ACTUALITÉS SCIENTIFIQUES ET INDUSTRIELLES

ÉLÉMENTS DE MATHÉMATIQUE

PAR

N. BOURBAKI

PREMIÈRE PARTIE

LES STRUCTURES FONDAMENTALES DE L'ANALYSE

LIVRE II

ALGÈBRE

PARIS
HERMANN & Cie, ÉDITEURS
6, Rue de la Sorbonne, 6

ЭЛЕМЕНТЫ МАТЕМАТИКИ

Н. БУРБАКИ

АЛГЕБРА

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ ЛИНЕЙНАЯ И ПОЛИЛИНЕЙНАЯ АЛГЕБРА

ПЕРЕВОД С ФРАНЦУЗСКОГО
Д. А. РАЙКОВА

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1962

АННОТАЦИЯ

Группа французских математиков, объединенная под псевдонимом «Бурбаки», поставила перед собой цель — написать под общим заглавием «Элементы математики» полный трактат по современной математике. Многие выпуски этого трактата уже вышли во Франции, вызвав большой интерес математиков всего мира.

Настоящей книгой открывается перевод части этого трактата, посвященной алгебре и состоящей из девяти глав.

Книга содержит первые три главы этой части под названиями: «Алгебраические структуры», «Линейная алгебра» и «Полилинейная алгебра».

Книга рассчитана на математиков — научных работников, аспирантов и студентов старших курсов университетов и пединститутов.

Н. Бурбаки.

Алгебра.

М., Физматгиз, 1962 г., 516 стр.

Редактор *С. М. Половинкин.*

Техн. редактор *К. Ф. Брудно.* Корректор *Т. С. Плетнева.*

Сдано в набор 4/IV 1962 г. Подписано к печати 13/X 1962 г. Бумага 60×90/16. Физ. печ. л. 32.25+4 вкл. Условн. печ. л. 34.25. Уч.-изд. л. 29.73. Тираж 10 000 экз. Цена книги 1р. 64 к. Заказ 319.

Государственное издательство физико-математической литературы.
Москва, В-71, Ленинский проспект, 15.

Московская типография № 5 Мосгорсовнархоза. Москва, Трехпрудный пер., 9.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Заниматься алгеброй — значит, по существу, *вычислять*, т. е. выполнять над элементами некоторого множества «алгебраические операции», наиболее известный пример которых доставляют «четыре действия» элементарной арифметики.

Здесь не место описывать медленный, но неуклонный процесс абстракции, посредством которой понятие алгебраической операции, первоначально ограниченное натуральными числами и измеряемыми величинами, постепенно расширялось параллельно расширению понятия «числа», покуда не переросло это последнее и не стало применяться к элементам совершенно не «числового» характера, как, например, перестановки множества (см. Исторический очерк к гл. I). Несомненно, именно возможность этих последовательных расширений, при которых *форма* вычислений оставалась одной и той же, но *природа* математических объектов, над которыми производились вычисления, существенно менялась, позволила постепенно выявить руководящий принцип современной математики: математические объекты сами по себе не столь существенны — важны их *отношения* (см. Книгу 1). Во всяком случае можно определенно утверждать, что алгебра достигла этого уровня абстракции значительно раньше других областей математики, и уже давно стало привычным рассматривать ее как науку об алгебраических операциях, независимую от математических объектов, к которым эти операции могут применяться.

Общепринятое представление, связываемое с обычными алгебраическими операциями, если отвлечься от их конкретного характера, весьма просто: выполнить алгебраическую операцию над двумя элементами a, b одного и того же множества E — значит сопоставить паре (a, b) вполне определенный третий элемент c множества E. Иначе говоря, в этом понятии нет ничего, кроме

понятия *функции*: задать алгебраическую операцию — значит задать функцию, определенную на $E \times E$ и принимающую значения из E; единственная особенность сводится к тому, что областью определения функции служит произведение двух множеств, идентичных с множеством, из которого берутся значения функции; именно такую функцию мы называем *внутренним законом композиции*.

Наряду с этими «внутренними» законами были введены в рассмотрение (главным образом под влиянием геометрии) «законы композиции» другого типа, а именно «внешние» законы, в которых кроме множества E (остающегося, так сказать, на первом плане) участвует еще вспомогательное множество Ω, элементы которого именуются *операторами*: на этот раз закон сопоставляет паре (α, a), образованной оператором $\alpha \in \Omega$ и элементом $a \in E$, некоторый элемент b множества E. Например, в евклидовом пространстве E гомотетия с заданным центром относит вещественному числу k («коэффициенту гомотетии», являющемуся здесь оператором) и точке A пространства E определенную точку A' в E; это — внешний закон композиции в E.

В соответствии с общими определениями (Теор. мн., Рез.*), § 8) задание на множестве E одного или нескольких законов композиции (внутренних или внешних) определяет в E *структуру*; структуры, определяемые таким способом, мы и называем *алгебраическими структурами*, изучение их и составляет предмет алгебры.

Имеются многочисленные *роды* (Теор. мн., Рез., § 8) алгебраических структур, характеризуемые, с одной стороны, определяющими их законами композиции, а с другой — *аксиомами*, которым эти законы подчинены. Разумеется, эти аксиомы не могут выбираться произвольно; они представляют собой не что иное, как свойства, принадлежащие большинству законов композиции, встречающихся в приложениях, таких, как ассоциативность, коммутативность и т. д. Глава I посвящена главным образом изложению этих аксиом и вытекающих из них общих следствий; при этом проведено более подробное исследование двух наиболее

*) «Теор. мн., Рез.» — ссылка на сводку результатов Книги 1 «Теория множеств», перевод которой помещен в виде приложения в книге «Общая топология. Основные структуры» (Физматгиз, М., 1958).

важных родов алгебраических структур, а именно *групповых* (где участвует лишь *один* внутренний закон композиции) и *кольцевых* (с *двумя* внутренними законами композиции), частным случаем которых является структура *тела*.

В главе I определены также *группы с операторами* и *кольца с операторами*, где, наряду с внутренними законами композиции, участвуют один или несколько *внешних* законов. Наиболее важными группами с операторами являются *модули*, к которым относятся, в частности, *векторные пространства*, играющие определяющую роль как в классической геометрии, так и в современном анализе. Изучение модульных структур ведет начало от исследования *линейных уравнений*, откуда и его название — *линейная алгебра*; относящиеся к ней общие результаты будут содержаться в главе II.

Точно так же наиболее часто встречающиеся кольца с операторами — это так называемые *алгебры* (или *гиперкомплексные системы*). В главах III и IV будет проведено подробное исследование двух специальных алгебр: *внешней алгебры*, являющейся, вместе с содержащейся в ней теорией определителей, ценным вспомогательным средством линейной алгебры, и *кольца полиномов*, лежащего в основе теории алгебраических уравнений.

В главе V изложена общая теория *полей* и их классификации. Отправным пунктом этой теории является исследование алгебраических уравнений с одним неизвестным; приведшие к этому вопросы в настоящее время представляют лишь исторический интерес, но сама теория полей продолжает играть фундаментальную роль в алгебре, составляя основу теории алгебраических чисел, с одной стороны, и алгебраической геометрии — с другой.

Поскольку множество натуральных чисел наделено двумя внутренними законами композиции — сложением и умножением,— классическая арифметика (или теория чисел), имеющая своим предметом изучение натуральных чисел, охватывается алгеброй. Однако на почве алгебраической структуры определяемой этими двумя законами, здесь возникает структура, определяемая *отношением порядка* «a делит b»; сущность же классической арифметики как раз и состоит в изучении связей между этими двумя выступающими вместе структурами. И это не единственный пример, когда структура порядка ассоциируется так с некоторой

алгебраической структурой посредством отношения «делимости»: последнее отношение играет отнюдь не менее важную роль в кольцах полиномов. Поэтому оно подвергнуто общему рассмотрению в главе VI; результаты этого рассмотрения применяются в главе VII к установлению модульных структур в некоторых особенно простых кольцах и, в частности, к теории «элементарных делителей».

Глава VIII закладывает начала *некоммутативной алгебры*; особое внимание в ней уделено исследованию некоторых типов модулей и колец, играющих фундаментальную роль во всех вопросах, относящихся к *линейному представлению групп*. Наконец, глава IX посвящена элементарной теории *квадратичных форм*, *эрмитовых форм* и связанных с ними линейных групп — понятий, встречающихся почти во всех областях современной математики.

ГЛАВА I

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

§ 1. Внутренние законы композиции; ассоциативность; коммутативность

1. *Внутренние законы композиции*

Определение 1. *Внутренним законом композиции элементов множества E называется отображение f некоторого подмножества A произведения $E \times E$ в E. Значение $f(x, y)$ отображения f при $(x, y) \in A$ называется композицией x и y относительно этого закона.*

Допуская вольность речи, говорят, что такой закон задан (или определен) на E. Наиболее важны внутренние законы композиции, определенные для всех пар $(x, y) \in E \times E$; допуская вольность речи, говорят, что такой закон *определен всюду на* E. Нас будут интересовать главным образом всюду определенные законы.

Для записи композиции x и y чаще всего выписывают x и y в определенном порядке, отделяя их характеристическим знаком рассматриваемого закона (а иногда уславливаясь этот знак опускать). Из наиболее часто употребляемых знаков укажем уже теперь $+$ и $\cdot$ и согласимся последний знак при желании опускать; посредством этих знаков композиция x и y записывается соответственно в виде $x+y$ и $x \cdot y$ или xy. Закон, обозначаемый знаком $+$, чаще всего называют *сложением* (называя тогда композицию $x+y$ *суммой* x и y) и говорят, что для него принято *аддитивное обозначение*; закон, обозначаемый знаком $\cdot$, чаще всего называют *умножением* (называя тогда композицию $x \cdot y = xy$ *произведением* x и y) и говорят, что для него принято *мультипликативное обозначение*. В общих рассмотрениях §§ 1—5 этой

главы мы будем обычно для обозначения произвольных законов композиции пользоваться символами $\top$ и $\bot$.

В алгебре необходимо уметь *переводить* каждое предложение, относящееся к какому-либо закону композиции, непосредственно с одних обозначений на другие. В целях облегчения задачи читателя в этом отношении в конце книги (вклейка 2) помещен *словарик* терминов и символов, относящихся к основным понятиям, связанным с законами композиции, в переводе на наиболее употребительные обозначения (а именно на аддитивные и мультипликативные).

Примеры. 1) Отображения $(X, Y) \to X \cup Y$ и $(X, Y) \to X \cap Y$ являются (всюду определенными) внутренними законами композиции подмножеств множества E.

2) В множестве N натуральных чисел сложение, умножение и возведение в степень являются всюду определенными законами композиции (композиции $x \in \mathbf{N}$ и $y \in \mathbf{N}$ при этих законах обозначают соответственно $x+y$. xy или $x \cdot y$ и x^y; см. Теор. мн., гл. III).

3) В множестве N натуральных чисел вычитание $x - y$ есть внутренний закон композиции, определенный лишь для тех пар (x, y), в которых $x \geqslant y$; точно так же деление $\frac{x}{y}$ определено лишь для тех пар (x, y), в которых $y \neq 0$ и x кратно y.

4) Пусть E — произвольное множество; отображение $(X, Y) \to X \circ Y$ является законом композиции подмножеств произведения $E \times E$ (Теор. мн., Рез., § 3, n° 10); отображение $(f, g) \to f \circ g$ есть закон композиции отображений E в E (Теор. мн., Рез., § 2, n° 11).

5) В множестве всевозможных отображений подмножеств множества E в E (Теор. мн., Рез., § 3, n° 5) отображение $(f, g) \to f \circ g$ есть внутренний закон композиции, определенный лишь для тех пар (f, g), которые, если обозначить через A и B те подмножества множества E, где определены соответственно f и g, удовлетворяют условию $g(B) \subset A$.

6) Пусть E — решетка (Теор. мн. Рез., § 6, n° 8) и $\sup(x, y)$ означает верхнюю грань множества $\{x, y\}$. Отображение $(x, y) \to \sup(x, y)$ есть всюду определенный закон композиции элементов множества E. Аналогично для нижней грани $\inf(x, y)$. Приведенный выше пример 1 подпадает под это, если считать множество $\mathfrak{P}(E)$ всех подмножеств множества E упорядоченным по включению.

Пусть $(x, y) \to x \top y$ — закон композиции элементов множества E, определенный на некотором подмножестве A произведения $E \times E$. Каковы бы ни были $X \subset E$, $Y \subset E$, будем обозначать через $X \top Y$ (если только это не может повлечь путаницы *)) множество всех

*) Вот пример, в котором этот принцип обозначения мог бы повлечь путаницу и потому не должен применяться. Пусть речь идет о законе ком-

элементов $x \top y \in E$ таких, что $x \in X$, $y \in Y$ и $(x, y) \in A$ (иными словами — образ следа $X \times Y$ на A при отображении $(x, y) \to x \top y$).

Таким образом, отображение $(X, Y) \to X \top Y$ является *всюду определенным* законом композиции подмножеств множества E (если $(x, y) \notin A$, то $\{x\} \top \{y\} = \varnothing$).

Пусть $(x, y) \to x \top y$ — всюду определенный закон композиции элементов множества E; отображение $(x, y) \to y \top x$ также есть всюду определенный закон композиции; он называется *противоположным* предыдущему. Если закон $(x, y) \to x \top y$ определен на некотором подмножестве A произведения $E \times E$, то, поскольку отношение $(y, x) \in A$ эквивалентно отношению $(x, y) \in A^{-1}$ (Теор. мн., Рез., § 3, n° 4), $(x, y) \to y \top x$ есть отображение A^{-1} в E; оно по-прежнему называется законом композиции, *противоположным* предыдущему. Иными словами:

Определение 2. *Два закона композиции элементов множества E* (всюду определенные или нет) *называются противоположными, если каждый из них является композицией канонической симметрии произведения $E \times E$ и другого закона. Если один из них всюду определен, то всюду определен и другой.*

Согласно нашим общим определениям (Теор. мн., Рез., § 8, n° 2), задание закона композиции элементов множества E определяет в этом множестве *структуру*; это — специальный род *алгебраической структуры* (общее определение которой будет дано в § 4 этой главы). Мы будем называть ее структурой, *определяемой* в E рассматриваемым законом композиции.

Пусть E и E' — множества, наделенные каждое структурой, определяемой некоторым внутренним законом композиции; будем обозначать оба эти закона композиции знаком $\top$. Пусть A —

позиции $A \cup B$ подмножеств множества E; он порождает закон композиции $(\mathfrak{A}, \mathfrak{B}) \to F(\mathfrak{A}, \mathfrak{B})$ подмножеств множества $\mathfrak{P}(E)$, где $F(\mathfrak{A}, \mathfrak{B})$ означает множество всех $A \cup B$, в которых $A \in \mathfrak{A}$, $B \in \mathfrak{B}$; но $F(\mathfrak{A}, \mathfrak{B})$ нельзя было бы обозначать $\mathfrak{A} \cup \mathfrak{B}$, поскольку этому обозначению уже приписан другой смысл (а именно объединения $\mathfrak{A}$ и $\mathfrak{B}$, рассматриваемых как подмножества множества $\mathfrak{P}(E)$).

та часть $E \times E$ и A' — та часть $E' \times E'$, где соответственно определены эти два закона. Согласно общим определениям (Теор. мн., Рез., § 8, n° 5), *изоморфизмом E на E'* называется *взаимно однозначное* отображение f E *на* E', распространение которого на $E \times E$ отображает A на A' и для которого

$$f(x \top y) = f(x) \top f(y) \tag{1}$$

всякий раз, когда $x \top y$ определено (т. е. для каждой пары $(x, y) \in A$). Если существует изоморфизм E на E', то говорят, что E и E' *изоморфны* (или что имеется *изоморфизм* их структур).

Более общим образом, говорят, что отображение f E *в* E' есть *представление E в E'*, если всякий раз, когда определена композиция $x \top y$, композиция $f(x) \top f(y)$ также определена и удовлетворяет соотношению (1) (это частный случай понятия, определяемого в § 4 для произвольной алгебраической структуры).

Если закон $\top$ на E всюду определен, то ясно, что изоморфизм E на E' есть не что иное, как *взаимно однозначное представление E на E'*. Но это предложение уже неверно, если закон $\top$ не всюду определен на E, ибо тогда может случиться, что $f(x) \top f(y)$, где f — взаимно однозначное представление E на E', определено, а $x \top y$ — нет.

2. *Композиция серии элементов*

Напомним (Теор. мн., Рез., § 2, n° 14), что *семейство* элементов множества E определяется заданием множества индексов I и его отображения $\iota \longrightarrow x_\iota$ в E; семейство $(x_\iota)_{\iota \in I}$ называется *конечным*, если множество индексов конечно.

Множество индексов I семейства может иногда наделяться *структурой* (Теор. мн., Рез., § 8); если I и K — множества индексов, наделенные структурами одинакового рода, то говорят, что семейства $(x_\iota)_{\iota \in I}$ и $(y_\varkappa)_{\varkappa \in K}$ элементов *одного и того же* множества E *подобны* (относительно структур, заданных в I и K), если существует *изоморфизм* φ I на K такой, что $x_\iota = y_{\varphi(\iota)}$ для каждого $\iota \in I$.

Удобно дать особое наименование семействам, множества индексов которых наделены специальной структурой, особенно когда на множестве индексов одного и того же семейства $(x_\iota)_{\iota \in I}$ рассматриваются различные структуры. Это как раз имеет место в алгебре, где нам придется рассматривать в особенности случай

конечного семейства $(x_\iota)_{\iota \in I}$, множество I индексов которого наделено структурой *совершенно упорядоченного* множества; мы будем говорить, что задание семейства $(x_\iota)_{\iota \in I}$ и структуры совершенно упорядоченного множества в I определяет *серию* элементов множества E; эта серия обозначается по-прежнему $(x_\iota)_{\iota \in I}$, но это обозначение определяет серию лишь при дополнительном указании структуры совершенно упорядоченного множества в I.

Заданному конечному семейству $(x_\alpha)_{\alpha \in A}$ элементов множества E отвечает столько серий, сколько в A имеется структур совершенно упорядоченного множества (т. е. $p!$, если A — множество, состоящее из p элементов); все эти серии должны рассматриваться как различные. В частности, всякой конечной *последовательности* $(x_i)_{i \in H}$, где H — конечное подмножество множества $\mathbf{N}$ натуральных чисел, соответствует специальная серия, получающаяся, если ввести в H структуру, определяемую отношением порядка $m \leqslant n$ между натуральными числами (Теор. мн., Рез., § 6, n°2): рассматривая последовательность как серию без указания отношения порядка в H, мы всегда будем подразумевать, что H наделено этим специальным отношением порядка. При этом условии можно сказать, что любая серия $(x_\alpha)_{\alpha \in A}$ *подобна* (в определенном выше смысле) конечной последовательности, ибо существует взаимно однозначное возрастающее отображение совершенно упорядоченного множества A на некоторый интервал $[0, n]$ множества $\mathbf{N}$.

Пусть теперь E — множество, наделенное *всюду определенным* внутренним законом композиции $\top$.

Определение 3. *Пусть* $(x_\alpha)_{\alpha \in A}$ — *серия элементов из* E. *Для каждого непустого множества* $B \subset A$ (совершенно упорядоченного индуцированным отношением порядка) *композицией серии* $(x_\alpha)_{\alpha \in B}$ (*относительно закона* $\top$) *называется элемент из* E, *обозначаемый* $\top\limits_{\alpha \in B} x_\alpha$, *определяемый индукцией по числу элементов множества* B *следующим образом*:

1° *если* $B = \{\beta\}$, *то* $\top\limits_{\alpha \in B} x_\alpha = x_\beta$;

2° *если* B *состоит из* $p > 1$ *элементов*, β — *его наименьший элемент и* B' — *множество всех элементов* $> \beta$ *из* B, *то* $\top\limits_{\alpha \in B} x_\alpha = x_\beta \top \left(\top\limits_{\alpha \in B'} x_\alpha\right)$.

Легко убедиться (индукцией по числу элементов множеств индексов) в том, что композиции двух *подобных* серий *равны*; в частности, композиция произвольной серии равна композиции некоторой конечной последовательности (что позволяет при желании ограничиться этими последними). Когда A состоит из двух элементов, $A=\{\lambda, \mu\}$ $(\lambda < \mu)$, композиция $\top\limits_{\alpha \in A} x_\alpha$ есть не что иное, как $x_\lambda \top x_\mu$.

Композиция серии $(x_\alpha)_{\alpha \in A}$ относительно закона, обозначаемого $\perp$, записывается в виде $\perp\limits_{\alpha \in A} x_\alpha$; для аддитивно обозначаемого закона принято записывать эту композицию в виде $\sum\limits_{\alpha \in A} x_\alpha$ и называть *суммой* серии $(x_\alpha)_{\alpha \in A}$ (а x_α называть *членами* этой суммы); для закона, обозначаемого мультипликативно, указанную композицию записывают чаще всего в виде $\prod\limits_{\alpha \in A} x_\alpha$ и называют *произведением* серии $(x_\alpha)_{\alpha \in A}$ (а x_α называют *сомножителями* произведения) *).

Если нет опасности недоразумений по поводу множества индексов (а также его структуры порядка), то при обозначении композиции серии это множество часто опускают, т. е., скажем, при аддитивном обозначении закона вместо $\sum\limits_{\alpha \in A} x_\alpha$ пишут $\sum\limits_{\alpha} x_\alpha$ или даже $\sum x_\alpha$; аналогично при других обозначениях.

При законе, обозначаемом $\top$, композиция *последовательности* (x_i), имеющей множеством своих индексов интервал $[p, q]$ множества $\mathbf{N}$, обозначается $\top\limits_{p \leqslant i \leqslant q} x_i$, или $\top\limits_{i=p}^{q} x_i$, или также $x_p \top x_{p+1} \top \ldots \top x_q$; аналогично для законов, обозначаемых другими символами.

Замечания. 1) При не всюду определенном внутреннем законе $\top$ можно по-прежнему вводить понятие композиции серии, как в определении 3, но это определение будет иметь смысл лишь для серий, удовлетворяющих некоторым условиям.

---

*) Однако в случае, когда x_α — множества, употребления этого термина и обозначения $\coprod\limits_{\alpha \in A} x_\alpha$ следует избегать, чтобы не получилось смешения с аналогичными термином и обозначением из теории множеств.

2) Заметим, что в определении композиции серии имеется некоторый произвол; введенная нами индукция действует «справа налево»: композиция последовательности $(x_i)_{1\leqslant i\leqslant n}$ явно заданных n элементов есть не что иное, как $x_1 \top (x_2 \top (x_3 \top (\dots \top (x_{n-1} \top x_n)\dots)))$ ($n-2$ пар скобок). Было бы также вполне законно определять композицию, действуя «слева направо» или любым другим способом (произвольно группируя скобки); но, как мы увидим, этот произвол исчезает в случае наиболее важных на практике *ассоциативных* законов.

3. *Ассоциативные законы*

Определение 4. *Всюду определенный закон композиции* $(x, y) \to x \top y$ *элементов множества* E *называется ассоциативным, если, каковы бы ни были элементы* x, y, z *из* E,

$$(x \top y) \top z = x \top (y \top z). \tag{2}$$

Множество, наделенное структурой, определяемой ассоциативным всюду определенным законом, будет называться моноидом.

Очевидно, закон, противоположный ассоциативному, ассоциативен.

Закон $x \top y$, не являющийся всюду определенным, называют иногда ассоциативным, если ассоциативен порождаемый им (n° 1) закон композиции $X \top Y$ подмножеств множества E, который уже всюду определен; иногда же не всюду определенный закон называют ассоциативным, если соотношение (2) выполнено всякий раз, когда обе его части определены (впрочем, это второе условие является следствием первого). Часть нижеследующих результатов распространяется, с надлежащими видоизменениями, и на не всюду определенные ассоциативные (в одном из указанных двух смыслов) законы.

Примеры. 1) Среди примеров законов композиции, указанных в n° 1, ассоциативны следующие: $X \cap Y$ и $X \cup Y$ (пример 1); $x + y$ и xy (пример 2); $X \circ Y$ и $f \circ g$ (пример 4), $\sup(x, y)$ и $\inf(x, y)$ (пример 6). Если $x \top y$ — ассоциативный закон композиции элементов множества E, то $X \top Y$ есть ассоциативный закон композиции элементов множества $\mathfrak{P}(E)$. С другой стороны, возведение натуральных чисел в степень (пример 2) не ассоциативно; действительно, $(2^1)^2 \neq 2^{(1^2)}$.

2) Свободные моноиды. Пусть A — некоторое множество и E — множество всех *конечных последовательностей* элементов из A; отношение «s и s' — подобные конечные последовательности» (в смысле n° 2), очевидно, есть отношение эквивалентности в E; обозначим через $L(A)$ фактормножество E/R, где R — указанное

отношение. Определим на этом множестве внутренний закон композиции следующим образом.

Рассмотрим два элемента $s=(a_i)_{i\in I}$, $s'=(b_j)_{j\in J}$ из E, где $i<\iota$ при любых $i\in I$, $j\in J$; и пусть $K=I\cup J$ и для каждого $k\in K$ $c_k=a_k$, если $k\in I$, $c_k=b_k$, если $k\in J$; мы будем говорить, что последовательность $s''=(c_k)_{k\in K}$ получена путем *приписывания* s' к s. Нетрудно видеть, что если $s_1\equiv s \pmod R$, $s'_1\equiv s' \pmod R$ и приписывание s'_1 к s_1 определено, то оно дает последовательность $s''_1\equiv s'' \pmod R$; таким образом, класс (mod R) последовательности s'' зависит лишь от классов последовательностей s и s'; будем по-прежнему говорить, что он получен путем *приписывания* класса последовательности s' к классу последовательности s; тем самым нами получен закон композиции в $L(A)$. Этот закон *всюду определен*, ибо для любых двух последовательностей $s=(a_i)_{i\in I}$ и $s'=(b_j)_{j\in J}$ из E существует последовательность s'_1 такая, что $s'_1\equiv s' \pmod R$ и приписывание s'_1 к s определено (если h — наибольший элемент в I, то достаточно рассмотреть множество индексов K, образованное числами $h+j+1$, где j пробегает J, и положить $s'_1=(b_{k-h-1})_{k\in K}$). Кроме того, легко проверить, что этот закон *ассоциативен*.

Множество $L(A)$, наделенное этим законом композиции, называется *свободным моноидом*, порожденным множеством A, а элементы множества $L(A)$ — *словами*, образованными из элементов множества A. Если e — *пустое слово* (класс пустой последовательности), то $ex=xe=x$ для каждого слова x. В каждом непустом слове x существует одна и только одна последовательность $(a_i)_{1\leqslant i\leqslant n}$, множеством индексов которой служит некоторый интервал $[1, n]$ из N; n называют *длиной* слова x и x часто отождествляют с последовательностью (a_i). За длину пустого слова принимают 0.

Основным свойством ассоциативных законов является следующая теорема, выявляющая всё значение понятия композиции серии, определенного в n° 2:

Теорема 1 (теорема ассоциативности). *Пусть A — непустое совершенно упорядоченное конечное множество, являющееся объединением непустых подмножеств B_i $(1\leqslant i\leqslant p)$ таких, что отношения $\alpha\in B_i$, $\beta\in B_j$ $(1\leqslant i<j\leqslant p)$ влекут $\alpha<\beta$; и пусть $(x_\alpha)_{\alpha\in A}$ — серия элементов из E, имеющая A своим множеством индексов. Тогда для каждого ассоциативного закона $\top$, заданного на E, имеет место формула*

$$\top_{\alpha\in A} x_\alpha = \top_{1\leqslant i\leqslant p}\Big(\top_{\alpha\in B_i} x_\alpha\Big). \tag{3}$$

Теорема доказывается индукцией по числу n элементов множества A. Если $n=1$, то, поскольку B_i непустые, необходимо $p=1$, и теорема очевидна. В противном случае, предполагая теорему справедливой для множеств индексов, имеющих меньше чем n элементов, рассмотрим два случая:

а) B_1 состоит из одного элемента β. Пусть $C=B_2 \cup B_3 \cup \ldots \cup B_p$. Левая часть формулы (3) есть (по определению) не что иное, как $x_\beta \top (\top_{\alpha \in C} x_\alpha)$, а правая часть (по определению) — не что иное, как $x_\beta \top (\top_{2 \leqslant i \leqslant p} (\top_{\alpha \in B_i} x_\alpha))$; равенство вытекает из предположенной справедливости теоремы для C и $B_2, B_3, \ldots, B_p$.

б) В противном случае пусть β — наименьший элемент в A (а значит, и в B_1); пусть A' — множество всех элементов $> \beta$ в A, и пусть $B_1' = A' \cap B_1$; так как A' состоит из $n-1$ элемента, а условия теоремы выполнены для A' и его подмножеств $B_1', B_2, \ldots, B_p$, то, согласно предположению,

$$\top_{\alpha \in A'} x_\alpha = (\top_{\alpha \in B_1'} x_\alpha) \top (\top_{2 \leqslant i \leqslant p} (\top_{\alpha \in B_i} x_\alpha)).$$

Образуем композицию x_β с каждой из частей этого равенства; слева мы будем иметь, по определению, $\top_{\alpha \in A} x_\alpha$, справа же (применяя определение ассоциативного закона) получим

$$\left(x_\beta \top \left(\top_{\alpha \in B_1'} x_\alpha\right)\right) \top \left(\top_{2 \leqslant i \leqslant p} \left(\top_{\alpha \in B_i} x_\alpha\right)\right),$$

а это (по определению 4) есть не что иное, как правая часть формулы (3).

В теореме 1 содержится как частный случай формула

$$x_0 \top x_1 \top \ldots \top x_n = (x_0 \top x_1 \top \ldots \top x_{n-1}) \top x_n,$$

позволяющая определять композицию конечной последовательности индукцией, действующей «слева направо» (вместо данного выше определения, действовавшего «справа налево»); таким образом, для ассоциативного закона эти два определения эквивалентны.

Если все члены серии, состоящей из n членов, равны одному и тому же элементу $x \in E$, то их композиция обозначается $\overset{n}{\top} x$ при законе, обозначаемом $\top$, $\overset{n}{\perp} x$ при законе, обозначаемом $\perp$, x^n при законе, обозначаемом мультипликативно, и чаще всего nx

при законе, обозначаемом аддитивно (за исключением некоторых случаев, где это последнее обозначение могло бы повлечь путаницу; см. § 3, n° 1). Теорема ассоциативности в применении к серии, состоящей из одинаковых членов, дает формулу

$$\overset{n_1+n_2+\ldots+n_p}{\top} x = (\overset{n_1}{\top} x) \top (\overset{n_2}{\top} x) \top \ldots \top (\overset{n_p}{\top} x),$$

и значит, в частности, при $p=2$ — формулу

$$\overset{m+n}{\top} x = (\overset{m}{\top} x) \top (\overset{n}{\top} x), \tag{4}$$

а при $n_1=n_2=\ldots=n_p=m$ — формулу

$$\overset{pm}{\top} x = \overset{p}{\top} (\overset{m}{\top} x). \tag{5}$$

Если $X \subset E$, то, в соответствии с введенными обозначениями, $\overset{p}{\top} X$ означает множество $X_1 \top X_2 \top \ldots \top X_p$, где $X_1=X_2=\ldots=X_p=X$; таким образом, это есть множество всевозможных композиций $x_1 \top x_2 \top \ldots \top x_p$, где $x_1 \in X$, $x_2 \in X$, $\ldots$, $x_p \in X$.

Важно не смешивать это множество с множеством композиций $\overset{p}{\top} x$, где x пробегает X.

Положим $\overset{\infty}{\top} X = \bigcup_{p>0} (\overset{p}{\top} X)$; это — множество композиций всевозможных конечных последовательностей, члены которых принадлежат X; в случае ассоциативного закона имеем $X \top (\overset{\infty}{\top} X) = (\overset{\infty}{\top} X) \top X \subset \overset{\infty}{\top} X$.

4. *Устойчивые множества. Индуцированные законы*

Определение 5. *Подмножество A множества E называется устойчивым относительно закона композиции элементов множества E, если композиция двух элементов из A всякий раз, когда она определена, принадлежит A.*

Иными словами, для того чтобы A было устойчиво относительно закона $\top$, необходимо и достаточно, чтобы $A \top A \subset A$.

Пересечение семейства устойчивых подмножеств множества E очевидно устойчиво; поэтому, в частности, существует наименьшее устойчивое подмножество Z множества E, содержащее задан-

ное множество $X \subset E$ (Теор. мн., Рез., § 6, n° 5); его называют устойчивым множеством, *порожденным* множеством X. Индукцией по n легко убедиться в том, что композиция всякой n-членной серии, элементы которой принадлежат X, принадлежит Z; иными словами, всегда $\overset{\infty}{\top} X \subset Z$. При этом имеет место

Теорема 2. *Для ассоциативного закона* $\top$ *на* E *устойчивое множество, порожденное множеством* $X \subset E$, *совпадает с* $\overset{\infty}{\top} X$.

Достаточно убедиться в том, что $\overset{\infty}{\top} X$ при ассоциативности закона $\top$ *устойчиво*; но любые два элемента u и v из $\overset{\infty}{\top} X$ имеют вид $u = x_0 \top x_1 \top \ldots \top x_{n-1}$, $v = x_n \top x_{n+1} \top \ldots \top x_{n+p}$, где $x_i \in X$ $(0 \leqslant i \leqslant n+p)$; следовательно (теорема 1), $u \top v = x_0 \top x_1 \top \ldots \top x_{n+p}$ принадлежит $\overset{\infty}{\top} X$.

Примеры. 1) В множестве N натуральных чисел устойчивым относительно сложения множеством, порожденным множеством, состоящим из одного числа 1, является множество всех натуральных чисел $\geqslant 1$; относительно умножения множество $\{1\}$ само устойчиво.

2) Пусть $\top$ — всюду определенный закон композиции элементов множества E; для того чтобы множество $\{h\}$, состоящее из одного элемента, было устойчивым относительно закона $\top$, необходимо и достаточно, чтобы $h \top h = h$; тогда h называют *идемпотентом*. Например, всякий элемент решетки идемпотентен относительно каждого из законов $\sup(x, y)$ и $\inf(x, y)$.

3) Если $\top$ — ассоциативный закон на множестве E, то устойчивое относительно него множество, порожденное множеством $\{a\}$, состоящим из одного элемента, есть множество, образованное элементами $\overset{n}{\top} a$, где n пробегает все натуральные числа > 0.

4) Из определений примера 2 n° 3 явствует, что каждая непустая конечная последовательность $(x_i)_{i \in I}$ элементов из A представляет собой результат последовательного приписывания одночленных последовательностей $(x_k)_{k=i}$, где i пробегает I; таким образом, свободный моноид $L(A)$ *порождается* пустым словом и множеством всех слов *длины* 1, которое обычно отождествляют с A.

Если $\top$ — всюду определенный закон композиции на E и F — подмножество множества E, *устойчивое* относительно этого закона, то *сужение* функции $x \top y$ на $F \times F$ является *всюду определенным*

законом композиции на F; его называют законом, *индуцированным* на F законом $\top$. Более общим образом:

Определение 6. *Пусть $\top$ — закон композиции элементов множества E, определенный на некоторой части A произведения $E \times E$; законом, индуцированным законом $\top$ на множестве $F \subset E$, называется закон композиции элементов множества F, определенный на множестве тех $(x, y) \in F \times F$, для которых $(x, y) \in A$ и $x \top y \in F$, и относящий каждой такой паре (x, y) композицию $x \top y$. Структуру, определяемую в F этим законом, мы будем называть структурой, индуцированной в F структурой, определяемой законом $\top$ в E.*

Закон, индуцированный на F законом $\top$, мы будем (допуская вольность) обозначать тем же знаком $\top$, если это не сможет внести путаницу.

На множестве, устойчивом относительно ассоциативного закона $\top$, индуцированный им закон ассоциативен.

5. *Перестановочные элементы. Коммутативные законы*

Определение 7. *Пусть $\top$ — закон композиции элементов множества E. Элементы x, y из E называются перестановочными относительно закона $\top$, если $x \top y$ и $y \top x$ определены и $x \top y = y \top x$.*

Определение 8. *Закон композиции $\top$ элементов множества E называется коммутативным, если для любой пары (x, y) элементов из E, для которой $x \top y$ определено, x и y перестановочны.*

Коммутативный закон совпадает с противоположным ему законом.

Примеры. 1) Сложение и умножение натуральных чисел — коммутативные законы.

2) Законы $\sup(x, y)$ и $\inf(x, y)$ в решетке коммутативны; в частности, коммутативны законы композиции $\cup$ и $\cap$ подмножеств множества E.

3) Закон композиции $(X, Y) \to X \circ Y$ подмножеств произведения $E \times E$ не коммутативен (если E содержит более одного элемента): действительно, если $A = \{(a, b)\}$, $B = \{(b, c)\}$ и $a \neq c$, то $B \circ A = \{(a, c)\}$, а $A \circ B = \varnothing$. Но диагональ Δ произведения $E \times E$ перестановочна с каждым его подмножеством. Точно так же закон композиции $f \circ g$ отображений E в E не коммутативен (если E содержит более одного

элемента), в чем можно убедиться, беря в качестве f и g различные постоянные отображения; но тождественное отображение переставновочно со всяким.

4) Если $x \top y$ — коммутативный закон композиции элементов множества E, то $X \top Y$ — коммутативный закон композиции подмножеств множества E.

Предложение 1. *Если элемент x перестановочен с каждым из элементов y и z относительно ассоциативного закона $\top$, то он перестановочен и с $y \top z$.*

Действительно, $x \top (y \top z)$ записывается последовательно в виде

$$x \top (y \top z) = (x \top y) \top z = (y \top x) \top z = y \top (x \top z) = y \top (z \top x) = (y \top z) \top x.$$

Предложение 2. *Если при ассоциативном законе $\top$ каждый элемент множества $X \subset E$ перестановочен с каждым элементом множества $Y \subset E$, то каждый элемент устойчивого множества, порожденного множеством X, перестановочен с каждым элементом устойчивого множества, порожденного множеством Y.*

Действительно, из предложения 1 индукцией по n получается, что если x перестановочен с каждым членом n-членной последовательности, то x перестановочен и с ее композицией; поэтому (теорема 2) каждое $x \in X$ перестановочно с каждым элементом устойчивого множества Y', порожденного множеством Y; но отсюда таким же путем вытекает, что каждый элемент из Y' перестановочен с каждым элементом устойчивого множества X', порожденного множеством X.

Отметим два частных случая предложения 2: когда $X = \{x\}$, $Y = \{y\}$ и когда $X = Y$:

Следствие 1. *Если x и y перестановочны относительно ассоциативного закона $\top$, то это верно и для $\overset{m}{\top} x$ и $\overset{n}{\top} y$, каковы бы ни были целые $m > 0$ и $n > 0$; в частности, $\overset{m}{\top} x$ и $\overset{n}{\top} x$ перестановочны, каковы бы ни были x и целые $m > 0$, $n > 0$.*

Следствие 2. *Если элементы множества X попарно перестановочны относительно ассоциативного закона $\top$, то закон, индуцированный им на устойчивом множестве, порожденном множеством X, ассоциативен и коммутативен.*

Определение 9. *Центральным элементом множества E относительно некоторого закона композиции элементов этого множества называется каждый элемент, перестановочный со всеми элементами из E. Центром множества E называется множество всех его центральных элементов.*

Из предложения 1 вытекает, что центр множества E относительно ассоциативного закона является *устойчивым* множеством; закон композиции, индуцированный на центре, очевидно коммутативен.

Основное свойство законов, *одновременно ассоциативных и коммутативных*, заключается в том, что композиции всех последовательностей, отличающихся от заданной конечной последовательности лишь порядком следования членов, имеют одно и то же значение; докажем это.

Теорема 3 (теорема коммутативности). *Пусть $\top$ — коммутативный ассоциативный закон композиции на E и $(x_\alpha)_{\alpha\in A}$ — непустое конечное семейство элементов из E; каким бы образом ни было совершенно упорядочено множество A, композиция $\top\limits_{\alpha\in A} x_\alpha$ имеет одно и то же значение.*

Если A состоит из одного элемента β, то теорема справедлива; композицией служит тогда x_β. Докажем индукцией по p справедливость теоремы для каждого множества A из p элементов: для этого достаточно показать, что она верна для множества индексов, состоящего из p элементов, если она верна для каждого его подмножества, имеющего менее p элементов. Итак, пусть A — множество, состоящее из p элементов, и $i\to\alpha_i$ — взаимно однозначное отображение интервала $[0, p-1]\subset\mathbf{N}$ на A; перенеся посредством этого отображения порядок интервала $[0, p-1]$ в A, мы совершенно упорядочим A, причем композицией серии $(x_\alpha)_{\alpha\in A}$, определяемой этим отношением порядка, будет не что иное, как $\top\limits_{i=0}^{p-1} x_{\alpha_i}$.

Пусть теперь A совершенно упорядочено иным способом и α_h — наименьший элемент в A при этом упорядочении, а A' — множество всех остальных элементов из A (совершенно упорядоченное индуцированным порядком). Предположим сначала, что $0<h<p-1$, и положим $B=\{\alpha_0, \alpha_1, \ldots, \alpha_{h-1}\}$, $C=\{\alpha_{h+1}, \ldots, \alpha_{p-1}\}$;

так как теорема, по предположению, справедлива для A', то, применяя теорему ассоциативности (поскольку $A' = B \cup C$), имеем

$$\top_{\alpha \in A'} x_\alpha = \left(\top_{i=0}^{h-1} x_{\alpha_i} \right) \top \left(\top_{i=h+1}^{p-1} x_{\alpha_i} \right),$$

откуда, образуя композицию x_{α_h} с обеими частями и повторно применяя коммутативность и ассоциативность $\top$, получаем

$$\top_{\alpha \in A} x_\alpha = x_{\alpha_h} \top \left(\top_{\alpha \in A'} x_\alpha \right) = x_{\alpha_h} \top \left(\top_{i=0}^{h-1} x_{\alpha_i} \right) \top \left(\top_{i=h+1}^{p-1} x_{\alpha_i} \right) =$$

$$= \left(\top_{i=0}^{h-1} x_{\alpha i} \right) \top x_{\alpha_h} \top \left(\top_{i=h+1}^{p-1} x_{\alpha_i} \right) = \top_{i=0}^{p-1} x_{\alpha_i};$$

таким образом, теорема в рассматриваемом случае доказана. Если $h=0$ или $h=p-1$, то получаем тот же результат, но более простым путем, поскольку члены, относящиеся к B или к C, исчезают.

Для коммутативного ассоциативного закона на множестве E *композицией конечного семейства* $(x_\alpha)_{\alpha \in A}$ элементов из E будет, по определению, называться общее значение композиций серий, получаемых при всевозможных способах превращения A в совершенно упорядоченное множество. Эта композиция для закона, обозначаемого $\top$, будет по-прежнему обозначаться $\top_{\alpha \in A} x_\alpha$; аналогично при других обозначениях.

Комбинируя теоремы 1 и 3, получаем:

Теорема 4. *Пусть* $\top$ *— коммутативный ассоциативный закон на* E *и* $(x_\alpha)_{\alpha \in A}$ *— непустое конечное семейство элементов из* E. *Если* A *— объединение своих попарно не пересекающихся непустых подмножеств* $B_1, B_2, \ldots, B_p$, *то*

$$\top_{\alpha \in A} x_\alpha = \top_{i=1}^{p} \left(\top_{\alpha \in B_i} x_\alpha \right). \tag{6}$$

Действительно, это вытекает из теоремы 3, если совершенно упорядочить A так, чтобы B_i удовлетворяли условиям теоремы 1

Отметим два важных частных случая этой теоремы. Во-первых, если $(x_{\alpha\beta})_{(\alpha, \beta) \in A \times B}$ — конечное семейство, множеством индексов

которого служит произведение двух непустых конечных множеств A, B («двойное семейство»), то

$$\top_{(\alpha,\,\beta)\in A\times B} x_{\alpha\beta} = \top_{\alpha\in A}\left(\top_{\beta\in B} x_{\alpha\beta}\right) = \top_{\beta\in B}\left(\top_{\alpha\in A} x_{\alpha\beta}\right); \tag{7}$$

действительно, это вытекает из теоремы 4, если рассматривать $A\times B$, с одной стороны, как объединение множеств $\{\alpha\}\times B$, а с другой стороны, как объединение множеств $A\times\{\beta\}$.

В частности, если B состоит из n элементов и все $x_{\alpha\beta}$ с одним и тем же $\alpha\in A$ имеют одно и то же значение x_α, то

$$\top_{\alpha\in A}\left(\top^{n} x_\alpha\right) = \top^{n}\left(\top_{\alpha\in A} x_\alpha\right). \tag{8}$$

Основываясь на формуле (7), композицию двойной последовательности (x_{ij}), имеющей множеством своих индексов произведение интервалов $[p, q]$ и $[r, s]$ из N, относительно аддитивно обозначаемого коммутативного ассоциативного закона часто обозначают

$$\sum_{i=p}^{q}\sum_{j=r}^{s} x_{ij} \quad \text{или} \quad \sum_{j=r}^{s}\sum_{i=p}^{q} x_{ij},$$

и аналогично для законов, обозначаемых иначе.

Во-вторых, пусть A — множество всех пар целых чисел (i, j) таких, что $0\leqslant i\leqslant n$, $0\leqslant j\leqslant n$ и $i<j$; пусть, далее, композиция семейства $(x_{ij})_{(i,\,j)\in A}$ (относительно коммутативного ассоциативного закона) обозначается по-прежнему $\top_{0\leqslant i<j\leqslant n} x_{ij}$ (или просто $\top_{i<j} x_{ij}$, если это не может повлечь недоразумений); теорема 4 приводит здесь к формулам

$$\top_{0\leqslant i<j\leqslant n} x_{ij} = \top_{i=0}^{n-1}\left(\top_{j=i+1}^{n} x_{ij}\right) = \top_{j=1}^{n}\left(\top_{i=0}^{j-1} x_{ij}\right). \tag{9}$$

Существуют формулы, аналогичные (7), для семейства, множеством индексов которого служит произведение более чем двух множеств, и формулы, аналогичные (9), для семейства, множеством индексов которого является множество S_p *строго возрастающих последовательностей* $(i_k)_{1\leqslant k\leqslant p}$ p целых чисел, в которых $0\leqslant i_k\leqslant n$ $(p\leqslant n+1)$; в этом последнем случае композиция семейства $(x_{i_1\dots i_p})_{(i_1,\dots,i_p)\in B_p}$ обозначается $\top_{0\leqslant i_1<i_2<\dots<i_p\leqslant n} x_{i_1 i_2\dots i_p}$ или просто $\top_{i_1<i_2<\dots<i_p} x_{i_1 i_2\dots i_p}$.

Отметим, наконец, что, в силу следствия 2 предложения 2, теоремы 3 и 4 применимы также в случае ассоциативного закона и семейств элементов, попарно перестановочных относительно этого закона.

Упражнения. 1) Пусть T — закон композиции (всюду определенный или нет) на множестве E. Каковы бы ни были семейства $(X_\alpha)_{\alpha\in A}$ и $(Y_\beta)_{\beta\in B}$ подмножеств из E,

$$(\bigcup_{\alpha\in A} X_\alpha)\,\mathsf{T}\,(\bigcup_{\beta\in B} Y_\beta) = \bigcup_{(\alpha,\beta)\in A\times B} (X_\alpha\,\mathsf{T}\,Y_\beta).$$

2) Пусть T — не всюду определенный закон композиции на множестве E и E' — подмножество множества $\mathfrak{P}(E)$, состоящее из множеств $\{x\}$, где x пробегает E, и пустого подмножества $\varnothing$ множества E. Показать, что E' — устойчивое множество в $\mathfrak{P}(E)$ относительно закона $X\,\mathsf{T}\,Y$; вывести отсюда, что, обозначив через $\bar{E}$ множество, полученное путем *присоединения* (Теор. мн., Рез., § 4, n° 5) к E элемента ω, можно продолжить закон T на $\bar{E}\times\bar{E}$ так, чтобы T совпадал с законом индуцированным на E этим продолженным законом.

3) Пусть T — не всюду определенный закон композиции на E.

а) Для того чтобы закон композиции $X\,\mathsf{T}\,Y$ подмножеств множества E был ассоциативным, необходимо и достаточно, чтобы при любых x, y и z из E, если определена *одна* из частей формулы (2), была определена также вторая и равна первой. [При доказательстве достаточности условия использовать упражнение 1.]

б) Предполагая это условие выполненным, показать, что теорема 1 обобщается следующим образом: если определена одна из частей формулы (3), то определена также вторая и равна первой.

4) а) Пусть E — заданное множество, Φ — множество всех отображений в E всевозможных его подмножеств и f, g, h — элементы из Φ. Показать, что если композиция $(f\circ g)\circ h$ определена, то определена и композиция $f\circ(g\circ h)$, но обратное неверно; если же обе эти композиции определены, то они равны.

б) Пусть $\mathfrak{R}$ — семейство попарно не пересекающихся непустых подмножеств множества E и Ψ — подмножество множества Φ, образованное всевозможными *взаимно однозначными* отображениями множества из $\mathfrak{R}$ *на* множество из $\mathfrak{R}$. Показать, что для закона, индуцированного на Ψ законом $f\circ g$, условие упражнения 3а) выполнено.

°5) Показать, что единственными тройками (m, n, p) натуральных чисел $\neq 0$, для которых $(m^n)^p = m^{np}$, являются: $(1, n, p)$, где n и p произвольны; $(m, n, 1)$ и $(m, 2, 2)$, где m и n произвольны.

6) Пусть T — всюду определенный закон композиции элементов множества E и A — подмножество множества E, образованное

элементами x, для которых $x \top (y \top z) = (x \top y) \top z$, каковы бы ни были y и z из E. Показать, что A — устойчивое множество и закон, который $\top$ индуцирует на A, ассоциативен.

7) Если $\top$ — ассоциативный закон на E, то, каковы бы ни были элементы a и b из E, множества $\{a\} \top E$, $E \top \{b\}$, $\{a\} \top E \top \{b\}$ и $E \top \{a\} \top E$ устойчивы относительно $\top$.

8) Пусть $\top$ — ассоциативный закон на E и a — элемент из E; для любых x и y из E положим $x \perp y = x \top a \top y$. Показать, что закон $\perp$ ассоциативен.

9) Отображения $(x, y) \to x$ и $(x, y) \to y$ являются противоположными ассоциативными законами композиции на множестве E.

10) Пусть X и Y — произвольные подмножества множества E; положим $X \top Y = X \cup Y$, если $X \cap Y = \varnothing$, и $X \top Y = E$, если $X \cap Y \neq \varnothing$. Показать, что определенный так закон композиции на $\mathfrak{P}(E)$ ассоциативен и коммутативен.

11) Пусть $\top$ — ассоциативный закон на E и $A \subset E$, $B \subset E$ — устойчивые относительно него множества. Показать, что если $B \top A \subset A \top B$, то $A \top B$ устойчиво относительно $\top$.

°12) Единственными различными натуральными числами $\neq 0$, перестановочными относительно закона $(x, y) \to x^y$, являются 2 и 4.

13) Показать, что относительно закона композиции $X \circ Y$ подмножеств произведения $E \times E$ центром служит множество $\{\varnothing\} \cup \{\Delta\}$ (где Δ — диагональ $E \times E$).

14) Показать, что относительно закона композиции $f \circ g$ отображений E в E центр сводится к тождественному отображению.

15) Закон, заданный на множестве E, называют *идемпотентным*, если все элементы из E идемпотентны (n° 4) относительно этого закона, т. е. если $x \top x = x$ для каждого $x \in E$. Показать, что если закон $\top$ на E ассоциативен, коммутативен и идемпотентен, то отношение $x \top y = y$ есть отношение порядка в E; записывая его $x \leqslant y$, показать, что любые два элемента x, y из E обладают верхней гранью (относительно этого отношения порядка), равной $x \top y$. Обращение.

16) Пусть E — моноид (n° 3) и X — устойчивое множество, порожденное непустым множеством $A \subset E$. Показать, что если каждому слову $u = (a_i)_{0 \leqslant i \leqslant n}$ свободного моноида $L(X)$, порождаемого множеством X, отнести композицию $f(u)$ последовательности (a_i) в E, то определенное так отображение f будет представлением (n° 1) $L(X)$ на A.

§ 2. Нейтральный элемент; регулярные элементы; симметричные элементы

1. *Нейтральный элемент*

Определение 1. *Пусть* $\top$ *— закон композиции элементов множества* E. $e \in E$ *называется нейтральным элементом относительно* $\top$, *если* $e \top x$ *и* $x \top e$ *определены и равны* x *для каждого* $x \in E$.

Заданный закон $\top$ обладает не более чем одним нейтральным элементом, ибо если e и e' — нейтральные элементы, то $e = e \top e' = e'$. Нейтральный элемент, если он существует, перестановочен с каждым элементом и, значит, является центральным.

Примеры. 1) В множестве всех подмножеств множества E $\varnothing$ есть нейтральный элемент относительно закона $\cup$, а E — относительно закона $\cap$. Более общим образом, наименьший элемент решетки, если он существует, является нейтральным элементом относительно закона $\sup(x, y)$; обратно, нейтральный элемент относительно этого закона, если он существует, является наименьшим элементом решетки.

Аналогично для наибольшего элемента и закона $\inf(x, y)$.

2) Число 0 является нейтральным элементом относительно сложения натуральных чисел, а 1 — относительно их умножения. Заков $(x, y) \to x^y$ не обладает нейтральным элементом.

3) Нейтральным элементом относительно закона композиции $X \circ Y$ подмножеств произведения $E \times E$ служит диагональ Δ. Нейтральным элементом относительно закона композиции $f \circ g$ отображений E в E является тождественное отображение E на E.

4) Если e — нейтральный элемент относительно закона композиции $\top$ элементов множества E, то $\{e\}$ — нейтральный элемент относительно закона композиции $(X, Y) \to X \top Y$ *подмножеств* множества E.

5) В свободном моноиде $L(A)$ (§ 1, п° 3) пустое слово является нейтральным элементом.

Если существует нейтральный элемент e относительно закона $\top$ на множестве E и если F — подмножество множества E, содержащее e, то e является нейтральным элементом относительно закона, который $\top$ индуцирует на F. Но может случиться, что индуцированный на F закон обладает нейтральным элементом e', когда F не содержит e или даже когда относительно закона $\top$ на E не существует нейтрального элемента.

Например, если $\top$ — ассоциативный закон на E и $h \in E$ — *идемпотент* относительно $\top$ (§ 1, n° 4), то h — нейтральный элемент относительно закона, индуцированного законом $\top$ на устойчивом множестве, образованном элементами $h \top x \top h$, где x пробегает E; при этом h может и не быть нейтральным элементом относительно $\top$ в E. В частности, когда $\top$ — закон $\sup(x, y)$ на решетке E, в качестве h можно взять любой элемент из E.

Пусть E и F — множества, каждое из которых наделено внутренним законом композиции, обозначаемым $\top$; если f — представление E в F и закон $\top$ на E обладает нейтральным элементом e, то $f(e)$ является нейтральным элементом относительно закона, индуцированного на $f(E)$ законом, заданным на F.

Определение 2. *Пусть на множестве E задан ассоциативный закон, обладающий нейтральным элементом. Композицией пустого семейства элементов из E называется нейтральный элемент e.*

Таким образом, если $\varnothing$ — пустое подмножество множества индексов, то мы будем, в условиях определения 2, писать $\top\limits_{\alpha \in \varnothing} x_\alpha = e$; точно так же, каково бы ни было x, будем считать $\top^{0} x = e$. *При этих определениях теоремы* 1 *и* 4 § 1 *остаются справедливыми и без предположения непустоты множеств A и B_i.* Точно так же формулы $\top^{m+n} x = (\top^{m} x) \top (\top^{n} x)$ и $\top^{mn} x = \top^{m} (\top^{n} x)$ сохраняют тогда силу для $m \geqslant 0$, $n \geqslant 0$.

Нейтральный элемент *аддитивно* записываемого закона обозначается 0 и называется *нулем* или *началом*, если только это не сопряжено с риском смешения (например, с натуральным числом 0); при законе, записываемом *мультипликативно*, нейтральный элемент обозначается 1 и называется *единицей* (или *единичным элементом*), с той же оговоркой.

2. *Регулярные элементы*

Определение 3. *Пусть $\top$ — заданный всюду определенный закон композиции элементов множества E. Левым* (соответственно *правым*) *переносом, соответствующим элементу $a \in E$, называется отображение $x \to a \top x$* (соответственно $x \to x \top a$) *множества E в себя.*

Прилагательные «левый» и «правый» проистекают от обычной записи большинства законов композиции. При переходе к противоположному закону левый перенос становится правым, и обратно.

Левый и правый переносы, соответствующие элементу $a \in E$, будут иногда обозначаться γ_a и δ_a, т. е.

$$\gamma_a(x) = a \top x, \qquad \delta_a(x) = x \top a.$$

Предложение 1. *Если* $\top$ *— ассоциативный закон, то левый перенос* $\gamma_{x \top y}$, *соответствующий композиции* x *и* y, *совпадает с композицией* $\gamma_x \circ \gamma_y$ *переносов* γ_y *и* γ_x; *а правый перенос* $\delta_{x \top y}$ *— с композицией* $\delta_y \circ \delta_x$ *переносов* δ_x *и* δ_y.

Действительно,

$$\gamma_{x \top y}(z) = (x \top y) \top z = x \top (y \top z) = \gamma_x(\gamma_y(z)),$$
$$\delta_{x \top y}(z) = z \top (x \top y) = (z \top x) \top y = \delta_y(\delta_x(z)).$$

Иными словами, отображение $x \to \gamma_x$ есть *представление* множества E (наделенного законом $\top$) в множество E^E всех отображений E в себя, наделенное законом $f \circ g$; а $x \to \delta_x$ есть представление E в множество E^E, наделенное законом, *противоположным* $f \circ g$.

Определение 4. *Пусть* $\top$ *— всюду определенный закон композиции элементов множества* E. *Элемент* $a \in E$ *называется регулярным относительно закона* $\top$, *если соответствующие* a *правый и левый переносы являются взаимно однозначными отображениями* E *в себя.*

Иными словами, для того чтобы a был регулярным, необходимо и достаточно, чтобы каждое из соотношений $a \top x = a \top y$, $x \top a = y \top a$ влекло $x = y$ (т. е. чтобы эти равенства, как говорят, можно было «сократить на a»). Если закон $\top$ обладает нейтральным элементом e, то последний регулярен относительно этого закона: переносы γ_e и δ_e являются тогда тождественными отображениями E на себя.

Если X и Y — подмножества множества E и a — регулярный элемент этого множества, то каждое из соотношений $\{a\} \top X = \{a\} \top Y$, $X \top \{a\} = Y \top \{a\}$ влечет $X = Y$.

Напротив, даже если каждый элемент множества $A \subset E$ регулярен, соотношение $A \top X = A \top Y$ (как и соотношение $X \top A = Y \top A$), вообще говоря, не влечет $X = Y$.

Примеры. 1) Каждое натуральное число регулярно относительно сложения; каждое натуральное число $\neq 0$ регулярно относительно умножения; каждое натуральное число, кроме 0 и 1, регулярно относительно возведения в степень.

2) В решетке не может существовать никакого регулярного элемента относительно закона $\sup(x, y)$, кроме нейтрального (т. е. наименьшего) элемента; аналогичное верно для $\inf(x, y)$. В частности, в множестве всех подмножеств множества E $\varnothing$ есть единственный элемент, регулярный относительно закона $\cup$, а E — единственный элемент, регулярный относительно закона $\cap$.

Предложение 2. *Множество всех регулярных относительно ассоциативного закона элементов устойчиво относительно этого закона.*

Действительно, если γ_y и γ_x взаимно однозначны, то это верно и для $\gamma_{x \top y} = \gamma_x \circ \gamma_y$ (предложение 1). Аналогично для $\delta_{x \top y}$.

Если элемент x регулярен относительно закона $\top$, то он регулярен и относительно закона, индуцированного этим законом на каждом устойчивом множестве A, содержащем x (но элемент из A может быть регулярным в A, не будучи регулярным в E); в частности, если R — множество всех элементов множества E, регулярных относительно ассоциативного закона $\top$, то *все элементы из R регулярны* относительно закона, индуцированного законом $\top$ на R.

3. *Симметричные элементы*

Определение 5. *Пусть $\top$ — закон композиции элементов множества E, обладающий нейтральным элементом e. Элемент x' называется симметричным элементу x, если $x \top x' = x' \top x = e$; элемент x называется симметризуемым, если существует элемент, симметричный x.*

Примеры. 1) Нейтральный элемент, если он существует, симметричен сам себе. Может случиться, что в E не существует других симметричных элементов; так обстоит дело для сложения и умножения в N; так же обстоит дело и для закона $\sup(x, y)$ в решетке.

2) В множестве всех отображений E в E симметризуемыми элементами относительно закона $f \circ g$ являются *взаимно однозначные отображения E на E* (Теор. мн., Рез., § 2, n° 12); симметричным такому отображению f служит обратное отображение.

Пусть E и F — множества, каждое из которых наделено внутренним законом, обозначаемым $\top$, и f — представление E в F; если x и x' симметричны в E, то $f(x)$ и $f(x')$ симметричны в $f(E)$.

Предложение 3. *Относительно ассоциативного закона $\top$ на E каждый симметризуемый элемент x регулярен и обладает единственным симметричным, а соответствующие левый и правый переносы γ_x и δ_x являются взаимно однозначными отображениями E на E.*

Пусть x' — элемент, симметричный x; если $x\top y=x\top z$, то $x'\top(x\top y)=x'\top(x\top z)$ или (по ассоциативности) $e\top y=e\top z$, т. е. $y=z$. Точно так же, если $y\top x=z\top x$, то $(y\top x)\top x'=(z\top x)\top x'$, откуда $y=z$. Таким образом, x регулярен. Если x'' — элемент, симметричный x, то $x\top x'=x\top x''=e$, а тогда $x'=x''$: элемент, симметричный x, единственен. Наконец, γ_x есть отображение E *на* E; иными словами, каково бы ни было $y\in E$, существует z такое, что $\gamma_x(z)=y$; в самом деле, для $z=x'\top y$ имеем $\gamma_x(z)=x\top(x'\top y)=e\top y=y$, и аналогично для δ_x.

Предложение 3 допускает следующее обращение:

Предложение 4. *Пусть $\top$ — ассоциативный закон на E. Если $x\in E$ таково, что левый и правый переносы γ_x и δ_x являются отображениями E на E, то $\top$ обладает нейтральным элементом и x симметризуемо.*

Так как $\gamma_x(E)=E$, то существует $e\in E$ такое, что $\gamma_x(e)=x$, т. е. $x\top e=x$; далее, так как $\delta_x(E)=E$, то для каждого $y\in E$ существует $z\in E$ такое, что $z\top x=y$, откуда $y\top e=z\top x\top e=z\top x=y$. Аналогично (меняя ролями γ_x и δ_x) убеждаемся в существовании e' такого, что $e'\top y=y$ для каждого y. Но в таком случае, с одной стороны, $e'\top e=e'$, а с другой, $e'\top e=e$, так что $e=e'$, $y\top e=e\top y=y$ при любом y, т. е. e — нейтральный элемент. Тогда существуют x' и x'' такие, что $x\top x'=e$, $x''\top x=e$; поэтому $x''\top(x\top x')=x''$, $(x''\top x)\top x'=x'$, откуда $x'=x''$ и x' — элемент, симметричный x.

Предложение 5. *Пусть $\top$ — ассоциативный закон. Если x' и y' соответственно симметричны x и y, то $y'\top x'$ симметрично $x\top y$.*

Действительно, $(y'\top x')\top(x\top y)=y'\top(x'\top x)\top y=y'\top y=e$, и аналогично для $(x\top y)\top(y'\top x')$.

Следствие 1. *Пусть* $\top$ *— ассоциативный закон на* E. *Если каждый элемент* x_α *серии* $(x_\alpha)_{\alpha\in A}$ *элементов из* E *обладает симметричным* x'_α, *то элементом, симметричным композиции* $\top\limits_{\alpha\in A} x_\alpha$, *служит композиция* $\top\limits_{\alpha\in A'} x'_\alpha$, *где* A' *— совершенно упорядоченное множество, полученное из* A *заменой его порядка противоположным.*

Это следствие получается из предложения 5 индукцией по числу элементов множества A.

В частности, если x и x' симметричны, то $\overset{n}{\top} x$ и $\overset{n}{\top} x'$ симметричны для каждого целого $n \geqslant 0$.

Следствие 2. *Множество всех симметризуемых элементов относительно ассоциативного закона устойчиво.*

Предложение 6. *Если* x *и* x' *симметричны относительно ассоциативного закона и* x *перестановочно с* y, *то также* x' *перестановочно с* y.

Действительно, из $x \top y = y \top x$ вытекает $x' \top (x \top y) \top x' = x' \top (y \top x) \top x'$ или $(x' \top x) \top (y \top x') = (x' \top y) \top (x \top x')$, т. е. $y \top x' = x' \top y$.

Следствие. *Если закон композиции ассоциативен, то элементы, симметричные центральным элементам, центральны.*

Из предложения 6 вытекает также, что при существовании нейтрального элемента предложение 2 § 1 можно заменить следующим более полным результатом:

Предложение 7. *Пусть* $\top$ *— ассоциативный закон композиции элементов множества* E, *обладающий нейтральным элементом* e; *пусть* X *и* Y *— подмножества множества* E, X'' (соответственно Y'') *— устойчивое множество, порожденное объединением* X (соответственно Y), $\{e\}$ *и множества элементов, симметричных всевозможным симметризуемым элементам из* X (соответственно Y). *Если тогда каждый элемент из* X *перестановочен с каждым элементом из* Y, *то каждый элемент из* X'' *перестановочен с каждым элементом из* Y''.

4. *Симметризация коммутативного ассоциативного закона*

Элемент $x \in E$, симметризуемый относительно ассоциативного закона $\top$, *регулярен* относительно закона, индуцированного законом $\top$ на каждом устойчивом множестве, содержащем x. Обратно, можно задаться вопросом, возможно ли множество E с заданным *ассоциативным* законом $\top$ «погрузить» в более широкое множество $\overline{E}$, определив на последнем закон композиции так, чтобы он индуцировал $\top$ на E и чтобы относительно него *каждый регулярный элемент из $\overline{E}$ был симметризуем*. Это не всегда возможно *), но, как мы увидим, при *коммутативности* закона $\top$ задача разрешима.

Итак, предположим, что $\top$ коммутативен, и обозначим через E^* множество всех регулярных элементов из E. Откинем прежде всего тот неинтересный случай, когда E^* пусто: задача тогда тривиально решается принятием за $\overline{E}$ самого множества E. Таким образом, будем в дальнейшем предполагать, что $E^* \neq \varnothing$. Говоря точно, нашей задачей является определить множество $\overline{E}$, коммутативный ассоциативный закон $\overline{\top}$ на $\overline{E}$ и изоморфизм f множества E на устойчивое подмножество A множества $\overline{E}$ (наделенное законом, индуцированным законом $\overline{\top}$) так, чтобы:

1° $\overline{E}$ обладало нейтральным элементом относительно закона $\overline{\top}$;

2° $f(x)$ было симметризуемо в $\overline{E}$ для каждого регулярного элемента $x \in E^*$.

Предположим сначала, что задача решена; пусть $A^* = f(E^*)$ и A' — множество элементов, симметричных всевозможным элементам из A^*. Устойчивость множеств A и A' относительно $\overline{\top}$ влечет устойчивость $A \overline{\top} A'$, поскольку тогда, вследствие коммутативности и ассоциативности закона $\overline{\top}$, $(A \overline{\top} A') \overline{\top} (A \overline{\top} A') = (A \overline{\top} A) \overline{\top} (A' \overline{\top} A') \subset A \overline{\top} A'$. $A \overline{\top} A'$ содержит нейтральный элемент множества $\overline{E}$; далее, $A \overline{\top} A'$ содержит A^*, ибо если $y \in A^*$ и y' — элемент, симметричный y, то $y = y \overline{\top} (y \overline{\top} y') = (y \overline{\top} y) \overline{\top} y' \in$

*) См. A. M a l c e v, On the immersion of an algebraic ring into a field, Math. Ann., т. 113, 1937, стр. 686.

$\in A \overline{\top} A'$; наконец, $A \overline{\top} A'$ содержит также A', ибо в тех же обозначениях имеем $y' = (y \overline{\top} y') \overline{\top} y' = y \overline{\top} (y' \overline{\top} y') \in A \overline{\top} A'$. Таким образом, множество $A \overline{\top} A'$, наделенное законом, индуцированным законом $\overline{\top}$, удовлетворяет всем условиям задачи. Поэтому, если задача разрешима, можно наложить на $\overline{E}$ дополнительное условие:

3° $\overline{E}$ порождается объединением множества $A = f(E)$ и множества A', состоящего из элементов, симметричных образам всевозможных регулярных элементов из E при отображении f.

Покажем, что условия 1°, 2°, 3° влекут *единственность* $\overline{E}$ (с точностью до изоморфизма). Действительно, снова в предположении разрешимости задачи, каждый элемент из $\overline{E}$ имеет вид $x \overline{\top} y'$, где $x \in A$, а y' — элемент, симметричный некоторому $y \in A^*$. Для того чтобы $x_1 \overline{\top} y_1' = x_2 \overline{\top} y_2'$, необходимо и достаточно (принимая во внимание регулярность y_1 и y_2), чтобы

$$(x_1 \overline{\top} y_1') \overline{\top} (y_1 \overline{\top} y_2) = (x_2 \overline{\top} y_2') \overline{\top} (y_1 \overline{\top} y_2),$$

т. е. (поскольку $\overline{\top}$ коммутативен) чтобы $x_1 \overline{\top} y_2 = x_2 \overline{\top} y_1$. Отсюда тотчас следует, что это последнее отношение есть *отношение эквивалентности* между элементами (x_1, y_1) и (x_2, y_2) произведения $A \times A^*$ и что существует взаимно однозначное отображение множества $\overline{E}$ на фактормножество множества $A \times A^*$ по этому отношению.

Переходя с помощью изоморфизма, обратного f, от A к E, мы видим, что если задача разрешима, то отношение $u_1 \top v_2 = u_2 \top v_1$ между элементами (u_1, v_1) и (u_2, v_2) произведения $E \times E^*$ есть отношение эквивалентности и существует взаимно однозначное отображение множества $\overline{E}$ на фактормножество произведения $E \times E^*$ по этому отношению. Кроме того, если перенести с помощью этого отображения структуру, определяемую законом $\overline{\top}$ в $\overline{E}$, то композицией класса эквивалентности элемента (u_1, v_1) и класса эквивалентности элемента (u_2, v_2) будет класс эквивалентности элемента $(u_1 \top u_2, v_1 \top v_2)$; действительно, если $x_1 \in A$, $x_2 \in A$, $y_1 \in A^*$, $y_2 \in A^*$, то $(x_1 \overline{\top} y_1') \overline{\top} (x_2 \overline{\top} y_2') = (x_1 \overline{\top} x_2) \overline{\top} (y_1' \overline{\top} y_2')$, а $y_1' \overline{\top} y_2'$ есть элемент, симметричный $y_1 \overline{\top} y_2$. Таким образом, всё это показывает, что *если можно определить* $\overline{E}$, *закон* $\overline{\top}$ *и изомор-*

физм f так, чтобы удовлетворялись условия 1°, 2°, 3°, *то E будет определяться с точностью до изоморфизма заданием E и закона* $\top$.

При этом каждый *регулярный* элемент из $\overline{E}$ *симметризуем*; действительно, если $x \overline{\top} y'$ (где $x \in A$, $y \in A^*$) регулярно в $\overline{E}$, то (предложение 2) это верно и для $(x \overline{\top} y') \overline{\top} y = x$; тогда x тем более регулярно в A и, значит, по предположению симметризуемо в $\overline{E}$; следовательно, и $x \overline{\top} y'$ симметризуемо. Таким образом, это свойство множества $\overline{E}$ является следствием предположенной справедливости свойств 1°, 2°, 3°.

Остается доказать, что задача действительно разрешима. Руководствуясь предшествующим, прежде всего покажем, что отношение $u_1 \top v_2 = u_2 \top v_1$ между элементами (u_1, v_1) и (u_2, v_2) произведения $E \times E^*$ есть *отношение эквивалентности*. Действительно, очевидно, это отношение R рефлексивно и симметрично; оно также транзитивно, ибо отношения $u_1 \top v_2 = u_2 \top v_1$, $u_2 \top v_3 = u_3 \top v_2$ влекут $u_1 \top v_2 \top v_3 = u_2 \top v_1 \top v_3 = u_2 \top v_3 \top v_1 = u_3 \top v_2 \top v_1$, и значит (в силу регулярности v_2), $u_1 \top v_3 = u_3 \top v_1$.

Обозначим теперь через $\overline{E}$ фактормножество произведения $E \times E^*$ по отношению R. Пусть x_1 и x_2 — элементы из $\overline{E}$, (u_1, v_1) и (u_2, v_2) — элементы из классов эквивалентности x_1 и x_2; класс эквивалентности, содержащий $(u_1 \top u_2, v_1 \top v_2)$, зависит только от x_1 и x_2, ибо при замене (u_1, v_1) эквивалентным элементом (u_3, v_3) будем иметь $u_1 \top v_3 = u_3 \top v_1$ и потому $(u_1 \top u_2) \top (v_3 \top v_2) = (u_3 \top u_2) \top (v_1 \top v_2)$; аналогичный результат получим, заменив (u_2, v_2) эквивалентным элементом (u_4, v_4). Обозначим класс, которому принадлежит $(u_1 \top u_2, v_1 \top v_2)$, через $x_1 \overline{\top} x_2$. $\overline{\top}$ есть закон композиции элементов множества $\overline{E}$, очевидно, ассоциативный и коммутативный.

Покажем, что $\overline{E}$ обладает *нейтральным элементом* относительно этого закона. Действительно, все элементы из $E \times E^*$ вида (w, w), где $w \in E^*$, эквивалентны; и обратно, если (u, v) эквивалентен (w, w), то $u \top w = v \top w$, и значит (в силу регулярности w), $u = v$. Пусть e — класс, образованный элементами (w, w). Если $(u, v) \in E \times E^*$ и $w \in E^*$, то $(u \top w, v \top w)$ эквивалентно (u, v); следовательно, e является нейтральным элементом относительно закона $\overline{\top}$, и условие 1° выполнено.

Рассмотрим в $E \times E^*$ множество всех элементов вида $(u \top v, v)$, где u — заданный элемент из E, а v пробегает E^*; все элементы этого множества эквивалентны, и обратно, если (u_1, v_1) эквивалентно одному из этих элементов $(u \top v, v)$, то $u \top v \top v_1 = u_1 \top v$. откуда (в силу регулярности v) $u_1 = u \top v_1$; иными словами, элементы $(u \top v, v)$ образуют класс эквивалентности; обозначив его $f(u)$, мы тем самым определим взаимно однозначное отображение f множества E на некоторую часть A множества $\overline{E}$; легко проверяется, что A устойчиво относительно закона $\overline{\top}$ и что f есть изоморфизм E на A. Наконец, если u — регулярный элемент из E, то $f(u)$, т. е. класс $(u \top v, v)$, обладает в $\overline{E}$ симметричным элементом, а именно классом $(v, u \top v)$ (поскольку в этом случае $u \top v \in E^*$); тем самым условие 2° выполнено и поставленная задача решена. Итак, мы доказали следующую теорему:

Теорема 1 (теорема симметризации). *Если $\top$ — всюду определенный коммутативный ассоциативный закон композиции элементов множества E, то можно определить множество $\overline{E}$, коммутативный ассоциативный закон композиции $\overline{\top}$ элементов этого множества и подмножество A множества $\overline{E}$, устойчивое относительно закона $\top$, так, чтобы выполнялись следующие условия:*

1° *существует изоморфизм E* (наделенного законом $\top$) *на A* (наделенное законом, индуцированным законом $\overline{\top}$), *относящий каждому регулярному элементу из E элемент из A, симметризуемый в $\overline{E}$;*

2° *$\overline{E}$ порождается объединением A и множества A' элементов, симметричных всевозможным регулярным элементам из A.*

При этом указанные условия определяют множество $\overline{E}$ однозначно (с точностью до изоморфизма) и каждый регулярный элемент из $\overline{E}$ симметризуем.

Следствие. *Если все элементы множества E регулярны, то все элементы множества $\overline{E}$ симметризуемы.*

Действительно, это вытекает из условий 1° и 2° теоремы 1 и предложения 5.

Структура, определяемая в $\overline{E}$ законом $\overline{\top}$, подпадает тогда под род *групповых* структур, рассматриваемый в § 6.

Множество $\overline{E}$, построенное при доказательстве теоремы 1, наделенное законом $\overline{\top}$, будет называться *симметризованным* множеством (или *результатом симметризации*) множества E (относительно $\top$); мы будем говорить, что $\overline{\top}$ получен путем *симметризации* закона $\top$. В применениях теоремы 1 E чаще всего удобно *отождествлять* (Теор. мн., Рез., § 8, n° 5) с множеством, обозначенным выше через A, что позволяет (допуская вольность) говорить, что E «погружено» в его симметризованное $\overline{E}$ и что $\overline{\top}$ есть *продолжение по симметрии* закона $\top$. Этот условный язык будет применяться, в частности, в следующих двух важных примерах.

5. *Применения: I. Рациональные целые числа*

Примем за E множество $\mathbf{N}$ натуральных чисел, а за закон композиции — *сложение*; все элементы из $\mathbf{N}$ регулярны относительно этого закона. Результат симметризации множества $\mathbf{N}$ обозначим $\mathbf{Z}$; его элементы называют *рациональными целыми числами*; закон, полученный путем симметризации сложения, заданного в $\mathbf{N}$, называется *сложением рациональных целых чисел* и по-прежнему обозначается $+$. Элементами множества $\mathbf{Z}$ являются, по определению, классы эквивалентности, определяемые в $\mathbf{N}\times\mathbf{N}$ отношением между (m_1, n_1) и (m_2, n_2), записываемым равенством $m_1+n_2=m_2+n_1$; все эти элементы *симметризуемы*; элемент $m\in\mathbf{N}$ отождествляется с классом, образованным парами $(m+n, n)$, где n пробегает $\mathbf{N}$; симметричным ему элементом в $\mathbf{Z}$ служит класс пар $(n, m+n)$. Но каждая пара (p, q) из $\mathbf{N}\times\mathbf{N}$ может быть записана в виде $(m+n, n)$, если $p\geqslant q$, или в виде $(n, m+n)$, если $p\leqslant q$; отсюда вытекает, что $\mathbf{Z}$ есть *объединение* $\mathbf{N}$ *и множества элементов, симметричных всевозможным элементам из* $\mathbf{N}$. При этом нейтральный элемент 0 является единственным элементом из $\mathbf{N}$, симметричный к которому принадлежит $\mathbf{N}$.

Рациональное целое, симметричное натуральному числу $m\neq 0$, обозначается $-m$; $\mathbf{Z}$ есть объединение $\mathbf{N}$ и множества всех элементов $-m$, где $m\in\mathbf{N}$, $m\neq 0$; m отождествляется с классом, содержащим $(m, 0)$, а $-m$ с классом, содержащим $(0, m)$; отсюда (принимая во внимание сказанное при доказательстве теоремы 1) легко получаем выражение для суммы двух рациональных целых; при $m\in\mathbf{N}$, $n\in\mathbf{N}$, $n\neq 0$ имеем:

а) если $m \geqslant n$, то $m+(-n)=p$, где p — элемент из $\mathbf{N}$ такой, что $m=n+p$;

б) если $m < n$, то $m+(-n)=-p$, где p — элемент из $\mathbf{N}$ такой, что $m+p=n$;

в) если $m \neq 0$, то $(-m)+(-n)=-(m+n)$.

Эти соотношения остаются в силе и без ограничения $n \neq 0$, а в случае в) — также $m \neq 0$, если условиться, что -0 означает 0.

Более общим образом, через $-x$ обозначают элемент, симметричный x, для произвольного рационального целого x и называют его чаще всего элементом, *противоположным* x; композиция $x+(-y)$ обозначается сокращенно $x-y$.

Отношение порядка $m \leqslant n$ между натуральными числами (Теор. мн., гл. III) обладает следующим свойством: если $m \leqslant n$, то $m+p \leqslant n+p$ для каждого $p \in \mathbf{N}$; покажем, что в $\mathbf{Z}$ можно определить, и притом *единственное*, отношение порядка, которое будет обозначаться по-прежнему $x \leqslant y$, индуцирующее в $\mathbf{N}$ указанное отношение и такое, что $x \leqslant y$ влечет $x+z \leqslant y+z$ для каждого $z \in \mathbf{Z}$ (этот порядок в $\mathbf{Z}$ называют *инвариантным относительно переносов*; см. гл. VI).

Действительно, при таком отношении мы для каждого $m \in \mathbf{N}$ должны иметь $0 \leqslant m$, откуда $(-m) \leqslant m+(-m)=0$; если x и y — рациональные целые такие, что $x \leqslant y$, то $0=x-x \leqslant y-x$, следовательно, $y-x=m \in \mathbf{N}$ и, значит, $y=x+m$; обратно, если существует $m \in \mathbf{N}$ такое, что $y=x+m$, то $0+x \leqslant m+x$, т. е. $x \leqslant y$; таким образом, если существует отношение порядка, удовлетворяющее указанным условиям, оно необходимо эквивалентно отношению «существует $m \in \mathbf{N}$ такое, что $y=x+m$» (или также $y-x \in \mathbf{N}$). Обратно, это последнее отношение действительно является отношением порядка, ибо оно, очевидно, транзитивно, и если $y=x+m$, $x=y+n$, $m \in \mathbf{N}$, $n \in \mathbf{N}$, то $m+n=0$, откуда $m=n=0$ и $x=y$; при этом оно действительно удовлетворяет поставленным условиям; наконец, $\mathbf{Z}$ *совершенно упорядочено* этим отношением, ибо $x-y=-(y-x)$ и потому, каковы бы ни были x и y из $\mathbf{Z}$, всегда $y-x \in \mathbf{N}$ или $x-y \in \mathbf{N}$, т. е. $x \leqslant y$ или $y \leqslant x$.

Рассматривая в дальнейшем $\mathbf{Z}$ как упорядоченное множество, мы всюду, где не оговорено противное, будем считать, что порядок определен в нем описанным образом. Натуральные числа совпадают с целыми $\geqslant 0$; они называются также *положительными целы-*

ми; целые $\leqslant 0$ — числа, симметричные положительным целым, — называются *отрицательными* целыми; целые >0 (соответственно <0) называются *строго положительными* *) (соответственно *строго отрицательными*); множество всех целых >0 обозначается $\mathbf{N}^*$.

6. *Применения: II. Положительные рациональные числа*

Примем за E множество $\mathbf{N}$ натуральных чисел, а за закон композиции на этот раз *умножение*; множеством всех регулярных элементов из $\mathbf{N}$ относительно этого закона служит $\mathbf{N}^*$. Результат симметризации множества $\mathbf{N}$ относительно умножения будет обозначаться $\mathbf{Q}_+$, а его элементы называться *положительными рациональными числами*; закон, полученный путем симметризации умножения, будет называться *умножением положительных рациональных чисел* и обозначаться мультипликативно. Элементами $\mathbf{Q}_+$ являются классы эквивалентности, определяемые в $\mathbf{N}\times\mathbf{N}^*$ отношением между (p_1, q_1) и (p_2, q_2), записываемым $p_1q_2=p_2q_1$; элемент из $\mathbf{Q}_+$, содержащий $(p, q)\in\mathbf{N}\times\mathbf{N}^*$, условились обозначать $\frac{p}{q}$ или p/q; таким образом, произведением p_1/q_1 и p_2/q_2 является $(p_1p_2)/(q_1q_2)$; натуральное число m *отождествляется с рациональными числами* $\frac{mn}{n}$ $(n\in\mathbf{N}^*)$. Мы не будем продолжать здесь далее изучение множества $\mathbf{Q}_+$, поскольку ниже (§ 9, n° 5) снова встретимся с ним как с частью множества $\mathbf{Q}$ всех *рациональных чисел* (где будет введено не только умножение, индуцирующее на $\mathbf{Q}_+$ умножение, определенное выше, но также *сложение*).

7. *Продолжение представления по симметрии*

Пусть E — множество, наделенное коммутативным ассоциативным законом. Нижеследующая теорема позволяет *продолжать* на *симметризованное* множество $\overline{E}$ (n° 4) некоторые представления E в множество F, наделенное ассоциативным законом:

*) Заметим, что, сообразуясь с общей терминологией, принятой для упорядоченных множеств (Теор. мн., Рез., § 6) и упорядоченных групп (см. гл. VI), мы отклонились от обычного словоупотребления (где *положительное* означает >0); при нашей терминологии 0 *одновременно положителен и отрицателен* (причем это единственное рациональное целое, обладающее таким свойством).

Теорема 2. *Пусть $\overline{E}$ — множество, наделенное коммутативным ассоциативным законом, и E — его устойчивое подмножество такое, что*: 1° *каждый регулярный элемент из E симметризуем в $\overline{E}$*: 2° *$\overline{E}$ порождается объединением E и множества элементов, симметричных всевозможным регулярным элементам из E. Пусть f — представление E в множество F, наделенное ассоциативным законом, относящее каждому регулярному элементу из E симметризуемый элемент в F; тогда f может быть, и притом единственным способом, продолжено до представления $\overline{E}$ в F.*

Будем законы, заданные в $\overline{E}$ и F, обозначать $\top$, а элемент, симметричный элементу $x \in \overline{E}$ (соответственно $y \in F$), обозначать x' (соответственно y'). Очевидно, закон, индуцированный на $f(E)$ законом $\top$, заданным на F, коммутативен. С другой стороны, из доказательства теоремы 1 следует, что каждый элемент $w \in \overline{E}$ имеет вид $x \top y'$, где $x \in E$, а y — регулярный элемент из E; если $x \top y' = x_1 \top y_1'$, то $x \top y_1 = x_1 \top y$, и поэтому $f(x) \top f(y_1) = f(x_1) \top f(y)$; так как $f(y)$ и $f(y_1)$ по предположению симметризуемы и, кроме того, перестановочны друг с другом, а также с $f(x)$ и $f(x_1)$, то $f(x) \top (f(y))' = f(x_1) \top (f(y_1))'$, так что $f(x) \top (f(y))'$ зависит только от элемента w, но не от выбора его представления в виде $x \top y'$; если при этом $w \in E$, то $x = w \top y$; значит, $f(x) = f(w) \top f(y)$ и $f(w) = f(x) \top (f(y))'$. Таким образом, положив $f(x \top y') = f(x) \top (f(y))'$, мы продолжим отображение f множества E в F на $\overline{E}$, и выкладки, аналогичные проведенным выше, показывают, что это продолжение является представлением $\overline{E}$ в F. Единственность вытекает из того, что каждое представление g $\overline{E}$ в F удовлетворяет условию $g(x \top y') = g(x) \top (g(y))'$ для всякого симметризуемого y из E.

8. *Применение: умножение рациональных целых чисел*

Рассмотрим множество рациональных целых чисел $\mathbf{Z}$ (n° 5) и множество натуральных чисел $\mathbf{N} \subset \mathbf{Z}$ со структурами, определяемыми в них одним сложением. Если $m \in \mathbf{N}$, то (Теор. мн., гл. III) для $x \in \mathbf{N}$, $y \in \mathbf{N}$ имеет место тождество $m(x+y) = mx + my$, означающее, что отображение $x \longrightarrow mx$ $\mathbf{N}$ в себя есть представление.

Его можно также рассматривать как представление $\mathbf{N}$ в $\mathbf{Z}$ и на этом основании применить к нему теорему 2; поэтому оно может быть продолжено до представления $\mathbf{Z}$ в $\mathbf{Z}$, которое по-прежнему будет обозначаться $x \to mx$; согласно доказательству теоремы 2, для $x = -n$, где $n \in \mathbf{N}^*$, mx равно $-(mn)$.

Определим теперь *все* представления f $\mathbf{Z}$ в $\mathbf{Z}$. Пусть $f(1) = a$. Предположим сначала, что $a \geqslant 0$. Имеем $f(x+1) = f(x) + a$, откуда по индукции следует, что $f(x) = ax$ для всех $x \in \mathbf{N}$; применяя теорему 2 к $\mathbf{Z}$ и $\mathbf{N}$, имеем поэтому $f(x) = ax$, каково бы ни было $x \in \mathbf{Z}$. Пусть теперь $a = -n$, где $n \in \mathbf{N}^*$; отображение $x \to -f(x)$ есть композиция f и отображения $x \to -x$ (являющегося, в силу коммутативности сложения, представлением) и, значит, представление, отображающее 1 в $n > 0$, откуда $-f(x) = nx$ и $f(x) = -(nx)$, каково бы ни было $x \in \mathbf{Z}$; здесь снова по определению полагают $f(x) = ax$, полагая тем самым $(-n)x = -(nx)$ для всех $n \in \mathbf{N}^*$, $x \in \mathbf{Z}$.

Таким образом, произведение ab определено, каковы бы ни были $a \in \mathbf{Z}$, $b \in \mathbf{Z}$. Для $m \in \mathbf{N}$, $n \in \mathbf{N}$ имеем $(-m)n = -(mn)$, $m(-n) = -(mn)$, $(-m)(-n) = mn$, откуда непосредственно следует, что умножение в $\mathbf{Z}$ ассоциативно и коммутативно; по самому способу, каким было получено произведение, имеем $x(y+z) = xy + xz$, откуда (по коммутативности) $(x+y)z = xz + yz$, каковы бы ни были x, y, z, и $x \cdot 0 = 0 \cdot x = 0$, $x \cdot 1 = 1 \cdot x = x$.

Очевидно, $\mathbf{N}$ есть устойчивое множество относительно так определенного в $\mathbf{Z}$ умножения; иными словами, отношения $x \geqslant 0$, $y \geqslant 0$ влекут $xy \geqslant 0$. Поэтому, если $x \leqslant y$ и $z \geqslant 0$, то $z(y-x) \geqslant 0$, т. е. $zx \leqslant zy$.

В § 8 (п° 1) мы увидим, что рассуждение, приведшее к определению умножения в $\mathbf{Z}$, позволяет при надлежащем его обобщении определить кольцо эндоморфизмов произвольной коммутативной группы.

9. *Обозначения элемента, симметричного данному*

Множество $\mathbf{Z}$ рациональных целых чисел позволяет ввести обозначение, содержащее обозначение $\overset{n}{\top} x$, введенное в п° 3 § 1, как частный случай. Напомним, что для ассоциативного закона $\top$, обладающего нейтральным элементом e, мы положили $\overset{0}{\top} x = e$, каково бы ни было x; *если при этом существует элемент* x',

симметричный x, то, по определению, полагают $\overset{-n}{\top} x = \overset{n}{\top} x'$, каково бы ни было $n \in \mathbf{N}^*$: тогда $\overset{a}{\top} x$ определено, каково бы ни было $a \in \mathbf{Z}$, и, в частности, имеем $\overset{-1}{\top} x = x'$. Легко убедиться в том, что, каковы бы ни были $a \in \mathbf{Z}$, $b \in \mathbf{Z}$,

$$\overset{a+b}{\top} x = (\overset{a}{\top} x) \top (\overset{b}{\top} x), \tag{1}$$

$$\overset{ab}{\top} x = \overset{a}{\top} (\overset{b}{\top} x). \tag{2}$$

Сделаем еще несколько общих замечаний относительно терминологии и обозначений для законов композиции, записываемых аддитивно или мультипликативно:

а) *Если только определенно не указано противное*, $+$ употребляется лишь для обозначения *коммутативного ассоциативного* закона композиции элементов некоторого множества E. Для обозначаемого так закона считают $+x$, где $x \in E$, означающим само x; если при этом x симметризуемо, то элемент, симметричный x, обозначается $-x$ и чаще всего называется *противоположным* x. Кроме того, композиция $x+(-y)$ обозначается сокращенно $x-y$; аналогично такие обозначения, как $x+y-z$, $x-y-z$, $x-y+z-t$, означают соответственно $x+y+(-z)$, $x+(-y)+(-z)$, $x+(-y)+z+(-t)$. Наконец, во всех случаях, когда композицию последовательности из n ($n \in \mathbf{N}^*$) элементов, каждый из которых равен x, обозначают nx и в E существует нейтральный элемент, условливаются понимать под $0x$ этот нейтральный элемент (а самого его чаще всего обозначать 0 и соответственно именовать *нулем*); если же x обладает противоположным элементом $-x$, то через $(-n)x$ обозначают элемент $n(-x) = -(nx)$.

б) *Если только определенно не указано противное*, мультипликативное обозначение употребляется только для *ассоциативного* закона. При такой записи закона, если существует элемент x', симметричный x, его чаще всего называют *обратным* к x, а элемент x — *обратимым*; при тех же условиях x^a, где $a \in \mathbf{Z}$, означает элемент, обозначавшийся выше для закона $\top$ через $\overset{a}{\top} x$; в частности, элемент, обратный x, обозначается x^{-1}.

Если, кроме того, рассматриваемый мультипликативный закон *коммутативен* (и только в этом случае), а 1 означает нейтральный элемент (чаще всего называемый в этом случае, соответственно его обозначению, *единицей*), то иногда условливаются, если y обратимо, записывать элемент y^{-1} в виде $\frac{1}{y}$ и элемент $xy^{-1}=y^{-1}x$ в виде $\frac{x}{y}$; вместо $\frac{x}{y}$ пишут также x/y, если только это не может вызвать путаницу. Элемент, обозначаемый таким способом, называют *дробью*; при этом x называется *числителем*, а y — *знаменателем* дроби.

в) В дальнейшем, при общих рассуждениях, относящихся к *ассоциативным законам* композиции, мы чаще всего будем пользоваться мультипликативным обозначением (но если закон, кроме того, коммутативен, то иногда и аддитивным).

Упражнения. 1) Пусть $\top$ — всюду определенный закон композиции на множестве E. Обозначая через F «сумму» (Теор. мн., Рез., § 4, n° 5) E и множества $\{e\}$, состоящего из одного элемента, и отождествляя E и $\{e\}$ с соответствующими подмножествами множества F, показать, что на F можно, и притом единственным способом, определить закон композиции $\overline{\top}$, индуцирующий на E закон $\top$ и имеющий e нейтральным элементом; если $\top$ ассоциативен, то и $\overline{\top}$ ассоциативен. (Если в E нет нейтрального элемента относительно $\top$, то говорят, что F получается из E «путем присоединения нейтрального элемента».)

2) Пусть $\top$ — всюду определенный закон на E. Для его ассоциативности необходимо и достаточно, чтобы каждый левый перенос γ_x был перестановочен с каждым правым переносом δ_y (относительно закона $f\circ g$ в множестве всех отображений E в E).

3) Для того чтобы в множестве F всех отображений E в E отношение $f\circ g=f\circ h$ влекло $g=h$, необходимо и достаточно, чтобы f было взаимно однозначным отображением E в E; для того чтобы отношение $g\circ f=h\circ f$ влекло $g=h$, необходимо и достаточно, чтобы f было отображением E на E; для того чтобы f было регулярным (относительно закона $\circ$), необходимо и достаточно, чтобы f было взаимно однозначным отображением E на E.

4) В свободном моноиде (§ 1, n° 3) каждый элемент регулярен.

5) Определить на множестве E, состоящем из n элементов, где $2\leqslant n\leqslant 5$, все всюду определенные законы с нейтральным элементом, относительно которых каждый элемент из E регулярен; показать, что при $n=5$ существуют также неассоциативные законы, удовлетворяющие этим условиям.

Упражнения с 6 по 16 включительно относятся к *мультипликативно* обозначаемым ассоциативным законам на множестве E; e означает нейтральный элемент, если таковой существует, γ_a и δ_a — левый и правый переносы, соответствующие элементу $a \in E$; если $X \subset E$, то, по определению, $\gamma_a(X) = aX$, $\delta_a(X) = Xa$.

6) Для ассоциативного закона на *конечном* множестве каждый регулярный элемент обратим. [Использовать предложение 4.]

7) Пусть заданы ассоциативный закон на множестве E и элемент $x \in E$, и пусть A — множество всех x^n, где $n \in \mathbf{N}^*$; далее, если существует нейтральный элемент, пусть B — множество всех x^n, где $n \in \mathbf{N}$; если, кроме того, x обратимо, то пусть C — множество всех x^a, где $a \in \mathbf{Z}$. Показать, что если A (соответственно B, C) бесконечно, то (наделенное законом, индуцированным законом, заданным на E) оно изоморфно $\mathbf{N}^*$ (соответственно $\mathbf{N}$, $\mathbf{Z}$), наделенному сложением.

8) В обозначениях упражнения 7 предположим, что A конечно. Показать, что A содержит идемпотент h (§ 1, n° 4), и притом только один. [Если x^p и x^q — идемпотенты, то $x^p = x^{pq}$, $x^q = x^{pq}$, и значит, $x^p = x^q$.] Если $h = x^p$, то множество D всех x^n с $n \geqslant p$ есть устойчивое подмножество множества E такое, что относительно закона, индуцированного на D, h является нейтральным элементом и все элементы из D обратимы.

*9) Пусть на множестве E задан мультипликативный закон и a — элемент из E такой, что левый перенос γ_a есть взаимно однозначное отображение E в E.

а) Показать, что если существует элемент u, для которого $au = a$, то $ux = x$ для всякого $x \in E$; в частности, если $xu = x$ для каждого $x \in E$, то u — нейтральный элемент.

б) Показать, что если существуют $u \in E$, для которого $au = a$, и $b \in E$, для которого $ab = u$, то $ba = u$. [Образовать aba.] В частности, если существуют нейтральный элемент e и элемент b, для которого $ab = e$, то b — элемент, обратный a.

10) Показать, что если a и b — такие элементы из E, что γ_{ba} — взаимно однозначное отображение E в E, то γ_a — взаимно однозначное отображение E в E. Вывести отсюда, что для коммутативного ассоциативного закона на E множество S всех нерегулярных элементов из E обладает свойством $ES \subset S$ (и, в частности, устойчиво).

*11) E называют *полугруппой с левым сокращением*, если γ_x есть взаимно однозначное отображение E в E для *каждого* $x \in E$.

а) Если u — идемпотент (§ 1, n° 4), то $ux = x$ для каждого $x \in E$. [Использовать упражнение 9а.] u — нейтральный элемент относительно закона, индуцированного на Eu.

б) Если u и v — два различных идемпотента из E, то $Eu \cap Ev = \varnothing$ [показать, что отношение $xu = yv$ влечет $xu = xv$] и множества Eu и Ev (наделенные законами, индуцированными законом, заданным на E) изоморфны.

в) Пусть R — дополнение к объединению множеств Eu, где u пробегает множество всех идемпотентов из E. Показать, что $ER \subset R$. [Доказать, что идемпотент u не может удовлетворять равенству $xy = xyu$ при $x \in E$, $y \in R$.] Следовательно, R — устойчивое подмножество множества E. Если R не пусто, то $aR \neq R$ для каждого $a \in R$. [Для доказательства того, что в противном случае R содержало бы идемпотент, воспользоваться упражнением 9а.] В частности, R тогда бесконечно. R называется *остаточным множеством* полугруппы с левым сокращением E.

г) Если R не пусто и в E существует хотя бы один идемпотент u (т. е. $E \neq R$), то для каждого $x \in REu$ имеем $xEu \neq Eu$. [Показать, что в противном случае существовало бы $a \in R$, для которого $aR = R$.] В частности, ни один элемент из REu не обратим в Eu и REu — бесконечное множество. [Использовать упражнение 8.]

д) Если E обладает нейтральным элементом e, то он является единственным идемпотентом в E и R пусто. [Заметить, что $E = Ee$.]

е) Если существует $a \in E$ такое, что правый перенос δ_a является *взаимно однозначным* отображением E в E (в частности, если заданный на E закон коммутативен), то либо E обладает нейтральным элементом, либо $E = R$. [Заметить, что если существует идемпотент u, то $xa = xua$ для каждого $x \in E$.]

ж) Если существует $a \in E$ такое, что δ_a является отображением E *на* E, то либо E обладает нейтральным элементом, либо $E = R$. [Рассмотреть отдельно случаи $a \in R$ и $a \in Eu$, где u — идемпотент.]

*12) Пусть на E задан мультипликативный закон и $a \in E$ таково, что γ_a является отображением E *на* E.

а) Показать, что если существует u, для которого $ua = a$, то $ux = x$ для всякого $x \in E$.

б) Для того чтобы γ_{la} было взаимно однозначным отображением E в E, необходимо и достаточно, чтобы γ_a было взаимно однозначным отображением E на E, а γ_b — взаимно однозначным отображением E в E.

*13) Предположим, что γ_x для *каждого* $x \in E$ есть отображение E *на* E. Показать, что если γ_a для некоторого $a \in E$ есть взаимно однозначное отображение E на E, то γ_x для каждого $x \in E$ есть взаимно однозначное отображение E на E. [Использовать упражнение 12б.] То же, в частности, верно, если в E существуют элементы a, b такие, что $ab = b$. [Использовать упражнение 12а.] E является тогда полугруппой с левым сокращением, остаточное множество R которой пусто; кроме того, для каждого идемпотента u все элементы из Eu обратимы в Eu.

*14) Для ассоциативного закона на *конечном* множестве E существуют *минимальные* множества вида aE (т. е. минимальные элементы множества всех подмножеств множества E, имеющих такой вид, упорядоченного по включению).

а) Если $M = aE$ минимально, то $xM = xE = M$ для каждого $x \in M$; наделенное индуцированным законом, M является полугруппой с левым сокращением (упражнение 11), в которой каждый левый перенос есть взаимно однозначное отображение M на себя. [См. упражнение 13.]

б) Если $M = aE$ и $M' = a'E$ минимальны и различны, то $M \cap M' = \varnothing$: для каждого $b \in M$ отображение $x' \to bx'$ множества M' в M есть взаимно однозначное отображение M' на M. Вывести отсюда, что существуют идемпотент $u' \in M'$, для которого $bu' = b$, и идемпотент $u \in M$, для которого $uu' = u$. [Взять за u идемпотент, для которого $bu = b$.] Показать, что $u'u = u'$ [рассмотреть $uu'u$] и что каждое $y' \in M'$, для которого $y'u = y'$, принадлежит $M'u'$.

в) Показать, что отображение $x' \to ux'$ множества $M'u'$ в M есть изоморфизм $M'u'$ на Mu; вывести отсюда, что M и M' — изоморфные полугруппы с левым сокращением.

г) Пусть M_i $(1 \leqslant i \leqslant r)$ — попарно различные минимальные множества вида aE; вывести из б), что идемпотенты каждой полугруппы с левым сокращением M_i можно расположить в последовательность (u_{ij}) $(1 \leqslant j \leqslant s)$ так, чтобы $u_{ij}u_{kj} = u_{ij}$ для любых i, j, k. Показать, что $Eu_{ij} \subset K$, где K — объединение полугрупп M_i. [Заметить, что $xu_{ij}E$ для каждого $x \in E$ есть минимальное множество вида aE.] Вывести отсюда, что Eu_{ij} есть объединение множеств $u_{kj}Eu_{kj}$ $(1 \leqslant k \leqslant r)$ [показать, что $(Eu_{ij}) \cap M_k = u_{kj}Eu_{kj}$] и что $Eu_{ij}E = K$. Наконец, доказать, что каждое минимальное множество вида Eb совпадает с одним из s множеств Eu_{ij}. [Заметить, что на основании а) $Ebu_{ij}b = Eb$, и вывести отсюда, что $Eb \subset K$.]

15) Пусть $(x_i)_{1 \leqslant i \leqslant n}$ — конечная последовательность элементов, для которых левые переносы γ_{x_i} являются взаимно однозначными отображениями E в E.

а) Показать, что соотношение $x_1x_2 \ldots x_n = e$ влечет все соотношения $x_{i+1} \ldots x_nx_1x_2 \ldots x_i = e$ $(1 \leqslant i \leqslant n)$, получающиеся из него «круговой перестановкой».

б) Вывести отсюда, что если композиция последовательности (x_i) обратима, то каждое x_i обратимо.

16) Если x и y обратимы, то элемент $y^{-1}x^{-1}yx$ называется *коммутатором* x и y и обозначается $x \circ y$. Показать, что для того, чтобы x и y (предполагаемые обратимыми) были перестановочны, необходимо и достаточно, чтобы $x \circ y = e$. Доказать тождества

$$y \circ x = (x \circ y)^{-1}, \qquad x \circ (yz) = (x \circ y)\,(z \circ (x \circ y))\,(x \circ z),$$
$$(x \circ y)\,(z \circ (x \circ y))\,(z \circ x)^{-1}\,(y \circ z)\,(x \circ (y \circ z))\,(x \circ y)^{-1}\,(z \circ x)\,(y \circ (z \circ x))\,(y \circ z)^{-1} = e.$$

[Третье получается из второго круговой перестановкой x, y, z и почленным перемножением полученных тождеств.]

17) Распространить доказательство теоремы симметризации (теорема 1) на тот случай, когда $\top$ — ассоциативный закон и каждый регулярный относительно него элемент — *центральный*.

*18) Пусть $\top$ — ассоциативный закон на множестве E и E^* — множество всех регулярных относительно него элементов; предположим, что E^* не пусто и что каждый регулярный элемент — центральный. Обозначим через $\mathfrak{F}$ множество всех $X \subset E$, обладающих следующим свойством: существует $y \in E^*$, для которого $\delta_y(E) \subset X$.

а) Показать, что пересечение двух множеств из $\mathfrak{F}$ принадлежит $\mathfrak{F}$.

б) Пусть Φ — множество всех функций, определенных на множествах из $\mathfrak{F}$, принимающих значения в E и таких, что, каковы бы ни были $f \in \Phi$ и $X \in \mathfrak{F}$, $f^{-1}(X)$ принадлежит $\mathfrak{F}$. Обозначим через R следующее отношение между элементами f и g множества Φ: «существует множество $X \in \mathfrak{F}$ такое, что сужения f и g на X совпадают». Показать, что R — отношение эквивалентности; пусть $\Psi = \Phi/R$ — фактормножество множества Φ по этому отношению.

в) Пусть f и g — элементы из Φ, $A \in \mathfrak{F}$ и $B \in \mathfrak{F}$ — множества, на которых f и g соответственно определены, и пусть существует $X \subset B$, принадлежащее $\mathfrak{F}$, для которого $g(X) \subset A$; обозначая через g_X сужение g на X, показать, что отображение $f \circ g_X$ принадлежит Φ и что его класс (mod R) зависит только от классов функций f и g (но не от X); этот класс называется композицией класса функции f и класса функции g; показать, что так определенный закон композиции в Ψ ассоциативен и обладает нейтральным элементом.

г) Показать, что левый перенос γ_a для каждого $a \in E$ принадлежит Φ; пусть φ_a — его класс (mod R). Показать, что отображение $x \to \varphi_x$ есть изоморфизм E в Ψ и что если $x \in E^*$, то φ_x обратимо в Ψ. [Рассмотреть отображение, обратное к γ_x, и показать, что оно принадлежит Φ, а его класс (mod R) симметричен φ_x.] Получить отсюда новое доказательство теоремы 1 и ее обобщения, сформулированного в упражнении 17.

§ 3. Внешние законы композиции

1. *Внешние законы композиции*

Определение 1. *Внешним законом композиции элементов множества Ω, называемого множеством операторов* (или *областью операторов*) *закона, и элементов множества E называется отображение f некоторого множества $A \subset \Omega \times E$ в E. Значение $f(\alpha, x)$, принимаемое f в $(\alpha, x) \in A$, называется композицией α и x относительно этого закона. Элементы из Ω называются операторами закона.*

Как и в случае внутренних законов, допуская вольность, говорят, что внешний закон задан (или определен) на E. Наиболее

важны законы *всюду определенные*, т. е. определенные на $A=\Omega\times E$; они и будут чаще всего рассматриваться в дальнейшем.

Из наиболее распространенных обозначений для композиции α и x приведем мультипликативное слева $\alpha\cdot x$ (где точка может при желании опускаться), мультипликативное справа $x\cdot\alpha$ и экспоненциальное x^α; при рассмотрениях §§ 3—5 мы для обозначения произвольных внешних законов будем обычно пользоваться знаком $\perp$.

Примеры. 1) Если на множестве E задан мультипликативно обозначаемый ассоциативный внутренний закон, то $(n, x)\to x^n$ есть всюду определенный внешний закон композиции элементов из $\mathbf{N}^*$ и E; для $a\in\mathbf{Z}$ $(a, x)\to x^a$ есть закон композиции элементов из $\mathbf{Z}$ и E, всюду определенный лишь когда все элементы из E обратимы. Сказанное относится также к законам $(n, x)\to nx$ и $(a, x)\to ax$ для аддитивно обозначаемого внутреннего закона на E *).

2) При заданных множествах E и F отображение $(X, Y)\to X\circ Y$ есть (всюду определенный) закон композиции множеств $X\subset F\times F$ и $Y\subset E\times F$, где первые служат операторами; отображение $(Z, Y)\to Y\circ Z$ есть закон композиции множеств $Z\subset F\times F$ (операторов) и множеств $Y\subset F\times E$.

3) При заданном внутреннем законе композиции $\top$ на E через $x\top A$, где $x\subset E$, $A\subset E$, обозначают множество всех $x\top y$, где y пробегает A (т. е. множество $\{x\}\top A$); этим определяется закон композиции элементов из E (операторов) и подмножеств множества E.

Если $\perp$ — внешний закон композиции операторов $\alpha\in\Omega$ и элементов $x\in E$, определенный на множестве $A\subset\Omega\times E$, то через $\Xi\perp X$ для каждого $\Xi\subset\Omega$ и каждого $X\subset E$ обозначают множество всех $\alpha\perp x$, где $\alpha\in\Xi$, $x\in X$ и $(\alpha, x)\in A$; если Ξ сводится к одному элементу α, вместо $\{\alpha\}\perp X$ пишут $\alpha\perp X$.

Отображение $(\Xi, X)\to\Xi\perp X$ есть *всюду определенный* закон композиции подмножеств множеств Ω и E.

---

*) Может случиться, что наряду с этим внутренним законом на E задан мультипликативно обозначаемый внешний закон, область операторов которого содержит множество $\mathbf{N}$ натуральных чисел (или его часть). В этом случае во избежание путаницы следует пользоваться для суммы последовательности n членов, равных x, каким-нибудь обозначением, отличным от $n\cdot x$ (если только эта сумма не равна всегда композиции n и x относительно заданного внешнего закона).

Если $\alpha \perp x$ — внешний закон композиции операторов $\alpha \in \Omega$ и элементов $x \in E$, то $x \to f_\alpha(x) = \alpha \perp x$ есть отображение в E некоторого его подмножества, а именно множества тех x, для которых $\alpha \perp x$ определено. Это отображение называется *умножением* на оператор α.

Обратно, пусть $(f_\alpha)_{\alpha \in \Omega}$ — семейство отображений подмножеств множества E в E, имеющее Ω своим множеством индексов; тогда отображение $(\alpha, x) \to f_\alpha(x)$ есть закон композиции элементов из Ω и E. Таким образом, совершенно безразлично, задаться ли таким семейством (f_α) или же задаться законом композиции элементов из Ω и E. Если $\perp$ — внешний закон композиции элементов из Ω и E, то элемент $x \in E$ называется *инвариантным* относительно оператора $\alpha \in \Omega$, когда $\alpha \perp x$ определено и равно x; элемент $\varepsilon \in \Omega$ называется *нейтральным оператором*, если все элементы множества E инвариантны относительно ε.

2. *Раздвоение внутреннего закона*

Множество Ω операторов внешнего закона на множестве E может совпадать с самим E; если $\Omega = E$, то налицо отображение в E некоторого $A \subset E \times E$, и это отображение можно с равным правом считать определяющим внутренний закон композиции элементов из E. Более точно: отображение $(x, y) \to f(x, y)$ множества $A \subset E \times E$ в E можно рассматривать как определяющее следующие законы, *которые важно ясно различать*:

1° внутренний закон $\top$, при котором композицией x и y служит $x \top y = f(x, y)$;

2° внутренний закон $\overline{\top}$, противоположный предыдущему (§ 1, n° 1), при котором композицией x и y служит $x \overline{\top} y = y \top x = f(y, x)$;

3° внешний закон $\perp$ композиции *операторов* $x \in E$ и элементов $y \in E$, при котором композицией x и y является $x \perp y = f(x, y)$; он называется *левым внешним законом*, порожденным законом $\top$;

4° внешний закон $\underline{\perp}$ композиции операторов $x \in E$ и элементов $y \in E$, при котором композицией x и y является $x \underline{\perp} y = f(y, x)$; он называется *правым внешним законом*, порожденным законом $\top$, и является также левым внешним законом, порожденным законом $\overline{\top}$.

Если можно не опасаться путаницы, для обозначения внешних законов, порожденных внутренним законом $\top$, пользуются тем же

символом $\top$, записывая композицию x и y при левом внешнем законе в виде $x \top y$ и при правом внешнем законе — в виде $y \top x$.

Если $\top$ — всюду определенный закон на E, то порожденный им левый внешний закон есть закон, соответствующий (описанным выше образом) семейству всех левых переносов $(\gamma_x)_{x \in E}$, а правый внешний закон — семейству всех правых переносов δ_x. Сказать, что $e \in E$ есть нейтральный элемент относительно закона $\top$, все равно, что сказать, что e есть нейтральный оператор для левого и правого внешних законов, порожденных законом $\top$.

Мы будем говорить, что два внешних закона, порожденных заданным внутренним, получаются путем *раздвоения* последнего. Всякий раз, когда область операторов внешнего закона на E совпадает с E и есть опасность путаницы, эта область будет заменяться некоторым множеством E', поставленным во взаимно однозначное соответствие с E, а композиция $x' \in E'$ и $y \in E$ считаться, по определению, равной композиции оператора $x \in E$ и элемента $y \in E$ при заданном законе, где x — элемент из E, соответствующий элементу $x' \in E'$. Разумеется, одновременно с этим в E' будут при необходимости переноситься и все структуры, заданные в E (Теор. мн., Рез., § 8, n° 5).

3. *Устойчивые множества. Индуцированные законы*

Определение 2. *Подмножество A множества E называется устойчивым относительно внешнего закона композиции $\alpha \perp x$ операторов $\alpha \in \Omega$ и элементов $x \in E$, если композиция $\alpha \perp x$ принадлежит A всякий раз, когда $x \in A$ и $\alpha \perp x$ определено.*

Иными словами, A устойчиво, если $\Omega \perp A \subset A$.

Пересечение семейства устойчивых подмножеств множества E, очевидно, устойчиво, так что существует наименьшее устойчивое множество, содержащее заданное $X \subset E$; оно называется устойчивым множеством, *порожденным* X.

Пример. Для внешнего закона, полученного путем раздвоения умножения натуральных чисел, устойчивое множество, порожденное множеством $\{1\}$, содержит $n \cdot 1 = n$ для каждого $n \in \mathbf{N}$ и тем самым совпадает с $\mathbf{N}$. На этом примере видна необходимость тщательно отличать внутренний закон от внешних, получающихся путем его раздвоения, поскольку относительно умножения натуральных чисел

множество $\{1\}$ само устойчиво. Более общим образом, если множество $A \subset E$ устойчиво относительно левого (или правого) внешнего закона, порожденного внутренним законом $\top$, то оно устойчиво и относительно $\top$; но, как показывает предыдущий пример, обратное неверно.

Если $\perp$ — всюду определенный внешний закон композиции операторов $\alpha \in \Omega$ и элементов $x \in E$ и A — подмножество множества E, *устойчивое* относительно этого закона, то, каково бы ни было $\Phi \subset \Omega$, *сужение* функции $\alpha \perp x$ на $\Phi \times A$ есть *всюду определенный внешний закон композиции* операторов $\alpha \in \Phi$ и элементов $x \in A$; он называется законом, *индуцированным* законом $\perp$ на множествах Φ и A. Более общим образом:

Определение 3. *Пусть $\perp$ — внешний закон композиции операторов $\alpha \in \Omega$ и элементов $x \in E$, определенный на $A \subset \Omega \times E$, и $\Phi \subset \Omega$, $F \subset E$; законом композиции операторов $\alpha \in \Phi$ и элементов $x \in F$, индуцированным законом $\perp$, называется закон, определенный на множестве тех $(\alpha, x) \in \Phi \times F$, для которых $(\alpha, x) \in A$ и $\alpha \perp x \in F$, и относящий каждой такой паре (α, x) композицию $\alpha \perp x$.*

Там, где нет опасности путаницы, закон, индуцированный законом $\perp$, мы будем (допуская вольность) обозначать снова $\perp$. Говоря (без дополнительных уточнений) о законе, индуцированном законом $\perp$ на некотором множестве $F \subset E$, мы будем всегда подразумевать, что $\Phi = \Omega$.

Напротив, рассматривая случай, когда $F = E$ и $\Phi \subset \Omega$, мы будем по-прежнему говорить, что закон, индуцированный на Φ и E, получен путем *сужения* области операторов заданного закона до множества Φ.

Упражнение. Пусть $\perp$ — всюду определенный закон композиции операторов $\alpha \in \Omega$ и элементов $x \in E$. Пусть, далее, F — множество всех отображений E в E, G — его подмножество, образованное умножениями f_α на всевозможные операторы α закона $\perp$, и H — устойчивое относительно закона $f \circ g$ подмножество множества F, порожденное множеством G и тождественным отображением E на себя.

а) Показать, что каждое подмножество множества E, устойчивое относительно закона $\perp$, устойчиво относительно закона $(f, x) \to f(x)$ композиции операторов $f \in H$ и элементов $x \in E$, и обратно.

б) Устойчивое относительно закона $\perp$ множество, порожденное множеством $X \subset E$, совпадает с множеством всех $f(x)$, где f пробегает H, а x пробегает X.

§ 4. Алгебраические структуры

1. *Определение алгебраической структуры*

Предметом алгебры является изучение *структур*, определяемых заданием одного или нескольких внутренних или внешних законов композиции элементов одного или нескольких множеств. Чаще всего все эти множества, кроме одного, рассматриваются как вспомогательные (Теор. мн., Рез., § 8, n° 2), что приводит к следующему определению.

Определение 1. *Алгебраической структурой в множестве E называется всякая структура, определяемая в E одним или несколькими внутренними законами композиции элементов из E и одним или несколькими внешними законами композиции операторов из областей операторов Ω, Θ,... и элементов из E, причем эти законы могут быть подчинены некоторым условиям* (например, ассоциативности, коммутативности и т. п.) *или быть связаны друг с другом некоторыми отношениями* (см. § 5).

Аналогично определяется алгебраическая структура на нескольких основных (и, возможно, нескольких вспомогательных) множествах путем задания внутренних или внешних законов композиции на некоторых основных множествах; часть основных множеств может служить областями операторов внешних законов структуры.

Таким образом, *род алгебраической структуры* Σ (Теор. мн., гл. IV, § 1), определенный на основных множествах базы x_1, ..., x_n и ее вспомогательных множествах A_1, ..., A_r (в теории более сильной, чем теория множеств), имеет общую структуру вида $(s_1, \ldots, s_p)$ и типовую характеристику вида

$$«s_1 \in T_1 \text{ и } s_2 \in T_2 \text{ и } \ldots \text{ и } s_p \in T_p»,$$

где каждое T_j получается путем замены в терме $\mathfrak{P}((u \times v) \times v)$ буквы v одной из букв x_i, буквы u — одним из термов x_i или A_k. При этом *аксиома* рода Σ записывается в виде «P и Q», где P есть отношение «s_1 есть функциональный график и ...

... и s_p есть функциональный график»

(выражающее таким образом, что s_i являются графиками законов композиции); отношение Q (выражающее дополнительные условия, наложенные на законы композиции рода структуры Σ) называют вообще (допуская вольность речи) *аксиомой* рода Σ (и, разумеется, чаще всего оно представляется в виде конъюнкции нескольких отношений, называемых *аксиомами* рода Σ).

С таким родом структуры Σ можно ассоциировать род алгебраической структуры Σ_0, имеющий те же множества базы и ту же типовую характеристику, но аксиома которого сводится к P; Σ_0 называется *обедненным* родом структуры, соответствующим Σ. Два рода алгебраической структуры, имеющие один и тот же обедненный род структуры, называются *гомологичными*, и две структуры гомологичных родов называются *гомологичными*.

Определение алгебраической структуры естественно порождает понятие *изоморфизма* (Теор. мн., Рез., § 8, n° 5): если на E и E' заданы алгебраические структуры одинакового рода, то *изоморфизм* E на E' есть биекция*) $f: E \to E'$ такая, что внутренние и внешние законы на E' получаются из соответствующих законов на E *переносом* структуры посредством f и тождественным отображением каждой из областей операторов внешних законов (являющейся вспомогательным множеством для обеих структур).

Если речь идет о роде алгебраической структуры Σ, определенном на нескольких основных множествах базы $x_1, \ldots, x_n$, то об *изоморфизме* $E_1, \ldots, E_n$ на $E'_1, \ldots, E'_n$ еще говорят, когда ни одно x_i не является областью операторов внешнего закона. В противном случае систему $(f_1, \ldots, f_n)$, где f_i — биекция E_i на E'_i и законы композиции структуры, рассматриваемой в $E'_1, \ldots, E'_n$, получаются из законов композиции структуры, заданной в $E_1, \ldots, E_n$, переносом структуры посредством отображений f_i и тождественного отображения каждого из вспомогательных множеств рода Σ, — предпочитают называть *полиизоморфизмом* (*биизоморфизмом* при $n=2$); если же рассматриваемые структуры совпадают, то говорят о *полиавтоморфизме* (*биавтоморфизме* при $n=2$).

Это различение между полиизоморфизмом и изоморфизмом введено главным образом из-за того, что обычно, допуская вольность, отождествляют два рода алгебраических структур, отличающиеся

*) То есть взаимно однозначное отображение на.— *Перев.*

лишь тем, что некоторые основные множества базы одного рассматриваются как вспомогательные множества базы другого °(например, в модуле над кольцом последнее рассматривают то как вспомогательное множество, то как основное)$_{\circ}$.

2. *Устойчивые множества. Индуцированная алгебраическая структура*

Определение 2. *Пусть E — множество, наделенное алгебраической структурой. Множество $A \subset E$ называется устойчивым* (относительно структуры, заданной в E), *если оно устойчиво относительно каждого из внутренних и внешних законов, определяющих эту структуру.*

Пересечение произвольного семейства устойчивых множеств есть снова устойчивое множество; в частности, существует наименьшее устойчивое множество, содержащее заданное множество $X \subset E$; оно называется устойчивым множеством, *порожденным* множеством X.

Определение 3. *Пусть E — множество, наделенное алгебраической структурой. Индуцированной ею структурой в множестве $F \subset E$ называется структура, определяемая в F внутренними и внешними законами, индуцированными на F законами, определяющими структуру в E.*

Часто говорят, что структура, заданная в E, является *продолжением* структуры, индуцированной ею в множестве $F \subset E$.

Если структура, рассматриваемая в E, есть структура рода Σ и Σ_0 — соответствующий обедненный род структуры (n° 1), то индуцированная структура в F есть структура рода Σ_0, но не обязательно рода Σ, даже когда F — *устойчивое* множество.

В § 6 будет показано на примере, что структура, индуцированная в устойчивом подмножестве F группы E заданной в E групповой структурой, вообще говоря, не является уже групповой структурой.

3. *Факторструктуры*

В дальнейшем будут рассматриваться отношения эквивалентности R, S, ... между элементами множеств, наделенных алгебраическими структурами. Напомним (Теор. мн., Рез., § 5, n° 2), что отношение R между элементами x, y часто записывается в ви

де $x \equiv y \pmod R$ или просто $x \equiv y$, если нет опасности смешения с другим отношением.

Определение 4. *Пусть* $\top$ *— внутренний закон композиции элементов множества* E. *Говорят, что отношение эквивалентности* R *согласуется с законом* $\top$, *если* $x \top y \equiv x' \top y' \pmod R$ *всякий раз, когда* $x \equiv x' \pmod R$, $y \equiv y' \pmod R$ *и композиции* $x \top y$ *и* $x' \top y'$ *определены. Закон, относящий классам эквивалентности элементов* x *и* y *класс эквивалентности элемента* $x \top y$, *есть внутренний закон композиции элементов фактормножества* E/R, *называемый факторзаконом закона* $\top$ *по* R.

Если $\top$ всюду определен, то всюду определен и его факторзакон по R; если $\top$ ассоциативен, то и факторзакон ассоциативен; если $\top$ коммутативен, то и факторзакон коммутативен (кратко говорят, что ассоциативность и коммутативность *сохраняются при факторизации*). Если $\top$ обладает нейтральным элементом e, то и факторзакон обладает нейтральным элементом (а именно классом эквивалентности, которому принадлежит e); элементам из E, симметричным относительно $\top$, соответствуют в E/R элементы, симметричные относительно факторзакона, и значит, симметризуемому элементу из E отвечает симметризуемый элемент из E/R. С другой стороны, регулярному элементу из E не обязательно соответствует регулярный элемент в E/R (см. пример ниже).

Определение 5. *Пусть* $\perp$ *— внешний закон композиции операторов* $\alpha \in \Omega$ *и элементов множества* E. *Говорят, что отношение эквивалентности* R *между элементами из* E *согласуется с законом* $\perp$, *если* $\alpha \perp x \equiv \alpha \perp x' \pmod R$ *всякий раз, когда* $x \equiv x' \pmod R$ *и композиции* $\alpha \perp x$ *и* $\alpha \perp x'$ *определены. Закон, относящий оператору* α *и классу эквивалентности элемента* x *класс эквивалентности элемента* $\alpha \perp x$, *есть внешний закон композиции операторов* $\alpha \in \Omega$ *и элементов из* E/R, *называемый факторзаконом закона* $\perp$ *по* R.

Если отношение R согласуется с внутренним законом $\top$, то оно согласуется также, с одной стороны, с противоположным законом, а с другой — с двумя внешними законами, получающимися из $\top$ путем раздвоения. Факторизация по этим четырем законам дает

два противоположных внутренних закона композиции элементов из E/R и два внешних закона композиции элементов из E, служащих операторами, и элементов из E/R.

Обратно, пусть $\top$ — всюду определенный внутренний закон и R — отношение эквивалентности, согласующееся с обоими порождаемыми $\top$ внешними законами. Тогда отношения $x \equiv x' \pmod R$, $y \equiv y' \pmod R$ влекут, с одной стороны, $x' \top y \equiv x \top y \pmod R$, а с другой, $x' \top y \equiv x' \top y' \pmod R$, и значит, $x \top y \equiv x' \top y' \pmod R$; тем самым R согласуется с $\top$.

Если отношение R согласуется с левым (соответственно правым) внешним законом, порожденным внутренним законом $\top$, то мы кратко говорим, что R *согласуется слева* (соответственно *справа*) с $\top$. Таким образом, имеем:

Предложение 1. *Для того чтобы отношение эквивалентности согласовалось со всюду определенным внутренним законом, необходимо и достаточно, чтобы оно согласовалось слева и справа с этим законом.*

Определение 6. *Пусть E — множество, наделенное алгебраической структурой, определяемой внутренними или внешними законами композиции. Говорят, что отношение эквивалентности R между элементами множества E согласуется со структурой, заданной в E, если оно согласуется со всеми этими законами; структура, определяемая в фактормножестве E/R их факторзаконами по R, будет называться факторструктурой структуры, заданной в E, по R, а E/R, наделенное этой факторструктурой, — результатом факторизации множества E, наделенного заданной структурой, по R.*

Если структура, рассматриваемая в E, — рода Σ и Σ_0 — соответствующий обедненный род структуры (n° 1), то факторструктура в E/R будет рода Σ_0; но нужно в каждом случае исследовать, будет ли она также рода Σ (так, во всяком случае, будет, в частности, когда Σ есть род групповых структур (§ 6) или род кольцевых структур (§ 8)).

Пример: Сравнения в $\mathbf{Z}$.

Пусть $a \in \mathbf{Z}$; отношение между элементами x и y из $\mathbf{Z}$ «существует $z \in \mathbf{Z}$ такое, что $x - y = az$» есть отношение эквивалентности;

его раз навсегда условились записывать $x \equiv y \pmod{a}$ или, короче, $x \equiv y\ (a)$ и называть *сравнением по модулю* a. Заменив a на $-a$, получим эквивалентное отношение, так что можно считать $a \geqslant 0$; если $a = 0$, то $x \equiv y\ (0)$ означает, что $x = y$; таким образом, отношение, отличное от равенства, получается лишь при $a \neq 0$; поэтому в дальнейшем, если только явно не указано противное, будет предполагаться, что $a > 0$.

Фактормножество множества $\mathbf{Z}$ по сравнению $x \equiv y\ (a)$, где $a > 0$, есть *конечное множество из* a *элементов*, называемое *множеством рациональных целых по модулю* a; этот факт вытекает из следующего свойства, обобщающего на рациональные целые евклидово деление натуральных чисел (Теор. мн., гл. III):

Если $a \in \mathbf{N}^*$ *и* $x \in \mathbf{Z}$, *то существуют однозначно определенные рациональные целые* q *и* r *такие, что* $x = qa + r$ *и* $0 \leqslant r \leqslant a - 1$.

Действительно, если $x = qa + r$ и $0 \leqslant r \leqslant a - 1$, то $qa \leqslant x < (q+1)a$, откуда $ma \leqslant x$ при $m \leqslant q$ и $ma > x$ при $m > q$; следовательно, q (если оно существует) однозначно определено как наибольший элемент множества тех $m \in \mathbf{Z}$, для которых $ma \leqslant x$. Но существование q в случае $x \geqslant 0$ было доказано (Теор. мн., гл. III); если же $x < 0$, то существует $q' \in \mathbf{Z}$ такое, что $q'a \leqslant -x < (q'+1)a$; а отсюда $qa \leqslant x < (q+1)a$, где $q = -q'$, если $-x = q'a$, и $q = -(q'+1)$, если $q'a < -x$.

Определенное так число r называется *вычетом* x *по модулю* a; для того чтобы $x \equiv y\ (a)$, необходимо и достаточно, чтобы x и y обладали одинаковым вычетом по модулю a, ибо два натуральных числа, принадлежащих интервалу $[0, a-1]$, могут быть сравнимыми по модулю a только если они равны. Отсюда следует, что фактормножество множества $\mathbf{Z}$ по отношению $x \equiv y\ (a)$ находится во взаимно однозначном соответствии с интервалом $[0, a-1]$ и тем самым есть множество, состоящее из a элементов; его часто отождествляют с этим интервалом.

Легко видеть, что, каково бы ни было $a \in \mathbf{Z}$, отношение $x \equiv y\ (a)$ *согласуется* со сложением и умножением в $\mathbf{Z}$; следовательно, при факторизации они порождают коммутативные ассоциативные законы; эти законы называют *сложением* и *умножением по модулю* a ($a > 0$). При отождествлении фактормножества множества $\mathbf{Z}$ по сравнению $(\mathrm{mod}\ a)$ с интервалом $[0, a-1]$ суммой (соответственно произведением) по модулю a элементов r, s этого интервала

является вычет по модулю a их суммы $r+s$ (соответственно произведения rs) в $\mathbf{Z}$.

Отношение $x \equiv 0 \pmod{a}$ выражают также следующим образом: «x кратно a», «a — делитель x», «a делит x».

Заметим, что если $x \neq 0$ кратно a, то x регулярно относительно умножения в $\mathbf{Z}$, но его класс (mod a) не является регулярным элементом относительно умножения по модулю a.

Ясно, что фактормножество множества $\mathbf{N}$ по отношению, индуцированному на $\mathbf{N}$ отношением $x \equiv y$ (a), совпадает с множеством всех рациональных целых по модулю a; сложение и умножение по модулю a можно получить также, взяв факторзаконы сложения и умножения в $\mathbf{N}$ по этому индуцированному отношению.

В § 6 мы увидим, что отношения сравнения $x \equiv y$ (a) являются *единственными* отношениями эквивалентности в $\mathbf{Z}$, согласующимися со сложением.

4. *Представления; гомоморфизмы*

Определение 7. *Пусть E и F — множества, наделенные гомологичными алгебраическими структурами, и f — отображение E в F. При обозначении соответственных законов композиции на E и F одинаковыми символами, f называется представлением E в F, если:*

1° *для каждого внутреннего закона композиции $\top$, заданного на E и F, всякий раз, когда определено $x \top y$, определено также $f(x) \top f(y)$ и $f(x \top y) = f(x) \top f(y)$;*

2° *для каждого внешнего закона $\perp$, заданного на E и F, всякий раз, когда определено $\alpha \perp x$, определено также $\alpha \perp f(x)$ и $f(\alpha \perp x) = \alpha \perp f(x)$.*

Из определения 7 следует, в частности, что для каждой пары соответственных внутренних законов $\top$, заданных на E и F, f есть представление E в F при структурах, определяемых одними этими законами (§ 1, n° 1); если законы $\top$ всюду определены, то для каждой серии $(x_\lambda)_{\lambda \in L}$ элементов из E имеет место тождество

$$f\left(\top_{\lambda \in L} x_\lambda\right) = \top_{\lambda \in L} f(x_\lambda), \tag{1}$$

в справедливости чего можно убедиться индукцией по числу элементов множества L.

Более общим образом, пусть $(E_1, \ldots, E_n)$ и $(E'_1, \ldots, E'_n)$ — две системы множеств, наделенные гомологичными алгебраическими структурами. Пусть f_i $(1 \leqslant i \leqslant n)$ — отображение E_i в E'_i. Говорят, что $(f_1, \ldots, f_n)$ есть *представление* $(E_1, \ldots, E_n)$ в $(E'_1, \ldots, E'_n)$, если выполнены следующие условия: 1° f_i удовлетворяет условию 1° определения 7 для каждого внутреннего закона $\top$, заданного на E_i и E'_i; 2° f_i удовлетворяет условию 2° определения 7 для каждого внешнего закона $\perp$, заданного на E_i и E'_i и имеющего своей областью операторов некоторое вспомогательное множество; 3° для каждого внешнего закона, заданного на E_i (соответственно E'_i) и имеющего своей областью операторов E_j (соответственно E'_j), всякий раз, когда $x_j \perp x_i$ (где $x_i \in E_i$, $x_j \in E_j$) определено, $f_j(x_j) \perp f_i(x_i)$ определено и равно $f_i(x_j \perp x_i)$.

Если все законы композиции, определяющие структуру в E, *всюду определены*, представление f E в F называется также *гомоморфизмом**) E в F; если при этом $f(E) = F$, то f называют гомоморфизмом E *на* F; гомоморфизм E в себя называют *эндоморфизмом* E.

Если существует гомоморфизм E *на* F, то говорят, что структура в F *гомоморфна* структуре в E (или является ее *гомоморфным образом*). Структуры, гомоморфные заданной, характеризуются следующей теоремой, доказательство которой непосредственно вытекает из определений:

√ Теорема 1 (теорема о гомоморфизмах). *Пусть E и F — множества, наделенные гомологичными алгебраическими структурами, и законы композиции в E всюду определены. Если f — гомоморфизм E в F, то $f(E)$ есть устойчивое подмножество множества F и, наделенное индуцированной структурой, изоморфно результату факторизации E по отношению эквивалентности $f(x) = f(y)$* (которое согласуется со структурой, заданной в E).

---

*) Когда E и F наделены не только алгебраическими структурами, но и *топологиями*, удовлетворяющими определенным условиям, термин «гомоморфизм» употребляется в более ограниченном значении и уже не является синонимом «представления» (см. Общ. топ., гл. III, § 2). Но при отсутствии топологических структур эта синонимия не доставляет никаких неудобств.

Если законы композиции на E не всюду определены, то теорема может утратить силу, поскольку тогда композиция $f(x)$ и $f(y)$ относительно внутреннего закона, заданного на F, может быть определена также, когда композиция x и y относительно соответствующего закона на E не определена, и аналогично для внешних законов.

Если гомоморфизм f E в F *инъективен* *), $f(E)$ по теореме 1 изоморфно E; f можно рассматривать тогда как изоморфизм E на $f(E)$, наделенное индуцированной структурой. В частности, для каждого устойчивого подмножества A множества E со всюду определенными законами композиции каноническая инъекция **) A (наделенного индуцированной структурой) в E есть гомоморфизм.

Если R — отношение эквивалентности в множестве E, согласующееся с заданной в E алгебраической структурой, то каноническое отображение E на E/R есть представление; оно называется *каноническим представлением* E на E/R (или *каноническим гомоморфизмом* E на E/R, если все законы композиции на E всюду определены).

Пусть законы композиции на E и F всюду определены, f — гомоморфизм E в F и R — отношение эквивалентности $f(x) = f(y)$; теорема 1 показывает, что *каноническое разложение* (Теор. мн., Рез., § 5, n° 3) гомоморфизма f дает:

1° канонический гомоморфизм E на E/R;

2° изоморфизм E/R на $f(E)$, называемый *взаимно однозначным представлением, ассоциированным с* f;

3° каноническую инъекцию $f(E)$ в F.

Предложение 2. *Пусть E, F, G — множества, наделенные гомологичными алгебраическими структурами, f — представление E в F и g — представление F в G; тогда $g \circ f$ есть представление E в G.*

Это предложение непосредственно следует из определения 7.

Предложение 3. *Пусть E — множество, наделенное алгебраической структурой, R — согласующееся с ней отношение эквивалентности, f — каноническое представление E на E/R и F — множество, наделенное структурой, гомологичной заданной в E.*

*) То есть является взаимно однозначным отображением E в F.— *Перев.*

**) Инъекция — взаимно однозначное отображение в. Каноническая инъекция множества $A \subset E$ в E — отображение относящее каждому элементу из A этот же элемент в E.— *Перев.*

Для того чтобы отображение g E/R в F было представлением, необходимо и достаточно, чтобы $g \circ f$ было представлением E в F.

Необходимость условия вытекает из предложения 2. Легко убеждаемся в его достаточности: если композиция $u \top v$ элементов u и v из E/R относительно внутреннего закона $\top$ определена, то в E существуют элемент x класса u и элемент y класса v, для которых $x \top y$ определено; тогда $g(f(x)) \top g(f(y))$ определено и равно $g(f(x \top y))$, т. е. $g(u) \top g(v)$ определено и равно $g(u \top v)$; аналогичное рассуждение для внешних законов.

В остающейся части этого n° мы будем рассматривать множество E, наделенное алгебраической структурой, задаваемой *всюду определенными* законами композиции. В обозначениях предложения 3, пусть S — отношение $g(x') = g(y')$ в E/R и T — отношение $g(f(x)) = g(f(y))$ в E; S есть *факторотношение* T/R отношения T по R (Теор. мн., Рез., § 5, n° 9); по теореме 1 образ E/R при отображении g изоморфен $(E/R)/S$; но он есть также образ E при отображении $g \circ f$, и теорема 1 показывает, что он изоморфен E/T. Тем самым, беря в качестве g канонический гомоморфизм E/R на $(E/R)/S$, получаем следующую теорему:

Теорема 2 (первая теорема об изоморфизме). *Пусть E — множество, наделенное алгебраической структурой, и R — согласующееся с ней отношение эквивалентности в E. Тогда каждое отношение эквивалентности S в E/R, согласующееся с факторструктурой множества E по R в E/R, имеет вид T/R, где T — отношение эквивалентности в E, являющееся следствием R и согласующееся со структурой, заданной в E; и обратно. При этом каноническое отображение E/T на $(E/R)/(T/R)$ есть изоморфизм.*

Будем обозначать через f канонический гомоморфизм E на E/R; пусть A — устойчивое подмножество множества E, наделенное индуцированной структурой; сужение f на A есть представление A в E/R, и значит, по теореме 1, $f(A)$ изоморфно A/R_A, где R_A — отношение, индуцированное отношением R в A (Теор. мн., Рез., § 5, n° 5). Пусть B — подмножество множества E, полученное путем *насыщения* A по R (Теор. мн., Рез., § 5, n° 6); B также *устойчиво*. Действительно, пусть $x \in B$, $y \in B$; по определению, существуют $x' \in A$ и $y' \in A$ такие, что $x \equiv x'$ и $y \equiv y' \pmod{R}$; для

любого внутреннего закона $\top$ из определяющих заданную в E алгебраическую структуру имеем $x' \top y' \in A$ и $x \top y \equiv x' \top y' \pmod{R}$, откуда $x \top y \in B$; аналогично для внешних законов. Поскольку B/R_B изоморфно $f(B)$, а $f(B) = f(A)$, нами получена

Теорема 3 (вторая теорема об изоморфизме). *Пусть E — множество, наделенное алгебраической структурой, A — его устойчивое подмножество и R — отношение эквивалентности, согласующееся со структурой, заданной в E. Множество B, получающееся путем насыщения A по R, устойчиво; отношения R_A и R_B, индуцированные отношением R в A и B, согласуются со структурами, индуцированными в A и B из E, и каноническое отображение**) *A/R_A на B/R_B есть изоморфизм.*

Пусть $L(A)$ — свободный моноид, порожденный множеством A, M — моноид с нейтральным элементом e и f — отображение A в M. Существует, и притом единственное, представление g моноида $L(A)$ в M, переводящее $\varnothing$ в e и служащее продолжением f (так что $L(A)$ есть решение универсальной проблемы (см. Теор. мн., гл. IV, § 3)). Действительно, если $s = (a_i)_{i \in I}$ — непустое слово из $L(A)$, то примем за $g(s)$, по определению, композицию последовательности $(f(a_i))_{i \in I}$; кроме того, положим $g(\varnothing) = e$; по теореме ассоциативности, g — представление. С другой стороны, пусть g' — представление $L(A)$ в M, являющееся продолжением f и переводящее $\varnothing$ в e, и пусть B — та часть $L(A)$, на которой g и g' совпадают; тогда $\varnothing \in B$, $A \subset B$, B устойчиво относительно заданного в $L(A)$ умножения, значит, $B = L(A)$, и следовательно, $g' = g$.

Пусть A и B — два множества и f — отображение A в B. Согласно предыдущему, существует, и притом только одно, представление f' моноида $L(A)$ в $L(B)$, переводящее $\varnothing$ в $\varnothing$ и служащее продолжением f. Пусть C — третье множество, f_1 — отображение B в C и f_1' — порождаемое им представление $L(B)$ в $L(C)$; тогда $f_1' \circ f'$ есть представление $L(A)$ в $L(C)$, порождаемое отображением $f_1 \circ f$ множества A в C.

---

*) Это каноническое отображение (композиция канонического отображения A/R_A на $f(A)$ и канонического отображения множества $f(B) = f(A)$ на B/R_B) относит каждому классу $(\mathrm{mod}\, R_A)$ в A содержащий его класс $(\mathrm{mod}\, R)$ в E.

5. *Произведения алгебраических структур*

Определение 8. *Пусть* $(E_\iota)_{\iota\in I}$ *— семейство множеств, наделенных гомологичными алгебраическими структурами, и* $E=\prod_{\iota\in I} E_\iota$ *— его произведение. Будем предполагать, что каждый из* (внутренних и внешних) *законов обедненного рода структуры* Σ_0, *соответствующего родам структур, заданных в множествах* E_ι, *обозначается одним знаком для всех* E_ι.

1° *Для внутреннего закона* $\top$ *на множествах* E_ι, $x=(x_\iota)$ *и* $y=(y_\iota)$ *положим* $x\top y=(x_\iota\top y_\iota)$ *всякий раз, когда* $x_\iota\top y_\iota$ *определены для всех* $\iota\in I$; *определенный так внутренний закон композиции на* E *будем называть произведением законов* $\top$, *заданных на множествах* E_ι.

2° *Для внешнего закона* $\perp$ *на множествах* E_ι, *оператора* α *относительно этих законов и* $x=(x_\iota)$ *положим* $\alpha\perp x=(\alpha\perp x_\iota)$ *всякий раз, когда* $\alpha\perp x_\iota$ *определены для всех* $\iota\in I$; *определенный так внешний закон композиции на* E *будем называть произведением законов* $\perp$, *заданных на множествах* E.

3° *Если для каждого из характеристических законов рода структуры* Σ_0 *будет образовано на* E *произведение соответствующих законов на множествах* E_ι, *то структура, определяемая в* E *всеми этими произведениями законов, будет называться произведением структур, заданных в множествах* E_ι, *а* E, *наделенное этой структурой, — произведением множеств* E_ι, *наделенных заданными структурами.*

Произведение структур, очевидно, *гомологично* структурам, заданным в множествах E_ι; но если последние структуры принадлежат все одному роду, нужно в каждом случае еще исследовать, принадлежит ли и их произведение этому роду.

В дальнейшем мы встретимся как с примерами, где это всегда так (структуры группы, кольца и т. д), так и с примерами, где это не так (структура тела).

В обозначениях определения 8, если A_ι — устойчивое подмножество множества E_ι, то $A=\prod_{\iota\in I} A_\iota$ есть устойчивое подмножество произведения E, а структура, индуцированная в A из E, есть произведение структур, индуцированных в множествах A_ι из E_ι.

Отображение pr_ι произведения E на E_ι есть представление E на E_ι; аналогично для проекции на любое частичное произведение $\prod_{\iota\in J} E_\iota$. Если $(I_\varkappa)_{\varkappa\in K}$ — разбиение множества I и $F_\varkappa = \prod_{\iota\in I_\varkappa} E_\iota$, то каноническое отображение (Теор. мн., Рез., § 4, n° 11) E на $\prod_{\varkappa\in K} F_\varkappa$ есть изоморфизм.

Если f_ι — представление множества F (наделенного структурой, гомологичной структурам, заданным в множествах E_ι) в E_ι, то $f=(f_\iota)$ есть представление F в E.

Пусть $(F_\iota)_{\iota\in I}$ — второе семейство множеств, наделенных алгебраическими структурами, гомологичными заданным в множествах E_ι, обладающее тем же множеством индексов; если f_ι для каждого ι есть представление E_ι в F_ι, то отображение $(x_\iota)\to(f_\iota(x_\iota))$ есть представление $\prod_{\iota\in I} E_\iota$ в $\prod_{\iota\in I} F_\iota$.

В частности, когда I — множество, состоящее из двух элементов, а f_ι — канонические представления на фактормножества, получаем следующее предложение:

Предложение 4. *Пусть E и F — множества, наделенные гомологичными алгебраическими структурами, R — отношение эквивалентности, согласующееся со структурой, заданной в E, и S — отношение эквивалентности, согласующееся со структурой, заданной в F. Каноническое отображение $(E/R)\times(F/S)$ на $(E\times F)/(R\times S)$* (Теор. мн., Рез., § 5, n° 10) *есть изоморфизм.*

Если рассматриваемые структуры определяются в каждом E_ι единственным внутренним законом (обозначаемым $\top$ для всех E_ι) и если все эти законы $\top$ ассоциативны, их произведение тоже ассоциативно; для того чтобы элементы (x_ι), (y_ι) были перестановочными относительно произведения законов $\top$, необходимо и достаточно, чтобы x_ι и y_ι были перестановочны при каждом ι; в частности, если все законы $\top$ коммутативны, то и их произведение коммутативно; для краткости говорят также, что ассоциативность и коммутативность *сохраняются при переходе к произведениям.* Для того чтобы произведение законов $\top$ обладало нейтральным элементом $e=(e_\iota)$, необходимо и достаточно, чтобы каждое e_ι было нейтральным элементом в E_ι; для того чтобы $x=(x_\iota)$ было регулярным относительно произведения законов $\top$, необходимо

и достаточно, чтобы каждое x_ι было регулярно в E_ι; для того чтобы $x=(x_\iota)$ и $y=(y_\iota)$ были симметричны, необходимо и достаточно, чтобы x_ι и y_ι были симметричны при каждом ι.

Наконец, рассмотрим тот случай, когда все E_ι совпадают с одним и тем же множеством F, наделенным произвольной алгебраической структурой; E есть тогда множество F^I всех отображений $\iota \to f(\iota)$ множества индексов I в F; композиция $f \top g$ двух таких отображений относительно каждого внутреннего закона $\top$ на F есть отображение $\iota \to f(\iota) \top g(\iota)$; а для каждого внешнего закона $\perp$ на F композиция $\alpha \perp f$ оператора α и отображения f есть отображение $\iota \to \alpha \perp f(\iota)$.

Заметим, что *гомоморфизмы* алгебраических структур (со всюду определенными законами) удовлетворяют условиям (MO_I), $(\mathrm{MO}_\mathrm{II})$ и $(\mathrm{MO}_\mathrm{III})$ § 2 главы IV Книги 1, характеризующим *морфизмы*.

Упражнения. 1) Рассмотрим алгебраическую структуру, определяемую в множестве E заданием нескольких внешних законов. Показать, что эти законы можно (с точностью до полиизоморфизма) рассматривать как законы, полученные путем *сужения единственного* внешнего закона $\perp$ на некоторые подмножества его области операторов. [Рассмотреть «сумму» (Теор. мн., Рез., § 4, n° 5) множеств операторов всевозможных внешних законов, заданных на E.] Устойчивые подмножества множества E относительно заданной структуры и структуры, определяемой этим единственным законом $\perp$, одни и те же; каждое отношение эквивалентности, согласующееся с заданной структурой, согласуется с законом $\perp$, и обратно.

2) Напомним, что, отождествляя (допуская вольность) отношения эквивалентности в множестве E с определяемыми ими подмножествами произведения $E \times E$ (Теор. мн., гл. II), говорят, что отношение эквивалентности R *содержит* отношение эквивалентности S, если часть $E \times E$, определяемая отношением R, содержит часть, определяемую отношением S (что означает, иными словами, что S влечет R); аналогично говорят о *пересечении* семейства отношений эквивалентности.

а) Показать, что пересечение семейства отношений эквивалентности, согласующихся с алгебраической структурой, заданной в множестве E, есть отношение эквивалентности, также согласующееся с этой структурой.

б) Пусть a и b — заданные два элемента из E; среди всех отношений эквивалентности R, согласующихся с рассматриваемой в E алгебраической структурой и удовлетворяющих условию $a \equiv b \pmod{R}$, существует содержащееся во всех остальных; это отношение $R_{a,\,b}$ называют отношением эквивалентности, полученным путем *отождестеле-*

ния a и b, а $E/R_{a,b}$—фактормножеством, полученным путем отождествления a и b.

в) Если R — отношение эквивалентности, согласующееся с заданной в E алгебраической структурой, то существует семейство пар (a_ι, b_ι) элементов из E такое, что R есть наименьшее отношение эквивалентности, содержащее все отношения R_{a_ι, b_ι}; E/R называется фактормножеством, полученным путем отождествления a_ι и b_ι для каждого ι.

*3) Пусть E — моноид (§ 1, n° 3) с мультипликативным обозначением.

а) Каково бы ни было множество $A \subset E$, отношение $\overset{-1}{\gamma}_x(A) = \overset{-1}{\gamma}_y(A)$ между элементами x и y из E есть отношение эквивалентности, согласующееся справа с заданным на E законом; будем обозначать его $R_d(A)$.

б) Пусть R — отношение эквивалентности, согласующееся справа с заданным на E законом, и A — произвольный класс (mod R). Показать, что R влечет $R_d(A)$ и что пересечение (упражнение 2) отношений $R_d(A)$, где A пробегает множество всех классов mod R, есть следующее отношение эквивалентности (между элементами x и y из E): «каково бы ни было z, $xz \equiv yz \pmod R$».

в) Множество $A \subset E$ называется *разделяющим* множеством, если отношение $\overset{-1}{\gamma}_x(A) \cap \overset{-1}{\gamma}_y(A) \neq \varnothing$ влечет $\overset{-1}{\gamma}_x(A) = \overset{-1}{\gamma}_y(A)$. Показать, что если A — разделяющее, то отношение $\overset{-1}{\delta}_x(A) \cap \overset{-1}{\delta}_y(A) \neq \varnothing$ влечет $\overset{-1}{\delta}_x(A) = \overset{-1}{\delta}_y(A)$, и что классамк эквивалентности mod $R_d(A)$ служат множества $\overset{-1}{\delta}_x(A)$, где x пробегает E, и множество $W(A)$ тех $x \in E$, для которых $\overset{-1}{\gamma}_x(A) = \varnothing$. Пусть F — дополнение к $W(A)$ в E; при тех же условиях доказать, что отношения $xz \in F$, $yz \in F$, $xz \equiv yz \pmod{R_d(A)}$ влекут $x \equiv y \pmod{R_d(A)}$.

г) Пусть R — отношение эквивалентности, согласующееся справа с заданным на E законом и такое, что $xz \equiv yz \pmod R$ влечет $x \equiv y \pmod R$. Показать, что каждый класс mod R является разделяющим множеством; если A — класс mod R, то, в введенных выше обозначениях, отношения, индуцированные в дополнении F к $W(A)$ отношениями R и $R_d(A)$, равносильны.

4) Показать, что каждое отношение эквивалентности в $\mathbf{Z}$, согласующееся со сложением, имеет вид $x \equiv y\ (a)$, где $a \in \mathbf{Z}$. [Показать, что класс числа 0 по такому отношению имеет вид $a \cdot \mathbf{Z}$, для чего рассмотреть наименьший элемент > 0 этого класса, если таковой существует.] Вывести отсюда, что если, в обозначениях упражнения 7 § 2, множество C конечно и состоит из p элементов, то оно изоморфно множеству всех целых чисел по модулю p (наделенному сложением по модулю p); то же верно и для множества D упражнения 8 § 2, если оно состоит из p элементов.

5) Пусть E и E' — множества, наделенные гомологичными алгебраическими структурами, и f — представление E в E'. Показать, что если A'—устойчивое множество в E', то $\overset{-1}{f}(A')$ — устойчивое множество в E.

6) Рассмотрим в свободном моноиде $L(A)$, порожденном множеством A, следующее отношение R между словами $u=(a_i)_{0\leqslant i\leqslant n}$ и $v=(b_i)_{0\leqslant i\leqslant n}$: «существует такая подстановка π интервала $[0, n]$, что $b_i=a_{\pi(i)}$» (иными словами, последовательности (a_i) и (b_i) различаются лишь порядком следования членов). Показать, что R есть отношение эквивалентности, согласующееся с приписыванием в $L(A)$; фактормножество $L(A)/R$ называется *свободным коммутативным моноидом*, порожденным множеством A; показать, что он изоморфен устойчивому подмножеству произведения $\mathbf{N}^A$ (наделенного произведением законов сложения в сомножителях N), образованному всеми семействами $(n_\alpha)_{\alpha\in A}$ натуральных чисел такими, что $n_\alpha=0$ для всех, за исключением *конечного* числа, индексов α.

§ 5. Отношения между законами композиции

В определении большинства алгебраических структур фигурируют несколько законов композиции, находящихся в определенных взаимных отношениях; типы этих отношений довольно разнообразны; мы рассмотрим здесь главнейшие из них и укажем, как принято отражать их в обозначениях.

