мы автоматически получаем следующий результат.

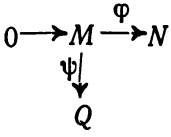
**Теорема 1.4.** *Следующие условия равносильны:*

*1) модуль $Q^*$ проективен (иными словами, $Q \simeq P^*$, где $P$ — проективный модуль);*

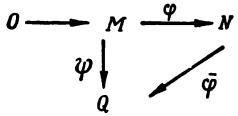
*2) $Q$ — прямое слагаемое модуля $nA^*$ для некоторого $n$ ($A^*$ — модуль, двойственный к регулярному, в дальнейшем он будет называться корегулярным);*

*3)* $Q \simeq \bigoplus_i k_i P_i^*$, *где* $P_i$ — *главные модули;*

*4) всякую диаграмму вида*



*с точной строкой можно дополнить до коммутативной диаграммы*



*Иными словами, уравнение* $x\varphi = \psi$ *разрешимо для любого* $\psi : M \to Q$ *и любого мономорфизма* $\varphi$;

*5) всякий мономорфизм* $Q \to M$ *расщепляем, т. е.* $Q$ *выделяется прямым слагаемым из любого модуля, в который он вложен как подмодуль.*

Модули, обладающие свойством (4) из теоремы 1.4, называются инъективными. Таким образом, теорема 1.4 дает характеристику инъективных модулей над конечномерными алгебрами.

Из доказанной теоремы, в частности, вытекает, что неразложимые инъективные модули — это модули, двойственные к главным. Мы будем называть их коглавными модулями.

Из следствий 1.3, III.2.5 и III.2.9 вытекает такое следствие.

**Следствие 1.5.** *Если* $Q$ — *коглавный* $A$-*модуль, то его цоколь — простой модуль. Сопоставляя* $Q$ *простой модуль* $\operatorname{soc} Q$, *мы устанавливаем взаимно однозначное соответствие между коглавными и простыми* $A$-*модулями.*

По аналогии с понятием проективного накрытия, можно ввести понятие инъективной оболочки, т. е. наименьшего инъективного модуля, в который данный модуль $M$ можно вложить как подмодуль. Точнее, инъективный модуль $Q$ является инъективной оболочкой модуля $M$, если существует мономорфизм $\varphi : M \to Q$, такой, что $\operatorname{Im}\varphi \supset \operatorname{soc} Q$, или, что то же, из $\operatorname{Im}\varphi \cap X = 0$, где $X$ — подмодуль $Q$, следует $X = 0$. В этом случае будем писать $Q = Q(M)$.

Существование и свойства инъективных оболочек, ввиду двойственности, непосредственно вытекают из аналогичных результатов для проективных накрытий. Мы сформулируем нужные нам факты в виде следующей теоремы, доказательство которой предоставляется читателю.

**Теорема 1.6.** 1) *Если* $P$ — *проективное накрытие* $M^*$, *то* $P^*$ — *инъективная оболочка* $M$.

2) $Q(M) = Q(\operatorname{soc} M)$.

3) $Q(M_1 \oplus M_2) \simeq Q(M_1) \oplus Q(M_2)$.

*4) Если* $\psi : M \to Q'$ *— мономорфизм, а* $Q'$ *— инъективный модуль, то* $Q' = Q \oplus Q_1$, *где* $Q \simeq Q(M)$ *и* $\operatorname{Im}\psi \subset Q$.

**Следствие 1.7.** *Если* $\operatorname{soc} M$ *— простой модуль, а* $l(M) \geqslant l(Q_i)$ *для любого коглавного модуля* $Q_i$, *то* $M$ *— коглавный модуль.*

Доказательство следует из того, что если $Q = Q(M)$, то $\operatorname{soc} Q \simeq \operatorname{soc} M$. Поэтому $Q$ — коглавный модуль.

Заметим, что $l(Q_i) = l(Q_i^*)$, а $Q_i^*$ — главный $A$-модуль. Поэтому максимум длин правых коглавных $A$-модулей совпадает с максимумом длин левых главных $A$-модулей (но, вообще говоря, не совпадает с максимумом длин правых главных модулей, см. упражнение 1 к этой главе).

## § 2. Лемма о выбрасывании

В этом параграфе мы изучим свойства модулей, которые одновременно являются проективными и инъективными. Такие модули называются биективными. Заметим, что у произвольной алгебры $A$ биективных модулей, вообще говоря, может и не быть (см. упражнение 2 к этой главе). Более того, существование биективного модуля позволяет свести изучение $A$-модулей к изучению модулей над некоторой собственной факторалгеброй алгебры $A$. Это обстоятельство оказывается полезным при изучении некоторых классов алгебр и модулей над ними.

Установим вначале следующий простой, но важный факт.

**Предложение 2.1.** *Если* $P$ *— проективный, а* $M$ *— точный* $A$*-модуль, то для некоторого* $n$ *существует мономорфизм* $P \to nM$. *Аналогично, если* $Q$ *— инъективный* $A$*-модуль, то существует эпиморфизм* $mM \to Q$.

Доказательство. Обозначим $E = E_A(M)$. Рассматривая $M$ как левый $E$-модуль, мы можем построить эпиморфизм $nE \to M$ для некоторого $n$. Применяя точный слева функтор $\operatorname{Hom}_E(\cdot, M)$, мы получим мономорфизм $\varphi$: $\operatorname{Hom}_E(M, M) \to \operatorname{Hom}_E(nE, M) \simeq nM$. Более того, поскольку $M$ является $E$-$A$-бимодулем, $\varphi$ — это гомоморфизм $A$-модулей. Но, сопоставляя всякому $a \in A$ отображение $f(a)$: $M \to M$, переводящее $m$ в $ma$, мы получим гомоморфизм $f: A \to \operatorname{Hom}_E(M, M)$. Очевидно, $\operatorname{Ker} f = \operatorname{Ann} M = 0$ (так как $M$ точен). Композиция $\varphi f$ является тогда мономорфизмом $A \to nM$. Для того чтобы отсюда получить утверждение для любого проективного $P$, достаточно вспомнить, что $P$ является подмодулем (даже прямым слагаемым) свободного модуля $kA$ для некоторого $k$, а гомоморфизм $kA \to knM = k(nM)$, совпадающий на каждой компоненте с $\varphi f$, конечно, также является мономорфизмом.

Утверждение об инъективных модулях следует после этого из двойственности (поскольку $M$ и $M^*$ точны одновременно).

Выведем из полученного результата следующую основную лемму.

**Лемма 2.2** (о выбрасывании). *Пусть* $W$ *— биективный* $A$*-модуль. Существует такой ненулевой идеал* $I \subset A$, *что всякий* $A$*-модуль* $M$ *разлагается в прямую сумму* $M_1 \oplus M_2$, *где* $\operatorname{Ann} M_1 \supset I$, *а всякое*

*неразложимое прямое слагаемое модуля $M_2$ изоморфно прямому слагаемому модуля $W$.*

Доказательство. Очевидно, достаточно проверить, что для всякого неразложимого модуля $M$, не изоморфного прямому слагаемому $W$, $\operatorname{Ann} M \supset I$. Поэтому за $I$ можно принять пересечение аннуляторов всех неразложимых $A$-модулей, не изоморфных прямым слагаемым $W$ (класс таких модулей обозначим через $\mathfrak{M}$). Остается показать, что $I \neq 0$.

Предположим противное. Поскольку алгебра $A$ конечномерна, в ней нет бесконечных цепочек подпространств. Следовательно, на самом деле $I = \bigcap_{i=1}^{t} \operatorname{Ann} M_i$, где $M_1, \ldots, M_t$ — конечный набор модулей из $\mathfrak{M}$. Но тогда, очевидно, $I = \operatorname{Ann} M$, где $M = M_1 \oplus \ldots \ldots \oplus M_t$, т. е. $M$ — точный $A$-модуль. По предложению 2.1 существует мономорфизм $W \to nM$ ($W$ — проективный модуль). Но, поскольку $W$ также и инъективен, отсюда следует, что $nM \simeq W \oplus X$ и по теореме Крулля — Шмидта всякое неразложимое прямое слагаемое $W$ изоморфно одному из $M_i$, что невозможно по предложению. Полученное противоречие и доказывает лемму.

Итак, если $W = k_1 W_1 \oplus \ldots \oplus k_s W_s$, где $W_i$ — неразложимые модули, то всякий $A$-модуль имеет вид $M_1 \oplus l_1 W_1 \oplus \ldots \oplus l_s W_s$, где $M_1$ — модуль над факторалгеброй $A/I$. Эту факторалгебру мы будем обозначать $A^-(W)$.

Особенно просто лемма о выбрасывании выглядит в случае неразложимого модуля $W$ (такой модуль назовем б и г л а в н ы м): всякий $A$-модуль $M$ имеет вид $M \simeq M_1 \oplus kW$, где $M_1$ — модуль над $A^-(W)$. В этом случае имеет место и обратное утверждение.

**Лемма 2.3.** *Пусть $W$ — такой неразложимый $A$-модуль, что всякий $A$-модуль $M$ имеет вид $M_1 \oplus kW$, где $M_1$ — модуль над некоторой собственной факторалгеброй $B$ алгебры $A$. Тогда $W$ — биглавный модуль.*

Доказательство. Поскольку регулярный и корегулярный $A$-модули точны, они не являются $B$-модулями. Следовательно, они должны содержать прямое слагаемое, изоморфное $W$. Поэтому $W$ проективен и инъективен одновременно, что и требовалось доказать.

Зафиксируем теперь биглавный $A$-модуль $W$. Уточним вид главных и коглавных модулей над факторалгеброй $B = A^-(W)$.

**Предложение 2.4.** *Всякий главный $B$-модуль является либо главным $A$-модулем (отличным от $W$), либо фактормодулем $W$ по минимальному подмодулю $W_1$ (единственному по следствию 1.5). Всякий коглавный $B$-модуль является либо коглавным $A$-модулем, либо максимальным подмодулем $W_2$ модуля $W$ (единственным по следствию III.2.5). Наоборот, если $W$ — не простой модуль, то $W/W_1$ — главный, а $W_2$ — коглавный $B$-модуль.*

Доказательство. Очевидно, $W/W_1$ является $B$-модулем. Обозначим $P = P_B(W/W_1)$. Тогда эпиморфизм $W \to W/W_1$ про-

должается до эпиморфизма $\varphi : W \to P$, который не является изоморфизмом (так как $W$ — не $B$-модуль). Поэтому $\operatorname{Ker} \varphi \supset W_1$ и $l(P) \leqslant l(W/W_1)$, откуда $P \simeq W/W_1$. Аналогично, $W_2 \simeq Q_B(W_2)$. Кроме того, $W/W_1$ содержит, как и $W$, ровно один максимальный подмодуль и потому неразложим. $W_2$ также неразложим, поскольку содержит один минимальный подмодуль.

Пусть теперь $P$ — произвольный главный $B$-модуль, $P' = P_A(P)$. Если $P' \not\simeq W$, то $P'$ — проективный $B$-модуль и потому $P' \simeq P$. Если же $P' \simeq W$, то эпиморфизм $W \to P$ не является изоморфизмом, а потому пропускается через эпиморфизм $W/W_1 \to P$, откуда $P \simeq W/W_1$. Утверждение о коглавных модулях получается из двойственности.

Из предложения 2.4 и леммы 2.2 непосредственно вытекает такое следствие.

**Следствие 2.5.** *Пусть $W$ — биглавный $A$-модуль, причем $A = P_1 \oplus P_2$, где $P_1 \simeq nW$, а $P_2$ не содержит прямых слагаемых, изоморфных $W$. Тогда* $\operatorname{soc} P_1$ *— идеал в $A$ и $A^-(W) = A/\operatorname{soc} P_1$.*

**Предложение 2.6.** *Алгебра $A$ имеет простой биективный модуль $W$ тогда и только тогда, когда $A \simeq A_1 \times A_2$, где $A_1 \simeq M_n(D)$ ($D$ — тело), а $A_2 = A^-(W)$.*

Доказательство. Пусть $W$ — простой биективный $A$-модуль, причем $A \simeq nW \oplus P$, где $P$ не содержит прямых слагаемых, изоморфных $W$. Всякий гомоморфизм $\varphi : W \to P$ либо нулевой, либо мономорфизм. Но во втором случае $P \simeq W \oplus X$, так как $W$ инъективен, что невозможно. Следовательно, $\operatorname{Hom}_A(nW, P) = 0$. Аналогично, $\operatorname{Hom}_A(P, nW) = 0$. Поэтому $A \simeq A_1 \times A_2$, где $A_1 = E_A(nW) \simeq M_n(D)$, причем $D = E_A(W)$ — тело, а $A_2 = E_A(P)$. Очевидно, $A_2 = A^-(W)$. Обратное утверждение тривиально.

**§ 3. Квазифробениусовы алгебры**

Как мы уже отмечали, произвольная алгебра может и не иметь ни одного биективного модуля. Важный класс алгебр, введенный в рассмотрение Накаямой, составляет те алгебры, у которых всякий проективный модуль инъективен (а потому и биективен). Очевидно, для этого достаточно, чтобы регулярный модуль был инъективным. Такие алгебры называются квазифробениусовыми.

В принципе следовало бы определять квазифробениусовы справа и слева алгебры. Однако имеет место такая теорема.

