Л.А.СКОРНЯКОВ

ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1983

22.14
С 44
УДК 512

Скорняков Л. А. **Элементы общей алгебры.**— М.: Наука, 1983.—272 с.

Автор, по возможности, приближается к осуществлению идеи — привести по нетривиальной теореме из каждого раздела современной общей алгебры. В книге отражены следующие разделы: универсальные алгебры, структуры (решетки) и булевы алгебры, поля и тела, кольца и модули, группы и кольца Ли, упорядоченные и топологические алгебраические системы, категории. От читателя требуется знакомство с материалом, входящим в обязательный курс алгебры университетов и педагогических институтов.

Для преподавателей, аспирантов и студентов старших курсов математических факультетов университетов и пединститутов. Может быть использована при подготовке к кандидатскому экзамену по специальности «Математическая логика, алгебра и теория чисел».

Лев Анатольевич Скорняков

ЭЛЕМЕНТЫ ОБЩЕЙ АЛГЕБРЫ

Редакторы *Л. А. Койфман, Ф. И. Кизнер*
Технический редактор *В. Н. Кондакова*
Корректор *Н. Б. Румянцева*

ИБ № 12210

Сдано в набор 19.01.83. Подписано к печати 30.05.83. Формат 84×108¹/₃₂. Бумага тип. № 2. Литературная гарнитура. Высокая печать. Условн. печ. л. 14,28. Уч.-изд. л. 15,03. Тираж 11 500 экз. Заказ № 1220. Цена 1 р. 20 к.

Издательство «Наука» Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ордена Октябрьской Революции и ордена Трудового Красного Знамени Первая Образцовая типография имени А. А. Жданова Союзполиграфпрома при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. Москва, М-54, Валовая, 28

Отпечатано в типографии № 2 изд-ва «Наука»,
121099, Москва, Г-99, Шубинский пер., 10. Заказ № 2946.

С $\frac{1702030000-102}{053(02)-83}$ 29-83

СОДЕРЖАНИЕ

ПРЕДИСЛОВИЕ

Предлагаемая вниманию читателя книга ставит своей целью дать представление о важнейших разделах современной общей алгебры. Именно, дать представление, а не помочь изучить основы той или иной теории. Так, например, сходив в зоопарк, мы не изучим основ зоологии, но все-таки получим некоторое представление о животном мире нашей планеты. В соответствие с этой задачей было бы идеалом привести по одной нетривиальной теореме из каждой теории. Правда этот идеал, по-видимому, недостижим, тем более, что настоящее руководство имеет и другую задачу: охватить весь общеалгебраический материал, входящий в обязательную программу кандидатского экзамена по алгебре и не нашедший отражения в учебной литературе. Общее впечатление о содержании можно извлечь из названий глав и параграфов. Более точную информацию дают вводные абзацы глав. Для закрепления изученного материала в конце каждого параграфа предлагаются упражнения. Библиография, сопровождающая каждую главу, содержит, главным образом, монографии на русском языке, позволяющие более глубоко изучить затронутые в тексте теории. Иностранные источники приведены лишь в тех случаях, когда они посвящены тем или иным важным специальным вопросам, не нашедшим достаточно полного отражения в русскоязычной литературе. Автор воздерживается от исторических замечаний. Однако если какое-либо утверждение имеет установившееся название или традиционную связь с теми или иными именами, то формулировка сопровождается соответствующим указанием.

Эту книгу следует рассматривать как второй концентр общего алгебраического образования. Поэтому предполагается, что читатель знаком с алгеброй в объеме обязательного университетского курса. В частности, элементарные свойства основных алгебраических систем — полугрупп, групп, колец и модулей — считаются известными и часто используются без всяких ссылок. Если же ссылки

даются, то читатель, как правило, отсылается к учебному пособию автора (Скорняков Л. А. Элементы алгебры.— М.: Наука, 1980), хотя соответствующий материал, можно, разумеется, найти и в других учебниках (Кострикин А. И. Введение в алгебру.— М.: Наука, 1977; Куликов Л. Я. Алгебра и теория чисел.— М.: Высшая школа, 1979; Курош А. Г. Курс высшей алгебры.— М.: Наука, 1975). Книга автора цитируется как ЭА.

Если φ — отображение множества A в множество B, то образ элемента $a \in A$ обозначается как через $\varphi(a)$, так и через $a\varphi$. Последнее обозначение используется, главным образом, в тех случаях, когда рассматривается произведение отображений, ибо в книге принято, что $\varphi\psi$, где φ — отображение A в B, а ψ — отображение B в C,— это отображение A в C, определяемое равенством $a(\varphi\psi) = (a\varphi)\psi$ или, что то же самое, равенством $(\varphi\psi)(a) = \psi(\varphi(a))$ для каждого $a \in A$. Символ $\varphi\colon A \to B$ также используется для обозначения отображения множества A в множество B. Тождественное отображение множества A на себя обозначается через 1_A. Для обозначения мощности множества A используются обозначения $\operatorname{Card} A$ и $|A|$. Символы $\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$ и $\mathbf{C}$ обозначают множества натуральных, целых, рациональных, действительных и комплексных чисел соответственно. Как обычно, ссылка на теорему IV.2.3 означает, что имеется в виду теорема 3 из § 2 главы IV. Теорема 2.3 подразумевает теорему 3 из § 2 той же главы, а теорема 3 — теорему 3 из того же параграфа. Ссылка, например, на теорему 2(в) означает ссылку на утверждение (в) теоремы 2.

Отдельные главы книги были прочитаны В. А. Андрунакиевичем, Б. И. Арнаутовым, В. А. Артамоновым, Ю. А. Бахтуриным, А. Г. Григоряном, Е. Б. Кацовым, А. В. Михалевым, Ю. М. Рябухиным, Т. С. Фофановой и А. Л. Шмелькиным, сделавшими ряд весьма полезных замечаний. Немало замечаний сделал и тщательно работавший над текстом научный редактор Л. А. Койфман. Автор глубоко благодарен всем этим алгебраистам, а также Т. А. Гуровой, оказавшей большую помощь при подготовке рукописи.

ГЛАВА I

ЧАСТИЧНО УПОРЯДОЧЕННЫЕ МНОЖЕСТВА И ПОЛНЫЕ СТРУКТУРЫ

Понятие частично упорядоченного множества является одним из фундаментальных понятий современной математики и находит широкое применение как в самой математике, так и в ее приложениях. В частности, повсюду встречаются доказательства, использующие трансфинитную индукцию. В настоящей главе напоминаются основные понятия теории частично упорядоченных множеств, обсуждаются вопросы, связанные с условием минимальности, обосновывается метод трансфинитной индукции и учение о мощности. Наконец, устанавливаются некоторые свойства полных структур (решеток) и доказывается теорема о вложении любого частично упорядоченного множества в полную структуру, обобщающая хорошо известную конструкцию пополнения множества рациональных чисел сечениями.

§ 1. Трансфиниты

Напомним, что *отношением* на непустом множестве P называется подмножество ρ прямого произведения $P \times P$. Вместо $(a, b) \in \rho$ часто пишется $a \rho b$. Отношение $\leqslant$ на множестве P называется *порядком*, если:

1) $a \leqslant a$ для всех $a \in P$ (рефлексивность);

2) если $a \leqslant b$ и $b \leqslant c$, то $a \leqslant c$ (транзитивность);

3) если $a \leqslant b$ и $b \leqslant a$, то $a = b$ (антисимметричность).

Запись $a < b$ означает, что $a \leqslant b$ и $a \neq b$.

Порядок $\leqslant$ называется *тривиальным*, если $a \leqslant b$ в том и только в том случае, когда $a = b$.

Множество P называется *частично упорядоченным*, если оно непусто и на нем зафиксирован некоторый порядок. Множество с тривиальным порядком называется *тривиальным частично упорядоченным множеством*. Всякое подмножество частично упорядоченного множества, очевидно, является частично упорядоченным множеством относительно того же самого порядка. Отображение φ частично упорядоченного множества P в частично упорядоченное

множество P' называется *изотонным* [*антиизотонным*], если $a \leqslant b$ влечет $\varphi(a) \leqslant \varphi(b)$ [$\varphi(a) \geqslant \varphi(b)$].

Частично упорядоченные множества P и P' называются *изоморфными* [*антиизоморфными*], если существует изоморфизм [антиизоморфизм] P на P', т. е. такое взаимно однозначное отображение φ множества P на множество P', что $a \leqslant b$ имеет место тогда и только тогда, когда $\varphi(a) \leqslant \varphi(b)$ [$\varphi(a) \geqslant \varphi(b)$]. Для практических целей часто оказывается полезным

Предложение 1. *Если P и P' — частично упорядоченные множества, φ: $P \to P'$ — наложение и $a \leqslant b$ в P тогда и только тогда, когда $\varphi(a) \leqslant \varphi(b)$ [$\varphi(a) \geqslant \varphi(b)$] в P', то φ — изоморфизм* [*антиизоморфизм*] *частично упорядоченных множеств.*

Доказательство. Достаточно доказать, что φ — вложение. Но если a, $b \in P$ и $\varphi(a) = \varphi(b)$, то, по условию, $a \leqslant b$ и $b \leqslant a$, откуда $a = b$, в силу антисимметричности.

Элементы a и b частично упорядоченного множества называются *сравнимыми*, если имеет место $a \leqslant b$ или $b \leqslant a$. Два элемента тривиального частично упорядоченного множества, очевидно, сравнимы тогда и только тогда, когда они совпадают.

Если любые два элемента частично упорядоченного множества сравнимы, то оно называется *цепью* (или *линейно упорядоченным множеством*).

Элемент v частично упорядоченного множества P называется *наибольшим*, если $x \leqslant v$ для всех $x \in P$. Если же $u \leqslant x$ для всех $x \in P$, то элемент u называется *наименьшим*. Наибольший элемент часто называют *единицей*, а наименьший — *нулем*. Конечно, частично упорядоченное множество может не содержать ни нуля, ни единицы. Таким, в частности, будет неодноэлементное тривиальное частично упорядоченное множество. Однако более одного наибольшего элемента частично упорядоченное множество содержать не может. В самом деле, если v и v' — наибольшие элементы частично упорядоченного множества P, то $v \leqslant v'$ и $v' \leqslant v$, а, следовательно, $v = v'$ по свойству антисимметричности. Аналогично устанавливается единственность наименьшего элемента. Элемент w частично упорядоченного множества P называется *максимальным*, если из $w \leqslant x$ для некоторого $x \in P$ вытекает $x = w$. Если из $x \leqslant m$ для некоторого $x \in P$ следует, что $x = m$, то m называется *минимальным* элементом. Легко проверяется,

что всякий наибольший элемент является максимальным, а всякий наименьший элемент — минимальным. Обратное, вообще говоря, места не имеет. Так, например, в тривиальном частично упорядоченном множестве всякий элемент является как максимальным, так и минимальным.

Заметим, что определение наименьшего элемента получается из определения наибольшего элемента простой заменой символа $\leqslant$ на $\geqslant$. Точно таким же образом связаны понятия минимального и максимального элементов. Вообще, имея какое-либо высказывание о частично упорядоченном множестве и заменяя $\leqslant$ на $\geqslant$, получаем новое высказывание. Высказывания, связанные таким образом, называются *двойственными*.