1. *Дистрибутивность*

Определение 1. *Всюду определенный внешний закон композиции* $\perp$ *операторов* $\alpha\in\Omega$ *и элементов множества* E *называют дистрибутивным относительно внутреннего закона композиции* $\top$ *элементов из* E, *если всякий раз, когда композиция* $x\top y$ *определена, композиция* $(\alpha\perp x)\top(\alpha\perp y)$ *определена для всех* $\alpha\in\Omega$ *и имеет место равенство*

$$\alpha\perp(x\top y)=(\alpha\perp x)\top(\alpha\perp y). \tag{1}$$

Это определение равносильно требованию, чтобы отображение $x\longrightarrow\alpha\perp x$ было для каждого $\alpha\in\Omega$ *представлением* E в E относительно структуры, определяемой в E одним только внутренним законом $\top$.

Ограничимся в дальнейшем рассмотрением того случая, когда закон $\top$ всюду определен. Сделанное только что замечание и тождество (1) § 4 показывают тогда, что, какова бы ни была серия

$(x_\lambda)_{\lambda\in L}$ элементов из E,

$$\alpha\perp\left(\overline{\top}_{\lambda\in L}x_\lambda\right)=\overline{\top}_{\lambda\in L}(\alpha\perp x_\lambda). \qquad (2)$$

Если рассматриваемый внутренний закон записывается мультипликативно, то для внешнего закона, дистрибутивного относительно этого умножения, часто пользуются экспоненциальным обозначением x^α, так что дистрибутивность выражается тождеством $(xy)^\alpha=x^\alpha y^\alpha$. Если внутренний закон записывается аддитивно, то внешний закон, дистрибутивный относительно этого сложения, часто обозначают в виде умножения слева $\alpha\cdot x$ или умножения справа $x\cdot\alpha$, в соответствии с чем дистрибутивность выражается соответственно тождеством $\alpha(x+y)=\alpha x+\alpha y$ или $(x+y)\alpha=x\alpha+y\alpha$.

Определение 2. *Пусть $\perp$ — всюду определенный закон композиции операторов $\alpha\in\Omega$ и элементов из E, $\top$ — внутренний закон композиции элементов из E и $\overline{\top}$ — внутренний закон композиции элементов из Ω. Говорят, что закон $\perp$ дистрибутивен относительно совокупности законов $\top$, $\overline{\top}$, если всякий раз, когда композиция $\alpha\,\overline{\top}\,\beta$ определена, композиция $(\alpha\perp x)\top(\beta\perp x)$ определена для всех $x\in E$ и имеет место равенство*

$$(\alpha\,\overline{\top}\,\beta)\perp x=(\alpha\perp x)\,\widehat{\overline{\top}}\,(\beta\perp x). \qquad (3)$$

Не следует смешивать эту дистрибутивность с определенной выше: дистрибутивность $\perp$ относительно совокупности законов $\top$, $\overline{\top}$ никоим образом не влечет дистрибутивности $\perp$ относительно закона $\top$ (см. примеры ниже).

Определение 2 равносильно требованию, чтобы отображение $\alpha\to\alpha\perp x$ было для каждого $x\in E$ *представлением* Ω в E (для структур, определяемых соответственно законами $\overline{\top}$ и $\top$).

Ограничимся снова рассмотрением лишь того случая, когда законы $\top$ и $\overline{\top}$ всюду определены. Внутренние законы, действующие в Ω и E, чаще всего обозначаются аддитивно (и значит (§ 2, n° 9), считаются ассоциативными и коммутативными); тогда внешний закон, дистрибутивный относительно совокупности этих внутренних законов, записывают в виде умножения слева или справа, так что дистрибутивность выражается соответственно тождеством $(\alpha+\beta)x=\alpha x+\beta x$ или $x(\alpha+\beta)=x\alpha+x\beta$.

При обозначении внешнего закона умножением слева $\alpha \cdot x$ обычно говорят, что он *дистрибутивен слева*, если имеет место тождество $(\alpha+\beta)x=\alpha x+\beta x$; тождество же $\alpha(x+y)=\alpha x+\alpha y$ выражает так называемую *дистрибутивность справа* (т. е. дистрибутивность внешнего закона относительно заданного на E сложения); для закона, обозначаемого $x \cdot \alpha$, эти наименования меняются ролями. При тех же обозначениях, внешний закон называется *двояко дистрибутивным* (относительно двух внутренних законов), если он дистрибутивен и слева и справа. Тогда для любого конечного семейства $(x_\lambda)_{\lambda \in L}$ элементов из E и любого конечного семейства $(\alpha_\iota)_{\iota \in I}$ элементов из Ω имеем

$$\Big(\sum_{\iota \in I} \alpha_\iota\Big) \cdot \Big(\sum_{\lambda \in L} x_\lambda\Big) = \sum_{(\iota,\, \lambda) \in I \times L} (\alpha_\iota \cdot x_\lambda) \tag{4}$$

(и аналогичную формулу при записи умножением справа), в чем можно убедиться индукцией по числу элементов множеств I и L.

Определение 3. *Пусть* $\top$ *и* $\perp$ *— два внутренних закона, заданных на множестве* E. *Говорят, что закон* $\perp$ *двояко дистрибутивен относительно закона* $\top$, *если он всюду определен и каждый из внешних законов, получающихся из* $\perp$ *путем раздвоения, дистрибутивен относительно* $\top$.

Чаще всего один из этих внутренних законов записывается аддитивно (и значит, ассоциативен и коммутативен), а другой мультипликативно (и значит, ассоциативен); в этих обозначениях двоякая дистрибутивность умножения относительно сложения выражается тождествами $x(y+z)=xy+xz$ и $(y+z)x=yx+zx$.

В случае, когда умножение *коммутативно*, эти два тождества равносильны, и при их выполнении говорят просто (допуская вольность речи), что умножение *дистрибутивно* относительно сложения. В прежнем предположении ассоциативности (но не обязательно коммутативности) умножения, пусть A — вполне упорядоченное конечное множество, $(S_\alpha)_{\alpha \in A}$ — серия, элементами которой являются конечные семейства $S_\alpha = (x_{\alpha\lambda})_{\lambda \in L_\alpha}$ элементов из E, и $L = \coprod_{\alpha \in A} L_\alpha$; индукцией по числу элементов множества A получаем «общую формулу дистрибутивности»

$$\prod_{\alpha \in A} \Big(\sum_{\lambda \in L_\alpha} x_{\alpha\lambda}\Big) = \sum_{l \in L} \Big(\prod_{\alpha \in A} x_{\alpha,\, l(\alpha)}\Big). \tag{5}$$

При коммутативности умножения из этой формулы вытекает, что для целых $m>0$, $n>0$ и каждого семейства $(x_i)_{1\leqslant i\leqslant m}$ элементов из E имеет место формула

$$(x_1+x_2+\ldots+x_m)^n=\sum c_{p_1p_2\ldots p_m}x_1^{p_1}x_2^{p_2}\ldots x_m^{p_m},$$

где суммирование в правой части производится по всем последовательностям $(p_i)_{1\leqslant i\leqslant m}$ из m целых чисел $\geqslant 0$ таким, что $\sum_{i=1}^{m}p_i=n$, а

$$c_{p_1p_2\ldots p_m}=\frac{n!}{p_1!p_2!\ldots p_m!}$$

есть число всевозможных отображений $[1, n]$ на $[1, m]$, принимающих p_k раз значение k $(1\leqslant k\leqslant m)$ (Теор. мн., гл. III, § 5).

При $m=2$ получаем формулу, известную под наименованием *бинома Ньютона*:

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

где $\binom{n}{p}=\frac{n!}{p!\,(n-p)!}$ — так называемые *биномиальные коэффициенты*.

Примеры. 1) Если мультипликативно записываемый закон на E ассоциативен и коммутативен, то закон композиции $(n, x)\to x^n$ операторов $n\in\mathbf{N}^*$ и элементов $x\in E$ дистрибутивен относительно указанного умножения (§ 1, формула (8)); но, *вообще говоря, это уже не будет так, если умножение не коммутативно*. Если коммутативное и ассоциативное умножение обладает, кроме того, нейтральным элементом, то закон x^n дистрибутивен для $n\in\mathbf{N}$, и это верно также для $n\in\mathbf{Z}$, если, сверх того, каждый элемент из E обратим.

Аналогичные результаты имеют место и для аддитивно записываемого коммутативного ассоциативного закона на E при замене обозначения x^n на $n\cdot x$.

2) Если мультипликативно записываемый закон на E ассоциативен, то закон $(n, x)\to x^n$ дистрибутивен относительно совокупности сложения в $\mathbf{N}^*$ и умножения в E, поскольку $x^{m+n}=x^mx^n$. Значит, если рассматриваемое умножение коммутативно, то закон x^n двояко дистрибутивен. Если каждый элемент из E обратим, эти результаты распространяются на все $n\in\mathbf{Z}$.

3) Внешний закон композиции $(K, X)\to K(X)$ операторов $K\subset\subset E\times E$ и элементов X из $\mathfrak{P}(E)$ дистрибутивен относительно внутреннего закона $\cap$ на $\mathfrak{P}(E)$, но не относительно $\cap$ (Теор. мн., Рез., § 3,

n°8); он также дистрибутивен относительно совокупности внутренних законов $\cup$ на $\mathfrak{P}(E)$ и $\mathfrak{P}(E\times E)$, т. е. если $K=K'\cup K''$, то

$$K(X)=K'(X)\cup K''(X).$$

Аналогичные результаты имеют место для внешнего закона композиции $A\circ X$ операторов $A\subset F\times F$ и элементов X из $\mathfrak{P}(E\times F)$.

4) Каждый из внутренних законов $\cup$, $\cap$ на $\mathfrak{P}(E)$ (двояко) дистрибутивен относительно другого.

5) В $\mathbf{Z}$ умножение дистрибутивно относительно сложения; сложение дистрибутивно относительно законов $\sup(x, y)$ и $\inf(x, y)$; каждый же из этих двух последних законов дистрибутивен относительно другого и самого себя. В $\mathbf{N}$ и умножение дистрибутивно относительно $\sup(x, y)$ и $\inf(x, y)$.

6) Пусть $\top$ — внутренний закон на множестве E; правый внешний закон, порождаемый законом $f\circ g$, дистрибутивен относительно закона композиции $f\top g$ отображений E в E, т. е. $(f\top g)\circ h=(f\circ h)\top(g\circ h)$; но для левого внешнего закона, порождаемого законом $f\circ g$, это уже неверно.

Подобно ассоциативности и коммутативности, определенные выше различные виды дистрибутивности *сохраняются при факторизации и переходе к произведениям*. Точнее говоря, если, например, внутренний закон $\perp$ на E двояко дистрибутивен относительно внутреннего закона $\top$, а R — отношение эквивалентности, согласующееся с законами $\perp$ и $\top$, то факторзакон закона $\perp$ по R двояко дистрибутивен относительно факторзакона закона $\top$ по R; аналогично для других видов дистрибутивности и перехода к произведениям.

Замечание. Если $\perp$ — внешний закон, дистрибутивный относительно внутреннего закона $\top$ на E, A и B — подмножества множества E и Φ — подмножество множества Ω операторов закона $\perp$, то формула $\Phi\perp(A\top B)=(\Phi\perp A)\top(\Phi\perp B)$, вообще говоря, не верна (иными словами, распространение закона $\perp$ на множества подмножеств не дистрибутивно относительно распространения закона $\top$). Действительно, $\Phi\perp(A\top B)$ есть множество всевозможных элементов $\alpha\perp(x\top y)=(\alpha\perp x)\top(\alpha\perp y)$, где $\alpha\in\Phi$, $x\in A$, $y\in B$, тогда как $(\Phi\perp A)\top(\Phi\perp B)$ есть множество всевозможных элементов $(\alpha\perp x)\top(\beta\perp y)$, где $\alpha\in\Phi$, $\beta\in\Phi$, $x\in A$, $y\in B$, и вообще можно лишь утверждать, что $\Phi\perp(A\top B)\subset(\Phi\perp A)\top(\Phi\perp B)$. С другой стороны, очевидно, что для каждого $\alpha\in\Omega$ имеем

$$\alpha\perp(A\top B)=(\alpha\perp A)\top(\alpha\perp B).$$

2. *Ассоциативность*

Определение 4. *Пусть* $\perp$ *— всюду определенный внешний закон композиции операторов* $\alpha \in \Omega$ *и элементов множества* E *и* $\top$ *— всюду определенный ассоциативный закон композиции элементов из* Ω; *говорят, что закон* $\perp$ *ассоциативен относительно закона* $\top$, *если имеет место тождество*

$$(\alpha \top \beta) \perp x = \alpha \perp (\beta \perp x). \tag{6}$$

В других терминах, если положить $f_\alpha(x) = \alpha \perp x$ (так что $(f_\alpha)_{\alpha \in \Omega}$ — семейство отображений E в E, порождаемых операторами закона $\perp$), должно иметь место равенство $f_{\alpha \top \beta} = f_\alpha \circ f_\beta$, т. е. отображение $\alpha \to f_\alpha$ есть *представление* множества Ω (наделенного законом $\top$) в множество всех отображений E в E (наделенное законом $f \circ g$).

Если внешний закон ассоциативен относительно некоторого внутреннего закона (заданного на его области операторов) и если этот последний записывается мультипликативно, то чаще всего рассматриваемый внешний закон записывают посредством умножения слева $\alpha \cdot x$, так что ассоциативность выражается тождеством $(\alpha\beta)\, x = \alpha\, (\beta x)$; эта композиция обозначается тогда $\alpha\beta x$; точно так же (в силу ассоциативности умножения в Ω) $(\alpha\beta\gamma)\, x = \alpha\, (\beta\gamma x) = (\alpha\beta)\, (\gamma x) = \alpha(\beta\, (\gamma x))$, и общее значение этих композиций обозначается $\alpha\beta\gamma x$; аналогичные формулы имеют место для произведения любого числа операторов.

Если внешний закон ассоциативен относительно закона, *противоположного* мультипликативному закону, заданному на его области операторов, то для этого внешнего закона принимается либо обозначение посредством умножения справа $x \cdot \alpha$, либо экспоненциальное обозначение x^α, так что ассоциативность выражается соответственно тождеством $x(\beta\alpha) = (x\beta)\alpha$ или $x^{\beta\alpha} = (x^\beta)^\alpha$.

Примеры. 1) Если на множестве E задан мультипликативно записываемый ассоциативный закон, то внешний закон $(n, x) \to x^n$ ассоциативен относительно умножения в $\mathbf{N}^*$, поскольку $(x^m)^n = x^{mn}$ (ввиду коммутативности, умножение в $\mathbf{N}^*$ ничем не отличается от противоположного ему закона). Аналогично для $n \in \mathbf{N}$, если в E имеется нейтральный элемент, и для $n \in \mathbf{Z}$, если все элементы из E обратимы.

2) Если на множестве E задан ассоциативный закон $\top$, то внешний закон композиции $(a, X) \to a \top X$ элементов из E (операторов) и подмножеств X множества E ассоциативен относительно закона $\top$

на E; внешний закон $(a, X) \to X \top a$ ассоциативен относительно закона, противоположного $\top$.

3) Внешний закон композиции $(f, x) \to f(x)$ отображений f множества E в E (операторов) и элементов из E ассоциативен относительно внутреннего закона $f \circ g$; точно так же закон композиции $(A, X) \to A(X)$ множеств $A \subset E \times E$ (операторов) и множеств $X \subset E$ ассоциативен относительно внутреннего закона $A \circ B$.

4) Внешний закон композиции $(A, X) \to A \circ X$ операторов $A \subset F \times F$ и множеств $X \subset E \times F$ ассоциативен относительно закона композиции $A \circ B$ операторов; внешний закон композиции $(B, Y) \to Y \circ B$ операторов $B \subset E \times E$ и множеств $Y \subset E \times F$ ассоциативен относительно закона, противоположного закону композиции $B \circ C$ операторов.

Непосредственно ясно, что ассоциативность внешнего закона относительно внутреннего закона, заданного на его области операторов, *сохраняется при факторизации и переходе к произведениям.*

3. Перестановочность

Определение 5. *Пусть* $\top$ *— всюду определенный внешний закон композиции операторов* $\alpha \in \Omega$ *и элементов из* E *и* $\perp$ *— всюду определенный внешний закон композиции операторов* $\beta \in \Theta$ *и элементов из* E. *Говорят, что эти два закона перестановочны, если имеет место тождество*

$$\alpha \top (\beta \perp x) = \beta \perp (\alpha \top x). \tag{7}$$

Иными словами, если $(f_\alpha)_{\alpha \in \Omega}$ и $(g_\beta)_{\beta \in \Theta}$ — семейства отображений E в E, порождаемых соответственно операторами законов $\top$ и $\perp$, f_α должно быть перестановочно с g_β относительно закона $f \circ g$, каковы бы ни были α и β. Внешние законы, о которых идет речь, обычно обозначаются мультипликативно; если все они записываются посредством умножения слева, то перестановочность двух законов выражается тождеством $\alpha(\beta x) = \beta(\alpha x)$; если один записывается посредством умножения слева, а другой — умножения справа, то перестановочность выражается тождеством $\alpha(x\beta) = (\alpha x)\beta$, и общее значение обеих частей равенства обозначается просто $\alpha x \beta$; эта запись оправдывает наименование рассматриваемой пары внешних законов *двояко ассоциативной*, что в данном случае рассматривается как синоним «перестановочности».

Перестановочность двух внешних законов *сохраняется при факторизации и переходе к произведениям.*

Примеры. 1) Если $\top$ — ассоциативный закон на множестве E, то внешние законы композиции $(a, X) \to a \top X$ и $(b, X) \to X \top b$ операторов из E и множеств $X \subset E$ перестановочны.

2) Внешний закон композиции $(A, X) \to A \circ X$ операторов $A \subset F \times F$ и множеств $X \subset E \times F$ перестановочен с внешним законом композиции $(B, X) \to X \circ B$ операторов $B \subset E \times E$ и множеств $X \subset E \times F$.

Упражнения. 1) Пусть $\perp$ — всюду определенный внутренний закон на E, двояко дистрибутивный относительно ассоциативного внутреннего закона $\top$; показать, что если $x \perp x'$ и $y \perp y'$ регулярны относительно закона $\top$, то $x \perp y'$ перестановочно с $y \perp x'$ относительно этого закона. [Вычислить композицию $(x \top y) \perp (x' \top y')$ двумя различными способами.] В частности, если закон $\perp$ обладает нейтральным элементом, то два элемента, регулярных относительно $\top$, перестановочны относительно этого закона; если все элементы из E регулярны относительно $\top$, то этот закон коммутативен.

2) Пусть $\top$ и $\perp$ — всюду определенные внутренние законы на множестве E и левый внешний закон, порожденный законом $\perp$, дистрибутивен относительно $\top$.

а) Если закон $\top$ обладает нейтральным элементом e, то каково бы ни было $x \in E$, $x \perp e$ есть идемпотент относительно $\top$; если при этом существует y такое, что $x \perp y$ регулярно относительно $\top$, то $x \perp e = e$.

б) Если закон $\perp$ обладает нейтральным элементом u и существует элемент $z \in E$, регулярный одновременно относительно обоих законов $\perp$ и $\top$, то u регулярен относительно $\top$.

*3) Пусть $\top$ и $\perp$ — всюду определенные внутренние законы на E, обладающие каждый нейтральным элементом. Если левые внешние законы, порожденные законами $\top$ и $\perp$, дистрибутивны друг относительно друга, то все элементы из E являются идемпотентами относительно каждого из этих двух законов. [Пусть e — нейтральный элемент относительно $\top$ и u — нейтральный элемент относительно $\perp$; доказать прежде всего, что $e \perp e = e$, воспользовавшись тем, что $e = e \perp (u \top e)$.]

4) Пусть на множестве E заданы три всюду определенных внутренних закона композиции: сложение (не обязательно ассоциативное или коммутативное), умножение (не обязательно ассоциативное) и некоторый закон $\top$. Предположим, что умножение обладает ней-

тральным элементом e, что левый внешний закон, порожденный законом $\top$, дистрибутивен относительно умножения и что правый внешний закон, порожденный законом $\top$, дистрибутивен относительно сложения. Показать, что если существуют x, y, z, для которых $x \top z$, $y \top z$ и $(x+y) \top z$ регулярны относительно умножения, то $e+e=e$. [Использовать упражнение 2а.]

*5) Говорят, что всюду определенный внутренний закон композиции $\top$ на E определяет в E структуру *квазигруппы*, если левый и правый переносы γ_x и δ_x являются для всех $x \in E$ взаимно однозначными отображениями E на себя. Квазигруппа называется *дистрибутивной*, если закон $\top$ двояко дистрибутивен относительно самого себя.

а) Определить все структуры дистрибутивной квазигруппы в множестве из n элементов, где $2 \leqslant n \leqslant 6$.

б) °Показать, что множество $\mathbf{Q}$ рациональных чисел, наделенное законом композиции $(x, y) \to \frac{1}{2}(x+y)$, есть дистрибутивная квазигруппа.

в) Каждый элемент дистрибутивной квазигруппы E идемпотентен. Вывести отсюда, что если E содержит более одного элемента, то $\top$ не может ни обладать нейтральным элементом, ни быть ассоциативным.

г) Левые и правые переносы в E являются автоморфизмами.

д) Если E *конечно*, то структура, индуцированная в каждом его устойчивом подмножестве, есть структура дистрибутивной квазигруппы.

е) Если R — отношение эквивалентности, согласующееся слева (соответственно справа) с $\top$, то классы mod R являются устойчивыми множествами. Если E конечно, то все эти классы получаются из одного из них посредством левого (соответственно правого) переноса; при тех же условиях, если R согласуется с $\top$, то факторструктура в E/R есть структура дистрибутивной квазигруппы.

ж) Множество A_a всех элементов из E, перестановочных с заданным элементом a, устойчиво; если E конечно, то для каждого $x \in A_a$ имеем $A_x = A_a$ [используя д), заметить, что существует $y \in A_a$, для которого $x \in a \top y$], и множества A_x, где x пробегает E, совпадают с классами эквивалентности по некоторому отношению, согласующемуся с $\top$.

з) Если E конечно, а $\top$ коммутативен, то число элементов множества E нечетно. [Рассмотреть пары (x, y) элементов из E, для которых $x \top y = y \top x = a$, где a задано.]

6) Пусть на множестве E заданы (ассоциативное и коммутативное) сложение, относительно которого все элементы из E симметризуемы °(иными словами — закон композиции аддитивной группы), и (ассо-

циативное) умножение, двояко дистрибутивное относительно сложения; положим $x \circ y = xy - yx$; закон $x \circ y$ двояко дистрибутивен относительно сложения. Для того чтобы x и y были перестановочны относительно умножения, необходимо и достаточно, чтобы $x \circ y = 0$; имеют место тождества

$$x \circ y = -(y \circ x); \quad x \circ (y \circ z) + y \circ (z \circ x) + z \circ (x \circ y) = 0$$

(второе из которых известно под наименованием «тождества Якоби»). Второе тождество записывается также в виде

$$x \circ (y \circ z) - (x \circ y) \circ z = (z \circ x) \circ y,$$

выражающем «отклонение закона $x \circ y$ от ассоциативности».

7) В тех же предположениях, что и в упражнении 6, положим $x \top y = xy + yx$; тогда закон $\top$ коммутативен, двояко дистрибутивен относительно сложения, но вообще не ассоциативен.

а) Показать, что, каково бы ни было $x \in E$, $\overset{m+n}{\top} x = (\overset{m}{\top} x) \top (\overset{n}{\top} x)$.

б) Положим $[x, y, z] = (x \top y) \top z - x \top (y \top z)$ (отклонение закона $\top$ от ассоциативности). Доказать тождества

$$[x, y, z] + [z, y, x] = 0,$$
$$[x, y, z] + [y, z, x] + [z, x, y] = 0,$$
$$[x \top y, u, z] = u \circ ((x \top y) \circ z)$$

(где $x \circ y$ имеет тот же смысл, что и в упражнении 6) и

$$[x \top y, u, z] + [y \top z, u, x] + [z \top x, u, y] = 0.$$

*8) Пусть на E заданы (ассоциативное и коммутативное) сложение, относительно которого все элементы из E симметризуемы, и умножение, не ассоциативное, однако коммутативное и двояко дистрибутивное относительно сложения. Предположим, кроме того, что в E отношение $n \cdot x = 0$ (где n — любое целое $\neq 0$) влечет $x = 0$. Положим $[x, y, z] = (xy)\, z - x\, (yz)$. Показать, что если имеет место тождество

$$[xy, u, z] + [yz, u, x] + [zx, u, y] = 0,$$

то $x^{m+n} = x^m x^n$ для всех $x \in E$. [Показать с помощью индукции по p, что при $1 \leqslant q < p$ имеет место тождество $[x^q, y, x^{p-q}] = 0$.]

§ 6. Группы и группы с операторами

1. *Группы*

Определение 1. *Говорят, что всюду определенный внутренний закон композиции на множестве G определяет в G структуру группы* (или *групповую структуру*), *если* 1° *он ассоциативен*; 2° *он обладает нейтральным элементом*; 3° *для каждого элемента*

из G в G существует элемент, симметричный ему относительно этого закона. Множество, наделенное групповой структурой, называют группой.

В силу предложений 3 и 4 § 2, то же самое можно выразить, сказав, что группа G — это *непустой моноид* (§ 1, n° 3), такой, что левый и правый переносы γ_x и δ_x являются для каждого $x \in G$ отображениями G *на* G: тогда они являются *взаимно однозначными* отображениями G на G (см. упражнение 2).

Примеры. 1) В произвольном моноиде E, обладающем нейтральным элементом, множество всех симметризуемых элементов, наделенное индуцированной структурой, есть группа. В частности, множество всех взаимно однозначных отображений F на себя (т. е. всех *подстановок* множества F) есть группа относительно закона $f \circ g$; она называется *симметрической группой* множества F; мы еще вернемся к этой группе и более детально рассмотрим ее в § 7.

2) Если E — множество, наделенное коммутативным ассоциативным законом $\top$, и $\overline{E}$ — *результат симметризации* множества E (§ 2, n° 4) относительно $\top$, то множество всех регулярных элементов из $\overline{E}$ образует группу относительно индуцированного на нем из $\overline{E}$ закона. В частности, множество $\mathbf{Z}$, наделенное сложением, есть группа; она называется *аддитивной группой рациональных целых чисел*; точно так же и множество $\mathbf{Q}_+^*$ рациональных чисел > 0, наделенное умножением, есть группа.

Группа G называется *конечной*, если множество ее элементов конечно, и *бесконечной* — в противном случае. Число элементов конечной группы называют *порядком* этой группы.

Если закон композиции на G определяет в G структуру группы, то это же верно и для противоположного закона; две определенные так группы называются *противоположными*. Отображение группы G на себя, относящее каждому элементу из G *симметричный* ему элемент, есть *изоморфизм* группы G на противоположную группу (§ 2, предложение 5); оно называется *симметрией* или *отображением симметрии* группы G на себя и является инволютивной подстановкой этой группы.

В настоящем параграфе всюду, где явно не оговорено противное, мы обозначаем закон композиции группы *мультипликативно*, а нейтральный элемент записываемого так группового закона

обозначаем e (напомним, что в этом случае e часто называется *единичным элементом* группы); симметрия группы G на себя записывается тогда $x \longrightarrow x^{-1}$.

Следуя нашим общим соглашениям (Теор. мн., Рез., § 2, n° 4), мы обозначаем образ множества $A \subset G$ при симметрии $x \longrightarrow x^{-1}$ через A^{-1}. Но важно отметить, что, несмотря на сходство обозначений, A^{-1} отнюдь не является элементом, обратным A относительно закона композиции $(X, Y) \longrightarrow XY$ подмножеств множества G (напомним, что XY есть множество всех xy, где $x \in X$, $y \in Y$); действительно, нейтральным элементом относительно этого закона служит $\{e\}$, а единственными элементами из $\mathfrak{P}(G)$, обратимыми относительно этого закона, являются множества $A = \{a\}$, сводящиеся к одному элементу (причем такое A действительно имеет своим обратным A^{-1}). Имеет место тождество $(AB)^{-1} = B^{-1}A^{-1}$ ($A \subset G$, $B \subset G$). Если $A = A^{-1}$, то A называется *симметричным* подмножеством группы G. Каково бы ни было $A \subset G$, $A \cup A^{-1}$, $A \cap A^{-1}$ и AA^{-1} симметричны.

2. Подгруппы

Определение 2. *Подгруппой группы G называется всякое непустое множество $H \subset G$ такое, что структура, индуцированная в нем из G, есть структура группы.*

Предложение 1. *Пусть H — непустое подмножество группы G; следующие утверждения равносильны:*

а) *H — подгруппа группы G.*

б) *H — устойчивое множество* (иными словами, отношения $x \in H$, $y \in H$ влекут $xy \in H$) *и отношение $x \in H$ влечет $x^{-1} \in H$.*

в) *Отношения $x \in H$, $y \in H$ влекут $xy^{-1} \in H$.*

Покажем сначала, что из а) следует б). Поскольку закон композиции, индуцированный в H из G, должен быть всюду определенным, H должно быть устойчивым множеством в G. При этом, поскольку индуцированный закон должен обладать нейтральным элементом u, последний удовлетворяет условию $u \cdot u = u$, откуда $u = u \cdot u^{-1} = e$, так что H содержит e; следовательно, если элемент $x \in H$ обратим в H, его обратный в H совпадает с его обратным x^{-1} в G; тем самым б) полностью доказано.

Обратно, из б) следует а); действительно, для каждого $x \in H$ имеем $x^{-1} \in H$ и, значит, $x \cdot x^{-1} = e \in H$; тем самым закон композиции, индуцированный в H из G, определяет в H структуру группы.

Наконец, ясно, что из б) следует в); обратно, если в) выполнено, то $x \in H$ влечет $x \cdot x^{-1} = e \in H$ и, далее, $e \cdot x^{-1} = x^{-1} \in H$; следовательно, отношения $x \in H$, $y \in H$ влекут $x(y^{-1})^{-1} = xy \in H$, чем доказано, что из в) следует б).

Замечания. 1) Так же доказывается, что утверждение б) предложения 1 равносильно следующему:

в′) *Отношения* $x \in H$, $y \in H$ *влекут* $y^{-1}x \in H$.

2) Утверждение б) может быть также записано в виде $H \cdot H \subset H$ и $H^{-1} \subset H$. Таким образом, в случае *непустого* множества $H \subset G$ из этих отношений следует, что H — подгруппа; тогда $e \in H$, откуда $X \subset H \cdot X$ для каждого $X \subset G$ и, в частности, $H \subset H \cdot H$; с другой стороны, отображение симметрии группы G преобразует включение $H^{-1} \subset H$ в $H \subset H^{-1}$. Тем самым для каждой подгруппы H группы G выполняются отношения

$$H \cdot H = H, \quad H^{-1} = H. \tag{1}$$

Утверждение в) записывается также в виде $H \cdot H^{-1} \subset H$; таким образом, для непустого множества $H \subset G$ это отношение равносильно отношениям (1); то же верно и для отношения $H^{-1} \cdot H \subset H$.

Ясно, что если H — подгруппа группы G, а K — подгруппа группы H, то K — подгруппа группы G.

Множество $\{e\}$ есть подгруппа группы G, очевидно, наименьшая (ибо содержится во всех подгруппах). Пересечение H семейства подгрупп (H_ι) есть подгруппа, ибо оно не пусто ($e \in H_\iota$ для каждого ι) и отношения $x \in H$, $y \in H$, влекущие $xy^{-1} \in H_\iota$ для каждого ι, влекут тем самым $xy^{-1} \in H$.

Следовательно, существует наименьшая подгруппа G, содержащая заданное множество $X \subset G$; она называется *подгруппой, порожденной множеством* X, а X — *системой образующих* этой подгруппы.

Пример. Найдем все подгруппы аддитивной группы $\mathbf{Z}$ рациональных целых чисел. Если H — такая подгруппа, не сводящаяся к одному элементу 0, то пусть $x \in H$ таково, что $x \neq 0$; тогда либо $x > 0$, либо, при $x < 0$, $x' = -x > 0$ и $x' \in H$; таким образом, множество всех элементов > 0 из H не пусто; пусть a — его наименьший элемент. Индукцией по $m \in \mathbf{N}^*$ убеждаемся в том, что $ma \in H$ для всех $m \in \mathbf{N}^*$; значит, также $-ma \in H$ для всех $m \in \mathbf{N}^*$, и так как $0 \in H$, то, следовательно, $na \in H$, каково бы ни было $n \in \mathbf{Z}$. Пусть $x \in H$, тогда (§ 4, n° 3) $x = qa + r$, где $q \in \mathbf{Z}$ и $0 \leqslant r < a$; так как $qa \in H$, то $r = x - qa \in H$; но, по определению элемента a, $0 < r < a$ влекло бы $r \notin H$; значит, $r = 0$ и $x = qa$. Тем самым H совпа-

дает с множеством всех na, где $n \in \mathbf{Z}$, иными словами, $H = a \cdot \mathbf{Z}$. Обратно, очевидно, $a\mathbf{Z}$ есть подгруппа группы $\mathbf{Z}$ для всякого $a \in \mathbf{N}^*$; если $a = 0$, то $a \cdot \mathbf{Z} = \{0\}$; если $a < 0$, то $a' = -a > 0$ и $a\mathbf{Z} = a'\mathbf{Z}$. Из проведенного выше доказательства видно также, что $a\mathbf{Z}$ есть подгруппа, порожденная множеством $\{a\}$, и что устойчивым подмножеством множества $\mathbf{Z}$, порожденным $\{a\}$, служит множество $a\mathbf{N}^*$ всех ma, где m пробегает $\mathbf{N}^*$.

Этот пример показывает, что следует остерегаться смешения устойчивого подмножества группы G, порожденного множеством $X \subset G$, с подгруппой, порожденной этим множеством: первое всегда содержится во второй, но вообще отлично от нее. Способ образования подгруппы, порождаемой множеством X, точно описывается следующим предложением:

Предложение 2. *Подгруппа, порожденная непустым подмножеством X группы G, совпадает с устойчивым множеством Y^∞, порожденным множеством $Y = X \cup X^{-1}$.*

Действительно, Y^∞ есть множество композиций всевозможных последовательностей, все члены которых — либо элементы из X, либо обратны таким элементам; так как элемент, обратный композиции этого вида, снова есть композиция того же вида (§ 2, предложение 5), то (предложение 1) Y^∞ есть подгруппа группы G; обратно, каждая подгруппа, содержащая X, очевидно, содержит Y, а потому и Y^∞.

3. Факторгруппы

Выясним, какие отношения эквивалентности согласуются с законом композиции группы. Согласно предложению 1 § 4, достаточно рассмотреть отдельно согласованность слева и согласованность справа; вопрос решается следующей теоремой:

Теорема 1. *Если отношение эквивалентности R в группе G согласуется слева (справа) с групповым законом, то оно равносильно отношению вида $x^{-1}y \in H$* (соответственно $yx^{-1} \in H$), *где H — подгруппа группы G. Обратно, для любой подгруппы H отношение $x^{-1}y \in H$* (соответственно $yx^{-1} \in H$) *есть отношение эквивалентности, согласующееся слева* (соответственно *справа*) *с заданным в G групповым законом.*

Ограничимся рассмотрением того случая, когда отношение R согласуется слева с групповым законом (случай отношения, согла-

сующегося справа, получается отсюда переходом от G к противоположной группе). Отношение $y \equiv x \pmod{R}$ равносильно отношению $x^{-1}y \equiv e \pmod{R}$, ибо $y \equiv x$ влечет $x^{-1}y \equiv x^{-1}x$ и, обратно, $x^{-1}y \equiv e$ влечет $x(x^{-1}y) \equiv x$. Таким образом, R равносильно отношению $x^{-1}y \in H$, где H — класс, образованный элементами $x \equiv e$. Покажем, что H — *подгруппа* группы G; для этого достаточно установить (предложение 1), что $x \in H$ и $y \in H$ влекут $x^{-1}y \in H$, т. е. что $x \equiv e$ и $y \equiv e$ влекут $x \equiv y$; но это вытекает из транзитивности отношения R.

Обратно, пусть H — подгруппа группы G; отношение $x^{-1}y \in H$ рефлексивно, поскольку $x^{-1}x = e \in H$; оно симметрично, поскольку $x^{-1}y \in H$ влечет $y^{-1}x = (x^{-1}y)^{-1} \in H$; оно транзитивно, ибо $x^{-1}y \in H$ и $y^{-1}z \in H$ влекут $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$; наконец, оно согласуется слева с законом композиции группы G, ибо $x^{-1}y = (zx)^{-1}(zy)$ для любого $z \in G$.

Отношение $x^{-1}y \in H$ (соответственно $yx^{-1} \in H$) записывается также в равносильной форме $y \in xH$ (соответственно $y \in Hx$). Таким образом, каждая подгруппа H группы G определяет два отношения квивалентности в G, а именно: $y \in xH$ и $y \in Hx$; классами эквивалентности по этим отношениям служат соответственно множества xH, называемые *левыми классами по* H (или *по модулю* H), и множества Hx, называемые *правыми классами по* H (или *по модулю* H). *Насыщая* множество $A \subset G$ по этим отношениям (Теор. мн., Рез., § 5, n° 6), получаем соответственно множества AH и HA. При переходе к противоположной группе каждая подгруппа H остается подгруппой, причем левые классы превращаются в правые и обратно; при симметрии группы G каждая ее подгруппа H отображается на себя, а левые классы преобразуются в правые и обратно.

Если число различных левых классов (mod H) *конечно*, оно называется *индексом* подгруппы H относительно G и обозначается $(G:H)$; оно равно также числу правых классов. Если существует бесконечное множество различных левых классов, то H называется подгруппой бесконечного индекса.

Подгруппа K группы G, содержащая H, является объединением левых (равно как и правых) классов по H; если при этом K — объединение конечного числа различных левых классов по H т. е. индекс $(K:H)$ конечен), то и каждый левый класс по K есть

объединение такого же числа различных левых классов по H, ибо он получается из K путем левого переноса. В частности, имеет место

Предложение 3. *Пусть H и K — подгруппы группы G, причем $H \subset K$. Если индекс $(G:H)$ конечен, то также индексы $(G:K)$ и $(K:H)$ конечны и*

$$(G:H) = (G:K)\,(K:H). \tag{2}$$

Обратно, если $(G:K)$ и $(K:H)$ конечны, то $(G:H)$ конечно и имеет место формула (2).

Следствие. *Если G — конечная группа порядка g и H — ее подгруппа порядка h, то*

$$(G:H) = \frac{g}{h} \tag{3}$$

(в частности, порядок и индекс подгруппы H являются *делителями* порядка группы G).

Теорема 1 позволяет охарактеризовать отношения эквивалентности, согласующиеся с групповым законом в G: так как такое отношение R согласуется с групповым законом одновременно и слева и справа, то класс H нейтрального элемента e $(\mathrm{mod}\, R)$ есть подгруппа, для которой отношения $y \in xH$ и $y \in Hx$ (будучи оба равносильными R) равносильны; таким образом, $xH = Hx$, каково бы ни было $x \in G$. Обратно, если это условие выполнено, то оба отношения эквивалентности $y \in xH$ и $y \in Hx$ согласуются с групповым законом, поскольку они согласуются с ним одновременно и слева и справа (§ 4, предложение 1). Принимая во внимание, что равенство $xH = Hx$ эквивалентно равенству $xHx^{-1} = H$, вводим следующее определение:

Определение 3. *Подгруппа H группы G называется нормальной* (или *инвариантной*), *если $xHx^{-1} = H$ для всех $x \in G$.*

> Для установления нормальности подгруппы H достаточно показать, что $xHx^{-1} \subset H$ для всех $x \in G$; действительно, тогда для всех $x \in G$ также $x^{-1}Hx \subset H$, т. е. $H \subset xHx^{-1}$, и, следовательно, $H = xHx^{-1}$.

Пусть H — нормальная подгруппа группы G и R — определяемое ею отношение эквивалентности $y \in xH$; факторзакон закона группы G по R на фактормножестве G/R ассоциативен; класс

нейтрального элемента e группы G является нейтральным элементом относительно этого факторзакона, и классы двух взаимно обратных элементов из G взаимно обратны относительно него (§ 4, п° 3). Таким образом, резюмируя полученные результаты, имеем:

Теорема 2. *Отношения эквивалентности, согласующиеся с законом группы G,— это отношения вида $y \in xH$, где H — ее нормальная подгруппа* (причем отношение $y \in xH$ для такой подгруппы H равносильно отношению $y \in Hx$); *факторструктура структуры группы G по этому отношению есть структура группы.*

Определение 4. *Результат факторизации группы G по отношению эквивалентности, определяемому ее нормальной подгруппой H, называется факторгруппой группы G по H и обозначается G/H.*

Отношение эквивалентности, определяемое нормальной подгруппой H группы G, иногда записывают в виде $x \equiv y \pmod{H}$ или $x \equiv y\ (H)$; факторзакон закона группы G по этому отношению часто для краткости называется факторзаконом закона группы G по H.

Замечания. 1) Если H — нормальная подгруппа группы G, то, каково бы ни было $A \subset G$, $AH = HA$; это — множество, получающееся путем насыщения множества A по отношению $x \equiv y \pmod{H}$.

2) Композицией любых двух элементов xH и yH факторгруппы G/H служит элемент xyH, равный композиции $(xH)(yH)$ в $\mathfrak{P}(G)$, ибо $HyH = y(y^{-1}Hy)H = y(HH) = yH$. Точно так же обратным к xH в G/H служит элемент $x^{-1}H$, равный $(xH)^{-1}$, поскольку последнее есть не что иное, как $H^{-1}x^{-1} = Hx^{-1}$.

3) Если H — нормальная подгруппа конечного индекса, то факторгруппа G/H есть конечная группа порядка $(G:H)$.

Пример. Если закон композиции группы G коммутативен, то $xyx^{-1} = y$, каковы бы ни были x и y, так что всякая подгруппа группы G — нормальная; так обстоит дело, например, для аддитивной группы $\mathbf{Z}$ рациональных целых чисел. Ее подгруппы были определены выше (п° 2): это — множества $a\mathbf{Z}$, где $a \in \mathbf{Z}$; отношение эквивалентности, определяемое подгруппой $a\mathbf{Z}$,— не что иное, как отношение $x - y \in a\mathbf{Z}$, т. е. сравнение $x \equiv y \pmod{a}$ (§ 4, п° 3): сравнения — единственные отношения эквивалентности, согласующиеся со сложением в $\mathbf{Z}$. При $a > 0$ факторгруппа аддитивной группы $\mathbf{Z}$ по сравнению $\bmod a$ называется *аддитивной группой рациональных целых по модулю a*; это — *конечная* группа порядка a.

Подгруппы G и $\{e\}$ каждой группы G — нормальные (а G/G и $G/\{e\}$ изоморфны соответственно $\{e\}$ и G); если это единственные нормальные подгруппы, то группу G называют *простой*. Пересечение всякого семейства нормальных подгрупп группы G есть нормальная подгруппа; поэтому можно говорить о наименьшей нормальной подгруппе группы G, содержащей множество $X \subset G$.

Заметим, что (как мы убедимся на примерах) нормальная подгруппа K нормальной подгруппы H группы G не всегда есть нормальная подгруппа группы G.

4. *Представления*

Общее определение представления (§ 4, определение 7) приводит, в частности, в случае групп к следующему определению:

Определение 5. *Пусть G — группа и G' — множество, наделенное внутренним законом композиции. Отображение f группы G в G' называется представлением* (или *гомоморфизмом*) *G в G', если* (при мультипликативном обозначении заданных в G и G' законов), *каковы бы ни были $x \in G$ и $y \in G$, $f(x)f(y)$ определено и*

$$f(xy) = f(x)f(y). \tag{4}$$

Каноническое отображение группы G на ее факторгруппу G/H по нормальной подгруппе H есть гомоморфизм; он называется *каноническим гомоморфизмом* G на G/H.

Если f — гомоморфизм G в G', то отношение $f(x) = f(y)$ равносильно отношению $f(x^{-1}y) = f(e)$; поэтому общая теорема о гомоморфизмах (§ 4, теорема 1) в соединении с установленной выше теоремой 2 приводит к следующему результату:

Теорема 3. *Пусть f — представление группы G в множество G', наделенное внутренним законом композиции. Тогда $f(G)$ есть группа* (относительно закона, индуцированного из G') *с нейтральным элементом $e' = f(e)$. Прообраз $H = f^{-1}(e')$ последнего есть нормальная подгруппа группы G (называемая ядром представления f); группа $f(G)$ (называемая образом представления f) изоморфна факторгруппе G/H, и представление f есть композиция канонического гомоморфизма G на G/H и инъективного гомоморфизма G/H в G'.*

Иными словами, каноническое разложение представления f (Теор. мн., Рез., § 5, n° 3) дает: 1° канонический гомоморфизм G на G/H; 2° изоморфизм G/H на $f(G)$, называемый *взаимно однозначным представлением, ассоциированным с* f; 3° каноническую инъекцию $f(G)$ в G' (ср. § 4, n° 4).

Следуя снова § 4, мы будем называть представление группы G в себя *эндоморфизмом* группы G, и, как всегда, *автоморфизмом* группы G будет изоморфизм G на себя. Композиция двух эндоморфизмов группы G относительно закона $f \circ g$ есть снова эндоморфизм этой группы; композиция двух автоморфизмов группы G относительно того же закона, равно как и отображение, обратное к автоморфизму, есть автоморфизм группы G.

Иными словами, автоморфизмы группы G образуют *группу* относительно закона $f \circ g$ (см. § 7).

Предложение 4. *Каков бы ни был элемент x группы G, ее отображение α_x в себя, определяемое формулой $\alpha_x(y) = xyx^{-1}$, является автоморфизмом этой группы.*

Действительно, α_x — эндоморфизм группы G, ибо

$$x \cdot yz \cdot x^{-1} = (xyx^{-1})(xzx^{-1}).$$

С другой стороны, так как отношение $xyx^{-1} = u$ равносильно отношению $y = x^{-1}ux$, то для каждого $u \in G$ существует, и притом единственное, y такое, что $\alpha_x(y) = u$, иными словами, α_x есть взаимно однозначное отображение группы G на себя. Тем самым α_x — ее автоморфизм.

Автоморфизмы α_x называются *внутренними автоморфизмами* группы G.

При мультипликативной записи группы G иногда пишут

$$y^x = \alpha_{x^{-1}}(y) = x^{-1}yx.$$

Это обозначение оправдывается (по соглашениям § 5) тем, что отображение $(x, y) \to y^x$, рассматриваемое как *внешний* закон композиции операторов $x \in G$ и элементов $y \in G$, дистрибутивно относительно группового закона для элементов y и ассоциативно относительно противоположного закона для операторов x — свойства, выражаемые тождествами

$$(xy)^u = x^u y^u, \quad x^{uv} = (x^u)^v.$$

Однако мы будем пользоваться этим экспоненциальным обозначением лишь когда оно не сможет вызвать недоразумений, и притом каждый раз напоминая его смысл.

Очевидно, автоморфизм группы G, и в частности внутренний автоморфизм, преобразует каждую ее подгруппу в изоморфную подгруппу; определение 3 означает, что подгруппа группы G— нормальная, если она преобразуется в себя каждым внутренним автоморфизмом группы.

5. *Произведения групп*

Замечания, сделанные в n° 5 § 4, показывают, что произведение групповых структур является групповой структурой, что позволяет ввести следующее определение:

Определение 6. *Произведением семейства групп* $(G_\iota)_{\iota\in I}$ *называется произведение* $G=\prod_{\iota\in I} G_\iota$ *семейства множеств* $(G_\iota)_{\iota\in I}$, *наделенное групповой структурой, определяемой законом, относящим любым двум элементам* $x=(x_\iota)$ *и* $y=(y_\iota)$ *этого произведения элемент* $xy=(x_\iota y_\iota)$.

Если H_ι — подгруппы (соответственно нормальные подгруппы) групп G_ι, то $\prod_{\iota\in I} H_\iota$, наделенное структурой, индуцированной из G, есть подгруппа (соответственно нормальная подгруппа) группы G, изоморфная произведению групп H_ι. В частности, пусть $J\subset I$ и $K=\complement J$; произведение $G_J=\prod_{\iota\in J} G_\iota$ изоморфно нормальной подгруппе $G'_J=\left(\prod_{\iota\in J} G_\iota\right)\times\left(\prod_{\iota\in K}\{e_\iota\}\right)$ группы G и часто отождествляется с ней посредством изоморфизма (называемого *каноническим*), относящего каждому элементу $(x_\iota)_{\iota\in J}\in G_J$ элемент $(y_\iota)_{\iota\in I}\in G'_J$ такой, что $y_\iota=x_\iota$ для всех $\iota\in J$ и $y_\iota=e_\iota$ для всех $\iota\notin J$. Проекция pr_J группы G на G_J есть гомоморфизм G на G_J; прообраз нейтрального элемента группы G_J относительно этого гомоморфизма есть не что иное, как G'_K, так что G_J изоморфно G/G'_K, а G — произведению $G'_J\times(G/G'_J)$. Из определения 6 следует, что если J_1 и J_2 — два непересекающихся подмножества множества I, то каждый элемент из G'_{J_1} *перестановочен* с каждым элементом из G'_{J_2}.

Предложение 4 § 4 дает здесь следующее:

Предложение 5. *Пусть G_1 и G_2 — группы и H_1, H_2 — их нормальные подгруппы. Каноническое отображение произведения факторгрупп $(G_1/H_1)\times(G_2/H_2)$ на факторгруппу $(G_1\times G_2)/(H_1\times H_2)$ есть изоморфизм.*

Более общим образом, пусть $(G_\iota)_{\iota\in I}$ — произвольное семейство групп и $G=\prod_{\iota\in I} G_\iota$ — его произведение; пусть, далее, H_ι для каждого $\iota\in I$ — нормальная подгруппа группы G_ι и f_ι — канонический гомоморфизм G_ι на G_ι/H_ι. Ясно, что отображение $(x_\iota)\to(f_\iota(x_\iota))$ группы G в группу $G'=\prod_{\iota\in I} G_\iota/H_\iota$ есть сюръективный *) гомоморфизм, ядром которого служит нормальная подгруппа $H=\prod_{\iota\in I} H_\iota$ группы G; поэтому заключаем (теорема 3), что G/H *канонически изоморфно* G'.

Важным частным случаем произведения групп является группа, образованная всеми отображениями некоторого множества E в группу G, с композицией $h=fg$ отображений f и g, определенной условием, что $h(x)=f(x)\,g(x)$ для всех $x\in E$; эта группа есть не что иное, как произведение G^E групп G.

6. *Прямое произведение подгрупп*

Пусть $G=\prod_{1\leqslant i\leqslant n} G_i$ — произведение *конечного* семейства групп G_i; согласно предыдущему, G_i изоморфно нормальной подгруппе $G'_i=G_i\times\prod_{j\neq i}\{e_j\}$ группы G и при $i\neq j$ каждый элемент из G'_i перестановочен с каждым элементом из G'_j. Всякий элемент $x=(x_i)\in G$ представим в виде $x=u_1u_2\ldots u_n$, где $u_i=(u_{ij})$ — элемент из G'_i такой, что $u_{ii}=x_i$ и $u_{ij}=e_j$ для всех $j\neq i$; обратно, если $x=v_1v_2\ldots v_n$, где $v_i\in G'_i$ $(1\leqslant i\leqslant n)$, и $\mathrm{pr}_i(v_i)=y_i$, то $x=(y_i)$, откуда $y_i=x_i$ и $v_i=u_i$; таким образом, элементы u_i однозначно определяются заданием x; при этом x есть также композиция любой последовательности, получающейся из последовательности $(u_i)_{1\leqslant i\leqslant n}$ перестановкой членов (§ 1, теорема 3).

*) Сюръективное отображение — отображение на.— *Перев.*

Введем следующее определение:

Определение 7. *Мультипликативная группа G называется прямым произведением конечного семейства $(H_i)_{1\leqslant i\leqslant n}$ своих различных подгрупп, если при $i\neq j$ каждый элемент из H_i перестановочен с каждым элементом из H_j и если каждое $x\in G$ представимо, притом единственным способом, в виде $x=u_1u_2\ldots u_n$, где $u_i\in H_i$ $(1\leqslant i\leqslant n)$. Элемент u_i называется компонентой x в H_i.*

Таким образом, можно сказать, что каждое произведение $G=\prod\limits_{1\leqslant i\leqslant n} G_i$ конечного семейства групп есть прямое произведение подгрупп G_i', изоморфных G_i.

Обратно, допустим, что группа G есть прямое произведение семейства $(H_i)_{1\leqslant i\leqslant n}$ своих подгрупп. Для каждого $x\in G$ отношение $x=u_1u_2\ldots u_n$, где $u_i\in H_i$ $(1\leqslant i\leqslant n)$, по предположению, однозначно определяет элементы u_i; положим $u_i=f_i(x)$. Покажем, что f_i — *гомоморфизм* G на H_i. Действительно, так как $f_i(H_i)=H_i$, то f_i отображает G на H_i. С другой стороны, если $y\in G$, $v_i=f_i(y)$, $y=v_1v_2\ldots v_n$, то условие перестановочности подгрупп H_i влечет $xy=(u_1v_1)(u_2v_2)\ldots(u_nv_n)$; в самом деле, достаточно доказать индукцией по p, что

$$(u_1u_2\ldots u_p)(v_1v_2\ldots v_p)=(u_1v_1)(u_2v_2)\ldots(u_pv_p);$$

а это очевидно, если заметить, что, согласно предложению 2 § 1, $u_pv_1v_2\ldots v_{p-1}=v_1v_2\ldots v_{p-1}u_p$. Отсюда следует, что отображение $x\longrightarrow(f_i(x))$ есть *изоморфизм* группы G на произведение групп $\prod\limits_{1\leqslant i\leqslant n} H_i$, переводящий H_i в нормальную подгруппу H_i' этого произведения, образованную теми $u=(u_i)$, в которых $u_j=e$ при $j\neq i$. Резюмируя, имеем:

Предложение 6. *Если группа G есть прямое произведение конечного семейства $(H_i)_{1\leqslant i\leqslant n}$ своих подгрупп H_i, то последние являются ее нормальными подгруппами, и отображение, относящее каждому элементу $u=(u_i)$ произведения $\prod\limits_{1\leqslant i\leqslant n} H_i$ групп H_i композицию $u_1u_2\ldots u_n$ последовательности (u_i), есть* (называемый *каноническим*) *изоморфизм $\prod\limits_{1\leqslant i\leqslant n} H_i$ на G.*

Основываясь на этом изоморфизме, часто не делают различия между понятиями *произведения* и *прямого произведения* конечного семейства подгрупп заданной группы.

Если G — прямое произведение своих подгрупп H_i $(1 \leqslant i \leqslant n)$, то из указанного изоморфизма явствует, что

$$(H_1 H_2 \ldots H_{i-1} H_{i+1} \ldots H_n) \cap H_i = \{e\} \quad (1 \leqslant i \leqslant n).$$

Обратно:

Предложение 7. *Если $(H_i)_{1 \leqslant i \leqslant n}$—конечное семейство нормальных подгрупп группы G, обладающее тем свойством, что*

$$(H_1 H_2 \ldots H_i) \cap H_{i+1} = \{e\} \qquad (1 \leqslant i \leqslant n-1),$$

то $H_1 H_2 \ldots H_n$ есть нормальная подгруппа группы G, являющаяся прямым произведением подгрупп H_i.

Применение индукции по n сразу сводит вопрос к доказательству предложения для $n = 2$. Покажем сначала, что любые два элемента $x \in H_1$ и $y \in H_2$ *перестановочны*; действительно, так как $xyx^{-1}y^{-1} = (xyx^{-1})\,y^{-1} = x\,(yx^{-1}y^{-1})$, то (вследствие нормальности подгрупп H_1 и H_2) $xyx^{-1}y^{-1} \in H_1 \cap H_2$, т. е., в силу предположения, $xyx^{-1}y^{-1} = e$. Отсюда следует (согласно предложению 1), что $H_1 H_2$ есть подгруппа группы G, и непосредственно проверяется, что эта подгруппа — нормальная. Пусть, наконец, $xy = x'y'$, где $x \in H_1$, $x' \in H_1$, $y \in H_2$, $y' \in H_2$; тогда $x'^{-1}x = y'y^{-1}$, значит, $x'^{-1}x \in H_1 \cap H_2 = \{e\}$, $x' = x$, и так же $y' = y$. Тем самым $H_1 H_2$ есть прямое произведение подгрупп H_1 и H_2.

Для аддитивных групп вместо «прямое произведение» употребляют термин *прямая сумма*.

7. *Коммутативные группы; моногенные группы*

Определение 8. *Группу называют коммутативной* (или *абелевой*), *если ее закон композиции коммутативен.*

Коммутативная группа будет часто записываться *аддитивно*, а ее нейтральный элемент обозначаться тогда 0 (и называться нулем).

В коммутативной группе каждый внутренний автоморфизм сводится к тождественному и, значит, всякая подгруппа нормальна.

Всякая факторгруппа коммутативной группы коммутативна; всякое произведение коммутативных групп коммутативно.

Пусть G — произвольная группа и A — ее подмножество, элементы которого попарно перестановочны; в силу доказанного выше предложения 2 и предложения 7 § 2, подгруппа группы G, порожденная множеством A, коммутативна.

Рассмотрим, в частности, тот случай, когда A сводится к одному элементу x; тогда подгруппа X, порожденная множеством A, образована степенями x^n, где n пробегает $\mathbf{Z}$ (предложение 2), и всегда коммутативна; в силу тождества $x^{m+n}=x^m x^n$, отображение $n \to x^n$ есть гомоморфизм аддитивной группы $\mathbf{Z}$ на X; следовательно (теорема 3), X изоморфна либо группе $\mathbf{Z}$, либо ее факторгруппе, т. е. (n° 3) аддитивной группе целых чисел по модулю a, где $a > 0$; в этом последнем случае X есть конечная группа, состоящая из a элементов.

Определение 9. *Группа называется моногенной, если она порождается одним из своих элементов; конечная моногенная группа называется также циклической группой.*

Мы доказали следующее предложение:

Предложение 8. *Моногенная группа коммутативна; если она бесконечна, то она изоморфна аддитивной группе* $\mathbf{Z}$ *рациональных целых чисел; если она — конечная группа порядка* n, *то она изоморфна аддитивной группе целых чисел по модулю* n.

Если (моногенная) подгруппа произвольной группы G, порожденная элементом $x \in G$, имеет конечный порядок p, то x называют элементом *p-го порядка*; тем самым p есть наименьшее целое число > 0, для которого $x^p = e$; если подгруппа, порожденная элементом x, бесконечна, то x называют элементом *бесконечного порядка*. Эти определения в соединении с предложением 3 влекут, в частности, что в *конечной* группе G порядок каждого элемента есть *делитель* порядка группы; в качестве следствия отсюда вытекает

Предложение 9. *В конечной группе* G *n-го порядка* $x^n = e$ *для каждого* $x \in G$.

Действительно, если p — порядок элемента x, то $n = pq$, где q — целое, и потому $x^n = (x^p)^q = e$.

8. *Центр группы; коммутант*

Предложение 10. *Центр Z группы G есть ее коммутативная подгруппа, преобразуемая каждым автоморфизмом группы G в себя; каждая подгруппа центра Z есть нормальная подгруппа группы G.*

То, что Z — подгруппа группы G, вытекает из предложения 1 § 1 и предложения 6 § 2; то, что каждый автоморфизм группы G преобразует эту подгруппу в себя, очевидно; наконец, так как $xyx^{-1}=y$ для каждого $x\in G$ и каждого $y\in Z$, то всякая подгруппа группы Z есть нормальная подгруппа группы G.

Если G коммутативна, то она совпадает со своим центром. Для некоммутативной группы G центр может сводиться к одному нейтральному элементу e (в частности, это имеет место в случае, когда G *простая*).

Следует иметь в виду, что коммутативная подгруппа группы G не обязательно содержится в центре этой группы; например, если G — некоммутативная простая группа, то моногенные группы, порожденные элементами из G, коммутативны и не сводятся к e.

Выясним теперь, какому условию должна удовлетворять нормальная подгруппа H группы G, чтобы факторгруппа G/H была *коммутативна*. Каковы бы ни были $x\in G$, $y\in G$, мы должны иметь $xy\equiv yx \pmod H$ или, что равносильно этому, $y^{-1}x^{-1}yx\equiv e\ (H)$, т. е. $y^{-1}x^{-1}yx\in H$. Элемент $y^{-1}x^{-1}yx$ называется *коммутатором* x и y (и иногда обозначается $x\circ y$); мы видим, таким образом, что H должно содержать множество коммутаторов всевозможных пар (x, y) элементов из G, а следовательно, также *порожденную* им подгруппу C группы G. Эта подгруппа C называется *коммутантом* (или *производной группой*) группы G; очевидно, она преобразуется в себя каждым автоморфизмом группы G и, в частности, является *нормальной* подгруппой группы G; более общим образом, всякий эндоморфизм φ группы G преобразует каждый коммутатор в коммутатор, так что $\varphi(C)\subset C$. Резюмируя, имеем:

Предложение 11. *Для того чтобы факторгруппа G/H группы G была коммутативной, необходимо и достаточно, чтобы нормальная подгруппа H группы G содержала коммутант C этой группы.*

Если G коммутативна, то ее коммутант сводится к e; для некоммутативной группы коммутант может совпадать с G (что, например, имеет место в случае, когда группа G *простая*).

Заметим, что *множество* всех коммутаторов группы G вообще не совпадает с (порождаемым им) *коммутантом*: произведение двух коммутаторов не есть вообще коммутатор.

9. Группы с операторами

Определение 10. *Группой с операторами называют множество G, наделенное алгебраической структурой, определяемой одним* (внутренним) *групповым законом и одним или несколькими дистрибутивными относительно него внешними законами композиции.*

Иными словами, при мультипликативной записи группового закона, для любого оператора α любого внешнего закона $\perp$ группы с операторами G имеет место тождество

$$\alpha \perp (xy) = (\alpha \perp x)(\alpha \perp y).$$

В дальнейшем нам встретятся довольно разнообразные структуры групп с операторами; каждый род их будет характеризоваться заданием соответствующих областей операторов и чаще всего — также дополнительными условиями, наложенными на рассматриваемые законы композиции.

В группе с операторами G каждый оператор порождает *эндоморфизм* ее *групповой* структуры; задание каждого из внешних законов, определяющих структуру группы с операторами, сводится к заданию семейства эндоморфизмов группы G; эти эндоморфизмы будут часто называться *гомотетиями* группы с операторами G. В дальнейшем при мультипликативном обозначении группового закона мы будем (согласно соглашениям § 5, n° 1) пользоваться для гомотетий экспоненциальным обозначением, т. е. записывать композицию оператора α и элемента $x \in G$ в виде x^α, так что дистрибутивность будет выражаться тождеством $(xy)^\alpha = x^\alpha y^\alpha$.

Группу с операторами G называют *коммутативной*, если ее групповой закон коммутативен; при аддитивной записи этого закона внешние законы обычно записываются в виде умножения слева или справа (см. § 5, n° 1).

На группе G всегда можно ввести внешний закон с областью операторов, сводящейся к единственному элементу ε, определяемый условием $x^{\varepsilon}=x$ для всех $x \in G$ (иными словами, внешний закон, единственный оператор которого является нейтральным). Этот внешний закон и групповой закон определят в G структуру группы с операторами; но она по сути ничем не отличается от заданной в G структуры группы, поскольку все введенные в § 4 понятия, относящиеся к алгебраическим структурам (устойчивые множества; отношения эквивалентности, согласующиеся со структурой; представления), для этих двух структур *одинаковы*. Тем самым это позволяет рассматривать группы как *частный случай* групп с операторами и применять все формулируемые дальше результаты, относящиеся к группам с операторами, также к группам.

В *коммутативной* группе G, записываемой, скажем, мультипликативно, для всех $n \in \mathbf{Z}$ имеет место тождество $(xy)^n=x^n y^n$ (§ 1, формула (8)); следовательно, внешний закон композиции $(n, x) \longrightarrow x^n$ целых чисел $n \in \mathbf{Z}$ и элементов $x \in G$ в соединении с групповым законом определяет в G структуру группы с операторами; и здесь по той же причине, что и выше, эта структура по сути ничем не отличается от исходной групповой.

Более общим образом, структуру коммутативной группы с операторами не отличают от получаемой путем присоединения к определяющим ее законам еще внешнего закона $(n, x) \longrightarrow x^n$.

10. *Устойчивые подгруппы групп с операторами*

Пусть G — группа с операторами; для того чтобы структура, индуцированная ее структурой в непустом множестве $H \subset G$, была структурой группы с операторами, очевидно, необходимо и достаточно, чтобы H было *подгруппой* группы G и чтобы эта подгруппа была *устойчивой* относительно заданных на G внешних законов; поэтому вводим следующее определение:

Определение 11. *Устойчивой подгруппой группы с операторами G называется подгруппа группы G, устойчивая относительно заданных на G внешних законов* (т. е. отображаемая заданными на G гомотетиями в себя), *наделенная структурой группы с операторами, индуцированной из G.*

G и $\{e\}$ всегда являются устойчивыми подгруппами группы с операторами G; коммутант группы G устойчив относительно любой структуры группы с операторами в G, имеющей тот же групповой закон; но центр группы G уже не обладает аналогичным свойством. Пересечение любого семейства устойчивых подгрупп группы с операторами G есть ее устойчивая подгруппа; наименьшая устойчивая подгруппа, содержащая множество $X \subset G$, называется устойчивой подгруппой, *порожденной* этим множеством.

Замечания. 1) При рассмотрении группы как группы с операторами (а именно с единственным оператором ε, определяемым условием $x^{\varepsilon}=x$) понятие устойчивой подгруппы сливается с понятием подгруппы. Точно так же, если G — коммутативная группа с операторами, понятие устойчивой подгруппы не изменится от присоединения к заданным внешним законам еще закона x^n.

2) Нормальную подгруппу группы G можно определить также как подгруппу, устойчивую относительно внешнего закона $(s, x) \to s^{-1}xs$, имеющего своей областью операторов G; этот закон в соединении с заданным на G групповым законом индуцирует в каждой нормальной подгруппе группы G структуру группы с операторами, имеющей областью операторов G.

11. *Факторгруппы групп с операторами*

Теорема 1 распространяется на группы с операторами. Достаточно сформулировать ее для отношения, согласующегося слева с групповым законом:

Теорема 4. *Если отношение эквивалентности R в группе с операторами G согласуется слева с групповым законом и согласуется с внешними законами, заданными на G, то оно равносильно отношению вида $x^{-1}y \in H$, где H — устойчивая подгруппа группы G. Обратно, для любой устойчивой подгруппы H отношение $x^{-1}y \in H$ есть отношение эквивалентности, согласующееся слева с групповым законом и согласующееся с заданными на G внешними законами.*

Действительно, R равносильно отношению $x^{-1}y \in H$, где H — класс $e \pmod R$ и H — подгруппа (теорема 1); так как для любого оператора α отношение $x \equiv e$ влечет $x^{\alpha} \equiv e^{\alpha}=e$, то $H^{\alpha} \subset H$, т. е. H устойчиво. Обратно, если H — устойчивая подгруппа, то отношение $y \in xH$ влечет $y^{\alpha} \in x^{\alpha}H^{\alpha} \subset x^{\alpha}H$, так что отношение эквивалентности $x^{-1}y \in H$ согласуется с заданными на G внешними законами.

Теорема 2 непосредственно распространяется теперь на группы с операторами. То же для определения 4: если H — устойчивая нормальная подгруппа группы с операторами G, то фактормножество множества G по отношению эквивалентности, определяемому этой подгруппой H, наделенное факторструктурой структуры группы с операторами G по этому отношению, есть группа с операторами; она называется *факторгруппой* группы с операторами G по H и обозначается G/H.

12. *Представления групп с операторами*

Пусть G — группа с операторами; ее *представление* в G' можно определить, если G' наделено алгебраической структурой, определяемой, с одной стороны, внутренним законом композиции и, с другой, множеством внешних законов, поставленным во взаимно однозначное соответствие с множеством внешних законов, заданных на G и имеющих каждый ту же область операторов, что и соответствующий закон на G (т. е. структурой, *гомологичной* структуре, заданной в G (§ 4, n° 1)); отображение f группы с операторами G в G' есть тогда *представление* (или *гомоморфизм*), если, каковы бы ни были элементы $x \in G$, $y \in G$ и оператор α на G, $f(x)f(y)$ и $(f(x))^{\alpha}$ определены и

$$f(xy) = f(x)\,f(y), \quad f(x^{\alpha}) = (f(x))^{\alpha}.$$

Отметим, в частности, что эндоморфизм *группы с операторами* G есть не что иное, как эндоморфизм *группы* G, *перестановочный со всеми заданными на* G *гомотетиями*.

Поскольку гомотетии группы с операторами G не обязательно перестановочны, *гомотетия, вообще говоря, не является эндоморфизмом структуры группы с операторами, заданной в* G.

Теорема 3 сохраняется без существенных изменений и принимает следующий вид.

Теорема 5. *Пусть f — представление группы с операторами G в множество G', наделенное гомологичной структурой. Тогда $f(G)$ есть группа с операторами* (относительно структуры, индуцированной из G') *с нейтральным элементом $e' = f(e)$. Прообраз $H = f^{-1}(e')$ последнего есть устойчивая нормальная подгруппа*

группы G; группа с операторами $f(G)$ изоморфна факторгруппе G/H, и представление f есть композиция канонического гомоморфизма G на G/H и инъективного гомоморфизма G/H в G'.

13. Подгруппы факторгруппы группы с операторами

Общие теоремы об изоморфизме (§ 4, теоремы 2 и 3), разумеется, применимы также к группам с операторами (и тем более к группам); они позволяют (используя также доказанную выше теорему 5) охарактеризовать устойчивые подгруппы и факторгруппы любой факторгруппы заданной группы с операторами:

Теорема 6. *Пусть G — группа с операторами, H — ее устойчивая нормальная подгруппа и f — канонический гомоморфизм G на $G' = G/H$.*

а) *Прообраз $K = f^{-1}(K')$ устойчивой подгруппы K' группы с операторами G' есть устойчивая подгруппа группы с операторами G, содержащая H; при этом $K' = f(K)$ и K' изоморфна K/H.*

б) *Отношение $K = f^{-1}(K')$ устанавливает взаимно однозначное соответствие между устойчивыми подгруппами группы с операторами G' и устойчивыми подгруппами группы с операторами G, содержащими H.*

в) *Если K' — устойчивая нормальная подгруппа группы с операторами G', то $K = f^{-1}(K')$ есть устойчивая нормальная подгруппа группы с операторами G, содержащая H, и обратно; при этом G/K изоморфно G'/K'.*

г) *Если L — устойчивая подгруппа* (соответственно *устойчивая нормальная подгруппа*) *группы с операторами G, то это же верно и для $LH = HL$; $H \cap L$ есть устойчивая нормальная подгруппа группы с операторами L, и $L/(H \cap L)$ изоморфно $(HL)/H$.*

Докажем сначала а); если K' — устойчивая подгруппа группы с операторами G', то отношения $f(x) \in K'$, $f(y) \in K'$ влекут $f(xy^{-1}) = f(x)(f(y))^{-1} \in K'$ и $f(x^\alpha) = (f(x))^\alpha \in K'$ для каждого заданного на G оператора α; значит, $K = f^{-1}(K')$ есть устойчивая подгруппа группы с операторами G, очевидно содержащая H; отображая G *на* G', f отображает K на K', и в этих условиях группа с операторами K' изоморфна K/H по теореме 5.

Обратно, если K — устойчивая подгруппа группы с операторами G, содержащая H, то K *насыщена* по отношению $y \in xH$, значит, полагая $K' = f(K)$, имеем $K = \overset{-1}{f}(K')$, чем доказано б).

Докажем теперь г). Если L — устойчивая подгруппа группы с операторами G, то сужение f на L есть представление L в G'; согласно теореме 5, прообраз $H \cap L$ нейтрального элемента относительно этого представления есть устойчивая нормальная подгруппа группы с операторами L, и $f(L)$ изоморфно $L/(H \cap L)$; *насыщение* L по отношению $y \in xH$ дает множество $HL = LH = \overset{-1}{f}(f(L))$, являющееся поэтому устойчивой подгруппой группы с операторами G; а вторая теорема об изоморфизме (§ 4, теорема 3) показывает, что $f(L)$ изоморфно $(HL)/H$. Легко проверяется, что если подгруппа L нормальная, то это же верно и для HL.

Наконец, в) есть не что иное, как перевод первой теоремы об изоморфизме (§ 4, теорема 2) на язык групп с операторами.

Для всякой устойчивой подгруппы $K \supset H$ группы с операторами G обычно $f(K)$ *отождествляют* с факторгруппой K/H; утверждение в) теоремы 6 выражают тогда, говоря, что факторгруппа $(G/H)/(K/H)$ изоморфна G/K (для каждой устойчивой нормальной подгруппы $K \supset H$).

Замечание. То, что прообраз $\overset{-1}{f}(K')$ подгруппы K' группы G' есть подгруппа группы G, вытекает из следующего более общего предложения:

Для любых множеств $A' \subset G'$ и $B' \subset G'$ имеем

$$\overset{-1}{f}(A'B') = \overset{-1}{f}(A')\overset{-1}{f}(B'), \quad \overset{-1}{f}(A'^{-1}) = (\overset{-1}{f}(A'))^{-1}.$$

Действительно, очевидно $\overset{-1}{f}(A')\overset{-1}{f}(B') \subset \overset{-1}{f}(A'B')$; с другой стороны, если $z \in \overset{-1}{f}(A'B')$, существуют $x \in \overset{-1}{f}(A')$ и $y \in \overset{-1}{f}(B')$ такие, что $f(z) = f(x)f(y) = f(xy)$, и значит, $z \in xyH \subset \overset{-1}{f}(A')\overset{-1}{f}(B')$. Точно так же, отношение $z \in \overset{-1}{f}(A'^{-1})$ равносильно отношению $f(z) \in A'^{-1}$, а значит отношению $f(z^{-1}) \in A'$ или $z^{-1} \in \overset{-1}{f}(A')$, и, наконец, — отношению $z \in (\overset{-1}{f}(A'))^{-1}$.

Следствие. *Пусть f — представление группы с операторами G в группу с операторами G', L — устойчивая подгруппа группы G, K — устойчивая нормальная подгруппа группы L и $H = \overset{-1}{f}(e')$.*

Тогда KH, $K(L \cap H)$ *и* $f(K)$ — *устойчивые нормальные подгруппы соответственно групп с операторами* LH, L *и* $f(L)$, *и факторгруппы* $(LH)/(KH)$, $L/(K(L \cap H))$ *и* $f(L)/f(K)$ *изоморфны друг другу.*

Действительно, пусть g — сужение f на L; g есть гомоморфизм L на $f(L)$ и $g(K) = f(K)$, $\overset{-1}{g}(e') = L \cap H$; поэтому (теорема 6) $\overset{-1}{g}(f(K)) = K(L \cap H)$ есть устойчивая нормальная подгруппа группы с операторами L, и $f(L)/f(K)$ изоморфно $L/(K(L \cap H))$. С другой стороны, $\overset{-1}{f}(f(L)) = LH$, $\overset{-1}{f}(f(K)) = KH$; то же рассуждение применительно к сужению f на LH показывает, что KH нормальна в LH, а $(LH)/(KH)$ изоморфна $f(L)/f(K)$.

14. Теорема Жордана — Гёльдера

Одним из важных следствий теоремы 6 является теорема, известная под названием теоремы Жордана — Гёльдера; она устанавливает свойство структуры некоторых групп (особенно *конечных*), *инвариантное относительно изоморфизма*, и на этом основании играет фундаментальную роль в алгебре (см. особенно главы II и VII).

Определение 12. *Композиционным рядом группы с операторами* G *будет называться конечный ряд* $(G_i)_{0 \leqslant i \leqslant n}$ *ее устойчивых подгрупп, имеющий своим первым членом* $G_0 = G$, *последним членом* $G_n = \{e\}$ *и такой, что* G_{i+1}, *где* $0 \leqslant i \leqslant n-1$, — *нормальная подгруппа группы* G_i. *Факторгруппы* G_i/G_{i+1} *называются факторами композиционного ряда. Композиционный ряд* Σ' *называется уплотнением композиционного ряда* Σ, *если* Σ *есть подряд ряда* Σ'.

Композиционные ряды $(G_i)_{0 \leqslant i \leqslant n}$ *и* $(H_j)_{0 \leqslant j \leqslant m}$ *групп с операторами* G *и* H (имеющих гомологичные структуры) *называются эквивалентными, если* $m = n$ *и существует взаимно однозначное отображение* φ *интервала* $[0, n-1] \subset \mathbf{N}$ *на себя такое, что* G_i/G_{i+1} *для каждого* i *изоморфно* $H_{\varphi(i)}/H_{\varphi(i)+1}$.

Заметим, что подряд композиционного ряда (G_i), вообще говоря, не есть композиционный ряд, ибо G_j при $j > i+1$ вообще не есть нормальная подгруппа группы G_i.

Теорема 7 (Шрейер). *Любые два композиционных ряда* Σ_1, Σ_2 *группы с операторами* G *обладают эквивалентными уплотнениями* Σ_1', Σ_2'.

Пусть $\Sigma_1=(G_i)_{0\leqslant i\leqslant n}$ и $\Sigma_2=(H_j)_{0\leqslant j\leqslant m}$ — два заданных композиционных ряда, состоящие соответственно из $n+1$ и $m+1$ членов; мы покажем, что композиционный ряд Σ_1' можно образовать путем *вставки* между каждыми двумя подгруппами G_i и G_{i+1}, где $0\leqslant i\leqslant n-1$, по $m-1$ подгруппе G'_{ij} $(1\leqslant j\leqslant m-1)$ и композиционный ряд Σ_2' — путем *вставки* между каждыми двумя подгруппами H_j и H_{j+1}, где $0\leqslant j\leqslant m-1$, по $n-1$ подгруппе H'_{ji} $(1\leqslant i\leqslant n-1)$; это даст два ряда из $mn+1$ подгрупп группы G; надлежащим образом выбирая вставляемые подгруппы, мы получим эквивалентные композиционные ряды.

Заметим, что $G_i\cap H_j$ есть подгруппа и группы G_i, и группы H_j, поэтому (теорема 6) $G_{i+1}(G_i\cap H_j)$ есть подгруппа группы G_i, содержащая G_{i+1}, и $H_{j+1}(G_i\cap H_j)$ — подгруппа группы H_j, содержащая H_{j+1}; если положить

$$G'_{ij}=G_{i+1}(G_i\cap H_j)\quad(1\leqslant j\leqslant m-1)$$

и

$$H'_{ji}=H_{j+1}(G_i\cap H_j)\quad(1\leqslant i\leqslant n-1),$$

то $G'_{i,j+1}$ будет подгруппой группы G'_{ij}, $H'_{j,i+1}$ — подгруппой группы H'_{ji}; при этом, в тех же обозначениях, $G'_{i,0}=G_i$, $G'_{im}=G_{i+1}$, $H'_{j,0}=H_j$, $H'_{jn}=H_{j+1}$; поэтому доказываемая теорема будет непосредственно вытекать из следующей леммы:

Лемма (Цасенхауз). *Пусть H, K — устойчивые подгруппы группы с операторами G и H', K' — их устойчивые нормальные подгруппы. Тогда $H'(H\cap K')$ есть нормальная подгруппа группы $H'(H\cap K)$, $K'(K\cap H')$ — нормальная подгруппа группы $K'(K\cap H)$, причем факторгруппы*

$$(H'(H\cap K))/(H'(H\cap K'))$$

и

$$(K'(K\cap H))/(K'(K\cap H'))$$

изоморфны.

Согласно теореме 6, примененной к группе H, $H'\cap K=H'\cap(H\cap K)$ есть нормальная подгруппа группы $H\cap K$; точно так же $K'\cap H$ есть нормальная подгруппа группы $K\cap H$; поэтому (теорема 6) $(H'\cap K)(K'\cap H)$ есть нормальная подгруппа группы $H\cap K$. Согласно следствию теоремы 6, примененному к группе H,

$$H'(H'\cap K)(K'\cap H)=H'(H\cap K')$$

есть нормальная подгруппа группы $H'(H \cap K)$, а факторгруппа $(H'(H \cap K))/(H'(H \cap K'))$ изоморфна $(H \cap K)/((H' \cap K)(K' \cap H))$. В эту последнюю факторгруппу H и H', с одной стороны, K и K', с другой, входят симметрично; их перестановка приводит к сформулированному результату, и лемма доказана.

Определение 13. *Рядом Жордана — Гёльдера группы с операторами G будет называться ее строго убывающий композиционный ряд Σ, не обладающий никаким отличным от него строго убывающим уплотнением.*

Определение 14. *Группа с операторами G называется простой, если она не сводится к одному своему нейтральному элементу e и не обладает никакой устойчивой нормальной подгруппой, отличной от G и $\{e\}$.*

Предложение 12. *Для того чтобы строго убывающий композиционный ряд группы с операторами G был ее рядом Жордана — Гёльдера, необходимо и достаточно, чтобы все факторы этого ряда были простыми.*

Действительно, если строго убывающий композиционный ряд Σ не есть ряд Жордана — Гёльдера, то он обладает отличным от него строго убывающим уплотнением Σ'. Значит, существуют два соседних члена G_i, G_{i+1} ряда Σ, не являющиеся соседними в Σ'; пусть H — первый член, следующий за G_i в Σ'; H есть устойчивая нормальная подгруппа группы с операторами G_i, содержащая G_{i+1} и отличная от этой последней; поэтому H/G_{i+1} есть устойчивая нормальная подгруппа группы с операторами G_i/G_{i+1}, отличная от этой последней и от нейтрального элемента; тем самым G_i/G_{i+1} — не простая. Обратно, если Σ — строго убывающий композиционный ряд, имеющий не простой фактор G_i/G_{i+1}, то этот фактор обладает устойчивой нормальной подгруппой, отличной от него самого и нейтрального элемента, и ее прообраз H в G_i будет устойчивой нормальной подгруппой в G_i, отличной от G_i и G_{i+1} (теорема 6); тогда достаточно вставить H между G_i и G_{i+1}, чтобы получить строго убывающий композиционный ряд, отличный от ряда Σ и являющийся его уплотнением.

Теорема 8 (Жордан — Гёльдер). *Любые два ряда Жордана — Гёльдера группы с операторами эквивалентны.*

Пусть Σ_1 и Σ_2 — два ряда Жордана — Гёльдера группы с операторами G; применение теоремы 7 дает два *эквивалентных* композиционных ряда Σ_1' и Σ_2', являющихся соответственно уплотнениями рядов Σ_1 и Σ_2; но так как эти последние — ряды Жордана—Гёльдера, то Σ_1' либо совпадает с Σ_1, либо получается из Σ_1 повторением некоторых членов; поэтому ряд факторов для Σ_1' получается из ряда факторов для Σ_1 путем добавления некоторого числа членов, изоморфных группе $\{e\}$; поскольку композиционный ряд Σ_1 строго убывающий, его ряд факторов получается тогда из ряда факторов для Σ_1' путем удаления *всех* членов последнего, изоморфных $\{e\}$. И то же для Σ_2 и Σ_2'. Так как ряды факторов композиционных рядов Σ_1' и Σ_2' различаются (с точностью до изоморфизма) лишь порядком следования членов, то тогда то же верно для рядов факторов композиционных рядов Σ_1 и Σ_2, и теорема доказана.

Следствие. *Пусть G — группа с операторами, обладающая рядом Жордана — Гёльдера. Тогда любой ее строго убывающий композиционный ряд Σ допускает уплотнение, являющееся рядом Жордана — Гёльдера.*

Действительно, пусть Σ_0 — ряд Жордана—Гёльдера группы G; согласно теореме 7, Σ и Σ_0 обладают эквивалентными друг другу уплотнениями Σ' и Σ_0'; рассуждение, проведенное при доказательстве теоремы 8, показывает, что выбрасывание из Σ' повторяющихся членов дает ряд Σ'', эквивалентный Σ_0, и тем самым — ряд Жордана — Гёльдера, поскольку все его факторы простые (предложение 12); при этом, поскольку ряд Σ строго убывающий, Σ'' есть его уплотнение, и следствие доказано.

Замечание. Не всякая группа с операторами G обладает рядом Жордана — Гёльдера. Примером может служить аддитивная группа $\mathbf{Z}$ рациональных целых чисел: $(2^n\mathbf{Z})_{n\geqslant 0}$ есть бесконечный строго убывающий ряд (нормальных) подгрупп группы $\mathbf{Z}$; каково бы ни было p, p первых членов этого ряда вместе с группой $\{0\}$ образуют строго убывающий композиционный ряд; если бы $\mathbf{Z}$ обладала рядом Жордана—Гёльдера, он содержал бы, по следствию теоремы 8, не менее $p+1$ членов, что в силу произвольности p невозможно.

Напротив, каждая *конечная* группа с операторами G обладает рядом Жордана — Гёльдера: достаточно применить индукцию по порядку группы G и заметить, что среди устойчивых нормальных подгрупп этой группы, отличных от нее, имеется *максимальная* H_1, факторгруппа G/H_1 по которой тем самым простая.

Схолия. Если группа с операторами G обладает рядом Жордана — Гёльдера, то число его факторов называют *длиною* G; таким образом, простая группа есть группа длины 1. Если G и G' — две изоморфные группы с операторами и G обладает рядом Жордана — Гёльдера, то это же верно для G' и ряды Жордана — Гёльдера для G и G' *эквивалентны*; в частности, длины G и G' равны. Следует заметить, что длина ряда факторов ряда Жордана — Гёльдера группы G вообще *не характеризует* эту группу с точностью до изоморфизма (см. упражнение 1).

Замечание. Всё сказанное о произведениях групп и прямых произведениях подгрупп (n°n° 5 и 6) непосредственно распространяется на группы с операторами, если заменить всюду «группу» на «группу с операторами», а «подгруппу» — на «устойчивую подгруппу».

Упражнения. 1) Определить все групповые структуры в множествах из n элементов, где $2 \leqslant n \leqslant 6$ (см. § 2, упражнение 5). Определить подгруппы и факторгруппы этих групп, а также их ряды Жордана — Гёльдера; показать, в частности, что существуют две неизоморфные группы четвертого порядка, факторы рядов Жордана — Гёльдера которых изоморфны.

*2) а) Ассоциативный закон $(x, y) \to xy$ на множестве E является групповым законом, если существует $e \in E$ такое, что $ex = x$ для всех $x \in E$, и для всякого $x \in E$ существует $x' \in E$ такое, что $x'x = e$. [Рассмотрев композицию $x'xx'$, показать, что $xx' = e$; вывести отсюда, что e — нейтральный элемент.]

б) Показать справедливость того же результата, если *все* левые переносы γ_x и хотя бы *один* правый перенос δ_a являются отображениями E на E. [Воспользоваться предложением 4 § 2 для сведения к а) или к упражнениям 11 и 13 § 2.]

3) Каждое непустое *конечное* устойчивое подмножество группы G является ее подгруппой. [См. § 2, упражнение 8.]

4) Пусть A и B — подгруппы группы G.

а) Показать, что наименьшая подгруппа, содержащая A и B (т. е. подгруппа, порожденная множеством $A \cup B$), совпадает с множеством композиций всевозможных последовательностей $(x_i)_{1 \leqslant i \leqslant 2n+1}$, состоящих из (какого угодно) нечетного числа элементов и таких, что $x_i \in A$ для нечетного i и $x_i \in B$ для четного i.

б) Для того чтобы AB было подгруппой группы G (в таком случае это будет подгруппа, порожденная множеством $A \cup B$), необходимо и достаточно, чтобы A и B были перестановочны, т. е. $AB=BA$.

в) Если A и B перестановочны, то, какова бы ни была подгруппа C группы G, содержащая A, A перестановочна с $B \cap C$ и $A(B \cap C)=C \cap (AB)$.

5) Всякая подгруппа группы G, имеющая индекс 2, нормальна.

6) Пусть (G_α)—семейство нормальных подгрупп группы G такое, что $\bigcap_\alpha G_\alpha=\{e\}$. Показать, что G изоморфна некоторой подгруппе произведения $\prod_\alpha (G/G_\alpha)$ факторгрупп G/G_α.

7) Если группа G есть прямое произведение своих подгрупп A и B, то каждая ее подгруппа H, содержащая A, есть прямое произведение A и $H \cap B$.

8) Пусть H — нормальная подгруппа группы G. Для того чтобы G была прямым произведением этой подгруппы H и некоторой подгруппы K, необходимо и достаточно, чтобы существовало представление f группы G на H, при котором $f(x)=x$ для каждого $x \in H$.

9) Пусть G — коммутативная группа и H — ее подгруппа, для которой G/H есть бесконечная моногенная группа. Показать, что G изоморфна произведению $H \times (G/H)$. [Рассмотреть подгруппу, порожденную элементом класса по H, порождающего G/H.]

10) Пусть H — нормальная подгруппа группы G, содержащаяся в центре последней. Показать, что если факторгруппа G/H моногенна, то группа G коммутативна.

11) Если все элементы группы G, отличные от нейтрального, имеют порядок 2, то G коммутативна; если G конечна, то ее порядок n является тогда степенью двойки. [Индукцией по n.]

12) Пусть G — группа такая, что для некоторого целого $n > 1$ и всех $x \in G$, $y \in G$ имеет место равенство $(xy)^n=x^n y^n$. Пусть $G^{(n)}$ означает множество всех x^n, где x пробегает G, а $G_{(n)}$ — множество тех $x \in G$, для которых $x^n=e$. Показать, что $G^{(n)}$ и $G_{(n)}$— нормальные подгруппы группы G; если G конечна, то порядок $G^{(n)}$ равен индексу $G_{(n)}$.

13) Пусть A — непустое множество элементов группы G; его *нормализатором* называют множество N тех $x \in G$, для которых $xAx^{-1}=A$, а *централизатором* — множество K тех $x \in G$, для которых $xax^{-1}=a$, каково бы ни было $a \in A$. Показать, что N — подгруппа группы G, а K — нормальная подгруппа группы N. Нормализатор N подгруппы A группы G есть наибольшая из подгрупп H этой группы, имеющих A своей нормальной подгруппой.

14) Обозначая через $D(G)$ коммутант, или производную группу, группы G, можно определить по индукции k-ю производную группу $D^k(G)$ последней как коммутант $D(D^{k-1}(G))$ группы $D^{k-1}(G)$. Показать, что $D^k(G)$ есть подгруппа группы G, обладающая тем свойством, что для всякого эндоморфизма φ последней $\varphi(D^k(G)) \subset D^k(G)$.

Для всякой подгруппы H группы G имеем $D^k(H) \subset D^k(G)$; если H нормальна, то $D^k(G/H)$ изоморфна $(HD^k(G))/H$.

Группу G называют *разрешимой* (или *метабелевой*), если она обладает композиционным рядом (G_i), все факторы которого G_i/G_{i+1} коммутативны. Показать, что для того, чтобы G была разрешимой, необходимо и достаточно, чтобы существовало целое k такое, что $D^k(G)=\{e\}$. Вывести отсюда, что каждая подгруппа и каждая факторгруппа разрешимой группы разрешимы.

*15) Пусть $\mathfrak{F}$ — некоторое множество устойчивых подгрупп группы с операторами G; говорят, что $\mathfrak{F}$ удовлетворяет условию максимальности (соответственно условию минимальности), если каждое его подмножество, упорядоченное по включению, обладает максимальным (соответственно минимальным) элементом.

Предположим, что множество всех устойчивых подгрупп группы с операторами G удовлетворяет условию минимальности.

а) Доказать, что никакая устойчивая подгруппа группы G, отличная от G, не изоморфна G. [Рассуждая от противного, показать, что из существования такой подгруппы следовало бы, что G обладает бесконечным строго убывающим рядом устойчивых подгрупп.]

б) Назовем минимальные элементы множества всех устойчивых нормальных подгрупп группы G, не сводящихся к e, ее *минимальными* нормальными подгруппами. Пусть $\mathfrak{M}$ — некоторое множество минимальных нормальных подгрупп группы G и S — наименьшая ее устойчивая подгруппа, содержащая все подгруппы, принадлежащие $\mathfrak{M}$; показать, что S есть прямое произведение *конечного* числа минимальных нормальных подгрупп группы G. [Пусть (M_n) — последовательность минимальных нормальных подгрупп группы G, принадлежащих $\mathfrak{M}$, такая, что M_{n+1} не содержится в устойчивой подгруппе, порожденной объединением подгрупп $M_1, M_2, \ldots, M_n$; пусть S_k — устойчивая подгруппа, порожденная объединением всех M_n с индексами $n \geqslant k$; показать, что с некоторого места $S_{k+1}=S_k$ и, следовательно, последовательность (M_n) конечна; затем применить предложение 7.]

в) Если G — группа без операторов, то каждая ее минимальная нормальная подгруппа M является прямым произведением конечного числа изоморфных друг другу простых подгрупп. [Пусть N — минимальная нормальная подгруппа *группы* M; показать, что M — наименьшая подгруппа группы G, содержащая все aNa^{-1}, где a пробегает G, и применить б) к группе M.]

16) Если множество всех устойчивых подгрупп группы с операторами G удовлетворяет условию максимальности или минимальности (упражнение 15), то G обладает рядом Жордана — Гёльдера. [Рассмотреть для подгруппы H группы G максимальный элемент множества всех устойчивых нормальных подгрупп группы H, отличных от H.]

*17) Пусть G — группа с операторами; ее композиционный ряд (G_i) назовем *нормальным*, если все G_i — устойчивые нормальные под-

группы *группы* G; *главным* рядом называется строго убывающий нормальный ряд, не обладающий никаким отличным от него строго убывающим нормальным уплотнением.

а) Показать, что любые два нормальных ряда (G_i) и (H_j) группы G обладают эквивалентными нормальными уплотнениями. [Применить теорему Шрейера, рассматривая надлежащую область операторов на G.] Дать второе доказательство этого предложения, «вставляя» в ряды (G_i) и (H_j) соответственно подгруппы $G'_{ij}=G_i\cap(G_{i+1}H_j)$ и $H'_{ji}=H_j\cap(H_{j+1}G_i)$.

б) Если G обладает главным рядом, то любые два ее главных ряда эквивалентны; для каждого строго убывающего нормального ряда Σ существует главный ряд, являющийся его уплотнением. Вывести отсюда, что для того, чтобы G обладала главным рядом, необходимо и достаточно, чтобы множество всех ее устойчивых нормальных подгрупп удовлетворяло условиям максимальности и минимальности.

в) Если G — группа без операторов, обладающая главным рядом (G_i), и множество всех ее подгрупп удовлетворяет условию минимальности, то каждая факторгруппа G_i/G_{i+1} есть прямое произведение конечного числа своих простых подгрупп. [См. упражнение 15.]

*18) Пусть (H_ι) — произвольное семейство устойчивых подгрупп группы с операторами G; G по-прежнему называют *прямым произведением* этого семейства, если: 1° при $\iota\neq\varkappa$ каждый элемент из H_ι перестановочен с каждым элементом из $H_\varkappa$; 2° каково бы ни было $x\in G$, для всякого ι существует однозначно определенный элемент $x_\iota\in H_\iota$ такой, что $x_\iota=e$ для всех индексов ι, кроме конечного их числа $\iota_1,\iota_2,\ldots,\iota_n$, и $x=x_{\iota_1}x_{\iota_2}\ldots x_{\iota_n}$. G называется *вполне приводимой*, если она является прямым произведением семейства своих *простых* подгрупп.

а) Показать, что если G есть прямое произведение семейства своих подгрупп (H_ι), то она изоморфна подгруппе их произведения $H=\prod_\iota H_\iota$, притом отличной от H, если семейство (H_ι) бесконечно; вывести отсюда, что H_ι — нормальные подгруппы группы G.

б) Пусть G — группа с операторами, порождаемая объединением семейства $(H_\iota)_{\iota\in I}$ своих *простых* устойчивых нормальных подгрупп, а K — устойчивая нормальная подгруппа. Показать, что G есть прямое произведение K и некоторого подсемейства $(H_\iota)_{\iota\in J}$. [Рассмотреть множества $L\subset I$, обладающие тем свойством, что устойчивая подгруппа, порожденная объединением K и подсемейства $(H_\iota)_{\iota\in L}$, является прямым произведением K и этого подсемейства; взять в множестве этих множеств L максимальный элемент.]

в) Если вполне приводимая группа является прямым произведением двух конечных семейств $(H_i)_{i\in I}$ и $(H')_{j\in J}$ своих простых

подгрупп, то существует взаимно однозначное отображение φ множества I на J такое, что $H'_{\varphi(i)}$ изоморфна H_i для каждого $i \in I$.

19) Пусть L — свободный моноид (§ 1, n° 3), порожденный нейтральным элементом e и двумя семействами (x_ι), (y_ι) с одинаковым множеством индексов. Показать, что его фактормножество, полученное путем отождествления всех композиций $x_\iota y_\iota$ и $y_\iota x_\iota$ с e [§ 4, упражнение 2в], есть группа, порожденная семейством (x_ι); она называется *свободной группой*, порожденной этим семейством. Показать, что всякая группа G, порожденная семейством (a_ι) своих элементов, изоморфна факторгруппе свободной группы G', порожденной этим семейством; эта факторгруппа всегда может рассматриваться как полученная путем *отождествления* каждого элемента некоторого семейства (x_λ) элементов из G' с соответствующим элементом второго такого семейства (y_λ) (имеющего то же множество индексов) [см. § 4, упражнение 2в]; говорят, что G есть группа, порожденная *образующими* a_ι, подчиненными *определяющим соотношениям* $x_\lambda = y_\lambda$.

*20) а) Пусть G — конечная группа порядка mn, обладающая циклической нормальной подгруппой H порядка m, факторгруппа G/H по которой — циклическая (порядка n). Показать, что G порождается двумя элементами a, b, удовлетворяющими условиям $a^m = e$, $b^n = a^r$, $bab^{-1} = a^s$, где r и s — целые такие, что $r(s-1)$ и $s^n - 1$ кратны m. [Взять за a элемент, порождающий H, и за b — элемент класса, порождающего G/H; выразить элементы $b^h a^k b^{-h}$ через степени a и применить это, в частности, к случаям $h=n$, $k=1$ и $h=1$, $k=r$.]

б) Обратно, пусть $G(m, n, r, s)$ — группа, порожденная двумя образующими a, b, подчиненными определяющим соотношениям $a^m = e$, $b^n = a^r$, $bab^{-1} = a^s$, где m и n — целые числа $\geqslant 0$, а r и s — любые целые числа. Показать, что если m, $r(s-1)$ и $s^n - 1$ не все равны нулю, то $G(m, n, r, s)$ — конечная группа порядка qn, где q — наибольший общий делитель чисел m, $|r(s-1)|$ и $|s^n - 1|$; ее подгруппа H, порожденнаая элементом a, есть нормальная подгруппа порядка q, а G/H — циклическая группа порядка n. [Доказать, что каждый элемент группы $G(m, n, r, s)$ может быть записан в виде $a^x b^y$, где x и y — целые, удовлетворяющие неравенствам $0 \leqslant x \leqslant q-1$, $0 \leqslant y \leqslant n-1$, и что $G(m, n, r, s)$ изоморфна группе, образованной парами (x, y) таких целых чисел, с законом композиции

$$(x, y)\cdot(x', y') = \begin{cases} (x + x's^y,\ y + y'), & \text{если } y + y' \leqslant n-1, \\ (x + x's^y + r,\ y + y' - n), & \text{если } y + y' \geqslant n, \end{cases}$$

где первые координаты в правой части — суммы по модулю q.] Исследовать случай $m = r(s-1) = s^n - 1 = 0$.

$G(n, 2, 0, -1)$ называется *диэдральной группой* порядка $2n$ и обозначается $\mathfrak{D}_{2n}$; $G(4, 2, 2, -1)$ есть группа восьмого порядка,

называемая *кватернионной группой* и обозначаемая $\mathfrak{Q}$. Показать, что в $\mathfrak{Q}$ каждая подгруппа нормальна и что пересечение ее подгрупп, отличных от $\{e\}$, есть подгруппа, отличная от $\{e\}$. Доказать, что $\mathfrak{D}_8$ не изоморфна $\mathfrak{Q}$.

*21) Пусть E — мультипликативно записываемая неассоциативная квазигруппа (§ 5, упражнение 5), обладающая идемпотентом e и такая, что $(xy)(zt)=(xz)(yt)$, каковы бы ни были x, y, z, t. Обозначим через $u(x)$ элемент из E, для которого $u(x)e=x$, и через $v(x)$ — элемент, для которого $ev(x)=x$. Показать, что закон композиции $(x, y)\to u(x)v(y)$ есть коммутативный групповой закон на E, для которого e служит нейтральным элементом, что отображения $x\to xe$ и $y\to ey$ — перестановочные эндоморфизмы этой групповой структуры и что $xy=u(xe)\,v(ey)$. [Вначале установить тождества $e(xy)=(ex)(ey)$, $(xy)e=(xe)(ye)$, $e(xe)=(ex)e$; далее принять во внимание, что отношения $x=y$, $ex=ey$ и $xe=ye$ эквивалентны.] Обращение.

*22) Рассмотрим на множестве E мультипликативно записываемый *не всюду определенный* внутренний закон, удовлетворяющий следующим условиям: 1° если одна из композиций $(xy)z$, $x(yz)$ определена, то определена и другая и они равны (см. § 1, упражнение 3); 2° если x, x', y таковы, что xy и $x'y$ (или yx и yx') определены и равны, то $x=x'$; 3° для каждого $x\in E$ существуют такие три элемента e_x, e'_x и x^{-1}, что $e_x x=x$, $xe'_x=x$ и $x^{-1}x=e'_x$; будем называть e_x левой единицей для x, e'_x — правой единицей для x, и x^{-1} (допуская вольность речи) — элементом, обратным к x.

а) Показать, что композиции xx^{-1}, $x^{-1}e_x$, $e'_x x^{-1}$, $e_x e_x$, $e'_x e'_x$ определены и $xx^{-1}=e_x$, $x^{-1}e_x=e'_x x^{-1}=x^{-1}$, $e_x e_x=e_x$, $e'_x e'_x=e'_x$.

б) Каждый идемпотент e в E (§ 1, n° 4) является левой единицей для всех тех x, для которых ex определено, и правой единицей для всех тех y, для которых ye определено.

в) Для того чтобы была определена композиция xy, необходимо и достаточно, чтобы левая единица для y совпадала с правой единицей для x. [При доказательстве достаточности условия воспользоваться соотношением $e_y=yy^{-1}$.] Если $xy=z$, то $x^{-1}z=y$, $zy^{-1}=x$, $y^{-1}x^{-1}=z^{-1}$, $z^{-1}x=y^{-1}$, $yz^{-1}=x^{-1}$ (композиции, стоящие в левых частях, определены).

г) Для любых двух идемпотентов e, e' из E обозначим через $G_{e,e'}$ множество тех $x\in E$, для которых e служит левой, а e' — правой единицей. Показать, что $G_{e,e}$ есть группа относительно индуцированного из E закона.

E называется *группоидом*, если оно удовлетворяет еще следующему условию:

4° каковы бы ни были идемпотенты e, e', множество $G_{e,e'}$ не пусто.

д) Пусть E — группоид и $a\in G_{e,e'}$. Показать, что $x\to xa$ — взаимно однозначное отображение $G_{e,e}$ на $G_{e,e'}$, $y\to ay$ — взаимно

однозначное отображение $G_{e',e'}$ **на** $G_{e,e'}$ **и** $x \to a^{-1}xa$ **— изоморфизм** группы $G_{e,e}$ на группу $G_{e',e'}$.

е) Показать, что закон, определенный в упражнении 4б § 1, в случае, когда все множества семейства $\mathfrak{F}$ равномощны, определяет в множестве Ψ структуру группоида.

23) а) Введем на произведении $E \times E$, где E — произвольное множество, мультипликативно записываемый не всюду определенный закон, для которого композиция (x, y) и (y', z) определена лишь если $y' = y$, и имеет в этом случае значение (x, z). Показать, что $E \times E$, наделенное этим законом композиции, есть группоид (упражнение 22).

б) Пусть $(x, y) \equiv (x', y')$ (R) — отношение эквивалентности, согласующееся с законом композиции, указанным в а) (т. е. такое, что из $(x, y) \equiv (x', y')$ и $(y, z) \equiv (y', z')$ следует $(x, z) \equiv (x', z')$); пусть R удовлетворяет, кроме того, следующему условию: каковы бы ни были x, y, z, существует, и притом только одно, $t \in E$ такое, что $(x, y) \equiv (z, t)$, и существует $u \in E$ такое, что $(x, y) \equiv (u, z)$. Показать, что в этих условиях факторструктура структуры группоида в $E \times E$ по R есть структура группы. [Доказать сначала, что факторзакон всюду определен; затем, что если классы $\dot{x}$, $\dot{y}$, $\dot{z}$ удовлетворяют равенству $\dot{x}\dot{y} = \dot{x}\dot{z}$, то $\dot{y} = \dot{z}$; наконец, что $(x, x) \equiv (y, y)$, каковы бы ни были $x \in E$, $y \in E$.]

в) Пусть G — группа, полученная в результате наделения фактормножества $E \times E$ по R указанной структурой. Пусть, далее, a — произвольный элемент из E и $f_a(x)$ для каждого $x \in E$ означает класс $(a, x) \bmod R$. Показать, что f_a — взаимно однозначное отображение E на G и что отношение $(x, y) \equiv (x', y')$ эквивалентно отношению $f_a(x)\,(f_a(x'))^{-1} = f_a(y)\,(f_a(y'))^{-1}$.

Для коммутативности группы G необходимо и достаточно, чтобы $(x, y) \equiv (x', y')$ влекло $(x, x') \equiv (y, y')$.

*24) Пусть E — множество и f — отображение E^m в E, записываемое в виде $f(x_1, \ldots, x_m) = x_1 \ldots x_m$ и удовлетворяющее следующим условиям:

1° имеет место тождество

$$(x_1 \ldots x_m)\, x_{m+1} \ldots x_{2m-1} = x_1 (x_2 \ldots x_{m+1})\, x_{m+2} \ldots x_{2m-1};$$

2° каковы бы ни были $a_1, a_2, \ldots, a_{m-1}$,

$$x \to x a_1 a_2 \ldots a_{m-1},$$
$$x \to a_1 \ldots a_i x a_{i+1} \ldots a_{m-1} \quad (1 \leqslant i \leqslant m-2),$$
$$x \to a_1 a_2 \ldots a_{m-1} x$$

— взаимно однозначные отображения E на E.

а) Показать, что для всех индексов i таких, что $1 \leqslant i \leqslant m-1$, имеет место тождество

$$(x_1 \ldots x_m)\, x_{m+1} \ldots x_{2m-1} = x_1 \ldots x_i\, (x_{i+1} \ldots x_{i+m})\, x_{i+m+1} \ldots x_{2m-1}.$$

[Провести индукцию по i, введя в рассмотрение элемент

$$((x_1 \dots x_m)\, x_{m+1} \dots x_{2m-1})\, a_1 a_2 \dots a_{m-1}.]$$

б) Каковы бы ни были $a_1, a_2, \dots, a_{m-2}$, существует $u \in E$ такое, что

$$x = x a_1 a_2 \dots a_{m-2} u = u a_1 a_2 \dots a_{m-2} x$$

тождественно относительно x. [Рассуждать, как в предложении 4 § 2.]

в) Рассмотреть в множестве E^k всех последовательностей $(u_1, u_2, \dots, u_k)$ по k элементов из E $(1 \leqslant k \leqslant m-1)$ следующее отношение эквивалентности R_k: каковы бы ни были $x_1, \dots, x_{m-k}$,

$$u_1 u_2 \dots u_k x_1 x_2 \dots x_{m-k} = v_1 v_2 \dots v_k x_1 x_2 \dots x_{m-k};$$

обозначим фактормножество E^k/R_k через E_k и «сумму» множеств $E_1 = E$, $E_2, \dots, E_{m-1}$ (Теор. мн., Рез., § 4, n° 5) — через G. Пусть $\alpha \in E_i$, $\beta \in E_j$; для любой последовательности $(u_1, u_2, \dots, u_i)$ класса α и любой последовательности $(v_1, v_2, \dots, v_j)$ класса β рассмотрим последовательность

$$(u_1, u_2, \dots, u_i, v_1, v_2, \dots, v_j)$$

из E^{i+j}, если $i+j < m$, и последовательность

$$(u_1, u_2, \dots, u_{i+j-m}, (u_{i+j-m+1} \dots u_i v_1 v_2 \dots v_j))$$

из $E^{i+j-m+1}$, если $i+j \geqslant m$. Показать, что класс этой последовательности в E_{i+j} (соответственно $E_{i+j-m+1}$) зависит только от классов α и β; обозначим его $\alpha \cdot \beta$. Показать, что этим определен на G групповой закон, что $H = E_{m-1}$ — нормальная подгруппа группы G и что G/H есть циклическая группа порядка $m-1$; доказать, наконец, что E совпадает с классом по H, порождающим G/H, и что $x_1 x_2 \dots x_m$ есть не что иное, как композиция последовательности $(x_1, x_2, \dots, x_m)$ в группе G.

§ 7. Группы преобразований

1. *Группы преобразований*

Как мы уже отмечали (§ 6, n° 1), множество всех взаимно однозначных отображений множества E на себя образует группу относительно закона композиции $f \circ g$; эта группа обозначается $\mathfrak{S}_E$ и называется *симметрической группой* (или *группой всех подстановок*) множества E. Если E и E' — равномощные множества, φ — взаимно однозначное отображение E на E' и ψ — отображение, обратное φ, то отображение $f \to \varphi \circ f \circ \psi$ есть *изоморфизм* симметрической группы $\mathfrak{S}_E$ на симметрическую группу $\mathfrak{S}_{E'}$.

Симметрическую группу интервала $[1, n]$ множества $\mathbf{N}$ натуральных чисел обозначают $\mathfrak{S}_n$; это — конечная группа порядка $n!$;

симметрическая группа любого множества, состоящего из n элементов, изоморфна $\mathfrak{S}_n$.

Определение 1. *Подгруппы симметрической группы $\mathfrak{S}_E$ называются группами подстановок, или преобразований, множества E.*

Чаще всего употребление терминов «группа подстановок» и «симметрическая группа» ограничивают тем случаем, когда E конечно; каждая группа подстановок множества E тогда конечна. Группы подстановок множества E, состоящего из n элементов, называются группами подстановок *степени* n.

Примеры. 1) Знакопеременная группа. Положим $V_n = \prod_{1 \leqslant i < j \leqslant n} (j - i)$ и образуем для каждой подстановки $\pi \in \mathfrak{S}_n$ произведение $\pi(V_n) = \prod_{1 \leqslant i < j \leqslant n} (\pi(j) - \pi(i))$. Обозначая через ν число тех пар (i, j), для которых $1 \leqslant i < j \leqslant n$ и $\pi(i) > \pi(j)$ (называемое *числом инверсий* подстановки π), имеем $\pi(V_n) = \varepsilon_\pi V_n$, где $\varepsilon_\pi = (-1)^\nu$. Каково бы ни было отображение f N в N °(или, более общим образом, в коммутативное кольцо)$_c$, имеет место

$$\prod_{1 \leqslant i < j \leqslant n} (f(\pi(j)) - f(\pi(i))) = \varepsilon_\pi \prod_{1 \leqslant i < j \leqslant n} (f(j) - f(i)).$$

Число ε_π называется *сигнатурой* подстановки π; подстановку π называют *четной* или *нечетной* соответственно тому, будет ли ε_π равно $+1$ или -1. Тождественная подстановка ω (нейтральный элемент группы $\mathfrak{S}_n$) — четная. *Транспозицией* двух натуральных чисел i, j, удовлетворяющих неравенствам $1 \leqslant i < j \leqslant n$, называется подстановка $\tau \in \mathfrak{S}_n$ такая, что $\tau(i) = j$, $\tau(j) = i$ и $\tau(h) = h$ для всех h, отличных от i и j; транспозиция — *нечетная* подстановка.

Если π и ϱ — подстановки из $\mathfrak{S}_n$ и $\sigma = \pi\varrho$, то

$$\sigma(V_n) = \varepsilon_\varrho \pi(V_n) = \varepsilon_\pi \varepsilon_\varrho V_n,$$

откуда вытекает соотношение

$$\varepsilon_{\pi\varrho} = \varepsilon_\pi \varepsilon_\varrho, \tag{1}$$

показывающее, что отображение $\pi \to \varepsilon_\pi$ есть *представление* $\mathfrak{S}_n$ *на* мультипликативную группу, образованную числами $+1$ и -1. Множество всех четных подстановок из $\mathfrak{S}_n$, будучи прообразом $+1$ при этом представлении, является нормальной подгруппой индекса 2 (и следовательно, порядка $\frac{n!}{2}$) группы $\mathfrak{S}_n$; эта подгруппа называется *знакопеременной группой степени* n и обозначается $\mathfrak{A}_n$.

Обозначим через τ_i, где $1 \leqslant i \leqslant n-1$, транспозицию, меняющую местами i и $i+1$ и оставляющую все остальные целые из интервала $[1,n]$ на месте. Группа $\mathfrak{S}_n$ *порождается транспозициями* τ_i. Чтобы убедиться в этом, применим индукцию по n. Для $n=1$ предложение очевидно. Пусть π — любая подстановка из $\mathfrak{S}_n$ и $\pi(n)=k$; если $k=n$, то π принадлежит подгруппе в $\mathfrak{S}_n$, образованной подстановками, оставляющими n на месте; эта подгруппа отождествима с $\mathfrak{S}_{n-1}$, так что к ней применимо предположение индукции. Если же $k<n$, положим

$$\pi' = \tau_{n-1}\tau_{n-2}\dots\tau_{k+1}\tau_k\pi.$$

По определению транспозиций, тогда $\pi'(n)=n$, и мы приходим к предыдущему случаю.

2) Группы переносов произвольной группы. *Левые переносы* γ_x группы G (§ 2, n° 2) являются ее подстановками (§ 2, предложение 3); множество Γ всех этих переносов есть *группа* подстановок группы G, *изоморфная* G. Действительно, отображение $x \to \gamma_x$ группы G на Γ есть *представление* (§ 2, предложение 1), и оно *взаимно однозначно*, ибо отношение $\gamma_x = \gamma_y$ влечет $xe = ye$, т. е. $x=y$.

Так же устанавливается, что множество Δ всех правых переносов группы G есть группа ее подстановок, изоморфная группе, противоположной G, а значит, и самой группе G.

°3) *Движения* образуют группу преобразований евклидова пространства; *параллельные переносы* образуют ее подгруппу, и то же верно для *вращений* вокруг фиксированной точки (см. главу IX).°

2. *Представления группы в группу преобразований*

Если φ — инъективный гомоморфизм группы G в симметрическую группу $\mathfrak{S}_E$ множества E, то $\varphi(G)$ называется *реализацией группы G в виде группы преобразований множества E*.

Всякая группа G допускает реализации в виде групп преобразований, а именно групп ее переносов.

Более общим образом, рассмотрим *представление* группы G в симметрическую группу $\mathfrak{S}_E$ множества E и обозначим через f_α подстановку множества E, относимую элементу $\alpha \in G$ этим представлением; образ Γ группы G при представлении $\alpha \to f_\alpha$ есть группа преобразований множества E, изоморфная факторгруппе G/K группы G по ее нормальной подгруппе K, образованной теми элементами $\alpha \in G$, для которых f_α — тождественная подстановка (§ 6, теорема 3).

Таким образом, можно сказать, что Γ есть *реализация* G/K в виде группы преобразований.

Представление $\alpha \to f_\alpha$ определяет *на множестве* E *внешний закон композиции* операторов $\alpha \in G$ и элементов $x \in E$, при котором композицией α и x служит $f_\alpha(x)$ (см. § 3, n° 1); этот закон удовлетворяет следующим двум условиям: а) он *ассоциативен* относительно закона группы G (§ 5, n° 2), поскольку $f_\alpha \circ f_\beta = f_{\alpha\beta}$; б) нейтральный элемент ε группы G является *нейтральным оператором* рассматриваемого внешнего закона, поскольку f_ε есть тождественная подстановка множества E.

В частности, задание любой *группы преобразований* Γ множества E определяет на E внешний закон, удовлетворяющий указанным условиям, при котором композицией оператора $\sigma \in \Gamma$ и элемента $x \in E$ служит $\sigma(x)$.

Покажем, что условия а) и б) *характеризуют* внешние законы, полученные описанным способом, а именно:

Предложение 1. *Пусть* E *— множество, наделенное внешним законом композиции* $(\alpha, x) \to \alpha x$, *имеющим своей областью операторов группу* G *и удовлетворяющим следующим условиям:*

а) *этот внешний закон ассоциативен относительно закона группы* G (иными словами, при мультипликативной записи группы G, $\alpha(\beta x) = (\alpha\beta)x$, каковы бы ни были α, β, x);

б) *нейтральный элемент* ε *группы* G *есть нейтральный оператор внешнего закона* (иными словами, $\varepsilon x = x$ для всех $x \in E$).

При этих условиях отображение f_α, *порождаемое каждым* $\alpha \in G$, *является подстановкой множества* E, *а отображение* $\alpha \to f_\alpha$ *есть представление* G *в симметрическую группу* $\mathfrak{S}_E$.

В самом деле, $y = \alpha x$ влечет $\alpha^{-1}y = \alpha^{-1}(\alpha x) = (\alpha^{-1}\alpha)x = \varepsilon x = x$, и обратно, так что $x \to \alpha x$ действительно есть подстановка множества E; вторая же часть предложения вытекает из ассоциативности внешнего закона относительно закона группы.

Множество E, наделенное структурой, определяемой внешним законом, удовлетворяющим условиям предложения 1, называют для краткости множеством, *наделенным группой операторов* G; говорят также, что в множестве E *действует* группа G.

3. *Распространения группы преобразований*

Важный пример представлений группы на группу преобразований доставляют *распространения* групп преобразований. Если заданы (скажем) три множества F_1, F_2, F_3, их подстановки f_1, f_2, f_3 и множество M *шкалы множеств* (Теор. мн., Рез., § 8), имеющей в качестве базы множества F_1, F_2, F_3, то можно, следуя шаг за шагом по шкале, определить подстановку множества M, называемую *распространением* f_1, f_2, f_3 на M; будем обозначать ее $\varphi_M(f_1, f_2, f_3)$.

Напомним вкратце, как строится это определение. Следует различать два случая:

1° $M = \mathfrak{P}(L)$, где L — множество шкалы, для которого $\varphi_L(f_1, f_2, f_3)$ уже определено; тогда $\varphi_M(f_1, f_2, f_3)$ есть не что иное, как распространение $\varphi_L(f_1, f_2, f_3)$ на множество подмножеств (Теор. мн., Рез., § 2, n° 9);

2° $M = P \times Q$, где P и Q — множества шкалы, для которых $\varphi_P(f_1, f_2, f_3)$ и $\varphi_Q(f_1, f_2, f_3)$ уже определены; тогда $\varphi_M(f_1, f_2, f_3)$ есть распространение этих отображений на произведения множеств (Теор. мн., Рез., § 3, n° 14).

Если g_1, g_2, g_3 — еще три подстановки соответственно множеств F_1, F_2, F_3, то, как непосредственно следует из предыдущего определения,

$$\varphi_M(f_1 \circ g_1, f_2 \circ g_2, f_3 \circ g_3) = \varphi_M(f_1, f_2, f_3) \circ \varphi_M(g_1, g_2, g_3);$$

иными словами, φ_M есть *представление* группы $\mathfrak{S}_{F_1} \times \mathfrak{S}_{F_2} \times \mathfrak{S}_{F_3}$ в группу $\mathfrak{S}_M$. Если Γ_1, Γ_2, Γ_3 — группы преобразований соответственно множеств F_1, F_2, F_3, то сужение φ_M на группу $\Gamma_1 \times \Gamma_2 \times \Gamma_3$ называется *каноническим представлением* этой группы в $\mathfrak{S}_M$; образ группы $\Gamma_1 \times \Gamma_2 \times \Gamma_3$ при этом представлении называется *распространением* этой группы на множество M.

Пусть теперь G — произвольная группа и h_i — ее представление в группу Γ_i преобразований множества F_i $(i = 1, 2, 3)$; положив для каждого $\sigma \in G$ $\sigma_M = \varphi_M(h_1(\sigma), h_2(\sigma), h_3(\sigma))$, мы получим *представление* $\sigma \longrightarrow \sigma_M$ группы G в $\mathfrak{S}_M$, называемое *распространением* представлений h_1, h_2, h_3 на множество M.

В частности, если за G принята группа Γ_1 преобразований множества F_1, за h_1 — тождественное отображение Γ_1 на себя, а за h_2 и h_3 — постоянные отображения Γ_1 на группы Γ_2 и Γ_3, сводящиеся к тождественным подстановкам соответственно множеств F_2 и F_3, распространение этих представлений на M по-прежнему называется

каноническим представлением Γ_1 в $\mathfrak{S}_M$; легко видеть (идя шаг за шагом по шкале), что это — инъективный гомоморфизм Γ_1 в $\mathfrak{S}_M$, если только M не принадлежит шкале, имеющей в качестве базы одни множества F_2, F_3.

Может оказаться, что множество $P \subset M$ таково, что *сужение* σ_M на P есть подстановка этого P для каждого $\sigma \in G$; обозначив эту подстановку σ_P, мы будем иметь тогда представление $\sigma \longrightarrow \sigma_P$ группы G в $\mathfrak{S}_P$, по-прежнему называемое *распространением* представлений h_1, h_2, h_3 на P.

Важный пример этого имеем, когда M — множество всех подмножеств произведения $K \times L$ множеств K и L шкалы, а P — множество всех *отображений* K в L, отождествимое с подмножеством множества M, образованным *графиками* этих отображений (Теор. мн., Рез., § 3, n° 5); элемент множества M, относимый представлением σ_M графику отображения w множества K в L, будет графиком отображения $\sigma_K(z) \longrightarrow \sigma_L(w(z))$.

4. Инварианты группы операторов. Группы автоморфизмов

Определение 2. *Пусть E — множество, наделенное группой операторов G. Говорят, что элемент $x \in E$ есть инвариант группы G* (или что *x инвариантен относительно G*, или что *G оставляет x инвариантным*), *если x инвариантен относительно всех операторов группы G* (иными словами, если $\alpha x = x$ для каждого $\alpha \in G$).

Задание представления f группы G на группу Γ преобразований множества E превращает G в группу операторов на E (n° 2); инвариант этой группы операторов называется также *инвариантом группы G относительно представления f*.

Более общим образом, пусть, скажем, F_1, F_2, F_3 — три множества, Γ_i ($i=1, 2, 3$) — группа преобразований множества F_i, h_i — представление G на Γ_i и M — множество шкалы, имеющей в качестве базы множества F_1, F_2, F_3 (или инвариантное подмножество множества этой шкалы). Если $\sigma \longrightarrow \sigma_M$ — распространение представлений h_1, h_2, h_3 на M (n° 3), инвариант группы G относительно этого представления называют (допуская вольность речи) ее инвариантом *относительно представлений h_1, h_2, h_3*.

Важным частным случаем этого понятия является понятие *инвариантного отображения* относительно группы G. Пусть K

и L — два множества шкалы, имеющей в качестве базы множества F_1, F_2, F_3; отображение w множества K в L называют *инвариантным* относительно G, если $\sigma_L(w(z)) = w(\sigma_K(z))$ для всех $z \in K$ и $\sigma \in G$. В этом случае говорят также, что $w(z)$ есть *ковариант* элемента z (относительно группы G и представлений h_1, h_2, h_3).

Рассматривая группу преобразований Γ_1 множества F_1 и говоря, без дальнейших уточнений, о ее *инварианте* в множестве M шкалы, имеющей в качестве базы множества F_1 и, скажем, F_2, F_3, имеют в виду инвариант группы Γ_1 относительно канонического представления (n° 3) Γ_1 в $\mathfrak{S}_M$.

Примеры. 1) Пусть Γ — группа преобразований множества E и a — произвольный элемент из E. Множество всех элементов $\sigma(a)$, где σ пробегает Γ, есть подмножество множества E, *инвариантное* относительно Γ (см. n° 5).

2) Пусть в множестве F задан аддитивно записываемый коммутативный ассоциативный закон композиции. Рассмотрим множество P всех последовательностей $(x_i)_{1 \leqslant i \leqslant n}$ по n элементов из F, т. е. множество всех отображений интервала $I = [1, n] \subset \mathbf{N}$ в F; относя каждому элементу (x_i) из P элемент $\sum_{i=1}^{n} x_i$ из F, мы получим отображение P в F, являющееся, как вытекает из теоремы коммутативности (§ 1, теорема 3), *инвариантом* симметрической группы $\mathfrak{S}_n = \mathfrak{S}_I$ *).

Точно так же, если, в частности, взять за F множество $\mathbf{Z}$ рациональных целых чисел °(или коммутативное кольцо)$_\circ$, произведение $\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)$, рассматриваемое как отображение P в $\mathbf{Z}$, является *инвариантом* знакопеременной группы $\mathfrak{A}_n$ (но не симметрической группы $\mathfrak{S}_n$).

°3) В трехмерном вещественном евклидовом пространстве $E = \mathbf{R}^3$ *расстояние*

$$\sqrt{(x'-x)^2+(y'-y)^2+(z'-z)^2}$$

между точками (x, y, z) и (x', y', z'), рассматриваемое как отображение $E \times E$ в $\mathbf{R}$, есть инвариант группы движений (см. главу IX).$_\circ$

---

*) Выражение $\sum_{i=1}^{n} x_i$ есть только одна из так называемых «симметрических функций» от $x_1, x_2, \ldots, x_n$ (см. главы III и V), которые все являются *инвариантами* относительно группы $\mathfrak{S}_n$; от этого свойства и происходит наименование «симметрическая группа».

Замечание. Если заданы группа преобразований Г множества E и множество M шкалы, имеющей в качестве базы E (и, возможно, еще некоторые другие множества), то не следует смешивать *подмножество* множества M, *инвариантное относительно* Г (элемент из $\mathfrak{P}(M)$, инвариантный относительно Г), и множество *элементов* из M, *инвариантных относительно* Г (такое множество очевидно является элементом из $\mathfrak{P}(M)$, инвариантным относительно Г, но обратное, вообще говоря, неверно).

Теорема 1. *Пусть E — множество, наделенное группой операторов G, и A — его непустое подмножество. Множество H всех операторов $\alpha \in G$, оставляющих инвариантным каждый элемент из A, есть подгруппа группы G.*

Действительно, если $\alpha x = x$ и $\beta x = x$, то также $(\alpha\beta)x = \alpha(\beta x) = \alpha x = x$ и $\alpha^{-1}x = \alpha^{-1}(\alpha x) = (\alpha^{-1}\alpha)x = \varepsilon x = x$ (где ε — нейтральный элемент группы G).

Каково бы ни было $\gamma \in G$, множество всех операторов $\alpha \in G$, оставляющих инвариантным каждый элемент из γA, есть подгруппа $\gamma H \gamma^{-1}$, поскольку отношение $\alpha\gamma x = \gamma x$ эквивалентно отношению $(\gamma^{-1}\alpha\gamma)x = x$.

Допуская вольность речи, говорят, что так определенная подгруппа H есть *подгруппа группы G, оставляющая инвариантными элементы множества A*.

Замечание. Множество всех инвариантов этой подгруппы очевидно содержит A, но может содержать и элементы из E, не принадлежащие A.

Пример. °Подгруппа группы движений евклидова пространства, оставляющая инвариантными две различные точки,— это группа всех вращений вокруг соединяющей эти точки прямой и, значит, оставляет инвариантными все точки этой прямой.°

Рассмотрим, в частности, *структуру* $\mathscr{S}$, заданную в множестве E (Теор. мн., Рез., § 8). Это — элемент некоторого множества M шкалы, имеющей в качестве базы множество E и некоторое число вспомогательных множеств. Каждая подстановка f множества E, образ которой в $\mathfrak{S}_M$ (при каноническом отображении $\mathfrak{S}_E$ в $\mathfrak{S}_M$) оставляет элемент $\mathscr{S}$ инвариантным, есть, по определению (Теор. мн., Рез., § 8, n° 5), *автоморфизм* структуры $\mathscr{S}$. Таким образом:

Предложение 2. *Автоморфизмы структуры $\mathscr{S}$, заданной в множестве E, образуют группу преобразований этого множества* (называемую *группой автоморфизмов* структуры $\mathscr{S}$, или множества E, наделенного структурой $\mathscr{S}$).

Пусть $\mathscr{S}'$ — изоморфная $\mathscr{S}$ структура, определенная в множестве E', φ — изоморфизм $\mathscr{S}$ на $\mathscr{S}'$ и ψ — обратный изоморфизм; очевидно, отображение $f \to \varphi \circ f \circ \psi$ есть изоморфизм группы автоморфизмов структуры $\mathscr{S}$ на группу автоморфизмов структуры $\mathscr{S}'$.

Пример. Группа автоморфизмов группы. Пусть G — заданная группа. Ее автоморфизмы, согласно предложению 2, образуют подгруппу Γ симметрической группы $\mathfrak{S}_G$. *Внутренние автоморфизмы* α_x группы G (§ 6, n° 4) образуют *подгруппу* Δ группы Γ, как следует из непосредственно проверяемого тождества $\alpha_{xy} = \alpha_x \circ \alpha_y$. Оно показывает, кроме того, что отображение $x \to \alpha_x$ есть *представление* G на Δ; для того чтобы α_x было тождественным отображением G на себя, необходимо и достаточно, чтобы $xyx^{-1} = y$ для каждого $y \in G$, т. е. $xy = yx$ для каждого $y \in G$; иными словами, x должно принадлежать центру Z группы G; в силу теоремы 3 § 6, это снова показывает, что Z — *нормальная* подгруппа группы G, и мы видим вместе с тем, что группа Δ всех внутренних автоморфизмов группы G изоморфна факторгруппе G/Z.

Заметим, что группа Δ может совпадать с Γ; она может также сводиться к тождественному отображению; для этого необходимо и достаточно, чтобы $Z = G$, т. е. чтобы G была *коммутативна*. Автоморфизмы группы G, не являющиеся ее внутренними автоморфизмами, иногда называют *внешними* автоморфизмами этой группы.

Если G наделена структурой *группы с операторами*, автоморфизмы этой структуры образуют группу Γ', очевидно являющуюся подгруппой группы Γ всех автоморфизмов заданной в G структуры *группы*; заметим, что, вообще говоря, группа Δ внутренних автоморфизмов не есть подгруппа группы Γ'.

5. *Транзитивные группы*

Пусть Γ — группа преобразований множества E. Отношение «существует $f \in \Gamma$ такое, что $y = f(x)$» есть *отношение эквивалентности* в E; действительно, оно *рефлексивно*, ибо тождественная подстановка u принадлежит Γ и $x = u(x)$; оно *симметрично*, ибо если $f \in \Gamma$ таково, что $y = f(x)$, то обратное ему отображение g принадлежит Γ и $x = g(y)$; наконец, оно *транзитивно*, ибо из $y = f(x)$ и $z = g(y)$ следует $z = g(f(x))$, а если f и g принадлежат Γ, то и $g \circ f$ принадлежит Γ.

Классы по этому отношению эквивалентности называются *классами интранзитивности группы* Γ; класс интранзитивности, которому принадлежит элемент $a \in E$,— это множество всех $f(a)$, где f пробегает Γ; его называют также *орбитой* элемента a относительно группы Γ. Если существует только один класс интранзитивности (совпадающий тогда с E), то группу Γ называют *транзитивной*; в противном случае — *интранзитивной*. Условие транзитивности группы Γ может быть выражено следующим образом: при любом заданном $a \in E$ для каждого $x \in E$ существует $f \in \Gamma$ такое, что $x = f(a)$.

Примеры. 1) Симметрическая группа $\mathfrak{S}_n$ очевидно транзитивна; то же верно и для знакопеременной группы $\mathfrak{A}_n$, если $n > 2$, ибо для любых трех различных целых чисел i, j, k из интервала $[1, n]$ его подстановка σ, определяемая условиями $\sigma(i) = j$, $\sigma(j) = k$, $\sigma(k) = i$ и $\sigma(h) = h$ для всех h, отличных от i, j, k («круговая подстановка»), как легко убедиться, — четная.

2) Группа всех левых переносов группы G транзитивна, ибо для нейтрального элемента e этой группы имеем $\gamma_x(e) = x$; точно так же и группа всех правых переносов транзитивна.

3) Группа Δ всех внутренних автоморфизмов группы G (содержащей более одного элемента) интранзитивна, ибо $\alpha_x(e) = e$, каково бы ни было $x \in G$; элементы одного и того же класса интранзитивности группы Δ называются *сопряженными* элементами группы G; каждый элемент центра группы G уже сам образует класс интранзитивности группы Δ.

4) Если Γ — интранзитивная группа преобразований множества E и A — ее класс интранзитивности, множество сужений на A всевозможных подстановок из Γ есть транзитивная группа преобразований множества A.

6. Однородные пространства

Пусть E — множество, наделенное группой операторов G (n° 2); говорят, что G *транзитивно действует в* E, если (в обозначениях n° 2) образ G в $\mathfrak{S}_E$ при представлении $\alpha \to f_\alpha$ есть *транзитивная* группа подстановок множества E.

Определение 3. *Однородным пространством называется множество E, наделенное транзитивно действующей в нем группой операторов G.*

Таким образом, каждая транзитивная группа Γ подстановок множества E определяет в E структуру однородного пространства с внешним законом композиции, относящим подстановке $\sigma \in \Gamma$ и элементу $x \in E$ элемент $\sigma(x)$.

Пример. °Всякое евклидово пространство есть однородное пространство, группой операторов которого служит группа движений (см. главу IX).

Замечание. Можно также сказать, что однородное пространство — это множество E с группой операторов G, внешний закон которого удовлетворяет следующему условию: каковы бы ни были $x \in E$ и $y \in E$, существует $\alpha \in G$ такое, что $y = \alpha x$. Заметим, что из этого условия, в соединении с ассоциативностью внешнего закона относительно закона группы G, следует, что нейтральный элемент ε группы G является нейтральным оператором: действительно так как существует $\lambda \in G$ такое, что $x = \lambda x$, то $\varepsilon x = \varepsilon(\lambda x) = (\varepsilon\lambda)x = \lambda x = x$.

Какова бы ни была группа G, *левый внешний закон* (§ 3, n° 2), порождаемый законом группы, определяет в G структуру *однородного пространства*, группой операторов которого служит сама группа G (ибо группа подстановок Γ, являющаяся образом G в $\mathfrak{S}_G$, есть не что иное, как группа левых переносов группы G). Рассмотрим теперь однородное пространство E, имеющее G своей группой операторов, и пусть a — произвольный фиксированный элемент из E; отображение $\alpha \to \alpha a$ есть *представление* G (наделенного определенной выше структурой *однородного пространства*) в однородное пространство E, и это — представление *на* E, поскольку G действует в E транзитивно. Поэтому (§ 4, теорема 1) E изоморфно результату факторизации G (рассматриваемого как однородное пространство) по отношению эквивалентности $\alpha a = \beta a$. Но это отношение, *согласуясь слева* с законом группы G, имеет вид $\beta \in \alpha H_a$, где H_a — подгруппа группы G, образованная всеми $\alpha \in G$, *оставляющими* a *инвариантным*; а результат факторизации G по этому отношению есть множество всех *левых классов* по H_a, наделенное внешним законом композиции, относящим каждому оператору $\alpha \in G$ и каждому левому классу ξH_a левый класс $\alpha\xi H_a$.

Обратно, пусть H — *произвольная* подгруппа группы G и G/H — фактормножество множества G по отношению эквивалентности $\beta \in \alpha H$ (согласующемуся слева с групповым законом); фактор-закон левого внешнего закона, порожденного законом группы, заданным в G, по этому отношению определяет в G/H структуру

однородного пространства, имеющего G своей группой операторов; действительно, достаточно показать, что G транзитивно действует в G/H; но для любых двух элементов $u=\alpha H$ и $v=\beta H$ фактормножества G/H имеем $v=(\beta\alpha^{-1})u$. Множество G/H, наделенное этой структурой, называется *однородным пространством*, *определяемым подгруппой* H *группы* G.

В случае произвольной подгруппы H множество G/H, вообще говоря, не наделено никаким *внутренним* законом; если же H — *нормальная* подгруппа, то, как мы видели, внутренний закон на G/H, являющийся факторзаконом закона группы G по H, есть закон группы; в этом случае не следует смешивать *факторгруппу* G/H, определяемую этим законом, с *однородным пространством* G/H.

Резюмируя полученные результаты, приходим к следующей теореме:

Теорема 2. *Пусть E — однородное пространство и G — его группа операторов. Пусть, далее, a — любой элемент из E и H_a — подгруппа группы G, образованная всеми операторами α, оставляющими a инвариантным. Тогда однородное пространство E изоморфно однородному пространству G/H_a, определяемому подгруппой H_a.*

Взяв другой элемент $b \in E$, получим, что E изоморфно также однородному пространству G/H_b; при этом для $\beta \in G$ такого, что $b = \beta a$, отношения $\alpha b = b$ и $\beta^{-1}\alpha\beta a = a$ эквивалентны и потому $H_b = \beta H_a \beta^{-1}$. Пересечение всех H_x, где x пробегает E, есть не что иное, как группа K всех нейтральных операторов однородного пространства E; таким образом, можно сказать, что K — *наибольшая* нормальная подгруппа группы G, содержащаяся во всех H_x.

Отсюда получается характеристика всех *реализаций* (п° 2) группы G как *транзитивной* группы преобразований (или, как мы будем еще говорить, *транзитивных реализаций* группы G):

Предложение 3. *Всякая транзитивная реализация группы G есть* (с точностью до изоморфизма) *группа, образованная подстановками, порождаемыми операторами однородного пространства G/H, где H — некоторая подгруппа группы G, не содержащая никакой ее нормальной подгруппы, отличной от $\{e\}$.*

Взяв, в частности, $H=\{e\}$, получим в качестве транзитивной реализации группы G группу всех ее левых переносов.

7. *Примитивные группы*

Определим *факторструктуры* структуры однородного пространства; в силу теоремы 2, можно ограничиться случаем однородного пространства G/H, определяемого подгруппой H группы G. Если наделить G структурой однородного пространства, определяемой левым внешним законом, порожденным законом группы, структура однородного пространства в G/H будет факторструктурой этой структуры однородного пространства в G по отношению $y \in xH$; пусть R — это отношение. Из первой теоремы об изоморфизме (§ 4, теорема 2) следует, что каждое отношение эквивалентности в G/H, согласующееся со структурой этого однородного пространства, имеет вид S/R, где S — отношение, согласующееся слева с законом группы в G и являющееся следствием R; поэтому (§ 6, теорема 1) S имеет вид $y \in xK$, где K — подгруппа группы G, содержащая H; и та же первая теорема об изоморфизме показывает, что факторструктура структуры однородного пространства G/H по отношению S/R изоморфна структуре однородного пространства G/K. Резюмируя, имеем:

Предложение 4. *Каждая факторструктура структуры однородного пространства G/H, определяемого подгруппой H группы G, изоморфна структуре однородного пространства G/K, где K — подгруппа группы G, содержащая H; и обратно, каждая подгруппа K, содержащая H, определяет факторструктуру структуры однородного пространства G/H.*

Рассмотрим, в частности, структуру однородного пространства, определяемую в множестве E транзитивной группой Γ его преобразований; согласно предыдущему, однородное пространство E изоморфно Γ/Δ, где Δ — подгруппа группы Γ, оставляющая инвариантным элемент $a \in E$, и факторструктуры структуры этого однородного пространства находятся во взаимно однозначном соответствии с подгруппами Θ группы Γ такими, что $\Delta \subset \Theta \subset \Gamma$. По крайней мере две такие подгруппы всегда имеются, а именно Δ и Γ; первая соответствует самому E, а вторая — однородному пространству, сводящемуся к *единственному* элементу; если других подгрупп Θ, удовлетворяющих условиям $\Delta \subset \Theta \subset \Gamma$, не существует, то группу преобразований Γ называют *примитивной*, в противном случае — *imprimитивной*.

Таким образом, сказать, что группа преобразований Γ примитивна, все равно, что сказать, что Δ является *максимальным* элементом множества всех подгрупп группы Γ, отличных от Γ.

Предложение 5. *Для того чтобы транзитивная группа* Γ *подстановок множества* E *была импримитивной, необходимо и достаточно, чтобы существовало множество* $A \subset E$, *содержащее более одного элемента, отличное от* E *и такое, что, какова бы ни была подстановка* $\sigma \in \Gamma$, *либо* $\sigma(A) \subset A$, *либо* $A \cap \sigma(A) = \varnothing$.

Покажем сначала, что это условие *необходимо*. Действительно, если, в прежних обозначениях, существует подгруппа Θ, отличная от Δ и Γ и такая, что $\Delta \subset \Theta \subset \Gamma$, то она определяет в E отношение эквивалентности R, согласующееся со структурой однородного пространства в E, и классы эквивалентности по R содержат более одного элемента и отличны от E; для каждого из этих классов A также $\sigma(A)$, где σ — любая подстановка из Γ, есть класс по R, и справедливость утверждения следует из того, что эти классы образуют *разбиение* множества E.

Чтобы убедиться в *достаточности* условия, заметим сначала, что, как следует из него, если подстановка $\sigma \in \Gamma$ удовлетворяет условию $\sigma(A) \subset A$, то $\sigma(A) = A$; действительно, тогда $A \subset \sigma^{-1}(A)$, значит, $A \cap \sigma^{-1}(A) \neq \varnothing$, и следовательно, $\sigma^{-1}(A) \subset A$, так что $A = \sigma^{-1}(A) = \sigma(A)$. Отсюда сразу следует (теорема 1), что множество Θ тех подстановок $\sigma \in \Gamma$, для которых $\sigma(A) \subset A$ (или, что по предположению равносильно этому, для которых $A \cap \sigma(A) \neq \varnothing$), есть подгруппа группы Γ. Эта подгруппа отлична от Γ, ибо по условию $A \neq E$, а Γ транзитивна; она отлична и от Δ, ибо A содержит по крайней мере один элемент $b \neq a$, и для подстановки $\tau \in \Gamma$ такой, что $\tau(a) = b$, имеем $\tau \notin \Delta$ и $\tau(A) \cap A \neq \varnothing$, т. е. $\tau \in \Theta$; следовательно, Γ импримитивна.

Классы эквивалентности по отношению R, соответствующему подгруппе Θ, называются *классами импримитивности* группы Γ, соответствующими этой подгруппе; это элементы однородного пространства, получающегося в результате факторизации E по отношению R (и изоморфного Γ/Θ).

Упражнения. 1) Показать, что число элементов конечной группы G, сопряженных (n° 5) с ее элементом a, равно индексу его нормализатора (§ 6, упражнение 13) и, следовательно, является делителем порядка группы G.

*2) Число автоморфизмов конечной группы n-го порядка G не превосходит $n^{\frac{\log n}{\log 2}}$. [Показать, что G обладает системой образующих $\{a_1, a_2, \ldots, a_m\}$ такой что a_i не принадлежит подгруппе, порожденной элементами $a_1, \ldots, a_{i-1}$ $(2 \leqslant i \leqslant m)$; вывести отсюда, что $2^m \leqslant n$ и что число автоморфизмов группы G не превосходит n^m.]

3) Пусть Γ — группа всех автоморфизмов, а Δ — группа всех внутренних автоморфизмов группы G; показать, что Δ — нормальная подгруппа группы Γ. Для того чтобы автоморфизм σ группы G был перестановочен со всеми ее внутренними автоморфизмами, необходимо и достаточно, чтобы $x^{-1}\sigma(x)$ принадлежало центру группы G для всех $x \in G$; вывести отсюда, что если центр группы G сводится к одному нейтральному элементу, то это же верно и для централизатора (§ 6, упражнение 13) подгруппы Δ в Γ.

*4) а) Пусть G — простая некоммутативная группа, Γ — группа всех ее автоморфизмов и Δ — группа всех внутренних автоморфизмов группы G (изоморфная G). Показать, что, каков бы ни был автоморфизм s группы Γ, $s(\Delta) = \Delta$. [Используя предыдущее упражнение 3 и предложение 7 § 6, заметить, что $\Delta \cap s(\Delta)$ не может сводиться к нейтральному элементу группы Γ.]

б) Показать, что единственный автоморфизм группы Γ, оставляющий инвариантным каждый элемент из Δ, — тождественный. [Записать, что, каковы бы ни были $\alpha \in \Delta$ и $\sigma \in \Gamma$, этот автоморфизм оставляет инвариантными α и $\sigma\alpha\sigma^{-1}$, и воспользоваться упражнением 3.]

в) Пусть s — автоморфизм группы Γ, φ — изоморфизм $x \to \alpha_x$ группы G на Δ, ψ — обратный ему изоморфизм и σ — автоморфизм $\psi \circ s \circ \varphi$ группы G; показать, что автоморфизм $\xi \to \sigma^{-1}s(\xi)\sigma$ группы Γ — тождественный. [Использовать б), приняв во внимание, что $s(\alpha_x) = \alpha_{\sigma(x)}$ для всех $x \in G$.] Вывести отсюда, что каждый автоморфизм группы Γ — внутренний.

*5) а) Пусть G — группа, Σ — группа ее автоморфизмов и Γ — группа левых переносов группы G (изоморфная G). Показать, что в симметрической группе $\mathfrak{S}_G$ пересечение $\Sigma \cap \Gamma$ сводится к нейтральному элементу и $\Sigma\Gamma = \Gamma\Sigma$. Вывести отсюда, что $\Omega = \Gamma\Sigma$ есть подгруппа группы $\mathfrak{S}_G$; ее называют *голоморфом* группы G. [См. § 6, упражнение 4.]

б) Показать, что Γ — нормальная подгруппа группы Ω и всякий автоморфизм группы Γ имеет вид $\gamma \to \sigma\gamma\sigma^{-1}$, где $\sigma \in \Sigma$.

в) Группа Δ всех правых переносов группы G есть нормальная подгруппа группы Ω, а $\Gamma \cap \Delta$ является центром каждой из групп Γ, Δ.

г) Показать, что Ω есть нормализатор (§ 6, упражнение 13) Γ в $\mathfrak{S}_G$. [Пусть τ — элемент нормализатора Γ в $\mathfrak{S}_G$; положив $\tau\gamma_x\tau^{-1} = \gamma_{\sigma(x)}$, доказать, что $\sigma(x) = \tau(xu)$, где $u = \tau^{-1}(e)$; далее, показать, что σ есть автоморфизм группы G, и использовать в).]

д) Показать, что Δ — централизатор (§ 6, упражнение 13) Γ в $\mathfrak{S}_G$.

6) а) Пусть (E_ι) — разбиение множества E и Γ — множество всех подстановок σ этого множества таких, что $\sigma(E_\iota) \subset E_\iota$ для каждого индекса ι. Показать, что Γ — подгруппа группы $\mathfrak{S}_E$; обозначая через Γ_ι подгруппу группы Γ, образованную теми подстановками σ, для которых $\sigma(E_\iota) = E_\iota$ и $\sigma(x) = x$ для всех $x \notin E_\iota$, показать, что Γ_ι изоморфна $\mathfrak{S}_{E_\iota}$, а Γ изоморфна произведению $\prod_\iota \Gamma_\iota$.

б) Пусть σ — произвольная подстановка множества E и (E_ι) — его разбиение, образованное классами интранзитивности моногенной подгруппы группы $\mathfrak{S}_E$, порождаемой этой подстановкой. Компонента σ_ι подстановки σ в группе Γ_ι, соответствующей E_ι, порождает в этой группе моногенную подгруппу, транзитивную в E_ι, и называется *циклической подстановкой* или *циклом*; σ_ι называются *циклическими компонентами* подстановки σ. Если число циклических компонент подстановки σ, не сводящихся к тождественной подстановке, конечно, то σ равна их произведению (в любом порядке, поскольку циклические компоненты подстановки попарно перестановочны). В случае, когда какое-нибудь E_ι состоит из конечного числа элементов, их можно расположить в конечную последовательность $(a_i)_{1 \leqslant i \leqslant n}$ так, чтобы $a_{i+1} = \sigma(a_i)$ $(1 \leqslant i \leqslant n-1)$ и $a_1 = \sigma(a_n)$; соответствующую циклическую компоненту подстановки σ обозначают тогда $(a_1 a_2 \dots a_n)$ и говорят, что ее длина равна n. Для любой подстановки τ из $\mathfrak{S}_E$ имеем

$$\tau \cdot (a_1 a_2 \dots a_n) \cdot \tau^{-1} = (\tau(a_1)\, \tau(a_2) \dots \tau(a_n)). \qquad (1)$$

*7) а) Показать, что каждая подстановка из $\mathfrak{S}_n$ есть произведение транспозиций. [Индукцией по числу элементов, не инвариантных относительно рассматриваемой подстановки.]

б) Вывести, что $\mathfrak{S}_n$ порождается $n-1$ транспозициями (1 2), (1 3), ..., (1 n), а также $n-1$ транспозициями (1 2), (2 3), ..., ($n-1$ n). [Воспользоваться формулой (1) упражнения 6.]

в) Вывести, что $\mathfrak{S}_n$ порождается *двумя* подстановками (1 2) и (1 2 3 ... n). [Тем же методом.]

*8) а) Показать, что каждая подстановка $\sigma \in \mathfrak{A}_n$ есть произведение циклов длины 3 (не являющихся, вообще говоря, ее компонентами). [Доказать это утверждение для произведения двух транспозиций и использовать упражнение 7а.]

б) Вывести, что $\mathfrak{A}_n$ порождается $n-2$ подстановками (1 2 3), (1 2 4), ..., (1 2 n). [Воспользоваться формулой (1) упражнения 6.]

в) Вывести, что $\mathfrak{A}_n$ при нечетном n порождается *двумя* подстановками (1 2 3) и (1 2 ... n), а при четном n — двумя подстановками (1 2 3) и (2 3 ... n).

г) Показать, что нормальная подгруппа группы $\mathfrak{A}_n$, содержащая цикл длины 3, совпадает с $\mathfrak{A}_n$. [С помощью формулы (1) упражнения 6 доказать, что эта подгруппа содержит все циклы $(1\ 2\ k)$, где $3 \leqslant k \leqslant n$.]

9) Группа преобразований Г множества E называется *r-кратно транзитивной*, если для любых двух последовательностей $(a_1, a_2, \ldots, a_r)$ и $(b_1, b_2, \ldots, b_r)$ по r различных элементов из E существует подстановка $\sigma \in \Gamma$ такая, что $\sigma(a_i) = b_i$ для $1 \leqslant i \leqslant r$, и это свойство не имеет уже места хотя бы для одной пары последовательностей по $r+1$ различных элементов из E.

а) Показать, что r-кратно транзитивная группа при $r > 1$ примитивна. [Применить предложение 5.]

б) Порядок r-кратно транзитивной группы подстановок Г степени n имеет вид $n(n-1)\ldots(n-r+1)d$, где d — делитель $(n-r)!$ [Рассмотреть подгруппу подстановок из Г, оставляющих инвариантными r элементов, и вычислить ее индекс.]

*10) Пусть Г — r-кратно транзитивная группа подстановок множества E, состоящего из n элементов, и $n - s$ — число элементов множества E, инвариантных относительно нетождественной подстановки $\sigma \in \Gamma$. Показать, что если $s > r$, то существует подстановка $\tau \in \Gamma$ такая, что $\sigma^{-1}\tau\sigma\tau^{-1}$ — нетождественная подстановка, оставляющая инвариантными $\geqslant n - 2(s-r+1)$ элементов из E. [Воспользоваться разложением σ на ее циклические компоненты (упражнение 6) и формулой (1) упражнения 6.] Показать также, что при $s = r$ существует $\tau \in \Gamma$, для которого $\sigma^{-1}\tau\sigma\tau^{-1}$ есть цикл длины 3. Вывести отсюда, что если $r \geqslant 3$ и Г не содержит знакопеременной группы $\mathfrak{A}_n$, то $s \geqslant 2r - 2$ для каждой подстановки из Г. [Использовать упражнение 8.] Наконец, доказать, что если Г не совпадает с $\mathfrak{A}_n$ или с $\mathfrak{S}_n$, то $r \leqslant \frac{n}{3} + 1$.

*11) а) Показать, что знакопеременная группа $\mathfrak{A}_n$ $(n-2)$-кратно транзитивна.

б) Показать, что группа $\mathfrak{A}_n$ при $n \neq 4$ *простая*. [Используя а), метод упражнения 10 и упражнение 8г, показать, что $\mathfrak{A}_n$ простая при $n > 6$; аналогичным образом исследовать случай $n \leqslant 6$.]

12) Пусть Г — транзитивная группа подстановок множества E. Показать, что каждый класс интранзитивности ее нормальной подгруппы Δ является классом импримитивности для Г. [Воспользоваться предложением 5.] Вывести отсюда, что если Г примитивна, то Δ транзитивна.

*13) Пусть Г — интранзитивная группа подстановок множества E, A — ее класс интранзитивности и $B = CA$ — его дополнение. Обозначим через Γ_A и Γ_B группы, образованные сужениями подстановок из Г соответственно на A и B, через Δ_A и Δ_B — подгруппы группы Г, оставляющие инвариантными каждый элемент соответственно из A и B. Показать, что Δ_A и Δ_B — нормальные подгруппы группы Г и что Γ_A изоморфно Γ/Δ_A, а Γ_B изоморфно Γ/Δ_B; обозначая через

Δ_{AB} (соответственно Δ_{BA}) группу, образованную сужениями подстановок из Δ_A (соответственно Δ_B) на B (соответственно A), показать, что факторгруппы Γ_A/Δ_{BA}, Γ_B/Δ_{AB} и $\Gamma/(\Delta_A\Delta_B)$ изоморфны. [Применить теорему 6 § 6 к представлению $\sigma \to \sigma_A$, относящему каждой подстановке $\sigma \in \Gamma$ ее сужение на A.]

*14) а) Пусть Γ — группа подстановок множества E, состоящего из m элементов; показать, что индекс $(\Gamma:\Delta_a)$ ее подгруппы Δ_a, оставляющей инвариантным элемент $a \in E$, равен числу элементов того класса интранзитивности группы Γ, которому принадлежит a.

б) Пусть ν_k — число подстановок из Γ, оставляющих инвариантными k элементов из E, n — порядок группы Γ и t — число ее классов интранзитивности. Доказать формулу

$$nt = \sum_{k=0}^{m} k\nu_k. \tag{2}$$

[Обозначая через $p(\sigma)$ число элементов, инвариантных относительно подстановки $\sigma \in \Gamma$, вычислить двумя разными способами $\sum_{\sigma\in\Gamma} p(\sigma)$ и применить а).]

в) Показать, что если число $p(\sigma)=k$ одно и то же для всех нетождественных подстановок из Γ и порядок Δ_a больше 1 для каждого a, то $k \leqslant t < 2k$. [Заметить, что $m \leqslant kn$.] В том частном случае, когда $k=2$, найти все возможные порядки подгрупп Δ_a, соответствующих классам интранзитивности группы Γ; показать, что при $t=3$ порядок подгруппы Δ_a для элементов двух из трех классов интранзитивности не может быть >2, если только n не равно ни 12, ни 24, ни 60.