**Теорема 3.1.** *Следующие условия равносильны:*

*1) правый регулярный $A$-модуль инъективен;*

*1а) левый регулярный $A$-модуль инъективен;*

*2) правый корегулярный $A$-модуль проективен;*

*2а) левый корегулярный $A$-модуль проективен.*

Доказательство. Эквивалентности 1) $\Leftrightarrow$ 2а) и 1а) $\Leftrightarrow$ 2) следуют из двойственности. Поэтому остается доказать, например, эквивалентность 1) $\Leftrightarrow$ 2). Заметим, что число коглавных правых $A$-модулей равно числу главных левых $A$-модулей, т. е. по следствию III.2.9 — числу простых левых $A$-модулей, иными словами,

числу простых компонент полупростой алгебры $A/\operatorname{rad} A$. Но тому же равно и число простых правых $A$-модулей, а значит, и число главных правых $A$-модулей. Но сказать, что регулярный модуль инъективен — это все равно, что сказать, что всякий главный $A$-модуль инъективен, т. е. что число биглавных $A$-модулей совпадает с числом главных. С учетом вышесказанного это равносильно тому, что число биглавных модулей совпадает с числом коглавных, т. е. всякий коглавный модуль, или, что то же, корегулярный модуль проективен. Теорема доказана.

Теперь квазифробениусовы алгебры можно охарактеризовать так: если $A \simeq k_1P_1 \oplus \ldots \oplus k_kP_k$, где $P_i$ — главные модули, то $A^* \simeq l_1P_1 \oplus \ldots \oplus l_sP_s$. При этом, вообще говоря, $k_i \neq l_i$ (см. упражнение 4 к гл. IX), т. е. $A \not\simeq A^*$. Те алгебры, для которых $A \simeq A^*$, образуют собственный подкласс в классе квазифробениусовых алгебр. Такие алгебры называются фробениусовыми. Важным примером фробениусовых алгебр являются групповые алгебры конечных групп (см. упражнение 8 к гл. IX).

Те же рассуждения, что и при доказательстве теоремы 3.1, приводят к следующему результату.

**Теорема 3.2.** *Если кратности вхождения всех главных $A$-модулей в регулярный одинаковы, или, что то же, $A/\operatorname{rad} A \simeq M_n(D_1) \times \ldots \times M_n(D_s)$, где $D_i$ — тела, и алгебра $A$ квазифробениусова, то она фробениусова. В частности, приведенная квазифробениусова алгебра фробениусова.*

Поскольку определение квазифробениусовости было дано в терминах категории модулей, мы получаем такое следствие.

**Следствие 3.3.** *Однотипные алгебры квазифробениусовы одновременно. В частности, всякая квазифробениусова алгебра однотипна некоторой фробениусовой (именно, своей базисной алгебре).*

Из предложения 2.1 и теоремы Крулля — Шмидта вытекает также еще и такое следствие.

**Следствие 3.4.** *Пусть $A$ — квазифробениусова алгебра, $A \simeq k_1P_1 \oplus \ldots \oplus k_sP_s$, где $P_i$ — главные модули, $M_0 = P_1 \oplus \ldots \oplus P_s$. Всякий точный $A$-модуль содержит прямое слагаемое, изоморфное $M_0$.*

Из предложения 2.6 и определения схемы алгебры вытекает следствие.

**Следствие 3.5.** *Пусть $S$ — схема квазифробениусовой алгебры $A$. Если из точки $i \in S$ не выходит ни одна стрелка или в эту точку не входит ни одна стрелка, то $A \simeq A_1 \times A_2$, где $A_1 \simeq M_n(D)$ ($D$ — тело).*

Для доказательства достаточно вспомнить, что если из точки $i$ не выходит стрелка, то соответствующий главный модуль прост (утверждение о входящих стрелках получается из двойственности).

Сравнивая следствие 3.5 с результатом о схемах наследственных алгебр (следствие III.7.3), мы получаем такое следствие.

**Следствие 3.6.** *Наследственная квазифробениусова алгебра полупроста.*

Если $A$ — квазифробениусова алгебра, то всякий главный $A$-модуль $P$ является коглавным и по следствию 1.5 его цоколь — простой $A$-модуль. Более того, если $P'$ — главный модуль, не изоморфный $P$, то и $\operatorname{soc} P' \simeq \operatorname{soc} P$. Оказывается, имеет место и обратное утверждение, которое дает довольно простой и удобный критерий квазифробениусовости.

**Теорема 3.7.** *Алгебра $A$ квазифробениусова тогда и только тогда, когда цоколь любого главного $A$-модуля—простой модуль, причем если $P_1$ и $P_2$ неизоморфные главные $A$-модули, то* $\operatorname{soc} P_1 \not\simeq \operatorname{soc} P_2$.

Доказательство. Поскольку условие теоремы формулируется в терминах категории $A$-модулей, мы можем, заменяя $A$ на однотипную алгебру, считать ее приведенной. Тогда $A = P_1 \oplus \ldots \oplus P_s$, где $P_i$ — попарно неизоморфные главные модули. Обозначим $Q_i = Q(P_i)$. По теореме 1.6 $\operatorname{soc} Q_i \simeq \operatorname{soc} P_i$ — простой модуль, причем $\operatorname{soc} Q_i \not\simeq \operatorname{soc} Q_j$ при $i \neq j$. Следовательно, $Q_i$ — попарно неизоморфные коглавные модули. Но тогда $Q_i^*$ — попарно неизоморфные левые главные модули и, поскольку $A$ — приведенная алгебра, $A \simeq Q_1^* \oplus \ldots \oplus Q_s^*$ (напомним, что число левых и правых главных модулей одинаково). Нам нужно показать, что $P_i \simeq Q_i$. Но $\dim P_i \leqslant \dim Q_i = \dim Q_i^*$, а

$$\sum_{i=1}^{s} \dim P_i = \dim A = \sum_{i=1}^{s} \dim Q_i^* = \sum_{i=1}^{s} \dim Q_i,$$

откуда вытекает, что $\dim P_i = \dim Q_i$ для всех $i$. Поэтому $P_i \simeq Q_i$. Теорема доказана.

Предположим, что алгебра $A$ фробениусова. Тогда, поскольку $A^* \simeq A$, из следствия 1.3 вытекает, что структуры левых и правых идеалов алгебры $A$ антиизоморфны. Оказывается, то же имеет место и для любых квазифробениусовых алгебр. Более того, это условие является критерием квазифробениусовости.

**Теорема 3.8.** *Алгебра $A$ квазифробениусова тогда и только тогда, когда структуры левых и правых идеалов в ней антиизоморфны.*

Доказательство. Пусть $\varphi$ — антиизоморфизм структур левых и правых идеалов в $A$. Очевидно, $\varphi(A) = 0$ и $\varphi(0) = A$. Разложим регулярный левый $A$-модуль в прямую сумму главных: $A = P_1 \oplus P_2 \oplus \ldots \oplus P_s$. Это означает, что $P_i$ — левые идеалы в $A$, причем $\sum_{i=1}^{s} P_i = A$ и для любого $i$ $P_i \cap \left(\sum_{j \neq i} P_j\right) = 0$.

Применяя антиизоморфизм структур $\varphi$, мы получим в $A$ правые идеалы $\varphi(P_i)$, такие, что $\bigcap_{i=1}^{s} \varphi(P_i) = 0$ и $\varphi(P_i) + \left(\bigcap_{j \neq i} \varphi(P_j)\right) = A$

для любого $i$. Обозначим $P_i' = \bigcap_{j \neq i} \varphi(P_j)$. Тогда $A = \varphi(P_i) \oplus P_i'$ для любого $i$. Покажем индукцией по $k$, что

$$A = P_1' \oplus \ldots \oplus P_k' \oplus \left( \bigcap_{j=1}^{k} \varphi(P_j) \right), \quad k \leqslant n.$$

База индукции, $k = 1$, уже доказана. Предположим, что наша формула верна для какого-нибудь $k < n$. Тогда $\bigcap_{j=1}^{k} \varphi(P_j) \supset P_{k+1}'$ и, поскольку $A = P_{k+1}' \oplus \varphi(P_{k+1})$, $\bigcap_{j=1}^{k} \varphi(P_j) = P_{k+1}' \oplus \left( \bigcap_{j=1}^{k+1} \varphi(P_j) \right)$, что и требовалось доказать. В частности, $A = P_1' \oplus \ldots \oplus P_s'$, откуда следует, что все $P_i'$ — главные правые модули. Кроме того, поскольку $P_i' = A/\varphi(P_i)$, структура подмодулей и $P_i'$ изоморфна структуре подмодулей $A$, содержащих $\varphi(P_i)$, т. е. антиизоморфна структуре подмодулей $P_i$ (поскольку $\varphi^{-1}(A) = 0$). Но $P_i$ содержит один максимальный подмодуль. Значит, $P_i'$ содержит один минимальный подмодуль, т. е. $U_i = \operatorname{soc} P_i'$ прост.

Ввиду теоремы 3.7 для доказательства квазифробениусовости алгебры $A$ остается проверить, что если $P_i' \ncong P_j'$, то $U_i \ncong U_j$.

Заметим, что $\varphi^{-1}(P_i') = \sum_{j \neq i} P_j$, откуда $P_i = \bigcap_{j \neq i} \varphi^{-1}(P_j')$, т. е. соответствие между $P_i$ и $P_i'$ симметрично.

Мы покажем, что если $P_i \ncong P_j$, то и $U_i \ncong U_j$, а следовательно, $P_i' \ncong P_j'$. Отсюда, очевидно, следует, что если $P_i' \ncong P_j'$, то $P_i \ncong P_j$, а значит, $U_i \ncong U_j$, что и требуется доказать.

Обозначим $P = P_i + P_j$. Тогда, поскольку $P_i \cap P_j = 0$, $P/P_i \simeq P_j$, а $P/P_j \simeq P_i$. Так как $P_i/\operatorname{rad} P_i \ncong P_j/\operatorname{rad} P_j$, в $P$ есть ровно два максимальных подмодуля, один из которых содержит $P_i$, а другой $P_j$. Но $\varphi(P) = \varphi(P_i) \cap \varphi(P_j)$. Значит, структура подмодулей в $P$ антиизоморфна структуре подмодулей в $A = \varphi(0)$, содержащих $\varphi(P_i) \cap \varphi(P_j)$. Поскольку $\varphi(P_i) + \varphi(P_j) = A$, $A/\varphi(P_i) \cap \cap \varphi(P_j) \simeq A/\varphi(P_i) \oplus A/\varphi(P_j) \simeq P_i' \oplus P_j'$. Итак, в $P_i' \oplus P_j'$ есть ровно два минимальных подмодуля, что невозможно при $U_i \simeq U_j$ (в этом случае любой элемент вида $a + b$, где $a \in U_i$, $b \in U_j$, порождает в $U_i \oplus U_j$ простой подмодуль и потому их по меньшей мере три).

Предположим теперь, что алгебра $A$ квазифробениусова. Тогда можно указать явный антиизоморфизм структур левых и правых $A$-идеалов следующим образом. Для всякого правого идеала $I$ положим $l(I) = \{a \in A \mid aI = 0\}$, и для всякого левого идеала $J$ положим $r(J) = \{b \in A/Jb = 0\}$. Очевидно, $l(I)$ — левый, а $r(J)$ — правый идеалы, причем из $I \supset I'$ ($J \supset J'$) следует $l(I) \subset l(I')$

(соответственно, $r(J) \subset r(J')$). Мы покажем, что $l$ и $r$ — взаимно обратные отображения, откуда, конечно, и следует, что они осуществляют искомый антиизоморфизм структур.

Рассмотрим точную последовательность $A$-модулей

$$0 \to I \to A \to A/I \to 0.$$

Применяя к ней функтор $h_A$ и учитывая, что $A$ — инъективный модуль, получаем точную последовательность

$$0 \to \mathrm{Hom}_A(A/I, A) \to \mathrm{Hom}_A(A, A) \to \mathrm{Hom}_A(I, A) \to 0.$$

Но всякий гомоморфизм $A/I \to A$ однозначно определяется образом класса $1 + I$, причем, очевидно, этим образом может быть любой элемент $a \in A$, такой, что $aI = 0$. Иными словами, $\mathrm{Hom}_A(A/I, A) \simeq l(I)$, т. е. нашу последовательность можно переписать в виде

$$0 \to l(I) \to A \to A/l(I) \to 0.$$

Вновь применяя функтор $h_A$ и отождествляя $\mathrm{Hom}_A(A/l(I), A)$ с $rl(I)$, получим точную последовательность

$$0 \to rl(I) \to A \to A/rl(I) \to 0,$$

в которой $rl(I) \simeq \mathrm{Hom}_A(\mathrm{Hom}_A(I, A), A)$.

Заметим теперь, что существует единственный гомоморфизм модулей $M \to \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A)$, переводящий элемент $m \in M$ в гомоморфизм $\overline{m} : \mathrm{Hom}_A(M, A) \to A$, такой, что $\overline{m}(f) = f(m)$ для любого $f \in \mathrm{Hom}_A(M, A)$. Очевидно, совокупность всех таких гомоморфизмов образует морфизм функторов $Id_{A\text{-mod}} \to h_A^2$. В частности, получаем коммутативную диаграмму с точными строками

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I & \longrightarrow & A & \longrightarrow & A/I & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & rl(I) & \to & A & \longrightarrow & A/rl(I) & \to & 0. \end{array} \tag{1}$$

Среднее отображение в ней — изоморфизм.