Если A — непустое подмножество частично упорядоченного множества P, то *верхним* [*нижним*] *конусом* множества A называем множество всех таких элементов $x \in P$, что $a \leqslant x$ $[x \leqslant a]$ для всех $a \in A$. Верхним [нижним] конусом пустого множества будем считать само множество P. Верхний и нижний конусы множества A будем обозначать символами $A^{\triangle}$ и $A^{\triangledown}$ соответственно. Наименьший [наибольший] элемент верхнего [нижнего] конуса множества A (если он существует) называется *точной верхней* [*нижней*] *гранью множества* A. В частности, точной верхней [нижней] гранью пустого множества является наименьший [наибольший] элемент частично упорядоченного множества P. Точную верхнюю [нижнюю] грань множества A в частично упорядоченном множестве P будем обозначать $\sup_P A$ $[\inf_P A]$. Впрочем, индекс P часто будет опускаться. Подчеркнем, что $\sup_P A$ и $\inf_P A$ (если они существуют) — однозначно определенные элементы множества P, ибо, как было отмечено выше, $A^{\triangle}$ $[A^{\triangledown}]$ содержит не более одного наименьшего [наибольшего] элемента. Примеры, иллюстрирующие введенные понятия, можно найти, например, в ЭА, гл. II, § 7. Определение точной верхней грани множества A можно перефразировать так: $u = \sup A$ в том и только в том случае, если $u \geqslant a$ для всех $a \in A$ и $x \geqslant u$ всякий раз, когда $x \geqslant a$ для всех $a \in A$. Аналогичную перефразировку допускает и определение точной нижней грани.

Трансфинитная индукция базируется на следующем факте:

Теорема 1. *Следующие свойства частично упорядоченного множества P эквивалентны*:

(1) (условие минимальности). *Всякое непустое подмножество множества P является частично упорядоченным множеством, содержащим минимальные элементы.*

(2) (условие индуктивности). *Если все минимальные элементы множества P обладают некоторым свойством $\mathscr{E}$ и из того, что все элементы x из P, удовлетворяющие условию $x < a$, обладают свойством $\mathscr{E}$, вытекает, что элемент a также обладает свойством $\mathscr{E}$, то свойством $\mathscr{E}$ обладают все элементы множества P.*

(3) (условие обрыва убывающих цепей). *Для всякой цепи*

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_k \geqslant \ldots$$

элементов из P найдется такой номер n, что

$$a_n = a_{n+1} = a_{n+2} = \ldots$$

Доказательство. (1)$\Rightarrow$(2). Допустим, что выполнены посылки условия индуктивности, и рассмотрим множество M всех элементов из P, не обладающих свойством $\mathscr{E}$. Если заключение условия (2) места не имеет, то M не пусто. Ввиду (1) в M имеется минимальный элемент a. По условию этот элемент не может быть минимальным элементом множества P. Если $x < a$, то $x \notin M$, и, следовательно, x обладает свойством $\mathscr{E}$ по условию. Противоречие.

(2)$\Rightarrow$(3). Условимся считать, что элемент $a \in P$ обладает свойством $\mathscr{E}$, если всякая убывающая цепь, начинающаяся с элемента a, обрывается, т. е. удовлетворяет условию (3). Всякий минимальный элемент $m \in P$ обладает свойством $\mathscr{E}$, так как для соответствующей цепи обязательно

$$m = a_1 = a_2 = \ldots$$

Если $a \in P$ таков, что все $x < a$ обладают свойством $\mathscr{E}$, то рассмотрим цепь

$$a \geqslant a_1 \geqslant a_2 \geqslant \ldots$$

Если знаки равенства стоят не всюду, то найдем такой номер i, что $a = a_1 = \ldots = a_{i-1}$ и $a_{i-1} > a_i$. Но тогда элемент a_i обладает свойством $\mathscr{E}$, т. е. цепь

$$a_i \geqslant a_{i+1} \geqslant \ldots,$$

а, значит, и цепь

$$a_1 \geqslant \ldots \geqslant a_i \geqslant a_{i+1} \geqslant \ldots$$

обрывается. Таким образом, элемент a обладает свойством $\mathscr{E}$. Ввиду (2) все элементы из P обладают свойством $\mathscr{E}$, а это и означает, что P удовлетворяет условию (3).

(3)$\Rightarrow$(1). Допустим, что непустое подмножество M множества P является частично упорядоченным множеством без минимальных элементов. Выберем в качестве a_1 произвольный элемент из M и допустим, что построена цепь

$$a_1 > a_2 > \ldots > a_n$$

элементов из M. Так как a_n не минимален в M, то в M существует элемент $a_{n+1} < a_n$. Таким образом, возникает бесконечная цепь $a_1 > a_2 > \ldots > a_n > \ldots$, не удовлетворяющая условию (3).

Цепь, удовлетворяющая условию минимальности (а значит, и остальным условиям теоремы 1), называется *вполне упорядоченным множеством*. Элементы вполне упорядоченного множества носят название *трансфинитов* или *трансфинитных чисел*. Вполне упорядоченным множеством является всякая конечная цепь. Естественным образом упорядоченное множество натуральных чисел также вполне упорядочено. Множество всех целых чисел не является вполне упорядоченным относительно естественного порядка, так как оно не имеет наименьшего элемента. Однако оно становится вполне упорядоченным, если установить порядок следующим образом:

$$1 < 2 < 3 < \ldots < 0 < -1 < -2 < -3 < \ldots$$

Другим примером не вполне упорядоченной цепи служит отрезок действительных чисел $[0, 1]$.

Из определения вполне упорядоченного множества вытекает, что оно всегда содержит наименьший элемент 0. Последующие элементы естественно обозначать через 1, 2, ... и т. д. Если α — некоторый трансфинит, то нижний конус α^{∇}, из которого удален элемент α, называется *начальным отрезком* и обозначается через $[0, \alpha)$. Символ $[0, 0)$ понимается как пустое множество. Если $\alpha \neq 0$ и начальный отрезок $[0, \alpha)$ не содержит наибольшего элемента, то трансфинит α называется *предельным*. Примером предельного трансфинита может служить число 0 в рассмотренном выше вполне упорядоченном множестве целых чисел. Для всякого трансфинита α среди трансфинитов верхнего конуса α^{Δ}, отличных от α, существует наименьший, который будем обозначать через $\alpha + 1$.

Предложение 2. *Если α — предельный трансфинит, то*

$$[0, \alpha) = \bigcup_{\beta<\alpha} [0, \beta).$$

Доказательство. Если $\gamma \in [0, \alpha)$, то, поскольку между γ и $\gamma+1$ элементов нет, $\gamma+1 \leqslant \alpha$. Однако равенство, в силу предельности α, невозможно. Таким образом,

$$\gamma \in [0, \gamma+1) \subseteq \bigcup_{\beta<\alpha} [0, \beta), \text{ т. е. } [0, \alpha) \subseteq \bigcup_{\beta<\alpha} [0, \beta).$$

Обратное включение очевидно.

Предложение 3. *Если Q — вполне упорядоченное множество и $\Xi \subseteq Q$, то или $\bigcup_{\xi\in\Xi} [0, \xi) = Q$, или $\bigcup_{\xi\in\Xi} [0, \xi) = [0, \alpha)$ для некоторого $\alpha \in Q$.*

Доказательство. Положим $Q' = \bigcup_{\xi\in\Xi} [0, \xi)$. Если $Q' \neq Q$, то множество $Q \setminus Q'$ не пусто и, следовательно, содержит наименьший элемент α. Если $\alpha \leqslant \gamma$, где $\gamma \in Q'$, то $\gamma \in [0, \xi)$ для некоторого $\xi \in \Xi$. Следовательно, $\alpha \leqslant \gamma < \xi$, откуда $\alpha \in Q'$, вопреки выбору элемента α. Таким образом, $Q' \subseteq [0, \alpha)$. Если же $\beta < \alpha$, то $\beta \in Q'$, в силу выбора элемента α, т. е. $[0, \alpha) \subseteq Q'$.

Примем в качестве аксиомы следующее утверждение:

Аксиома о полном упорядочении. *На всяком непустом множестве можно задать порядок, превращающий его во вполне упорядоченное множество.*

Теорема 2 (лемма Куратовского — Цорна). *Если верхний конус любой цепи частично упорядоченного множества P не пуст, то P содержит максимальные элементы.*

Доказательство. В соответствии с общим определением назовем цепь C частично упорядоченного множества P *максимальной*, если для всякого элемента x из P, не принадлежащего C, подмножество $C \cup \{x\}$ уже не является цепью. Пусть $\leqslant$ — порядок на P.

Лемма (теорема Хаусдорфа). *Всякая цепь любого частично упорядоченного множества может быть вложена в максимальную цепь.*

Для доказательства рассмотрим цепь C в частично упорядоченном множестве P. Если $C = P$, то все доказано. В противном случае рассмотрим множество $L = P \setminus C$ и, воспользовавшись аксиомой о полном упорядочении, зададим на нем порядок $\trianglelefteq$, превращающий его во вполне упорядоченное множество. Будем говорить, что трансфинит $\alpha \in L$ обладает свойством $\mathcal{E}$, если существует

цепь C_α, обладающая следующими свойствами: а) $C \subseteq C_\alpha$; б) $(\gamma \in C_\alpha) \Leftrightarrow (\gamma \trianglelefteq \alpha$ и γ сравним со всеми элементами из $C \cup (C_\alpha \cap [0, \gamma))$ в смысле порядка $\leqslant$). Для наименьшего трансфинита $0 \in L$ положим

$$C_0 = \begin{cases} C, \text{ если } 0 \text{ не сравним с каким-либо } c \in C; \\ C \cup \{0\} \text{ в противном случае.} \end{cases}$$

Ясно, что 0 автоматически обладает свойством $\mathscr{E}$. Допустим, что все трансфиниты, меньшие α, обладают свойством $\mathscr{E}$. Если $\gamma \trianglelefteq \beta \triangleleft \alpha$, то, ввиду б), $C_\gamma \subseteq C_\beta$. Поэтому множество $\bar{C} = \bigcup\limits_{\beta \triangleleft \alpha} C_\beta$ является цепью. Положим

$$C_\alpha = \begin{cases} \bar{C}, \text{ если } \alpha \text{ не сравним с каким-либо } \bar{c} \in \bar{C} \text{ в смысле порядка } \leqslant. \\ \bar{C} \cup \{\alpha\} \text{ в противном случае.} \end{cases}$$

Этим, как легко видеть, показано, что трансфинит α обладает свойством $\mathscr{E}$. Так как, в силу теоремы 1, множество L удовлетворяет условию индуктивности, то свойством $\mathscr{E}$ обладают все трансфиниты из L. Другими словами, цепи C_α существуют для всех $\alpha \in L$. Положим

$$Q = \bigcup_{\alpha \in L} C_\alpha.$$

Ясно, что Q — цепь. Если она не максимальная, то для некоторого $\xi \in L \setminus Q$ множество $Q \cup \{\xi\}$ также является цепью. Однако $\xi \notin C$, и, следовательно, ξ является некоторым трансфинитом из L, причем $\xi \notin C_\xi$. Из условия б) вытекает, что ξ не сравним с некоторым элементом из Q. Это, однако, противоречит тому, что $Q \cup \{\xi\}$ — цепь.

Пусть теперь частично упорядоченное множество P удовлетворяет посылкам теоремы 2. Одноэлементное множество $\{a\}$, где $a \in P$, является цепью, которую, в силу леммы, можно вложить в максимальную цепь C. По условию существует элемент $c \in C^\Delta$. Если c не является максимальным элементом частично упорядоченного множества P, то $c < x$ для некоторого $x \in P$. Конечно, $x \in C^\Delta \setminus C$, и, следовательно, $C \cup \{x\}$ — цепь, что противоречит максимальности цепи C.

Теорема 3 (аксиома выбора). *Для всякого непустого множества $\mathfrak{M}$ существует такое отображение φ множества $2^{\mathfrak{M}}$ всех подмножеств множества $\mathfrak{M}$ в множество $\mathfrak{M}$, что $\varphi(A) \in A$ для всех непустых $A \subseteq \mathfrak{M}$.*

Доказательство. Если $\mathfrak{M}$ — некоторое непустое множество, то по аксиоме о полном упорядочении его можно считать вполне упорядоченным. Нетрудно заметить, что отображение φ, ставящее в соответствие каждому непустому подмножеству A его первый элемент, удовлетворяет требованиям теоремы.

Можно доказать, что аксиома о полном упорядочении может быть выведена как из аксиомы выбора, так и из леммы Куратовского—Цорна (см., например, Скорняков Л. А. Элементы теории структур.— М.: Наука, 1982, § 2, теорема 3).