15) Пусть E — множество, наделенное внешним законом композиции $(\alpha, x) \to \alpha x$, который имеет своей областью операторов группу G и ассоциативен (§ 5, n° 2) относительно ее группового закона. Показать, что множество $A=\varepsilon E$, где ε — нейтральный элемент группы G, устойчиво относительно рассматриваемого внешнего закона и что A является относительно индуцированного закона множеством, наделенным группой операторов G, в смысле n° 2. Каждый класс интранзитивности группы Γ всех подстановок множества A, порожденных операторами из G, есть устойчивое подмножество этого множества, а структура, индуцированная в любом из этих классов, есть структура однородного пространства.

*16) а) Пусть G — группа, H — ее подгруппа и r — взаимно однозначное отображение множества G/H всех левых классов по H в G, относящее каждому $X \in G/H$ элемент $r(X) \in X \subset G$, так что $X=r(X)H$. Определим на G/H внутренний закон композиции $\top$, положив $X \top Y = r(X)\,r(Y)\,H$. Показать, что $X \top H = X$ для всех X и что каждый левый перенос закона $\top$ есть взаимно однозначное отображение G/H на себя. Если G' — подгруппа группы G, порожденная

множеством всех элементов $r(X)$, и $H'=H\cap G'$, то внутренний закон, определяемый аналогичным образом на G'/H' отображением r, определяет в этом множестве структуру, изоморфную определяемой в G/H законом $\top$.

б) Для ассоциативности закона $\top$ необходимо и достаточно, чтобы H' была нормальной подгруппой группы G', причем в этом случае структура, определяемая законом $\top$, изоморфна структуре факторгруппы G'/H'. [Для установлении необходимости условия показать сначала с помощью упражнения 2а § 6, что если закон $\top$ ассоциативен, то он определяет в G/H структуру группы; обозначая через K наибольшую нормальную подгруппу группы G', содержащуюся в H', показать далее, выписывая условие ассоциативности для $\top$, что $(r(X\top Y))^{-1}r(X)r(Y)\in K$ для всех X, Y; вывести отсюда, что отображение $X\to r(X)K$ есть изоморфизм группы G/H (относительно закона $\top$) на факторгруппу G'/K; учтя, что H' есть объединение классов по K, заключить, что $H'=K$.]

в) Обратно, пусть на множестве E задан всюду определенный внутренний закон $\top$ такой, что каждый левый перенос является взаимно однозначным отображением E на себя и существует $e\in E$ такое, что $x\top e=x$ для всех $x\in E$. Пусть, далее, Γ — группа подстановок множества E, порожденная всеми левыми переносами γ_x, и Δ — подгруппа тех подстановок из Γ, которые оставляют e инвариантным. Показать, что каждому левому классу X по Δ соответствует однозначно определенный элемент $x\in E$ такой, что $\gamma_x\in X$; если положить $r(X)=\gamma_x$, то отображение $x\to\gamma_x$ есть изоморфизм множества E, наделенного законом $\top$, на множество Γ/Δ, наделенное законом $(X, Y)\to r(X)r(Y)\Delta$.

§ 8. Кольца и кольца с операторами

1. Кольца

Определение 1. *Структурой кольца* (или *кольцевой структурой*) *в множестве A называется алгебраическая структура, задаваемая двумя всюду определенными внутренними законами композиции, первый из которых есть закон коммутативной группы в A, а второй ассоциативен и двояко дистрибутивен относительно первого. Множество, наделенное кольцевой структурой, называют кольцом.*

Чаще всего коммутативный групповой закон в кольце A записывают *аддитивно*, а второй внутренний закон композиции —

мультипликативно. Предположения, относящиеся к сложению в A, выражаются тогда тождествами

$$x+(y+z)=(x+y)+z \quad \text{(ассоциативность)}, \tag{1}$$

$$x+y=y+x \quad \text{(коммутативность)}, \tag{2}$$

требованием существования нейтрального элемента, обозначаемого 0, так что тождественно

$$x+0=x, \tag{3}$$

и, наконец, требованием существования для каждого x элемента, *противоположного* x, обозначаемого $-x$, так что

$$x+(-x)=0. \tag{4}$$

Предположения же, относящиеся к умножению, выражаются тождествами

$$x(yz)=(xy)z \quad \text{(ассоциативность)}, \tag{5}$$

$$\left.\begin{aligned} x(y+z)&=xy+xz,\\ (y+z)x&=yx+zx \end{aligned}\right\} \quad \text{(двоякая дистрибутивность)}. \tag{6}$$

Если умножение в кольце A обладает нейтральным элементом, он называется *единичным элементом* или *единицей* кольца A и часто обозначается 1 (если это не может повлечь путаницы). Точно так же, говоря о *регулярных*, или *обратимых*, или *перестановочных*, или *центральных* элементах, или *центре* кольца A, имеют в виду регулярность, обратимость и т. д. относительно заданного в A умножения.

Закон, *противоположный* заданному в кольце A умножению, вместе со сложением также определяет в A структуру кольца; она называется *противоположной* первоначально заданной; два кольца с противоположными структурами называются *противоположными*.

Кольцо называют *коммутативным*, если его умножение коммутативно; такое кольцо совпадает со своим противоположным.

В кольце A сложение и два внешних закона, получающиеся путем *раздвоения* (§ 3, п° 2) умножения, определяют структуру *коммутативной группы с операторами*, причем областью операторов каждого из этих двух внешних законов служит само A; *левой* (соответственно *правой*) *гомотетией* кольца A, соответствующей любому его элементу a, называется эндоморфизм $x \to ax$ (соответственно $x \to xa$) аддитивной группы A.

Примеры колец. I. Кольцо рациональных целых чисел. Мы определили на множестве $\mathbf{Z}$ рациональных целых чисел сложение (§ 2, n° 5) и умножение (§ 2, n° 8); при этом сложение является законом коммутативной группы, а умножение двояко дистрибутивно относительно сложения; следовательно, $\mathbf{Z}$, наделенное этими двумя законами, есть кольцо; оно называется *кольцом рациональных целых чисел*. Очевидно, это кольцо коммутативно и имеет $+1$ своим единичным элементом.

II. °*Полиномы* вещественного переменного с вещественными (или же целыми) коэффициентами образуют коммутативное кольцо, имеющее своим единичным элементом постоянную 1 (см. главу IV). Более общим образом, вещественные функции вещественного переменного образуют коммутативное кольцо, имеющее постоянную 1 своим единичным элементом.°

III. В любой (аддитивно записываемой) коммутативной группе G можно определить структуру коммутативного кольца, приняв за умножение закон $(x, y) \to 0$, который ассоциативен, коммутативен и дистрибутивен относительно сложения. Можно также сказать, что это умножение определено условием $GG = \{0\}$; кольца, удовлетворяющие этому условию, называются кольцами *с нулевым квадратом*; такое кольцо, если только оно не сводится к одному нулю, очевидно, не имеет единичного элемента.

IV. Кольцо эндоморфизмов коммутативной группы. Пусть G — аддитивно записываемая коммутативная группа. Множество G^G всех ее отображений в себя наделено двумя ассоциативными законами композиции: с одной стороны, законом $(f, g) \to f + g$ (напомним, что $h = f + g$ есть отображение G в G такое, что $h(x) = f(x) + g(x)$ для всех $x \in G$), определяющим в G^G структуру *коммутативной группы* (§ 6, n° 5), и, с другой стороны, законом $(f, g) \to f \circ g$, который мы будем обозначать здесь $f \cdot g$. Множество E всех *эндоморфизмов* группы G есть *подгруппа* коммутативной группы G^G; действительно, если f и g — эндоморфизмы и $h = f - g$, то $h(x + y) = f(x + y) - g(x + y) = f(x) + f(y) - (g(x) + g(y)) = (f(x) - g(x)) + (f(y) - g(y)) = h(x) + h(y)$, так что h — эндоморфизм. Очевидно, при этом E *устойчиво* относительно закона $(f, g) \to f \cdot g$; наконец, закон, индуцируемый на E этим последним законом, *двояко дистрибутивен* относительно закона $(f, g) \to f + g$; действительно, если $\varphi = (g + h) \cdot f$, то $\varphi(x) =$

$= g(f(x)) + h(f(x))$, так что $\varphi = g \cdot f + h \cdot f$; с другой стороны, если $\psi = f \cdot (g + h)$, то $\psi(x) = f(g(x) + h(x)) = f(g(x)) + f(h(x))$ (поскольку f — эндоморфизм), и значит, $\psi = f \cdot g + f \cdot h$.

Таким образом, структура, индуцированная в E рассмотренными двумя законами, есть структура кольца; наделенное этой структурой, E называется *кольцом эндоморфизмов* группы G. Кольцо эндоморфизмов коммутативной группы G всегда обладает единицей, а именно тождественным отображением G на себя; но оно, вообще говоря, не коммутативно (см. упражнение 2).

Кольца, определенные описанным способом, играют в алгебре важную роль (см. главы II и VIII).

Заметим, что кольцо эндоморфизмов коммутативной группы $\mathbf{Z}$ изоморфно кольцу $\mathbf{Z}$ рациональных целых чисел (§ 2, n° 8).

2. Кольца с операторами

Определение 2. *Кольцом с операторами называют множество A, наделенное структурой кольца и одним или несколькими внешними законами композиции, дистрибутивными относительно сложения в A и такими, что для любого из них, если записывать его в виде $(\alpha, x) \to \alpha x$, тождественно*

$$\alpha(xy) = (\alpha x)\, y = x\, (\alpha y). \tag{7}$$

Внешние законы композиции кольца с операторами A вместе с двумя внешними законами, получающимися путем раздвоения заданного в A умножения, определяют в A (вместе со сложением в качестве внутреннего закона) структуру *коммутативной группы с операторами*; условие (7) выражает, что внешние законы кольца A *перестановочны* (§ 5, n° 3) с каждым из двух внешних законов, получающихся путем раздвоения умножения.

Эндоморфизмы $x \to \alpha x$ структуры *аддитивной группы* (без операторов) в A, порождаемые операторами α кольца A, часто называются его *внешними гомотетиями*; таким образом, они перестановочны (в кольце эндоморфизмов аддитивной группы A) с левыми и правыми гомотетиями кольца A; можно также сказать, что это есть эндоморфизмы структуры *группы с операторами* в A, определяемой сложением и двумя внешними законами, получающимися путем раздвоения умножения.

Пример. Если A — кольцо и K — подмножество его *центра*, то закон композиции $(a, x) \to ax$ операторов $a \in K$ и элементов $x \in A$ определяет в A (вместе с заданной в A структурой кольца) структуру

кольца с операторами; свойства этой структуры существенно зависят от рассматриваемого множества K, и следует тщательно отличать друг от друга различные структуры кольца с операторами, которые могут быть получены таким способом (см. главы II и VIII).

Закон, *противоположный* заданному в кольце с операторами A умножению, как вытекает из (7), вместе со сложением и заданными на A внешними законами также определяет в A структуру кольца с операторами; она называется *противоположной* первоначально заданной; кольцо с операторами, получающееся при наделении A этой структурой, называется *противоположным* кольцу A.

В соответствии с общими обозначениями (§ 2, n° 7), в произвольном кольце A через $n \cdot x$ или nx, где $n \in \mathbf{Z}$ и $x \in A$, обозначают обычно сумму последовательности из n членов, равных x, если $n > 0$, элемент 0, если $n = 0$, и элемент $-((-n) \cdot x)$, если $n < 0$. Этим определяется внешний закон композиции рациональных целых чисел и элементов из A (который не следует смешивать с умножением в A); этот закон дистрибутивен относительно сложения и, в силу двоякой дистрибутивности умножения в A относительно сложения, удовлетворяет тождествам (7); тем самым он определяет в A вместе с заданными там сложением и умножением структуру *кольца с операторами*. Но эта структура по сути ничем не отличается от заданной в A кольцевой структуры, ибо все относящиеся к алгебраическим структурам основные понятия, определенные в § 4 (устойчивые множества, согласующиеся со структурой, отношения эквивалентности, гомоморфизмы), одинаковы для обеих структур.

Более общим образом, структуру кольца с операторами не отличают от получающейся путем присоединения к ее внешним законам еще внешнего закона $(n, x) \to nx$.

Это замечание позволяет рассматривать кольца без операторов как частные случаи колец с операторами; поэтому во всей оставшейся части настоящего параграфа будут рассматриваться только эти последние. Там, где не будет опасности путаницы, мы будем, допуская вольность речи, употреблять термин «кольцо» в смысле «кольцо с операторами»; в тех же случаях, где утверждаемый результат справедлив лишь для колец *без операторов* (или, что

то же, для колец с операторами, единственным внешним законом которых является $(n, x) \to nx$), это будет специально отмечаться.

3. *Делители нуля. Кольца целостности*

Пусть A — кольцо. Обобщая терминологию, употребляемую в случае натуральных чисел (Теор. мн., гл. III), элемент $a \in A$ называют *левым* (соответственно *правым*) *кратным элемента* $b \in A$, если существует $c \in A$ такое, что $a = cb$ (соответственно $a = bc$); при этом говорят также, что b есть *правый* (соответственно *левый*) *делитель* элемента a или что a *делится слева* (соответственно *справа*) на b.

Если A коммутативно, то, поскольку порядок следования множителей безразличен, говорят просто «кратное» и «делитель».

Заметим, что если в A нет единицы, элемент $a \in A$ не обязательно является делителем (правым или левым) самого себя, как это показывает пример кольца с нулевым квадратом (пример III). Точно так же, если A не содержит единицы, то nx, где $n \in \mathbf{Z}$, не будет вообще кратным x. Напротив, если A обладает единицей e, то $n \cdot x = n \cdot ex = (ne)\, x = x\,(ne)$.

Для каждого элемента x кольца A имеем $x^2 = x(x + 0) = x^2 + x0$, откуда $x0 = 0$; точно так же и $0x = 0$: всякое (левое или правое) кратное элемента 0 равно 0. Следовательно, каковы бы ни были x и y, имеем $(-x)\,y = x\,(-y) = -(xy)$, ибо $(-x)\,y + xy = (-x + x)\,y = 0y = 0$; отсюда $(-x)\,(-y) = xy$. С помощью индукции по целому $n > 0$ заключаем, что $(-x)^n = x^n$, если n четно, и $(-x)^n = -x^n$, если n нечетно.

Отношение $x0 = 0$ показывает также, что если кольцо A не сводится к 0 и обладает единицей e, то $e \neq 0$.

В соответствии с введенной выше терминологией каждый элемент $x \in A$ должен был бы рассматриваться как (правый и левый) делитель нуля; но, допуская вольность речи, наименование *левый* (соответственно *правый*) *делитель нуля* сохраняют за 0 и каждым элементом a, *отличным от* 0, для которого существует b, *отличное* от 0, удовлетворяющее соотношению $ab = 0$ (соответственно $ba = 0$). Можно еще сказать, что левые и правые делители нуля — это *не регулярные* элементы (§ 2, n° 2) кольца A (если только A не сводится к одному элементу 0); действительно,

отношение $ax = ay$ (соответственно $xa = ya$) равносильно отношению $a(x-y) = 0$ (соответственно $(x-y)a = 0$). Элемент $a \in A$ называют *нильпотентным*, если существует целое $n > 0$, для которого $a^n = 0$; взяв наименьшее целое n, обладающее этим свойством, убеждаемся в том, что тогда a — делитель нуля в A. Если в A нет делителей нуля, отличных 0, то, допуская вольность речи, A называют *кольцом без делителей нуля*.

В кольце без делителей нуля отношение $ab = 0$ равносильно «$a = 0$ или $b = 0$»; отношение $a^n = 0$ (где n — целое > 0) равносильно $a = 0$.

Определение 3. *Кольцом целостности называется* коммутативное *кольцо без делителей нуля, не сводящееся к* 0.

Примеры. 1) Кольцо $\mathbf{Z}$ рациональных целых чисел есть кольцо целостности; напротив, кольцо эндоморфизмов произвольной коммутативной группы, вообще говоря, содержит делители нуля, отличные от 0 (см. упражнение 2).

2) В кольце с нулевым квадратом (пример III) каждый элемент есть делитель нуля.

4. Подкольца

Определение 4. *Подкольцом кольца (с операторами) A называется всякое непустое множество $B \subset A$, в котором структура, индуцированная из A, есть структура кольца с операторами.*

Предложение 1. *Для того чтобы непустое множество B элементов кольца A было подкольцом этого кольца, необходимо и достаточно, чтобы B было подгруппой аддитивной группы A, устойчивой относительно умножения и заданных на A внешних законов.*

Справедливость предложения непосредственно вытекает из определений.

Условия, которым должно подчиняться непустое множество $B \subset A$, чтобы быть подкольцом, записываются также следующим образом (§ 6, предложение 1): $B + B \subset B$, $-B \subset B$, $BB \subset B$ и $\alpha B \subset B$ для каждого оператора α на A. Первые три из этих условий необходимы и достаточны для того, чтобы имеющаяся в A структура кольца (без операторов) индуцировала в B структуру кольца, иными словами, чтобы B было подкольцом в A, рассматриваемом как кольцо без операторов (т. е. наделенном своей структурой кольца, но не наделенном внешними законами).

Примеры. 1) Каждая подгруппа аддитивной группы $\mathbf{Z}$, имея вид $n\mathbf{Z}$, где $n \in \mathbf{N}$, есть подкольцо кольца $\mathbf{Z}$; таким образом, подкольца кольца $\mathbf{Z}$ совпадают с подгруппами его аддитивной группы. Ни одно из этих подколец, кроме самого $\mathbf{Z}$ и $\{0\}$, не обладает единичным элементом.

°2) Рассмотрим в теле $\mathbf{C}$ комплексных чисел структуру кольца с операторами, определяемую внешним законом композиции $(\alpha, z) \to \alpha z$ вещественных операторов α и комплексных чисел z (см. n° 2). При этой структуре единственным подкольцом кольца $\mathbf{C}$, отличным от $\{0\}$ и $\mathbf{C}$, является множество $\mathbf{R}$ вещественных чисел. Действительно, если подкольцо A кольца $\mathbf{C}$ содержит не вещественное число z, то оно содержит также z^2, а значит, и комплексные числа $\alpha z + \beta z^2$, где α и β принимают всевозможные вещественные значения; но так как отношение z^2/z не вещественно, получаемое так множество совпадает с $\mathbf{C}$. Таким образом, множество $\mathbf{Z}$ рациональных целых чисел не является подкольцом кольца с операторами $\mathbf{C}$, хотя и является подкольцом в $\mathbf{C}$, рассматриваемом как кольцо без операторов.

Замечание. Этот последний пример показывает, что понятие подкольца кольца с операторами A существенно зависит от внешних законов заданной в A структуры, а не только от его структуры кольца. Очевидно, подкольцо кольца с операторами A останется таковым также при *сужении* заданных на A внешних законов на подмножества областей их операторов или же при сохранении только некоторых из этих законов и отбрасывании других; но обратное неверно. Однако наличие или отсутствие внешнего закона $(n, x) \to nx$ $(n \in \mathbf{Z})$ в заданной структуре кольца с операторами не отражается на понятии подкольца относительно этой структуры; это объясняется тем, что всякая подгруппа аддитивной группы A *устойчива* относительно этого закона.

Если в множестве A рассматриваются несколько структур кольца с операторами, в основе которых лежит одна и та же кольцевая структура, то подкольца относительно этих структур различаются посредством указания тех внешних законов, относительно которых они *устойчивы*.

Всякое пересечение подколец кольца A есть снова подкольцо этого кольца; поэтому можно определить подкольцо, *порожденное* произвольным множеством $X \subset A$, как наименьшее подкольцо, содержащее X.

Предложение 2. *Множество всех элементов кольца A, перестановочных с каждым элементом произвольного фиксированного множества $M \subset A$, есть подкольцо этого кольца.*

Действительно, это множество устойчиво относительно умножения (§ 1, предложение 1); оно устойчиво относительно каждого из заданных на A внешних законов, ибо если x перестановочно с $z \in M$, то, в силу (7), для каждого оператора α кольца A имеем $(\alpha x)\, z = \alpha\,(xz) = \alpha\,(zx) = z\,(\alpha x)$. Наконец, если x и y перестановочны с $z \in M$, то $x - y$ перестановочно с z, ибо $(x-y)\, z = xz - yz = zx - zy = z\,(x-y)$.

Следствие 1. *Центр кольца A есть подкольцо этого кольца.*

Следствие 2. *Множество всех эндоморфизмов коммутативной группы с операторами G есть подкольцо кольца E всех эндоморфизмов группы G.*

Действительно, эти эндоморфизмы совпадают с эндоморфизмами *групповой* структуры в G, перестановочными со всеми заданными на G гомотетиями. Подкольцо кольца E, образованное этими эндоморфизмами, называется *кольцом эндоморфизмов* группы с операторами G.

5. *Отношения эквивалентности в кольце. Идеалы. Факторкольца*

Определим отношения эквивалентности, согласующиеся со структурой кольца A. По теореме 4 § 6, отношение R, согласующееся со сложением и заданными на A внешними законами, имеет вид $x - y \in H$, где H — подгруппа аддитивной группы A, *устойчивая* относительно этих внешних законов. Согласованность отношения R с умножением выражается порознь согласованностью слева и справа (§ 4, предложение 1). Но согласованность слева означает, что $x \equiv y \pmod R$ влечет $zx \equiv zy \pmod R$, т. е. $x - y \in H$ влечет $zx - zy = z\,(x-y) \in H$ для каждого $z \in A$. Это приводит к следующему определению:

Определение 5. *Левым* (соответственно *правым*) *идеалом кольца A называют всякую подгруппу H аддитивной группы A, устойчивую относительно заданных на A внешних законов и такую, что $zH \subset H$* (соответственно $Hz \subset H$) *для всех $z \in A$. Подмножество кольца A, являющееся в A одновременно и левым и правым идеалом, называется двухсторонним идеалом кольца A.*

Таким образом, условия, которым должно подчиняться непустое множество H элементов кольца A, чтобы быть его левым (соответственно правым) идеалом, записываются так: $H+H \subset H$, $-H \subset H$, $AH \subset H$ (соответственно $HA \subset H$) и $\alpha H \subset H$ для каждого заданного на A оператора α. Очевидно, каждый идеал кольца A является его подкольцом, обратное же неверно. Идеалы кольца обычно обозначаются строчными готическими буквами.

Каждый левый идеал кольца A есть правый идеал противоположного кольца, и обратно. Если A коммутативно, три рода идеалов совпадают и говорят просто об *идеалах* кольца A.

Замечания. 1) Левый идеал кольца A есть не что иное, как подгруппа аддитивной группы A, *устойчивая* относительно внешних законов кольца A и левого внешнего закона, порождаемого заданным на A умножением.

2) Как и понятие подкольца, понятие идеала кольца с операторами A существенно зависит от заданных на A внешних законов; замечания, сделанные в n° 4 по поводу подколец, равным образом применимы и к идеалам. В частности, если в множестве A рассматривается несколько структур кольца с операторами, в основе которых лежит одна и та же кольцевая структура, идеалы относительно этих структур различают посредством указания, относительно каких внешних законов они *устойчивы*.

Теорема 1. *Всякое отношение эквивалентности, согласующееся со структурой кольца A, имеет вид $x - y \in \mathfrak{a}$, где $\mathfrak{a}$ — двусторонний идеал кольца A, и результат факторизации A по этому отношению есть кольцо.*

Первое утверждение теоремы вытекает из сказанного ранее. С другой стороны, факторзакон заданного на A сложения по рассматриваемому отношению эквивалентности R есть закон коммутативной группы на A/R, а факторзаконы заданных на A внешних законов дистрибутивны относительно этого группового закона (§ 6, n° 11); наконец, факторзакон по R заданного на A умножения есть ассоциативный закон на A/R (§ 4, n° 3), двояко дистрибутивный относительно факторзакона сложения (§ 5, n° 1), и легко видеть, что он удовлетворяет тождествам (7).

Отношение эквивалентности $x - y \in \mathfrak{a}$, определяемое в кольце A двусторонним идеалом $\mathfrak{a}$, часто записывают $x \equiv y \pmod{\mathfrak{a}}$ или $x \equiv y\ (\mathfrak{a})$ и называют *сравнением по модулю* $\mathfrak{a}$. Таким обра-

зом, отношения $x \equiv y$ (a), $x' \equiv y'$ (a) влекут $x + x' \equiv y + y'$ (a), $-x \equiv -y$ (a), $xx' \equiv yy'$ (a) и $\alpha x \equiv \alpha y$ (a) для каждого оператора α (*правила действий над сравнениями*).

Отметим, что, напротив, отношение $xy \equiv xz$ (a) *не обязательно влечет* $y \equiv z$ (a), ибо класс $\bmod \mathfrak{a}$ элемента x, даже если этот элемент регулярен относительно заданного на A умножения, не обязательно регулярен относительно факторзакона (см. ниже пример 4).

Определение 6. *Результат факторизации кольца A по сравнению по двустороннему идеалу $\mathfrak{a}$ называется факторкольцом кольца A по $\mathfrak{a}$ и обозначается $A/\mathfrak{a}$.*

Примеры идеалов и факторколец. 1) Кольцо A всегда является своим двусторонним идеалом. Точно так же множество, сводящееся к одному элементу 0, есть двусторонний идеал кольца A; он называется *нулевым идеалом* и обозначается (0). Факторкольцо $A/(0)$ изоморфно A; факторкольцо A/A сводится к 0.

2) Каков бы ни был элемент a кольца A, множество Aa (соответственно aA) есть левый (соответственно правый) идеал этого кольца; заметим, что, если A не обладает единицей, этот идеал не обязательно содержит a.

3) Пусть M — произвольное множество элементов кольца A. Множество тех элементов $x \in A$, для которых $xy = 0$ (соответственно $yx = 0$), каково бы ни было $y \in M$, есть левый (соответственно правый) идеал кольца A; он называется *левым* (соответственно *правым*) *аннуляторомм* множества M. Если A не обладает делителями нуля, а M содержит элемент $\neq 0$, аннуляторы M сводятся к нулевому идеалу.

4) Идеалы кольца $\mathbf{Z}$ рациональных целых чисел, являясь подгруппами аддитивной группы $\mathbf{Z}$, имеют вид $n\mathbf{Z}$, где $n \in \mathbf{N}$; но и, обратно, очевидно, каждое множество такого вида есть идеал кольца $\mathbf{Z}$; иными словами, идеалы кольца $\mathbf{Z}$ совпадают с подгруппами аддитивной группы $\mathbf{Z}$; идеал $n\mathbf{Z}$ обозначается также (n). При $n > 0$ факторкольцо $\mathbf{Z}/(n)$ есть конечное коммутативное кольцо, состоящее из n элементов, внутренними законами которого являются сложение и умножение по модулю n (§ 4, n° 3); заметим, что, вообще говоря, оно обладает делителями нуля: например, $2 \not\equiv 0 \pmod 4$, но $2 \cdot 2 \equiv 0 \pmod 4$, так что класс числа 2 $(\bmod 4)$ есть делитель нуля в кольце $\mathbf{Z}/(4)$.

6. *Свойства идеалов*

В этом и следующем n°n° рассматриваются только левые идеалы; соответствующие предложения для правых и двусторонних идеалов предоставляем сформулировать читателю.

Если A — кольцо и $\mathfrak{a}$ — его левый идеал, а B — подкольцо, то $B \cap \mathfrak{a}$ есть левый идеал кольца B. В частности, если $\mathfrak{a} \subset B$, то $\mathfrak{a}$ есть левый идеал в B; но, обратно, левый идеал *в* B не обязательно является левым идеалом *в* A.

Так как левые идеалы кольца A совпадают с устойчивыми подгруппами относительно структуры группы с операторами A, то на них распространяются все свойства устойчивых подгрупп группы с операторами (§ 6, n° 10). Так, пересечение семейства $(\mathfrak{a}_\iota)$ левых идеалов есть левый идеал; среди левых идеалов, содержащих заданное множество $M \subset A$, существует наименьший; он называется левым идеалом, *порожденным* множеством M, а M — *системой образующих* этого идеала.

В частности, в кольце A, *обладающем единицей* e, левый идеал, порожденный множеством, сводящимся к одному элементу a, есть множество Aa всех элементов вида xa, где x пробегает A; действительно, это множество является левым идеалом, содержит $a = ea$ и содержится в каждом левом идеале, содержащем a. Если при этом A *коммутативно*, идеал $Aa = aA$, порожденный элементом a, обозначается (a) и называется *главным идеалом*.

Мы видели выше, что в кольце $\mathbf{Z}$ *каждый идеал — главный*.

Предложение 3. *Левый идеал кольца* A, *порожденный объединением семейства* $(\mathfrak{a}_\iota)_{\iota \in I}$ *левых идеалов этого кольца, есть множество всевозможных сумм вида* $\sum_{\iota \in H} x_\iota$, *где* $x_\iota \in \mathfrak{a}_\iota$, *а* H — *конечные подмножества множества индексов* I.

Как легко видеть, множество всех сумм $\sum_{\iota \in H} x_\iota$ есть *подгруппа* аддитивной группы A, порожденная объединением идеалов $\mathfrak{a}_\iota$; действительно, достаточно заметить, что если $x = \sum_{\iota \in H} x_\iota$ и $y = \sum_{\iota \in K} y_\iota$ — две такие суммы, то, положив $x_\iota = 0$ при $\iota \notin H$ и $y = 0$ при $\iota \notin K$, можно написать $x = \sum_{\iota \in H \cup K} x_\iota$, $y = \sum_{\iota \in H \cup K} y_\iota$, а тогда $x + y = \sum_{\iota \in H \cup K} (x_\iota + y_\iota)$, где $x_\iota + y_\iota \in \mathfrak{a}_\iota$. С другой стороны, для каждого $z \in A$ имеем $z\left(\sum_{\iota \in H} x_\iota\right) = \sum_{\iota \in H} z x_\iota$, где $z x_\iota \in \mathfrak{a}_\iota$.

Наконец, для каждого оператора α на A таким же образом имеем $\alpha\left(\sum_{\iota\in H} x_\iota\right) = \sum_{\iota\in H} \alpha x_\iota$, где $\alpha x_\iota \in \mathfrak{a}_\iota$.

Следствие. *Наименьшим левым идеалом, содержащим конечное число левых идеалов* $\mathfrak{a}_i$ $(1 \leqslant i \leqslant n)$, *служит их сумма* $\sum_{i=1}^{n} \mathfrak{a}_i$.

По аналогии также левый идеал, порожденный объединением бесконечного семейства $(\mathfrak{a}_\iota)_{\iota\in I}$ левых идеалов кольца A, называют *суммой* этого семейства и обозначают $\sum_{\iota\in I} \mathfrak{a}_\iota$ (см. главу II, § 1).

Ясно, что левый идеал кольца A, порожденный *произвольным* множеством $M \subset A$, содержит левые идеалы $\mathfrak{a}_x$, порожденные любыми элементами $x \in M$, и, таким образом, совпадает с *суммой* $\sum_{x\in M} \mathfrak{a}_x$. В частности:

Предложение 4. *В кольце* A, *обладающем единицей, левый идеал, порожденный непустым множеством* $M \subset A$, *совпадает с множеством всех сумм вида* $\sum_i x_i a_i$, *где* (a_i) — *произвольные конечные семейства элементов из* M, *а* x_i — *произвольные элементы из* A.

Пример. Идеал кольца $\mathbf{Z}$, порожденный множеством, состоящим из двух элементов m и n, есть сумма $(m)+(n)$ главных идеалов, порожденных каждым из этих элементов; как всякий идеал кольца $\mathbf{Z}$, он совпадает с некоторым главным идеалом (d) $(d \in \mathbf{N})$. Но для того, чтобы главный идеал (a) содержал m, необходимо и достаточно, чтобы a было *делителем* m. Мы видим таким образом, что все общие делители рациональных целых m и n являются делителями одного и того же $d \in \mathbf{N}$, которое само есть общий делитель m и n. Следовательно, d — *наибольший* из общих делителей $\geqslant 0$ чисел m и n; поэтому его называют *наибольшим общим делителем* (сокращенно: н. о. д.) m и n, и мы видим вместе с тем, что существуют (положительные или отрицательные) целые p и q такие, что $d = pm + qn$.

Заметим, кстати, что наибольший идеал, содержащийся в идеалах (m) и (n), т. е. их пересечение $(m) \cap (n)$, также совпадает с некоторым главным идеалом (r) $(r \in \mathbf{N})$; аналогичное рассуждение доказывает, что каждое общее кратное рациональных целых m и n кратно r и что r — *наименьшее* из общих кратных $\geqslant 0$ чисел m и n; его называют *наименьшим общим кратным* (н. о. к.) m и n.

Эти рассмотрения легко обобщаются на любое конечное число рациональных целых чисел (см. главу VI).

7. Максимальные идеалы

Определение 7. *Максимальным левым идеалом кольца A называется каждый максимальный элемент упорядоченного по включению множества всех левых идеалов кольца A, отличных от A.*

Пример. Максимальный идеал кольца $\mathbf{Z}$ — это главный идеал (p), где $p > 1$ есть целое число, не обладающее *никаким делителем* q, удовлетворяющим неравенствам $1 < q < p$; такое число называют *простым*; так, например, числа 2, 3, 5, 7 — простые.

Каждое целое $n > 1$ обладает простым делителем, ибо наименьший из делителей $\neq 1$ числа n очевидно простой.

Можно также сказать, что в $\mathbf{Z}$ каждый идеал $(n) \neq \mathbf{Z}$ содержится в максимальном идеале; в такой форме это предложеняе является частным случаем следующей общей теоремы:

Теорема 2 (Круль). *В кольце A с единицей каждый левый идеал, отличный от A, содержится в максимальном левом идеале.*

В силу теоремы Цорна (Теор. мн., Рез., § 6, n° 10) достаточно доказать, что множество $\mathfrak{F}$ всех левых идеалов $\neq A$, упорядоченное по включению, индуктивно, т. е., каково бы ни было *совершенно упорядоченное* множество $\mathfrak{G} \subset \mathfrak{F}$, *объединение* $\mathfrak{m}$ всех входящих в него идеалов есть левый идеал $\neq A$. Но так как никакой идеал из $\mathfrak{G}$ не содержит единицы e кольца A, то $e \notin \mathfrak{m}$; с другой стороны, так как каждое $x \in \mathfrak{m}$ принадлежит некоторому $\mathfrak{a} \in \mathfrak{G}$, то $zx \in \mathfrak{a} \subset \mathfrak{m}$ и $\alpha x \in \mathfrak{a} \subset \mathfrak{m}$ для каждого $z \in A$ и каждого оператора α на A; наконец, для любых двух элементов x и y из $\mathfrak{m}$ существуют идеалы $\mathfrak{a}$, $\mathfrak{b}$, принадлежащие $\mathfrak{G}$ и такие, что $x \in \mathfrak{a}$ и $y \in \mathfrak{b}$; так как один из этих идеалов содержит другой, то $x - y$ принадлежит одному из идеалов $\mathfrak{a}$, $\mathfrak{b}$ и, следовательно, идеалу $\mathfrak{m}$.

Замечание. Теорема 2 уже не всегда будет верна, если не предполагать, что A обладает единицей (см. упражнение 14б).

8. Гомоморфизмы колец

Общие определения § 4 (n° 4) позволяют определить *представление* кольца A в множество A', наделенное структурой, *гомологичной* структуре, заданной в A (§ 4, n° 1); это означает здесь, что заданная в A' структура определяется, с одной стороны, двумя внутренними законами, сопоставляемыми соответственно задан-

ными на A сложению и умножению, и, с другой стороны, внешними законами, взаимно однозначно сопоставляемыми внешним законам кольца A так, что соответственные законы имеют одну и ту же область операторов. В этих условиях (при одинаковом обозначении соответственных законов) введем

Определение 8. *Отображение f кольца A в множество A', наделенное гомологичной структурой, называется представлением* (или *гомоморфизмом*) *A в A', если, каковы бы ни были элементы $x \in A$, $y \in A$ и оператор α кольца A, композиции $f(x) + f(y)$, $f(x)f(y)$ и $\alpha f(x)$ определены, причем $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, $f(\alpha x) = \alpha f(x)$.*

Каноническое отображение кольца A на его факторкольцо есть гомоморфизм, называемый *каноническим*.

В соединении с доказанной выше теоремой 1 теорема о гомоморфизмах (§ 4, теорема 1) дает для колец следующий результат:

Теорема 3. *Пусть f — представление кольца A в множество A', наделенное гомологичной структурой. Тогда $f(A)$ — кольцо* (при индуцированной из A' структуре), *в котором $f(0)$ есть нейтральный элемент относительно сложения* (также обозначаемый 0). *Прообраз $\mathfrak{a} = \overset{-1}{f}(0)$ этого нейтрального элемента есть двусторонний идеал кольца A; кольцо $f(A)$ изоморфно факторкольцу $A/\mathfrak{a}$, а представление f есть композиция канонического гомоморфизма A на $A/\mathfrak{a}$ и инъективного гомоморфизма $A/\mathfrak{a}$ в A'.*

Пример. Пусть A — кольцо без операторов, не сводящееся к 0 и обладающее единицей e; отображение $n \to ne$ есть представление кольца $\mathbf{Z}$ в A; следовательно, подкольцо кольца A, образованное элементами ne, изоморфно факторкольцу $\mathbf{Z}/(q)$, где q — некоторое целое $\geqslant 0$; q называется *характеристикой* кольца A (см. главу V, § 1); если $q > 0$, то его можно определить как наименьшее из целых чисел $m > 0$ таких, что $mx = 0$ для каждого $x \in A$. В частности, кольцо $\mathbf{Z}/(n)$ имеет характеристику n.

Предложение 5. *Если a — обратимый элемент кольца A, то отображение $x \to axa^{-1}$ есть автоморфизм этого кольца.*

Действительно, $a(x+y)a^{-1} = axa^{-1} + aya^{-1}$, $a(xy)a^{-1} = (axa^{-1})(aya^{-1})$, и для каждого оператора α кольца A, в силу (7),

$a(\alpha x)\,a^{-1} = \alpha\,(axa^{-1})$; с другой стороны, так как отношение $y = axa^{-1}$ равносильно отношению $x = a^{-1}ya$, то $x \longrightarrow axa^{-1}$ есть взаимно однозначное отображение A на себя. Его называют *внутренним автоморфизмом* кольца A.

9. Подкольца и идеалы факторкольца

Теорема 4. *Пусть f — канонический гомоморфизм кольца A на его факторкольцо $A' = A/\mathfrak{a}$ по двустороннему идеалу $\mathfrak{a}$.*

а) *Прообраз $B = \overset{-1}{f}(B')$ подкольца B' кольца A' есть подкольцо кольца A, содержащее $\mathfrak{a}$; при этом $B' = f(B)$ и кольцо B' изоморфно факторкольцу $B/\mathfrak{a}$.*

б) *Отношение $B = \overset{-1}{f}(B')$ устанавливает взаимно однозначное соответствие между подкольцами кольца A' и подкольцами кольца A, содержащими $\mathfrak{a}$.*

в) *Каково бы ни было подкольцо B кольца A, $B + \mathfrak{a}$ есть подкольцо кольца A, а $f(B)$ — подкольцо кольца A', изоморфное факторкольцам $B/(B \cap \mathfrak{a})$ и $(B + \mathfrak{a})/\mathfrak{a}$.*

Непосредственная проверка показывает, что если B' — подкольцо кольца A', то $B = \overset{-1}{f}(B')$ есть подкольцо кольца A и содержит $\mathfrak{a}$; так как f отображает A на A', то оно отображает B на B', и значит, согласно теореме 3, B' изоморфно $B/\mathfrak{a}$; тем самым а) доказано.

Обратно, если B — подкольцо кольца A, содержащее $\mathfrak{a}$, то B насыщено по сравнению $\bmod \mathfrak{a}$, значит, для $B' = f(B)$ имеем $B = \overset{-1}{f}(B')$, чем доказано б).

Установим, наконец, справедливость утверждения в). Каково бы ни было подкольцо B кольца A, сужение f на B есть представление B в A', причем прообразом нуля относительно этого представления является $B \cap \mathfrak{a}$; следовательно, согласно теореме 3, $f(B)$ изоморфно $B/(B \cap \mathfrak{a})$. Множество $B + \mathfrak{a}$ получается путем насыщения B по отношению $x \equiv y\ (\mathfrak{a})$; согласно второй теореме об изоморфизме (§ 4, теорема 3), оно устойчиво относительно умножения и внешних законов кольца A и, будучи подгруппой аддитивной группы A, является подкольцом кольца A; вторая теорема об изоморфизме показывает тогда, что $(B + \mathfrak{a})/\mathfrak{a}$ изоморфно $B/(B \cap \mathfrak{a})$.

Теорема 5. *Пусть* f — *канонический гомоморфизм кольца* A *на его факторкольцо* $A' = A/\mathfrak{a}$ *по двустороннему идеалу* $\mathfrak{a}$.

а) *Прообраз* $\mathfrak{b} = \overset{-1}{f}(\mathfrak{b}')$ *левого* (соответственно *правого*) *идеала* $\mathfrak{b}'$ *кольца* A' *есть левый* (соответственно *правый*) *идеал кольца* A, *содержащий* $\mathfrak{a}$, *причем* $\mathfrak{b}' = f(\mathfrak{b})$.

б) *Отношение* $\mathfrak{b} = \overset{-1}{f}(\mathfrak{b}')$ *устанавливает взаимно однозначное соответствие между левыми* (соответственно *правыми*) *идеалами кольца* A' *и левыми* (соответственно *правыми*) *идеалами кольца* A, *содержащими* $\mathfrak{a}$. *Для любых двух левых* (соответственно *правых*) *идеалов* $\mathfrak{b}'$ *и* $\mathfrak{c}'$ *кольца* A' *имеем*

$$\overset{-1}{f}(\mathfrak{b}' + \mathfrak{c}') = \overset{-1}{f}(\mathfrak{b}') + \overset{-1}{f}(\mathfrak{c}'), \quad \overset{-1}{f}(\mathfrak{b}' \cap \mathfrak{c}') = \overset{-1}{f}(\mathfrak{b}') \cap \overset{-1}{f}(\mathfrak{c}'). \tag{8}$$

в) *Если* $\mathfrak{b}'$ — *двусторонний идеал кольца* A', *то* $\mathfrak{b} = \overset{-1}{f}(\mathfrak{b}')$ — *двусторонний идеал кольца* A, *содержащий* $\mathfrak{a}$, *и* $A/\mathfrak{b}$ *изоморфно* $A'/\mathfrak{b}'$.

Непосредственная проверка показывает, что если $\mathfrak{b}'$ — левый (соответственно правый, двусторонний) идеал кольца A', то $\mathfrak{b} = \overset{-1}{f}(\mathfrak{b}')$ есть левый (соответственно правый, двусторонний) идеал кольца A, содержащий $\mathfrak{a}$; так как f отображает A на A', то оно отображает $\mathfrak{b}$ на $\mathfrak{b}'$, и а) доказано. Обратно, если $\mathfrak{b}$ — левый идеал кольца A, то $f(\mathfrak{b})$ — левый идеал кольца A', ибо если $x \in \mathfrak{b}$ и $z' \in A'$, то существует $z \in A$ такое, что $z' = f(z)$, и значит, $z'f(x) = f(z)f(x) = f(zx) \in f(\mathfrak{b})$; доказательство для правых идеалов аналогично. В частности, если $\mathfrak{b} \supset \mathfrak{a}$, то $\mathfrak{b}$ насыщено по сравнению mod $\mathfrak{a}$, так что для $\mathfrak{b}' = f(\mathfrak{b})$ имеем $\mathfrak{b} = \overset{-1}{f}(\mathfrak{b}')$, чем доказана первая часть утверждения б); соотношения же (8) выполняются для *произвольных* подмножеств $\mathfrak{b}'$ и $\mathfrak{c}'$ кольца A' (§ 6, n° 13).

Можно также заметить, что сумма двух идеалов есть их *верхняя грань* в множестве всех идеалов кольца A', упорядоченном по включению, а пересечение — *нижняя грань*; и то же в множестве всех идеалов кольца A, содержащих $\mathfrak{a}$; формулы (8) вытекают тогда из того, что взаимно однозначное отображение $\mathfrak{b}' \to \overset{-1}{f}(\mathfrak{b}')$ первого из этих множеств на второе — *возрастающее*.

Наконец, если $\mathfrak{b}'$ — двусторонний идеал кольца A и $\mathfrak{b} = f^{-1}(\mathfrak{b}')$, то изоморфизм $A/\mathfrak{b}$ и $A'/\mathfrak{b}'$ вытекает из первой теоремы об изоморфизме (§ 4, теорема 2).

Для подколец B кольца A, содержащих $\mathfrak{a}$, кольца $f(B)$ и $B/\mathfrak{a}$ обычно *отождествляются*; в частности, идеал $f(\mathfrak{b})$ кольца A', соответствующий идеалу $\mathfrak{b} \supset \mathfrak{a}$, обозначают $\mathfrak{b}/\mathfrak{a}$; поэтому в случае двустороннего идеала $\mathfrak{b}$ утверждение в) теоремы 5 выражают, говоря, что факторкольцо $(A/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ изоморфно $A/\mathfrak{b}$.

10. Произведения колец

Из замечаний, сделанных в n°5 § 4 и n°1 § 5, явствует, что произведение структур семейства (A_ι) гомологичных колец с операторами также есть структура кольца с операторами; это приводит к следующему определению:

Определение 9. *Произведением семейства $(A_\iota)_{\iota \in I}$ гомологичных колец с операторами называется множество $A = \prod_{\iota \in I} A_\iota$, наделенное структурой кольца с операторами, определяемой законами*

$$((x_\iota), (y_\iota)) \to (x_\iota + y_\iota), \quad ((x_\iota), (y_\iota)) \to (x_\iota y_\iota), \quad (\alpha, (x_\iota)) \to (\alpha x_\iota)$$

(где α пробегает все операторы колец A_ι).

Важным частным случаем произведений колец является кольцо, образованное всевозможными отображениями множества E в кольцо A, совпадающее с произведением A^E (см. § 4, n° 5).

Если B_ι — подкольцо (соответственно левый идеал, правый идеал) кольца A_ι, то $B = \prod_{\iota \in I} B_\iota$ есть подкольцо (соответственно левый идеал, правый идеал) кольца $A = \prod_{\iota \in I} A_\iota$. В частности, пусть J — непустое подмножество множества I, $K = \complement J$ и $B_\iota = A_\iota$ для $\iota \in J$, $B_\iota = \{0\}$ для $\iota \in K$; тогда подкольцо $A'_J = \prod_{\iota \in I} B_\iota$ есть двусторонний идеал в A, структура кольца (с операторами) которого изоморфна структуре кольца $A_J = \prod_{\iota \in J} A_\iota$; A'_J часто

отождествляют с A_J посредством *канонического* изоморфизма аддитивной группы A_J на аддитивную группу A'_J, являющегося также изоморфизмом кольцевых структур. Проекция pr_J кольца A на J есть гомоморфизм; прообраз нуля относительно этого гомоморфизма есть не что иное, как A'_K, так что A_J изоморфно A/A'_K, а A изоморфно произведению $A'_J \times (A/A'_J)$. Кроме того, по определению умножения в A, имеем $A'_J A'_K = \{0\}$: говорят, что подкольца A'_J и A'_K *взаимно аннулируются*. Отсюда следует, что каждый идеал *в* A'_J есть также идеал *в* A.

Вместе с тем мы видим, что каждое произведение колец, не сводящихся к 0, содержит *делители нуля*, отличные от 0.

В случае, когда J — множество $\{\iota\}$, состоящее из одного элемента, подкольцо A'_J, изоморфное A_ι, обозначается также A'_ι. Если $\mathfrak{a}$ — левый (соответственно правый) идеал в A, его проекция на A_ι есть левый (соответственно правый) идеал в A_ι (теорема 5); при этом:

Предложение 6. *Если произведение A колец A_ι обладает единицей* (т. е. каждое из колец A_ι обладает единицей), *то идеал $\mathfrak{a} \cap A'_\iota$ изоморфен проекции $\mathfrak{a}$ на A_ι; при этом в случае конечного множества индексов I $\mathfrak{a}$ совпадает с произведением своих проекций на кольца A_ι.*

Действительно, пусть $x = (x_\iota)$ — элемент из $\mathfrak{a}$, e_ι — единица кольца A_ι, e'_ι — единица кольца A'; $\mathfrak{a}$ содержит $e'_\iota x$, т. е. элемент, все координаты которого, за исключением координаты с индексом ι, равной x_ι, равны нулю; а отсюда сразу следует справедливость предложения.

Без предположения, что A содержит единицу, предложение становится неверным (см. упражнение 14в).

11. *Прямая композиция подколец*

Пусть $A = \prod_{1 \leqslant i \leqslant n} A_i$ — произведение *конечного* семейства подколец A_i; в обозначениях предыдущего n° аддитивная группа A есть *прямая сумма* (§ 6, n° 6) аддитивных групп A'_i (допуская вольность речи, это выражают, говоря, что *кольцо* A есть *прямая сумма подколец* A'_i). Но более того, если $x = \sum_{i=1}^{n} x_i$ и $y = \sum_{i=1}^{n} y_i$,

где $x_i \in A_i'$, $y_i \in A_i'$, — (однозначно определенные) разложения произвольных элементов x, y кольца A, то $xy = \sum_{i=1}^{n} x_i y_i$.

Определение 10. *Кольцо A называется прямой композицией конечного семейства $(B_i)_{1 \leqslant i \leqslant n}$ своих подколец, если A есть прямая сумма подколец B_i и тождественно*

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right) = \sum_{i=1}^{n} x_i y_i \quad (x_i \in B_i,\ y_i \in B_i).$$

Тем самым кольцо A, являющееся прямой композицией своих подколец, изоморфно их *произведению*.

Не следует смешивать понятия *прямой суммы* и *прямой композиции* подколец: кольцо вполне может быть прямой суммой своих подколец (и даже правых или левых идеалов), не будучи их прямой композицией; мы встретимся с примерами этого в главе II.

Предложение 7. *Пусть кольцо A есть прямая сумма конечного семейства $(B_i)_{1 \leqslant i \leqslant n}$ своих подколец. Следующие утверждения равносильны:*

а) *A есть прямая композиция подколец B_i;*

б) *B_i являются двусторонними идеалами кольца A;*

в) *B_i взаимно аннулируются.*

Действительно, а) влечет б), поскольку A изоморфно $\prod_{1 \leqslant i \leqslant n} B_i$; б) влечет в), ибо если B_i — двусторонние идеалы, то

$$B_i B_j \subset B_i \cap B_j = \{0\} \text{ при } i \neq j;$$

наконец, в) влечет а) в силу дистрибутивности умножения и определения 10.

Пример. Рассмотрим подкольцо A факторкольца $\mathbf{Z}/(6)$, образованное классами чисел 0 и 3 (mod 6), и подкольцо B, образованное классами чисел 0, 2 и 4 (mod 6); A изоморфно $\mathbf{Z}/(2)$, а B изоморфно $\mathbf{Z}/(3)$; $\mathbf{Z}/(6)$ есть прямая сумма подколец A и B, ибо $1 = 3 - 2$ и сравнения $u \equiv v$ (6), $u \equiv 0$ (2) и $v \equiv 0$ (3) могут одновременно выполняться лишь если $u \equiv v \equiv 0$ (6); наконец, очевидно A и B взаимно аннулируются; таким образом, $\mathbf{Z}/(6)$ есть прямая композиция своих подколец A и B и, следовательно, изоморфно произведению $(\mathbf{Z}/(2)) \times (\mathbf{Z}/(3))$ (см. главу VII).

Если кольцо A есть прямая композиция своих подколец B_i, то, вследствие изоморфизма прямой композиции произведению,

центр C кольца A есть прямая композиция центров C_i подколец B_i и $C_i = C \cap B_i$ (§ 4, n° 5).

Предложение 8. *Если кольцо* A *есть прямая композиция своих подколец* B_i $(1 \leqslant i \leqslant n)$, $\mathfrak{a}_i$ — *двусторонний идеал в* B_i *и* $\mathfrak{a} = \sum_{i=1}^{n} \mathfrak{a}_i$, *то факторкольцо* $A/\mathfrak{a}$ *изоморфно произведению факторколец* $B_i/\mathfrak{a}_i$.

Это — непосредственное следствие предложения 4 § 4.

Упражнения. 1) Определить все кольцевые структуры в множестве, состоящем из n элементов, где $2 \leqslant n \leqslant 5$, а также идеалы этих колец.

2) Показать, что кольцо эндоморфизмов коммутативной группы, являющейся произведением двух циклических групп второго порядка, некоммутативно и обладает делителями нуля, отличными от 0.

3) Пусть A — кольцо (без операторов) и на множестве $\mathbf{Z} \times A$ следующим образом определены сложение и умножение:

$$(m, x) + (n, y) = (m + n, x + y),$$
$$(m, x)(n, y) = (mn, my + nx + xy).$$

Показать, что эти законы определяют в $\mathbf{Z} \times A$ структуру кольца с единицей и что A изоморфно двустороннему идеалу этого кольца.

4) Пусть A — кольцо, не сводящееся к 0 и имеющее единицу e. Если для некоторого элемента $a \in A$ существует, и притом *единственный* элемент $a' \in A$ такой, что $aa' = e$, то a обратим и a' обратен a. [Показать сначала, что a не есть левый делитель нуля, а затем рассмотреть произведение $aa'a$.]

*5) Пусть A — кольцо без делителей нуля, имеющее единицу e. Предположим, что на A задан всюду определенный внутренний закон $\top$ такой, что порожденный им правый внешний закон дистрибутивен относительно сложения, а левый — относительно умножения.

а) Показать, что если A не есть кольцо характеристики 2, то $x \top y = 0$ для всех x и y из A. [Использовать упражнение 4 § 5.] *).

б) Если A имеет характеристику 2, а $x \top y = 0$ не для всякой пары (x, y) элементов из A, то множество G тех $u \in A$, для которых $u \top e = 0$, есть подгруппа индекса 2 аддитивной группы A и закон $\top$ опре-

*) В главе IV будет приведен пример кольца целостности с любой характеристикой, один из законов $\top$ на котором таков, что порожденный им правый внешний закон дистрибутивен одновременно относительно сложения и умножения, а $x \top y$ равно нулю лишь если $x = 0$ или $y = 0$.

деляется знанием всех композиций $a\,\mathsf{T}\,x$, где a — (произвольный) фиксированный элемент $\notin G$. Обратно, задание подгруппы G индекса 2 аддитивной группы A и отображении f A в себя такого, что $f(xy) = f(x)\,f(y)$, определяет закон T, обладающий указанными свойствами

6) Пусть A — кольцо с операторами, B — произвольное множество его элементов и B' — порожденное им в A множество, устойчивое относительно заданных на A внешних законов.

а) Пусть $B'' = B'^{\omega}$ — порожденное B' множество, устойчивое относительно умножения. Тогда подкольцо, порожденное множеством B, совпадает с подгруппой аддитивной группы A, порожденной множеством B''.

б) Левый идеал, порожденный множеством B, совпадает с подгруппой аддитивной группы, порожденной миожеством $B'+AB'$, а двусторонний идеал, порожденный множеством B, — с подгруппой аддитивной группы, порожденной множеством $B'+AB'+B'A+AB'A$.

*7) Пусть A — кольцо (без операторов), не содержащее делителей нуля и такое, что каждая его аддитивная подгруппа является левым идеалом. Показать, что A изоморфно подкольцу кольца $\mathbf{Z}$ или факторкольцу вида $\mathbf{Z}/(p)$, где p — простое. [Выразив, что аддитивная группа, порожденная элементом $a \neq 0$, является левым идеалом, показать, что этим определяется изоморфизм A в $\mathbf{Z}$ или в факторкольцо кольца $\mathbf{Z}$.]

8) Правый идеал, порожденный левым идеалом кольца, является двусторонним идеалом.

9) Правый аннулятор правого идеала кольца есть двусторонний идеал.

10) Двусторонний идеал кольца A, порожденный элементами $xy - yx$, где x и y пробегают A, есть наименьший из двусторонних идеалов $\mathfrak{a}$ таких, что $A/\mathfrak{a}$ коммутативно.

11) Пусть $(\mathfrak{a}_\alpha)$ — семейство двусторонних идеалов кольца A, для которого $\bigcap\limits_\alpha \mathfrak{a}_\alpha = \{0\}$. Показать, что A изоморфно подкольцу произведения $\prod\limits_\alpha (A/\mathfrak{a}_\alpha)$.

*12) Двусторонний идеал $\mathfrak{a}$ кольца A называется *неприводимым*, если не существует пары двусторонних идеалов $\mathfrak{b}$, $\mathfrak{c}$, отличных от $\mathfrak{a}$ и таких, что $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$.

а) Показать, что пересечение всех неприводимых идеалов кольца A сводится к 0. [Заметить, что множество всех двусторонних идеалов, не содержащих элемента $a \neq 0$, индуктивно, и применить теорему Цорна.]

б) Вывести отсюда, что каждый двусторонний идеал кольца A есть пересечение всех содержащих его неприводимых идеалов. [Использовать теорему 5.]

*13) Идеал $\mathfrak{p}$ коммутативного кольца A, отличный от A, называют *простым*, если факторкольцо $A/\mathfrak{p}$ есть кольцо целостности (иными словами, если отношения $x \notin \mathfrak{p}$, $y \notin \mathfrak{p}$ влекут $xy \notin \mathfrak{p}$).

а) Если A обладает единицей, то каждый максимальный идеал $\mathfrak{a}$ в A — простой. [Заметить, что в факторкольце $A/\mathfrak{a}$ идеал, порожденный любым ненулевым элементом, совпадает с $A/\mathfrak{a}$, и вывести отсюда, что каждый ненулевой элемент из $A/\mathfrak{a}$ обратим.]

б) Каждый простой идеал неприводим (упражнение 12).

в) Если множество $\mathfrak{F}$ всех простых идеалов, содержащих заданный идеал $\neq A$, не пусто (что всегда верно, когда A обладает единицей), то оно индуктивно по отношению $\supset$; если A обладает единицей, то $\mathfrak{F}$ индуктивно по отношению $\subset$.

г) Пусть $\mathfrak{a}$ — произвольный идеал $\neq A$ и $\mathfrak{b}$ — множество тех $x \in A$, у которых некоторая степень $x^n \in \mathfrak{a}$ (где n зависит от x). Показать, что $\mathfrak{b}$ — идеал и что, если $\mathfrak{b} \neq A$, пересечение всех простых идеалов, содержащих $\mathfrak{a}$, совпадает с $\mathfrak{b}$. [Заметить, что для $a \notin \mathfrak{b}$ множество всех идеалов, содержащих $\mathfrak{a}$, но не содержащих никакой степени a^n, индуктивно по отношению $\subset$, и доказать, что всякий максимальный элемент $\mathfrak{p}$ этого множества — простой.]

14) При структуре кольца с нулевым квадратом (n° 1, пример III), определенной в заданной коммутативной группе G, идеалы кольца G совпадают с подгруппами аддитивной группы G.

а) Примем за G аддитивную группу $\mathbf{Z}/(p)$ целых чисел по простому модулю p. Показать, что в кольце G с нулевым квадратом идеал (0) — максимальный, но не простой.

°б) Примем за G подгруппу аддитивной группы $\mathbf{Q}/\mathbf{Z}$ рациональных чисел по модулю 1, образованную классами (mod 1) рациональных чисел вида k/p^n, где k и n — произвольные целые $\geqslant 0$, а p — фиксированное простое число. Показать, что каждая подгруппа группы G имеет вид G_n, где G_n — множество всех классов (mod 1) чисел вида k/p^n с фиксированным $n \geqslant 0$ и произвольным k. Вывести отсюда, что в кольце G с нулевым квадратом не существует ни максимальных, ни простых идеалов.

в) Приняв за G аддитивную группу $\mathbf{Z}$ рациональных целых чисел, привести пример идеала в произведении $G \times G$ кольца G с нулевым квадратом на самого себя, который не совпадал бы с произведением своих проекций на кольца-сомножители.

15) Пусть A — кольцо с единицей e. Если оно является прямой суммой конечного числа своих левых идеалов $\mathfrak{l}_i$ $(1 \leqslant i \leqslant n)$ и $e = \sum_{i=1}^{n} e_i$ $(e_i \in \mathfrak{l}_i)$, то $e_i^2 = e_i$, $e_i e_j = 0$ при $i \neq j$ и $\mathfrak{l}_i = Ae_i$. [Записать, что $x = xe$ для каждого $x \in A$.] Обратно, если e_i $(1 \leqslant i \leqslant n)$ — n идемпотентов таких, что $e_i e_j = 0$ при $i \neq j$ и $e = \sum_{i=1}^{n} e_i$, то A есть

прямая сумма n левых идеалов Ae_i. Для того чтобы все эти идеалы Ae_i были двусторонними, необходимо и достаточно, чтобы все e_i принадлежали центру кольца A. [Использовать предложение 7.]

*16) Пусть e — идемпотент кольца A.

а) Показать, что A есть прямая сумма левого идеала $\mathfrak{a}=Ae$ и левого аннулятора $\mathfrak{b}$ элемента e. [Заметить, что, каково бы ни было $x\in A$, $x-xe\in\mathfrak{b}$.]

б) Каждый правый идеал $\mathfrak{d}$ кольца A есть прямая сумма $\mathfrak{d}\cap\mathfrak{a}$ (правого идеала подкольца $\mathfrak{a}$) и $\mathfrak{d}\cap\mathfrak{b}$ (правого идеала подкольца $\mathfrak{b}$).

в) Если $Ae=eA$, то e есть единичный элемент подкольца $\mathfrak{a}$, $\mathfrak{b}$ — двусторонний идеал кольца A и A — прямая композиция подколец $\mathfrak{a}$ и $\mathfrak{b}$; каждый левый (соответственно правый) идеал $\mathfrak{c}$ кольца A есть прямая сумма левых (соответственно правых) идеалов $\mathfrak{c}\cap\mathfrak{a}$ и $\mathfrak{c}\cap\mathfrak{b}$ этого кольца.

*17) Пусть A — кольцо с единицей e. Если центр C кольца A есть прямая композиция подколец C_i $(1\leqslant i\leqslant n)$, то A есть прямая композиции порожденных ими двусторонних идеалов $\mathfrak{a}_i$. [Для доказательства того, что A есть сумма идеалов $\mathfrak{a}_i$, воспользоваться тем, что каждое $x\in A$ представимо в виде $x=xe=\sum_{i=1}^{n} xe_i$, где e_i — единичный элемент подкольца C_i; чтобы убедиться в том, что эта сумма — прямая, показать, что, каково бы ни было $z\in\mathfrak{a}_i$, $ze_i=z$ и $ze_j=0$ для всех $j\neq i$].

*18) Кольцо без операторов A называют *булевским кольцом*, если каждый его элемент идемпотентен (иными словами, если $x^2=x$ для каждого $x\in A$).

а) Показать, что если для любых $A\subset E$, $B\subset E$ положить $AB=A\cap B$ и $A+B=(A\cap\complement B)\cup(B\cap\complement A)$, то этим в множестве $\mathfrak{P}(E)$ всех подмножеств множества E определится структура булевского кольца. Это кольцо изоморфно кольцу K^E всех отображений E в кольцо $K=\mathbf{Z}/(2)$ целых чисел по модулю 2. [Рассмотреть для каждого $X\subset E$ его «характеристическую функцию» φ_X, определяемую условиями $\varphi_X(x)=1$, если $x\in X$, и $\varphi_X(x)=0$, если $x\notin X$.]

б) Каждое булевское кольцо A коммутативно и имеет характеристику 2. [Записать, что $x+x$ — идемпотент, а затем, что $x+y$ — идемпотент.]

в) Булевское кольцо A без делителей нуля сводится к 0 или изоморфно $\mathbf{Z}/(2)$. [Показать, что $xy(x+y)=0$ для любых двух элементов x и y из A.] Вывести отсюда, что в булевском кольце каждый простой идеал (упражнение 13) — максимальный.

г) Каждый идеал $\mathfrak{a}$ булевского кольца A, отличный от A, есть пересечение содержащих его простых идеалов. [Применить упражнение 13г.] Вывести отсюда, что каждый неприводимый идеал кольца A (упражнение 12) — максимальный (тем самым для булевского кольца

понятия неприводимого идеала, простого идеала и максимального идеала совпадают).

д) Показать, что каждое булевское кольцо изоморфно подкольцу произведения K^E, где $K=\mathbf{Z}/(2)$. [Использовать г) и упражнение 11.]

е) Пусть $\mathfrak{p}_i$ $(1 \leqslant i \leqslant n)$ — n различных максимальных идеалов булевского кольца A и $\mathfrak{a}=\bigcap_{1\leqslant i\leqslant n}\mathfrak{p}_i$. Показать, что $A/\mathfrak{a}$ изоморфно K^n. [Индукцией по n, находя максимальные идеалы кольца K^n с помощью предложения 6.] Вывести отсюда, что каждое конечное булевское кольцо есть кольцо вида K^n.

ж) В булевском кольце A отношение $xy=x$ есть отношение порядка; будем обозначать его $x \leqslant y$ [§ 1, упражнение 15]; показать, что A — дистрибутивная решетка (Теор. мн., гл. III, § 1, упражнение 16), обладающая наименьшим элементом $\mathfrak{a}$, и что для каждой пары (x, y) ее элементов таких, что $x \leqslant y$, существует элемент $d(x, y)$, для которого $\inf(x, d(x, y))=\mathfrak{a}$, $\sup(x, d(x, y))=y$. Обратно, показать, что если дистрибутивная решетка A обладает указанными свойствами, то законы композиции $xy=\inf(x, y)$ и $x+y=d(\inf(x, y), \sup(x, y))$ определяют в A структуру булевского кольца.

19) *Кольцоидом* называется множество E, наделенное двумя внутренними законами композиции: а) всюду определенным ассоциативным умножением xy; б) аддитивно записываемым *не всюду определенным* законом, удовлетворяющим следующим условиям:

1° он *коммутативен* (иными словами, если $x+y$ определено, то определено также $y+x$, и $x+y=y+x$; мы будем в этом случае говорить, что x и y *суммируемы*);

2° если x и y суммируемы, то для того, чтобы $x+y$ и z были суммируемы, необходимо и достаточно, чтобы были суммируемы как x и z, так y и z; тогда также x и $y+z$ суммируемы и $(x+y)+z=x+(y+z)$;

3° существует нейтральный элемент 0;

4° если как x и z, так y и z суммируемы и $x+z=y+z$, то $x=y$;

5° умножение двояко дистрибутивно относительно сложения.

Каждое кольцо есть кольцоид; для того чтобы кольцоид, имеющий единичный элемент e, был кольцом, необходимо и достаточно, чтобы существовал элемент x такой, что x и e суммируемы и $x+e=0$.

Исследовать, как распространяются на кольцоиды определения и результаты § 8 и приведенных выше упражнений (левым идеалом кольцоида E называется множество $\mathfrak{a} \subset E$, устойчивое относительно сложения и удовлетворяющее условию $E\mathfrak{a} \subset \mathfrak{a}$).

20) Пусть G — группа с операторами, а f и g — ее эндоморфизмы. Для того чтобы отображение $x \to f(x)\,g(x)$ также было ее эндоморфизмом, необходимо и достаточно, чтобы каждый элемент подгруппы $f(G)$ был перестановочен с каждым элементом подгруппы $g(G)$; обозначая тогда этот эндоморфизм через $f+g$, а композицию $x \to f(g(x))$ эндоморфизмов g и f через fg, показать, что множество E всех эндомор-

физмов группы с операторами G, наделенное этими двумя законами композиции, есть *кольцоид* с единицей (упражнение 19); для того чтобы E было кольцом, необходимо и достаточно, чтобы группа G была коммутативна.

Для того чтобы элемент $f \in E$ был суммируемым со всеми элементами из E, необходимо и достаточно, чтобы $f(G)$ содержалось в центре группы G; множество N всех таких эндоморфизмов есть *кольцо*, называемое *ядром* кольцоида E.

Эндоморфизм f группы с операторами G называется *нормальным*, если он перестановочен со всеми ее внутренними автоморфизмами; какова бы ни была устойчивая нормальная подгруппа H группы G, тогда и $f(H)$ будет устойчивой нормальной подгруппой этой группы. Показать, что множество D всех нормальных эндоморфизмов группы с операторами G образует подкольцоид кольцоида E, а ядро N есть двусторонний идеал кольцоида D.

§ 9. Тела

1. *Тела и тела с операторами*

Определение 1. *Телом называется кольцо K, множество ненулевых элементов которого образует группу относительно закона, индуцированного заданным на K умножением.*

Кольцо с операторами K, обладающее этим свойством, называется *телом с операторами*. Так же как и для колец, мы в случае отсутствия опасности путаницы вместо «тело с операторами» будем говорить просто «тело».

Множество ненулевых элементов тела K будет обычно обозначаться K^*; наделенное групповой структурой, определяемой в нем заданным на K умножением, оно называется *мультипликативной группой* тела K. Будучи по самому определению группой, K^* не пусто; его нейтральный элемент e является *единичным элементом* тела K; так как он $\neq 0$, то тело содержит по крайней мере *два* элемента.

Кольцо, *противоположное* телу, очевидно, снова есть тело. Тело называют *коммутативным*, если его умножение коммутативно; такое тело совпадает с противоположным ему. Некоммутативные тела иногда называют *косыми*. Коммутативные тела будут называться *полями*.

Примеры полей *). °1) Наиболее важными для математики полями являются *поле рациональных чисел*, которое будет определено в n° 5, *поле вещественных чисел* и *поле комплексных чисел*, которые мы определим в «Общей топологии» (Общ. топ., главы IV и VIII).

2) В множестве E, состоящем из двух элементов, можно определить структуру тела, и притом (с точностью до перестановки) только одну. Действительно, один элемент из E должен быть нейтральным элементом 0 аддитивной группы, а другой — нейтральным элементом e мультипликативной группы. Аддитивная группа вполне определяется заданием $e+e$, которым может быть лишь 0; мультипликативная группа сводится к e; наконец, должны иметь место равенства $e\cdot 0=0\cdot e=0$. Легко видеть, что всем этим действительно определяется в E структура (коммутативного) тела.

2. *Подтела*

Пусть B — множество элементов кольца A, не сводящееся к 0; для того чтобы B, наделенное индуцированной из A структурой, было *телом*, нужно прежде всего, чтобы B было *подкольцом* кольца A; кроме того, это подкольцо должно обладать единицей e (не обязательно являющейся единицей кольца A) и каждый элемент $x \neq 0$ из B должен быть *обратимым* в B. Обратно, если эти условия выполнены, B есть тело; действительно, тогда множество B^* его ненулевых элементов устойчиво относительно умножения (§ 2, следствие 2 предложения 5) и предложение 1 § 6 показывает, что оно является группой.

Если A — *тело*, то условия, которым должно удовлетворять множество $B \subset A$, чтобы быть телом, упрощаются следующим образом: необходимо и достаточно, чтобы B было подкольцом в A, не сводящимся к 0 и *содержащим элементы, обратные* (в A) *ко всевозможным своим ненулевым элементам* (действительно, множество B^*, будучи подгруппой группы A^*, должно содержать единицу тела A).

Более общим образом, если подкольцо B тела A не сводится к 0 и обладает единичным элементом u, то u равно единице e тела A, ибо из $u^2=u$ и $u \neq 0$ следует $u=u\cdot u^{-1}=e$.

Подкольцо B тела K, являющееся телом, называют *подтелом* тела K, а K часто называется *надтелом* или *расширением* своего подтела B.

*) В главах II и VIII будут даны примеры некоммутативных тел.

Всякое пересечение подтел тела K снова есть его подтело; поэтому можно определить подтело, *порожденное* произвольным множеством $X \subset K$, как наименьшее подтело тела K, содержащее X.

Предложение 1. *Множество всех элементов тела K, перестановочных с каждым элементом произвольного фиксированного множества $M \subset K$, есть подтело тела K.*

Действительно (§ 8, предложение 2) это множество образует в K подкольцо; с другой стороны, если $x \neq 0$ перестановочно с $z \in M$, то это же верно для x^{-1} (§ 2, предложение 6), и предложение доказано.

Следствие. *Центр тела K есть* (коммутативное) *подтело этого тела.*

3. Гомоморфизмы тел

Предложение 2. *Единственными левыми* (соответственно *правыми*) *идеалами тела K являются* (0) *и K.*

Действительно, если $x \neq 0$ принадлежит левому идеалу $\mathfrak{a}$, то $x^{-1}x = e \in \mathfrak{a}$, и значит, $\mathfrak{a} = K$.

Теорема 1. *Если f — гомоморфизм тела K в множество E, наделенное гомологичной структурой, то либо $f(K)$ есть кольцо, сводящееся к 0, либо $f(K)$ есть тело, а f — изоморфизм K на $f(K)$.*

Действительно, прообраз $f^{-1}(0)$ элемента 0 кольца $f(K)$, как двусторонний идеал в K, совпадает с K или с (0), и справедливость утверждения теоремы следует из теоремы 3 § 8.

Предложение 2 допускает следующее обращение:

Предложение 3. *Если в кольце A, не сводящемся к 0 и обладающем единицей, не существует ни одного левого идеала, отличного от* (0) *и A, то A — тело.*

Действительно, пусть x — произвольный ненулевой элемент из A; так как A обладает единицей e, то левым идеалом, порожденным элементом x, служит множество Ax; содержа $x \neq 0$, этот идеал совпадает с A, и значит, существует $x' \in A$ такое, что $x'x = e$. Поскольку $x' \neq 0$, таким же рассуждением устанавливается суще-

ствование $x'' \in A$ такого, что $x''x' = e$; следовательно, $xx' = exx' = x''x'xx' = x''ex' = x''x' = e$, иными словами, x' есть элемент, *обратный* к x, и предложение доказано.

Замечания. 1) Предложение 3 теряет силу, если не предполагать, что A обладает единицей (см. упражнение 3).

2) Некоммутативное кольцо (с операторами) A вполне может не иметь никакого *двустороннего* идеала, отличного от (0) и A, без того, чтобы быть телом (такие кольца будут изучаться в главе VIII).

Из предложения 3 вытекает следующая теорема:

Теорема 2. *Пусть A — кольцо с единицей и $\mathfrak{a}$ — его двусторонний идеал. Для того чтобы факторкольцо $A/\mathfrak{a}$ было телом, необходимо и достаточно, чтобы $\mathfrak{a}$ было максимальным левым идеалом кольца A.*

Действительно, $A/\mathfrak{a}$ обладает единичным элементом, а сформулированное условие выражает в силу теоремы 5 § 8, что единственными левыми идеалами в $A/\mathfrak{a}$ являются (0) и $A/\mathfrak{a}$.

Отсюда видно, в частности, что для того, чтобы кольцо $\mathbf{Z}/(p)$ было полем, необходимо и достаточно, чтобы p было *простым*; так, например, $\mathbf{Z}/(2)$ есть поле, состоящее из двух элементов, изоморфное полю из двух элементов, определенному в n° 1.

4. *Поле отношений кольца целостности*

Поскольку каждый ненулевой элемент тела K обратим и, значит, *регулярен* относительно умножения, любое *подкольцо* в K есть кольцо *без делителей нуля*; в частности, всякое подкольцо *поля* есть *кольцо целостности*. Мы покажем, что и, обратно, каждое кольцо целостности может быть «погружено» в поле.

Более общим образом:

Предложение 4. *Пусть A — коммутативное кольцо с операторами и $\overline{A}$ — результат его симметризации относительно одного лишь умножения* (§ 2, теорема 1).

а) *В $\overline{A}$ можно определить, и притом только одну, структуру кольца с операторами, индуцирующую в A заданную структуру.*

б) *Всякое представление f кольца с операторами A в кольцо с операторами A', переводящее каждый регулярный элемент из A в обратимый элемент кольца A', можно, и притом лишь единственным образом, продолжить до представления $\overline{f}$ $\overline{A}$ в A'.*

а) Будем, как обычно, считать A погруженным в $\overline{A}$; тогда каждый регулярный элемент из A обратим в $\overline{A}$ и каждый элемент из $\overline{A}$ имеет вид $\frac{x}{y}$, где $x \in A$, $y \in A$ и y регулярен. Попытаемся определить сумму двух элементов $z = \frac{x}{y}$ и $z' = \frac{x'}{y'}$ из $\overline{A}$ таким образом, чтобы определенное так сложение индуцировало в A его аддитивный закон, а заданное в $\overline{A}$ умножение было дистрибутивно относительно этого сложения; так как $z = \frac{xy'}{yy'}$ и $z' = \frac{x'y}{yy'}$, то из этих требований с необходимостью следует, что $z + z' = \frac{xy' + x'y}{yy'}$.

Обратно, покажем прежде всего, что определенный так элемент из $\overline{A}$ зависит только от z и z', но не от их представления в форме дробей; действительно, если $z = \frac{x_1}{y_1}$, то $x_1 y = x y_1$, значит, $(x_1 y' + x' y_1)\, y = (xy' + x'y)\, y_1$, откуда $\frac{x_1 y' + x' y_1}{y_1 y'} = \frac{xy' + x'y}{yy'}$.

Без труда устанавливается, что так определенное в $\overline{A}$ сложение ассоциативно и коммутативно, что каждый элемент $z = \frac{x}{y}$ обладает противоположным $z' = \frac{-x}{y}$ и, наконец, что умножение дистрибутивно относительно этого сложения, так что эти два закона определяют в $\overline{A}$ структуру коммутативного кольца, являющуюся продолжением структуры коммутативного кольца, заданной в A.

Остается продолжить на $\overline{A}$ внешние законы кольца A так, чтобы по-прежнему выполнялись тождества (7) § 8; и это возможно здесь лишь единственным образом, ибо в силу указанного условия, если α — оператор на A и $z = \frac{x}{y}$, то должно иметь место равенство $\alpha z = \frac{\alpha x}{y}$. Определенный так элемент αz зависит только от α и z, но не от представления z в виде дроби, ибо если $\frac{x_1}{y_1} = \frac{x}{y}$, то $\alpha\,(x_1 y) = \alpha\,(x y_1)$, и значит, $(\alpha x_1)\, y = (\alpha x)\, y_1$; а определенный таким образом внешний закон действительно дистрибутивен относительно заданного на A сложения и удовлетворяет тождествам (7) § 8.

б) Если рассматривать в A структуру, определяемую одним лишь умножением, то, как мы знаем (§ 2, теорема 2), f продолжается единственным образом до представления $\bar{f}$ множества $\bar{A}$, наделенного одним лишь умножением, в A' (наделенное одним лишь умножением); $\bar{f}$ определяется формулой $\bar{f}\left(\frac{x}{y}\right) = f(x)\,(f(y))^{-1}$. Остается проверить, что, каковы бы ни были $z \in \bar{A}$, $z' \in \bar{A}$ и оператор α, $\bar{f}(z+z') = \bar{f}(z) + \bar{f}(z')$ и $\bar{f}(\alpha z) = \alpha \bar{f}(z)$; это не представляет труда.

Определение 2. *Кольцом отношений* (или *кольцом дробей*) *коммутативного кольца* A *называется коммутативное кольцо, получающееся путем наделения результата симметризации* $\bar{A}$ *кольца* A (*относительно* одного лишь умножения) *структурой, определенной в предложении* 4.

Предложение 5. *Кольцо отношений* $\bar{A}$ *кольца целостности* A *есть поле*; оно называется *полем отношений* (или *полем дробей*) *кольца целостности* A.

Действительно, поскольку каждый ненулевой элемент из A регулярен, каждый ненулевой элемент из $\bar{A}$ обратим (§ 2, следствие теоремы 1).

Предложение 6. *Если кольцо целостности* A *содержится в* (не обязательно коммутативном) *теле* K, *то множество всех элементов* xy^{-1} *из* K, *где* x *пробегает* A, *а* y — *множество всех ненулевых элементов из* A, *есть коммутативное подтело тела* K, *изоморфное полю отношений кольца целостности* A.

Это — непосредственное следствие второй части предложения 4, примененной к тождественному отображению A на себя; представление $\bar{A}$ в K, получающееся путем продолжения, в силу теоремы 1 необходимо является изоморфизмом.

5. *Поле рациональных чисел*

Определение 3. *Полем рациональных чисел называют поле отношений кольца* $\mathbf{Z}$ *рациональных целых чисел*; *элементы этого поля, обозначаемого* $\mathbf{Q}$, *называют рациональными числами.*

В $\mathbf{Z}$ определено *отношение порядка* $x \leqslant y$ (§ 2, n° 5), удовлетворяющее следующим двум условиям:

а) $x \leqslant y$ влечет $x + z \leqslant y + z$ для всех z;

б) структура порядка, определяемая отношением $x \leqslant y$, есть структура *совершенно упорядоченного* множества.

Покажем, что в $\mathbf{Q}$ можно определить отношение порядка, и притом только одно, по-прежнему удовлетворяющее этим двум условиям и индуцирующее в $\mathbf{Z}$ первоначальное отношение порядка (см. главу VI).

Действительно, заметим прежде всего, что из отношения $x > 0$, в силу а), индукцией по p выводится, что $px > 0$ для каждого целого $p > 0$; отсюда следует, что если n — целое > 0, то $\frac{1}{n} > 0$: в противном случае, в силу б), мы имели бы $\frac{1}{n} < 0$, значит, $-\frac{1}{n} > 0$ и $n \cdot \left(-\frac{1}{n}\right) = -1 > 0$, что абсурдно. Поэтому заключаем, что если p и q — целые числа > 0, то рациональное число $\frac{p}{q} = p \cdot \frac{1}{q} > 0$; так как каждое рациональное число может быть записано в виде $\frac{p}{q}$, где $p \in \mathbf{Z}$, $q \in \mathbf{N}^*$, то мы видим, что множество $\mathbf{Q}_+$ всех рациональных чисел $\geqslant 0$ совпадает с множеством всех чисел вида $\frac{p}{q}$, где $p \in \mathbf{N}$, $q \in \mathbf{N}^*$. В силу а), отношение $x \leqslant y$ должно быть эквивалентно отношению $y - x \geqslant 0$; если существует отношение порядка в $\mathbf{Q}$, удовлетворяющее поставленным требованиям, то оно необходимо эквивалентно отношению $y - x \in \mathbf{Q}_+$. Обратно, легко видеть, что это отношение действительно есть отношение порядка в $\mathbf{Q}$, удовлетворяющее условиям а) и б) и индуцирующее в $\mathbf{Z}$ первоначально определенное отношение порядка.

Говоря о $\mathbf{Q}$ как об упорядоченном множестве, мы всюду, где не оговорено противное, будем иметь в виду определенное здесь отношение порядка.

Рациональные числа $\geqslant 0$ (соответственно $\leqslant 0$, > 0, < 0) называются *положительными* (соответственно *отрицательными*, *строго положительными*, *строго отрицательными*) *).

*) И здесь мы отклоняемся от обычной терминологии, по которой положительное означает >0 (см. § 2, сноску в n° 5 .

В силу определения отношения $x \geqslant 0$ в $\mathbf{Q}$, отношения $x \geqslant 0$, $y \geqslant 0$ влекут $xy \geqslant 0$; точно так же $x \geqslant 0$ и $y \leqslant 0$ влекут $xy \leqslant 0$, $x \leqslant 0$ и $y \leqslant 0$ влекут $xy \geqslant 0$ (*правила знаков*). Отсюда, в частности, следует, что множество всех рациональных чисел > 0, обозначаемое $\mathbf{Q}_+^*$, является *подгруппой* мультипликативной группы $\mathbf{Q}^*$ всех рациональных чисел $\neq 0$; так как каждое рациональное число $x \neq 0$ представимо, и притом единственным образом, в одной из форм $(+1)y$, $(-1)y$, где $y > 0$, то мы видим, что мультипликативная группа $\mathbf{Q}^*$ является *прямым произведением* подгрупп $\mathbf{Q}_+^*$ и $\{-1, +1\}$; компонента y числа x в $\mathbf{Q}_+^*$ называется *абсолютным значением* x и обозначается $|x|$ (см. главу V); компонента x в $\{-1, +1\}$ (равная $+1$, если $x > 0$, и -1, если $x < 0$) называется *знаком* x и обозначается $\operatorname{sgn} x$.

Обычно эти две функции продолжают на всё $\mathbf{Q}$, полагая $|0| = 0$ и $\operatorname{sgn} 0 = 0$.

У п р а ж н е н и я. 1) Какие из кольцевых структур, определенных в упражнении 1 § 8, являются структурами тела?

2) *Конечное* кольцо без делителей нуля есть тело. [§ 2, упражнение 6.]

*3) Пусть A — кольцо с операторами, имеющее своими единственными левыми идеалами (0) и A. Показать, что *либо* A есть кольцо *с нулевым квадратом* (§ 8, п° 1), а его аддитивная группа с операторами — *простая*, *либо* A есть *тело*.

Отбросив первую из этих возможностей, показать последовательно, что: а) существует $a \in A$, для которого $Aa \neq (0)$; б) существует $e \in A$, для которого $ea = a$ и $e^2 = e$; в) e — единица кольца A. [Рассмотреть множество всех элементов $x - xe$, а затем множество всех элементов $x - ex$, где x пробегает A.]

4) Поле Q рациональных чисел не обладает никаким подполем, отличным от Q.

*5) Пусть K — поле характеристики $\neq 2$ и G — подгруппа его аддитивной группы такая, что множество H, составленное из 0 и элементов, обратных всевозможным ненулевым элементам из G, также есть подгруппа аддитивной группы K. Показать, что существуют элемент $a \in K$ и подполе K' поля K такие, что $G = aK'$. [Установить сначала, что если x, y принадлежат G и $y \neq 0$, то $\dfrac{x^2}{y} \in G$; вывести отсюда, что если x, y, z принадлежат G и $z \neq 0$, то $\dfrac{xy}{z} \in G$.]

6) Пусть K — поле характеристики $\neq 2$ и f — отображение K в K такое, что $f(x+y)=f(x)+f(y)$ для любых x и y и $f(x)f\left(\frac{1}{x}\right)=1$ для любого $x\neq 0$. Показать, что f или $-f$ есть изоморфизм K на его подполе. [Доказать, что $f(x^2)=(f(x))^2$.]

*7) Пусть A — коммутативное кольцо с единицей и $\bar{A}$ — его кольцо отношений. Для каждого множества $S\subset A$, *устойчивого* относительно умножения и состоящего из регулярных элементов, обозначим через A_S подкольцо кольца $\bar{A}$, образованное элементами $\frac{x}{s}$, где x пробегает A, а s пробегает S.

а) Идеал кольца A_S, порожденный идеалом $\mathfrak{a}$ кольца A, совпадает с множеством $\mathfrak{a}A_S$ всех элементов $\frac{x}{s}$, где x пробегает $\mathfrak{a}$, а s пробегает S. Каковы бы ни были идеалы $\mathfrak{a}$ и $\mathfrak{b}$ кольца A, $(\mathfrak{a}+\mathfrak{b})A_S=\mathfrak{a}A_S+\mathfrak{b}A_S$ и $(\mathfrak{a}\cap\mathfrak{b})A_S=(\mathfrak{a}A_S)\cap(\mathfrak{b}A_S)$.

б) Если $\mathfrak{c}$ — идеал кольца A_S, то $(\mathfrak{c}\cap A)A_S=\mathfrak{c}$.

в) Если $\mathfrak{a}$ — идеал кольца A, то $\mathfrak{a}\subset(\mathfrak{a}A_S)\cap A$; идеал $(\mathfrak{a}A_S)\cap A$ есть множество тех элементов $x\in A$, для каждого из которых существует $s\in S$ такое, что $sx\in\mathfrak{a}$.

г) Пусть $\mathfrak{a}$ — идеал кольца A и φ — каноническое отображение A на $A/\mathfrak{a}$; для того чтобы элементы множества $\varphi(S)$ были регулярны в $A/\mathfrak{a}$, необходимо и достаточно, чтобы $(\mathfrak{a}A_S)\cap A=\mathfrak{a}$; факторкольцо $A_S/(\mathfrak{a}A_S)$ изоморфно тогда $(A/\mathfrak{a})_{\varphi(S)}$.

д) Для того чтобы дополнение S к идеалу $\mathfrak{p}$ кольца A было устойчиво относительно умножения, необходимо и достаточно, чтобы $\mathfrak{p}$ был простым (§ 8, упражнение 13); если A — кольцо целостности, то $S/(\mathfrak{p}A_S)$ есть поле, изоморфное полю отношений факторкольца $A/\mathfrak{p}$.

*8) Пусть A — некоммутативное кольцо без делителей нуля. Говорят, что A допускает *тело левых отношений*, если оно изоморфно подкольцу A' некоторого тела K такому, что каждый элемент из K имеет вид $x^{-1}y$, где $x\in A'$, $y\in A'$.

а) Пусть A^* — множество всех ненулевых элементов кольца A. Для того чтобы A допускало тело левых отношений, необходимо, чтобы было выполнено следующее условие: (G) каковы бы ни были $x\in A$, $x'\in A^*$, существуют $u\in A^*$ и $v\in A$ такие, что $ux=vx'$.

б) Обратно, предположим, что условие (G) выполнено. Показать, что отношение R между элементами (x, x') и (y, y') произведения $A\times A^*$: «для каждой пары (u, v) ненулевых элементов таких, что $ux'=vy'$, выполняется равенство $ux=vy$» — есть отношение эквивалентности.

Пусть (x, x') и (y, y') — элементы произведения $A\times A^*$, ξ и η соответственно — их классы $\bmod R$. Показать, что для каждой пары $(u, u')\in A\times A^*$ такой, что $u'x=uy'$, класс $\bmod R$ пары $(uy, u'x')$ зависит лишь от ξ и η; обозначая его $\xi\eta$, получим закон композиции в множестве $K=(A\times A^*)/R$. Пусть K^* — множество всех элементов

из K, отличных от класса 0 элементов $(0, x') \in A \times A^*$. Наделенное законом, индуцированным введенным законом композиции, K^* есть группа.

Для всякого $x \in A$ элементы $(x'x, x')$, где x' пробегает A^*, образуют класс $\bmod R$. Отнесение этого класса элементу x определяет изоморфизм A (относительно одного лишь умножения) на некоторое подкольцо в K. При отождествлении A с его образом при этом изоморфизме класс $\bmod R$ пары $(x, x') \in A \times A^*$ отождествляется с элементом $x'^{-1}x$.

Если теперь $\xi = x'^{-1}x$ — элемент из K и 1 — единичный элемент группы K^*, то обозначим через $\xi + 1$ элемент $x'^{-1}(x + x')$, не зависящий от представления ξ в виде $x'^{-1}x$. Положим, далее, $\xi + 0 = \xi$ и $\xi + \eta = \eta(\eta^{-1}\xi + 1)$ при $\eta \neq 0$. Показать, что введенные так на K сложение и умножение определяют в этом множестве структуру тела, являющуюся продолжением структуры кольца A; иными словами, условие (G) также *достаточно* для того, чтобы A допускало тело левых отношений.

9) Пусть A — кольцо без делителей нуля. Для того чтобы A допускало тело левых отношений (упражнение 8), необходимо и достаточно, чтобы пересечение двух левых идеалов кольца A, отличных от $\{0\}$, никогда не сводилось к 0.

ИСТОРИЧЕСКИЙ ОЧЕРК

К ГЛАВЕ I

(Римские цифры относятся к библиографии, помещенной в конце настоящего очерка.)

В математике мало понятий, которые были бы первичней понятия закона композиции; оно представляется неотделимым уже от самых зачаточных вычислений с натуральными числами и измеряемыми величинами. Наиболее древние из дошедших до нас документов, относящихся к математике египтян и вавилонян, обнаруживают уже владение полной системой правил вычислений с целыми числами >0, рациональными числами >0, длинами и площадями; хотя в дошедших до нас текстах рассматриваются лишь задачи с определенными числовыми данными *), эти тексты не оставляют никаких сомнений в общности, приписывавшейся употребляемым правилам, и обнаруживают прямо-таки замечательное техническое мастерство в обращении с уравнениями первой и второй степени ((I), стр. 179 и след.). Но при всем этом там нет и следа заботы ни об обосновании применяемых правил, ни о точном определении входящих в них операций: и те и другие сохраняют чисто эмпирический характер.

Напротив, подобная забота уже весьма определенно проявляется у греков классической эпохи; правда, у них еще нет аксиоматической трактовки теории натуральных чисел (такая аксиоматизация появилась лишь в конце XIX века; см. Исторический очерк к главе IV Книги I); но во многих местах «Начал» Евклида даются формальные доказательства правил действий, столь же интуитивно «очевидных», как правила действий над целыми числами

*) Не следует забывать, что обозначение всех (известных и неизвестных) элементов алгебраической задачи буквами ввел в употребление лишь Вьета (XVI век). До этого в алгебраических руководствах рассматривались лишь уравнения с числовыми коэффициентами; высказывая общее правило обращения с аналогичными уравнениями, автор формулировал его (и это было лучшее, что он мог сделать) словесно; при отсутствии явной формулировки этого рода обладание таким правилом с большей или меньшей вероятностью обнаруживалось самим ходом выкладок в рассматриваемых числовых примерах.

(например, коммутативности произведения двух рациональных чисел). Наиболее замечательны доказательства этого рода, относящиеся к *теории величин*, являющейся самым оригинальным творением греческой математики (и, как известно, эквивалентной нашей теории вещественных чисел > 0; см. Исторический очерк к главе IV Книги III): рассматривая, среди прочего, произведение двух отношений величин, Евклид доказывает, что оно не зависит от формы, в которой представлены эти отношения (первый пример «факторизации» закона композиции по отношению эквивалентности в смысле § 4), и что оно коммутативно ((II), Книга V, предложения 22—23) *).

Однако не следует скрывать, что этот прогресс в строгости сопровождается у Евклида застоем, а в некоторых отношениях даже попятным движением в том, что касается техники алгебраических вычислений. Подавляющий перевес геометрии (для целей которой явно задумана и теория величин) парализует всякое самостоятельное развитие алгебраической символики: элементы, входящие в вычисления, должны быть все время «представлены» геометрически; при этом участвующие в вычислениях законы композиции не определены на одном и том же множестве (сложение отношений в общем виде не определено, произведение же двух длин есть не длина, а площадь); проистекающая отсюда недостаточная гибкость делает оперирование с алгебраическими соотношениями выше второй степени почти невыполнимым.

Лишь на закате классической греческой математики мы видим Диофанта, который возвращается к традиции «логистов», т. е. профессиональных вычислителей, продолжавших применять в прежнем виде правила, унаследованные от египтян и вавилонян: не стесненный более геометрическим представлением рассматриваемых им «чисел», он естественно приходит к разработке правил абстрактных алгебраических действий; так, например, он дает правила, которые (на современном языке) равносильны формуле $x^{m+n}=x^m x^n$ для небольших (положительных или отрицательных) значений m и n ((III), т. I, стр. 8—13); несколько дальше формулируется «правило знаков»—первый зародыш действий над отрицательными числами **); наконец, Диофант впервые употребляет буквенный символ для представления неизвестной уравнения. Но, в противовес этому, он отнюдь не кажется озабоченным увязкой методов, применяемых им для решения его задач, с какими-либо общими идеями; аксиоматический же подход к законам композиции, подобный наметившемуся у Евклида, по-видимому, был чужд мышлению Диофанта, равно как и его непосредственных продолжателей; он вновь появляется в алгебре лишь в начале XIX века.

---

*) Правда, Евклид не дает в этом месте формального определения произведения двух отношений, а определение, находящееся в «Началах» несколько дальше (Книга VI, определение 5), считается позднейшей вставкой; тем не менее, он, конечно, имел совершенно ясное представление об этой операции и ее свойствах.

**) Диофант не знает отрицательных чисел; поэтому указанное правило можно истолковывать лишь как относящееся к действиям над многочленами и позволяющее «раскрывать» произведения, подобные $(a-b)(c-d)$.

Потребовалось сначала, чтобы в течение промежуточных столетий, с одной стороны, развилась система алгебраических обозначений, пригодная для адекватного выражения абстрактных законов, а с другой — понятие «числа» настолько расширилось, чтобы наблюдение достаточно разнообразных частных случаев позволяло подыматься до общих понятий. Для этих целей созданная греками аксиоматическая теория отношения величин была недостаточной, ибо она лишь уточняла интуитивное понятие вещественного числа >0 и те операции над этими числами, которые в более смутной форме были известны еще вавилонянам; теперь же, напротив, дело касалось «чисел», о которых греки не имели представления и которые вначале не вызывали никаких наглядных «представлений»: с одной стороны, нуля и отрицательных чисел, появившихся в индийской математике в раннее средневековье, с другой стороны, мнимых чисел, этого творения итальянских алгебраистов XVI века.

Если оставить в стороне нуль, который первоначально появился как нумерационный символ и лишь потом стал рассматриваться как число (см. Исторический очерк к главе III Книги I), общим у всех этих расширений понятия числа был (по крайней мере вначале) их чисто «формальный» характер. Под этим следует понимать, что новые «числа» появлялись первоначально как результаты операций, примененных в условиях, где эти операции не имеют, если придерживаться их точного определения, никакого смысла (например, разность $a - b$ двух натуральных чисел, когда $a < b$); отсюда и присваивавшиеся им наименования чисел «ложных», «фиктивных», «абсурдных», «невозможных», «мнимых» и т. д. Грекам классической эпохи, увлеченным прежде всего ясностью мысли, подобные расширения были недоступны; они могли возникнуть только у вычислителей, в противоположность грекам более склонных к несколько мистической вере в мощь своих методов («общность анализа», как скажут в XVIII веке) и позволявших увлечь себя механизму вычислений, не проверяя обоснованности каждого его шага; впрочем, эта вера чаще всего оправдывалась апостериори точными результатами, к которым приводило распространение на эти новые математические создания вычислительных правил, строго говоря, применимых лишь к ранее известным числам. Вот почему эти обобщения понятия числа, вначале встречавшиеся лишь в виде промежуточных звеньев цепи операций, исходным пунктом которой и окончательным результатом были настоящие «числа», понемногу стали все смелее рассматривать сами по себе (независимо ни от каких применений к конкретным вычислениям); а отважившись однажды на этот шаг, начали искать более или менее осязаемые истолкования новых созданий, приобретших таким путем право гражданства в математике *).

*) Впрочем, эти изыскания составили лишь переходный этап в эволюции рассматриваемых понятий; с середины XIX века вновь вернулись, на этот раз вполне сознательно, к формальной концепции различных расширений понятия числа, и она завершилась включением в «формалистскую» и аксиоматическую точку зрения, господствующую в современной математике.

В этом отношении уже индийцам было известно истолкование, которое в некоторых случаях следует давать отрицательным числам (например, как долга в задачах коммерческого характера). В последующие века, по мере проникновения на Запад (через посредство арабов) методов и результатов греческой и индийской математики, все больше осваиваются с оперированием этими числами и начинают находить другие их «представления», геометрического или кинематического характера. Вот, собственно, вместе с прогрессировавшим улучшением алгебраической символики, и все заметные успехи алгебры в конце средних веков.

В начале XVI века алгебра познает новый подъем, вызванный открытием математиками итальянской школы решения уравнения третьей, а затем и четвертой степени «в радикалах» (о чем подробнее будет сказано в Историческом очерке к главе V); в связи с этим они были, так сказать, вынуждены, несмотря на всё отвращение, ввести в свои вычисления мнимые числа; впрочем, мало-помалу возникает доверие к вычислениям с этими «невозможными» числами, как и к вычислениям с отрицательными, хотя в течение более чем двух веков не было придумано для них никакого «представления».

С другой стороны, Вьета и Декарт вносят в алгебраическую символику решающие усовершенствования; начиная с Декарта, алгебраическое правописание, с точностью до незначительных деталей, приобретает уже современный нам вид.

С середины XVII и до конца XVIII века обширные горизонты, открытые созданием исчисления бесконечно малых, по-видимому, несколько отодвигают на задний план алгебру вообще и особенно математическое исследование законов композиции или природы вещественных и комплексных чисел *). Так, например, сложение сил и сложение скоростей, хорошо известные в механике с конца XVII века, не нашли в алгебре никакого отражения, хотя и содержали уже в зародыше векторное исчисление. В самом деле, пришлось ждать идейного движения, приведшего примерно в 1800 г. к геометрическому представлению комплексных чисел (см. Исторический очерк к главе VIII Книги III), чтобы в чистой математике появилось сложение векторов **).

К этому же времени понятие закона композиции, впервые в алгебре, распространяется, в двух различных направлениях, на элементы, имеющие уже с «числами» (в наиболее широком смысле, придававшемся к тому времени

---

*) Следует оставить в стороне попытки Лейбница, с одной стороны, придать алгебраическую форму умозаключениям формальной логики, с другой — создать «геометрическое исчисление», оперирующее прямо с геометрическими элементами, без посредства координат ((IV), т. V, стр. 141). Эти попытки остались в стадии набросков и не вызвали никакого отклика у современников; к ним вернулись лишь в XIX веке (см. ниже).

**) Причем эта операция была введена без всякого отношения к механике; связь между обеими теориями была явно осознана лишь основателями векторного исчисления во второй трети XIX века.

этому слову) лишь отдаленную аналогию. Первое из этих распространений принадлежит К. Ф. Гауссу и связано с его арифметическими исследованиями, посвященными квадратичным формам $ax^2 + bxy + cy^2$ с целыми коэффициентами. Лагранж определил в множестве всех форм с одинаковым дискриминантом отношение эквивалентности *) и, с другой стороны, доказал тождество, дающее в этом множестве некоторый (не всюду определенный) коммутативный закон композиции; отправляясь от этих результатов Гаусс показывает, что этот закон согласуется (в смысле § 4) с упомянутым отношением эквивалентности ((V), т. I, стр. 272): «*Отсюда видно*, — говорит он затем,— *что́ следует понимать под композицией двух или нескольких классов*». Он приступает затем к изучению полученного им так «факторзакона» и устанавливает по существу, что это (на нынешнем языке) — закон коммутативной группы, притом с помощью рассуждений, общность которых чаще всего выходит далеко за пределы исследуемого Гауссом специального случая (например, рассуждение, которым он доказывает единственность элемента, симметричного данному, совпадает с примененным нами при доказательстве предложения 3 § 2 для произвольного закона композиции (там же, стр.273)). Но он не останавливается на этом: возвращаясь немного позже к тому же вопросу, он отмечает аналогию между композицией классов и умножением целых чисел по простому модулю **) (там же, стр. 371), устанавливая, однако, при этом, что группа классов квадратичных форм с заданным дискриминантом не всегда циклическая; замечания, которые он делает по этому поводу, дают основание полагать, что ему было известно, по крайней мере на этом частном случае, общее строение конечных коммутативных групп, которое мы изучим в главе VII ((V), т. I, стр. 374 и т. II, стр. 266).

Другая серия исследований, о которой мы хотим сказать, также подводит к понятию группы, которое этим путем и входит окончательно в математику: это — «теория подстановок», развившаяся из идей Лагранжа, Вандермонда и Гаусса относительно решения алгебраических уравнений. Мы не

*) Две формы эквивалентны, если одна из них получается из другой путем «замены переменных» $x' = \alpha x + \beta y$, $y' = \gamma x + \delta y$, где α, β, γ, δ— целые такие, что $\alpha\delta - \beta\gamma = 1$.

**) Весьма замечательно, что Гаусс пользуется для композиции классов квадратичных форм *аддитивным* обозначением, несмотря на аналогию, отмеченную им самим, а также на то, что тождеством Лагранжа, определяющим композицию двух форм, гораздо естественнее подсказывается мультипликативное обозначение (к которому, кстати, и вернулись все продолжатели Гаусса). В этом безразличии к выбору обозначения следует видеть лишнее свидетельство общности, несомненно достигнутой в понимании Гауссом законов композиции. При этом в своих рассмотрениях он не ограничивался коммутативными законами, как это показывает относящийся к 1819—1820 гг., но не опубликованный при жизни Гаусса отрывок, где более чем за двадцать лет до Гамильтона даются формулы умножения кватернионов ((V), т. VIII, стр. 357).

собираемся подробно излагать здесь историю этого вопроса (см. Исторический очерк к главе V); следует лишь напомнить данное Руффини, а затем Коши ((VI), (2), т. I, стр. 64) определение «произведения» двух подстановок конечного множества *) и первоначальных понятий, относящихся к конечным группам подстановок: транзитивности, примитивности, нейтрального элемента, перестановочных элементов и т. д. Но эти первые исследования оставались, в целом, довольно поверхностными, и действительным родоначальником теории должен считаться Эварист Галуа: сведя в своих знаменитых работах (VIII) изучение алгебраических уравнений к изучению связанных им с ними групп подстановок, он значительно углубил это последнее как в том, что касается общих свойств групп (так, Галуа первый определил понятие нормальной подгруппы и осознал его важность), так и в нахождении групп, обладающих специальными свойствами (где полученные им результаты и ныне числятся среди наиболее тонких результатов теории). Галуа принадлежит также первая идея «линейного представления групп» **), а этот факт ясно показывает, что он владел понятием *изоморфизма* двух групповых структур, независимого от их «реализаций».

Однако, хотя и представляется несомненным, что гениальные методы Гаусса и Галуа привели их к весьма широкому взгляду на понятие закона композиции, им не представилось случая специально развить свои идеи на этот счет, и их работы не оказали непосредственного воздействия на эволюцию абстрактной алгебры ***). Наиболее ощутимый прогресс по пути абстракции был достигнут в третьем направлении: развивая идеи относительно природы мнимых чисел (геометрическое представление последних вызвало в начале XIX века появление довольно многочисленных работ), алгебраисты английской школы в 1830—1850 гг. первыми выделили абстрактное понятие закона композиции и немедленно расширили область алгебры, применив это понятие к множеству новых математических созданий: алгебре логики у Буля (см. Исторический очерк к главе IV Книги I), векторам, кватернионам и общим гиперкомплексным системам у Гамильтона (IX), матрицам и неассоциативным законам у Кэли ((X), т. I, стр. 127 и 301 и т. II, стр. 185 и 475). Параллельная эволюция независимо протекала на континенте Европы, особенно в том, что касается векторного исчисления (Мёбиус, Бел-

---

*) Разумеется, понятие сложной функции было известно гораздо раньше, по крайней мере для функций вещественного или комплексного переменного, но алгебраический аспект этого закона композиции и связь с произведением двух подстановок были выяснены лишь работами Абеля ((VII), т. I, стр. 478) и Галуа.

**) Именно в этой связи Галуа, смело распространяя «формализм», приведший к комплексным числам, рассматривает «мнимые корни» сравнения по простому модулю и открывает так *конечные* поля, изучаемые нами в главе V.

***) При этом идеи Галуа до 1846 г. оставались неизвестными, а идеи Гаусса оказали прямое воздействие лишь на теорию чисел.

лавитис), линейной алгебры и гиперкомплексных систем (Грассман), о чём подробнее будет сказано в Историческом очерке к главам II и III *).

Из этого кипения оригинальных и плодотворных идей, которое в первой половине XIX века вдохнуло в алгебру новую жизнь, она вышла обновленной до самих своих устремлений. Прежде ее методы и результаты концентрировались вокруг задачи решения алгебраических уравнений (или диофантовых уравнений в теории чисел): «*Алгебра*,— говорит Серре во введении к своему «Курсу высшей алгебры» (XII),—*есть, собственно говоря, анализ уравнений*». После 1850 г., хотя руководства по алгебре и предоставляли еще долгое время приоритет теории уравнений, над новыми исследованиями уже не доминировала забота о непосредственных применениях к решению числеяных уравнений, и они всё более и более ориентировались на то, что мы сегодня рассматриваем как основную задачу алгебры, а именно изучение алгебраических структур самих по себе.

Эти работы довольно отчетливо разбиваются на три течения, продолжавшие соответственно три рассмотренных выше направления идей и продвигавшиеся параллельно без ощутимого взаимного влияния вплоть до последних лет XIX века **).

Это, прежде всего, построение немецкой школой XIX века (Дирихле, Куммер, Кронекер, Дедекинд, Гильберт) теории алгебраических чисел, восходящей к Гауссу, которому принадлежит первое исследование такого рода, а именно исследование чисел $a + bi$ (где a и b рациональные). Мы не будем прослеживать здесь эволюцию этой теории: для наших целей нужно лишь отметить порожденные ею абстрактные алгебраические понятия. Начиная с первых преемников Гаусса, идея *поля* (алгебраических чисел) лежит в основе всех работ в этом направлении (как и исследований Абеля и Галуа по теории алгебраических уравнений); область ее применений расширяется, когда Дедекинд и Вебер (XIII) строят теорию алгебраических функций одной переменной по образцу теории алгебраических чисел. Дедекинду (XIV) мы обязаны также введением понятия *идеала*, дающего новый пример закона композиции *множеств* элементов; к Дедекинду и Кронекеру восходит обнаружение роли, далее всё более возрастающей, которую играют коммутативные группы и модули в теории алгебраических полей; мы вернемся к этому в главах II, V и VII.

В последующих главах (главы II, III и VIII) мы вернемся также к истории развития линейной алгебры и гиперкомплексных систем, которое в кон-

---

*) Основные теории, развитые в течение этого периода, замечательно изложены в относящемся к нему труде Ганкеля (XI), где абстрактное понятие закона композиции осмыслено и изложено с совершенной отчетливостью.

**) Мы сознательно оставляем здесь в стороне всё относящееся в этот период к эволюции алгебраической геометрии и тесно связанной с ней теории инвариантов; эти две теории развивались на базе своих собственных методов, ориентированных на анализ не в меньшей мере, чем на алгебру, и лишь в недавнее время нашли свое место в обширном здании современной алгебры.

це XIX и начале XX веков идет, без введения новых алгебраических понятий, по пути, проложенному Гамильтоном и Кэли, в Англии (Сильвестр, В. Клиффорд) и Америке (Б. и К. Пирс, Диксон, Веддербэрн) и совсем независимо от англосаксов, на базе довольно отличающихся методов, в Германии (Вейерштрасс, Дедекинд, Фробениус, Молин *)) и Франции (Лагерр, Э. Картан).

Что касается теории групп, то вначале она развивалась главным образом в виде теории конечных групп подстановок, вслед за публикацией сочинений Галуа и распространением его идей трудами Серре (XII) и, особенно, большим «Трактатом о подстановках» К. Жордана (XV). Этот последний подытожил, в значительно усовершенствованном виде, работы своих предшественников по специальным свойствам групп подстановок (транзитивности, примитивности и т. д.) и получил результаты, в большинстве своем не превзойденные в дальнейшем; вместе с тем он подверг углубленному исследованию весьма важные специальные группы — линейные группы и их подгруппы (см. главы II и IX), причем именно им было введено фундаментальное понятие представления одной группы на другую, а также (несколько позже) понятие факторгруппы, и он доказал часть теоремы, известной под названием «теоремы Жордана — Гёльдера» **). Наконец, к Жордану восходит и первое исследование *бесконечных* групп (XVI), которое несколькими годами позже было значительно развито в двух различных направлениях, с одной стороны, С. Ли, а с другой — Ф. Клейном и А. Пуанкаре.

Тем временем Кэли ((X), т. II, стр. 123 и 131) дал в 1854 г. определение «абстрактных» групп и, одновременно, однородных пространств, правда, в форме, корректной лишь для конечных групп. Однако даже исследования по конечным абстрактным группам в течение долгого времени воспринимались как относящиеся к группам подстановок, и лишь к 1880 г. началось сознательное развитие автономной теории конечных групп. Мы не будем прослеживать дальнейшего развития этой теории, затрагиваемой в этом трактате лишь весьма поверхностно; читателя, желающего углубиться в рассматриваемые ею вопросы и поставленные в ней многочисленные трудные задачи, мы отошлем к современным монографиям Бэрнсайда (XVII), Шпайзера (XVIII) и Цасенхауза (XIX).

Здесь нет уже места говорить о чрезвычайном успехе, который с конца XIX века приобрела идея группы (а также тесно связанная с ней идея *инварианта*) в анализе, геометрии, механике и теоретической физике. Аналогичным вторжением этого понятия и родственных ему алгебраических понятий (групп с операторами, колец, идеалов, модулей) в те разделы алгебры, которые до того казались довольно далекими от естественной области его приме-

*) Ф. Э. Молин жил и работал в России и СССР.— *Перев.*

**) Жордан установил лишь инвариантность (с точностью до расположения) *порядков* факторгрупп «ряда Жордана — Гёльдера» конечной группы; независимость же (с точностью до расположения) самих факторгрупп от рассматриваемого ряда показал О. Гёльдер.

нимости, как раз и отмечен последний период излагаемой здесь эволюции, приведший к синтезу прослеженных выше трех тенденций. Это объединение есть главным образом дело новой немецкой школы: начатая Дедекиндом и Гильбертом в последние годы XIX века работа по аксиоматизации алгебры была мощно продолжена Э. Штейницем и далее, с 1920 г., под влиянием Э. Артина,— Э. Нетер и алгебраистами ее школы (Хассе, Круль, О. Шрейер. Ван-дер-Варден). Книга Ван-дер-Вардена (XX), опубликованная в 1930 г., впервые объединила эти работы в обобщающем изложении, открыв путь и сделавшись путеводителем для многих исследований по абстрактной алгебре в эти последние годы.

БИБЛИОГРАФИЯ

(I) O. Neugebauer, Vorlesungen über Geschichte der antiken Mathematik, т. I: Vorgriechische Mathematik, Berlin (Springer), 1934. [О. Нейгебауер, Лекции по истории античных математических наук, т. I: Догреческая математика, М.— Л., ОНТИ, 1937.]

(II) Euclidis Elementa, 5 тт., изд. J. L. Heiberg, Lipsiae (Teubner), 1883—1888. [Начала Евклида, 3 тт., Гостехиздат, М.— Л., 1948—50.]

(II bis) T. L. Heath, The thirteen books of Euclid's Elements..., 3 тт., Cambridge, 1908.

(III) Diophanti Alexandrini Opera Omnia..., 2 тт., изд. P. Tannery, Lipsiae (Teubner), 1893—1895.

(III bis) Diophante d'Alexandrie, перев. P. Ver Eecke, Bruges (Desclée-de Brouwer), 1926.

(IV) G. W. Leibniz, Mathematische Schriften, изд. C. I. Gerhardt, т. V, Halle (Schmidt), 1858.

(V) C. F. Gauss, Werke, т. I (Göttingen, 1870), т. II (там же, 1863) и VIII (там же, 1900).

(VI) A. L. Cauchy, Oeuvres complètes (2), т. I, Paris (Gauthier-Villars), 1905.

(VII) N. H. Abel, Oeuvres, 2 тт., изд. Sylow и Lie, Christiania, 1881.

(VIII) E. Galois, Oeuvres mathématiques, Paris (Gauthier-Villars), 1897. [Эварист Галуа, Сочинения, М.— Л., ОНТИ, 1936.]

(IX) W. R. Hamilton, Lectures on Quaternions, Dublin, 1853.

(X) A. Cayley, Collected mathematical papers, тт. I и II, Cambridge (University Press), 1889.

(XI) H. Hankel, Vorlesungen über die complexen Zahlen und ihre Functionen, 1. Teil: Theorie der complexen Zahlensysteme, Leipzig (Voss), 1867.

(XII) J. A. Serret, Cours d'Algèbre supérieure, 3-e изд., Paris (Gauthier-Villars), 1866.

(XIII) R. Dedekind und H. Weber, Theorie der algebraischen Funktionen einer Veränderlichen, J. de Crelle, т. XCII (1882), стр. 181.

(XIV) R. Dedekind, Gesammelte mathematische Werke, 3 тт., Braunschweig (Vieweg), 1932.

(XV) C. Jordan, Traité des substitutions et des équations algébriques, Paris (Gauthier-Villars), 1870.

(XVI) C. Jordan, Mémoire sur les groupes de mouvements, Ann. di Mat. (2), т. II (1868), стр. 167.

(XVII) W. Burnside, Theory of groups of finite order, 2-е изд., Cambridge, 1911.

(XVIII) A. Speiser, Theorie der Gruppen von endlicher Ordnung, 3-е изд., Berlin (Springer), 1937.

(XIX) H. Zassenhaus, Lehrbuch der Gruppentheorie, т. I, Leipzig—Berlin (Teubner), 1937.

(XX) B. L. van der Waerden, Moderne Algebra, 2-е изд., т. I, Berlin (Springer), 1937; т. II (там же), 1940. [Б. Л. Ван-дер-Варден, Современная алгебра, ч. I, М.— Л., Гостехиздат, 1947; ч. II (там же), 1947.]

ГЛАВА II

ЛИНЕЙНАЯ АЛГЕБРА

В этой главе, если только не оговорено противное, никаких специальных предположений о рассматриваемых кольцах операторов не делается: они могут быть коммутативны или нет, иметь или не иметь единицу, содержать или нет делители нуля.

§ 1. Модули

Эта глава посвящена в основном изучению специального вида *коммутативных групп с операторами* (гл. I, § 6, n° 9), а именно *модулей*. Некоторые свойства модулей, сформулированные в первых двух параграфах, справедливы (как и их доказательства) для всех коммутативных групп с операторами, что в соответствующих местах отмечается. Впрочем, как будет показано в n° 9 § 7, изучение любой коммутативной группы с операторами всегда может быть сведено к изучению надлежащим образом ассоциированного с ней модуля.

1. Определение модулей

Определение 1. *Левым модулем относительно заданного кольца A* (или *левым модулем над A*, или также *левым A-модулем*) *называют множество E, наделенное алгебраической структурой, определяемой заданием:*

1° *коммутативного группового закона на E (с аддитивной записью);*

2° *всюду определенного внешнего закона композиции $(\alpha, x) \to \alpha \top x$, имеющего своей областью операторов кольцо A и удовлетворяющего следующим аксиомам:*

(M_I) $\alpha \top (x+y) = (\alpha \top x) + (\alpha \top y)$, *каковы бы ни были* $\alpha \in A$, $x \in E$, $y \in E$;

(M_{II}) $(\alpha+\beta) \top x = (\alpha \top x) + (\beta \top x)$, *каковы бы ни были* $\alpha \in A$, $\beta \in A$, $x \in E$;

M_{III}) $\alpha \top (\beta \top x) = (\alpha\beta) \top x$, *каковы бы ни были* $\alpha \in A$, $\beta \in A$, $x \in E$.

Аксиома (M_I) означает, что внешний закон A-модуля *дистрибутивен* относительно заданного на E сложения; тем самым модуль всегда является коммутативной группой с операторами.

Если в определении 1 вместо аксиомы (M_{III}) выполняется аксиома

(M'_{III}) $\alpha \top (\beta \top x) = (\beta\alpha) \top x$, *каковы бы ни были* $\alpha \in A$, $\beta \in A$, $x \in E$.

то E, наделенное определяемой так алгебраической структурой, **называют** *правым модулем относительно* A, или *правым модулем над* A, или также *правым* A*-модулем*.

Для внешнего закона композиции левого (соответственно правого) модуля чаще всего используют *мультипликативное* обозначение, записывая оператор слева (соответственно справа); условие (M_{III}) записывается тогда в виде $\alpha(\beta x) = (\alpha\beta)\, x$, а условие ($M'_{III}$) — в виде $(x\beta)\alpha = x(\beta\alpha)$.

Каждый *правый* модуль над кольцом A есть *левый* модуль над кольцом A^0, *противоположным* A (гл. I, § 8, n° 1). Это показывает, что при изложении свойств модулей можно систематически ограничиваться рассмотрением либо левых, либо правых модулей; за исключением § 6 (где в целях удобства обозначения рассматриваются правые модули), мы будем вести изложение применительно к левым модулям и, говоря (просто) *модуль*, всегда будем подразумевать левый модуль с мультипликативно записываемым внешним законом.

Если кольцо A *коммутативно*, понятия правого и левого модулей относительно A совпадают.

Отображения $x \to \alpha x$ модуля E в себя называются его *гомотетиями* (гл. I, § 6, n° 9); в силу (M_I) они являются эндоморфизмами структуры коммутативной группы E (*без операторов*), но, вообще, не эндоморфизмами структуры модуля E (гл. I, § 6, n° 12). Для

каждого $\alpha \in A$ имеем $\alpha 0 = 0$; в силу (M_{II}) также $0x = 0$ для каждого $x \in E$; из этих двух тождеств вытекает, что $\alpha(-x) = (-\alpha)x = -(\alpha x)$, каковы бы ни были $\alpha \in A$ и $x \in E$.

Если в множестве E задана структура модуля относительно кольца A и B — любое *подкольцо* этого кольца, то заданный на E коммутативный групповой закон и *сужение* внешнего закона на B (гл. I, § 3) определяют в E структуру модуля *относительно* B.

Примеры. 1) Кольцо есть одновременно левый и правый модуль относительно самого себя, а значит, также относительно любого своего подкольца. Рассматривая кольцо A как левый (соответственно правый) A-модуль, мы будем, во избежание всякой путаницы, обозначать его A_s (соответственно A_d).

2) Структура группы с операторами, определяемая в (аддитивно обозначаемой) коммутативной группе G внешним законом $(n, x) \to nx$ (гл. I, § 6, n° 9), есть структура модуля относительно кольца $\mathbf{Z}$ рациональных целых чисел.

3) Пусть G — аддитивно обозначаемая коммутативная группа и $\mathscr{E}$ — ее *кольцо эндоморфизмов* (гл I, § 8, n° 1; напомним, что произведением fg эндоморфизмов f и g служит, по определению эндоморфизм $f \circ g$); внешний закон композиции $(f, x) \to f(x)$ операторов $f \in \mathscr{E}$ и элементов $x \in G$ определяет в G структуру левого модуля относительно кольца $\mathscr{E}$.

4) Пусть G, как всегда, — аддитивная группа и A — любое кольцо. Положив $\alpha x = 0$ для каждого $\alpha \in A$ и каждого $x \in G$, мы определим в G структуру левого A-модуля.

2. *Унитарные модули. Векторные пространства*

Определение 2. *A-модуль E называется унитарным, если кольцо A обладает единицей ε, являющейся одновременно нейтральным оператором внешнего закона* (иными словами, если $\varepsilon x = x$ для каждого $x \in E$).

В унитарном модуле E для каждого целого $n \in \mathbf{Z}$ и каждого $x \in E$ имеем $nx = (n\varepsilon)x$. Если α — *обратимый* элемент кольца A, то гомотетия $x \to \alpha x$ есть *автоморфизм* структуры коммутативной группы E (без операторов), ибо $y = \alpha x$ влечет $x = \alpha^{-1}(\alpha x) = \alpha^{-1}y$.

Встречающиеся в алгебре модули в большинстве своем унитарны. Если кольцо A обладает единицей, то A-модули A_s и A_d унитарны; модули, определенные в примерах 2 и 3 n° 1, унитарны.

Наиболее важны унитарные модули, кольцом операторов которых служит *тело*:

Определение 3. *Левым* (соответственно *правым*) *векторным пространством над телом K называют унитарный левый* (соответственно *правый*) *K-модуль.*

Элементы векторного пространства часто называют *векторами*; элементы тела операторов именуются тогда *скалярами*. Допуская вольность речи, эту терминологию переносят иногда на произвольные модули.

Примеры. 1) Тело есть одновременно левое и правое векторное пространство относительно любого своего подтела.

°2) Трехмерное числовое пространство $\mathbf{R}^3$ классической аналитической геометрии есть векторное пространство относительно поля $\mathbf{R}$ вещественных чисел, если за произведение tx числа t и точки x с координатами x_1, x_2, x_3 принята точка с координатами tx_1, tx_2, tx_3.

Точно так же множество всех числовых функций, определенных на произвольном фиксированном множестве F, есть векторное пространство относительно $\mathbf{R}$, если за произведение tf вещественного числа t и такой функции f принята числовая функция $x \to tf(x)$.$_\circ$

Согласно предыдущему, в векторном пространстве E над телом K каждая гомотетия $x \to \alpha x$, соответствующая элементу $\alpha \neq 0$ из K, есть автоморфизм структуры коммутативной группы (без операторов) E.

3. Подмодули и фактормодули

Пусть E — модуль; если M — его *устойчивая* подгруппа (гл. I, § 6, n° 10), то, очевидно, структура, индуцированная в M гл. I, § 4, n° 2) структурой модуля E, является структурой модуля; множество M, наделенное этой структурой, называется *подмодулем* модуля E. Тем самым подмодули обладают всеми свойствами устойчивых подгрупп. В частности, сумма $M+N$ и пересечение $M \cap N$ любых двух подмодулей M и N модуля E снова являются его подмодулями.

Если E — унитарный модуль, то и все его подмодули унитарны. В частности, каждый подмодуль *векторного пространства* E есть векторное пространство; его называют *векторным подпространством* (или просто *подпространством*, если нет опасности смешения) векторного пространства E.

Примеры. 1) Множество, сводящееся к 0, является подмодулем любого модуля E (*нулевой* подмодуль).

2) Пусть A — кольцо. Подмодули модуля A_s (соответственно A_d) — это не что иное, как *левые* (соответственно *правые*) *идеалы* кольца A.

3) Пусть E — A-модуль, $x \in E$ и $\mathfrak{a}$ — левый идеал кольца A. Множество всех элементов ax, где a пробегает $\mathfrak{a}$, образует в E подмодуль, обозначаемый $\mathfrak{a}x$.

4) Каждая подгруппа аддитивной группы G, рассматриваемой как модуль относительно $\mathbf{Z}$ (с законом $(n, x) \to nx$), образует в G подмодуль.

°5) Пусть I — открытый интервал числовой прямой $\mathbf{R}$; множество C всех числовых функций, определенных и *непрерывных* на I, есть подпространство векторного пространства всех числовых функций на I. Аналогично множество D всех *дифференцируемых* функций на I есть подпространство пространства C.$_0$

Замечание. Пусть E — A-модуль и B — подкольцо кольца A. Каждый подмодуль A-модуля E есть также подмодуль B-модуля E, но обратное неверно: например, если A — тело и B — его подтело, то подпространство B_s векторного пространства A_s (относительно тела B) при $B \neq A$ не будет векторным пространством относительно тела A.

Пусть E — модуль. Каждое отношение эквивалентности, *согласующееся* (гл. I, § 4, n° 3) со структурой модуля E, имеет вид $x - y \in M$, где M — устойчивая подгруппа группы с операторами E (гл. I, § 6, n° 11), т. е. *подмодуль* модуля E. При этом, как непосредственно проверяется (см. гл. I, § 5), структура группы с операторами E/M (гл. I, § 6, n° 11) есть структура модуля; наделенное этой структурой, E/M называется *фактормодулем* модуля E по подмодулю M.

Каждый фактормодуль E/M унитарного A-модуля E унитарен, ибо единица ε кольца A, оставляя инвариантным каждый элемент из E, тем более оставляет инвариантным каждый класс по модулю M. В частности, каждый фактормодуль *векторного пространства* E есть векторное пространство; оно называется *векторным факторпространством* (или просто *факторпространством*) векторного пространства E.

Пример. Каждый левый идеал $\mathfrak{a}$ кольца A определяет фактормодуль $A_s/\mathfrak{a}$ A-модуля A_s; этот фактормодуль часто для краткости обозначают $A/\mathfrak{a}$; но когда $\mathfrak{a}$ — *двусторонний* идеал, не следует смешивать структуру *факторкольца* в $A/\mathfrak{a}$ (гл. I, § 8, n° 5) с его структурой левого модуля относительно кольца A.

4. Произведение модулей. Прямая сумма конечного семейства подмодулей. Дополнительные подмодули

Пусть $(E_\iota)_{\iota\in I}$ — семейство модулей над одним и тем же кольцом A. Как легко видеть, *произведение* структур модулей, заданных в множествах E_ι (гл. I, § 4, n° 5), есть структура A-модуля в множестве $E=\prod_{\iota\in I}E_\iota$. Наделенное этой структурой, E называется *произведением модулей* E_ι; таким образом, если $x=(x_\iota)$, $y=(y_\iota)$ — элементы этого модуля, то $x+y=(x_\iota+y_\iota)$ и $\alpha x=(\alpha x_\iota)$ для каждого элемента $\alpha\in A$.

Все свойства произведений групп с операторами, установленные в § 6 главы I, относятся и к произведениям модулей. В частности, если M_ι для каждого $\iota\in I$ — подмодуль модуля E_ι, то множество $M=\prod_{\iota\in I}M_\iota\subset E$ есть подмодуль модуля E, изоморфный произведению модулей M_ι. Если $M_\iota=E_\iota$ для каждого индекса из некоторого $J\subset I$ и $M_\iota=\{0\}$ для всех индексов $\iota\in\complement J$, то подмодуль $E'_J=\coprod_{\iota\in I}M_\iota$ модуля E изоморфен произведению $E_J=\prod_{\iota\in J}E_\iota$ модулей E_ι с $\iota\in J$. В случае, когда J сводится к одному индексу $\varkappa$, подмодуль E'_J обозначается также $E'_\varkappa$ и называется *компонентой* с индексом $\varkappa$ (или $\varkappa$-*й компонентой*) модуля E; он изоморфен модулю $E_\varkappa$ и чаще всего отождествляется с ним.

Если все модули E_ι унитарны, то унитарно и их произведение. В частности, произведение семейства *векторных пространств* над одним и тем же телом K есть векторное пространство над K.

Важным примером произведения модулей является произведение, все сомножители E_ι которого совпадают с модулем A_s; это произведение обозначается A_s^I или просто A^I, если можно не опасаться смешения; его элементами являются всевозможные *отображения* I *в* A.

Произведение E *конечного* семейства $(E_i)_{1\leqslant i\leqslant n}$ модулей есть *прямая сумма* (гл. I, § 6, n° 6) подмодулей-компонент E'_i $(1\leqslant i\leqslant n)$; обратно, если модуль E есть прямая сумма конечного семейства $(M_i)_{1\leqslant i\leqslant n}$ своих подмодулей, то отображение, относящее элементу $(x_i)_{1\leqslant i\leqslant n}$ из $\coprod_{1\leqslant i\leqslant n}M_i$ сумму $\sum_{i=1}^{n}x_i$, есть (называемый *каноническим*) *изоморфизм* $\coprod_{1\leqslant i\leqslant n}M_i$ на E (гл. I, § 6, предложение 6).

Определение 4. *Подмодули M_1, M_2 модуля E называются дополнительными, а каждый из них — дополнением другого, если E есть прямая сумма M_1 и M_2.*

Для того чтобы M_1 и M_2 были дополнительными, необходимо и достаточно, чтобы $E = M_1 + M_2$ и $M_1 \cap M_2 = \{0\}$ (гл. I, § 6, предложение 7).

В произвольном модуле E не всякий подмодуль обладает дополнением (см. упражнения 11 и 26).

Предложение 1. *Если M_1 и M_2 — дополнительные подмодули модуля E, то отображение, относящее каждому $x \in M_2$ его класс* (mod M_1), *есть изоморфизм M_2 на E/M_1.*

Действительно, это отображение, будучи сужением на M_2 канонического отображения E на E/M_1, есть представление M_2 в E/M_1; оно отображает M_2 *на* E/M_1, поскольку каждый элемент из E сравним (mod M_1) с некоторым элементом из M_2; наконец, оно *взаимно однозначно*, поскольку $M_1 \cap M_2 = \{0\}$.

Изоморфизм, определенный в предложении 1, и обратный ему изоморфизм называются *каноническими*.

Следствие. *Если M_2 и M_3 — подмодули, дополнительные к одному и тому же подмодулю M_1, то отношение $x_2 \equiv x_3$* (mod M_1) *между элементами $x_2 \in M_2$ и $x_3 \in M_3$ устанавливает взаимно однозначное соответствие между M_2 и M_3.*

Это соответствие и два составляющих его взаимно обратных изоморфизма называются *каноническими*.

Замечания. 1) При (каноническом) отождествлении E с $M_1 \times M_2$ изоморфизм, определяемый в предложении 1, превращается в канонический изоморфизм M_2 на $(M_1 \times M_2)/M_1$ (гл. I, § 6, n° 5). По этой причине канонический изоморфизм M_3 на M_2 называют также *проектированием M_3 на M_2 параллельно M_1* (при указанном отождествлении это действительно сужение на M_3 проектирования E на M_2).

2) Определение 4, предложение 1 и его следствие справедливы для любых коммутативных групп с операторами.

5. *Линейные комбинации*

Пусть I — произвольное множество индексов и $(x_\iota)_{\iota \in I}$ — семейство элементов A-модуля (или, более общим образом, коммутативной группы с операторами) E такое, что множество J

тех индексов ι, для которых $x_\iota \neq 0$, *конечно*; условимся обозначать через $\sum_{\iota \in I} x_\iota$ и называть *суммой* семейства $(x_\iota)_{\iota \in I}$ сумму $\sum_{\iota \in J} x_\iota$; если $x_\iota = 0$ для всех $\iota \in I$, то $J = \varnothing$ и, следовательно (гл. 1, § 2, определение 2), $\sum_{\iota \in I} x_\iota = 0$. Можно также сказать, что сумма семейства $(x_\iota)_{\iota \in I}$ есть общее значение сумм $\sum_{\iota \in H} x_\iota$ для всех конечных множеств $H \subset I$ таких, что $x_\iota = 0$ при $\iota \in \complement H$; в случае конечного I это вновь дает понятие суммы конечного семейства (определенное в главе I).

Разумеется, символ $\sum_{\iota \in I} x_\iota$ не имеет смысла для семейства $(x_\iota)_{\iota \in I}$, в котором $x_\iota \neq 0$ для бесконечного множества индексов ι (во всяком случае, покуда E не наделено топологической структурой; см. Общ. топ., гл. III, § 4). Всюду в этой главе, где используется указанное обозначение, подразумевается, если только не оговорено противное, что $x_\iota = 0$ для всех кроме конечного числа индексов ι.

Очевидно, имеют место формулы

$$\sum_{\iota \in I} (x_\iota + y_\iota) = \sum_{\iota \in I} x_\iota + \sum_{\iota \in I} y_\iota, \tag{1}$$

$$\sum_{\iota \in I} \alpha x_\iota = \alpha \sum_{\iota \in I} x_\iota \qquad (\alpha \in A). \tag{2}$$

Определение 5. *Говорят, что элемент x A-модуля E есть линейная комбинация семейства $(a_\iota)_{\iota \in I}$ элементов из E с коэффициентами из A, если существует семейство $(\lambda_\iota)_{\iota \in I}$ элементов из A такое, что $\lambda_\iota = 0$ для всех кроме конечного числа индексов ι и $x = \sum_{\iota \in I} \lambda_\iota a_\iota$. Каждое семейство $(\lambda_\iota)_{\iota \in I}$, обладающее этим свойством, называется семейством коэффициентов линейной комбинации x* (относительно семейства (a_ι)).

Вообще говоря, существуют *различные* семейства коэффициентов, удовлетворяющие соотношению $x = \sum_\iota \lambda_\iota a_\iota$ (см. n° 6).

Заметим, что (в силу соглашения, принятого в n° 1 § 2 главы I) 0 есть линейная комбинация *пустого семейства* элементов из E.

Предложение 2. *Подмодуль унитарного A-модуля E, порожденный* (гл. I, § 6, п° 10) *семейством $(a_\iota)_{\iota\in I}$ элементов из E, совпадает с множеством всевозможных линейных комбинаций семейства (a_ι).*

Действительно, каждый подмодуль модуля E, содержащий все a_ι, содержит также все их линейные комбинации; обратно, из формул (1) и (2) вытекает, что множество M всех линейных комбинаций элементов a_ι есть подмодуль модуля E; так как при этом $a_\iota = \varepsilon a_\iota$, где ε — единица кольца A, то M содержит все a_ι и, следовательно, есть наименьший содержащий их подмодуль модуля E.

Определение 6. *Моногенным модулем называется модуль, порожденный одним элементом.*

Предложение 2 показывает, что если E — унитарный моногенный A-модуль и a — любой порождающий его элемент, то E совпадает с множеством Aa всех элементов λa, где λ пробегает A.

Примеры. 1) Каждая моногенная группа, будучи коммутативной, является моногенным Z-модулем.

2) Если A — коммутативное кольцо с единицей, то моногенные подмодули A-модуля A — это не что иное, как *главные идеалы* (гл. I, § 8, п° 6) кольца A.

6. Свободные семейства. Базисы

Определение 7. *Семейство $(a_\iota)_{\iota\in I}$ элементов A-модуля E называется свободным, если отношение* $\sum_{\iota\in I} \lambda_\iota a_\iota = 0$ (где $\lambda_\iota = 0$ для всех кроме конечного числа индексов ι) *влечет $\lambda_\iota = 0$ для всех ι.*

Семейство (a_ι), не являющееся свободным, называется *зависимым*.

Любые два элемента свободного семейства (a_ι) в унитарном A-модуле E, имеющие различные индексы, сами *различны*; действительно, из $a_\alpha = a_\beta$, где $\alpha \neq \beta$, вытекало бы $\sum_\iota \lambda_\iota a_\iota = 0$, где $\lambda_\alpha = \varepsilon$, $\lambda_\beta = -\varepsilon$ (ε — единица кольца A) и $\lambda_\iota = 0$ для всех остальных индексов. $S \subset E$ называется *свободным множеством* (или *свободной системой*), если семейство, определяемое

тождественным отображением S на себя, свободное (причем в этом случае и каждое семейство, определяемое взаимно однозначным отображением какого-нибудь множества индексов на S, свободное). Элементы свободного подмножества модуля E называют также *линейно независимыми*. Множество в E, не являющееся свободным, называют *зависимым* (или *зависимой системой*), а его элементы — *линейно зависимыми*.

Предложение 3. *Для того чтобы семейство $(a_\iota)_{\iota\in I}$ элементов модуля E было свободным, необходимо и достаточно, чтобы каждое его конечное подсемейство было свободным.*

Доказательство непосредственно вытекает из определения 7 и определения суммы бесконечного семейства элементов из E.

Каждое подмножество свободного множества свободное. В частности, пустое подмножество A-модуля E — свободное; каждое подмножество свободного множества, сводящееся к одному элементу, свободное. Элемент $x\in E$ называется *свободным*, если $\{x\}$ есть свободное множество, т. е. если $\alpha x=0$ влечет $\alpha=0$.

Замечания. 1) В векторном пространстве E каждый элемент $x\neq 0$ свободный, поскольку из $\alpha x=y$ при $\alpha\neq 0$ следует $x=\alpha^{-1}y$.

2) Из предложения 3 вытекает, что множество всех свободных подмножеств A-модуля E, упорядоченное по включению, *индуктивно* (Теор. ми., Рез., § 6, n° 9); будучи непустым, оно, в силу теоремы Цорна, обладает *максимальным* элементом (a_ι). Отсюда следует, что для каждого $x\in E$ в кольце A существуют элемент $\mu\neq 0$ и семейство элементов (λ_ι) таких, что $\mu x=\sum_\iota \lambda_\iota a_\iota$ (см. § 3).

В силу определения 7, никакой элемент $a_\varkappa$ свободного семейства (a_ι) в унитарном A-модуле не является линейной комбинацией элементов a_ι с индексами $\neq\varkappa$. Но, обратно, семейство (a_ι), удовлетворяющее этому условию, не обязательно является свободным (см., однако, § 3, n° 1).

Например, пусть A — кольцо целостности с единицей и a, b — его ненулевые элементы; в A, рассматриваемом как A-модуль, a и b образуют зависимую систему, ибо $(-b)a+ab=0$. Но, вообще говоря, не существует элемента $x\in A$, для которого бы $b=xa$ или $a=xb$.

Если B — подкольцо кольца A, то семейство, свободное в A-модуле E, будет свободным также в структуре B-модуля,

полученной путем *сужения* кольца операторов до B; обратное же, вообще говоря, неверно (см. § 5). Во избежание недоразумений, семейство, свободное в структуре A-модуля (соответственно B-модуля), называется *свободным относительно* A (соответственно *относительно* B).

Определение 8. *Базисом унитарного модуля E называется всякое свободное семейство элементов из E, порождающее E. Унитарный модуль E, обладающий базисом, называется свободным.*

Допуская вольность речи, множество всех элементов базиса унитарного модуля E мы также называем *базисом* этого модуля.

Каждое свободное семейство элементов унитарного модуля E есть базис порожденного этим семейством подмодуля; в частности, пустое семейство элементов из E есть базис подмодуля $\{0\}$.

Замечания. 1) Унитарный модуль не обязательно обладает базисом. Например, мы видели выше, что в кольце целостности A с единицей, рассматриваемом как A-модуль, не существует свободных множеств, содержащих более одного элемента; поэтому *неглавный* идеал в A не может иметь базиса; а ниже нам встретятся кольца целостности, обладающие неглавными идеалами.

2) Свободный модуль может содержать элементы $\neq 0$, не являющиеся свободными. Например, если A—кольцо с единицей, то A-модуль A_s свободный, но (правые) делители нуля кольца A не являются в A_s свободными элементами.

Пусть $(a_\lambda)_{\lambda\in L}$ — базис унитарного A-модуля E. Согласно предложению 2, каждое $x\in E$ есть линейная комбинация элементов a_λ: $x=\sum_{\lambda\in L}\xi_\lambda a_\lambda$; при этом ξ_λ *однозначно* определены, ибо соотношение $\sum_\lambda \xi_\lambda a_\lambda=\sum_\lambda \xi'_\lambda a_\lambda$ может быть переписано в виде $\sum_\lambda (\xi_\lambda-\xi'_\lambda)a_\lambda=0$, откуда $\xi_\lambda=\xi'_\lambda$ для каждого λ, поскольку (a_λ) — свободное семейство; ξ_λ называют *компонентой* (или, допуская вольность речи, *координатой*) *с индексом* λ (или λ-*й компонентой*) элемента x относительно базиса (a_λ).

В частности, если E—*моногенный* унитарный A-модуль и a—элемент, образующий его базис, то каждое $x\in E$ единственным образом записывается в виде $x=\xi a$; ξ называют иногда *отношением*

вектора x к вектору a; если при этом кольцо A *коммутативно*, то иногда отношение $x = \xi a$, допуская вольность, записывают в виде $\xi = \frac{x}{a}$.

Предложение 4. *Пусть фактормодуль E/M_1 унитарного модуля E по его подмодулю M_1 обладает базисом $(\dot{a}_\iota)_{\iota \in I}$. Каковы бы ни были элементы a_ι классов $\dot{a}_\iota \pmod{M_1}$, семейство $(a_\iota)_{\iota \in I}$ является свободным и порождает подмодуль M_2, дополнительный к M_1.*

Действительно, по предположению, отношение $\sum_\iota \lambda_\iota \dot{a}_\iota = 0$ влечет $\lambda_\iota = 0$ для всех ι; так как оно равносильно отношению $\sum_\iota \lambda_\iota a_\iota \in M_1$, то мы видим, с одной стороны, что (a_ι) есть свободное семейство и, с другой стороны, что порожденный им подмодуль M_2 обладает свойством $M_1 \cap M_2 = \{0\}$. Наконец, так как каждый элемент из E/M_1 есть линейная комбинация классов $\dot{a}_\iota$, то каждое $x \in E$ сравнимо $(\mathrm{mod}\, M_1)$ с некоторой линейной комбинацией элементов a_ι, а это показывает, что $E = M_1 + M_2$.

Следствие. *Если фактормодуль E/M_1 свободный, то M_1 обладает в E дополнением.*

7. Сумма и прямая сумма любого семейства подмодулей

Предложение 5. *Подмодуль, порожденный объединением семейства $(M_\iota)_{\iota \in I}$ подмодулей модуля E, совпадает с множеством сумм $\sum_{\iota \in I} x_\iota$, где $(x_\iota)_{\iota \in I}$ пробегает множество всех тех семейств элементов из E, в которых $x_\iota = 0$ для всех кроме конечного числа индексов ι и $x_\iota \in M_\iota$ для каждого $\iota \in I$.*

Действительно, каждый подмодуль модуля E, содержащий объединение $\bigcup_{\iota \in I} M_\iota$, содержит и все эти суммы, а, с другой стороны, из формул (1) и (2) следует, что множество, образованное этими суммами, есть подмодуль модуля E.

Если I конечно, то подмодуль, порожденный объединением подмодулей M_ι, есть не что иное, как их *сумма* $\sum_{\iota \in I} M_\iota$ (гл. I, § 1). Распространяя это, вводим следующее определение:

Определение 9. *Суммой* $\sum_{\iota\in I} M_\iota$ *произвольного семейства* $(M_\iota)_{\iota\in I}$ *подмодулей модуля* E *называется подмодуль, порожденный объединением этого семейства.*

Замечание. Предложение 5 может рассматриваться как обобщение предложения 2: действительно, это последнее сразу вытекает из предложения 5 и того факта, что подмодуль унитарного A-модуля, порожденный элементом a, есть множество Aa всех λa, где λ пробегает A.

Определение 10. *Сумма семейства* $(M_\iota)_{\iota\in I}$ *подмодулей модуля* E *называется прямой, если каждый элемент этой суммы единственным образом записывается в виде* $\sum_{\iota\in I} x_\iota$ (где $x_\iota \in M_\iota$ для каждого ι и $x_\iota = 0$ для всех кроме конечного числа индексов).

Определение 10 обобщает определение прямой суммы, уже данное в n° 6 § 6 главы I для случая *конечного* I. Оно означает, что отношение $\sum_{\iota\in I} x_\iota = \sum_{\iota\in I} y_\iota$, где $x_\iota \in M_\iota$ и $y_\iota \in M_\iota$ для каждого ι, влечет $x_\iota = y_\iota$ для всех ι или также (в силу (1) и того, что M_ι — подмодули) что *отношение* $\sum_{\iota\in I} z_\iota = 0$, *где* $z_\iota \in M_\iota$ *для каждого* ι, *влечет* $z_\iota = 0$ *для всех* ι.

Этому условию можно придать также следующий вид:

Предложение 6. *Для того чтобы сумма семейства* $(M_\iota)_{\iota\in I}$ *подмодулей модуля* E *была прямой, необходимо и достаточно, чтобы пересечение* $M_\varkappa$ *с суммой тех* M_ι, *индексы* ι *которых* $\neq \varkappa$, *для каждого* $\varkappa \in I$ *сводилось к* 0.

Необходимость условия очевидна; достаточность его вытекает из того, что отношение $\sum_{\iota\in I} z_\iota = 0$ может быть для каждого $\varkappa \in I$ записано в виде $z_\varkappa = \sum_{\iota\neq\varkappa} (-z_\iota)$ и потому влечет $z_\varkappa = 0$.

Если E — прямая сумма семейства (M_ι) своих подмодулей, то каждому $x \in E$ отвечает *однозначно* определенное семейство (x_ι) такое, что $x_\iota \in M_\iota$ для каждого ι и $x = \sum_\iota x_\iota$; элемент x_ι, соответствующий ι, называется для каждого ι *компонентой* x в подмодуле M_ι; полагая $x_\iota = k_\iota(x)$, имеем следующее предложение:

Предложение 7. *Каковы бы ни были* $x \in E$, $y \in E$ *и* $\alpha \in A$,

$$k_\iota(x+y) = k_\iota(x) + k_\iota(y). \qquad (3)$$

$$k_\iota(\alpha x) = \alpha k_\iota(x). \qquad (4)$$

Действительно, с одной стороны, $x+y = \sum_\iota k_\iota(x+y)$, а с другой, согласно (1), $x+y = \sum_\iota k_\iota(x) + \sum_\iota k_\iota(y) = \sum_\iota (k_\iota(x) + k_\iota(y))$; из определения 10 следует тогда (3) для каждого ι. Аналогично доказывается (4).

Пусть модуль E есть прямая сумма семейства $(M_\iota)_{\iota \in I}$ своих подмодулей; если $(J_\lambda)_{\lambda \in L}$ — любое *разбиение* множества I и N_λ означает (тоже прямую) сумму $\sum_{\iota \in J_\lambda} M_\iota$, то E есть прямая сумма подмодулей N_λ. Обратно, если $(M_\iota)_{\iota \in I}$ — семейство подмодулей модуля E такое, что сумма N_λ каждого подсемейства $(M_\iota)_{\iota \in J_\lambda}$ прямая, а E есть прямая сумма семейства $(N_\lambda)_{\lambda \in L}$, то E есть также прямая сумма семейства $(M_\iota)_{\iota \in I}$.

Для любого семейства $(M_\iota)_{\iota \in I}$ A-модулей можно определить A-модуль, являющийся прямой суммой семейства своих подмодулей, соответственно изоморфных модулям M_ι; достаточно взять в произведении $\prod_{\iota \in I} M_\iota$ модулей M_ι подмодуль M', являющийся суммой модулей-компонент M'_ι (n° 4), которая будет очевидно прямой; допуская вольность речи, мы будем (если это не сможет привести к путанице), отождествляя каждое M_ι с модулем M'_ι, отмеченным тем же индексом, называть M *прямой суммой* семейства $(M_\iota)_{\iota \in I}$; если I *конечно*, то M' совпадает с произведением $\prod_{\iota \in I} M_\iota$ модулей M_ι. Если все M_ι совпадают с одним и тем же модулем M, то их прямая сумма обозначается $M^{(I)}$.

Предложение 8. *Пусть* (M_ι) *— семейство подмодулей модуля* E *и* M *— прямая сумма этого семейства. Тогда сумма* N *подмодулей* M_ι *изоморфна некоторому фактормодулю модуля* M.

Действительно, каждый элемент из M имеет вид (x_ι), где $x_\iota \in M_\iota$ для каждого ι и $x_\iota = 0$ для всех кроме конечного числа

индексов. Поставив ему в соответствие элемент $\sum_{\iota\in I} x_\iota$ суммы N, в силу формул (1) и (2) и предложения 5 получим *представление M на N*, откуда и следует справедливость утверждения (гл. I, § 6, теорема 5).

Отметим, наконец, что если модуль E есть прямая сумма семейства $(M_\iota)_{\iota\in I}$ своих подмодулей и каждый модуль M_ι обладает базисом B_ι, то объединение всех B_ι будет базисом модуля E.

Замечание. За исключением последнего свойства, все определения и предложения, сформулированные в этом n°, без всяких изменений распространяются на любые коммутативные группы с операторами.

8. *Модули формальных линейных комбинаций*

Понятие прямой суммы позволяет дать другое истолкование понятиям свободного семейства и базиса. Для того чтобы семейство (a_ι) элементов унитарного A-модуля E было свободным, *необходимо и достаточно, чтобы каждый из элементов a_ι был свободным, а сумма моногенных подмодулей Aa_ι* (порожденных соответственно элементами a_ι) — *прямой*.

Предложение 9. *Для того чтобы унитарный A-модуль E обладал базисом $(a_\lambda)_{\lambda\in L}$, необходимо и достаточно, чтобы он был изоморфен модулю $A_s^{(L)}$.*

Действительно, отображение, относящее каждому $x\in E$ семейство $(\xi_\lambda)_{\lambda\in L}$ его компонент относительно базиса $(a_\lambda)_{\lambda\in L}$ модуля E, в силу предложения 7 и определения базиса есть изоморфизм E на $A_s^{(L)}$.

Обратно, пусть L — произвольное множество и e_λ для каждого $\lambda\in L$ — элемент из $A_s^{(L)}$, компонента которого с индексом λ равна единице ε кольца A, а все остальные компоненты равны нулю; для каждого $x=(\xi_\lambda)$ из $A_s^{(L)}$ имеем $x=\sum_{\lambda\in L}\xi_\lambda e_\lambda$, так что элементы e_λ образуют базис модуля $A_s^{(L)}$; он называется *каноническим базисом* этого модуля.

Следствие. *Моногенный подмодуль Aa унитарного A-модуля E, порожденный свободным элементом $a\in E$, изоморфен A_s.*

Пусть T — произвольное множество; так как его отображение $t \longrightarrow e_t$ на канонический базис модуля $A_s^{(T)}$ взаимно однозначно, то часто T *отождествляют* посредством указанного отображения с этим базисом. Иными словами, элементы модуля $A_s^{(T)}$ записывают в виде $\sum_{t \in T} \xi_t t$ вместо $\sum_{\iota \in I} \xi_\iota e_\iota$. При этом соглашении элементы модуля $A_s^{(T)}$ называют *формальными линейными комбинациями* (с коэффициентами из A) *элементов множества* T, а модуль $A_s^{(T)}$ — *модулем формальных линейных комбинаций* (с коэффициентами из A) *элементов множества* T.

Предложение 10. *Пусть* $(a_\iota)_{\iota \in I}$ — *любое непустое семейство элементов унитарного* A-*модуля* E. *Подмодуль* M *модуля* E, *порожденный семейством* (a_ι), *изоморфен фактормодулю модуля* $A_s^{(I)}$ *по его подмодулю* N, *образованному теми элементами* (ξ_ι), *для которых* $\sum_\iota \xi_\iota a_\iota = 0$.

Действительно, отнесение каждому элементу (ξ_ι) из $A_s^{(I)}$ элемента $\sum_\iota \xi_\iota a_\iota$ из E, в силу формул (1) и (2) и предложения 2, определяет представление u модуля $A_s^{(I)}$ на M. Так как, по своему определению, $N = \overset{-1}{u}(0)$, то справедливость предложения вытекает из теоремы 5 § 6 главы I.

Допуская вольность речи, подмодуль N модуля $A_s^{(I)}$ часто называют *модулем линейных соотношений между элементами семейства* (a_ι).

9. *Аннуляторы. Точные модули. Строение моногенных модулей*

Определение 11. *Аннулятором подмножества* F A-*модуля* E *называется множество тех элементов* $\alpha \in A$, *для которых* $\alpha x = 0$, *каково бы ни было* $x \in F$.

Очевидно, аннулятор любого множества $F \subset E$ есть *левый идеал* кольца A. Если $F \subset E$, $G \subset E$ и $F \subset G$, то аннулятор G содержится в аннуляторе F. Аннулятор объединения $\bigcup_\iota F_\iota$ любо-

го семейства (F_ι) подмножеств модуля E есть пересечение аннуляторов этих подмножеств. В частности, аннулятор множества F есть пересечение аннуляторов его элементов. Сказать, что элемент модуля E свободный, — все равно что сказать, что его аннулятор *нулевой*, т. е. сводится к элементу 0 (гл. I, § 8, n° 5).

В частности, так как каждый ненулевой элемент векторного пространства свободный (n° 6), то аннулятор любого множества элементов векторного пространства, из которых хоть один $\neq 0$, нулевой.

Аннулятор *подмодуля* M модуля E есть *двусторонний идеал* кольца A: действительно, если $\alpha x = 0$ для каждого $x \in M$, то также $\alpha(\beta x) = 0$ для каждого $x \in M$ и каждого $\beta \in A$, так что $\alpha\beta$ принадлежит аннулятору подмодуля M для каждого $\beta \in A$. В частности, аннулятор $\mathfrak{a}$ модуля E есть двусторонний идеал кольца A.

Обозначим через u_α для каждого $\alpha \in A$ гомотетию $x \to \alpha x$, порожденную оператором α; рассмотрим отображение $\alpha \to u_\alpha$ кольца A в кольцо $\mathscr{E}$ всех эндоморфизмов коммутативной группы (без операторов) E; аксиомы (M_{II}) и (M_{III}) показывают, что это отображение есть *представление* кольца A в кольцо $\mathscr{E}$; прообраз нулевого эндоморфизма относительно этого отображения есть как раз *аннулятор* $\mathfrak{a}$ модуля E; поэтому образ A при отображении $\alpha \to u_\alpha$ изоморфен факторкольцу $A/\mathfrak{a}$.