Покажем, что отображение $M \to \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A)$ мономорфно для любого $M$. Для этого вложим $M$ в инъективный модуль $Q$ и заметим, что ввиду квазифробениусовости $A$ $Q$ биективен. Следовательно, он является прямым слагаемым свободного модуля. Итак, существует мономорфизм $M \to nA$ для некоторого $n$. Но тогда, очевидно, для любого ненулевого $m \in M$ найдется гомоморфизм $f : M \to A$, такой, что $f(m) \neq 0$. Значит, $\overline{m}(f) = f(m) \neq 0$, т. е. $\overline{m} \neq 0$ и наше отображение действительно мономорфно.

Остается заметить, что если в диаграмме (1) крайние отображения мономорфны, то они обязаны быть и изоморфны (например,

из мономорфности отображения $I \to rl(I)$ следует эпиморфность, а потому и изоморфность $A/I \to A/rl(I)$, и остается применить лемму о 5 гомоморфизмах). Теорема полностью доказана.

**Следствие 3.9.** *Алгебра $A$ квазифробениусова тогда и только тогда, когда $rl(I) = I$ для любого правого идеала $I$ и $lr(J) = J$ для любого левого идеала $J$.*

## § 4. Однорядные алгебры

Если алгебра $A$ квазифробениусова, то, как мы видели, описание ее представлений сводится к описанию представлений некоторой факторалгебры $B$. Однако, вообще говоря, алгебра $B$ и ее представления могут быть устроены достаточно сложно. Положение существенно упрощается, если предположить, что все факторалгебры $A$ также квазифробениусовы. В этом случае описание модулей сводится к последовательному применению следствия 3.4. Оказывается, что и сами алгебры, удовлетворяющие этому условию, допускают сравнительно простое описание. Кроме того, в этих алгебрах всякий идеал является главным, т. е. имеет вид $aA$ для некоторого $a \in A$. Наоборот, всякая алгебра главных идеалов обладает этим свойством.

Сформулируем соответствующее утверждение.

**Теорема 4.1.** *Следующие условия равносильны:*

*1) всякая факторалгебра алгебры $A$ квазифробениусова;*

*2) всякий идеал алгебры $A$ является главным правым идеалом (т. е. имеет вид $aA$);*

*2а) всякий идеал алгебры $A$ является главным левым идеалом;*

*3) всякий правый идеал алгебры $A$ главный;*

*3а) всякий левый идеал алгебры $A$ главный;*

*4) $A \simeq A_1 \times \ldots \times A_s$, где $A_i \simeq M_{n_i}(B_i)$, а $B_i$ — локальная алгебра, причем $\operatorname{rad} B_i$ — главный идеал.*

Если, кроме того, алгебра $A$ неразложима в прямое произведение, то эти условия равносильны еще такому условию:

*1а) алгебра $A$ и ее факторалгебра по какому-нибудь минимальному идеалу квазифробениусовы.*

Доказательство. Очевидно, можно считать, что алгебра $A$ неразложима в прямое произведение. Импликации 1) $\Rightarrow$ 1а), 3) $\Rightarrow$ 2), 3а) $\Rightarrow$ 2а) тривиальны.

1а) $\Rightarrow$ 4). Пусть $I$ — минимальный идеал, причем $A$ и $A/I$ — квазифробениусовы алгебры. Найдется главный (следовательно, и биглавный) $A$-модуль $P$, не являющийся $A/I$-модулем. Но тогда, очевидно, $A/I = A^-(P)$ (см. лемму 2.2). Пусть $A \simeq nP \oplus P'$, где $P'$ не содержит прямых слагаемых, изоморфных $P$. Обозначим через $P_1$ максимальный подмодуль $P$, а $P_2 = P/U_1$, где $U_1 = \operatorname{soc} P$. По предложению 2.4 $P_1$ — коглавный, а $P_2$ — главный $A/I$-модуль. Поскольку $A/I$ — квазифробениусова алгебра, $P_1$ — главный $A/I$-модуль. По предложению 2.4 либо $P_1 \simeq P_2$, либо $P_1$ изоморфен прямому слагаемому $P'$. Но в последнем случае $P_1$ был бы биективным $A$-модулем, а тогда $P = P_1 \oplus X$, что невозможно.

Итак, $P_1 \simeq P_2$. Значит, $P_2$ содержит один минимальный подмодуль $U_2 \simeq \operatorname{soc} P_1 = U_1$, причем $P_2/U_2 \simeq P_1/U_1$, откуда следует, что $P_2/U_2$ также содержит один минимальный подмодуль $U_3$, изоморфный $U_2$, т. е. и $U_1$. Продолжая эту процедуру, мы построим в $P$ композиционный ряд, все факторы которого изоморфны $U_1$. Кроме того, этот композиционный ряд единствен. Ввиду теоремы Жордана — Гёльдера отсюда, в частности, вытекает, что $\operatorname{Hom}_A(P', P) = 0$. Ввиду двойственности $P^*$ — также главный модуль с единственным композиционным рядом, откуда и $\operatorname{Hom}_A(P, P') \simeq \operatorname{Hom}_A(P'^*, P^*) = 0$. Следовательно, $A \simeq A_1 \times A_2$, где $A_1 = E_A(nP) \simeq M_n(B)$ ($B = E_A(P)$ — локальная алгебра), а $A_2 = E_A(P')$. Поскольку $A$ неразложима, $P' = 0$ и $A \simeq A_1$.

Обозначим $R = \operatorname{rad} B$. Тогда $\operatorname{rad} M_n(B) = M_n(R)$ (предложение III.3.11). Но $\operatorname{rad} A = nP_1$, а $P(P_1) \simeq P$, поэтому существует эпиморфизм $A \to \operatorname{rad} A$, т. е. $\operatorname{rad} A$, а потому и $\operatorname{rad} B$ — циклический модуль, что и требовалось доказать.

4) $\Rightarrow$ 3). Пусть $A = M_n(B)$, причем $R = \operatorname{rad} B$ — главный правый идеал. Тогда существует эпиморфизм $\varphi : B \to R$. Значит, $R^2$ — единственный максимальный подмодуль в $R$. Кроме того, $\varphi(R) = R^2$. Значит, $\varphi(R^2) = R^3$ — единственный максимальный подмодуль в $B$ и т. д. Учитывая это, получаем, что всякий правый идеал в $B$ имеет вид $R^m$. Но $B \simeq E_A(P)$, где $P$ — главный $A$-модуль. Из теоремы Мориты следует тогда, что структура $B$-подмодулей в $B$ такая же, как и структура $A$-подмодулей в $B \otimes_B P \simeq P$ и для всякого $A$-подмодуля $M \subset P$ существует эпиморфизм $P \to M$. Отсюда индукцией по $k$ тривиально выводится, что для любого подмодуля $M \subset kP$ существует эпиморфизм $kP \to M$. В частности, для любого правого идеала $I \subset A$ существует эпиморфизм $A \to I$, т. е. $I$ — главный идеал.

2) $\Rightarrow$ 1). Пусть $A \simeq nP \oplus P'$, где $P$ —главный модуль, а в $P'$ нет прямых слагаемых, изоморфных $P$. Если $M_1 = \operatorname{rad} P$, то $I_1 = nM_1 \oplus P'$ — идеал в $A$, а значит, и циклический $A$-модуль. Поэтому существует эпиморфизм $A \to I_1$, откуда следует существование эпиморфизма $P \to M_1$. Следовательно, у $M_1$ также всего один максимальный подмодуль $M_2$, причем $M_1/M_2 \simeq P/M_1$. Но тогда $I_2 = nM_2 \oplus P'$ — снова идеал, откуда вытекает существование эпиморфизма $P \to M_2$. Продолжая этот процесс, мы проведем в $P$ единственный композиционный ряд с изоморфными факторами. Отсюда, как и выше, следует, что $\operatorname{Hom}_A(P, P') = \operatorname{Hom}_A(P', P) = 0$, т. е. $A \simeq A_1 \times A_2$, и, ввиду неразложимости, $P' = 0$. Поскольку $P$ содержит единственный минимальный подмодуль, из теоремы 3.7 получаем, что $A$ квазифробениусова. Но, очевидно, условие 2) переносится с $A$ на все факторалгебры. Значит, все факторалгебры алгебры $A$ квазифробениусовы, что и требовалось доказать.

Ввиду симметричности условий 1) и 1а) аналогично получаем 1а) $\Rightarrow$ 4) $\Rightarrow$ 3а) $\Rightarrow$ 2а) $\Rightarrow$ 1). Теорема полностью доказана.

Алгебры, удовлетворяющие условиям теоремы 4.1, называются однорядными (или алгебрами главных идеалов).

Из теоремы 4.1 и следствия 3.4 непосредственно вытекает такое следствие.

**Следствие 4.2.** *Всякий неразложимый модуль над однорядной алгеброй изоморфен фактормодулю главного модуля. Ввиду двойственности всякий неразложимый модуль над однорядной алгеброй изоморфен также подмодулю главного модуля.*

Заметим, что в процессе доказательства теоремы 4.1 мы установили также, что в главном модуле над однорядной алгеброй существует единственный композиционный ряд и потому ровно один подмодуль данной длины. Отсюда получаем такое следствие.

**Следствие 4.3.** *Неразложимый модуль над однорядной алгеброй однозначно (с точностью до изоморфизма) определяется своей длиной и проективным накрытием (или инъективной оболочкой).*

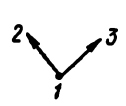
Из теоремы 4.1. легко следует также такой критерий однорядности.

**Предложение 4.4.** *Алгебра $A$ однорядна тогда и только тогда, когда ее схема является несвязным объединением точек и одноточечных циклов.*

**Следствие 4.5.** *Алгебры $A$ и $A/R^2$, где $R = \operatorname{rad} A$, однорядны одновременно.*

## *Упражнения к главе IX*

1. Пусть $A$ — минимальная алгебра, соответствующая частично упорядоченному множеству




(см. упражнение 8 к гл. III). Найти длины главных правых и главных левых $A$-модулей, убедиться, что их максимумы не равны.

2. Доказать, что у трехмерной алгебры $A$ с базисом $\{1, a, b\}$ и таблицей умножения $a^2 = b^2 = ab = ba = 0$ нет биективных модулей.

3. Пусть $A = T_n(K)$ (алгебра треугольных матриц), $W = nK$ — пространство $n$-мерных числовых векторов над полем $K$, рассматриваемое как $A$-модуль. Доказать, что $W$ — единственный биглавный $A$-модуль, и найти $A^-(W)$.

4. Рассмотрим алгебру $K(S)$ путей схемы $S$

Пусть $J$ — идеал путей ненулевой длины, $A = K(S)/J^2$, $e_1$ и $e_2$ — идемпотенты, соответствующие точкам 1 и 2, $P_i = e_iA$, $P_i' = Ae_i$. Доказать, что $P_1^* \simeq P_2'$, $P_2^* \simeq P_1'$. Таким образом, $A$ — фробениусова алгебра. Вывести отсюда, что если $P = P_1 \oplus 2P_2$, то алгебра $B = E_A(P)$ квазифробениусова, но не фробениусова.

5. Доказать, что полупростая алгебра фробениусова.

6. Доказать, что если $A$ — фробениусова алгебра, то и $M_n(A)$ — фробениусова алгебра.

7. Доказать, что алгебра $A$ фробениусова тогда и только тогда, когда на ней существует невырожденная билинейная форма $T$, которая внутренне билинейна (в смысле § 3 гл. VIII), т. е. $T(ba, c) = T(b, ac)$ для всех $a, b, c \in A$.

8. Для элементов групповой алгебры $KG$ конечной группы $G$, $a = \sum_g \alpha_g g$ и $b = \sum_g \beta_g g$, определим $T(a, b) = \sum_g \alpha_{g^{-1}} \beta_g$. Доказать, что $T(a, b)$ — невырожденная внутренне билинейная форма на $KG$ и, следовательно, $KG$ — фробениусова алгебра.

9. Доказать, что алгебра $A$ фробениусова тогда и только тогда, когда для любого правого идеала $I$ и для любого левого идеала $J$ имеют место равенства

$$\dim I + \dim l(I) = [A : K], \quad \dim J + \dim r(J) = [A : K].$$

(Указание: доказать, что $A$ — квазифробениусова; рассмотреть затем идеал $I = k$ (rad $P$) $\oplus X$, где $A = kP \oplus X$, $P$ — главный модуль, не входящий в $X$ прямым слагаемым.)

10. Доказать, что для любого правого или левого главного модуля $P$ над алгеброй $T_n(K)$ треугольных матриц soc $P$ прост (заметим, что из упражнения 3 следует, что эта алгебра не квазифробениусова).

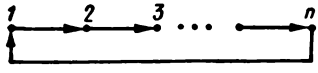
11. Пусть $D$ — некоторое тело, $\sigma$ — его автоморфизм. Алгеброй скрученных многочленов $A = D[t, \sigma]$ называется алгебра (бесконечномерная), элементами которой являются «многочлены от $t$ с коэффициентами из $D$», т. е. выражения вида $a_n t^n + a_{n-1} t^{n-1} + \ldots + a_0$, где $a_i \in D$, а умножение определяется правилом $ta = \sigma(a) t$ для любого $a \in D$. Проверить, что $t^n A = At^n$, и доказать, что $A/t^n A$ — локальная однорядная алгебра.

12. Доказать, что всякая локальная однорядная алгебра сепарабельного типа (см. § 5 гл. VIII) имеет вид $A/t^n A$, где $A = D[t, \sigma]$ — алгебра скрученных многочленов над сепарабельным телом $D$, построенная в предыдущем упражнении, причем тело $D$ и показатель $n$ определяются однозначно, а автоморфизм $\sigma$ — с точностью до сопряжения (в группе автоморфизмов) и внутреннего автоморфизма тела $D$.