Напомним, что *прямым произведением* непустого семейства непустых множеств $\{P_\iota \mid \iota \in \mathfrak{I}\}$ называется множество всех отображений a множества $\mathfrak{I}$ в объединение $\bigcup_{\iota \in \mathfrak{I}} P_\iota$, ставящих в соответствие каждому индексу ι элемент $a_\iota \in P_\iota$. Существование таких функций вытекает из теоремы 3, примененной к множеству $\bigcup_{\iota \in \mathfrak{I}} P_\iota$. Отображение a часто изображают в виде строки

$$(\ldots, a_\iota, \ldots),$$

ι-й координатой которой служит элемент $a_\iota \in P_\iota$.

Упражнения

1. Элемент, являющийся минимальным и максимальным одновременно, не сравним ни с каким отличным от него элементом.

2. Если a и b — максимальные элементы, то $\sup\{a, b\}$ существует тогда и только тогда, когда $a = b$.

3. Доказать, что $\inf\limits_i \left(\sup\limits_j \{x_{ij}\}\right) \geqslant \sup\limits_j \left(\inf\limits_i \{x_{ij}\}\right)$, предполагая, что обе части этого неравенства существуют.

4. Сформулировать и доказать теорему, двойственную теореме 1. Замечание. Условия, двойственные условиям минимальности и обрыва убывающих цепей, называются *условиями максимальности* и *обрыва возрастающих цепей* соответственно.

5. Если трансфинитy α предшествует бесконечное множество элементов, то существует такой предельный трансфинит $\alpha_0 \leqslant \alpha$, что интервал $[\alpha_0, \alpha]$ содержит лишь конечное число элементов.

6. Если цепь C и цепь, двойственная ей, вполне упорядочены, то C конечна.

7. Если цепь не вполне упорядочена, то она содержит подцепь, двойственную натуральному ряду.

8. Если частично упорядоченное множество не содержит ни бесконечных цепей, ни бесконечных тривиальных частично упорядоченных подмножеств, то оно конечно.

9. Доказать эквивалентность следующих свойств частично упорядоченного множества P: а) P удовлетворяет условию минимальности и не содержит бесконечных тривиальных частично упорядо-

ченных подмножеств; б) никакое бесконечное подмножество множества P не удовлетворяет условию максимальности.

10. Доказать, что лемма Куратовского—Цорна равносильна соответствующему утверждению, сформулированному для вполне упорядоченных цепей.

11. Пусть L — непустое множество подмножеств некоторого множества $\mathfrak{M}$, причем подмножество A множества $\mathfrak{M}$ принадлежит L тогда и только тогда, когда L содержит все конечные подмножества A. Рассматривая L как частично упорядоченное множество относительно включения, доказать, что оно содержит максимальные элементы.

§ 2. Учение о мощности

Решающим фактом, обеспечивающим возможность сравнивать множества, является:

Предложение 1 (теорема о сравнении вполне упорядоченных множеств). *Для двух вполне упорядоченных множеств P и P' осуществляется одна и только одна из следующих возможностей*:

(1) *P изоморфно P'*;

(2) *P изоморфно начальному отрезку множества P'*;

(3) *P' изоморфно начальному отрезку множества P.*

Доказательство. Рассмотрим вполне упорядоченное множество $\overline{P}$, полученное присоединением к P нового элемента Ω, стоящего после всех элементов из P. Аналогичным добавлением элемента Ω' к множеству P' получим вполне упорядоченное множество $\overline{P'}$. Ясно, что $P=[0, \Omega)$ и $P'=[0, \Omega')$.

Лемма 1. *Если θ — изоморфизм вполне упорядоченного множества Q в себя, то $\theta(x)\geqslant x$ для всех $x\in Q$.*

Действительно, положим $S=\{s \mid s\in Q,\ \theta(s)<s\}$. Если лемма неверна, то множество S не пусто. Если a — наименьший элемент множества S, то $\theta(a)<a$ и, следовательно, $\theta(a)\notin S$. Отсюда

$$\theta(\theta(a))\leqslant\theta(a)\leqslant\theta(\theta(a)),$$

т. е. $\theta(a)=\theta(\theta(a))$, что ввиду $a\neq\theta(a)$ противоречит взаимной однозначности отображения θ.

Лемма 2. *Вполне упорядоченное множество не может быть изоморфно своему начальному отрезку.*

В самом деле, если θ — изоморфизм вполне упорядоченного множества Q на его начальный отрезок $[0, a)$, то $\theta(a)<a$, вопреки лемме 1.

Лемма 3. *Пусть Q — вполне упорядоченное множество, $a \in Q$ и φ — изоморфизм множества $[Q$ на начальный отрезок $[0, b')$ вполне упорядоченного множества Q'. Если ψ — изоморфизм начального отрезка $[0, a)$ на начальный отрезок $[0, a')$ множества Q', то $a' < b'$ и $\psi(x) = \varphi(x)$ для всех $x \in [0, a)$.*

В самом деле, допустим, что $a' \geqslant b'$. Тогда

$$\psi^{-1}([0, a')) = [0, a) \subsetneq Q,$$

откуда

$$\varphi(\psi^{-1}([0, a'))) \subsetneq \varphi(Q) = [0, b') \subseteq [0, a').$$

Таким образом, последовательное применение отображений ψ^{-1} и φ осуществляет изоморфизм вполне упорядоченного множества $[0, a')$ на свой начальный отрезок, что невозможно в силу леммы 2. Итак, $a' < b'$. Если, далее, $\varphi(x) \neq \psi(x)$ для некоторого $x < a$, то $\psi(x) < a' < b'$ и, следовательно, $\psi(x) = \varphi(y)$, где $x \neq y < a$. Последовательное применение отображений φ и ψ^{-1} осуществляет изоморфизм отрезка $[0, y)$ на отрезок $[0, x)$. По лемме 2, $x = y$. Противоречие.

Приступая к доказательству теоремы, рассмотрим множество S всех таких трансфинитов σ множества $\overline{P}$, что отрезок $[0, \sigma)$ не допускает изоморфизма ни на какой начальный отрезок множества $\overline{P}'$. Если $S = \varnothing$, то имеет место случай (1) или (2). Если $S \neq \varnothing$, то множество S содержит наименьший элемент α. Ясно, что $\alpha \neq 0$. Если $\alpha - 1$ существует, то существует изоморфизм φ отрезка $[0, \alpha - 1)$ на отрезок $[0, \beta')$ множества $\overline{P}'$. Если $\beta' = \Omega'$, то имеет место случай (3). Если это не так, то существует трансфинит $\beta' + 1$. Поэтому, положив

$$\overline{\varphi}(\xi) = \begin{cases} \varphi(\xi), & \text{если } \xi < \alpha - 1, \\ \beta', & \text{если } \xi = \alpha - 1, \end{cases}$$

получим изоморфизм $\overline{\varphi}$ отрезка $[0, \alpha)$ на отрезок $[0, \beta' + 1)$, что противоречит выбору α. Обратимся к случаю, когда α — предельный трансфинит. Тогда, согласно предложению 1.2,

$$[0, \alpha) = \bigcup_{\beta < \alpha} [0, \beta).$$

По выбору α для каждого β существует изоморфизм φ_β

отрезка $[0, \beta)$ на отрезок $[0, \beta')$ множества $\overline{P}'$. Поскольку $\Omega' \notin \bigcup [0, \beta')$, то, в силу предложения 1.3,

$$\bigcup_{\beta < \alpha} [0, \beta') = [0, \alpha')$$

для некоторого $\alpha' \in \overline{P}'$. Если $\xi < \alpha$, то $\xi + 1 < \alpha$ и можно положить $\varphi(\xi) = \varphi_{\xi+1}(\xi)$. Ясно, что φ отображает $[0, \alpha)$ в $[0, \alpha')$. Более того, если $\xi' \in [0, \alpha')$, то для некоторого $\beta < \alpha$ имеем $\xi' \in [0, \beta')$. Ввиду леммы 3, для некоторого $\xi \in [0, \beta)$ получаем

$$\xi' = \varphi_\beta(\xi) = \varphi_{\xi+1}(\xi) = \varphi(\xi),$$

т. е. φ оказывается наложением. Если, далее $\xi \leqslant \eta$, то, ввиду леммы 3,

$$\varphi(\xi) = \varphi_{\xi+1}(\xi) = \varphi_{\eta+1}(\xi) \leqslant \varphi_{\eta+1}(\eta) = \varphi(\eta).$$

Если же $\varphi(\xi) \leqslant \varphi(\eta)$, то по тем же соображениям

$$\varphi_{\eta+1}(\xi) = \varphi_{\xi+1}(\xi) = \varphi(\xi) \leqslant \varphi(\eta) = \varphi_{\eta+1}(\eta),$$

откуда $\xi \leqslant \eta$. В силу предложения 1.1, φ — изоморфизм отрезка $[0, \alpha)$ на отрезок $[0, \alpha')$. Если $\alpha' = \Omega'$, то имеет место случай (3). Если же $\alpha' < \Omega'$, то возникает противоречие с выбором α. Этим доказано, что по крайней мере один из случаев (1)—(3) имеет место. Из леммы 2 легко вывести, что случай (1) не совместим ни со случаем (2), ни со случаем (3). Если же одновременно имеют место случаи (2) и (3), то последовательное выполнение указанных там изоморфизмов позволяет получить изоморфизм множества P на его начальный отрезок, что опять противоречит лемме 2.

Предложение 2 (теорема Кантора—Бернштейна). *Если существуют взаимно однозначные отображения множества A на подмножество множества B и множества B на подмножество множества A, то существует взаимно однозначное отображение множества A на множество B.*

Доказательство. Последовательное осуществление отображений, указанных в формулировке, дает взаимно однозначное отображение θ множества A на свое подмножество. Пусть φ — упомянутое в формулировке отображение множества B в A. Положим $A_0 = A$ и $A_1 = \varphi(B)$. Конечно, можно считать, что $A_1 \subset A_0$. Далее, положим

$A_i = \theta(A_{i-2})$, $i = 2, 3, \ldots$, и $D = \bigcap_{i=1}^{\infty} A_i$. Ясно, что

$$A_0 \supset A_1 \supset A_2 \supset \ldots,$$

$$A = D \cup \left[\bigcup_{i=0}^{\infty} (A_{2i} \setminus A_{2i+1})\right] \cup \left[\bigcup_{i=1}^{\infty} (A_{2i-1} \setminus A_{2i})\right],$$

$$A_1 = D \cup \left[\bigcup_{i=0}^{\infty} (A_{2i+2} \setminus A_{2i+3})\right] \cup \left[\bigcup_{i=1}^{\infty} (A_{2i-1} \setminus A_{2i})\right],$$

причем объединяемые множества в последних двух равенствах попарно не пересекаются. Так как $A_{2i} \setminus A_{2i+1}$ отображаются на $A_{2i+2} \setminus A_{2i+3}$ при помощи θ, легко построить взаимно однозначное отображение ψ множества A на множество A_1. Поэтому последовательное осуществление отображений ψ и φ^{-1} дает искомое отображение A на B.

Множества A и B называются *эквивалентными*, если существует взаимно однозначное отображение множества A на множество B.

Теорема 1 (теорема о сравнении множеств). *Для любых двух множеств A и B существует одна и только одна из следующих возможностей*:

(1) *A эквивалентно B*;

(2) *A эквивалентно подмножеству множества B, но B не эквивалентно никакому подмножеству множества A*;

(3) *B эквивалентно подмножеству множества A, но A не эквивалентно никакому подмножеству множества B.*

Доказательство. Из аксиомы о полном упорядочении и предложения 1 вытекает или справедливость одного из свойств (1)—(3), или же выполнение условий предложения 2. В последнем случае выполнено условие (1). Попарная несовместимость высказанных утверждений очевидна.

Теорема 1 служит основанием для построения учения о *мощности множеств*. В случае (1) говорят, что мощности множеств A и B равны и пишут $\operatorname{Card} A = \operatorname{Card} B$, в случае (2)—что мощность множества A меньше мощности множества B (в записи $\operatorname{Card} A < \operatorname{Card} B$), а в случае (3), что мощность множества B меньше мощности множества A. Подчеркнем, что этим не определяется само понятие мощности, а только обеспечивается возможность сравнивать множества по их мощности. Легко проверить, что для конечных множеств сравнение по мощности равносильно сравнению по числу элементов.