Мы называем модуль E *точным*, если его аннулятор $\mathfrak{a}$ *нулевой*. Пусть E — не точный модуль и $\dot{\alpha}$ — произвольный элемент факторкольца $A/\mathfrak{a}$; для каждого $x \in E$ элемент αx будет одним и тем же для всех α, принадлежащих классу $\dot{\alpha}$ (mod $\mathfrak{a}$); обозначим его $\dot{\alpha}x$; легко видеть, что отображение $(\dot{\alpha}, x) \to \dot{\alpha}x$ определяет в E (вместе со сложением) структуру *точного* модуля относительно факторкольца $A/\mathfrak{a}$; множество E, наделенное этой структурой, называется *точным модулем*, *ассоциированным* с заданным A-модулем E. Заметим, что каждый подмодуль A-модуля E есть также подмодуль ассоциированного с E точного модуля, и обратно.

Предложение 11. *Пусть A — кольцо с единицей. Каждый унитарный моногенный A-модуль изоморфен фактормодулю $A_s/\mathfrak{a}$, где $\mathfrak{a}$ — некоторый левый идеал кольца A; обратно, каждый фактормодуль модуля A_s есть унитарный моногенный A-модуль.*

Первое утверждение есть следствие предложения 10, примененного к случаю, когда I сводится к одному элементу: унитарный A-модуль E, порожденный элементом a, изоморфен $A_s/\mathfrak{a}$, где $\mathfrak{a}$ — аннулятор a. Обратное очевидно, ибо если $\mathfrak{a}$ — левый идеал кольца A с единицей ε, то модуль $A_s/\mathfrak{a}$ порождается классом $\varepsilon \pmod{\mathfrak{a}}$.

Поэтому, в силу теоремы 6 § 6 главы I, каждый подмодуль унитарного моногенного A-модуля E изоморфен фактормодулю $\mathfrak{b}/\mathfrak{a}$, где $\mathfrak{a}$ и $\mathfrak{b}$ — левые идеалы кольца A такие, что $\mathfrak{a} \subset \mathfrak{b}$; каждый фактормодуль модуля E изоморфен фактормодулю $A_s/\mathfrak{b}$ и, значит, сам является моногенным.

Не следует думать, что подмодуль моногенного модуля всегда является моногенным модулем; например, неглавные идеалы коммутативного кольца A с единицей являются немоногенными подмодулями моногенного A-модуля A.

Упражнения. 1) Пусть A — произвольное кольцо и A' — кольцо, полученное путем присоединения к A единицы по методу упражнения 3 § 8 главы I. Показать, что структуру любого A-модуля E можно рассматривать как получающуюся путем сужения до A области операторов структуры унитарного A'-модуля. E, наделенное как той, так и другой структурами, имеет одинаковые подмодули.

2) Пусть E — A-модуль и μ — центральный элемент кольца A такой, что $\mu x = \mu^2 x$ для каждого $x \in E$ (что, в частности, имеет место, если μ — *идемпотент* (гл. I, § 1, п° 4) кольца A); показать, что E есть прямая сумма своего подмодуля μE и подмодуля M, образованного теми $y \in E$, для которых $\mu y = 0$. В частности, если A обладает единицей ε, E есть прямая сумма унитарного подмодуля εE и подмодуля M такого, что $\alpha M = \{0\}$ для каждого $\alpha \in A$.

3) Моногенный подмодуль, порожденный элементом a произвольного A-модуля E, совпадает с множеством всех элементов вида $na + \lambda a$, где $n \in \mathbf{Z}$ и $\lambda \in A$.

4) Пусть M и N — подмножества A-модуля E, $\mathfrak{m}$ и $\mathfrak{n}$ — их аннуляторы; показать, что аннулятор пересечения $M \cap N$ содержит $\mathfrak{m} + \mathfrak{n}$, и привести пример, где он отличен от $\mathfrak{m} + \mathfrak{n}$.

5) Аннулятор подмножества F произведения $\prod_\iota E_\iota$ модулей E_ι есть пересечение аннуляторов проекций этого подмножества.

6) Аннулятор любого ненулевого элемента свободного унитарного A-модуля содержит лишь 0 и левые делители нуля кольца A; в частности, все элементы свободного A-модуля, где A — кольцо без делителей нуля, свободные.

7) Пусть A — кольцо без делителей нуля, содержащее единицу. Показать, что модуль A_s^n при $n>1$ не может быть моногенным. [См. § 3, упражнение 8, и гл. III, § 5.]

8) Пусть A — факторкольцо $\mathbf{Z}/(6)$, (e_1, e_2) — канонический базис A-модуля A^2 и $a=2e_1+3e_2$; показать, что хотя e_1 и e_2 образуют свободную систему, a и e_1, равно как a и e_2, образуют зависимые системы.

9) Пусть A — кольцо без делителей нуля, содержащее единицу, но не допускающее тела левых отношений (см. гл. I, § 9, упражнение 8). Показать, что для всякого свободного элемента a унитарного A-модуля E существуют элементы $b=\beta a$ и $c=\gamma a$ моногенного подмодуля, порожденного элементом a, образующие свободную систему.

10) Пусть A — кольцо с единицей, допускающее тело левых отношений (гл. I, § 9, упражнение 8), и E — унитарный A-модуль; показать, что если $(x_i)_{1\leqslant i\leqslant r}$ — свободная система в E и элементы y, z таковы, что как $x_1, \ldots, x_r, y$, так и $x_1, \ldots, x_r, z$ — зависимые системы, то также $x_2, \ldots, x_r, y, z$ — зависимая система. [Индукцией по r.]

11) Пусть A — кольцо с единицей, допускающее кольцо левых отношений. Показать, что в A-модуле A_s подмодуль, отличный от A_s и $\{0\}$, не обладает дополнением. [См. гл. I, § 9, упражнение 9.]

12) Пусть A — кольцо без делителей нуля, содержащее единицу. Показать, что если каждый его левый идеал является моногенным A-модулем, то A допускает тело левых отношений. [Использовать приведенное выше упражнение 7 и упражнение 9 § 9 главы I.]

*13) Пусть E — A-модуль, являющийся прямой суммой *бесконечного* семейства $(M_\iota)_{\iota\in I}$ своих подмодулей (не сводящихся к 0). Показать, что каждая система S образующих модуля E имеет мощность, не меньшую мощности множества I. [Пусть S — система образующих модуля E, F_x для каждого $x\in S$ — конечное множество тех индексов $\iota\in I$, для которых ι-я компонента x отлична от 0, и F — объединение множеств F_x, где x пробегает S. Показать, что F имеет мощность, не превосходящую мощности произведения $S\times\mathbf{N}$, а тем самым — мощности S, и что мощность F не может быть строго меньше мощности I.]

Вывести отсюда, что если E есть прямая сумма каждого из семейств $(M_\iota)_{\iota\in I}$, $(N_\varkappa)_{\varkappa\in K}$ своих моногенных подмодулей, то I и K равномощны. В частности, если E обладает бесконечным базисом B, то каждый другой базис модуля E равномощен B.

14) Показать, что каждый унитарный A-модуль, обладающий базисом с множеством индексов I, равномощен множеству $A\times I$, если хотя бы одно из множеств A, I бесконечно. [Воспользоваться тем, что множество всех конечных подмножеств бесконечного множества F равномощно F.]

*15) а) Говорят, что A-модуль удовлетворяет условию максимальности (соответственно минимальности), если множество *всех* его подмодулей удовлетворяет условию максимальности (соответственно минимальности; см. гл. I, § 6, упражнение 15). Показать, что

произведение $E \times F$ A-модулей E, F, удовлетворяющих условию максимальности (минимальности), также удовлетворяет этому условию. [Пусть (M_k) — возрастающая (соответственно убывающая) последовательность подмодулей модуля $E \times F$; рассматривая их проекции на E, установить существование индекса p такого, что для всех $k \geqslant p$ имеет место равенство $M_k = M_p + (M_k \cap F)$ (соответственно $M_p = M_k + (M_p \cap F)$, откуда следует, что M_p/M_k изоморфно $(M_p \cap F)/(M_k \cap F)$).]

б) Вывести отсюда, что для того, чтобы A-модуль A^n удовлетворял условию максимальности (соответственно минимальности), необходимо и достаточно, чтобы этому условию удовлетворяло A_s.

*16) а) Пусть A — кольцо с единицей такое, что A-модуль A_s удовлетворяет условию максимальности (упражнение 15). Показать, что каждая система образующих модуля A_s^n содержит по меньшей мере n элементов. [В противном случае при некотором $p < n$ существовали бы представление A_s^p на A_s^n и, следовательно, эндоморфизм u модуля A_s^n такой, что $u(A_s^n) = A_s^n$ и $u^{-1}(0) \neq \{0\}$; показать, что это несовместимо с условием максимальности в A_s^n.]

б) Пусть B — подкольцо кольца A, имеющее тот же единичный элемент, что и A. Показать, что также каждая система образующих B-модуля B_s^n содержит по меньшей мере n элементов. [Показать, что каждая система образующих модуля $B_s^n \subset A_s^n$ есть также система образующих модуля A_s^n.] Вывести отсюда, что если унитарный B-модуль E обладает конечным базисом, то всякий другой базис модуля E состоит из такого же числа элементов.

17) Пусть A — кольцо с единицей такое, что A-модуль A_s удовлетворяет условию минимальности (упражнение 15). Показать, что каждое свободное подмножество модуля A_s^n содержит не более n элементов. [В противном случае для некоторого $p > n$ существовал бы подмодуль модуля A_s^p, изоморфный A_s^p, но отличный от него, что несовместимо с условием минимальности в A_s^p (см. гл. I, § 6, упражнение 15).]

Вывести отсюда, что если унитарный A-модуль E обладает конечным базисом, то всякий другой базис этого модуля состоит из такого же числа элементов.

*18) Пусть A — кольцо без делителей нуля, содержащее единицу.

а) Показать, что если A допускает тело левых отношений K (гл. I, § 9, упражнение 8), E — векторное пространство над K и M — A-модуль, содержащийся в E, то каждое множество в M, свободное *относительно* A, будет также свободным *относительно* K.

б) Для того чтобы в A-модуле A_s^n не содержалось свободного множества, имеющего более n элементов, необходимо и достаточно,

чтобы A допускало тело левых отношений. [При доказательстве необходимости условия воспользоваться упражнением 9 § 9 гл. I; при доказательстве достаточности использовать а), заметив, что $A_s^n \subset K_s^n$, и применить упражнение 17 к K_s^n.]

19) Унитарный A-модуль E, обладающий рядом Жордана—Гёльдера длины n (гл. I, § 6, n° 14), имеет систему образующих, состоящую из n элементов. [Заметить, что если M и N — подмодули модуля E такие, что $M \supset N$ и M/N — простой модуль, то существует $a \in M$ такое, что $M = N + Aa$.]

*20) Пусть M — *простой* модуль (гл. I, § 6, определение 14) относительно кольца A. Показать, что *либо* $\mathfrak{a}M = \{0\}$ для каждого $\mathfrak{a} \in A$ и M состоит из конечного числа p элементов, где p — простое, *либо* $M = Aa$ для каждого $a \neq 0$, принадлежащего M. [Заметить, что $Ax \subset M$ для каждого $x \in M$, и рассмотреть подмодуль модуля M, образованный теми $x \in M$, для которых $Ax = \{0\}$.] Во втором случае аннулятор $\mathfrak{a}$ элемента a есть максимальный левый идеал кольца A и M изоморфно $A_s/\mathfrak{a}$. Обратно, если $\mathfrak{a}$ — максимальный левый идеал кольца A, то A-модуль $A_s/\mathfrak{a}$ — простой.

21) Пусть M и N — два полупростых подмодуля *) модуля E, имеющие соответственно длины m и n. Если пересечение $M \cap N$ имеет длину q, то сумма $M + N$ есть полупростой модуль длины p такой, что $p + q = m + n$.

22) Пусть E — вполне приводимый модуль (гл. I, § 6, упражнение 18), а M и N — его подмодули с полупростыми фактормодулями E/M и E/N, имеющими соответственно длины m и n. Показать, что $E/(M \cap N)$ и $E/(M + N)$ — полупростые, а их длины q и p связаны с m и n соотношением $p + q = m + n$.

*23) Вполне приводимый модуль (гл. I, § 6, упражнение 18) называется *однородным*, если он является прямой суммой своих простых подмодулей, изоморфных одному и тому же модулю. Пусть E — вполне приводимый модуль, являющийся прямой суммой семейства $(M_\iota)_{\iota \in I}$ своих простых подмодулей; тогда каждый его простой подмодуль изоморфен одному из M_ι (гл. I, § 6, упражнение 18б); сумма G_ι *всех* простых подмодулей модуля E, изоморфных M_ι, называется для каждого $\iota \in I$ ι-й *однородной компонентой* модуля E. Показать, что E есть прямая сумма семейства всех своих *различных* однородных компонент, а G_ι — сумма всех $M_\varkappa$, изоморфных M_ι.

*24) а) Пусть H — *однородный* вполне приводимый A-модуль (упражнение 23), являющийся прямой суммой семейства $(M_\iota)_{\iota \in I}$

*) Модуль M называется простым, если он не сводится к $\{0\}$ и не обладает подмодулями, отличными от M и $\{0\}$. Модуль M называется здесь полупростым модулем длины n, если он является прямой суммой некоторого конечного семейства $(M_i)_{1 \leqslant i \leqslant n}$ своих простых подмодулей (общее определение полупростого модуля см. в гл. VIII, § 3).— *Перев.*

своих попарно изоморфных простых подмодулей. Если E есть также прямая сумма второго семейства $(N_\varkappa)_{\varkappa\in K}$ своих простых подмодулей, то все они изоморфны подмодулям M_ι, а K равномощно I. [Ограничиться случаем бесконечного I; согласно упражнению 20, рассмотреть два случая соответственно тому, будет ли $AE=\{0\}$ или нет; в первом случае рассматривать E как вполне приводимый $\mathbf{Z}$-модуль; затем применить в обоих случаях упражнение 13.]

б) Пусть E — произвольный вполне приводимый A-модуль. Если E — прямая сумма каждого из двух семейств $(M_\iota)_{\iota\in I}$ и $(N_\varkappa)_{\varkappa\in K}$ своих простых подмодулей, то существует такое взаимно однозначное отображение φ множества I на K, что $N_{\varphi(\iota)}$ изоморфно M_ι для каждого ι. [С помощью упражнения 23 свести к а).]

25) Пусть E и F — изоморфные полупростые модули, V — подмодуль модуля E и W — подмодуль модуля F; если V и W изоморфны, то также E/V и F/W изоморфны. Показать на примере, что соответствующий результат для вполне приводимых модулей бесконечной длины неверен.

*26) Пусть E — A-модуль, каждый подмодуль которого обладает дополнением.

а) Показать, что и все подмодули F модуля E обладают этим свойством, т. е. каждый подмодуль в F обладает дополнением относительно F.

б) Показать, что каждый подмодуль модуля E обладает *простым* подмодулем. [Используя упражнение 1, свести к случаю унитарного A-модуля E; затем, используя а), упражнение 20 и теорему Круля (гл. I, § 8, теорема 2), доказать, что каждый моногенный подмодуль модуля E содержит простой подмодуль.]

в) Показать, что E есть сумма своих простых подмодулей и, следовательно (гл. I, § 6, упражнение 18), *вполне приводимо*. [Рассмотреть подмодуль модуля E, являющийся суммой всех простых подмодулей этого модуля.]

§ 2. Линейные отображения

1. Линейные функции

Определение 1. *Пусть E и F — модули относительно одного и того же кольца A. Линейным отображением E в F называется всякое представление* (гл. I, § 4, п° 4) *E в F.*

Иными словами, отображение u модуля E в F линейное, если $u(x+y)=u(x)+u(y)$, каковы бы ни были $x\in E$, $y\in E$, и $u(\lambda x)=\lambda u(x)$ при любых $x\in E$ и $\lambda\in A$.

Замечание. Если E и F — коммутативные группы, рассматриваемые как модули над кольцом $\mathbf{Z}$ (§ 1, n° 1), то каждое представление u группы (без операторов) E в группу (без операторов) F есть также линейное отображение E в F, поскольку соотношение $u(nx)=nu(x)$ сводится к $u(x+y)=u(x)+u(y)$ индукцией по n.

Примеры. 1) Проекция pr_J произведения $\prod_{\iota\in I} E_\iota$ семейства модулей на частичное произведение $\prod_{\iota\in J} E_\iota$ есть линейное отображение. Точно так же, если модуль E есть *прямая сумма* семейства (M_ι) своих подмодулей, а $k_\iota(x)$ — компонента $x\in E$ в M_ι (§ 1, n° 7), то k_ι — линейное отображение (§ 1, предложение 7).

2) Пусть a — элемент A-модуля E; отображение $\lambda\to\lambda a$ A-модуля A_S в E линейно; обозначим его θ_a; если E — унитарный модуль, то $\theta_a(\varepsilon)=a$ (где ε — единица кольца A).

°3) Пусть I — открытый интервал числовой прямой $\mathbf{R}$, E — векторное пространство всех дифференцируемых числовых функций на I и F — векторное пространство всех числовых функций на I. Отображение $x\to x'$, относящее каждой дифференцируемой функции x ее производную, есть линейное отображение E в F.°

Все свойства представлений произвольных групп с операторами (гл. I, § 6, n°n° 12 и 13) сохраняют силу и для линейных отображений; напомним их вкратце.

Для того чтобы отображение модуля E в модуль F было *изоморфизмом* E в F, необходимо и достаточно, чтобы оно было *взаимно однозначным* линейным отображением E в F, или чтобы $u^{-1}(0)$ сводилось к 0.

Пусть u — линейное отображение E в F, тогда $u(E)$ есть подмодуль модуля F; $H=u^{-1}(0)$ есть подмодуль модуля E, и $u(E)$ изоморфно фактормодулю E/H; u есть композиция канонического гомоморфизма E на E/H, изоморфизма E/H на $u(E)$ и канонического изоморфизма $u(E)$ в F. Если M — подмодуль модуля E, то $u(M)$ — подмодуль модуля F, изоморфный фактормодулям $M/(M\cap H)$ и $(M+H)/H$; в частности, если сумма $M+H$ прямая (т. е. если $M\cap H=\{0\}$), то *сужение* u на M есть *изоморфизм* M на $u(M)$. Если M' — подмодуль модуля F, то $u^{-1}(M')$ — подмодуль модуля E, содержащий H, а фактормодуль $u^{-1}(M')/H$ изоморфен $M'\cap u(E)$.

Если S — система образующих подмодуля M модуля E, то $u(S)$ есть система образующих для $u(M)$. В частности, если $u(x)=0$ для всех $x\in S$, то $u(x)=0$ также для всех $x\in M$.

Ссылаясь на этот результат, мы будем называть его иногда *«принципом продолжения линейных тождеств»* или *«принципом продолжения по линейности»*.

Наконец, если E, F, G — A-модули, u — линейное отображение E в F и v — линейное отображение F в G, то *композиция* $v\circ u$ есть линейное отображение E в G.

Множество всех линейных отображений модуля E в модуль F будет обозначаться $\mathscr{L}(E,F)$. Ясно, что если u и v — такие отображения, то также $-u$ и $u+v$ являются линейными отображениями E в F; тем самым $\mathscr{L}(E,F)$ есть *аддитивная подгруппа* модуля F^E (множества всех отображений E в F); напротив, если A некоммутативно, то $w=\alpha u$, где $\alpha\in A$, *не будет, вообще говоря, линейным отображением* E в F; действительно, $w(\lambda x)=\alpha u(\lambda x)=(\alpha\lambda)u(x)$, а $\lambda w(x)=(\lambda\alpha)u(x)$, и потому $w(\lambda x)=\lambda w(x)$ для всех $x\in E$ и всех $\lambda\in A$, вообще говоря, лишь если α принадлежит *центру* C кольца A. Иначе говоря, вообще $\mathscr{L}(E,F)$ можно наделить структурой модуля *относительно* C (но не относительно A).

2. *Линейные отображения фактормодуля*

Пусть E — A-модуль, H — его подмодуль и φ — канонический гомоморфизм E на фактормодуль E/H. Если f — линейное отображение E/H в A-модуль F, то $f\circ\varphi$ есть линейное отображение E в F, аннулирующееся для всех $x\in H$; обратно, если g — линейное отображение E в F, аннулирующееся для всех $x\in H$, то $x\equiv y \pmod H$ влечет $g(x-y)=0$, т. е. $g(x)=g(y)$; тем самым g *согласуется* с отношением $x\equiv y \pmod H$ (Теор. мн., Рез., § 5, n° 7) и, следовательно, имеет вид $f\circ\varphi$, где f — отображение E/H в F, линейность которого легко проверяется. Другими словами:

Предложение 1. *Пусть E и F — A-модули, H — подмодуль модуля E и φ — канонический гомоморфизм E на E/H. Отображение, относящее каждому линейному отображению f фактормодуля E/H в F линейное отображение $f\circ\varphi$ модуля E в F, есть*

изоморфизм модуля $\mathscr{L}(E/H, F)$ (относительно центра C кольца A) *на подмодуль модуля* $\mathscr{L}(E, F)$, *образованный теми линейными отображениями* E *в* F, *которые аннулируются на* H.

Этот изоморфизм и изоморфизм, обратный ему, будут называться *каноническими*.

Замечание. Предыдущее рассуждение может быть обобщено следующим образом: если u — линейное отображение E в F, M — произвольный подмодуль в E и функция u *согласуется* (Теор. мн., Рез., § 5, n° 8) с отношениями эквивалентности $x \equiv y \pmod{M}$ в E и $x' \equiv y' \pmod{u(M)}$ в F, то отображение $\dot{u}$ фактормодуля E/M в $F/u(M)$, получающееся путем ее *факторизации*, линейно и отображает E/M на $u(E)/u(M)$; при этом $\dot{u} \circ \varphi = \psi \circ u$, где φ—канонический гомоморфизм E на E/M, а ψ — канонический гомоморфизм F на $F/u(M)$ *).

3. *Линейные отображения в прямую сумму*

Пусть E и F — A-модули и F является прямой суммой *конечного* семейства $(N_j)_{1 \leqslant j \leqslant n}$ своих подмодулей; для каждого $y \in F$ обозначим через $k_j(y)$ компоненту y в N_j $(1 \leqslant j \leqslant n)$. Пусть u — линейное отображение E в F; для каждого $x \in E$ имеем $u(x) = \sum_{j=1}^{n} k_j(u(x))$, т. е. $u = \sum_{j=1}^{n} k_j \circ u$; иными словами, линейное отображение u вполне определяется знанием линейных отображений $u_j = k_j \circ u$ модуля E в модули N_j $(1 \leqslant j \leqslant n)$. Обратно, если u_j для каждого j — произвольное линейное отображение E в N_j, то $u = \sum_{j=1}^{n} u_j$ есть линейное отображение E в F такое, что $u_j = k_j \circ u$. В итоге, если рассматривать линейные отображения E в N_j $(1 \leqslant j \leqslant n)$ как линейные отображения E в F и тем самым модуль $\mathscr{L}(E, N_j)$ — как подмодуль модуля $\mathscr{L}(E, F)$, то получаем:

Предложение 2. *Если* F — *прямая сумма конечного семейства* (N_j) *своих подмодулей, то модуль* $\mathscr{L}(E, F)$ *есть прямая сумма своих подмодулей* $\mathscr{L}(E, N_j)$.

*) Эти результаты сохраняют силу также, когда E и F — *произвольные* группы с операторами (коммутативные или нет), u — представление E *на* F и M — устойчивая нормальная подгруппа группы E (откуда следует, что $u(M)$ есть устойчивая нормальная подгруппа группы $u(E) = F$).

4. *Линейные отображения прямой суммы*

Пусть теперь E—A-модуль, являющийся прямой суммой *произвольного* семейства (M_λ) своих подмодулей, и F — произвольный A-модуль. Для каждого $x \in E$ обозначим через $h_\lambda(x)$ компоненту x в M_λ, так что $x = \sum_\lambda h_\lambda(x)$. Если u — линейное отображение E в F, то $u(x) = u\left(\sum_\lambda h_\lambda(x)\right) = \sum_\lambda u(h_\lambda(x)) = \sum_\lambda u_\lambda(h_\lambda(x))$, где u_λ — *сужение* u на подмодуль M_λ. Тем самым значение u для каждого $x \in E$ определяется знанием сужений u на подмодули M_λ. Обратно, пусть для каждого λ задано линейное отображение u_λ модуля M_λ в F; если для каждого $x \in E$ положить $u(x) = \sum_\lambda u_\lambda(h_\lambda(x))$ (выражение, имеющее смысл, поскольку $h_\lambda(x) \neq 0$ и, значит, $u_\lambda(h_\lambda(x)) = 0$ для всех кроме конечного числа индексов λ), то ясно, что u будет линейным отображением E в F, сужение которого на каждое M_λ совпадает с u_λ. В итоге:

Предложение 3. *Пусть E и F — A-модули, причем E есть прямая сумма семейства (M_λ) своих подмодулей. Каково бы ни было семейство (u_λ) линейных отображений u_λ модулей M_λ в F, существует, и притом только одно, линейное отображение u модуля E в F, сужение которого на M_λ равно u_λ для каждого λ.*

Следствие 1. *Модуль $\mathscr{L}(E, F)$ изоморфен произведению $\prod_\lambda \mathscr{L}(M_\lambda, F)$ модулей $\mathscr{L}(M_\lambda, F)$.*

Следствие 2. *Если E обладает базисом (a_λ), то для каждого семейства (b_λ) элементов из F существует однозначно определенное линейное отображение u модуля E в F такое, что $u(a_\lambda) = b_\lambda$ для каждого λ.*

Это отображение определяется формулой $u\left(\sum_\lambda \xi_\lambda a_\lambda\right) = \sum_\lambda \xi_\lambda b_\lambda$. Следовательно, для того чтобы u было *изоморфизмом* E *в* F, необходимо и достаточно, чтобы (b_λ) было *свободным семейством*; для того чтобы u было *изоморфизмом* E *на* F, необходимо и достаточно, чтобы (b_λ) было *базисом* модуля F.

Замечание. Пусть T — произвольное множество, отождествленное с каноническим базисом модуля $A_s^{(T)}$ *формальных линей*

ных комбинаций (с коэффициентами из A) элементов множества T (§ 1, n° 8). Следствие 2 предложения 3 показывает, что *любое* отображение f множества T в A-модуль F может быть, и притом единственным образом, продолжено до *линейного* отображения $\bar{f}$ модуля $A^{(T)}$ в F, а именно по формуле $\bar{f}\left(\sum_t \xi_t t\right) = \sum_t \xi_t f(t)$.

Предположим теперь, что E есть прямая сумма *конечного* семейства $(M_i)_{1\leqslant i\leqslant m}$ своих подмодулей. В тех же обозначениях, что и выше, изоморфизм $\prod_{i=1}^{m} \mathscr{L}(M_i, F)$ на $\mathscr{L}(E, F)$, определенный при доказательстве предложения 3, запишется в виде $(u_i) \longrightarrow \sum_{i=1}^{m} u_i \circ h_i$; когда u_i пробегает $\mathscr{L}(M_i, F)$, $u_i \circ h_i$ пробегает подмодуль P'_i модуля $\mathscr{L}(E, F)$, образованный теми линейными отображениями E в F, которые аннулируются на подмодуле $P_i = \sum_{k\neq i} M_k$, *дополнительном* к M_i. Тем самым имеем:

Предложение 4. *Пусть E — модуль, являющийся прямой суммой конечного семейства $(M_i)_{1\leqslant i\leqslant m}$ своих подмодулей; далее, P_i для каждого индекса i — подмодуль $\sum_{k\neq i} M_k$, дополнительный к M_i, и P'_i — подмодуль модуля $\mathscr{L}(E, F)$, образованный теми линейными отображениями E в F, которые аннулируются на P_i. Тогда P'_i изоморфен $\mathscr{L}(M_i, F)$ и $\mathscr{L}(E, F)$ есть прямая сумма подмодулей P'_i $(1 \leqslant i \leqslant m)$.*

Замечание. Изоморфизм $u_i \to u_i \circ h_i$ модуля $\mathscr{L}(M_i, F)$ на P'_i есть композиция изоморфизма $\mathscr{L}(M_i, F)$ на $\mathscr{L}(E/P_i, F)$, порождаемого каноническим изоморфизмом M_i на E/P_i (§ 1, предложение 1), и канонического изоморфизма $\mathscr{L}(E/P_i, F)$ на P'_i, определенного в предложении 1. $\mathscr{L}(M_i, F)$ и P'_i часто отождествляются посредством изоморфизма $u_i \to u_i \circ h_i$ и изоморфизма, обратного ему, которые мы называем *каноническими*.

Следствие. *Подмодуль M'_i модуля $\mathscr{L}(E, F)$, образованный теми линейными отображениями E в F, которые аннулируются на M_i, равен* $\sum_{k\neq i} P'_k$.

Действительно, поскольку все h_k с индексами $k \neq i$ аннулируются на M_i, то для того, чтобы $u = \sum_{k=1}^{m} u_k \circ h_k$ аннулировалось на M_i, необходимо и достаточно, чтобы $u_i \circ h_i = 0$.

Еще более специализируя наши предположения, допустим, наконец, что, с одной стороны, E есть прямая сумма конечного семейства $(M_i)_{1 \leqslant i \leqslant m}$ своих подмодулей и, с другой стороны, F есть также прямая сумма конечного семейства $(N_j)_{1 \leqslant j \leqslant n}$ своих подмодулей. Предложения 2 и 3 показывают тогда, что модуль $\mathscr{L}(E, F)$ изоморфен произведению mn модулей $\mathscr{L}(M_i, N_j)$. Говоря точнее, каждое линейное отображение u модуля E в F определяется своими m сужениями u_i на M_i, каждое же u_i определяется n отображениями $k_j \circ u_i = u_{ji}$ по формуле $u_i(x) = \sum_{j=1}^{n} u_{ji}(x)$; u_{ji} — линейное отображение M_i в N_j, и эти mn отображений могут быть выбраны произвольно.

Пусть G — третий A-модуль, прямая сумма семейства $(P_k)_{1 \leqslant k \leqslant p}$ своих подмодулей, и v — линейное отображение F в G, а (v_{kj}) — соответствующие ему np линейных отображений (где v_{kj} — отображение N_j в P_k). Для каждого $x \in M_i$ имеем

$$v(u_i(x)) = \sum_{j=1}^{n} v(u_{ji}(x)) = \sum_{j=1}^{n} \sum_{k=1}^{p} v_{kj}(u_{ji}(x)).$$

Полагая

$$w_{ki} = \sum_{j=1}^{n} v_{kj} \circ u_{ji}, \tag{1}$$

видим, что семейство, образованное mp линейными отображениями w_{ki}, соответствует линейному отображению $w = v \circ u$ модуля E в G (см. § 6, n° 4).

Замечание. Все предыдущие определения и предложения (кроме определения структуры C-модуля в $\mathscr{L}(E, F)$, следствия 2 предложения 3 и сделанных вслед за ним замечаний) применимы без изменения к произвольным коммутативным группам с операторами.

5. *Эндоморфизмы модуля*

Пусть E — A-модуль; в соответствии с общими определениями (гл. I, § 4, n° 4), *эндоморфизм* модуля E — это *линейное отображение E в E*; таким образом, множеством всех этих эндоморфизмов служит множество, которое мы обозначили $\mathscr{L}(E, E)$ и будем в дальнейшем для краткости обозначать $\mathscr{L}(E)$. Очевидно, закон

композиции $(u, v) \longrightarrow u \circ v$ определяет в $\mathscr{L}(E)$ вместе со сложением структуру *кольца*, единичным элементом которого служит тождественное отображение E на себя. $\mathscr{L}(E)$, наделенное, кроме того, внешним законом композиции $(\gamma, u) \longrightarrow \gamma u$ операторов γ, принадлежащих *центру* C кольца A, и эндоморфизмов u модуля E, есть *кольцо с операторами* (гл. I, § 8, n° 2), ибо для любых двух эндоморфизмов u, v имеем $(\gamma u) \circ v = u \circ (\gamma v) = \gamma (u \circ v)$.

Автоморфизмы модуля E — это не что иное, как *обратимые элементы* кольца $\mathscr{L}(E)$; они образуют *группу*, которую обозначают $\mathbf{GL}(E)$ и называют *линейной группой* модуля E; при $E = A_s^n$ вместо $\mathbf{GL}(E)$ пишут $\mathbf{GL}_n(A)$.

Кольцо (без операторов) $\mathscr{L}(E)$ есть подкольцо кольца $\mathscr{E}$ всех эндоморфизмов *аддитивной группы* (без операторов) E; оно состоит из тех элементов кольца $\mathscr{E}$, которые *перестановочны со всеми гомотетиями* модуля E (гл. I, § 8, следствие 2 предложения 2). Как было уже отмечено (§ 1, n° 1, и гл. I, § 6, n° 12), если кольцо A некоммутативно, гомотетия модуля E, вообще говоря, *не* является эндоморфизмом структуры *модуля* в E.

Если γ принадлежит центру C кольца A, то гомотетия $x \longrightarrow \gamma x$ есть эндоморфизм модуля E. Эти гомотетии называются *центральными гомотетиями* модуля E; они образуют подкольцо кольца $\mathscr{L}(E)$ и перестановочны со всеми эндоморфизмами модуля E. При этом:

Предложение 5. *Если E — свободный A-модуль, имеющий базис, содержащий не менее двух элементов, то каждый эндоморфизм модуля E, перестановочный со всеми автоморфизмами этого модуля, является центральной гомотетией.*

Пусть (a_λ) — базис модуля E и f — эндоморфизм, перестановочный со всеми автоморфизмами этого модуля. Зафиксируем какой-нибудь индекс λ, и пусть $f(a_\lambda) = \gamma_\lambda a_\lambda + \sum_{\mu \neq \lambda} \gamma_{\lambda\mu} a_\mu$; для каждого индекса $\mu \neq \lambda$ обозначим через $u_{\lambda\mu}$ автоморфизм модуля E, определяемый (следствие 2 предложения 3) условиями $u_{\lambda\mu}(a_\mu) = a_\lambda + a_\mu$, $u_{\lambda\mu}(a_\nu) = a_\nu$ при $\nu \neq \mu$; записывая, что $f(u_{\lambda\mu}(a_\lambda)) = u_{\lambda\mu}(f(a_\lambda))$, получаем $\gamma_{\lambda\mu} = 0$; поскольку это верно для всех $\mu \neq \lambda$, имеем $f(a_\lambda) = \gamma_\lambda a_\lambda$ для каждого индекса λ. Пусть теперь $v_{\lambda\mu}$ для каждой пары различных индексов (λ, μ) означает автоморфизм модуля E,

определяемый условиями $v_{\lambda\mu}(a_\lambda)=a_\mu$, $v_{\lambda\mu}(a_\mu)=a_\lambda$ и $v_{\lambda\mu}(a_\nu)=a_\nu$ для всех ν, отличных от λ и μ; записывая, что $f(v_{\lambda\mu}(a_\lambda))=v_{\lambda\mu}(f(a_\lambda))$, получаем $\gamma_\lambda=\gamma_\mu$, так что все γ_λ равны одному и тому же элементу $\gamma\in A$. Наконец, пусть w_α для каждого $\alpha\in A$ означает автоморфизм, определяемый условиями $w_\alpha(a_\lambda)=a_\lambda+\alpha a_\mu$ и $w_\alpha(a_\nu)=a_\nu$ для всех $\nu\neq\lambda$ (где λ и μ — любые два фиксированных различных индекса); записывая, что $f(w_\alpha(a_\lambda))=w_\alpha(f(a_\lambda))$, получаем $\alpha\gamma=\gamma\alpha$, так что γ принадлежит центру C кольца A. Тогда для каждого $x=\sum_\lambda \xi_\lambda a_\lambda\in E$ имеем

$$f(x)=\sum_\lambda \xi_\lambda f(a_\lambda)=\sum_\lambda \xi_\lambda\gamma a_\lambda=\sum_\lambda \gamma\xi_\lambda a_\lambda=\gamma x,$$

чем и доказано, что f — центральная гомотетия.

Следствие 1. *Если E — свободный A-модуль, то центр кольца $\mathscr{L}(E)$ есть кольцо всех центральных гомотетий модуля E, которое тогда изоморфно центру C кольца A.*

То, что каждый эндоморфизм, принадлежащий центру кольца $\mathscr{L}(E)$, является центральной гомотетией, в случае, когда E имеет базис, содержащий не менее двух элементов, вытекает из предложения 5; если E изоморфно A_s, то, поскольку каждый эндоморфизм u модуля A_s имеет вид $\xi\longrightarrow\xi\alpha$, где $\alpha=u(\varepsilon)$, два таких эндоморфизма перестановочны тогда и только тогда, когда перестановочны их значения для $\xi=\varepsilon$, так что центр кольца $\mathscr{L}(E)$ и в этом случае образован центральными гомотетиями. Остается показать, что если E — свободный A-модуль, то кольцо его центральных гомотетий изоморфно C; но отображение $\gamma\longrightarrow\varphi_\lambda$, где φ_λ — центральная гомотетия $x\longrightarrow\gamma x$, есть представление C в $\mathscr{L}(E)$, и $\varphi_\gamma=0$, имея своим следствием $\gamma a_\lambda=0$ для каждого элемента базиса (a_λ) модуля E, влечет $\gamma=0$.

Следствие 2. *Если E — свободный A-модуль, имеющий базис, содержащий не менее двух элементов, то центром линейной группы $\mathbf{GL}(E)$ служит группа обратимых центральных гомотетий модуля E, изоморфная тогда группе обратимых элементов центра C кольца A.*

Замечание. Это следствие остается еще верным для моногенного *векторного пространства* E; но оно не распространяется на A-модуль A_s с *произвольным* кольцом A, ибо можно указать примеры некоммутативных колец, каждый элемент которых перестановочен

со всеми обратимыми элементами кольца; °так, этим свойством обладает тензорная алгебра векторного пространства размерности >1 (гл. III, § 4).°

Упражнения. 1) Пусть E — A-модуль и $F=\prod_\iota F_\iota$ — произведение A-модулей F_ι; показать, что $\mathscr{L}(E, F)$ изоморфно произведению $\prod_\iota \mathscr{L}(E, F_\iota)$.

2) Пусть E — свободный A-модуль, F — произвольный A-модуль, M — подмодуль модуля E, N — подмодуль модуля F. Пусть, далее, Γ — подмодуль модуля $\mathscr{L}(E, F)$, образованный теми линейными отображениями u, для которых $u(M)\subset N$, и Γ_0 — подмодуль модуля Γ, образованный теми линейными отображениями u, для которых $u(E)\subset N$. Показать, что модуль $\mathscr{L}(E/M, F/N)$ изоморфен фактормодулю Γ/Γ_0. [Показать, что каждому линейному отображению E в F/N можно поставить в соответствие класс (mod Γ_0) линейных отображений E в F.]

3) Пусть E и F — A-модули и u — линейное отображение E в F. Показать, что отображение $(x, y)\to(x, y-u(x))$ модуля $E\times F$ в себя есть его *автоморфизм*. Вывести отсюда, что если существуют $v\in\mathscr{L}(F, E)$ и $a\in E$ такие, что $v(u(a))=a$, то существует такой автоморфизм w модуля $E\times F$, что $w(a, 0)=(0, u(a))$.

4) а) Изоморфизм u модуля E в E не может быть левым делителем нуля в кольце $\mathscr{L}(E)$.

б) Если E — свободный модуль и $u\in\mathscr{L}(E)$ не является левым делителем нуля в $\mathscr{L}(E)$, то u — изоморфизм E в E.

в) Пусть G — подгруппа аддитивной группы $\mathbf{Q}$ рациональных чисел, образованная рациональными числами k/p^n, где p — фиксированное простое число, n пробегает множество всех целых чисел $\geqslant 0$, а k — множество всех рациональных целых чисел. Пусть, далее, E — факторгруппа $G/\mathbf{Z}$. Показать, что эндоморфизм $x\to px$ $\mathbf{Z}$-модуля E не есть левый делитель нуля в $\mathscr{L}(E)$, но не есть также изоморфизм E в E.

5) а) Эндоморфизм u модуля E на себя не является правым делителем нуля в кольце $\mathscr{L}(E)$.

б) Показать, что если E — свободный $\mathbf{Z}$-модуль, то существуют его эндоморфизмы u такие, что $u(E)\neq E$, но u не является правым делителем нуля в $\mathscr{L}(E)$.

6) а) Пусть E — свободный A-модуль и u, v — его эндоморфизмы. Показать, что если $u(E)\subset v(E)$, то существует эндоморфизм w модуля E такой, что $u=v\circ w$.

б) Пусть E — $\mathbf{Z}$-модуль упражнения 4в, u — тождественное отображение E на себя и v — эндоморфизм $x\to px$. Показать, что $v(E)=u(E)=E$, но E не обладает никаким эндоморфизмом w, для которого бы $u=v\circ w$.

7) Показать, что Z-модуль Z обладает эндоморфизмами u, w такими, что $u^{-1}(0) = w^{-1}(0) = 0$, но не существует никакого эндоморфизма v, для которого бы $u = v \circ w$.

§ 3. Строение векторных пространств

Относительно тел операторов, участвующих в рассмотрениях этого параграфа, не делается никаких специальных предположений; они могут быть как коммутативными, так и некоммутативными.

1. Базисы векторного пространства

Предложение 1. *Для того чтобы семейство (a_ι) элементов векторного пространства было свободным, необходимо и достаточно, чтобы $a_\varkappa$ ни для какого индекса $\varkappa$ не было линейной комбинацией элементов a_ι с индексами $\neq \varkappa$.*

Мы видели (§ 1, n° 6), что это условие необходимо (но не достаточно) для любого унитарного модуля. Чтобы убедиться в его достаточности для векторных пространств, нужно только заметить, что соотношение вида $\lambda_\varkappa a_\varkappa + \sum_{\iota \neq \varkappa} \lambda_\iota a_\iota = 0$, где $\lambda_\varkappa \neq 0$, равносильно соотношению $a_\varkappa = \sum_{\iota \neq \varkappa} (-\lambda_\varkappa^{-1}\lambda_\iota)\, a_\iota$.

Сформулированное условие можно выразить и иначе: для того чтобы (a_ι) было свободным семейством, необходимо и достаточно, чтобы $a_\varkappa$ ни для какого $\varkappa$ *не принадлежало подпространству, порожденному элементами a_ι с индексами $\iota \neq \varkappa$.*

Отсюда снова следует, что каждый ненулевой элемент векторного пространства *свободный* (§ 1, n° 6).

Предложение 2. *Если (a_ι) — свободное семейство элементов векторного пространства E и $b \in E$ не принадлежит подпространству, порожденному этим семейством, то множество, образованное всеми a_ι и b, свободное.*

Действительно, рассуждение, проведенное при доказательстве предложения 1, показывает, что не может существовать соотношения вида $\mu b + \sum_\iota \lambda_\iota a_\iota = 0$ с $\mu \neq 0$; с другой стороны, из сде-

ланного предположения следует, что если имеется такое соотношение с $\mu=0$, то также все $\lambda_\iota = 0$.

Предложение 3. *Пусть E — векторное пространство. Следующие три свойства множества $B \subset E$ равносильны:*

а) *B — базис пространства E;*

б) *B — максимальное свободное множество в E;*

в) *B — минимальная система образующих для E.*

Покажем прежде всего, что а) влечет б) и в) в любом унитарном модуле E. Действительно, если B — базис модуля E, то каждый элемент этого модуля есть линейная комбинация элементов из B, так что никакое множество в E, содержащее B и отличное от B, не является свободным. С другой стороны, если S — часть B, отличная от B, и $a \in B$ не принадлежит S, то a не принадлежит подпространству, порожденному множеством S (§ 1, предложение 2), и, значит, S не служит системой образующих для E.

Покажем далее, что в векторном пространстве E в) влечет а): достаточно доказать, что минимальная система B образующих пространства E является свободным множеством. Но в противном случае, в силу предложения 1, существовало бы $x \in B$, принадлежащее подпространству, порожденному множеством $S = B \cap \complement\{x\}$; тем самым S служило бы системой образующих для E, что противоречит предположению.

Наконец, в векторном пространстве E б) влечет а) в силу следующего более общего предложения:

Предложение 4. *Если S — система образующих векторного пространства E, то каждое ее максимальное свободное подмножество есть базис этого пространства.*

Действительно, пусть B — максимальное свободное подмножество множества S; если бы B не было системой образующих пространства E, то S не содержалось бы в порожденном B подпространстве, так что существовало бы $x \in S$, не принадлежащее этому подпространству; но тогда, в силу предложения 2, $B \cup \{x\}$ было бы свободным подмножеством множества S, что противоречит предположению.

Теорема 1. *Каждое векторное пространство обладает базисом.*

Эта теорема содержится в следующей более точной:

Теорема 2. *Для каждой системы S образующих векторного пространства E и каждого его свободного подмножества L, содержащегося в S, существует базис B пространства E такой, что $L \subset B \subset S$.*

Действительно, множество $\mathfrak{F}$ всех *свободных подмножеств* множества S, упорядоченное по включению, в силу предложения 3 § 1 есть множество *конечного характера* (Теор. мн., Рез., § 6, n° 11) и потому *индуктивно* (Теор. мн., Рез., § 6, n° 9); следовательно, то же верно и для множества $\mathfrak{G}$ всех свободных подмножеств множества S, содержащих L. В силу теоремы Цорна $\mathfrak{G}$ обладает *максимальным* элементом B, и B есть базис пространства E в силу предложения 4.

Замечание. В случае, когда S конечно, доказательство теоремы 2 опирается лишь на то, что каждое множество подмножеств *конечного* множества обладает максимальным элементом, а этот результат не зависит от аксиомы выбора (Теор. мн., гл. III).

Пример. Каждое кольцо, содержащее тело K и имеющее единицу тела K своей единицей, есть векторное пространство над K и, значит, обладает базисом относительно K (см. § 7); в частности, всякое *надтело* тела K обладает базисом относительно K. °Поэтому и *поле* $\mathbf{R}$ *вещественных чисел* обладает (бесконечным) базисом относительно *поля* $\mathbf{Q}$ *рациональных чисел*; всякий базис $\mathbf{R}$ относительно $\mathbf{Q}$ называется *базисом Хамеля*.°

Следствие 1. *Каждое левое векторное пространство над телом K изоморфно векторному пространству вида $K_s^{(I)}$.*

Следствие 2 («теорема о замене»). *Для каждой системы S образующих векторного пространства E и каждого его свободного подмножества L существует множество $S' \subset S$ такое, что $L \cup S'$ есть базис пространства E и $L \cap S' = \varnothing$.*

Достаточно применить теорему 2 к свободному множеству L и системе образующих $L \cup S$.

Заметим, что это следствие равносильно теореме 2, ибо применение теоремы о замене к свободной системе L, содержащейся в S, в свою очередь приводит к утверждению теоремы 2.

2. *Конечномерные векторные пространства*

Теорема 3. *Если векторное пространство E над телом K обладает конечным базисом, состоящим из n элементов, то и каждый другой базис пространства E состоит из n элементов.*

Достаточно доказать, что если B — базис пространства E, состоящий из n элементов, то всякий другой базис B' этого пространства содержит *не более* n элементов. Применим индукцию по n; при $n=0$ справедливость утверждения очевидна. Пусть $a \in B'$; существует множество $C \subset B$ такое, что $\{a\} \cup C$ есть базис пространства E и $a \notin C$ (теорема о замене); так как B — базис пространства E, то $C \neq B$, так что C содержит не более $n-1$ элементов. Пусть V — порожденное им подпространство и V' — подпространство, порожденное множеством $B' \cap \mathbf{C}\{a\}$; будучи оба дополнительными к подпространству Ka, V и V' изоморфны (§ 1, следствие предложения 1). Так как V обладает базисом с числом элементов, не превосходящим $n-1$, то $B' \cap \mathbf{C}\{a\}$ содержит не более $n-1$ элементов и, значит, B' — не более n элементов.

Этой теореме можно дать другое доказательство, основывающееся на том, что каждое *моногенное* векторное пространство над телом K есть *простой* K-модуль (гл. I, § 6, определение 14), поскольку оно порождается любым своим элементом $\neq 0$. Векторное пространство E над K, обладающее конечным базисом, является тем самым *полупростым* K-модулем*); поэтому то, что два *конечных* базиса пространства E имеют одинаковое число элементов, непосредственно вытекает из теоремы Жордана — Гёльдера (гл. I, § 6, теорема 8), а ее следствие показывает, что E не может иметь бесконечного базиса.

Можно было бы также установить связь теорем 1 и 2 этого параграфа с более общими предложениями, относящимися к произвольным группам с операторами (коммутативным или нет; см. гл. I, § 6, упражнение 18).

Определение 1. *Говорят, что векторное пространство E над телом K конечномерно, или имеет конечный ранг* (или также *имеет конечную размерность*) *относительно K, если оно обладает конечным базисом. Число элементов любого его базиса называется тогда размерностью или рангом пространства E* (или также *числом измерений E*) *относительно K и обозначается* $[E : K]$ *или* $\dim_K E$.

*) См. сноску на стр. 201.

В силу теоремы 3, векторное пространство над K, обладающее бесконечным базисом, не может быть изоморфно конечномерному векторному пространству; такое пространство называют *бесконечномерным* (или имеющим *бесконечный ранг*, или *бесконечную размерность*) относительно K.

Векторное подпространство V векторного пространства E над K, порождаемое *конечным* множеством M его элементов, конечномерно, ибо V обладает базисом, содержащимся в M (теорема 2). Если M — любое (конечное или бесконечное) множество элементов пространства E и порожденное им векторное пространство V конечномерно, то размерность V называется *рангом* M относительно K; если же V бесконечномерно, то говорят, что M — бесконечного ранга относительно K.

Допуская вольность, всюду, где это не может повлечь путаницы, дополнение «относительно K» в приведенных выше выражениях мы опускаем и вместо $\dim_K E$ пишем $\dim E$.

Замечания. 1) Говоря, что векторное пространство над телом K имеет размерность $\geqslant n$, желают сказать, что оно имеет относительно K *либо* конечную размерность $\geqslant n$, *либо* бесконечную размерность. Это равносильно утверждению, что в E существует свободная система, состоящая из n элементов.

2) В случае, когда E есть *надтело* тела K, термина «размерность» и обозначения $\dim_K E$ следует избегать, ибо это может повести к смешению с другим смыслом слова «размерность» (см. главу V); чтобы избежать всякой двусмысленности, лучше говорить о *ранге* E относительно K.

Приведем некоторые следствия теоремы 3 и определения 1

Следствие 1. *Для того чтобы левое векторное пространство над K было n-мерно, необходимо и достаточно, чтобы оно было изоморфно K_s^n. Пространства K_s^m и K_s^n при $m \neq n$ не изоморфны.*

Следствие 2. *Каждая система образующих n-мерного векторного пространства E содержит не менее n элементов; система образующих пространства E, состоящая из n элементов, является базисом этого пространства.*

Это — непосредственное следствие теорем 2 и 3.

Следствие 3. *Каждое свободное множество в n-мерном векторном пространстве E содержит не более n элементов; свободное множество, состоящее из n элементов, является базисом пространства E.*

Действительно, согласно теореме 2, каждое свободное подмножество пространства E содержится в некотором базисе этого пространства.

Замечания. 1) Метод, на котором основано данное выше первое доказательство теоремы 3, может, при надлежащем развитии, служить для явного определения компонент элементов базиса B относительно базиса B', если явно заданы компоненты элементов базиса B' относительно B. Мы проведем это вычисление в эквивалентной форме при рассмотрении теории матриц (см. § 6, n° 10).

2) Теорема 3 справедлива не только для векторных пространств, но и для некоторых видов модулей (см. § 1, упражнения 16 и 17, и Приложение II к главе III, n° 11). Однако можно указать примеры модулей, обладающих двумя конечными базисами, состоящими из разного числа элементов (см. упражнение 8).

3) Теорема 3 выражает, что два базиса одного и того же векторного пространства, один из которых конечен, *равномощны*; но в действительности это свойство справедливо без всяких ограничений (см. § 1, упражнение 24).

3. Подпространства векторного пространства

Предложение 5. *Каждое подпространство V векторного пространства E обладает в E дополнением.*

Действительно, в силу теоремы 1, факторпространство E/V обладает базисом; а тогда утверждаемое свойство есть следствие предложения 4 § 1.

Замечание. В случае, когда E/V обладает *конечной* системой образующих, этот результат не зависит от аксиомы выбора (см. замечание после теоремы 2).

Предложение 6. *Каждое подпространство V векторного пространства E конечной размерности n имеет размерность $\leqslant n$; если его размерность $=n$, то оно совпадает с E.*

Действительно, каждое свободное множество в V имеет не более n элементов (следствие 3 теоремы 3); свободное множество в V, имеющее наибольшее возможное число p элементов.

есть максимальное свободное множество в V и тем самым его базис (предложение 3); если $p=n$, то это множество является также базисом пространства E (следствие 3 теоремы 3) и, значит, $V=E$.

Определение 2. *Говорят, что подпространство V векторного пространства E имеет в E конечную факторразмерность, если факторпространство E/V конечномерно. Размерность E/V называется тогда факторразмерностью V в E и обозначается* $\operatorname{codim}_E V$ *или просто* $\operatorname{codim} V$.

В случае, когда E/V бесконечномерно, говорят, что V имеет бесконечную факторразмерность в E. Факторразмерность подпространства V векторного пространства E может быть определена также как размерность дополнения к V; следовательно, когда E конечномерно, имеем

$$\operatorname{codim}_E V = \dim E - \dim V. \tag{1}$$

Предложение 7. *Если M и N — конечномерные подпространства векторного пространства E, то $M \cap N$ и $M+N$ конечномерны и*

$$\dim (M+N) + \dim (M \cap N) = \dim M + \dim N. \tag{2}$$

Предложение очевидно, когда $M \cap N = \{0\}$, ибо тогда $M+N$ есть прямая сумма. Для получения равенства (2) в общем случае достаточно применить этот результат к подпространствам $M_1 = M/(M \cap N)$ и $N_1 = N/(M \cap N)$ факторпространства $E/(M \cap N)$, приняв во внимание формулу (1), дающую размерность этих подпространств; действительно, имеем $M_1 \cap N_1 = \{0\}$ и $M_1 + N_1 = (M+N)/(M \cap N)$ (гл. I, § 6, теорема 6).

Предложение 8. *Если M и N — подпространства векторного пространства E, имеющие конечную факторразмерность, то $M \cap N$ и $M+N$ также имеют конечную факторразмерность и*

$$\operatorname{codim} (M+N) + \operatorname{codim} (M \cap N) = \operatorname{codim} M + \operatorname{codim} N. \tag{3}$$

Действительно, $M/(M \cap N)$ изоморфно $(M+N)/N$, т. е. подпространству пространства E/N, и, следовательно (предложение 6), конечномерно. Отсюда вытекает конечномерность про-

странства $E_1=E/(M\cap N)$. В обозначениях предложения 7 имеем:

$$\dim M_1=\operatorname{codim}(M\cap N)-\operatorname{codim}M,$$
$$\dim N_1=\operatorname{codim}(M\cap N)-\operatorname{codim}N,$$
$$\dim(M_1+N_1)=\operatorname{codim}(M\cap N)-\operatorname{codim}(M+N);$$

внося эти выражения в соотношение $\dim(M_1+N_1)=\dim M_1+\dim N_1$, получаем (3).

Одномерные (соответственно двумерные) подпространства векторного пространства E над произвольным телом K, по аналогии с языком классической аналитической геометрии, часто называют *прямыми* (соответственно *плоскостями*); с другой стороны, подпространство H векторного пространства E, имеющее факторразмерность 1, называют *гиперплоскостью* *). Можно также определить гиперплоскости как *максимальные* элементы упорядоченного по включению множества $\mathfrak{S}$ всех подпространств векторного пространства E, *отличных от* E. Действительно, между подпространствами пространства E, содержащими заданное его подпространство H, и подпространствами факторпространства E/H имеется взаимно однозначное соответствие (гл. I, § 6, теорема 6); поэтому для максимальности H необходимо и достаточно, чтобы E/H не содержало никакого подпространства, отличного от $\{0\}$ и самого E/H, а это означает, что E/H одномерно.

Заметим, что гиперплоскости векторного пространства конечной размерности n — это его подпространства размерности $n-1$.

Предложение 9. *Каждое подпространство V векторного пространства E над телом K есть пересечение гиперплоскостей, содержащих это подпространство.*

Достаточно показать, что для каждого $x\notin V$ существует гиперплоскость, содержащая V и не содержащая x. Пересечение V с прямой Kx сводится к 0, иными словами, $V_1=V+Kx$ есть

*) В Приложении II к этой главе словам «прямая», «плоскость» и «гиперплоскость» будет придан более широкий смысл, а то, что было названо выше этими словами, будет именоваться соответственно *однородной прямой*, *однородной плоскостью* и *однородной гиперплоскостью*. Но вплоть до Приложения II можно не опасаться путаницы, и потому прилагательное «однородная» будет нами опускаться.

прямая сумма. Пусть W — подпространство, дополнительное к V_1; E есть прямая сумма подпространств $H=V+W$ и Kx, иными словами, H есть гиперплоскость, содержащая V и не содержащая x.

4. Ранг линейного отображения

Пусть E и F — векторные пространства над телом K и u — линейное отображение E в F. $u(E)$ изоморфно векторному пространству E/H, где $H=u^{-1}(0)$; значит, $u(E)$ *изоморфно подпространству* G *в* E, *дополнительному к* H (предложение 5), а сужение u на G есть *изоморфизм* G на $u(G)=u(E)$. Следовательно, если (a_ι) — базис в G, элементы $u(a_\iota)$ образуют базис в $u(E)$.

Определение 3. *Если линейное отображение u векторного пространства E в векторное пространство F таково, что подпространство $u(E)$ имеет в F конечную размерность, то последняя называется рангом u и обозначается* $\varrho(u)$.

В случае, когда $u(E)$ бесконечномерно, говорят, что u — линейное отображение *бесконечного ранга.*

Предложение 10. *Ранг линейного отображения u пространства E в F равен факторразмерности подпространства $u^{-1}(0)$ в E.*

Это сразу вытекает из сделанных выше замечаний. Следовательно,

$$\dim u(E) = \operatorname{codim}_E u^{-1}(0) = \varrho(u), \tag{4}$$

если все три числа конечны. В случае, когда E конечномерно, можно также написать

$$\varrho(u) = \dim E - \dim u^{-1}(0). \tag{5}$$

Предложение 11. *Пусть E и F — конечномерные векторные пространства; для каждого линейного отображения u пространства E в F имеем*

$$\varrho(u) \leqslant \min(\dim E, \dim F); \tag{6}$$

для того чтобы $\varrho(u)=\dim E$, необходимо и достаточно, чтобы u было изоморфизмом E в F; для того чтобы $\varrho(u)=\dim F$, необходимо и достаточно, чтобы u отображало E на F.

Это — следствие определения 3 и предложения 10.

Следствие. *Пусть E — векторное пространство конечной размерности n; следующие четыре свойства его эндоморфизма u равносильны:*

а) *u — автоморфизм пространства E;*

б) *u — взаимно однозначное отображение E в E;*

в) *u — отображение E на E;*

г) *u — линейное отображение ранга n.*

Напротив, когда E бесконечномерно, его эндоморфизм может быть взаимно однозначным или отображающим E на E, не будучи автоморфизмом (упражнение 8).

Упражнения. 1) Показать, что если E — векторное пространство над телом K, содержащим бесконечное число элементов, то множество всех систем образующих этого пространства не индуктивно относительно отношения порядка $\supset$. [Образовать убывающую последовательность (S_n) систем образующих пространства E, имеющую пустое пересечение.]

2) Пусть u — линейное отображение m-мерного векторного пространства E в n-мерное векторное пространство F; положим $H = u^{-1}(0)$. Показать, что если V — p-мерное подпространство пространства E и $V \cap H$ q-мерно, то $u(V)$ $(p-q)$-мерно. Показать, что если W — подпространство пространства F такое, что $W \cap u(E)$ r-мерно, то $u^{-1}(W)$ имеет размерность $r+m-\varrho(u)$.

3) Пусть u и v — линейные отображения m-мерного векторного пространства в n-мерное векторное пространство. Показать, что

$$|\varrho(u)-\varrho(v)| \leqslant \varrho(u+v) \leqslant \min(m, n, \varrho(u)+\varrho(v)),$$

причем $\varrho(u+v)$ может принимать всякое целое значение, удовлетворяющее этим неравенствам.

4) Пусть E, F, G — конечномерные векторные пространства над телом K, u — линейное отображение E в F и v — линейное отображение F в G. Показать, что размерность $u(E) \cap v^{-1}(0)$ равна $\varrho(u)-\varrho(v \circ u)$; вывести отсюда, что если F n-мерно, то

$$\max(0, \varrho(u)+\varrho(v)-n) \leqslant \varrho(v \circ u) \leqslant \min(\varrho(u), \varrho(v)),$$

причем $\varrho(v \circ u)$ может принимать всякое целое значение, удовлетворяющее этим неравенствам.

Пусть H — четвертое конечномерное векторное пространство над K и w — линейное отображение G в H. Показать, что

$$\varrho(v \circ u)+\varrho(w \circ v) \leqslant \varrho(v)+\varrho(w \quad v \circ u).$$

5) Если u и v — два эндоморфизма векторного пространства E *конечной* размерности такие, что $u \circ v$ есть тождественное отображение

E на себя, то u и v — взаимно обратные автоморфизмы пространства E (см. упражнение 8).

6) Пусть E — произвольное векторное пространство. Показать, что если u — его эндоморфизм, не являющийся правым делителем нуля в кольце $\mathscr{L}(E)$, то $u(E)=E$. [См. § 2, упражнение 5.]

7) Пусть E — произвольное векторное пространство и u, w — два его эндоморфизма, удовлетворяющие условию $\overset{-1}{w}(0) \subset \overset{-1}{u}(0)$. Показать, что существует эндоморфизм v пространства E такой, что $u = v \circ w$. [Разложить E в прямую сумму $\overset{-1}{w}(0)$ и некоторого другого подпространства.]

8) Пусть E — векторное пространство, имеющее бесконечный счетный базис (e_n).

а) Эндоморфизм u_1 пространства E, определяемый условиями $u_1(e_{2n-1})=0$, $u_1(e_{2n})=e_n$ для всех n, отображает E на себя, но не является автоморфизмом этого пространства; существует взаимно однозначный эндоморфизм v_1 пространства E такой, что $v_1(E) \neq E$, а $u_1 \circ v_1$ есть тождественное отображение E на себя.

б) Аналогично пусть u_2 — эндоморфизм пространства E, определяемый условиями $u_2(e_{2n})=0$, $u_2(e_{2n-1})=e_n$ для всех n, и A — кольцо эндоморфизмов пространства E. Показать, что u_1 и u_2 образуют *базис* A-модуля A_s. Вывести отсюда, что A-модуль A_s^p для каждого $p>0$ изоморфен A_s.

*9) а) Пусть E — векторное пространство над телом K. Каждое отображение f пространства E в себя, перестановочное со всеми *автоморфизмами* u этого пространства (т. е. такое, что $f(u(x))=u(f(x))$ для каждого $x \in E$ и каждого автоморфизма u пространства E), имеет вид $x \to \alpha x$, где α принадлежит K. [Записать, что f перестановочно с каждым автоморфизмом u, оставляющим инвариантным элемент $x \in E$, и вывести отсюда, что $f(x)=\varrho(x)x$, где $\varrho(x) \in K$.]

б) Пусть f — отображение $E \times E$ в E такое, что для каждого *автоморфизма* u пространства E тождественно $f(u(x), u(y))=u(f(x, y))$. Показать, что для всех пар (x, y) линейно независимых элементов из E имеет место равенство $f(x, y)=\alpha x+\beta y$, где α и β — постоянные скаляры, и что $f(\lambda x, \mu x)=\varphi(\lambda, \mu)x$, где φ — произвольное отображение $K \times K$ в K. [Тот же метод.] Если при этом $f(u(x), u(y))=u(f(x, y))$ для каждого *эндоморфизма* u пространства E, то $f(x, y)=\alpha x+\beta y$, каковы бы ни были x, y. Обобщить на отображения E^n в E.

§ 4. Двойственность

1. *Линейные формы. Сопряженный модуль*

Определение 1. *Линейной формой на левом A-модуле E называется всякое линейное отображение E в A-модуль A_s* (т. е. в кольцо A, рассматриваемое как левый модуль относительно A).

Пример. °Отображение $x \to \int_a^b x(t)\,dt$ есть линейная форма на векторном пространстве C (относительно $\mathbf{R}$) всех непрерывных числовых функций на интервале $[a, b]$.°

Каковы бы ни были линейная форма u на E и $\alpha \in A$, отображение $x \to u(x)\alpha$ тоже есть линейная форма на E, ибо для каждого $\lambda \in A$ имеем $u(\lambda x)\alpha = (\lambda u(x))\alpha = \lambda(u(x)\alpha)$; эта линейная форма обозначается $u\alpha$. Непосредственно ясно, что в множестве $\mathscr{L}(E, A_s)$ всех линейных форм на E закон аддитивной группы и внешний закон $(\alpha, u) \to u\alpha$ определяют структуру *правого модуля* относительно A. Наделенное этой структурой, $\mathscr{L}(E, A_s)$ называется *модулем, сопряженным* к E (или просто *сопряженным* к E*)); мы будем впредь обозначать его E^*.

Предложение 1. *Если A — кольцо с единицей, то модуль, сопряженный к левому модулю A_s, изоморфен правому модулю A_d.*

Действительно, пусть ε — единица кольца A и u — линейная форма на A_s; для каждого $\xi \in A$, полагая $\alpha = u(\varepsilon)$, имеем: $u(\xi) = u(\xi\varepsilon) = \xi u(\varepsilon) = \xi\alpha$; обратно, $\xi \to \xi\alpha$ для каждого $\alpha \in A$ есть линейная форма u на A_s такая, что $u(\varepsilon) = \alpha$; поэтому отображение $u \to u(\varepsilon)$ есть изоморфизм модуля, сопряженного к A_s, на правый модуль A_d. Основываясь на этом изоморфизме, модуль, сопряженный к A_s, обычно *отождествляют* с A_d, отождествляя каждую линейную форму u на A_s с $u(\varepsilon)$.

Пусть E — левый A-модуль и E^* — модуль, сопряженный к E; каждой паре элементов $x \in E$, $x' \in E^*$ соответствует элемент $x'(x)$ кольца A; этот элемент часто обозначают $\langle x, x' \rangle$. Отображение $(x, x') \to \langle x, x' \rangle$ называется *канонической билинейной*

*) Далее в этом трактате для векторных пространств, наделенных *топологией*, будет определено понятие «сопряженного пространства», зависящего от этой топологии и отличного от определенного здесь. Мы предостерегаем читателя против опрометчивого распространения на «топологическое» сопряженное пространство свойств «алгебраического» сопряженного, устанавливаемых в этом параграфе.

*формой**), *определенной на* $E \times E^*$; имеем тождественно

$$\langle x + y, x' \rangle = \langle x, x' \rangle + \langle y, x' \rangle, \tag{1}$$

$$\langle x, x' + y' \rangle = \langle x, x' \rangle + \langle x, y' \rangle, \tag{2}$$

$$\langle \alpha x, x' \rangle = \alpha \langle x, x' \rangle. \tag{3}$$

$$\langle x, x' \alpha \rangle = \langle x, x' \rangle \alpha. \tag{4}$$

Замечание. Модуль E^*, сопряженный к *правому* A-модулю E, есть *левый* A-модуль; значение $x'(x)$ канонической билинейной формы на $E \times E^*$ записывают тогда $\langle x', x \rangle$, а формулы, соответствующие (3) и (4), принимают вид $\langle x', x\alpha \rangle = \langle x', x \rangle \alpha$ и $\langle \alpha x', x \rangle = \alpha \langle x', x \rangle$. В случае, когда A коммутативно, можно пользоваться и тем и другим обозначеяием.

Каждую линейную форму x' на E можно рассматривать как *частичное* отображение (Теор. мн., Рез., § 3, n° 13) $x \to \langle x, x' \rangle$, порожденное канонической билинейной формой.

Точно так же для каждого $x \in E$ частичное отображение $x' \to \langle x, x' \rangle$ является *линейной формой* на правом A-модуле E^*; обозначая ее $\widetilde{x}$, имеем тождественно $\langle x, x' \rangle = \langle \widetilde{x}, x' \rangle$; непосредственно ясно, что $x \to \widetilde{x}$ есть (называемое *каноническим*) *линейное отображение* модуля E в *модуль* E^{**}, *сопряженный к модулю* E^*, *сопряженному к* E (и называемый *вторым сопряженным к* E).

В случае, когда A обладает единицей ε, каноническое отображение модуля A_s в его второй сопряженный, в силу предложения 1, есть *тождественное* отображение A_s на себя; поскольку каждая линейная форма x' на A_s отождествима с элементом $\xi' = x'(\varepsilon)$, канонической билинейной формой является отображение $(\xi, \xi') \to \xi\xi'$.

2. Ортогональность

Определение 2. *Пусть* E — *модуль и* E^* — *сопряженный модуль; элементы* $x \in E$ *и* $x' \in E^*$ *называются ортогональными, если* $\langle x, x' \rangle = 0$.

Множества $M \subset E$ и $M' \subset E^*$ называются *ортогональными*, если ортогональны любые два элемента $x \in M$ и $x' \in M'$. В част-

*) Общее понятие *билинейной формы* будет определено и изучено в главах III и IX.

ности, говорят, что $x' \in E^*$ (соответственно $x \in E$) ортогонально к M (соответственно к M'), если оно ортогонально к любому элементу из M (соответственно M'). Если x' и y' ортогональны к M, то в силу (2) и (4) то же верно для $x'+y'$, а также для $x'\alpha$ при каждом $\alpha \in A$; этим оправдывается следующее определение:

Определение 3. *Пусть M — произвольное множество элементов из E* (соответственно *M' — произвольное множество элементов из E^**). *Полным подмодулем, ортогональным к M* (соответственно к *M'*) (или, допуская вольность речи, просто *подмодулем, ортогональным к M* (соответственно к *M'*), если можно не опасаться путаницы), *называется множество тех $x' \in E^*$* (соответственно тех $x \in E$), *которые ортогональны к M* (соответственно к *M'*).

По определению линейной формы, подмодуль модуля E^*, ортогональный к E, сводится к 0; подмодулем в E^*, ортогональным к $\{0\}$, служит всё E^*.

Предложение 2. *Пусть M и N — подмножества модуля E такие, что $M \subset N$; если M' и N' — подмодули сопряженного модуля E^*, ортогональные соответственно к M и N, то $N' \subset M'$.*

Предложение 3. *Пусть (M_ι) — произвольное семейство подмножеств модуля E; подмодуль, ортогональный к объединению всех M_ι, есть пересечение $\bigcap_\iota M'_\iota$ ортогональных к ним подмодулей M'_ι; он есть также подмодуль, ортогональный к подмодулю в E, порожденному объединением всех M_ι.*

Предложения 2 и 3 являются непосредственными следствиями определения 3. Два аналогичных предложения относительно подмодулей модуля E, ортогональных к подмножествам сопряженного модуля E^*, мы предоставляем сформулировать читателю.

Если M — подмодуль модуля E, M' — подмодуль сопряженного модуля E^*, ортогональный к M, и M'' — подмодуль в E, ортогональный к M', то $M \subset M''$; но может случиться, что $M \neq M''$ (см. упражнения 3 и 5).

3. *Сопряженный к фактормодулю. Сопряженный к прямой сумме*

Предложение 4. *Пусть E — A-модуль, M — его подмодуль и φ — канонический гомоморфизм E на E/M. Отображение, относящее каждой линейной форме u на E/M линейную форму $u \circ \varphi$ на E, есть изоморфизм модуля, сопряженного к E/M, на ортогональный к M подмодуль M' модуля E^*.*

Это предложение сразу следует из предложения 1 § 2, если заметить, что определенный в нем канонический изоморфизм $u \longrightarrow u \circ \varphi$ есть также изоморфизм структур *правого* A-*модуля* в сопряженном к E/M и в M'.

Точно так же предложение 3 § 2 показывает, что если модуль E является *прямой суммой* семейства $(M_\lambda)_{\lambda \in L}$ своих подмодулей, то сопряженный модуль E^* изоморфен *произведению* $\prod_{\lambda \in L} M_\lambda^*$ модулей M_λ^*, сопряженных к M_λ. В частности, модуль, сопряженный к $A_s^{(L)}$, изоморфен (в силу предложения 1) модулю A_d^L.

В случае, когда E есть прямая сумма *конечного* семейства своих подмодулей, имеет место следующее более точное предложение:

Предложение 5. *Пусть E — модуль, являющийся прямой суммой конечного семейства $(M_i)_{1 \leqslant i \leqslant n}$ своих подмодулей, и N_i для каждого индекса i означает подмодуль $\sum_{j \neq i} M_j$, дополнительный к M_i. Тогда модуль E^*, сопряженный к E, есть прямая сумма своих подмодулей N_i', ортогональных соответственно к N_i; N_i' для каждого индекса i изоморфно модулю M_i^*, сопряженному к M_i, и подмодуль M_i', ортогональный к M_i, равен $\sum_{j \neq i} N_j'$.*

Это предложение вытекает из предложения 4 § 2 и его следствия, если принять во внимание, что определенные там изоморфизмы являются здесь изоморфизмами рассматриваемых *правых* A-*модулей*.

В соответствии со сказанным в n° 4 § 2, модуль M_i^*, сопряженный к M_i, часто *отождествляется* с подмодулем N_i' посредством отождествления каждой линейной формы u на M_i с (однозначно определенной) линейной формой x', служащей *продолжением* u на E и аннулирующейся на N_i.

4. *Координатные формы. Сопряженные базисы*

Пусть E — унитарный A-модуль, обладающий *конечным базисом* $(a_i)_{1\leqslant i\leqslant n}$; так как E есть прямая сумма n своих подмодулей, изоморфных A_s, то, в силу предложений 1 и 5, сопряженный модуль E^* есть прямая сумма n своих подмодулей, изоморфных A_d. Точнее, обозначим через a_i' для каждого индекса i линейную форму на E такую, что $a_i'(x)$ для каждого $x=\sum_{i=1}^{n}\xi_i a_i\in E$ равно его компоненте ξ_i; a_i' называется *i-й координатной формой* (относительно базиса (a_i)). a_i' образуют *базис* сопряженного модуля E^*; действительно, для каждой линейной формы x' на E имеем $x'(x)=\sum_{i=1}^{n}\xi_i x'(a_i)=\sum_{i=1}^{n}a_i'(x)\,x'(a_i)$, т. е. $x'=\sum_{i=1}^{n}a_i' x'(a_i)$; обратно, для каждой линейной формы $y'=\sum_{i=1}^{n}a_i'\beta_i$ имеем $y'(a_i)=\beta_i$, поскольку $a_i'(a_i)=\varepsilon$ (единице кольца A) и $a_j'(a_i)=0$ для всех $j\neq i$. Базис (a_i') модуля E^* называется *сопряженным* к базису (a_i) модуля E; согласно следствию 2 предложения 3 § 2, он однозначно определяется условиями

$$\langle a_i,\ a_j'\rangle=\delta_{ij}\quad(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant n), \tag{5}$$

где δ_{ij} есть функция пары (i, j), равная ε при $j=i$ и 0 при $j\neq i$, называемая *кронекеровским символом*.

Для любых двух элементов $x=\sum_{i=1}^{n}\xi_i a_i\in E$ и $x'=\sum_{i=1}^{n}a_i'\xi_i'\in E^*$ имеем

$$\langle x,\ x'\rangle=\sum_{i=1}^{n}\xi_i\xi_i'. \tag{6}$$

Замечания. 1) При отождествлении модуля, сопряженного к A_s^n, с модулем A_d^n базис, сопряженный к каноническому базису (§ 1, n° 8) модуля A_s^n, отождествляется с каноническим базисом модуля A_d^n.

2) В случае, когда E есть *правый* A-модуль с базисом $(a_i)_{1\leqslant i\leqslant n}$, формула (6) заменяется формулой

$$\langle x',\ x\rangle=\sum_{i=1}^{n}\xi_i'\xi_i,$$

справедливой для любой пары элементов $x=\sum_{i=1}^{n} a_i\xi_i \in E$, $x'=\sum_{i=1}^{n} \xi'_i a'_i \in E^*$.

Соотношения (5) позволяют установить, что каноническое отображение $x \to \widetilde{x}$ модуля E в его второй сопряженный E^{**} есть в этом случае *изоморфизм E на E^{**}*; действительно, так как $\langle \widetilde{a}_i, a'_j\rangle = \langle a_i, a'_j\rangle = \delta_{ij}$, каковы бы ни были i и j, то $(\widetilde{a}_j)$ есть базис в E^{**}, сопряженный к (a'_i). Тогда E *отождествляют* с E^{**} посредством изоморфизма $x \to \widetilde{x}$, что позволяет называть (a_i) *базисом, сопряженным к* (a'_i).

В случае, когда E обладает *бесконечным базисом* (a_ι), можно по-прежнему определить для каждого индекса ι *координатную форму* a'_ι, относящую каждому $x \in E$ его ι-ю компоненту относительно базиса (a_ι). Но семейство (a'_ι), всё еще являющееся свободным, уже не будет теперь базисом модуля E^*.

5. Двойственность для конечномерных векторных пространств

Результаты, полученные в n° 4, применимы, в частности, к конечномерным векторным пространствам:

Предложение 6. *Сопряженное к n-мерному левому векторному пространству E над телом K есть n-мерное правое векторное пространство над K; каноническое отображение $x \to \widetilde{x}$ пространства E в его второе сопряженное E^{**} есть изоморфизм E на E^{**}.*

Значит, если при этом K *коммутативно*, то пространство E^*, сопряженное к векторному пространству E над K конечной размерности n, *изоморфно* E.

Можно показать, что в этом случае при $n > 1$ не существует *канонического изоморфизма* E на его сопряженное, понимая под этим изоморфизм, зависящий лишь от структуры векторного пространства E (см. упражнение 16). В главе IX будут изучены изоморфизмы E на E^*, тесно связанные с теорией *билинейных форм* на $E \times E$.

Предложение 7. *Пусть E — векторное пространство конечной размерности n; если V — его подпространство размерности p, то подпространство V' сопряженного пространства E^*, ортогональное к V, имеет размерность $n-p$; подпространство пространства E, ортогональное к V', совпадает с V.*

Действительно, V' изоморфно сопряженному к E/V (предложение 4), а это факторпространство имеет размерность $n-p$, значит, согласно предложению 6, и V' имеет размерность $n-p$. Отсюда (вследствие отождествимости E с E^{**}) вытекает, что подпространство V'' пространства E, ортогональное к V', имеет размерность p; а так как оно содержит V, которое тоже имеет размерность p, то они совпадают.

Предложение 8. *Пусть V и W — подпространства конечномерного векторного пространства E, а V' и W' — ортогональные к ним подпространства в E^*. Подпространством в E^*, ортогональным к $V+W$, служит $V' \cap W'$; подпространством в E^*, ортогональным к $V \cap W$, служит $V'+W'$.*

Первая часть предложения является частным случаем предложения 3. Для доказательства второй заметим, что подпространством в E, ортогональным к $V'+W'$, является $V \cap W$; отождествляя E^{**} с E, заключаем из предложения 7, что $V'+W'$ есть подпространство пространства E^*, ортогональное к $V \cap W$.

6. *Двойственность для произвольных векторных пространств*

Пусть E — произвольное векторное пространство над телом K. Предложение 7 обобщается следующим образом:

Теорема 1. а) *Пусть V — подпространство векторного пространства E. Для того чтобы подпространство в E^*, ортогональное к V, имело конечную размерность p, необходимо и достаточно, чтобы V имело в E факторразмерность p.*

б) *Для того чтобы подпространство в E, ортогональное к заданному подпространству V' пространства E^*, имело конечную факторразмерность p, необходимо и достаточно, чтобы V' имело размерность p.*

в) *Пусть $\mathfrak{F}$ — множество всех подпространств пространства E, имеющих конечную факторразмерность, и $\mathfrak{F}'$ — множество всех*

конечномерных подпространств пространства E^*; отображение, относящее каждому подпространству $V \in \mathfrak{F}$ ортогональное к нему подпространство $V' \in \mathfrak{F}'$, есть взаимно однозначное отображение $\mathfrak{F}$ на $\mathfrak{F}'$; обратное отображение относит каждому подпространству $V' \in \mathfrak{F}'$ ортогональное к нему подпространство $V \in \mathfrak{F}$.

а) Подпространство V' пространства E^*, ортогональное к подпространству V пространства E, изоморфно пространству, сопряженному к факторпространству E/V (предложение 4); значит, если E/V конечномерно, V' имеет размерность, равную размерности E/V (предложение 6). С другой стороны, если V' имеет конечную размерность p, то E/V не может быть бесконечномерным, ибо V содержалось бы тогда в некотором подпространстве W факторразмерности $p+1$ и V' содержало бы подпространство W' пространства E^*, ортогональное к W, имеющее размерность $p+1$, что невозможно.

б) Пусть V' — p-мерное подпространство пространства E^* и $(a'_i)_{1 \leqslant i \leqslant p}$ — его базис. Рассмотрим отображение $x \longrightarrow (\langle x, a'_i \rangle)_{1 \leqslant i \leqslant p}$ пространства E в K_s^p; это — линейное отображение u ранга $p' \leqslant p$. Подпространство $V = \overset{-1}{u}(0)$ есть не что иное, как подпространство пространства E, ортогональное к V'; в силу предложения 10 § 3, оно имеет факторразмерность $p' \leqslant p$. Согласно а), подпространство в E^*, ортогональное к V, имеет размерность p'; так как оно содержит V', то они необходимо совпадают, и $p' = p$.

Обратно, предположим, что подпространство V пространства E, ортогональное к V', имеет конечную факторразмерность p; тогда, согласно а), ортогональное к V подпространство V'' в E^* имеет размерность p; так как оно содержит V', то V' конечномерно, и следовательно, факторразмерность V равна размерности V'.

в) При доказательстве утверждения б) мы уже видели, что если V' — подпространство в E^* размерности p и V — ортогональное к нему подпространство в E, то V' совпадает с подпространством в E^*, ортогональным к V. Точно так же, если V — подпространство в E, имеющее факторразмерность p, то ортогональное к нему подпространство V' в E^* имеет размерность p, значит, подпространство V'' в E, ортогональное к V', имеет факторразмерность p; поскольку оно содержит V, они совпадают.

Тем самым два отображения, рассматриваемые в третьей части теоремы, действительно взаимно однозначны и обратны друг к другу.

Замечания. 1) В силу предложения 2, два взаимно обратные отображения, определенные в теореме 1, являются *убывающими*, когда $\mathfrak{F}$ и $\mathfrak{F}'$ упорядочены по включению; поэтому они относят сумме (соответственно пересечению) двух подпространств пересечение (соответственно сумму) соответствующих им подпространств (обобщение предложения 8).

2) Первая часть теоремы 1 показывает, в частности, что если сопряженное E^* к векторному пространству E *конечномерно*, то это же верно и для E: достаточно применить теорему 1 к случаю, когда $V=\{0\}$.

Теорема 1 позволяет охарактеризовать *гиперплоскости* векторного пространства E:

Предложение 9. *Для каждой гиперплоскости H векторного пространства E существует линейная форма x'_0 на E такая, что $H=\overset{-1}{x'_0}(0)$; для того чтобы линейная форма $x'\in E^*$ обладала тем свойством, что $H=\overset{-1}{x'}(0)$, необходимо и достаточно, чтобы $x'=x'_0\alpha$, где $\alpha\neq 0$. Обратно, для каждой линейной формы $x'\neq 0$ на E подпространство $\overset{-1}{x'}(0)$ есть гиперплоскость.*

Справедливость этих утверждений сразу следует из теоремы 1, примененной к случаю $p=1$.

Если H — гиперплоскость и x'_0 — любая линейная форма, для которой $H=\overset{-1}{x'_0}(0)$, то отношение $x'_0(x)=0$, характеризующее элементы $x\in H$, называют *уравнением гиперплоскости* H.

Более общим образом, если (x'_ι) — семейство ненулевых линейных форм на E и V означает пересечение семейства гиперплоскостей $\overset{-1}{x'_\iota}(0)$, то отношение «каково бы ни было ι, $x'_\iota(x)=0$» характеризует элементы $x\in V$; говорят, что отношения $x'_\iota(x)=0$ образуют *систему уравнений* подпространства V.

В силу предложения 9 § 3, *каждое подпространство векторного пространства E может быть определено системой уравнений.*

Пусть, в частности, V — подпространство *конечной факторразмерности* p, так что ортогональное к нему подпространство V', по теореме 1, имеет размерность p; если (a'_i) — его базис,

то V есть пересечение p гиперплоскостей $\overset{-1}{a_i'}(0)$; иными словами, p уравнений $a_i'(x)=0$ $(1\leqslant i\leqslant p)$ образуют систему уравнений подпространства V, левые части которых являются линейно независимыми формами.

Отметим еще, что предложение 9 § 3 равносильно следующему утверждению, обобщающему часть утверждения в) теоремы 1:

Предложение 10. *Пусть V — произвольное подпространство векторного пространства E; если V' — подпространство в E^*, ортогональное к E, то подпространство в E, ортогональное к V', совпадает с V.*

Действительно, V' есть множество тех линейных форм x', для которых $V\subset\overset{-1}{x'}(0)$; принимая во внимание предложение 9, видим, что подпространство в E, ортогональное к V', есть пересечение всех гиперплоскостей, содержащих V, и, значит, совпадает с V.

Замечание. Для подпространств пространства E^* не существует аналога предложения 10; если V' — подпространство в E^*, имеющее *бесконечную* размерность, то подпространство в E^*, ортогональное к подпространству V пространства E, ортогональному к V', может не совпадать с V' (упражнение 9) *).

Наконец, если принять во внимание предложение 9, из третьей части теоремы 1 вытекает, что *если подпространство V векторного пространства E есть пересечение конечного числа гиперплоскостей $\overset{-1}{x_i'}(0)$, то каждая линейная форма на E, аннулирующаяся на V, есть линейная комбинация форм x_i'.*

7. *Линейные уравнения*

Пусть E и F — A-модули. Каждое уравнение вида $u(x)=y_0$, где неизвестное x принимает значения из E, u — линейное отображение E в F и y_0 — заданный элемент из F, называется *линейным уравнением*; y_0 называется *свободным членом* (или *правой*

*) Как мы позже узнаем, можно, наделяя E и E^* надлежащими *топологиями* и рассматривая в E и E^* лишь подпространства, *замкнутые* в этих топологиях, восстановить полную симметрию в свойствах E и E^* также в случае, когда E бесконечномерно.

частью) этого уравнения; линейное уравнение, в котором $y_0 = 0$, называется *однородным*.

Примеры. 1) Линейное уравнение $u(x) = y_0$, в котором u — *линейная форма* на E (и, следовательно, $F = A$), называется *скалярным*. Система уравнений

$$\langle x, x'_\iota \rangle = \eta_\iota \qquad (\iota \in I), \tag{7}$$

где $(x'_\iota)_{\iota \in I}$ — заданное семейство линейных форм на E, $(\eta_\iota)_{\iota \in I}$ — заданное семейство элементов из A, имеющее то же множество индексов, а неизвестное x принимает значения из E, называется *системой линейных* (скалярных) *уравнений* или просто *линейной системой*; элементы η_ι называются *свободными членами* системы; если все они равны нулю, система называется *однородной*.

Система (7) линейных уравнений *равносильна одному линейному уравнению* $u(x) = y_0$, где за F принято A_s^I, за y_0 принято (η_ι), а u означает отображение $x \to (\langle x, x'_\iota \rangle)$ модуля E в F.

Более общим образом, каждая система линейных уравнений

$$u_\iota(x) = y_\iota \qquad (\iota \in I),$$

где u_ι — линейное отображение E в модуль F_ι, а y_ι (для каждого $\iota \in I$) — заданный элемент из F_ι, равносильна одному линейному уравнению $u(x) = y$, где u — отображение (u_ι) модуля E в $F = \prod_\iota F_\iota$, а $y = (y_\iota)$.

Пусть E — унитарный A-модуль, обладающий базисом $(a_\lambda)_{\lambda \in L}$. Если положить $x = \sum_\lambda \xi_\lambda a_\lambda$ и $\alpha_{\lambda\iota} = \langle a_\lambda, x'_\iota \rangle$, то система (7) примет вид

$$\sum_{\lambda \in L} \xi_\lambda \alpha_{\lambda\iota} = \eta_\iota \quad (\iota \in I). \tag{8}$$

Обратно, отыскание семейства $(\xi_\lambda)_{\lambda \in L}$ скаляров такого, что $\xi_\lambda = 0$ для всех кроме конечного числа индексов λ и соотношение (8) выполняется для каждого $\iota \in I$, равносильно отысканию решения системы линейных уравнений (7) с $E = A_s^{(L)}$, $x = \sum_\lambda \xi_\lambda a_\lambda$ (где (a_λ) — канонический базис прямой суммы E) и x'_ι, означающими

соответственно линейные формы $x \longrightarrow \sum_{\lambda} \xi_\lambda \alpha_{\lambda\iota}$. ξ_λ называются *неизвестными* системы (8), $\alpha_{\lambda\iota}$ — ее *коэффициентами*.

В случае, когда кольцо A некоммутативно, во избежание всяких недоразумений систему (8) называют *системой левых скалярных линейных уравнений*. Аналогично система

$$\sum_{\lambda \in L} \alpha_{\lambda\iota} \xi_\lambda = \eta_\iota \qquad (\iota \in I)$$

называется *системой правых скалярных линейных уравнений*, относительно *неизвестных* ξ_λ (лишь конечное число которых отлично от нуля); $\alpha_{\lambda\iota}$ по-прежнему называются *коэффициентами*, η_ι — *свободными членами* такой системы, которая, впрочем, сводится к системе вида (8), если считать ξ_λ, η_ι и $\alpha_{\lambda\iota}$ принадлежащими кольцу A^0, *противоположному* A.

В постоянном предположении, что (a_λ) — базис модуля E, соотношение $u(x) = y_0$ равносильно, в прежних обозначениях, соотношению

$$\sum_{\lambda \in L} \xi_\lambda b_\lambda = y_0, \tag{9}$$

где $b_\lambda = u(a_\lambda)$. Обратно, отыскание семейства $(\xi_\lambda)_{\lambda \in L}$ (в котором $\xi_\lambda = 0$ для всех кроме конечного числа индексов λ), удовлетворяющего соотношению вида (9), равносильно разрешению линейного уравнения $u(x) = y_0$, где неизвестная $x = \sum_{\lambda} \xi_\lambda a_\lambda$ принимает значения из $E = A_s^{(L)}$, (a_λ) — канонический базис прямой суммы E и u — линейное отображение E в F, определяемое соотношениями $u(a_\lambda) = b_\lambda$ для всех $\lambda \in L$ (§ 2, следствие 2 предложения 3).

°2) Решением *системы линейных дифференциальных уравнений*

$$y_i'(x) - \sum_{j=1}^{n} a_{ij}(x)\, y_j(x) = b_i(x) \qquad (1 \leqslant i \leqslant n) \tag{10}$$

на открытом интервале $I =]\alpha, \beta[$ вещественной прямой $\mathbf{R}$, где a_{ij} и b_i — определенные на I вещественные функции, называется конечная последовательность $(y_i)_{1 \leqslant i \leqslant n}$ дифференцируемых вещественных функций на I, удовлетворяющих n соотношениям (10) для каждого $x \in I$. Отыскание таких решений равносильно разрешению *одного линейного уравнения*. Действительно, пусть F — множество всех отображений $x \longrightarrow (z_i(x))$ интервала I в $\mathbf{R}^n$ и E — подмножество этого множества, образованное теми отображениями, в которых функции $z_i(x)$ $(1 \leqslant i \leqslant n)$

дифференцируемы на I; F есть векторное пространство над $\mathbf{R}$, а E — его подпространство; функция $b(x)=(b_i(x))$ есть элемент пространства F; наконец, если для каждой функции $y=(y_i)\in E$ положить

$$u(y)=\Big(y_i'-\sum_{j=1}^{n} a_{ij}y_j\Big)_{1\leqslant i\leqslant n},$$

то $y\to u(y)$ будет линейным отображением E в F. А тогда разрешение дифференциальной системы (10) равносильно разрешению линейного уравнения $u(y)=b$.

Замечание. Допуская вольность речи, задачу, равносильную разрешению линейного уравнения, часто называют *линейной* задачей.

Если $u(x)=y_0$ — заданное линейное уравнение, то уравнение $u(x)=0$ называют *однородным линейным уравнением, ассоциированным с* $u(x)=y_0$ (и говорят также, что оно получается путем *отбрасывания в уравнении* $u(x)=y_0$ *свободного члена*). Аналогично систему $\langle x, x_\iota'\rangle=0$ $(\iota\in I)$ называют однородной системой, *ассоциированной* с системой (7).

Предложение 11. *Если* x_0 *— решение линейного уравнения* $u(x)=y_0$, *то множество всех решений этого уравнения совпадает с множеством элементов* x_0+x_1, *где* x_1 *пробегает множество всех решений однородного уравнения, ассоциированного с* $u(x)=y_0$.

Действительно, соотношение $u(x)=y_0$ записывается в виде $u(x)=u(x_0)$, т. е. $u(x-x_0)=0$.

Иными словами, если уравнение $u(x)=y_0$ имеет хотя бы одно решение x_0, то множеством всех решений этого уравнения служит $x_0+\overset{-1}{u}(0)$. Заметим, что $\overset{-1}{u}(0)$ является *подмодулем* модуля E и, значит, не пусто, ибо во всяком случае содержит 0 (называемый *нулевым* или *тривиальным решением* однородного уравнения $u(x)=0$).

В силу предложения 11, для того чтобы линейное уравнение $u(x)=y_0$ имело *не более одного решения*, необходимо и достаточно, чтобы $\overset{-1}{u}(0)=\{0\}$ (иными словами, чтобы ассоциированное однородное уравнение не имело нетривиальных решений); в этом случае линейное уравнение $u(x)=y$ имеет не более одного решения при *каждом* $y\in F$ (или, что то же, u есть *изоморфизм* E в F).

8. *Линейные уравнения на векторном пространстве*

Мы ограничимся в дальнейшем изучением *скалярных* линейных систем (7), где E — *векторное пространство* над телом K (коммутативным или нет).

Определение 4. *Система скалярных линейных уравнений*

$$\langle x, x'_\iota\rangle = \eta_\iota \qquad (\iota \in I), \tag{7}$$

где неизвестная x принимает значения в векторном пространстве E, называется системой конечного ранга, если подпространство сопряженного пространства E^*, порожденное семейством (x'_ι), конечномерно; его размерность называется рангом системы (7).

Система (7), не являющаяся системой конечного ранга, называется системой *бесконечного ранга.*

Предложение 12. *Для того чтобы система скалярных линейных уравнений* (7), *где неизвестная x принимает значения из векторного пространства E над телом K, имела конечный ранг r, необходимо и достаточно, чтобы линейное отображение $x \longrightarrow (\langle x, x'_\iota\rangle)$ пространства E в K_s^I было отображением ранга r.*

Обозначим линейное отображение $x \longrightarrow (\langle x, x'_\iota\rangle)$ через u и подпространство сопряженного пространства E^*, порожденное семейством (x'_ι), — через V'. Подпространство V пространства E, ортогональное к V', есть не что иное, как $\overset{-1}{u}(0)$; если V' r-мерно, то V имеет в E факторразмерность r, и обратно (теорема 1,б)), а отсюда, в силу предложения 10 § 3, и следует справедливость утверждения.

Теорема 2. *Пусть*

$$\langle x, x'_\iota\rangle = \eta_\iota \qquad (\iota \in I) \tag{7}$$

— система скалярных линейных уравнений на векторном пространстве E относительно тела K, имеющая конечный ранг r. Для того чтобы эта система имела по крайней мере одно решение, необходимо и достаточно, чтобы равенство $\sum_\iota x'_\iota \varrho_\iota = 0$ (где (ϱ_ι) — семейство скаляров, отличных от нуля лишь для конечного числа индексов) *всегда влекло равенство $\sum \eta_\iota \varrho_\iota = 0$. Если x_0 —*

какое-нибудь решение этой системы, то множество всех решений имеет вид $x_0 + V$, *где* V *— подпространство факторразмерности* r *пространства* E.

Необходимость сформулированного условия существования решения системы (7) очевидна. Докажем, что оно *достаточно*. Среди форм x'_ι существует r форм x'_{ι_k} $(1 \leqslant k \leqslant r)$, образующих базис подпространства V' в E^*, порожденного всеми x'_ι (§ 3, теорема 2). Таким образом, для каждого индекса ι, отличного от всех индексов ι_k, имеем $x'_\iota = \sum_{k=1}^{r} x'_{\iota_k}\beta_{k,\iota}$; в силу условия, верно также $\eta_\iota = \sum_{k=1}^{r} \eta_{\iota_k}\beta_{k,\iota}$; следовательно, множество всех решений системы (7) совпадает с множеством всех решений частичной системы

$$\langle x, x'_{\iota_k}\rangle = \eta_{\iota_k} \qquad (1 \leqslant k \leqslant r). \tag{11}$$

Но, согласно предложению 12, линейное отображение $x \longrightarrow (\langle x, x'_{\iota_k}\rangle)$ пространства E в K^r (обозначенное нами через u) есть отображение ранга r, иначе говоря, отображение *на* K^r; это показывает, что система (11) обладает по крайней мере одним решением x_0; согласно предложению 11, множеством всех решений служит $x_0 + V$, где $V = \overset{-1}{u}(0)$, причем V имеет факторразмерность r.

Всякая система (7), состоящая *из конечного числа* m *уравнений*, имеет конечный ранг r, причем $r \leqslant m$; точно так же, если E — пространство *конечной размерности* n (что соответствует случаю системы (8), содержащей лишь n *неизвестных*), то его сопряженное E^* n-мерно, а значит, $r \leqslant n$.

В частности:

Следствие 1. *Система скалярных линейных уравнений на векторном пространстве, образованная конечным числом уравнений, в левых частях которых стоят линейно независимые формы, всегда обладает решением.*

Следствие 2. *Для того чтобы однородная система линейных уравнений* (8) *относительно* n *неизвестных* (с коэффициентами из тела K) *обладала нетривиальными решениями, необходимо и достаточно, чтобы ее ранг был* $< n$.

В частности, так всегда будет, если всех уравнений системы — конечное число $< n$.

Следствие 3. *Для того чтобы линейная система* (8) (с коэффициентами и свободными членами из тела K), *состоящая из n уравнений с n неизвестными, обладала одним и только одним решением, необходимо и достаточно, чтобы ассоциированная с ней однородная система не имела нетривиальных решений* (или, что то же, чтобы левые части уравнений системы были *линейно независимыми* формами).

Замечание. Критерий существования решения системы (7), сформулированный в теореме 2, уже не является достаточным, когда это система *бесконечного* ранга; например, если x'_ι — *координатные формы* в бесконечномерном пространстве $E = K_s^{(I)}$ (n° 4), то критерий теоремы 2 выполняется при любых свободных членах, поскольку x'_ι линейно независимы; но система (7) допускает решение только тогда, когда все η_i, за исключением конечного их числа, равны нулю.

9. Сопряженное линейное отображение

Пусть E и F — A-модули, E^* и F^* — сопряженные модули и u — линейное отображение E в F. Для каждой линейной формы $y' \in F^*$ композиция $x' = y' \circ u$ есть линейная форма на E.

Определение 5. *Отображением ${}^t u$, сопряженным к линейному отображению u модуля E в модуль F, называют отображение $y' \to y' \circ u$ сопряженного к F модуля F^* в сопряженный к E модуль E^*.*

Таким образом, сопряженное отображение ${}^t u$ определяется *тождеством относительно x и y'*

$$\langle u(x),\ y' \rangle = \langle x,\ {}^t u(y') \rangle. \tag{12}$$

Отображение ${}^t u$ *линейно*, ибо для всех $y' \in F^*$, $z' \in F^*$ и $\lambda \in A$ имеем $(y'+z') \circ u = y' \circ u + z' \circ u$ и $(y'\lambda) \circ u = (y' \circ u)\lambda$. Если u и v — линейные отображения E в F, то

$${}^t(u+v) = {}^t u + {}^t v \tag{13}$$

и

$${}^t(\lambda u) = \lambda\, {}^t u \tag{14}$$

для каждого λ, принадлежащего центру кольца A.

Пусть G — третий A-модуль, u — линейное отображение E в F и v — линейное отображение F в G; согласно (12), имеем, тождественно относительно $x \in E$ и $z' \in G^*$,

$$\langle v(u(x)),\ z' \rangle = \langle u(x),\ {}^t v(z') \rangle = \langle x,\ {}^t u({}^t v(z')) \rangle,$$

откуда

$${}^t(v \circ u) = {}^t u \circ {}^t v. \tag{15}$$

В случае, когда E и F — унитарные A-модули, обладающие *конечными базисами* и, значит, отождествимые каждый со своим вторым сопряженным (n° 4), тождество (12) показывает, что *отображение* ${}^t({}^t u)$, *сопряженное к отображению* ${}^t u$, *совпадает с* u и что каждое линейное отображение F^* в E^* является сопряженным к некоторому линейному отображению E в F.

Предложение 13. *Пусть u — линейное отображение модуля E в модуль F. Для того чтобы элемент $y' \in F^*$ был ортогонален к подмодулю $u(E)$ модуля F, необходимо и достаточно, чтобы ${}^t u(y') = 0$.*

Действительно, согласно (12), отношение «$\langle u(x), y' \rangle = 0$ для каждого $x \in E$» равносильно отношению «$\langle x, {}^t u(y') \rangle = 0$ для каждого $x \in E$», т. е. отношению ${}^t u(y') = 0$.

В случае, когда E и F — *векторные пространства*, из предложений 13 и 10 вытекает следующая *характеристика* подпространства $u(E)$:

Теорема 3. *Пусть u — линейное отображение векторного пространства E в векторное пространство F и $v = {}^t u$ — сопряженное отображение F^* в E^*. Для того чтобы уравнение $u(x) = y_0$ имело хотя бы одно решение* (т. е. чтобы $y_0 \in u(E)$), *необходимо и достаточно, чтобы y_0 было ортогонально к подпространству $V' = \overset{-1}{v}(0)$ пространства F^*.*

Действительно, согласно предложению 13, V' есть подпространство в F^*, ортогональное к $u(E)$, и значит (предложение 10) $u(E)$ есть подпространство в F, ортогональное к V'.

Следствие. *Для того чтобы линейное отображение u векторного пространства E в векторное пространство F было отображением E на F, необходимо и достаточно, чтобы ${}^t u$ было изоморфизмом F^* в E^*.*

Будем далее предполагать, что E и F — векторные пространства, и сохраним обозначения теоремы 3; в силу предложения 5, сопряженное к подпространству $u(E)$ пространства F изоморфно F^*/V' (поскольку $u(E)$ обладает в F дополнением); но, согласно определению V', F^*/V' изоморфно ${}^tu(F^*)$; таким образом:

Теорема 4. *Если u — линейное отображение векторного пространства E в векторное пространство F, то сопряженное к подпространству $u(E)$ пространства F изоморфно подпространству ${}^tu(F^*)$ пространства E^*. В частности, если u — отображение конечного ранга, то u и ${}^tu$ имеют одинаковый ранг.*

10. Контрагредиентные изоморфизмы

Предложение 14. *Пусть u — изоморфизм модуля E на модуль F; тогда ${}^tu$ есть изоморфизм F^* на E^*; если v — изоморфизм, обратный к u, то ${}^tv$ —изоморфизм, обратный к ${}^tu$.*

Действительно, так как $x'=y'\circ v$ влечет $y'=x'\circ v$, то ${}^tu$ есть изоморфизм F^* на E^*, а ${}^tv$ — обратный ему изоморфизм.

Определение 6. *Пусть u — изоморфизм модуля E на модуль F. Изоморфизмом, контрагредиентным к u* (или *отображением, контрагредиентным к u*), *называют изоморфизм $\check{u}$, сопряженный к изоморфизму, обратному u* (равный, согласно предложению 14, изоморфизму, обратному к ${}^tu$).

Таким образом, изоморфизм $\check{u}$ определяется *тождеством относительно $x\in E$ и $x'\in E^*$*

$$\langle u(x), \check{u}(x')\rangle = \langle x, x'\rangle. \tag{16}$$

Если E и F обладают конечными базисами и, значит, отождествимы каждое со своим вторым сопряженным, то u есть отображение, сопряженное к ${}^tu$, и, значит, изоморфизм, контрагредиентный к $\check{u}$.

Упражнения. 1) Пусть A — кольцо без делителей нуля. Показать, что если E — A-модуль, имеющий ненулевой аннулятор, то сопряженный модуль E^* сводится к 0.

2) Показать, что модуль, сопряженный к полю Q рациональных чисел (рассматриваемому как Z-модуль), сводится к 0.

3) Показать, что прообраз нуля относительно канонического отображения $x\to\tilde{x}$ A-модуля E в его второй сопряженный E^{**} есть

подмодуль E_0 в E, ортогональный к E^*. Привести пример, где E^* и E_0 не сводились бы к 0. [Рассмотреть модуль, содержащий элемент, в аннуляторе которого имеется элемент, не являющийся делителем нуля.]

4) Пусть E — модуль, M — его подмодуль и M' — подмодуль в E^*, ортогональный к M. Пусть, далее, x'_M для каждой линейной формы x' на E есть сужение x' на M; отношение $x'_M = y'_M$ равносильно отношению $x' - y' \in M'$; $x' \to x'_M$ есть линейное отображение E^* в модуль M^*, сопряженный к M, а ассоциированное взаимно однозначное отображение есть изоморфизм E^*/M' *в* M^*. Привести пример, где этот изоморфизм не отображал бы E^*/M' *на* M^*, т. е. где существовала бы линейная форма на M, не продолжаемая до линейной формы на E. [Принять $E=A$, где A — кольцо целостности, и в качестве M взять главный идеал кольца A, отличный от A.]

5) Пусть E означает A-модуль, а E_0 — его подмодуль, ортогональный к E^*; привести пример, где $E_0=\{0\}$, но существует подмодуль M модуля E такой, что подмодуль M'' в E, ортогональный к подмодулю M' в E^*, ортогональному к M, отличен от M. [См. упражнение 4.]

6) Пусть E — модуль, являющийся прямой суммой своих подмодулей M и N. Обозначим через E_0 (соответственно M_0, N_0) подмодуль в E (соответственно в M, N), ортогональный к E^* (соответственно к M^*, N^*); пусть, далее, M' (соответственно N') — подмодуль в E^*, ортогональный к M (соответственно к N), и M'' (соответственно N'') — подмодуль в E, ортогональный к M' (соответственно к N'). Показать, что $E_0=M_0+N_0$, $M_0=M \cap N''$, $N_0=N \cap M''$, $M''=M+N_0=M+E_0$.

7) Пусть V и W — подпространства произвольного векторного пространства E, а V' и W' — ортогональные к ним подпространства сопряженного пространства E^*. Показать, что подпространством в E^*, ортогональным к $V \cap W$, является $V'+W'$.

8) Привести пример модуля E, обладающего подмодулями M и N такими, что подмодуль в E^*, ортогональный к $M \cap N$, отличен от $M'+N'$, где M' и N' — подмодули в E^*, ортогональные соответственно к M и N. [Взять $E=A_s$, где A — кольцо без делителей нуля, обладающее единицей, но не допускающее тела левых отношений (см. гл. I, § 9, упражнение 9).]

*9) Пусть E — бесконечномерное векторное пространство. Показать, что:

а) Каноническое отображение $x \to \tilde{x}$ пространства E в E^{**} есть изоморфизм E в E^{**}, но не отображает E на E^{**}.

б) В E^* существует бесконечномерное подпространство V' такое, что подпространство в E^*, ортогональное к подпространству V в E, ортогональному к V', отлично от V'. [Принять за V' подпространство, порожденное координатными формами, соответствующими базису пространства E.] Вывести отсюда существование такого бесконечного семейства (V_ι) подпространств пространства E, что подпространство

в E^*, ортогональное к $\bigcap_\iota V_\iota$, отлично от $\sum_\iota V'_\iota$, где V'_ι — подпространство в E^*, ортогональное к V_ι.

в) Показать, что в E^* существуют такие бесконечномерные подпространства V' и W', что подпространство в E, ортогональное к $V' \cap W'$, отлично от $V+W$, где V и W — подпространства в E, ортогональные соответственно к V' и W'. [Использовать б).]

10) Показать, что теорема 2 для частного случая *конечной* системы линейных уравнений есть следствие теоремы 3. Напротив, для линейной системы (7) конечного ранга, образованной бесконечным множеством уравнений, критерии, получаемые путем применения теоремы 2, с одной стороны, и теоремы 3, с другой (если принять за u отображение $x \to (\langle x, x_\iota \rangle)$ и взять $y_0 = (\eta_\iota)$), различны. [Заметить, что при каноническом отображении на свое второе сопряжение $K_d^{(I)}$ отождествляется с подпространством сопряженного к K_s^I и что, с другой стороны, подпространство сопряженного к K_s^I, на котором аннулируется ${}^t u$, имеет факторразмерность r.]

11) Пусть u — линейное отображение модуля E в модуль F и $v = {}^t u$; показать, что для каждого подмодуля M модуля E подмодулем в E^*, ортогональным к $u(M)$, служит $\overset{-1}{v}(M')$, где M' — подмодуль в E^*, ортогональный к M; для каждого подмодуля N' модуля F^* подмодулем в E, ортогональным к $v(N')$, служит $\overset{-1}{u}(N)$, где N — подмодуль в E, ортогональный к N'.

12) Пусть E и F — векторные пространства, u — линейное отображение E в F, V — подпространство пространства E и V' — подпространство пространства E^*, ортогональное к V. Показать, что сопряженное к $u(V)$ изоморфно факторпространству ${}^t u(F^*)/(V' \cap {}^t u(F^*))$. Если W' — подпространство в F^*, для которого ${}^t u(W')$ конечномерно, а W — подпространство в F, ортогональное к W', то ${}^t u(W')$ изоморфно сопряженному к факторпространству $u(E)/(W \cap u(E))$.

13) Пусть u — линейное отображение векторного пространства E в векторное пространство F. Для того чтобы u было изоморфизмом E в F, необходимо и достаточно, чтобы ${}^t u$ было отображением F^* на E^*. [Для установления необходимости условия показать, что для любой линейной формы x' на E и базиса (a_ι) пространства E существует линейная форма y' на F такая, что $\langle a_\iota, x' \rangle = \langle a_\iota, {}^t u(y') \rangle$ для каждого ι.]

14) Пусть M — простой A-модуль.

а) Если $\alpha M = \{0\}$ для каждого $\alpha \in A$ и M состоит из p элементов (где p — простое; см. § 1, упражнение 20), то модуль, сопряженный к M, изоморфен правому идеалу кольца A, образованному всеми элементами p-го порядка правого аннулятора этого кольца.

б) Если $M=Aa$ для некоторого $a \in M$ (§ 1, упражнение 20) и $\mathfrak{a}$ — аннулятор элемента a, то модуль, сопряженный к M, изоморфен правому аннулятору $\mathfrak{b}$ множества $\mathfrak{a}$ в A. Для того чтобы $\mathfrak{b} \neq \{0\}$, необходимо и достаточно, чтобы существовали левые идеалы кольца A, изоморфные M. В этом случае подмодуль M_0 в M, ортогональный к модулю M^*, сопряженному к M, сводится к $\{0\}$.

*15) Распространить предложение 9 и теоремы 3 и 4 на вполне приводимые модули (§ 1, упражнения 22 и след., и гл. I, § 6, упражнение 18), никакой простой подмодуль которых не имеет сопряженного, сводящегося к $\{0\}$.

*16) Пусть E — векторное пространство конечной размерности $n > 1$ над полем K; показать, что не существует изоморфизма φ этого пространства E на E^*, зависящего лишь от заданной в E структуры векторного пространства. [Заметить, что для такого изоморфизма φ отображение $(x, y) \to \langle x, \varphi(y)\rangle$ произведения $E \times E$ в K было бы *инвариантным* (гл. I, § 7, п° 4) относительно всякого автоморфизма u пространства E, иными словами, каков бы ни был автоморфизм u, тождественно выполнялось бы равенство $\langle x, \varphi(y)\rangle = \langle u(x), \varphi(u(y))\rangle$.]

§ 5. Сужение тела скаляров

Пусть E — векторное пространство относительно тела K. При сужении области операторов заданного на E внешнего закона до *подтела* K_0 тела K E становится векторным пространством относительно K_0. В этом параграфе будет исследована связь между двумя определенными так структурами векторного пространства в E.

1. *Базисы относительно подтела*

Как мы знаем (§ 1, п° 2), тело K является левым векторным пространством относительно K_0.

Предложение 1. *Если* $(a_\lambda)_{\lambda \in L}$ — *базис* E *относительно* K *и* $(\beta_\mu)_{\mu \in M}$ — *базис* K *относительно* K_0, *то семейство* $(\beta_\mu a_\lambda)_{(\lambda, \mu) \in L \times M}$ *является базисом* E *относительно* K_0.

Действительно, очевидно, семейство $(\beta_\mu a_\lambda)$ порождает E, рассматриваемое как векторное пространство над K_0. С другой стороны, оно является свободным семейством в этом векторном пространстве; в самом деле, соотношение $\sum_{\lambda, \mu} \varrho_{\lambda\mu}\beta_\mu a_\lambda = 0$, где $\varrho_{\lambda\mu} \in K_0$ и $\varrho_{\lambda\mu} = 0$ для всех кроме конечного числа пар (λ, μ),

может быть записано в виде $\sum_{\lambda}\left(\sum_{\mu}\varrho_{\lambda\mu}\beta_{\mu}\right)a_{\lambda}=0$ и, значит, влечет $\sum_{\mu}\varrho_{\lambda\mu}\beta_{\mu}=0$ для всех λ; а для каждого λ соотношение $\sum_{\mu}\varrho_{\lambda\mu}\beta_{\mu}=0$ влечет $\varrho_{\lambda\mu}=0$ для всех μ.

Следствие. *Если* $[E:K]$ *и* $[K:K_0]$ *определены, то определено также* $[E:K_0]$ *и*

$$[E:K_0]=[E:K][K:K_0]. \tag{1}$$

Обратно, если $[E:K_0]$ *определено, то определены также* $[E:K]$ *и* $[K:K_0]$ *и имеет место равенство* (1).

Первое утверждение есть непосредственное следствие предложения 1. Обратно, если $[E:K_0]$ определено, то каждый базис пространства E относительно K_0, и в частности базис, определенный в предложении 1, конечен, а это влечет конечность множеств индексов L и M.

2. *Первичные элементы векторного подпространства*

Пусть $(a_\iota)_{\iota\in I}$ — базис векторного пространства E над телом K. Для каждого элемента $x=\sum_{\iota\in I}\xi_\iota a_\iota$ из E обозначим через $J(x)$ (конечное) множество тех индексов $\iota\in I$, для которых $\xi_\iota\neq 0$. Очевидно, $x\neq 0$ тогда и только тогда, когда $J(x)\neq\varnothing$.

Предложение 2. *Пусть* V *— подпространство векторного пространства* E *и* $J(x)$, *где* $x\in V$, *— минимальный элемент множества всех* $J(y)\subset I$, *соответствующих элементам* $y\neq 0$ *из* V (*упорядоченного по включению*). *Тогда для того, чтобы элемент* $z\in V$ *удовлетворял условию* $J(z)\subset J(x)$, *необходимо и достаточно, чтобы он имел вид* $z=\varrho x$, *где* $\varrho\in K$, *и тогда либо* $z=0$, *либо* $J(z)=J(x)$.

Последнее утверждение очевидно. Пусть теперь $x=\sum_{\iota}\xi_\iota a_\iota$, $z=\sum_{\iota}\zeta_\iota a_\iota$ таково, что $J(z)\subset J(x)$, и $\varkappa$ — какой-нибудь индекс из $J(x)$, так что $\xi_\varkappa\neq 0$. Положим $\varrho=\xi_\varkappa\xi_\varkappa^{-1}$ и $z'=z-\varrho x$. Тогда $J(z')\subset J(x)$ и $\varkappa\notin J(z')$, поэтому $J(z')\neq J(x)$ и, следовательно, $z'=0$.

В тех же предположениях и обозначениях, предложение 2 означает, что задание $J(x)$ определяет x с точностью до скалярного множителя; в частности, этот множитель всегда можно

выбрать так, чтобы сделать одну из компонент ξ_ι элемента x равной 1. Это оправдывает следующее определение:

Определение 1. *Пусть V — подпространство векторного пространства E. Элемент $x \in V$ называется первичным элементом этого подпространства относительно базиса $(a_\iota)_{\iota \in I}$ пространства E* (или, если можно не опасаться недоразумения, просто *первичным элементом подпространства V*), *если он удовлетворяет следующим двум условиям:*

а) *$J(x)$ есть минимальный элемент упорядоченного по включению множества $\mathfrak{S}_V$ тех $J(y) \subset I$, которые соответствуют элементам $y \neq 0$ из V;*

б) *хотя бы одна из компонент ξ_ι элемента x равна* 1.

Предложение 3. *Множество всех первичых элементов из V является системой образующих этого подпространства.*

Пусть $x = \sum_\iota \xi_\iota a_\iota$ — элемент из V; доказательство того, что x есть линейная комбинация первичных элементов, проведем индукцией по числу n элементов множества $J(x)$. При $n=0$ наше утверждение очевидно; предположим, что $n > 0$. Среди всех ненулевых элементов $z \in V$, для которых $J(z) \subset J(x)$, выберем элемент $y = \sum_\iota \eta_\iota a_\iota$, у которого $J(y)$ содержит наименьшее число элементов; тогда $J(y)$ минимально в $\mathfrak{S}_V$; согласно предложению 2, можно, в случае необходимости умножив предварительно y на надлежащий скаляр, считать, что существует $\varkappa \in J(y)$, для которого $\eta_\varkappa = 1$, так что y первичен. Пусть $z = x - \xi_\varkappa y$; z принадлежит V и $J(z)$ содержит не более $n-1$ элементов; значит, z, а следовательно и x, есть линейная комбинация первичных элементов.

3. *Первичные решения системы линейных уравнений*

Рассмотрим сначала *однородную* линейную систему

$$\sum_{\lambda \in L} \xi_\lambda \alpha_{\lambda\iota} = 0 \qquad (\iota \in I) \tag{2}$$

с коэффициентами $\alpha_{\lambda\iota}$ из K. Всевозможные ее решения $(\zeta_\lambda)_{\lambda \in L}$, составленные из элементов тела K, образуют векторное подпространство V пространства $E = K_s^{(L)}$; первичные элементы этого

подпространства V относительно канонического базиса пространства E будут называться *первичными решениями* системы (2).

Пусть теперь дана *неоднородная* линейная система

$$\sum_{\lambda \in L} \xi_\lambda a_{\lambda\iota} = \eta_\iota \qquad (\iota \in I), \tag{3}$$

где коэффициенты $a_{\lambda\iota}$ и свободные члены η_ι принадлежат K; сопоставим ей однородную систему

$$\sum_{\lambda \in L} \xi_\lambda a_{\lambda\iota} - \xi\eta_\iota = 0 \qquad (\iota \in I) \tag{4}$$

относительно неизвестных ξ и ξ_λ; будем, по определению, называть решение (ζ_λ) системы (3) *первичным*, если решение системы (4), образованное элементами ζ_λ и $\xi = 1$, есть первичное решение этой однородной системы.

Предложение 4. а) *Подпространство в* $K_s^{(L)}$, *образованное всеми решениями системы однородных линейных уравнений* (2), *порождается множеством первичных решений этой системы.*

б) *Неоднородная линейная система* (3), *имеющая хотя бы одно решение, имеет хотя бы одно первичное решение.*

Действительно, а) непосредственно вытекает из предложения 3. Применение а) к системе (4) показывает, что если (3) имеет хотя бы одно решение (ζ_λ), то решение системы (4), образованное всеми ζ_λ и $\xi = 1$, является линейной комбинацией первичных решений этой системы; отсюда следует, что (4) обладает по крайней мере одним первичным решением, в котором $\xi \neq 0$; умножив это решение на ξ^{-1}, мы и получим первичное решение системы (4), в котором $\xi = 1$.

Предложение 5. *Если коэффициенты* $a_{\lambda\iota}$ *и свободные члены* η_ι *системы скалярных линейных уравнений*

$$\sum_{\lambda \in L} \xi_\lambda a_{\lambda\iota} = \eta_\iota \tag{3}$$

принадлежат подтелу K_0 *тела* K, *то первичные решения* (ζ_λ) *этой системы состоят из элементов этого подтела.*

В силу определения первичных решений, достаточно провести доказательство для однородного случая ($\eta_\iota = 0$ при всех ι). Будем рассматривать K как *правое* векторное пространство над K_0,

и пусть F — его подпространство, порожденное элементами ζ_λ первичного решения системы (2); F содержит единицу тела K и конечномерно, а потому (§ 3, теорема 2) обладает базисом $(\varepsilon_i)_{0\leqslant i\leqslant n}$ относительно K_0, в котором $\varepsilon_0 = 1$. Для каждого $\lambda \in L$ имеем $\zeta_\lambda = \sum_{i=0}^{n} \varepsilon_i \zeta_{\lambda i}$, где $\zeta_{\lambda i}$ принадлежат K_0. Подставляя в (2), получаем

$$\sum_i \varepsilon_i \Big(\sum_\lambda \zeta_{\lambda i} a_{\lambda\iota}\Big) = 0 \qquad (\iota \in I),$$

откуда следует, что $\sum_\lambda \zeta_{\lambda i} a_{\lambda\iota} = 0$ для всех i $(0 \leqslant i \leqslant n)$ и всех ι. Иными словами, $(\zeta_{\lambda i})$ для каждого значения i есть решение системы (2); тем самым это относится, в частности, и к $(\zeta_{\lambda 0})$. Так как $\zeta_{\lambda 0}$ равно нулю всякий раз, когда ζ_λ равно нулю, а (ζ_λ) есть первичное решение системы (2), то предложение 2 показывает тогда, что, для каждого λ, $\zeta_{\lambda 0} = \varrho\zeta_\lambda$, где $\varrho \in K$. Кроме того, поскольку (ζ_λ) — первичное решение, существует $\mu \in L$, для которого $\zeta_\mu = 1$, т. е. $\zeta_\mu = \varepsilon_0$; по определению элементов $\zeta_{\lambda i}$, имеем тогда $\zeta_{\mu 0} = 1$ и $\zeta_{\mu i} = 0$ при $1 \leqslant i \leqslant n$; отсюда следует, что $\varrho = 1$ и потому $\zeta_\lambda = \zeta_{\lambda 0} \in K_0$ для всех λ.

Замечание. Предложение 5 показывает апостериори, что понятие первичного решения системы линейных уравнений зависит лишь от тела, порожденного коэффициентами и свободными членами системы, но не от надтела, в котором рассматриваются все решения этой системы.

Предложения 4 и 5 показывают, что справедлива

Теорема 1. а) *Подпространство в* $K_s^{(L)}$, *образованное всеми решениями системы однородных линейных уравнений* (2), *коэффициенты которой принадлежат подтелу* K_0 *тела* K, *порождается множеством тех решений, которые состоят из элементов этого подтела.*

б) *Если какая-нибудь линейная система* (3) *с коэффициентами и свободными членами, принадлежащими* K_0, *допускает решение, состоящее из элементов тела* K, *то она допускает решение, состоящее из элементов подтела* K_0.

4. *Применение к пространству линейных соотношений между заданными элементами векторного пространства*

Пусть $\mathfrak{F} = (a_\iota)_{\iota \in I}$ — заданное семейство элементов векторного пространства E над K. Напомним, что *пространством линейных соотношений* между элементами семейства $\mathfrak{F}$ мы назвали (§ 1, п° 8) подпространство $V(\mathfrak{F})$ прямой суммы $K_s^{(I)}$, образованное теми ее элементами $(\xi_\iota)_{\iota \in I}$, для которых

$$\sum_\iota \xi_\iota a_\iota = 0 \tag{5}$$

в пространстве E; мы будем называть ξ_ι *коэффициентами* линейного соотношения (5). Линейные соотношения (5), для которых (ξ_ι) есть первичный элемент подпространства $V(\mathfrak{F})$ относительно канонического базиса пространства $K_s^{(I)}$, будут называться *первичными соотношениями* между элементами a_ι.

Пусть $(e_\lambda)_{\lambda \in L}$ — базис пространства E и $a_\iota = \sum_{\lambda \in L} \alpha_{\iota\lambda} e_\lambda$; соотношение (5) равносильно системе однородных линейных уравнений

$$\sum_{\iota \in I} \xi_\iota \alpha_{\iota\lambda} = 0 \qquad (\lambda \in L) \tag{6}$$

относительно ξ_ι. Тем самым $V(\mathfrak{F})$ есть пространство решений системы (6), а первичные соотношения между элементами a_ι соответствуют первичным решениям этой системы.

Поэтому из предложения 5 и теоремы 1 вытекает

Предложение 6. *Пусть $(e_\lambda)_{\lambda \in L}$ — свободное семейство элементов векторного пространства E над телом K и $(a_\iota)_{\iota \in I}$ — семейство элементов из E, каждый из которых является линейной комбинацией элементов e_λ, с коэффициентами, принадлежащими подтелу K_0 тела K. При этих условиях коэффициенты первичных соотношений между элементами a_ι принадлежат K_0 и пространство линейных соотношений между этими элементами порождается множеством всех первичных соотношений.*

Следствие 1. *Если семейство (a_ι) свободное относительно K_0, то оно свободное относительно K.*

Следствие 2. *Если элемент $x \in E$ есть одновременно линейная комбинация элементов e_λ с коэффициентами из K_0 и линейная*

комбинация элементов a_ι с коэффициентами из K, то он является линейной комбинацией элементов a_ι с коэффициентами из K_0.

Чтобы убедиться в этом, достаточно применить предложение 6 к семейству, образованному всеми a_ι и x.

Следствие 3. *Ранг* (§ 3, n° 2) *множества A всех a_ι относительно K_0 равен рангу A относительно K.*

Действительно, в силу следствия 1, максимальное свободное множество $B \subset A$ относительно K_0 является таковым также относительно K, и обратно.

5. *Подтело, ассоциированное с подпространством*

Пусть E — векторное пространство над телом K, $(a_\iota)_{\iota \in I}$ — его базис и V — подпространство. Как мы знаем (§ 4, n° 6), существует по крайней мере одна система линейных уравнений («система уравнений подпространства V») с коэффициентами из K:

$$\sum_{\iota \in I} \xi_\iota a_{\iota\mu} = 0 \qquad (\mu \in M), \tag{7}$$

такая, что V совпадает с множеством всех $x = \sum_\iota \xi_\iota a_\iota$, где (ξ_ι) пробегает множество всевозможных решений системы (7), состоящих из элементов тела K.

Предложение 7. *Пусть K_0 — подтело тела K. Для того чтобы подпространство V пространства E порождалось множеством V_0 тех его элементов, компоненты которых* (относительно (a_ι)) *принадлежат K_0, необходимо и достаточно, чтобы существовала система уравнений этого подпространства, все коэффициенты которой принадлежат K_0.*

Согласно теореме 1, а), условие достаточно. Оно также необходимо: действительно, V_0 есть подпространство векторного пространства E_0 *относительно* K_0, образованного всевозможными линейными комбинациями элементов a_ι с коэффициентами из K_0; поэтому существует система уравнений (7) подпространства V_0 с коэффициентами из K_0. Согласно теореме 1, а), V_0 порождает подпространство *пространства* E, определяемое той же системой; а так как, по предположению, V_0 порождает в E подпро-

странство V, то определенная так система (7) и есть как раз система уравнений последнего в E.

Предложение 8. *Если подпространство V пространства E порождается некоторым множеством элементов, компоненты которых* (относительно (a_ι)) *принадлежат подтелу K_0 тела K, то компоненты всех первичных элементов этого подпространства* (относительно базиса (a_ι)) *принадлежат K_0.*

Пусть $x = \sum_\iota \xi_\iota a_\iota$ — первичный элемент из V; по предположению, V порождается семейством элементов $b_\lambda = \sum_\iota \beta_{\lambda\iota} a_\iota$, где все $\beta_{\lambda\iota}$ принадлежат K_0. Покажем, что если (ζ_λ) — решение системы

$$\sum_\lambda \zeta_\lambda \beta_{\lambda\iota} = \xi_\iota \qquad (\iota \in H), \tag{8}$$

где H — множество тех $\iota \in I$, для которых $\xi_\iota = 0$ или $\xi_\iota = 1$, то $z = \sum_\lambda \zeta_\lambda b_\lambda$ есть не что иное, как x. Действительно, $J(z-x) \subset \mathbf{C}H$, и следовательно, $J(z-x) \subset J(x)$, причем $J(z-x) \neq J(x)$, поскольку элемент x первичный; значит, в силу предложения 2, $z - x = 0$. Но коэффициенты и свободные члены системы (8) принадлежат K_0; следовательно (теорема 1, б)), эта система обладает решением, состоящим из элементов подтела K_0, чем предложение и доказано.

Предложение 8 подсказывает следующее определение:

Определение 2. *Пусть E — векторное пространство над телом K, (a_ι) — его базис и V — подпространство. Подтелом тела K, ассоциированным с подпространством V относительно базиса (a_ι), называется тело, порожденное компонентами первичных элементов из V относительно (a_ι).*

Из предложений 7 и 8, если принять во внимание предложение 3, непосредственно вытекает другая характеристика подтела, ассоциированного с подпространством V:

Теорема 2. *Подтело, ассоциированное с подпространством V пространства E относительно базиса (a_ι) этого пространства, есть наименьшее из подтел K_0 тела K, обладающих тем свойством,*

что V порождается множеством всех своих элементов, компоненты которых принадлежат K_0, а также наименьшее из подтел K_0 таких, что существует система уравнений подпространства V, все коэффициенты которых принадлежат K_0.

6. Применение: кольца эндоморфизмов тела относительно его подтел

Пусть K — произвольное тело и $\mathscr{E}(K)$ — *кольцо эндоморфизмов* его *аддитивной группы* (без операторов) (гл. I, § 8, n° 1); $\mathscr{E}(K)$ есть часть множества K^K всех отображений K в себя; если наделить K^K его структурой *левого* векторного пространства над K (произведением структур векторного пространства его сомножителей (§ 1, n° 4); напомним, что произведением αu элементов $\alpha \in K$ и $u \in K^K$ служит отображение $\xi \to \alpha u(\xi)$ тела K в себя), то $\mathscr{E}(K)$ будет подпространством векторного пространства K^K, ибо для каждого $u \in \mathscr{E}(K)$ имеем $\alpha u(\xi+\eta) = \alpha(u(\xi)+u(\eta)) = \alpha u(\xi) + \alpha u(\eta)$, каковы бы ни были ξ, η и α из K.

Заметим, что если $\alpha \in K$, $u \in \mathscr{E}(K)$, $v \in \mathscr{E}(K)$, то $\alpha(uv) = (\alpha u)v$, но, вообще говоря, $\alpha(uv) \neq u(\alpha v)$.

Для каждого *подтела* L тела K обозначим через K_L тело K, наделенное его структурой *правого* векторного пространства над L. *Кольцо эндоморфизмов* $\mathscr{L}(K_L)$ этого векторного пространства (§ 2, n° 5) есть подкольцо кольца $\mathscr{E}(K)$, образованное теми эндоморфизмами u аддитивной группы тела K, для которых $u(\xi\lambda) = u(\xi)\lambda$, каковы бы ни были $\xi \in K$ и $\lambda \in L$; ясно, что $\mathscr{L}(K_L)$ есть также *векторное подпространство* (левого) векторного пространства $\mathscr{E}(K)$ над K. Нашей целью будет *охарактеризовать* среди всех подколец кольца $\mathscr{E}(K)$ кóльца эндоморфизмов $\mathscr{L}(K_L)$, соответствующие тем подтелам L тела K, для которых размерность K_L относительно L (которую мы будем для краткости называть *индексом* L в K) конечна.

Заметим прежде всего, что (в прежних обозначениях) каждый элемент λ из L обладает тем свойством, что $u(\xi\lambda) = u(\xi)\lambda$ для каждого $\xi \in K$ и каждого $u \in \mathscr{M} = \mathscr{L}(K_L)$. Обратно, для любого $\mathscr{M} \subset \mathscr{E}(K)$ множество всех $\lambda \in K$, обладающих этим свойством, есть подтело тела K. Более общим образом:

Предложение 9. *Пусть E и F — правые векторные пространства над телом K и $\mathscr{M}$ — некоторое множество представлений аддитивной группы* (без операторов) *E в аддитивную группу* (без операторов) *F. Множество $K_0 = \chi(\mathscr{M})$ тех $\lambda \in K$, для которых $f(x\lambda) = f(x)\lambda$, каковы бы ни были $x \in E$ и $f \in \mathscr{M}$, есть подтело тела K; K_0 есть наибольшее из подтел L тела K таких, что каждое $f \in \mathscr{M}$ есть линейное отображение E в F, где E и F рассматриваются как векторные пространства над L.*

В самом деле, если L обладает этим последним свойством, то для каждого $\lambda \in L$ действительно $f(x\lambda) = f(x)\lambda$, каковы бы ни были $x \in E$ и $f \in \mathscr{M}$; таким образом, достаточно доказать справедливость первого утверждения. Прежде всего, K_0 содержит единицу тела K и, значит, не сводится к 0; при этом, если $\lambda \in K_0$ и $\mu \in K_0$, то очевидно $\lambda - \mu \in K_0$ и $\lambda\mu \in K_0$, так что K_0 — подкольцо кольца K. Наконец, если $\lambda \in K_0$ и $\lambda \neq 0$, то для всех $x \in E$ и $f \in \mathscr{M}$ имеем $f(x) = f((x\lambda^{-1})\lambda) = f(x\lambda^{-1})\lambda$, откуда $f(x\lambda^{-1}) = f(x)\lambda^{-1}$, и значит, $\lambda^{-1} \in K_0$.

Мы будем называть тело $\chi(\mathscr{M})$, определенное в предложении 9, *подтелом тела K, ассоциированным с множеством представлений $\mathscr{M}$*. В дальнейшем будет рассматриваться лишь случай $E = F = K$: в этом случае $\mathscr{M}$ есть некоторое множество *эндоморфизмов аддитивной группы K*. Если, в частности, $\mathscr{M}$ состоит из *изоморфизмов* структуры тела K на структуру его подтела, то $\chi(\mathscr{M})$ есть не что иное, как множество тех элементов из K, которые *инвариантны относительно всех изоморфизмов $f \in \mathscr{M}$*; действительно, отношение «$f(\xi\lambda) = f(\xi)\lambda$ для всех $\xi \in K$ и $f \in \mathscr{M}$» принимает тогда вид $f(\xi)f(\lambda) = f(\xi)\lambda$ и, значит, равносильно отношению «$f(\lambda) = \lambda$ для всех $f \in \mathscr{M}$».

Нам потребуется также следующее вспомогательное предложение:

Предложение 10. *Пусть E — левое векторное пространство над телом K, (a_ι) — его базис и V — подпространство. Пусть, далее, $\mathscr{M}$ — некоторое множество эндоморфизмов аддитивной группы K и $\bar{f}$ для каждого $f \in \mathscr{M}$ — отображение E в E, определяемое формулой $\bar{f}\left(\sum_\iota \xi_\iota a_\iota\right) = \sum_\iota f(\xi_\iota)\, a_\iota$. Если в этих условиях $\bar{f}(V) \subset V$ для каждого $f \in \mathscr{M}$, то подтело $\chi(\mathscr{M})$ тела K, ассоциированное с $\mathscr{M}$,*

содержит подтело тела K, ассоциированное с V относительно базиса (a_ι).

Пусть $x \in E$. Очевидно, в обозначениях n° 2, $J(\bar{f}(x)) \subset J(x)$ для всех $f \in \mathscr{M}$. В частности, если $y = \sum_\iota \eta_\iota a_\iota$ — первичный элемент подпространства V, то из предположения $\bar{f}(V) \subset V$ и предложения 2 n° 2 вытекает, что для каждого $\xi \in K$ существует $\mu \in K$ такое, что $\bar{f}(\xi y) = \mu y$. Так как $\eta_\varkappa = 1$ для некоторого $\varkappa$, то $f(\xi) = \mu$, и следовательно, $f(\xi\eta_\iota) = f(\xi)\eta_\iota$ для каждого индекса ι, каждого $\xi \in K$ и каждого $f \in \mathscr{M}$; это означает, что компоненты каждого первичного элемента из V принадлежат $\chi(\mathscr{M})$, откуда, принимая во внимание определение 2, и вытекает справедливость предложения.

Следствие. *Если $\mathscr{M}$ — некоторое множество таких изоморфизмов структуры тела K на структуру его подтела, что $\bar{f}(V) \subset V$ для каждого $f \in \mathscr{M}$, то каждый элемент ассоциированного с V подтела тела K инвариантен относительно всех изоморфизмов $f \in \mathscr{M}$.*

Теперь мы в состоянии решить вопрос, поставленный в начале этого n°.

Теорема 3. *Пусть K — тело и $\mathscr{E}(K)$ — кольцо эндоморфизмов его аддитивной группы, наделенное одновременно своей структурой левого векторного пространства над K.*

а) *Пусть L — подтело тела K; для того чтобы кольцо эндоморфизмов $\mathscr{L}(K_L)$ правого векторного пространства K_L над L было (левым) векторным подпространством в $\mathscr{E}(K)$, имеющим конечную размерность n над K, необходимо и достаточно, чтобы L имело в K индекс n.*

б) *Пусть $\mathscr{M}$ — подкольцо кольца $\mathscr{E}(K)$, содержащее тождественное отображение K на себя и являющееся (левым) векторным подпространством в $\mathscr{E}(K)$ над K; для того чтобы подтело $\chi(\mathscr{M})$ тела K, ассоциированное с $\mathscr{M}$, имело в K конечный индекс n, необходимо и достаточно, чтобы $\mathscr{M}$ было размерности n над K.*

в) *Пусть Φ — множество всех подтел L конечного индекса тела K и Ψ — множество всех подколец $\mathscr{M}$ кольца $\mathscr{E}(K)$, содер-*

жащих тождественное отображение K на себя и являющихся конечномерными (левыми) векторными подпространствами в $\mathscr{E}(K)$ над K: $L \to \mathscr{L}(K_L)$ есть взаимно однозначное отображение Φ на Ψ, имеющее своим обратным отображение $\mathscr{M} \to \chi(\mathscr{M})$.

а) Заметим прежде всего, что каждая *линейная форма* x' на векторном пространстве K_L есть линейное отображение K_L в $L \subset K$ и, значит, *эндоморфизм* векторного пространства K_L.

Предположим, что K_L имеет размерность n над L, и пусть $(a_i)_{1 \leqslant i \leqslant n}$ —базис K_L, а (a'_i) — *сопряженный базис в* K_L^*. Покажем, что (a'_i) есть также *базис* (левого) *векторного пространства* $\mathscr{L}(K_L)$ над телом K; действительно, для каждого эндоморфизма u этого тела и каждого элемента $x = \sum_i a_i \xi_i$ имеем $u(x) = \sum_i u(a_i)\xi_i = \sum_i u(a_i)\, a'_i(x)$; иными словами, в векторном пространстве $\mathscr{L}(K_L)$ над K $u = \sum_i u(a_i)\, a'_i$, и значит, элементы a'_i порождают $\mathscr{L}(K_L)$: при этом они линейно независимы в $\mathscr{L}(K_L)$, ибо $\sum_i \lambda_i a'_i = 0$ ($\lambda_i \in K$) означает, что $\sum_i \lambda_i a'_i(x) = 0$ для каждого $x \in K$, и в частности, $\sum_i \lambda_i a'_i(a_j) = 0$, т. е. $\lambda_j = 0$, для каждого индекса j. Эта последняя часть рассуждения сохраняет силу также в случае, когда K_L обладает бесконечным базисом (a_ι), и показывает, что в этом случае координатные формы a'_i линейно независимы в $\mathscr{L}(K_L)$, так что $\mathscr{L}(K_L)$ в этом случае бесконечномерно над K.

б) Покажем, что если $\mathscr{M}$ — подкольцо кольца $\mathscr{E}(K)$, содержащее тождественное отображение K на себя (служащее в $\mathscr{E}(K)$ единицей) и являющееся n-мерным (левым) векторным пространством над K, то тело $L = \chi(\mathscr{M})$ будет иметь в K индекс $n' \leqslant n$; отсюда будет следовать, что $\mathscr{M}$, которое (по определению подтела L) содержится в $\mathscr{L}(K_L)$, будет, согласно а), иметь размерность $\leqslant n'$ и, следовательно, что $n' = n$ и $\mathscr{L}(K_L) = \mathscr{M}$.

Пусть b_i $(1 \leqslant i \leqslant n+1)$ — произвольные $n+1$ элементов из K_L; мы покажем, что они образуют зависимую систему в K_L, чем будет доказано, что размерность K_L не превосходит n. Рассмотрим

отображение $u \longrightarrow (u(b_i))$ пространства $\mathscr{M}$ в левое векторное пространство K_s^{n+1}; это — линейное отображение, и его ранг $\leqslant n$, поскольку $\mathscr{M}$ n-мерно. Пусть V — образ $\mathscr{M}$ при этом отображении; V есть подпространство в K_s^{n+1}, имеющее размерность $\leqslant n$. В обозначениях предложения 10 (и при отнесении K_s^{n+1} к его каноническому базису), для любой пары эндоморфизмов u и v из $\mathscr{M}$ имеем тогда $\overline{(v(u(b_i)))} = (v(u(b_i))) \in V$, поскольку $v \circ u \in \mathscr{M}$; иными словами, $\overline{v}(V) \subset V$ для каждого эндоморфизма $v \in \mathscr{M}$; значит, согласно предложению 10, тело $L = \chi(\mathscr{M})$ содержит подтело тела K, ассоциированное с V (относительно канонического базиса в K_s^{n+1}). Согласно теореме 2, существует система уравнений подпространства V, все коэффициенты которой принадлежат L; следовательно (поскольку V имеет размерность $\leqslant n$), существует хотя бы одно семейство (λ_i), состоящее из $n+1$ элементов тела L, не всех равных нулю, такое, что $\sum_i u(b_i)\lambda_i = 0$ для *каждого* эндоморфизма $u \in \mathscr{M}$; согласно определению подтела $L = \chi(\mathscr{M})$, это соотношение может быть записано также в виде $u\left(\sum_i b_i\lambda_i\right) = 0$; беря, в частности, за u тождественное отображение K на себя, получаем $\sum_i b_i\lambda_i = 0$, чем и доказано, что b_i образуют в K_L зависимую систему.

Обратно, если предположить $\mathscr{M}$ таким, что K_L имеет конечную размерность n, то $\mathscr{M}$, которое содержится в $\mathscr{L}(K_L)$, в силу а), конечномерно, и значит, по предыдущему, размерность K_L равна размерности $\mathscr{M}$.

в) При доказательстве утверждения б) мы видели, что если $\mathscr{M} \in \Psi$ и $L = \chi(\mathscr{M})$, то $\mathscr{L}(K_L) = \mathscr{M}$. С другой стороны, если $L \in \Phi$ имеет в K конечный индекс n, то $\mathscr{M} = \mathscr{L}(K_L)$ имеет размерность n над K, и значит, тело $L' = \chi(\mathscr{M})$ в K имеет индекс n; так как $L \subset L'$, то, согласно следствию предложения 1, отсюда вытекает, что L' имеет размерность 1 над L, т. е. что $L' = L$.

Следствие. $L \longrightarrow \mathscr{L}(K_L)$ *есть убывающее отображение* Φ *на* Ψ (упорядоченных по включению). *Если* L, L' *— подтела конечных индексов тела* K, *то подтело* L'' *тела* K, *порожденное множеством* $L \cup L'$, *будет конечного индекса в* K, *а* $\mathscr{L}(K_{L''})$ *будет пересечением*

$\mathscr{L}(K_L)$ и $\mathscr{L}(K_{L'})$; если при этом и тело $L\cap L'$ — конечного индекса в K, то $\mathscr{L}(K_{L\cap L'})$ есть наименьшее принадлежащее Ψ кольцо, содержащее $\mathscr{L}(K_L)$ и $\mathscr{L}(K_{L'})$.

То, что отношение $L\subset L'$ равносильно отношению $\mathscr{L}(K_L)\supset \mathscr{L}(K_{L'})$, вытекает из определения $\mathscr{L}(K_L)$ и теоремы 3; а отсюда сразу вытекает сформулированное следствие (то, что тело L'', порожденное множеством $L\cup L'$, будет иметь конечный индекс в K, если хотя бы одно из тел L, L' имеет конечный индекс, вытекает из следствия предложения 1).

Замечания. 1) Отметим, что доказательство теоремы 3 сохраняет силу, если в ее пунктах б) и в) не предполагать, что $\mathscr{M}$ содержит единицу кольца $\mathscr{E}(K)$, но потребовать лишь, чтобы $\mathscr{M}$ удовлетворяло следующему (более слабому) условию: для каждого ненулевого элемента ξ из K существует $u\in\mathscr{M}$ такое, что $u(\xi)\neq 0$. Тем самым это условие для подкольца $\mathscr{M}$ в $\mathscr{E}(K)$, являющегося конечномерным (левым) векторным пространством над K, влечет, что $\mathscr{M}$ содержит единицу кольца $\mathscr{E}(K)$; заметим, кроме того, что тогда $\mathscr{M}$ вместе с каждым своим элементом u, обратимым в $\mathscr{E}(K)$, содержит и обратный ему элемент v; в самом деле, для каждого $\lambda\in\chi(\mathscr{M})$ и каждого $\xi\in K$ имеем $u(v(\xi\lambda))=\xi\lambda$, откуда $u(v(\xi\lambda)\lambda^{-1})=\xi$, т. е. $v(\xi\lambda)\lambda^{-1}=v(\xi)$, и, наконец, $v(\xi\lambda)=v(\xi)\lambda$.

2) Наиболее интересные приложения теоремы 3 относятся к случаю *поля* K; как мы увидим в главе V, отсюда вытекают важные результаты *теории Галуа*.

У п р а ж н е н и я. 1) Определим в произведении $A=\mathbf{Z}\times(\mathbf{Z}/(2))$ структуру коммутативного кольца, приняв за аддитивный групповой закон произведение аддитивных законов, заданных на $\mathbf{Z}$ и $\mathbf{Z}/(2)$, и определив умножение формулой $(n,\varepsilon)(n',\varepsilon')=(nn',n\varepsilon'+n'\varepsilon+\varepsilon\varepsilon')$. Пусть A_0 — подкольцо кольца A, образованное элементами $(n,0)$, имеющее ту же единицу, что и A, и изоморфное кольцу $\mathbf{Z}$. Показать, что в A_0-модуле, порожденном каноническим базисом A-модуля A^n, существуют системы, свободные относительно A_0 и не свободные относительно A.

*2) Пусть K_0 — подтело тела K такое, что $[K:K_0]=2$, E — векторное пространство относительно K, E_0 — его подмножество, являющееся векторным пространством относительно K_0, и V — наибольшее подпространство векторного пространства E (относительно K), содержащееся в E_0. Показать, что если W_0 — подпространство в E_0 (относительно K_0), дополнительное к V в E_0, и W — порожденное им подпространство в E (относительно K), то $V\cap W=\{0\}$, иными словами, сумма $V+W$ прямая. [Показать, что если $(x_k)_{1\leqslant k\leqslant n}$ — семей-

ство элементов из W_0, свободное относительно K_0, то $\sum_{k=1}^{n} \lambda_k x_k$ может принадлежать E_0 лишь тогда, когда все λ_k принадлежат K_0; взяв элемент μ из K, не принадлежащий K_0, представить коэффициенты λ_k в виде $\varrho_k + \mu\sigma_k$, где ϱ_k и σ_k принадлежат K_0.]

Предполагая E конечномерным относительно K, показать, что если E_0 и E_0' — векторные пространства относительно K_0, содержащиеся в E, а V и V' — наибольшие подпространства пространства E (относительно K), содержащиеся соответственно в E_0 и E_0', то для существования автоморфизма пространства E, преобразующего E_0 в E_0', необходимо и достаточно, чтобы E_0 и E_0' имели одинаковую размерность относительно K_0, а V и V' — одинаковую размерность относительно K.

*3) Пусть L — бесконечное множество индексов и K — произвольное тело. Показать, что мощность каждого базиса векторного пространства K^L не меньше мощности множества $\mathfrak{P}(L)$. [Пусть $(a_\mu)_{\mu \in M}$ — семейство всевозможных различных элементов из K^L, каждая координата которых равна 0 или 1, E — порожденное им подпространство пространства K^L и $N \subset M$ таково, что $(a_\mu)_{\mu \in N}$ есть базис пространства E (§ 3, теорема 2); для каждого индекса $\mu \in \complement N$ пусть $a_\mu = \sum_{\nu \in N} \xi_{\mu\nu} a_\nu$; проектируя это соотношение на сомножители произведения K^L, показать, применяя теорему 1, что коэффициенты $\xi_{\mu\nu}$ принадлежат подтелу K_0 тела K, порожденному элементами 0 и 1; заметив, что K_0 счетно, показать, что N и M равномощны; в заключение воспользоваться теоремой 2 § 3 и упражнением 24 § 1.]

В случае, когда мощность K не превосходит мощности $\mathfrak{P}(L)$, показать, что каждый базис пространства K^L равномощен $\mathfrak{P}(L)$.

Вывести отсюда, что бесконечномерное векторное пространство над полем никогда не изоморфно своему сопряженному.

4) Пусть K — произвольное тело и $\mathscr{E}(K)$ — кольцо эндоморфизмов аддитивной группы (без операторов) K; для каждого $u \in \mathscr{E}(K)$ и каждого $\lambda \in K$ обозначим через $u\lambda$ эндоморфизм $\xi \to u(\lambda\xi)$ группы K; показать, что сложение и внешний закон $(\lambda, u) \to u\lambda$ определяют в $\mathscr{E}(K)$ структуру *правого векторного пространства* над телом K. Пусть L — произвольное подтело тела K. Показать, что кольцо эндоморфизмов правого векторного пространства K_L есть (правое) векторное подпространство в $\mathscr{E}(K)$, наделенном указанной структурой. Показать, что в утверждениях б) и в) теоремы 3 предположение, что $\mathscr{M}$ содержит единицу кольца $\mathscr{E}(K)$, можно, не нарушая справедливости заключений теоремы, заменить предположением, что $\mathscr{M}$ есть *правое* векторное подпространство пространства $\mathscr{E}(K)$.

§ 6. Матрицы

1. Определение матриц

Определение 1. *Матрицей над непустым множеством E называется всякое семейство $(\alpha_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$ элементов из E, множеством индексов которого является произведение двух конечных множеств L, M. Семейство $(\alpha_{\lambda\mu})_{\mu\in M}$ для каждого $\lambda\in L$ называется строкой с индексом λ (или λ-й строкой) матрицы; семейство $(\alpha_{\lambda\mu})_{\lambda\in L}$ для каждого $\mu\in M$ называется столбцом с индексом μ (или μ-м столбцом) матрицы.*

Наименования «строка» и «столбец» происходят от того, что в случае, когда L и M — интервалы $[1, m]$ и $[1, n]$ натурального ряда, элементы матрицы представляют размещенными по ячейкам прямоугольной таблицы, состоящей из m строк (расположенных горизонтально) и n столбцов (расположенных вертикально):

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}.$$

По условию, если m и n — *явно* заданные целые числа, такая таблица действительно считается символом рассматриваемой матрицы; эта запись освобождает от указания индексов, поскольку подразумевается, что индексы элемента определяются его местом в таблице; например, говоря о матрице

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix},$$

имеют в виду матрицу $(\alpha_{ij})_{1\leqslant i\leqslant 2, 1\leqslant j\leqslant 3}$, в которой $\alpha_{11}=a$, $\alpha_{12}=b$, $\alpha_{13}=c$, $\alpha_{21}=d$, $\alpha_{22}=e$, $\alpha_{23}=f$.

Говоря о матрице из m строк и n столбцов без указания множеств индексов строк и столбцов, подразумевают, что этими множествами служат соответственно интервалы $[1, m]$ и $[1, n]$ натурального ряда.

Каждая матрица, одно из множеств L, M индексов которой пустое, есть не что иное, как пустое семейство элементов множества E; она называется также *пустой матрицей*. В случае, когда $L=\{\lambda_0\}$ и $M=\{\mu_0\}$—множества, сводящиеся к одному элементу, матрицу, имеющую L и M своими множествами индексов, часто отождествляют с единственным образующим ее элементом.

Мы будем обычно обозначать матрицы прописными латинскими буквами.

Подсемейство $(\alpha_{\lambda\mu})_{(\lambda,\mu)\in H\times K}$ матрицы $(\alpha_{\lambda\mu})_{(\lambda,\mu)\in L\times M}$, множеством индексов которого служит произведение множеств $H\subset L$ и $K\subset M$,

называется *подматрицею* рассматриваемой матрицы, полученною путем *вычеркивания* строк с индексами $\lambda \in \complement H$ и столбцов с индексами $\mu \in \complement K$; а про матрицу $(\alpha_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$, обратно, говорят, что она получена путем *окаймления* подматрицы $(\alpha_{\lambda\mu})_{(\lambda,\,\mu)\in H\times K}$ строками с индексами $\lambda \in \complement H$ и столбцами с индексами $\mu \in \complement K$.

Множество всех матриц над множеством E, соответствующих заданным множествам индексов L, M, совпадает с произведением $E^{L\times M}$. Если φ (соответственно ψ) — взаимно однозначное отображение множества L (соответственно M) на множество L' (соответственно M'), то отображение, относящее каждой матрице $(\alpha_{\lambda'\mu'})_{(\lambda',\,\mu')\in L'\times M'}$ над E матрицу $(\beta_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$, где $\beta_{\lambda\mu} = \alpha_{\varphi(\lambda),\,\psi(\mu)}$, есть взаимно однозначное отображение множества $E^{L'\times M'}$ всех матриц над E, соответствующих множествам индексов L', M', на множество $E^{L\times M}$ всех матриц над E, соответствующих множествам индексов L, M.

2. *Матрицы над кольцом*

Наибольшую важность для математики имеют матрицы *над кольцами* с единицей. Множество $A^{L\times M}$ всех матриц над кольцом A с единицей, соответствующих заданным множествам индексов L, M, можно наделить структурой *аддитивной группы*, являющейся произведением структур аддитивной группы сомножителей A произведения $A^{L\times M}$; *суммой* матриц $X = (\xi_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$ и $Y = (\eta_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$ будет тогда матрица $X+Y = (\xi_{\lambda\mu}+\eta_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$.