13. Вывести из упражнения 12 описание всех однорядных алгебр сепарабельного типа.

14. Пусть $1 = e_1 + \ldots + e_n$ — минимальное разложение единицы алгебры $A$, $n \geqslant 3$. Доказать, что если для любого идемпотента $e$, который есть суммой трех различных идемпотентов из данного разложения, алгебра $eAe$ квазифробениусова, то и алгебра $A$ квазифробениусова. (Указание: пусть $P_i = e_i A$ и soc $P_i$ не прост; тогда $P_i \supset U_j \oplus U_k$, где $U_i$ и $U_j$ — простые $A$-модули, причем $P(U_j) \simeq P_j = e_j A$, $P(U_k) \simeq P_k = e_k A$; $i, j, k$ не обязательно различные. Принимая за $P$ прямую сумму попарно различных модулей из $P_i$, $P_j$, $P_k$, показать, что если $B = E_A(P)$, то цоколь главного $B$-модуля $\overline{P}_i = \mathrm{Hom}_A(P, P_i)$ не прост, что противоречит квазифробениусовости $B$ и теореме 3.7. Аналогично, если $P_i \simeq P_j$, но soc $P_i \simeq$ soc $P_j \simeq U_k$, показать, что soc $\overline{P}_i \simeq$ soc $\overline{P}_j$, что вновь противоречит теореме 3.7, так как, ввиду теоремы VIII. 4.4, $\overline{P}_i \not\simeq \overline{P}_j$.)

15. Пусть $A = K(S)/J^2$, где $K(S)$ — алгебра путей схемы $S$, являющейся циклом ($n \geqslant 3$)



а $J$ — идеал, порожденный путями ненулевой длины. Доказать, что алгебра $A$ квазифробениусова, но алгебра $eAe$, где $e = e_1 + \ldots + e_k$ ($k < n$, $e_i$ — идемпотент, соответствующий $i$-й точке цикла), не квазифробениусова. (Указание: в последнем случае воспользоваться следствием 3.5.) Таким образом, утверждение, обратное сформулированному в упражнении 14, неверно.

16. Пусть $1 = e_1 + \ldots + e_n$ — минимальное разложение единицы алгебры $A$, $n \geqslant 2$. Доказать, что если для любой пары индексов $i$, $j$ алгебра $eAe$, где $e = e_i + e_j$, однорядна, то и алгебра $A$ однорядна.

# X

ГЛАВА

# ОБОБЩЕННО ОДНОРЯДНЫЕ АЛГЕБРЫ

Следствия IX.4.2 и IX.4.3 дают простое описание модулей над однорядными алгебрами. Нетрудно, однако, заметить, что это описание использует не столько квазифробениусовость всех факторалгебр, сколько существование у каждой из них биективного модуля. В этой главе мы рассмотрим более общий класс алгебр, также введенный Накаямой,— обобщенно однорядные алгебры, которые характеризуются тем, что у всякой факторалгебры есть биективный модуль. Мы покажем, что это наиболее общий класс алгебр, для которых имеют место аналоги следствий IX.4.2 и IX.4.3. Строение обобщенно однорядных алгебр существенно более сложно, чем у однорядных алгебр. Однако для этих алгебр также можно получить полное описание при достаточно общих предложениях (основные результаты здесь были получены Купишем).

## § 1. Теорема Накаямы—Скорнякова

Пусть $M$ — правый или левый модуль над некоторой алгеброй $A$. Модуль $M$ называется цепным, если структура его подмодулей является цепью (т. е. линейно упорядоченным множеством). Очевидно, это условие равносильно тому, что всякий ненулевой подмодуль $N \subset M$ имеет один максимальный подмодуль, который является радикалом модуля $N$. Еще одно эквивалентное условие: для любого ненулевого подмодуля $N \subset M$ фактормодуль $N/\operatorname{rad} N$ прост.

Прямая сумма цепных модулей называется полуцепным модулем. Очевидным примером цепного модуля является всякий простой модуль, а полуцепного — полупростой. Из теоремы Крулля—Шмидта следует, что всякое прямое слагаемое полуцепного модуля само является полуцепным модулем. В частности, если оно неразложимо, то является цепным модулем.

**Теорема 1.1.** (Накаямы—Скорнякова). *Пусть $A$ — некоторая алгебра. Следующие условия равносильны:*

*1) всякий правый $A$-модуль полуцепной;*

*1а) всякий левый $A$-модуль полуцепной;*

*2) регулярный правый и регулярный левый $A$-модули полуцепные;*

*2а) регулярный и корегулярный правые $A$-модули полуцепные;*

*2б) регулярный и корегулярный левые $A$-модули полуцепные;*

*3) всякий неразложимый $A$-модуль (правый или левый) изоморфен фактормодулю главного модуля;*

*3а) всякий неразложимый $A$-модуль (правый или левый) изоморфен подмодулю коглавного модуля;*

*4) всякий неразложимый $A$-модуль $M$ (правый или левый) проективен как модуль над факторалгеброй $A/\mathrm{Ann}\, M$;*

*4а) всякий неразложимый $A$-модуль $M$ (правый или левый) инъективен как модуль над факторалгеброй $A/\mathrm{Ann}\, M$;*

*5) у всякой факторалгебры алгебры $A$ есть биективный правый модуль;*

*5а) у всякой факторалгебры алгебры $A$ есть биективный левый модуль.*

Алгебры, удовлетворяющие равносильным условиям данной теоремы, называются обобщенно однорядными.

Доказательство. Равносильность условий 1) $\Leftrightarrow$ 1а), 2) $\Leftrightarrow$ 2а), 3) $\Leftrightarrow$ 3а), 4) $\Leftrightarrow$ 4а), 5) $\Leftrightarrow$ 5а) следует из двойственности (заметим, что, как легко проверить, $\mathrm{Ann}\, M^* = \mathrm{Ann}\, M$ для любого модуля $M$).

1) $\Rightarrow$ 2а) и 4) $\Rightarrow$ 3) очевидно.

2) $\Rightarrow$ 5). Заметим, что условие 2) сохраняется при переходе к факторалгебре: если $A = P_1 \oplus \ldots \oplus P_n$, где все $P_i$ цепные, то $A/I = P_1/P_1I \oplus \ldots \oplus P_n/P_nI$ и, очевидно, фактормодули $P_i/P_iI$ также все цепные. Поэтому достаточно проверить, что из условия 2) следует существование биективного модуля у самой алгебры $A$. Нам удобно заменить условие 2) равносильным условием 2а).

Выберем из главных и коглавных правых $A$-модулей модуль $M$ наибольшей длины. Поскольку $M$ цепной, у него есть ровно один максимальный и ровно один минимальный подмодуль. Но тогда из следствий III.2.8 и IX.1.7 вытекает, что $M$ — главный и коглавный модуль, т. е. $M$ биективен.

5) $\Rightarrow$ 4). Пусть $M$ — неразложимый $A$-модуль, $W$ — биективный модуль над факторалгеброй $B = A/\mathrm{Ann}\, M$. Поскольку $M$ — точный неразложимый $B$-модуль, из леммы о выбрасывании (лемма IX.2.2) сразу следует, что $M$ изоморфен прямому слагаемому $W$, т. е. $B$-модуль $M$ биективен и, в частности, проективен.

3) $\Rightarrow$ 1). Пусть $M$ — неразложимый $A$-модуль. Поскольку он изоморфен фактормодулю главного модуля, в $M$ есть ровно один максимальный подмодуль $M_1 = \mathrm{rad}\, M$ (следствие III.2.8). С другой стороны, $M$ (а потому и $M_1$) изоморфен подмодулю коглавного модуля и, следовательно, неразложим. Поэтому к $M_1$ применимо то же рассуждение: $M_2 = \mathrm{rad}\, M_1$ — единственный максимальный подмодуль в $M_1$, причем $M_2$ также неразложим. Продолжая эту процедуру, мы получим в $M$ цепочку подмодулей $M \supset M_1 \supset M_2 \supset M_3 \supset \ldots$, в которой каждый следующий подмодуль является

единственным максимальным подмодулем в предыдущем. Очевидно, отсюда следует, что $M_1, M_2, M_3, \ldots$ — это все подмодули в $M$, т. е. $M$ цепной. Теорема полностью доказана.

Замечание. В условиях 2), 3) и 4) весьма существенно требование и для правых, и для левых модулей: алгебра может удовлетворять любому из этих условий для правых (или для левых) модулей, но не быть обобщенно однорядной. Простейшим примером для такой алгебры является подалгебра $A \subset M_3(K)$, состоящая из всех матриц вида

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_4 & 0 \\ 0 & 0 & a_5 \end{pmatrix}, \quad a_i \in K.$$

Как показано в упражнении 1 к гл. X, эта алгебра не является обобщенно однорядной, однако для нее выполнены условия 3) и 4) для правых модулей и условие 2) для левого регулярного модуля.

Поскольку подмодуль главного модуля над обобщенно однорядной алгеброй однозначно определяется своей длиной, мы получаем и аналог следствия IX.4.3.

**Следствие 1.2.** *Неразложимый модуль над обобщенно однорядной алгеброй однозначно (с точностью до изоморфизма) определяется своей длиной и проективным накрытием (или инъективной оболочкой).*

Поскольку обобщенная однорядность может быть охарактеризована в терминах категории модулей (например, условием 1) теоремы 1.1), однотипные алгебры обобщенно однорядны одновременно. В частности, алгебра $A$ обобщенно однорядна тогда и только тогда, когда обобщенно однорядна ее базисная алгебра.

Условие 2) теоремы 1.1 показывает, что алгебра $A$ обобщенно однорядна тогда и только тогда, когда всякий подмодуль главного правого и главного левого $A$-модуля содержит один максимальный подмодуль. Оказывается, это условие достаточно проверить только для максимальных подмодулей главных модулей.

**Предложение 1.3.** *Предположим, что радикал любого главного правого (левого) $A$-модуля содержит ровно один максимальный подмодуль. Тогда всякий главный правый (левый) $A$-модуль цепной.*

Доказательство. Пусть $P$ — произвольный главный $A$-модуль, $M_1 = \operatorname{rad} P$ — его единственный максимальный подмодуль. Поскольку $M_1$ содержит ровно один максимальный подмодуль $M_2 = \operatorname{rad} M_1$, он является фактормодулем некоторого главного $A$-модуля $P_1$ (следствие III.2.8), а тогда $M_2$ есть фактормодуль $\operatorname{rad} P_1$. Но $\operatorname{rad} P_1$ в свою очередь является фактормодулем главного $A$-модуля $P_2$, следовательно, и $M_2$ — фактормодуль $P_2$, т. е. содержит один максимальный подмодуль $M_3 = \operatorname{rad} M_2$. Аналогично и $M_3$ есть фактормодуль некоторого главного $A$-модуля $P_3$ и т. д. Продолжая этот процесс, мы получим в $P$ ряд подмодулей $P \supset \supset M_1 \supset M_2 \supset M_3 \supset \ldots$, в котором каждый последующий явля-

ется единственным максимальным подмодулем в предыдущем. Отсюда, очевидно, следует, что всякий подмодуль $P$ совпадает с каким-нибудь $M_i$. Значит, $P$ цепной.

**Следствие 1.4.** *Алгебры $A$ и $A/R^2$, где $R = \operatorname{rad} A$, обобщенно однорядны одновременно.*

Для доказательства достаточно напомнить, что $\operatorname{rad} P = PR$, а $\operatorname{rad}(\operatorname{rad} P) = PR^2$, и по предложению 1.3 достаточно проверять простоту модулей $PR/PR^2$ ($RQ/R^2Q$) для каждого главного правого модуля $P$ (левого главного модуля $Q$).

Из этого результата и теоремы IX.3.7 вытекает такое следствие.

**Следствие 1.5.** *Если факторалгебра $A/R^2$, где $R = \operatorname{rad} A$, квазифробениусова, то $A$ обобщенно однорядна.*

Доказательство. Пусть $P$ — главный правый модуль над алгеброй $A/R^2$. Если он не прост, т. е. $\operatorname{rad} P \neq 0$, то его единственный максимальный подмодуль $\operatorname{rad} P$ совпадает с цоколем (поскольку $(\operatorname{rad} P)R = PR^2 = 0$). Тогда по теореме IX. 3.7 $\operatorname{rad} P$ прост. Значит, $P$ цепной. Аналогично и всякий левый главный $A/R^2$-модуль является цепным. Поэтому $A/R^2$, а следовательно, и $A$ обобщенно однорядна.

Замечание. Как показывает пример алгебры треугольных матриц, обратное утверждение неверно: если алгебра $A$ обобщенно однорядна, то $A/R^2$ может и не быть квазифробениусовой.

## § 2. Праворядные алгебры

Перейдем к изучению строения обобщенно однорядных алгебр. На самом деле мы опишем строение более широкого класса алгебр — праворядных, т. е. таких, у которых регулярный правый модуль является полуцепным. Аналогичное описание допускают, конечно, и леворядные алгебры, т. е. такие, над которыми регулярный левый модуль полуцепной. Формулировки соответствующих утверждений для леворядных алгебр мы оставляем читателю.

Заметим, что из предложения 1.3 вытекает такое следствие.

**Следствие 2.1.** *Алгебры $A$ и $A/R^2$ праворядны одновременно.*

Доказательство аналогично доказательству следствия 1.4 (без упоминания о левых модулях).

Более того, праворядность полностью характеризуется схемой алгебры (см. § 6 гл. III).