Множества, эквивалентные множеству натуральных чисел, называются *счетными*. Символически счетность множества A записывается как $\operatorname{Card} A = \aleph_0$.

Установим некоторые результаты о мощности, часто используемые в алгебраических рассуждениях.

Предложение 3. *Пусть A, B, C — множества. Тогда*:

(а) *если* $\operatorname{Card} A \leqslant \operatorname{Card} B$ *и* $\operatorname{Card} B \leqslant \operatorname{Card} C$, *то* $\operatorname{Card} A \leqslant \operatorname{Card} C$;

(б) *если* $\operatorname{Card} A \leqslant \operatorname{Card} B$ *и* $\operatorname{Card} B \leqslant \operatorname{Card} A$, *то* $\operatorname{Card} A = \operatorname{Card} B$;

(в) *если* $\operatorname{Card} A \leqslant \operatorname{Card} B$, *то* $\operatorname{Card}(A \times C) \leqslant \operatorname{Card}(B \times C)$;

(г) *если A бесконечно*, $\operatorname{Card} B = \aleph_0$ *и* $A \cap B = \varnothing$, *то* $\operatorname{Card} B \leqslant \operatorname{Card} A$ *и* $\operatorname{Card}(A \cup B) = \operatorname{Card} A$.

Доказательство. (а) Условие означает, что существуют взаимно однозначные отображения множеств A и B на подмножества множеств B и C соответственно. Последовательное применение этих отображений отображает множество A на подмножество множества C, что и требовалось.

(б) Вытекает из предложения 2.

(в) Если φ — взаимно однозначное отображение множества A на подмножество B' множества B, то, положив $\psi(x, y) = (\varphi(x), y)$ для всех $x \in A$ и $y \in C$, получим нужное отображение множества $A \times C$ на подмножество $B' \times C$ множества $B \times C$.

(г) Считая $B = \{1, 2, \ldots\}$, выберем $\varphi(1) \in A$. Если выбраны различные элементы $\varphi(1), \ldots, \varphi(n)$, то $A \setminus \{\varphi(1), \ldots, \varphi(n)\}$ не пусто и, следовательно, в A можно выбрать элемент $\varphi(n+1) \neq \varphi(1), \ldots, \varphi(n)$. Тем самым построено взаимно однозначное отображение множества B на подмножество множества A, т. е. $\operatorname{Card} B \leqslant \operatorname{Card} A$. Далее определим взаимно однозначное отображение ψ множества $A \cup B$ на A, положив

$$\psi(x) = \begin{cases} \varphi(2k), & \text{если } x = \varphi(k), \\ \varphi(2k-1), & \text{если } x = k \in B, \\ x, & \text{если } x \in A \setminus \{\varphi(1), \varphi(2), \ldots\}, \end{cases}$$

и применим предложение 2.

Предложения 3(а) и 3(б) провоцируют на высказывание, что нами определен порядок. Но где?! Ведь совокупность всех множеств множеством не является.

Теорема 2. *Если A — бесконечное множество и*

$$A^n = \underbrace{A \times \ldots \times A}_{n},$$

то $\operatorname{Card} A^n = \operatorname{Card} A$.

Доказательство. Установим сначала некоторые леммы.

Лемма 1. *Пусть C — вполне упорядоченное множество, $P = C \times C$ и отношение $\trianglelefteq$ на P определено условием*

$$(\alpha, \beta) \trianglelefteq (\gamma, \delta) \Leftrightarrow \begin{array}{l} \max\{\alpha, \beta\} < \max\{\gamma, \delta\} \\ \text{или} \\ \max\{\alpha, \beta\} = \max\{\gamma, \delta\} \text{ и } \alpha < \gamma \\ \text{или} \\ \max\{\alpha, \beta\} = \max\{\gamma, \delta\}, \ \alpha = \gamma \\ \qquad\qquad \text{и } \beta \leqslant \delta. \end{array}$$

Тогда $\trianglelefteq$ — порядок, превращающий P во вполне упорядоченное множество.

В самом деле, рефлексивность отношения $\trianglelefteq$ очевидна. Если $(\alpha, \beta) \trianglelefteq (\gamma, \delta)$ и $(\gamma, \delta) \trianglelefteq (\alpha, \beta)$, то, ввиду невозможности соотношений $\alpha < \gamma \leqslant \alpha$, $\alpha \leqslant \gamma < \alpha$,

$$\max\{\alpha, \beta\} < \max\{\gamma, \delta\} \leqslant \max\{\alpha, \beta\}$$

и

$$\max\{\alpha, \beta\} \leqslant \max\{\gamma, \delta\} < \max\{\alpha, \beta\},$$

данные неравенства установлены по третьему правилу. Следовательно, $\alpha = \gamma$ и $\beta \leqslant \delta \leqslant \beta$, что доказывает антисимметричность отношения $\trianglelefteq$. Чтобы установить его транзитивность, допустим, что $(\alpha, \beta) \trianglelefteq (\gamma, \delta)$ и $(\gamma, \delta) \trianglelefteq (\varepsilon, \varkappa)$. Если хотя бы одно из этих неравенств установлено по первому правилу, то $(\alpha, \ ) \trianglelefteq (\varepsilon, \varkappa)$ по тому же правилу. Если первое правило не использовалось, но хотя бы один раз применено второе правило, то $(\alpha, \beta) \trianglelefteq (\varepsilon, \varkappa)$ по этому же правилу. Если же данные неравенства установлены по третьему правилу, то оно применимо и для установления неравенства $(\alpha, \beta) \trianglelefteq (\varepsilon, \varkappa)$. Так что $\trianglelefteq$ — транзитивное отношение, т. е. порядок. Пусть теперь $(\alpha, \beta) \neq (\gamma, \delta)$. Конечно, $\max(\alpha, \beta)$ и $\max(\gamma, \delta)$ связаны одним из отношений $>$, $<$ или $=$. В первых

двух случаях сравнимость данных элементов устанавливается по первому правилу. Если $\alpha \neq \gamma$, то, используя второе правило, придем к тому же результату и в третьем случае. При $\alpha = \gamma$ применимо третье правило. Таким образом, P — цепь. Пусть, наконец, $\varnothing \neq Q \subseteq P$ и

$$K = \{\gamma \mid \gamma \in C,\ \gamma = \max\{\alpha,\ \beta\} \text{ для некоторого } (\alpha,\ \beta) \in Q\}.$$

Если γ_0 — наименьший элемент из K, то положим $L = \{\alpha \mid \alpha \in C$ и существует $\beta \in C$ такой, что $(\alpha,\ \beta) \in Q$ и

$$\max(\alpha,\ \beta) = \gamma_0\}$$

и

$$M = \{\beta \mid \beta \in C,\ (\alpha_0,\ \beta) \in Q \text{ и } \max\{\alpha_0,\ \beta\} = \gamma_0\},$$

где α_0 — наименьший элемент множества L, и пусть β_0 — наименьший элемент множества M. Тогда $(\alpha_0,\ \beta_0) \in Q$. Если $(\alpha,\ \beta) \in Q$ и $\gamma = \max\{\alpha,\ \beta\}$, то $\gamma_0 \leqslant \gamma$. Если $\gamma_0 < \gamma$, то $(\alpha_0,\ \beta_0) \trianglelefteq (\alpha,\ \beta)$ по первому правилу. Если же $\gamma_0 = \gamma$, то $\alpha \in L$ и, следовательно, $\alpha_0 \leqslant \alpha$. Поэтому $(\alpha_0,\ \beta_0) \trianglelefteq (\alpha,\ \beta)$ по второму правилу, если $\alpha_0 < \alpha$. Если же $\alpha_0 = \alpha$, то $\beta \in M$. Отсюда $\beta_0 \leqslant \beta$, а значит $(\alpha_0,\ \beta_0) \trianglelefteq (\alpha,\ \beta)$ по третьему правилу. Таким образом, $(\alpha_0,\ \beta_0)$ — наименьший элемент из Q, т. е. P вполне упорядочено.

Лемма 2. $\operatorname{Card} A^2 = \operatorname{Card} A$.

Для доказательства допустим сначала, что $A = \{1,\ 2,\ \ldots\}$. Тогда A^2 можно изобразить как

$$\begin{array}{l} (1,\ 1),\ (1,\ 2),\ (1,\ 3),\ \ldots. \\ (2,\ 1),\ (2,\ 2),\ (2,\ 3),\ \ldots. \\ (3,\ 1),\ (3,\ 2),\ (3,\ 3),\ \ldots. \\ \ldots\ldots\ldots\ldots\ldots \end{array}$$

и расположить в виде последовательности

$$(1,\ 1),\ (1,\ 2),\ (2,\ 1),\ (1,\ 3),\ (2,\ 2),\ (3,\ 1),\ (1,\ 4),\ (2,\ 3),\ (3,\ 2),\ (4,\ 1),\ \ldots,$$

что и доказывает справедливость леммы в этом случае. Допустим теперь, что существует бесконечное множество A, для которого лемма не верна. Поскольку каждое множество можно отождествить с отрезком $[0,\ \Omega)$, где Ω — некоторый трансфинит, то существуют бесконечные трансфиниты, для которых лемма не верна. Пусть Ω — наименьший из таких трансфинитов. Лемма 1 позволяет превратить $P = [0,\ \Omega)^2$ во вполне упорядоченное мно-

жество. Поскольку $\operatorname{Card}[0, \Omega) < \operatorname{Card} P$, то, согласно предложению 1, $\operatorname{Card}[0, \Omega) = \operatorname{Card} P'$, где

$$P' = \{(\xi, \eta) \mid (\xi, \eta) \trianglelefteq (\alpha, \beta) \neq (\xi, \eta)\}$$

для некоторого $(\alpha, \beta) \in P$. В силу доказанного выше, $[0, \Omega) \neq \{0, 1, 2, \ldots\}$. Это позволяет выбрать $\gamma < \Omega$ так, что $\alpha, \beta \leqslant \gamma$ и $[0, \gamma)$ бесконечно. Тогда $P' \subseteq [0, \gamma)^2$ и, следовательно,

$$\operatorname{Card}[0, \Omega) = \operatorname{Card} P' \leqslant \operatorname{Card}[0, \gamma)^2 = \operatorname{Card}[0, \gamma).$$

Ввиду предложения 3(в) отсюда вытекает, что

$$\operatorname{Card}[0, \Omega)^2 \leqslant \operatorname{Card}[0, \gamma)^2 = \operatorname{Card}[0, \gamma) \leqslant \leqslant \operatorname{Card}[0, \Omega) < \operatorname{Card}[0, \Omega)^2.$$

Полученное противоречие завершает доказательство леммы.

Возвращаясь к доказательству теоремы, замечаем, что для $n = 2$ она справедлива по лемме 2. Если же $n > 2$, то, используя индуктивное предположение и предложение 3(в), получаем

$$\operatorname{Card} A^n = \operatorname{Card}(A^{n-1} \times A) \leqslant \operatorname{Card} A^2 = \operatorname{Card} A \leqslant \operatorname{Card} A^n,$$

после чего остается лишь применить предложение 3(б).

Теорема 3. *Мощность множества всех конечных подмножеств бесконечного множества A равна мощности множества A.*

Доказательство. Пусть B_n—множество всех n-элементных подмножеств множества A. Поскольку каждое n-элементное множество можно рассматривать как элемент множества A^n, то ввиду теоремы 2

$$\operatorname{Card} B_n \leqslant \operatorname{Card} A^n = \operatorname{Card} A.$$

Следовательно, существует взаимно однозначное отображение φ_n множества B_n на подмножество A_n множества A. Равенство $\varphi(x) = (\varphi_n(x), n)$, если $x \in B_n$, определяет взаимно однозначное отображение φ множества $B = \bigcup B_n$ на подмножество

$$\{(\varphi_n(x), n) \mid x \in B\}$$

множества $A \times \{1, 2, \ldots\}$. Отсюда с помощью теоремы 2 и предложений 3(в) и 3(г) получаем

$$\operatorname{Card} A = \operatorname{Card} B_1 \leqslant \operatorname{Card} B \leqslant \operatorname{Card}(A \times \{1, 2, \ldots\}) \leqslant \leqslant \operatorname{Card} A^2 = \operatorname{Card} A.$$

Остается принять во внимание предложение 3(б).