> Таким образом, сумма матриц X, Y определена, лишь если множества индексов строк и индексов столбцов у обеих матриц *одни и те же*.

Точно так же $A^{L\times M}$ можно наделить структурой *левого* (соответственно *правого*) A-*модуля*, являющейся произведением соответствующих структур сомножителей; произведением ϱX (соответственно $X\varrho$) оператора $\varrho \in A$ и матрицы $X = (\xi_{\lambda\mu})$ будет матрица $(\varrho\xi_{\lambda\mu})$ (соответственно $(\xi_{\lambda\mu}\varrho)$).

Если φ (соответственное ψ) — взаимно однозначное отображение L (соответственно M) на L' (соответственно M'), то взаимно однозначное отображение множества матриц $A^{L'\times M'}$ на множество

матриц $A^{L\times M}$, определяемое отображениями φ и ψ (n° 1), есть изоморфизм каждой из структур A-модуля первого из этих множеств на структуру того же рода второго.

Поэтому можно при желании ограничиться тем случаем, когда L и M — интервалы $[1, m]$ и $[1, n]$ натурального ряда. Предположим, что имеет место этот случай, и пусть ε — единица кольца A. Пусть E_{ij} для каждой пары $(i,j)\in L\times M$ — матрица (α_{hk}), в которой $\alpha_{hk}=0$ при $(h,k)\neq(i,j)$ и $\alpha_{ij}=\varepsilon$; при наделении множества $A^{L\times M}$ одной из двух указанных структур модуля, mn матриц E_{ij} образуют *канонический базис* этого модуля (§ 1, n° 8).

3. *Матрицы и линейные отображения*

Пусть A — кольцо с единицей и L, M — *конечные* множества индексов. Пусть, далее, E и F — унитарные *правые* A-модули, допускающие соответственно *базисы* $(a_\lambda)_{\lambda\in L}$ и $(b_\mu)_{\mu\in M}$, которые имеют своими множествами индексов L и M. Как известно (§ 2, следствие 2 предложения 3), линейное отображение u модуля E в F определяется заданием элементов $y_\lambda = u(a_\lambda)\in F$, причем каждое семейство $(y_\lambda)_{\lambda\in L}$ элементов из F определяет линейное отображение u модуля E в F условиями $u(a_\lambda)=y_\lambda$. Пусть $u(a_\lambda)=\sum_{\mu\in M} b_\mu\alpha_{\mu\lambda}$; коэффициенты $\alpha_{\mu\lambda}$ вполне определяются заданием u и, обратно, определяют элементы $u(a_\lambda)$, а вместе с ними u. Обозначим матрицу $(\alpha_{\mu\lambda})_{(\mu,\lambda)\in M\times L}$, отнесенную отображению u, через $M(u;(a_\lambda),(b_\mu))$ (или, если можно не опасаться путаницы, просто через $M(u)$); мы будем называть ее *матрицей отображения u относительно базисов* (a_λ) *и* (b_μ); таким образом, λ-й столбец этой матрицы образован компонентами $\alpha_{\mu\lambda}$ элемента $u(a_\lambda)$ относительно базиса (b_μ) модуля F. Очевидно, каковы бы ни были линейные отображения u и v модуля E в F,

$$M(u+v)=M(u)+M(v). \tag{1}$$

Иными словами, отображение $u\longrightarrow M(u;(a_\lambda),(b_\mu))$ есть *изоморфизм* аддитивной группы $\mathscr{L}(E,F)$ линейных отображений E в F на аддитивную группу матриц (над A), имеющих M множеством индексов строк и L — множеством индексов столбцов.

Если задана матрица $M(u)=(\alpha_{\mu\lambda})$ отображения u относительно базисов (a_λ) и (b_μ), то каждая компонента η_μ элемента $u(x)$

относительно базиса (b_μ) выражается через компоненты ξ_λ элемента x относительно базиса (a_λ) формулой

$$\eta_\mu = \sum_{\lambda \in L} \alpha_{\mu\lambda} \xi_\lambda. \tag{2}$$

Замечание. В случае кольца A без единицы формула (2) все еще относит каждому элементу (ξ_λ) правого модуля A_d^L элемент (η_μ) правого модуля A_d^M, и определенное так отображение очевидно линейно; но в этом случае различные матрицы могут определять *одно и то же* линейное отображение, и, с другой стороны, могут существовать линейные отображения A_d^L в A_d^M, которые нельзя получить таким способом; примером может служить при $M = L$ тождественное отображение A_d^L на себя.

4. *Произведение двух матриц*

Пусть A — кольцо с единицей, L, M, N — конечные множества индексов, E, F, G — унитарные *правые* A-модули, обладающие соответственно базисами $(a_\lambda)_{\lambda \in L}$, $(b_\mu)_{\mu \in M}$, $(c_\nu)_{\nu \in N}$.

Пусть u — линейное отображение E в F, v — линейное отображение F в G. Найдем матрицу отображения $w = v \circ u$ модуля E в G относительно базисов (a_λ) и (c_ν), если известны матрицы

$$M(u;\ (a_\lambda),\ (b_\mu)) = (\alpha_{\mu\lambda})_{(\mu,\ \lambda) \in M \times L}$$

и

$$M(v;\ (b_\mu),\ (c_\nu)) = (b_{\nu\mu})_{(\nu,\ \mu) \in N \times M}.$$

Имеем

$$w(a_\lambda) = v(u(a_\lambda)) = v\Big(\sum_{\mu \in M} b_\mu \alpha_{\mu\lambda}\Big) = \sum_{\mu \in M} v(b_\mu)\, \alpha_{\mu\lambda} =$$

$$= \sum_{\mu \in M} \Big(\Big(\sum_{\nu \in N} c_\nu \beta_{\nu\mu}\Big) \alpha_{\mu\lambda}\Big) = \sum_{\nu \in N} c_\nu \Big(\sum_{\mu \in M} \beta_{\nu\mu} \alpha_{\mu\lambda}\Big).$$

Поэтому, если положить

$$M(w;\ (a_\lambda),\ (c_\nu)) = (\gamma_{\nu\lambda})_{(\nu,\ \lambda) \in N \times L},$$

для каждой пары индексов (ν, λ) будем иметь

$$\gamma_{\nu\lambda} = \sum_{\mu \in M} \beta_{\nu\mu} \alpha_{\mu\lambda}. \tag{3}$$

Определение 2. *Пусть L, M, N — конечные множества индексов, A — кольцо и*

$$X = (\alpha_{\mu\lambda})_{(\mu,\ \lambda) \in M \times L}, \quad Y = (\beta_{\nu\mu})_{(\nu,\ \mu) \in N \times M}$$

— матрицы над A. Произведением YX матриц Y и X называется матрица $Z=(\gamma_{\nu\lambda})_{(\nu,\,\lambda)\in N\times L}$, *элементы которой задаются формулой* (3).

Таким образом, при этом определении можно написать, что

$$M(v\circ u;\ (a_\lambda),\ (c_\nu))=M(v;\ (b_\mu),\ (c_\nu))\,M(u;\ (a_\lambda),\ (b_\mu)) \tag{4}$$

или, проще,

$$M(v\circ u)=M(v)\,M(u), \tag{5}$$

если можно не опасаться недоразумения.

Замечание. Таким образом, произведение YX определено, лишь если *множество индексов столбцов матрицы Y совпадает с множеством индексов строк матрицы X*; в частности, при $L\neq N$ произведение XY не имеет *никакого смысла*. В формуле (3) фигурируют элементы одной и той же *строки* матрицы Y, умноженные справа на элементы одного и того же *столбца* матрицы X: говорят, что произведение Y на X получается путем «умножения строк на столбцы».

Каждое свойство, относящееся к сумме или композиции линейных отображений, посредством формул (1) и (5) *переводится* в соответствующее свойство, относящееся к сумме или произведению матриц. В частности, имеют место правила *дистрибутивности* и *ассоциативности*

$$X(Y+Z)=XY+XZ, \tag{6}$$

$$(Y+Z)X=YX+ZX, \tag{7}$$

$$X(YZ)=(XY)Z, \tag{8}$$

справедливые всякий раз, когда фигурирующие в них операции имеют смысл.

Аналогичный перевод формулы (1) § 2, дающей композицию двух линейных отображений модулей, разложенных в прямые суммы, приводит к интересной формуле для вычисления произведения двух матриц.

Пусть $(L_i)_{1\leqslant i\leqslant p}$ и $(M_j)_{1\leqslant j\leqslant q}$ — *разбиения* множеств индексов L и M, далее, E_i (соответственно F_j) — подмодуль модуля E (соответственно F), имеющий своим базисом $(a_\lambda)_{\lambda\in L_i}$ (соответственно $(b_\mu)_{\mu\in M_j}$), где $1\leqslant i\leqslant p$ (соответственно $1\leqslant j\leqslant q$); E — есть *прямая сумма* подмодулей E_i и F — *прямая сумма* подмодулей F_j. Тем самым каждому линейному отображению u модуля E в F соответ-

ствует (§ 2, n° 4) семейство (u_{ji}) линейных отображений, где u_{ji} — отображение E_i в F_j, определяемое тем условием, что $u_{ji}(x)$ для каждого $x \in E_i$ есть компонента $u(x)$ в F_j. Из этого определения сразу видно, что если положить $M(u)=X$ и $M(u_{ji})=X_{ji}$ (относительно рассмотренных выше базисов в E, F и E_i, F_j), то матрица X_{ji} будет не чем иным, как *подматрицею* матрицы X, получаемою путем вычеркивания строк с индексами $\mu \in \complement M_j$ и столбцов с индексами $\lambda \in \complement L_i$; поэтому матрицу X можно представлять себе в виде «таблицы матриц», или *клеточной матрицы* из q «строк» и p «столбцов», соответствующих разбиению (M_j) множества индексов строк и (L_i) множества индексов столбцов:

$$\begin{pmatrix} X_{11} & X_{12} & \dots & X_{1p} \\ X_{21} & X_{22} & \dots & X_{2p} \\ \dots & \dots & \dots & \dots \\ X_{q1} & X_{q2} & \dots & X_{qp} \end{pmatrix}.$$

Аналогично пусть $(N_k)_{1 \leqslant k \leqslant r}$ — разбиение множества индексов N и G_k — подмодуль модуля G, имеющий своим базисом $(e_\nu)_{\nu \in N_k}$; G есть прямая сумма подмодулей G_k. Матрица $Y=M(v)$ любого линейного отображения v модуля F в G таким же образом может рассматриваться как клеточная матрица из r строк и q столбцов, образованная подматрицами («клетками») $Y_{kj}=M(v_{kj})$, где (v_{kj}) — семейство линейных отображений, соответствующих отображению v и разбиениям (M_j) и (N_k). Если теперь рассмотреть матрицу $Z=YX$ отображении $w=v \circ u$, то она представится в виде клеточной матрицы из r строк и p столбцов, образованной подматрицами Z_{ki}, соответствующими семейству (w_{ki}) линейных отображений, определяемых отображением w и разбиениями (L_i) и (N_k). Но, согласно формуле (1) § 2, $w_{ki} = \sum_{j=1}^{q} (v_{kj} \circ u_{ji})$; поэтому

$$Z_{ki} = \sum_{j=1}^{q} Y_{kj} X_{ji}. \tag{9}$$

Иными словами, *клеточная матрица* (Z_{ki}) *получается путем образования «произведения» клеточной матрицы* (Y_{kj}) *на клеточную матрицу* (X_{ji}), *как если бы они были обычными матрицами, имеющими соответственно* Y_{kj} *и* X_{ji} *своими элементами*. Вычисление произведения YX, выполняемое таким способом, называется «*поклеточным*». Разумеется, чтобы эта операция была возможна, нужно, чтобы разбиение множества индексов *столбцов* матрицы Y было *тем же*, что и разбиение множества индексов *строк* матрицы X.

Формулы (2), дающие компоненты $u(x)$ относительно базиса (b_μ), допускают следующее истолкование с помощью понятия

произведения матриц: каждый элемент $x = \sum_{\lambda \in L} a_\lambda \xi_\lambda$ модуля E определяет линейное отображение $\xi \longrightarrow x\xi$ модуля A_d в E (обозначенное в n° 1 § 2 через θ_x); этому отображению соответствует *матрица из одного столбца* $M(\theta_x) = (\xi_\lambda)_{\lambda \in L}$ (относительно базиса A_d, образованного единичным элементом ε, и базиса (a_λ) модуля E). Точно так же $y = u(x) = \sum_{\mu \in M} b_\mu \eta_\mu$ определяет линейное отображение θ_y модуля A_d в F, которому таким же образом соответствует матрица из одного столбца $M(\theta_y) = (\eta_\mu)_{\mu \in M}$; но $u(x\xi) = u(x)\xi$, иными словами, $\theta_y = u \circ \theta_x$; перевод этого соотношения на язык матриц, в силу формулы (4), и приводит к формулам (2). Чаще всего, если можно не опасаться путаницы, элемент $x \in E$ отождествляется с одностолбцовой матрицей $M(\theta_x)$ (образованной *компонентами* x относительно базиса (a_λ)); при этом соглашении формулы (2) объединяются в одной формуле

$$u(x) = M(u)\, x. \tag{10}$$

5. Квадратные матрицы

Определение 3. *Квадратной матрицей называют матрицу, строки и столбцы которой имеют одно и то же множество индексов.*

Квадратная матрица, имеющая n строк и n столбцов, называется матрицей *n-го порядка*.

Когда говорят о квадратной матрице n-го порядка, не указывая (общего) множества индексов строк и столбцов, под этим множеством подразумевают интервал $[1, n]$ натурального ряда.

Замечание. Следует иметь в виду, что матрица над A, у которой множества L, M индексов строк и столбцов имеют *одно и то же число элементов*, но *не совпадают*, не должна считаться квадратной матрицей; в частности, произведение двух таких матриц *не определено*.

Пусть L — конечное множество индексов, A — кольцо с единицей ε и E — правый A-модуль, имеющий базис $(a_\lambda)_{\lambda \in L}$, множеством индексов которого служит L. Матрица $M(u; (a_\lambda), (a_\lambda))$ каждого *эндоморфизма* u модуля E относительно *двух базисов, совпадающих* с (a_λ), квадратная; для краткости ее называют матрицей *и относительно базиса* (a_λ).

Сложение и умножение квадратных матриц, имеющих в качестве множества индексов строк и столбцов множество L из n элементов, определяют в множестве этих матриц (на основании формул (6), (7) и (8)) структуру *кольца*; если никакого недоразумения по поводу множества индексов можно не опасаться, определенное так кольцо матриц обозначается просто $\mathbf{M}_n(A)$.

Отображение $u \longrightarrow M(u)$ есть *изоморфизм* кольца $\mathscr{L}(E)$ эндоморфизмов модуля E на кольцо $\mathbf{M}_n(A)$. Единичный элемент кольца $\mathbf{M}_n(A)$ отвечает при этом изоморфизме тождественному автоморфизму модуля E; тем самым им служит матрица $(\delta_{\lambda\mu})$, где $\delta_{\lambda\mu}$ — кронекеровский символ (§ 4, n° 4). Там, где можно не опасаться путаницы, эта матрица будет обозначаться I_n (или 1_n, когда единичный элемент кольца A обозначается 1). Обратимые элементы кольца $\mathbf{M}_n(A)$, называемые *обратимыми матрицами*, при изоморфизме $u \longrightarrow \mathbf{M}(u)$ соответствуют автоморфизмам модуля E.

Примеры квадратных матриц. I. Диагональные матрицы. Элементы $\xi_{\lambda\lambda}$ квадратной матрицы $X = (\xi_{\lambda\mu})$, имеющие равные индексы, называют *диагональными элементами*, а семейство $(\xi_{\lambda\lambda})_{\lambda \in L}$ — *диагональю* матрицы X. Матрицу, все не диагональные элементы которой равны нулю, называют *диагональной матрицей*; единичная матрица I_n диагональная, равно как и все ее кратные $\varrho I_n = I_n \varrho$, где ϱ — скаляр (все диагональные элементы которых равны ϱ); заметим, что, какова бы ни была матрица $X \in A^{L \times M}$ (где M — любое конечное множество индексов), $(\varrho I_n) X = \varrho X$ и, какова бы ни была матрица $Y \in A^{M \times L}$, $Y(\varrho I_n) = Y\varrho$.

Если X и Y — диагональные матрицы, имеющие соответственно диагонали (ξ_λ) и (η_λ), то сумма $X + Y$ есть диагональная матрица с диагональю $(\xi_\lambda + \eta_\lambda)$, а произведение XY — диагональная матрица с диагональю $(\xi_\lambda \eta_\lambda)$; таким образом, диагональные матрицы образуют *подкольцо* кольца $\mathbf{M}_n(A)$, изоморфное *произведению* A^L (или A^n), а матрицы ϱI_n образуют подкольцо кольца диагональных матриц, изоморфное A.

II. Диагональные клеточные матрицы. Пусть $(L_i)_{1 \leqslant i \leqslant p}$ — разбиение множества L; каждая квадратная матрица, имеющая L множеством индексов строк и столбцов, может быть записана в виде «квадратной клеточной матрицы», соответствующей *одному*

и тому же разбиению (L_i) множества индексов строк и множества индексов столбцов (n° 4):

$$\begin{pmatrix} X_{11} & X_{12} & \dots & X_{1p} \\ X_{21} & X_{22} & \dots & X_{2p} \\ \dots & \dots & \dots & \dots \\ X_{p1} & X_{p2} & \dots & X_{pp} \end{pmatrix}.$$

Каждая из матриц X_{ii} есть квадратная матрица, имеющая L_i своим множеством индексов строк и столбцов.

Если теперь все матрицы X_{ij} с $i \neq j$ *нулевые*, то рассматриваемая клеточная матрица называется *диагональной*. Квадратные матрицы, для которых указанная клеточная матрица (соответствующая заданному разбиению (L_i)) диагональная, как вытекает из «поклеточного» получения произведения двух матриц, образуют *кольцо*; легко видеть, что это кольцо изоморфно *произведению* $\prod_{i=1}^{p} \mathscr{L}(E_i)$ колец эндоморфизмов подмодулей E_i модуля E, имеющих своими базисами семейства $(a_\lambda)_{\lambda \in L_i}$.

III. Матрицы подстановок. Пусть π — произвольная *подстановка* множества индексов L; существует, и притом только один, эндоморфизм u_π модуля E такой, что $u_\pi(a_\lambda) = a_{\pi(\lambda)}$ для каждого $\lambda \in L$ (§ 2, следствие 2 предложения 3). Каково бы ни было $\lambda \in L$, элемент матрицы $M(u_\pi)$, находящийся на пересечении столбца с индексом λ и строки с индексом $\pi(\lambda)$, равен ε, все же остальные элементы того же столбца равны нулю. Допуская вольность речи, матрицу $M(u_\pi)$ называют *матрицей подстановки* π. Очевидно, $n!$ матриц, соответствующих всевозможным подстановкам множества L, обратимы; при этом, поскольку для любых двух подстановок π, ϱ множества L имеет место равенство $u_{\pi\varrho} = u_\pi \circ u_\varrho$, матрицы $M(u_\pi)$ образуют мультипликативную *группу*, изоморфную симметрической группе $\mathfrak{S}_n$.

IV. Мономиальные матрицы. Каждая строка и каждый столбец матрицы подстановки содержат лишь один элемент $\neq 0$. Квадратная матрица R, обладающая этим свойством, называется *мономиальной*. Пусть ϱ_λ — единственный ненулевой элемент λ-го столбца матрицы R и $\pi(\lambda)$ — индекс строки, на которой находится этот элемент; ясно, что π есть подстановка множества индексов L, а R — произведение матрицы $M(u_\pi)$ этой подстановки и диагональной матрицы с диагональю (ϱ_λ).

V. **Треугольные матрицы.** В случае, когда множеством L индексов служит интервал $[1, n]$ натурального ряда, *треугольной матрицей* называют квадратную матрицу n-го порядка, в которой $a_{ij}=0$ при $j>i$; говорят также, что эта матрица *имеет над своей диагональю одни нули*. Легко видеть, что треугольные матрицы образуют подкольцо кольца $\mathrm{M}_n(A)$; оно очевидно содержит кольцо диагональных матриц.

6. Транспонированная матрица

Пусть E и F — унитарные правые A-модули, обладающие конечными базисами $(a_\lambda)_{\lambda\in L}$ и $(b_\mu)_{\mu\in M}$. Их *сопряженные* E^* и F^* являются *левыми* A-модулями; будем рассматривать их как *правые* модули над кольцом A^0, *противоположным* A (§ 1, n° 1); *базисы* (a'_λ) *и* (b'_μ), *сопряженные* соответственно к (a_λ) и (b_μ) (§ 4, n° 4), будут также базисами для E^* и F^*, рассматриваемых как правые A^0-модули. Пусть теперь u — линейное отображение E в F и $M(u)=(\alpha_{\mu\lambda})_{(\mu,\,\lambda)\in M\times L}$ — его матрица относительно базисов (a_λ) и (b_μ); найдем матрицу $M({}^tu)$ *сопряженного отображения* ${}^tu$ (§ 4, n° 9) относительно сопряженных базисов (b'_μ) и (a'_λ).

Определение 4. *Пусть* $X=(\alpha_{\mu\lambda})_{(\mu,\,\lambda)\in M\times L}$ *— заданная матрица над кольцом* A. *Транспонированной матрицей или матрицей, транспонированной по отношению к* X, *называется матрица* ${}^tX=(\beta_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$ над кольцом A^0, противоположным A, *такая, что* $\beta_{\lambda\mu}=\alpha_{\mu\lambda}$ *для каждой пары* (λ, μ).

Говорят также, что ${}^tX$ получается из X путем *перестановки строк и столбцов* (подразумевая при этом, что и структура кольца A заменяется одновременно противоположной структурой).

Предложение 1. *Матрица сопряженного отображения* ${}^tu$ *относительно базисов* (b'_μ) *и* (a'_λ) *равна транспонированной матрице отображения* u *и относительно базисов* (a_λ) *и* (b_μ).

Действительно, пусть $M({}^tu)=(b_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$ — матрица отображения ${}^tu$ относительно базисов (b'_μ) и (a'_λ); по определению, $\beta_{\lambda\mu}$ есть λ-я компонента элемента ${}^tu(b'_\mu)$ в E^*, т. е., согласно формуле (12) § 4, примененной к *правым* модулям,

$$\langle {}^tu(b'_\mu),\ a_\lambda\rangle=\langle b'_\mu,\ u(a_\lambda)\rangle;$$

но $\langle b'_\mu, u(a_\lambda)\rangle$ есть не что иное, как μ-я компонента элемента $u(a_\lambda)$ в F, т. е. $a_{\mu\lambda}$.

Очевидно, ${}^t({}^tX) = X$. В силу формул (13) и (15) § 4, имеем

$$ {}^t(X+Y) = {}^tX + {}^tY, \tag{11} $$

$$ {}^t(XZ) = {}^tZ\,{}^tX \tag{12} $$

всякий раз, когда матрицы $X+Y$ и XZ определены. Разумеется, следует помнить, что в правой части формулы (12) произведения элементов матрицы ${}^tZ$ на элементы матрицы ${}^tX$ должны браться *в кольце* A^0.

Применим предложение 1, в частности, к *линейной форме* x' на E. Сопряженное к ней отображение есть не что иное, как линейное отображение A_d^0 в E^* (рассматриваемое как правый A^0-модуль), обозначавшееся выше через $\theta_{x'}$ (n° 4). Тем самым транспонирование однострочной матрицы $M(x')$ (относительно базиса (a_λ) и базиса в A_d, образованного одним элементом ε) дает одностолбцовую матрицу, элементами которой являются *компоненты* ξ'_λ формы x' относительно базиса (a'_λ) (рассматриваемые как элементы кольца A^0); это также прямо вытекает из определения матрицы $M(x')$. В соответствии с принятым в n° 4 соглашением, эта одностолбцовая матрица отождествляется с элементом x' сопряженного модуля E^*, и следовательно, соотношение (10) при $u = x'$ дает

$$ \langle x', x\rangle = {}^tx' \cdot x. \tag{13} $$

Пусть u — линейное отображение E в F; для каждой линейной формы $y' \in F^*$, в силу (10) и предложения 1, имеем

$$ {}^tu(y') = M({}^tu)\cdot y' = {}^tM(u)\cdot y'; $$

поэтому соотношения (12) и (13) показывают, что

$$ \langle {}^tu(y'), x\rangle = {}^ty' \cdot M(u)\cdot x, \tag{14} $$

и фундаментальная формула (12) § 4 (записанная для правых модулей) принимает вид частного случая ассоциативности произведения матриц:

$$ {}^ty' \cdot (M(u)\cdot x) = ({}^ty' \cdot M(u))\cdot x. $$

Следует помнить, что в этих формулах элементы одностолбцовых матриц x', y' должны рассматриваться как принадлежащие A^0, а элементы однострочных матриц ${}^tx'$, ${}^ty'$ — как принадлежащие A.

Обратимые квадратные матрицы над A, с множеством L индексов строк и столбцов, соответствуют *автоморфизмам модуля* E (n° 5). Для каждого такого автоморфизма u *контрагредиентный* автоморфизм $\check{u}$ сопряженного модуля E^* (§ 4, n° 10), являющийся обратным к ${}^t u$, совпадает с сопряженным к автоморфизму, обратному к u; таким образом, полагая $X = M(u)$, в силу предложения 1 имеем $M(\check{u}) = ({}^t X)^{-1} = {}^t(X^{-1})$, что позволяет, не опасаясь двусмысленности, обозначать эту матрицу просто ${}^t X^{-1}$; она называется матрицей, *контрагредиентной* к обратимой матрице X, и иногда обозначается $\check{X}$. Если X и Y — обратимые квадратные матрицы одинакового порядка над A, то, в силу (12),

$$ {}^t(XY)^{-1} = ({}^t X^{-1})({}^t Y^{-1}) \tag{15} $$

(где произведения, входящие в матрицу, стоящую в правой части, берутся *в кольце* A^0).

7. *Матрицы над телом*

Матрицы из m строк и n столбцов над телом K оказываются во взаимно однозначном соответствии с линейными отображениями правого векторного пространства $E = K_d^n$ в правое векторное пространство $F = K_d^m$, если каждому такому отображению отнесена его матрица относительно канонических базисов пространств E и F. По определению, *ранг* такой матрицы X есть ранг того линейного отображения u пространства E в F, которому она соответствует; так как это число, по определению, есть размерность подпространства $u(E)$ пространства F, то это же можно выразить (отождествляя столбцы матрицы X с образами элементов канонического базиса пространства E при отображении u) посредством следующего определения:

Определение 5. *Пусть X — матрица из m строк и n столбцов над телом K. Ее рангом $\varrho(X)$ над K называется размерность подпространства в K_d^m, порожденного n столбцами матрицы X.*

Можно также сказать, что ранг матрицы X — это *наибольшее* число ее линейно независимых столбцов. Согласно определению 5, $\varrho(X) \leqslant \min(m, n)$; для каждой подматрицы Y матрицы X имеем $\varrho(Y) \leqslant \varrho(X)$.

Если E и F — конечномерные векторные пространства и u — линейное отображение E в F, то ранг матрицы $M(u)$ (относительно любых базисов в E и F) равен рангу u.

Понятие ранга матрицы лишь на вид зависит от тела, к которому считаются принадлежащими элементы матрицы. А именно:

Предложение 2. *Если элементы матрицы X из m строк и n столбцов принадлежат подтелу K_0 тела K, то ранг X относительно K_0 равен рангу X относительно K.*

Действительно, столбцы матрицы X принадлежат подпространству H_0 *над телом* K_0, порожденному каноническим базисом пространства K_d^m; поэтому справедливость предложения вытекает из следствия 3 предложения 6 § 5.

Из доказанного выше предложения 1 и теоремы 4 § 4 вытекает

Предложение 3. *Ранг матрицы X над телом K равен рангу транспонированной матрицы ${}^tX$.*

Тем самым ранг матрицы X равен также *наибольшему* числу ее линейно независимых строк (рассматриваемых как элементы левого модуля K_s^n).

Квадратные матрицы n-го порядка над телом K соответствуют эндоморфизмам пространства $E = K_d^n$; они образуют кольцо, изоморфное кольцу $\mathscr{L}(E)$ эндоморфизмов пространства E (n° 5); поскольку автоморфизмам этого пространства соответствуют обратимые квадратные матрицы, из следствия предложения 11 § 3 вытекает

Предложение 4. *Для того чтобы квадратная матрица n-го порядка над телом K была обратимой, необходимо и достаточно, чтобы она была матрицей ранга n.*

8. *Матрицы и линейные уравнения*

Пусть A — кольцо с единицей; рассмотрим систему m линейных (справа) уравнений с n неизвестными, коэффициенты которой и свободные члены принадлежат A:

$$\sum_{j=1}^{n} \alpha_{ij}\xi_j = \beta_i \qquad (1 \leqslant i \leqslant m). \tag{16}$$

Пусть (e_i) — канонический базис произведения $E = A_d^m$; как мы знаем (§ 4, n° 7), система (16) равносильна уравнению

$$\sum_{j=1}^{n} a_j \xi_j = b. \tag{17}$$

где $a_j = \sum_{i=1}^{m} e_i \alpha_{ij}$, $b = \sum_{i=1}^{m} e_i \beta_i$.

Матрица $A = (\alpha_{ij})$ из m строк и n столбцов называется *матрицей системы* (16); сказать, что система (16) имеет решение, все равно, что сказать, что матрица, образованная одним столбцом $b = (\beta_i)$, есть *линейная комбинация* n столбцов матрицы A.

Когда речь идет о системе (16) над *телом* K, приведенное только что истолкование в соединении с определением ранга матрицы дает

Предложение 5. *Для того чтобы система* (16) *m линейных уравнений с n неизвестными над телом K имела решение, необходимо и достаточно, чтобы матрица B, полученная путем окаймления матрицы* $A = (\alpha_{ij})$ *системы* $(n+1)$*-м столбцом* (β_i)*, образованным свободными членами уравнений, имела тот же ранг, что и A.*

Это условие всегда выполнено, когда $m = n$ и A — *обратимая* матрица, т. е. матрица ранга n (предложение 4). Замечая, что если обозначить через x матрицу, состоящую из одной строки $(\xi_j)_{1 \leqslant j \leqslant n}$ (n° 4), то уравнение (17) запишется в виде $A \cdot x = b$, заключаем, что в этом случае имеется *единственное* решение, а а именно задаваемое формулой $x = A^{-1} \cdot b$.

9. Переход к новому базису

Предложение 6. *Пусть E — унитарный правый A-модуль, имеющий базис* $(a_i)_{1 \leqslant i \leqslant n}$*, состоящий из n элементов. Для того чтобы семейство из n элементов* $\overline{a}_i = \sum_{j=1}^{n} a_i \alpha_{ji}$ $(1 \leqslant i \leqslant n)$ *было базисом модуля E, необходимо и достаточно, чтобы квадратная матрица n-го порядка* $P = (\alpha_{ji})$ *была обратима.*

Действительно, P есть не что иное, как матрица эндоморфизма u модуля E, определяемого условиями $u(a_i)=\overline{a}_i$ $(1 \leqslant i \leqslant n)$, относительно базиса (a_i). Но для того, чтобы u был автоморфизмом модуля E, необходимо и достаточно, чтобы $(\overline{a}_i)$ было базисом этого модуля (§ 2, следствие 2 предложения 3), чем справедливость предложения и доказана.

Обратимая матрица P называется *матрицей перехода от базиса* (a_i) *к базису* $(\overline{a}_i)$. Ее можно также рассматривать как матрицу *тождественного* отображения φ модуля E на себя относительно базисов $(\overline{a}_i)$ и (a_i) (*в этом порядке*); из формулы (4) сразу следует тогда, что матрицей перехода *от базиса* $(\overline{a}_i)$ *к базису* (a_i) служит матрица P^{-1}, *обратная* к P.

Предложение 7. *Пусть* (a'_i) *и* $(\overline{a}'_i)$ *— базисы, сопряженные соответственно к* (a_i) *и* $(\overline{a}_i)$; *матрицей перехода от базиса* (a'_i) *к базису* $(\overline{a}'_i)$ *служит матрица* ${}^tP^{-1}$, *контрагредиентная к матрице* P *перехода от базиса* (a_i) *к базису* $(\overline{a}_i)$.

Действительно, сопряженное к тождественному отображению φ модуля E на себя есть тождественное отображение φ' сопряженного модуля E^* на себя; согласно предложению 1, матрица отображения φ' относительно базисов $(\overline{a}'_i)$ и (a'_i) (в этом порядке) получается путем транспонирования матрицы отображения φ относительно базисов (a_i) и $(\overline{a}_i)$ (в этом порядке), т. е. транспонирования матрицы P^{-1}.

Предложение 8. *Пусть* E *и* F *— унитарные правые* A*-модули, имеющие соответственно базисы* $(a_i)_{1 \leqslant i \leqslant n}$ *и* $(b_j)_{1 \leqslant j \leqslant m}$, *состоящие из* n *и* m *элементов. Пусть, далее,* u *— линейное отображение* E *в* F *и* U *— его матрица* (из m строк и n столбцов) *относительно базисов* (a_i) *и* (b_j). *Наконец, пусть* $(\overline{a}_i)_{1 \leqslant i \leqslant n}$ *— второй базис в* E, $(\overline{b}_j)_{1 \leqslant j \leqslant m}$ *— второй базис в* F, P *— матрица перехода от* (a_i) *к* $(\overline{a}_i)$ *и* Q *— матрица перехода от* (b_j) *к* $(\overline{b}_j)$. *Тогда матрица* U' *отображения* u *относительно базисов* $(\overline{a}_i)$ *и* $(\overline{b}_j)$ *задается формулой*

$$U' = Q^{-1}UP. \tag{18}$$

Действительно, $u=\psi\circ u\circ\varphi$, где φ — тождественное отображение E на себя и ψ — тождественное отображение F на себя. Если в правой части этого соотношения взять матрицу φ относительно $(\overline{a}_i)$ и (a_i), матрицу u относительно (a_i) и (b_j) и матрицу ψ относительно (b_j) и $(\overline{b}_j)$, то формула (18) будет непосредственно следовать из формулы (4).

Следствие 1. *Если U и U' — матрицы эндоморфизма и модуля E соответственно относительно базисов (a_i) и $(\overline{a}_i)$, то*

$$U'=P^{-1}HP. \tag{19}$$

Следствие 2. *Если $x=(\xi_i)$ и $\overline{x}=(\overline{\xi}_i)$ — однострочные матрицы, образованные компонентами элемента $x\in E$ относительно базисов (a_i) и $(\overline{a}_i)$, то*

$$x=P\cdot\overline{x}. \tag{20}$$

Достаточно применить предложение 8 к отображению $\xi\to x\xi$ модуля A_d в E, взяв матрицы этого отображения, с одной стороны, относительно базисов $\{\varepsilon\}$ и (a_i), с другой стороны, относительно базисов $\{\varepsilon\}$ и $(\overline{a}_i)$.

Формула (20) равносильна формулам

$$\xi_i=\sum_{j=1}^{n}\alpha_{ij}\overline{\xi}_j \qquad (1\leqslant i\leqslant n), \tag{21}$$

называемым *формулами преобразования координат*; заметим, что они выражают компоненты x относительно базиса (a_i) через компоненты x относительно базиса $(\overline{a}_i)$ и элементы матрицы P, т. е. компоненты базиса $(\overline{a}_i)$ относительно базиса (a_i); говорят, что при переходе к новому базису компоненты элементов модуля E преобразуются *контравариантным* образом.

Пусть теперь $x'=(\xi'_i)$ и $\overline{x}'=(\overline{\xi}'_i)$ — одностолбцовые матрицы (элементы которых принадлежат A^0), образованные компонентами линейной формы $x'\in E^*$ относительно базисов (a'_i) и $(\overline{a}'_i)$, сопряженных к (a_i) и $(\overline{a}_i)$. Поскольку матрицей перехода от (a'_i) к $(\overline{a}'_i)$

служит ${}^tP^{-1}$, имеем $x' = {}^tP^{-1}\bar{x}'$, что может быть записано также в виде

$$ {}^t\bar{x}' = {}^tx'P \tag{22} $$

или

$$ \bar{\xi}'_i = \sum_{j=1}^{n} \xi'_j a_{ji} \qquad (1 \leqslant i \leqslant n). \tag{23} $$

Говорят, что при переходе к новому базису компоненты линейных форм на E преобразуются *ковариантным* образом.

10. *Эквивалентные матрицы*

Определение 6. *Матрицы X и X' из m строк и n столбцов над кольцом A с единицей называются эквивалентными, если существуют обратимая квадратная матрица m-го порядка P и обратимая квадратная матрица n-го порядка Q такие, что*

$$ X' = PXQ. \tag{24} $$

При этом определении предложение 8 можно выразить, сказав, что при переходе к новым базисам в унитарных A-модулях E и F (имеющих конечные базисы) матрица линейного отображения u модуля E в F относительно новых базисов *эквивалентна* матрице отображения u относительно старых базисов.

Другое истолкование состоит в рассмотрении линейных отображений u и u' модуля E в F, имеющих матрицы X и X' относительно *фиксированных* базисов $(a_i)_{1 \leqslant i \leqslant n}$ и $(b_j)_{1 \leqslant j \leqslant m}$ этих модулей; тогда соотношение (24) равносильно соотношению $u' = \psi \circ u \circ \varphi$, где φ и ψ — автоморфизмы E и F, имеющие относительно базисов (a_i) и (b_j) соответственно матрицы Q и P.

Очевидно, отношение «X и X' эквивалентны» действительно есть *отношение эквивалентности* (Теор. мн., Рез., § 5) в множестве матриц из m строк и n столбцов над A, чем и оправдывается принятая терминология.

Примеры эквивалентных матриц. 1) Говорят, что матрицы $X = (\xi_{ij})$ и $X' = (\xi'_{ij})$ из m строк и n столбцов «*отличаются лишь порядком строк*», если существует подстановка σ интервала $[1, m]$ натурального ряда такая, что $\xi'_{ij} = \xi_{\sigma(i),\, j}$ для каждой пары индексов (i, j) (говорят также, что X' получается путем выполнения над

строками матрицы X подстановки σ^{-1}). Матрицы X и X' тогда *эквивалентны*, ибо $X'=PX$, где P — матрица подстановки σ^{-1} (над индексами базиса (b_j) модуля F; см. n° 5).

Точно так же говорят, что X и X' *отличаются лишь порядком столбцов*, если существует подстановка τ интервала $[1, n]$ такая, что $\xi'_{ij}=\xi_{i,\,\tau(j)}$ для каждой пары индексов (i, j). Так как тогда матрицы, транспонированные по отношению к X и X', отличаются лишь порядком строк, то они эквивалентны и, значит, то же верно для X и X' (более точно: $X'=XQ$, где Q — матрица подстановки τ (над индексами базиса (a_i) модуля E)).

2) Предположим теперь, что для некоторого индекса j и всех i $(1 \leqslant i \leqslant m)$ имеют место равенства $\xi'_{ij} = \xi_{ij} + \xi_{ik}\mu$, где k — индекс $\neq j$ и μ — какой-нибудь элемент из A; говорят, что X' получается из X путем *прибавления к j-му столбцу матрицы X k-го столбца, умноженного справа на μ*. И в этом случае X и X' *эквивалентны*: действительно, при втором из рассмотренных выше истолкований имеем $u'(a_j)=u(a_j)+u(a_k)\mu=u(a_j+a_k\mu)$, значит, $u'=u\circ\varphi$, где φ—автоморфизм модуля E, определяемый условиями $\varphi(a_j)=a_j+a_k\mu$ и $\varphi(a_h)=a_h$ для всех $h \neq j$ (это действительно автоморфизм, ибо эндоморфизм φ', определяемый условиями $\varphi'(a_j)=a_j - a_k\mu$ и $\varphi'(a_h) = a_h$ для всех $h \neq j$, обратен φ).

Так же убеждаемся в эквивалентности матриц X и X', когда X' получается из X путем прибавлении к i-й *строке* матрицы X строки с индексом $h \neq i$, умноженной *слева* на какой-нибудь элемент $\lambda \in A$: тогда $X'=PX$, где P — матрица автоморфизма ψ модуля F, определяемого условиями $\psi(b_h)=b_h+b_i\lambda$ и $\psi(b_h)=b_h$ для всех $k \neq h$.

3) Наконец, X и X' эквивалентны также, если для заданного индекса j и всех i $(1 \leqslant i \leqslant m)$ имеют место равенства $\xi'_{ij}=\xi_{ij}\mu$, где μ—*обратимый* элемент кольца A; действительно, тогда $X'=XQ$, где Q — матрица автоморфизма φ модуля E, определяемого условиями $\varphi(a_j)=a_j\mu$ и $\varphi(a_k)=a_k$ для всех $k \neq j$. В этом случае говорят, что X' получается из X путем *умножения j-го столбца матрицы X справа на μ*.

Точно так же X' и X эквивалентны, если X' получается из X путем умножении i-й строки матрицы X слева на обратимый элемент $\lambda \in A$: тогда $X'=PX$, где P — матрица автоморфизма ψ модуля F, определяемого условиями $\psi(b_i)=b_i\lambda$ и $\psi(b_h)=b_h$ для всех $h \neq i$.

Предложение 9. *Для того чтобы две матрицы из m строк и n столбцов над телом K были эквивалентными, необходимо и достаточно, чтобы они имели одинаковый ранг.*

Согласно первому из приведенных выше истолкований эквивалентности, условие *необходимо*, поскольку ранг линейного

отображения равен рангу матрицы этого отображения относительно любых базисов.

Для установления *достаточности* условия покажем, что каждая матрица X ранга r эквивалентна матрице

$$U=\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \tag{25}$$

(где в правой части стоит клеточная матрица, соответствующая разбиению $[1, m]$ на $[1, r]$ и $[r+1, m]$ и разбиению $[1, n]$ на $[1, r]$ и $[r+1, n]$), называемой *канонической матрицей* ранга r из m строк и n столбцов над K.

Предположим для этого, что X есть матрица линейного отображения u модуля E в F относительно базисов (a_i) и (b_j), и покажем, что в E и F существуют базисы $(\overline{a}_i)$ и $(\overline{b}_j)$, относительно которых u имеет матрицу U. Так как u — ранга r, то $H=\overset{-1}{u}(0)$ — размерности $n-r$; пусть G — подмодуль в E, дополнительный к H; тогда существует базис $(\overline{a}_i)$ модуля E такой, что $(\overline{a}_i)_{1\leqslant i\leqslant r}$ будет базисом в G и $(\overline{a}_i)_{r+1\leqslant i\leqslant n}$ — базисом в H. В таком случае векторы $u(\overline{a}_j)$ $(1\leqslant j\leqslant r)$ образуют базис в $u(E)$; значит в F существует базис $(\overline{b}_j)_{1\leqslant j\leqslant m}$ такой, что $\overline{b}_j=u(\overline{a}_j)$ $(1\leqslant j\leqslant r)$ (§ 3, теорема 2). Очевидно, базисы $(\overline{a}_i)$, $(\overline{b}_j)$ удовлетворяют поставленному требованию.

В случае, когда $A=(\alpha_{ij})$ — *явно* заданная матрица из m строк и n столбцов над телом K, можно, как мы это увидим, *явно* определить обратимые квадратные матрицы P и Q, для которых $PAQ=U$, где U — каноническая матрица (25). Можно ограничиться случаем, когда $r=\varrho(A)>0$, ибо иначе A — нулевая матрица и нечего доказывать. Умножая A слева и справа на матрицы надлежащих подстановок, можно всегда свести дело к случаю, когда $\alpha_{11}\neq 0$, а умножая слева первую строку на α_{11}^{-1}, — к случаю, когда $\alpha_{11}=1$; вычтя тогда первую строку, умноженную каждый раз на надлежащий скаляр, из каждой другой, мы обратим все члены первого столбца, кроме α_{11}, в 0; другими словами, существуют обратимая квадратная матрица P_1 и матрица подстановки R_1 такие, что

$$P_1AR_1=\begin{pmatrix} 1 & \beta_{12} & \dots & \beta_{1n} \\ 0 & & & \\ \vdots & & B & \\ 0 & & & \end{pmatrix},$$

где $B=(\beta_{ij})$ есть матрица из $m-1$ строк и $n-1$ столбцов ($2 \leqslant i \leqslant m$, $2 \leqslant j \leqslant n$). Если B — ненулевая матрица, то, умножая ее слева и справа на матрицы надлежащих подстановок, можно добиться, чтобы $\beta_{22} \neq 0$. Поступая так последовательно с первыми r столбцами, убедимся в существовании обратимой квадратной матрицы P и матрицы подстановки R (*явно* задаваемых указанными операциями), для которых

$$PAR = \begin{pmatrix} & \mu_{1,\,r+1} & \cdots & \mu_{1n} \\ I_r & \cdot & \cdots & \cdot \\ & \mu_{r,\,r+1} & \cdots & \mu_{rn} \\ 0 & & 0 & \end{pmatrix}. \tag{26}$$

Наконец, вычтя из каждого из $n-r$ последних столбцов этой матрицы надлежащие кратные первых r столбцов, что сводится к умножению справа на (явно определяемую) обратимую квадратную матрицу S, придем к канонической матрице U.

В том частном случае, когда A есть *обратимая* квадратная матрица, в качестве R можно взять единичную матрицу; согласно формуле (26), тогда матрица P, определенная описанным способом, будет просто матрицей, *обратной* к A (см. § 3, n° 2, замечание 1 после следствия 3 теоремы 3, а также § 6, упражнение 9а).

Операции, приведшие к матрице (26), позволяют также явно определить решения линейного уравнения $Ax=b$ с явно заданным вектором b. Действительно, это уравнение может быть записано в виде $PAR(R^{-1}x)=Pb$; поскольку R — матрица подстановки, компоненты вектора $y=R^{-1}x$, с точностью до порядка, те же, что у x. Теперь, для того, чтобы уравнение имело решения, необходимо и достаточно, чтобы $m-r$ последних компонент вектора Pb были нулями; если это выполнено, то из соотношения $PARy=Pb$ сразу получаются первые r компонент вектора y в виде явных функций последних $n-r$, остающихся произвольными.

Этот метод явного разрешения линейных уравнений известен под названием *метода последовательных подстановок*; он действительно сводится к выражению первой компоненты вектора y через остальные с помощью первого уравнения, затем подстановке этого выражения в остальные уравнения и применению к этим последним той же процедуры до тех пор, пока мы не придем к системе, матрица которой имеет вид (26).

11. *Подобные квадратные матрицы*

Определение 7. *Квадратные матрицы n-го порядка X, X' над кольцом A с единицей называются подобными, если существует обратимая квадратная матрица n-го порядка P такая, что*

$$X' = PXP^{-1}. \tag{27}$$

При этом определении следствие 1 предложения 8 можно выразить, сказав, что при переходе в унитарном A-модуле E (имеющем конечный базис) к новому базису матрица эндоморфизма u модуля E относительно нового базиса *подобна* матрице u относительно старого базиса.

Другое истолкование состоит в рассмотрении эндоморфизмов u, u' и автоморфизма φ модуля E, имеющих X, X' и P своими матрицами относительно некоторого *фиксированного* базиса в E; соотношение (27) равносильно тогда соотношению $u'=\varphi\circ u\circ\varphi^{-1}$.

Очевидно, и здесь отношение «X и X' подобны» есть *отношение эквивалентности* в множестве всех квадратных матриц n-го порядка над A.

З а м е ч а н и я. 1) Две квадратные матрицы, отличающиеся лишь порядком строк (или столбцов), эквивалентны, но, вообще говоря, *не подобны*. Матрица, подобная квадратной матрице $X=(\xi_{ij})$, получится, если подвергнуть *одной и той же* подстановке σ^{-1} и строки и столбцы, т. е. если рассмотреть матрицу $X'=(\xi'_{ij})$, где $\xi'_{ij}=\xi_{\sigma(i),\,\sigma(j)}$ для каждой пары индексов $(i,\ j)$; действительно, легко видеть, что $X'=PXP^{-1}$, где P — матрица подстановки σ^{-1} (индексов базиса (a_i) модуля E).

2) Две подобные матрицы над одним и тем же *телом* K очевидно имеют одинаковый ранг, поскольку они эквивалентны (предложение 9). Но здесь это необходимое условие уже не достаточно для того, чтобы две квадратные матрицы над K были подобными; необходимые и достаточные условия в случае *поля* K будут даны в главе VII.

3) Пусть X и X' — квадратные матрицы n-го порядка, записываемые в форме «диагональных» клеточных квадратных матриц (n° 5):

$$X=\begin{pmatrix} X_1 & 0 & \dots & 0\\ 0 & X_2 & \dots & 0\\ \dots & \dots & \dots & \dots\\ 0 & 0 & \dots & X_p\end{pmatrix},\qquad X'=\begin{pmatrix} X'_1 & 0 & \dots & 0\\ 0 & X'_2 & \dots & 0\\ \dots & \dots & \dots & \dots\\ 0 & 0 & \dots & X'_p\end{pmatrix},$$

соответствующих *одному и тому же* разбиению множества индексов $[1, n]$ и для X, и для X'. Если X_i и X'_i для каждого i $(1\leqslant i\leqslant p)$ подобны, то X и X' подобны; действительно, если $X'_i=P_iX_iP_i^{-1}$ для всех i $(1\leqslant i\leqslant p)$, то, как показывает правило «поклеточного» вычисления произведения (n° 4), $X'=PXP'$, где

$$P=\begin{pmatrix} P_1 & 0 & \dots & 0\\ 0 & P_2 & \dots & 0\\ \dots & \dots & \dots & \dots\\ 0 & 0 & \dots & P_p\end{pmatrix}.$$

Упражнения. 1) Пусть E — унитарный правый A-модуль и A_r — кольцо квадратных матриц r-го порядка над A. Определим на множестве E^r внешний закон композиции, имеющий A_r своим множеством операторов, обозначив через $x \cdot P$, для каждого элемента $x=(x_i)_{1 \leqslant i \leqslant r}$ из E^r и каждой матрицы $P=(\alpha_{ij})$ из A_r, элемент $y=(y_i)$ из E^r, в котором

$$y_i = \sum_{j=1}^{r} x_j \alpha_{ji} \qquad (1 \leqslant i \leqslant r).$$

Этот внешний закон есть закон аддитивной группы на E^r, определяющий в этом множестве структуру правого модуля относительно кольца A_r. Показать, что для того, чтобы A-модуль E допускал систему r образующих, необходимо и достаточно, чтобы A_r-модуль E^r был моногенным.

2) Пусть A — кольцо с единицей, $(L_i)_{1 \leqslant i \leqslant p}$ — разбиение интервала $[1, n]$ натурального ряда и каждая квадратная матрица n-го порядка X над A представлена в форме квадратной клеточной матрицы (X_{ij}), соответствующей одному и тому же разбиению (L_i) множества индексов строк и множества индексов столбцов.

а) Показать, что матрицы X, для которых клеточная матрица (X_{ij}) «*треугольная*», т. е. такая, что $X_{ij}=0$ при $i < j$, образуют *подкольцо* кольца $\mathrm{M}_n(A)$. Как можно охарактеризовать эндоморфизмы, которым соответствуют эти матрицы?

б) Показать, что если каждая из квадратных подматриц X_{ii} $(1 \leqslant i \leqslant p)$ такой матрицы X обратима, то и X обратима, причем X^{-1} снова является треугольной клеточной матрицей. Доказать, что если A — *тело*, то это достаточное условие обратимости матрицы X также необходимо.

3) Пусть $A=\mathbf{Z}/(30)$. Показать, что у матрицы

$$\begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 3 \end{pmatrix}$$

над кольцом A строки линейно независимы, но любые два столбца линейно зависимы.

*4) Пусть X — матрица из m строк и n столбцов над телом K; показать, что ее ранг $\varrho(X)$ равен наибольшему из рангов ее квадратных подматриц. [Пусть $\varrho(X)=r$ и $a_1, a_2, \ldots, a_r$ — r столбцов матрицы X, образующие в K_d^m свободную систему; образовав базис пространства K_d^m из этих r векторов и $m-r$ векторов канонического базиса (e_i), показать, что компоненты векторов $a_1, a_2, \ldots, a_r$ по r остальным векторам канонического базиса образуют матрицу ранга r.]

5) Пусть X — матрица из m строк и n столбцов над телом K и r — ее ранг. Показать, что ранг подматрицы из m строк и s столбцов, получающейся путем вычеркивания $n-s$ столбцов матрицы X, $\geqslant r+s-n$.

6) Пусть $X=(\alpha_{ij})$ — матрица из m строк и n столбцов над телом K. Для того чтобы X была ранга 1, необходимо и достаточно, чтобы в K существовали семейства $(\lambda_i)_{1\leqslant i\leqslant m}$ из m элементов, не равных все нулю, и $(\mu_j)_{1\leqslant j\leqslant n}$ из n элементов, не равных все нулю, такие, что $\alpha_{ij}=\lambda_i\mu_j$ для каждой пары индексов (i, j).

*7) Пусть E — правое векторное пространство над телом K и H — его гиперплоскость. Всякий эндоморфизм u пространства E, оставляющий все элементы из H инвариантными, дает при факторизации эндоморфизм одномерного факторпространства E/H, тем самым имеющий вид $\dot{x}\to\dot{x}\mu(\dot{x})$, где $\mu(\dot{x})\in K$ и $\mu(\dot{x}\lambda)=\lambda^{-1}\mu(\dot{x})\lambda$. *Автоморфизм* u, оставляющий все элементы из H инвариантными, называется *сдвигом*, если соответствующий автоморфизм факторпространства E/H есть тождественное отображение, и *растяжением* — в противном случае; если u — растяжение, то множество всех элементов $\mu(\dot{x})$, являющееся классом сопряженных элементов (гл. I, § 7, п° 5) в мультипликативной группе K^* ненулевых элементов тела K, называется *классом* растяжения u.

а) Показать, что для каждого растяжения существует, и притом лишь одна, дополнительная к H прямая, инвариантная относительно этого растяжения.

б) Пусть φ — линейная форма, для которой $H=\overset{-1}{\varphi}(0)$; показать, что для каждого сдвига u существует однозначно определенный вектор $a\in H$ такой, что $u(x)=x+a\varphi(x)$. Обозначая через $\Gamma(E, H)$ группу всех автоморфизмов пространства E, оставляющих инвариантным каждый элемент из H, показать, что сдвиги (относительно H) образуют ее нормальную коммутативную подгруппу $\Theta(E, H)$, изоморфную аддитивной группе H; факторгруппа $\Gamma(E, H)/\Theta(E, H)$ изоморфна K^*.

в) Если E конечномерно, то для каждого сдвига u существует такой базис пространства E, что в матрице u относительно этого базиса все диагональные элементы равны 1 и по крайней мере еще один элемент $\neq 0$.

г) Показать, что *централизатор* (гл. I, § 6, упражнение 13) группы $\Theta(E, H)$ в группе $\mathbf{GL}(E)$ автоморфизмов пространства E есть композиция $Z(E)\Theta(E, H)=\Theta(E, H)Z(E)$ группы $\Theta(E, H)$ и центра $Z(E)$ группы $\mathbf{GL}(E)$ (§ 2, следствие 2 предложения 5). Единственными автоморфизмами, принадлежащими этому централизатору и оставляющими инвариантным по крайней мере один ненулевой элемент из E, являются сдвиги из $\Theta(E, H)$.

д) Показать, что *нормализатор* (гл. I, § 6, упражнение 13) группы $\Theta(E, H)$ в $\mathbf{GL}(E)$ есть подгруппа $\mathbf{GL}(E)$, образованная всеми автоморфизмами, оставляющими H инвариантным.

*8) Пусть $F(E)$ — нормальная подгруппа группы $\mathbf{GL}(E)$, образованная теми автоморфизмами u, для которых множество всех элементов из E, инвариантных относительно u, имеет *конечную* фактор-

размерность (если E конечномерно, то $F(E)=\mathbf{GL}(E)$). Пусть, далее, $C(E)$ — нормальная подгруппа группы $\mathbf{GL}(E)$, порожденная всеми сдвигами; она содержится в $F(E)$.

а) Показать, что если E — размерности >1, то для каждой пары ненулевых векторов x, y из E существует сдвиг или произведение двух сдвигов, переводящее x в y (иными словами, группа $C(E)$ *транзитивно* действует в дополнении к $\{0\}$ в E).

б) Пусть V и W — гиперплоскости, $\dot{x}_0=x_0+V$ — класс $\bmod V$, отличный от V, и $\dot{y}_0=y_0+W$ — класс $\bmod W$, отличный от W. Показать, что если E — размерности >1, то существует сдвиг или произведение двух сдвигов, преобразующее V в W и $\dot{x}_0$ в $\dot{y}_0$. [Рассмотреть сначала случай различных V и W.]

в) Показать, что если E — размерности >1, то любые два сдвига, отличные от тождественного отображения, являются *сопряженными элементами* (гл. I, § 7, n° 5) *группы* $F(E)$.

г) Показать, что если E — размерности >2, то любые два сдвига, отличные от тождественного отображения, являются *сопряженными элементами группы* $C(E)$. [С помощью б) свести к случаю, когда гиперплоскости обоих сдвигов совпадают, и затем использовать а).]

д) Если E двумерно, то для того, чтобы любые два сдвига были сопряженными элементами группы $C(E)$, необходимо и достаточно, чтобы подгруппа Q группы K^*, порожденная *квадратами* всевозможных элементов из K^*, совпадала с K^*. [Показать, что если u — сдвиг, а a — элемент из E, не инвариантный относительно u, и $b=u(a)-a$, то для каждого сдвига u', сопряженного к u в $C(E)$, имеет место равенство $u'(a)-a=a\lambda+b\mu$, где $\mu\in Q$ или $\mu=0$; воспользоваться для этого тем, что во всякой мультипликативной группе элементы $\alpha\beta\alpha^{-1}\beta$ и $\alpha\beta^2\alpha$ являются произведениями двух квадратов. Чтобы убедиться в том, что сформулированное условие влечет сопряженность в $C(E)$ каждого сдвига v со сдвигом u, свести рассмотрение к случаю, когда $v(a)=a\lambda+b$.]

е) Если E — размерности >1, то для того, чтобы растяжения u и u' были сопряженными относительно группы $C(E)$ (т. е. чтобы существовал автоморфизм $v\in C(E)$, для которого $u'=vuv^{-1}$), необходимо и достаточно, чтобы классы (упражнение 7) этих растяжений совпадали. [Использовать б).] Вывести отсюда, что если класс некоторого растяжения содержится в коммутанте (гл. I, § 6, n° 8) группы K^* то это растяжение принадлежит группе $C(E)$. [Воспользоваться тем, что $vuv^{-1}u^{-1}=v\,(uv^{-1}u^{-1})$.]

*9) а) Показать, что каждый автоморфизм u, принадлежащий $F(E)$, есть произведение автоморфизма, принадлежащего $C(E)$, и, возможно, растяжения, гиперплоскостью инвариантных элементов которого служит фиксированная гиперплоскость H_0. [Провести индукцию по факторразмерности подпространства элементов, инвариантных относительно u, используя 8а и 8е.]

б) Показать, что $C(E)$ содержит коммутант группы $F(E)$ и, за исключением того случая, когда $K=\mathbf{Z}/(2)$ и $\dim E=2$, совпадает с ним. [При доказательстве того, что $C(E)$ содержит коммутант группы $F(E)$, использовать а) и упражнение 8е; для установления того, что $C(E)$, кроме указанного исключительного случая, содержится в этом коммутанте, показать, используя упражнения 7б и 8в, что при всяком представлении $F(E)$ в коммутативную группу образом каждого сдвига служит нейтральный элемент.]

*10) Показать, что если E — размерности >2, то каждая нормальная подгруппа группы $\mathbf{GL}(E)$, не содержащаяся в центре $Z(E)$, содержит коммутант $C(E)$ группы $F(E)$, и что каждая нормальная подгруппа *группы* $C(E)$, не содержащаяся в $Z(E)$, совпадает с $C(E)$. [Показать, что если Γ — нормальная подгруппа группы $\mathbf{GL}(E)$ и u — автоморфизм, принадлежащий Γ и не принадлежащий $Z(E)$, то существует сдвиг v такой, что $w=v^{-1}u^{-1}vu$ оставляет инвариантной некоторую гиперплоскость H и не принадлежит $Z(E)$; для этого воспользоваться упражнением 7г и показать с помощью упражнения 7б, что $w(x)-x$ для каждого $x\in E$ принадлежит фиксированному двумерному подпространству. Доказать, далее, с помощью 7г, что либо w есть сдвиг, либо существует сдвиг t, оставляющий инвариантным каждый элемент из H и такой, что $twt^{-1}w^{-1}$ не принадлежит $Z(E)$. В заключение использовать 8в; аналогичное рассуждение для нормальных подгрупп группы $C(E)$ с использованием 8г.]

11) Пусть X и Y — матрицы из m строк и n столбцов над телом K; если существуют квадратные матрицы m-го порядка P, P_1 и квадратные матрицы n-го порядка Q, Q_1 такие, что $Y=PXQ$ и $X=P_1YQ_1$, то X и Y эквивалентны. [Использовать предложение 9.]

12) Пусть X, X', Y, Y' — квадратные матрицы n-го порядка над кольцом A с единицей, причем X обратима. Для того чтобы существовали обратимые квадратные матрицы n-го порядка P и Q такие, что $X'=PXQ$ и $Y'=PYQ$, необходимо и достаточно, чтобы X' была обратима, а матрицы YX^{-1} и $Y'X'^{-1}$ подобны.

§ 7. Алгебры

Все рассматриваемые в этом параграфе кольца операторов предполагаются коммутативными и содержащими единицу.

1. Определение алгебры

Определение 1. *Пусть* A — коммутативное *кольцо с единицей* ε. *Алгеброй* (или *гиперкомплексной системой*) *над* A (или *относительно* A) *или также* A*-алгеброй называется всякое кольцо с операторами* E, *внешний закон которого имеет множеством*

своих операторов кольцо A и вместе с заданным в E сложением определяет в E структуру унитарного A-модуля *).

Другими словами, алгебра над A есть *кольцо* E, наделенное внешним законом (записываемым в виде левого умножения), имеющим A своей областью операторов и удовлетворяющим следующим тождествам:

$$\alpha(x+y)=\alpha x+\alpha y, \tag{1}$$
$$(\alpha+\beta)x=\alpha x+\beta x, \tag{2}$$
$$\alpha(\beta x)=(\alpha\beta)x, \tag{3}$$
$$\varepsilon x=x, \tag{4}$$
$$\alpha(xy)=(\alpha x)y=x(\alpha y) \tag{5}$$

($\alpha\in A$, $\beta\in A$, $x\in E$, $y\in E$).

Отсюда вытекает общая формула дистрибутивности

$$\Big(\sum_i \alpha_i x_i\Big)\Big(\sum_j \beta_j y_j\Big)=\sum_{i,j}(\alpha_i\beta_j)(x_i y_j) \tag{6}$$

($\alpha_i\in A$, $\beta_j\in A$, $x_i\in E$, $y_j\in E$).

Примеры. 1) Каждое кольцо E с единицей может быть наделено структурой алгебры относительно любого подкольца A своего центра (с тем же единичным элементом, что и у E), если за композицию оператора $z\in A$ и элемента $x\in E$ принять произведение $zx(=xz)$ этих элементов в кольце E.

2) Структура кольца с операторами, определяемая в любом кольце E внешним законом $(n, x)\to nx$, где $n\in\mathbf{Z}$ (гл. I, § 8, п° 2), есть структура алгебры относительно кольца $\mathbf{Z}$.

°3) Пусть I — открытый интервал числовой прямой $\mathbf{R}$. Кольцо всех непрерывных числовых функций на I будет наделено структурой алгебры над полем $\mathbf{R}$, если для каждой непрерывной числовой функции f на I и каждого вещественного числа λ понимать под λf функцию $t\to\lambda f(t)$.

Структура кольца с операторами, *противоположная* заданной в алгебре E над A, также есть структура алгебры над A;

*) В обычно употреблявшейся до сих пор терминологии «алгебрами» назывались исключительно алгебры *над полем*; это действительно наиболее часто встречающиеся алгебры. Если на протяжении какой-нибудь главы нам придется рассматривать лишь алгебры этого рода, мы будем считать себя вправе придавать в этой главе слову «алгебра» всюду смысл «алгебра над полем», причем будем явно оговаривать эту вольность речи.

наделенное этой структурой алгебры, E называется алгеброй, *противоположной* заданной.

Если внешний закон алгебры E над A *сузить* на *подкольцо* B кольца A (имеющее тот же единичный элемент, что и A), то этот закон (вместе с заданными в E сложением и умножением) определит в множестве E новую структуру алгебры, которую следует отличать от структуры алгебры, имеющей своим кольцом операторов A.

Замечания. 1) Позже (в теории «алгебр Ли») нам придется рассматривать алгебраические структуры, определяемые в некотором множестве E заданием двух внутренних законов и внешнего закона, имеющего множеством своих операторов коммутативное кольцо, причем будут выполнены все аксиомы алгебр, за исключением *ассоциативности* умножения в E; по аналогии множество, наделенное такой структурой, будет называться «неассоциативной алгеброй».

2) Можно было бы попытаться обобщить определение 1, отбросив ограничение *коммутативностью*, наложенное на кольцо операторов A; но из условия (5) видно, что в наиболее важных случаях это обобщение было бы лишь кажущимся: действительно, *аннулятор* $\mathfrak{a}$ A-модуля E (§ 1, n° 9) есть двусторонний идеал, факторкольцо по которому $A/\mathfrak{a}$ *коммутативно*, а перейдя к точной структуре, ассоциированной со структурой A-модуля в E (§ 1, n° 9), мы увидели бы, что получили в E структуру алгебры относительно $A/\mathfrak{a}$ (см. упражнение 11).

Часто приходится рассматривать в алгебре E структуру *левого* (или правого) *модуля* относительно ее *некоммутативного* подкольца B; не следует думать, что E есть алгебра над B (для элементов $\alpha \in B$ соотношение (5), вообще говоря, не будет выполняться).

2. *Базисы алгебры. Таблицы умножения*

Наиболее интересны те алгебры, которые, рассматриваемые как *модули* относительно их кольца операторов A, допускают *базис* относительно A (§ 1, n° 6); это всегда имеет место для алгебр над *полем* (§ 3, теорема 1).

Как вытекает из формулы (6), в алгебре E, имеющей базис относительно своего кольца операторов A, умножение вполне определено, если известны, с одной стороны, умножение в кольце A, а с другой — всевозможные попарные произведения элементов базиса. Если $(a_\lambda)_{\lambda \in L}$ — базис в E относительно A, то каждый элемент из E однозначно представляется в виде $\sum_\lambda \xi_\lambda a_\lambda$;

поэтому, в частности,

$$a_\lambda a_\mu = \sum_\nu \gamma_{\lambda\mu\nu} a_\nu, \tag{7}$$

и знание элементов $\gamma_{\lambda\mu\nu}$, фигурирующих в этих соотношениях, полностью определяет умножение в E; говорят, что соотношения (7) образуют *таблицу умножения* рассматриваемого базиса (a_λ).

Это название происходит оттого, что в случае, когда множеством индексов базиса служит интервал $[1, n]$ натурального ряда, соотношения (7) обычно записывают, располагая правые части этих соотношений в виде *квадратной таблицы*

	a_1	a_2	. . . . .	a_j	. . . . .	a_n
a_1						
a_2						
. . . . .						
a_i				$\sum_k \gamma_{ijk} a_k$		
. . . . .						
a_n						

где подразумевается, что на пересечении *строки* элемента a_i и *столбца* элемента a_j стоит значение произведения $a_i a_j$.

Элементы $\gamma_{\lambda\mu\nu}$ кольца A, фигурирующие в соотношениях (7), *не произвольны*, ибо, каковы бы ни были индексы λ, μ, ν, должны выполняться *соотношения ассоциативности*

$$(a_\lambda a_\mu)\, a_\nu = a_\lambda\, (a_\mu a_\nu); \tag{8}$$

согласно (7), эти соотношения равносильны соотношениям

$$\sum_{\varrho} \gamma_{\lambda\mu\varrho}\gamma_{\varrho\nu\sigma} = \sum_{\varrho} \gamma_{\lambda\varrho\sigma}\gamma_{\mu\nu\varrho}, \tag{9}$$

которые должны выполняться для любых индексов λ, μ, ν, σ.

Обратно, пусть заданы унитарный A-модуль E, его базис $(a_\lambda)_{\lambda\in E}$ и семейство $(\gamma_{\lambda\mu\nu})$ элементов кольца A, удовлетворяющее соотношениям (9); тогда в E можно *определить* умножение, для любых $x=\sum_\lambda \xi_\lambda a_\lambda$, $y=\sum_\lambda \eta_\lambda a_\lambda$ положив $xy=\sum_{\lambda,\mu,\nu} \xi_\lambda\eta_\mu\gamma_{\lambda\mu\nu}a_\nu$; двоякая дистрибутивность этого закона относительно заданного на E сложения непосредственно очевидна, а условия (9) влекут его ассоциативность; следовательно, вместе со сложением он определяет в E структуру *кольца*; наконец, ясно, что заданный на E внешний закон в соединении с этой структурой кольца определяет в E структуру алгебры относительно A. Это — часто применяемый способ определения алгебры.

Заметим, что элементы $\gamma_{\lambda\mu\nu}$ зависят от выбранного базиса; при изменении базиса таблица умножения, вообще говоря, меняет свой вид. В главе III мы уточним способ преобразования коэффициентов $\gamma_{\lambda\mu\nu}$ при переходе к новому базису, а именно покажем, что в случае, когда E имеет конечный базис, они являются компонентами один раз контравариантного и дважды ковариантного *тензора* (глава III, § 3).

Если E — алгебра, определенная указанным образом, то взяв, при том же базисе (a_λ), таблицу умножения с коэффициентами $\gamma'_{\lambda\mu\nu}=\gamma_{\mu\lambda\nu}$, мы определим в E *противоположную* структуру. В частности, для *коммутативности* алгебры E необходимо и достаточно, чтобы $\gamma_{\lambda\mu\nu}=\gamma_{\mu\lambda\nu}$, каковы бы ни были λ, μ, ν.

Другими словами, таблица умножения алгебры, противоположной E (относительно того же базиса), получается путем «отражения» таблицы умножения алгебры E в ее «диагонали»; коммутативная алгебра характеризуется тем, что ее таблица умножения «симметрична относительно своей диагонали».

Точно так же для того, чтобы элемент $a_\varkappa$ рассматриваемого базиса был *единицей алгебры* E, необходимо и достаточно, чтобы $a_\varkappa a_\lambda = a_\lambda a_\varkappa = a_\lambda$, каково бы ни было λ, т. е. чтобы $\gamma_{\varkappa\lambda\mu}=\gamma_{\lambda\varkappa\mu}$ при $\mu\neq\lambda$ и $\gamma_{\varkappa\lambda\lambda}=\gamma_{\lambda\varkappa\lambda}=\varepsilon$, каково бы ни было λ.

Алгебра E относительно *поля* K является *векторным пространством* относительно K; его размерность относительно K (§ 3, определение 1) чаще всего называют *рангом* алгебры E относительно K (или *степенью* E относительно K, если E — *поле*); напомним, что этот ранг в случае его конечности обозначается $[E : K]$ (§ 3, n° 2).

3. Подалгебры. Идеалы. Факторалгебры

Пусть E — алгебра относительно кольца A. В любом *подкольце* F кольца с *операторами* E (т. е., по определению, *устойчивом* подкольце этого кольца; см. гл. I, § 8, n° 4) структура, индуцированная заданной в E структурой алгебры, тоже есть структура алгебры относительно A; наделенное этой структурой, F называется *подалгеброй* алгебры E. Каково бы ни было множество $M \subset E$, множество N тех элементов из E, которые перестановочны с каждым элементом из M, есть подалгебра алгебры E (гл. I, § 8, предложение 2); в частности, *центр* алгебры E есть ее подалгебра.

Нет необходимости вновь определять понятие (левого, правого или двустороннего) идеала алгебры: оно было определено более общим образом для любого кольца с операторами (гл. I, § 8, n° 5).

Если $\mathfrak{a}$ — двусторонний идеал алгебры E (относительно кольца A), то структура кольца с операторами в факторможестве $E/\mathfrak{a}$ есть структура алгебры относительно A; наделенное этой структурой, $E/\mathfrak{a}$ называется *факторалгеброй* E по $\mathfrak{a}$.

4. Представления

Пусть E и F — алгебры относительно одного и того же кольца A; мы уже определили (гл. I, § 8, n° 8) *представления* E в F; напомним, что отображение u алгебры E в F есть представление, если оно удовлетворяет тождествам

$$u(x+y) = u(x) + u(y), \quad u(xy) = u(x)\,u(y), \quad u(\alpha x) = \alpha u(x)$$
$$(\alpha \in A, \quad x \in E, \quad y \in E).$$

Можно также сказать, что u есть представление E в F, если оно есть *линейное отображение* A-модуля E в A-модуль F

и одновременно *представление* относительно мультипликативных законов, заданных в E и F.

Все свойства представлений колец с операторами относятся, в частности, к представлениям алгебр: если u—представление E в F, то $u(E)$ есть подалгебра алгебры F; $\mathfrak{a} = u^{-1}(0)$ есть двусторонний идеал алгебры E, $u(E)$ изоморфно факторалгебре $E/\mathfrak{a}$, и u есть композиция канонического гомоморфизма E на $E/\mathfrak{a}$ и изоморфизма $E/\mathfrak{a}$ на $u(E)$; если G — подалгебра алгебры E, то $u(G)$ — подалгебра алгебры F, изоморфная факторалгебрам $G/(G \cap \mathfrak{a})$ и $(G+\mathfrak{a})/\mathfrak{a}$.

Если алгебра E допускает *базис* (a_λ), то ее представление f в алгебру F полностью определяется элементами $f(a_\lambda)$ (§ 2, следствие 2 предложения 3); обратно, задание этих элементов определяет линейное отображение f A-модуля E в A-модуль F; для того чтобы f было *представлением* алгебры E в алгебру F, необходимо и достаточно, чтобы, согласно формулам (6) и (7), $f(a_\lambda) f(a_\mu) = \sum_\nu \gamma_{\lambda\mu\nu} f(a_\nu)$ для любой пары индексов (λ, μ).

В случае, когда E обладает *единичным элементом* e, причем этот элемент *свободный* (что всегда имеет место для алгебр над *полем*), отображение $\alpha \to \alpha e$ есть *изоморфизм* φ кольца A (рассматриваемого как алгебра относительно самого себя) в алгебру E; поскольку $\alpha x = (\alpha e)x = x(\alpha e)$, $\varphi(A)$ есть подкольцо центра алгебры E, и структура алгебры относительно A по сути ничем не отличается от структуры алгебры относительно $\varphi(A)$. Поэтому A и $\varphi(A)$ обычно *отождествляют*, рассматривая тем самым A как *подалгебру* алгебры E, содержащуюся в центре этой алгебры и имеющую тот же единичный элемент, что и E. Заметим, что в этом случае каждый идеал *кольца* (*без операторов*) E есть также идеал *алгебры* E (напротив, *подкольцо* кольца без операторов E не обязательно является *подалгеброй* алгебры E).

Вообще, в случае, когда E обладает единицей e, ее аннулятор $\mathfrak{a}$ (§ 1, n° 9) есть также аннулятор E; образ A при представлении $\alpha \to \alpha e$ есть подалгебра алгебры E, изоморфная $A/\mathfrak{a}$. Структура точного модуля (относительно $A/\mathfrak{a}$), *ассоциированного* (§ 1, n° 9) со структурой A-модуля в E, вместе с умножением определяет в E структуру *алгебры* относительно кольца $A/\mathfrak{a}$, в которой e является свободным элементом;

мы будем и эту структуру алгебры называть *ассоциированной* с заданной в E структурой алгебры относительно A.

Замечание. Как уже указывалось (гл. I, § 8), при рассмотрении в множестве E нескольких структур кольца с операторами (и, в частности, нескольких структур алгебры), в основе которых лежит одна и та же структура кольца (без операторов), следует тщательно различать понятия подалгебры, идеала, представления и т. д. относительно этих различных структур. В частности, рассмотрим в кольце E структуры алгебры относительно двух различных подколец A, B его центра, и пусть a — элемент из A, не принадлежащий B; если f — представление E, рассматриваемого как алгебра над A, то $f(ax) = af(x) = f(a)f(x)$ для всех $x \in E$; напротив, если g — представление E, рассматриваемого как алгебра над B, то $g(ax) = g(a)g(x)$, но, вообще говоря, $g(ax) \neq ag(x)$.

5. Произведения и прямые суммы алгебр

Пусть (E_ι) — семейство алгебр над одним и тем же кольцом A; очевидно, кольцо с операторами $E = \prod_\iota E_\iota$ (гл. I, § 8, n° 10) тоже есть алгебра над A; она называется *произведением алгебр* E_ι. Каждое свойство произведений колец с операторами относится, в частности, к произведениям алгебр.

В случае, когда семейство (E_ι) *конечно*, *компоненты* E'_ι модуля E, отождествляемые соответственно с E_ι (§ 1, n° 4), являются *подалгебрами* алгебры E и E есть *прямая композиция* (гл. I, § 8, n° 11) этих подалгебр. Но если, обратно, F есть алгебра над A и (F_ι) — конечное семейство ее *подалгебр* таких, что *A-модуль* F есть прямая сумма (§ 1, n° 7) *подмодулей* F_ι (что, допуская вольность речи, выражают, говоря, что *алгебра* F есть *прямая сумма подалгебр* F_ι), то, вообще говоря, отсюда еще никоим образом не следует, что F есть прямая композиция подалгебр F_ι (или, что то же, изоморфно произведению $\prod_\iota F_\iota$); как известно (гл. I, § 8, предложение 7), для того чтобы F было прямой композицией F_ι, необходимо и достаточно, чтобы $F_\lambda F_\mu = \{0\}$ для всех пар различных индексов (λ, μ). Если это условие не выполнено, то мультипликативный закон на F *не определяется однозначно* знанием мультипликативных законов на каждой из подалгебр F_ι; для его определения следует еще знать, как перемножаются элементы, принадлежащие двум различным F_ι.

6. Примеры алгебр: I. Кольца эндоморфизмов

Пусть E — унитарный правый модуль над кольцом A; как мы видели (§ 2, n° 5), множество $\mathscr{L}(E)$ всех эндоморфизмов модуля E наделено структурой кольца с операторами, имеющей своей областью операторов *центр* C кольца A; поскольку сложение и внешний закон этой структуры определяют в $\mathscr{L}(E)$ структуру унитарного C-модуля, мы видим, что $\mathscr{L}(E)$ есть *алгебра* относительно C, имеющая своим единичным элементом тождественное отображение E на себя.

Наиболее важен тот случай, когда E обладает *конечным базисом* из n элементов относительно A; тогда $\mathscr{L}(E)$ изоморфно *кольцу* $\mathbf{M}_n(A)$ *квадратных матриц n-го порядка над* A (§ 6, n° 5). Если A *коммутативно*, то $\mathbf{M}_n(A)$ есть алгебра *относительно* A; *канонический базис* (E_{ij}) этой алгебры (§ 6, n° 2) имеет таблицу умножения

$$\left.\begin{aligned} &E_{ij}E_{hk} = 0, \quad \text{если} \quad j \neq h, \\ &E_{ij}E_{jk} = E_{ik}, \ \text{каковы бы ни были } i,\ j,\ k. \end{aligned}\right\} \tag{10}$$

Единичный элемент 1_n алгебры $\mathbf{M}_n(A)$ равен $\sum_{i=1}^{n} E_{ii}$; кольцо A отождествимо с подкольцом матриц $\alpha 1_n$ $(\alpha \in A)$.

7. Примеры алгебр: II. Квадратичные расширения кольца

Пусть A — коммутативное кольцо с единицей. Его *квадратичным расширением* называется алгебра E относительно A, имеющая базис, состоящий из *двух* элементов, один из которых служит ее *единицей*; таким образом, при отождествлении единицы алгебры E с единицей кольца A, которую мы будем обозначать 1, A отождествляется с подкольцом кольца E. Если u — второй элемент рассматриваемого базиса, то каждый элемент из E однозначным образом записывается в виде $a + bu$, где $a \in A$ и $b \in A$. Поскольку, по предположению, $1 \cdot u = u \cdot 1 = u$, E *коммутативно*, и таблица умножения базиса $(1, u)$ полностью определяется заданием u^2, т. е. определяющего его соотношения

$$u^2 = \alpha u + \beta \quad (\alpha \in A,\ \beta \in A); \tag{11}$$

условия ассоциативности выполнены, каковы бы ни были α и β, так что последние могут быть выбраны произвольно.

Исследуем строение алгебры E, когда A есть *поле характеристики* $\neq 2$ (гл. I, § 8, n° 8). Замечая, что

$$(a+bu)^2=(\alpha b+2a)(a+bu)+\beta b^2-\alpha ab-a^2,$$

и полагая в этой формуле $b=1$, $a=-\frac{\alpha}{2}$, видим, что можно принять за новый базис в E множество, образованное элементами 1 и $v=u-\frac{\alpha}{2}$, где $v^2=\gamma\in A$. Возможны три случая:

1° γ *не является в* A *квадратом.* Тогда E есть *поле*; действительно, если $a+bv\neq 0$, то, в силу предположения, $(a+bv)\times(a-bv)=a^2-\gamma b^2\neq 0$, и значит, $\frac{a}{a^2-\gamma b^2}-\frac{b}{a^2-\gamma b^2}v$ есть элемент, обратный $a+bv$.

°Если A — поле вещественных чисел, то -1 не является в A квадратом; элементами квадратичного расширения E, соответствующего $\gamma=-1$, будут тогда *комплексные числа* (см. гл. V и Общ. топ., гл. VIII).°

2° γ *есть квадрат* $\mu^2\neq 0$. Рассмотрим тогда в E новый базис, образованный элементами $e_1=\frac{1}{2}\left(1+\frac{1}{\mu}v\right)$, $e_2=\frac{1}{2}\left(1-\frac{1}{\mu}v\right)$; имеем $e_1^2=e_1$, $e_2^2=e_2$, $e_1e_2=e_2e_1=0$; таким образом, E есть *прямая композиция двух полей* Ae_1, Ae_2, изоморфных A.

3° $\gamma=0$. Множество $\mathfrak{a}=Av$ есть тогда идеал в E такой, что $\mathfrak{a}\mathfrak{a}=\{0\}$, и факторалгебра $E/\mathfrak{a}$ изоморфна полю A.

°Если A — поле $\mathbf{R}$ вещественных чисел, элементы алгебры E над $\mathbf{R}$, имеющей базис $(1, v)$, в котором $v^2=0$, называют *дуальными числами*.°

Элемент $\bar{x}=a-bv$ называется *сопряженным* к элементу $x=a+bv$ алгебры E; непосредственная проверка показывает, что отображение $x\to\bar{x}$ есть *инволютивный* (т. е. совпадающий со своим обратным) *автоморфизм* алгебры E. Имеем $x+\bar{x}=2a\in A$ и $x\bar{x}=a^2-b^2\in A$; произведение $x\bar{x}$ называется *нормой* x и обозначается $N(x)$. Имеем

$$N(xy)=N(x)N(y), \tag{12}$$

ибо $N(xy)=xy\cdot\overline{xy}=x\bar{x}y\bar{y}$.

8. *Примеры алгебр: III. Кватернионы*

Пусть A — коммутативное кольцо с единицей и E — алгебра над A, имеющая базис, образованный четырьмя элементами, первым из которых служит *единица* алгебры E, отождествляемая с единицей 1 кольца A, а остальные три элемента u, v, w перемножаются согласно таблице

$$\left.\begin{aligned} &u^2=\alpha, \quad v^2=\beta, \quad w^2=-\alpha\beta,\\ &uv=-vu=w,\\ &vw=-wv=-\beta u,\\ &wu=-uw=-\alpha v, \end{aligned}\right\} \tag{13}$$

где α и β — элементы из A, для которых $\alpha\beta \neq 0$. Без труда проверяется, что эта таблица умножения удовлетворяет условиям ассоциативности. Определенная так алгебра E, *некоммутативная*, если характеристика A не равна 2, называется *алгеброй кватернионов* над A, соответствующей паре (α, β) элементов из A, а ее базис $(1, u, v, w)$ — *каноническим базисом* этой алгебры.

Таблица умножения базиса, образованного элементами $1, u' = \lambda u, v' = \mu v, w' = \lambda\mu w$, где λ и μ — обратимые элементы из A, получается из (13) заменой α на $\lambda^2\alpha$ и β на $\mu^2\beta$. Тем самым алгебры кватернионов над A, соответствующие парам (α, β) и $(\lambda^2\alpha, \mu^2\beta)$, *изоморфны*. Если α обратимо, то элементы $1, u' = u, v' = w, w' = \alpha v$ также образуют базис алгебры E; таблица умножения этого нового базиса оказывается совпадающей с таблицей умножения алгебры кватернионов, соответствующей паре $(\alpha, -\alpha\beta)$, так что эта алгебра изоморфна алгебре, соответствующей паре (α, β); наконец, ясно, что алгебры кватернионов, соответствующие парам (α, β) и (β, α), изоморфны.

Для каждого кватерниона $x = a + bu + cv + dw$ будем обозначать через $\bar{x}$ кватернион $a - bu - cv - dw$; он называется кватернионом, *сопряженным* к x; $x \to \bar{x}$ есть взаимно однозначное линейное отображение E на себя; при этом $\overline{uv} = \bar{w} = -w = v\bar{u}$, и так же проверяется, что $\overline{vw} = \bar{w}\bar{v}$, $\overline{wu} = \bar{u}\bar{w}$; таким образом, $x \to \bar{x}$ есть изоморфизм алгебры E на *противоположную* алгебру E^0 (и также изоморфизм E^0 на E); его называют *антиавтоморфизмом* алгебры E;

он совпадает с обратным к нему отображением. Далее, $x+\bar{x}=2a\in A$ и $x\bar{x}=\bar{x}x=a^2-\alpha b^2-\beta c^2+\alpha\beta d^2\in A$; произведение $x\bar{x}$ называют также *нормой* кватерниона x и обозначают $N(x)$. Имеем

$$N(xy)=N(x)N(y), \tag{14}$$

ибо $N(xy)=xy\overline{xy}=xy(\bar{y}\bar{x})=x(y\bar{y})\bar{x}=(y\bar{y})(x\bar{x})$, поскольку $y\bar{y}\in A$

Рассмотрим, в частности, тот случай, когда A есть *поле* (характеристики $\neq 2$), и исследуем, при каком условии алгебра кватернионов E над A (относительно элементов α, β) сама есть (*некоммутативное*) *тело*. Для этого необходимо, чтобы $x\neq 0$ влекло $N(x)\neq 0$, ибо, в силу (14), $N(x)N(x^{-1})=N(1)=1$. Но это условие также достаточно, ибо если оно удовлетворяется, то соотношения $x\bar{x}=\bar{x}x=N(x)\neq 0$ для каждого $x\neq 0$ из E показывают, что x обладает в E *обратным* $x^{-1}=\dfrac{\bar{x}}{N(x)}$.

В случае, когда A — поле $\mathbf{Q}$ рациональных чисел, условие удовлетворяется, если взять $\alpha<0$ и $\beta<0$. °То же верно и в том случае, когда A — поле $\mathbf{R}$ вещественных чисел; причем в этом случае все некоммутативные тела, полученные таким способом, изоморфны телу, соответствующему паре (α, β) с $\alpha=\beta=-1$; говоря о *теле кватернионов над* $\mathbf{R}$, всегда имеют в виду именно это последнее тело; его канонический базис обозначают $(1, i, j, k)$, и то же обозначение принимается обычно для канонического базиса алгебры кватернионов над любым полем, соответствующей паре $(-1, -1)$.°

Ясно, что когда один из элементов α, β, $-\alpha\beta$ является в поле A *квадратом*, то $N(x)$ может быть $=0$ и при $x\neq 0$. °В частности, мы видим, что алгебры кватернионов над полем $\mathbf{C}$ комплексных чисел (которые все изоморфны) не являются телами (см. упражнение 4).°

Заметим, что, каково бы ни было $x\in E$, $x^2=\lambda x+\mu$, где $\lambda=x+\bar{x}$ и $\mu=-x\bar{x}=-N(x)$ принадлежат A. Таким образом, если $x\notin A$, то подалгебра A_x алгебры E, порожденная элементами 1 и x, есть *квадратичное расширение* кольца A с базисом, образованным этими двумя элементами; очевидно, E есть (левый и правый) модуль относительно коммутативного кольца A_x, но не является алгеброй над этим кольцом (если A и A_x — поля, то E — векторное пространство размерности 2 над A_x).

9. *Примеры алгебр: IV. Моноидная алгебра. Групповая алгебра*

Пусть A — *коммутативное* кольцо с единицей, S — *моноид* (гл. I, § 1, n° 3), для которого мы примем мультипликативное обозначение, и $E = A^{(S)}$ — *модуль формальных линейных комбинаций* (с коэффициентами из A) *элементов моноида* S (§ 1, n° 8); как мы знаем, канонический базис этого модуля отождествляется с множеством S, так что каждый элемент из E записывается (однозначным образом) в виде $\sum_{s\in S} \alpha_s s$, где все $\alpha_s \in A$. В E можно определить теперь структуру *алгебры* относительно A, приняв за произведение элементов s, t канонического базиса S их произведение st в моноиде S; ясно, что условия ассоциативности (8) при таком определении удовлетворяются. Так определенная алгебра E называется *моноидной алгеброй моноида* S относительно кольца A. Таким образом, для любых элементов $x = \sum_s \alpha_s s$, $y = \sum_s \beta_s s$ этой алгебры имеем $xy = \sum_{s\in S} \left(\sum_{tu=s} \alpha_t \beta_u\right) s$.

Замечания. 1) В случае, когда S — *аддитивно* записываемый коммутативный моноид, его уже нельзя отождествлять с каноническим базисом модуля $A^{(S)}$, так как это могло бы повлечь смешение аддитивных законов, заданных в S и $A^{(S)}$; элемент канонического базиса модуля $A^{(S)}$, соответствующий элементу s моноида S, в этом случае можно, скажем, обозначать e_s; таблицей умножения этого базиса будет тогда $e_s e_t = e_{s+t}$.

2) Пусть S — мультипликативный моноид и (e_s) — канонический базис модуля $A^{(S)}$. Определение моноидной алгебры моноида S относительно A можно обобщить, приняв за таблицу умножения базиса (e_s) соотношения

$$e_s e_t = \alpha_{s,t} e_{st} \quad (\alpha_{s,t} \in A)$$

с условиями ассоциативности

$$\alpha_{s,t}\alpha_{st,u} = \alpha_{s,tu}\alpha_{t,u}$$

для произвольных s, t, u из S. Семейство $(\alpha_{s,t})$ называется *системой факторов* определенной так алгебры. Если γ_s для каждого s — обратимый элемент кольца A, то элементы $e'_s = \gamma_s e_s$ образуют базис модуля $A^{(S)}$, с таблицей умножения

$$e'_s e'_t = \frac{\gamma_s \gamma_t}{\gamma_{st}} \alpha_{s,t} e'_{st}.$$

Иными словами, алгебры, соответствующие системам факторов $(\alpha_{s,t})$ и $\left(\frac{\gamma_s\gamma_t}{\gamma_{st}}\alpha_{s,t}\right)$, *изоморфны* (см. упражнение 12).

Если S коммутативно, то это же верно и для алгебры $A^{(S)}$; если S обладает нейтральным элементом e, то e есть также единица алгебры $A^{(S)}$.

Если T — *устойчивое* множество элементов моноида S (гл. 1, § 4, n° 2), то множество всех элементов вида $\sum_{s\in T}\alpha_s s$ есть *подалгебра* алгебры $A^{(S)}$, изоморфная моноидной алгебре $A^{(T)}$ моноида T относительно A, и отождествляется с этой последней.

Пусть B — подкольцо кольца A, имеющее тот же единичный элемент, что и A; множество всех элементов $\sum_{s\in S}\alpha_s s$ алгебры $A^{(S)}$, в которых $\alpha_s\in B$ для каждого $s\in S$, есть *подкольцо* кольца (без операторов) $A^{(S)}$, но не подалгебра относительно кольца A; его структура алгебры относительно кольца B отождествима со структурой моноидной алгебры $B^{(S)}$ моноида S относительно кольца B.

Каждое *представление* f моноида S в алгебру E относительно A (рассматриваемую как моноид относительно одного умножения) можно, и притом единственным образом, продолжить до представления $\overline{f}$ *алгебры* $A^{(S)}$ в E, положив $\overline{f}\left(\sum_{s\in S}\alpha_s s\right)=\sum_{s\in S}\alpha_s f(s)$.

Пусть теперь φ — представление кольца A в коммутативное кольцо B с единицей; будем считать моноидные алгебры $A^{(S)}$ и $B^{(S)}$ одного и того же моноида S наделенными лишь их структурой кольца (*без операторов*), лежащей в основе их структуры алгебры. Положив тогда $f\left(\sum_{s\in S}\alpha_s s\right)=\sum_{s\in S}\varphi(\alpha_s)s$, мы получим представление f кольца $A^{(S)}$ в кольцо $B^{(S)}$. Если S обладает единицей, так что A (соответственно B) может быть отождествлено с подкольцом кольца $A^{(S)}$ (соответственно $B^{(S)}$), то представление f есть *продолжение* представления φ.

Наиболее важными моноидными алгебрами являются *групповые* алгебры относительно *полей*.

Применение: модули и группы с операторами. Понятие моноидной алгебры позволяет свести изучение любых коммутативных групп с операторами к изучению модулей.

Говоря точнее, с каждой структурой коммутативной группы с операторами в множестве E можно ассоциировать структуру модуля, имеющую тот же закон аддитивной группы и такую, что:

1° каждая устойчивая подгруппа в E (относительно заданных внешних законов) будет подмодулем в E (относительно ассоциированной структуры модуля), и обратно;

2° каждое представление группы с операторами E в *гомологичную* группу F (гл. I, § 4, n° 1) будет представлением модуля, ассоциированного с E, в модуль, ассоциированный с F, и обратно.

При доказательстве будем для всех заданных на E внешних законов пользоваться мультипликативным обозначением. Пусть Ω — *сумма* (Теор. мн., Рез., § 4, n° 5) областей операторов всех этих внешних законов, и отождествим каждую из этих областей с соответствующим ей подмножеством в Ω. Пусть $L(\Omega)$ — *свободный моноид* (гл. I, § 1, n° 3), порождаемый множеством Ω; мы определим внешний закон композиции $(\alpha, x) \to \alpha x$ на E, имеющий $L(\Omega)$ своей областью операторов, индукцией по длине *слова* α в $L(\Omega)$; если α — длины 1, то оно принадлежит одной (и только одной) из областей операторов заданных на E внешних законов, и αx определено. Если теперь λx определено для всех слов λ длины n — 1 и α — слово длины n, то имеем $\alpha = \beta\gamma$, где γ — длины n — 1, а β — длины 1, и мы полагаем тогда $\alpha x = \beta(\gamma x)$. Индукция по длине слова α показывает, что, каковы бы ни были слова α и β из $L(\Omega)$, $\alpha(\beta x) = (\alpha\beta)x$ для каждого $x \in E$. Пусть теперь A — моноидная алгебра моноида $L(\Omega)$ относительно кольца $\mathbf{Z}$ рациональных целых чисел; определим внешний закон композиции $(\alpha, x) \to \alpha x$ на E, имеющий A своей областью операторов, положив $\alpha x = \sum_{\lambda \in L(\Omega)} n_\lambda (\lambda x)$ для каждого $\alpha = \sum_{\lambda \in L(\Omega)} n_\lambda \lambda$ ($n_\lambda \in \mathbf{Z}$). Без труда проверяется, что этот внешний закон удовлетворяет аксиомам ($\mathrm{M_I}$), ($\mathrm{M_{II}}$) и ($\mathrm{M_{III}}$), тем самым определяя в E структуру унитарного левого A-модуля, и что эта структура удовлетворяет поставленным выше условиям 1° и 2°.

Описанный метод применим к любым коммутативным группам с операторами; но, рассматривая коммутативные группы с операторами, удовлетворяющие некоторым дополнительным аксиомам, часто можно удовлетворить условиям 1° и 2° (в предположении, что фигурирующие в условии 2° коммутативные группы E и F *обе* удовлетворяют рассматриваемым аксиомам), ассоциируя другим способом структуру модуля со структурой группы с операторами в E.

Часто встречающийся важный частный случай — это случай коммутативных групп с операторами, имеющих лишь один внешний закон, причем областью операторов его служит мультипликативный

моноид S (чаще всего являющийся *группой*), так что тождественно $\alpha(\beta x)=(\alpha\beta)x$ (где $\alpha\beta$ — произведение α и β в S). Если в этом случае B — моноидная алгебра моноида S относительно $\mathbf{Z}$, то мы получим структуру B-модуля в E, обладающую требуемыми свойствами, для каждого $\alpha = \sum_{\lambda \in S} n_\lambda \lambda$ $(n_\lambda \in \mathbf{Z})$ положив $\alpha x = \sum_{\lambda \in S} n_\lambda (\lambda x)$ (заметим, впрочем, что то, что мы делали выше для общего случая, состояло прежде всего в сведении к рассматриваемому частному случаю путем определения на E внешнего закона с областью операторов $L(\Omega)$).

10. *Примеры алгебр: V. Расширенная моноидная алгебра*

Моноидную алгебру моноида S относительно кольца A (коммутативного и имеющего единицу) можно также рассматривать как подмодуль произведения A^S, образованный теми семействами $(\alpha_s)_{s\in S}$, в которых $\alpha_s = 0$ для всех кроме конечного числа индексов, с произведением, определенным соотношением $(\alpha_s)(\beta_s) = (\gamma_s)$, где для каждого $s \in S$

$$\gamma_s = \sum_{tu=s} \alpha_t \beta_u \tag{15}$$

(сумма распространяется на все пары (t, u), для которых $tu=s$). Сумма в правой части формулы (15) имеет смысл, поскольку лишь конечное число α_s и β_s, а значит и произведений $\alpha_t\beta_u$, отлично от нуля. Но правая часть формулы (15) имеет смысл и для *любых* семейств (α_s) и (β_s), если моноид S удовлетворяет следующему условию:

(D) *Для каждого* $s \in S$ *существует лишь конечное число пар* (t, u) *элементов из* S *таких, что* $tu = s$.

Итак, предположим, что S удовлетворяет условию (D); определим на *произведении* A^S внутренний закон композиции $((\alpha_s), (\beta_s)) \to (\gamma_s)$, где γ_s задается для каждого $s \in S$ формулой (15). Ясно, что определенное так на A^S умножение *двояко дистрибутивно* относительно сложения и удовлетворяет тождествам (5); наконец, вследствие тождеств

$$\sum_{uvw=t} \alpha_u\beta_v\gamma_w = \sum_{vw=t} \Big(\Big(\sum_{uv=v} \alpha_u\beta_v\Big)\gamma_w\Big) = \sum_{us=t} \Big(\alpha_u\Big(\sum_{vw=s} \beta_v\gamma_w\Big)\Big)$$

оно *ассоциативно*.

Таким образом, это умножение и два закона композиции имеющейся в A^S структуры A-модуля определяют в A^S структуру *алгебры* относительно кольца A; множество A^S, наделенное этой структурой, мы называем *расширенной моноидной алгеброй моноида* S относительно кольца A.

Очевидно, *моноидная алгебра* $A^{(S)}$ моноида S относительно A (называемая также, при желании избежать всякой опасности путаницы, *узкой моноидной алгеброй* моноида S) есть *подалгебра* расширенной моноидной алгебры этого моноида (совпадающая с этой последней, когда S *конечно*). *Допуская вольность речи*, мы также всякий элемент $(\alpha_s)_{s\in S}$ расширенной моноидной алгебры моноида S относительно A обозначаем тем же символом $\sum_{s\in S} \alpha_s s$, что и элементы его узкой моноидной алгебры; разумеется, фигурирующий здесь знак суммы не выражает никакой алгебраической операции, поскольку им охватывается *бесконечное* множество членов $\neq 0$. При этом обозначении умножение в расширенной моноидной алгебре моноида S по-прежнему записывается в виде

$$\Big(\sum_{s\in S} \alpha_s s\Big)\Big(\sum_{s\in S} \beta_s s\Big) = \sum_{s\in S}\Big(\Big(\sum_{tu=s} \alpha_t \beta_u\Big) s\Big).$$

Все сформулированные в n° 9 свойства узких моноидных алгебр без изменений распространяются на расширенные моноидные алгебры, за исключением продолжения представления моноида S в алгебру E на его узкую моноидную алгебру, ибо такое продолжение на расширенную моноидную алгебру, вообще говоря, невозможно.

Из моноидов, удовлетворяющих условию (D), укажем, в частности, множество $\mathbf{N}$ натуральных чисел, наделенное структурой, определяемой *сложением*, и множество $\mathbf{N}^*$ целых чисел >0, наделенное структурой, определяемой *умножением*. В главе IV мы детально изучим узкую моноидную алгебру (кольцо полиномов от одной неизвестной) и расширенную моноидную алгебру (кольцо формальных рядов от одной неизвестной) аддитивного моноида $\mathbf{N}$ (относительно любого кольца); расширенная моноидная алгебра мультипликативного модуля $\mathbf{N}^*$ (кольцо формальных рядов Дирихле) играет важную роль в теории чисел.

Упражнения. 1) а) Пусть E — алгебра *конечного* ранга над полем K; показать, что если $a \in E$ не является ни левым, ни пра-

вым делителем нуля, то E обладает единичным элементом и a обратимо. [См. гл. I, § 2, предложение 4.]

б) Вывести отсюда, что если в E не существует делителей нуля, то E — *тело*.

2) Пусть K — поле характеристики 2 и E — его квадратичное расширение, имеющее базис, образованный элементами 1 и u, где $u^2=\alpha u+\beta$ ($\alpha \in K$, $\beta \in K$). Показать, что если уравнение $x^2-\alpha x-\beta=0$ не имеет в K корня, то E — тело; если это уравнение имеет два различных корня, то E есть прямая композиция двух полей, изоморфных K; наконец, если оно имеет только один корень (что возможно, лишь когда $\alpha=0$), то E изоморфно алгебре, обладающей базисом 1, v, где $v^2=0$.

Линейное отображение, оставляющее 1 инвариантной и заменяющее u на $u+\alpha$, есть автоморфизм алгебры E.

3) Если A — коммутативное кольцо с единицей и характеристикой $\neq 2$, то центр алгебры кватернионов над A, соответствующей паре элементов (α, β), не являющихся делителями нуля, совпадает с A.

4) Пусть K — поле характеристики $\neq 2$; показать, что алгебра кватернионов над K, соответствующая паре $(1, \beta)$, изоморфна алгебре всех матриц второго порядка над K. [Рассмотреть базис алгебры кватернионов, образованный элементами $\frac{1}{2}(1+u)$, $\frac{1}{2}(1-u)$, $\frac{1}{2\beta}(v+w)$, $\frac{1}{2}(v-w)$.]

*5) Каждая алгебра кватернионов E над полем K характеристики 2 коммутативна, и квадраты всех $x \in E$ принадлежат K. Поэтому подалгебра K_x алгебры E, порожденная элементом $x \notin K$, является квадратичным расширением K, а E — квадратичным расширением K_x.

Показать, что множество C тех элементов из E, квадрат которых равен квадрату какого-нибудь элемента из K, есть векторное подпространство в E размерности 1, 2 или 4. Если C одномерно (в этом случае $C=K$), то E — тело. Если C двумерно, то в E существует квадратичное расширение K_x поля K, являющееся телом, и E имеет базис относительно K_x, образованный элементами 1 и u, где $u^2=0$; множество $\mathfrak{a}$ тех $y \in E$, для которых $y^2=0$, есть идеал размерности 2, и $E/\mathfrak{a}$ изоморфно K_x. Наконец, если C имеет размерность 4 (и значит, совпадает с E), то множество $\mathfrak{a}$ тех $y \in E$, для которых $y^2=0$, есть идеал размерности 3 и $E/\mathfrak{a}$ изоморфно K; в E существует базис $(1, e_1, e_2, e_3)$ такой, что $e_1^2=e_2^2=e_3^2=0$, $e_1e_2=e_3$, $e_1e_3=e_2e_3=0$; $Ke_3=\mathfrak{b}$ есть единственный одномерный идеал в E; он является аннулятором идеала $\mathfrak{a}$, и $\mathfrak{a}/\mathfrak{b}$ есть прямая сумма двух взаимно аннулирующихся в $E/\mathfrak{b}$ одномерных идеалов.

*6) Пусть K — поле характеристики $\neq 2$ и E — алгебра ранга 4 над K, обладающая базисом $(1, u, v, w)$, где 1 — единичный элемент,

а попарные произведения элементов u, v, w задаются формулами (13), в которых α заменено нулем.

а) Если β не является в K квадратом, то в E не существует одномерного левого (соответственно правого) идеала; множество $\mathfrak{a}$ тех $x \in E$, для которых $x^2=0$, есть двусторонний идеал размерности 2, и $E/\mathfrak{a}$ есть тело, изоморфное некоторому квадратичному расширению поля K.

б) Если β является в K квадратом $\neq 0$, то в E существует базис (e_1, e_2, e_3, e_4) со следующей таблицей умножения:

	e_1	e_2	e_3	e_4
e_1	e_1	0	e_3	0
e_2	0	e_2	0	e_4
e_3	0	e_3	0	0
e_4	e_4	0	0	0

Множество $\mathfrak{a}$ тех $x \in E$, для которых $x^2=0$, есть двусторонний идеал размерности 2, являющийся прямой суммой взаимно аннулирующихся двусторонних идеалов Ke_3 и Ke_4; эти последние являются единственными одномерными (левыми или правыми) идеалами в E. Факторалгебра $E/\mathfrak{a}$ есть прямая композиция двух полей, изоморфных K.

в) Если $\beta=0$, то множество $\mathfrak{a}$ тех $x \in E$, для которых $x^2=0$, есть двусторонний идеал размерности 3; $Kw=\mathfrak{b}$ есть единственный одномерный (левый или правый) идеал в E; это — двусторонний идеал, являющийся левым и правым аннулятором идеала $\mathfrak{a}$. $\mathfrak{a}/\mathfrak{b}$ есть прямая сумма двух взаимно аннулирующихся одномерных двусторонних идеалов факторалгебры $E/\mathfrak{b}$; наконец, $E/\mathfrak{a}$ есть поле, изоморфное K.

7) Пусть K — поле характеристики $\neq 2$ и E — алгебра над K, обладающая базисом из четырех элементов 1, i, j, k (где 1 — единичный элемент), с таблицей умножения

$$i^2=j^2=k^2=1, \quad ij=ji=k, \quad jk=kj=i, \quad ki=ik=j.$$

Показать, что E есть прямая композиция четырех полей, изоморфных K. [Рассмотреть базис алгебры E, образованный элементами

$$(1+\varepsilon i)\ (1+\varepsilon' j),$$

где ε в ε' равны $+1$ или -1.]

E есть групповая алгебра (относительно K) произведения двух циклических групп второго порядка. Обобщить на групповую алгебру произведения n циклических групп второго порядка.

*8) *Кватернионная группа* $\mathfrak{Q}$ (гл. I, § 6, упражнение 20) изоморфна группе из восьми кватернионов ± 1, $\pm i$, $\pm j$, $\pm k$ в алгебре кватернионов (относительно пары $(-1, -1)$) над полем характеристики $\neq 2$. Показать, что групповая алгебра E группы $\mathfrak{Q}$ относительно поля K характеристики $\neq 2$ есть прямая композиция четырех полей, изоморфных K, и алгебры кватернионов (относительно пары $(-1\ -1)$) над K.

[Элементы группы $\mathfrak{Q}$ можно записать в виде e, i, j, k, c, ci, cj, ck, где c — элемент, соответствующий кватерниону -1; рассмотреть базис алгебры E, образованный элементами $\frac{1}{2}(e+c)$, $\frac{1}{2}(e-c)$, $\frac{1}{2}(e+c)i$, $\frac{1}{2}(e-c)i$, $\frac{1}{2}(e+c)j$, $\frac{1}{2}(e-c)j$, $\frac{1}{2}(e+c)k$, $\frac{1}{2}(e-c)k$.] .

*9) Показать, что групповая алгебра E *диэдральной группы* $\mathfrak{D}_8$ восьмого порядка (гл. I, § 6, упражнение 20) относительно поля K характеристики $\neq 2$ есть прямая композиция четырех полей, изоморфных K, и алгебры всех матриц второго порядка над K. [Элементы группы $\mathfrak{D}_8$ имеют вид $a^i b^j$ $(0 \leqslant i \leqslant 3,\ 0 \leqslant j \leqslant 1)$, где a и b — образующие этой группы, рассмотренные в упражнении 20 § 6 главы I; рассмотреть базис алгебры E, образованный элементами $\frac{1}{2}(e+a^2)$, $\frac{1}{2}(e-a^2)$, $\frac{1}{2}(a+a^3)$, $\frac{1}{2}(a-a^3)$ и четырьмя элементами, полученными из них умножением справа на b; использовать упражнение 4.] Вывести отсюда, что если -1 является в K квадратом, то групповые алгебры групп $\mathfrak{Q}$ и $\mathfrak{D}_8$ относительно K *изоморфны*.

Показать также, что групповая алгебра F диэдральной группы $\mathfrak{D}_6$ шестого порядка относительно поля K характеристики $\neq 2$ и $\neq 3$ есть прямая композиция двух полей, изоморфных K, и алгебры всех матриц второго порядка над K. [Рассмотреть здесь базис алгебры F, образованный элементами $e+a+a^2$, $a+a^2-2e$, $a-a^2$ и тремя элементами, полученными путем умножения их справа на b.]

10) Пусть G — группа, H — ее нормальная подгруппа и $\mathfrak{a}$ — двусторонний идеал групповой алгебры $A^{(G)}$, порожденный элементами $ts - s$, где t пробегает H и s пробегает G. Показать, что групповая алгебра $A^{(G/H)}$ изоморфна факторалгебре $A^{(G)}/\mathfrak{a}$.

11) Пусть E — левый модуль над некоммутативным кольцом A; предположим, что на E определено умножение, которое, вместе с законом аддитивной группы и внешним законом заданной в E структуры модуля, определяет в E структуру кольца с операторами, имеющую своей областью операторов A. Показать при этих условиях, что $(\alpha\beta)(xy) = (\beta\alpha)(xy)$, каковы бы ни были $\alpha \in A$, $\beta \in A$, $x \in E$, $y \in E$. Вывести отсюда, что если каждый элемент модуля E есть произведение двух элементов из E (что всегда выполняется, если E обладает единицей), то факторкольцо $A/\mathfrak{a}$, где $\mathfrak{a}$ — аннулятор E, *коммутативно*.

*12) Пусть A — коммутативное кольцо с единицей 1 и S — мультипликативный моноид с единичным элементом e. Предположим, что на A задан внешний закон $(s, x) \longrightarrow x^s$, имеющий S своей областью операторов и такой, что отображение $x \longrightarrow x^s$ при каждом $s \in S$ есть *автоморфизм* кольца A и $(x^s)^t = x^{st}$, каковы бы ни были s и t из S (откуда следует, что e есть нейтральный оператор рассматриваемого

внешнего закона). При этих условиях определим на A-модуле $A^{(S)}$, канонический базис которого мы обозначим (f_s), мультипликативный внутренний закон композиции соотношением

$$\Big(\sum_s x_s f_s\Big)\Big(\sum_y y_s f_s\Big)=\sum_s\Big(\sum_{tu=s} a_{t,u}x_t y_u^t\Big) f_s,$$

где $a_{s,t}$ — коэффициенты, принадлежащие A.

Показать, что этот закон и сложение определяют в $A^{(S)}$ структуру *кольца*, если только коэффициенты $a_{s,t}$ удовлетворяют условиям

$$a_{s,t}a_{st,u}=a_{t,u}^s a_{s,tu},$$

каковы бы ни были s, t, u из S. Если при этом $a_{e,s}=a_{s,e}=1$ для каждого $s\in S$, то f_e есть единичный элемент этой структуры; в этом случае A отождествимо с подкольцом кольца $A^{(S)}$, а $A^{(S)}$ есть алгебра над подкольцом C кольца A, образованным элементами, инвариантными относительно всех автоморфизмов $x\to x^s$; эта алгебра называется *скрещенным произведением* кольца A и моноида S относительно *системы факторов* $(a_{s,t})$. Если эту систему заменить системой факторов $\left(\frac{c_s c_t^s}{c_{st}}a_{s,t}\right)$, где c_s для каждого $s\in S$ есть обратимый элемент из A и $c_e=1$, то полученное так новое скрещенное произведение будет *изоморфно* скрещенному произведению, определяемому системой факторов $(a_{s,t})$.

Приняв, в частности, за A квадратичное расширение кольца B, а за S — циклическую группу второго порядка $\{e, s\}$, так, чтобы $x^s=\bar{x}$ для каждого $x\in A$, показать, что каждое скрещенное произведение A и S есть *алгебра кватернионов* над B (или алгебра с той же таблицей умножения, но в которой по крайней мере один из элементов α, β, $\alpha\beta$ равен нулю).

*13) Пусть S — мультипликативный моноид с единицей e, удовлетворяющий условию (D) n° 10 и такой, что в нем соотношение $st=e$ влечет $s=t=e$.

а) Показать, что для любого элемента $s\in S$ существует число $\nu(s)$, зависящее только от s, такое, что число n членов всякой конечной последовательности $(t_i)_{1\leqslant i\leqslant n}$ элементов, *отличных от* e, для которой $t_1 t_2 \dots t_n=s$, меньше $\nu(s)$.

б) Вывести отсюда, что для того, чтобы элемент $x=\sum_s \alpha_s s$ расширенной моноидной алгебры моноида S над кольцом A был обратимым, необходимо и достаточно, чтобы α_s был обратимым в A. [Свести к тому случаю, когда $\alpha_e=1$, и воспользоваться тождеством $e-z^{n+1}=(e-z)(e+z+z^2+\dots+z^n)$ в расширенной моноидной алгебре моноида S над A.]

ПРИЛОЖЕНИЕ I

К ГЛАВЕ II

ПОЛУЛИНЕЙНЫЕ ОТОБРАЖЕНИЯ

1. *Определение полулинейных отображений*

Пусть A и B — *изоморфные* кольца (коммутативные или нет) и σ — *изоморфизм* A на B; образ элемента $\lambda \in A$ при отображении σ будем обозначать λ^σ. Отображение u A-модуля E в B-модуль F называется *полулинейным* относительно изоморфизма σ, если оно удовлетворяет тождествам

$$u(x+y) = u(x) + u(y),$$

$$u(\lambda x) = \lambda^\sigma u(x).$$

Чаще всего встречаются на практике полулинейные отображения, относящиеся либо к случаю, когда $B = A$ (и, значит, σ — *автоморфизм* кольца A), либо к случаю, когда B есть кольцо A^0, *противоположное* A. Наиболее важны те случаи, где A — *квадратичное расширение* (§ 7, n° 7) поля K (соответственно *алгебра кватернионов* (§ 7, n° 8) над K), а σ — автоморфизм (соответственно антиавтоморфизм) $\xi \to \bar{\xi}$. В этих двух случаях полулинейное отображение называют также *антилинейным*.

Примеры. 1) Если σ — автоморфизм кольца A, то отображение, относящее каждому элементу (ξ_i) модуля A_s^n элемент (ξ_i^σ), есть полулинейное относительно σ отображение A_s^n на себя.

2) Если кольцо A некоммутативно, то, как мы видели, при $\alpha \in A$, не принадлежащем центру кольца A, гомотетия $x \to \alpha x$, вообще говоря, не является линейным отображением A-модуля E в себя (§ 1, n° 1 и § 2, n° 5); но если α обратимо, то эта гомотетия есть *полулинейное отображение* относительно внутреннего автоморфизма $\xi \to \alpha\xi\alpha^{-1}$ кольца A, ибо $\alpha(\lambda x) = (\alpha\lambda\alpha^{-1})(\alpha x)$.

Пусть E, F, G — модули относительно изоморфных колец A, B, C и u — полулинейное отображение E в F относительно изоморфизма σ кольца A

на B, а v — полулинейное отображение F в G относительно изоморфизма τ кольца B на C; тогда композиция $v \circ u$ является полулинейным отображением E в G относительно изоморфизма $\tau \circ \sigma$ кольца A на C.

2. *Линейное отображение, ассоциированное с полулинейным*

Пусть u — полулинейное отображение A-модуля E в B-модуль F относительно изоморфизма σ кольца A на B. Если u есть *взаимно однозначное* отображение E *на* F, то оно образует, вместе с изоморфизмом σ, *биизоморфизм* E на F (гл. I, § 4, n° 1); допуская вольность речи, говорят, что u само есть биизоморфизм E на F относительно σ.

В F можно определить структуру *A-модуля*, оставив прежний закон аддитивной группы и положив $\lambda y = \lambda^{\sigma} y$ для каждого $\lambda \in A$ и каждого $y \in F$ (выполнение аксиом модуля очевидно); обозначим полученный так A-модуль через F_{σ}. *Тождественное* отображение φ множества F на себя есть *биизоморфизм* (относительно σ) A-модуля F_{σ} на B-модуль F; ясно, что образ каждого подмодуля M модуля F_{σ} при отображении φ есть подмодуль в F, и обратно; кроме того, при факторизации φ порождает биизоморфизм фактормодуля F_{σ}/M на фактормодуль F/M.

Пусть теперь u — произвольное полулинейное отображение E в F; оно однозначным образом представляется в виде $u = \varphi \circ v$, где v — *линейное* отображение A-модуля E в A-модуль F_{σ}. v называется линейным отображением, *ассоциированным* с полулинейным отображением u. Благодаря этому разложению каждому свойству линейных отображений отвечает свойство полулинейных отображений (относительно одного и того же изоморфизма σ), полученное путем применения рассматриваемого свойства к ассоциированным с ними линейным отображениям; мы предоставляем читателю сформулировать бóльшую часть получающихся так предложений.

3. *Ранг полулинейного отображения*

Пусть K и K' — изоморфные *тела* и σ — изоморфизм K на K'. *Ранг* полулинейного относительно σ отображения u векторного пространства E над K в векторное пространство F над K' есть, по определению, размерность подпространства $u(E)$ пространства F (если эта размерность конечна; в противном случае говорят, что u — бесконечного ранга). Очевидно, этот ранг равен рангу линейного отображения v, *ассоциированного* с u (n° 2), ибо каждый базис подпространства V пространства F_{σ} относительно K есть также базис $\varphi(V)$ относительно K'.

4. *Сопряженное к полулинейному отображению*

Пусть A и B — изоморфные кольца, E — левый A-модуль, F — левый B-модуль, u — полулинейное отображение E в F относительно изоморфизма σ кольца A на B и σ^{-1} — изоморфизм B на A, обратный к σ. Для каждого $y' \in F^*$

отображение $x \longrightarrow \langle u(x), y' \rangle^{\sigma^{-1}}$ есть линейная форма на E; обозначив ее ${}^t u(y')$, мы определим отображение ${}^t u$ модуля F^* в E^*, называемое по-прежнему отображением, *сопряженным* к u; таким образом, ${}^t u$ определяется тождеством относительно $x \in E$ и $y' \in F^*$

$$\langle u(x), y' \rangle = \langle x, {}^t u(y') \rangle^{\sigma}. \tag{1}$$

Без труда проверяется, что ${}^t u$ есть *полулинейное* отображение F^* в E^* относительно изоморфизма σ^{-1}. Если v — линейное отображение E в F_σ, ассоциированное с u, и φ — тождественное отображение F_σ на F, так что $u = \varphi \circ v$ (n° 2), то, как легко видеть, ${}^t u = {}^t v \circ {}^t \varphi$, и ${}^t \varphi$ есть биизоморфизм F^* на $(F_\sigma)^*$ относительно изоморфизма σ^{-1}; это соотношение позволяет сразу распространить на сопряженные полулинейные отображения все установленные в § 4 свойства сопряженных линейных отображений.

5. Матрица полулинейного отображения

Пусть A и B — изоморфные кольца с единицей и σ — изоморфизм A на B. Для каждой матрицы $X = (\xi_{\lambda\mu})$ над A обозначим через X^σ матрицу $(\xi^\sigma_{\lambda\mu})$ над B; очевидно $(X+Y)^\sigma = X^\sigma + Y^\sigma$, $(XZ)^\sigma = X^\sigma Z^\sigma$, $(\alpha X)^\sigma = \alpha^\sigma X^\sigma$, $(X\alpha)^\sigma = X^\sigma \alpha^\sigma$ (в предположении, что рассматриваемые операции имеют смысл).

Пусть E — унитарный *правый* A-модуль с конечным базисом $(a_\lambda)_{\lambda \in L}$, F — унитарный *правый* B-модуль с конечным базисом $(b_\mu)_{\mu \in M}$ и u — полулинейное отображение E в F относительно изоморфизма σ; коэффициенты $\alpha_{\mu\lambda}$ разложений $u(a_\lambda) = \sum_{\mu \in M} b_\mu \alpha_{\mu\lambda}$ вполне определяются заданием u, и, обратно, их задание определяет элементы $u(a_\lambda)$, а следовательно, и u (§ 2, следствие 2 предложения 3); матрица $(\alpha_{\mu\lambda})_{(\mu,\lambda) \in M \times L}$ с элементами *из* B называется *матрицей отображения* u *относительно базисов* (a_λ) и (b_μ) и по-прежнему обозначается $M(u; (a_\lambda), (b_\mu))$ или просто $M(u)$.

Пусть C — кольцо, изоморфное A и B, τ — изоморфизм B на C, G — унитарный правый C-модуль с конечным базисом $(c_\nu)_{\nu \in N}$ и v — полулинейное отображение F в G относительно изоморфизма τ. Если U — матрица отображения u относительно базисов (a_λ) и (b_μ) и V — матрица отображения v относительно базисов (b_μ) и (c_ν), то матрица отображения $v \circ u$ относительно базисов (a_λ) и (c_ν) равна VU^τ.

В частности (см. § 6, n° 4), если, как обычно, отождествлять элемент $x \in E$ (соответственно $y \in F$) с одностолбцовой матрицей, образованной его компонентами относительно (a_λ) (соответственно (b_μ)), то

$$u(x) = M(u) \cdot x^\sigma. \tag{2}$$

Пусть (a'_λ) и (b'_μ) — базисы в E^* и F^*, *сопряженные* к (a_λ) и (b_μ); если U — матрица отображения u относительно базисов (a_λ) и (b_μ) то матрица отображения ${}^t u$ относительно базисов (b'_μ) и (a'_λ) равна ${}^t(U^{\sigma^{-1}})$.

Наконец, если $(\bar{a}_\lambda)_{\lambda\in L}$, $(\bar{b}_\mu)_{\mu\in M}$ — базисы модулей E и F, P — матрица перехода (§ 6, n° 9) от (a_λ) к $(\bar{a}_\lambda)$ и Q — матрица перехода от (b_μ) к $(\bar{b}_\mu)$, то матрица отображения u относительно базисов $(\bar{a}_\lambda)$ и $(\bar{b}_\mu)$ равна $Q^{-1}UP^\sigma$.

ПРИЛОЖЕНИЕ II

К ГЛАВЕ II

АФФИННЫЕ ПРОСТРАНСТВА

1. *Определение аффинных пространств*

Определение 1. *Аффинным пространством, ассоциированным с заданным левым* (соответственно *правым*) *векторным пространством T над телом K, называется каждое однородное пространство E аддитивной группы T* (гл. I, § 7, n° 6) *такое, что* 0 *является единственным ее оператором, оставляющим инвариантными все элементы из E* (т. е. что *T действует в E точно и транзитивно*). *При этих условиях T называется пространством переносов аффинного пространства E, а элементы из E — переносами пространства E* (или *свободными векторами этого пространства*).

В дальнейшем мы ограничимся случаем левого векторного пространства T над K. Размерность (над K) векторного пространства T переносов аффинного пространства E называется *размерностью* пространства E (над K) и обозначается $\dim E$ или $\dim_K E$. Одномерное (соответственно двумерное) аффинное пространство называется *аффинной прямой* (соответственно *аффинной плоскостью*). Элементы аффинного пространства именуются также *точками*.

В условиях определения 1 мы обозначаем через $t+a$ или $a+t$, где $t \in T$ и $a \in E$, образ точки a при отображении t. Таким образом, каковы бы ни были $s \in T$, $t \in T$ и $a \in E$,

$$s+(t+a)=(s+t)+a, \quad 0+a=a. \tag{1}$$

Кроме того, из определения 1 вытекает, что для каждого $a \in E$ отображение $t \to t+a$ есть *биекция* T на E. Иными словами, для

любых двух точек a, b из E существует, и притом только один, перенос t такой, что $b = t + a$; будем обозначать его $b - a$; каковы бы ни были $a \in E$, $b \in E$, $c \in E$, имеем

$$a - a = 0, \quad a - b = -(b - a), \quad b = (b - a) + a.$$
$$(c - b) + (b - a) = c - a. \tag{2}$$

Если точки a, b, a', b' пространства E таковы, что $b - a = b' - a'$, то, как следует из формулы

$$b' = (b' - b) + (b - a) + a = (b' - a') + (a' - a) + a$$

и коммутативности сложения в T,

$$b' - b = a' - a$$

(«правило параллелограмма»).

Для каждого $a \in E$ отображение $x \longrightarrow x - a$ есть биекция E на T; отождествляя E с T посредством этого отображения, говорят, что E рассматривается как векторное пространство, полученное путем *принятия a за начало* в E. Обратно, каждое векторное пространство T канонически наделено структурой ассоциированного с ним аффинного пространства, а именно структурой однородного пространства, соответствующего подгруппе $\{0\}$ аддитивной группы T (гл. I, § 7, n° 6).

Замечание. Определения этого n° и часть дальнейших результатов непосредственно распространяются на тот случай, когда вместо векторного пространства T рассматривается произвольная *коммутативная группа с операторами T*.

2. Барицентрическое исчисление

Предложение 1. *Пусть $(x_\iota)_{\iota \in I}$ — семейство точек аффинного пространства E над K, $(\lambda_\iota)_{\iota \in I}$ — семейство элементов из K, равных нулю для всех кроме конечного числа индексов и таких, что $\sum_{\iota \in I} \lambda_\iota = 1$ (соответственно $\sum_{\iota \in I} \lambda_\iota = 0$), и a — произвольная точка из E. Точка $x \in E$, определяемая формулой*

$$x - a = \sum_{\iota \in I} \lambda_\iota (x_\iota - a)$$

(соответственно *свободный вектор* $\sum_{\iota \in I} \lambda_\iota (x_\iota - a)$), *не зависит от рассматриваемой точки a.*

Действительно, для любой другой точки $a' \in E$ имеем

$$\sum_\iota \lambda_\iota (x_\iota - a') = \sum_\iota \lambda_\iota ((x_\iota - a) + (a - a')) =$$

$$= \sum_\iota \lambda_\iota (x_\iota - a) + \left(\sum_\iota \lambda_\iota\right)(a - a').$$

Если $\sum_\iota \lambda_\iota = 1$, то получаем $\sum_\iota \lambda_\iota (x_\iota - a') = (x - a) + (a - a') = x - a'$, если же $\sum_\iota \lambda_\iota = 0$, то $\sum_\iota \lambda_\iota (x_\iota - a') = \sum_\iota \lambda_\iota (x_\iota - a)$, и предложение доказано.

В условиях предложения 1 точка x, определяемая формулой $x - a = \sum_{\iota \in I} \lambda_\iota (x_\iota - a)$ (соответственно свободный вектор $\sum_{\iota \in I} \lambda_\iota (x_\iota - a)$), будет обозначаться $\sum_{\iota \in I} \lambda_\iota x_\iota$. В частности, таким образом вновь получается обозначение $b - a$, введенное в n° 1. В случае $\sum_\iota \lambda_\iota = 1$ точка $x = \sum_\iota \lambda_\iota x_\iota$ называется *центром тяжести семейства точек* x_ι, *снабженных массами* λ_ι.

Если $a_1, \ldots, a_m$ — точки из E, число m которых не делится на характеристику тела K (гл. I, § 8, n° 8), то точку $g = \sum_{i=1}^{m} \frac{1}{m} a_i$ называют (допуская вольность речи) *центром тяжести семейства точек* a_i $(1 \leqslant i \leqslant m)$ (при $m = 2$ вместо «центр тяжести» говорят «середина»); он характеризуется соотношением $\sum_{i=1}^{m} (a_i - g) = 0$.

3. *Линейные многообразия*

Определение 2. *Множество V точек аффинного пространства E называют аффинным линейным многообразием* (или просто *линейным многообразием*), *если для каждого семейства $(x_\iota)_{\iota \in I}$ точек из V и каждого семейства $(\lambda_\iota)_{\iota \in I}$ элементов из K, равных нулю для всех кроме конечного числа индексов и таких, что $\sum_{\iota \in I} \lambda_\iota = 1$, центр тяжести $\sum_{\iota \in I} \lambda_\iota x_\iota$ принадлежит V.*

Достаточно потребовать, чтобы условие определения 2 выполнялось для каждого *конечного* семейства точек из V.

Пустое множество есть линейное многообразие; пересечение любого семейства линейных многообразий есть линейное многообразие.

Пусть V — непустое множество в E и a — его точка; соотношение

$$x - a = \sum_{i=1}^{n} \lambda_i (x_i - a)$$

означает, что x есть центр тяжести $\sum_{i=1}^{n} \lambda_i x_i + \left(1 - \sum_{i=1}^{n} \lambda_i\right) a$ семейства, образованного всеми точками x_i и a. Следовательно:

Предложение 2. *Для того чтобы непустое множество V точек аффинного пространства E было линейным многообразием, необходимо и достаточно, чтобы V было векторным подпространством относительно структуры векторного пространства в E, получаемой путем принятия любой точки из V за начало.*

В частности, непустые аффинные линейные многообразия векторного пространства T (рассматриваемого как аффинное пространство) — это не что иное, как множества точек, получаемые путем *переносов* векторных подпространств этого пространства T; значит, векторные подпространства пространства T — это линейные многообразия, содержащие 0; их называют также *однородными* линейными многообразиями.

Пусть V — непустое линейное многообразие аффинного пространства E; множество D всех свободных векторов $x - y$, где x и y пробегают V, есть векторное подпространство пространства T переносов аффинного пространства E; действительно, если $a \in V$, то можно написать

$$x - y = (x - a) - (y - a)$$

и достаточно проверить, что множество всех свободных векторов $x - a$, где x пробегает V, есть векторное подпространство пространства T; но так как $(x - a) + (y - a) = (x + y - a) - a$ и $\lambda(x - a) = (\lambda x + (1 - \lambda) a) - a$, то это вытекает из определения 2. Мы будем

называть D *направляющим подпространством* или *направляющей* линейного многообразия V. Очевидно, D действует в V точно и транзитивно, так что V канонически наделено структурой *аффинного пространства, ассоциированного с* D. Под *размерностью* линейного многообразия V понимают его размерность в этой структуре аффинного пространства, т. е. размерность векторного пространства D. Линейные многообразия размерности 0 — это точки пространства E; линейные многообразия размерности 1 (соответственно 2) называются *прямыми* (соответственно *плоскостями*) аффинного пространства E.

> Каждый ненулевой вектор, принадлежащий направляющему подпространству прямой, называется *направляющим вектором* этой прямой; его компоненты относительно базиса векторного пространства T образуют так называемую систему *направляющих параметров* ассматриваемой прямой.

Факторразмерностью линейного многообразия V в E называется факторразмерность его направляющего подпространства D в T; линейное многообразие, имеющее в E факторразмерность 1, называется (аффинной) *гиперплоскостью* аффинного пространства E.

Два линейных многообразия с одной и той же направляющей называются *параллельными*; то же самое можно выразить, сказав, что параллельные линейные многообразия — это линейные многообразия, получающиеся друг из друга путем переноса. Направляющей линейного многообразия V в T (рассматриваемом как аффинное пространство) служит однородное линейное многообразие, параллельное V.

Предложение 3. *Каково бы ни было семейство* $(a_\iota)_{\iota\in I}$ *точек аффинного пространства* E, *множество* V *всевозможных центров тяжести* $\sum_{\iota\in I}\lambda_\iota a_\iota$ ($\lambda_\iota = 0$ для всех кроме конечного числа индексов и $\sum_{\iota\in I}\lambda_\iota = 1$) *есть линейное многообразие в* E.

Если семейство (a_ι) пустое, то, вследствие условия $\sum_\iota \lambda_\iota = 1$, $V = \varnothing$. Поэтому можно считать семейство (a_ι) непустым, а в этом случае предложение становится очевидным, если принять в E одну из точек a_ι за начало.

Очевидно, V есть наименьшее линейное многообразие, содержащее точки a_ι; оно называется аффинным многообразием, *порожденным* семейством (a_ι).

В обозначениях предложения 3, предполагая семейство (a_ι) непустым, для *единственности* представления каждой точки $x \in V$ в виде $x = \sum_\iota \lambda_\iota a_\iota$ необходимо и достаточно, чтобы семейство векторов $a_\iota - a_\varkappa$ пространства T, где $\varkappa$ — произвольный фиксированный индекс из I, а ι пробегает множество всех индексов $\iota \neq \varkappa$, было свободным. В этом случае семейство $(a_\iota)_{\iota \in I}$ точек из E называют *аффинно свободным* (а его элементы *аффинно независимыми*, или образующими *аффинно свободную систему*); λ_ι называется ι-*й барицентрической координатой* точки x относительно аффинно свободного семейства (a_ι).

Семейство $(a_\iota)_{\iota \in I}$ точек из E, не являющееся аффинно свободным, называется *аффинно зависимым*.

Предложение 4. *Для того чтобы непустое семейство $(a_\iota)_{\iota \in I}$ точек аффинного пространства E было аффинно зависимым, необходимо и достаточно, чтобы существовало семейство $(\lambda_\iota)_{\iota \in I}$ элементов тела K (равных нулю для всех кроме конечного числа индексов) такое, что $\sum_{\iota \in I} \lambda_\iota = 0$ и $\sum_{\iota \in I} \lambda_\iota a_\iota = 0$, но не все $\lambda_\iota = 0$.*

Действительно, утверждение, что семейство векторов $(a_\iota - a_\varkappa)$ из T, где $\varkappa$ — заданный индекс из I, а ι пробегает множество всех индексов $\iota \neq \varkappa$, линейно зависимое, означает, что существует семейство скаляров $(\lambda_\iota)_{\iota \neq \varkappa}$, не равных все нулю, такое, что $\sum_{\iota \neq \varkappa} \lambda_\iota (a_\iota - a_\varkappa) = 0$; но, положив $\lambda_\varkappa = -\sum_{\iota \neq \varkappa} \lambda_\iota$, можно переписать это соотношение в виде $\sum_{\iota \in I} \lambda_\iota a_\iota = 0$, где $\sum_{\iota \in I} \lambda_\iota = 0$.

Предложение 5. *Для того чтобы непустое семейство $(a_\iota)_{\iota \in I}$ точек аффинного пространства E было аффинно свободным, необходимо и достаточно, чтобы $a_\varkappa$ ни при каком индексе $\varkappa \in I$ не принадлежало линейному многообразию, порожденному точками a_ι с индексами $\iota \neq \varkappa$.*

Предложение очевидно, если I состоит только из одного элемента. В противном же случае оно вытекает из предложения 1 § 3, если принять в E за начало одну из точек a_ι с индексом $\iota \neq \varkappa$.

4. *Аффинные отображения*

Определение 3. *Пусть E и E' — аффинные пространства, ассоциированные с векторными пространствами T и T' над одним и тем же телом K. Отображение u пространства E в E' называется аффинным отображением (или аффинным линейным отображением), если, каковы бы ни были семейство $(x_\iota)_{\iota\in I}$ точек из E и семейство $(\lambda_\iota)_{\iota\in I}$ скаляров, для которого $\sum_{\iota\in I}\lambda_\iota = 1$,*

$$u\left(\sum_{\iota\in I}\lambda_\iota x_\iota\right) = \sum_{\iota\in I}\lambda_\iota u(x_\iota). \tag{3}$$

Предложение 6. *Для каждого аффинного отображения u аффинного пространства E в E' существует однозначно определенное линейное отображение v векторного пространства T в T' такое, что*

$$u(x+t) = u(x) + v(t),$$

каковы бы ни были $x\in E$, $t\in T$.

Действительно, пусть a — произвольная точка из E. Отображение

$$t \longrightarrow u(a+t) - u(a)$$

есть линейное отображение T в T', ибо, обозначая его через v_a и принимая во внимание, что

$$a + \lambda t = \lambda(a+t) + (1-\lambda)a,$$

$$a + s + t = (a+s) + (a+t) - a,$$

получаем из (3), что $v_a(\lambda t) = \lambda v_a(t)$ и $v_a(s+t) = v_a(s) + v_a(t)$. При этом, какова бы ни была другая точка $b\in E$, имеем $v_a = v_b$; действительно, из равенства $(a+t) - a + b = b + t$ следует, что

$$u(a+t) - u(a) + u(b) = u(b+t),$$

т. е. $u(a+t) - u(a) = u(b+t) - u(b)$. Этим существование v доказано; единственность очевидна.

v называется линейным отображением T в T', *ассоциированным* с u. Обратно, легко видеть, что для каждого линейного отображения v векторного пространства T в T' и каждой пары точек $a\in E$, $a'\in E'$

$$x \longrightarrow a' + v(x-a)$$

есть аффинное отображение E в E', имеющее v ассоциированным линейным отображением. Таким образом, утверждение, что u есть аффинное отображение E в E', означает также, что если принять в E за начало произвольную точку a, а в E' — точку $u(a)$, то u будет *линейным* отображением первого из получающихся так векторных пространств во второе.

Пусть E'' — третье аффинное пространство, T'' — его пространство переносов, u' — аффинное отображение E' в E'' и v' — линейное отображение T' в T'', ассоциированное с u'. Очевидно, $u' \circ u$ есть аффинное отображение E в E''; при этом, так как для любых $a \in E$ и $t \in T$

$$u'(u(a+t)) = u'(u(a)+v(t)) = u'(u(a))+v'(v(t)),$$

то $v' \circ v$ есть линейное отображение T в T'', ассоциированное с $u' \circ u$. Для того чтобы аффинное отображение u было биективным, необходимо и достаточно, чтобы таким было ассоциированное линейное отображение v; и u^{-1} есть тогда аффинное отображение, имеющее ассоциированным линейным отображением v^{-1}.

В частности, аффинные биекции аффинного пространства E на себя образуют группу G, называемую *аффинной группой* пространства E. Отображение, относящее каждому $u \in G$ линейное отображение v, ассоциированное с u, есть, согласно предыдущему, *гомоморфизм* группы G *на линейную группу* $\mathbf{GL}(T)$. Если u — перенос, то v — тождество, и обратно. Таким образом, ядром указанного гомоморфизма служит группа T переносов пространства E, являющаяся, следовательно, *нормальной подгруппой* группы G.

Если $u \in G$, то автоморфизм $t \to utu^{-1}$ группы T есть не что иное, как линейное отображение v, ассоциированное с u. Действительно, для всех $x \in E$ и $t \in T$ имеем

$$x + utu^{-1} = u(u^{-1}(x)+t) = u(u^{-1}(x))+v(t) = x+v(t),$$

так что $utu^{-1} = v(t)$.

Пусть $a \in E$ и G_a — подгруппа группы G, образованная теми $u \in G$, для которых $u(a)=a$. Если отождествить E с T, приняв a за начало, то G_a совпадает с $\mathbf{GL}(T)$. Каждое $u \in G$ однозначно представляется в виде $u = t_1 u_1$ (соответственно в виде $u = u_2 t_2$), где u_1, u_2 принадлежат G_a, а t_1, t_2 принадлежат T; действительно, положив $t_1 = u(a) - a$, будем иметь $u^{-1}t_1 \in G_a$, чем доказано существо-

вание u_1 и t_1; аналогичным способом получим существование u_2 и t_2. Единственность же вытекает из того, что $G_a \cap T$ сводится к нейтральному элементу группы G. Так как при этом

$$t_1 u_1 = u_1 (u_1^{-1} t_1 u_1),$$

то $u_2 = u_1$, а $t_2 = u_1^{-1} t_1 u_1$. Наконец, так как линейные отображения, ассоциированные с u и u_1, совпадают, то, если отождествить, как выше, G_a с $\mathbf{GL}(T)$, u_1 будет линейным отображением T в себя, ассоциированным с u.

Пусть E и E' — аффинные пространства над K. Образ (соответственно прообраз) линейного многообразия из E (соответственно E') относительно аффинного отображения u пространства E в E' есть линейное многообразие в E' (соответственно E); *ранг* u есть, по определению, размерность $u(E)$ (если она определена): он равен рангу линейного отображения, ассоциированного с u. Для любых двух линейных многообразий V и V' одинаковой (конечной) размерности m, принадлежащих соответственно E и E', существует аффинное отображение u пространства E в E' такое, что $u(V) = V'$: это непосредственно вытекает из следствия 2 предложения 3 § 2, если принять за начало в E и E' соответственно точки из V и V' и, далее, взять в E (соответственно E') базис, первые m векторов которого образуют базис в V (соответственно V').

Так как тело K канонически наделено структурой (одномерного) левого векторного пространства над K, то его можно рассматривать как одномерное аффинное пространство. Аффинное отображение аффинного пространства E (над K) в аффинное пространство K называется также *аффинной функцией* (или *аффинной линейной функцией*). Таким образом, если принять в E за начало какую-нибудь точку a, то каждая аффинная функция на E допускает однозначно определенное представление в виде $x \to \alpha + v(x)$, где $\alpha \in K$, а v — линейная форма на полученном так векторном пространстве E; тем самым аффинные функции на E образуют *правое векторное пространство над* K, имеющее размерность, равную $1 + \dim E$ (если размерность E определена). Если u — не постоянная аффинная функция на E и $\lambda \in K$, то множество всех $x \in E$, удовлетворяющих уравнению $u(x) = \lambda$, есть гиперплоскость; обратно, для каждой гиперплоскости H пространства E существует аффинная функция u_0 на E такая,

что $H=\overset{-1}{u_0}(0)$, и каждая аффинная функция u, для которой $H=\overset{-1}{u}(0)$, имеет вид $u_0\mu$, где $\mu\in K$ (§ 4, предложение 9). Если u — аффинная функция на E, то гиперплоскости, определяемые уравнениями $u(x)=\alpha$ и $u(x)=\beta$, параллельны.

Упражнения. 1) Четверка точек (a, b, c, d) аффинного пространства E над телом K называется *параллелограммом*, если $b-a=c-d$, причем в этом случае и (a, d, c, b) — параллелограмм. Показать, что если K — характеристики $\neq 2$, то середины пар (a, c) и (b, d) совпадают; что можно сказать в случае, когда K — характеристики 2?

2) Пусть a, b, c, d — любые четыре точки аффинного пространства E над телом характеристики $\neq 2$. Показать, что если x, y, z, t — середины пар (a, b), (b, c), (c, d) и (d, a), то (x, y, z, t) — параллелограмм (упражнение 1).

3) Пусть K — тело характеристики $\neq 2$, E — аффинная плоскость над K и a, b, c, d — четыре ее точки, никакие три из которых не лежат на одной прямой. Обозначая через D_{xy} прямую, проходящую через точки x и y, допустим, что прямые D_{ab} и D_{cd} имеют общую точку e, а прямые D_{ad} и D_{bc} — общую точку f. Показать, что середины пар (a, c), (b, d) и (e, f) лежат на одной прямой. Во что переходит это свойство, когда D_{ab} и D_{cd} или D_{ad} и D_{bc} параллельны? Случай тела K, состоящего из трех элементов.

4) Пусть K — тело характеристики $\neq 2$ и $\neq 3$, E — аффинное пространство над K, a, b, c — три его точки, не лежащие на одной прямой, и a', b', c' — соответственно середины пар (b, c), (c, a) и (a, b). Показать, что прямые $D_{aa'}$, $D_{bb'}$ и $D_{cc'}$ проходят через центр тяжести тройки точек a, b, c. Во что переходит это свойство, когда K — характеристики 2 или 3? Обобщить на систему n аффинно независимых точек.

5) Для того чтобы непустое множество V точек аффинного пространства E над телом K, содержащим по крайней мере три элемента, было линейным многообразием, необходимо и достаточно, чтобы для любой пары (x, y) различных точек из V прямая D_{xy}, проходящая через x и y, вся целиком содержалась в V. Если K состоит из двух элементов, то для того, чтобы V было линейным многообразием, необходимо и достаточно, чтобы центр тяжести любой тройки точек из V принадлежал V.

6) а) Пусть E — аффинное пространство над телом K. Для того чтобы аффинное отображение u этого пространства в себя преобразовывало каждую прямую в параллельную ей прямую, необходимо и достаточно, чтобы линейное отображение v, ассоциированное с u, было гомотетией $t\to\gamma t$ с коэффициентом $\gamma\neq 0$, принадлежащим центру тела K. Если $\gamma=1$, то u — перенос; показать, что если $\gamma\neq 1$,

то существует, и притом только одна, точка $a \in E$, для которой $u(a) = a$. Если принять a за начало в E, то u совпадет с некоторой центральной гомотетией относительно определенной так структуры векторного пространства в E; u называется тогда *центральной гомотетией* аффинного пространства E с центром a и коэффициентом γ.

б) Пусть u_1 и u_2 — аффинные отображения E в E, каждое из которых есть перенос или центральная гомотетия этого пространства. Показать, что и u_1u_2 есть его перенос или центральная гомотетия; показать, что если u_1, u_2 и u_1u_2 все три являются центральными гомотетиями, то их центры лежат на одной прямой. Что можно сказать в случае, когда u_1 и u_2 — центральные гомотетии, а u_1u_2 — перенос?

в) Показать, что множество H всех переносов и центральных гомотетий является нормальной подгруппой аффинной группы пространства E и что H/T изоморфно мультипликативной группе центра тела K; показать, что группа H может быть коммутативной только когда $H = T$, иными словами, когда центр тела K состоит лишь из двух элементов.

*7) Пусть E (соответственно E') — аффинное пространство конечной размерности $n \geqslant 2$ над телом K, содержащим по крайней мере 3 элемента (соответственно над телом K'), и u — инъективное отображение E в E', преобразующее любые три точки, лежащие на одной прямой, в три точки, лежащие на одной прямой, и такое, что линейное многообразие в E', порожденное множеством $u(E)$, равно E'.

а) Показать, что u преобразуют любую систему аффинно независимых точек из E в систему аффинно независимых точек. [Использовать упражнение 5.]

б) Пусть D_1, D_2 — две параллельные прямые в E и D_1', D_2' — прямые в E', содержащие соответственно $u(D_1)$ и $u(D_2)$. Показать, что D_1' и D_2' лежат в одной плоскости и, если, кроме того, u сюръективно, параллельны. [Показать, что в противном случае должны были бы существовать три точки, не лежащие на одной прямой, переводимые отображением u в точки одной прямой.] (См. Приложение III, упражнение 11.)

в) Будем предполагать, что если D_1, D_2 — параллельные прямые из E, то прямые в E', содержащие соответственно $u(D_1)$, $u(D_2)$, параллельны. Показать, выбрав в E начало a и в E' — начало $a' = u(a)$, что существует изоморфизм σ тела K на подтело K_1 тела K' такой, что если рассматривать E как векторное пространство над K, а E' — как векторное пространство над K_1, то u будет инъективным полулинейным (относительно σ) отображением E в E' (Приложение I). [Рассмотреть сначала случай $n = 2$. Показать, что, выбрав базис (e_1, e_2) в E, можно для любых двух элементов α и β тела K, отправляясь от точек 0, e_1, e_2, αe_1, βe_1, построить в E точки $(\alpha+\beta)e_1$ и $(\alpha\beta)e_1$

с помощью построения параллелей к заданным прямым и точек пересечения заданных прямых; вывести отсюда, что $u(\lambda e_1)=\lambda^\sigma u(e_1)$, где σ — изоморфизм тела K на подтело тела K'; далее, рассматривая прямую, соединяющую точки λe_1 и λe_2, показать, что также $u(\lambda e_2)=\lambda^\sigma u(e_2)$. Наконец, перейти отсюда к случаю произвольного n индукцией по n.] Показать, что если u биективно, то $K_1=K'$.

г) Распространить результат пункта в) на случай тела K, состоящего из двух элементов, предполагая дополнительно, что u преобразует каждую систему аффинно независимых точек из E в систему аффинно независимых точек из E'.

ПРИЛОЖЕНИЕ III

К ГЛАВЕ II

ПРОЕКТИВНЫЕ ПРОСТРАНСТВА

1. Определение проективных пространств

Определение 1. *Левым* (соответственно *правым*) *проективным пространством, порожденным левым* (соответственно *правым*) *векторным пространством V над телом K, называют фактормножество* $\mathbf{P}(V)$ *дополнения* V^* *к* $\{0\}$ *в* V *по отношению эквивалентности* $\Delta(V)$: «*в* K *существует* $\lambda \neq 0$ *такое, что* $y=\lambda x$ (соответственно $y=x\lambda$)» *между* x *и* y *в* V^*.

В случае, когда $V=K_s^{n+1}$, вместо $\mathbf{P}(K_s^{n+1})$ и $\Delta(K_s^{n+1})$ пишут также $\mathbf{P}_n(K)$ и $\Delta_n(K)$.

Определение 1 можно выразить также, сказав, что $\mathbf{P}(V)$ есть множество всех (однородных) прямых пространства V, лишенных начала, и, значит, канонически отождествляется с множеством всех (однородных) прямых пространства V. Элементы проективного пространства называют его *точками*.

В случае, когда V имеет конечную размерность n, *размерностью* проективного пространства $\mathbf{P}(V)$ называют целое число $n-1$ и обозначают его $\dim_K \mathbf{P}(V)$ или $\dim \mathbf{P}(V)$. Так, проективное пространство размерности -1 пусто, а проективное пространство размерности 0 сводится к одной точке. Проективное пространство размерности 1 (соответственно 2) называют *проективной прямой* (соответственно *проективной плоскостью*).

В дальнейшем рассматриваются только левые проективные пространства.

2. *Однородные координаты*

Пусть V — векторное пространство размерности $n+1$ над K, $\mathbf{P}(V)$ — порожденное им проективное пространство размерности n, $(e_i)_{0\leqslant i\leqslant n}$ — *базис* пространства V и π — каноническое отображение V^* на фактормножество $\mathbf{P}(V)$. Если $x=\sum_{i=0}^{n}\xi_i e_i\in V^*$, то $(\xi_0, \xi_1, \ldots, \xi_n)$ называют *системой однородных координат* точки $\pi(x)$ относительно базиса (e_i) пространства V. Таким образом, каждая система (ξ_i) $n+1$ элементов тела K, которые *не все равны нулю*, есть однородная система координат некоторой точки из $\mathbf{P}(V)$ относительно (e_i); для того чтобы две такие системы (ξ_i), (ξ'_i) были системами однородных координат одной и той же точки из $\mathbf{P}(V)$ относительно одного и того же базиса (e_i), необходимо и достаточно, чтобы в K существовал элемент $\lambda\neq 0$ такой, что $\xi'_i=\lambda\xi_i$ для всех i $(0\leqslant i\leqslant n)$.

Если $(\bar{e}_i)$ — второй базис пространства V, причем $e_i=\sum_{j=0}^{n}\alpha_{ij}\bar{e}_j$ $(0\leqslant i\leqslant n)$, и (ξ_i) — система однородных координат точки $\pi(x)$ относительно базиса (e_i), то для того, чтобы система $(\bar{\xi}_i)$ $n+1$ элементов из K была системой однородных координат точки $\pi(x)$ относительно базиса $(\bar{e}_i)$, необходимо и достаточно, чтобы в K существовало $\lambda\neq 0$ такое, что

$$\lambda\bar{\xi}_i=\sum_{j=0}^{n}\xi_j a_{ji}\quad(0\leqslant i\leqslant n).$$

В частности, при $e_i=\gamma_i\bar{e}_i$, где $\gamma_i\neq 0$ $(0\leqslant i\leqslant n)$, $\bar{\xi}_i=\mu\xi_i\gamma_i$, где $\mu\neq 0$.

Эти определения непосредственно обобщаются на случай бесконечномерного V.

3. *Проективные линейные многообразия*

Пусть W — векторное подпространство векторного пространства V; канонический образ множества $W^*=W-\{0\}$ в проективном пространстве $\mathbf{P}(V)$, порожденном V, называется *проективным линейным многообразием* (или просто *линейным многообразием*,

если можно не опасаться путаницы); так как отношение эквивалентности $\Delta(W)$ в W^* индуцируется отношением $\Delta(V)$, то проективное линейное многообразие в $\mathbf{P}(V)$, являющееся образом W^*, можно отождествлять с проективным пространством $\mathbf{P}(W)$, порожденным W, и, следовательно, говорить о размерности такого многообразия. Линейное многообразие в проективном пространстве $\mathbf{P}(V)$, являющееся каноническим образом гиперплоскости из V (лишенной начала), называется *проективной гиперплоскостью* (или просто *гиперплоскостью*) этого пространства; если $\mathbf{P}(V)$ n-мерно, то гиперплоскости в $\mathbf{P}(V)$ — это его $(n-1)$-мерные линейные многообразия.

Каждому предложению, относящемуся к векторным подпространствам векторного пространства, отвечает некоторое предложение, относящееся к проективным линейным многообразиям. Например, если $\mathbf{P}(V)$ есть n-мерное проективное пространство и $(e_i)_{0\leqslant i\leqslant n}$ — базис пространства V, то каждое r-мерное линейное многообразие $L\subset\mathbf{P}(V)$ может быть определено системой $n-r$ однородных линейных уравнений

$$\sum_{i=0}^{n}\xi_i a_{ij} \quad (1\leqslant j\leqslant n-r), \tag{1}$$

связывающих однородные координаты ξ_i $(0\leqslant i\leqslant n)$ точки из $\mathbf{P}(V)$ относительно базиса (e_i), где в левых частях уравнений стоят независимые линейные формы на V (§ 4, n° 6). В частности, проективная гиперплоскость определяется одним однородным линейным уравнением, не все коэффициенты которого равны нулю. Обратно, точки пространства $\mathbf{P}(V)$, удовлетворяющие произвольной системе однородных линейных уравнений относительно координат ξ_i, образуют в нем некоторое линейное многообразие L; если рассматриваемая система состоит из $k\leqslant n+1$ уравнений, то L будет размерности $\geqslant n-k$.

Пересечение любого семейства линейных многообразий пространства $\mathbf{P}(V)$ есть его линейное многообразие; для каждого множества $A\subset\mathbf{P}(V)$ существует наименьшее содержащее его линейное многообразие L; оно называется линейным многообразием, *порожденным множеством* A, а это множество — *системой образующих* линейного многообразия L; если W — векторное подпространство в V, порожденное множеством $\pi^{-1}(A)$, то $L=\mathbf{P}(W)$.