**Теорема 2.2.** *Алгебра $A$ праворядна тогда и только тогда, когда из каждой точки схемы $S(A)$ выходит не более одной стрелки.*

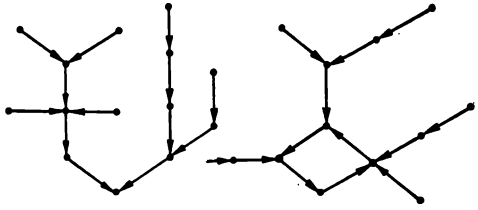
Доказательство. Ввиду предложения 1.3 праворядность равносильна тому, что для всякого главного (правого) $A$-модуля $P_i$ его радикал $\operatorname{rad} P_i$ либо нулевой, либо изоморфен фактормодулю главного модуля $P_j$. Но это и означает, что либо из точки $i$ схемы $S(A)$ не выходит ни одной стрелки, либо выходит ровно одна стрелка (в точку $j$).

Для описания схем праворядных алгебр введем следующие определения. Контуром схемы $S$ назовем такой набор попарно различных точек $\{i_1, \ldots, i_t\}$ и стрелок $\{\sigma_1, \ldots, \sigma_t\}$, что каждая стрелка $\sigma_k$ ведет либо из $i_k$ в $i_{k+1}$, либо из $i_{k+1}$ в $i_k$ (считая, что $i_{t+1} = i_1$).

Заметим, что, возможно, $t=1$. Конечно, всякий цикл является контуром, но обратное утверждение, вообще говоря, неверно. Связная схема без контуров называется деревом. Концевой точкой схемы $S$ назовем такую точку, из которой не выходит ни одной стрелки.

**Следствие 2.3.** *Неразложимая в прямое произведение алгебра $A$ праворядна тогда и только тогда, когда $S(A)$ есть либо дерево с одной концевой точкой, либо схема с одним контуром, который является циклом, такая, что если из нее удалить все стрелки, входящие в цикл, то получится несвязное объединение деревьев, все концевые точки которых — это точки, лежащие на цикле.*

Ниже приведены примеры таких схем.



Доказательство. Предположим, что $A$ праворядна, т. е. из каждой точки $S(A)$ выходит не более одной стрелки. Пусть набор точек $\{i_1, \ldots, i_t\}$ и стрелок $\{\sigma_1, \ldots, \sigma_t\}$ есть контур. Для определенности будем считать, что $\sigma_1 : i_2 \to i_1$. Тогда $\sigma_2 : i_2 \to i_3$ невозможно. Значит, $\sigma_2 : i_3 \to i_2$. Аналогично $\sigma_3 : i_4 \to i_3, \ldots, \sigma_t : i_1 \to i_t$, т. е. набор стрелок $\{\sigma_t, \sigma_{t-1}, \ldots, \sigma_1\}$ есть цикл (если $\sigma_1 : i_1 \to i_2$, то $\{\sigma_1, \sigma_2, \ldots, \sigma_t\}$ есть цикл). В частности, если в $S(A)$ нет циклов, то $S(A)$ — дерево. Предположим, что в $S(A)$ есть две концевые точки $i$, $j$, $i \neq j$. Обозначим через $S_1(S_2)$ множество тех точек схемы $S(A)$, из которых ведет путь в точку $i(j)$. Тогда, поскольку из точки выходит не более одной стрелки, точки $S_1$ и $S_2$ не могут быть соединены между собой стрелками и схема $S(A)$ несвязна, т. е. алгебра $A$ разложима (теорема III.6.2). Значит, в этом случае в $S(A)$ есть ровно одна концевая точка.

Пусть теперь $\{\sigma_1, \sigma_2, \ldots, \sigma_t\}$ — цикл в схеме $S(A)$. Очевидно, можно считать, что все стрелки $\sigma_k$ различны, причем если $\sigma_k : i_k \to i_{k+1}$ $(i_{t+1} = i_1)$, то и все точки $i_1, \ldots, i_t$ различны. Тогда $\sigma_k$ — это единственная стрелка, выходящая из точки $i_k$. Обозначим через $S_k$ множество тех точек схемы $S(A)$, из которых в точку $i_k$ ведет путь, не содержащий ни одной стрелки из данного цикла (считая и саму точку $i_k$), $S_0 = S \setminus \bigcup_{k=1}^{t} S_k$. Поскольку в $S(A)$ всякий контур является циклом, множества $S_k$ попарно не пересекаются. Если точка $i \in S_k$ $(k > 0)$, а $\sigma$ — первая стрелка пути, ведущего из $i$ в $i_k$, то $\sigma$ — единственная стрелка, выходящая из точки $i$. Поэтому в $S_k$ не может быть циклов (значит, и контуров). Кроме того, всякая стрелка, выходящая из точки $i \in S_k$, ведет сно-

ва в точку $j \in S_k$. Наконец, из точки $i \in S_0$ также не может вести стрелка в точку $j \in S_k$ ($k > 0$). Ввиду связности $S(A)$, это означает, что $S_0 = \varnothing$. Если из $S(A)$ удалить все стрелки $\sigma_1, \ldots, \sigma_t$, то останется несвязное объединение схем $S_k$, каждая из которых — дерево с единственной концевой точкой $i_k$.

Наоборот, пусть вначале $S(A)$ — дерево с одной концевой точкой. Покажем, что из каждой точки $i$ выходит не более одной стрелки. Действительно, пусть $\sigma$ и $\tau$ — две стрелки, выходящие из точки $i$. Поскольку в $S(A)$ нет циклов, длины всех путей ограничены и можно рассмотреть самые длинные пути $\varphi$ и $\psi$, начинающиеся соответственно со стрелок $\sigma$ и $\tau$. Тогда, если $\varphi : i \to j$, а $\psi : i \to k$, то $j$ и $k$ — концевые точки, откуда $j = k$, что невозможно, так как в $S(A)$ нет контуров.

Пусть теперь $\{\sigma_1, \ldots, \sigma_t\}$ — единственный цикл схемы $S(A)$, причем после удаления стрелок $\sigma_1, \ldots, \sigma_t$ схема превращается в несвязное объединение деревьев $S_k$, все концевые точки которых — это точки $i_1, \ldots, i_t$, лежащие на цикле. Тогда $\sigma_k$ — единственная стрелка, выходящая из точки $i_k$. А если точка $i$ не лежит на цикле, то, как было показано выше, из нее также выходит не более одной стрелки. Следовательно, алгебра $A$ праворядна и утверждение полностью доказано.

Напомним, что типом алгебры $A$ (§ 5 гл. VIII) называется пара $(B, V)$, где $B = A/R$, $V = R/R^2$. Из предложения 1.3 вытекает такое следствие.

**Следствие 2.4.** *Пусть $(B, V)$ — тип алгебры $A$. Алгебра $A$ праворядна тогда и только тогда, когда для любого минимального идемпотента $e \in B$ правый $B$-модуль $eV$ прост (или нулевой).*

$B$-бимодуль $V$, удовлетворяющий этому условию, будем называть праворядным.

Из следствия 2.4 и теоремы VIII.5.2 мы непосредственно получаем следующий результат.

**Теорема 2.5.** *Всякая праворядная алгебра сепарабельного типа изоморфна факторалгебре тензорной алгебры $T(V)$, где $V$ — праворядный бимодуль над сепарабельной алгеброй $B$, по некоторому правильному идеалу. Наоборот, всякая такая факторалгебра праворядна.*

Таким образом, для описания праворядных алгебр сепарабельного типа достаточно указать все правильные идеалы в тензорной алгебре $T = T(V)$ праворядного бимодуля $V$ над полупростой алгеброй $B$.

Пусть $1 = e_1 + \ldots + e_n$ — разложение единицы алгебры $B$, в котором идемпотенты $e_i$ минимальны, $I$ — правильный идеал алгебры $T$. Обозначим $T_i = e_i T$, $J_i = e_i J$ (где $J$ — фундаментальный идеал алгебры $T$, см. § 5 гл. VIII), $I_i = e_i I$. Тогда $I_i = T_i I$ — подмодуль в $T_i$, причем $I$ правильный тогда и только тогда, когда $T_i J^2 \supset I_i \supset T_i J^m$ для некоторого $m$, т. е. $l_i = l(T_i/I_i) < \infty$, причем если $J_i \neq 0$ (это равносильно тому, что $V_i = e_i V \neq 0$), то

$l_i \geqslant 2$. Из теоремы 2.5 следует, что $T_i/T_iJ^m$ — цепной модуль. Значит, задание $l_i$ однозначно определяет подмодуль $I_i = T_iJ^{l_i}$.

Наоборот, задав числа $l_i$, можно построить правый идеал $I = \bigoplus_{i=1}^{n} I_i$, где $I_i = T_iJ^{l_i}$, и нам нужно выяснить, при каких ограничениях на $l_i$ этот идеал будет двусторонним.

Заметим прежде всего, что если простые $B$-модули $e_iB$ и $e_jB$ изоморфны, то $e_i$ и $e_j$ сопряжены: $e_j = ae_ia^{-1}$, где $a$ — обратимый элемент в $B$. Тогда $aI_i = ae_iI = e_jaI = e_jI$, откуда следует, что $l_i = l(T_i/I_i) = l(T_j/I_j) = l_j$. Иными словами, соответствие $i \to l_i$ определяет функцию на схеме $S$ типа $(B, V)$.

Пусть теперь $e_iB \not\simeq e_jB$, причем на схеме $S$ из точки, соответствующей $e_i$, в точку, соответствующую $e_j$, ведет стрелка. Это означает, что $V_i = e_iV \simeq e_jB$. Тогда, поскольку $J = VT$, $T_iJ = e_iTJ = e_iVT = V_iT$, а $T_iJ^2 = V_iTJ = V_iV_jT$. Продолжая этот процесс, мы получаем

$$I_i = TJ^{l_i} = V_{i_1}V_{i_2}\ldots V_{i_l}T, \quad l = l_i,$$

где $\{i = i_1, i_2, \ldots, i_l\}$ — единственный набор индексов, такой, что на схеме $S$ из точки $i_k$ в точку $i_{k+1}$ ведет стрелка ($k = 1, \ldots, l-1$). Отсюда, в частности, следует, что $BI = I$, а $VI \subset I$ тогда и только тогда, когда для любой точки $i_0$, из которой в $i$ ведет стрелка, $V_{i_0}V_{i_1}\ldots V_{i_l}T \subset I$. Но $V_{i_0}V_{i_1}\ldots V_{i_l}T \subset e_{i_0}T$. Значит, $V_{i_0}V_{i_1}\ldots V_{i_l}T \subset I_{i_0} = V_{i_0}V_{i_1}\ldots V_{i_m}T$, где $m = l_{i_0} - 1$, что равносильно неравенству $l \geqslant m$, т. е. $l_i \geqslant l_{i_0} - 1$.

Если же точка $i$ — концевая на схеме $S$, то, очевидно, $V_i = 0$ и обязательно $l_i = 1$. Окончательно получаем такой результат.

**Предложение 2.6.** *Пусть $B$ — полупростая алгебра, $V$ — праворядный $B$-бимодуль, $S$ — схема типа $(B, V)$. Правильный идеал $I \subset T(V)$ однозначно определяется заданием для каждой точки $i \in S$ натурального числа $l_i$, такого, что $l_i = 1$ для любой концевой точки и $2 \leqslant l_i \leqslant l_j + 1$, если из точки $i$ в точку $j$ ведет стрелка.*

Из описания правильных идеалов в $T(V)$ уже нетрудно получить полную классификацию алгебр сепарабельного типа.

**Теорема 2.7.** *Праворядная алгебра $A$ сепарабельного типа $(B, V)$ определяется заданием для каждой точки $i \in S(A)$ натурального числа $l_i$, такого, что если $i$ — концевая точка, то $l_i = 1$, а если из $i$ в $j$ ведет стрелка, то $2 \leqslant l_i \leqslant l_j + 1$. При этом наборы $\{B, V, l_1, \ldots, l_s\}$ и $\{B', V', l'_1, \ldots, l'_{s'}\}$ определяют изоморфные алгебры тогда и только тогда, когда существует изоморфизм алгебр $\varphi: B \to B'$ и изоморфизм $B$-бимодулей [18] $f: V \to V'$, такие, что $l'_{\sigma(i)} = l_i$, где $\sigma$ — изоморфизм схем типа $(B, V)$ и типа $(B', V')$, индуцированный парой $(\varphi, f)$.*

---

[18] $V'$ превращается в $B$-бимодуль, если положить $b_1vb_2 = \varphi(b_1)v\varphi(b_2)$ для любых $v \in V'$, $b_1, b_2 \in B$.

Доказательство. Учитывая теорему VIII.5.2 и предложение 2.6, нам остается проверить только критерий изоморфизма. Предположим, что алгебра $A$, определенная набором $\{B, V, l_1, \ldots, l_s\}$, изоморфна алгебре $A'$, определенной набором $\{B', V', l'_1, \ldots, l'_{s'}\}$. Тогда изоморфизм $\psi: A \to A'$, очевидно, индуцирует изоморфизмы $\varphi: B \to B'$ и $f: V \to V'$, поскольку $B = A/R$, $B' = A'/R'$, $V = R/R^2$ и $V' = R'/R'^2$, где $R = \operatorname{rad} A$, $R' = \operatorname{rad} A'$. При этом если $A = P_1 \oplus \ldots \oplus P_n$, где $P_i$ — главные $A$-модули, то $A' = P'_1 \oplus \ldots \oplus P'_n$, где $P'_i = \psi(P_i)$ — главные $A'$-модули, причем $l(P_i) = l(P'_i)$. Но если $i$ — точка схемы $S(A)$, то число $l_i$, как мы видели, есть не что иное, как длина соответствующего главного $A$-модуля. Следовательно, $l'_{\sigma(i)} = l'_i$, где $\sigma: S(A) \to S(A')$ — изоморфизм схем, индуцированный изоморфизмом $\psi$, или парой $(\varphi, f)$.