Упражнения

1. Для двух множеств A и B существует одна и только одна из следующих возможностей: а) A эквивалентно B; б) A отображается на B, но B не отображается на A; в) B отображается на A, но A не отображается на B.

2. Доказать, что возможность б) из упражнения 1 осуществляется тогда и только тогда, когда $\operatorname{Card} B < \operatorname{Card} A$.

3. Каждое бесконечное множество A можно представить в виде объединения попарно не пересекающихся эквивалентных ему подмножеств, причем мощность множества этих подмножеств равна мощности множества A.

4. Если A — бесконечное множество, то, каково бы ни было множество B, $\operatorname{Card}(A \cup B) \leqslant \max\{\operatorname{Card} A, \operatorname{Card} B\}$.

5. Если $\{A_\iota \mid \iota \in \mathfrak{S}\}$ — семейство неодноэлементных подмножеств, то

$$\operatorname{Card}\left(\bigcup_{\iota \in \mathfrak{S}} A_\iota\right) \leqslant \operatorname{Card}\left(\prod_{\iota \in \mathfrak{S}} A_\iota\right).$$

6. Если A и B — непустые множества, причем B бесконечно и $\operatorname{Card} A \leqslant \operatorname{Card} B$, то $\operatorname{Card}(A \times B) = \operatorname{Card} B$.

§ 3. Полные структуры

Частично упорядоченное множество называется *полной структурой*, если всякое его подмножество (в том числе пустое) имеет точную нижнюю и точную верхнюю грани. Впрочем приведенное определение оказывается избыточным, так как справедливо:

Предложение 1. *Если всякое подмножество частично упорядоченного множества P имеет точную нижнюю грань, то P — полная структура.*

Доказательство. Пусть A — подмножество в P. Если $A = \varnothing$, то, по определению, $\sup \varnothing = \inf P$, где $\inf P$ существует по условию. Допустим, что $A \neq \varnothing$. По условию, существует $a = \inf A^\triangle$. Если $x \in A$, то $x \in A^{\triangle\triangledown}$. Вспоминая, что a — наибольший элемент множества $A^{\triangle\triangledown}$, получаем, что $x \leqslant a$ для всех $x \in A$, т. е. $a \in A^\triangle$. Если $x \in A^\triangle$, то, очевидно, $a \leqslant x$. Следовательно, a — наименьший элемент множества $A^\triangle$, т. е. $a = \sup A$.

Из предложения 1 вытекает, что полными структурами являются множество всех подгрупп данной группы, множество всех замкнутых подмножеств топологического пространства, всякое вполне упорядоченное множество с наибольшим элементом и др.

Предложение 2. *Если* φ: $L \to L'$ *— изоморфизм частично упорядоченных множеств, являющихся полными*

структурами, то для любого $A \subseteq L$ *имеет место*

$$\varphi(\sup_L A) = \sup_{L'} \varphi(A) \; [\varphi(\inf_L A) = \inf_{L'} \varphi(A)].$$

Доказательство. Пусть $a = \sup_L A$ и $a' = \sup_L \varphi(A)$. Тогда $a \geqslant x$ для всех $x \in A$. Поэтому $\varphi(a) \geqslant \varphi(x)$ для всех $x \in A$, откуда $a' \leqslant \varphi(a)$. С другой стороны, $\varphi^{-1}(a') \geqslant x$ для всех $x \in A$. Отсюда $\varphi^{-1}(a') \geqslant a$, а значит, $a' \geqslant \varphi(a)$. Таким образом, $a' = \varphi(a)$. Второе утверждение доказывается двойственным рассуждением.

Предложение 3 (обобщенная ассоциативность). *Если* $\{A_\iota, \iota \in \Im\}$ *— непустое множество непустых подмножеств полной структуры и* $A = \bigcup_{\iota \in \Im} A_\iota$, *то*

$$\sup A = \sup \{\sup A_\iota \mid \iota \in \Im\} \quad [\inf A = \inf \{\inf A_\iota \mid \iota \in \Im\}].$$

Доказательство. Положим $a = \sup A$, $a_\iota = \sup A_\iota$ и $b = \sup \{a_\iota \mid \iota \in \Im\}$. Поскольку $a \geqslant x$ для всех $x \in A = \bigcup_{\iota \in \Im} A_\iota$, то $a \geqslant a_\iota$ для каждого $\iota \in \Im$, откуда $a \geqslant b$. С другой стороны, $b \geqslant a_\iota$ для всех $\iota \in \Im$, а $a_\iota \geqslant x$ для всех $x \in A_\iota$. Следовательно, $b \geqslant x$ для всех $x \in \bigcup_{\iota \in \Im} A_\iota = A$, откуда $b \geqslant a$. Таким образом, $a = b$. Второе утверждение доказывается двойственным рассуждением.

Изотонное отображение φ частично упорядоченного множества P в себя называется *оператором замыкания*, если $\varphi(x) \geqslant x$ и $\varphi(\varphi(x)) = \varphi(x)$ для всех $x \in L$. Ведущим примером служит полная структура всех подмножеств топологического пространства с отображением, ставящим в соответствие каждому подмножеству его замыкание. Операторы замыкания возникают и во многих других ситуациях. В частности, если L — полная структура всех подмножеств группы, кольца или линейного пространства, то операторами замыкания будут отображения, ставящие в соответствие каждому подмножеству порожденную им подгруппу, нормальную подгруппу, подкольцо, идеал или подпространство. В качестве тривиального примера можно указать отображение, ставящее в соответствие каждому элементу полной структуры ее наибольший элемент.

Если φ — оператор замыкания на полной структуре L и $x \in L$, то $\varphi(x)$ называется φ-*замыканием* элемента x. Элемент x, для которого $\varphi(x) = x$, называется φ-*замкнутым*. В рассмотренных выше примерах φ-замкнутыми элементами оказываются замкнутые множества, подгруп-

пы, нормальные подгруппы, подкольца, идеалы, подпространства и наибольший элемент соответственно.

Предложение 4. *Если φ — оператор замыкания на полной структуре P, то частично упорядоченное множество L всех φ-замкнутых элементов из P, рассматриваемое как подмножество частично упорядоченного множества P, также является полной структурой. При этом*

$$1 \in L$$

и для всякого непустого подмножества A множества L имеет место

$$\inf_L A = \inf_P A$$

и

$$\sup_L A = \varphi(\sup_P A).$$

Кроме того, для всякого $x \in P$ справедливо

$$\varphi(x) = \inf_P \{u \mid u \in P,\ x \leqslant u = \varphi(u)\}.$$

Доказательство. Пусть 1 — наибольший элемент полной структуры P. Поскольку $\varphi(1) \geqslant 1 \geqslant \varphi(1)$, то 1 принадлежит L и, очевидно, является наибольшим элементом этого частично упорядоченного множества. Если, далее, A — непустое подмножество в L, то положим $a = \inf_P A$. Разумеется, $a \leqslant \varphi(a)$. С другой стороны, поскольку $a \leqslant x$ для всех $x \in A$, то $\varphi(a) \leqslant \varphi(x) = x$ для всех $x \in A$ и, следовательно, $\varphi(a) \leqslant a$. Таким образом, $\varphi(a) = a$, т. е. $a \in L$. Кроме того, если $v \in L$ и $v \leqslant x$ для всех $x \in A$, то $v \leqslant a$. Но $a \leqslant x$ для всех $x \in A$ и, следовательно, $a = \inf_L A$. Теперь предложение 1 позволяет заключить, что L — полная структура. Если, наконец, $b = \sup_P A$ и $\bar{b} = \sup_L A$, то $\bar{b} \in L$ и $\bar{b} \geqslant x$ для всех $x \in A$. Отсюда $\bar{b} \geqslant b$, а значит, $\bar{b} = \varphi(\bar{b}) \geqslant \varphi(b)$. Кроме того, поскольку $\varphi(b) \geqslant \varphi(x) = x$ для всех $x \in A$, то $\varphi(b) \geqslant \bar{b}$. Таким образом, $\bar{b} = \varphi(b)$. Наконец, импликации

$$(x \leqslant u = \varphi(u)) \Rightarrow (\varphi(x) \leqslant \varphi(u) = u)$$

и

$$(\varphi(x) \leqslant u = \varphi(u)) \Rightarrow (x \leqslant \varphi(x) \leqslant u = \varphi(u))$$

показывают, что

$$\{u \mid u \in P,\ \varphi(x) \leqslant u = \varphi(u)\} = \{u \mid u \in P,\ x \leqslant u = \varphi(u)\}.$$

Поэтому из уже доказанного вытекает

$$\varphi(x) = \inf_L \{u \mid u \in P,\ \varphi(x) \leqslant u = \varphi(u)\} = \\ = \inf_P \{u \mid u \in P,\ \varphi(x) \leqslant u = \varphi(u)\} = \\ = \inf_P \{u \mid u \in P,\ x \leqslant u = \varphi(u)\}.$$

Из последнего утверждения предложения 4 вытекает

Следствие. *Операторы замыкания* φ *и* ψ *на полной структуре* P *совпадают тогда и только тогда, когда совпадают множества* φ- *и* ψ-*замкнутых элементов.*

Предложение 5. *Подмножество* L *полной структуры* P *совпадает с множеством всех* φ-*замкнутых элементов для некоторого оператора замыкания* φ *на* P *в том и только в том случае, когда* $1 \in L$ *и* $\inf_P A \in L$ *для любого подмножества* $A \subseteq L$.

Доказательство. Необходимость указанных условий вытекает из предложения 4. Если же они выполнены, то для каждого $x \in P$ положим

$$A(x) = \{x\}^{\Delta} \cap L$$

и

$$\varphi(x) = \inf_P A(x).$$

Ясно, что $\varphi(x) \in L$ и $x \leqslant \varphi(x)$. Отсюда

$$\varphi(x) \leqslant \varphi(\varphi(x)) = \inf_P A(\varphi(x)) = \inf_P (\{\varphi(x)\}^{\Delta} \cap L) = \varphi(x),$$

т. е. $\varphi(\varphi(x)) = \varphi(x)$. Если $x \leqslant y$, то, очевидно, $\{x\}^{\Delta} \supseteq \{y\}^{\Delta}$. Отсюда $A(x) \supseteq A(y)$, а значит, наименьший элемент множества $A(x)$ меньше или равен наименьшего элемента множества $A(y)$, т. е.

$$\varphi(x) = \inf_P A(x) \leqslant \inf_P A(y) = \varphi(y).$$

Таким образом, φ — оператор замыкания. Если $x = \varphi(x)$, то, как было отмечено, $x = \varphi(x) \in L$. Если $x \in L$, то $x \in A(x)$ и, следовательно, $\varphi(x) \leqslant x \leqslant \varphi(x)$, т. е. $x = \varphi(x)$. Таким образом, L совпадает с множеством φ-замкнутых элементов.

Оказывается, что любое частично упорядоченное множество M можно вложить в полную структуру. Требование существования нуля и единицы в доказываемой ниже теореме несущественны, так как при отсутствии в частично упорядоченном множестве M нуля или единицы соответствующий элемент может быть присоединен с соблюдением условий $0 < x$ для всех $x \in M$ и $x < 1$ для всех $x \in M$.