Если L и M — два произвольных линейных многообразия в $\mathbf{P}(V)$ и N — линейное многообразие, порожденное их объединением $L \bigcup M$, то (§ 3, предложение 7)

$$\dim L + \dim M = \dim (L \bigcap M) + \dim N \qquad (2)$$

в предположении, что обе части этого соотношения определены. Из (2), в частности, следует, что если $\dim L + \dim M \geqslant \dim \mathbf{P}(V)$, то $L \bigcap M$ не пусто.

Пусть (x_ι), (y_ι) — семейства точек векторного пространства V, имеющие одно и то же множество индексов и такие, что $y_\iota = \lambda_\iota x_\iota$, где $\lambda_\iota \neq 0$ для каждого ι. Если (x_ι) — свободное семейство, то это же верно для (y_ι), и обратно; в этом случае семейство точек $\pi(x_\iota)$ пространства $\mathbf{P}(V)$ называют *проективно свободным* (или просто *свободным*). То же самое можно выразить, сказав, что никакая точка $\pi(x_\varkappa)$ не принадлежит линейному многообразию, порожденному точками $\pi(x_\iota)$ с индексами $\iota \neq \varkappa$. Семейство точек пространства $\mathbf{P}(V)$, не являющееся проективно свободным, называется *проективно зависимым* (или просто *зависимым*).

Для того чтобы семейству (x_ι) точек из V соответствовало проективно свободное семейство $(\pi(x_\iota))$, порождающее $\mathbf{P}(V)$, необходимо и достаточно, чтобы (x_ι) было базисом пространства V. Значит, если $\mathbf{P}(V)$ n-мерно, то число элементов такого семейства равно $n+1$. Заметим, что задание такого семейства $(\pi(x_\iota))$ в $\mathbf{P}(V)$ еще не определяет (даже с точностью до левого множителя) однородных координат заданной точки пространства $\mathbf{P}(V)$ относительно базиса (y_ι) в V, для которого $\pi(y_\iota) = \pi(x_\iota)$ при каждом ι (см. n° 2).

4. *Проективное пополнение аффинного пространства*

Пусть V — (левое) векторное пространство над телом K; рассмотрим векторное пространство $K_s \times V$ над K; проективное пространство $\mathbf{P}(K_s \times V)$ будет называться проективным пространством, *канонически ассоциированным* с векторным пространством V. Если V имеет конечную размерность n, то $\mathbf{P}(K_s \times V)$ имеет ту же размерность n. Рассмотрим в $K_s \times V$ аффинную гиперплоскость $V_1 = \{1\} \times V$, имеющую своей направляющей (Приложение II, n° 3) (однородную) гиперплоскость $V_0 = \{0\} \times V$: если (однородная) прямая из $K_s \times V$ не содержится в V_0, то она

содержит точку (α, x) с $\alpha \neq 0$ и $x \in V$, а значит, точку $\alpha^{-1}(\alpha, x) = (1, \alpha^{-1}x)$ из V_1; обратное очевидно. Таким образом устанавливается взаимно однозначное соответствие между точками гиперплоскости V_1 и (однородными) прямыми произведения $K_s \times V$, не содержащимися в V_0, поскольку каждая из этих прямых пересекает V_1 в одной и только одной точке. Отсюда следует, что отображение $x \longrightarrow \varphi(x) = \pi(1, x)$ есть (называемая *канонической*) инъекция векторного пространства V в проективное пространство $\mathbf{P}(K_s \times V)$; V часто отождествляют с его образом при этой инъекции. Дополнением к $\varphi(V)$ в $\mathbf{P}(K_s \times V)$ служит проективная гиперплоскость $\mathbf{P}(V_0)$; ее называют *бесконечно удаленной гиперплоскостью* пространства $\mathbf{P}(K_s \times V)$ (или, допуская вольность речи, пространства V), а точки этой гиперплоскости — «бесконечно удаленными точками» пространства $\mathbf{P}(K_s \times V)$ (или V). Если (a_ι) — базис пространства V и в $K_s \times V$ выбран базис, образованный всеми элементами $e_\iota = (0, a_\iota)$ и элементом $e_\omega = (1, 0)$, то бесконечно удаленные точки пространства $\mathbf{P}(K_s \times V)$ — это точки, однородные координаты которых с индексом ω равны 0.

Пусть M — аффинное линейное многообразие в V (Приложение II, n° 3) и D — его направляющая; канонический образ $\varphi(M)$ многообразия M в $\mathbf{P}(K_s \times V)$ содержится в каноническом образе $\overline{M} = \pi(M_2)$ векторного подпространства M_2, порожденного в $K_s \times V$ его аффинным линейным многообразием $M_1 = \{1\} \times M$. Более точно, если (a_ι) — аффинно свободная система точек из M, порождающая M, то элементы $(1, a_\iota)$ образуют базис подпространства M_2, и следовательно, $\overline{M}$ есть не что иное, как *проективное линейное многообразие, порожденное множеством* $\varphi(M)$; если M конечномерно, то $\overline{M}$ имеет ту же размерность, что и M. Дополнение к $\varphi(M)$ в $\overline{M}$ есть пересечение многообразия $\overline{M}$ с бесконечно удаленной гиперплоскостью и равно каноническому образу $\pi(M_0)$ подпространства $M_0 = \{0\} \times D$.

Обратно, пусть N — проективное линейное многообразие, не содержащееся в бесконечно удаленной гиперплоскости, и $R = \pi^{-1}(N)$; $R \cap V_1$ есть аффинное линейное многообразие в $K_s \times V$ вида $\{1\} \times M$, где M — аффинное линейное многообразие в V; легко видеть, что N совпадает с аффинным линейным многообразием $\overline{M}$, порожденным множеством $\varphi(M)$.

Таким образом, имеется взаимно однозначное соответствие между аффинными линейными многообразиями из V и проективными линейными многообразиями из $\mathbf{P}(K_s \times V)$, не содержащимися в бесконечно удаленной гиперплоскости; для того чтобы два аффинных линейных многообразия из V были *параллельны*, необходимо и достаточно, чтобы порождаемые ими проективные линейные многообразия имели одно и то же пересечение с бесконечно удаленной гиперплоскостью (что иногда выражают, говоря, что рассматриваемые два аффинных линейных многообразия имеют одни и те же бесконечно удаленные точки).

5. *Продолжение рациональных функций*

Применение результатов n° 4 к одномерному векторному пространству $V=K_s$ показывает, что существует его каноническое вложение φ в проективную прямую $\mathbf{P}_1(K)=\mathbf{P}(K_s \times K_s)$; $\varphi(\xi)$ для каждого $\xi \in K$ есть точка с однородными координатами $(1, \xi)$ относительно канонического базиса (§ 1, n° 8) произведения $K_s \times K_s$. Дополнение к $\varphi(K)$ в $\mathbf{P}_1(K)$ сводится к точке с однородными координатами $(0, 1)$ относительно указанного базиса, называемой «бесконечно удаленной точкой». $\mathbf{P}_1(K)$ называется также *проективным телом*, ассоциированным с K, и обозначается $\tilde{K}$, а его бесконечно удаленная точка обозначается ∞.

°Рассмотрим, в частности, случай *поля* K, и пусть $f \in K(X)$ — рациональная дробь от одной неизвестной над K (гл. IV, § 4); f однозначным образом представляется в виде $f=(\alpha p)/q$, где $\alpha \in K^*$, а p и q — взаимно простые унитарные полиномы (гл. VII, § 1); пусть m и n — их степени и, скажем, $m \leqslant n$. Положим $p_1(T, X)= T^n p(X/T)$, $q_1(T, X)=T^n q(X/T)$; p_1 и q_1 — однородные полиномы степени n над K такие, что $p(X)=p_1(X, 1)$, $q(X)=q_1(X, 1)$. Для каждого элемента $\xi \in K$, не являющегося нулем полинома $q(X)$, $f(\xi)=\alpha p(\xi)/q(\xi)$ определено, и можно написать

$$f(\xi)=\alpha p_1(1, \xi)/q_1(1, \xi)=\alpha p_1(\lambda, \lambda\xi)/q_1(\lambda, \lambda\xi),$$

каково бы ни было $\lambda \neq 0$ из K. Рассмотрим тогда отображение

$$(\eta, \xi) \longrightarrow (q_1(\eta, \xi), \alpha p_1(\eta, \xi))$$

произведения K^2 в себя; это отображение согласуется с отношением эквивалентности $\Delta(K^2)$ и, следовательно, порождает при

факторизации отображение $\widetilde{f}$ проективного поля $\widetilde{K}$ в себя, совпадающее с $\xi \to f(\xi)$ в тех точках, где эта рациональная функция определена; допуская вольность речи, $\widetilde{f}$ называют *каноническим продолжением* f на $\widetilde{K}$.

Например, если $f = 1/X$, то $\widetilde{f}(0) = \infty$ и $\widetilde{f}(\infty) = 0$; если $f = (aX+b)/(cX+d)$, где $ad - bc \neq 0$, то $\widetilde{f}(-d/c) = \infty$, $\widetilde{f}(\infty) = a/c$, если $c \neq 0$, и $\widetilde{f}(\infty) = \infty$, если $c = 0$. Для полинома $f = a_0X^n + \ldots + a_n$ степени $n > 0$ имеем $\widetilde{f}(\infty) = \infty$.

6. *Проективные отображения*

Пусть V и V' — левые векторные пространства над телом K, f — линейное отображение V в V' и $N = f^{-1}(0)$ — его ядро. Очевидно, при этом отображении (однородная) прямая пространства V, не содержащаяся в N, переходит в (однородную) прямую пространства V'; поэтому при факторизации f порождает отображение g множества $\mathbf{P}(V) - \mathbf{P}(N)$ в $\mathbf{P}(V')$. Это отображение g называется *проективным отображением* (или *проективным линейным отображением*); хотя оно определено на $\mathbf{P}(V) - \mathbf{P}(N)$, а не (при $N \neq \{0\}$) на всем $\mathbf{P}(V)$, допуская вольность речи, говорят, что g есть проективное отображение $\mathbf{P}(V)$ в $\mathbf{P}(V')$. Проективное линейное многообразие $\mathbf{P}(N)$, на котором g не определено, называется *центром* отображения g.

Заметим, что в случае, когда g определено на всем $\mathbf{P}(V)$ (т. е. когда $N = \{0\}$), g есть *инъекция* $\mathbf{P}(V)$ в $\mathbf{P}(V')$.

Если в V и V' заданы соответственно базисы $(a_\lambda)_{\lambda \in L}$ и $(b_\mu)_{\mu \in M}$, проективное отображение g пространства $\mathbf{P}(V)$ в $\mathbf{P}(V')$ относит точке из $\mathbf{P}(V)$ с однородными координатами ξ_λ $(\lambda \in L)$ точку в $\mathbf{P}(V')$, обладающую системой однородных координат η_μ $(\mu \in M)$ вида

$$\eta_\mu = \sum_{\lambda \in L} \xi_\lambda \alpha_{\lambda\mu} \qquad (\alpha_{\lambda\mu} \in K). \tag{3}$$

Центр отображения g есть линейное многообразие, определяемое уравнениями

$$\sum_{\lambda \in L} \xi_\lambda \alpha_{\lambda\mu} = 0 \qquad (\mu \in M).$$

Если C — центр отображения g и M — линейное многообразие в $\mathbf{P}(V)$, то *образ* $M - (M \cap C)$ при отображении g есть линейное многообразие в $\mathbf{P}(V')$, которое (допуская вольность) обозначают $g(M)$. Имеем

$$\dim g(M) = \dim M - \dim (M \cap C) - 1, \tag{4}$$

если числа, фигурирующие в этой формуле, определены (§ 3, формула (5)). Если M' — линейное многообразие в $\mathbf{P}(V')$, то $g^{-1}(M') \cup C$ есть линейное многообразие в $\mathbf{P}(V)$, и

$$\dim (g^{-1}(M') \cup C) = \dim C + \dim (M' \cap g(\mathbf{P}(V))) + 1. \tag{5}$$

Допуская вольность речи, говорят, что $g^{-1}(M') \cup C$ есть *прообраз* M' относительно g.

Так как значения из V', принимаемые линейным отображением на базисе (e_ι) пространства V, могут выбираться произвольно, то заключаем, что существует проективное отображение $\mathbf{P}(V)$ в $\mathbf{P}(V')$, принимающее в точках $\pi(e_\iota)$ *произвольно* заданные значения. Но (даже когда g всюду определено) задание элементов $g(\pi(e_\iota))$ не определяет g однозначным образом (упражнение 3).

Композиция двух биективных проективных отображений есть проективное отображение; то же верно и для отображения, обратного к такой биекции. Таким образом, взаимно однозначные проективные отображения проективного пространства $\mathbf{P}(V)$ на себя образуют группу; она называется *проективной группой* пространства $\mathbf{P}(V)$ и обозначается $\mathbf{PGL}(V)$; вместо $\mathbf{PGL}(K_s^n)$ пишут $\mathbf{PGL}_n(K)$.

Замечание. Пусть $H = \mathbf{P}(W)$ — гиперплоскость проективного пространства $\mathbf{P}(V)$ над телом K. Существует взаимно однозначное линейное отображение f пространства V на $K_s \times W$ такое, что $f(W) = W$; пусть g — проективное отображение, получающееся из f при факторизации. Как мы видели (п° 4), дополнение к $\mathbf{P}(W)$ в $\mathbf{P}(K_s \times W)$ отождествимо с аффинным пространством, пространством переносов которого служит W. Отождествляя $\mathbf{P}(V)$ с $\mathbf{P}(K_s \times W)$ посредством отображения g, говорят, что H *принимается в* $\mathbf{P}(V)$ *за бесконечно удаленную гиперплоскость*; дополнение к H в $\mathbf{P}(V)$ отождествляется тогда с аффинным пространством, имеющим W своим пространством переносов.

7. Структура проективного пространства

Структура (левого) проективного пространства в множестве E относительно тела K определяется заданием непустого множества Φ *биекций* подмножеств проективного пространства $\mathbf{P}(K_s^{(F)})$ *на* E, удовлетворяющего следующим аксиомам:

($\mathrm{EP_I}$) *Областью определения каждого отображения* $f \in \Phi$ *служит некоторое линейное многообразие из* $\mathbf{P}(K_s^{(E)})$.

($\mathrm{EP_{II}}$) *Для любой пары элементов* f, g *из* Φ, *определенных соответственно на линейных многообразиях* $\mathbf{P}(V)$ *и* $\mathbf{P}(W)$, *биекция* $h = g^{-1} \circ f$ *пространства* $\mathbf{P}(V)$ *на* $\mathbf{P}(W)$ *есть проективное отображение.*

($\mathrm{EP_{III}}$) *Обратно, если* $f \in \Phi$ *определено на линейном многообразии* $\mathbf{P}(V)$ *и* h *— взаимно однозначное проективное отображение* $\mathbf{P}(V)$ *на линейное многообразие* $\mathbf{P}(W) \subset \mathbf{P}(K_s^{(E)})$, *то* $f \circ h^{-1} \in \Phi$.

Пусть E — множество, $(V_\lambda)_{\lambda \in L}$ — семейство векторных пространств над телом K и для каждого $\lambda \in L$ задана биекция f_λ пространства $\mathbf{P}(V_\lambda)$ на E такая, что $f_\lambda^{-1} \circ f_\mu$ для каждой пары индексов (λ, μ) есть *проективное отображение* $\mathbf{P}(V_\mu)$ на $\mathbf{P}(V_\lambda)$. Тогда можно определить в E структуру проективного пространства относительно K следующим образом. Пусть $(e_\iota)_{\iota \in I}$ — базис пространства V_λ и $a_\iota = f_\lambda(\pi(e_\lambda))$, а b_ι — элемент с индексом a_ι в каноническом базисе пространства $K_s^{(E)}$ (§ 1, n° 8). В силу предположенной биективности отображения f_λ, $b_\iota \neq b_\varkappa$ при $\iota \neq \varkappa$; поэтому b_ι образуют базис векторного подпространства W_0 пространства $K_s^{(E)}$, и следовательно, существует взаимно однозначное отображение h пространства $\mathbf{P}(W_0)$ на $\mathbf{P}(V_\lambda)$ такое, что $h(\pi(b_\iota)) = \pi(e_\iota)$ для каждого $\iota \in I$. Легко проверить, что множество Φ всех отображений $f_\lambda \circ h \circ g^{-1}$, где g пробегает множество всевозможных взаимно однозначных проективных отображений $\mathbf{P}(W_0)$ на линейные многообразия $\mathbf{P}(W) \subset \mathbf{P}(K_s^{(E)})$, удовлетворяет аксиомам ($\mathrm{EP_I}$), ($\mathrm{EP_{II}}$) и ($\mathrm{EP_{III}}$). При этом, очевидно, Φ не зависит ни от выбора индекса $\lambda \in L$, ни от выбора базиса (e_ι) в V_λ, ни от выбора h.

В частности (если взять L, сводящееся к одному элементу), каждое проективное пространство $\mathbf{P}(V)$, порожденное каким-нибудь векторным пространством V (определение 1), наделено так вполне определенной «структурой проективного простран-

ства» в смысле определения, данного в этом n°. Поэтому *проективным пространством* можно называть всякое множество, наделенное структурой проективного пространства.

В тех же обозначениях *линейное многообразие* в проективном пространстве E — это множество $M \subset E$, для которого $\overset{-1}{f}(M)$ хотя бы для *одной* биекции $f \in \Phi$, определенной на $\mathbf{P}(V) \subset \mathbf{P}(K_s^{(E)})$, есть линейное многообразие в $\mathbf{P}(V)$ в смысле n° 3 (этим свойством обладает тогда *каждое* $f \in \Phi$). Из предыдущего следует, что каждое линейное многообразие проективного пространства канонически наделено структурой проективного пространства.

Говорят, что проективное пространство E имеет *размерность* n, если $\overset{-1}{f}(E)$ для каждого $f \in \Phi$ есть линейное многообразие размерности n (достаточно, чтобы это имело место для *одного* из отображений $f \in \Phi$).

Упражнения. 1) Пусть K — конечное тело, состоящее из q элементов, и V — n-мерное векторное пространство над K.

а) Показать, что число элементов множества всевозможных последовательностей $(x_1, x_2, \ldots, x_m)$ из $m \leqslant n$ векторов пространства V, образующих свободную систему, равно

$$(q^n - 1)(q^n - q) \ldots (q^n - q^{m-1}).$$

[Индукцией по m.]

б) Вывести из а), что число m-мерных линейных многообразий в n-мерном проективном пространстве над K равно

$$\frac{(q^{n+1} - 1)(q^{n+1} - q) \ldots (q^{n+1} - q^m)}{(q^{m+1} - 1)(q^{m+1} - q) \ldots (q^{m+1} - q^m)}.$$

2) а) Показать, что проективная группа $\mathbf{PGL}(V)$ изоморфна факторгруппе линейной группы $\mathbf{GL}(V)$ векторного пространства V по центру этой группы (изоморфному мультипликативной группе центра тела K, см. § 2, следствие 2 предложения 5).

б) Вывести из а), что если V — конечной размерности > 2, то коммутант группы $\mathbf{PGL}(V)$ простой. [См. § 6, упражнение 10.]

°в) Показать, что если K — конечное тело, состоящее из q элементов, то проективная группа n-мерного проективного пространства над K есть группа порядка

$$(q^{n+1} - 1)(q^{n+1} - q) \ldots (q^{n+1} - q^{n-1})\, q^n.$$

[Использовать а) и упражнение 1а, а также то, что K необходимо коммутативно (см. гл. V, § 11, упражнение 14, и гл. V III).]

3) *Проективным репером* в n-мерном проективном пространстве $\mathbf{P}(V)$ над телом K называется множество S из $n+2$ точек, каждые $n+1$

из которых образуют проективно свободную систему. Показать, что для любых двух проективных реперов $S=(a_i)_{0\leqslant i\leqslant n+1}$ и $S'=(a'_i)_{0\leqslant i\leqslant n+1}$ пространства $\mathbf{P}(V)$ существует преобразование $f\in\mathbf{PGL}(V)$ такое, что $f(a_i)=a'_i$ для всех i $(0\leqslant i\leqslant n+1)$. Для единственности этого преобразования необходимо и достаточно, чтобы K было коммутативно. [Свести к случаю $S'=S$ и заметить, что всегда можно считать $a_i=\pi(b_i)$, где $(b_i)_{1\leqslant i\leqslant n+1}$ — базис пространства V, а $b_0=b_1+b_2+\ldots+b_{n+1}$.]

Привести пример, где K есть тело кватернионов (§ 7, n° 8) или где существуют бесконечное множество T точек из $\mathbf{P}(V)$, любые $n+1$ из которых образуют проективно свободную систему, и нетождественное преобразование $f\in\mathbf{PGL}(V)$, оставляющее инвариантной каждую точку из T.

4) Пусть V — двумерное векторное пространство над телом K и a, b, c, d — четыре различные точки проективной прямой $\mathbf{P}(V)$. *Двойным отношением* четверки (a, b, c, d) называют множество $\begin{bmatrix} a & b \\ d & c \end{bmatrix}$ тех элементов $\xi\in K$, для которых в V существуют векторы u, v такие, что $a=\pi(u)$, $b=\pi(v)$, $c=\pi(u+v)$, $d=\pi(u+\xi v)$. Это определение непосредственно распространяется на каждую четверку различных точек множества, наделенного структурой проективной прямой (n° 7).

а) Показать, что $\begin{bmatrix} a & b \\ d & c \end{bmatrix}$ есть множество всех элементов, сопряженных к некоторому элементу $\neq 1$ мультипликативной группы K^*, и что, обратно, для любых трех различных точек a, b, c из $\mathbf{P}(V)$ и множества ϱ всех элементов, сопряженных к какому-нибудь элементу $\neq 1$ из K^*, существует точка $d\in\mathbf{P}(V)$ такая, что $\begin{bmatrix} a & b \\ d & c \end{bmatrix}=\varrho$. Для единственности d необходимо и достаточно, чтобы ϱ сводилось к одному элементу.

б) Показать, что

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}=\begin{bmatrix} b & a \\ d & c \end{bmatrix}=\begin{bmatrix} a & b \\ d & c \end{bmatrix}^{-1}$$

и

$$\begin{bmatrix} d & a \\ c & b \end{bmatrix}=1-\begin{bmatrix} a & b \\ d & c \end{bmatrix}$$

(где ϱ^{-1} (соответственно $1-\varrho$) означает множество всевозможных сопряженных $\lambda\xi^{-1}\lambda^{-1}=(\lambda\xi\lambda^{-1})^{-1}$ (соответственно всевозможных $1-\lambda\xi\lambda^{-1}=\lambda(1-\xi)\lambda^{-1}$) для элементов ξ из ϱ).

в) Пусть (a, b, c, d) и (a', b', c', d') — две четверки различных точек из $\mathbf{P}(V)$. Для того чтобы существовало биективное полулинейное (Приложение I) отображение V на себя такое, что порождаемое им при факторизации биективное отображение f пространства $\mathbf{P}(V)$

на себя удовлетворяет условиям $f(a)=a'$, $f(b)=b'$, $f(c)=c'$, $f(d)=d'$, необходимо и достаточно, чтобы существовал автоморфизм σ тела K, для которого

$$\begin{bmatrix} a' & b' \\ d' & c' \end{bmatrix} = \begin{bmatrix} a & b \\ d & c \end{bmatrix}^{\sigma}.$$

Для существования в проективной группе $\mathbf{PGL}(V)$ преобразования f, удовлетворяющего указанным условиям, необходимо и достаточно, чтобы

$$\begin{bmatrix} a' & b' \\ d' & c' \end{bmatrix} = \begin{bmatrix} a & b \\ d & c \end{bmatrix}.$$

5) Пусть $\mathbf{P}(V)$ — (левое) проективное пространство конечной размерности n над телом K. Показать, что в множестве всех проективных гиперплоскостей пространства $\mathbf{P}(V)$ существует структура (правого) проективного пространства размерности n над K, канонически изоморфная структуре проективного пространства $\mathbf{P}(V^*)$ (где V^* — векторное пространство, сопряженное к V). Получить отсюда структуру проективного пространства размерности $n-r-1$ в множестве всех проективных гиперплоскостей, содержащих заданное линейное многообразие M размерности $r<n$ пространства $\mathbf{P}(V)$. В частности, если M имеет размерность $n-2$, можно определить двойное отношение $\begin{bmatrix} H_1 & H_2 \\ H_4 & H_3 \end{bmatrix}$ четверки (H_1, H_2, H_3, H_4) различных гиперплоскостей, содержащих M. Показать, что если $D \subset \mathbf{P}(V)$ — прямая, не пересекающая M, и a_i — пересечение D с H_i $(1 \leqslant i \leqslant 4)$, то

$$\begin{bmatrix} a_1 & a_2 \\ a_4 & a_3 \end{bmatrix} = \begin{bmatrix} H_1 & H_2 \\ H_4 & H_3 \end{bmatrix}.$$

°6) Пусть K — поле, $\widetilde{K}$ — проективное поле, полученное путем присоединения к K бесконечно удаленной точки (n° 5), и f, g — две рациональные дроби из $K(X)$. Показать, что если $h(X)=f(g(X))$, а $\widetilde{f}$, $\widetilde{g}$ и $\widetilde{h}$ — канонические продолжения f, g и h на K, то $\widetilde{h}=\widetilde{f}\circ\widetilde{g}$.

7) Пусть a, b, c, d — четыре точки проективной плоскости $\mathbf{P}(V)$ над телом K характеристики $\neq 2$, образующие проективный репер (упражнение 3), e, f, g — точки пересечения прямых D_{ab} и D_{cd}, D_{ac} и D_{bd}, D_{ad} и D_{bc} (где D_{xy} означает прямую, проходящую через различные точки x, y) и h — точка пересечения прямых D_{bc} и D_{ef}. Показать, что $\begin{bmatrix} b & c \\ h & g \end{bmatrix} = \{-1\}$. [«Теорема о полном четырехстороннике»; свести к случаю, когда D_{ad} — бесконечно удаленная прямая аффинной плоскости.] Каков соответствующий результат в случае тела K характеристики 2?

8) Пусть D и D' — две различные прямые проективной плоскости $\mathbf{P}(V)$ над телом K, содержащим не менее трех элементов. Для того чтобы для любых трех различных точек a, b, c прямой D и любых

трех различных точек a', b', c' прямой D' точки пересечения r, q, p прямых $D_{ab'}$ и $D_{ba'}$, $D_{ac'}$ и $D_{ca'}$, $D_{bc'}$ и $D_{cb'}$ лежали на одной прямой, необходимо и достаточно, чтобы K было коммутативно. [«Теорема Паппа»; свести к случаю, когда q и r находятся на бесконечно удаленной прямой аффинной плоскости.] Применить эту теорему к проективному пространству прямых пространства $\mathbf{P}(V)$ (упражнение 5).

9) Пусть s, a, b, c, a', b', c' — семь различных точек проективной плоскости над телом K, содержащим не менее трех элементов, причем s, a, b, c и s, a', b', c' — проективные реперы, а прямые D_{sa}, D_{sb}, D_{sc} проходят соответственно через a', b', c'. Показать, что точки пересечения r, p, q прямых D_{ab} и $D_{a'b'}$, D_{bc} и $D_{b'c'}$, D_{ca} и $D_{c'a'}$ лежат на одной прямой. [«Теорема Дезарга»; метод, аналогичный методу упражнения 8.]

*10) Пусть $E=\mathbf{P}(V)$ и $E'=\mathbf{P}(V')$ — проективные пространства одинаковой конечной размерности $n \geqslant 2$ соответственно над телами K и K' и u — биективное отображение E на E', преобразующее любые три точки, лежащие на одной прямой, в три точки, лежащие на одной прямой. Показать, что существуют изоморфизм σ тела K на K' и биективное полулинейное (относительно σ) отображение v пространства V на V' такие, что u есть отображение, порождаемое отображением v при факторизации. [Использовать упражнение 7 Приложения II.] Если $V'=V$ и K коммутативно, то для того, чтобы u было проективным отображением, необходимо и достаточно, чтобы для каждой четверки (a, b, c, d) различных точек пространства $\mathbf{P}(V)$, лежащих на одной прямой, выполнялось равенство $\begin{bmatrix} u(a) & u(b) \\ u(d) & u(c) \end{bmatrix} = \begin{bmatrix} a & b \\ d & c \end{bmatrix}$.

11) Пусть V — векторное пространство конечной размерности n над телом K, $(e_i)_{1 \leqslant i \leqslant n}$ — базис этого пространства, K' — подтело тела K и V' — n-мерное векторное пространство над K, порожденное элементами e_i. Дать пример инъективного отображения V' в V, преобразующего любые три точки, лежащие на одной прямой, в три точки, лежащие на одной прямой, но не обязательно преобразующего две параллельные прямые в множества, содержащиеся в двух параллельных прямых. [Погрузить V в канонически ассоциированное с ним проективное пространство E и рассмотреть проективное отображение u последнего на себя такое, что прообраз относительно u бесконечно удаленной гиперплоскости отличен от нее и не содержит ни одной точки из V'; можно было бы, например, взять бесконечное K и конечное K'.]

*12) Пусть $E=\mathbf{P}(V)$ — проективная плоскость над телом K и u — биективное отображение E на себя, получающееся путем факторизации из некоторого биективного отображения v пространства V на себя, полулинейного относительно автоморфизма σ тела K.

а) Показать равносильность следующих четырех свойств: α) каково бы ни было $x \in E$, x, $u(x)$ и $u^2(x)$ лежат на одной прямой; β) каждая прямая на E содержит точку, инвариантную относительно u; γ) через

каждую точку из E проходит прямая, инвариантная относительно u; δ) какова бы ни была прямая D на E, прямые D, $u(D)$ и $u^2(D)$ имеют общую точку. [Доказать сначала равносильность α) и γ); вывести отсюда по двойственности (упражнение 5) равносильность β) и δ); наконец, показать, что γ) влечет β), и вывести отсюда по двойственности, что β) влечет γ).]

б) Пусть u обладает свойствами, сформулированными в а). Показать, что если на E имеется прямая D, содержащая лишь одну точку a, инвариантную относительно u, то u получается путем факторизации из некоторого сдвига v пространства V (§ 6, упражнение 7). [Показать, что каждая прямая, инвариантная относительно u, проходит через a; рассматривая прямую, не проходящую через a, показать, что существует прямая D_0, проходящая через a и содержащая по крайней мере две точки, инвариантные относительно u; заключить, что все точки прямой D_0 необходимо инвариантны относительно u.]

в) Пусть u обладает свойствами, сформулированными в а), и на E не существует прямой, которая содержала бы только одну точку, инвариантную относительно u. Показать, что если на E имеется прямая D, содержащая лишь две точки, инвариантные относительно u, то u получается путем факторизации из некоторого растяжения v пространства V (§ 6, упражнение 7). [Показать, что если a и b — те две точки прямой D, которые инвариантны относительно u, то каждая прямая, инвариантная относительно u, проходит через a или b; заметить далее, что существуют по крайней мере две другие точки c, d, отличные от a и b, инвариантные относительно u, и, следовательно, что прямая D_{cd} проходит через a или b; в заключение доказать, что все точки прямой D_{cd} инвариантны относительно u.]

г) Пусть u обладает свойствами, сформулированными в а), и каждая прямая на E содержит по крайней мере три различные точки, инвариантные относительно u; тогда в E существует проективный репер S (упражнение 3), каждая точка которого инвариантна относительно u; заключить отсюда, что в V существует базис $(e_i)_{1\leqslant i\leqslant 3}$ такой, что u получается путем факторизации из полулинейного отображения v пространства V на себя, для которого $v(e_i)=e_i$ $(1 \leqslant i \leqslant 3)$. Множеством точек из E, инвариантных относительно u, является тогда проективная плоскость $\mathrm{P}(V_0)$, где V_0 — векторное пространство над телом K_σ инвариантов относительно σ, порожденное элементами e_1, e_2, e_3.

д) Пусть теперь u удовлетворяет условиям пунктов а) и г) и ни u, ни u^2 не есть тождественное отображение. Доказать существование $\gamma \in K$ такого, что $\gamma^\sigma=\gamma$ и

$$(\xi^\sigma-\xi)^\sigma=\gamma(\xi^\sigma-\xi) \tag{1}$$

для каждого $\xi \in K$. [Воспользоваться условием α) пункта а) и существованием $\xi \in K$, для которого $\zeta^\sigma \neq \zeta$.] Показать, что $\gamma=-1$.

поскольку

$$(1+\gamma)\,\xi^{\sigma}\gamma = \gamma\xi\,(1+\gamma) \tag{2}$$

для каждого $\xi \in K$ с $\xi^{\sigma} \neq \xi$. [Применить (1), заменив ξ на ξ^2.] Заметив, что $\xi = \eta - \zeta$, где $\eta^{\sigma} \neq \eta$ и $\zeta^{\sigma} \neq \zeta$, распространить (2) на все $\xi \in K$. Заключить отсюда, что $\gamma \neq 1$, и далее вывести из (1) и (2), что

$$\xi^{\sigma} = (1+\gamma)\,\xi\,(1+\gamma)^{-1} \tag{3}$$

для всех $\xi \in K$, и что $\gamma + \gamma^{-1}$ принадлежит центру тела K. Обращение. Привести пример, где γ не принадлежит центру тела K, а $\gamma + \gamma^{-1}$ принадлежит.

ГЛАВА III

ПОЛИЛИНЕЙНАЯ АЛГЕБРА

Там, где не оговорено противное, все кольца операторов, рассматриваемые в этой главе (за исключением Приложений), предполагаются коммутативными и имеющими единицу, а все модули над этими кольцами — унитарными. Всякие дополнительные предположения явно отмечаются в своем месте, а если они относятся ко всему параграфу — в его начале.

§ 1. Тензорные произведения модулей

1. *Билинейные функции*

Определение 1. *Пусть A — коммутативное кольцо с единицей и E, F, G — унитарные A-модули. Отображение f произведения $E \times F$ в G называют билинейным, если для каждого $y \in F$ частичное отображение $x \to f(x, y)$ есть линейное отображение E в G и для каждого $x \in E$ частичное отображение $y \to f(x, y)$ — линейное отображение F в G.*

Иными словами, f должно удовлетворять следующим тождествам:

$$\left.\begin{aligned} f(x,\ y+y') &= f(x,\ y)+f(x,\ y'),\\ f(x+x',\ y) &= f(x,\ y)+f(x',\ y), \end{aligned}\right\} \tag{1}$$

$$f(\alpha x,\ y) = f(x,\ \alpha y) = \alpha f(x,\ y) \tag{2}$$

для всех $\alpha \in A$, $x \in E$, $x' \in E$, $y \in F$, $y' \in F$.

Примеры. Отображение $(x,\ y) \to xy$ произведения $A \times A$ в A билинейно; то же верно в случае, когда E — *алгебра* (гл. II, § 7) над A, для отображения $(x, y) \to xy$ произведения $E \times E$ в E. Каков бы

ни был унитарный A-модуль F, $(\alpha, x) \mapsto \alpha x$ есть билинейное отображение $A \times F$ в F.

Из определения 1, в частности, вытекает, что $f(0, y) = f(x, 0) = 0$ для всех $x \in E$ и $y \in F$.

Если $x = \sum_{\lambda} \xi_\lambda a_\lambda$, $y = \sum_{\mu} \eta_\mu b_\mu$, то (как устанавливается индукцией по числу ненулевых коэффициентов ξ_λ, η_μ)

$$f(x, y) = \sum'_{\lambda, \mu} \xi_\lambda \eta_\mu f(a_\lambda, b_\mu).$$

В частности, если (a_λ) — *базис* модуля E, (b_μ) — *базис* модуля F, то для любого заданного семейства $(c_{\lambda\mu})$ элементов из G существует, и притом единственное, билинейное отображение f произведения $E \times F$ в G такое, что $f(a_\lambda, b_\mu) = c_{\lambda\mu}$ для каждой пары индексов (λ, μ).

Ясно, что если f и g — билинейные отображения $E \times F$ в G, то $f + g$ и αf $(\alpha \in A)$ — тоже билинейные отображения $E \times F$ в G; иными словами, билинейные отображения $E \times F$ в G образуют A-*модуль*; мы будем обозначать его $\mathscr{L}(E, F; G)$ или $\mathscr{L}_2(E; G)$, если $F = E$. Из предыдущего следует, что если $(a_\lambda)_{\lambda \in L}$ и $(b_\mu)_{\mu \in M}$ — базисы модулей E и F, то A-модуль $\mathscr{L}(E, F; G)$ *изоморфен произведению* $G^{L \times M}$.

Предложение 1. *Модуль $\mathscr{L}(E, F; G)$ билинейных отображений $E \times F$ в G изоморфен модулю $\mathscr{L}(E, \mathscr{L}(F, G))$ линейных отображений модуля E в модуль линейных отображений F в G (а также аналогичному модулю $\mathscr{L}(F, \mathscr{L}(E, G))$).*

Действительно, $y \to u(x, y)$ для каждого $u \in \mathscr{L}(E, F; G)$ и каждого $x \in E$ есть линейное отображение F в G; если обозначить его u_x, то $x \to u_x$ будет линейным отображением E в $\mathscr{L}(F, G)$. Обратно, каково бы ни было линейное отображение $x \to f_x$ модуля E в $\mathscr{L}(F, G)$, $(x, y) \to f_x(y)$ есть билинейное отображение $E \times F$ в G, и, обозначая его u, имеем $u_x = f_x$ для каждого $x \in E$. Ясно, что этим определены изоморфизм $\mathscr{L}(E, F; G)$ на $\mathscr{L}(E, \mathscr{L}(F, G))$ и изоморфизм, ему обратный; эти изоморфизмы будут называться *каноническими*.

Определение 2. *Каждое билинейное отображение произведения $E \times F$ унитарных A-модулей E, F в кольцо A (рассматриваемое как A-модуль) называется билинейной формой на $E \times F$.*

Согласно предыдущему, билинейные формы на $E \times F$ образуют A-модуль $\mathscr{L}(E, F; A)$; причем, если E обладает базисом $(a_\lambda)_{\lambda \in L}$ и F — базисом $(b_\mu)_{\mu \in M}$, то этот модуль изоморфен $A^{L \times M}$. Кроме того, из предложения 1 вытекает:

Предложение 2. *Модуль билинейных форм на $E \times F$ изоморфен модулям $\mathscr{L}(E, F^*)$ и $\mathscr{L}(F, E^*)$* (где E^* и F^* означают модули, *сопряженные* соответственно к E и F).

Следствие. *Пусть u — билинейная форма на $E \times F$; если E и F обладают конечными базисами $(a_i)_{1 \leqslant i \leqslant n}$ и $(b_i)_{1 \leqslant i \leqslant n}$, состоящими из одинакового числа элементов и такими, что $u(a_i, b_j) = \delta_{ij}$* (где δ_{ij} — кронекеровский символ) *для каждой пары индексов (i, j), то u канонически соответствует некоторому изоморфизму E на F^* и некоторому изоморфизму F на E^*.*

Действительно, тогда линейное отображение $x \to u_x$ модуля E в F^*, канонически соответствующее u, таково, что $u_{a_i} = b'_i$ $(1 \leqslant i \leqslant n)$, где (b'_i) — *сопряженный к (b_i) базис* модуля F^* (гл. II, § 4, n° 4).

2. Тензорное произведение двух модулей

Мы увидим, что понятие *билинейного* отображения можно с помощью понятия *тензорного произведения* свести к понятию *линейного* отображения.

Покажем, что для заданных унитарных A-модулей E и F существуют A-модуль M и билинейное отображение φ произведения $E \times F$ в M такие, что, каково бы ни было билинейное отображение f произведения $E \times F$ в *произвольный* A-модуль N, существует *линейное* отображение g модуля M в N, удовлетворяющее соотношению $f = g \circ \varphi$.

Заметим прежде всего, что если M обладает этим свойством, то им обладает также подмодуль M_1 в M, *порожденный* множеством $\varphi(E \times F)$ (для чего нужно только рассмотреть сужение g на M_1); поэтому достаточно ограничиться тем случаем, когда дополнительно требуется, чтобы M *порождалось* множеством $\varphi(E \times F)$, т. е. совпадало с множеством всевозможных *линейных комбинаций*

(гл. II, § 1, n° 5) элементов из $\varphi(E \times F)$; в этом случае линейное отображение g, для которого $f = g \circ \varphi$, *однозначно* определяется билинейным отображением f. Покажем, что если такой модуль M существует, то он определен с точностью до изоморфизма *однозначно*; говоря точно, имеет место

Предложение 3. *Пусть M_i $(i = 1, 2)$ — два A-модуля и φ_i для каждого i — билинейное отображение $E \times F$ в M_i, обладающее следующими свойствами*: 1° *M_i порождается множеством $\varphi_i(E \times F)$*; 2° *для каждого билинейного отображения f произведения $E \times F$ в произвольный A-модуль N существует линейное отображение g_i модуля M_i в N такое, что $f = g_i \circ \varphi_i$. При этих условиях существует изоморфизм u модуля M_1 на M_2 такой, что $\varphi_2 = u \circ \varphi_1$.*

Действительно, беря в качестве N модуль M_2, видим, что существует линейное отображение h_1 модуля M_1 в M_2 такое, что $\varphi_2 = h_1 \circ \varphi_1$; и точно так же существует линейное отображение h_2 модуля M_2 в M_1 такое, что $\varphi_1 = h_2 \circ \varphi_2$; отсюда $\varphi_1 = (h_2 \circ h_1) \circ \varphi_1$, где $h_2 \circ h_1$ — линейное отображение M_1 в себя; но так как $\varphi_1(E \times F)$ порождает M_1, то из последнего соотношения вытекает, что $z = h_2(h_1(z))$ для каждого $z \in M_1$; иными словами, $h_2 \circ h_1$ есть *тождественное* отображение M_1 на себя; совершенно так же $h_1 \circ h_2$ есть тождественное отображение M_2 на себя; следовательно (Теор. мн., Рез., § 2, n° 12), h_1 есть взаимно однозначное отображение M_1 на M_2, а h_2 — обратное ему отображение.

Покажем теперь, что модуль M, удовлетворяющий требуемым условиям, действительно существует. Рассмотрим A-модуль $G = A^{(E \times F)}$ *формальных линейных комбинаций* (с коэффициентами из A) элементов множества $E \times F$ (гл. II, § 1, n° 8); как мы знаем, канонический базис этого модуля можно отождествить с множеством $E \times F$ так, что каждый элемент из G будет однозначно представляться в виде $\sum_{(x, y) \in E \times F} \alpha_{x, y}(x, y)$ (где $\alpha_{x, y}$ принадлежат A и равны нулю для всех кроме конечного числа пар (x, y)).

Пусть теперь N — *произвольный* A-модуль; как мы знаем (гл. II, § 2, n° 4), *каждое* отображение f множества $E \times F$ в N может быть, и притом единственным образом, продолжено до *линейного* отображения $\bar{f}$ модуля G в N, а именно определяемого

формулой

$$\bar{f}\left(\sum_{x,\,y} \alpha_{x,\,y}\,(x,\,y)\right) = \sum_{x,\,y} \alpha_{x,\,y}\, f\,(x,\,y).$$

Отображение $f \to \bar{f}$ есть изоморфизм модуля $N^{E\times F}$ всех отображений $E \times F$ в N *на* модуль $\mathscr{L}\,(G, N)$ линейных отображений G в N. Охарактеризуем линейные отображения $\bar{f}$, соответствующие *билинейным* отображениям f произведения $E \times F$ в N; условия (1) и (2) означают, что линейная функция $\bar{f}$ обращается в *нуль* на всех элементах из G видов

$$(x,\ y+y') - (x,\ y) - (x,\ y'), \quad (x+x',\ y) - (x,\ y) - (x',\ y),$$
$$(\alpha x,\ y) - \alpha\,(x,\ y), \quad (x,\ \alpha y) - (x,\ y).$$

В силу своей линейности, $\bar{f}$ равна нулю также для всех элементов *подмодуля* H в G, *порожденного* элементами указанных видов, причем этот подмодуль *не зависит* от N; допуская вольность речи, мы будем называть H *подмодулем в* G, *на котором аннулируются все билинейные функции*. Итак, образом модуля $\mathscr{L}\,(E, F; N)$ билинейных отображений $E \times F$ в N при изоморфизме $f \to \bar{f}$ служит подмодуль в $\mathscr{L}\,(G, N)$, образованный теми линейными отображениями G в N, которые *аннулируются на* H. Но тогда (гл. II, § 2, предложение 1) $g \to g \circ \theta$, где θ — каноническое отображение G на G/H, есть *изоморфизм* $\mathscr{L}(G/H, N)$ *на* подмодуль в $\mathscr{L}(G, N)$, образованный линейными отображениями, аннулирующимися на H. Таким образом, обозначая через φ сужение θ на $E \times F$, видим, что каждое билинейное отображение $E \times F$ в N однозначно представляется в виде $g \circ \varphi$, где g — *линейное* отображение G/H в N, причем $g \to g \circ \varphi$ есть *изоморфизм* $\mathscr{L}(G/H, N)$ *на* $\mathscr{L}(E, F; N)$ (который, как и обратный ему изоморфизм, мы будем называть *каноническим*).

Так как φ — *билинейное* отображение $E \times F$ в G/H, а $\varphi\,(E \times F)$ *порождает* G/H, то модуль $M = G/H$ и отображение φ удовлетворяют всем условиям предложения 3. Для каждой пары $(x, y) \in E \times F$ мы положим отныне $\varphi\,(x, y) = x \otimes y$ (вместо чего будем иногда допускать также запись xy, если это не сможет вызвать путаницу).

Определение 3. *Пусть* E *и* F — *А-модули. А-модуль* G/H (фактормодуль модуля G формальных линейных комбинаций элементов произведения $E \times F$ по подмодулю H, на котором

аннулируются все билинейные функции) *называется тензорным произведением модулей E и F и обозначается $E \otimes F$.*

Допуская вольность речи, мы будем каждый элемент из $E \otimes F$ вида $x \otimes y$ называть *тензорным произведением* x и y. Имеем тождественно

$$(x + x') \otimes y = x \otimes y + x' \otimes y, \quad x \otimes (y + y') = x \otimes y + x \otimes y', \tag{3}$$

$$(ax) \otimes y = x \otimes (ay) = a(x \otimes y) \tag{4}$$

и, в частности, $x \otimes 0 = 0 \otimes y = 0$, каковы бы ни были $x \in E$ и $y \in F$.

Любой элемент из $E \otimes F$ может быть (в силу (4)) представлен в виде $\sum_i (x_i \otimes y_i)$ и, значит, является суммой конечного числа тензорных произведений элементов из E и F; но, как показывают тождества (3) и (4), элемент из $E \otimes F$ представим в таком виде вообще *различными способами.*

Замечания. 1) Пусть E и F — коммутативные группы без операторов; их всегда можно рассматривать как *модули* над кольцом $\mathbf{Z}$ рациональных целых чисел (гл. II, § 1, n° 1); под тензорным произведением $E \otimes F$ двух таких групп всегда понимается произведение их структур $\mathbf{Z}$-модулей.

2) Тензорное произведение двух модулей, не сводящихся к 0, может сводиться к 0. Например, для $\mathbf{Z}$-модулей $E = \mathbf{Z}/(2)$ и $F = \mathbf{Z}/(3)$ имеем $2x = 0$ и $3y = 0$, каковы бы ни были $x \in E$ и $y \in F$; следовательно,

$$x \otimes y = 3(x \otimes y) - 2(x \otimes y) = (x \otimes (3y)) - ((2x) \otimes y) = 0$$

для всех $x \in E$ и $y \in F$.

В связи с этим примером см. ниже следствие предложения 6.

3) Заметим, что отображение $(x, y) \to x \otimes y$ произведения $E \times F$ в $E \otimes F$ вообще *не взаимно однозначно*, поскольку для $x \neq 0$ имеем $x \otimes 0 = 0 \otimes 0 = 0$; поэтому $E \times F$ нельзя рассматривать как часть $E \otimes F$.

Резюмируем основные свойства тензорного произведения $E \otimes F$:

Схолия. *Линейные отображения $E \otimes F$ в произвольный A-модуль N связаны с билинейными отображениями $E \times F$ в N следующим взаимно однозначным соответствием: линейное отображение f модуля $E \otimes F$ в N определено, если известно его значение $f(x \otimes y)$ для каждой пары $(x, y) \in E \times F$ и отображение $(x, y) \to f(x \otimes y)$ билинейно. Обратно, для определения линейного отображения*

$E \otimes F$ в N достаточно задать отображение $(x, y) \to g(x, y)$ произведения $E \times F$ в N, проверив его билинейность; тогда существует, и притом единственное, линейное отображение f модуля $E \otimes F$ в N такое, что $f(x \otimes y) = g(x, y)$ для всех $(x, y) \in E \times F$.

В частности, *невачем* проверять, что $\sum_i (x_i \otimes y_i) = \sum_k (x'_k \otimes y'_k)$ влечет $\sum_i g(x_i, y_i) = \sum_k g(x'_k, y'_k)$; это есть следствие определения тензорного произведения и предположенной билинейности g.

Для дальнейших приложений (§ 3) будет полезно вывести из предыдущего следующее правило определения *билинейного* отображения произведения $G_1 \times G_2$ тензорных произведений $G_1 = E_1 \otimes F_1$ и $G_2 = E_2 \otimes F_2$ в модуль N: достаточно задаться отображением g произведения $E_1 \times F_1 \times E_2 \times F_2$ в N таким, что каждое из частичных отображений $(x_1, y_1) \to g(x_1, y_1, x_2, y_2)$ и $(x_2, y_2) \to$ $\to g(x_1, y_1, x_2, y_2)$ *билинейно*; тогда существует однозначно определенное билинейное отображение f произведения $G_1 \times G_2$ в N такое, что тождественно $f(x_1 \otimes y_1, x_2 \otimes y_2) = g(x_1, y_1, x_2, y_2)$. Действительно, для каждой пары (x_2, y_2) существует линейное отображение u_{x_2, y_2} тензорного произведения G_1 в N такое, что $u_{x_2, y_2}(x_1 \otimes y_1) =$ $= g(x_1, y_1, x_2, y_2)$, и отображение $(x_2, y_2) \to u_{x_2, y_2}$ произведения $E_2 \times F_2$ в $\mathscr{L}(G_1, N)$ билинейно; поэтому существует линейное отображение v тензорного произведения G_2 в $\mathscr{L}(G_1, N)$ такое, что $v(x_2 \otimes y_2) = u_{x_2, y_2}$, и справедливость утверждения сразу следует из предложения 1.

3. Свойства тензорных произведений

Предложение 4. *Тензорные произведения $E \otimes F$ и $F \otimes E$ изоморфны* («коммутативность» тензорного произведения).

Действительно, так как $(x, y) \to y \otimes x$ есть билинейное отображение $E \times F$ в $F \otimes E$, то (n° 2, схолия), положив $u(x \otimes y) = y \otimes x$, мы определим линейное отображение u модуля $E \otimes F$ в $F \otimes E$; точно так же, положив $v(y \otimes x) = x \otimes y$, мы определим линейное отображение v модуля $F \otimes E$ в $E \otimes F$; так как $u \circ v$ и $v \circ u$ — соответственно тождественные отображения $F \otimes E$ и $E \otimes F$ в себя, то u и v — взаимно обратные изоморфизмы (Теор. мн., Рез., § 2, n° 12) (которые будут называться *каноническими*).

Предложение 5. *Для каждого унитарного A-модуля E тензорное произведение $A\otimes E$ изоморфно E.*

Действительно, отображения $u(\alpha\otimes x)=\alpha x$ и $v(x)=\varepsilon\otimes x$ (где ε — единица кольца A) определяют линейные отображения u модуля $A\otimes E$ в E и v модуля E в $A\otimes E$; очевидно, $u\circ v$ есть тождественное отображение E на себя, а $v\circ u$, в силу соотношения $\varepsilon\otimes(\alpha x)=\alpha\otimes x$, — тождественное отображение $A\otimes E$ на себя; следовательно, u и v — взаимно обратные изоморфизмы (которые будут называться *каноническими*).

Следствие. *Тензорное произведение $A\otimes A$ A-модуля A на себя изоморфно A.*

Таким образом, канонический изоморфизм $A\otimes A$ на A относит элементу $\alpha\otimes\beta$ произведение $\alpha\beta$ в A.

Предложение 6. *Пусть M — подмодуль модуля E и N — подмодуль модуля F. Тензорное произведение $(E/M)\otimes(F/N)$ изоморфно фактормодулю $(E\otimes F)/\Gamma(M, N)$, где $\Gamma(M, N)$ — подмодуль в $E\otimes F$, порожденный элементами $x\otimes y$ с $x\in M$ или $y\in N$.*

Применим критерий предложения 3. Обозначим соответственно через $x\to\bar{x}$ и $y\to\bar{y}$ канонические отображения E на E/M и F на F/N, а через ω — каноническое отображение $E\otimes F$ на $S=(E\otimes F)/\Gamma(M, N)$. Тогда $(x, y)\to\omega(x\otimes y)$ есть билинейное отображение $E\times F$ в S, аннулирующееся, в силу определения ω и $\Gamma(M, N)$, как для $x\equiv 0\pmod M$, так и для $y\equiv 0\pmod N$; это показывает, что $\omega(x\otimes y)$ зависит лишь от класса $\bar{x}$ элемента $x\pmod M$ и класса $\bar{y}$ элемента $y\pmod N$, так что можно написать $\omega(x\otimes y)=u(\bar{x}, \bar{y})$. Отображение u произведения $R=(E/M)\times(F/N)$ в S билинейно, и ясно, что элементы вида $u(\bar{x}, \bar{y})$ порождают S.

Пусть теперь f — билинейное отображение произведения R в произвольный A-модуль Q. Для любых $x\in E$, $y\in F$ положим $f_1(x, y)=f(\bar{x}, \bar{y})$; так как f_1 — билинейное отображение $E\times F$ в Q, то существует линейное отображение g_1 модуля $E\otimes F$ в Q, такое, что $g_1(x\otimes y)=f_1(x, y)=f(\bar{x}, \bar{y})$; тогда $g_1(x\otimes y)$ аннулируется как для $x\equiv 0\pmod M$, так и для $y\equiv 0\pmod N$ и, значит, g_1 аннулируется на $\Gamma(M, N)$; отсюда вытекает (гл. II, § 2, предложение 1), что

$g_1 = g \circ \omega$, где g — линейное отображение S в Q. Поэтому $f(\overline{x}, \overline{y}) = g(\omega(x \otimes y)) = g(u(\overline{x}, \overline{y}))$, т. е. $f = g \circ u$. В силу предложения 3, примененного к модулям E/M, F/N, S и отображению u, модуль S изоморфен $(E/M) \otimes (F/N)$; изоморфизм S на $(E/M) \otimes (F/N)$, определяемый отображением предложения 3, относит классу $x \otimes y$ по модулю $\Gamma(M, N)$ тензорное произведение $\overline{x} \otimes \overline{y}$; мы будем называть этот изоморфизм и изоморфизм, обратный ему, *каноническими*.

Следствие. *Пусть* $\mathfrak{a}$ *и* $\mathfrak{b}$ — *любые два идеала кольца* A; *тензорное произведение моногенных модулей* $A/\mathfrak{a}$ *и* $A/\mathfrak{b}$ *изоморфно моногенному модулю* $A/(\mathfrak{a} + \mathfrak{b})$.

Действительно, при каноническом отождествлении модулей $A \otimes A$ и A (следствие предложения 5) подмодуль $\Gamma(\mathfrak{a}, \mathfrak{b})$ модуля $A \otimes A$ отождествляется с идеалом $\mathfrak{a} + \mathfrak{b}$, откуда и следует справедливость утверждения.

Пусть M — произвольный подмодуль модуля E, N — произвольный подмодуль модуля F, φ — каноническое отображение M в E и ψ — каноническое отображение N в F. Отображение $(x, y) \to \varphi(x) \otimes \psi(y)$ произведения $M \times N$ в $E \otimes F$, будучи билинейным, определяет (называемое *каноническим*) линейное отображение θ модуля $M \otimes N$ в $E \otimes F$ (такое, что $\theta(x \otimes y) = \varphi(x) \otimes \psi(y)$); образ $\theta(M \otimes N)$ модуля $M \otimes N$ при этом отображении есть подмодуль в $E \otimes F$, порожденный элементами $\varphi(x) \otimes \psi(y)$, где x пробегает M и y пробегает N; по вообще θ *не есть изоморфизм* $M \otimes N$ в $E \otimes F$ (см. упражнение 1), что тем самым не позволяет отождествлять $M \otimes N$ с $\theta(M \otimes N)$. Однако справедливо следующее предложение:

Предложение 7. *Пусть* E *и* F — A-*модули, являющиеся прямыми суммами семейств* (E_λ) *и* (F_μ) *своих подмодулей. Каноническое отображение* $E_\lambda \otimes F_\mu$ *в* $E \otimes F$ *для каждой пары индексов* (λ, μ) *есть изоморфизм на некоторый подмодуль* $G_{\lambda\mu}$ *модуля* $E \otimes F$, *и* $E \otimes F$ *есть прямая сумма подмодулей* $G_{\lambda\mu}$.

Пусть G — *прямая сумма* семейства A-модулей $(E_\lambda \otimes F_\mu)$ (гл. II, § 1, n° 7); мы определим билинейное отображение u произведения $E \times F$ в G, удовлетворяющее условиям предложения 3, откуда будет следовать, что G изоморфно $E \otimes F$. Для каждого

элемента $x = \sum_{\lambda} x_\lambda$ из E, где $x_\lambda \in E_\lambda$, и каждого элемента $y = \sum_{\mu} y_\mu$ из F, где $y_\mu \in F_\mu$, положим $u(x, y) = \sum_{\lambda, \mu} (x_\lambda \otimes y_\mu)$; ясно, что u — билинейное отображение и $u(E \times F)$ порождает G. Пусть теперь N — произвольный A-модуль и f — билинейное отображение $E \times F$ в N; пусть, далее, $f_{\lambda\mu}$ для любой пары (λ, μ) — сужение f на произведение $E_\lambda \times F_\mu$. Так как $f_{\lambda\mu}$ билинейно, то существует линейное отображение $g_{\lambda\mu}$ модуля $E_\lambda \otimes F_\mu$ в N такое, что $f_{\lambda\mu}(x_\lambda, y_\mu) = g_{\lambda\mu}(x_\lambda \otimes y_\mu)$ для всех $x_\lambda \in E_\lambda$, $y_\mu \in F_\mu$; с другой стороны, для $x = \sum_{\lambda} x_\lambda \in E$ и $y = \sum_{\mu} y_\mu \in F$ имеем $f(x, y) = \sum_{\lambda, \mu} f(x_\lambda, y_\mu) = \sum_{\lambda, \mu} f_{\lambda\mu}(x_\lambda, y_\mu) = \sum_{\lambda, \mu} g_{\lambda\mu}(x_\lambda \otimes y_\mu)$; поэтому, обозначая через g линейное отображение G в N, сужение которого на $E_\lambda \otimes F_\mu$ для каждой пары (λ, μ) равно $g_{\lambda\mu}$ (гл. II, § 2; предложение 3), имеем $f(x, y) = g\left(\sum_{\lambda, \mu} (x_\lambda \otimes y_\mu)\right) = g(u(x, y))$, или $f = g \circ u$. Следовательно, модули $E \otimes F$ и G изоморфны; изоморфизм v модуля $E \otimes F$ на G, определяемый отображением предложения 3, относит тензорному произведению $x \otimes y$ элементов $x = \sum_{\lambda} x_\lambda$ и $y = \sum_{\mu} y_\mu$ элемент $\sum_{\lambda, \mu} (x_\lambda \otimes y_\mu)$ из G, где каждое тензорное произведение $x_\lambda \otimes y_\mu$ берется *в модуле* $E_\lambda \otimes F_\mu$; ясно, что сужение v на $G_{\lambda\mu}$ есть изоморфизм $G_{\lambda\mu}$ на $E_\lambda \otimes F_\mu$, обратным к которому служит канонический изоморфизм $E_\lambda \otimes F_\mu$ в $E \otimes F$.

При выполнении условий предложения 7 модули $G_{\lambda\mu}$ и $E_\lambda \otimes F_\mu$ посредством изоморфизма v *отождествляются*.

Следствие 1. *Если F обладает базисом $(b_\mu)_{\mu \in M}$, то модуль $E \otimes F$ изоморфен модулю $E^{(M)}$ и каждый элемент из $E \otimes F$ может быть, и притом единственным образом, представлен в виде $\sum_{\mu} (x_\mu \otimes b_\mu)$, где $x_\mu \in E$.*

Действительно, при указанном отождествлении $E \otimes F$ есть прямая сумма подмодулей $E \otimes (A b_\mu)$; так как $\xi \to \xi b_\mu$ есть изоморфизм A на $A b_\mu$, то из предложения 5 вытекает, что $x \to x \otimes b_\mu$ есть изоморфизм E на $E \otimes (A b_\mu)$, чем утверждение и доказано.

Следствие 2. *Если* (a_λ) *— базис модуля* E *и* (b_μ) *— базис модуля* F, *то элементы* $a_\lambda \otimes b_\mu$ *образуют базис модуля* $E \otimes F$.

Допуская вольность речи, мы будем называть базис $(a_\lambda \otimes b_\mu)$ *тензорным произведением* базисов (a_λ) и (b_μ).

Мы видим, что если E и F — *векторные пространства* над полем K, а x и y — ненулевые элементы из E и F, то $x \otimes y \neq 0$; действительно, в E существует базис, содержащий x, и в F — базис, содержащий y.

Следствие 2 показывает также, что если E и F — *конечномерные векторные пространства* над полем K, то и $E \otimes F$ — конечномерное векторное пространство над K, причем

$$\dim (E \otimes F) = \dim E \dim F. \tag{5}$$

Следствие 3. *Пусть* E *и* F — A*-модули, а* M *и* N — *их подмодули. Если* M *обладает дополнением в* E *и* N — *дополнением в* F, *то каноническое отображение* $M \otimes N$ *в* $E \otimes F$ *есть изоморфизм и образ* $M \otimes N$ *при этом изоморфизме обладает дополнением в* $E \otimes F$.

В этом случае (всегда реализующемся, когда E и F — *векторные пространства* (гл. II, § 3, предложение 5)) модуль $M \otimes N$ *отождествляется* с его каноническим образом в $E \otimes F$.

То, что для подмодуля M модуля E и подмодуля N модуля F каноническое отображение $M \otimes N$ в $E \otimes F$ не обязательно является изоморфизмом, можно также выразить следующим образом: если $(x_i)_{1 \leqslant i \leqslant n}$ и $(y_i)_{1 \leqslant i \leqslant n}$ — конечные последовательности элементов из E и F, для которых $\sum_i (x_i \otimes y_i) = 0$ *в* $E \otimes F$, а M и N — подмодули в E и F, *порожденные* соответственно элементами x_i и y_i, то $\sum_i (x_i \otimes y_i)$ не обязательно $= 0$ *в* $M \otimes N$. Отметим, однако, следующее предложение:

Предложение 8. *Пусть* $(x_i)_{1 \leqslant i \leqslant n}$ *и* $(y_i)_{1 \leqslant i \leqslant n}$ — *семейства элементов из* E *и* F, *для которых* $\sum_i (x_i \otimes y_i) = 0$ *в* $E \otimes F$. *Тогда существуют подмодуль* E_1 *в* E, *содержащий все* x_i, *и подмодуль* F_1 *в* F, *содержащий все* y_i, *имеющие конечное число образующих и такие, что* $\sum_i (x_i \otimes y_i) = 0$ *в* $E_1 \otimes F_1$.

Действительно, по предположению, в модуле $G = A^{(E\times F)}$ формальных линейных комбинаций элементов из $E \times F$ элемент $\sum_i (x_i, y_i)$ принадлежит подмодулю H, на котором аннулируются все билинейные функции (n° 2). Значит, согласно определению H, $\sum_i (x_i, y_i)$ можно представить в виде линейной комбинации конечного числа элементов $z_\nu \in G$ видов

$$(u, v+v') - (u, v) - (u, v'),$$

$$(u+u', v) - (u, v) - (u', v),$$

$$(\alpha u, v) - \alpha\,(u, v), \quad (u, \alpha v) - \alpha\,(u, v).$$

Пусть тогда E_1 (соответственно F_1) — подмодуль модуля E (соответственно F), порожденный элементами x_i (соответственно y_i) и всеми элементами из E (соответственно F), фигурирующими в упомянутых выражениях для элементов z_ν. Модуль $G_1 = A^{(E_1\times F_1)}$ можно считать подмодулем в G; тогда подмодуль H_1 в G_1, на котором аннулируются все билинейные функции, определенные на $E_1 \times F_1$, будет подмодулем в $H \cap G_1$, содержащим все z_ν, а, значит, также $\sum_i (x_i, y_i)$, чем предложение и доказано.

Замечание. Пусть B — подкольцо кольца A, имеющее тот же единичный элемент, что и A, и пусть E и F — A-модули. Сузив области операторов внешних законов этих модулей до кольца B, мы определим в множествах E и F структуры B-модуля; пусть E_B и F_B — определенные так B-модули. Тогда можно рассматривать, с одной стороны, B-модуль $E_B \otimes F_B$, а с другой — B-модуль, полученный путем сужения области операторов A-модуля $E \otimes F$ до B; вообще эти два модуля *не изоморфны*. Например, пусть A — поле и B — его подполе, степень $[A : B]$ которого есть конечное число m; так как векторное пространство $A \otimes A$ над A изоморфно A, то при сужении области операторов до B мы получим m-мерное векторное пространство над B; напротив, согласно формуле (5), $A_B \otimes A_B$ будет иметь относительно B размерность m^2.

Таким образом, говорить о тензорном произведении двух модулей не имеет смысла до тех пор, пока не указано кольцо операторов, относительно которого это произведение берется; явное указание этого кольца будет опускаться, лишь когда контекст не будет оставлять никакого места сомнениям насчет него.

4. Тензорное произведение линейных отображений

Пусть E_1, E_2, F_1, F_2 — A-модули и u_i $(i=1,2)$ — линейное отображение E_i в F_i. Согласно схолии из n° 2, положив $u(x_1 \otimes x_2) = u_1(x_1) \otimes u_2(x_2)$ для каждого тензорного произведения $x_1 \otimes x_2 \in E_1 \otimes E_2$, мы определим линейное отображение u модуля $E_1 \otimes E_2$ в модуль $F_1 \otimes F_2$. Обозначим временно это отображение u через $\varphi(u_1, u_2)$; очевидно (n° 2, схолия) φ есть *билинейное* отображение произведения $\mathscr{L}(E_1, F_1) \times \mathscr{L}(E_2, F_2)$ в модуль $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$; следовательно (n° 2), существует, и притом только одно, *линейное* отображение ψ *тензорного произведения* $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$ в $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$ такое, что $\varphi(u_1, u_2) = \psi(u_1 \otimes u_2)$. Вообще ψ *не есть изоморфизм* $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$ *на* $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$ (см. упражнение 3); тем не менее это будет так в наиболее важном случае:

Предложение 9. *Если* E_1, E_2, F_1, F_2 — *унитарные* A-*модули, имеющие каждый конечный базис, то* ψ *есть* (называемый *каноническим*) *изоморфизм* $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$ *на* $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$.

Действительно, мы покажем, что ψ отображает базис модуля $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$ на базис модуля $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$. Пусть (a_{i,λ_i}) — базис модуля E_i и (b_{i,μ_i}) — базис модуля F_i $(i=1,2)$; положим $a_{\lambda_1\lambda_2} = a_{1,\lambda_1} \otimes a_{2,\lambda_2}$ для каждой пары (λ_1, λ_2) и $b_{\mu_1\mu_2} = b_{1,\mu_1} \otimes b_{2,\mu_2}$ для каждой пары (μ_1, μ_2); $a_{\lambda_1\lambda_2}$ образуют базис в $E_1 \otimes E_2$, а $b_{\mu_1\mu_2}$ — в $F_1 \otimes F_2$ (следствие 2 предложения 7). В таком случае отображения $u_{\lambda_i\mu_i}$ $(i=1,2)$, определяемые условиями $u_{\lambda_i\mu_i}(a_{i,\lambda_i}) = b_{i,\mu_i}$ и $u_{\lambda_i\mu_i}(a_{i,\lambda_i'}) = 0$ для $\lambda_i' \neq \lambda_i$, образуют базис в $\mathscr{L}(E_i, F_i)$ (гл. II, § 2, n° 4); точно так же отображения $u_{\lambda_1\lambda_2\mu_1\mu_2}$, определяемые условиями $u_{\lambda_1\lambda_2\mu_1\mu_2}(a_{\lambda_1\lambda_2}) = b_{\mu_1\mu_2}$, $u_{\lambda_1\lambda_2\mu_1\mu_2}(a_{\lambda_1'\lambda_2'}) = 0$ для $(\lambda_1', \lambda_2') \neq (\lambda_1, \lambda_2)$, образуют базис в $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$. Но, очевидно, $u_{\lambda_1\lambda_2\mu_1\mu_2} = \varphi(u_{\lambda_1\mu_1}, u_{\lambda_2\mu_2}) = \psi(u_{\lambda_1\mu_1} \otimes u_{\lambda_2\mu_2})$, и так как тензорные произведения $u_{\lambda_1\mu_1} \otimes u_{\lambda_2\mu_2}$ образуют базис в $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$, то предложение доказано.

Таким образом, в случае, когда E_1, E_2, F_1, F_2 имеют конечные базисы, модуль $\mathscr{L}(E_1 \otimes E_2, F_1 \otimes F_2)$ можно *отождествлять* с тензорным произведением $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$ посредством изоморфизма ψ и вместо $\varphi(u_1, u_2)$ писать $u_1 \otimes u_2$ (или даже $u_1 u_2$). *Допу-*

ская вольность речи, мы и в случае невыполнения условий предложения 9 будем называть линейное отображение $\varphi(u_1, u_2)$ *тензорным произведением* линейных отображений u_1 и u_2 и обозначать его $u_1 \otimes u_2$; эта вольность речи не сможет вызвать путаницы, покуда речь будет идти лишь о линейных отображениях (поскольку элементы тензорного произведения $\mathscr{L}(E_1, F_1) \otimes \mathscr{L}(E_2, F_2)$ *не являются* линейными отображениями).

Предложение 10. *Если* $E_1, E_2, F_1, F_2, G_1, G_2$ — *A-модули*, u_i — *линейное отображение* E_i *в* F_i *и* v_i — *линейное отображение* F_i *в* G_i $(i = 1, 2)$, *то*

$$(v_1 \circ u_1) \otimes (v_2 \circ u_2) = (v_1 \otimes v_2) \circ (u_1 \otimes u_2). \tag{6}$$

Это утверждение есть непосредственное следствие определения тензорного произведения линейных отображений.

Следствие. *Если* u_i $(i = 1, 2)$ *есть изоморфизм* E_i *на* F_i, *а* v_i — *обратный изоморфизм, то* $u_1 \otimes u_2$ *есть изоморфизм* $E_1 \otimes E_2$ *на* $F_1 \otimes F_2$ *и* $v_1 \otimes v_2$ — *обратный ему изоморфизм.*

5. Модуль, сопряженный к тензорному произведению

Пусть E_1 и E_2 — унитарные A-модули; согласно n° 2, модуль $\mathscr{L}(E_1, E_2; A)$ *билинейных форм* на $E_1 \times E_2$ изоморфен модулю *линейных форм* на тензорном произведении $E_1 \otimes E_2$, т. е. модулю, *сопряженному* к этому тензорному произведению; канонический изоморфизм $\mathscr{L}(E_1, E_2; A)$ на $(E_1 \otimes E_2)^*$ относит каждой билинейной форме f на $E_1 \times E_2$ линейную форму u на $E_1 \otimes E_2$, определяемую условиями $u(x_1 \otimes x_2) = f(x_1, x_2)$ для каждого тензорного произведения $x_1 \otimes x_2$.

Предположим теперь, что каждый из модулей E_1, E_2 имеет *конечный базис*; предложение 9 определяет тогда канонический изоморфизм модуля $E_1^* \otimes E_2^*$ на модуль линейных отображений $E_1 \otimes E_2$ в $A \otimes A$; но следствие предложения 5 устанавливает канонический изоморфизм $A \otimes A$ на A, откуда непосредственно получается изоморфизм модуля $\mathscr{L}(E_1 \otimes E_2, A \otimes A)$ на $\mathscr{L}(E_1 \otimes E_2, A) = (E_1 \otimes E_2)^*$; таким образом, имеем:

Предложение 11. *Пусть E_1 и E_2 — унитарные A-модули с конечным базисом. Тензорное произведение $E_1^* \otimes E_2^*$ модулей E_1^* и E_2^*, сопряженных соответственно к E_1 и E_2, изоморфно модулю, сопряженному к тензорному произведению $E_1 \otimes E_2$; изоморфизм $E_1^* \otimes E_2^*$ на $(E_1 \otimes E_2)^*$ определяется отнесением каждому тензорному произведению $x_1' \otimes x_2' \in E_1^* \otimes E_2^*$ линейной формы и на $E_1 \otimes E_2$, определяемой условием* $u(x_1 \otimes x_2) = x_1'(x_1)\, x_2'(x_2)$.

Изоморфизм, определенный в предложении 11, и изоморфизм, обратный ему, называются *каноническими*; в дальнейшем $E_1^* \otimes E_2^*$ будет *отождествляться* с сопряженным к $E_1 \otimes E_2$ посредством этих изоморфизмов; таким образом, тождественно

$$\langle x_1 \otimes x_2,\ x_1' \otimes x_2' \rangle = \langle x_1,\ x_1' \rangle \langle x_2,\ x_2' \rangle. \tag{7}$$

Предложение 12. *Пусть E_1, E_2, F_1, F_2 — унитарные A-модули с конечным базисом и u_i $(i=1, 2)$ — линейное отображение E_i в F_i; сопряженное к линейному отображению $u_1 \otimes u_2$ модуля $E_1 \otimes E_2$ в $F_1 \otimes F_2$ равно тензорному произведению ${}^t u_1 \otimes {}^t u_2$ сопряженных к u_1 и u_2.*

Действительно, для всех $x_i \in E_i$, $y_i' \in F_i^*$ $(i=1, 2)$ имеем

$$\langle u_1'(x_1) \otimes u_2(x_2),\ y_1' \otimes y_2' \rangle = \langle u_1(x_1),\ y_1' \rangle \langle u_2(x_2),\ y_2' \rangle =$$
$$= \langle x_1,\ {}^t u_1(y_1') \rangle \langle x_2,\ {}^t u_2(y_2') \rangle = \langle x_1 \otimes x_2,\ {}^t u_1(y_1') \otimes {}^t u_2(y_2') \rangle,$$

чем предложение и доказано.

6. Тензорное произведение матриц

Пусть E_1, E_2, F_1, F_2 — A-модули и u_i $(i=1, 2)$ — линейное отображение E_i в F_i. Предположим, что E_i имеет конечный базис (a_{i, λ_i}), F_i — конечный базис (b_{i, μ_i}) $(i=1, 2)$, и пусть $X_i = (\alpha_{\mu_i \lambda_i})$ — матрица линейного отображения u_i относительно этих базисов; матрица $X = (\alpha_{\mu_1 \mu_2 \lambda_1 \lambda_2})$ линейного отображения $u = u_1 \otimes u_2$ относительно базисов $(a_{\lambda_1 \lambda_2})$ и $(b_{\mu_1 \mu_2})$ (в обозначениях предложения 9) называется *тензорным* (или *кронекеровским*) *произведением* матриц X_1 и X_2 и обозначается $X_1 \otimes X_2$. По определению,

$$u(a_{\lambda_1 \lambda_2}) = u_1(a_{1, \lambda_1}) \otimes u_2(a_{2, \lambda_2}) = \sum_{\mu_1, \mu_2} \alpha_{\mu_1 \lambda_1} \alpha_{\mu_2 \lambda_2} b_{1, \mu_1} \otimes b_{2, \mu_2};$$

поскольку $u(a_{\lambda_1 \lambda_2})$ есть столбец матрицы X с индексом (λ_1, λ_2), видим, что элементы матрицы $X_1 \otimes X_2$ задаются соотношениями

$$\alpha_{\mu_1 \mu_2 \lambda_1 \lambda_2} = \alpha_{\mu_1 \lambda_1} \alpha_{\mu_2 \lambda_2}. \tag{8}$$

Если ограничиться рассмотрением матриц, имеющих своими множествами индексов интервалы из N вида $[1, r]$, то тензорное произведение $A \otimes B$ матрицы $A=(\alpha_{ij})$ из m строк и n столбцов и матрицы $B=(\beta_{ik})$ из p строк и q столбцов может быть записано в форме «клеточной матрицы» (гл. II, § 6, n° 4)

$$\begin{pmatrix} \alpha_{11}B & \alpha_{12}B & \dots & \alpha_{1n}B \\ \alpha_{21}B & \alpha_{22}B & \dots & \alpha_{2n}B \\ \dots & \dots & \dots & \dots \\ \alpha_{m1}B & \alpha_{m2}B & \dots & \alpha_{mn}B \end{pmatrix},$$

соответствующей разбиению множества индексов строк на множества $\{i\}\times[1, p]$ $(1 \leqslant i \leqslant m)$ и множества индексов столбцов на множества $\{j\}\times[1, q]$ $(1 \leqslant j \leqslant n)$, или в форме клеточной матрицы

$$\begin{pmatrix} \beta_{11}A & \beta_{12}A & \dots & \beta_{1q}A \\ \beta_{21}A & \beta_{22}A & \dots & \beta_{2q}A \\ \dots & \dots & \dots & \dots \\ \beta_{p1}A & \beta_{p2}A & \dots & \beta_{pq}A \end{pmatrix},$$

соответствующей разбиению множества индексов строк на множества $[1, m]\times\{h\}$ $(1 \leqslant h \leqslant p)$ и множества индексов столбцов на множества $[1, n]\times\{k\}$ $(1 \leqslant k \leqslant q)$.

Билинейность $u_1 \otimes u_2$ и тождество (6) в переводе на язык матриц выражаются тождествами

$$\left.\begin{aligned} X_1 \otimes (X_2+Y_2) &= X_1 \otimes X_2 + X_1 \otimes Y_2, \\ (X_1+Y_1) \otimes X_2 &= X_1 \otimes X_2 + Y_1 \otimes X_2, \end{aligned}\right\} \tag{9}$$

$$(\alpha X_1) \otimes X_2 = X_1 \otimes (\alpha X_2) = \alpha (X_1 \otimes X_2), \tag{10}$$

$$(X_1 \otimes X_2)(Y_1 \otimes Y_2) = (X_1Y_1) \otimes (X_2Y_2). \tag{11}$$

Если X_1 и X_2 — обратимые квадратные матрицы, то $X_1 \otimes X_2$ — обратимая квадратная матрица, обратной к которой служит $X_1^{-1} \otimes X_2^{-1}$. Если Y_1, Y_2 — матрицы, *эквивалентные* (гл. II, § 6, n° 10) соответственно матрицам X_1, X_2 (или квадратные матрицы, *подобные* (гл. II, § 6, n° 11) квадратным матрицам X_1, X_2), то $Y_1 \otimes Y_2$ есть матрица, эквивалентная $X_1 \otimes X_2$ (соответственно квадратная матрица, подобная $X_1 \otimes X_2$).

Пусть $(\overline{a}_{i,\lambda_i})$ — второй базис в E_i $(i=1, 2)$; если P_i — матрица перехода от базиса (a_{i,λ_i}) к базису $(\overline{a}_{i,\lambda_i})$ (гл. II, § 6, n° 9), то матрица перехода от базиса в $E_1 \otimes E_2$, образованного элемен-

тами $a_{\lambda_1\lambda_2} = a_{\lambda_1, \lambda_1 a_{2, \lambda_2}}$, к базису, образованному элементами $\overline{a}_{\lambda_1\lambda_2} = \overline{a}_{\lambda_1, \lambda_1}\overline{a}_{2, \lambda_2}$, равна тензорному произведению $P_1 \otimes P_2$.

Наконец, согласно предложению 12, матрица, транспонированная к тензорному произведению $X_1 \otimes X_2$ матриц X_1 и X_2, равна тензорному произведению ${}^tX_1 \otimes {}^tX_2$ транспонированных к ним матриц.

7. *Полилинейные функции; тензорное произведение конечного числа модулей*

Определение билинейных функций обобщается следующим образом:

Определение 4. *Пусть A — коммутативное кольцо с единицей, $E = \prod_{i=1}^{n} E_i$ — произведение n унитарных A-модулей E_i и F — унитарный A-модуль. f называется полилинейным отображением E в F, если, каковы бы ни были индекс i и $n-1$ элементов $a_k \in E_k$ $(k \neq i)$, частичное отображение*

$$x_i \longrightarrow f(a_1, \ldots, a_{i-1}, x_i, a_{i+1}, \ldots, a_n)$$

есть линейное отображение E_i в F.

Пример. Если E — алгебра над A, то

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

есть полилинейное отображение E^n в E.

Замечание. Разумеется, определение 4 непосредственно распространяется на случай множества индексов i, являющегося не интервалом из N вида $[1, n]$, а любым конечным множеством.

Полилинейное отображение A-модуля $E = \prod_{i=1}^{n} E_i$ в кольцо A (рассматриваемое как A-модуль) называется *полилинейной формой*.

Свойства билинейных отображений, перечисленные в n° 1, непосредственно распространяются на полилинейные отображения; формулирование этих обобщений предоставим читателю. Отметим лишь, что полилинейные отображения $E = \prod_{i=1}^{n} E_i$ в F образуют A-модуль, обозначаемый $\mathscr{L}(E_1, \ldots, E_n; F)$ или $\mathscr{L}_n(E; F)$, если все E_i совпадают с одним и тем же модулем E.

Рассмотрения n° 2 можно теперь перенести на любое конечное семейство $(E_i)_{1\leqslant i\leqslant n}$ A-модулей; ими определяется A-модуль M, обладающий следующими свойствами:

1° существует полилинейное отображение φ произведения $\prod_{i=1}^{n} E_i$ в M такое, что M порождается множеством $\varphi\left(\prod_{i=1}^{n} E_i\right)$;

2° для любого полилинейного отображения f произведения $\prod_{i=1}^{n} E_i$ в *любой* A-модуль A существует, и притом единственное, *линейное* отображение g модуля M в N такое, что $f=g\circ\varphi$.

При этом каждый A-модуль, обладающий этими свойствами, изоморфен M (обобщение предложения 3).

Детальное проведение доказательства предоставляем читателю.

Определенный так A-модуль M называется *тензорным произведением* семейства (E_i) и обозначается $\bigotimes_{i=1}^{n} E_i$ или $E_1\otimes E_2\otimes\ldots\otimes E_n$; если все E_i совпадают с одним и тем же модулем E, то их тензорное произведение обозначается также $\bigotimes^{n} E$ и называется *n-й тензорной степенью* модуля E. Значение $\varphi(x_1, x_2, \ldots, x_n)$, принимаемое полилинейным отображением φ для каждого $(x_i)\in\prod_{i=1}^{n} E_i$, обозначают $\bigotimes_{i=1}^{n} x_i$ или $x_1\otimes x_2\otimes\ldots\otimes x_n$ и (допуская вольность речи) называют *тензорным произведением* последовательности (x_i).

Каково бы ни было разбиение $(I_k)_{1\leqslant k\leqslant p}$ интервала $[1, n]$ множества $\mathbf{N}$, тензорное произведение $\bigotimes_{i=1}^{n} E_i$ изоморфно тензорному произведению $\bigotimes_{k=1}^{p}\left(\bigotimes_{i\in I_k} E_i\right)$ («ассоциативность» тензорного произведения). Это устанавливается методом, использованным в доказательствах предложений 6 и 7: условием $u(x_1, \ldots, x_n) = \bigotimes_{k=1}^{p}\left(\bigotimes_{i\in I_k} x_i\right)$ определяется полилинейное отображение u про-

изведения $\prod_{i=1}^{n} E_i$ в $\bigotimes_{k=1}^{p} \bigotimes_{i\in I_k} E_i)$ и доказывается, что это полилинейное отображение удовлетворяет условиям предложения 3 (обобщенного на случай n модулей). Определенный так изоморфизм $\bigotimes_{i=1}^{n} E_i$ на $\bigotimes_{k=1}^{p} (\bigotimes_{i\in I_k} E_i)$, называемый, как и обратный ему изоморфизм, *каноническим*, относит каждому тензорному произведению $\bigotimes_{i=1}^{n} x_i$ элемент $\bigotimes_{k=1}^{p} (\bigotimes_{i\in I_k} x_i)$.

Читатель без труда обобщит на тензорное произведение любого конечного числа модулей предложения 6 и 7, определение тензорного произведения любого числа линейных отображений (или матриц) и предложения 8—12.

Упражнения. 1) Пусть $E\otimes F$ — тензорное произведение $\mathbf{Z}$-модуля $E=\mathbf{Z}$ на $\mathbf{Z}$-модуль $F=\mathbf{Z}/(2)$ и M — подмодуль $2\mathbf{Z}$ (четных чисел) модуля E. Показать, что канонический образ тензорного произведения $M\otimes F$ в $E\otimes F$ (n° 3) не изоморфен $M\otimes F$.

2) а) Пусть G — аддитивная группа, рассматриваемая как $\mathbf{Z}$-модуль; показать, что тензорное произведение $(\mathbf{Z}/(n))\otimes G$ $\mathbf{Z}$-модулей $\mathbf{Z}/(n)$ и G изоморфно факторгруппе G/nG группы G по ее подгруппе nG, образованной элементами nx, где x пробегает G.

б) Ядро канонического представления $(n\mathbf{Z})\otimes G$ в $\mathbf{Z}\otimes G$ изоморфно подгруппе в G, образованной теми элементами x, для которых $nx=0$.

3) Пусть E — любой унитарный A-модуль и F — унитарный A-модуль с базисом.

а) Показать, что, каков бы ни был подмодуль M модуля E, каноническое отображение $M\otimes F$ в $E\otimes F$ есть изоморфизм.

б) Показать, что если x — свободный элемент модуля E и y — ненулевой элемент из F, то $x\otimes y\neq 0$; если при этом и y свободный, то $x\otimes y$ есть свободный элемент модуля $E\otimes F$.

4) Пусть p — простое число, A — коммутативное кольцо $\mathbf{Z}/(p^2)$, E — аддитивная группа $\mathbf{Z}/(p)$, рассматриваемая как A-модуль (в котором произведением класса по модулю p^2 и элемента $x\in E$ служит элемент nx, где n — любое целое из рассматриваемого класса по модулю p^2). Пусть, далее, u и v — любые два линейных отображения E в A (рассматриваемое как A-модуль). Показать, что линейное отображение f модуля $E\otimes E$ в $A\otimes A$, удовлетворяющее условию $f(x\otimes y)=u(x)\otimes v(y)$, тождественно нулевое, хотя тензорное произведение $E^*\otimes E^*$ сопряженного к E на себя и не сводится к 0.

5) Пусть E_1, E_2, F_1, F_2 — векторные пространства над полем K, u_i $(i=1, 2)$ — линейное отображение E_i в F_i и $u=u_1\otimes u_2$. Пусть, далее, H_i — векторное подпространство пространства E_i $(i=1, 2)$,

H — векторное подпространство $H_1 \otimes H_2$ пространства $E_1 \otimes E_2$ (следствие 3 предложения 7) и H' — подпространство $(u_1(H_1)) \otimes (u_2(H_2))$ пространства $F_1 \otimes F_2$. Показать, что $u(H) = H'$. В частности, если ранги $\varrho(u_1)$ и $\varrho(u_2)$ конечны, то $\varrho(u_1 \otimes u_2) = \varrho(u_1)\varrho(u_2)$.

6) Пусть z — элемент тензорного произведения $E \otimes F$ конечномерных векторных пространств E и F над некоторым полем; каков бы ни был базис (b_j) пространства F, z может быть однозначно представлен в виде $\sum_j (x_j \otimes b_j)$, где $x_j \in E$ (следствие 1 предложения 7). Показать, что векторное подпространство V пространства E, порожденное элементами x_j, не зависит от рассматриваемого базиса (b_j) пространства F. Если V r-мерно, то существуют его базис $(a_i)_{1 \leqslant i \leqslant r}$ и r элементов c_i $(1 \leqslant i \leqslant r)$ пространства F такие, что $z = \sum_{i=1}^{r} (a_i \otimes c_i)$, причем r — наименьшее возможное число слагаемых в представлении z в виде суммы тензорных произведений элемента из E на элемент из F.

§ 2. Расширение кольца операторов модуля

В этом параграфе нас будут интересовать структуры модуля относительно различных колец операторов, причем одно и то же множество сможет наделяться различными такими структурами; во избежание всяких недоразумений мы будем называть отображение E в F, *линейное* при наделении E и F структурами A-модуля, *A-линейным* или *A-гомоморфизмом*. Аналогично будут определяться *A-изоморфизм*, *A-билинейное* отображение и т. д.

1. Расширение кольца операторов модуля

Пусть B — кольцо (коммутативное или нет) с единицей e, A — подкольцо кольца B, содержащееся в его центре и имеющее ту же единицу, так что B может рассматриваться как *алгебра* над A, и M — любой (левый) *B-модуль*. Сужение его кольца операторов до A (гл. II, § 1, n° 1) определяет в M структуру *A-модуля*; говоря о структуре A-модуля в заданном B-модуле, мы всюду имеем в виду структуру, полученную указанным способом.

Пусть теперь E — произвольный *унитарный A-модуль*; исследуем, можно ли *погрузить* E в *унитарный B-модуль*, т. е., говоря точно, найти *A-изоморфизм* модуля E *в* унитарный B-модуль. Легко видеть, что эта задача не всегда допускает решение.

Примером может служить тот случай, когда $A=\mathbf{Z}$, $B=\mathbf{Q}$, а E — коммутативная группа, имеющая элементы конечного порядка и рассматриваемая как $\mathbf{Z}$-модуль; такая группа очевидно не может быть погружена в векторное пространство над $\mathbf{Q}$ (см. ниже, n° 3, теорема 2).

Более общим образом, мы изучим A-линейные отображения модуля E в произвольный унитарный B-модуль и установим существование унитарного B-модуля F и A-линейного отображения φ модуля E в F таких, что, каково бы ни было A-линейное отображение f модуля E в *любой* унитарный B-модуль N, существует *B-линейное* отображение g модуля F в N, для которого $f=g\circ\varphi$. Тогда поставленная выше задача «погружения» будет иметь очевидное решение: для существования A-изоморфизма модуля E в унитарный B-модуль необходимо и достаточно, чтобы φ было *взаимно однозначно*.

Заметим прежде всего, что если B-модуль F обладает указанным свойством, то им обладает и его подмодуль F_1, порожденный множеством $\varphi(E)$; поэтому можно дополнительно потребовать, чтобы $\varphi(E)$ *порождало* F; тогда B-линейное отображение g, для которого $f=g\circ\varphi$, будет определяться A-линейным отображением f *однозначно*. При этом такой B-модуль F, если он существует, определен, с точностью до изоморфизма, *однозначно*. Говоря точно, имеет место следующее предложение:

Предложение 1. *Пусть F_i $(i=1, 2)$ — унитарные B-модули и φ_i для каждого i — A-линейное отображение E в F_i такое, что:* 1° *$\varphi_i(E)$ порождает F_i и* 2° *каково бы ни было A-линейное отображение f модуля E в произвольный унитарный B-модуль N, существует B-линейное отображение g_i модуля F_i в N такое, что $f=g_i\circ\varphi_i$. При этих условиях существует B-изоморфизм u модуля F_1 на F_2, для которого $\varphi_2=u\circ\varphi_1$.*

Действительно, беря в качестве N B-модуль F_2 (соответственно F_1) видим, что существует B-линейное отображение h_1 (соответственно h_2) F_1 в F_2 (соответственно F_2 в F_1) такое, что $\varphi_2=h_1\circ\varphi_1$ (соответственно $\varphi_1=h_2\circ\varphi_2$); тогда $\varphi_1=(h_2\circ h_1)\circ\varphi_1$, и так как $\varphi_1(E)$ порождает F_1, то $h_2\circ h_1$ есть тождественное отображение F_1 на себя; совершенно так же $h_1\circ h_2$ есть тождественное отображение F_2 на себя, и предложение доказано.

Покажем теперь, что B-модуль F и отображение φ, удовлетворяющие требуемым условиям, действительно существуют. Рассмотрим A-модуль $B \otimes E$ (где B рассматривается как A-модуль); пусть t — произвольный элемент из B; если для каждого тензорного произведения $x \otimes y$ ($x \in B$, $y \in E$) положить $\psi_t(x \otimes y) = (tx) \otimes y$, то, поскольку отображение $(x, y) \to (tx) \otimes y$ очевидно билинейно, этим определится A-линейное отображение ψ_t модуля $B \otimes E$ в себя (§ 1, n° 2). Положив $t \cdot z = \psi_t(z)$ для каждого $t \in B$ и каждого $z \in B \otimes E$, получим внешний закон композиции $(t, z) \to t \cdot z$ на $B \otimes E$, имеющий B своей областью операторов; непосредственная проверка показывает, что этот внешний закон вместе со сложением определяет в множестве $B \otimes E$ структуру *унитарного левого B-модуля*. Во избежание смешения с *A-модулем* $B \otimes E$ обозначим полученный так B-модуль через $E_{(B)}$. Заметим, что $B \otimes E$ есть не что иное, как модуль, получающийся путем *сужения* кольца операторов B-модуля $E_{(B)}$ *до* A.

Теперь, имеет место следующее предложение:

Предложение 2. *B-модуль $E_{(B)}$ порождается образом E_1 модуля E при A-линейном отображении $x \to e \otimes x$ этого модуля в $E_{(B)}$; для каждого A-линейного отображения f модуля E в произвольный унитарный B-модуль N существует однозначно определенное B-линейное отображение g модуля $E_{(B)}$ в N такое, что $f(x) = g(e \otimes x)$, каково бы ни было $x \in E$.*

Первая часть предложения очевидна, поскольку каждый элемент из $E_{(B)}$ может быть записан в виде $\sum_i (t_i \otimes x_i) = \sum_i (t_i \cdot (e \otimes x_i))$, где $t_i \in B$ и $x_i \in E$. Для доказательства второй части заметим, что отображение $(t, x) \to tf(x)$ произведения $B \times E$ в N A-билинейно; поэтому (§ 1, n° 2) существует A-линейное отображение g модуля $B \otimes E$ в N такое, что $g(t \otimes x) = tf(x)$; покажем, что g — *B-линейное* отображение $E_{(B)}$ в N. В самом деле, достаточно (по линейности) доказать, что $g(s \cdot (t \otimes x)) = sg(t \otimes x)$ при любых $s \in B$, $t \in B$, $x \in E$; но так как, по определению, $s \cdot (t \otimes x) = (st) \otimes x$, то

$$g(s \cdot (t \otimes x)) = g((st) \otimes x) = (st) f(x) = s(tf(x)) = sg(t \otimes x).$$

Поскольку, очевидно, $g(e \otimes x) = ef(x) = f(x)$, предложение доказано.

Говорят, что B-модуль $E_{(B)}$ получен путем *расширения* кольца A операторов модуля E *до* B; A-линейное отображение $x \to e \otimes x$ модуля E в $E_{(B)}$ называется *каноническим* отображением этого модуля в его расширение $E_{(B)}$. В случае, когда это отображение есть *A-изоморфизм*, E чаще всего отождествляется с его образом E_1.

Предложение 3. *Для каждого A-линейного отображения f A-модуля E в A-модуль E' существует однозначно определенное B-линейное отображение g B-модуля $E_{(B)}$ в $E'_{(B)}$ такое, что $g(e \otimes x) = e \otimes f(x)$ для каждого $x \in E$.*

Достаточно применить предложение 2 к A-линейному отображению $x \to e \otimes f(x)$ модуля E в $E'_{(B)}$.

В случае, когда канонические отображения E в $E_{(B)}$ и E' в $E'_{(B)}$ являются изоморфизмами, посредством которых E и E' отождествляются соответственно с подмодулями A-модулей $B \otimes E$ и $B \otimes E'$, можно также сказать, что каждое A-линейное отображение E в E' однозначно *продолжается* до B-линейного отображения $E_{(B)}$ в $E'_{(B)}$.

Расширение кольца операторов модуля есть *транзитивная* операция; говоря точно, имеет место следующее предложение:

Предложение 4. *Пусть C — кольцо* (коммутативное или нет) *с единицей e и A, B — подкольца этого кольца, содержащиеся в его центре, причем $e \in A \subset B$. Каков бы ни был A-модуль E, C-модуль $E_{(C)}$ изоморфен C-модулю $(E_{(B)})_{(C)}$.*

Применим критерий предложения 1. Пусть f — A-линейное отображение модуля E в унитарный C-модуль N и φ — каноническое отображение E в $E_{(B)}$; согласно предложению 2, существует B-линейное отображение g модуля $E_{(B)}$ в N такое, что $g(\varphi(x)) = f(x)$; точно так же, если обозначить через ψ каноническое отображение $E_{(B)}$ в $(E_{(B)})_{(C)}$, существует C-линейное отображение h модуля $(E_{(B)})_{(C)}$ в N такое, что $h(\psi(\varphi(x))) = g(\varphi(x)) = f(x)$; так как $x \to \psi(\varphi(x))$ есть A-линейное отображение E в $(E_{(B)})_{(C)}$, предложение 1 устанавливает существование изоморфизма $E_{(C)}$ на $(E_{(B)})_{(C)}$ (называемого, как и изоморфизм, обратный ему, *каноническим*), относящего каждому элементу вида $e \otimes x$ ($x \in E$) из $E_{(C)}$ элемент $\psi(\varphi(x))$ из $(E_{(B)})_{(C)}$.

Замечания. 1) Поскольку вообще A-модуль $B \otimes E$ не изоморфен E, было бы неправильно думать, что *сужение* кольца операторов модуля (гл. II, § 1, n° 1, и § 5) и *расширение* этого кольца операторов являются взаимно обратными операциями.

2) В случае, когда A — *произвольное* (не обязательно коммутативное) подкольцо кольца B, содержащее его единицу, также можно определить *расширение* кольца операторов произвольного унитарного (левого) A-модуля *до* B и обобщить предыдущие предложения (см. упражнение 7 и Приложение II к этой главе).

2. Расширение кольца операторов свободного модуля

Каноническое отображение $x \longrightarrow e \otimes x$ A-модуля E в B-модуль $E_{(B)}$ вообще не есть A-изоморфизм (оно может быть тождественно нулевым, когда ни B, ни E не сводятся к 0; см. ниже теорему 2). Однако оно является A-изоморфизмом в двух важных случаях, которые мы теперь рассмотрим.

Теорема 1. *Пусть B — кольцо* (коммутативное или нет), *обладающее единицей e, и A — подкольцо этого кольца, содержащееся в его центре и такое, что $e \in A$. Каноническое отображение $x \longrightarrow e \otimes x$ унитарного A-модуля E, имеющего базис (a_λ), в $E_{(B)}$ есть A-изоморфизм; по отождествлении E с его образом E_1 при этом изоморфизме базис (a_λ) модуля E относительно A является также базисом B-модуля $E_{(B)}$. Каждое A-линейное отображение f модуля E в произвольный B-модуль однозначно продолжается до B-линейного отображения $\bar{f}$ модуля $E_{(B)}$ в N такого, что*

$$\bar{f}\left(\sum_\lambda \xi_\lambda a_\lambda\right) = \sum_\lambda \xi_\lambda f(a_\lambda)$$

для каждого элемента $\sum_\lambda \xi_\lambda a_\lambda$ из $E_{(B)}$ $(\xi_\lambda \in B)$.

Действительно, при $x = \sum_\lambda \xi_\lambda a_\lambda$ соотношение $e \otimes x = 0$ записывается в виде $\sum_\lambda ((\xi_\lambda e) \otimes a_\lambda) = 0$ и, значит (§ 1, следствие 1 предложения 7), влечет $\xi_\lambda e = 0$ для каждого λ, откуда $\xi_\lambda = 0$ для каждого λ; тем самым каноническое отображение $x \longrightarrow e \otimes x$ есть изоморфизм. То, что (a_λ) служит базисом для $E_{(B)}$, непосредственно вытекает из следствия 1 предложения 7 § 1 и определения внешнего закона B-модуля $E_{(B)}$, поскольку для каждого индекса λ и каждого $t \in B$ можно, по отождествлении E с E_1, написать

$t \cdot a_\lambda = (te) \otimes a_\lambda$. Наконец, последнее утверждение теоремы есть непосредственное следствие предложения 2, раз только E отождествлено с подмодулем (над A) модуля $E_{(B)}$.

Предположения теоремы 1 выполнены, в частности, когда E — *векторное пространство* над полем A, а B — *надтело* этого поля (коммутативное или нет), содержащее A в своем центре; к этому случаю мы всюду и будем ее применять.

3. *Модули над кольцом целостности*

Рассмотрим теперь модули над *кольцом целостности* A (гл. I, § 8, п° 3) и *векторные пространства*, получающиеся из них путем расширения A до его *поля отношений* (гл. I, § 9, п° 4).

Теорема 2. *Пусть A — кольцо целостности с единицей (обозначаемой 1) и K — его поле отношений. Пусть, далее, E — произвольный унитарный A-модуль, $E_{(K)}$ — векторное пространство над K, получающееся путем расширения кольца операторов модуля E до K, и φ — каноническое отображение $x \to 1 \otimes x$ модуля E в $E_{(K)}$. При этих условиях*:

1° *Векторное пространство $E_{(K)}$ равно $K\varphi(E)$* (множеству элементов λz, где λ пробегает K, а z пробегает $\varphi(E)$).

2° *Для того чтобы $\varphi(x) \neq 0$, необходимо и достаточно, чтобы x был свободным элементом в E.*

1° Каждый элемент из $E_{(K)}$ имеет вид $z = \sum_i \xi_i \varphi(x_i)$, где $\xi_i \in K$ и $x_i \in E$ (предложение 2); для каждого i существует $\alpha_i \in A$ такое, что $\alpha_i \neq 0$ и $\alpha_i \xi_i \in A$; поэтому $\alpha = \prod_i \alpha_i \neq 0$ и $\alpha \xi_i = \beta_i$ принадлежит A для каждого i; следовательно, в $E_{(K)}$

$$z = \alpha^{-1}(\alpha z) = \alpha^{-1} \sum_i \beta_i \varphi(x_i) = \alpha^{-1} \varphi\left(\sum_i \beta_i x_i\right),$$

поскольку φ A-линейно.

2° Если элемент $x \in E$ не свободный, то в A существует $\alpha \neq 0$ такое, что $\alpha x = 0$; тогда в векторном пространстве $E_{(K)}$ имеем $\alpha\varphi(x) = \varphi(\alpha x) = 0$, откуда $\varphi(x) = 0$.

Обратно, предположим, что $\varphi(x) = 1 \otimes x = 0$ в $K \otimes E$, и покажем, что элемент x не свободный. Согласно предложению 8 § 1, в K (рассматриваемом как A-модуль) существует подмодуль K_1,

содержащий A, порождённый конечным числом элементов $\xi_i \in K$ и такой, что $1 \otimes x = 0$ также *в тензорном произведении* $K_1 \otimes E$. Но, как мы видели в 1°, в A существует $\alpha \neq 0$ такое, что все $\beta_i = \alpha\xi_i$ принадлежат A. Отсюда сразу следует, что каждый элемент из K_1 имеет вид $\alpha^{-1}\xi$, где $\xi \in A$, иными словами, что K_1 содержится в A-модуле $K_\alpha = \alpha^{-1}A$. Очевидно, $1 \otimes x = 0$ в тензорном произведении $K_\alpha \otimes E$. Но отображение $\xi \to \alpha\xi$ есть изоморфизм A-модуля K_α на A-модуль A; при этом, согласно предложению 5 § 1, канонический изоморфизм $A \otimes E$ на E относит тензорному произведению $\lambda \otimes x$ элемент $\lambda x \in E$; поэтому существует *изоморфизм* $K_\alpha \otimes E$ на E, относящий тензорному произведению $\xi \otimes x$ элемент $(\alpha\xi)x \in E$. Следовательно, предположение, что $1 \otimes x = 0$ в $K_\alpha \otimes E$, влечет, что $\alpha x = 0$ в E, иными словами, что элемент $x \in E$ не свободный.

Следствие 1. *Пусть E — унитарный A-модуль, все ненулевые элементы которого свободные. Тогда его каноническое отображение φ в векторное пространство $F = E_{(K)}$ есть A-изоморфизм такой, что*:

1° *Векторное пространство F равно $K\varphi(E)$.*

2° *При отождествлении E посредством изоморфизма φ с модулем $\varphi(E)$ каждое A-линейное отображение f модуля E в произвольное векторное пространство G над K однозначно продолжается до K-линейного отображения $\overline{f}$ пространства F в G; при этом, если f — A-изоморфизм E в G, то $\overline{f}$ есть K-изоморфизм F в G.*

Нужно лишь убедиться в том, что вместе с f также $\overline{f}$ является изоморфизмом; но так как каждый ненулевой элемент из F имеет вид λx, где $\lambda \in K$, $x \in E$, $\lambda \neq 0$ и $x \neq 0$, то $\overline{f}(\lambda x) = \lambda f(x) \neq 0$, поскольку $f(x) \neq 0$ в силу предположения.

Векторное пространство $E_{(K)}$, получающееся из унитарного A-модуля E, все ненулевые элементы которого свободные, путем расширения кольца операторов A до его поля отношений K, будет называться *векторным пространством, ассоциированным* с E; при этом E всегда будет отождествляться с его образом в $E_{(K)}$ при каноническом изоморфизме $x \to 1 \otimes x$.

Размерность $E_{(K)}$ будет называться *рангом* A-модуля E; более общим образом, *ранг* любого множества $M \subset E$ будет, по опреде-

лению, считаться равным рангу канонического образа M в $E_{(K)}$, т. е. (гл. II, § 3, n° 2) размерности векторного подпространства, порождаемого этим образом. *Рангом* каждого отображения g множества L в E будет считаться, по определению, ранг $g(L)$.

Следствие 2. *Пусть E — унитарный A-модуль, все ненулевые элементы которого свободные. Всякий его A-изоморфизм ψ в векторное пространство F_1 над K такой, что $F_1 = K\psi(E)$, продолжается до K-изоморфизма векторного пространства $F = E_{(K)}$, ассоциированного с E, на векторное пространство F_1.*

Это непосредственно вытекает из следствия 1 и условия $F_1 = K\psi(E)$.

Следствие 3. *Множество S всех зависимых элементов произвольного унитарного A-модуля E является его подмодулем; все ненулевые элементы фактормодуля E/S свободные, а векторное пространство $E_{(K)}$ изоморфно векторному пространству, ассоциированному с модулем E/S.*

Действительно, S есть прообраз нуля относительно канонического A-линейного отображения φ модуля E в $K \otimes E$, и $\varphi(E)$ изоморфно E/S; так как $E_{(K)} = K\varphi(E)$, то $E_{(K)}$ изоморфно векторному пространству, ассоциированному с E/S.

Если E — векторное пространство над K, то оно совпадает с ассоциированным с ним (как с A-модулем) векторным пространством; при этом имеет место следующее свойство:

Предложение 5. *Пусть A — кольцо целостности, K — его поле отношений и E — векторное пространство над K. Всякое семейство (x_λ) элементов из E, свободное относительно A, является свободным относительно K.*

Действительно, если $\sum_\lambda \alpha_\lambda x_\lambda = 0$, где α_λ принадлежат K и все кроме конечного их числа равны нулю, то, как показывает рассуждение, проведенное при доказательстве теоремы 2, в A существует элемент $\gamma \neq 0$ такой, что $\gamma\alpha_\lambda = \beta_\lambda$ принадлежит A для каждого λ; поэтому $\sum_\lambda \beta_\lambda x_\lambda = \gamma\left(\sum_\lambda \alpha_\lambda x_\lambda\right) = 0$, откуда, в силу предположения, $\beta_\lambda = 0$ для каждого λ, а тогда и $\alpha_\lambda = 0$ для каждого λ, поскольку $\gamma \neq 0$.

Замечание. Тензорное произведение $E_1 \otimes E_2$ унитарных A-модулей E_1 и E_2 может содержать ненулевые зависимые элементы, даже если каждый ненулевой элемент модулей E_1 и E_2 свободный (см. упражнение 4).

Упражнения. 1) Пусть B — коммутативное кольцо с единицей e и A — его подкольцо, содержащее e. Показать, что если E и F — унитарные A-модули, то B-модуль $(E \otimes F)_{(I)}$ изоморфен B-модулю $E_{(B)} \otimes F_{(B)}$.

*2) Пусть E — векторное пространство над полем K. Показать, что для множества $F \subset E$ следующие предложения равносильны:

а) F есть векторное пространство относительно подполя L поля K; каноническое отображение F в E продолжается (следствие теоремы 1) до K-изоморфизма $F_{(K)}$ на E; группа автоморфизмов поля K, оставляющих инвариантным каждый элемент из L, не оставляет инвариантным никакого другого элемента из K.

б) Группа Г биавтоморфизмов (Приложение I к главе II) пространства E, оставляющих инвариантным каждый элемент из F, не оставляет инвариантным никакого другого элемента из E и не содержит никакого нетождественного автоморфизма пространства E. [Показать, что поле L есть множество тех элементов $\lambda \in K$, для которых $x \in F$ влечет $\lambda x \in F$.]

*3) Пусть A — кольцо целостности с единицей и E, F — произвольные A-модули. Показать, что если x — свободный элемент из E и y — свободный элемент из F, то $x \otimes y$ есть *свободный* элемент в $E \otimes F$. [Достаточно доказать, что $x \otimes y \neq 0$; начать с рассмотрения случая, когда все ненулевые элементы из E и F свободные; использовать предложение 8 § 1 для сведения к случаю, когда E и F имеют конечное число образующих, и, далее, следствие 1 теоремы 2 для установления существования такого A-билинейного отображения f произведения $E \times F$ в поле отношений K кольца A, что $f(x, y) \neq 0$. Перейти к общему случаю с помощью предложения 6 § 1.]

*°4) Пусть A — кольцо $K_0[X, Y]$ полиномов от двух неизвестных X, Y над полем K_0 и E — идеал $(X)+(Y)$ этого кольца (множество всех полиномов, не содержащих члена нулевой степени). Показать, что в тензорном произведении $E \otimes E$ A-модуля E на себя элемент $X \otimes Y - Y \otimes E$ отличен от нуля, но $XY(X \otimes Y - Y \otimes X) = 0$. [Рассмотреть билинейные отображения $E \times E$ в фактормодуль A/E.]

5) Пусть A — произвольное коммутативное кольцо с единицей и K — его кольцо отношений (гл. I, § 9, n° 4). Пусть, далее, E — произвольный унитарный A-модуль и S — множество тех элементов $x \in E$, аннулятор которых (гл. II, § 1, n° 9) содержит по крайней мере один элемент из A, не являющийся делителем нуля. Показать, что S есть подмодуль модуля E и что каноническое отображение $x \to 1 \otimes x$

модуля E в $E_{(K)}$ есть A-линейное отображение E на A-модуль E_1, изоморфный E/S, такое, что $E_{(K)}=KE_1$.

6) В обозначениях упражнения 5, дать прямое доказательство существования K-модуля F и A-линейного отображения φ модуля E в F таких, что $E_1=\varphi(E)$ изоморфно E/S, $F=KE_1$ и для каждого A-линейного отображения f модуля E в произвольный K-модуль N существует K-линейное отображение $\overline{f}$ модуля F в N такое, что $f=\overline{f}\circ\varphi$. [Для построения F воспользоваться способом, применённым для симметризации коммутативного ассоциативного закона (гл. I, § 2, n° 4).]

*7) Пусть B — кольцо (коммутативное или нет), обладающее единицей e, A — его произвольное подкольцо, содержащее e, и E — произвольный унитарный A-модуль.

а) Обобщить на E предложение 1.

б) Определим в тензорном произведении $B\otimes E$, где B и E рассматриваются как **Z-*модули*** (аддитивные группы без операторов), структуру левого B-модуля, положив $t(x\otimes y)=(tx)\otimes y$ для всех $t\in B$, $x\in B$ и $y\in E$. Пусть H — подмодуль этого B-модуля, порождённый множеством элементов вида $(a\otimes x)-(e\otimes(ax))$, где a пробегает A и x пробегает E, далее, $F=B$-модуль $(B\otimes E)/H$ и $\varphi(x)$ для каждого $x\in E$ — класс $e\otimes x \pmod H$. Показать, что: 1° $\varphi(E)$ порождает F; 2° для каждого A-линейного отображения f модуля E в произвольный унитарный B-модуль N существует однозначно определённое B-линейное отображение g модуля F в N такое, что $f=g\circ\varphi$.

в) Вывести из а) и б), что если A содержится в центре кольца B, то существует такой изоморфизм ψ B-модуля $E_{(B)}$, определённого в n° 1, на B-модуль $F=(B\otimes E)/H$, определённый в б), что $\varphi(x)=\psi(e\otimes x)$ для каждого $x\in E$. Следовательно, когда A содержится в центре кольца B, $E_{(B)}$ ***отождествляется*** посредством этого изоморфизма с F; в случае произвольного A модуль F также будет обозначаться $E_{(B)}$, и мы будем говорить, что он получен путём *расширения* кольца операторов модуля E *до* B, а отображение φ, определённое в б), будем называть каноническим отображением E в $E_{(B)}$.

г) Показать, что если $B=A$, то A-модуль $E_{(A)}$ изоморфен A-модулю E.

д) Обобщить на E предложение 3.

е) Если E — прямая сумма семейства (E_λ) своих подмодулей, то $E_{(B)}$ изоморфно прямой сумме B-модулей $(E_\lambda)_{(B)}$. В частности, если (a_λ) — базис модуля E, то каноническое отображение φ этого модуля в $E_{(B)}$ есть изоморфизм; по отождествлении E с $\varphi(E)$ посредством изоморфизма φ (a_λ) будет также базисом модуля $E_{(B)}$; каждое A-линейное отображение модуля E в произвольный унитарный B-модуль N однозначно продолжается до B-линейного отображения $E_{(B)}$ в N.

ж) Предположим, что A есть кольцо, допускающее *тело левых отношений* K (гл. I, § 9, упражнение 8). Пусть E — унитарный A-модуль, $E_{(K)}$ — левое векторное пространство над K, полученное путем расширения кольца операторов модуля E до K, и φ — каноническое отображение E в $E_{(K)}$. Показать, что утверждения теоремы 2 и ее следствий полностью сохраняют силу. [Заметить, что для любого конечного числа элементов ξ_i $(1 \leqslant i \leqslant n)$ из K в A существует $\alpha \neq 0$ такое, что все $\alpha\xi_i$ принадлежат A.]

§ 3. Тензорные произведения алгебр

1. Тензорное произведение алгебр

Пусть E и F — алгебры над коммутативным кольцом A с единицей. Они наделены структурой A-модуля, лежащей в основе их структуры алгебры. Пусть $G = E \otimes F$ — тензорное произведение A-модулей E и F; мы определим на G *умножение*, которое вместе со структурой A-модуля определит в G структуру *алгебры* относительно A. Для этого заметим, что, поскольку умножение на G есть билинейное отображение $G \times G$ в G, достаточно (§ 1, n° 2) определить его для всевозможных пар (z, z') тензорных произведений $z = x \otimes y$, $z' = x' \otimes y'$, проверив, что каждое из частичных отображений

$$(x, y) \longrightarrow (x \otimes y)(x' \otimes y'), \qquad (x', y') \longrightarrow (x \otimes y)(x' \otimes y')$$

билинейно на $E \times F$. Но эти условия будут очевидно удовлетворены, если принять

$$(x \otimes y)(x' \otimes y') = (xx') \otimes (yy'). \tag{1}$$

Остается проверить, что определенное так на G умножение *ассоциативно*; ввиду его двоякой дистрибутивности относительно сложения все сводится к установлению того, что

$$((x \otimes y)(x' \otimes y'))(x'' \otimes y'') = (x \otimes y)((x' \otimes y')(x'' \otimes y''));$$

но это свойство вытекает из ассоциативности умножения на E и F, поскольку обе части формулы равны $(xx'x'') \otimes (yy'y'')$.

Множество $E \otimes F$, наделенное определенной так структурой алгебры, называется *тензорным произведением алгебр* E *и* F.

В случае, когда E и F — кольца *без операторов*, под тензорным произведением $E \otimes F$, по определению, понимается тензорное произведение E и F, рассматриваемых как *алгебры над кольцом* $\mathbf{Z}$ рациональных целых чисел.

Тензорное произведение $E^0 \otimes F^0$ алгебр E^0 и F^0, *противоположных* E и F, изоморфно алгебре, *противоположной* $E \otimes F$, и *отождествляется* с нею; в частности, если E и F — *коммутативные* алгебры, то это же верно и для $E \otimes F$.

Предложения 4 и 5 § 1 распространяются на случай, когда E и F — *алгебры* над A, поскольку определенные там канонические изоморфизмы являются одновременно изоморфизмами структур алгебры.

Предложению 6 § 1 соответствует следующее предложение:

Предложение 1. *Пусть E и F — алгебры над A, $\mathfrak{a}$ — двусторонний идеал алгебры E и $\mathfrak{b}$ — двусторонний идеал алгебры F. Подмодуль $\Gamma(\mathfrak{a}, \mathfrak{b})$ в $E \otimes F$, порожденный всевозможными элементами вида $x \otimes y$, где $x \in \mathfrak{a}$ и $y \in \mathfrak{b}$, является двусторонним идеалом алгебры $E \otimes F$, и факторалгебра $(E \otimes F)/\Gamma(\mathfrak{a}, \mathfrak{b})$ изоморфна тензорному произведению $(E/\mathfrak{a}) \otimes (F/\mathfrak{b})$ факторалгебр $E/\mathfrak{a}$ и $F/\mathfrak{b}$.*

Доказательство предложения 6 § 1 без всяких изменений применимо и здесь, поскольку, как легко видеть, линейные отображения, определенные в этом доказательстве, являются *представлениями* соответствующих структур алгебры.

Пусть M и N — подалгебры алгебр E и F; каноническое отображение модуля $M \otimes N$ в модуль $E \otimes F$ (§ 1, n° 3) есть также *представление алгебры* $M \otimes N$ на подалгебру алгебры $E \otimes F$; в случае, когда A — *поле*, это представление есть *изоморфизм* (§ 1, следствие 3 предложения 7), и алгебра $M \otimes N$ отождествляется с ее образом при этом каноническом изоморфизме.

Точно так же (предполагая A снова произвольным коммутативным кольцом), если E и F — прямые суммы семейств своих подалгебр (E_λ) и (F_μ), то каноническое отображение каждой из алгебр $E_\lambda \otimes F_\mu$ в $E \otimes F$ есть изоморфизм, и при отождествлении каждой алгебры $E_\lambda \otimes F_\mu$ с ее образом при этом каноническом изоморфизме $E \otimes F$ является прямой суммой подалгебр $E_\lambda \otimes F_\mu$. При этом:

Предложение 2. *Если алгебра E есть прямая композиция* (гл. I, § 8) *подалгебр E_i $(1 \leqslant i \leqslant m)$, а алгебра F — прямая композиция подалгебр F_j $(1 \leqslant j \leqslant n)$, то алгебра $E \otimes F$ есть прямая композиция подалгебр $E_i \otimes F_j$.*

Достаточно доказать, что подалгебры $E_i \otimes F_j$ взаимно аннулируются (гл. I, § 8, предложение 7); но если $x \in E_i$, $x' \in E_h$, $y \in F_j$, $y' \in F_k$ и $(i, j) \neq (h, k)$, то $(x \otimes y)(x' \otimes y') = (xx') \otimes (yy') = 0$, поскольку одно из произведений xx', yy' равно нулю.

Замечания. 1) Замечание, сделанное в n° 3 § 1, применимо к тензорным произведениям алгебр, т. е. тензорное произведение двух алгебр существенно зависит от их общего *кольца операторов*, а не только от их структур *кольца* (без операторов).

2) Легко определить тензорное произведение любого конечного числа алгебр E_i над одним и тем же кольцом A; предоставляем читателю сформулировать для такого произведения свойства, установленные выше для тензорного произведения двух алгебр (см. Приложение I к этой главе). Отметим лишь, что канонические изоморфизмы, определенные в n° 7 § 1 («ассоциативность» тензорного произведения), в случае, когда E_i — алгебры, являются также изоморфизмами структур *алгебры*.

2. Примеры тензорных произведений алгебр

I. Пусть E и F — унитарные A-модули с конечными базисами; как мы видели (§ 1, предложение 9), структуры *A-модуля* в $\mathscr{L}(E \otimes F)$ и $\mathscr{L}(E) \otimes \mathscr{L}(F)$ канонически *отождествимы*; формула (6) § 1 показывает, что при этом отождествлении структура *алгебры* в $\mathscr{L}(E \otimes F)$ отождествляется с тензорным произведением структур алгебры в $\mathscr{L}(E)$ и $\mathscr{L}(F)$. Этот результат можно выразить также следующим образом (гл. II, § 6, n° 5):

Предложение 3. *Тензорное произведение алгебр квадратных матриц порядков p и q над коммутативным кольцом A с единицей изоморфно алгебре квадратных матриц порядка pq над A.*

II. Пусть E — алгебра над A, обладающая единичным элементом, свободным в E (и, следовательно, отождествимым с единицей кольца A); кольцо $\mathbf{M}_n(E)$ квадратных матриц n-го порядка *над E* есть также алгебра над A; покажем, что она *изоморфна тензорному произведению* $E \otimes \mathbf{M}_n(A)$. Действительно, отнеся

каждому тензорному произведению $t \otimes X \in E \otimes \mathbf{M}_n(A)$ матрицу $tX = Xt \in \mathbf{M}_n(E)$, мы получим представление алгебры $E \otimes \mathbf{M}_n(A)$ в $\mathbf{M}_n(E)$, поскольку $(tX)(t'X') = (tt')(XX')$. Чтобы убедиться в том, что это представление есть *изоморфизм* $E \otimes \mathbf{M}_n(A)$ *на* $\mathbf{M}_n(E)$, заметим, что матрицы E_{ij} канонического базиса A-модуля $\mathbf{M}_n(A)$ образуют также канонический базис в $\mathbf{M}_n(E)$ (рассматриваемом как правый или левый E-модуль); с другой стороны, каждый элемент из $E \otimes \mathbf{M}_n(A)$ однозначно представим в виде $\sum_{i,j} (t_{ij} \otimes E_{ij})$ (§ 1, следствие 1 предложения 7), и ему соответствует при рассматриваемом представлении матрица $\sum_{i,j} t_{ij} E_{ij} \in \mathbf{M}_n(E)$; тем самым предложение доказано.

III. Пусть S и T — любые два моноида, а $E = A^{(S)}$ и $F = A^{(T)}$ — их моноидные алгебры относительно кольца A (гл. II, § 7, n° 9); *тензорное произведение* $E \otimes F$ этих двух алгебр изоморфно моноидной алгебре $G = A^{(S \times T)}$ *моноида* $S \times T$ (гл. I, § 4, n° 5). Действительно, когда u и v пробегают соответственно S и T, элементы $u \otimes v$ образуют базис в $E \otimes F$, а элементы (u, v) — базис в G; тем самым отнесение элементу (u, v) элемента $u \otimes v$ определяет изоморфизм структуры модуля в $E \otimes F$ на структуру модуля в G, и в силу (1) ясно, что это отображение есть также изоморфизм структуры алгебры в $E \otimes F$ на структуру алгебры в G.

3. *Характеризация тензорного произведения двух алгебр над полем*

Пусть E и F — алгебры над *полем* K, имеющие каждая *единичный элемент*; K можно отождествить тогда (гл. II, § 7, n° 4) с подалгеброй каждой из алгебр E и F, сделав единицу e поля K общим единичным элементом этих алгебр. Тогда $e \otimes e$ будет единичным элементом в $E \otimes F$ и K можно будет отождествить также с подалгеброй $K(e \otimes e)$ алгебры $E \otimes F$. При этих соглашениях имеем:

Предложение 4. *Отображение* $x \longrightarrow x \otimes e$ (соответственно $y \longrightarrow e \otimes y$) *есть изоморфизм* E (соответственно F) *на некоторую подалгебру* E_1 (соответственно F_1) *алгебры* $E \otimes F$, *и каждый элемент из* E_1 *перестановочен с каждым элементом из* F_1.

Очевидно, $x \longrightarrow x \otimes e$ есть представление E в $E \otimes F$, ибо $(x \otimes e)(x' \otimes e) = (xx') \otimes e$; точно так же $y \longrightarrow e \otimes y$ есть представление F в $E \otimes F$, и так как

$$x \otimes y = (x \otimes e)(e \otimes y) = (e \otimes y)(x \otimes e),$$

то каждый элемент из E_1 перестановочен с каждым элементом из F_1. При этом, если $x \neq 0$ в E, то $x \otimes e \neq 0$, поскольку $e \neq 0$, а E и F — векторные пространства над K (§ 1, следствие 2 предложения 7). Тем самым отображения $x \longrightarrow x \otimes e$ и $y \longrightarrow e \otimes y$ — изоморфизмы (называемые в дальнейшем *каноническими*).

Эти изоморфизмы позволяют *отождествлять* E и F с их *образами* E_1 и F_1; тензорное произведение $x \otimes y$ отождествляется тогда с произведением $xy\,(=yx)$ в алгебре $E \otimes F$, что позволяет отказаться от обозначения $x \otimes y$; в частности, при $F = K$ тензорное произведение $E \otimes K$ отождествляется с E. Если M (соответственно N) — подалгебра в E (соответственно в F), то алгебра $M \otimes N$ отождествляется с подалгеброй в $E \otimes F$, порожденной произведениями $xy\,(=yx)$, где x пробегает M, а y пробегает N.

Пусть заданы алгебра G над полем K, имеющая единицу e (отождествляемую с единицей поля K), и две ее подалгебры F и G, содержащие K; исследуем, при каких условиях существует *изоморфизм* φ алгебры $E \otimes F$ на G, совпадающий на E и F (отождествленных указанным выше образом с подалгебрами алгебры $E \otimes F$) с тождественным отображением. Первое необходимое условие существования такого изоморфизма дает нам предложение 4: каждый элемент из E должен быть *перестановочным* с каждым элементом из F; мы говорим тогда, что E и F — две *коммутирующие* подалгебры алгебры G. При выполнении этого условия изоморфизм φ (если он существует) вполне определен, ибо тогда $\varphi(x \otimes y) = \varphi(x)\,\varphi(y) = xy$ в G. В любом случае, в силу билинейности отображения $(x, y) \longrightarrow xy$ произведения $E \times F$ в G, существует *линейное отображение* φ модуля $E \otimes F$ в G такое, что $\varphi(x \otimes y) = xy$ (§ 1, n° 2), и так как каждый элемент из E, по предположению, перестановочен с каждым элементом из F, то ясно, что φ есть *представление* алгебры $E \otimes F$ в алгебру G; будем называть его *каноническим представлением*.

Введем следующее определение:

Определение 1. *Пусть G — алгебра над полем K, имеющая единицу e* (отождествляемую с единицей поля K), *и E, F — подалгебры этой алгебры, содержащие K. E и F называются линейно раздельными над K, если:* 1° *подалгебры E и F коммутирующие;* 2° *каноническое представление $E \otimes F$ в G есть изоморфизм $E \otimes F$ в G.*

Тогда имеет место следующий критерий:

Теорема 1. *Пусть G — алгебра над полем K, имеющая единицу, и E, F — ее коммутирующие подалгебры, содержащие K.*

Для того чтобы E и F были линейно раздельными над K, необходимо и достаточно, чтобы в E существовал базис относительно K, являющийся свободным множеством в G при наделении G структурой правого модуля относительно F.

При этих условиях каноническое представление φ алгебры $E \otimes F$ в G есть изоморфизм $E \otimes F$ на подалгебру H в G, порожденную множеством $E \cup F$; далее, $E \cap F = K$, и каждое свободное множество в E (соответственно в F) *относительно K есть свободное множество в G, наделенном структурой правого модуля относительно F* (соответственно E).

Сформулированное условие очевидно *необходимо*, поскольку, в силу следствия 1 предложения 7 § 1, каждый базис в E есть базис в $E \otimes F$ относительно структуры правого F-модуля. Обратно, условие *достаточно*; действительно, образ H алгебры $E \otimes F$ при ее каноническом представлении φ совпадает с множеством всевозможных сумм $\sum_i x_i y_i$ в G, где $x_i \in E$ и $y_i \in F$; поэтому, если (a_λ) — базис E относительно K, H есть также *подмодуль* правого F-модуля G, *порожденный* семейством (a_λ). Таким образом, условие теоремы означает, что в E существует базис (a_λ) (относительно K), являющийся также базисом F-модуля H; а отсюда вытекает, что φ — взаимно однозначное отображение (гл. II, § 2, п° 4).

Остается убедиться в том, что $E \cap F = K$ в G; достаточно показать, что $E \cap F = K$ *в* $E \otimes F$. Возьмем в E базис, содержащий e, и пусть (b_ι) — семейство остальных элементов этого базиса; если $x \otimes e = e \otimes y$ для $x \in E$, $y \in F$, то, поскольку можно написать $x = \xi_0 e + \sum_\iota \xi_\iota b_\iota$, имеем $\xi_0 e \otimes e + \sum_\iota (\xi_\iota b_\iota \otimes e) = e \otimes y$, откуда, в силу следствия 1 предложения 7 § 1, вытекает, что $\xi_\iota = 0$ для всех ι, значит, $x \otimes e = e \otimes y \in K$.

Следствие 1. *Для того чтобы каноническое представление $E \otimes F$ в G было изоморфизмом $E \otimes F$ на G, необходимо и достаточно, чтобы в E существовал базис относительно K, который являлся бы базисом для G, рассматриваемого как правый модуль относительно F.*

Следствие 2. *Пусть E и F — коммутирующие подалгебры в G, имеющие каждая конечный ранг над K. Для того чтобы E и F были линейно раздельными над K, необходимо и достаточно, чтобы подалгебра в G, порожденная множеством $E \cup F$, имела ранг над K, равный произведению рангов E и F.*

Заметим, что понятие линейно раздельных подалгебр существенно зависит от того подполя K центра алгебры G, которое рассматривается как поле операторов этой алгебры; действительно, E и F, линейно раздельные над K, не могут быть линейно раздельными ни над каким подполем K_0 поля K, отличным от K, поскольку не выполнено необходимое для этого условие $E \cap F = K_0$ (кстати сказать, отнюдь еще не достаточное для того, чтобы подалгебры E и F были линейно раздельными над K_0; см. гл. V, § 3).

4. Расширение кольца операторов алгебры

Пусть B — коммутативное кольцо с единицей e и A — его подкольцо, содержащее e; B может рассматриваться как *алгебра* над A. Пусть E — алгебра над A; как мы видели (§ 2, n° 1), в тензорном произведении $B \otimes E$ A-модулей B и E условием $t \cdot (x \otimes y) = (tx) \otimes y$ $(t \in B,\ x \in B,\ y \in E)$ определяется структура *унитарного B-модуля*. Эта структура и умножение, введенное на $B \otimes E$ в n° 1, определяют в множестве $B \otimes E$ структуру *алгебры относительно B*; чтобы убедиться в этом, достаточно показать, что, каковы бы ни были $t \in B$, $z \in B \otimes E$, $z' \in B \otimes E$, имеют место равенства $t(zz') = (tz)\, z' = z\, (tz')$; так как каждое из этих трех произведений является линейной функцией от z и от z', достаточно проверить их равенство для $z = x \otimes y$ и $z' = x' \otimes y'$ (где x, x' — элементы из B и y, y' — элементы из E); но, в силу предположенной коммутативности кольца B, последнее очевидно.

Мы по-прежнему говорим, что определенная так алгебра над B получена путем *расширения* кольца операторов алгебры E *до* B,

и обозначаем ее $E_{(B)}$ во избежание всякого смешения с алгеброй $B \otimes E$ *над кольцом* A (получающейся при этом путем *сужения* кольца операторов алгебры $E_{(B)}$ *до* A).

Теперь, в каждой алгебре относительно B сужение кольца операторов до A определяет структуру алгебры относительно A; говоря о структуре алгебры относительно A в алгебре относительно B, мы всегда имеем в виду структуру, полученную указанным способом; при этом для обозначения представления алгебры относительно A (соответственно B) в алгебре относительно того же кольца мы, как и в § 2, вводим термины *A-представление* (соответственно *B-представление*).

Ясно, что каноническое отображение (§ 2, n° 1) $x \to e \otimes x$ алгебры E в $E_{(B)}$ есть A-представление E на подалгебру алгебры $B \otimes E$, поскольку $(e \otimes x)\,(e \otimes x') = e \otimes (xx')$ для всех $x \in E$ и $x' \in E$.

Предложение 5. *Для каждого A-представления f алгебры E в произвольную алгебру N относительно B существует однозначно определенное B-представление g алгебры $E_{(B)}$ в N такое, что $f(x) = g(e \otimes x)$ для всех $x \in E$.*

Принимая во внимание предложение 2 § 2, достаточно показать, что $g(yy') = g(y)\,g(y')$ в $E_{(B)}$, и так как образ E при каноническом отображении $x \to e \otimes x$ порождает $E_{(B)}$ (рассматриваемое как B-модуль), то можно ограничиться случаем, когда $y = e \otimes x$, $y' = e \otimes x'$, где x и x' принадлежат E; тогда имеем $yy' = e \otimes (xx')$, и соотношение $g(yy') = g(y)\,g(y')$ вытекает из того, что f есть A-представление.

Предложение 1 § 2 также распространяется на алгебры; проверку выполнения этого мы предоставим читателю. В силу установленного только что предложения 5, доказательство предложения 4 § 2 показывает тогда, что расширение кольца операторов алгебры также есть *транзитивная* операция; точнее говоря, если C — коммутативное кольцо с единицей e, A и B — его подкольца такие, что $e \in A \subset B$, и E — алгебра над A, то алгебра $E_{(C)}$ изоморфна алгебре $(E_{(B)})_{(C)}$.

Предложение 6. *Если алгебра E обладает базисом (a_λ) относительно A, то ее каноническое отображение $x \to e \otimes x$ в $E_{(B)}$*

есть A-изоморфизм; по отождествлении E с ее образом E_1 при этом изоморфизме (a_λ) является базисом алгебры $E_{(B)}$ относительно B, и каждое A-представление алгебры E в алгебру N относительно B однозначно продолжается до B-представления $\overline{f}$ алгебры $E_{(B)}$ в N.

Это непосредственно следует из установленного выше предложения 5 и теоремы 1 § 2.

Заметим, что *таблица умножения* базиса (a_λ) (гл. II, § 7, n° 2) *одна и та же* для алгебр E и $E_{(B)}$.

Предложение 7. *Пусть A — кольцо целостности, обладающее единицей (обозначаемой 1), K — его поле отношений и E — алгебра над A, все ненулевые элементы которой свободные* (относительно структуры A-модуля в A). *Тогда каноническое отображение $x \longrightarrow 1 \otimes x$ алгебры E в алгебру $E_{(K)}$ над полем K есть A-изоморфизм E на подалгебру E_1 в $K \otimes E$ такую, что $E_{(K)} = KE_1$; при отождествлении E с E_1 посредством этого изоморфизма каждое A-представление f алгебры E в алгебру G над K однозначно продолжается до K-представления $\overline{f}$ алгебры $E_{(K)}$ в G; если f — A-изоморфизм, то $\overline{f}$ — K-изоморфизм.*

Справедливость предложения вытекает из установленного выше предложения 5 и следствия 1 теоремы 2 § 2.

Упражнения. 1) Пусть E и F — алгебры над коммутативным кольцом A с единицей. Если $\mathfrak{a}$ — левый идеал в E и $\mathfrak{b}$ — левый идеал в F, то аддитивная подгруппа в $E \otimes F$, порожденная элементами $x \otimes y$, где x пробегает $\mathfrak{a}$ и y пробегает $\mathfrak{b}$, есть левый идеал алгебры $E \otimes F$.

2) Пусть E и F — алгебры над полем K, имеющие каждая единичный элемент, и C — центр алгебры E. Показать, что подалгебра алгебры $E \otimes F$, порожденная элементами, перестановочными со всеми элементами из E, совпадает с $C \otimes F$; центром алгебры $E \otimes F$ служит подалгебра $C \otimes D$, где D — центр F.

3) Пусть E_1, E_2, F_1, F_2 — алгебры над кольцом A. Если u — представление E_1 в E_2 и v — представление F_1 в F_2, то тензорное произведение $u \otimes v$ есть представление алгебры $E_1 \otimes F_1$ в алгебру $E_2 \otimes F_2$.

4) Пусть B — коммутативное кольцо с единицей e, A — его подкольцо, содержащее e, и E, F — алгебры над A. Показать, что алгебра $(E \otimes F)_{(B)}$ изоморфна алгебре $E_{(B)} \otimes F_{(B)}$.

5) Пусть E — алгебра над полем K и L — надполе этого поля. Показать, что если алгебра $E_{(L)}$ обладает единицей, то это же верно и для алгебры E. [Воспользоваться теоремой 1 § 5 главы II.]

§ 4. Тензоры и тензорные пространства

1. Тензоры

Определение 1. *Пусть E — унитарный модуль над коммутативным кольцом A. p раз контравариантным и q раз ковариантным тензором над E называется всякий элемент тензорного произведения $\bigotimes_{i=1}^{p+q} E_i$, где p из модулей E_i совпадают с E, а остальные q — с сопряженным модулем E^*; число $p+q$ называется порядком *) тензора.*

В случае, когда $q = 0$ (соответственно $p = 0$), имеется лишь один модуль тензоров порядка $p + q$, а именно p-я тензорная степень E (соответственно q-я тензорная степень E^*); его тензоры называют *контравариантными тензорами p-го порядка* (соответственно *ковариантными тензорами q-го порядка*); контравариантные тензоры первого порядка, т. е. элементы модуля E, называют также *контравариантными векторами*; точно так же ковариантные тензоры первого порядка, т. е. элементы сопряженного модуля E^* (линейные формы на E), называют *ковариантными векторами*. В дополнение к определению 1 условимся рассматривать *скаляры* (элементы кольца A) как тензоры и называть их *тензорами нулевого порядка*.

В случае, когда p и q отличны от нуля, p раз контравариантные и q раз ковариантные тензоры называют *смешанными*; они образуют $\frac{(p+q)!}{p!q!}$ различных модулей, но между любыми двумя из этих модулей существует каноническое взаимно однозначное соответствие (§ 1, п° 7); во многих случаях можно ограничиться рассмотрением лишь одного из них, например произведения $(\bigotimes^p E) \otimes (\bigotimes^q E^*)$, которое будет обозначаться $T_q^p(E)$ или просто E_q^p, если это не сможет повлечь путаницы. Элементами E_q^p служат

*) В русской математической литературе вместо «порядок тензора» говорят *валентность* (или, реже, *ранг*) тензора.— *Перев.*

всевозможные линейные комбинации тензоров вида $x_1x_2 \ldots$ $\ldots x_p x'_1 x'_2 \ldots x'_q$ (называемых также *разложимыми* тензорами), где x_i — произвольные элементы из E, а x'_j — произвольные элементы из E^* (мы опускаем символ $\otimes$ в обозначении этих тензоров). Пусть $\bigotimes_{\nu=1}^{p+q} E_\nu$ — другой модуль p раз контравариантных и q раз ковариантных тензоров такой, что $E_\nu = E$, когда ν есть один из членов строго возрастающей последовательности $(h_i)_{1\leqslant i\leqslant p}$ из p чисел интервала $[1, p+q]$, и $E_\nu = E^*$, когда ν есть один из членов строго возрастающей последовательности $(k_j)_{1\leqslant j\leqslant q}$, образованной остальными числами этого интервала; канонический изоморфизм E_q^p на $\bigotimes_{\nu=1}^{p+q} E_\nu$ относит каждому разложимому тензору $x_1 \ldots x_p x'_1 \ldots x'_q$ ($x_i \in E$, $x'_j \in E^*$) разложимый тензор $y_1 y_2 \ldots y_{p+q}$, где $y_{h_i} = x_i$ и $y_{k_j} = x'_j$ ($1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$).

Предположим теперь, что E обладает *конечным базисом* $(a_\lambda)_{1\leqslant\lambda\leqslant n}$ (что, несомненно, является наиболее важным случаем); будем в дальнейшем обозначать через $(a^\lambda)_{1\leqslant\lambda\leqslant n}$ базис в E^*, *сопряженный* к (a_λ) (гл. II, § 4, n° 4); тогда модуль E_q^p обладает базисом из n^{p+q} элементов, образованным разложимыми тензорами $a_{\lambda_1} \ldots a_{\lambda_p} a^{\mu_1} \ldots a^{\mu_q}$, где (λ_i) пробегает множество I^p всех последовательностей из p элементов интервала $I = [1, n] \subset \mathbf{N}$, а (μ_j) — множество I^q всех последовательностей из q элементов этого интервала. Говоря о *компонентах* тензора $x \in E_q^p$, мы всюду, где не оговорено противное, имеем в виду компоненты x относительно базиса, полученного таким способом, отправляясь от некоторого базиса (a_λ) модуля E; допуская вольность речи, их называют компонентами x *относительно базиса* (a_λ); компонента x относительно элемента $a_{\lambda_1} \ldots a_{\lambda_p} a^{\mu_1} \ldots a^{\mu_q}$ обозначается $\xi^{\lambda_1 \ldots \lambda_p}_{\mu_1 \ldots \mu_q}$, причем верхние индексы называются *контравариантными*, а нижние — *ковариантными*; таким образом,

$$x = \sum_{(\lambda_i),(\mu_j)} \xi^{\lambda_1 \ldots \lambda_p}_{\mu_1 \ldots \mu_q} a_{\lambda_1} \ldots a_{\lambda_p} a^{\mu_1} \ldots a^{\mu_q}. \qquad (1)$$

Если теперь $\bigotimes_{\nu=1}^{p+q} E_\nu$ — второй модуль p раз контравариантных и q раз ковариантных тензоров такой, что $E_\nu = E$ для $\nu = h_i$

$(1 \leqslant i \leqslant p)$ и $E_\nu = E^*$ для $\nu = k_j$ $(1 \leqslant j \leqslant q)$, то базис этого модуля, соответствующий базису (a_λ) модуля E, образован тензорами $b_1 b_2 \dots b_{p+q}$, где $b_{h_i} = a_{\lambda_i}$ и $b_{k_j} = a^{\mu_j}$, причем (λ_i) пробегает I^p, а (μ_j) пробегает I^q. Компоненты тензора, принадлежащего этому модулю, обозначают чаще всего так же, как и в случае модуля E_q^p; однако при желании избежать смешения этого модуля с другими контравариантный индекс λ_i помещают на i-м месте, незанятые же места оставляют пустыми или помечают точкой; например, компоненты тензора, принадлежащего $E \otimes E^* \otimes E^* \otimes E$, обозначают $\xi^{\lambda_1 \cdot\cdot \lambda_2}_{\cdot\ \mu_1 \mu_2 \cdot}$ или $\xi^{\lambda_1\ \ \lambda_2}_{\ \mu_1 \mu_2}$, когда предпочитают точную запись, и $\xi^{\lambda_1 \lambda_2}_{\mu_1 \mu_2}$ — в противном случае.

Пусть $(\bar{a}_\lambda)$ — другой базис модуля E и $(\bar{a}^\lambda)$ — сопряженный базис в E^*; если P — матрица перехода от (a_λ) к $(\bar{a}_\lambda)$ (гл. II, § 6, n° 9), то матрицей перехода от (a^λ) к $(\bar{a}^\lambda)$ будет матрица ${}^tP^{-1}$, *контрагредиентная* к P (гл. II, § 6, n° 9); отсюда следует, что в E_q^p матрицей перехода от базиса $(a_{\lambda_1} \dots a_{\lambda_p} a^{\mu_1} \dots a^{\mu_q})$ к базису $(\bar{a}_{\lambda_1} \dots \bar{a}_{\lambda_p} \bar{a}^{\mu_1} \dots \bar{a}^{\mu_q})$ служит *тензорное произведение* $P_1 \otimes P_2 \otimes \dots \otimes P_{p+q}$, где $P_i = P$ $(1 \leqslant i \leqslant p)$ и $P_{p+j} = {}^tP^{-1}$ $(1 \leqslant j \leqslant q)$. Аналогичный результат справедлив для любого другого модуля p раз контравариантных и q раз ковариантных тензоров.

Как мы увидим ниже (n° 4), при вычислениях с тензорами элементы матрицы перехода P принято обозначать α_λ^μ (или, лучше, $\alpha_\lambda^{\cdot\mu}$), где λ — индекс *столбца* рассматриваемого элемента, а μ — индекс *строки*; напротив, элементы контрагредиентной матрицы ${}^tP^{-1}$ обозначаются β_μ^λ (или, лучше, $\beta^\lambda_{\cdot\mu}$), где λ — индекс столбца элемента, а μ — индекс строки; при этих обозначениях компоненты $\xi^{\lambda_1 \dots \lambda_p}_{\mu_1 \dots \mu_q}$ тензора относительно базиса (a_λ) выражаются через компоненты $\bar{\xi}^{\lambda_1 \dots \lambda_p}_{\mu_1 \dots \mu_q}$ этого тензора относительно базиса $(\bar{a}_\lambda)$ по формулам

$$\xi^{\lambda_1 \dots \lambda_p}_{\mu_1 \dots \mu_q} = \sum_{(\varrho_i)\,(\sigma_j)} \alpha^{\lambda_1}_{\varrho_1} \dots \alpha^{\lambda_p}_{\varrho_p} \beta^{\sigma_1}_{\mu_1} \dots \beta^{\sigma_q}_{\mu_q} \bar{\xi}^{\varrho_1 \dots \varrho_p}_{\sigma_1 \dots \sigma_q}. \qquad (2)$$

Замечание. Многие авторы придерживаются при вычислениях с тензорами такого соглашения: если написано выражение,

содержащее компоненты некоторых тензоров и, возможно, векторов выбранного базиса модуля E (или сопряженного базиса), то под ним подразумевается выражение, получающееся из него следующим способом: каждому из индексов, фигурирующих в написанном выражении *один раз как верхний индекс и один раз как нижний* (такие индексы называют «*немыми индексами*» выражения), придают все значения от 1 до n и затем образуют *сумму* всех полученных так элементов. При таком соглашении запись формул (1) и (2) принимает соответственно вид

$$x = \xi_{\mu_1 \dots \mu_q}^{\lambda_1 \dots \lambda_p} a_{\lambda_1} \dots a_{\lambda_p} a^{\mu_1} \dots a^{\mu_q},$$

$$\xi_{\mu_1 \dots \mu_q}^{\lambda_1 \dots \lambda_p} = \alpha_{\varrho_1}^{\lambda_1} \dots \alpha_{\varrho_p}^{\lambda_p} \beta_{\mu_1}^{\sigma_1} \dots \beta_{\mu_q}^{\sigma_q} \xi_{\sigma_1 \dots \sigma_q}^{\varrho_1 \dots \varrho_p}.$$

В настоящем трактате мы не пользуемся этим соглашением, которое могло бы повлечь досадную путаницу.

2. *Тензорные пространства; тензорные отображения*

Пусть u — *автоморфизм* модуля E и $\check{u}$ — контрагредиентный автоморфизм сопряженного модуля E^* (гл. II, § 4, n° 10); тензорное произведение $\bigotimes_{i=1}^{p+q} u_i$, где $u_i = u$, когда $1 \leqslant i \leqslant p$, и $u_i = \check{u}$, когда $p+1 \leqslant i \leqslant p+q$, есть *автоморфизм* модуля E_q^p (§ 1, следствие предложения 10); мы будем обозначать его u_q^p. В силу формулы (6) § 1, отображение $u \longrightarrow u_q^p$ есть *представление* группы $\mathbf{GL}(E)$ автоморфизмов модуля E в группу $\mathbf{GL}(E_q^p)$ автоморфизмов модуля E_q^p. Тем самым автоморфизмы модуля E выступают в качестве *операторов* внешнего закона $(u, x) \longrightarrow u_q^p(x)$ на E_q^p; если это не сможет повлечь путаницу, мы будем обозначать композицию $u_q^p(x)$ оператора u и тензора x просто $u \cdot x$ (или ux); при этом обозначении имеем $(u \circ v) \cdot x = u \cdot (v \cdot x)$. Аналогичный внешний закон определяется на каждом модуле p раз контравариантных и q раз ковариантных тензоров, где p и q не равны одновременно нулю. Для каждого автоморфизма u модуля E условимся обозначать через u_0^0 тождественное отображение кольца $A = E_0^0$ на себя; это позволит распространить определение указанного внешнего закона и на случай, когда $p = q = 0$.

Определение 2. *Тензорным пространством над A-модулем E называется каждый подмодуль H модуля тензоров* $\bigotimes_{i=1}^{p+q} E_i$ (где

p множителей равны E, а остальные q равны E^*), *устойчивый относительно внешнего закона* $(u, x) = u \cdot x$ *на* $\bigotimes_{i=1}^{p+q} E_i$ (иначе говоря, такой, что для каждого тензора $x \in H$ и каждого автоморфизма u модуля E имеем $u \cdot x \in H$), *наделенный алгебраической структурой, определяемой, с одной стороны, двумя законами, определяющими его структуру A-модуля, и, с другой стороны, внешним законом, индуцированным на H законом* $(u, x) = u \cdot x$.

Замечания. 1) Тензорное пространство H, наделенное структурой, определяемой внешним законом $(u, x) \to u \cdot x$, есть пример множества, наделенного *группой операторов*, в смысле гл. I, § 7, n° 2; при этом указанный внешний закон дистрибутивен относительно заданного на H сложения и перестановочен с внешним законом $(\lambda, x) \to \lambda x$ структуры A-модуля в H.

2) В случае, когда $q = 0$ (иными словами, когда речь идет о модуле *контравариантных* тензоров над E), u_0^p можно определить не только для автоморфизмов модуля E, но также для любого его *эндоморфизма* u, как тензорное произведение p эндоморфизмов, совпадающих с u; если v — второй эндоморфизм модуля E и $w = v \circ u$, то $w_0^p = v_0^p \circ u_0^p$; но заметим, что $(u + v)_0^p$ вообще не равно $u_0^p + v_0^p$; следовательно, определенный на E_0^p внешний закон $(u, x) \to u_0^p(x)$, имеющий своим множеством операторов кольцо $\mathscr{L}(E)$, *не определяет структуру левого модуля*.

Подмножество L тензорного пространства H над E, являющееся *подмодулем* модуля H и *устойчивое* относительно внешнего закона $(u, x) \to u \cdot x$, будучи наделенным индуцированной из H структурой, очевидно является тензорным пространством над E; мы будем называть L *тензорным подпространством* тензорного пространства H.

Определение 3. *Пусть F и G — тензорные пространства над A-модулем E. Тензорным отображением F в G называется всякое представление f F в G относительно структур тензорного пространства в этих двух множествах.*

Согласно общему определению представлений (гл. I, § 4, n° 4), то же можно выразить, сказав, что f есть *линейное* отображение модуля F в модуль G такое, что $f(u \cdot x) = u \cdot f(x)$ для

каждого автоморфизма u модуля E и каждого тензора $x \in F$. Если, например, $F = E_q^p$, $G = E_s^r$, то это соотношение равносильно соотношению $f(u_q^p(x)) = u_s^r(f(x))$.

Другой способ выражения этого тождества состоит в утверждении, что $f(x)$ есть *ковариант* тензора x относительно представлений $u \to u_q^p$ и $u \to u_s^r$ группы $\mathbf{GL}(E)$ (гл. I, § 7, n° 4).

Из определения 3 явствует, что если H есть тензорное подпространство в F, то $f(H)$ есть тензорное подпространство в G; если K — тензорное подпространство в G, то $f^{-1}(K)$ — тензорное подпространство в F.

Пусть теперь F, G, H — тензорные пространства над E; отображение f произведения $F \times G$ в H называется *тензорным отображением*, если f — *билинейное* отображение такое, что для каждого автоморфизма u модуля E имеет место тождество $f(u \cdot x,\ u \cdot y) = u \cdot f(x, y)$; при $F = E_q^p$, $G = E_{q'}^{p'}$, $H = E_s^r$ это последнее соотношение равносильно соотношению $f(u_q^p(x), u_{q'}^{p'}(y)) = u_s^r(f(x, y))$. Аналогично определяются тензорные отображения произведения любого числа тензорных пространств в тензорное пространство.

Согласно схолии из n° 2 § 1, для определения тензорного отображения f тензорного пространства E_q^p в E_s^r достаточно задать значения f на *разложимых* тензорах $x_1 \dots x_p x'_1 \dots x'_q$ (в функции от элементов x_i и x'_j) и проверить, с одной стороны, что отображение

$$(x_1, \dots, x_p, x'_1, \dots, x'_q) \to f(x_1 \dots x_p x'_1 \dots x'_q)$$

полилинейно и, с другой стороны, что для любого автоморфизма u модуля E выполняется тождество

$$f(u(x_1) \dots u(x_p)\, \check{u}(x'_1) \dots \check{u}(x'_q)) = u_s^r(f(x_1 \dots x_p x'_1 \dots x'_q)).$$

Из этого критерия сразу следует, что определенные в n° 1 *канонические изоморфизмы* различных модулей p раз контравариантных и q раз ковариантных тензоров (с фиксированными p и q) являются изоморфизмами структур *тензорных пространств* в этих модулях.

3. Умножение и свертывание

Пусть $F = \bigotimes_{i=1}^{p+q} E'_i$ — модуль p раз контравариантных и q раз ковариантных тензоров над E ($E'_i = E$ для p индексов i, $E'_i = E^*$ для q остальных индексов) и $G = \bigotimes_{j=1}^{r+s} E''_j$ — модуль r раз контравариантных и s раз ковариантных тензоров ($E''_j = E$ для r индексов j и $E''_j = E^*$ для остальных s индексов). Как мы знаем (§ 1, n° 7), тензорное произведение $F \otimes G$ можно отождествить посредством канонического изоморфизма с модулем $H = \bigotimes_{k=1}^{p+q+r+s} E_k$ $p + r$ раз контравариантных и $q + s$ раз ковариантных тензоров, определяемым условиями $E_k = E'_k$, когда $1 \leqslant k \leqslant p + q$, и $E_{p+q+h} = E''_h$, когда $1 \leqslant h \leqslant r + s$. Когда это отождествление произведено, $(x, y) \longrightarrow x \otimes y$ есть билинейное отображение $F \times G$ в H, значением которого для пары разложимых тензоров $x = \bigotimes_{i=1}^{p+q} x_i \in F$, $y = \bigotimes_{j=1}^{r+s} y_j \in G$ служит тензор $x \otimes y = \bigotimes_{k=1}^{p+q+r+s} z_k$, где $z_k = x_k$, когда $1 \leqslant k \leqslant p + q$, и $z_{p+q+h} = y_h$, когда $1 \leqslant h \leqslant r + s$. Это отображение, очевидно являющееся *тензорным*, называется *умножением* тензоров из F и G; в соответствии с общими соглашениями, тензор $x \otimes y \in H$ ($x \in F$, $y \in G$) при отсутствии опасности смешения обозначается также xy.