Наоборот, если существуют $\varphi$ и $f$ с указанными свойствами, то, очевидно, изоморфизм $T(V) \to T(V')$, индуцированный парой $(\varphi, f)$, переводит идеал $I$, заданный набором $(l_1, \ldots, l_s)$, в идеал $I'$, заданный набором $(l'_1, \ldots, l'_s)$. Значит, факторалгебры $T(V)/I$ и $T(V')/I'$ также изоморфны и теорема доказана.

Если алгебра $A$ расщепима (например, поле $K$ алгебраически замкнуто), то тип алгебры $A$ определяется заданием «кратностей» $n_i$ для каждой точки $i \in S(A)$: это соответствует разложению $A/R \simeq \prod_{i=1}^{s} M_{n_i}(K)$. Поэтому для таких алгебр мы получаем следствие.

**Следствие 2.8.** *Расщепимая праворядная алгебра определяется набором $\{S; n_1, \ldots, n_s; l_1, \ldots, l_s\}$, где $S$ — схема, связные компоненты которой удовлетворяют условию, сформулированному в следствии 2.3, а $n_i$ и $l_i$ ($i \in S$) — натуральные числа, причем $l_i = 1$, если точка $i$ концевая, и $2 \leqslant l_i \leqslant l_j + 1$, если из $i$ в $j$ ведет стрелка. Наборы $\{S; n_1, \ldots, n_s; l_1, \ldots, l_s\}$ и $\{S'; n'_1, \ldots, n'_{s'}; l'_1, \ldots, l'_{s'}\}$ определяют изоморфные алгебры тогда и только тогда, когда существует изоморфизм схем $\sigma: S \to S'$, такой, что $l'_{\sigma(i)} = l_i$ и $n'_{\sigma(i)} = n'_i$ для любой точки $i \in S$.*

## § 3. Строение обобщенно однорядных алгебр

Поскольку обобщенно однорядные алгебры являются, в частности, праворядными, к ним применимы все результаты предыдущего параграфа. Нужно только уточнить вид схемы и возможные типы таких алгебр.

**Теорема 3.1.** *Пусть $A$ — неразложимая в прямое произведение алгебра, $(B, V)$ — ее тип, причем $B = M_{n_1}(D_1) \times \ldots \times M_{n_s}(D_s)$, где $D_i$ — тела. Алгебра $A$ обобщенно однорядна тогда и только тогда, когда $S(A)$ есть либо цикл, либо цепочка и, кроме того, $D_1 \simeq D_2 \simeq \ldots \simeq D_s$.*

Доказательство. Используя следствие 2.4 и его аналог для леворядных алгебр, мы видим, что $A$ обобщенно однорядна тог-

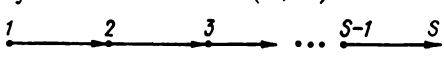
да и только тогда, когда для любого минимального идемпотента $e \in B$ правый $B$-модуль $eV$ и левый $B$-модуль $Ve$ просты. Кроме того, алгебру $A$, очевидно, можно считать приведенной.

Пусть $1 = e_1 + \ldots + e_s$ — разложение единицы алгебры $B$, такое, что $e_iB \simeq D_i$. Из точки $j$ в точку $i$ схемы $S = S(A)$ ведет стрелка тогда и только тогда, когда $V_{ji} = e_jVe_i \neq 0$. Но если $V_{ji} \neq 0$ и $V_{ki} \neq 0$, то левый модуль $Ve_i$ содержит прямые слагаемые $V_{ji}$ и $V_{ki}$ и, следовательно, не прост. Поэтому в каждую точку $i$ схемы $S$ входит не более одной стрелки. Поскольку по теореме 2.2 из каждой точки выходит не более одной стрелки, схема $S$, как легко видеть, может быть либо циклом, либо цепочкой.

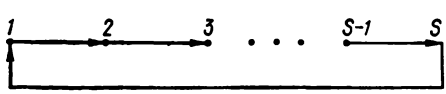
Выберем теперь в $S$ любую пару точек $i$, $j$, такую, что из $j$ в $i$ ведет стрелка. Тогда $V_{ji} \neq 0$, откуда, очевидно, следует, что $e_jV = V_{ji} = Ve_i$ — простой правый $B$-модуль и простой левый $B$-модуль. Поскольку $V_{ji}e_i \neq 0$, то отсюда вытекает, что $V_{ji} \simeq D_i$ как правый $B$-модуль. Аналогично $V_{ji} \simeq D_j$ как левый $B$-модуль. Итак, мы построили $D_j$-$D_i$-бимодуль $U = V_{ji}$, который изоморфен $D_i$ ($D_j$) как правый $D_i$-модуль (левый $D_j$-модуль). Сопоставляя каждому элементу $a \in D_j$ $D_i$-гомоморфизм $U \to U$, переводящий $u \in U$ в $au$, мы получаем гомоморфизм алгебр $\varphi : D_j \to E_{D_i}(U) \simeq D_i$. Поскольку $D_j$ — тело, $\varphi$ — мономорфизм, а поскольку $[D_j : K] = [D_i : K]$, $\varphi$ — изоморфизм, т. е. $D_j \simeq D_i$. Но если алгебра $A$ неразложима, то схема $S$ связна. Значит, все тела $D_1, \ldots, D_s$ изоморфны между собой.

Наоборот, пусть $S$ — либо цепочка, либо цикл и $D_1 \simeq D_2 \simeq \ldots \ldots \simeq D_s$. По теореме 2.2 алгебра $A$ тогда праворядна. Но если $i$ — любая точка схемы $S$, то $Ve_i$ — либо 0, либо совпадает с $V_{ji}$ для единственной точки $j$, из которой в $i$ ведет стрелка. Поскольку $A$ праворядна, $V_{ji}$ — простой правый $B$-модуль, т. е. $V_{ji} \simeq D_i$. С другой стороны, так как $e_jV_{ji} = V_{ji}$, то $V_{ji} \simeq mD_j$ как левый $B$-модуль. Но поскольку $[D_i : K] = [D_j : K]$, это возможно лишь при $m = 1$, а тогда $Ve_i$ — простой левый $B$-модуль и алгебра $A$ леворядна, т. е. и обобщенно однорядна, что и требовалось доказать.

Из теорем 3.1 и 2.7 нетрудно получить полное описание обобщенно однорядных алгебр сепарабельного типа. Поскольку, очевидно, можно ограничиться неразложимыми приведенными алгебрами, нам нужно только описать такие бимодули $V$ над алгеброй $B = D^s$, где $D$ — тело, которые одновременно являются право- и леворядными. В этом случае схема $S$ типа $(B, V)$ есть либо цепочка




либо цикл




Обозначим $V_i = e_iV$, где $e_i$ — минимальный идемпотент алгебры $B$, соответствующий точке $i$ схемы $S$. Тогда $V_i = Ve_{i+1}$, $i = 1, \ldots$

$\ldots, s-1$, а $V_s = 0$ в случае цепочки и $V_s = Ve_1$ в случае цикла. Кроме того, $V_i$ есть одномерный $D$-бимодуль, т. е. $V_i$ задается некоторым автоморфизмом $\sigma_i$ тела $D$ (см. § 1 гл. IV, пример 3). Можно считать, что $V_i = D$, а $a \circ v \circ b = \sigma_i(a)\, vb$ (здесь слева от знака равенства — умножение в $D$-бимодуле $V_i$, а справа — в теле $D$). Рассмотрим автоморфизм $\varphi$ алгебры $B$, который тождествен на всех компонентах, кроме $i$-й, где он индуцирует автоморфизм $\tau$ тела $D$. Тогда на $V$ можно ввести новую структуру $B$-бимодуля $V^{\varphi}$, полагая $a * v * b = \varphi(a) \circ v \circ \varphi(b)$. Если $v \in V_j$, где $j \neq i$ и $j \neq i-1$, то, конечно, $a * v * b = a \circ v \circ b$. Если $v \in V_i$, то $a * v * b = \tau(a) \circ v \circ b = \sigma_i \tau(a)\, vb$. Наконец, если $v \in V_{i-1}$, то $a * v * b = a \circ v \circ \tau(b) = \sigma_{i-1}(a)\, v\tau(b)$. В частности, при $v = 1$, $a * 1 = \sigma_{i-1}(a) = 1 * \tau^{-1}\sigma_{i-1}(a)$, так что автоморфизм, соответствующий $i$-й компоненте бимодуля $V^{\varphi}$, есть $\sigma_i\tau$, а $(i-1)$-й компоненте — $\tau^{-1}\sigma_{i-1}$. По теореме 2.7 пару $(B, V)$ можно заменить на $(B, V^{\varphi})$ (беря за $f$ тождественное отображение $V \to V^{\varphi}$).

Принимая $i = 2$, $\tau = \sigma_1$, мы заменим таким образом исходный набор автоморфизмов на набор с $\sigma_1 = 1$. Затем, принимая $i = 3$, $\tau = \sigma_2$ и т. д., мы добьемся того, что $\sigma_1 = \ldots = \sigma_{s-1} = 1$. В случае, когда $S$ — цикл, остается еще автоморфизм $\sigma = \sigma_s$. Применяя к каждой точке $i \in S$ ту же конструкцию с одним и тем же автоморфизмом $\tau$, мы, как легко убедиться, заменим набор $\{1, \ldots, 1, \sigma\}$ на набор $\{1, \ldots, 1, \tau^{-1}\sigma\tau\}$. Конечно, той же процедурой можно заменить $\{1, \ldots, 1, \sigma\}$ на $\{1, \ldots, 1, \sigma, 1, \ldots, 1\}$ ($\sigma$ — на любом заданном месте).

Заметим теперь, что если $U$ — одномерный $D$-бимодуль, заданный автоморфизмом $\sigma$, а $W$ — одномерный $D$-бимодуль, заданный автоморфизмом $\tau$, то $U \otimes_D W$ — также одномерный $D$-бимодуль, причем если отождествлять $U$ и $W$ с $D$, то $a \circ (1 \otimes 1) = (a \circ 1) \otimes 1 = \sigma(a) \otimes 1 = (1 \circ \sigma(a)) \otimes 1 = 1 \otimes (\sigma(a) \circ 1) = 1 \otimes \tau(\sigma(a)) = (1 \otimes 1) \circ \tau\sigma(a)$, т. е. $U \otimes_D W$ — бимодуль, задаваемый автоморфизмом $\tau\sigma$.

Отсюда следует, что если $B$-бимодуль $V_i$ задается автоморфизмом $\sigma_i$, то бимодуль $\bar{V} = V_1 \otimes_B V_2 \otimes_B \ldots \otimes_B V_s$ задается автоморфизмом $\bar{\sigma} = \sigma_s \ldots \sigma_2\sigma_1$.

Пусть теперь схема $S$ есть цикл, $V'$ — $B$-бимодуль, задаваемый набором автоморфизмов $\{\sigma_1', \ldots, \sigma_s'\}$, $\psi : B \to B$ — автоморфизм алгебры $B$, а $f : V \to V'$ — такой изоморфизм, что $f(a \circ v \circ b) = \psi(a) \circ f(v) \circ \psi(b)$. Тогда, очевидно, $f(V_i) = V'_{k(i)}$, где $k(i)$ — циклическая перестановка номеров $\{1, 2, \ldots, s\}$. Пусть, как и выше, $\bar{V} = V_1 \otimes_B V_2 \otimes_B \ldots \otimes_B V_s$, $\bar{V}' = V'_{k(1)} \otimes_B V'_{k(2)} \otimes_B \ldots \otimes_B V'_{k(s)}$. Тогда $f$ индуцирует отображение $\bar{f} : \bar{V} \to \bar{V}'$, такое, что $\bar{f}(a \circ \bar{v} \circ b) = \psi(a) \circ \bar{f}(\bar{v}) \circ \psi(b)$. Обозначая через $\tau$ автоморфизм тела $D$, с которым совпадает ограничение $\psi$ на первую компоненту алгебры $B$, и принимая за $\bar{v}$ элемент $1 \otimes 1 \otimes \ldots \otimes 1$, получаем

$$\bar{f}(a \circ \bar{v}) = \tau(a) \circ \bar{f}(\bar{v}) = \bar{f}(\bar{v} \circ \bar{\sigma}(a)) = \bar{f}(\bar{v}) \circ \tau\bar{\sigma}(a).$$

Принимая $\bar{f}(\bar{v})$ за базисный элемент одномерного $D$-бимодуля $\bar{V}'$, мы видим, что $\bar{V}'$ — это бимодуль, задаваемый автоморфизмом $\bar{\tau}\bar{\sigma}\bar{\tau}^{-1}$. Но, с другой стороны, $\bar{V}'$ задается автоморфизмом $\bar{\sigma}'=\sigma'_{k(s)}\ldots$ $\ldots\sigma'_{k(2)}\sigma'_{k(1)}$. Следовательно, $\bar{\tau}\bar{\sigma}\bar{\tau}^{-1}$ и $\bar{\sigma}'$ отличаются лишь на внутренний автоморфизм тела $D$ (см. пример 3 из § 1 гл. IV).

Учитывая, что $V$ всегда можно считать заданным набором $\{1, \ldots$ $\ldots, 1, \sigma\}$, мы получаем полную классификацию обобщенно однорядных алгебр сепарабельного типа.