Теорема 1. *Пусть M — частично упорядоченное множество с наименьшим элементом 0 и наибольшим элементом 1, P — полная структура всех подмножеств множества M, содержащих 0,*

$$L = \{X \mid X \in P,\ X^{\Delta\nabla} = X\}.$$

Для каждого $x \in M$ положим

$$\theta(x) = x^{\Delta\nabla}$$

(здесь и дальше не различаются x и $\{x\}$). *Тогда L — полная структура, а θ — изоморфизм частично упорядоченного множества M на подмножество полной структуры L. При этом справедливы следующие свойства:*

(i) *если $\varnothing \neq A \subseteq M$ и $\inf_M A$ существует, то*

$$\theta(\inf_M A) = \inf_L \theta(A);$$

(ii) *если $\varnothing \neq A \subseteq M$ и $\sup_M A$ существует, то*

$$\theta(\sup_M A) = \sup_L \theta(A);$$

(iii) *если $X \in L$, то найдутся такие подмножества A и B множества M, что*

$$X = \sup_L \theta(A) = \inf_L \theta(B).$$

Доказательство. Предварительно установим:

Лемма 1. *Если $\varnothing \neq A, B \subseteq M$, то*: (а) $A \subseteq B$ *влечет* $B^{\Delta} \subseteq A^{\Delta}$ *и* $B^{\nabla} \subseteq A^{\nabla}$, (б) $A \subseteq A^{\Delta\nabla} \cap A^{\nabla\Delta}$; (в) $A^{\Delta} = A^{\Delta\nabla\Delta}$.

В самом деле, (а) и (б) сразу следует из определения конусов. Используя (а) и (б), получаем

$$A^{\Delta} \subseteq A^{\Delta\nabla\Delta} \subseteq A^{\Delta},$$

т. е. $A^{\Delta} = A^{\Delta\nabla\Delta}$.

Положим $\varphi(A) = A^{\Delta\nabla}$ для каждого $A \in P$.

Лемма 2. *φ — оператор замыкания на P.*

Действительно, из леммы 1(а) вытекает, что $\varphi(A) \subseteq \varphi(B)$, если $A \subseteq B$, а из леммы 1(б) — что $A \subseteq \varphi(A)$ для любых A, $B \in P$. Наконец, из леммы 1(в) следует, что

$$\varphi(\varphi(A)) = A^{\Delta\nabla\Delta\nabla} = A^{\Delta\nabla} = \varphi(A).$$

Ввиду леммы 1 и предложения 4, множество L всех φ-замкнутых элементов из P является полной структурой. Справедливость теоремы является следствием доказываемых ниже лемм 5, 6, 8 и 9.

Лемма 3. *Если* $v \in M$, *то* $t \in v^{\Delta\nabla}$ *тогда и только тогда, когда* $t \leqslant v$.

Действительно, если $t \leqslant v$, то для всякого $x \in v^{\Delta}$ имеем $t \leqslant v \leqslant x$, что и означает справедливость соотношения $t \in v^{\Delta\nabla}$. Если, наоборот, $t \in v^{\Delta\nabla}$, то $t \leqslant x$ для всех $x \in v^{\Delta}$. В частности, $t \leqslant v$, ибо $v \in v^{\Delta}$.

Лемма 4. *Если* $x, y \in M$, *то* $x \leqslant y$ *тогда и только тогда, когда* $\theta(x) \leqslant \theta(y)$.

В самом деле, если $x \leqslant y$, то, в силу леммы 3, $x \in y^{\Delta\nabla}$. Ввиду лемм 1(а) и 1(в), отсюда вытекает, что

$$\theta(x) = x^{\Delta\nabla} \subseteq y^{\Delta\nabla} = \theta(y).$$

Если же $\theta(x) \subseteq \theta(y)$, то, учитывая лемму 3, получим $x \in x^{\Delta\nabla} \subseteq y^{\Delta\nabla}$, и вторичное применение леммы 3 дает $x \leqslant y$.

Из леммы 4 и предложения 1.1 вытекает:

Лемма 5. θ — *изоморфизм частично упорядоченного множества* M *на подмножество полной структуры* L.

Лемма 6. *Если* $a = \inf_M A$, *то* $\theta(a) = \inf_L \theta(A)$.

Для доказательства, ввиду предложения 4, достаточно установить, что $a^{\Delta\nabla} = \bigcap\limits_{x \in A} x^{\Delta\nabla}$. Но в силу леммы 3, из $t \in a^{\Delta\nabla}$ вытекает, что $t \leqslant a$. Отсюда $t \leqslant x$ для всех $x \in A$. Согласно лемме 3, $t \in x^{\Delta\nabla}$ для всех $x \in A$, т. е. $t \in \bigcap\limits_{x \in A} x^{\Delta\nabla}$. Таким образом,

$$a^{\Delta\nabla} \subseteq \bigcap_{x \in A} x^{\Delta\nabla}.$$

Обратное включение является следствием следующей цепочки импликаций, вытекающей из леммы 3 и определения $\inf_M A$:

$$\left(t \in \bigcap_{x \in A} x^{\Delta\nabla}\right) \Rightarrow \left(\forall x \in A\,(t \in x^{\Delta\nabla})\right) \Rightarrow$$

$$\Rightarrow (\forall x \in A\,(t \leqslant x)) \Rightarrow (t \in A^{\nabla}) \Rightarrow (t \leqslant \inf_M A = a) \Rightarrow (t \in a^{\Delta\nabla}).$$

Лемма 7. *Если* $a = \sup_M A$, *то* $v \geqslant a$ *тогда и только тогда, когда* $v \in \left(\bigcup\limits_{x \in A} x^{\Delta\nabla}\right)^{\Delta}$.

В самом деле, если $v \geqslant a$, то, ввиду леммы 5, имеем

$$v^{\Delta\nabla} = \theta(v) \supseteq \theta(a) \supseteq \theta(x) = x^{\Delta\nabla}$$

для всех $x \in A$. Отсюда $\bigcup\limits_{x \in A} x^{\Delta\nabla} \subseteq v^{\Delta\nabla}$ и, используя лем-

мы 1(а) и 1(в), получаем

$$v \in v^{\Delta} = v^{\Delta\nabla\Delta} \subseteq \Big(\bigcup_{x \in A} x^{\Delta\nabla}\Big)^{\Delta}.$$

Если же $v \in \Big(\bigcup_{x \in A} x^{\Delta\nabla}\Big)^{\Delta}$, то $v \in x^{\Delta\nabla\Delta} = x^{\Delta}$ для всех $x \in A$ и, следовательно, $v \geqslant \sup_M A = a$.

Лемма 8. *Если* $a = \sup_M A$, *то* $\theta(a) = \sup_L \theta(A)$.

В самом деле, из леммы 7 вытекает, что $a^{\Delta} = \Big(\bigcup_{x \in A} x^{\Delta\nabla}\Big)^{\Delta}$, откуда, учитывая предложение 4, получаем

$$\theta(a) = a^{\Delta\nabla} = \Big(\bigcup_{x \in A} x^{\Delta\nabla}\Big)^{\Delta\nabla} = \sup_L \theta(A).$$

Лемма 9. *Если* $A \in L$, *то*

$$A^{\Delta\nabla} = \sup_L \theta(A^{\Delta\nabla}) = \inf_L \theta(A^{\Delta}).$$

Для доказательства, воспользовавшись леммой 1, получим

$$\bigcup_{x \in A^{\Delta\nabla}} x^{\Delta\nabla} \subseteq A^{\Delta\nabla\Delta\nabla} = A^{\Delta\nabla} = \bigcup_{x \in A^{\Delta\nabla}} x \subseteq \bigcup_{x \in A^{\Delta\nabla}} x^{\Delta\nabla}.$$

Следовательно, $A^{\Delta\nabla} = \bigcup_{x \in A^{\Delta\nabla}} x^{\Delta\nabla}$, откуда, принимая во внимание предложение 4 и лемму 1(в), выводим

$$\sup_L \theta(A^{\Delta\nabla}) = \Big(\bigcup_{x \in A^{\Delta\nabla}} x^{\Delta\nabla}\Big)^{\Delta\nabla} = A^{\Delta\nabla\Delta\nabla} = A^{\Delta\nabla}.$$

Если, далее, $t \in \bigcap_{x \in A^{\Delta}} x^{\Delta\nabla}$, то, согласно лемме 3, $t \leqslant x$ для всех $x \in A^{\Delta}$, т. е. $t \in A^{\Delta\nabla}$. Если же $t \in A^{\Delta\nabla}$, то $t \leqslant x$ для всех $x \in A^{\Delta}$ и $t \in \bigcap_{x \in A^{\Delta}} x^{\Delta\nabla}$ в силу леммы 3. Таким образом, учитывая предложение 4, получаем

$$\inf_L \theta(A^{\Delta}) = \bigcap_{x \in A^{\Delta}} x^{\Delta\nabla} = A^{\Delta\nabla}.$$

Пополнение частично упорядоченного множества, описанное в теореме 1, является обобщением известного построения действительных чисел как сечений на множестве рациональных чисел и носит название *пополнения сечениями* (ср. упр. 7). Свойство (iii) показывает, что при этом присоединяется минимум новых элементов.

Упражнения

1. Если к тривиальному частично упорядоченному множеству присоединить наибольший и наименьший элементы, то возникает полная структура.

2. Если частично упорядоченное множество P удовлетворяет условию минимальности или условию максимальности и всякое его конечное подмножество имеет как точную верхнюю, так и точную нижнюю грани, то P — полная структура.

3. Прямое произведение полных структур является полной структурой (по определению $(\ldots, a_\iota, \ldots) \leqslant (\ldots, b_\iota, \ldots)$, если $a_\iota \leqslant b_\iota$ для всех ι).

4. Если φ — оператор замыкания на частично упорядоченном множестве P, то все максимальные элементы из P являются φ-замкнутыми.

5. Отображение φ частично упорядоченного множества P в себя является оператором замыкания тогда и только тогда, когда $\varphi(x) \geqslant x$ для любого $x \in P$ и $x \leqslant \varphi(y)$ влечет $\varphi(x) \leqslant \varphi(y)$ для любых $x, y \in P$.

6. Отображение φ полной структуры P в себя является оператором замыкания тогда и только тогда, когда

$$\varphi(\sup_P \{x, y\}) = \sup_P \{\varphi(x), y\}$$

для любых $x, y \in P$.

7. Пусть Φ — множество всех операторов замыкания на полной структуре P. Для $\varphi, \psi \in \Phi$ положим $\varphi \trianglelefteq \psi$, если $\varphi(x) \leqslant \psi(x)$ при всех $x \in P$. Убедиться, что отношение $\trianglelefteq$ является порядком, превращающим Φ в полную структуру.

8. Пополнение сечениями цепи рациональных чисел, лежащих между 0 и 1, изоморфно отрезку $[0, 1]$ с естественным порядком.

9. Пополнение сечениями цепи является цепью.

10. Пополнение сечениями прямого произведения двух частично упорядоченных множеств с 0 и 1 изоморфно прямому произведению пополнения сечениями сомножителей.

11. Пусть Ξ — полная структура всех эквивалентностей на некотором множестве $\mathfrak{M}$. Если $W \subseteq \Xi$ и $x, y \in \mathfrak{M}$, то положим

$x\theta y \Leftrightarrow$ существуют натуральное число m, элементы $z_1, \ldots, z_{m-1} \in \mathfrak{M}$ и эквивалентности $\theta_1, \ldots, \theta_m \in W$ такие, что $x\theta_1 z_1$, $z_1\theta_2 z_2$, $\ldots$, $z_{m-2}\theta_{m-1} z_{m-1}$, $z_{m-1}\theta_m y$.

Доказать, что

$$\theta = \sup_{\Xi} W.$$

ЛИТЕРАТУРА

Александров П. С. Введение в теорию множеств и общую топологию.— М.: Наука, 1977.

Архангельский А. В., Пономарев В. И. Основы общей топологии в задачах и упражнениях.— М.: Наука, 1974.

Биркгоф Г. Теория решеток.— М.: Наука, 1983.

Бурбаки Н. Теория множеств.— М.: Мир, 1965.

Коэн П. Дж. Теория множеств и континуум-гипотеза.— М.: Мир, 1969.

Скорняков Л. А. Элементы теории структур.— М.: Наука, 1982.