В предыдущем определении неявно предполагается, что p и q не равны одновременно нулю; на случай $p = q = 0$ определение умножения распространяется путем принятия произведения скаляра $\alpha \in A$ и тензора $y \in G$ равным их произведению αy относительно внешнего закона структуры A-модуля в G. Аналогично определение и для случая $r = s = 0$.

Понятие произведения любых двух смешанных тензоров позволяет придать определению тензорного отображения произведения $F \times G$ тензорных пространств F и G в тензорное пространство H такой вид: это — отображение f, для которого существует тензорное отображение g тензорного пространства $F \otimes G$ в H, удовлетворяющее тождеству $f(x, y) = g(xy)$.

Пусть $p > 0$ и $q > 0$. *Свертыванием* i-го контравариантного индекса с j-м ковариантным ($1 \leqslant i \leqslant p$, $1 \leqslant j \leqslant q$) называется линейное отображение c_j^i тензорного пространства E_q^p в E_{q-1}^{p-1}, относящее каждому разложимому тензору $z = x_1 \dots x_p x_1' \dots x_q'$ тензор

$$c_j^i(z) = \langle x_i, x_j' \rangle x_1 \dots x_{i-1} x_{i+1} \dots x_p x_1' \dots x_{j-1}' x_{j+1}' \dots x_q'.$$

Ясно, что этим действительно определяется линейное отображение (§ 1, n° 2, схолия); при этом, так как для каждого автоморфизма u модуля E имеем $\langle u(x_i), \overset{\vee}{u}(x_j') \rangle = \langle x_i, x_j' \rangle$, то

$$c_j^i(u \cdot z) = \langle x_i, x_j' \rangle u(x_1) \dots u(x_{i-1}) u(x_{i+1}) \dots u(x_p) \overset{\vee}{u}(x_1') \dots$$
$$\dots \overset{\vee}{u}(x_{j-1}') \overset{\vee}{u}(x_{j+1}') \dots \overset{\vee}{u}(x_q') = u \cdot c_j^i(z),$$

что показывает, что c_j^i есть *тензорное* отображение E_q^p в E_{q-1}^{p-1}. Так же определяются свертывания в любых модулях p раз контравариантных и q раз ковариантных тензоров.

Пусть $\zeta_{\mu_1 \dots \mu_q}^{\lambda_1 \dots \lambda_p}$ — компоненты z относительно базиса (a_λ) модуля E, так что

$$z = \sum_{(\lambda_i), (\mu_j)} \zeta_{\mu_1 \dots \mu_q}^{\lambda_1 \dots \lambda_p} a_{\lambda_1} \dots a_{\lambda_p} a^{\mu_1} \dots a^{\mu_q}.$$

Так как $\langle a_\lambda, a^\mu \rangle = \delta_\lambda^\mu$ (кронекеровский символ), то

$$c_j^i(z) = \sum \Big(\sum_{\lambda_i=1}^{n} \zeta_{\mu_1 \dots \mu_{j-1} \lambda_i \mu_{j+1} \dots \mu_q}^{\lambda_1 \dots \lambda_i \dots \lambda_p} \Big) a_{\lambda_1} \dots a_{\lambda_{i-1}} a_{\lambda_{i+1}} \dots a_{\lambda_p} a^{\mu_1} \dots$$
$$\dots a^{\mu_{j-1}} a^{\mu_{j+1}} \dots a^{\mu_q},$$

где первая сумма распространяется на все индексы, отличные от λ_i и μ_j. Иными словами, компоненты свернутого тензора $c_j^i(z)$ относительно базиса (a_λ) задаются формулой

$$\zeta_{\mu_1 \dots \mu_{j-1} \mu_{j+1} \dots \mu_q}^{\lambda_1 \dots \lambda_{i-1} \lambda_{i+1} \dots \lambda_p} = \sum_{\varrho=1}^{n} \zeta_{\mu_1 \dots \mu_{j-1} \varrho \mu_{j+1} \dots \mu_q}^{\lambda_1 \dots \lambda_{i-1} \varrho \lambda_{i+1} \dots \lambda_p}. \tag{3}$$

Разумеется, в смешанном тензоре можно свертывать *несколько* пар индексов, что, очевидно, сводится к *последовательному* свертыванию каждой из этих пар (в любом порядке).

Часто приходится выполнять операцию, состоящую в образовании *произведения* двух тензоров (не являющихся одновре-

менно ни контравариантными, ни ковариантными) и затем *свертывании* в полученном смешанном тензоре одной или нескольких пар индексов; определяемое этим отображение, называемое *свернутым произведением* (для рассматриваемых пар индексов), также является тензорным отображением.

Например, пусть x_1x_2 — контравариантный тензор, произведение двух векторов x_1, x_2, и $x'_1x'_2$ — ковариантный тензор, произведение двух линейных форм x'_1, x'_2; если образовать произведение этих двух тензоров и затем свернуть в нем первый контравариантный индекс с первым ковариантным, а второй контравариантный индекс — со вторым ковариантным, то получится скаляр (тензор нулевого порядка) $\langle x_1, x'_1\rangle \langle x_2, x'_2\rangle$.

4. *Эндоморфизмы смешанных тензоров второго порядка*

Пусть E и F — A-модули с *конечными базисами*. Предложение 2 § 1, примененное к модулям E и F^*, определяет канонический изоморфизм модуля билинейных форм на $E \times F^*$ на модуль $\mathscr{L}(E, F^{**})$ линейных отображений E во второй сопряженный к F: билинейной форме f на $E \times F^*$ отвечает линейное отображение, относящее каждому $x \in E$ линейную форму $y' \to f(x, y')$ на F^*. Но F^{**} отождествимо с F (гл. II, § 4, n° 4); с другой стороны, ранее был определен канонический изоморфизм тензорного произведения $E^* \otimes F$ на модуль билинейных форм на $E \times F^*$ (§ 1, n° 5), относящий тензорному произведению $x' \otimes y$ билинейную форму

$$(x, y') \to \langle x, x'\rangle \langle y, y'\rangle$$

на $E \times F^*$. Отсюда:

Предложение 1. *Если E и F — A-модули с конечными базисами, то линейное отображение $E^* \otimes F$ в $\mathscr{L}(E, F)$, относящее каждому тензорному произведению $x' \otimes y$ линейное отображение $x \to \langle x, x'\rangle y$, есть изоморфизм $E^* \otimes F$ на $\mathscr{L}(E, F)$.*

Этот изоморфизм и изоморфизм, обратный ему, будут называться *каноническими*.

Из предложения 1, в частности, вытекает, что каждое линейное отображение u модуля E в F есть сумма конечного числа

линейных отображений вида $x \to \langle x, x' \rangle y$. Впрочем, это легко установить и непосредственно: если (a_i) — базис модуля E, то для каждого $x = \sum_i \xi_i a_i \in E$ имеем

$$u(x) = \sum_i \xi_i u(a_i) = \sum_i \langle x, a^i \rangle u(a_i),$$

где (a^i) — сопряженный базис модуля E^*. Мы видим при этом, что если $\widetilde{u}$ — элемент из $E^* \otimes F$, отвечающий u при каноническом изоморфизме, то для каждого базиса (a_i) модуля E

$$\widetilde{u} = \sum_i a^i \otimes u(a_i). \tag{4}$$

В том случае, когда $F = E$, канонический изоморфизм $u \to \widetilde{u}$ относит каждому эндоморфизму u модуля E *смешанный тензор* $\widetilde{u}$ на E (принадлежащий $E^* \otimes E$), один раз контравариантный и один раз ковариантный. Если x_i^j — компоненты этого тензора относительно базиса (a_i) модуля E, так что $\widetilde{u} = \sum_{i,j} \alpha_i^j a^i a_j$, то, как показывает сравнение с (4), $u(a_i) = \sum_j \alpha_i^j a_j$; иными словами, *компонента* α_i^j *тензора* $\widetilde{u}$ *есть элемент матрицы эндоморфизма* u (относительно того же базиса), *находящийся на пересечении* i*-го столбца с* j*-й строкой.*

Замечания. 1) Каждому эндоморфизму u' модуля E^*, сопряженного к E, так же соответствует смешанный тензор $\widetilde{u'}$, принадлежащий на этот раз модулю $E \otimes E^*$ (при отождествлении E^{**} с E); так же, как выше, устанавливается, что для каждого базиса (a_i) модуля E

$$\widetilde{u'} = \sum_i u_i u'(a^i),$$

так что компонентой $\beta_{\cdot j}^i$ тензора $\widetilde{u'}$ относительно (a_i) служит элемент матрицы эндоморфизма u' (относительно базиса (a^i)), стоящий на пересечении i-го столбца и j-й строки. В частности, если $u' = {}^t u$, то тензоры $\widetilde{u}$ и $\widetilde{u'}$ соответствуют друг другу при канонических изоморфизмах между $E^* \otimes E$ и $E \otimes E^*$ (№ 1).

2) Как мы знаем (§ 1, № 2), каждому *билинейному* отображению $E \times E$ в E можно отнести линейное отображение $E \otimes E$ в E, и следовательно, согласно предыдущему,— элемент из $(E \otimes E)^* \otimes E$, иными словами, *дважды ковариантный и один раз контравариантный тензор*, принадлежащий модулю $E^* \otimes E^* \otimes E$. В частности, каждой структуре алгебры в E (гл. II, § 7), поскольку она определяется билинейным

отображением $(x, y) \to xy$, соответствует такой тензор; коэффициенты $\gamma_{\lambda\mu\nu}$, входящие в таблицу умножения этой алгебры относительно базиса (a_λ) (гл. II, § 7, n° 2),— это не что иное, как компоненты соответствующего тензора относительно указанного базиса.

3) Более общим образом, каждый модуль p раз контравариантных и q раз ковариантных тензоров над E изоморфен модулю линейных отображений $E_{r'}^{r}$ в $E_{s'}^{s}$ при всякой системе целых положительных r, s, r', s' такой, что $r' + s = p$ и $r + s' = q$.

5. *След эндоморфизма. След матрицы*

Определение 4. *Пусть E — A-модуль с конечным базисом. Следом* $\mathrm{Tr}\,(u)$ *его эндоморфизма u называется скаляр $c_1^1(\widetilde{u})$, полученный путем свертывания смешанного тензора $\widetilde{u}$, соответствующего u.*

То же самое можно выразить, сказав, что для любых пар конечных семейств (x_i') элементов из E^* и (y_i) элементов из E таких, что тождественно $u(x) = \sum_i \langle x, x_i' \rangle y_i$, имеет место равенство

$$\mathrm{Tr}\,(u) = \sum \langle y_i, x_i' \rangle. \tag{5}$$

°Как мы впоследствии узнаем, это последнее определение дает в некоторых случаях отправной пункт для обобщения понятия следа на (непрерывные) эндоморфизмы топологических векторных пространств.°

Если $U = (\alpha_j^i)$ — матрица эндоморфизма u относительно базиса (a_i) модуля E, след $\mathrm{Tr}\,(u)$ принимается, по определению, также за *след матрицы* U и обозначается тогда $\mathrm{Tr}\,(U)$; согласно формуле (4), имеем $\mathrm{Tr}\,(u) = \sum_i \langle u(a_i), a^i \rangle = \sum_i \alpha_i^i$; иными словами, *след квадратной матрицы — это сумма ее диагональных элементов.*

Определение следа матрицы показывает, что следы *подобных* матриц X и PXP^{-1} (гл. II, § 6, n° 11) *равны*. Это предложение может быть также выведено из следующего более общего:

Предложение 2. *Каковы бы ни были матрица X из m строк и n столбцов и матрица Y из n строк и m столбцов над коммутативным кольцом A,*

$$\mathrm{Tr}\,(XY) = \mathrm{Tr}\,(YX). \tag{6}$$

Доказательство этого утверждения сводится к доказательству того, что $\mathrm{Tr}(u \circ v) = \mathrm{Tr}(v \circ u)$ для линейного отображения u модуля $E = A^n$ в $F = A^m$ и линейного отображения v модуля F в E; при этом можно ограничиться тем случаем, когда u имеет вид $x \longrightarrow \langle x, a' \rangle b$ ($b \in F$, $a' \in E^*$), а v — вид $y \longrightarrow \langle y, b' \rangle a$ ($a \in E$, $b' \in F^*$), поскольку каждое линейное отображение есть сумма отображений этого вида, а $\mathrm{Tr}(w)$ — линейная функция от w; но в этом частном случае имеем

$$\mathrm{Tr}(u \circ v) = \mathrm{Tr}(v \circ u) = \langle a, a' \rangle \langle b, b' \rangle$$

согласно определению 4.

Следствие. *Пусть* $(X_i)_{1 \leqslant i \leqslant p}$ — *конечная последовательность* p *матриц над коммутативным кольцом* A *таких, что, обозначая через* m_i *число строк и через* n_i *число столбцов матрицы* X_i, *имеем* $n_i = m_{i+1}$ *при* $1 \leqslant i \leqslant p-1$ *и* $n_p = m_1$. *При этих условиях*

$$\mathrm{Tr}(X_1 X_2 \ldots X_p) = \mathrm{Tr}(X_i X_{i+1} \ldots X_p X_1 \ldots X_{i-1}) \qquad (7)$$

(«инвариантность относительно круговых подстановок»).

Достаточно применить (6) к произведению $(X_i \ldots X_p)(X_1 \ldots \ldots X_{i-1})$.

Заметим, что, напротив, для произвольных матриц X, Y, Z вообще говоря, $\mathrm{Tr}(XYZ) \neq \mathrm{Tr}(XZY)$.

Пусть $X = (\xi_{ij})$, $Y = (\eta_{ij})$ — квадратные матрицы n-го порядка; тогда $\mathrm{Tr}(XY) = \sum_{i,j} \xi_{ij} \eta_{ji}$ (что дает второе доказательство предложения 2); кроме того, эта формула показывает, что каждая *линейная форма* на A-модуле $\mathbf{M}_n(A)$ квадратных матриц n-го порядка над A может быть представлена, и притом единственным способом, в виде $X \longrightarrow \mathrm{Tr}(PX)$, где P — фиксированная квадратная матрица; это отображение может быть тождественно нулевым, лишь если $P = 0$.

Мы выведем из этого замечания, что предложение 2 *характеризует* (с точностью до постоянного множителя) след матрицы среди линейных форм на $\mathbf{M}_n(A)$; а именно:

Предложение 3. *Если* f — *линейная форма на модуле* $\mathbf{M}_n(A)$, *для которой тождественно* $f(XY) = f(YX)$, *то существует скаляр* $\varrho \in A$ *такой, что* $f(X) = \varrho\,\mathrm{Tr}(X)$ *для каждой матрицы* X.

Действительно, существует фиксированная матрица P такая, что $f(X) = \mathrm{Tr}(PX)$ для всех $X \in \mathrm{M}_n(A)$; поэтому условие $f(XY) = f(YX)$ записывается в виде $\mathrm{Tr}(PXY) = \mathrm{Tr}(PYX)$, или, на основании (7), $\mathrm{Tr}(PXY) = \mathrm{Tr}(XPY)$, или, наконец, $\mathrm{Tr}((PX - XP)Y) = 0$; так как это соотношение имеет место для каждой матрицы Y, заключаем, что $PX = XP$ для каждой матрицы X, откуда, в силу следствия 1 предложения 5 § 2 главы II, $P = \rho I$ (где I — единичная матрица), и предложение доказано.

В случае квадратных матриц над полем K предложение 3 допускает следующее истолкование: векторное подпространство векторного пространства $\mathrm{M}_n(K)$, порожденное матрицами $XY - YX$, есть *гиперплоскость*.

6. Тензорная алгебра

Пусть E — унитарный A-модуль и $T(E)$ — *прямая сумма* всех его тензорных степеней $\bigotimes^p E$, где p пробегает множество $\mathbf{N}$ целых чисел $\geqslant 0$. Понятие произведения двух тензоров позволяет определить в $T(E)$ структуру *алгебры* относительно A. Действительно, каждый элемент $z \in T(E)$ однозначно представим в виде $z = \sum_{p=0}^{\infty} z_p$, где z_p — контравариантный тензор p-го порядка (равный нулю для всех кроме конечного числа значений p). Пусть также $z' = \sum_{p=0}^{\infty} z'_p \in T(E)$. Положим $zz' = \sum_{p,\,q} z_p z'_q$. Очевидно, определенное так на $T(E)$ умножение двояко дистрибутивно относительно сложения; оно ассоциативно в силу соотношения $(z_p z_q) z_r = z_p (z_q z_r)$ между тремя тензорами порядков p, q, r, очевидного для разложимых тензоров и распространяющегося на произвольные тензоры по дистрибутивности. Наконец, ясно, что $\alpha(zz') = (\alpha z) z' = z(\alpha z')$ для каждого скаляра $\alpha \in A$. Тем самым $T(E)$ действительно есть алгебра над A; она называется *тензорной алгеброй модуля* E. Эта алгебра имеет своим единичным элементом единицу ε кольца A и вообще не коммутативна; для элементов из E (контравариантных векторов) умножение в $T(E)$ дает не что иное, как *тензорное произведение*, определенное-

в n° 2 § 1; тем самым множество $A \bigcup E$ составляет *систему образующих* алгебры $T(E)$. Если E обладает базисом (a_λ), то $T(E)$ обладает (бесконечным) базисом, образованным единичным элементом и всеми тензорами $a_{\lambda_1} a_{\lambda_2} \ldots a_{\lambda_p}$, где (λ_i) пробегает множество всевозможных конечных последовательностей (с любым числом членов) элементов множества индексов; таблица умножения этого базиса задается соотношениями

$$(a_{\lambda_1} \ldots a_{\lambda_p})(a_{\mu_1} \ldots a_{\mu_q}) = a_{\lambda_1} \ldots a_{\lambda_p} a_{\mu_1} \ldots a_{\mu_q}.$$

Каждое *линейное отображение* u модуля E в произвольный A-модуль F однозначно продолжается до *представления* алгебры $T(E)$ в алгебру $T(F)$. Действительно, если $\bar{u}$ — такое продолжение, то $\bar{u}(\varepsilon) = \varepsilon$, откуда $\bar{u}(\alpha) = \bar{u}(\alpha\varepsilon) = \alpha\bar{u}(\varepsilon) = \alpha$ для любого скаляра α; с другой стороны, для всякого разложимого тензора $z_p = x_1 x_2 \ldots x_p$ порядка $p > 0$ мы должны иметь

$$\bar{u}(z_p) = u(x_1)\, u(x_2) \ldots u(x_p) = u^p(z_p),$$

где u^p означает p-ю тензорную степень u, и это соотношение должно выполняться также для любого контравариантного тензора p-го порядка, поскольку такой тензор есть сумма разложимых тензоров. Следовательно, для каждого элемента $z = \sum_{p=0}^{\infty} z_p$ из $T(E)$, разложенного в сумму тензоров различных порядков, должно выполняться равенство $\bar{u}(z) = \sum_{p=0}^{\infty} \bar{u}(z_p) = \sum_{p=0}^{\infty} u^p(z_p)$ (где u^0 означает тождественное отображение A на себя). Обратно, ясно, что так определенное отображение $\bar{u}$ действительно является представлением $T(E)$ в $T(F)$. $\bar{u}$ будет называться *каноническим продолжением* u на $T(E)$. Если v — линейное отображение F в A-модуль G и $\bar{v}$ — его каноническое продолжение на $T(F)$, то каноническое продолжение композиции $v \circ u$ на $T(E)$ совпадает с $\bar{v} \circ \bar{u}$. В частности, если u — автоморфизм модуля E, то $\bar{u}$ — автоморфизм алгебры $T(E)$.

Если E — *подмодуль* модуля F и u — каноническое отображение E в F, то $\bar{u}$ есть представление $T(E)$ в $T(F)$, также называемое *каноническим*; оно не всегда взаимно однозначно (см. § 2, упражнение 4). Однако, если F — *векторное пространство*, то

$\widetilde{u}$ есть *изоморфизм* $T(E)$ в $T(F)$ (§ 1, следствие 3 предложения 7), и $T(E)$ часто *отождествляется* посредством него с подалгеброй в $T(F)$, являющейся его образом.

Упражнения. 1) Пусть E — конечномерное векторное пространство и z — тензор, принадлежащий E_q^p. Пусть, далее, W_i' для каждого контравариантного индекса i ($1 \leqslant i \leqslant p$) есть подпространство в E^*, образованное теми $x' \in E^*$, для которых $c_{q+1}^{i}(z \cdot x') = 0$, и V_i — подпространство в E, ортогональное к W_i'. Пусть, наконец, W_j для каждого ковариантного индекса j ($1 \leqslant j \leqslant q$) — подпространство в E, образованное теми $x \in E$, для которых $c_j^1(x \cdot z) = 0$, и V_j' — подпространство в E^*, ортогональное к W_j. Показать, что z принадлежит тензорному произведению $(\bigotimes_{i=1}^{p} V_i) \otimes (\bigotimes_{j=1}^{q} V_j')$; при этом, если $(U_i)_{1 \leqslant i \leqslant p}$ — семейство подпространств из E и $(U_j')_{1 \leqslant j \leqslant q}$ — семейство подпространств из E^* такие, что z принадлежит тензорному произведению $(\bigotimes_{i=1}^{p} U_i) \otimes (\bigotimes_{j=1}^{q} U_j')$, то $V_i \subset U_i$ и $V_j' \subset U_j'$, каковы бы ни были i и j. [См. § 1, упражнение 6.]

2) Пусть $\widetilde{u}$ для каждого эндоморфизма u A-модуля E с конечным базисом означает соответствующий u смешанный тензор (принадлежащий $E^* \otimes E$).

а) Показать, что, каков бы ни был вектор $x \in E$, вектор $u(x)$ получается путем свертывания первого контравариантного индекса тензора $x\widetilde{u}$ с ковариантным индексом.

б) Показать, что если $w = u \circ v$ — композиция эндоморфизмов v и u, то тензор $\widetilde{w}$ получается путем свертывания второго контравариантного индекса тензора $\widetilde{u}\widetilde{v}$ с первым ковариантным индексом.

в) Пусть φ — произвольный автоморфизм модуля E; показать, что произведение $\varphi \cdot \widetilde{u}$ (относительно структуры тензорного пространства в $E^* \otimes E$) есть тензор, соответствующий эндоморфизму $\varphi u \varphi^{-1}$.

3) Пусть E — A-модуль с конечным базисом (a_i). Каждому билинейному отображению u произведения $E \times E$ в E соответствует (n° 4) дважды ковариантный и один раз контравариантный тензор

$$\widetilde{u} = \sum_{i,j} a^i a^j u(a_i, a_j),$$

принадлежащий модулю $E^* \otimes E^* \otimes E$. Для того чтобы u определяло *ассоциативный* закон композиции на E, необходимо и достаточно, чтобы тензоры $c_3^1(\widetilde{u} \cdot \widetilde{u})$ (полученный путем свертывания третьего ковариантного индекса произведения $\widetilde{u} \cdot \widetilde{u}$ с первым контравариантным

индексом) и $c_3^2(\widetilde{u\cdot u})$ (полученный путем свертывания второго ковариантного индекса того же произведения со вторым контравариантным индексом) соответствовали друг другу при каноническом изоморфизме $E^*\otimes E^*\otimes E^*\otimes E$ на $E^*\otimes E\otimes E^*\otimes E^*$.

4) Если A и B квадратные матрицы над коммутативным кольцом A, то $\mathrm{Tr}(A\otimes B)=\mathrm{Tr}(A)\,\mathrm{Tr}(B)$.

5) Пусть A *некоммутативное* кольцо с единицей; предположим, что в A не существует элемента $\varrho\neq 0$, для которого бы $(\xi\eta-\eta\xi)\varrho=0$ при всякой паре элементов $(\xi,\ \eta)$ из A. Показать, что если f – линейная форма на левом A-модуле $\mathbf{M}_n(A)$ матриц порядка $n>1$ над A такая, что $f(XY)=f(YX)$ для любой пары квадратных матриц X, Y n-го порядка над A, то $f=0$. Вывести отсюда, что если A — *некоммутативное тело*, то при $n>1$ матрицы $XY-YX$, где X и Y пробегают левое векторное пространство $\mathbf{M}_n(A)$, порождают всё $\mathbf{M}_n(A)$.

*6) Пусть E - векторное пространство над полем K и $T(E)$ — тензорная алгебра этого пространства.

а) Показать, что $T(E)$ — некоммутативное кольцо, если размерность E больше 1, и есть кольцо без делителей нуля. Единственными обратимыми элементами в $T(E)$ являются ненулевые скаляры.

б) Пусть x и y — тензоры, принадлежащие $T(E)$. Показать, что если в $T(E)$ существуют элементы a, b такие, что $xa=yb$, то один из тензоров x, y является правым кратным другого.

в) Показать, что единственными элементами в $T(E)$, перестановочными с тензором x порядка >0, являются линейные комбинации степеней x. [Использовать б).] Вывести отсюда, что если E — размерности >1, то центр $T(E)$ совпадает с K.

г) Показать (используя (б)), что если $\dim E>1$, то кольцо $T(E)$ не допускает тела левых отношений (гл. I, § 9, упражнение 8).

7) Пусть $L(I)$ — *свободный моноид* (гл. I, § 1, n° 3), порожденный произвольным множеством I. Показать, что моноидная алгебра этого моноида $L(I)$ относительно коммутативного кольца A с единицей изоморфна *тензорной алгебре* $T(A^{(I)})$ модуля $A^{(I)}$.

8) Пусть A — коммутативное кольцо с единицей, E — алгебра над A, обладающая единичным элементом (обозначаемым ε), $(x_\iota)_{\iota\in I}$ — произвольное семейство элементов из E и T — тензорная алгебра A-модуля $A^{(I)}$. Если каждому элементу $z=\lambda_0+\sum_{(\iota_k)}\lambda_{\iota_1\dots\iota_n}e_{\iota_1}\dots e_{\iota_n}\in T$, отнесенному к базису алгебры T, соответствующему каноническому базису (e_ι) модуля $A^{(I)}$, поставить в соответствие элемент

$$z((x_\iota))=\lambda_0\varepsilon+\sum_{(\iota_k)}\lambda_{\iota_1\dots\iota_n}x_{\iota_1}\dots x_{\iota_n}$$

алгебры E, то этим определится представление алгебры T в алгебру E, и образом T при этом представлении будет подалгебра в E, порожденная единичным элементом и элементами x_ι.

§ 5. Внешняя алгебра

1. Операторы симметрии

Пусть I и E — произвольные множества. В соответствии с общими определениями (гл. I, § 7, n° 3), каждой *подстановке* σ множества I и каждому его отображению f в E соответствует отображение I в E, обозначаемое σf и определяемое формулой

$$\sigma f(x) = f(\sigma^{-1}x) \tag{1}$$

для всех $x \in I$. $f \longrightarrow \sigma f$ есть *подстановка* множества E^I всех отображений I в E, называемая *распространением* σ на это множество; E^I *наделено группой операторов* $\mathfrak{S}_I$ (гл. I, § 7, n° 2) внешнего закона $(\sigma, f) \longrightarrow \sigma f$; отображение $\sigma \longrightarrow \varphi_\sigma$, где φ_σ означает подстановку $f \longrightarrow \sigma f$, есть представление группы $\mathfrak{S}_I$ в группу подстановок множества E^I, являющееся, если E содержит более одного элемента, изоморфизмом.

В случае, когда I есть интервал $[1, p] \subset \mathbf{N}$, множество E^I есть не что иное, как произведение E^p; тем самым для каждой подстановки σ из симметрической группы $\mathfrak{S}_p$ и каждого элемента $x = (x_i)_{1 \leqslant i \leqslant p}$ из E^p имеем $\sigma x = (y_i)$, где $y_i = x_{\sigma^{-1}(i)}$ $(1 \leqslant i \leqslant p)$.

Каждая подстановка $x \longrightarrow \sigma x$ произведения E^p определяет теперь таким же образом подстановку $f \longrightarrow \sigma f$ множества G всевозможных отображений произведения E^p в множество F; согласно (1), для каждого $\sigma \in E^p$ имеем $\sigma f(x) = f(\sigma^{-1}x)$, т. е.

$$\sigma f(x_1, \ldots, x_p) = f(x_{\sigma(1)}, \ldots, x_{\sigma(p)}). \tag{2}$$

В этом параграфе мы ограничимся тем случаем, когда E и F являются *унитарными модулями* над коммутативным кольцом A с единицей. Из (2) следует тогда, что если f — *полилинейное* отображение E^p в F, то то же верно для σf, какова бы ни была подстановка $\sigma \in \mathfrak{S}_p$. Иначе говоря, отображение $f \longrightarrow \sigma f$ есть *автоморфизм* модуля $\mathscr{L}_p(E; F)$, оказывающегося тем самым наделенным группой операторов $\mathfrak{S}_p$.

Как мы знаем (§ 1, n°n° 2 и 7), имеется каноническое взаимно однозначное соответствие между *полилинейными* отображениями

E^p в F и *линейными* отображениями $\bigotimes^p E$ в F. Если g — линейное отображение $\bigotimes^p E$ в F, соответствующее полилинейному отображению f, то через σg для каждой подстановки $\sigma \in \mathfrak{S}_p$ будет обозначаться линейное отображение $\bigotimes^p E$ в F, соответствующее σf; таким образом, это отображение определяется условием

$$\sigma g(x_1 \otimes x_2 \dots \otimes x_p) = g(x_{\sigma(1)} \otimes x_{\sigma(2)} \otimes \dots \otimes x_{\sigma(p)}). \quad (3)$$

σg можно определить также, отправляясь от подстановки p-й тензорной степени $\bigotimes^p E$, с помощью способа распространения, который мы напомнили в начале этого n°. Действительно, так как отображение $(x_1, x_2, \dots, x_p) \to x_{\sigma^{-1}(1)} \otimes x_{\sigma^{-1}(2)} \otimes \dots \otimes x_{\sigma^{-1}(p)}$ E^p в $\bigotimes^p E$ полилинейно, то существует линейное отображение $\bigotimes^p E$ в себя, которое мы обозначим $z \to \sigma z$, такое, что

$$\sigma(x_1 \otimes x_2 \otimes \dots \otimes x_p) = x_{\sigma^{-1}(1)} \otimes x_{\sigma^{-1}(2)} \otimes \dots \otimes x_{\sigma^{-1}(p)}$$

(§ 1, n°n° 2 и 7). Без труда проверяется, что определенный так на $\bigotimes^p E$ внешний закон $(\sigma, z) \to \sigma z$ наделяет $\bigotimes^p E$ группой операторов $\mathfrak{S}_p$ (гл. I, § 7, n° 2) и, в частности, что $z \to \sigma z$ есть *автоморфизм* структуры A-модуля в $\bigotimes^p E$ (равно как и структуры *тензорного пространства* в $\bigotimes^p E$; см. § 4, n° 2). Из этого определения и формулы (3) вытекает теперь, что для всякого тензора $z \in \bigotimes^p E$ выполняется равенство

$$\sigma g(z) = g(\sigma^{-1} z), \quad (4)$$

в полном согласии с формулой (1).

Определение 1. *Унитарный модуль M над коммутативным кольцом A называется связанным с симметрической группой $\mathfrak{S}_p$, если M наделен группой операторов $\mathfrak{S}_p$* (гл. I, § 7, n° 2) *относительно внешнего закона $(\sigma, z) \to \sigma z$ такого, что каждое из отображений $z \to \sigma z$ модуля M в себя линейно* (и, значит (гл. I, § 7, предложение 1), является *автоморфизмом* структуры A-модуля в M).

Таким образом, модули $\mathscr{L}_p(E; F)$, $\mathscr{L}(\bigotimes^p E, F)$ и $\bigotimes^p E$ связаны с группой $\mathfrak{S}_p$ относительно определенных нами внешних законов.

В случае, когда M — A-модуль, связанный с группой $\mathfrak{S}_p$, в нем можно определить структуру *унитарного левого модуля* относительно *групповой алгебры* B *группы* $\mathfrak{S}_p$ (гл. II, § 7, n° 9) над кольцом A; достаточно для каждого элемента $t = \sum_\sigma \lambda_\sigma \sigma$ этой алгебры ($\lambda_\sigma \in A$) и каждого элемента $z \in M$ положить $t \cdot z = \sum_\sigma \lambda_\sigma \sigma z$; выполнение аксиом модуля без труда проверяется (на основании линейности каждого отображения $z \to \sigma z$).

Тогда операторы $t \in B$ называются *операторами симметрии* на M; среди этих операторов, разумеется, фигурируют подстановки $\sigma \in \mathfrak{S}_p$, линейными комбинациями которых с коэффициентами из A являются все операторы симметрии. Отметим, что структура A-модуля в M получается путем *сужения* кольца операторов структуры B-модуля в M до A.

Обратно, если M — унитарный B-модуль, то A-модуль, получающийся путем сужения его кольца операторов до A, связан с группой $\mathfrak{S}_p$ относительно внешнего закона $(\sigma, z) \to \sigma z$, получающегося путем сужения кольца операторов модуля M до $\mathfrak{S}_p$. Поэтому нет оснований различать понятия унитарного B-модуля и A-модуля, связанного с группой $\mathfrak{S}_p$.

Определение 2. *Пусть M — A-модуль, связанный с симметрической группой $\mathfrak{S}_p$. Элемент $z \in M$ называется симметрическим, если $\sigma z = z$ для всех $\sigma \in \mathfrak{S}_p$, и антисимметрическим* *), *если для каждого $\sigma \in \mathfrak{S}_p$ имеем $\sigma z = \varepsilon_\sigma z$, где ε_σ — сигнатура подстановки σ* (гл. I, § 7, n° 1).

Множество всех антисимметрических (соответственно симметрических) элементов из M является *подмодулем* в M относительно его структуры B-модуля; действительно, если $\sigma z = \varepsilon_\sigma z$ (соответственно $\sigma z = z$) для каждого $\sigma \in \mathfrak{S}_p$, то для всех $\tau \in \mathfrak{S}_p$ имеем $\sigma(\tau z) = \sigma(\varepsilon_\tau z) = \varepsilon_\tau \sigma z = \varepsilon_\tau \varepsilon_\sigma z = \varepsilon_\sigma(\tau z)$ (соответственно $\sigma(\tau z) = \sigma(z) =$

*) В русской математической литературе вместо «антисимметрический» более принято говорить *кососимметрический*.—*Перев.*

$= z = \tau z$). Если $M = \bigotimes^{p} E$, то эти подмодули совпадают с *тензорными подпространствами* (§ 4, n° 2) тензорного пространства $\bigotimes^{p} E$.

Предложение 1. *Для того чтобы элемент z был симметрическим* (соответственно *антисимметрическим*), *необходимо и достаточно, чтобы* $\tau z = z$ (соответственно $\tau z = -z$) *для каждой транспозиции* (гл. I, § 7, n° 1) $\tau \in \mathfrak{S}_p$.

Необходимость условия очевидна. Его достаточность следует из того, что каждая подстановка $\sigma \in \mathfrak{S}_p$ является *произведением транспозиций* (гл. I, § 7, n° 1), а $\sigma \longrightarrow \varepsilon_\sigma$ есть представление группы $\mathfrak{S}_p$ на мультипликативную группу $\{-1, +1\}$.

Определение 3. *Пусть M — A-модуль, связанный с группой $\mathfrak{S}_p$. Элемент* $\boldsymbol{a} = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon_\sigma \sigma$ *групповой алгебры B группы $\mathfrak{S}_p$ относительно A называется оператором антисимметрирования* *), *а* $\boldsymbol{a}z = \sum_{\sigma} \varepsilon_\sigma \sigma z$, *где $z \in M$, — результатом антисимметрирования элемента z.*

$z \longrightarrow \boldsymbol{a}z$ есть линейное отображение модуля M на его подмодуль (при $M = \bigotimes^{p} E$ являющийся *тензорным подпространством*).

Предложение 2. *Антисимметрирование любого элемента $z \in M$ приводит к антисимметрическому элементу* (чем и оправдывается термин «антисимметрирование»).

Действительно, для каждой подстановки $\varrho \in \mathfrak{S}_p$ имеем

$$\varrho(\boldsymbol{a}z) = \sum_{\sigma} \varepsilon_\sigma \varrho \sigma z = \varepsilon_\varrho \sum_{\sigma} \varepsilon_{\varrho\sigma} \varrho\sigma z = \varepsilon_\varrho (\boldsymbol{a}z),$$

поскольку $\sigma \longrightarrow \varrho z$ взаимно однозначное отображение $\mathfrak{S}_p$ на себя.

Следствие. *Если z — антисимметрический элемент из M, то* $\boldsymbol{a}z = p!z$.

Действительно, для каждого $\sigma \in \mathfrak{S}_p$ имеем тогда $\varepsilon_\sigma \sigma z = z$.

Замечания. 1) Как видно из доказательства предложения 2, подмодуль в M, образованный результатами антисимметрирования всевозможных элементов из M, *инвариантен* относительно каждой

*) В русской математической литературе антисимметрирование называют *альтернированием*.— *Перев.*

подстановки $\sigma \in \mathfrak{S}_p$; другими словами, он является *подмодулем относительно структуры B-модуля* в M. Доказательство этого, данное при доказательстве предложения 2, показывает, что в кольце B множество всех λa ($\lambda \in A$) является *левым идеалом*. Более общим образом, если $\mathfrak{l}$ -любой левый идеал кольца B, аддитивная подгруппа в M, порожденная элементами tz, где t пробегает $\mathfrak{l}$, а z пробегает M, есть подмодуль B-модуля M, или, иначе, подмодуль A-модуля M, инвариантный относительно всех операторов симметрии. В наиболее важных случаях можно показать, что *каждый* подмодуль B-модуля M может быть получен таким способом.

2) Антисимметрический элемент модуля M *не всегда является результатом антисимметрирования какого-либо элемента из* M (см. n° 2, замечание, и n° 3, следствие предложения 5). Однако если уравнение $p!x=a$ при каждом $a \in M$ обладает в M однозначно определенным решением, то всякий антисимметрический элемент $z \in M$ получается путем антисимметрирования. Действительно, если z' — элемент из M, для которого $p!\,z'=z$, то $p!\,(az')=az=p!z$, откуда $z=az'$.

2. *Знакопеременные полилинейные функции*

Пусть E — унитарный A-модуль и f — *антисимметрическое* полилинейное отображение E^p в A-модуль F, так что для каждого $x=(x_i)_{1\leqslant i\leqslant p} \in E^p$ имеем $f(\tau x) = -f(x)$, какова бы ни была транспозиция τ. Существование транспозиции τ, для которой $\tau x = x$, равносильно существованию *двух различных индексов* i, j, для которых $x_i = x_j$; если это имеет место, то $f(x) = f(\tau x) = -f(x)$, откуда $2f(x) = 0$. Если в модуле F соотношение $2y = 0$ влечет $y = 0$ (а это как раз имеет место, если кольцом операторов A служит *поле характеристики* $\neq 2$), то тогда каждое антисимметрическое полилинейное отображение E^p в F аннулируется на всяком $x = (x_i)$, имеющем (по крайней мере) *две равные координаты*. Этим подсказывается введение следующего определения, уже без всяких предположений относительно модуля F.

Определение 4. *Полилинейное отображение f модуля E^p в F называется знакопеременным, если $f(x_1, x_2, \ldots, x_p) = 0$ для всякого $x = (x_i) \in E^p$, имеющего* (по крайней мере) *две равные координаты x_i. Линейное отображение g модуля $\bigotimes^p E$ в F называется знакопеременным, если знакопеременно соответствующее полилинейное отображение*

$$(x_1, x_2, \ldots, x_p) \longrightarrow g(x_1 \otimes x_2 \otimes \ldots \otimes x_p).$$

Таким образом, знакопеременность g означает, что g аннулируется на каждом тензоре $z = x_1 \otimes x_2 \otimes \ldots \otimes x_p$ таком, что $\tau z = z$ хотя бы для одной транспозиции τ. *Подмодуль в* $\bigotimes^p E$, *порожденный такими тензорами* $z = x_1 \otimes x_2 \otimes \ldots \otimes x_p$, *будет вплоть до конца настоящего параграфа обозначаться через* H. *Знакопеременными линейными* отображениями модуля $\bigotimes^p E$ в модуль F будут тогда те линейные отображения $\bigotimes^p E$ в F, *которые аннулируются на подмодуле* N. Допуская вольность речи, мы будем называть N *подмодулем в* $\bigotimes^p E$, *на котором аннулируются все знакопеременные линейные функции*.

Предложение 3. *Для каждого тензора* $z \in \bigotimes^p E$ *и каждой подстановки* $\sigma \in \mathfrak{S}_p$ *элемент* $z - \varepsilon_\sigma \sigma z$ *принадлежит* N.

Поскольку каждая подстановка $\sigma \in \mathfrak{S}_p$ является произведением транспозиций (гл. I, § 7, n° 1), мы докажем справедливость предложения для произведения n транспозиций индукцией по n. При $n = 1$ следует показать, что $z + \tau z \in N$ для каждого $z \in \bigotimes^p E$ и каждой транспозиции $\tau \in \mathfrak{S}_p$. Достаточно рассмотреть тот случай, когда z — элемент вида $x_1 \otimes x_2 \otimes \ldots \otimes x_p$. Предположим, что τ переставляет различные индексы i и j. Обозначим для каждого $y \in E$ через $\varphi(y)$ элемент из $\bigotimes^p E$, получающийся путем подстановки в тензорное произведение $x_1 \otimes x_2 \otimes \ldots \otimes x_p$ элемента y вместо каждого из элементов x_i и x_j. Для каждого $y \in E$, по определению, имеем $\varphi(y) \in H$. Но $z + \tau z = \varphi(x_i + x_j) - \varphi(x_i) - \varphi(x_j)$. Следовательно, $z + \tau z \in N$. Отсюда вытекает, что если $z \in N$, то для каждой транспозиции τ также $\tau z \in N$, иными словами, $\tau(N) = N$.

Предположим теперь, что предложение справедливо для подстановки ϱ, являющейся произведением n транспозиций, и покажем, что оно справедливо для подстановки $\sigma = \tau\varrho$, где τ — произвольная транспозиция. По предположению, $\varrho z \equiv \varepsilon_\varrho z \pmod N$, откуда $\sigma z = \tau\varrho z \equiv \varepsilon_\varrho \tau z \pmod N$, поскольку $\tau(N) = N$; так как $\tau z \equiv \varepsilon_\tau z \pmod N$, то заключаем, что $\sigma z \equiv \varepsilon_\varrho \varepsilon_\tau z = \varepsilon_\sigma z \pmod N$.

Из этого предложения вытекает, что N *инвариантно* относительно каждого $\sigma \in \mathfrak{S}_p$, иными словами, является *подмодулем* относительно структуры *B-модуля* в $\overset{p}{\bigotimes} E$.

Следствие. *Каждое знакопеременное полилинейное отображение антисимметрично.*

Действительно, если g — знакопеременное линейное отображение $\overset{p}{\bigotimes} E$ в F, то $g(z - \varepsilon_\sigma \sigma z) = 0$ для каждого $z \in \overset{p}{\bigotimes} E$ и каждой подстановки $\sigma \in \mathfrak{S}_p$, откуда, в силу (4), $\sigma g = \varepsilon_\sigma g$.

Замечание. Если в F соотношение $2y = 0$ не обязательно влечет $y = 0$, то антисимметрическое полилинейное отображение E^p в F не обязательно знакопеременно. Например, если K — поле характеристики 2, то на векторном пространстве E относительно K *симметрические* полилинейные формы совпадают с *антисимметрическими*, и существуют не знакопеременные симметрические полилинейные формы, например билинейная форма $(x, y) \to u(x)\, u(y)$, где u — ненулевая линейная форма на E.

3. Антисимметрированные линейные функции

Предложение 4. *Пусть g — линейное отображение $\overset{p}{\bigotimes} E$ в A-модуль F. Каков бы ни был тензор $z \in \overset{p}{\bigotimes} E$,*

$$\boldsymbol{a} g(z) = g(\boldsymbol{a} z). \tag{5}$$

Действительно, умножив обе части соотношения (4) на $\varepsilon_\sigma = \varepsilon_\sigma^{-1}$ и просуммировав по σ, получим (5).

Следствие. *Результат антисимметрирования любого линейного отображения $\overset{p}{\bigotimes} E$ в A-модуль F аннулируется на каждом тензоре z, для которого $\boldsymbol{a} z = 0$.*

Будем в дальнейшем обозначать через N_1 подмодуль в $\overset{p}{\bigotimes} E$, образованный теми тензорами z, для которых $\boldsymbol{a} z = 0$. Следствие предложения 4 показывает, что *результат антисимметрирования* каждого линейного отображения модуля $\overset{p}{\bigotimes} E$ в A-модуль F *аннулируется на подмодуле N_1*.

Следует, однако, заметить, что это условие *не характеризует* антисимметрированные линейные отображения; иными словами, может оказаться, что линейное отображение $\bigotimes^p E$ в F аннулируется на N_1 и тем не менее не является результатом антисимметрирования какого-нибудь линейного отображения (см. упражнение 5 и теорему 1).

Предложение 5. *Для каждого тензора z, принадлежащего подмодулю N, на котором аннулируются все знакопеременные линейные функции, имеет место равенство $az = 0$* (иными словами, $N \subset N_1$).

Действительно, N порождается тензорами z такими, что $\tau z = z$ для некоторой транспозиции τ. Покажем, более общим образом, что в модуле M, связанном с группой $\mathfrak{S}_p$, каждый элемент z такой, что $\tau z = z$ для некоторой транспозиции τ, удовлетворяет условию $az = 0$. Для этого рассмотрим в $\mathfrak{S}_p$ подгруппу Γ второго порядка, образованную транспозицией τ и тождественной подстановкой. Возьмем в каждом из $\frac{p!}{2}$ левых классов по Γ четную подстановку σ_k. Согласно определению 3, для каждого $z \in M$ можно написать $az = \sum_k \sigma_k (z - \tau z)$, где сумма распространяется на все четные подстановки, а отсюда непосредственно следует наше утверждение.

Можно привести примеры модулей E, для которых $N \neq N_1$ (см. упражнение 6).

Следствие. *Результат антисимметрирования всякого полилинейного отображения знакопеременен.*

Действительно (следствие предложения 4), всякое антисимметрированное линейное отображение модуля $\bigotimes^p E$ в A-модуль F аннулируется на N_1 и тем более на N.

4. *Знакопеременные полилинейные функции на свободном модуле*

Пусть E — свободный A-модуль и $(e_\lambda)_{\lambda \in L}$ — его *базис*. Отнесем каждой последовательности $s = (\lambda_i)_{1 \leqslant i \leqslant p}$, образованной p элементами множества L (различными или нет), элемент $e_{\lambda_1} \otimes \ldots \otimes e_{\lambda_p}$; будем в этом п° обозначать его e_s. Множество этих элементов e_s (где s пробегает множество L^p всех последовательностей по p

элементов из L) образует *базис* модуля $\bigotimes^p E$ (§ 1, следствие 2 предложения 7). Имеются два сорта последовательностей s: 1° такие, что $\tau s = s$ хотя бы для одной транспозиции $\tau \in \mathfrak{S}_p$ (иными словами, последовательности s, имеющие два равных члена); множество всех таких последовательностей обозначим $\mathscr{A}$; 2° последовательности $s = (\lambda_i)$, образованные попарно различными элементами; для такой последовательности s имеем $\sigma s \neq s$, какова бы ни была нетождественная подстановка $\sigma \in \mathfrak{S}_p$, и, следовательно, $\sigma e_s = e_{\sigma s} \neq e_s$. Рассмотрим в множестве последовательностей этой второй категории отношение эквивалентности «s_1 и s_2 отличаются лишь расположением членов», которое может быть также выражено в форме «существует $\sigma \in \mathfrak{S}_p$ такое, что $\sigma s_1 = s_2$». Выберем в каждом классе эквивалентности по этому отношению какую-нибудь (безразлично какую) последовательность, и пусть $\mathscr{B}$ — множество всех выбранных последовательностей. Мы получим базис модуля $\bigotimes^p E$, взяв:

1° элементы e_s, соответствующие последовательностям $s \in \mathscr{B}$;

2° элементы $e_{\sigma s}$, соответствующие последовательностям $s \in \mathscr{B}$ и всевозможным нетождественным подстановкам $\sigma \in \mathfrak{S}_p$;

3° элементы e_s, соответствующие последовательностям $s \in \mathscr{A}$.

Мы получим также базис модуля $\bigotimes^p E$, взяв:

α) элементы e_s, соответствующие последовательностям $s \in \mathscr{B}$;

β) элементы $\varepsilon_\sigma e_{\sigma s} - e_s$, соответствующие последовательностям $s \in \mathscr{B}$ и всевозможным нетождественным подстановкам $\sigma \in \mathfrak{S}_p$;

γ) элементы e_s, соответствующие последовательностям $s \in \mathscr{A}$.

Элементы этого базиса, относящиеся к категориям γ) и β), принадлежат подмодулю N, на котором аннулируются все знакопеременные линейные функции; для γ) это вытекает из определения подмодуля N (n° 2), а для β) — из предложения 3. Покажем, что подмодуль, порожденный элементами базиса, относящимися к категориям γ) и β), есть не что иное, как подмодуль N_1 тензоров z, антисимметрирование которых дает нуль. Так как $N \subset N_1$ (предложение 5), то отсюда попутно получится, что $N_1 = N$. Достаточно показать, что для тензора $z = \sum_{s \in \mathscr{B}} \alpha_s e_s$ (линейной ком-

бинации элементов категории α)) соотношение $az = 0$ влечет $\alpha_s = 0$ для всех $s \in \mathscr{B}$. Но это соотношение записывается в виде

$$\sum_{s \in \mathscr{B},\, \sigma \in \mathfrak{S}_p} \varepsilon_\sigma a_s e_{\sigma s} = 0,$$

откуда и следует справедливость утверждения.

Пусть теперь g — линейное отображение модуля $\bigotimes^p E$ в A-модуль F. Для того чтобы g было *знакопеременным*, необходимо и достаточно, чтобы оно аннулировалось на базисе подмодуля N, образованном элементами указанных выше категорий β) и γ); а отсюда вытекает система *необходимых и достаточных условий знакопеременности отображения* g:

$g(e_s) = 0$ для каждой последовательности s, у которой (по крайней мере) два члена равны;

$g(e_{\sigma s}) = \varepsilon_\sigma g(e_s)$ для каждой последовательности s с попарно различными членами и каждой подстановки $\sigma \in \mathfrak{S}_p$.

Если линейное отображение g модуля $\bigotimes^p E$ в F удовлетворяет указанным условиям, то обозначим через h линейное отображение, определяемое условиями

$h(e_s) = g(e_s)$ для каждой последовательности $s \in \mathscr{B}$;

$h(e_s) = 0$ для каждой последовательности $s \notin \mathscr{B}$.

Очевидно, $ah = g$: каждое знакопеременное линейное отображение есть *результат антисимметрирования* некоторого линейного отображения.

В итоге (учитывая следствие предложения 5) имеем:

Теорема 1. *Пусть E — свободный A-модуль.*

а) *Подмодуль N в $\bigotimes^p E$, на котором аннулируются все знакопеременные линейные функции* (№ 2), *совпадает с подмодулем N_1 тензоров, антисимметрирование которых дает нуль.*

б) *Для того чтобы линейное отображение g модуля $\bigotimes^p E$ в A-модуль F было знакопеременным, необходимо и достаточно, чтобы оно получалось путем антисимметрирования некоторого линейного отображения $\bigotimes^p E$ в F.*

Замечание. Вторая часть теоремы 1 остается верной и без предположения, что E обладает базисом, если только уравнение $p!y=b$ для каждого $b \in F$ имеет, и притом единственное, решение в F. Действительно (замечание 2 в n° 1), тогда каждое антисимметрическое полилинейное отображение E^p в F является результатом антисимметрирования некоторого полилинейного отображения, и, в частности, это верно для каждого знакопеременного полилинейного отображения E^p в F (следствие 2 предложения 3). Таким образом, в этом случае понятия антисимметрированного, знакопеременного и антисимметрического полилинейных отображений E^p в F *совпадают* (что, например, имеет место для каждого целого p, когда E и F — *векторные пространства* над *полем характеристики* 0).

5. *Внешние степени модуля*

Пусть E — произвольный унитарный A-модуль. Так как каждое знакопеременное линейное отображение g модуля $\bigotimes^p E$ в A-модуль F аннулируется на подмодуле N модуля $\bigotimes^p E$, то оно может быть записано в виде $h \circ \psi$, где ψ — каноническое отображение модуля $\bigotimes^p E$ в фактормодуль $(\bigotimes^p E)/N$, а h — однозначно определенное линейное отображение этого фактормодуля в F (гл. II, § 2, предложение 1). Поэтому каждое *знакопеременное полилинейное* отображение E^p в F может быть однозначно представлено в виде

$$(x_1, \ldots, x_p) \to h(\psi(x_1 \otimes \ldots \otimes x_p)).$$

Всюду в дальнейшем через $x_1 \wedge x_2 \wedge \ldots \wedge x_p$ для каждого элемента $(x_i) \in E^p$ будет обозначаться образ $x_1 \otimes x_2 \otimes \ldots \otimes x_p$ при каноническом отображении ψ модуля $\bigotimes^p E$ на его фактормодуль $(\bigotimes^p E)/N$.

Определение 5. *Пусть E — унитарный A-модуль. Фактормодуль модуля $\bigotimes^p E$ по его подмодулю N (порожденному разложимыми тензорами $x_1 \otimes x_2 \otimes \ldots \otimes x_p$, в которых по крайней мере два элемента x_i, x_j равны) называется p-й внешней степенью модуля E*

и обозначается $\bigwedge^p E$. *Элементы из* $\bigwedge^p E$ *называются* p*-векторами над* E; *каждый* p*-вектор вида* $x_1 \wedge x_2 \wedge \ldots \wedge x_p$ (где все $x_i \in E$) *называется разложимым.*

Приведенное определение имеет смысл лишь при $p \geqslant 2$; в дополнение к нему будем, по условию, понимать под $\bigwedge^1 E$ сам модуль E, а под $\bigwedge^0 E$ — кольцо операторов A; таким образом, 1-вектор — это элемент из E, а 0-вектор — скаляр.

Поскольку каждый тензор есть сумма разложимых тензоров, каждый p-вектор над E есть сумма разложимых p-векторов.

Так как $(x_1, x_2, \ldots, x_p) \longrightarrow x_1 \wedge x_2 \wedge \ldots \wedge x_p$ есть знакопеременное отображение, то каждый разложимый p-вектор, в котором по крайней мере два элемента x_i, x_j *равны*, есть *нуль*, и для каждой подстановки $\sigma \in \mathfrak{S}_p$ (согласно следствию предложения 3) имеем

$$x_{\sigma(1)} \wedge x_{\sigma(2)} \wedge \ldots \wedge x_{\sigma(p)} = \varepsilon_\sigma \cdot x_1 \wedge x_2 \wedge \ldots \wedge x_p. \qquad (6)$$

Из схолии, приведенной в n° 2 § 1, и введенного выше определения 5 непосредственно вытекает следующая аналогичная

Схолия. *Линейные отображения* $\bigwedge^p E$ *в* F *связаны со знакопеременными полилинейными отображениями* E^p *в* F *следующим взаимно однозначным соответствием: линейное отображение* f *модуля* $\bigwedge^p E$ *в* F *определено, если известно его значение* $f(x_1 \wedge \ldots \wedge x_p)$ *для каждой последовательности* $(x_i)_{1 \leqslant i \leqslant p}$ *из* p *элементов модуля* E *и* $(x_1, \ldots, x_p) \longrightarrow f(x_1 \wedge \ldots \wedge x_p)$ *есть знакопеременное полилинейное отображение. Обратно, для определения линейного отображения* $\bigwedge^p E$ *в* E *достаточно задать отображение* $(x_1, \ldots, x_p) \longrightarrow g(x_1, \ldots, x_p)$ *модуля* E^p *в* F, *проверив его полилинейность и знакопеременность; тогда существует, и притом единственное, линейное отображение* f *модуля* $\bigwedge^p E$ *в* F *такое, что* $f(x_1 \wedge \ldots \wedge x_p) = g(x_1, \ldots, x_n)$ *для всех* $(x_i) \in E^p$.

В частности, *незачем* проверять, что соотношение $x_1 \wedge \ldots \wedge x_p = y_1 \wedge \ldots \wedge y_p$ влечет $g(x_1, \ldots, x_p) = g(y_1, \ldots, y_p)$.

Далее, для определения *билинейного* отображения произведения $G \times H$ внешних степеней $G = \bigwedge^p E$ и $H = \bigwedge^q F$ в модуль N достаточно задать отображение g произведения $E^p \times F^q$ в N, для которого бы каждое частичное отображение

$$(x_1, \ldots, x_p) \longrightarrow g(x_1, \ldots, x_p, y_1, \ldots, y_q),$$
$$(y_1, \ldots, y_q) \longrightarrow g(x_1, \ldots, x_p, y_1, \ldots, y_q)$$

было знакопеременным полилинейным отображением; тогда существует, и притом единственное, билинейное отображение f произведения $G \times H$ в N такое, что тождественно

$$f(x_1 \wedge \ldots \wedge x_p, y_1 \wedge \ldots \wedge y_q) = g(x_1, \ldots, x_p, y_1, \ldots, y_q)$$

(см. § 1, n° 2).

Замечание. Если E обладает конечной системой образующих, число которых равно n, то $\bigwedge^p E$ при $p > n$ сводится к 0.

6. *Внешние степени свободного модуля*

Предложение 5 показывает, что линейное отображение $z \longrightarrow az$ модуля $\bigotimes^p E$ в себя *знакопеременно* и потому может быть записано в виде $\theta \circ \psi$, где ψ — каноническое отображение $\bigotimes^p E$ на $\bigwedge^p E = (\bigotimes^p E)/N$, а θ — однозначно определенное линейное отображение $\bigwedge^p E$ *на* подмодуль U в $\bigotimes^p E$, образованный *антисимметрическими тензорами p-го порядка*; мы будем называть θ *каноническим отображением* $\bigwedge^p E$ на U. Таким образом,

$$\theta(x_1 \wedge \ldots \wedge x_p) = a(x_1 \otimes \ldots \otimes x_p)$$

для каждой последовательности $(x_i)_{1 \leqslant i \leqslant p}$ из p элементов модуля F.

Отношение $\theta(u) = 0$ для элемента $u \in \bigwedge^p E$ равносильно отношению $u \in N_1/N$; в случае, когда E — *свободный* модуль, имеем $N_1 = N$ (теорема 1, а)), и значит, θ — *изоморфизм*. Иными словами:

Предложение 6. *Если A-модуль E обладает базисом, то взаимно однозначное отображение, ассоциированное* (гл. I, § 6, n° 4)

с эндоморфизмом $z \to az$ *модуля* $\overset{p}{\bigotimes} E$, *есть изоморфизм* $\overset{p}{\bigwedge} E$ *на подмодуль антисимметрических тензоров* p*-го порядка.*

p-вектор часто отождествляют тогда посредством изоморфизма 0 (обратный к которому также именуется *каноническим*) с соответствующим антисимметрированным тензором.

В обозначениях n° 4, каноническое отображение модуля $\overset{p}{\bigotimes} E$ на фактормодуль $(\overset{p}{\bigotimes} E)/N$ преобразует семейство $(e_s)_{s \in \mathscr{B}}$, являющееся базисом дополнения к N, в *базис модуля* $\overset{p}{\bigwedge} E$.

Рассмотрим, в частности, тот случай, когда модуль E имеет *конечный* базис $(e_i)_{1 \leqslant i \leqslant n}$. Примем во всей остающейся части этой главы следующее соглашение: если $(x_i)_{1 \leqslant i \leqslant n}$ — заданная *серия* (гл. I, § 1, n° 2) элементов унитарного A-модуля E, то для каждого множества H, состоящего из p целых чисел интервала $[1, n] \subset \mathbf{N}$, через x_H будет обозначаться p*-вектор* $x_{i_1} \wedge \ldots \wedge x_{i_p}$, где $(i_k)_{1 \leqslant k \leqslant p}$ — *строго возрастающая* последовательность, образованная p элементами множества H.

Это определение имеет смысл лишь при $p \geqslant 2$; условимся для множества $H = \{i\}$, сводящегося к одному элементу, полагать $x_H = x_i$, а для пустого подмножества $\varnothing$ интервала $[1, n]$ считать $x_\varnothing = 1$ (единичному элементу кольца A).

При этих соглашениях, предшествующее замечание показывает, что справедлива

Теорема 2. *Пусть* E — *модуль, обладающий конечным базисом* $(e_i)_{1 \leqslant i \leqslant n}$. *Если* $p \leqslant n$, *то модуль* $\overset{p}{\bigwedge} E$ *имеет своим базисом семейство* (e_H), *где* H *пробегает множество* $\binom{n}{p}$ *подмножеств интервала* $[1, n]$, *состоящих из* p *элементов. Если* $p > n$, *то модуль* $\overset{p}{\bigwedge} E$ *сводится к* 0.

Заметим, что, напротив, если E обладает *бесконечным* базисом, то ни один из модулей $\overset{p}{\bigwedge} E$ не сводится к 0.

Следствие 1. *Если E обладает базисом, состоящим из n элементов, то модули $\bigwedge^p E$ и $\bigwedge^{n-p} E$, где $0 \leqslant p \leqslant n$, изоморфны.*

В частности, $\bigwedge^n E$ обладает базисом, образованным единственным элементом $e_1 \wedge e_2 \wedge \ldots \wedge e_n$.

Можно показать, что при $p \neq n - p$ не существует *канонического изоморфизма* $\bigwedge^p E$ на $\bigwedge^{n-p} E$, понимая под этим изоморфизм, зависящий лишь от структур внешней степени в $\bigwedge^p E$ и $\bigwedge^{n-p} E$ (упражнение 12). В гл. VIII будут изучены некоторые изоморфизмы $\bigwedge^p E$ на $\bigwedge^{n-p} E$, связанные с теорией билинейных форм.

Следствие 2. *Если унитарный модуль E над коммутативным кольцом A обладает базисом, состоящим из n элементов, то и каждый другой базис этого модуля конечен и содержит n элементов.*

Действительно, n есть наибольшее из целых p, для которых $\bigwedge^p E$ не сводится к 0, так что E не может обладать конечным базисом с числом элементов $\neq n$; с другой стороны, если бы E обладало бесконечным базисом, то ни одна из его внешних степеней $\bigwedge^p E$ не сводилась бы к 0.

7. *Внешние степени линейного отображения*

Пусть u — линейное отображение A-модуля E в A-модуль F; очевидно,

$$(x_1, \ldots, x_p) \longrightarrow u(x_1) \wedge \ldots \wedge u(x_p)$$

есть знакопеременное полилинейное отображение E^p в $\bigwedge^p F$; поэтому (схолия из n° 5) существует однозначно определенное линейное отображение $\bigwedge^p E$ в $\bigwedge^p F$, которое мы будем обозначать $\bigwedge^p u$ (или u_p, если это не сможет повлечь путаницу) и называть *p-й внешней степенью u*, такое, что тождественно

$$\bigwedge^p u\,(x_1 \wedge \ldots \wedge x_p) = u(x_1) \wedge \ldots \wedge u(x_p). \tag{7}$$

Замечания. 1) Пусть u^p — линейное отображение $\bigotimes^p E$ в $\bigotimes^p F$, являющееся тензорным произведением p линейных отображений, совпадающих с u (§ 1, n°n° 4 и 7), и $N(E)$ (соответственно $N(F)$) — подмодуль в $\bigotimes^p E$ (соответственно в $\bigotimes^p F$), порожденный всевозможными тензорными произведениями p элементов, по крайней мере два из которых равны между собой. Ясно, что $u^p(N(E)) \subset N(F)$; отображение модуля $\bigwedge^p E = (\bigotimes^p E)/N(E)$ в $\bigwedge^p F = (\bigotimes^p F)/N(F)$, получающееся из u^p путем *факторизации*, и есть как раз $\bigwedge^p u$.

2) Если E и F — свободные модули, так что $\bigwedge^p E$ (соответственно $\bigwedge^p F$) канонически отождествимо с модулем $U(E)$ (соответственно $U(F)$) антисимметрированных тензоров p-го порядка над E (соответственно над F; см. предложение 6), то из замечания 1 следует, что $\bigwedge^p u$ отождествляется при этом с сужением u^p на подмодуль $U(E)$.

Пусть G — третий A-модуль и v — линейное отображение F в G; из (7) по линейности сразу следует, что

$$\bigwedge^p (v \circ u) = (\bigwedge^p v) \circ (\bigwedge^p u). \tag{8}$$

Если u — отображение E *на* F, то $\bigwedge^p u$ есть отображение $\bigwedge^p E$ *на* $\bigwedge^p F$; если u — *изоморфизм* E *на* F и v — обратный ему, то $\bigwedge^p u$ есть *изоморфизм* $\bigwedge^p E$ *на* $\bigwedge^p F$, а $\bigwedge^p v$ — обратный изоморфизм.

Напротив, если u — *изоморфизм* E *в* F, $\bigwedge^p u$ не обязательно является изоморфизмом $\bigwedge^p E$ в $\bigwedge^p F$ (упражнение 10). Однако справедливо следующее предложение:

Предложение 7. *Если F — подмодуль модуля E такой, что существует конечный базис $(e_i)_{1 \leqslant i \leqslant n}$ модуля E, первые m элементов которого образуют базис для F, то $\bigwedge^p \varphi$, где φ — каноническое отображение F в E, есть изоморфизм $\bigwedge^p F$ в $\bigwedge^p E$.*

Это сразу следует из способа образования базисов модулей $\bigwedge^p E$ и $\bigwedge^p F$, отправляясь от базисов $(e_i)_{1\leqslant i\leqslant n}$ и $(e_i)_{1\leqslant i\leqslant m}$ (теорема 2).

Поэтому внешняя степень $\bigwedge^p F$ *отождествима* посредством отображения $\bigwedge^p \varphi$ со своим образом при этом отображении; другими словами, для любых p элементов x_i $(1\leqslant i\leqslant p)$ из F можно отождествлять p-вектор $x_1\wedge\ldots\wedge x_p$, где x_i рассматриваются как *принадлежащие* F, с p-вектором $\varphi(x_1)\wedge\ldots\wedge\varphi(x_p)$ над E.

В частности, такое отождествление всегда возможно, когда E — конечномерное *векторное пространство*, а F — любое его векторное подпространство (гл. II, § 3, теорема 2).

8. *Внешнее произведение p-вектора и q-вектора*

Пусть E — заданный A-модуль. Рассмотрим отображение

$$(x_1, \ldots, x_p, y_1, \ldots, y_q) \longrightarrow x_1\wedge\ldots\wedge x_p\wedge y_1\wedge\ldots\wedge y_q$$

произведения $E^p\times E^q$ в $\bigwedge^{p+q} E$; каждое из частичных отображений

$$(x_1, \ldots, x_p) \longrightarrow x_1\wedge\ldots\wedge x_p\wedge y_1\wedge\ldots\wedge y_q,$$

$$(y_1, \ldots, y_q) \longrightarrow x_1\wedge\ldots\wedge x_p\wedge y_1\wedge\ldots\wedge y_q$$

полилинейно и знакопеременно; поэтому (n° 5) существует *билинейное* отображение $\left(\bigwedge^p E\right)\times\left(\bigwedge^q E\right)$ в $\bigwedge^{p+q} E$, значение которого для $u\in\bigwedge^p E$ и $v\in\bigwedge^q E$ будет обозначаться $u\wedge v$ и называться *внешним произведением* u и v, такое, что тождественно

$$(x_1\wedge\ldots\wedge x_p)\wedge(y_1\wedge\ldots\wedge y_q) = x_1\wedge\ldots\wedge x_p\wedge y_1\wedge\ldots\wedge y_q. \quad (9)$$

Это определение распространяется на случай, когда $p=0$ (соответственно $q=0$), условием, что внешнее произведение $\alpha\wedge v$ скаляра α и q-вектора v (соответственно внешнее произведение $u\wedge\alpha$ p-вектора u и скаляра α) равно αv (соответственно αu).

Замечания. 1) В случае, когда $p=q=1$, внешнее произведение векторов $x\in E$ и $y\in F$ совпадает с бивектором $x\wedge y$, чем и оправдывается общее обозначение $u\wedge v$ для внешнего произведения p-вектора и q-вектора.

2) Пусть N_p, N_q и N_{p+q} — подмодули в $\bigotimes^p E$, $\bigotimes^q E$ и $\bigotimes^{p+q} E$, на которых аннулируются все знакопеременные линейные функции. Рассмотрим отображение $(z, z') \to zz'$ произведения $(\bigotimes^p E) \times (\bigotimes^q E)$ в $\bigotimes^{p+q} E$ (§ 4, n° 3); соотношения $z_1 \equiv z_2 \pmod{N_p}$ и $z'_1 \equiv z'_2 \pmod{N_q}$ влекут $z_1 z'_1 \equiv z_2 z'_2 \pmod{N_{p+q}}$, ибо

$$z_1 z'_1 - z_2 z'_2 = z_1 (z'_1 - z'_2) + (z_1 - z_2) z'_2.$$

Поэтому отображение $(z, z') \to zz'$ порождает путем *факторизаций* относительно z и z' (Теор. мн., Рез., § 5, n° 8) билинейное отображение $(\bigwedge^p E) \times (\bigwedge^q E)$ в $\bigwedge^{p+q} E$; это и есть наше внешнее произведение.

3) Заметим, что в случае, когда E обладает базисом и p-векторы, где $0 \leqslant p \leqslant n$, канонически отождествляются (предложение 6) с антисимметрированными тензорами p-го порядка, внешнее произведение p-вектора и q-вектора отнюдь не отождествляется с произведением (в указанном в n° 3 § 4 смысле) тензоров, с которыми соответственно отождествлены эти p-вектор и q-вектор (см. упражнение 3).

Билинейность отображения $(u, v) \to u \wedge v$ находит свое выражение в формулах

$$(u_1 + u_2) \wedge (v_1 + v_2) = u_1 \wedge v_1 + u_1 \wedge v_2 + u_2 \wedge v_1 + u_2 \wedge v_2, \qquad (10)$$

$$(\alpha u) \wedge v = u \wedge (\alpha v) = \alpha (u \wedge v) \qquad (\alpha \in A). \qquad (11)$$

Кроме того, для p-вектора u и q-вектора v имеем

$$v \wedge u = (-1)^{pq} u \wedge v. \qquad (12)$$

Действительно, пусть σ — подстановка множества $[1, p+q]$ такая, что $\sigma(i) = q+i$, когда $1 \leqslant i \leqslant p$, и $\sigma(i) = i - p$, когда $p+1 \leqslant i \leqslant p+q$. Имеем $\varepsilon_\sigma = (-1)^{pq}$, ибо для пар (i, j), в которых $i < j$, разность $\sigma(j) - \sigma(i)$ может быть < 0 лишь если $1 \leqslant i \leqslant p$ и $p+1 \leqslant j \leqslant p+q$. Отсюда и из формул (6) и (9) следует формула (12), когда u и v разложимы, а соотношение (10) позволяет тогда распространить эту формулу на случай произвольных u и v.

Наконец, для любых p-вектора u, q-вектора v и r-вектора w имеем

$$(u \wedge v) \wedge w = u \wedge (v \wedge w). \qquad (13)$$

Действительно, в силу (9) эта формула очевидна, когда u, v и w разложимы, а по линейности она распространяется на общий случай. Общее значение обеих частей равенства (13) обозначается также $u \wedge v \wedge w$.

9. Внешняя алгебра

Обозначим через $\bigwedge E$, где E — заданный A-модуль, *прямую сумму* ненулевых модулей $\bigwedge^n E$ для всех $n \geqslant 0$ (гл. II, § 1, n° 7). Определение внешнего произведения позволяет ввести в $\bigwedge E$ структуру *алгебры* относительно A. В самом деле, каждый элемент $z \in \bigwedge E$ однозначно представим в виде $z = \sum_{p=0}^{\infty} z_p$, где z_p — p-вектор (равный нулю для всех кроме конечного числа индексов p). Для любых двух элементов $z = \sum_{p=0}^{\infty} z_p$ и $z' = \sum_{p=0}^{\infty} z'_p$ из $\bigwedge E$ положим $z \wedge z' = \sum_{p,q} (z_p \wedge z'_q)$. В силу (10), определенное так на $\bigwedge E$ умножение двояко дистрибутивно относительно сложения; в силу соотношения (13), распространяющегося по дистрибутивности на любые элементы из $\bigwedge E$, это умножение ассоциативно; наконец, согласно (11), имеем $\alpha(z \wedge z') = (\alpha z) \wedge z' = z \wedge (\alpha z')$ для любого скаляра α. Таким образом, $\bigwedge E$ действительно является алгеброй над A; она называется *внешней алгеброй модуля* E. Эта алгебра имеет своим единичным элементом единицу 1 кольца A и, в силу (12), вообще не коммутативна. В силу ассоциативности умножения, разложимый p-вектор $x_1 \wedge \ldots \wedge x_p$ есть не что иное, как *композиция* (относительно умножения на $\bigwedge E$) серии $(x_i)_{1 \leqslant i \leqslant p}$ элементов из E, что оправдывает одинаковость обозначений внешнего произведения и разложимого p-вектора и показывает в то же время, что множество $A \bigcup E$ является *системой образующих* алгебры $\bigwedge E$.

В случае, когда E обладает конечным базисом $(e_i)_{1 \leqslant i \leqslant n}$, $\bigwedge E$ обладает базисом, образованным 2^n элементами e_H (n° 6), где H пробегает множество всех подмножеств интервала $[1, n] \subset \mathbf{N}$. Таблица умножения этого базиса задается следующими соотношениями:

$$\left.\begin{aligned} e_H \wedge e_K &= 0 && \text{при } H \bigcap K \neq \varnothing, \\ e_H \wedge e_K &= \varrho_{H,K} e_{H \bigcup K} && \text{при } H \bigcap K = \varnothing, \end{aligned}\right\} \qquad (14)$$

где $\varrho_{H,K} = (-1)^{\nu}$, а ν — число всех пар (i, j), в которых $i \in H$, $j \in K$ и $j < i$.

Каждое *линейное отображение* u модуля E в произвольный унитарный A-модуль F однозначно продолжается до *представления* внешней алгебры $\bigwedge E$ во внешнюю алгебру $\bigwedge F$. Действительно, если $\overline{u}$ — такое продолжение, то $\overline{u}(1)=1$, откуда $\overline{u}(\alpha)=\overline{u}(\alpha\cdot 1)=\alpha\overline{u}(1)=\alpha$ для каждого скаляра α; с другой стороны, для любого разложимого p-вектора $z=x_1\wedge\ldots\wedge x_p$ мы должны иметь $\overline{u}(z)=u(x_1)\wedge\ldots\wedge u(x_p)=u_p(z)$, где u_p означает p-ю внешнюю степень u (n° 7). Наконец, для каждого элемента $z=\sum_{p=0}^{\infty} z_p$ из E, разложенного в сумму p-векторов, должно выполняться равенство $\overline{u}(z)=\sum_{p=0}^{\infty}\overline{u}(z_p)=\sum_{p=0}^{\infty}u_p(z_p)$ (где u_0 означает тождественное отображение A на себя). Обратно, непосредственная проверка показывает, что определенное так отображение $\overline{u}$ действительно является представлением $\bigwedge E$ в $\bigwedge F$; мы будем называть его *каноническим продолжением* u на $\bigwedge E$.

Если v — линейное отображение модуля F в A-модуль G и $\overline{v}$ — его продолжение до представления $\bigwedge F$ в $\bigwedge G$, то продолжение композиции $v\circ u$ до представления $\bigwedge E$ в $\bigwedge G$ совпадает с $\overline{v}\circ\overline{u}$. В частности, если u — автоморфизм модуля E, то $\overline{u}$ есть автоморфизм алгебры $\bigwedge E$.

Если E — *подмодуль* модуля F, а u — каноническое отображение E в F, то $\overline{u}$ есть представление $\bigwedge E$ в $\bigwedge F$, также называемое *каноническим*; оно не всегда взаимно однозначно (см. упражнение 9). Однако в случае, когда F — конечномерное *векторное пространство*, $\overline{u}$ есть *изоморфизм* $\bigwedge E$ в $\bigwedge F$ (предложение 7), и алгебра $\bigwedge E$ часто *отождествляется* посредством него с подалгеброй в $\bigwedge F$, являющейся ее образом при этом изоморфизме. Если такое отождествление произведено для каждого подпространства E пространства F, то для любых двух подпространств E_1, E_2 будем иметь $\bigwedge(E_1\cap E_2)=(\bigwedge E_1)\cap(\bigwedge E_2)$. В самом деле, пусть $\dim E_1=n_1$, $\dim E_2=n_2$, $\dim(E_1\cap E_2)=m$; для доказательства утверждаемого соотношения достаточно взять в F базис, первые m векторов которого образуют базис для $E_1\cap E_2$, дальнейшие n_1-m дополняют его до базиса в E_1, а следующие за ними n_2-m

векторов дополняют первые m до базиса в E_2; образование соответствующего базиса алгебры $\bigwedge F$ и дает требуемое соотношение.

Отсюда следует, что если F — канечномерное векторное пространство, то для любого элемента z алгебры $\bigwedge F$ существует *наименьшее векторное подпространство* E пространства F такое, что z принадлежит $\bigwedge E$; размерность этого подпространства E называется *рангом* элемента z алгебры $\bigwedge F$.

Упражнения. 1) Показать, что определение σz, данное в n° 1 для тензора $z \in \bigotimes^p E$ и подстановки $\sigma \in \mathfrak{S}_p$, совпадает с определением, получающимся общим методом распространения группы подстановок (гл. I, § 7, n° 3), отправляясь от определения $\bigotimes^p E$ (§ 1, n° 2) как фактормножества множества $A^{(E^p)}$, где последнее само является частью A^{E^p}.

*2) Пусть E и F — заданные аддитивные группы и n — целое $\geqslant 1$. Будем обозначать через $\mathscr{F}_n(E, F)$ аддитивную группу, образованную всеми отображениями E^n в F (т. е. группу F^{E^n}).

Для каждого $u \in \mathscr{F}_n(E, F)$ будем обозначать через ∂u отображение E^{n+1} в F, определяемое формулой

$$\partial u(x_1, \ldots, x_n, x_{n+1}) = u(x_2, \ldots, x_n, x_{n+1}) + \sum_{k=1}^{n} (-1)^k u(x_1, \ldots, x_{k-1}, x_k + x_{k+1}, x_{k+2}, \ldots, x_{n+1}) + (-1)^{n+1} u(x_1, \ldots, x_n).$$

а) Показать, что, каково бы ни было $u \in \mathscr{F}_n(E, F)$,

$$\partial(\partial u) = 0.$$

б) Для каждого $u \in \mathscr{F}_n(E, F)$ $(n \geqslant 2)$ будем обозначать через Su отображение E^{n-1} в $\mathscr{F}_1(E, F)$, относящее каждому элементу $(x_1, \ldots, x_{n-1}) \in E^{n-1}$ отображение

$$x_n \to \sum_{k=0}^{n-1} (-1)^k u(x_1, \ldots, x_{n-k-1}, x_n, x_{n-k}, \ldots, x_{n-1})$$

E в F. Доказать, что

$$S(\partial u) = \partial(Su).$$

в) Вывести из б), что если $u \in \mathscr{F}_n(E, F)$ удовлетворяет условию $\partial u = 0$, то результат его антисимметрирования au является *полилинейным* отображением E^n в F; если $v \in \mathscr{F}_n(E, F)$ таково, что $v = \partial u$ для некоторого $u \in \mathscr{F}_{n-1}(E, F)$, то антисимметрирование v дает 0.

3) Пусть M — A-модуль, связанный с симметрической группой $\mathfrak{S}_p$, и H — произвольное подмножество интервала $[1, p]$. *Результатом антисимметрирования элемента* $z \in M$ *по индексам* $i \in H$ называется элемент

$$a_H z = \sum_{\sigma} \varepsilon_\sigma \sigma z,$$

где σ пробегает подгруппу в $\mathfrak{S}_p$ (изоморфную $\mathfrak{S}_H$), образованную теми подстановками, которые оставляют инвариантным каждый индекс, не принадлежащий H.

а) $a(a_H z) = r! a z$, где r — число элементов множества H.

б) Пусть E — унитарный A-модуль, z — контравариантный тензор p-го порядка над E и z' — контравариантный тензор q-го порядка. Показать, что если $az' = 0$ в $\overset{q}{\bigotimes} E$ (соответственно $az = 0$ в $\overset{p}{\bigotimes} E$), то $a(zz') = 0$ в $\overset{p+q}{\bigotimes} E$. [Заметить, что если $H = [p+1, p+q]$, то $a_H(zz') = z \cdot az'$.] Вывести отсюда, что если $z = az_1$ и $z' = az_1'$ — тензоры, получающиеся в результате антисимметрирования тензоров z_1 и z_1' порядков p и q, то тензор $a(z_1 z_1')$ порядка $p+q$ зависит лишь от z и z', но не от тензоров z_1 и z_1', антисимметрированием которых z и z' получены. Если z (соответственно z') — канонический образ (n° 6) p-вектора u (соответственно q-вектора u'), то $a(z_1 z_1')$ есть канонический образ $(p+q)$-вектора $u \wedge u'$.

4) Пусть E — унитарный A-модуль, обладающий системой n образующих. Показать, что каждое знакопеременное полилинейное отображение модуля E^n в произвольный A-модуль F есть результат антисимметрирования некоторого полилинейного отображения.

*°5) Пусть K — поле характеристики 2 и A — кольцо $K[X, Y, Z]$ полиномов от трех неизвестных X, Y, Z над K; пусть, далее, E — фактормодуль A^3/M модуля A^3 по его подмодулю M, порожденному элементом (X, Y, Z); пусть, наконец, F — фактормодуль модуля A по идеалу $(X^2)+(Y^2)+(Z^2)$. Показать, что существует знакопеременное билинейное отображение E^2 в F, не получающееся путем антисимметрирования никакого билинейного отображения E^2 в F.

Показать также, что в $E \otimes F$ подмодуль N_1 тензоров, антисимметрирование которых дает 0, совпадает с подмодулем N, на котором аннулируются все знакопеременные линейные функции. [Рассматривая $E \otimes E$ как фактормодуль модуля $A^3 \otimes A^3$ (§ 1, n° 3, предложение 6), показать, что тензоры, дающие при антисимметрировании 0, являются каноническими образами симметрических тензоров из $A^3 \otimes A^3$.]

*°6) В обозначениях упражнения 5, пусть B — факторкольцо кольца A по идеалу $\mathfrak{a} = (X^2)+(Y^2)+(Z^2)$ и G — фактормодуль B^2/P модуля B^2 по его подмодулю P, порожденному элементом, имеющим своими координатами соответственно классы X, Y, Z (mod $\mathfrak{a}$). Показать, что в $G \otimes G$ подмодуль N_1' тензоров, дающих при антисимметри-

ровании 0, отличен от подмодуля N', на котором аннулируются все знакопеременные линейные функции. [Тем же методом, что и в упражнении 5.]$_0$

7) Пусть A-модуль E есть прямая сумма своих подмодулей E_1, E_2. Показать, что модуль $\bigwedge^p E$ изоморфен прямой сумме G модулей $(\bigwedge^q E_1) \otimes (\bigwedge^{p-q} E_2)$, где q пробегает все целые значения от 0 до p. [Опираясь на схолию из n° 5, определить линейные отображения $\bigwedge^p E$ в G и G в $\bigwedge^p E$, которые были бы взаимно обратны.]

Обобщить на случай модуля E, заданного в виде прямой суммы произвольного конечного числа его подмодулей.

8) Пусть E — A-модуль и M — его подмодуль. Показать, что модуль $\bigwedge^p (E/M)$ изоморфен фактормодулю $(\bigwedge^p E)/\Gamma(M)$ модуля $\bigwedge^p E$ по его подмодулю $\Gamma(M)$, порожденному p-векторами $x_1 \wedge \cdots \wedge x_p$, в которых по крайней мере одно x_i принадлежит M. [Метод упражнения 7.]

9) Пусть A — кольцо целостности с единицей и K — его поле отношений (гл. I, § 9, n° 4).

а) Внешняя степень $\bigwedge^2 K$, где K рассматривается как A-модуль, сводится к 0.

б) Показать, что если E — A-модуль, содержащийся в K, то никакая его внешняя степень $\bigwedge^p E$ $(p > 1)$ не содержит свободных элементов.

в) Показать, что если E — модуль, определенный в упражнении 4 § 2, то $\bigwedge^2 E$ не сводится к 0. Привести пример кольца целостности A и A-модуля E, содержащегося в его поле отношений K, таких, что никакая внешняя степень $\bigwedge^p E$ не сводится к 0.

10) Привести пример кольца A, обладающего следующим свойством: в A-модуле $E = A^2$ существует подмодуль F такой, что $\bigwedge^2 \varphi$, где φ — каноническое отображение F в E, есть тождественный нуль, тогда как ни $\bigwedge^2 E$, ни $\bigwedge^2 F$ не сводятся к 0. [См. упражнение 4 § 1.]

11) Пусть E и F — векторные пространства над одним и тем же полем и u — линейное отображение E в F, имеющее конечный ранг r. Показать, что если $p \leqslant r$, то ранг $\bigwedge^p u$ равен $\binom{r}{p}$, а если $p > r$, то $\bigwedge^p u$ есть тождественный нуль. [Взять в E базис, r векторов которого обра-

зуют базис подпространства, дополнительного к $u^{-1}(0)$, а остальные — базис подпространства $u^{-1}(0)$.]

*12) Пусть E — A-модуль, обладающий базисом (e_i), состоящим из n элементов. Показать, что если $n > 1$ и $p \neq n - p$, то не существует изоморфизма φ модуля $\bigwedge^p E$ на $\bigwedge^{n-p} E$, который бы зависел лишь от структуры A-модуля в E. [Такой изоморфизм должен был бы удовлетворять тождеству $\varphi \circ u_p = u_{n-p} \circ \varphi$ для каждого автоморфизма u модуля E; взять за u автоморфизм, определяемый условиями $u(e_i) = e_i + e_j$, $u(e_k) = e_k$ при $k \neq i$, и придавать i и j всевозможные значения.]

13) Показать, что внешняя алгебра $\bigwedge E$ модуля E изоморфна факторалгебре тензорной алгебры $T(E)$ (§ 4, n° 6) этого модуля по ее двустороннему идеалу, a, порожденному элементами $x \otimes x$, где x пробегает E.

14) Пусть E — векторное пространство над полем.

а) Для того чтобы элемент $z = \sum_{p=0}^{\infty} z_p$ $(z_p \in \bigwedge^p E)$ внешней алгебры $\bigwedge E$ был обратимым, необходимо и достаточно, чтобы $z_0 \neq 0$. [Доказать это сначала для случая конечномерного E и перейти далее к общему случаю, заметив, что для каждого элемента $z \in \bigwedge E$ в E существует конечномерное подпространство F такое, что $z \in \bigwedge F$.]

б) Если размерность E бесконечна либо конечна и четна, то центр внешней алгебры $\bigwedge E$ образован теми ее элементами z, у которых $z_p = 0$ для всех *нечетных* индексов p; если E имеет нечетную конечную размерность n, то центр алгебры $\bigwedge E$ является суммой подпространства, образованного указанными элементами, и n-й внешней степени E.

15) Пусть A — коммутативное кольцо с единицей и E — алгебра над A, обладающая единичным элементом, который мы будем обозначать ε. Пусть, далее, $(x_i)_{1 \leqslant i \leqslant n}$ — конечная последовательность элементов из E такая, что $x_i x_j = -x_j x_i$ при $i \neq j$ и $x_i^2 = 0$ $(1 \leqslant i \leqslant n)$, и L — внешняя алгебра модуля A^n. Если каждому элементу

$$z = \alpha_0 + \sum_{(i_k)} \alpha_{i_1 \dots i_p} e_{i_1} \wedge \dots \wedge e_{i_p}$$

из L, отнесенному к каноническому базису (e_i) модуля A^n, поставить в соответствие элемент

$$z(x_1, \dots, x_n) = \alpha_0 \varepsilon + \sum_{(i_k)} \alpha_{i_1 \dots i_p} x_{i_1} \dots x_{i_p}$$

из E, то этим определится представление алгебры L в алгебру E, и образом L при этом представлении будет служить подалгебра в E, порожденная единичным элементом ε и элементами x_i $(1 \leqslant i \leqslant n)$.

§ 6. Определители

В этом параграфе рассматриваются лишь коммутативные кольца с единицей и унитарные модули над такими кольцами, обладающие конечным базисом.

1. Определение определителей

Пусть u — эндоморфизм A-модуля E, имеющего базис, состоящий из n элементов; n-я внешняя степень $\bigwedge^n u$ этого эндоморфизма (§ 5, n° 7) есть эндоморфизм модуля $\bigwedge^n E$; но этот последний модуль имеет базис, состоящий из *единственного* элемента (§ 5, n° 6), иными словами, изоморфен A (рассматриваемому как A-модуль), и следовательно, каждый эндоморфизм модуля $\bigwedge^n E$ есть *гомотетия* $z \to \lambda z$ (гл. II, § 4, предложение 1).

Определение 1. *Определителем эндоморфизма u модуля E, имеющего базис, состоящий из n элементов, называют скаляр λ, обозначаемый* $\det u$, *такой, что внешняя степень $\bigwedge^n u$ совпадает с гомотетией $z \to \lambda z$ модуля $\bigwedge^n E$.*

Согласно определению $\bigwedge^n u$, каковы бы ни были n элементов $x_i \in E$,

$$u(x_1) \wedge \ldots \wedge u(x_n) = (\det u) \cdot x_1 \wedge \ldots \wedge x_n. \tag{1}$$

Определитель тождественного эндоморфизма равен 1.

Теорема 1. *Если u и v — эндоморфизмы модуля E, то*

$$\det(u \circ v) = (\det u)(\det v). \tag{2}$$

Действительно (§ 5, формула (8)), $\bigwedge^n (u \circ v) = (\bigwedge^n u) \circ (\bigwedge^n v)$.

Определение 2. *Пусть X — квадратная матрица n-го порядка над коммутативным кольцом A с множеством I индексов строк и столбцов. Определитель эндоморфизма A-модуля A^I,*

имеющего матрицу X относительно канонического базиса этого модуля (гл. II, § 6, n° 5), *называется определителем матрицы X и обозначается* $\det X$ *или* $\boxed{X}$.

В том (наиболее часто встречающемся) случае, когда I есть интервал $[1, n] \subset \mathbf{N}$, так что $X = (\xi_{ij})_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n}$, определитель матрицы X обозначают также $\det(\xi_{ij})_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n}$ (или просто $\det(\xi_{ij})$, если это не грозит никакой путаницей), или $\boxed{\xi_{ij}}$, или, наконец,

$$\begin{vmatrix} \xi_{11} & \xi_{12} & \cdots & \xi_{1n} \\ \xi_{21} & \xi_{22} & \cdots & \xi_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \xi_{n1} & \xi_{n2} & \cdots & \xi_{nn} \end{vmatrix}.$$

Если $(e_i)_{1 \leqslant i \leqslant n}$ — канонический базис модуля A^n, эндоморфизм u, матрицей которого служит X, — это эндоморфизм, для которого $u(e_i)$ есть *столбец* $x_i = \sum_{j=1}^{n} e_j \xi_{ji}$ матрицы X (гл. II, § 6, n° 3); таким образом, согласно (1), определитель матрицы X определяется соотношением

$$x_1 \wedge \ldots \wedge x_n = (\det X) \cdot e_1 \wedge \ldots \wedge e_n, \tag{3}$$

так что можно написать (см. гл. II, § 1, n° 6)

$$\det X = \frac{x_1 \wedge \ldots \wedge x_n}{e_1 \wedge \ldots \wedge e_n}.$$

Матрицу X, у которой $\det X = 1$, называют *унимодулярной*.

Пусть E — A-модуль, имеющий базис (a_i), состоящий из n элементов. *Определителем n векторов* $x_j = \sum_{i=1}^{n} a_i \xi_{ij}$ $(1 \leqslant j \leqslant n)$ этого модуля относительно базиса (a_i) называют определитель матрицы (ξ_{ij}), j-й столбец которой образован компонентами x_j относительно базиса (a_i); этот определитель обозначают иногда $[x_1, x_2, \ldots, x_n]$ (если никакая неясность по поводу базиса невозможна).

Таким образом, имеем

$$x_1 \wedge \ldots \wedge x_n = [x_1, \ldots, x_n] \cdot a_1 \wedge \ldots \wedge a_n.$$

Примеры. Определитель квадратной матрицы первого порядка равен ее единственному элементу. Для матрицы второго порядка

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

имеем в предыдущих обозначениях

$$x_1 \wedge x_2 = (e_1 a_{11} + e_2 a_{21}) \wedge (e_1 a_{12} + e_2 a_{22}) = a_{11} a_{22} e_1 \wedge e_2 + a_{21} a_{12} e_2 \wedge e_1,$$

откуда

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11} a_{22} - a_{12} a_{21}.$$

Замечание. Рассматривая определитель матрицы $X = (\xi_{ij})$, часто позволяют себе, допуская вольность речи, говорить об «элементах определителя», «строках определителя», «столбцах определителя», понимая под этим элементы, строки и столбцы матрицы X.

Если X и Y — квадратные матрицы над A с одинаковым множеством индексов I, то их *произведение* XY соответствует композиции эндоморфизмов модуля A^I, соответствующих матрицам Y и X (гл. II, § 6, n° 4); поэтому, согласно теореме 1, имеем:

Предложение 1. *Определитель произведения XY квадратных матриц X и Y* (имеющих одно и то же множество индексов) *равен произведению определителей этих матриц.*

Другими словами, если рассматривать в A и множестве $\mathbf{M}_n(A)$ всех квадратных матриц n-го порядка над A лишь алгебраические структуры, определяемые одними *мультипликативными* законами этих двух колец, можно сказать, что $X \to \det X$ есть *представление* $\mathbf{M}_n(A)$ в A.

Следствие 1. *Если X и Y — квадратные матрицы одинакового порядка, то* $\det(XY) = \det(YX)$.

Отметим аналогию между этим следствием и предложением 2 § 4, относящимся к *следу* произведения двух матриц. Однако эта аналогия не полна: действительно, если X — матрица из m строк и n столбцов, Y — матрица из n строк и m столбцов и $n < m$, то, как можно показать, $\det(XY) = 0$, тогда как вообще $\det(YX) \neq 0$ (упражнение 6).

Сужение представления $X \to \det X$ на (мультипликативную) *группу обратимых* матриц n-го порядка над A (изоморфную

линейной группе $\mathrm{GL}_n(A)$) является представлением этой группы в группу обратимых элементов кольца A. Отсюда:

Следствие 2. *Если X — обратимая квадратная матрица над A, то ее определитель обратим в A, причем*

$$\det(X^{-1}) = (\det X)^{-1}. \tag{4}$$

Ниже мы увидим (теорема 2), что, и обратно, если $\det X$ обратим в A, то матрица X обратима.

Отметим, что образом алгебры $\mathbf{M}_n(A)$ при отображении $X \to \det X$ является все кольцо A, ибо определитель диагональной матрицы

$$\begin{pmatrix} \alpha & 0 \dots 0 \\ 0 & 1 \dots 0 \\ \cdot & \cdot \quad \cdot \\ 0 & 0 \dots 1 \end{pmatrix}$$

равен α. На том же основании образ группы обратимых матриц при отображении $X \to \det X$ совпадает с группой всех обратимых элементов из A.

Предложение 2. *Две подобные квадратные матрицы имеют одинаковые определители.*

Если X и X' подобны, то существует обратимая матрица P такая, что $X' = PXP^{-1}$; поэтому справедливость утверждения вытекает из предложения 1 и его следствия. Предложение 2 можно доказать также, заметив, что две подобные матрицы могут рассматриваться как матрицы одного и того же эндоморфизма модуля A^n относительно двух разных базисов.

Следствие. *Определитель матрицы не изменится, если подвергнуть строки и столбцы этой матрицы одной и той же подстановке* (гл. II, § 6, n° 11).

2. *Вычисление определителя*

Предложение 3. *Определитель матрицы X n-го порядка является знакопеременной полилинейной формой относительно n столбцов x_i этой матрицы.*

Это утверждение есть непосредственное следствие формулы (3) и того, что

$$(x_1, \dots, x_n) \longrightarrow x_1 \wedge \dots \wedge x_n$$

— знакопеременное полилинейное отображение (см. § 8).

В частности, определитель с двумя совпадающими столбцами равен нулю. Если произвести над столбцами определителя подстановку σ, он умножится на ε_σ. Если к столбцу определителя прибавить скалярное кратное другого столбца, определитель не изменится.

Следствие. *Каждая знакопеременная полилинейная форма относительно n векторов x_i из A^n может быть записана в виде*

$$(x_1, \ldots, x_n) \longrightarrow \lambda [x_1, \ldots, x_n] \quad (\lambda \in A).$$

Действительно, такой форме соответствует линейная форма на n-й внешней степени G модуля A^n (§ 5, n° 5); так как G имеет базис, образованный единственным элементом e, то каждая линейная форма на G записывается в виде $\xi e \longrightarrow \lambda\xi$, где $\lambda \in A$, чем утверждение следствия и доказано.

Заменяя в формуле (3) каждый из столбцов x_i его выражением $\sum_{j=1}^{n} e_j \xi_{ji}$ и раскрывая внешнее произведение, видим, что

$$(\det X) \cdot e_1 \wedge \ldots \wedge e_n = \sum_\sigma \xi_{\sigma(1),\,1} \ldots \xi_{\sigma(n),\,n}\, e_{\sigma(1)} \wedge \ldots \wedge e_{\sigma(n)},$$

и так как $e_{\sigma(1)} \wedge \ldots \wedge e_{\sigma(n)} = \varepsilon_\sigma \cdot e_1 \wedge \ldots \wedge e_n$, то получаем, что

$$\det X = \det (\xi_{ij}) = \sum_\sigma \varepsilon_\sigma \xi_{\sigma(1),\,1} \ldots \xi_{\sigma(n),\,n}, \tag{5}$$

где сумма распространяется на все $n!$ подстановок σ симметрической группы $\mathfrak{S}_n$.

Правая часть формулы (5) будет называться *полным разложением* определителя матрицы X.

Так как кольцо A коммутативно, то для любой пары подстановок σ, τ группы $\mathfrak{S}_n$ имеем

$$\xi_{\sigma(1),\,1} \ldots \xi_{\sigma(n),\,n} = \xi_{\sigma(\tau(1)),\,\tau(1)} \ldots \xi_{\sigma(\tau(n)),\,\tau(n)}.$$

Беря, в частности, $\tau = \sigma^{-1}$ и замечая, что $\varepsilon_{\sigma^{-1}} = \varepsilon_\sigma$, мы видим поэтому также, что

$$\det X = \sum_\sigma \varepsilon_\sigma \xi_{1,\,\sigma(1)} \ldots \xi_{n,\,\sigma(n)}. \tag{6}$$

Для каждой пары индексов (i, j) положим $\eta_{ij} = \xi_{ji}$; формулы (5) и (6) показывают, что $\det (\eta_{ij}) = \det (\xi_{ij})$; иными словами:

Предложение 4. *Определитель матрицы, получающейся путем транспонирования матрицы X, равен определителю матрицы X.*

Это свойство выражают также, говоря, что *замена строк столбцами не изменяет значения определителя.*

В главе VI будет дано другое доказательство этого предложения, основанное на неприводимости определителя, рассматриваемого как полином от своих элементов.

Следствие. *Определитель квадратной матрицы X является знакопеременной полилинейной функцией ее строк.*

Чтобы убедиться в этом, достаточно применить предложение 3 к транспонированной матрице ${}^tX$.

Отсюда вытекают те же следствия, что и из предложения 3, с заменой в формулировках слова «столбец» словом «строка».

Из формулы (6) непосредственно видно, что определитель общей матрицы X n-го порядка над A, рассматриваемый как функция ее n столбцов x_i $(1 \leqslant i \leqslant n)$, является *результатом антисимметрирования* полилинейной формы

$$(x_1, \ldots, x_n) \longrightarrow \langle x_1, e'_1\rangle \ldots \langle x_n, e'_n\rangle,$$

где (e'_i) означает базис, сопряженный к каноническому базису (e_i) модуля A^n (см. теорему 1 § 5); рассматриваемый как функция n строк x^i $(1 \leqslant i \leqslant n)$ матрицы X, ее определитель опять-таки есть результат антисимметрирования той же полилинейной формы в силу предложения 4.

3. *Миноры матрицы*

Каждой прямоугольной матрице $X = (\xi_{\lambda\mu})$, множества L, M индексов строк и столбцов которой различны, но имеют *одно и то же число элементов* n, как мы видели (гл. II, § 6, n° 5), можно несколькими способами поставить в соответствие *квадратную* матрицу n-го порядка, множеством индексов строк и столбцов которой служит интервал $[1, n] \subset \mathbf{N}$, располагая элементы множества L в последовательность (λ_i) и элементы множества M — в последовательность (μ_i); соответствующей квадратной матрицей будет матрица $(\eta_{ij})_{1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n}$, где $\eta_{ij} = \xi_{\lambda_i \mu_j}$.

Определение 3. *Пусть X — прямоугольная матрица из m строк и n столбцов. Ее минорами p-го порядка* (где $p \leqslant \min(m, n)$) *называют определители квадратных матриц p-го порядка, получающихся из подматриц матрицы X, имеющих p строк и p столбцов.*

Различные квадратные матрицы, получающиеся из заданной подматрицы матрицы X, отличаются друг от друга лишь порядком строк и столбцов, а потому их определители *с точностью до знака* совпадают; тем самым миноры p-го порядка матрицы X определены с точностью до знака. Во всей остающейся части этой главы мы ограничимся тем случаем, когда множеством индексов строк матрицы $X=(\xi_{ij})$ служит интервал $[1, m] \subset \mathbf{N}$, а множеством индексов столбцов — интервал $[1, n]$. Пусть тогда H (соответственно K) — подмножество множества индексов $[1, m]$ (соответственно $[1, n]$), состоящее из p элементов, и рассмотрим подматрицу матрицы X, получающуюся путем вычеркивания в X строк с индексами $i \in \complement H$ и столбцов с индексами $j \in \complement K$; обозначим через $\mathbf{X}_{H, K}$ определитель квадратной матрицы, получающейся из этой подматрицы путем расположения индексов ее строк и столбцов в *возрастающую последовательность* (i_k) (соответственно (j_k)); тем самым минор $\mathbf{X}_{H, K}$ определен соотношением

$$(e_{i_1}\xi_{i_1 j_1} + \ldots + e_{i_p}\xi_{i_p j_1}) \wedge \ldots \wedge (e_{i_1}\xi_{i_1 j_p} + \ldots + e_{i_p}\xi_{i_p j_p}) = \\ = \mathbf{X}_{H, K} \cdot e_{i_1} \wedge \ldots \wedge e_{i_p}. \quad (7)$$

Понятие минора матрицы позволяет выразить *компоненты разложимого p-вектора* $x_1 \wedge \ldots \wedge x_p$ относительно базиса (e_H) модуля $\bigwedge^p E$, соответствующего базису (e_i) модуля E, через компоненты элементов x_k относительно базиса (e_i). Действительно, пусть X — матрица (ξ_{ij}) из n строк и p столбцов, j-м столбцом которой для $1 \leqslant j \leqslant p$ служит x_j; формула (7) показывает, что компонентой p-вектора $x_1 \wedge \ldots \wedge x_p$ с индексом H служит *минор p-го порядка* матрицы X, имеющий H множеством индексов строк.

Рассмотрим теперь линейное отображение u модуля $E=A^n$ в $F=A^m$; пусть X — его матрица (из m строк и n столбцов) относительно канонических базисов $(e_j)_{1 \leqslant j \leqslant n}$ и $(f_i)_{1 \leqslant i \leqslant m}$ модулей E и F; поставим своей целью найти матрицу *p-й внешней степени* $\bigwedge^p u$ относи-

тельно базисов (e_K) и (f_H) модулей $\bigwedge^p E$ и $\bigwedge^p F$. Если (j_k) — последовательность индексов, образующих K, расположенных в порядке возрастания, то $\bigwedge^p u(e_K) = u(e_{j_1}) \wedge \ldots \wedge u(e_{j_p})$; поэтому элемент матрицы отображения $\bigwedge^p u$, стоящий на пересечении строки с индексом H и столбца с индексом K, есть не что иное, как H-я компонента разложимого p-вектора $\bigwedge^p u(e_K)$, т. е. *минор* $\mathbf{X}_{H,K}$ матрицы X. Иными словами, матрицей отображения $\bigwedge^p u$ служит матрица $(\mathbf{X}_{H,K})$ (из $\binom{m}{p}$ строк и $\binom{n}{p}$ столбцов), образованная минорами p-го порядка матрицы X (со знаком, установленным описанным выше образом); мы будем обозначать ее $\bigwedge^p X$ и называть *p-й внешней степенью* матрицы X.

4. *Разложения определителя*

Вернемся к формуле (3), задающей определитель матрицы $X=(\xi_{ij})$ n-го порядка. Пусть H — подмножество множества индексов $[1, n]$, состоящее из p элементов $(1 \leqslant p \leqslant n)$, H' — его дополнение относительно $[1, n]$ и (i_k) (соответственно (j_k)) — последовательность индексов, образующих H (соответственно H'), расположенных в порядке возрастания; можно написать

$$x_1 \wedge \ldots \wedge x_n = \varepsilon_{H,H'}(x_{i_1} \wedge \ldots \wedge x_{i_p}) \wedge (x_{j_1} \wedge \ldots \wedge x_{j_{n-p}}), \qquad (8)$$

где $\varepsilon_{H,H'} = (-1)^\nu$, а ν означает число тех пар (i, j), в которых $i \in H$, $j \in H'$ и $j < i$ (§ 5, n° 9). В обозначениях из n° 3 имеем

$$x_{i_1} \wedge \ldots \wedge x_{i_p} = \sum_K e_K \mathbf{X}_{K,H},$$

$$x_{j_1} \wedge \ldots \wedge x_{j_{n-p}} = \sum_L e_L \mathbf{X}_{L,H'},$$

где K пробегает множество всех подмножеств интервала $[1, n]$, состоящих из p элементов, а L — множество всех подмножеств этого интервала, состоящих из $n-p$ элементов. Подставляя эти выражения в (8) и принимая во внимание таблицу умножения базиса (e_H) внешней алгебры (§ 5, n° 9, формула (14)), мы видим, что $e_K \wedge e_L = 0$, если только L не равно дополнению K' множества K

относительно $[1, n]$. Это приводит к следующей формуле для определителя матрицы X:

$$\det X = \varrho_{H, H'} \sum_K \varrho_{K, K'} \mathbf{X}_{K, H} \mathbf{X}_{K', H'}. \tag{9}$$

Эта формула известна под названием *лапласовского разложения* определителя матрицы X по p столбцам с индексами из H (или по $n-p$ столбцам с индексами из H'); миноры $\mathbf{X}_{K, H}$ и $\mathbf{X}_{K', H'}$ называются *дополнительными* друг к другу.

Важный случай лапласовского разложения имеем при $p=1$, $H=\{j\}$; тогда для каждого множества $K=\{i\}$, состоящего из одного элемента, $\mathbf{X}_{K, H}=\xi_{ij}$; $\mathbf{X}_{K', H'}$ есть минор $(n-1)$-го порядка, получающийся путем вычеркивания в X j-го столбца и i-й строки и обозначаемый далее $\mathbf{X}^{ij}$. Так как, очевидно, $\varrho_{H, H'}=(-1)^{j-1}$ и $\varrho_{K, K'}=(-1)^{i-1}$, то формула (9) принимает в этом частном случае вид

$$\det X = \sum_{i=1}^{n} (-1)^{i+j} \xi_{ij} \mathbf{X}^{ij}; \tag{10}$$

ее называют *разложением определителя матрицы X по j-му столбцу*. Минор $(-1)^{i+j}\mathbf{X}^{ij}$ называется *алгебраическим дополнением* элемента ξ_{ij}.

Отметим, что при заданном множестве $H \subset [1, n]$ из p элементов миноры $\mathbf{X}_{K, H}$ зависят лишь от элементов матрицы X, находящихся в столбцах с индексами, принадлежащими H; из этого замечания вытекает, что если L — подмножество в $[1, n]$, состоящее из $n-p$ элементов и не совпадающее с дополнением H' к H, то

$$\sum_K \varrho_{K, K'} \mathbf{X}_{K, H} \mathbf{X}_{K', L} = 0. \tag{11}$$

Действительно, это выражение дает, с точностью до знака, лапласовское разложение (по столбцам с индексами $i \in H$) определителя, получающегося путем замены в определителе матрицы X столбцов, индексы которых принадлежат H', столбцами, индексы которых принадлежат L (с соблюдением расположения индексов). Так как H и L имеют по крайней мере один общий индекс, то этот новый определитель имеет по крайней мере два одинаковых столбца и, значит (предложение 2), равен нулю.

В частности, при $k \neq j$ имеем

$$\sum_{i=1}^{n} (-1)^i \xi_{ij} \mathbf{X}^{ih} = 0. \tag{12}$$

Рассматривая определитель матрицы, *транспонированной* к X, мы, в силу предложения 4, снова получаем «разложения» для $\det X$, на этот раз по *строкам* этого определителя.

Замечание. Лапласовское разложение существенно опирается на *ассоциативность* внешнего произведения; было бы выгоднее прямо воспользоваться этим свойством, не прибегая к помощи формулы (9).

Примеры. 1) Определитель Вандермонда. Пусть $(z_i)_{1 \leqslant i \leqslant n}$ — заданная последовательность n элементов кольца A. *Определителем Вандермонда* этой последовательности называется определитель n-го порядка

$$V(z_1, z_2, \ldots, z_n) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ z_1 & z_2 & \ldots & z_n \\ z_1^2 & z_2^2 & \ldots & z_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ z_1^{n-1} & z_2^{n-1} & \ldots & z_n^{n-1} \end{vmatrix}.$$

Покажем, что

$$V(z_1, \ldots, z_n) = \prod_{i<j} (z_j - z_i). \tag{13}$$

Принимая во внимание очевидность утверждения при $n=1$, проведем доказательство индукцией по n. Для каждого индекса $k \geqslant 2$ вычтем из k-й строки $(k-1)$-ю, умноженную на z_1; значение определителя не изменится, и мы получим, что

$$V(z_1, z_2, \ldots, z_n) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ 0 & z_2 - z_1 & \ldots & z_n - z_1 \\ 0 & z_2(z_2 - z_1) & \ldots & z_n(z_n - z_1) \\ \ldots & \ldots & \ldots & \ldots \\ 0 & z_2^{n-2}(z_2 - z_1) & \ldots & z_n^{n-2}(z_n - z_1) \end{vmatrix}.$$

Разлагая этот определитель по первому столбцу и затем вынося из $(k-1)$-го столбца получающегося так минора множитель $z_k - z_1$ $(2 \leqslant k \leqslant n)$, будем иметь

$$V(z_1, z_2, \ldots, z_n) = (z_2 - z_1)(z_3 - z_1) \ldots (z_n - z_1) V(z_2, \ldots, z_n),$$

откуда и следует справедливость формулы (13).

2) Рассмотрим квадратную матрицу n-го порядка, имеющую вид «квадратной клеточной матрицы» (гл. II, § 6, п° 5):

$$X = \begin{pmatrix} Y & T \\ 0 & Z \end{pmatrix}.$$

Покажем, что

$$\det X = (\det Y)(\det Z). \tag{14}$$

Пусть h — порядок матрицы Y; столбцы $x_1, x_2, \ldots, x_h$ матрицы X принадлежат подмодулю, имеющему базис $e_1, e_2, \ldots, e_h$, и, в силу формулы (3),

$$x_1 \wedge \ldots \wedge x_h = (\det Y) \cdot e_1 \wedge \ldots \wedge e_h. \tag{15}$$

С другой стороны, для каждого индекса $i > h$ можно написать $x_i = x_i' + x_i''$, где x_i' — линейная комбинация элементов $e_1, \ldots, e_h$, а x_i'' — линейная комбинация элементов $e_{h+1}, \ldots, e_n$. В силу (15), для каждого $i > h$ имеем тогда $x_1 \wedge \ldots \wedge x_h \wedge x_i' = 0$, и значит,

$$x_1 \wedge \ldots \wedge x_n = (\det Y) \cdot e_1 \wedge \ldots \wedge e_h \wedge (x_{h+1}'' \wedge \ldots \wedge x_n'').$$

Но так как, по определению $\det Z$,

$$x_{h+1}'' \wedge \ldots \wedge x_n'' = (\det Z) \cdot e_{h+1} \wedge \ldots \wedge e_n,$$

то мы и получили формулу (14).

Из нее индукцией по p сразу следует, что если X имеет вид клеточной матрицы

$$X = \begin{pmatrix} X_{11} & X_{12} & \ldots & X_{1p} \\ 0 & X_{22} & \ldots & X_{2p} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & X_{pp} \end{pmatrix},$$

где все матрицы, находящиеся под диагональю, *нулевые*, то

$$\det X = (\det X_{11})(\det X_{22}) \ldots (\det X_{pp}).$$

5. *Выражение для обратной матрицы. Применение к линейным уравнениям*

Пусть $A = (\alpha_{ij})$ — заданная квадратная матрица n-го порядка над коммутативным кольцом C с единицей; положим $\beta^{ji} = (-1)^{i+j} \mathbf{A}^{ij}$ (алгебраическое дополнение элемента α_{ij}); формулы (10) и (12) допускают следующую запись:

$$\sum_{i=1}^{n} \beta^{ji} \alpha_{ik} = \delta_{jk} \det A, \tag{16}$$

где δ_{jk} — кронекеровский символ; обозначая через B квадратную матрицу (β^{ij}), можно записать соотношение (16) также в виде

$$BA = (\det A) \cdot I_n. \tag{17}$$

Рассматривая разложения определителя матрицы A по ее строкам, получим аналогично формулу

$$AB = (\det A) \cdot I_n. \tag{18}$$

Принимая во внимание следствие 2 предложения 1, мы видим, таким образом, что справедлива следующая теорема:

Теорема 2. *Для того чтобы квадратная матрица над коммутативным кольцом C* (с единицей) *была обратимой, необходимо и достаточно, чтобы ее определитель был обратимым в C.*

Матрица $\widetilde{A} = (\mathbf{A}^{ij})$ есть не что иное, как $(n-1)$-*я внешняя степень* матрицы A. Формулы (17) и (18) показывают, что если A обратима, то обратная к ней матрица получается путем взятия матрицы, *транспонированной к* $\widetilde{A}$, умножения в этой матрице i-й строки на $(-1)^i$ и j-го столбца на $(-1)^j$ для всех i и j от 1 до n и, наконец, умножения полученной матрицы на $(\det A)^{-1}$ (см. § 8, предложение 5).

Рассмотрим на кольце C систему n линейных уравнений с n неизвестными

$$\sum_{i=1}^{n} a_{ij}\xi_j = \eta_i \qquad (1 \leqslant i \leqslant n). \tag{19}$$

При обычном отождествлении матрицы из одного столбца, образованного элементами ξ_i (соответственно η_i), с элементом $x = (\xi_i)$ (соответственно $y = (\eta_i)$) из C^n, система (19) записывается также (гл. II, § 6, n° 4) в виде

$$Ax = y. \tag{20}$$

Пусть u — эндоморфизм $x \to Ax$ C-модуля C^n; утверждение, что уравнение (20) имеет (по крайней мере одно) решение для *каждого* $y \in C^n$, равносильно утверждению, что u есть отображение модуля $E = C^n$ на себя; тогда и $\bigwedge^n u$ отображает $\bigwedge^n E$ *на* себя; но $\bigwedge^n E$ изоморфно C-модулю C, а $\bigwedge^n u$ есть гомотетия $z \to (\det A)\, z$ модуля $\bigwedge^n E$; поэтому существует $\mu \in C$ такое, что $\mu(\det A) = 1$, иными словами, $\det A$ обратим в C. Обратно, согласно теореме 2, обратимость $\det A$ в C влечет, что u есть *автоморфизм* модуля E. В итоге имеем:

Предложение 5. *Для того чтобы система n линейных уравнений с n неизвестными на коммутативном кольце* (с единицей) *обладала по крайней мере одним решением при любых правых частях, необходимо и достаточно, чтобы определитель матрицы этой системы был обратимым; и в этом случае решение системы единственно.*

Полагая $\Delta = \det A$, получаем из (17) и (20), что

$$\Delta x = By, \tag{21}$$

т. е.

$$\Delta\xi_i = \sum_{j=1}^{n} (-1)^{i+j}\eta_j \mathbf{A}^{ji} \quad (1 \leqslant i \leqslant n)$$

или, иначе,

$$\Delta\xi_i = \Delta_i \quad (1 \leqslant i \leqslant n), \tag{22}$$

где Δ_i означает определитель, получающийся из Δ путем замены его i-го столбца столбцом $y=(\eta_j)$. Если Δ обратим, единственное решение системы (19) задается формулами (22), называемыми *формулами Крамера*. Кроме того, принимая $y=0$, получаем из (22)

Предложение 6. *Если* однородная *линейная система n уравнений с n неизвестными на коммутативном кольце обладает ненулевым решением, то определитель ее матрицы является делителем нуля.*

Можно показать, что это необходимое условие также *достаточно* (§ 7, упражнение 2).

Замечание. Формулы Крамера могут быть получены также следующим образом. Обозначим столбцы матрицы A через a_i $(1 \leqslant i \leqslant n)$; тогда система (19) равносильна уравнению

$$\sum_{j=1}^{n} a_j\xi_j = y \tag{23}$$

на $E=C^n$. Умножив (внешне) обе части формулы (23) слева на $a_1 \wedge \ldots \wedge a_{i-1}$, а справа — на $a_{i+1} \wedge \ldots \wedge a_n$, получим

$$\xi_i \cdot a_1 \wedge \ldots \wedge a_n = a_1 \wedge \ldots \wedge a_{i-1} \wedge y \wedge a_{i+1} \wedge \ldots \wedge a_n,$$

что, в силу формулы (3), равносильно формуле (22).

Упражнения. 1) Если в определителе Δ n-го порядка заменить i-й столбец для каждого индекса i суммой всех столбцов с индексами $\neq i$, то получится определитель, равный $(-1)^{n-1}(n-1)\Delta$. Если в Δ из i-го столбца для каждого индекса i вычесть сумму всех столбцов с индексами $\neq i$, то получится определитель, равный $-(n-2)\,2^{n-1}\Delta$.

2) Пусть $\Delta=\det(\alpha_{ij})$ — определитель n-го порядка; для всех i и j от 1 до $n-1$ положим

$$\beta_{ij}=\begin{vmatrix}\alpha_{1j} & \alpha_{1,\,j+1}\\ \alpha_{i+1,\,j} & \alpha_{i+1,\,j+1}\end{vmatrix}.$$

Доказать, что определитель $\det(\beta_{ij})$ $(n-1)$-го порядка равен $\alpha_{12}\alpha_{13}\dots\alpha_{1n}\Delta$.

3) Доказать тождество

$$\begin{vmatrix} x_1 & y_1 & \alpha_{13} & \alpha_{14}\dots\alpha_{1n}\\ \lambda_1x_2 & x_2 & y_2 & \alpha_{24}\dots\alpha_{2n}\\ \lambda_1\lambda_2x_3 & \lambda_2x_3 & x_3 & y_3\dots\alpha_{3n}\\ \dots\dots & \dots\dots\dots\dots\dots\dots\dots & & \\ \lambda_1\lambda_2\dots\lambda_{n-1}x_n & \lambda_2\dots\lambda_{n-1}x_n & \lambda_3\dots\lambda_{n-1}x_n & \lambda_4\dots\lambda_{n-1}x_n\dots x_n\end{vmatrix}=$$
$$=(x_1-\lambda_1y_1)(x_2-\lambda_2y_2)\dots(x_{n-1}-\lambda_{n-1}y_{n-1})\,x_n.$$

Вывести из него следующие тождества:

$$\begin{vmatrix}1 & 1 & 1\dots 1\\ b_1 & a_1 & a_1\dots a_1\\ b_1 & b_2 & a_2\dots a_2\\ \dots & \dots & \\ b_1 & b_2 & b_3\dots a_n\end{vmatrix}=(a_1-b_1)(a_2-b_2)\dots(a_n-b_n),$$

$$\begin{vmatrix}a_1b_1 & a_1b_2 & a_1b_3\dots a_1b_n\\ a_1b_2 & a_2b_2 & a_2b_3\dots a_2b_n\\ a_1b_3 & a_2b_3 & a_3b_3\dots a_3b_n\\ \dots & \dots & \\ a_1b_n & a_2b_n & a_3b_n\dots a_nb_n\end{vmatrix}=a_1b_n(a_2b_1-a_1b_2)\dots(a_nb_{n-1}-a_{n-1}b_n),$$

$$\begin{vmatrix}a_2a_3\dots a_n & a_3a_4\dots a_nb_1 & a_4\dots a_nb_1b_2\dots a_1b_2b_3\dots b_{n-1}\\ b_2b_3\dots b_n & a_3a_4\dots a_na_1 & a_4\dots a_na_1b_2\dots a_1a_2b_3\dots b_{n-1}\\ a_2b_3\dots b_n & b_3b_4\dots b_nb_1 & a_4\dots a_na_1a_2\dots a_1a_2a_3\dots b_{n-1}\\ \dots & \dots & \\ a_2a_3\dots b_n & a_3a_4\dots b_nb_1 & a_4\dots b_nb_1b_2\dots a_1a_2a_3\dots a_{n-1}\end{vmatrix}=$$
$$=(a_1a_2\dots a_n-b_1b_2\dots b_n)^{n-1}.$$

$$\begin{vmatrix}x & a_1 & a_2\dots a_{n-1} & 1\\ a_1 & x & a_2\dots a_{n-1} & 1\\ a_1 & a_2 & x\dots a_{n-1} & 1\\ \dots & \dots & & \\ a_1 & a_2 & a_3\dots x & 1\\ a_1 & a_2 & a_3\dots a_n & 1\end{vmatrix}=(x-a_1)(x-a_2)\dots(x-a_n),$$

$$\begin{vmatrix} x & a_1 & a_2 & \dots & a_n \\ a_1 & x & a_2 & \dots & a_n \\ a_1 & a_2 & x & \dots & a_n \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & x \end{vmatrix} = (x+a_1+a_2+\dots+a_n)(x-a_1)(x-a_2)\dots(x-a_n).$$

[Свести последний определитель к предыдущему.]

4) Вычислить определитель

$$\Delta_n = \begin{vmatrix} a_1+b_1 & b_1 & b_1 & \dots & b_1 \\ b_2 & a_2+b_2 & b_2 & \dots & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ b_n & b_n & b_n & \dots & a_n+b_n \end{vmatrix}.$$

[Выразить Δ_n с помощью Δ_{n-1}.]

5) Предполагая a_i и b_j элементами поля такими, что $a_i+b_j \neq 0$ для каждой пары индексов (i, j), доказать, что

$$\det\left(\frac{1}{a_i+b_j}\right) = \frac{\prod_{i<j}(a_j-a_i)(b_j-b_i)}{\prod_{i,j}(a_i+b_j)}.$$

6) Показать, что если X — матрица из n строк и m столбцов, Y — матрица из p строк и n столбцов, так что их произведение $Z = YX$ есть матрица из p строк и m столбцов, то при $n < q$ миноры q-го порядка матрицы Z равны нулю, а при $q \leqslant n$ они задаются формулой

$$\mathbf{Z}_{L,H} = \sum_K \mathbf{Y}_{L,K}\mathbf{X}_{K,H},$$

где K пробегает множество всех подмножеств интервала $[1, n]$, состоящих из q элементов. [Воспользоваться формулой (8) § 5.]

7) Пусть $\Delta = \det(\alpha_{ij})$ — определитель n-го порядка; обозначим через Δ_i для каждого индекса i определитель, получающийся путем умножения в Δ каждого элемента α_{ij} $(1 \leqslant j \leqslant n)$ на β_j. Показать, что

$$\Delta_1+\Delta_2+\dots+\Delta_n = (\beta_1+\beta_2+\dots+\beta_n)\Delta.$$

[Разложить Δ_i по i-й строке.]

8) Пусть $\Delta = \det(\alpha_{ij})$ — определитель n-го порядка и σ — подстановка из $\mathfrak{S}_n$; пусть, далее, Δ_i для каждого индекса i $(1 \leqslant i \leqslant n)$ — определитель, получающийся путем замены в Δ каждого элемента α_{ij} $(1 \leqslant j \leqslant n)$ элементом $\alpha_{i,\sigma(j)}$, и p — число индексов, инвариантных относительно подстановки σ. Показать, что

$$\Delta_1+\Delta_2+\dots+\Delta_n = p\Delta.$$

[Тот же метод, что и в упражнении 7.]

9) Пусть A — квадратная матрица n-го порядка, B — ее подматрица из p строк и q столбцов и C — матрица, получающаяся путем умножения в A каждого элемента из B на один и тот же скаляр α. Показать, что каждый член полного разложения определителя матрицы C равен соответствующему члену полного разложения определителя матрицы A, умноженному на скаляр вида α^r, где $r \geqslant p+q-n$ и зависит от рассматриваемого члена. [Образовать для $\det C$ надлежащее лапласовское разложение.]

10) Пусть Γ и Δ — определители n-го порядка, H и K — любые два подмножества интервала $[1, n]$, состоящие каждое из p элементов, (i_k) (соответственно (j_k)) — последовательность, полученная путем расположения членов множества H (соответственно K) в возрастающем порядке; пусть, далее, $\Gamma_{H,K}$ — определитель, получающийся путем замены в Γ каждого столбца с индексом i_k $(1 \leqslant k \leqslant p)$ столбцом определителя Δ с индексом j_k, и аналогично $\Delta_{K,H}$ — определитель, получающийся путем замены в Δ каждого столбца с индексом j_k $(1 \leqslant k \leqslant p)$ столбцом определителя Γ с индексом i_k. Показать, что для каждого $H \subset [1, n]$, состоящего из p элементов,

$$\Gamma\Delta = \sum_K \Gamma_{H,K}\Delta_{K,H},$$

где K пробегает множество всех подмножеств интервала $[1, n]$, состоящих из p элементов. [Воспользоваться формулами (9) и (11).]

11) Пусть Δ — определитель квадратной матрицы X n-го порядка и Δ_p — определитель квадратной матрицы $\bigwedge^p X$, порядка $\binom{n}{p}$. Показать, что

$$\Delta_p \Delta_{n-p} = \Delta^{\binom{n}{p}}.$$

[Воспользоваться формулами (9) и (11).]

12) Определитель $\det(\alpha_{ij})$ n-го порядка называется *центросимметрическим* (соответственно *косоцентросимметрическим*), если $\alpha_{n-i+1,\,n-j+1} = \alpha_{ij}$ (соответственно $\alpha_{n-i+1,\,n-j+1} = -\alpha_{ij}$) для всех i и j.

а) Показать, что центросимметрический определитель четного порядка $2p$ можно представить в виде произведения двух определителей p-го порядка, а центросимметрический определитель нечетного порядка $2p+1$ — в виде произведения определителей p-го и $(p+1)$-го порядков.

б) Показать, что косоцентросимметрический определитель четного порядка $2p$ можно представить в виде произведения двух определителей p-го порядка. Косоцентросимметрический определитель нечетного порядка $2p+1$ над A равен нулю, если в A соотношение $2\xi = 0$ влечет $\xi = 0$, и представим в виде произведения α_{pp} и двух определителей p-го порядка в противном случае.

13) Пусть $\Delta=\det(\alpha_{ij})$ — определитель n-го порядка и Δ_{ij} — минор $(n-1)$-го порядка, дополнительный к α_{ij}. Показать, что

$$\begin{vmatrix} \alpha_{11} & \alpha_{12} \dots \alpha_{1n} & x_1 \\ \alpha_{21} & \alpha_{22} \dots \alpha_{2n} & x_2 \\ \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} \dots \alpha_{nn} & x_n \\ y_1 & y_2 \dots y_n & z \end{vmatrix} = \Delta z - \sum_{i,j} (-1)^{i+j} \Delta_{ij} x_i y_j.$$

Показать, что если $\Delta=0$, а элементы α_{ij} принадлежат *полю*, то определитель, стоящий в левой части, является произведением линейной формы от $x_1, x_2, \dots, x_n$ на линейную форму от $y_1, y_2, \dots, y_n$. [Воспользоваться упражнением 11 § 5 и упражнением 6 § 6 главы II.]

Привести пример, где этот результат теряет силу, когда кольцо скаляров A не является полем. [Принять за A кольцо $\mathbf{Z}/(6)$ и n равным 2.]

14) Доказать тождество

$$\begin{vmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & a_1+a_2 & a_1+a_3 & \dots & a_1+a_n \\ 1 & a_2+a_1 & 0 & a_2+a_3 & \dots & a_2+a_n \\ 1 & a_3+a_1 & a_3+a_2 & 0 & \dots & a_3+a_n \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & a_n+a_1 & a_n+a_2 & a_n+a_3 & \dots & 0 \end{vmatrix} = (-1)^n 2^{n-1} \sum_{i=1}^{n} a_1 \dots a_{i-1} a_{i+1} \dots a_n.$$

[Использовать упражнение 13.]

§ 7. Определители над полем; разложимые p-векторы над векторным пространством

В этом параграфе рассматриваются лишь конечномерные векторные пространства над полем.

1. Свободные системы разложимых p-векторов

Теорема 1. *Пусть E — векторное пространство конечной размерности n над полем. Для того чтобы p векторов x_i $(1 \leqslant i \leqslant p)$ образовывали в E свободную систему, необходимо и достаточно, чтобы разложимый p-вектор $x_1 \wedge \dots \wedge x_p$ не равнялся нулю.*

Действительно, если векторы x_i образуют зависимую систему, то один из них равен линейной комбинации других (гл. II, § 3, предложение 1); при его замене этой комбинацией внешнее произведение $x_1 \wedge \dots \wedge x_p$ разлагается в сумму внешних произведений, содержащих каждое два одинаковых множителя и, следовательно, равных нулю.

Если, напротив, x_i образуют свободную систему, то в E существует $n-p$ других векторов, образующих вместе с векторами x_i *базис* пространства E; p-вектор $x_1 \wedge \ldots \wedge x_p$ будет тогда (с точностью до знака) элементом соответствующего базиса для $\bigwedge^p E$ (§ 5, n° 6) и, значит, не равен нулю.

Теорема и ее доказательство непосредственно распространяются на бесконечномерные векторные пространства. По поводу обобщения на модули над кольцом см. упражнение 2.

Предложение 1. *Ранг* $\varrho(X)$ *матрицы* X *над полем* K *равен наибольшему из целых* p, *для которых в* X *существует по крайней мере один ненулевой минор* p*-го порядка.*

Действительно, $\varrho(X)$ есть наибольшее число линейно независимых столбцов матрицы X (гл. II, § 6, n° 7), иными словами (теорема 1), — столбцов, внешнее произведение которых отлично от нуля; но тем самым предложение доказано, поскольку компоненты внешних произведений произвольных p столбцов матрицы X — это, с точностью до знака, не что иное, как ее миноры p-го порядка (§ 6, n° 3).

Из этого предложения получается новое доказательство теоремы 2 § 6 для частного случая квадратных матриц над полем: как мы знаем (гл. II, § 6, предложение 4), для *обратимости* такой матрицы необходимо и достаточно, чтобы ее ранг равнялся ее порядку, а в силу предложения 1 для этого в свою очередь необходимо и достаточно, чтобы *определитель матрицы не равнялся нулю.*

2. *Применение определителей к решению линейных уравнений над полем*

Понятие определителя позволяет представить в сжатом виде условия существования решений системы (скалярных) линейных уравнений над *полем* K и выражение для решений такой системы, когда они существуют.

Рассмотрим систему m линейных уравнений с n неизвестными над K:

$$\sum_{j=1}^{n} \alpha_{ij}\xi_j = \beta_i \qquad (1 \leqslant i \leqslant m). \tag{1}$$

Матрица $A=(\alpha_{ij})$ этой системы имеет тем самым m строк и n столбцов. Пусть B — матрица из m строк и $n+1$ столбцов, полученная путем *окаймления* A $(n+1)$-м столбцом (β_i); как мы знаем (гл. II, § 6, предложение 5), для того чтобы система (1) обладала решением, необходимо и достаточно, чтобы A и B имели *одинаковый ранг*. Предположим, что A — матрица ранга p (который предложение 1 в принципе позволяет вычислить) и что первые p ее столбцов a_i $(1\leqslant i\leqslant p)$ образуют свободную систему (чего всегда можно добиться, подвергнув индексы j надлежащей подстановке); для того чтобы B была матрицей ранга p, необходимо и достаточно, чтобы столбец $y=(\beta_i)$ являлся линейной комбинацией столбцов a_i, иначе говоря (теорема 1), чтобы

$$a_1\wedge\ldots\wedge a_p\wedge y=0,$$

или еще чтобы *все миноры $(p+1)$-го порядка в B, столбцы которых имеют индексы* $1, 2, \ldots, p$ *и* $n+1$, *равнялись нулю.*

Допустим, что это условие выполнено и, кроме того, первые p строк матрицы A линейно независимы (чего всегда можно добиться, подвергнув индексы i надлежащей подстановке); тогда множество всех решений системы (1) совпадает с множеством всех решений системы, образованной первыми p уравнениями (1) (гл. II, § 4, теорема 2). Иными словами, можно предполагать, что $p=m$ и, следовательно, $n\geqslant m$; при произвольном задании элементов ξ_{m+h} $(1\leqslant h\leqslant n-m)$ элементы ξ_i с индексами $\leqslant m$ будут определяться системой m уравнений с m неизвестными

$$\sum_{j=1}^{m}\alpha_{ij}\xi_j=\beta_i-\sum_{h=1}^{n-m}\alpha_{i,\,m+h}\xi_{m+h}\qquad(1\leqslant i\leqslant m),\tag{2}$$

а по предположению определитель Δ этой системы, являющийся не чем иным, как минором матрицы A, образованным ее первыми m столбцами, отличен от нуля; тем самым система обладает единственным решением, причем оно задается формулами Крамера (§ 6, предложение 5).

Отметим еще, что теорема 1, примененная к случаю $p=n$, позволяет вновь получить, в пополненном виде, предложение 6 § 6 относительно системы n однородных линейных уравнений с n неизвестными:

ПРЕДЛОЖЕНИЕ 2. *Для того чтобы однородная линейная система n уравнений с n неизвестными над полем обладала ненулевым решением, необходимо и достаточно, чтобы определитель ее матрицы равнялся нулю.*

3. Векторные подпространства и разложимые p-векторы

ПРЕДЛОЖЕНИЕ 3. *Пусть z — ненулевой p-вектор над векторным пространством E; векторы $x \in E$, для которых $z \wedge x = 0$, образуют в E векторное подпространство V_z; при этом, если $(x_i)_{1 \leqslant i \leqslant q}$ — свободная система векторов из V_z, то $q \leqslant p$ и существует $(p-q)$-вектор v такой, что $z = v \wedge x_1 \wedge \ldots \wedge x_q$.*

Действительно, образуем базис пространства E, первыми q векторами которого служат $x_1, \ldots, x_q$ (гл. II, § 3, теорема 2); пусть $x_{q+1}, \ldots, x_n$ — остальные векторы этого базиса. В обозначениях из n° 6 § 5 можно написать $z = \sum_H \alpha_H x_H$, где H пробегает множество всех подмножеств интервала $[1, n]$, состоящих из p элементов; из выполнения соотношения $z \wedge x_i = 0$ для индекса i вытекает тогда, что $\alpha_H = 0$ для каждого H, не содержащего i; так как по предположению $z \wedge x_i = 0$ для всех i от 1 до q, то мы видим, что $\alpha_H = 0$ для всех H, *не содержащих интервала* $[1, q] \subset \mathbf{N}$. Поэтому $p \geqslant q$ и существует $(p-q)$-вектор v такой, что $z = v \wedge x_1 \wedge \ldots \wedge x_q$.

СЛЕДСТВИЕ 1. *Для каждого ненулевого p-вектора z над векторным пространством E имеет место неравенство $\dim V_z \leqslant p$; для разложимости z необходимо и достаточно, чтобы $\dim V_z = p$.*

Неравенство $\dim V_z \leqslant p$ сразу следует из предложения 3, поскольку каждая свободная система в V_z содержит не более p элементов; если $\dim V_z = p$, то для установления разложимости нужно взять в предложении 3 в качестве (x_i) базис подпространства V_z; обратное очевидно, ибо если $z = y_1 \wedge \ldots \wedge y_p \neq 0$, то векторы y_i $(1 \leqslant i \leqslant p)$ образуют свободную систему (теорема 1) и принадлежат V_z, а значит, V_z p-мерно.

Если p-вектор z и вектор x отнесены к какому-нибудь базису $e_i)_{1 \leqslant i \leqslant p}$ пространства E, то соотношение $z \wedge x = 0$ равносильно системе $\binom{n}{p+1}$ однородных линейных уравнений для компонент

вектора x; необходимые и достаточные условия, которым должны удовлетворять компоненты p-вектора z, чтобы он был разложимым, получим, написав, что $\binom{n}{p+1}$ линейных форм, стоящих в левых частях упомянутых уравнений, являются линейными комбинациями каких-нибудь $n-p$ из них (см. § 8, упражнение 6). Компоненты p-вектора z иногда называют его *грассмановскими координатами* относительно базиса (e_i).

Следствие 2. *Пусть* $(x_i)_{1\leqslant i\leqslant p}$ *и* $(y_i)_{1\leqslant i\leqslant p}$ *— две свободные системы p векторов векторного пространства E. Для того чтобы (ненулевые) p-векторы* $x_1\wedge\ldots\wedge x_p$ *и* $y_1\wedge\ldots\wedge y_p$ *отличались друг от друга лишь скалярным множителем, необходимо и достаточно, чтобы (p-мерные) подпространства, порожденные соответственно векторами* $x_1, \ldots, x_p$ *и* $y_1, \ldots, y_p$, *совпадали.*

Таким образом, каждому ненулевому разложимому p-вектору z соответствует p-мерное векторное подпространство V_z пространства E; каждая (свободная) система $(x_i)_{1\leqslant i\leqslant p}$ p векторов из E такая, что $z=x_1\wedge\ldots\wedge x_p$, является базисом этого подпространства V_z; мы будем называть V_z векторным подпространством, *определяемым разложимым p-вектором z*. Следствие 2 предложения 3 показывает, что каждое p-мерное векторное подпространство может быть определено разложимым p-вектором и что все разложимые p-векторы, определяющие одно и то же подпространство, отличаются друг от друга лишь ненулевым скалярным множителем.

Замечание. Пусть $(x_i)_{1\leqslant i\leqslant p}$ и $(y_i)_{1\leqslant i\leqslant p}$ — два базиса одного и того же p-мерного подпространства V пространства E; пусть $y_i=\sum_{j=1}^{p}\alpha_{ij}x_j$ $(1\leqslant i\leqslant p)$ и A — квадратная матрица (α_{ij}) p-го порядка (*матрица перехода* от базиса (x_i) к базису (y_i) (гл. II, § 6, n° 9)). Согласно определению определителей (и предложению 7 § 5), имеем $y_1\wedge\ldots\wedge y_p=(\det A)\,x_1\wedge\ldots\wedge x_p$. Для равенства разложимых p-векторов $x_1\wedge\ldots\wedge x_p$ и $y_1\wedge\ldots\wedge y_p$ необходимо и достаточно, чтобы матрица перехода от (x_i) к (y_i) была *унимодулярной*.

Пусть E отнесено к определенному базису $(e_i)_{1\leqslant i\leqslant n}$; отнеся каждому свободному семейству $(x_j)_{1\leqslant j\leqslant p}$ p векторов пространства E матрицу X из n строк и p столбцов, j-й столбец которой для каждого j $(1\leqslant j\leqslant p)$ образуют компоненты вектора x_j относительно базиса (e_i),

мы получим взаимно однозначное отображение свободных семейств из p векторов пространства E (имеющих $[1, p]$ своим множеством индексов) на множество $L_{p,n}(K)$ всевозможных матриц из n строк и p столбцов над полем K, имеющих *ранг* p. Если X и Y — матрицы из n строк и p столбцов, соответствующие описанным способом свободным системам $(x_i)_{1\leqslant i\leqslant p}$ и $(y_i)_{1\leqslant i\leqslant p}$, то для равенства p-векторов $x_1\wedge\ldots\wedge x_p$ и $y_1\wedge\ldots\wedge y_p$ необходимо и достаточно, чтобы существовала *унимодулярная* квадратная матрица A p-го порядка такая, что $Y=XA$. Тем самым определяется взаимно однозначное отображение множества всех разложимых p-векторов над E на *фактормножество* множества $L_{p,n}(K)$ по *отношению эквивалентности*: «существует унимодулярная квадратная матрица A p-го порядка такая, что $Y=XA$».

Предложение 3 позволяет *перевести* некоторые свойства подпространств пространства E в свойства разложимых p-векторов, определяющих эти подпространства. Так, например, имеем следующие предложения:

Предложение 4. *Пусть V и W — векторные подпространства пространства E, имеющие соответственно размерности p и q; предположим, что $p\leqslant q$, и пусть v — разложимый p-вектор, определяющий V, и w — разложимый q-вектор, определяющий W. Для того чтобы $V\subset W$, необходимо и достаточно, чтобы существовал $(q-p)$-вектор u такой, что $w=u\wedge v$.*

Это предложение есть непосредственное следствие предложения 3, примененного к разложимому q-вектору w и p векторам, образующим базис подпространства V.

Предложение 5. *Пусть V и W — векторные подпространства пространства E, имеющие соответственно размерности p и q, v — разложимый p-вектор, определяющий V, и w — разложимый q-вектор, определяющий W; для того чтобы $V\bigcap W=\{0\}$, необходимо и достаточно, чтобы $v\wedge w\neq 0$; разложимый $(p+q)$-вектор $v\wedge w$ определяет тогда подпространство $V+W$.*

Действительно, если $V\bigcap W$ имеет размерность $r>0$, то существует разложимый r-вектор z, определяющий $V\bigcap W$, такой, что v будет произведением z и некоторого $(p-r)$-вектора, w — произведением z и некоторого $(q-r)$-вектора; но тогда $v\wedge w=0$. Если, напротив, $V\bigcap W=\{0\}$, то сумма $V+W$ прямая; поэтому, если $(x_i)_{1\leqslant i\leqslant p}$ — базис подпространства V, а $(y_j)_{1\leqslant j\leqslant q}$ — базис подпространства W, то $p+q$ векторов x_i и y_j образуют базис

подпространства $V+W$, и их внешнее произведение есть ненулевой разложимый $(p+q)$-вектор, определяющий $V+W$; но (следствие 2 предложения 3) оно лишь ненулевым скалярным множителем отличается от $v \wedge w$.

Пусть E — $(n+1)$-мерное векторное пространство над полем K; в векторном пространстве $F = \bigwedge^{p+1} E$ $(0 \leqslant p \leqslant n)$ размерности $h = \binom{n+1}{p+1}$ множество $D_{p+1}(E)$ всех ненулевых разложимых $(p+1)$-векторов насыщено по отношению $\Lambda(F)$: «существует $\lambda \neq 0$ такое, что $v = \lambda u$» между u и v (гл. II, Приложение III, n° 1). Его канонический образ $G_{p+1}(E)$ в проективном пространстве $\mathbf{P}(F)$ размерности $h-1$ называется $(p+1)$-м *грассманианом* пространства E (или проективного пространства $\mathbf{P}(E)$). Согласно предыдущему, существует каноническая биекция $G_{p+1}(E)$ на множество всех $(p+1)$-мерных векторных подпространств пространства E (или на множество всех p-мерных проективных линейных многообразий пространства $\mathbf{P}(E)$). В случае, когда $E = K^{n+1}$, вместо $G_{p+1}(E)$ пишут $G_{n,p}(K)$.

Упражнения. 1) Пусть X — матрица над полем. Для того чтобы она была матрицей ранга p, достаточно, чтобы она содержала такой ненулевой минор p-го порядка, что все содержащие его миноры $(p+1)$-го порядка равны нулю. [Показать, что каждый столбец матрицы X будет линейной комбинацией тех p столбцов, которым принадлежат элементы указанного минора.]

*2) Пусть E — модуль над коммутативным кольцом C, имеющий конечный базис, состоящий из n элементов.

а) Для того чтобы p элементов x_i $(1 \leqslant i \leqslant p)$ модуля E образовывали зависимую систему, необходимо и достаточно, чтобы $\mu x_1 \wedge \ldots \wedge x_p = 0$ для некоторого скаляра $\mu \neq 0$. [Для установления достаточности условия рассмотреть матрицу A из n строк и p столбцов, образованную компонентами элементов x_i; свести к случаю, когда произведение некоторого минора $(p-1)$-го порядка матрицы A на μ не равно нулю; далее, записать, что произведение на μ каждого из миноров p-го порядка, содержащих этот минор $(p-1)$-го порядка, равно нулю, и воспользоваться формулой (12) § 6.]

В частности, если $p > n$, элементы x_i всегда образуют зависимую систему.

б) Показать, что если (x_i) — свободная система p элементов модуля E, то при $q \leqslant p$ q-векторы x_H, где H пробегает множество всех подмножеств интервала $[1, p]$, состоящих из q элементов, образуют свободную систему в $\bigwedge^q E$. [Использовать а).]

в) Вывести из а), что если столбцы квадратной матрицы n-го порядка над C линейно независимы, то также строки этой матрицы линейно независимы. [См. гл. II, § 6, упражнение 3.]

3) Пусть E и F — C-модули, обладающие конечными базисами, состоящими соответственно из m и n элементов. Для того чтобы линейное отображение u модуля E в F было *изоморфизмом* E *в* F, необходимо и достаточно, чтобы $m \leqslant n$ и для матрицы X этого отображения относительно произвольных базисов в E и F не существовало бы скаляра $\mu \neq 0$, произведения которого на все ее миноры m-го порядка равнялись нулю. [Использовать упражнение 2.] При выполнении этих условий, $\bigwedge^p u$ для каждого $p \leqslant m$ есть изоморфизм $\bigwedge^p E$ в $\bigwedge^p F$.

4) Пусть

$$\sum_{j=1}^{n} \alpha_{ij}\xi_j = \beta_i \qquad (1 \leqslant i \leqslant m)$$

— система m уравнений с n неизвестными на коммутативном кольце C. Пусть, далее, x_j $(1 \leqslant j \leqslant n)$ — столбцы матрицы $A=(\alpha_{ij})$ этой системы и $y=(\beta_i)$; предположим, что в A все миноры порядка $>p$ равны нулю, но $x_1 \wedge \ldots \wedge x_p \neq 0$. Для того чтобы система имела решение, необходимо, чтобы $x_1 \wedge \ldots \wedge x_p \wedge y = 0$.

Обратно, если это условие выполнено, то в C существуют $n+1$ элементов ξ_j $(1 \leqslant j \leqslant n+1)$ таких, что $\xi_{n+1} \neq 0$ и

$$\sum_{j=1}^{n} \alpha_{ij}\xi_j = \beta_i\xi_{n+1} \qquad (1 \leqslant i \leqslant m).$$

*5) Пусть E и F — модули над коммутативным кольцом A, обладающие конечными базисами, состоящими соответственно из m и n элементов, u — линейное отображение E в F и X — его матрица относительно произвольных базисов в E и F.

а) Если $m \geqslant n$ и существует обратимый минор n-го порядка матрицы X, то u есть отображение E *на* F.

б) Показать, что если, обратно, u есть отображение E на F, то $m \geqslant n$ и в X существует ненулевой минор n-го порядка. Если, кроме того, идеал кольца A, порождаемый необратимыми элементами этого кольца, отличен от A, то в X существует обратимый минор n-го порядка. [Рассмотреть внешнюю степень $\bigwedge^n u$.]

в) Пусть B — коммутативное кольцо с единицей и A — кольцо $B \times B$ (гл. I, § 8, n° 10). Привести пример такого линейного отображения A-модуля A^2 на модуль A, чтобы все элементы его матрицы (относительно канонических базисов модулей A^2 и A) были делителями нуля.

6) Пусть u и v — разложимые p-векторы над векторным пространством E. Для разложимости p-вектора $u+v$ необходимо и доста-

точно, чтобы пересечение подпространств, определяемых соответственно p-векторами u и v, имело размерность $\geqslant p-1$.

7) Пусть $z=\sum_H \alpha_H e_H$ — ненулевой разложимый p-вектор над векторным пространством E, выраженный через свои компоненты относительно произвольного базиса $(e_i)_{1\leqslant i\leqslant n}$ этого пространства; G — множество p элементов интервала $[1, n]$ такое, что $\alpha_G\neq 0$; $(i_h)_{1\leqslant h\leqslant p}$ — последовательность, полученная путем расположения индексов из G в возрастающем порядке, и $(j_k)_{1\leqslant k\leqslant n-p}$ — последовательность, полученная путем расположения в возрастающем порядке индексов дополнения G' к G относительно $[1, n]$. Пусть, далее, β_{hk} для любой пары (h, k) индексов таких, что $1\leqslant h\leqslant p$, $1\leqslant k\leqslant n-p$, есть компонента α_H p-вектора z, соответствующая множеству $H\subset[1, n]$, образованному $p-1$ индексами из G, отличными от i_h, и индексом j_k, и X — матрица (β_{hk}) из p строк и $n-p$ столбцов. Пусть, наконец, L — произвольное множество p элементов интервала $[1, n]$ такое, что $L\cap \complement G$ содержит $q>1$ элементов. Показать, что $(\alpha_G)^{q-1}\alpha_L$ равно минору q-го порядка матрицы X, образованному строками с индексами h, для которых $i_h\in G\cap \complement L$, и столбцами с индексами k, для которых $j_k\in L\cap \complement G$. [Записать, что z имеет вид $a_G y_1\wedge\cdots\wedge y_p$, где векторы y_i таковы, что в матрице Y из n строк и p столбцов, столбцы которой образованы компонентами этих векторов, подматрица, составленная из строк, индексы которых принадлежат G, является единичной матрицей p-го порядка.]

8) Показать, что коммутант линейной группы $\mathrm{GL}_n(K)$ обратимых квадратных матриц n-го порядка над полем K совпадает с группой матриц, определитель которых равен 1, за исключением того случая, когда $n=2$, а K есть поле $\mathbf{Z}/(2)$ из двух элементов. [См. гл. II, § 6, упражнение 9.]

§ 8. Двойственность для внешней алгебры

Всюду, где не оговорено противное, модули, рассматриваемые в настоящем параграфе, — это унитарные модули (над коммутативным кольцом), *имеющие конечный базис.*

1. Знакопеременные линейные формы и антисимметрированные ковариантные тензоры

Пусть E — унитарный A-модуль с конечным базисом. Как мы видели (§ 1, п°п° 5 и 7), модуль, сопряженный к модулю $\bigotimes^p E$ контравариантных тензоров p-го порядка над E, канонически

отождествим с модулем $\bigotimes^p E^*$ ковариантных тензоров p-го порядка над E, так что по отождествлении *каноническая билинейная форма* $\langle z, z'\rangle$ (гл. II, § 4, n° 1) на $(\bigotimes^p E) \times (\bigotimes^p E^*)$ определяется соотношением

$$\langle x_1 \otimes \ldots \otimes x_p,\ x'_1 \otimes \ldots \otimes x'_p\rangle = \langle x_1,\ x'_1\rangle \ldots \langle x_p,\ x'_p\rangle, \qquad (1)$$

каковы бы ни были $x_i \in E$ и $x'_i \in E^*$. Каждый ковариантный тензор $z' \in \bigotimes^p E^*$ отождествляется так с линейной формой $z \to \langle z, z'\rangle$ на $\bigotimes^p E$.

Исследуем, с какой линейной формой на $\bigotimes^p E$ отождествляется тензор $\sigma z'$ (§ 5, n° 1), где σ — произвольная подстановка из $\mathfrak{S}_p$. Заметим для этого, что имеет место тождество

$$\langle \sigma z,\ \sigma z'\rangle = \langle z,\ z'\rangle; \qquad (2)$$

по линейности достаточно доказать его для разложимых тензоров $z = x_1 \otimes \ldots \otimes x_p$ и $z' = x'_1 \otimes \ldots \otimes x'_p$; но в этом случае левая часть формулы (2), по определению, равна $\prod_{i=1}^{p} \langle x_{\sigma^{-1}(i)}, x'_{\sigma^{-1}(i)}\rangle$; в силу же коммутативности A, это выражение равно правой части формулы (1) и тем самым равно $\langle z, z'\rangle$.

Заменив теперь в (2) z на $\sigma^{-1}z$, получим

$$\langle z,\ \sigma z'\rangle = \langle \sigma^{-1}z,\ z'\rangle. \qquad (3)$$

Иными словами, в силу формулы (4) § 5, линейная форма, с которой отождествляется тензор $\sigma z'$, получается путем применения к линейной форме, отождествляемой с z', оператора σ в соответствии с определением внешнего закона $(\sigma, g) \to \sigma g$ на $\mathscr{L}(\bigotimes^p E, F)$ (§ 5, n° 1).

Из тождества (3), умножая обе его части на $\varepsilon_\sigma = \varepsilon_{\sigma^{-1}}$ и суммируя по σ, получаем

$$\langle z,\ az'\rangle = \langle az,\ z'\rangle. \qquad (4)$$

Иными словами, линейная форма на $\bigotimes^p E$, отождествляемая с результатом антисимметрирования ковариантного тензора z', есть не что иное, как результат антисимметрирования линейной формы, отождествляемой с z'.

2. *Модуль, сопряженный к внешней степени*

Найдем теперь модуль, *сопряженный* к p-й внешней степени $\bigwedge^p E$. Как мы знаем (§ 5, п° 5), существует (каноническое) взаимно однозначное соответствие между *линейными формами* на $\bigwedge^p E$ и *знакопеременными линейными формами* на $\bigotimes^p E$. Так как E обладает базисом, то *знакопеременные* линейные формы на $\bigotimes^p E$ совпадают с *антисимметрированными* (§ 5, теорема 1). Но поскольку E обладает конечным базисом, антисимметрированные линейные формы на $\bigotimes^p E$ отождествимы (канонически) с *антисимметрированными ковариантными тензорами p-го порядка* над E (п° 1). Наконец, так как E^* обладает базисом, то существует канонический изоморфизм модуля антисимметрированных ковариантных тензоров p-го порядка над E на *p-ю внешнюю степень* $\bigwedge^p E^*$ (§ 5, предложение 6).