**Теорема 3.2.** *Неразложимая в прямое произведение обобщенно однорядная алгебра сепарабельного типа определяется набором* $\{S, D, \sigma; n_1, \ldots, n_s; l_1, \ldots, l_s\}$, *где* $S$ *— схема, являющаяся цепью или циклом,* $D$ *— сепарабельное тело,* $\sigma$ *— автоморфизм тела* $D$ *(если* $S$ *— цепь,* $\sigma = 1$*);* $n_i$ *и* $l_i$ *— натуральные числа, причем* $2 \leqslant b_i \leqslant l_{i+1} + 1$ *при* $i = 1, \ldots, s-1$, *а* $l_s = 1$, *если* $S$ *— цепь, и* $2 \leqslant l_s \leqslant l_1 + 1$, *если* $S$ *— цикл. При этом тело* $D$ *определено с точностью до изоморфизма, автоморфизм* $\sigma$ *— с точностью до сопряжения и внутреннего автоморфизма, а наборы чисел* $\{n_1, \ldots, n_s\}$ *и* $\{l_1, \ldots, l_s\}$ *определены однозначно, если* $S$ *— цепь, и с точностью до одновременной циклической перестановки, если* $S$ *— цикл.*

Укажем еще критерий обобщенной однорядности для приведенных алгебр, который напоминает характеризацию однорядных алгебр как алгебр главных идеалов.

**Теорема 3.3.** *Приведенная алгебра* $A$ *обобщенно однорядна тогда и только тогда, когда ее радикал* $R$ *является главным левым и главным правым идеалом.*

Доказательство. Очевидно, можно считать, что $A$ неразложима. Если $A$ обобщенно однорядна, то ее схема — либо цепь, либо цикл, т. е. главные правые $A$-модули $P_1, \ldots, P_s$ можно занумеровать так, что $P(P_iR) \simeq P_{i+1}$, $i = 1, \ldots, s-1$, и либо $P_sR = 0$, либо $P(P_sR) \simeq P_1$. Но тогда $P(R) \simeq \bigoplus_{i=1}^{s} P(P_iR)$ изоморфно прямому слагаемому $A$, т. е. $R$ — главный правый идеал. Аналогично $R$ — главный левый идеал.

Наоборот, пусть $R$ — главный левый и главный правый идеал. Тогда существует эпиморфизм $A \to R$. Следовательно, $P(R)$ — прямое слагаемое $A$, т. е. каждый из главных правых модулей $P_i$ входит в $P(R)$ не более одного раза. Пусть $1 = e_1 + \ldots + e_s$ — такое разложение единицы, что $P_i \simeq e_iA$, $V = R/R^2$ и $V_{ij} = e_iVe_j$. Напомним, что $P = P(R) \simeq P(V)$ и $P_i$ входит в $P$ столько раз, сколько раз в $V$ входит простой $A$-модуль $U_i = P_i/P_iR$ (теорема III.3.7). Поэтому существует не более одного номера $j$, такого, что $V_{ji} \neq 0$, причем в этом случае $V_{ji} \simeq U_i$. Аналогично из того, что $R$ — главный левый идеал, следует, что для любого $i$ существует не более одного номера $j$, такого, что $V_{ij} \neq 0$, причем в этом случае $V_{ij}$— простой левый $A$-модуль.

Покажем теперь, что из каждой точки $i$ схемы $S(A)$ выходит не более одной стрелки. Действительно, стрелки в две разные точки

$j$ и $k$, из $i$ выходить не могут, так как тогда было бы $V_{ij} \neq 0$ и $V_{ik} \neq$ $\neq 0$. Если же из $i$ в $j$ идет по крайней мере две стрелки, то в $V_{ij}$ модуль $U_j$ входит по крайней мере дважды, что также невозможно. Следовательно, алгебра $A$ праворядна (теорема 2.2). Аналогично $A$ леворядна, т. е. обобщенно однорядна.

**§ 4. Квазифробениусовы и наследственные праворядные алгебры**

Если квазифробениусова алгебра $A$ праворядна, т. е. всякий главный правый $A$-модуль цепной, то, поскольку левые главные $A$-модули являются коглавными, т. е. двойственны к правым главным, они также цепные и $A$ обобщенно однорядна. Итак, для квазифробениусовых алгебр праворядность, леворядность и обобщенная однорядность являются равносильными свойствами. Следующая теорема дает критерий квазифробениусовости для обобщенно однорядных алгебр.

**Теорема 4.1.** *Пусть $A$ — неразложимая обобщенно однорядная алгебра. $A$ квазифробениусова тогда и только тогда, когда $S(A)$ — цикл, а длины всех главных правых $A$-модулей равны.*

Доказательство. Предположим, что $A$ квазифробениусова. Поскольку $A$ неразложима, из следствия IX. 3. 5 вытекает, что в $S(A)$ нет концевых точек. Значит, $S(A)$ — цикл. Кроме того, если $\varphi : P_j \to R_i$—эпиморфизм главного $A$-модуля $P_j$ на радикал главного $A$-модуля $P_i$, то $\varphi$ — не мономорфизм (иначе $P_j$ как инъективный $A$-модуль выделялся бы из $P_i$ прямым слагаемым, что невозможно). Поэтому $l_j = l(P_j) > l(R_i) = l(P_i) - 1$, или $l_j \geqslant l_i$. Учитывая, что $S(A)$ — цикл, получаем $l_1 \leqslant l_2 \leqslant \ldots \leqslant l_s \leqslant l_1$, т. е. все $l_i$ одинаковые.

Наоборот, пусть $S(A)$ — цикл и $l_1 = \ldots = l_s = l$. Пусть $P = P_i$— главный правый $A$-модуль, $M_k$ — его единственный подмодуль, такой, что $l(P/M_k) = k$ (очевидно, $M_k = PR^k$, где $R = \operatorname{rad} A$). Для удобства обозначим $P_{s+1} = P_1$, $P_{s+2} = P_2$ и т. д. Тогда $P(M_1) \simeq$ $\simeq P_{i+1}$, значит, $M_2$ — эпиморфный образ $R_{i+1}$, откуда $P(M_2) \simeq$ $\simeq P_{i+2}$ и т. д., вообще $P(M_k) \simeq P_{i+k}$ (если только $M_k \neq 0$). В частности, $\operatorname{soc} P = M_{l-1}$, откуда $P(\operatorname{soc} P_i) = P_{i+l-1}$. Очевидно, при разных $i = 1, \ldots, s$ модули $P_{i+l-1}$ неизоморфны. Итак, для любого главного правого $A$-модуля $P_i$ его цоколь — простой модуль и при $P_i \not\simeq P_j$ $\operatorname{soc} P_i \not\simeq \operatorname{soc} P_j$. По теореме IX. 3. 7 $A$ — квазифробениусова алгебра, что и требовалось доказать.

**Следствие 4.2.** *Неразложимая квазифробениусова обобщенно однорядная сепарабельного типа алгебра $A$ определяется набором $\{s, D, \sigma, l; n_1, \ldots, n_s\}$, где $D$— сепарабельное тело, $\sigma$ — автоморфизм $D$, $s$, $l$, $n_1, \ldots, n_s$ — натуральные числа, причем $D$ определено с точностью до изоморфизма, $\sigma$ — с точностью до сопряжения и внутреннего автоморфизма и набор $\{n_1, \ldots, n_s\}$ — с точностью до циклической перестановки ($s$ — число точек цикла $S(A)$ и $l$ — длина главного $A$-модуля определены однозначно).*

Перейдем к описанию наследственных праворядных алгебр. Заметим прежде всего, что по следствию III.7.3 в схеме $S$ такой

алгебры нет циклов. Из следствия 2.3 вытекает, что тогда $S$ — несвязное объединение деревьев с одной концевой точкой. Для алгебр сепарабельного типа полное описание получается из теорем VIII.5.4 и 2.5: такая алгебра изоморфна $T(V)$, где $V$ — такой праворядный бимодуль над сепарабельной алгеброй $B$, что в схеме типа $(B, V)$ нет циклов. Однако, оказывается, это утверждение остается верным и без предположения сепарабельности. Это вытекает из следующего результата.

**Теорема 4. 3.** *Пусть $A$ — конечномерная алгебра, $R = \operatorname{rad} A$, $S = S(A)$, $B = A/R$, $V = R/R^2$. Предположим, что для любой стрелки $\varphi : i \to j$ в схеме $S$ не существует пути $\sigma : i \to j$ длины 2 или более (в частности, в $S$ нет циклов). Тогда алгебра $A$ изоморфна факторалгебре тензорной алгебры $T(V)$ $B$-бимодуля $V$ по некоторому правильному идеалу.*

Доказательство. Как и в доказательстве теоремы VIII.5.2, нам достаточно проверить, что в $A$ содержится подалгебра $\bar{A} \simeq B$, а в $R$ — такой $B$-подбимодуль $\bar{R}$, что $R = \bar{R} \oplus R^2$.

Обозначим через $P_1, \ldots, P_s$ различные $A$-модули, $R_i = \operatorname{rad} P_i$, $R_{ij} = \operatorname{Hom}_A(P_j, P_i)$. Если $f : P_i \to P_i$ — гомоморфизм, который не является изоморфизмом, то $\operatorname{Im} f \subset R_i$. Следовательно, $f = \psi g$, где $\psi : P(R_i) \to R_i$ — эпиморфизм, а $g$ — какой-то гомоморфизм $P_i \to P(R_i)$. Поскольку в $S$ нет циклов, если $P_j$ — прямое слагаемое $P(R_i)$, то $j \neq i$ и из точки $j$ в точку $i$ не ведет путь. Тогда по лемме III. 6. 1 $R_{ji} = 0$, откуда вытекает, что $g = 0$ и $f = 0$. Следовательно, $E_A(P_i) = D_i$ — тело. Пусть $A \simeq n_1 P_1 \oplus \ldots \oplus n_s P_s$. Применяя теорему III. 5.2 к кольцу $A \simeq E_A(A)$, мы видим, что

$$R = \bigoplus_{i \neq j} R_{ij}, \text{ а } B = A/R \simeq \prod_{i=1}^{s} M_{n_i}(D_i), \text{ причем } A \supset \bar{A} \simeq B.$$

Пусть теперь из $i$ в $j$ ведет стрелка. Тогда всякий путь, ведущий из $i$ в $j$, есть стрелка, и из леммы III. 6.1 вытекает, что $R_{ij} \simeq V_{ij} = e_i V e_j$, где $e_i$ и $e_j$ — такие идемпотенты, что $e_i A \simeq P_i$, $e_j A \simeq P_j$. Обозначая $\bar{R} = \bigoplus_{i \to j} R_{ij}$ (сумма берется по таким парам $(i, j)$, что из $i$ в $j$ идет стрелка), мы получаем в $R$ подмодуль, такой, что $R = \bar{R} \oplus R^2$, откуда и вытекает утверждение теоремы.

**Следствие 4.4.** *Праворядная наследственная алгебра изоморфна $T(V)$, где $V$ — такой бимодуль над полупростой алгеброй $B$, что схема типа $(B, V)$ есть несвязное объединение деревьев с одной концевой точкой.*

**Следствие 4.5.** *Наследственная обобщенно однорядная алгебра однотипна прямому произведению алгебр треугольных матриц над телами.*

Доказательство. Очевидно, достаточно проверить, что неразложимая приведенная обобщенно однорядная наследственная алгебра $A$ изоморфна алгебре треугольных матриц над некоторым телом. Но ввиду теоремы 2.3 и следствия 4.4 такая алгебра изо-

морфна $T(V)$, где $V$ — бимодуль над алгеброй $B = D \times \ldots \times D = D^s$ ($D$ — тело), такой, что $V_{ij} = e_i V e_j = 0$, если $j \neq i+1$, и $V_{i(i+1)}$ — регулярный $D$-бимодуль (здесь $1 = e_1 + \ldots + e_s$ — минимальное разложение единицы алгебры $B$). Обозначим через $e_{i(i+1)}$ тот элемент из $V_{i(i+1)}$, для которого $ae_{i(i+1)} = e_{i(i+1)}a$, $a \in D$.

Вычислим $V^{\otimes 2}$. Очевидно, при $j \neq i+1$ $V_{i(i+1)} \otimes_B V_{j(j+1)} = 0$. В то же время $V_{i(i+1)} \otimes_B V_{(i+1)(i+2)} \simeq D \otimes_D D \simeq D$, причем базисом этого модуля является элемент $e_{i(i+2)} = e_{i(i+1)} \otimes e_{(i+1)(i+2)}$. Аналогично строятся элементы $e_{i(i+3)} = e_{i(i+2)} \otimes e_{(i+2)(i+3)}$ и вообще все элементы $e_{ij}$ при $s \geqslant j > i$. Заметим, что $V^{\otimes s} = 0$, так как в схеме типа $(B, V)$ нет путей длины $s$. Поэтому всякий элемент алгебры $T(V)$ однозначно записывается в виде $\sum_{1 \leqslant i < j \leqslant s} a_{ij}e_{ij} = \sum_{i,j} e_{ij}a_{ij}$, где $a_{ij} \in D$. Поскольку, как легко видеть, $e_{ij}e_{kl} = 0$ при $j \neq k$ и $e_{ij}e_{jl} = e_{il}$, то, сопоставляя этому элементу матрицу

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1s} \\ 0 & a_{22} & \ldots & a_{2s} \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & a_{ss} \end{pmatrix},$$

мы получим изоморфизм $T(V) \simeq T_s(D)$, что и требовалось доказать.