ГЛАВА II

УНИВЕРСАЛЬНЫЕ АЛГЕБРЫ

При изучении основ теории групп и колец можно было заметить ряд параллельных моментов: сходным образом определялись гомоморфизмы, допустимые разбиения, фактор-группы и фактор-кольца и т. п. Оказалось, что эти общие моменты объединяются в рамках общей теории — теории универсальных алгебр. В настоящей главе, помимо основных определений, излагаются вопросы, связанные с подпрямыми разложениями и многообразиями. В связи с этим изучаются свободные универсальные алгебры. Их описание для классических случаев (полугруппы, группы, кольца и др.) дается в последнем параграфе.

§ 1. Операции. Алгебры. Конгруэнции

Если A — непустое миожество и $n \geqslant 1$, то *n-арной операцией* на множестве A назовем отображение прямого произведения $\underbrace{A \times \ldots \times A}_{n \text{ раз}}$ в A. Рассматриваются и *0-арные операции*, которые, по определению, отмечают некоторый элемент из A. В классических алгебраических системах (группах, полугруппах, кольцах и т. п.) основной упор делается на бинарные операции. Однако, по существу, там рассматривались и унарные (например, в группах отображение $a \mapsto a^{-1}$) и 0-арные операции (например, выделяющие 0 и 1 в кольце). Примером тернарной операции на множестве векторов обычной плоскости может служить нахождение их центра тяжести: $f(x, y, z) = (x+y+z)/3$. Другой пример доставляет множество всех взаимно однозначных отображений множества A на множество B с операцией $(\varphi, \psi, \chi) = \varphi\psi^{-1}\chi$.

Пара (A, Ω), где A — непустое множество, а Ω — (возможно, пустое) множество операций на A, называется

универсальной алгеброй или, короче, *алгеброй*. Элемент алгебры A, отмечаемый 0-арной операцией ν, условимся обозначать через $\nu(A)$. Подмиожество $B \subseteq A$ называется *подалгеброй*, если $\nu(A) \in B$ для всякой 0-арной операции $\nu \in \Omega$, а если $n \geqslant 1$ и f — n-арная операция из Ω, то $f(b_1, \ldots, b_n) \in B$ для любых $b_1, \ldots, b_n \in B$. Таким образом, если Ω содержит 0-арные операции, то всякая подалгебра непуста. В противном случае пустое подмножество считается подалгеброй. Легко проверяется, что пересечение любого множества подалгебр является подалгеброй. Каждая непустая подалгебра является, очевидно, алгеброй с теми же операциями. Если $M \subseteq A$, то пересечение всех подалгебр алгебры A, содержащих множество M, называется *подалгеброй, порожденной множеством* M. Если зто пересечение совпадает с A, т. е. A является единственной подалгеброй, содержащей M, то говорят, что алгебра A *порождается множеством* M.

Совокупность операций можно рассматривать отдельно от алгебры. Правда в этом случае правильнее было бы говорить о множестве операционных символов, которое будем называть *сигнатурой* (мы воздержимся от формализации этого понятия). Если Ω — сигнатура и каждому операционному символу из Ω поставлена в соответствие операция той же самой арности на множестве A, то возникает алгебра сигнатуры Ω. Например, полугруппы — это алгебры сигнатуры, состоящей из одной бинарной операции. На группы можно смотреть как на алгебры той же сигнатуры. Но их можно рассматривать и как алгебры, сигнатура которых состоит из бинарной, унарной и нульарной операций. Сигнатура кольца может быть записана как $\Omega = \{+, \cdot, -, 0\}$, где $+$ и $\cdot$ — бинарные операции сложения и умножения, $-$ — унарная операция $x \mapsto -x$, 0 — нульарная операция, отмечающая нуль. Для кольца с единицей сигнатурой может служить множество $\Omega = \{+, \cdot, -, 0, 1\}$, а для левого модуля над R — множество $\Omega = \{+, -, 0\} \cup R$, где $\{+, -, 0\}$ — сигнатура абелевой группы, а каждый элемент $\lambda \in R$ рассматривается как символ унарной операции $x \mapsto \lambda x$. Подчеркнем, что множество $\{+, \cdot, -, 0, {}^{-1}, 1\}$ нельзя рассматривать как сигнатуру поля, так как унарная операция ${}^{-1}$ не определена для нуля.

Если A_ι, $\iota \in \mathfrak{I}$, — алгебры сигнатуры Ω, то прямое произведение $A = \prod_{\iota \in \mathfrak{I}} A_\iota$ становится алгеброй той же

сигнатуры, если для каждой 0-арной операции $\nu \in \Omega$ положить

$$\nu(A) = (\ldots, \nu(A_\iota), \ldots),$$

а для n-арной операции $f \in \Omega$, где $n \geqslant 1$, —

$$f((\ldots, x_{1\iota}, \ldots), \ldots, (\ldots, x_{n\iota}, \ldots)) = \\ = (\ldots, f(x_{1\iota}, \ldots, x_{n\iota}), \ldots).$$

Возникающая таким образом алгебра (A, Ω) называется *прямым произведением* алгебр A_ι.

Если A и B — алгебры сигнатуры Ω, то отображение φ: $A \to B$ называется *гомоморфизмом*, если

$$\varphi(\nu(A)) = \nu(B)$$

для всякой 0-арной операции $\nu \in \Omega$ и при $n \geqslant 1$

$$\varphi(f(a_1, \ldots, a_n)) = f(\varphi(a_1), \ldots, \varphi(a_n))$$

для любой n-арной операции $f \in \Omega$ и любых $a_1, \ldots, a_n \in A$. Нетрудно проверить, что естественные проекции прямого произведения алгебр на прямые сомножители являются гомоморфными наложениями. Взаимно однозначный гомоморфизм называется *изоморфизмом*. Если φ — изоморфизм, то нетрудно проверить, что обратное отображение φ^{-1} также является изоморфизмом. Поэтому корректно определение: алгебры A и B называются *изоморфными*, если существует изоморфизм φ: $A \to B$. Если φ: $A \to B$ — гомоморфизм, то множество

$$\operatorname{Im}\varphi = \{\varphi(a) \mid a \in A\}$$

называется *образом гомоморфизма* φ. Нетрудно проверить, что $\operatorname{Im}\varphi$ — подалгебра алгебры B.

Гомоморфизм [изоморфизм] алгебры A в себя [на себя] называется *эндоморфизмом* [*автоморфизмом*] алгебры A. Если φ: $A \to B$ и ψ: $B \to C$ — гомоморфизмы, то, как нетрудно проверить, отображение $\varphi\psi$ является гомоморфизмом алгебры A в алгебру C. Отсюда вытекает, что эндоморфизмы алгебры A образуют моноид, а автоморфизмы — группу.

Конгруэнцией на алгебре A называется всякая подалгебра θ прямого квадрата $A \times A$, обладающая следующими свойствами: 1) (рефлексивность): $(a, a) \in \theta$ для всех $a \in A$; 2) (симметричность) если $(a, b) \in \theta$, то $(b, a) \in \theta$; 3) (тран-

зитивность) если $(a, b)\in\theta$ и $(b, c)\in\theta$, то $(a, c)\in\theta$*). Поскольку $A\times A$ — конгруэнция и пересечение подалгебр, обладающих свойствами 1)—3), также обладает ими, то из предложения I.3.1 вытекает, что совокупность всех конгруэнций на алгебре A образует полную структуру, которую будем обозначать через $\Theta(A)$. Наименьшим элементом этой полной структуры служит *нулевая конгруэнция*

$$0_A=\{(a, a)\mid a\in A\},$$

а наибольшим — *единичная конгруэнция*

$$1_A=A\times A.$$

Наименьшая конгруэнция, содержащая пару (a, b), называется *главной конгруэнцией*, порожденной парой (a, b).

Если $\theta\in\Theta(A)$ и $a\in A$, то множество

$$\theta(a)=\{x\mid(a, x)\in\theta\}$$

называется *классом конгруэнции* θ. Стандартные рассуждения позволяют установить, что классы конгруэнции θ образуют *допустимое разбиение* алгебры A в том смысле, что для любой n-арной операции f из Ω, где $n\geqslant 1$, справедлива импликация: если для каждого i элементы a_i и b_i, $i=1, \ldots, n$, принадлежат одному классу разбиения, то элементы $f(a_1, \ldots, a_n)$ и $f(b_1, \ldots, b_n)$ также лежат в одном классе (ср. ЭА, с. 61, 76, 92, 111).

Как известно, в случае групп, колец и модулей допустимые разбиения исчерпываются разбиениями по нормальной подгруппе, идеалу и подмодулю соответственно. С целью обобщения этих фактов назовем *мультиоператорным кольцом* универсальную алгебру A сигнатуры $\{+, -, 0\}\cup\Omega$ такую, что $(A, \{+, -, 0\})$ является группой (не обязательно абелевой) и для любой n-арной операции $f\in\Omega$, где $n\geqslant 1$, и любых $a_1, \ldots, a_{i-1}, a_i', a_i'', a_{i+1}, \ldots, a_n\in A$ имеет место

$$f(a_1, \ldots, a_{i-1}, a_i'+a_i'', a_{i+1}, \ldots, a_n)=$$
$$=f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)+$$
$$+f(a_1, \ldots, a_{i-1}, a_i'', a_{i+1}, \ldots, a_n).$$

Стандартные рассуждения показывают справедливость

*) Заметим, что условия 1)—3) означают, что θ — эквивалентность на множестве A.

следующих равенств:

$$f(a_1, \ldots, a_{i-1}, 0, a_{i+1}, \ldots, a_n) = 0,$$
$$f(a_1, \ldots, a_{i-1}, -a, a_{i+1}, \ldots, a_n) = -f(a_1, \ldots, a_{i-1}, a, a_{i+1}, \ldots, a_n)$$

и

$$f(a_1, \ldots, a_{i-1}, a_i' - a_i'', a_{i+1}, \ldots, a_n) = f(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n) - f(a_1, \ldots, a_{i-1}, a_i'', a_{i+1}, \ldots, a_n),$$

где, по определению, $a - b = a + (-b)$. Подалгебра H мультиоператорного кольца A называется *идеалом*, если H — нормальная подгруппа группы A и для любой n-арной операции $f \in \Omega$, где $n \geqslant 1$, при любом i, где $1 \leqslant i \leqslant n$, при любом выборе элементов $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in A$ и элемента $h \in H$ имеет место $f(a_1, \ldots, a_{i-1}, h, a_{i+1}, \ldots, a_n) \in H$.

Предложение 1. *Пусть A — мультиоператорное кольцо, H — его идеал и*

$$\theta = \{(a, b) \mid a, b \in A,\ a \in b + H\}.$$

Тогда θ — конгруэнция и всякая конгруэнция на A имеет такую форму для подходящего идеала H.

Доказательство. Поскольку $0 \in H$, то $(a, a) \in \theta$. Если $(a, b) \in \theta$, то $a = b + h$, где $h \in H$. Отсюда $b = a + (-h) \in a + H$, т. е. $(b, a) \in \theta$. Если (a, b), $(b, c) \in \theta$, то $a = b + h''$ и $b = c + h'$, где $h', h'' \in H$. Отсюда $a = c + (h' + h'') \in c + H$, т. е. $(a, c) \in \theta$. Если (a, b), $(c, d) \in \theta$, то $a = b + h'$ и $c = d + h''$, где $h', h'' \in H$. Отсюда, вспоминая определение нормальной подгруппы, получаем

$$-a = -h' - b = (-b) + (b + (-h') - b) \in -b + H$$

и

$$a + c = b + h' + d + h'' = (b + d) + ((-d + h' + d) + h'') \in (b + d) + H,$$

т. е. $(-a, -b)$, $(a + c, b + d) \in \theta$. Ясно, что $\nu(A \times A) = (\nu(A), \nu(A)) \in \theta$ для каждой 0-арной операции $\nu \in \Omega$. Если, наконец, f — n-арная операция из Ω, $n \geqslant 1$, $a_i, b_i \in A$ и $a_i = b_i + h_i$ для некоторого $h_i \in H$, то, как нетрудно заметить,

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

где h — сумма элементов вида $f(x_1, \ldots, x_n)$, где хотя бы один из x_i принадлежит H. Но тогда все эти слагаемые, а значит и h, лежат в H, т. е.

$$(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)) \in \theta.$$

Таким образом, $\theta \in \Theta(A)$ Допустим теперь, что $\theta \in \Theta(A)$, и положим

$$H = \{a \mid (a, 0) \in \theta\}.$$

Ясно, что H — идеал и, в частности, нормальная подгруппа группы $(A, \{+, -, 0\})$. Следовательно, θ, будучи допустимым разбиением этой группы, является разбиением на смежные классы по H, т. е. имеет вид, указанный в формулировке.