Таким образом, в силу этих замечаний, можно установить *канонический изоморфизм* модуля, сопряженного к $\bigwedge^p E$, *на* модуль $\bigwedge^p E^*$. Для точного определения этого изоморфизма достаточно указать линейную форму f на $\bigwedge^p E$, которой соответствует *разложимый p-вектор* $x'_1 \wedge \ldots \wedge x'_p$ на E^* (§ 5, п° 5, схолия); с другой стороны, значения f будут известны для каждого p-вектора над E, если они известны для каждого *разложимого* p-вектора $x_1 \wedge \ldots \wedge x_p$ (§ 5, п° 5, схолия). Но, согласно предыдущему, f канонически соответствует ковариантному тензору

$$a(x'_1 \otimes \ldots \otimes x'_p) = \sum_\sigma \varepsilon_\sigma x'_{\sigma(1)} \otimes \ldots \otimes x'_{\sigma(p)}.$$

Этот последний отождествим с линейной формой на $\bigotimes^p E$, значением которой для тензора $x_1 \otimes \ldots \otimes x_p$, принимая во внимание (4), служит

$$\sum_\sigma \varepsilon_\sigma \langle x_{\sigma(1)}, x'_1 \rangle \ldots \langle x_{\sigma(p)}, x'_p \rangle. \tag{5}$$

Так как $x_1 \wedge \ldots \wedge x_p$ есть канонический образ $x_1 \otimes \ldots \otimes x_p$ в $\bigwedge^p E$ (§ 5, n° 5), то выражение (5) и есть искомое значение $f(x_1 \wedge \ldots \wedge x_p)$; согласно формуле (5) § 6, это выражение есть не что иное, как *определитель* матрицы $(\langle x_i, x'_j \rangle)$. Иными словами, справедлива следующая теорема:

Теорема 1. *Пусть E — модуль над коммутативным кольцом A, имеющий конечный базис. Линейное отображение модуля $\bigwedge^p E^*$ в модуль, сопряженный к $\bigwedge^p E$, относящее каждому разложимому p-вектору $x'_1 \wedge \ldots \wedge x'_p$ над E^* линейную форму f на $\bigwedge^p E$ такую, что*

$$f(x_1 \wedge \ldots \wedge x_p) = \det(\langle x_i, x'_j \rangle)$$

для каждого разложимого p-вектора над E, есть изоморфизм модуля $\bigwedge^p E^*$ на модуль, сопряженный к $\bigwedge^p E$ (называемый, как и изоморфизм, обратный ему, *каноническим*).

Всюду в дальнейшем модуль, сопряженный к $\bigwedge^p E$, будет *отождествляться* с $\bigwedge^p E^*$ посредством установленного нами канонического изоморфизма; каноническая билинейная форма (гл. II, § 4, n° 1) на $\left(\bigwedge^p E\right) \times \left(\bigwedge^p E^*\right)$ будет определяться тогда фундаментальной формулой

$$\langle x_1 \wedge \ldots \wedge x_p, x'_1 \wedge \ldots \wedge x'_p \rangle = \det(\langle x_i, x'_j \rangle). \qquad (6)$$

Элементы модуля $\bigwedge^p E^*$ (p-векторы над E^*), отождествленные так с линейными формами на $\bigwedge^p E$ (и канонически соответствующие знакопеременным полилинейным формам на E^p), будут называться также *p-формами на E*.

Пусть $(e_i)_{1 \leqslant i \leqslant n}$ — базис модуля E и $(e'_i)_{1 \leqslant i \leqslant n}$ — сопряженный базис в E^*; формула (6) показывает, что

$$\langle e_{i_1} \wedge \ldots \wedge e_{i_p}, e'_{j_1} \wedge \ldots \wedge e'_{j_p} \rangle = \det(\langle e_{i_h}, e'_{j_k} \rangle).$$

Но если существует индекс j_k, отличный от всех i_h, то определитель, стоящий в правой части, имеет нулевой столбец; другими

словами, в обозначениях из n° 6 § 5 имеем

$$\left.\begin{aligned}&\langle e_H, e'_K\rangle = 0, \text{ если } H \neq K,\\ &\langle e_H, e'_H\rangle = 1\end{aligned}\right\} \tag{7}$$

для каждого множества $H \subset [1, n]$, состоящего из p элементов. Мы видим, таким образом, что базис (e_H) модуля $\bigwedge^p E$ имеет своим *сопряженным базисом* (e'_H). Для любого p-вектора $x = \sum_H a_H e_H$ и любой p-формы $x' = \sum_H a'_H \epsilon'_H$ на E имеем

$$\langle x, x'\rangle = \sum_H a_H a'_H, \tag{8}$$

где H пробегает множество всех подмножеств интервала $[1, n]$, состоящих из p элементов.

Следствие. *Пусть X и X' — две матрицы из n строк и p столбцов над кольцом A. Для каждого множества $H \subset [1, n]$, состоящего из p элементов, обозначим через $\mathbf{X}_H$* (соответственно $\mathbf{X}'_H$) *минор матрицы X* (соответственно X'), *множеством индексов строк которого служит H* (а множеством индексов столбцов — интервал $[1, p]$). *Тогда*

$$\det({}^t X)X') = \sum_H \mathbf{X}_H \mathbf{X}'_H, \tag{9}$$

где H пробегает множество всех подмножеств интервала $[1, n]$, состоящих из p элементов.

Действительно, эта формула вытекает из формулы (6), примененной к столбцам x_i $(1 \leqslant i \leqslant p)$ матрицы X и столбцам x'_j $(1 \leqslant j \leqslant p)$ матрицы X', и формулы (8), примененной к $x = x_1 \wedge \ldots \wedge x_p$ и $x' = x'_1 \wedge \ldots \wedge x'_p$ (см. § 6, упражнение 6).

В частности, при $X' = X$, получаем соотношение

$$\det({}^t X)X) = \sum_H (\mathbf{X}_H)^2, \tag{10}$$

называемое *тождеством Лагранжа*.

Предложение 1. *Пусть E и F — A-модули с конечным базисом и u — линейное отображение E в F. Отображение, сопряженное к p-й внешней степени $\bigwedge$ и отображения u, совпадает с p-й внешней степенью $\bigwedge^p({}^t u)$ отображения, сопряженного к u.*

Действительно, пусть v — отображение, сопряженное к $\bigwedge^p u$. Для каждого разложимого p-вектора $x_1 \wedge \ldots \wedge x_p$ над E и каждой разложимой p-формы $y'_1 \wedge \ldots \wedge y'_p$ на F, по определению, имеем

$$\langle x_1 \wedge \ldots \wedge x_p,\ v(y'_1 \wedge \ldots \wedge y'_p)\rangle = \\ = \langle u(x_1) \wedge \ldots \wedge u(x_p),\ y'_1 \wedge \ldots \wedge y'_p\rangle,$$

откуда, согласно (6),

$$\langle x_{i_1} \wedge \ldots \wedge x_{i_p},\ v(y'_1 \wedge \ldots \wedge y'_p)\rangle = \\ = \det(\langle u(x_i),\ y'_j\rangle) = \det(\langle x_i,\ {}^t u(y'_j)\rangle) = \\ = \langle x_1 \wedge \ldots \wedge x_p,\ {}^t u(y'_1) \wedge \ldots \wedge {}^t u(y'_p)\rangle,$$

а это и показывает, что

$${}^t\left(\bigwedge^p u\right) = \bigwedge^p ({}^t u). \tag{1}$$

Следствие. *Если u — автоморфизм модуля E, то автоморфизм модуля $\bigwedge^p E^*$, контрагредиентный к автоморфизму $\bigwedge^p u$, совпадает с p-й внешней степенью $\bigwedge^p \check{u}$ автоморфизма $\check{u}$, контрагредиентного к u.*

Это сразу следует из установленной только что формулы (11) и формулы (8) § 5.

Таким образом, для всех $x \in \bigwedge^p E$ и $x' \in \bigwedge^p E^*$ имеем

$$\left\langle \bigwedge^p u(x),\ \bigwedge^p \check{u}(x')\right\rangle = \langle x,\ x'\rangle. \tag{12}$$

3. *Модуль, сопряженный к $\bigwedge E$*

В дальнейшем в множествах $\bigwedge E$ и $\bigwedge E^*$, определенных в n° 9 § 5, будут одновременно рассматриваться, с одной стороны, их структура *A-модуля*, а с другой, их структура *кольца* — две структуры, которые надо будет тщательно различать.

A-модуль $\bigwedge E$ есть, по определению, прямая сумма $n+1$ модулей $\bigwedge^p E$ $(0 \leqslant p \leqslant n)$, где n — число элементов базиса модуля E; следовательно (гл. II, § 4, предложение 5), модуль, *сопряженный* к $\bigwedge E$, есть A-модуль, изоморфный прямой сумме модулей,

сопряженных к модулям $\bigwedge^p E$, т. е. (теорема 1) — прямой сумме $n+1$ модулей $\bigwedge^p E^*$ $(0 \leqslant p \leqslant n)$, или *A-модулю* $\bigwedge E^*$. Говоря точно (гл. II, § 4, n° 3), мы будем канонически *отождествлять* $\bigwedge E^*$ с модулем, сопряженным к $\bigwedge E$, так, что каноническая билинейная форма $\langle x, x' \rangle$ на $(\bigwedge E) \times (\bigwedge E^*)$ будет определяться формулой

$$\left\langle \sum_{p=0}^{n} x_p, \sum_{p=0}^{n} x'_p \right\rangle = \sum_{p=0}^{n} \langle x_p, x'_p \rangle \quad (x_p \in \bigwedge^p E,\ x'_p \in \bigwedge^p E^*). \tag{13}$$

Если $(e_i)_{1 \leqslant i \leqslant n}$ — базис модуля E и $(e'_i)_{1 \leqslant i \leqslant n}$ — сопряженный базис в E^*, то из формул (7) и (13) следует, что (e_H) и (e'_H) являются *сопряженными базисами* соответственно для $\bigwedge E$ и $\bigwedge E^*$, где H пробегает теперь множество *всех* подмножеств интервала $[1, n]$. Можно также сказать, что первая из формул (7) справедлива и без предположения, что H и K имеют одинаковое число элементов.

Для каждого линейного отображения u модуля E в модуль F мы определили (§ 5, n° 9) его *каноническое продолжение* $\overline{u}$ на $\bigwedge E$ (как отображение, совпадающее на каждом $\bigwedge^p E$ с $\bigwedge^p u$). Формула (11) показывает, что отображение, *сопряженное* к $\overline{u}$, есть не что иное, как *каноническое продолжение* отображения ${}^t u$ на $\bigwedge E^*$.

4. *Внутренние произведения p-вектора и q-формы*

Для каждого элемента $x \in \bigwedge E$ отображение $z \longrightarrow z \wedge x$ есть *эндоморфизм* структуры A-модуля в $\bigwedge E$ (правая гомотетия *кольца* $\bigwedge E$). Поэтому *сопряженное* отображение есть эндоморфизм модуля $\bigwedge E^*$.

Определение 1. *Левым внутренним произведением* $x \lrcorner x'$ *элемента* $x \in \bigwedge E$ *и элемента* $x' \in \bigwedge E^*$ *называется значение, принимаемое в* x' *отображением, сопряженным к эндоморфизму* $z \longrightarrow z \wedge x$ *модуля* $\bigwedge E$.

Согласно определению сопряженного линейного отображения (гл. II, § 4, формула (12)), для всех $x \in \bigwedge E$, $x' \in \bigwedge E^*$ и $z \in \bigwedge E$ имеем

$$\langle z, x \lrcorner x' \rangle = \langle z \wedge x, x' \rangle. \tag{14}$$

Предложение 2. *Сложение и внешний закон композиции* $(x, x') \longrightarrow x \lrcorner x'$ *на* $\bigwedge E^*$ *определяют в этом множестве структуру левого модуля относительно кольца* $\bigwedge E$.

Действительно, из (14) следует, что отображение $(x, x') \longrightarrow x \lrcorner x'$ *билинейно* (относительно структур A-модуля в $\bigwedge E$ и $\bigwedge E^*$); тем самым все сводится к доказательству тождества

$$(x \wedge y) \lrcorner x' = x \lrcorner (y \lrcorner x') \tag{15}$$

относительно $x \in \bigwedge E$, $y \in \bigwedge E$, $x' \in \bigwedge E^*$. Но в правой его части стоит значение, принимаемое в x' *композицией* эндоморфизма, сопряженного к $z \longrightarrow z \wedge x$, и эндоморфизма, сопряженного в $z \longrightarrow z \wedge y$; эта композиция есть не что иное (гл. II, § 4, формула (15)), как отображение, сопряженное к композиции $z \longrightarrow (z \wedge x) \wedge y$ этих эндоморфизмов, т. е., вследствие ассоциативности умножения в кольце $\bigwedge E$, — к эндоморфизму $z \longrightarrow z \wedge (x \wedge y)$; а отсюда и вытекает формула (15).

Пусть $(e_i)_{1 \leqslant i \leqslant n}$ — базис модуля E; как билинейная функция от (x, x'), произведение $x \lrcorner x'$ для любых $x \in \bigwedge E$ и $x' \in \bigwedge E^*$ определяется значениями произведений $e_H \lrcorner e'_L$, где H и L — произвольные подмножества интервала $[1, n]$. Но согласно формулам (14) § 5, матрица $(\mu_{L,K})$ эндоморфизма $z \longrightarrow z \wedge e_H$ модуля $\bigwedge E$ относительно базиса (e_K) задается соотношениями $\mu_{L,K} = 0$, если $K \cap H \neq \varnothing$ или $K \cap H = \varnothing$ и $L \neq K \cup H$, и $\mu_{L,K} = \varrho_{K,H}$, если $K \cap H = \varnothing$ и $L = K \cup H$ (напомним, что $\varrho_{K,H} = (-1)^{\nu}$, где ν — число тех пар (i, j), в которых $i \in K$, $j \in H$ и $j < i$). Так как матрица эндоморфизма $x' \longrightarrow e_H \lrcorner x'$ есть матрица, транспонированная к $(\mu_{L,K})$, то мы видим, что

$$\left.\begin{aligned} e_H \lrcorner e'_L &= 0, && \text{если } H \not\subset L, \\ e_H \lrcorner e'_L &= \varrho_{K,H} e'_K, && \text{если } H \subset L, \end{aligned}\right\} \tag{16}$$

где K означает *дополнение к* H *относительно* L.

Эти формулы показывают, в частности, что если x есть *p-вектор* (элемент из $\bigwedge^p E$), а x' — *q-форма* (элемент из $\bigwedge^q E^*$), то внутреннее произведение $x \lrcorner x'$ равно *нулю* при $p > q$ и является *$(q-p)$-формой при* $p \leqslant q$. При $p = q$, как показывает сравнение формул (16) и (7), $x \lrcorner x' = \langle x, x' \rangle$.

Предложение 3. *Пусть u — автоморфизм модуля E и $\overline{u}$ — его каноническое продолжение на $\bigwedge E$. Каковы бы ни были $x \in \bigwedge E$ и $x' \in \bigwedge E^*$,*

$$\overset{\vee}{u}(x \lrcorner x') = \overline{u}(x) \lrcorner \overset{\vee}{u}(x'). \tag{17}$$

Покажем прежде всего, что для канонического продолжения $\overline{u}$ любого линейного отображения u модуля E в модуль F имеет место равенство

$$x \lrcorner {}^t\overline{u}(x') = {}^t\overline{u}(\overline{u}(x) \lrcorner x'). \tag{18}$$

Действительно, отображение $x' \to x \lrcorner {}^t\overline{u}(x')$ есть композиция отображений ${}^t\overline{u}$ и $y' \to x \lrcorner y'$, сопряженных соответственно к отображениям $\overline{u}$ и $z \to z \wedge x$, и, значит, является сопряженным к отображению $z \to \overline{u}(z \wedge x)$ (гл. II, § 4, формула (15)); но так как $\overline{u}$ есть *представление* кольца $\bigwedge E$ в кольцо $\bigwedge F$ (§ 5, n° 9), то $\overline{u}(z \wedge x) = \overline{u}(z) \wedge \overline{u}(x)$; вновь применяя формулу, дающую сопряженное к композиции двух линейных отображений, получаем (18). В случае, когда u есть автоморфизм модуля E, заменяя в (18) x' на $\overline{u}(x')$, получим требуемую формулу (17).

Рассмотрим теперь для произвольного элемента $x' \in \bigwedge E^*$ эндоморфизм $z' \to x' \wedge z'$ модуля $\bigwedge E^*$ (левую гомотетию кольца $\bigwedge E^*$). Сопряженное к нему отображение есть эндоморфизм модуля $\bigwedge E$.

Определение 2. *Правым внутренним произведением $x \llcorner x'$ элемента $x \in \bigwedge E$ и элемента $x' \in \bigwedge E^*$ называется значение, принимаемое в x отображением, сопряженным к эндоморфизму $z' \to x' \wedge z'$ модуля $\bigwedge E^*$.*

Таким образом, имеем тождественно

$$\langle x \llcorner x', z' \rangle = \langle x, x' \wedge z' \rangle. \tag{19}$$

Так же, как при доказательстве предложения 2, устанавливается, что сложение и внешний закон $(x', x) \to x \llcorner x'$ на $\bigwedge E$ определяют в этом множестве структуру *правого модуля* относительно *кольца* $\bigwedge E^*$; иными словами, имеет место тождество

$$x \llcorner (x' \wedge y') = (x \llcorner x') \llcorner y'. \tag{20}$$

Для любого базиса $(e_i)_{1\leqslant i\leqslant n}$ модуля E имеем

$$\left.\begin{aligned} e_L \llcorner e'_H &= 0, && \text{если } H \not\subset L,\\ e_L \llcorner e'_H &= \varepsilon_{H,K} e_K, && \text{если } H \subset L, \end{aligned}\right\} \tag{21}$$

где K означает *дополнение к H относительно L*. Отсюда, в частности, следует, что если x — *p-вектор* и x' — *q-форма*, то $x \llcorner x' = 0$ при $p < q$ и есть *$(p-q)$-вектор* при $p \geqslant q$; при $p = q$ снова имеем $x \llcorner x' = \langle x, x' \rangle$.

Наконец, если u — линейное отображение E в F и $\overline{u}$ — его каноническое продолжение на $\bigwedge E$, то тождественно

$$\overline{u}(x) \llcorner x' = \overline{u}(x \llcorner {}^t\overline{u}(x')), \tag{22}$$

и, в частности, если u — *автоморфизм* модуля E, то

$$\overline{u}(x) \llcorner \overset{\vee}{u}(x') = \overline{u}(x \llcorner x'). \tag{23}$$

5. *Канонические изоморфизмы p-векторов и $(n-p)$-форм*

Пусть E — модуль, обладающий базисом, состоящим из n элементов; как мы знаем (§ 5, теорема 2), внешняя степень $\bigwedge^n E$ имеет базис, образованный *единственным элементом*.

Предложение 4. *Пусть e — элемент из $\bigwedge^n E$, образующий базис этого модуля, и e' — элемент из $\bigwedge^n E^*$, образующий базис, сопряженный к e. Тогда отображение $x \longrightarrow x \llcorner e'$ есть изоморфизм φ модуля $\bigwedge E$ на модуль $\bigwedge E^*$, отображающий $\bigwedge^p E$ на $\bigwedge^{n-p} E^*$ для каждого p $(0 \leqslant p \leqslant n)$; изоморфизмом, обратным к φ, является отображение $x' \longrightarrow e \llcorner x'$.*

В E имеется базис $(e_i)_{1\leqslant i\leqslant n}$ такой, что $e = e_1 \wedge \ldots \wedge e_n$, откуда $e' = e'_1 \wedge \ldots \wedge e'_n$, где (e'_i) — базис, сопряженный к (e_i); поэтому, согласно формулам (16), для каждого $H \subset [1, n]$ имеем

$$\varphi(e_H) = \varepsilon_{H',H} e'_{H'}, \tag{24}$$

где H' — дополнение к H в $[1, n]$. Эти формулы показывают, что φ есть изоморфизм $\bigwedge E$ на $\bigwedge E^*$ и отображает $\bigwedge^p E$ на $\bigwedge^{n-p} E^*$ (гл. II, § 2, n° 3). Точно так же, если ψ означает отображение $x' \longrightarrow e \llcorner x'$,

формулы (21) дают

$$\psi(e'_{H'}) = \varrho_{H',H} e_H, \tag{25}$$

откуда явствует, что ψ есть изоморфизм, обратный к φ (поскольку $\varrho_{H',H}$ равно 1 или -1); мы будем в дальнейшем обозначать его $\overset{-1}{\varphi}$. Сужение φ на подмодуль $\overset{p}{\bigwedge} E$, являющееся изоморфизмом $\overset{p}{\bigwedge} E$ на $\overset{n-p}{\bigwedge} E^*$, мы обозначим φ_p, а изоморфизм, обратный к φ_p, будет обозначаться $\overset{-1}{\varphi}_p$.

Изоморфизм φ зависит от выбранного в $\overset{n}{\bigwedge} E$ базиса e; по всякий другой базис этого модуля получается умножением e на обратимый элемент кольца A; следовательно, изоморфизмы φ, соответствующие различным базисам для $\overset{n}{\bigwedge} E$, совпадают *с точностью до обратимого множителя*. При заданном базисе e модуля $\overset{n}{\bigwedge} E$ мы будем называть изоморфизм φ (соответственно каждое из его сужений φ_p) и обратный изоморфизм $\overset{-1}{\varphi}$ (соответственно $\overset{-1}{\varphi}_p$) *каноническими изоморфизмами* $\bigwedge E$ на $\bigwedge E^*$ и $\bigwedge E^*$ на $\bigwedge E$ (соответственно $\overset{p}{\bigwedge} E$ на $\overset{n-p}{\bigwedge} E^*$ и $\overset{n-p}{\bigwedge} E^*$ на $\overset{p}{\bigwedge} E$), соответствующими базису e.

Можно показать (упражнение 8), что вообще не существует изоморфизма, который зависел бы лишь от структуры модуля в E (Теор. мн., гл. IV, Приложение) (см. упражнение 12). В главе IX будут рассмотрены некоторые изоморфизмы $\overset{p}{\bigwedge} E$ на $\overset{n-p}{\bigwedge} E$, связанные с теорией билинейных форм.

Формула (14) при $x' = e'$ дает

$$\langle z, \varphi(x) \rangle = \langle z \wedge x, e' \rangle.$$

Если x—*p-вектор* и z—*$(n-p)$-вектор*, то $z \wedge x = \lambda e$, где λ—скаляр, откуда $\langle z \wedge x, e' \rangle = \lambda$ и, следовательно,

$$\langle z, \varphi_p(x) \rangle e = z \wedge x. \tag{26}$$

Таким же образом для *p-формы* x' и $(n-p)$-*формы* z' получаем из (19) формулу

$$\langle \overset{-1}{\varphi}_{n-p}(x'), z' \rangle e' = x' \wedge z'. \tag{27}$$

Заменим теперь в тождестве (15) x' на e'; мы получим

$$\varphi(x \wedge y) = x \lrcorner \varphi(y)$$

или, заменяя $\varphi(y)$ на x',

$$x \lrcorner x' = \varphi(x \wedge \overset{-1}{\varphi}(x')). \tag{28}$$

Таким же образом из (20) получим

$$x \llcorner x' = \overset{-1}{\varphi}(\varphi(x) \wedge x'). \tag{29}$$

Формулы (28) и (29) сводят с помощью изоморфизма φ внутренние произведения к внешним.

Отображение, *сопряженное* к φ_p, являющееся изоморфизмом $\bigwedge^{n-p} E$ на $\bigwedge^{p} E^*$, для каждого p $(0 \leqslant p \leqslant n)$ равно $(-1)^{p(n-p)}\varphi_{n-p}$; в самом деле, для каждого p-вектора x и каждого $(n-p)$-вектора z имеем (гл. II, § 4, формула (12)) $\langle x, {}^t\varphi_p(z)\rangle = \langle z, \varphi_p(x)\rangle$; поэтому, в силу (26) и формулы (12) § 5,

$$\langle x, {}^t\varphi_p(z)\rangle e = z \wedge x = (-1)^{p(n-p)} x \wedge z = (-1)^{p(n-p)} \langle x, \varphi_{n-p}(z)\rangle,$$

откуда

$${}^t\varphi_p = (-1)^{p(n-p)}\varphi_{n-p}.$$

Заметим, что для каждого целого p число $-p^2$ имеет ту же четность, что и p; поэтому

$$(-1)^{p(n-p)} = (-1)^{p(n+1)} = (-1)^{(n-p)(n+1)}.$$

Каждое линейное отображение v модуля $\bigwedge^{p} E$ в модуль G может быть записано в виде $v = \sum_{p=0}^{n} v_p$, где v_p — сужение v на $\bigwedge^{p} E$ $(0 \leqslant p \leqslant n)$; положим $\eta v = \sum_{p=0}^{n} (-1)^p v_p$; η есть оператор на множестве $\mathscr{L}\left(\bigwedge E, G\right)$, имеющий своим квадратом нейтральный оператор. При этих соглашениях из предыдущего и формулы (13) вытекает, что отображение, *сопряженное* к каноническому изоморфизму φ, задается формулой

$${}^t\varphi = \eta^{n+1}\varphi.$$

Наконец, имеет место следующее предложение:

Предложение 5. *Пусть u — автоморфизм модуля E и $\overline{u}$ — его каноническое продолжение на $\bigwedge E$. Автоморфизм, контрагредиентный к $\overline{u}$, задается формулой*

$$\overset{\vee}{u} = (\det u)^{-1} \cdot \varphi \circ \overline{u} \circ \overset{-1}{\varphi}. \tag{30}$$

Предположим сначала лишь что u есть *эндоморфизм* модуля E, и применим формулу (18) с заменой x' n-вектором e'; по определению определителя, имеем ${}^t\overline{u}(e') = (\det {}^t u)\cdot e' = (\det u)\cdot e'$ (§ 6, предложение 4); это показывает, что

$$(\det u)\cdot \varphi(x) = {}^t\overline{u}(\varphi(\overline{u}(x))),$$

или

$$(\det u)\cdot \varphi = {}^t\overline{u} \circ \varphi \circ \overline{u}, \tag{31}$$

откуда и следует (30), когда u — автоморфизм.

Замечание. В случае, когда $\Delta = \det u$ *обратим*, из (31) вытекает, что $v = \Delta^{-1}\overset{-1}{\varphi_1} \circ {}^t u_{n-1} \circ \varphi_1$ есть эндоморфизм модуля E такой, что $v \circ u$ — тождественное отображение E на себя. С другой стороны, заменяя в (22) x на e, получаем для каждого эндоморфизма u модуля E формулу, аналогичную (31):

$$(\det u)\cdot \overset{-1}{\varphi} = \overline{u} \circ \overset{-1}{\varphi} \circ {}^t\overline{u},$$

откуда вытекает (в предположении обратимости Δ), что $u \circ v$ также есть тождественное отображение E на себя и, следовательно, u является автоморфизмом модуля E. Иными словами, этим способом получается новое доказательство теоремы 2 § 6, равно как и выражение для обратной матрицы через транспонированную к взаимной матрице (§ 6, n° 5).

6. *Истолкование внутренних произведений над векторными пространствами*

Правое внутреннее произведение $x \llcorner x'$ допускает простое истолкование в случае, когда E есть *векторное пространство* над полем C, а x — ненулевой *разложимый* p-*вектор*. Действительно, пусть V — p-мерное подпространство в E, определяемое p-вектором x (§ 7, n° 3); как мы видели (§ 5, n° 9), векторное пространство $\bigwedge V$ канонически отождествимо с подпространством про-

странства $\bigwedge E$, порожденным единичным элементом из C и r-векторами $y_1 \wedge \ldots \wedge y_r$, где r изменяется от 1 до n, а y_i пробегают V. Тогда *сужение* на $\bigwedge V$ произвольной линейной формы $z' \in \bigwedge E^*$, определенной на $\bigwedge E$, есть линейная форма на $\bigwedge V$, и каждая линейная форма на $\bigwedge V$ может быть получена таким способом (гл. II, § 4, предложение 5). Теперь, имеет место следующее предложение:

Предложение 6. *Пусть E — векторное пространство конечной размерности n, x — ненулевой разложимый p-вектор над E и V — определяемое им в E p-мерное подпространство. Для каждой определенной на $\bigwedge E$ линейной формы x' внутреннее произведение $x \llcorner x'$ есть элемент подпространства $\bigwedge V$ пространства $\bigwedge E$; при этом сужение на $\bigwedge V$ линейной формы x' соответствует элементу $x \llcorner x'$ при каноническом изоморфизме $\bigwedge V$ на $\bigwedge^p V^*$* (n° 5) *относительно базиса x пространства $\bigwedge^p V$.*

Действительно, выберем в E базис (e_i) такой, что $x = e_1 \wedge \ldots \wedge e_p$; достаточно доказать справедливость предложения для $x' = e'_H$ (где H — произвольное подмножество интервала $[1, n]$); но, так как $x = e_L$, где $L = [1, p]$, она непосредственно следует из формул (21) и формулы (24), примененных к векторному пространству V.

Следствие 1. *Для того чтобы сужение линейной формы x' на $\bigwedge V$ было тождественно нулевым, необходимо и достаточно, чтобы $x \llcorner x' = 0$.*

Согласно (29), эквивалентным условием является $\varphi(x) \wedge x' = 0$.

Следствие 2. *Пусть x—ненулевой разложимый p-вектор над E, V — определяемое им в E p-мерное подпространство, x' — ненулевая разложимая q-форма на E, W' — определяемое ею в E^* q-мерное подпространство и W — $(n-q)$-мерное подпространство в E, ортогональное к W'. Тогда $x \llcorner x'$ при $q < p$ есть разложимый $(p-q)$-вектор, равный нулю, если $\dim(V \cap W) > p - q$, и определяющий подпространство $V \cap W$ в противном случае.*

Действительно, пусть $U = V \cap W$, и предположим, что U r-мерно; в таком случае всегда можно предполагать, что $e_1, \ldots, e_r$

образуют его базис, а $e_{p+1}, \ldots, e_{p+n-q-r}$—базис дополнения к U относительно W; тогда x' есть скалярное кратное e'_H, где H — объединение интервалов $[r+1, p]$ и $[p+n-q-r+1, n]$, и справедливость утверждения следствия вытекает из формул (21).

Аналогичные предложения имеют место, если поменять ролями E и E^* и заменить правое внутреннее произведение левым. Сформулировать их мы вообще предоставим читателю; частный случай аналога следствия 2 предложения 6, относящийся к произведению $x \lrcorner e' = \varphi(x)$, где x — разложимый p-вектор, дает следующее предложение:

Предложение 7. *Пусть E — векторное пространство конечной размерности n; если x — ненулевой разложимый p-вектор над E, то $\varphi(x)$ — ненулевая разложимая $(n-p)$-форма; если V — подпространство в E, определяемое этим p-вектором x* (§ 7, n° 3), *то подпространством в E^*, определяемым $\varphi(x)$, является подпространство, ортогональное к V.*

Следствие. *Каждый $(n-1)$-вектор над n-мерным векторным пространством E разложим.*

Достаточно применить предложение 7, поменяв в нем ролями E и E^* и приняв $p=1$ (см. упражнение 7).

Пусть E — $(n+1)$-мерное векторное пространство над полем K, E^* — сопряженное пространство, F — пространство $\bigwedge^{p+1} E$ и F' — пространство $\bigwedge^{n-p} E^*$; каноническое отображение φ пространства F на F' (относительно базиса e' в $\bigwedge^{n+1} E^*$) дает при факторизации проективную биекцию $\bar{\varphi}$ пространства $\mathbf{P}(F)$ на $\mathbf{P}(F')$, которая, на основании сказанного в n° 5, не зависит от выбора базиса e' в $\bigwedge^{n+1} E^*$ и называется *канонической*. Ее сужение на грассманиан $G_{p+1}(E)$ (§ 7) является биекцией на $G_{n-p}(E^*)$, относящей каждому p-мерному проективному линейному многообразию $\pi^{-1}(V)$ из $\mathbf{P}(E)$ (гл. II, Приложение III, n° 3) $(n-p-1)$-мерное проективное линейное многообразие $\pi^{-1}(V^0)$ в $\mathbf{P}(E^*)$, где V^0 означает подпространство пространства E^*, ортогональное к V (предложение 7).

Упражнения. 1) Пусть E — модуль, обладающий конечным базисом, состоящим из n элементов, x — p-вектор над E и x' — $(p+q)$-форма на E; x канонически отождествим (§ 5, предложение 6) с результатом αx_1 антисимметрирования контравариантного тензора x_1 p-го порядка, а x' — с антисимметрированным ковариантным тензором $(p+q)$-го порядка. Показать, что если в смешанном тензоре $x_1 x'$ для каждого k такого, что $1 \leqslant k \leqslant p$, свернуть k-й контравариантный индекс с $(p+k)$-м ковариантным, то полученный так ковариантный тензор q-го порядка также будет антисимметрированным, и притом канонически отождествимым с q-формой $x \llcorner x'$.

2) Пусть $x = x_1 \wedge \ldots \wedge x_p$ — разложимый p-вектор над конечномерным векторным пространством E, являющийся внешним произведением p линейно независимых векторов x_i; пусть, далее, y' — q-форма $(q \leqslant p)$ и z' — произвольный элемент из $\bigwedge E^*$. Показать, что

$$x \llcorner (y' \wedge z') = \sum_H \varepsilon_{H,K} \langle x_H, y' \rangle (x_K \llcorner z'),$$

где H пробегает множество всех подмножеств интервала $[1, p]$, состоящих из q элементов, а K означает дополнение к H относительно $[1, p]$. [Взять в E базис, p элементами которого служат x_i.]

3) Пусть E — конечномерное векторное пространство и x — произвольный элемент пространства $\bigwedge E$. Множество V' тех линейных форм y' на E, для которых элемент $x \llcorner y'$ пространства $\bigwedge E$ равен нулю, образует в E^* подпространство. Показать, что подпространство V в E, ортогональное к V', есть наименьшее из подпространств W пространства E, для которых x принадлежит $\bigwedge W$.

4) Пусть E — модуль, обладающий конечным базисом, состоящим из n элементов. *Обратным произведением* $x \vee y$ элементов x и y из $\bigwedge E$ относительно базиса e модуля $\bigwedge^n E$ называется элемент $\varphi^{-1}(\varphi(x) \wedge \varphi(y))$, где φ — изоморфизм, соответствующий базису e. Это произведение определено лишь с точностью до обратимого множителя, зависящего от выбранного базиса e. Показать, что если x — p-вектор и y — q-вектор, то при $p+q \leqslant n$ будем иметь $x \vee y = 0$, в противном же случае $x \vee y$ есть $(p+q-n)$-вектор такой, что $y \vee x = (-1)^{(n-p)(n-q)} x \vee y$. Обратное произведение ассоциативно и дистрибутивно относительно сложения и определяет в $\bigwedge E$ алгебраическую структуру, изоморфную структуре внешней алгебры. Выразить компоненты $x \vee y$ через компоненты x и y.

5) Пусть E — n-мерное векторное пространство, x — разложимый p-вектор, y — разложимый q-вектор и V (соответственно W) — подпространство в E, определяемое p-вектором x (соответственно q-век-

тором y). Для того чтобы $V+W=E$, необходимо и достаточно, чтобы $x \vee y \neq 0$; тогда $(p+q-n)$-вектор $x \vee y$ разложим и определяет векторное подпространство $V \cap W$.

*6) Для того чтобы p-вектор z над n-мерным векторным пространством E был разложимым, необходимо и достаточно, чтобы $z \vee (z \wedge x) = 0$ для каждого разложимого $(n-p-1)$-вектора x. [Для установления достаточности условия применить его, взяв в качестве x внешние произведения $n-p-1$ векторов базиса, и вывести существование $n-p$ линейно независимых линейных форм u_i' $(1 \leqslant i \leqslant n-p)$ на E таких, что $\varphi(z) \wedge u_i' = 0$.]

7) а) Дать прямое доказательство (без использования изоморфизмов φ_p) разложимости каждого $(n-1)$-вектора над n-мерным векторным пространством.

б) Пусть A — коммутативная алгебра над полем K, обладающая базисом, образованным единичным элементом 1 и тремя элементами c_1, c_2, c_3, все попарные произведения которых равны нулю. Пусть, далее, E — A-модуль A^3 и $(e_i)_{1 \leqslant i \leqslant 3}$ — его канонический базис. Показать, что бивектор

$$x = c_1(e_2 \wedge e_3) + c_2(e_3 \wedge e_1) + c_3(e_1 \wedge e_2)$$

неразложим.

8) Пусть E — A-модуль, обладающий конечным базисом, состоящим из $n > 1$ элементов. Показать, что каждое линейное отображение ψ модуля $\bigwedge^p E$ в $\bigwedge^{n-p} E^*$ такое, что $\left(\bigwedge^{n-p} \check{u}\right) \circ \psi = \psi \circ \left(\bigwedge^p u\right)$ для каждого автоморфизма u модуля E с определителем, равным 1, является одним из изоморфизмов φ_p, определенных в n° 5. [Рассуждать, как в упражнении 12 § 5.] Вывести отсюда, что если в A существуют обратимые элементы $\neq 1$, то не существует изоморфизма $\bigwedge^p E$ на $\bigwedge^{n-p} E^*$, который бы зависел лишь от структуры A-модуля в E.

9) Пусть E — A-модуль, обладающий конечным базисом, состоящим из n элементов. Пусть, далее, u — изоморфизм E на сопряженный модуль E^*, Δ — определитель матрицы u относительно базиса (e_i) модуля E и сопряженного базиса (e_i') модуля E^* и $\bar{u}$ — каноническое продолжение u до изоморфизма $\bigwedge E$ на $\bigwedge E^*$. Доказать формулу

$${}^t\bar{u} = \eta^{n+1} \Delta \cdot \varphi \circ \overset{-1}{\bar{u}} \circ \varphi,$$

где φ — изоморфизм, соответствующий базису $e_1 \wedge \ldots \wedge e_n$ модуля $\bigwedge^n E$.

10) Пусть X — квадратная матрица n-го порядка над коммутативным кольцом и $\tilde{X} = \bigwedge^{n-1} X$. Показать, что если X обратима, то

$\det \widetilde{X} = (\det X)^{n-1}$, и что каждый минор $\widetilde{\mathbf{X}}_{H,K}$ p-го порядка матрицы $\widetilde{X}$ (§ 6, n° 3) задается формулой

$$\widetilde{\mathbf{X}}_{H,K} = (\det X)^p \mathbf{X}_{H',K'}, \tag{1}$$

где H' и K' — соответственно дополнения к H и K относительно $[1, n]$ («тождества Якоби»). [Воспользоваться соотношением (30).]

11) Из каждого тождества $\Phi = 0$, связывающего миноры общей обратимой квадратной матрицы X n-го порядка над коммутативным кольцом A, можно вывести новое тождество $\widetilde{\Phi} = 0$, называемое *дополнительным* к $\Phi = 0$, применяя тождество $\Phi = 0$ к минорам матрицы $\widetilde{X}$ (упражнение 10) и далее заменяя эти последние их выражением через миноры матрицы X посредством тождества (1) упражнения 10. Доказать этим способом следующее тождество:

$$\mathbf{X}^{ih}\mathbf{X}^{jk} - \mathbf{X}^{ik}\mathbf{X}^{jh} = (\det X) \cdot \mathbf{X}^{ij,hk},$$

где $\mathbf{X}^{ij,hk}$ означает минор $(n-2)$-го порядка матрицы X, получающийся путем вычеркивания в ней строк с индексами i и j и столбцов с индексами h и k.

*12) Пусть $\Phi = 0$ — тождество, связывающее миноры общей обратимой квадратной матрицы n-го порядка над коммутативным кольцом A, $\widetilde{\Phi} = 0$ — дополнительное тождество (упражнение 11), Y — обратимая квадратная матрица $(n+k)$-го порядка, где k — целое > 0, и $\widetilde{Y}_0$ — подматрица матрицы $\widetilde{Y}$ (см. упражнение 10), полученная путем вычеркивания в $\widetilde{Y}$ строк и столбцов с индексами $\leqslant k$. Если предположить, что $\widetilde{Y}_0$ обратима, и применить к ее минорам тождество $\widetilde{\Phi} = 0$, далее заменить каждый минор, фигурирующий в этом тождестве (рассматриваемый как *минор матрицы* $\widetilde{Y}$), его выражением через миноры матрицы Y посредством тождества (1) упражнения 10, то получится тождество $\Phi_k = 0$ для миноров матрицы Y (справедливое, когда Y и $\widetilde{Y}_0$ обратимы), называемое *распространением k-го порядка* тождества $\Phi = 0$.

В частности, пусть $A = (a_{ij})$ — обратимая квадратная матрица $(n+k)$-го порядка, B — ее подматрица k-го порядка, полученная путем вычеркивания в A строк и столбцов с индексами $> k$, Δ_{ij} — определитель матрицы $(k+1)$-го порядка, полученной путем вычеркивания в A строк с индексами $> k$, за исключением $(k+i)$-й, и столбцов с индексами $> k$, за исключением $(k+j)$-го, и C — матрица (Δ_{ij}) n-го порядка. Доказать, что если матрица B обратима, то

$$\det C = (\det A)(\det B)^{n-1}.$$

[Показать, что это тождество есть распространение k-го порядка полного разложения определителя n-го порядка.]

Указать тождества, получающиеся путем распространения лапласовского разложения (§ 6, n° 4), а также тождества упражнения 2 § 6.

*13) Пусть $X=(\xi_{ij})$ — обратимая квадратная матрица n-го порядка над полем K, H — подмножество интервала $[1, n]$, состоящее из p элементов, и H' — дополнение к H относительно $[1, n]$. Предположим, что для каждой пары индексов $h \in H$, $k \in H'$ имеет место равенство

$$\sum_i \xi_{ih}\xi_{ik} = 0.$$

Показать, что для любых двух подмножеств L, M интервала $[1, n]$, состоящих из p элементов, выполняется равенство

$$\varrho_{M, M'}\mathbf{X}_{L, H}\mathbf{X}_{M', H'} - \varrho_{L, L'}\mathbf{X}_{M, H}\mathbf{X}_{L', H'} = 0.$$

[Рассматривая столбцы x_h матрицы X с индексами $h \in H$ как векторы пространства $E=K^n$, а столбцы x'_k с индексами $k \in H'$ как векторы сопряженного пространства E^*, показать, что $(n-p)$-форма $x'_{H'}$ пропорциональна $\varphi_p(x_H)$.]

14) Пусть Γ и Δ — обратимые определители n-го порядка над коммутативным кольцом и Γ_{ij} — определитель, получающийся путем замены в Γ его i-го столбца j-м столбцом определителя Δ. Показать, что

$$\det(\Gamma_{ij}) = \Gamma^{n-1}\Delta.$$

[Разложить Γ_{ij} по i-му столбцу и использовать упражнение 10.]

ПРИЛОЖЕНИЕ I

К ГЛАВЕ III

БЕСКОНЕЧНЫЕ ТЕНЗОРНЫЕ ПРОИЗВЕДЕНИЯ

1. Тензорные произведения модулей

Определение 4 § 1 без труда распространяется на тот случай, когда рассматривается *любое* (не обязательно конечное) семейство унитарных A-модулей E_ι ($\iota \in I$). *Тензорное произведение* $\bigotimes_{\iota\in I} E_\iota$ определяется аналогично как фактормодуль модуля формальных линейных комбинаций (с коэффициентами из A) элементов произведения $\prod_{\iota\in I} E_\iota$ по подмодулю, порожденному элементами следующих типов:

1° $(x_\iota)+(y_\iota)-(z_\iota)$, где $x_\varkappa + y_\varkappa = z_\varkappa$ для *некоторого* (произвольного) индекса $\varkappa$ и $x_\iota = y_\iota = z_\iota$ для всех $\iota \neq \varkappa$;

2° $(x_\iota)-\alpha(y_\iota)$, где $x_\varkappa = \alpha y_\varkappa$ для некоторого (произвольного) индекса $\varkappa$ и $x_\iota = y_\iota$ для всех $\iota \neq \varkappa$.

Существует каноническое полилинейное отображение $(x_\iota) \to \bigotimes_{\iota\in I} x_\iota$ произведения $\prod_{\iota\in I} E_\iota$ в $\bigotimes_{\iota\in I} E_\iota$ такое, что $\bigotimes_{\iota\in I} E_\iota$ порождается образом $\prod_{\iota\in I} E_\iota$ при этом отображении. Кроме того, для каждого полилинейного отображения f произведения $\prod_{\iota\in I} E_\iota$ в произвольный A-модуль F существует, и притом единственное, линейное отображение g модуля $\bigotimes_{\iota\in I} E_\iota$ в F такое, что тождественно

$$f((x_\iota)) = g\left(\bigotimes_{\iota\in I} x_\iota\right).$$

Каково бы ни было разбиение $(I_\lambda)_{\lambda\in L}$ множества индексов I, тензорное произведение $\bigotimes_{\iota\in I} E_\iota$ канонически изоморфно тензорному

произведению $\bigotimes_{\lambda\in L} F_\lambda$, где $F_\lambda = \bigotimes_{\iota\in I_\lambda} E_\iota$ (*ассоциативность* тензорного произведения).

Предложения 6 и 7 § 1 не распространяются на тензорные произведения *бесконечных* семейств модулей.

2. *Тензорные произведения алгебр*

Пусть $(E_\iota)_{\iota\in I}$ — произвольное (конечное или бесконечное) семейство алгебр над одним и тем же коммутативным кольцом A (с единицей). Введение на модуле $\bigotimes_{\iota\in I} E_\iota$ ассоциативного умножения по формуле

$$\Big(\bigotimes_\iota x_\iota\Big)\cdot\Big(\bigotimes_\iota y_\iota\Big) = \bigotimes_\iota (x_\iota y_\iota)$$

определяет в $\bigotimes_{\iota\in I} E_\iota$ структуру *алгебры* относительно A.

Наиболее интересен тот случай, когда каждая из алгебр E_ι обладает *единичным элементом* e_ι. Тогда для каждого $\varkappa\in I$ существуют канонический гомоморфизм $\varphi_\varkappa$ кольца A в $E_\varkappa$ и канонический гомоморфизм $f_\varkappa$ алгебры $E_\varkappa$ в $\bigotimes_{\iota\in I} E_\iota$, наделенное структурой алгебры, определяемые формулами

$$\varphi_\varkappa(\alpha) = \alpha e_\varkappa \text{ для всех } \alpha\in A,$$

$$f_\varkappa(x) = \bigotimes_{\iota\in I} y_\iota, \quad \text{где} \quad y_\iota = e_\iota \quad \text{для} \quad \iota\neq\varkappa \quad \text{и} \quad y_\varkappa = x\in E.$$

Подалгебры $f_\iota(E_\iota)$ попарно *коммутируют* (§ 3, п° 3), и порожденная ими подалгебра алгебры $\bigotimes_{\iota\in I} E_\iota$ состоит из (конечных) сумм элементов вида $\bigotimes_\iota x_\iota$, где $x_\iota = e_\iota$ для всех кроме конечного числа индексов. Вследствие ее употребительности именно этой подалгебре (а не всему $\bigotimes_{\iota\in I} E_\iota$) присвоено наименование *тензорного произведения алгебр* E_ι. Она обозначается $\bigotimes_{(I)} E_\iota$ и вообще отлична от алгебры $\bigotimes_{\iota\in I} E_\iota$, когда I бесконечно.

Предложение 1 § 3 распространяется на тензорное произведение любого семейства *алгебр*, обладающих каждая единичным

элементом. Это уже не верно ни для предложения 7 § 1, ни для предложения 2 § 3.

Предположим, однако, что каждая алгебра E_ι обладает *базисом* B_ι, в который входит единичный элемент e_ι (что всегда имеет место, когда кольцо A есть поле). Тогда элементы $\bigotimes_{\iota\in I} x_\iota$, в которых $x_\iota \in B_\iota$ для каждого $\iota \in I$ и $x_\iota = e_\iota$ для всех кроме конечного числа индексов ι, образуют *базис* B тензорного произведения $\bigotimes_{(I)} E_\iota$. Действительно, то, что эти элементы порождают $\bigotimes_{(I)} E_\iota$, очевидно, и нужно только доказать, что они образуют *свободную* систему. Для этого достаточно, согласно n° 1, доказать, что для каждого элемента $a = \bigotimes_{\iota\in I} a_\iota \in B$ существует полилинейное отображение g произведения $\prod_{\iota\in I} E_\iota$ в A такое, что $g((a_\iota)) = 1$ и $g((b_\iota)) = 0$ для всех элементов $b = \bigotimes_{\iota\in I} b_\iota$ из B, отличных от a. Но пусть u_ι для каждого $\iota \in I$ — координатная форма на E_ι, относящая каждому $z_\iota \in E_\iota$ коэффициент при a_ι в выражении z_ι в виде линейной комбинации элементов $x_\iota \in B_\iota$. Для каждого элемента $z = (z_\iota) \in \prod_{\iota\in I} E_\iota$ положим

$$\begin{cases} g(z) = 0, \text{ если } z_\iota \neq e_\iota \text{ для бесконечного множества индексов } \iota \in I; \\ g(z) = \prod_{\iota\in I} u_\iota(z_\iota) \text{ в противном случае.} \end{cases}$$

Последняя формула имеет смысл, поскольку $a_\iota = e_\iota$ для всех кроме конечного числа индексов; и следовательно, если $z_\iota = e_\iota$ для всех кроме конечного числа индексов, то $u_\iota(z_\iota) = 1$ для всех кроме конечного числа индексов. Непосредственно проверяется, что определенное так отображение g полилинейно и отвечает поставленным условиям.

Отсюда сразу следует, что в рассматриваемом случае гомоморфизмы f_ι и φ_ι, определенные в начале этого n°, *инъективны*; они позволяют отождествить алгебры E_ι с коммутирующими подалгебрами тензорного произведения $\bigotimes_{(I)} E_\iota$, а A — с общим

подкольцом всех этих подалгебр. Кроме того, каково бы ни было непустое множество $J \subset I$, $\bigotimes_{(J)} E_\iota$ канонически отождествимо с некоторой подалгеброй тензорного произведения $\bigotimes_{(I)} E_\iota$; по условию, $\bigotimes_{(\varnothing)} E_\iota$ означает кольцо A.

Тензорное произведение $\bigotimes_{(I)} E_\iota$ можно определить также как «индуктивный предел» тензорных произведений $\bigotimes_{\iota \in J} E_\iota$, где J пробегает множество всех конечных подмножеств множества I.

ПРИЛОЖЕНИЕ II

К ГЛАВЕ III

ТЕНЗОРНЫЕ ПРОИЗВЕДЕНИЯ НАД НЕКОММУТАТИВНЫМ КОЛЬЦОМ

Все кольца операторов, встречающиеся в этом приложении, предполагаются имеющими единичный элемент (но не обязательно коммутативными), а все модули над этими кольцами — унитарными. Так же, как в § 2, *одно и то же множество сможет наделяться структурами модуля относительно различных колец операторов. В случае, когда оба множества* E *и* F *наделены структурой левого (или правого)* A*-модуля, коммутативная группа всех* A*-линейных отображений* E *в* F*, во избежание всякой путаницы, обозначается* $\mathscr{L}_A(E, F)$. *Аналогично* $\mathscr{L}_A(E)$ *означает кольцо всех* A*-эндоморфизмов модуля* E.

1. Тензорное произведение двух модулей

Пусть A — кольцо, E — *правый* A-модуль и F — *левый* A-модуль. Рассмотрим $\mathbf{Z}$-модуль $C = \mathbf{Z}^{(E\times F)}$ формальных линейных комбинаций элементов произведения $E \times F$ с коэффициентами из кольца $\mathbf{Z}$ рациональных целых чисел (гл. II, § 1, n° 8); таким образом, модуль C имеет базис, образованный всевозможными парами (x, y), где $x \in E$ и $y \in F$. Пусть D — подгруппа коммутативной группы C, порожденная элементами следующих типов:

$$\left.\begin{array}{l}(x_1 + x_2,\ y) - (x_1,\ y) - (x_2,\ y),\\ (x,\ y_1 + y_2) - (x,\ y_1) - (x,\ y_2),\\ (x\lambda,\ y) - (x,\ \lambda y),\end{array}\right\} \qquad (1)$$

где x, x_1, x_2 принадлежат E, y, y_1, y_2 принадлежат F и $\lambda \in A$.

Определение 1. *Тензорным произведением правого A-модуля E и левого A-модуля F называют коммутативную группу C/D* (факторгруппу группы формальных линейных комбинаций элементов произведения $E \times F$ с целыми коэффициентами по ее подгруппе, порожденной элементами типов (1)). *Это тензорное произведение обозначается $E \underset{A}{\otimes} F$ или $E \otimes_A F$ (или просто $E \otimes F$, если нет опасности смешения). Для любых $x \in E$ и $y \in F$ элемент тензорного произведения $E \otimes F$, являющийся каноническим образом элемента $(x, y) \in C$ в C/D, обозначается $x \otimes y$.*

Отображение $(x, y) \longrightarrow x \otimes y$ произведения $E \times F$ в $E \otimes F$ называется *каноническим* отображением $E \times F$ в $E \otimes F$.

Очевидно, $E \otimes_A F$ канонически изоморфно факторгруппе группы $E \otimes_{\mathbf{Z}} F$ по ее подгруппе, порожденной всевозможными элементами вида $(x\lambda) \otimes y - x \otimes (\lambda y)$, где $\lambda \in A$.

Как мы увидим (n° 3), в случае, когда A — коммутативное кольцо, это определение и определение 3 § 1 действительно приводят к одной и той же коммутативной группе $E \otimes F$. Однако в смысле теперешнего определения $E \otimes F$ не наделено структурой A-модуля; в n° 3 мы увидим, что это расхождение двух определений несущественно.

Предложение 1. а) *Пусть g — $\mathbf{Z}$-линейное отображение группы $E \otimes_A F$ в коммутативную группу G. Тогда отображение $(x, y) \longrightarrow f(x, y) = g(x \otimes y)$ произведения $E \times F$ в G удовлетворяет следующим условиям:*

$$\left.\begin{aligned} f(x_1 + x_2, y) &= f(x_1, y) + f(x_2, y), \\ f(x, y_1 + y_2) &= f(x, y_1) + f(x, y_2), \\ f(x\lambda, y) &= f(x, \lambda y). \end{aligned}\right\} \tag{2}$$

б) *Обратно, пусть f — отображение произведения $E \times F$ в коммутативную группу G, удовлетворяющее условиям* (2). *Тогда существует, и притом единственное, $\mathbf{Z}$-линейное отображение g группы $E \otimes_A F$ в G такое, что $f(x, y) = g(x \otimes y)$ для всех $x \in E$, $y \in F$.*

По определению тензорного произведения $E \otimes_A F$. имеем

$$\begin{aligned} 0 &= (x_1 + x_2) \otimes y - x_1 \otimes y - x_2 \otimes y = \\ &= x \otimes (y_1 + y_2) - x \otimes y_1 - x \otimes y_2 = (x\lambda) \otimes y - x \otimes (\lambda y), \end{aligned}$$

откуда следует а). Для доказательства б) заметим, что, в обозначениях определения 1, f продолжается до $\mathbf{Z}$-линейного отобра-

жения $\overline{f}$ группы C в G (гл. II, § 2, замечание после следствия 2 предложения 3). В силу соотношений (2), $\overline{f}$ аннулируется на всех элементах типа (1), а значит, и на D. Следовательно, существует $\mathbf{Z}$-линейное отображение g факторгруппы $C/D = E \otimes_A F$ в G такое, что $\overline{f} = g \circ \varphi$, где φ — каноническое отображение C на C/D (гл. II, § 2, предложение 1); единственность g очевидна, поскольку $E \otimes_A F$ порождается (как $\mathbf{Z}$-модуль) элементами вида $x \otimes y$.

Таким образом, предложение 1 определяет *канонический изоморфизм* коммутативной группы всех отображений f произведения $E \times F$ в G, удовлетворяющих условиям (2), на коммутативную группу $\mathscr{L}_{\mathbf{Z}}(E \otimes_A F, G)$ $\mathbf{Z}$-линейных отображений $E \otimes_A F$ в G.

Следствие. *Пусть H — коммутативная группа и h — отображение $E \times F$ в H, удовлетворяющее условиям* (2) *и такое, что H порождается множеством $h(E \times F)$. Предположим, что для каждой коммутативной группы G и каждого отображения f произведения $E \times F$ в G, удовлетворяющего условиям* (2), *существует $\mathbf{Z}$-линейное отображение g группы H в G такое, что $f = g \circ h$. Тогда существует, и притом единственный, изоморфизм ψ группы $E \otimes_A F$ на H такой, что $h = \psi \circ \theta$, где θ означает каноническое отображение $E \times F$ в $E \otimes_A F$.*

Согласно предложению 1, существует, и притом единственное, $\mathbf{Z}$-линейное отображение ψ группы $E \otimes_A F$ в H такое, что $h = \psi \circ \theta$. С другой стороны, если принять за G коммутативную группу $E \otimes_A F$, а за f — отображение θ, то из предположений, сделанных относительно h и H, будет следовать существование $\mathbf{Z}$-линейного отображения ψ_1 группы H в $E \otimes_A F$ такого, что $\theta = \psi_1 \circ h$. Для завершения доказательства остается показать, что $\psi \circ \psi_1$ и $\psi_1 \circ \psi$ — тождественные отображения соответственно H и $E \otimes_A F$ на себя. Но так как $\psi_1 \circ \psi \circ \theta = \psi_1 \circ h = \theta$, то $\psi_1 \circ \psi$ есть тождественное отображение $E \otimes_A F$ на себя, поскольку $\theta(E \times F)$ порождает группу $E \otimes_A F$. Точно так же, $\psi \circ \psi_1 \circ h = \psi \circ \theta = h$, и потому $\psi \circ \psi_1$ есть тождественное отображение H на себя, поскольку $h(E \times F)$, по предположению, порождает H.

Отметим, что, в силу предложения 1, пара $(E \otimes_A F, \theta)$ является решением следующей *проблемы универсального отображения* (Теор. мн., гл. IV, § 3): род структуры Σ есть род структуры коммутативной группы, морфизмами являются $\mathbf{Z}$-линейные отображения, а α-отобра-

жения — это отображения $E \times F$ в коммутативную группу, удовлетворяющие условиям (2). Таким образом, свойство единственности, установленное в следствии, есть не что иное, как общее свойство единственности решения проблемы универсального отображения (там же).

Предложение 2. *Пусть E и E_1 — правые A-модули, F и F_1 — левые A-модули, G — коммутативная группа и f — $\mathbf{Z}$-полилинейное отображение $E \times F \times E_1 \times F_1$ в G такое, что*

$$f(x\lambda, y, x_1, y_1) = f(x, \lambda y, x_1, y_1),$$
$$f(x, y, x_1\lambda, y_1) = f(x, y, x_1, \lambda y_1)$$

для любых $x \in E$, $x_1 \in E_1$, $y \in F$, $y_1 \in F_1$ и $\lambda \in A$. Тогда существует, и притом единственное, $\mathbf{Z}$-билинейное отображение g произведения $(E \otimes_A F) \times (E_1 \otimes_A F_1)$ в G такое, что $f(x, y, x_1, y_1) = g(x \otimes y, x_1 \otimes y_1)$ для любых $x \in E$, $y \in F$, $x_1 \in E_1$, $y_1 \in F_1$.

Единственность g явствует из того, что элементы вида $x \otimes y$ (соответственно $x_1 \otimes y_1$) порождают $E \otimes_A F$ (соответственно $E_1 \otimes_A F_1$). Докажем его существование. Для каждой пары $(x_1, y_1) \in E_1 \times F_1$ существует, и притом единственное, $\mathbf{Z}$-линейное отображение h_{x_1, y_1} группы $E \otimes_A F$ в G такое, что $h_{x_1, y_1}(x \otimes y) = f(x, y, x_1, y_1)$. Отображение $(x_1, y_1) \longrightarrow h_{x_1, y_1}$ произведения $E_1 \times F_1$ в $\mathscr{L}_{\mathbf{Z}}(E \otimes_A F, G)$ $\mathbf{Z}$-билинейно, и $h_{x_1\lambda, y_1} = h_{x_1, \lambda y_1}$ для всех $\lambda \in A$. Поэтому существует $\mathbf{Z}$-линейное отображение h группы $E_1 \otimes_A F_1$ в $\mathscr{L}_{\mathbf{Z}}(E \otimes_A F, G)$ такое, что $h(x_1 \otimes y_1) = h_{x_1, y_1}$. В силу предложения 1 § 1, тогда существует $\mathbf{Z}$-билинейное отображение g произведения $(E \otimes_A F) \times (E_1 \otimes_A F_1)$ в G такое, что

$$g(x \otimes y, x_1 \otimes y_1) = (h(x_1 \otimes y_1))(x \otimes y) = h_{x_1, y_1}(x \otimes y) = f(x, y, x_1, y_1).$$

и предложение доказано.

2. Тензорное произведение двух линейных отображений

Пусть A — кольцо, E и E' — правые A-модули, F и F' — левые A-модули, $u\colon E \longrightarrow E'$ и $v\colon F \longrightarrow F'$ — A-линейные отображения. Непосредственная проверка показывает, что отображение $(x, y) \longrightarrow u(x) \otimes v(y)$ произведения $E \times F$ в $E' \otimes_A F'$ удовлетворяет условиям (2). Поэтому существует, и притом единственное, $\mathbf{Z}$-линейное отображение w $E \otimes_A F$ в $E' \otimes_A F'$ такое, что

$$w(x \otimes y) = u(x) \otimes v(y) \tag{3}$$

для всех $x \in E$, $y \in F$. Это отображение обозначается $u \otimes v$ и называется *тензорным произведением линейных отображений* u и v.

Если u, u_1, u_2 принадлежат $\mathscr{L}_A(E, E')$ и v, v_1, v_2 принадлежат $\mathscr{L}_A(F, F')$, то, в силу (3),

$$\left.\begin{aligned}(u_1 + u_2) \otimes v &= (u_1 \otimes v) + (u_2 \otimes v),\\ u \otimes (v_1 + v_2) &= (u \otimes v_1) + (u \otimes v_2).\end{aligned}\right\} \tag{4}$$

Пусть E'' — правый A-модуль, F'' — левый A-модуль и u': $E' \to E''$, v': $F' \to F''$ — A-линейные отображения. В силу (3),

$$(u' \circ u) \otimes (v' \circ v) = (u' \otimes v') \circ (u \otimes v). \tag{5}$$

Более общим образом, пусть A и A' — два кольца, E — правый A-модуль, E' — правый A'-модуль, F — левый A-модуль и F' — левый A'-модуль. Пусть, далее, φ: $A \to A'$ — гомоморфизм относительно кольцевых структур, а u: $E \to E'$ и v: $F \to F'$ — $\mathbf{Z}$-линейные отображения такие, что $u(x\lambda) = u(x)\varphi(\lambda)$ и $v(\lambda y) = \varphi(\lambda) v(y)$ для всех $x \in E$, $y \in F$, $\lambda \in A$. Отображение $(x, y) \to u(x) \otimes v(y)$ произведения $E \times F$ в $E' \otimes_A F'$ по-прежнему удовлетворяет условиям (2), ибо, в частности,

$$u(x\lambda) \otimes v(y) = (u(x)\varphi(\lambda)) \otimes v(y) = u(x) \otimes (\varphi(\lambda) v(y)) = u(x) \otimes v(\lambda y).$$

Поэтому существует, и притом единственное, $\mathbf{Z}$-линейное отображение w $E \otimes_A F$ в $E' \otimes_{A'} F'$ такое, что $w(x \otimes y) = u(x) \otimes v(y)$. Если нет опасности смешения, иногда и это отображение обозначают $u \otimes v$; очевидно, оно обладает свойствами, аналогичными (4) и (5).

3. *Операторы на* $E \otimes_A F$

Пусть u — эндоморфизм правого A-модуля E. Если 1 означает тождественный автоморфизм левого A-модуля F, то $u \otimes 1$ есть эндоморфизм коммутативной группы $E \otimes_A F$ (**п° 2**). При этом, согласно (4) и (5), для любых эндоморфизмов u_1, u_2 A-модуля E имеем $(u_1 + u_2) \otimes 1 = (u_1 \otimes 1) + (u_2 \otimes 1)$ и $(u_1 \circ u_2) \otimes 1 = (u_1 \otimes 1) \circ (u_2 \otimes 1)$. Отсюда, в частности, следует, что если B — кольцо и E наделено структурой левого (соответственно правого) B-модуля, внешний закон которого *перестановочен* (гл. I, § 5, определение 5) с внешним законом структуры A-модуля в E, то тензорное произведение $E \otimes_A F$ канонически наделимо структурой левого

(соответственно правого) B-модуля, при которой

$$\beta\cdot(x\otimes y)=(\beta x)\otimes y$$

(соответственно

$$(x\otimes y)\cdot\beta=(x\beta)\otimes y)$$

для всех $\beta\in B$, $x\in E$, $y\in F$.

Точно так же, если F наделено структурой левого (соответственно правого) C-модуля, внешний закон которого *перестановочен* с внешним законом структуры A-модуля в F, то $E\otimes_A F$ канонически наделимо структурой левого (соответственно прав го) C-модуля, при которой

$$\gamma\cdot(x\otimes y)=x\otimes(\gamma y)$$

(соответственно

$$(x\otimes y)\cdot\gamma=x\otimes(y\gamma))$$

для всех $\gamma\in C$, $x\in E$, $y\in F$. При этом, если $E\otimes_A F$ одновременно наделено структурой B-модуля и структурой C-модуля, то, вследствие предыдущих формул, внешние законы этих двух структур *перестановочны*.

Пусть E' — правый A-модуль, F' — левый A-модуль, $u\colon E\to E'$ и $v\colon F\to F'$ — A-линейные отображения. Если E и E' наделены структурами (скажем, левого) B-модуля, внешние законы которых перестановочны с внешними законами структур A-модуля, и если u B-линейно, то $u\otimes v$ *B-линейно*, ибо

$$(u\otimes v)(\beta(x\otimes y))=(u\otimes v)((\beta x)\otimes y)=u(\beta x)\otimes v(y)=$$
$$=(\beta u(x))\otimes v(y)=\beta\cdot(u(x)\otimes v(y))$$

для всех $\beta\in B$, $x\in E$, $y\in F$. Точно так же, если F и F' наделены структурами C-модуля, внешние законы которых перестановочны с внешними законами структур A-модуля, и если v C-линейно, то $u\otimes v$ *C-линейно*.

Пусть Γ — *центр* кольца A. Гомотетии, определяемые в E (соответственно в F) элементами из Γ, являются эндоморфизмами структуры A-модуля в E (соответственно в F). Тем самым, согласно предыдущему, это определяет в $E\otimes_A F$ две структуры Γ-*модуля* с внешними законами $(\gamma, x\otimes y)\to(x\gamma)\otimes y$ и $(\gamma, x\otimes y)\to x\otimes(\gamma y)$; по определению $E\otimes_A F$, эти две структуры *совпадают*. Если E' — правый A-модуль, F' — левый A-модуль, а $u\colon E\to E'$ и $v\colon F\to F'$ — A-линейные отображения, то $u\otimes v$ есть Γ-*линейное* отображение

$E\otimes_A F$ в $E'\otimes_A F'$. Отображение $(u, v)\to u\otimes v$ произведения $\mathscr{L}_A(E, E')\times\mathscr{L}_A(F, F')$ в $\mathscr{L}_\Gamma(E\otimes_A F, E'\otimes_A F')$ определяет тогда (называемое *каноническим*) отображение $\mathscr{L}_A(E, E')\otimes_\Gamma\mathscr{L}_A(F, F')$ в $\mathscr{L}_\Gamma(E\otimes_A F, E'\otimes_A F')$, которое, очевидно, Γ-линейно.

Заметим, что, так же как в n° 4 § 1, обозначение $u\otimes v$ может повлечь смешение элемента $u\otimes v$ из $\mathscr{L}_A(E, E')\otimes_\Gamma\mathscr{L}_A(F, F')$ с его образом в $\mathscr{L}_\Gamma(E\otimes_A F, E'\otimes_A F')$ при упомянутом отображении, который мы в n° 2 также условились обозначать $u\otimes v$.

В случае, когда A *коммутативно*, $E\otimes_A F$, согласно предыдущему, наделено структурой *A-модуля*, при которой $\alpha(x\otimes y) = (x\alpha)\otimes y = x\otimes(\alpha y)$ для всех $\alpha\in A$, $x\in E$, $y\in F$. Для любого A-билинейного отображения f произведения $E\times F$ в произвольный A-модуль N существует $\mathbf{Z}$-линейное отображение g модуля $E\otimes_A F$ в N такое, что $f(x, y) = g(x\otimes y)$ для всех $x\in E$, $y\in F$; так как при этом для всех $\alpha\in A$ имеем

$$g(\alpha(x\otimes y)) = g((x\alpha)\otimes y) = f(x\alpha, y) = \alpha f(x, y) = \alpha g(x\otimes y),$$

то g A-линейно. Поэтому существует (§ 1, предложение 3) A-изоморфизм модуля $E\otimes_A F$ на A-модуль, обозначенный в определении 3 § 1 через $E\otimes F$, преобразующий $x\otimes y$ (в смысле определения 1) в $x\otimes y$ (в смысле, установленном в n° 2 § 1). В дальнейшем эти два A-модуля будут посредством указанного изоморфизма отождествляться.

4. Тензорное произведение с основным кольцом

Пусть E — правый A-модуль. Так как внешние законы A-модулей A_s и A_d перестановочны, то тензорное произведение $E\otimes_A A_s$ канонически наделимо структурой правого A-модуля, при которой $(x\otimes\lambda)\mu = x\otimes(\lambda\mu)$ для всех $x\in E$, $y\in A$, $\mu\in A$. Так как отображение $(x, \lambda)\to x\lambda$ произведения $E\times A_s$ в E удовлетворяет условиям (2), то существует (называемое *каноническим*) $\mathbf{Z}$-линейное отображение g модуля $E\otimes_A A_s$ в E такое, что $g(x\otimes\lambda) = x\lambda$ для всех $x\in E$, $\lambda\in A$; ясно, что g A-линейно.

Предложение 3. *Отображение h: $x\to x\otimes 1$ правого A-модуля E в $E\otimes_A A_s$ есть изоморфизм правого A-модуля E на правый A-модуль $E\otimes_A A_s$; изоморфизм g, обратный к h, определяется условием $g(x\otimes\lambda) = x\lambda$.*

Действительно, очевидно, $g \circ h$ и $h \circ g$ — соответственно тождественные отображения E и $E \otimes_A A_s$ на себя; поэтому, в силу своей A-линейности, g и h являются взаимно обратными изоморфизмами.

Заметим, что если E наделено структурой (левого или правого) B-модуля, внешний закон которой перестановочен с внешним законом структуры A-модуля в E, то g и h являются также взаимно обратными изоморфизмами структур B-модуля в E и $E \otimes_A A_s$.

Пусть теперь F — левый A-модуль. Аналогичным образом определяются структура левого A-модуля в $A_d \otimes_A F$ и канонический A-изоморфизм $A_d \otimes_A F$ на F.

В частности, существует канонический изоморфизм $A_d \otimes_A A_s$ на A (для структур левого и правого A-модулей), преобразующий $\lambda \otimes \mu$ в $\lambda\mu$.

5. *Свойства $E \otimes_A F$ по отношению к подмодулям и фактормодулям*

Пусть E — правый A-модуль, F — левый A-модуль, M — подмодуль в E и N — подмодуль в F. Рассмотрим канонические отображения

$$M \xrightarrow{i} E \xrightarrow{p} E/M \text{ и } N \xrightarrow{j} F \xrightarrow{q} F/N.$$

Отображение $i \otimes j$ (называемое *каноническим*) вообще не инъективно, так что вообще $M \otimes_A N$ не отождествимо с подгруппой группы $E \otimes_A F$ (см., однако, n° 6). Но имеет место следующий результат, доказываемый совершенно так же, как предложение 6 § 1:

Предложение 4. *Отображение $p \otimes q$ группы $E \otimes_A F$ в $(E/M) \otimes_A (F/N)$ сюръективно, и его ядром служит сумма образов групп $E \otimes_A N$ и $M \otimes_A F$ соответственно при отображениях $1 \otimes j$ и $i \otimes 1$.*

Следствие. *Пусть F — левый A-модуль и $\mathfrak{a}$ — правый идеал кольца A. Тензорное произведение $(A_d/\mathfrak{a}) \otimes_A F$ канонически изоморфно факторгруппе $F/(\mathfrak{a}F)$, где мы под $\mathfrak{a}F$ (допуская вольность) понимаем подгруппу в F, образованную конечными суммами $\sum_i \lambda_i y_i$, в которых $\lambda_i \in \mathfrak{a}$ и $y_i \in F$.*

Действительно, в силу предложения 4, $(A_d/\mathfrak{a})\otimes_A F$ канонически изоморфно факторгруппе группы $A_d\otimes_A F$ по каноническому образу группы $\mathfrak{a}\otimes_A F$. Поэтому достаточно, на основании предложения 3, канонически отождествить $A_d\otimes_A F$ с F и заметить, что канонический образ группы $\mathfrak{a}\otimes_A F$ отождествится тогда с $\mathfrak{a}F$.

6. *Свойства $E\otimes_A F$ по отношению к прямым суммам и произведениям*

Предложение 5. *Пусть E — правый A-модуль, являющийся прямой суммой семейства $(E_\lambda)_{\lambda\in L}$ своих подмодулей, и F — левый A-модуль, являющийся прямой суммой семейства $(F_\mu)_{\mu\in M}$ своих подмодулей. Тогда для любой пары $(\lambda,\mu)\in L\times M$ каноническое отображение $E_\lambda\otimes_A F_\mu$ в $E\otimes_A F$ есть изоморфизм на некоторую подгруппу $G_{\lambda\mu}$ группы $E\otimes_A F$, и $E\otimes_A F$ есть прямая сумма этих подгрупп $G_{\lambda\mu}$.*

Это предложение доказывается совершенно так же, как предложение 7 § 1.

В условиях предложения 5, $E_\lambda\otimes_A F_\mu$ отождествляется с $G_{\lambda\mu}$ посредством канонического отображения. Если элементы $x_\lambda\in E_\lambda$ и $y_\mu\in F_\mu$ равны нулю для всех кроме конечного числа индексов, имеем тогда

$$\Big(\sum_\lambda x_\lambda\Big)\otimes\Big(\sum_\mu y_\mu\Big)=\sum_{\lambda,\mu} x_\lambda\otimes y_\mu. \tag{6}$$

Следствие. *Если F обладает базисом $(b_\mu)_{\mu\in M}$, то группа $E\otimes_A F$ изоморфна группе $E^{(M)}$ и каждый элемент из $E\otimes_A F$ представим, и притом единственным образом, в виде $\sum_\mu (x_\mu\otimes b_\mu)$, где элементы $x_\mu\in E$ для всех кроме конечного числа индексов равны нулю.*

Это доказывается, как следствие 1 предложения 7 § 1, с учетом установленного выше предложения 3.

В условиях следствия предложения 5, допустим, что модуль E также обладает конечным базисом $(a_\lambda)_{\lambda\in L}$. Тогда каждое $z\in E\otimes_A F$ представимо, и притом единственным образом, в виде

$\sum_{\lambda,\,\mu}((a_\lambda\zeta_{\lambda\mu})\otimes b_\mu)$, где $\zeta_{\lambda\mu}$ принадлежат A, и отображение $z\longrightarrow(\zeta_{\lambda\mu})_{(\lambda,\,\mu)\in L\times M}$ есть изоморфизм $E\otimes_A F$ на $A^{(L\times M)}$ относительно групповых структур (и даже относительно структур модуля над центром кольца A).

Пусть $(E_\lambda)_{\lambda\in L}$ — семейство правых A-модулей и $(F_\mu)_{\mu\in M}$ — семейство левых A-модулей; рассмотрим модули $E=\coprod_{\lambda\in L}E_\lambda$ и $F=\coprod_{\mu\in M}F_\mu$. Отображение $((x_\lambda),(y_\mu))\longrightarrow(x_\lambda\otimes y_\mu)$ произведения $E\times F$ в коммутативную группу $\prod_{(\lambda,\mu)\in L\times M}(E_\lambda\otimes_A F_\mu)$ удовлетворяет условиям (2) предложения 1; поэтому существует, и притом единственное, $\mathbf{Z}$-линейное отображение f группы $E\otimes_A F$ в $\prod_{\lambda,\,\mu}(E_\lambda\otimes_A F_\mu)$ (называемое *каноническим*) такое, что $f((x_\lambda)\otimes(y_\mu))=(x_\lambda\otimes y_\mu)$.

Предложение 6. *Если $(E_\lambda)_{\lambda\in L}$ — семейство правых векторных пространств над телом A и $(F_\mu)_{\mu\in M}$ — семейство левых векторных пространств над A, то каноническое отображение $\big(\prod_{\lambda\in L}E_\lambda\big)\otimes_A\big(\prod_{\mu\in M}F_\mu\big)$ в $\prod_{(\lambda,\,\mu)\in L\times M}(E_\lambda\otimes_A F_\mu)$ инъективно.*

Обозначим через g каноническое отображение $E\otimes_A F$ в $\prod_{\lambda\in L}(E_\lambda\otimes_A F)$ и через h_λ (для каждого $\lambda\in L$) — каноническое отображение $E_\lambda\otimes_A F$ в $\prod_{\mu\in M}(E_\lambda\otimes_A F_\mu)$; очевидно, f есть композиция отображения g и отображения (h_λ) произведения $\coprod_{\lambda\in L}(E_\lambda\otimes_A F)$ в $\prod_{\lambda\in L}\big(\prod_{\mu\in M}(E_\lambda\otimes_A F_\mu)\big)$; тем самым всё сводится к случаю, когда каждое из множеств L, M состоит из одного элемента. Покажем, например, что g инъективно; пусть (b_ϱ) — базис левого векторного пространства F; тогда каждый элемент из $E\otimes_A F$ может быть однозначно представлен в виде $z=\sum_\varrho((x_\lambda^{(\varrho)})\otimes b_\varrho)$; если $g(z)=0$, то $\sum_\varrho(x_\lambda^{(\varrho)}\otimes b_\varrho)=0$ для каждого $\lambda\in L$, значит, $x_\lambda^{(\varrho)}=0$, каковы бы ни были λ и ϱ (следствие предложения 5), и предложение доказано.

При выполнении условий предложения 6 тензорное произведение $\big(\coprod_\lambda E_\lambda\big)\otimes_A\big(\coprod_\mu F_\mu\big)$ часто отождествляется с его каноническим

образом в $\prod_{\lambda,\,\mu}(E_\lambda \otimes_A F_\mu)$. В частности, если F — левое векторное пространство над телом A, $A_d \otimes_A F$ канонически отождествляется с F (n° 4), значит, $A_d^L \otimes_A F$ канонически отождествляется с векторным подпространством в F^L путем отождествления элемента $\sum_i (u_i \otimes b_i)$, где $b_i \in F$ и u_i — отображение L в A, с отображением $\lambda \longrightarrow \sum_i u_i(\lambda)\, b_i$ множества L в F. Точно так же $E \otimes_A A_s^M$, где E — правое векторное пространство над A, отождествляется с подпространством в E^M. Еще специальней, $A_d^L \otimes_A A_s^M$ для любого тела A отождествляется с подпространством в $A^{L\times M}$ (рассматриваемом одновременно и как левое и как правое векторное пространство над A) путем отождествления каждого элемента $\sum_i (u_i \otimes v_i)$, где u_i — отображение L в A и v_i — отображение M в A, с отображением $(\lambda, \mu) \longrightarrow \sum_i u_i(\lambda)\, v_i(\mu)$ множества $L \times M$ в A.

7. *Дополнения относительно* $\mathscr{L}_A(E, F)$

Пусть E и F — два левых или два правых A-модуля. (В дальнейшем для краткости будет предполагаться, что E и F — левые A-модули.) Мы дополним в некоторых отношениях свойства $\mathscr{L}_A(E, F)$, установленные в главе II. Читатель отметит определенную аналогию между свойствами $\mathscr{L}_A(E, F)$ и $E \otimes_A F$.

Пусть E', F' — левые A-модули и u: $E \longrightarrow E'$, v: $F \longrightarrow F'$ — A-линейные отображения. Отнесение каждому элементу $f \in \mathscr{L}_A(E, F)$ элемента $v \circ f \circ u \in \mathscr{L}_A(E', F')$ устанавливает $\mathbf{Z}$-линейное отображение $\mathscr{L}_A(E, F)$ в $\mathscr{L}_A(E', F')$. Мы будем обозначать его $\mathscr{L}(u, v)$.

Каковы бы ни были u, u_1, u_2 из $\mathscr{L}_A(E', E)$ и v, v_1, v_2 из $\mathscr{L}_A(F, F')$, имеем

$$\left.\begin{aligned} \mathscr{L}(u_1 + u_2, v) &= \mathscr{L}(u_1, v) + \mathscr{L}(u_2, v), \\ \mathscr{L}(u, v_1 + v_2) &= \mathscr{L}(u, v_1) + \mathscr{L}(u, v_2). \end{aligned}\right\} \tag{7}$$

Если E'', F'' — левые A-модули и u': $E'' \longrightarrow E'$, v': $F' \longrightarrow F''$ — A-линейные отображения, то

$$\mathscr{L}(u \circ u', v' \circ v) = \mathscr{L}(u', v') \circ \mathscr{L}(u, v). \tag{8}$$

Пусть u — эндоморфизм A-модуля E. Если 1 — тождественный автоморфизм модуля F, то $\mathscr{L}(u, 1)$ есть эндоморфизм

коммутативной группы $\mathscr{L}_A(E, F)$. При этом для любых двух эндоморфизмов u_1, u_2 модуля E, согласно (7) и (8), имеем $\mathscr{L}(u_1+u_2, 1) = \mathscr{L}(u_1, 1)+\mathscr{L}(u_2, 1)$ и $\mathscr{L}(u_1 \circ u_2, 1) = \mathscr{L}(u_2, 1)\circ\mathscr{L}(u_1, 1)$. Отсюда, в частности, следует, что если B — кольцо и E наделено структурой левого (соответственно правого) B-модуля, внешний закон которого *перестановочен* с внешним законом структуры A-модуля в E, то $\mathscr{L}_A(E, F)$ наделимо структурой правого (соответственно левого) B-модуля, при которой

$$(f\cdot\beta)(x) = f(\beta x)$$

(соответственно $\quad (\beta\cdot f)(x) = f(x\beta)$)

для всех $\beta\in B$, $f\in\mathscr{L}_A(E, F)$, $x\in E$.

Точно так же, если F наделено структурой левого (соответственно правого) C-модуля, внешний закон которого *перестановочен* с внешним законом структуры A-модуля в F, то $\mathscr{L}_A(E, F)$ канонически наделимо структурой левого (соответственно правого) C-модуля, при которой

$$(\gamma\cdot f)(x) = \gamma f(x)$$

(соответственно $\quad (f\cdot\gamma)(x) = f(x)\gamma$)

для $\gamma\in C, f\in\mathscr{L}_A(E, F), x\in E$. При этом, если $\mathscr{L}_A(E, F)$ одновременно наделено так структурами B-модуля и C-модуля, то внешние законы этих двух структур, в силу предыдущих формул, *перестановочны*. В частности, если Γ — центр кольца A, мы вновь получаем так, двумя различными способами, структуру Γ-модуля в $\mathscr{L}_A(E, F)$, определенную в n° 1 § 2 главы II.

Пусть E' и F' — левые A-модули, $u\colon E'\to E$ и $v\colon F\to F'$ — A-линейные отображения. Если E и E' наделены структурами (скажем, левого) B-модуля, внешние законы которых соответственно перестановочны с внешними законами структур A-модуля, и если u B-линейно, то $\mathscr{L}(u, v)$ B-линейно. Действительно, если h и h' означают эндоморфизмы модулей E и E', порожденные одним и тем же элементом $\beta\in B$, то, в силу предположения, $h\circ u = u\circ h'$ и, значит,

$$\mathscr{L}(u, v)\circ\mathscr{L}(h, 1_F) = \mathscr{L}(h\circ u, v) = \mathscr{L}(u\circ h', v) = \mathscr{L}(h', 1_{F'})\circ\mathscr{L}(u, v),$$

где 1_F и $1_{F'}$ означают соответственно тождественные автоморфизмы модулей F и F'. Так как $\mathscr{L}(h, 1_F)$ и $\mathscr{L}(h', 1_{F'})$ — эндоморфизмы,

порожденные элементом β соответственно в $\mathscr{L}_A(E, F)$ и $\mathscr{L}_A(E', F')$, то наше утверждение тем самым доказано. Точно так же, если F и F' наделены структурами C-модуля, внешние законы которых перестановочны с внешними законами структур A-модуля, и если v C-линейно, то $\mathscr{L}(u, v)$ C-линейно.

Рассмотрим группу $\mathscr{L}_A(A_s, F)$, где F — левый A-модуль. Так как правые умножения $\xi \longrightarrow \xi\alpha$ являются эндоморфизмами левого A-модуля A_s, то, согласно предыдущему, $\mathscr{L}_A(A_s, F)$ канонически наделимо структурой левого A-модуля такой, что $(\alpha f)(\xi) = f(\xi\alpha)$ для всех $f \in \mathscr{L}_A(A_s, F)$ и всех α и ξ из A. Пусть θ_x для каждого $x \in F$ — элемент из $\mathscr{L}_A(A_s, F)$, определяемый формулой $\theta_x(\lambda) = \lambda x$. Тогда отображение $g: x \longrightarrow \theta_x$ модуля F в $\mathscr{L}_A(A_s, F)$, называемое *каноническим*, A-линейно.

Предложение 7. *Каноническое отображение* g: $x \longrightarrow \theta_x$ *левого* A*-модуля* F *в* $\mathscr{L}_A(A_s, F)$ *есть изоморфизм* A*-модуля* F *на* A*-модуль* $\mathscr{L}_A(A_s, F)$; *обратным ему изоморфизмом служит* h: $f \longrightarrow f(1)$.

Действительно, A-линейность h непосредственно проверяется; так как очевидно $g \circ h$ и $h \circ g$ являются соответственно тождественными отображениями $\mathscr{L}_A(A_s, F)$ и F на себя, то тем самым предложение доказано.

Заметим, что если F наделено, кроме того, структурой B-модуля, внешний закон которого перестановочен с внешним законом структуры A-модуля, то канонический изоморфизм $x \longrightarrow \theta_x$ также B-линеен.

Предыдущие свойства являются аналогами свойств $E \otimes_A F$, рассмотренных в n°n° 2, 3 и 4; свойства же, рассмотренные в n°n° 5 и 6, имеют своими аналогами свойства $\mathscr{L}_A(E, F)$, доказанные в n°n° 2, 3 и 4 § 2 главы II.

8. *Два канонических изоморфизма*

Пусть E — правый A-модуль, F — левый A-модуль, G — коммутативная группа и H — коммутативная группа всех отображений f: $E \times F \longrightarrow G$, удовлетворяющих условиям (2). Как мы видели (n° 1), существует канонический изоморфизм H на $\mathscr{L}_Z(E \otimes_A F, G)$.

С другой стороны, в $\mathscr{L}_Z(E, G)$ существует каноническая структура левого A-модуля, а в $\mathscr{L}_Z(F, G)$ — каноническая структура

правого A-модуля (n° 7). Поэтому можно рассматривать группы $\mathscr{L}_A(E, \mathscr{L}_{\mathbf{Z}}(F, G))$ и $\mathscr{L}_A(F, \mathscr{L}_{\mathbf{Z}}(E, G))$. Отображение f произведения $E \times F$ в G канонически отождествимо с отображением E в множество G^F всех отображений F в G (Теор. мн., Рез., § 4, n° 14); выражая, что это последнее отображение принадлежит $\mathscr{L}_A(E, \mathscr{L}_{\mathbf{Z}}(F, G))$, получаем как раз условия (2). Тем самым имеем канонический изоморфизм H на $\mathscr{L}_A(E, \mathscr{L}_{\mathbf{Z}}(F, G))$. Аналогично определяется канонический изоморфизм H на $\mathscr{L}_A(F, \mathscr{L}_{\mathbf{Z}}(E, G))$. Эти изоморфизмы позволяют отождествлять группы H, $\mathscr{L}_{\mathbf{Z}}(E \otimes_A F, G)$, $\mathscr{L}_A(E, \mathscr{L}_{\mathbf{Z}}(F, G))$, $\mathscr{L}_A(F, \mathscr{L}_{\mathbf{Z}}(E, G))$.

Предположим теперь, что E и G являются, кроме того, левыми (соответственно правыми) B-модулями и что внешний закон B-модуля в E перестановочен с внешним законом A-модуля. Тогда $E \otimes_A F$ канонически наделимо структурой левого (соответственно правого) B-модуля (см. n° 3), а $\mathscr{L}_B(E, G)$ канонически наделимо структурой левого A-модуля (n° 7). Поэтому можно рассматривать группы $\mathscr{L}_B(E \otimes_A F, G)$ и $\mathscr{L}_A(F, \mathscr{L}_B(E, G))$. Они являются соответственно подгруппами групп $\mathscr{L}_{\mathbf{Z}}(E \otimes_A F, G)$ и $\mathscr{L}_A(F, \mathscr{L}_{\mathbf{Z}}(E, G))$. Разыскивая условие, при котором отображение $f\colon E \times F \to G$, удовлетворяющее условиям (2), соответствует элементу из $\mathscr{L}_B(E \otimes_A F, G)$ или элементу из $\mathscr{L}_A(E, \mathscr{L}_B(E, G))$, в каждом из этих двух случаев находим *одно и то же* условие

$$f(\beta x, y) = \beta f(x, y)$$

(соответственно $\qquad f(x\beta, y) = f(x, y)\beta$)

тождественно относительно $\beta \in B$, $x \in E$, $y \in F$.

Аналогично, предположим, что F и G — левые (соответственно правые) C-модули и что внешний закон C-модуля в F перестановочен с внешним законом A-модуля. Тогда для того, чтобы отображение $f\colon E \times F \to G$, удовлетворяющее условиям (2), соответствовало элементу из $\mathscr{L}_C(E \otimes_A F, G)$ или элементу из $\mathscr{L}_A(E, \mathscr{L}_C(F, G))$, необходимо и достаточно, чтобы f удовлетворяло одному и тому же условию

$$f(x, \gamma y) = \gamma f(x, y)$$

(соответственно $\qquad f(x, y\gamma) = f(x, y)\gamma$)

тождественно относительно $\gamma \in C$, $x \in E$, $y \in F$.

Таким образом, установлен следующий результат:

Предложение 8. а) *Пусть g' для каждого $g \in \mathscr{L}_B(E \otimes_A F, G)$ есть отображение F в $\mathscr{L}_B(E, G)$, определяемое требованием, чтобы $(g'(y))(x) = g(x \otimes y)$ для всех $x \in E$, $y \in F$. Тогда $g \to g'$ есть изоморфизм коммутативной группы $\mathscr{L}_B(E \otimes_A F, G)$ на группу $\mathscr{L}_A(F, \mathscr{L}_B(E, G))$.*

б) *Пусть h' для каждого $h \in \mathscr{L}_C(E \otimes_A F, G)$ есть отображение E в $\mathscr{L}_C(F, G)$, определяемое требованием, чтобы $(h'(x))(y) = h(x \otimes y)$ для всех $x \in E$, $y \in F$. Тогда $h \to h'$ есть изоморфизм группы $\mathscr{L}_C(E \otimes_A F, G)$ на группу $\mathscr{L}_A(E, \mathscr{L}_C(F, G))$.*

9. Коммутативность и ассоциативность тензорного произведения

Пусть E — правый и F — левый A-модуль. F можно рассматривать также как правый A^0-модуль, а E — как левый A^0-модуль, где A^0 — кольцо, противоположное A.

Предложение 9. *Существует, и притом единственный, изоморфизм σ коммутативной группы $E \otimes_A F$ на коммутативную группу $F \otimes_{A^0} E$ такой, что $\sigma(x \otimes y) = y \otimes x$ для всех $x \in E$ и $y \in F$* («коммутативность» тензорного произведения).

Действительно, отображение $(x, y) \to y \otimes x$ произведения $E \times F$ в $F \otimes_{A^0} E$ удовлетворяет условиям (2), если вспомнить, что произведение λx (соответственно $y\lambda$) при структуре левого (соответственно правого) A^0-модуля в E (соответственно в F) есть, по определению, произведение $x\lambda$ (соответственно λy) при структуре правого (соответственно левого) A-модуля в E (соответственно в F). Поэтому (предложение 1) мы получаем $\mathbf{Z}$-линейное отображение σ группы $E \otimes_A F$ в $F \otimes_{A^0} E$ такое, что $\sigma(x \otimes y) = y \otimes x$. Так же определяется $\mathbf{Z}$-линейное отображение τ группы $F \otimes_{A^0} E$ в $E \otimes_A F$ такое, что $\tau(y \otimes x) = x \otimes y$, и ясно, что σ и τ — взаимно обратные изоморфизмы.

Изоморфизм σ и обратный изоморфизм τ называются *каноническими*; в случае, когда E (соответственно F) наделено структурой B-модуля (соответственно C-модуля), внешний закон которой перестановочен с внешним законом структуры A-модуля, эти изоморфизмы очевидно являются также изоморфизмами структур B-модуля (соответственно C-модуля), канонически определяемых в $E \otimes_A F$ и $F \otimes_{A^0} E$ (n° 3).

Пусть теперь A и B — кольца, E — правый A-модуль, F — коммутативная группа, наделенная структурами левого A-модуля и правого B-модуля с *перестановочными* внешними законами и G — левый B-модуль.

Пусть C — коммутативная группа $\mathbf{Z}^{(E\times F\times G)}$ и D — ее подгруппа, порожденная элементами следующих типов:

$$\left.\begin{array}{l}(x_1+x_2,\ y,\ z)-(x_1,\ y,\ z)-(x_2,\ y,\ z),\\ (x,\ y_1+y_2,\ z)-(x,\ y_1,\ z)-(x,\ y_2,\ z),\\ (x,\ y,\ z_1+z_2)-(x,\ y,\ z_1)-(x,\ y,\ z_2),\\ (x\lambda,\ y,\ z)-(x,\ \lambda y,\ z),\\ (x,\ y\mu,\ z)-(x,\ y,\ \mu z)\end{array}\right\} \tag{9}$$

со всевозможными x, x_1, x_2 из E, y, y_1, y_2 из F, z, z_1, z_2 из G, $\lambda\in A$ и $\mu\in B$. Коммутативная группа C/D обозначается $E\otimes_A F\otimes_B G$ или просто $E\otimes F\otimes G$, если это не может повлечь путаницы. Канонический образ $(x, y, z)\in C$ в C/D обозначается $x\otimes y\otimes z$.

Если g — $\mathbf{Z}$-линейное отображение $E\otimes_A F\otimes_B G$ в коммутативную группу H, то отображение $(x, y, z)\longrightarrow f(x, y, z)=g(x\otimes y\otimes z)$ очевидно удовлетворяет условиям

$$\left.\begin{array}{l}f(x_1+x_2,\ y,\ z)=f(x_1,\ y,\ z)+f(x_2,\ y,\ z),\\ f(x,\ y_1+y_2,\ z)=f(x,\ y_1,\ z)+f(x,\ y_2,\ z),\\ f(x,\ y,\ z_1+z_2)=f(x,\ y,\ z_1)+f(x,\ y,\ z_2),\\ f(x\lambda,\ y,\ z)=f(x,\ \lambda y,\ z),\\ f(x,\ y\mu,\ z)=f(x,\ y,\ \mu z).\end{array}\right\} \tag{10}$$

Обратно, пусть f — отображение $E\times F\times G$ в H, удовлетворяющее условиям (10); рассуждая тогда, как при доказательстве предложения 1, заключаем, что существует, и притом единственное, $\mathbf{Z}$-линейное отображение g группы $E\otimes_A F\otimes_B G$ в H такое, что $f(x, y, z)=g(x\otimes y\otimes z)$ для всех $x\in E$, $y\in F$, $z\in G$.

Тем же рассуждением, что и при выводе следствия предложения 1, устанавливается следующее свойство единственности. Пусть H — коммутативная группа и h — отображение $E\times F\times G$ в H, удовлетворяющее условиям (10) и такое, что $h(E\times F\times G)$ порождает H; предположим, что для каждой коммутативной группы L и каждого отображения f произведения $E\times F\times G$ в L, удовлетворяющего условиям (10), существует $\mathbf{Z}$-линейное отображение g группы H в L такое, что $f=g\circ h$. Тогда существует, и притом единственный, $\mathbf{Z}$-изоморфизм ψ группы $E\otimes_A F\otimes_B G$

на H такой, что $h=\psi\circ\theta$, где θ означает каноническое отображение $(x, y, z)\longrightarrow x\otimes y\otimes z$ произведения $E\times F\times G$ в $E\otimes_A F\otimes_L G$.

Построим снова коммутативные группы H, обладающие указанными свойствами. Поскольку внешние законы структур A-модуля и B-модуля в F *перестановочны*, можно (n° 3) канонически определить в $E\otimes_A F$ структуру правого B-модуля и, следовательно, образовать группу $H=(E\otimes_A F)\otimes_B G$. Пусть h — отображение $(x, y, z)\longrightarrow(x\otimes y)\otimes z$ произведения $E\times F\times G$ в H; оно очевидным образом удовлетворяет условиям (10), и группа H порождается множеством $h(E\times F\times G)$. Наконец, пусть f — отображение $E\times F\times G$ в коммутативную группу L, удовлетворяющее условиям (10). Для каждого $z\in G$ отображение $(x, y)\longrightarrow f(x, y, z)$ удовлетворяет условиям (2), а потому (предложение 1) существует $\mathbf{Z}$-линейное отображение g_z группы $E\otimes_A F$ в L такое, что $g_z(x\otimes y)=f(x, y, z)$, каковы бы ни были $x\in E$ и $y\in F$. Рассмотрим отображение $(u, z)\longrightarrow g_z(u)$ произведения $(E\otimes_A F)\times G$ в L. Имеем

$$g_{z_1+z_2}(u)=g_{z_1}(u)+g_{z_2}(u),\quad g_z(u_1+u_2)=g_z(u_1)+g_z(u_2)$$

и

$$g_z(u\mu)=g_{\mu z}(u)$$

(первое и третье из этих соотношений очевидны, когда u имеет вид $x\otimes y$, и распространяются на общий случай по линейности). Поэтому существует $\mathbf{Z}$-линейное отображение g группы $(E\otimes_A F)\otimes_B G$ в L такое, что $g((x\otimes y)\otimes z)=f(x, y, z)$ для всех $x\in E$, $y\in F$, $z\in G$. Аналогичное рассуждение можно провести для $E\otimes_A(F\otimes_B G)$, так что нами установлено следующее предложение:

Предложение 10. *Существует, и притом единственный, изоморфизм*

$$\varphi\colon E\otimes_A F\otimes_B G\longrightarrow(E\otimes_A F)\otimes_B G$$

такой, что $\varphi(x\otimes y\otimes z)=(x\otimes y)\otimes z$, *и однозначно определенный изоморфизм*

$$\psi\colon E\otimes_A F\otimes_B G\longrightarrow E\otimes_A(F\otimes_B G)$$

такой, что $\psi(x\otimes y\otimes z)=x\otimes(y\otimes z)$ («ассоциативность» тензорного произведения).

Эти изоморфизмы, а также обратные им изоморфизмы и композиции $\varphi \circ \psi^{-1}$ и $\psi \circ \varphi^{-1}$ называются *каноническими*. Если, например, F наделено структурой C-модуля, внешний закон которой перестановочен с внешними законами структур A-модуля и B-модуля в F, то, как в n° 3, устанавливается, что $E \otimes_A F \otimes_B G$ канонически наделимо структурой C-модуля и что предыдущие канонические изоморфизмы C-линейны; аналогично, когда E (соответственно G) наделено структурой модуля, внешний закон которой перестановочен с внешним законом A-модуля (соответственно B-модуля) в E (соответственно G).

Сказанное выше допускает обобщение на случай $n-1$ колец A_i $(1 \leqslant i \leqslant n-1)$ и n модулей $E_1, E_2, \ldots, E_n$. Предположим, что E_1 есть правый A_1-модуль, E_n — левый A_{n-1}-модуль и E_i при $1 < i < n$ наделено структурами левого A_{i-1}-модуля и правого A_i-модуля, внешние законы которых перестановочны. Тогда тензорное произведение $E_1 \otimes_{A_1} E_2 \otimes_{A_2} \ldots \otimes_{A_{n-2}} E_{n-1} \otimes_{A_{n-1}} E_n$, или просто $E_1 \otimes E_2 \otimes \ldots \otimes E_n$, определяется таким образом, что $\mathbf{Z}$-линейные отображения этой группы в коммутативную группу L взаимно однозначно соответствуют отображениям $E_1 \times E_2 \times \ldots \times E_n$ в L, удовлетворяющим условиям, которые обобщают условия (10) и формулирование которых мы предоставим читателю. И здесь имеются изоморфизмы «ассоциативности», которые читатель определит по приведенному выше образцу. В случае, когда все A_i совпадают с одним и тем же коммутативным кольцом A, мы вновь получаем тензорное произведение $E_1 \otimes E_2 \otimes \ldots \otimes E_n$, определенное в n° 7 § 1 (без его структуры A-модуля).

10. Изменение основного кольца

Пусть A и B — кольца и ϱ — гомоморфизм A в B, преобразующий единичный элемент в единичный элемент. Каждый левый (соответственно правый) B-модуль N может рассматриваться как левый (соответственно правый) A-модуль, если считать $\alpha \cdot x = \varrho(\alpha) x$ (соответственно $x \cdot \alpha = x\varrho(\alpha)$) для всех $x \in N$ и $\alpha \in A$; выполнение аксиом унитарного модуля при этом очевидно. Каждый гомоморфизм B-модуля M в B-модуль N будет также гомоморфизмом относительно соответствующих структур A-модуля в M и N.

В частности, B, наделенное структурой правого B-модуля (т. е. структурой B_d), может также рассматриваться как правый A-модуль; поэтому, если E — левый A-модуль, можно образовать тензорное произведение $B \otimes_A E$ (где подразумевается, что B наделено структурой, определяемой гомоморфизмом ϱ). Так как B наделено также структурой левого B-модуля (структурой B_s), а внешние законы в B_s и B_d перестановочны, $B \otimes_A E$ канонически наделимо структурой *левого B-модуля* (n° 3). Мы говорим, что этот B-модуль получен из E путем *расширения кольца скаляров посредством* ϱ *до* B, и обозначаем его $E_{(B,\varrho)}$ или просто $E_{(B)}$, если можно не опасаться путаницы. В случае, когда A есть подкольцо центра кольца B, содержащее единичный элемент, а ϱ — каноническая инъекция A в B, мы вновь получаем модуль $E_{(B)}$, определенный в n° 1 § 2.

Возвращаясь к общему случаю, будем называть $\mathbf{Z}$-линейное отображение $\varphi\colon x \longrightarrow 1 \otimes x$ модуля E в $B \otimes_A E = E_{(B)}$ *каноническим*. Для всех $a \in A$ и $x \in E$ имеем

$$\varphi(ax) = 1 \otimes (ax) = \varrho(a) \otimes x = \varrho(a)(1 \otimes x) = \varrho(a)\varphi(x),$$

иными словами, φ *A-линейно* (относительно структуры левого A-модуля в $E_{(B)}$, получающейся из его структуры B-модуля, как описано в начале этого n°). Канонический образ $\varphi(E)$ модуля E в $E_{(B)}$ порождает B-модуль $E_{(B)}$.

Предложение 11. *Для каждого A-линейного отображения f модуля E в левый B-модуль F существует, и притом единственное, B-линейное отображение $\overline{f}$ модуля $E_{(B)}$ в F такое, что $f(x) = \overline{f}(1 \otimes x)$ для всех $x \in E$.*

Это доказывается так же, как предложение 2 § 2, с использованием предложения 1, установленного в n° 1.

Согласно n° 3, для каждого A-линейного отображения g модуля E в левый A-модуль E' отображение $\widetilde{g} = 1 \otimes g$ модуля $E_{(B)}$ в $E'_{(B)}$ B-линейно; при этом, обозначая через φ' каноническое отображение E' в $E'_{(B)}$, имеем $\widetilde{g}(\varphi(x)) = (1 \otimes g)(1 \otimes x) = 1 \otimes g(x) = \varphi'(g(x))$ для каждого $x \in E$, т. е. $\widetilde{g} \circ \varphi = \varphi' \circ g$. Очевидно, $\widetilde{g}$ есть единственное B-линейное отображение $E_{(B)}$ в $E'_{(B)}$ такое, что $\widetilde{g}(1 \otimes x) = 1 \otimes g(x)$.

Пусть теперь C — кольцо и σ — гомоморфизм B в C, преобразующий единичный элемент в единичный элемент. Тогда можно рассматривать, с одной стороны, C-модуль $(E_{(B,\varrho)})_{(C,\sigma)}$, а с другой — C-модуль $E_{(C,\sigma\circ\varrho)}$, которые мы будем для упрощения обозначать $(E_{(B)})_{(C)}$ и $E_{(C)}$. Коммутативными группами этих модулей служат соответственно $C\otimes_B(B\otimes_A E)$ и $C\otimes_A E$. Но C-модуль $C\otimes_B(B\otimes_A E)$ канонически отождествим с C-модулем $(C\otimes_B B)\otimes_A E$ (предложение 10); с другой стороны, C-модуль $C\otimes_B B$ отождествим с C-модулем C_s посредством изоморфизма $\gamma\otimes\beta\to\gamma\sigma(\beta)$ (предложение 3), и этот изоморфизм есть также изоморфизм относительно структуры правого A-модуля в $C\otimes_B B$, определяемой гомоморфизмом ϱ, и структуры правого A-модуля в C, определяемой гомоморфизмом $\sigma\circ\varrho$. В итоге мы получаем изоморфизм θ C-модуля $(E_{(B)})_{(C)}$ на C-модуль $E_{(C)}$, называемый, как и изоморфизм, обратный ему, *каноническим*, такой, что

$$\theta(\gamma\otimes(\beta\otimes x))=(\gamma\sigma(\beta))\otimes x$$

для всех $x\in E$, $\beta\in B$, $\gamma\in C$. Если ψ и φ' означают соответственно канонические отображения E в $E_{(C)}$ и $E_{(B)}$ в $(E_{(B)})_{(C)}$, изоморфизм θ отождествляет $\varphi'\circ\varphi$ с ψ.

Пусть E — A-модуль, обладающий базисом $(a_\lambda)_{\lambda\in L}$, и φ — каноническое отображение $x\to 1\otimes x$ этого модуля в $E_{(B,\varrho)}$; из следствия предложения 5 вытекает, что $(\varphi(a_\lambda))_{\lambda\in L}$ есть базис B-модуля $E_{(B,\varrho)}$. Для того чтобы φ было инъективным, необходимо и достаточно, чтобы ϱ было инъективным, ибо $\varphi\left(\sum_{\lambda\in L}\xi_\lambda a_\lambda\right)=\sum_{\lambda\in L}\varrho(\xi_\lambda)(1\otimes a_\lambda)$.

Аналогичные определения и свойства получим, отправляясь от правого A-модуля E.

11. *Применение: размерность модуля*

Предложение 12. *Пусть A — кольцо и E — свободный левый A-модуль. Если существует гомоморфизм кольца A в тело D, переводящий единичный элемент в единичный элемент, то любые два базиса E над A равномощны.*

Действительно, пусть ϱ — гомоморфизм A в D и φ — каноническое отображение модуля E в векторное пространство $E_{(D,\varrho)}$; как мы видели в n° 10, для каждого базиса (a_λ) модуля E $(\varphi(a_\lambda))$

есть базис в $E_{(D,\,0)}$; мы видим таким образом, что если E обладает конечным базисом над A, то каждый другой базис конечен и состоит из такого же числа элементов (гл. II, § 3, теорема 3).

Предположим теперь, что E обладает бесконечным базисом $(a_\lambda)_{\lambda\in L}$, и пусть $(b_\mu)_{\mu\in M}$ — другой базис этого модуля. Пусть $C(\mu)$ для каждого $\mu\in M$ — конечное множество тех $\lambda\in L$, для которых компонента b_μ с индексом λ относительно базиса (a_λ) отлична от нуля, и $C=\bigcup_{\mu\in M} C(\mu)$. Имеем $\mathrm{Card}\,(C)\leqslant \mathrm{Card}\,(M)$ *) (Теор. мн., гл. III, § 6, следствие 4 теоремы 2); но так как b_μ для каждого $\mu\in M$ принадлежит подмодулю в E, порожденному теми a_λ, для которых $\lambda\in C$, откуда следует, что $C=L$, то $\mathrm{Card}\,(L)\leqslant \mathrm{Card}\,(M)$; так же устанавливается, что $\mathrm{Card}\,(M)\leqslant \mathrm{Card}\,(L)$, и предложение доказано.

Заметим, что вторая часть этого доказательства имеет силу независимо от каких бы то ни было предположений о кольце A.

В случае, когда A удовлетворяет условиям предложения 12, кардинальное число произвольного базиса свободного A-модуля E называется также *размерностью* E и обозначается $\dim_A E$ или $\dim E$.

Замечания. 1) В случае, когда A — тело и E обладает конечным базисом, предыдущее определение совпадает с данным в n° 2 § 3 главы II.

2) Условия предложения 12 выполнены, в частности, для каждого *коммутативного* кольца A (с единицей), ибо, в силу теоремы Круля (гл. I, § 8, теорема 2), существует гомоморфизм кольца A на поле (гл. I, § 9, теорема 2); в случае, когда E обладает конечным базисом, мы так другим способом вновь получаем следствие 2 теоремы 2 § 5.

3) Большинство свойств конечномерных векторных пространств уже не распространяется на конечномерные A-модули над коммутативным кольцом A. Например, идеал в A не обязательно обладает базисом (см. главу II, § 1, n° 6, замечание 1 после определения 8, и главу VII, § 1, упражнения 1 и 12); подмодуль F свободного модуля E может быть свободным, отличным от E и иметь туже размерность, что и E, как показывает пример главных идеалов в A; тот же пример (в случае, когда A есть кольцо целостности) показывает, что

*) $\mathrm{Card}\,(E)$ означает мощность (кардинальное число) множества E. — *Перев.*

свободный подмодуль свободного A-модуля не обязательно обладает дополнением.

Упражнения. 1) Пусть E — правый A-модуль и F — левый A-модуль. Пусть, далее, f — функция, определенная на множестве S всех конечных последовательностей $((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n))$ (n произвольно) элементов из $E \times F$, со значениями в множестве G, такая, что

1° $f((x_1, y_1), \ldots, (x_n, y_n)) = f((x_{\sigma(1)}, y_{\sigma(1)}), \ldots, (x_{\sigma(n)}, y_{\sigma(n)}))$

для каждой подстановки $\sigma \in \mathfrak{S}_n$;

2° $f((x_1 + x_1', y_1), \ldots, (x_n, y_n)) = f((x_1, y_1), (x_1', y_1), \ldots, (x_n, y_n))$;
3° $f((x_1, y_1 + y_1'), \ldots, (x_n, y_n)) = f((x_1, y_1), (x_1, y_1'), \ldots, (x_n, y_n))$;
4° $f((x_1\lambda, y_1), \ldots, (x_n, y_n)) = f((x_1, \lambda y_1), \ldots, (x_n, y_n))$.

Показать, что существует, и притом единственное, отображение g группы $E \otimes_A F$ в G такое, что $f((x_1, y_1), \ldots, (x_n, y_n)) = g\left(\sum_{i=1}^{n} (x_i \otimes y_i)\right)$.

[Заметить, что если $\sum_i (x_i \otimes y_i) = \sum_j (x_j' \otimes y_j')$, то разность $\sum_i (x_i, y_i) - \sum_j (x_j', y_j')$ в модуле $\mathbf{Z}^{(E \times F)}$ есть линейная комбинация с целыми коэффициентами элементов одного из типов (1).]

2) а) Пусть E — коммутативная группа, наделенная структурами правого и левого векторных пространств над полем K, внешние законы которых перестановочны. Предположим, кроме того, что размерности E как правого и левого векторных пространств над K обе равны одному и тому же конечному числу n. Показать, что в E существует семейство $(a_i)_{1 \leqslant i \leqslant n}$ элементов, являющееся базисом E для каждой из этих двух структур векторного пространства над K. [Заметить, что если $(b_j)_{1 \leqslant j \leqslant m}$ — семейство $m < n$ элементов из E, свободное при каждой из двух структур векторного пространства в E, и V — правое, а W — левое векторные подпространства, порожденные элементами b_j, то либо $V + W \neq E$, либо $V \cap \mathbf{C}W$ и $W \cap \mathbf{C}V$ не пусты; в этом последнем случае показать, что $y + z$, где $y \in V \cap \mathbf{C}W$ и $z \in W \cap \mathbf{C}V$, образует вместе с элементами b_j семейство $m + 1$ элементов, свободное при каждой из двух структур векторного пространства в E.]

б) Пусть F — коммутативная подгруппа в E, являющаяся его векторным подпространством при каждой из двух структур векторного пространства в E и такая, что обе индуцированные структуры векторного пространства в F обладают одинаковой размерностью $p < n$ (см. упражнение 3б). Показать, что существует семейство $(a_i)_{1 \leqslant i \leqslant n}$ n элементов из E, являющееся базисом для каждой из двух структур

векторного пространства в E, первые p элементов которого образуют базис для двух структур векторного пространства в F. [Тот же метод.]

в) Пусть $(b_j)_{1\leqslant j\leqslant n-1}$ — семейство $n-1$ элементов из E, свободное при каждой из двух структур векторного пространства в E. Пусть, далее, V — левая и W — правая гиперплоскости, порожденные этим семейством. Показать, что если $V \subset W$ (соответственно $W \subset V$), то $V=W$. [Используя соотношение $V \subset W$, показать, что если $a \notin W$, то множество тех $\lambda \in K$, для которых $\lambda a \in W$, есть идеал.]

°3) а) Пусть $K=K_0(X)$ — поле рациональных дробей над полем K_0 (гл. IV, § 3). В K определены: 1° структура левого векторного пространства над K, в которой произведением $t\cdot u$ элемента $u \in K$ на оператор $t \in K$ является рациональная дробь $t(X)\,u(X)$; 2° структура правого векторного пространства над K, в которой произведением $u\cdot t$ элемента $u \in K$ на оператор $t \in K$ является рациональная дробь $u(X)\,t(X^2)$. Показать, что внешние законы этих двух структур перестановочны, структура левого векторного пространства имеет размерность 1, а структура правого векторного пространства — размерность 2. Получить отсюда примеры коммутативных групп E, наделенных структурами левого и правого векторных пространств над K, внешние законы которых перестановочны, а размерностями являются произвольные целые числа.

б) Получить из а) пример коммутативной группы E, наделенной структурами левого и правого векторных пространств над K, внешние законы которых перестановочны и которые имеют одинаковую конечную размерность, но при этом E содержит подгруппу F, устойчивую относительно обоих внешних законов на E и такую, что две индуцированные в F структуры векторного пространства имеют различные размерности.

4) Пусть K — тело, L — его подтело, K_L — тело K, рассматриваемое как правое векторное пространство над L, и $E=\mathscr{L}_L(K_L)$ — кольцо эндоморфизмов этого векторного пространства. Вследствие того, что левые умножения определяют в K структуру левого векторного пространства над K, внешний закон которого перестановочен с внешним законом пространства K_L, E оказывается канонически наделимым структурами левого и правого векторных пространств над K, внешние законы которых перестановочны (n° 7; см. главу II, § 5, n° 5 и упражнение 4). Сопряженное $(K_L)^*$ к K_L содержится в E; это — правое векторное подпространство над K и левое векторное подпространство над L (относительно структуры, получающейся путем сужения тела скаляров K структуры левого векторного пространства в E до L). В случае, когда L содержится в центре тела K, структуры векторного L-пространства в E, получающиеся путем сужения до L тела скаляров двух структур векторного K-пространства в E, совпадают.

Далее предполагается, что L содержится в центре тела K, а размерность K_L конечна и равна n.

а) Показать, что $(K_L)^*$ имеет размерность 1 при структуре правого векторного пространства над K. [Заметить, что $(K_L)^*$ имеет размерность n при структуре векторного пространства над L.]

б) Вывести, что в этом случае E есть n-мерное правое векторное пространство над K. [Показать, что если (a_i) — базис пространства K_L относительно L и u_0 — ненулевая линейная форма на K_L, то элементы $a_i u_0$ образуют в E базис для структуры правого векторного пространства над K.]

в) Пусть F — правое векторное пространство конечной размерности над K и F_L — векторное пространство над L, получающееся путем сужения его тела скаляров до L. Показать, что если u_0 — ненулевая линейная форма на K_L, то отображение $x' \to u_0 \circ x'$ пространства F^*, сопряженного к F (рассматриваемого как векторное пространство над L), на пространство $(F_L)^*$, сопряженное к F_L, является изоморфизмом F^* на $(F_L)^*$. [При доказательстве инъективности этого отображения использовать а).]

5) Пусть K — тело конечного ранга над своим центром Z и L — подтело этого тела, содержащее Z.

а) Показать, что структуры левого и правого векторных пространств в K относительно L имеют одинаковую размерность.

б) Показать, что свойства а), б) и в) из упражнения 4 еще сохраняются в этом случае. [Заметить, что если u_0 — ненулевая линейная форма на L_Z и v_0 — ненулевая линейная форма на K_L, то $(u_0 \circ v_0)\cdot\lambda = u_0 \circ (v_0 \cdot \lambda)$ описывает $(K_Z)^*$, когда λ описывает K, и воспользоваться упражнением 4в.]

6) Пусть A — кольцо, Γ — его центр, E — правый A-модуль, F — левый A-модуль, а E^* и F^* — их сопряженные модули. Отображение f модуля $E^* \otimes_\Gamma F^*$ в A называется *двояко линейным*, если $f(aw) = af(w)$ и $f(wa) = f(w)a$ для всех $w \in E^* \otimes_\Gamma F^*$ и $a \in A$. Показать, что существует, и притом единственное, Γ-линейное отображение φ модуля $E \otimes_A F$ в Γ-модуль L всех двояко линейных отображений $E^* \otimes_\Gamma F^*$ в A такое, что

$$(\varphi(x \otimes y))(x' \otimes y') = \langle x', x\rangle \langle y, y'\rangle.$$

При этом, если каждый из A-модулей E и F обладает конечным базисом, то φ есть биекция $E \otimes_A F$ на L.

ИСТОРИЧЕСКИЙ ОЧЕРК

К ГЛАВАМ II и III

(Римские цифры относятся к библиографии, помещенной в конце настоящего очерка.)

Линейная алгебра является одновременно и одной из древнейших, и одной из новейших отраслей математики. С одной стороны, еще у истоков математики мы находим задачи, решающиеся одним умножением или делением, т. е. вычислением одного из значений функции вида $f(x) = ax$ или нахождением решения уравнения вида $ax = b$; но это — типичные задачи линейной алгебры, и их невозможно ни рассматривать, ни даже корректно ставить, не «мысля линейно».

С другой стороны, не только эти вопросы, но почти всё касающееся уравнений первой степени уже давно отошло в область элементарного преподавания, когда современное развитие понятий тела, кольца, топологического векторного пространства и т. д. выявило все значение основных понятий линейной алгебры (например, двойственности); именно тогда был подмечен существенно линейный характер почти всей современной алгебры, одной из отличительных черт которой и является эта «линеаризация», и линейной алгебре было отведено подобающее ей место. Поэтому проследить историю ее развития с точки зрения, на которой мы стоим, было бы задачей столь же важной, сколь и трудной; и мы вынуждены будем ограничиться здесь замечаниями довольно общего характера.

Из предыдущего видно, что возникновение линейной алгебры, несомненно, было вызвано нуждами вычислителей-практиков. Так, например, во всех практических руководствах по арифметике, начиная с египетского папируса Райнда, через Ариабхатту, арабов, Леонардо Пизанского, неисчислимые «вычислительные книги» средних веков и эпохи Возрождения и вплоть до почитаемых в наших начальных школах, важную роль играют более или менее ясно высказанные тройное правило и правило ложного положения *); но они, быть может, никогда не были чем-либо иным, как извлечением для нужд практиков из более развитых научных теорий.

---

*) См. J. Tropfke, Geschichte der Elementar-Mathematik, т. I, 2-е изд., Berlin — Leipzig (W. de Gruyter), 1921, стр. 150—155.

Что касается математиков в собственном смысле, характер их исследований по линейной алгебре является функцией общей структуры их науки. В древнегреческой математике, как она изложена в «Началах» Евклида, были развиты две абстрактные теории линейного характера, а именно, с одной стороны, теория величин ((II), Книга V; см. Исторический очерк к главе IV «Общей топологии»), с другой — теория целых чисел ((II), Книга VII). У вавилонян мы находим методы, значительно более близкие к нашей элементарной алгебре; они умели решать, и притом весьма изящно ((I), стр. 181—183), системы уравнений первой степени. Тем не менее в течение весьма долгого времени прогресс линейной алгебры зависит главным образом от прогресса алгебраической техники, и в этом аспекте, чуждом настоящему очерку, его и следовало бы рассматривать; так, для сведения линейной системы к уравнению вида $ax = b$ достаточно, если речь идет лишь об одном неизвестном, знать правила (по существу, сформулированные уже Диофантом) перенесения членов уравнения из одной его части в другую и приведения подобных членов; имея же дело с несколькими неизвестными, достаточно, сверх того, уметь последовательно исключать их, пока не останется только одно. Поэтому в руководствах по алгебре вплоть до XVIII века, в том, что относится к первой степени, цель считалась достигнутой, как только изложены эти правила; что же касается системы с одинаковым числом уравнений и неизвестных (а другие системы и не рассматриваются), левые части которой не являются линейно независимыми формами, то неизменно довольствовались беглым замечанием, что это указывает на плохо поставленную задачу. В руководствах XIX века и даже некоторых более поздних эта точка зрения сохраняется и прогресс наблюдается лишь в обозначениях, позволивших записывать системы n уравнений с n неизвестными, и введении определителей, позволившем давать явные формулы решения этих систем в «общем случае»; этим прогрессом, честь которого принадлежала бы Лейбницу ((VII), стр. 239), если бы он развил и опубликовал свои идеи по этому поводу, мы обязаны главным образом математикам XVIII и начала XIX веков.

Но нам следует прежде рассмотреть различные идейные течения, гораздо более способствовавшие развитию линейной алгебры в том смысле, как мы ее понимаем, чем изучение систем линейных уравнений. Вдохновленный изучением Аполлония, Ферма (IVa), даже до Декарта (V), приходит к принципам аналитической геометрии, к идее классификации плоских кривых по их порядку (идее, которая, становясь постепенно привычной для всех математиков, может считаться окончательно усвоенной к концу XVII века) и выдвигает фундаментальный принцип, что уравнение первой степени представляет на плоскости прямую, а уравнение второй степени — коническое сечение,— принцип, из которого он сразу выводит «весьма красивые» следствия, относящиеся к геометрическим местам. В то же время он предлагает (IVб) классификацию задач на задачи определенные, задачи, сводящиеся к уравнению с двумя неизвестными, уравнению с тремя неизвестными и т. д., и добавляет: первые состоят в определении точки, вторые — линии или плоского места, следующие — поверхности, и т. д. (...*«такая задача состоит в разыскании не одной лишь точки или линии, но целой связан-*

ной с вопросом поверхности; отсюда и возникают пространственные места и так же для последующих», там же, стр. 186; здесь уже виден зародыш n-мерной геометрии). Этот отрывок, выдвигая принцип размерности в алгебре и алгебраической геометрии, намечает слияние алгебры и геометрии, целиком согласующееся с современными идеями, хотя, как известно, понадобилось более двух веков, прежде чем оно овладело умами.

Всё же эти идеи привели скоро к расцвету аналитической геометрии, достигшему всей своей полноты в XVIII веке в трудах Клеро, Эйлера, Крамера, Лагранжа и многих других. Линейный характер формул преобразования координат на плоскости и в пространстве, который не мог не заметить уже Ферма, отчетливо выступает, например, у Эйлера ((VIIIa), гл. II—III, и Append., гл. IV), основывающего на нем классификацию плоских кривых, а также поверхностей по их порядку (инвариантному именно вследствие линейности этих формул); это Эйлер ((VIIIa), гл. XVIII) вводит также слово «affinitas» («родство» *)) для обозначения отношения между кривыми, которые могут быть получены одна из другой преобразованием вида $x' = ax$, $y' = by$ (не замечая, однако, ничего геометрически инвариантного в этом определении, остающемся связанным со специальным выбором координатных осей). Несколько позже мы видим Лагранжа (IXa), посвящающего целый мемуар, долгое время пользовавшийся заслуженной известностью, типично линейным и полилинейным задачам трехмерной аналитической геометрии. К этому же времени в связи с линейной задачей, состоящей в разыскании плоской кривой, проходящей через заданные точки, оформляется, сначала несколько эмпирическим путем, понятие определителя у Крамера (X) и Безу (XI); развитое затем различными авторами, это понятие с его основными свойствами получает окончательный вид у Коши (XIII) и Якоби (XVIa).

С другой стороны, в то время как математики проявляли тенденцию несколько пренебрежительного отношения к уравнениям первой степени, решение дифференциальных уравнений представляло, напротив, главную задачу; естественно, что среди этих уравнений уже очень рано выделили линейные уравнения с постоянными или переменными коэффициентами и что их изучение способствовало выявлению значения линейности и всего с ней связанного. Это заметно уже у Лагранжа (IXб) и Эйлера (VIIIб), по крайней мере в том, что касается однородных уравнений; ибо эти авторы не считают нужным сказать, что общее решение неоднородного уравнения есть сумма частного решения и общего решения соответствующего однородного уравнения, и не делают из этого принципа никакого употребления; отметим также, что, утверждая, что общее решение однородного линейного уравнения n-го порядка есть линейная комбинация n частных решений, они не добавляют, что эти решения должны быть линейно независимыми, и не делают никаких попыток к выяснению этого последнего понятия; ясность в эти вопросы, как и в ряд других, внесли, по-видимому, лишь лекции Коши в Политехнической школе ((XIV), стр. 573—574). Но уже Лагранж (там же) вводит также (правда, лишь для вычислительных целей и без наименования) уравнение $L^*(y) = 0$.

*) В русской литературе — аффинность.— *Перев.*

сопряженное к линейному дифференциальному уравнению $L(y) = 0$,— типичный пример двойственности в силу соотношения

$$\int zL(y)\,dx = \int L^*(z)\,y\,dx,$$

справедливого для y и z, обращающихся в нуль на концах интервала интегрирования; еще точнее, мы видим здесь, за 30 лет до того, как Гаусс явно определил подстановку, сопряженную к линейной подстановке трех переменных, несомненно первый пример «функционального оператора» L^*, «сопряженного» к оператору L, заданного посредством билинейной функции (здесь интеграла $\int yz\,dx$).

В то же время, и снова с Лагранжем (IXв), линейные подстановки, прежде всего двух и трех переменных, сумели завоевать арифметику. Ясно, что множество значений функции $F(x, y)$, где x и y принимают все целые значения, не изменяется, когда x и y подвергаются произвольной линейной подстановке с целыми коэффициентами и определителем, равным 1; на этом фундаментальном замечании Лагранж основывает теорию представления чисел формами и приведения форм, а Гаусс одним шагом, всю дерзость которого нам стало трудно теперь оценить, выделяет понятия эквивалентности и класса форм (см. Исторический очерк к главе I); в этой связи он уясняет необходимость некоторых элементарных принципов, относящихся к линейным подстановкам, и, в частности, вводит понятие транспонированной, или сопряженной подстановки ((XIIа), стр. 304). Начиная с этого момента арифметическое и алгебраическое исследование квадратичных форм от двух, трех, а позже n переменных, тесно связанных с ними билинейных форм, а в более близкий нам период обобщение этих понятий на бесконечное число переменных образуют, вплоть до нашего времени, один из наиболее плодотворных источников прогресса линейной алгебры (см. Исторический очерк к главе IX).

Но, что является, быть может, еще более решительным прогрессом, в тех же «Исследованиях» (см. Исторический очерк к главе I) Гаусс создает теорию конечных коммутативных групп, встречающихся там в четырех различных видах, а именно: аддитивной группы целых чисел по (целому) модулю m, мультипликативной группы чисел, взаимно простых с m, по модулю m, группы классов бинарных квадратичных форм и, наконец, мультипликативной группы корней m-й степени из единицы; причем, как мы уже отмечали, Гаусс явно трактует все эти группы как коммутативные группы, или, лучше сказать, модули над $\mathbf{Z}$, изучает их строение, их отношения изоморфизма и т. д. На модуле «целых комплексных чисел» $a + bi$ он исследует позже бесконечный модуль над $\mathbf{Z}$, изоморфизм которого с (открытым им же в комплексной области) модулем периодов эллиптических функций, несомненно, не остался для него незамеченным; во всяком случае, эта идея уже явно появляется у Якоби, например в его знаменитом доказательстве невозможности функции с тремя периодами и в его взглядах на задачу обращения абелевых интегралов (XVIб), и вскоре приводит к теоремам Кронекера (см. Исторический очерк к главе VII «Общей топологии»).

Здесь к течениям, трассы, а иногда и извилины которых мы пытались проследить, примешалось еще одно, долгое время остававшееся подспудным. Как будет подробнее изложено в другом месте (см. Исторический очерк к главе IX), «чистая» геометрия в том смысле, как ее понимали в течение прошлого века, т. е. в основном проективная геометрия плоскости и пространства без использования координат, была создана в XVII веке Дезаргом (VI), идеи которого, оцененные в их истинном значении самим Ферма и использованные самим Паскалем, были затем забыты, отодвинутые в тень блестящими успехами аналитической геометрии; она вновь попала в честь к концу XVIII века стараниями Монжа, а затем Понселе и его соперников Шаля и Брианшона иногда умышленно и полностью очищенная от аналитических методов, иногда (особенно в Германии) тесно переплетенная с ними. Но, с какой бы точки зрения их ни рассматривать (синтетической или аналитической), проективные преобразования все же являются просто линейными подстановками проективных или «барицентрических» координат; конические сечения (в XVII веке), а позже поверхности второго порядка, проективная теория которых долгое время составляла основной предмет исследований этой школы, являются просто квадратичными формами, на тесную связь которых с линейной алгеброй мы уже выше указывали. К этим понятиям присоединяется понятие полярности; теория полюсов и поляр, также созданная Дезаргом, становится в руках Монжа и его последователей, вскоре под наименованием принципа двойственности, мощным инструментом преобразования геометрических теорем; если и не брать на себя смелость утверждать, что были замечены ее связи с сопряженными дифференциальными уравнениями,— это было сделано с опозданием (они были указаны Пинкерле в конце XIX века),— все же от математиков не укрылось — тому свидетель Шаль (XVII) — ее родство с понятием полярных сферических треугольников, введенным в сферическую геометрию Вьета ((III), стр. 418) и Снеллием в XVI веке. Но двойственность в проективной геометрии есть лишь один из аспектов двойственности векторных пространств с учетом модификаций, накладываемых переходом от аффинного пространства к проективному (являющемуся его факторпространством по отношению «скалярного умножения»).

XIX век, более чем какой-либо другой период нашей истории, был богат первоклассными математиками, и трудно на нескольких страницах, даже только в главных чертах, описать всё, что создало их руками слияние этих идейных течений. Между чисто синтетическими методами, с одной стороны, — этим родом Прокрустова ложа, на котором сами предавали себя пыткам их ортодоксальные адепты,— и аналитическими методами, связанными с произвольно навязанной пространству системой координат, скоро ощутили потребность в чем-то вроде геометрического исчисления, задуманного, но не созданного Лейбницем и в несовершенном виде намеченного Карно; сперва появляется сложение векторов, в неявной форме у Гаусса в его геометрическом представлении мнимых чисел и применении их к элементарной геометрии (см. Исторический очерк к главе VIII «Общей топологии»), далее развитое Беллавитисом под названием «метода эквиполленций» и принявшее свой окончательный вид у Грассмана, Мёбиуса и Гамильтона;

одновременно Мёбиус предлагает его вариант под названием «барицентрического исчисления», приспособленный к нуждам проективной геометрии (XVIII).

К тому времени, и теми же людьми, совершается возвещенный, как мы видели, еще Ферма переход от «обычных» плоскости и пространства к пространству n измерений, столь естественный (раз уж вступили на этот путь) и даже неизбежный, поскольку алгебраические факты, которые для двух или трех переменных, как и сами эти переменные, истолковываются в геометрических терминах, остаются такими же для любого числа переменных; поэтому налагать на употребление геометрического языка ограничение двумя или тремя измерениями было бы для математиков этого времени столь же стеснительным ярмом, как и то, которое всегда мешало грекам распространить понятие числа на отношения несоизмеримых величин. Поэтому язык и идеи, относящиеся к пространству n измерений, почти одновременно появляются повсеместно, неявно у Гаусса и отчетливо у математиков следующего поколения, а их бо́льшая или меньшая смелость в пользовании этим языком, быть может, определяется не столько их математическими склонностями, сколько философскими или даже чисто практическими соображениями. Во всяком случае, Кэли и Грассман к 1846 г. обращаются с этими понятиями с весьма большой непринужденностью (и притом, говорит Кэли в отличие от Грассмана ((XXIIa), стр. 321), «*не прибегая ни к каким метафизическим понятиям*»); Кэли постоянно держится весьма близко к аналитическому истолкованию и координатам, тогда как у Грассмана уже с самого начала, со сложения векторов в n-мерном пространстве, одерживает верх геометрический аспект, что приводит его к рассмотрениям, на которых мы позже остановимся.

Тем временем импульс, полученный от Гаусса, двумя разными путями побуждал математиков к изучению алгебр и гиперкомплексных систем. С одной стороны, не могли не появиться попытки расширить область вещественных чисел иным путем, чем введением «мнимой единицы» $i=\sqrt{-1}$, и, быть может, открыть так области, более обширные, чем область комплексных чисел, и столь же плодотворные. Сам Гаусс был убежден ((XIIб), стр. 178) в невозможности такого расширения, по крайней мере если пытаться сохранить основные свойства комплексных чисел, т. е., на современном языке, те свойства, которые делают множество этих чисел коммутативным телом; и под его влиянием или независимо современники Гаусса, по-видимому, разделяли это убеждение, обоснованное лишь значительно позднее в виде точной теоремы Вейерштрассом (XXIII). Но раз только умножение комплексных чисел интерпретируется вращениями в плоскости, желание распространить эту идею на пространство неизбежно ведет к рассмотрению некоммутативных умножений (поскольку вращения в пространстве образуют некоммутативную группу); это и явлется одной из идей, которыми руководствовался Гамильтон*) в своем открытии кватернионов (XX), первого примера некоммутативного тела.

---

*) См. интересное предисловие к его «Лекциям о кватернионах» (XX), где он излагает всю историю своего открытия.

Своеобразие этого примера (единственного, который — как показал позже Фробениус — можно было построить над полем вещественных чисел) несколько ограничило сферу его влияния, вопреки или, быть может, даже благодаря образованию школы фанатичных «кватернионистов» — странному явлению, повторившемуся позже вокруг творения Грассмана,— а затем популяризаторов, извлекших у Гамильтона и Грассмана то, что было названо «векторным исчислением». Отказ от ассоциативности несколько позже у Грейвса и Кэли, построивших «числа Кэли», не открывает интересных путей. Но после того, как Сильвестр ввел матрицы и (не давая ему наименования) явно определил ранг (XXI), тот же Кэли (XXIIб) создает матричное исчисление, не преминув заметить (существенный факт, впоследствии часто упускавшийся из виду), что матрица есть просто сокращенное обозначение линейной подстановки, такое же, в сущности, как гауссовское обозначение (a, b, c) формы $aX^2 + 2bXY + cY^2$. Впрочем, это было лишь одним из, несомненно наиболее интересных для нас, аспектов относящейся к определителям и всему с ними связанному обильной продукции Сильвестра и Кэли, ощетинившейся замысловатыми тождествами и внушительными вычислениями.

Грассман открывает также (среди прочего) одну алгебру над полем вещественных чисел, а именно внешнюю алгебру, за которой закрепилось его имя. Его творение, даже более раннее, чем творение Гамильтона (XIXа), и созданное в почти полном духовном одиночестве, долгое время оставалось мало известным, несомненно вследствие своей оригинальности, а также философского тумана, окутывающего его начало и сперва оттолкнувшего, например, Мёбиуса. Побуждаемый замыслами, аналогичными имевшимся у Гамильтона, но более широкими (и, как он скоро заметил, совпадавшими с замыслами Лейбница), Грассман строит обширное алгебраико-геометрическое здание, покоящееся на геометрической, или «внутренней» (уже почти аксиоматизированной), концепции n-мерного векторного пространства; из наиболее элементарных результатов, к которым он приходит, упомянем, например, определение линейной независимости векторов, размерности и основное соотношение $\dim V + \dim W = \dim (V + W) + \dim (V \cap W)$ (там же, стр. 209; см. (XIXб), стр. 21). Но главным образом внешнее, а затем внутреннее умножение поливекторов доставляют ему средства, с помощью которых он легко справляется сначала с задачами собственно линейной алгебры, а затем относящимися к евклидовой структуре, т. е. ортогональности векторов (где он находит недостающий ему эквивалент двойственности).

Другой путь изучения гиперкомплексных систем, открытый Гауссом, имеет своим отправным пунктом целые комплексные числа $a + bi$; вполне естествен переход от них к более общим алгебрам или гиперкомплексным системам над кольцом целых чисел $\mathbf{Z}$ или полем рациональных чисел $\mathbf{Q}$, прежде всего к тем, уже рассмотренным Гауссом, которые порождаются корнями из единицы, и далее к полнм алгебраических чисел и модулям целых алгебраических чисел. Указанные поля составляют главный предмет работ Куммера, а модулям целых алгебраических чисел посвящают свои исследования Дирихле, Эрмит, Кронекер, Дедекинд. В противоположность тому, что имеет место для алгебр над полем вещественных чисел, здесь не нужно отказываться

ни от каких характерных свойств коммутативных тел; этим и ограничиваются в течение всего XIX века. Но линейные свойства, например разыскание базиса целых чисел поля (необходимое для общего определения дискриминанта), играют во многих вопросах существенную роль, и, во всяком случае, у Дедекинда, методы принимают типично «гиперкомплексную» окраску; при этом сам Дедекинд, не ставя перед собой в общем виде проблему алгебр, осознает этот характер своих работ и то, что роднит их, например, с результатами Вейерштрасса, относящимися к гиперкомплексным системам над полем вещественных чисел ((XXIV), в частности том 2, стр. 1). В то же время определение строения мультипликативной группы единиц поля алгебраических чисел, осуществленное в знаменитых сообщениях Дирихле (XV) и почти одновременно также Эрмитом, оказалось в высшей степени подходящим для прояснения представлений о модулях над $\mathbf{Z}$, их системах образующих и их базисах, когда последние существуют. Затем понятие идеала, определенное Дедекиндом в полях алгебраических чисел (как модуля над кольцом целых чисел поля), в то время как эквивалентное понятие в кольцах полиномов (под наименованием «систем модулей») вводит Кронекер, дает первые примеры модулей над кольцами более общими, чем $\mathbf{Z}$; и теми же авторами, а затем Гильбертом постепенно на частных случаях выкристаллизовывается понятие группы с операторами с возможностью всегда построить, исходя из такой группы, модуль над надлежаще определенным кольцом.

В то же время арифметико-алгебраическое исследование квадратичных и билинейных форм и их «приведения» (или, что то же самое, матриц и их «инвариантов») приводит к открытию общих принципов решения систем линейных уравнений, принципов, которые из-за отсутствия понятия ранга ускользнули от Якоби *). Задачу решения системы линейных уравнений с целыми коэффициентами в целых числах рассматривает и разрешает сначала в частном случае Эрмит и затем во всей общности Смит (XXV); результаты последнего вновь получает лишь в 1878 г. Фробениус, в рамках обширной программы исследований, намеченной Кронекером, в которой принимает участие также Вейерштрасс; лишь попутно, в ходе этой работы, Кронекер придает окончательный вид теоремам о линейных системах с вещественными (или комплексными) коэффициентами, излагаемым также в одном малоизвестном руководстве, с характерной для него скрупулезной аккуратностью, знаменитым автором «Алисы в стране чудес»; Кронекер же не снисходит до публикации этих результатов, оставляя это своим коллегам и ученикам; само слово «ранг» ввел лишь Фробениус. В своих лекциях в Берлинском университете Кронекер (XXVI) и Вейерштрасс вводят также «аксиоматическое» определение определителя (как знакопеременной полилинейной функции n векторов n-мерного пространства, нормированной так, чтобы для единичной матрицы она принимала значение 1); оно равносильно определению, получающемуся

*) О классификации систем n уравнений с n неизвестными, определитель которых равен нулю, он говорит ((XVIa), стр. 370): «paullo prolixum videtur negotium» (ее разъяснение не было бы кратким).

из грассмановского исчисления, равно как и принятому в настоящем трактате; в своих лекциях Кронекер, не ощущая нужды в наименовании и в форме еще не внутренней, вводит тензорное произведение пространств и «кронекеровское» произведение матриц (линейную подстановку, индуцированную в тензорном произведении заданными линейными подстановками в его сомножителях).

Эти изыскания не следовало бы также отделять от теории инвариантов, созданной Кэли, Эрмитом и Сильвестром («инвариантивистской троицей», как говорил позже в своих письмах Эрмит) и являющейся с современной точки зрения прежде всего теорией представлений линейной группы. Здесь появляется, в качестве алгебраического эквивалента двойственности в проективной геометрии, различение между сериями когредиентных и контрагредиентных переменных, т. е. между векторами пространства и векторами сопряженного пространства; и тогда как раньше внимание обращалось в первую очередь на формы низких, а затем и произвольных степеней от двух и трех переменных, теперь не мешкая переходят к рассмотрению билинейных форм, а затем и полилинейных форм от нескольких серий «когредиентных» или «контрагредиентных» переменных, что равносильно введению тензоров; это осознается и становится общим достоянием, когда в 1900 г. под влиянием теории инвариантов Риччи и Леви-Чивита вводят в дифференциальную геометрию «тензорное исчисление» (XXVIII), приобретшее позже большую известность благодаря его использованию физиками-«релятивистами». Уже прогрессирующее взаимопроникновение теории инвариантов, дифференциальной геометрии и теории уравнений с частными производными (особенно так называемой проблемы Пфаффа и ее обобщений) постепенно приводит геометров сначала к рассмотрению знакопеременных билинейных дифференциальных форм, в частности «билинейного ковариантa» формы первой степени (введенного в 1870 г. Липшицем и затем изученного Фробениусом), а в завершение к созданию Э. Картаном (XXIX) и Пуанкаре (XXX) исчисления внешних дифференциальных форм. Пуанкаре вводит их, имея в виду образование интегральных инвариантов, как выражения, фигурирующие в кратных интегралах, тогда как Картан, несомненно руководствуясь своими исследованиями по алгебрам, вводит их более формальным способом. но также не упуская заметить, что алгебраическая часть его исчнсления тождественна с грассмановским внешним умножением (откуда и принятое им наименование указанных форм), и тем самым окончательно определяя истинное место творения Грассмана. Перевод внешних дифференциальных форм на язык тензорного исчисления непосредственно обнаруживает при этом их связь с антисимметрическими тензорами, что, если оставаться на чисто алгебраической точке зрения, показывает, что они так же относятся к знакопеременным полилинейным формам, как ковариантные тензоры — к произвольным полилинейным формам; эта сторона дела еще более проясняется современной теорией представлений линейной группы; ею обнаруживается, например, существенная тождественность определения определителей, данного Вейерштрассом и Кронекером, и определения, вытекающего из грассмановского исчисления.

Мы подходим так к современному периоду, когда аксиоматический метод и понятие структуры (вначале только чувствуемое, определенное же лишь

совсем недавно) позволяют разделить понятия, до того безнадежно переплетенные, формулировать то, что было неотчетливым или неосознанным, и доказать в присущей им общности теоремы, которые были известны лишь для частных случаев. Пеано, один из создателей аксиоматического метода и также один из первых математиков, оценивших значение творения Грассмана, дает в 1888 г. ((XXVII), гл. IX) аксиоматическое определение векторных пространств (конечной или бесконечной размерности) над полем вещественных чисел и, с вполне современным обозначением,— линейных отображений одного такого пространства в другое; несколько позже Пинкерле пытается развить применения так понимаемой линейной алгебры к теории функций, правда, в направлении, оказавшемся мало плодотворным; всё же его точка зрения позволяет ему усмотреть в «лагранжевском сопряженном» частный случай сопряженного линейного отображения — то, что вскоре еще более выявляется, притом не только для обыкновенных дифференциальных уравнений, но также для уравнений в частных производных, по мере выхода памятных работ Гильберта и его школы по гильбертовым пространствам и их применением к анализу. В связи с этими последними исследованиями Теплиц (XXXI), тоже вводя (но посредством координат) наиболее общее векторное пространство над полем вещественных чисел, делает фундаментальное замечание, что для доказательства основных теорем линейной алгебры не нужна теория определителей, что позволяет без труда распространить их на пространства бесконечной размерности; он отмечает также, что так понимаемая линейная алгебра естественно применима при любом основном поле.

С другой стороны, с введением Банахом в 1922 г. пространств, носящих теперь его имя *), встретились, правда в проблеме столь же топологической, сколь и алгебраической, пространства, не изоморфные своему сопряженному. Уже между конечномерным векторным пространством и его сопряженным нет «канонического» изоморфизма, т. е. определяемого его структурой, что давно нашло свое отражение в различении когредиентного и контрагредиентного. Тем не менее представляется несомненным, что различение пространства от его сопряженного окончательно утвердилось лишь после работ Банаха и его школы; в этих же работах была обнаружена важность понятия фактор-размерности. Что касается двойственности, или «ортогональности», между векторными подпространствами пространства и его сопряженного, то способ, которым ее формулируют ныне, представляет не только внешнюю аналогию с современной формулировкой основной теоремы теории Галуа (см. гл. V) или с понтрягинской двойственностью локально компактных коммутативных групп; последняя восходит к Веберу, который в 1886 г. в связи с арифметическими исследованиями заложил ее основы для конечных групп; «двойственность» между подгруппами и подполями в теории Галуа выявляется Дедекиндом и Гильбертом; а ортогональность векторных подпространств, очевидно, имеет своим источником прежде всего двойственность линейных

*) А именно полных нормированных векторных пространств над полем вещественных или комплексных чисел.

многообразий в проективной геометрии, а также понятие и свойства ортогональных многообразий в евклидовом или гильбертовом пространстве (откуда и ее наименование). В наше время все эти нити сплетаются воедино в руках таких алгебраистов, как Э. Нетер, Артин и Хассе, и таких топологов, как Понтрягин и Уитни (не без взаимных влияний, оказанных одними на других), и каждая из этих областей приобретает законченный вид, результаты чего изложены в настоящем трактате.

В то же время производится критическая проверка, имеющая своей целью исключить в каждом пункте предположения, не являющиеся действительно необходимыми и особенно те, которые преграждали бы путь тем или иным приложениям. Так подмечают возможность заменить в понятии векторного пространства тела кольцами и, создав общее понятие модуля, рассматривать сразу эти пространства, коммутативные группы, модули специального вида, уже исследовавшиеся Кронекером, Вейерштрассом, Дедекиндом, Штейницем, и даже группы с операторами и применять ко всем им, например, теорему Жордана — Гёльдера; в то же время посредством различения правых и левых модулей осуществляется переход к некоммутативному случаю, к чему вело современное развитие теории алгебр американской (Веддерборн, Диксон) и, особенно, немецкой (Э. Нетер, Артин) школой.

Наконец, в недавнее время проявляется последняя из тенденций, которую мы здесь должны отметить: линеаризация теории Галуа, в зародыше содержащаяся в теореме Дедекинда ((XXIV), том 3, стр. 29) о линейной независимости любых автоморфизмов поля, завершается Артином (XXXII) и вскоре распространяется современной школой алгебраической геометрии на любые расширения полей, а затем некоммутативных тел; в § 5 главы II мы дали теоремы, лежащие в основе систематического изложения этих методов, которое в дальнейшем найдет свое место в этом трактате.

БИБЛИОГРАФИЯ

(I) O. Neugebauer, Vorlesungen über Geschichte der antiken Mathematik, т. I: Vorgriechische Mathematik, Berlin (Springer), 1934. [Русск. перевод: О. Нейгебауэр, Лекции по истории античных математических наук, т. I: Догреческая математика, ОНТИ, М.— Л., 1937.]

(II) Euclidis Elementa, 5 тт., изд. J. L. Heiberg, Lipsae (Teubner), 1883—1888.

(II bis) T. L. Heath, The thirteen books of Euclid's Elements..., 3 тт., Cambridge, 1908.

(III) Francisci Vietae, Opera mathematica..., Lugduni Batavorum (Elzevir), 1646.

(IV) P. Fermat, Oeuvres, т. I, Paris (Cauthier-Villars), 1891: а) Ad locos planos et solidos Isagoge (стр. 91—110; франц. перевод, там же, т. III, стр. 85); б) Appendix ad methodum... (стр. 184—188; франц. перевод, там же, т. III, стр. 159).

(V) R. Descartes, La Géométrie, Leyde (Jan Maire), 1637 (= Oeuvres, éd. Ch. Adam et P. Tannery, т. VI, Paris (L. Cerf), 1902). [Русск. перевод: Рене Декарт, Геометрия, с приложением избранных работ П. Ферма и переписки Декарта, ОНТИ, М.—Л., 1938.]

(VI) G. Desargues, Oeuvres..., т. I, Paris (Leiber), 1864: Brouillon proiect d'une atteinte aux éuénemens des rencontres d'un cône auec un plan (стр. 103—230).

(VII) G. W. Leibniz, Mathematische Schriften, éd. C. I. Gerhardt, т. I, Berlin (Asher), 1849.

(VIIIa) L. Euler, Introductio in Analysin Infinitorum, т. 2dus, Lausannae, 1748 (= Opera Omnia (1), т. IX, Zürich — Leipzig — Berlin (O. Füssli et B. G. Teubner), 1945). [Русск. перевод: Леонард Эйлер, Введение в анализ бесконечных, т. II, Физматгиз, М., 1961.]

(VIIIб) L. Euler, Institutionum Calculi Integralis, т. 2dum, Petropoli, 1769 (= Opera Omnia (1), т. XII, Leipzig — Berlin (B. G. Teubner), 1914). [Русск. перевод: Леонард Эйлер, Интегральное исчисление, т. II, Гостехиздат, М., 1957.]

(IX) J.-L. Lagrange, Oeuvres, Paris (Gauthier-Villars), 1867—1892: a) Solutions analytiques de quelques problèmes sur les pyra

mides triangulaires, т. III, стр. 661—692; б) Solution de différents problèmes de calcul intégral, т. I, стр. 471; в) Recherches d'arithmétique, т. III, стр. 695—795.

(X) G. Cramer, Introduction à l'analyse des lignes courbes, Genève (Cramer et Philibert), 1750.

(XI) E. Bezout, Théorie générale des équations algébriques, Paris. 1779.

(XII) C. F. Gauss, Werke, Göttingen, 1870—1927: a) Disquisitiones arithmeticae, т. I. [Русск. перевод в: Карл Фридрих Гаусс, Труды по теории чисел, Изд. АН СССР, М., 1959.] б) Selbstanzeige zur Theoria residuorum biquadraticorum, Commentatio secunda, т. II, стр. 169—178.

(XIII) A.-L. Cauchy, Mémoire sur les fonctions qui ne peuvent obtenir que deux valeures égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment, J. Ec. Polytechn., вып. 17 (т. X) (1815), стр. 29—112 (= Oeuvres complètes (2), т. I, Paris (Gauthier-Villars), 1905, стр. 91—169).

(XIV) A.-L. Cauchy, в «Leçons de calcul différentiel et de calcul intégral, rédigées principialement d'après les méthodes de M. A.-L. Cauchy», par l'abbé Moigno, т. II, Paris, 1844.

(XV) P. L. Lejeune-Dirichlet, Werke, т. I, Berlin (G. Reimer), 1889, стр. 619—644.

(XVI) C. G. J. Jacobi, Gesammelte Werke, Berlin (G. Reimer), 1881—1891: a) De formatione et proprietatibus determinantium, т. III, стр. 355—392; б) De fractionibus duarum variabilium..., т. II, стр. 25—50.

(XVII) M. Chasles, Aperçu historique sur l'origine et le développement des méthodes en géométrie..., Bruxelles, 1837.

(XVIII) A. F. Möbius, Der baryzentrische Calcul..., Leipzig, 1827 (= Gesammelte Werke, т. I, Leipzig (Hirzel), 1885).

(XIX) H. Grassmann: a) Die lineale Ausdehnungslehre, ein neuer Zweig der Mathematik, dargestellt und durch Anwendungen auf die übrigen Zweige der Mathematik, wie auch auf die Statik, Mechanik, die Lehre vom Magnetismus und die Kristallonomie erläutert, Leipzig (Wigand), 1844 (= Gesammelte Werke, т. I, ч. 1, Leipzig (Teubner), 1894); б) Die Ausdehnungslehre, vollständig und in strenger Form bearbeitet, Berlin, 1862 (= Gesammelte Werke, т. I, ч. 2, Leipzig (Teubner), 1896).

(XX) W. R. Hamilton, Lectures on Quaternions, Dublin, 1853.

(XXI) J. J. Sylvester, Collected Mathematical Papers, т. I, Cambridge, 1904: № 25, Addition to the articles..., стр. 145—151 (= Phil. Mag., 1850).

(XXII) A. Cayley, Collected Mathematical Papers, Cambridge, 1889—1898: a) Sur quelques théorèmes de la géométrie de position, т. I, стр. 317—328 (= J. de Crelle, т. XXXI (1846), стр. 213—227);

б) A memoir on the theory of matrices, т. II, стр. 475—496 (= Phil. Trans., 1858).

(XXIII) K. Weierstrass, Mathematische Werke, т. II, Berlin (Mayer und Müller), 1895: Zur Theorie der aus n Haupteinheiten gebildeten complexen Grössen, стр. 311—332.

(XXIV) R. Dedekind, Gesammelte mathematische Werke, 3 тт., Braunschweig (Vieweg), 1930—1932.

(XXV) H. J. Smith, Collected Mathematical Papers, т. I, Oxford, 1894: On system of linear indeterminate equations and congruences, стр. 367 (= Phil. Trans., 1861).

(XXVI) L. Kronecker, Vorlesungen über die Theorie der Determinanten..., Leipzig (Teubner), 1903.

(XXVII) G. Peano, Calcolo geometrico secondo l'Ausdehnungslehre di Grassmann, preceduto dalle operazioni della logica deduttiva, Torino, 1888.

(XXVIII) G. Ricci et Levi-Civita, Méthodes de calcul différentiel absolu et leurs applications, Math. Ann., т. LIV, 1901, стр. 125.

XXIX) E. Cartan, Sur certaines expressions différentielles et le problème de Pfaff, Ann. scient. Ecole norm. super. (3), т. XVI, 1899, стр. 239—332.

(XXX) H. Poincaré, Les méthodes nouvelles de la mécanique céleste, т. III, Paris (Gauthier-Villars), 1899, гл. XXII.

(XXXI) O. Toeplitz, Ueber die Auflösung unendlichvieler linearer Gleichungen mit unendlichvielen Unbekannten, Rend. Circolo mat. Palermo, т. XXVIII, 1909, стр. 88—96.

(XXXII) E. Artin, Galois Theory..., Ann Arbor, Mich., 1942.

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

УКАЗАТЕЛЬ ТЕРМИНОВ