Из проведенного вычисления $T(V)$ и теоремы 4.3 мы получаем такое следствие.

**Следствие 4.6.** *Пусть $A$ — неразложимая обобщенно однорядная алгебра, схема которой — цепь. Тогда $A$ однотипна факторалгебре $T_s(D)$, где $D$ — тело.*

## *Упражнения к главе X*

1. Пусть $A \subset M_3(K)$ — подалгебра, состоящая из всех матриц вида

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_4 & 0 \\ 0 & 0 & a_5 \end{pmatrix}, \qquad a_i \in K.$$

а) Проверить, что левый регулярный $A$-модуль полуцепной, а правый — не полуцепной.

б) Пусть $M$ — правый $A$-модуль, $e_{ij}$ — матричные единицы, $M_i = Me_{ii}$. Проверить, что умножение на $e_{12}$ ($e_{13}$) определяет линейное отображение $L_2 : M_1 \to M_2$ ($L_3 : M_1 \to M_3$). Наоборот, пусть $M_1$, $M_2$, $M_3$ — три векторных пространства, $L_2 : M_1 \to M_2$ и $L_3 : M_1 \to M_3$ — линейные отображения. Положим $M = M_1 \oplus M_2 \oplus M_3$ и определим умножение элементов на базисные элементы алгебры по формулам

$$(m_1, m_2, m_3)e_{11} = (m_1, 0, 0);\ (m_1, m_2, m_3)e_{22} = (0, m_2, 0);\ (m_1, m_2, m_3)e_{33} = (0, 0, m_3);\ (m_1, m_2, m_3)e_{12} = (0, m_1L_2, 0);\ (m_1, m_2, m_3)e_{13} = (0, 0, m_1L_3).$$

Проверить, что таким образом $M$ превращается в $A$-модуль, причем если $N$ — другой $A$-модуль, построенный по отображениям $L_2'$ и $L_3'$, то $M \simeq N$ тогда и только тогда, когда существуют такие автоморфизмы $\varphi_i$ пространств $M_i$, $i = 1, 2, 3$, что $L_i' = \varphi_1 L_i \varphi_i$, $i = 2, 3$.

в) Используя указанную в п. б) конструкцию, вычислить все неразложимые $A$-модули и проверить, что они удовлетворяют условиям (3) и (4) теоремы 1.1.

г) Проверить, что rad $A$ является главным правым, но не является главным левым идеалом.

2. Рассмотрим подалгебру $A \subset M_3(\mathbf{C})$, состоящую из всех матриц вида

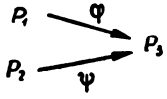
$$\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}, \quad a_1 \in \mathbf{R},\ a_2, a_3 \in \mathbf{C}.$$

Показать, что $A$ праворядна, но не леворядна, причем $S(A)$ — цепь, а rad $A$ — главный правый идеал.

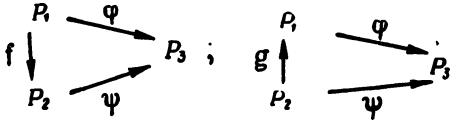
3. Пусть $A = T_2(K)$ (алгебра треугольных матриц), $P_i = e_{ii}A$ ($e_{ii}$ — матричные единицы), $P = 2P_1 \oplus P_2$, $B = E_A(P)$. Доказать, что $B$ — обобщенно однорядная алгебра, но rad $B$ не является главным правым идеалом.

4. Доказать, что если $R = \text{rad}\, A$ является главным правым и главным левым идеалом, то алгебра $A$ обобщенно однорядна. (Указание: пусть $A \simeq \bigoplus_{i=1}^{m} n_i P_i \simeq \bigoplus_{i=1}^{m} n_i P_i'$, где $P_i$ ($P_i'$)—попарно неизоморфные главные правые (главные левые) $A$-модули, причем если $P_i \simeq e_i A$, то $P_i' \simeq Ae_i$; $P(P_i R) = \bigoplus_{j=1}^{m} t_{ij} P_j$; $P(RP_i') = \bigoplus_{j=1}^{m} t_{ij}' P_j'$. Из упражнения 5 гл. III вывести, что $\sum_{i=1}^{m} t_{ij} n_i \leqslant n_j$ и $\sum_{i=1}^{m} t_{ij}' n_i \leqslant n_j$ для любого $j$. Пользуясь тем, что из $t_{ij} = 0$ следует $t_{ji}' = 0$ и наоборот, вывести из этих неравенств, что $\sum_{j=1}^{m} t_{ij} \leqslant 1$ и $\sum_{j=1}^{m} t_{ij}' \leqslant 1$ для любого $i$.) Обратное утверждение ввиду упражнения 3 неверно.

5. Доказать, что алгебра $A$ праворядна тогда и только тогда, когда любую диаграмму вида




где $P_1$, $P_2$, $P_3$ — главные $A$-модули (не обязательно различные), можно дополнить до одной из следующих двух коммутативных диаграмм:




6. Пусть $1 = e_1 + \ldots + e_n$ — минимальное разложение единицы алгебры $A$ ($n \geqslant 3$). Доказать, что алгебра $A$ праворядна (обобщенно однорядна) тогда и только тогда, когда для любой тройки индексов $i$, $j$, $k$ алгебра $eAe$, где $e = e_i +$

$+ e_j + e_k$, праворядна (обобщенно однорядна). (Указание: использовать теорему VIII.4.4 и предыдущее упражнение.)

7. Докажите теорему, аналогичную сформулированной в предыдущем упражнении, для праворядных наследственных алгебр.

8. Пусть $B = D^s$, где $D$ — конечномерное тело, $1 = e_1 + \ldots + e_s$ — минимальное разложение единицы алгебры $B$, $V$ — такой $B$-модуль, что $V_{ij} = e_i V e_j = 0$ для всех пар $(i, j)$, кроме $(i, i+1)$ и $(s, 1)$, $V_{i(i+1)}$ — регулярный $D$-бимодуль, а $V_{s1}$ — $D$-бимодуль, определенный автоморфизмом $\sigma$ тела $D$. Доказать, что тензорная алгебра $T(V)$ изоморфна алгебре матриц вида

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ ta_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ ta_{31} & ta_{32} & a_{33} & \ldots & a_{3n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ ta_{n1} & ta_{n2} & ta_{n3} & \ldots & a_{nn} \end{pmatrix},$$

где $a_{ij}$ — элементы кольца скрученных многочленов $D[t, \sigma]$ (см. упражнение 12 к гл. IX), а ее фундаментальный идеал $J$ состоит из матриц, в которых и все диагональные элементы $a_{ij}$ кратны $t$.

9. Вывести из упражнения 8 описание приведенных обобщенно однорядных алгебр сепарабельного типа. Как нужно изменить конструкцию соответствующей алгебры матриц, чтобы получить и неприведенные кольца?

10. Доказать, что квазифробениусова обобщенно однорядная алгебра $A$ сепарабельного типа $(B, V)$ изоморфна $T(V)/J^k$, где $J$ — фундаментальный идеал тензорной алгебры $B$-бимодуля $V$.

## СПИСОК ЛИТЕРАТУРЫ


1. *Ван дер Варден Б. Л.* Алгебра, М., «Наука», 1976.
2. *Вейль А.* Основы теории чисел. М., «Мир», 1972.
3. *Джекобсон Н.* Теория колец. М., ИЛ, 1947.
4. *Джекобсон Н.* Строение колец. М., ИЛ, 1961.
5. *Кон П.* Свободные кольца и их связи. М., «Мир», 1975.
6. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. М., «Наука», 1969.
7. *Ламбек И.* Кольца и модули. М., «Мир», 1971.
8. *Фейс К.* Алгебра: кольца, модули и категории. М., «Мир», 1977.
9. *Херстейн И.* Некоммутативные кольца. М., «Мир», 1972.
10. *Deuring M.* Algebren. Berlin, 1935.

## ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ . . . . . 3

Глава I. ВВЕДЕНИЕ . . . . . 6

§ 1. Основные понятия. Примеры . . . . . 6
§ 2. Изоморфизм и гомоморфизм. Тела . . . . . 11
§ 3. Представления и модули . . . . . 14
§ 4. Подмодули и фактормодули. Идеалы и факторалгебры . . . 18
§ 5. Теорема Жордана—Гёльдера . . . . . 24
§ 6. Прямые суммы . . . . . 26
§ 7. Эндоморфизмы. Пирсовское разложение . . . . . 28
*Упражнения к главе I* . . . . . 34

Глава II. ПОЛУПРОСТЫЕ АЛГЕБРЫ . . . . . 35

§ 1. Лемма Шура . . . . . 35
§ 2. Полупростые модули и алгебры . . . . . 36
§ 3. Векторные пространства и матрицы . . . . . 39
§ 4. Теорема Веддербёрна—Артина . . . . . 41
§ 5. Единственность разложения . . . . . 42
§ 6. Представления полупростых алгебр . . . . . 43
*Упражнения к главе II* . . . . . 45

Глава III. РАДИКАЛ . . . . . 46

§ 1. Радикал модуля и алгебры . . . . . 47
§ 2. Подъем идемпотентов. Главные модули . . . . . 50
§ 3. Проективные модули. Проективные накрытия . . . . . 53
§ 4. Теорема Крулля—Шмидта . . . . . 57
§ 5. Радикал алгебры эндоморфизмов . . . . . 59
§ 6. Схема алгебры . . . . . 61
§ 7. Наследственные алгебры . . . . . 66
*Упражнения к главе III* . . . . . 68

Глава IV. ЦЕНТРАЛЬНЫЕ ПРОСТЫЕ АЛГЕБРЫ . . . . . 70

§ 1. Бимодули . . . . . 70
§ 2. Тензорные произведения . . . . . 72
§ 3. Центральные простые алгебры . . . . . 75
§ 4. Основные теоремы теории тел . . . . . 76
§ 5. Подполя тел. Поля расщепления . . . . . 78
§ 6. Группа Брауэра. Теорема Фробениуса . . . . . 79
*Упражнения к главе IV* . . . . . 81

Глава V. ТЕОРИЯ ГАЛУА . . . . . 83

§ 1. Элементы теории полей . . . . . 83
§ 2. Конечные поля. Теорема Веддербёрна . . . . . 85
§ 3. Сепарабельные расширения . . . . . 87
§ 4. Нормальные расширения. Группа Галуа . . . . . 90
§ 5. Основная теорема теории Галуа . . . . . 92
§ 6. Скрещенные произведения . . . . . 95
*Упражнения к главе V* . . . . . 100

Глава VI. СЕПАРАБЕЛЬНЫЕ АЛГЕБРЫ . . . . . 103
§ 1. Бимодули над сепарабельными алгебрами . . . . . 104
§ 2. Теорема Веддербёрна—Мальцева . . . . . 106
§ 3. След, норма, дискриминант . . . . . 111
*Упражнения к главе VI* . . . . . 115
Глава VII. ПРЕДСТАВЛЕНИЯ КОНЕЧНЫХ ГРУПП . . . 117
§ 1. Теорема Машке . . . . . 117
§ 2. Число и размерности неприводимых представлений . . . 118
§ 3. Характеры . . . . . 119
§ 4. Теоремы целочисленности . . . . . 122
§ 5. Тензорное произведение представлений . . . . . 124
§ 6. Теорема Бернсайда . . . . . 127
*Упражнения к главе VII* . . . . . 129
Глава VIII. ТЕОРЕМА МОРИТЫ . . . . . 133
§ 1. Категории и функторы . . . . . 134
§ 2. Точные последовательности . . . . . 138
§ 3. Тензорные произведения . . . . . 141
§ 4. Теорема Мориты . . . . . 145
§ 5. Тензорные и наследственные алгебры . . . . . 150
*Упражнения к главе VIII* . . . . . 154
Глава IX. КВАЗИФРОБЕНИУСОВЫ АЛГЕБРЫ . . . . 157
§ 1. Двойственность. Инъективные модули . . . . . 158
§ 2. Лемма о выбрасывании . . . . . 161
§ 3. Квазифробениусовы алгебры . . . . . 163
§ 4. Однорядные алгебры . . . . . 168
*Упражнения к главе IX* . . . . . 170
Глава X. ОБОБЩЕННО ОДНОРЯДНЫЕ АЛГЕБРЫ . . . 172
§ 1. Теорема Накаямы — Скорнякова . . . . . 172
§ 2. Праворядные алгебры . . . . . 175
§ 3. Строение обобщенно однорядных алгебр . . . . . 179
§ 4. Квазифробениусовы и наследственные праворядные алгебры 183
*Упражнения к главе X* . . . . . 185

**Юрий Анатольевич Дрозд,**
**Владимир Васильевич Кириченко**

# КОНЕЧНОМЕРНЫЕ АЛГЕБРЫ

Редактор Ю. Е. Кострица
Переплет художника Ю. О. Стефанишина
Художественный редактор З. Т. Манойло
Технический редактор Н. Н. Бабюк
Корректор А. И. Король

Информ. бланк № 3564

Сдано в набор 28.09.79. Подп. в печать 11.04.80. Формат 60×90/16. Бумага типогр. № 1. Лит. гарн. Выс. печать. 12 усл. печ. л. 12,98 уч.-изд. л. Тираж 2500 экз. Изд. № 1213-к. Зак. № 9-907. Цена 70 к.

Издательство при Киевском государственном университете издательского объединения «Вища школа», 252001, Киев-1, Крещатик, 4.

Киевская книжная типография научной книги республиканского производственного объединения «Полиграфкнига» Госкомиздата УССР, Киев, Репина, 4.