Пусть теперь A — универсальная алгебра и $\theta \in \Theta(A)$. Множество всех классов конгруэнции θ будем обозначать через A/θ. Это множество можно превратить в алгебру той же сигнатуры Ω, что и алгебра A, с помощью следующих определений: а) если ν — нульарная операция из Ω, то $\nu(A/\theta) = \theta(\nu(A))$; б) если f — n-арная операция из Ω и $n \geqslant 1$, то $f(\theta(x_1), \ldots, \theta(x_n)) = \theta(f(x_1, \ldots, x_n))$.

Убедимся, что это определение корректно. Действительно, если $\theta(x_i) = \theta(y_i)$, $i = 1, \ldots, n$, то $(x_i, y_i) \in \theta$, откуда

$$(f(x_1, \ldots, x_n), f(y_1, \ldots, y_n)) = f((x_1, y_1), \ldots, (x_n, y_n)) \in \theta,$$

т. е. $\theta(f(x_1, \ldots, x_n)) = \theta(f(y_1, \ldots, y_n))$.

Получившаяся алгебра A/θ называется *фактор-алгеброй* алгебры A по конгруэнции θ. Очевидно, что отображение, ставящее в соответствие каждому элементу $a \in A$ класс $\theta(a) \in A/\theta$, является гомоморфным наложением алгебры A на фактор-алгебру A/θ, которое будем называть *естественным гомоморфизмом*.

Если $\varphi\colon A \to B$ — гомоморфизм универсальных алгебр, то, как нетрудно проверить, множество

$$\operatorname{Ker}\varphi = \{(a', a'') \mid a', a'' \in A, \varphi(a') = \varphi(a'')\}$$

оказывается конгруэнцией на алгебре A и называется *ядром гомоморфизма* φ.

Предложение 2 (теорема о гомоморфизме). *Если* $\varphi\colon A \to B$ *— гомоморфное наложение и* $\pi\colon A \to A/\operatorname{Ker}\varphi$ *— естественный гомоморфизм, то существует изоморфизм* $\chi\colon B \to A/\operatorname{Ker}\varphi$ *такой, что* $\varphi\chi = \pi$.

Доказательство. Положим $\chi(b)=\pi(a)$, где $a\in A$ выбрано так, что $b=\varphi(a)$. Если $b=\varphi(a')$, то $(a, a')\in \operatorname{Ker}\varphi$, откуда $\pi(a)=\pi(a')$. Следовательно, χ — корректно определенное отображение. Равенство $\varphi\chi=\pi$ очевидно. Из него же вытекает, что χ — наложение. Стандартные вычисления показывают, что χ — гомоморфизм. Если $\chi(b)=\chi(b')$, то $\pi(a)=\pi(a')$, где $b=\varphi(a)$ и $b'=\varphi(a')$. Отсюда $(a, a')\in \operatorname{Ker}\varphi$, и, следовательно, $b=b'$, что доказывает взаимную однозначность отображения χ.

Если теперь θ, $\rho\in\Theta(A)$ и $\theta\leqslant\rho$, то положим

$$\rho/\theta=\{(\theta(x),\ \theta(y))\mid(x,\ y)\in\rho\}.$$

Нетрудно проверить, что ρ/θ — подалгебра прямого квадрата $(A/\theta)\times(A/\theta)$, обладающая свойствами 1) и 2), входящими в определение конгруэнции. Допустим далее, что $(\theta(x),\ \theta(y))$, $(\theta(u),\ \theta(v))\in\rho/\theta$ и $\theta(y)=\theta(u)$. Тогда $(x, y)\in\rho$, $(y, u)\in\theta\subseteq\rho$ и $(u, v)\in\rho$, откуда $(x, v)\in\rho$, т. е. $(\theta(x),\ \theta(v))\in\rho/\theta$. Таким образом, $\rho/\theta\in\Theta(A/\theta)$.

Предложение 3. *Если* $\varphi\colon A\to B$ *— гомоморфизм универсальных алгебр,* $\theta\in\Theta(A)$, $\theta\subseteq\operatorname{Ker}\varphi$ *и* $\pi\colon A\to A/\theta$ *— естественный гомоморфизм, то существует гомоморфизм* $\psi\colon A/\theta\to B$ *такой, что* $\pi\psi=\varphi$. *При этом* $\psi(\theta(a))=\varphi(a)$ *для всех* $a\in A$.

Доказательство. Положим $\psi(\theta(a))=\varphi(a)$ для всех $a\in A$. Если $a, b\in A$ и $\theta(a)=\theta(b)$, то $(a, b)\in\theta$. Отсюда $(a, b)\in\operatorname{Ker}\varphi$, т. е. $\varphi(a)=\varphi(b)$. Этим доказана корректность определения отображения ψ. Стандартными вычислениями проверяется, что ψ — гомоморфизм. Остается заметить, что

$$a\pi\psi=\psi(\theta(a))=\varphi(a)=a\varphi$$

для всех $a\in A$.

Предложение 4 (теорема о соответствии). *Если* A *— универсальная алгебра сигнатуры* Ω *и* $\theta\in\Theta(A)$, *то полная структура*

$$\{\rho\mid\rho\in\Theta(A),\ \theta\subseteq\rho\}$$

изоморфна полной структуре $\Theta(A/\theta)$. *Изоморфизм осуществляет отображение* Γ, *определяемое равенством* $\Gamma(\rho)=\rho/\theta$.

Доказательство. Как уже было отмечено, $\Gamma(\rho)\in\Theta(A/\theta)$. Ясно, что $\rho'\subseteq\rho''$ влечет $\Gamma(\rho')\subseteq\Gamma(\rho'')$. Если, наоборот, $\Gamma(\rho')\subseteq\Gamma(\rho'')$ и $(x, y)\in\rho'$, то

$$(\theta(x),\ \theta(y))\in\Gamma(\rho')\subseteq\Gamma(\rho'').$$

Поэтому для подходящих $u, v \in A$ имеем $(u, v) \in \rho''$, $\theta(x) = \theta(u)$ и $\theta(y) = \theta(v)$. Следовательно, $(x, u) \in \theta \subseteq \rho''$, $(u, v) \in \rho''$ и $(v, y) \in \theta \subseteq \rho''$, откуда $(x, y) \in \rho''$, т. е. $\rho' \subseteq \rho''$. Если, наконец, $\bar{\rho} \in \Theta(A/\theta)$, то положим

$$\rho = \{(x, y) \mid x, y \in A, (\theta(x), \theta(y)) \in \bar{\rho}\}.$$

Если f — n-арная операция из Ω, $n \geqslant 1$, и $(x_i, y_i) \in \rho$, $i = 1, \ldots, n$, то $(\theta(x_i), \theta(y_i)) \in \bar{\rho}$. Отсюда

$$(\theta(f(x_1, \ldots, x_n)), \theta(f(y_1, \ldots, y_n))) = \\ = (f(\theta(x_1), \ldots, \theta(x_n)), f(\theta(y_1), \ldots, \theta(y_n))) \in \bar{\rho},$$

и значит,

$$(f(x_1, \ldots, x_n), f(y_1, \ldots, y_n)) \in \rho.$$

Таким образом, ρ — подалгебра в $A \times A$. После этого нетрудно проверить, что $\rho \in \Theta(A)$ и что $\Gamma(\rho) = \rho/\theta = \bar{\rho}$. Следовательно, Γ — наложение, и остается лишь принять во внимание предложение I.1.1.

Пусть Ω — некоторая сигнатура, а X — непустое множество. Само множество X и символы 0-арных операций из Ω назовем *словами веса* 0 сигнатуры Ω в алфавите X. *Слова веса* m определим по индукции как слова меньшего веса и символы $f(u_1, \ldots, u_n)$, где f — n-арные операции из Ω, $n \geqslant 1$, а u_i — слова веса $m-1$. Подчеркнем, что вес слова не определяется однозначно, хотя для каждого слова можно указать его наименьший вес.

Примеры. 1. $X = \{x, y\}$, $\Omega = \{\cdot, \theta\}$, где $\cdot$ — бинарная, а θ — 0-арная операции. Слова веса 0: x, y, θ. Слова веса 1, но не 0: xx, xy, yx, yy, $x\theta$, θx, $y\theta$, θy, $\theta\theta$. Словами веса 2 будут, например, $(xx)x$, $x(xx)$, $(xy)(\theta x)$, $(xx)(xx)$, а словами веса 3 — например, $x((xx)x)$, $((xy)(\theta x))\theta$, $(x(xx))(yy)$, $((xy)(\theta x))((xx)(yy))$.

2. $X = \{x\}$, $\Omega = \{f, +, g, 0\}$, где f — тернарная, $+$ — бинарная, g — унарная, а 0 — нульарная операции. Слова веса 0 — это x, 0. Словами веса 1 являются $f(x, x, 0)$, $f(x, 0, x)$, $f(0, x, x)$, $f(x, x, x)$, $f(0, 0, 0)$, $f(0, 0, x)$, $f(0, x, 0)$, $f(x, 0, 0)$, $x+0$, $0+x$, $x+x$, $0+0$, $g(x)$, $g(0)$. Из слов веса 2 укажем $g(x)+0$, $f(x, x, 0)+f(0, 0, 0)$, $f(x+x, 0, g(0))$ и $g(f(x, x, x))$. В качестве слова веса 4 приведем

$$([f(x, x, x)+g(0)]+g(x+x))+f(g(x+0), x, f(x, x, x)).$$

Подсловом слова веса 0 назовем само это слово. Если w — слово веса $m > 0$, то $w = f(u_1, \ldots, u_n)$, где f — n-арная операция из Ω, а u_i — слова веса $m-1$. *Подсловами* слова w назовем само w, слова $u_1, \ldots, u_n$, а также все их подслова, которые можно считать уже определенными. Например, подсловами последнего из рассмотренных выше слов служат 0, x, $x+x$, $x+0$, $f(x, x, x)$, $g(0)$, $g(x+x)$, $g(x+0)$, $f(x, x, x)+g(0)$, $f(g(x+0), x, f(x, x, x))$ и $[f(x, x, x)+g(0)]+g(x+x)$, а также само это слово.

Совокупность W всех слов сигнатуры Ω в алфавите X естественным образом превращается в алгебру той же сигнатуры. Для этого полагаем $\nu(W) = \nu$, если ν — нульарная операция из Ω, а слово $f(u_1, \ldots, u_n)$, где $u_i \in W$, а f — n-арная операция из Ω и $n \geqslant 1$, считаем результатом применения операции f к словам $u_1, \ldots, u_n$. Эта алгебра называется *алгеброй слов сигнатуры Ω в алфавите X* или *абсолютно свободной алгеброй сигнатуры Ω со свободной порождающей системой X*.

Пусть w — слово сигнатуры Ω в алфавите X и $x_1, \ldots, x_s$ — элементы из X, являющиеся подсловами слова w. Эту ситуацию мы часто будем изображать символически как $w = w(x_1, \ldots, x_s)$. Впрочем, та же запись будет использоваться и в том случае, когда среди x_i есть и лишние буквы, т. е. буквы, не являющиеся подсловами слова w. Если A — алгебра сигнатуры Ω и $a_1, \ldots, a_s \in A$, то положим

$$w(a_1, \ldots, a_s) = \begin{cases} a_i, & \text{если } w = x_i, \\ \nu(A), & \text{если } w = \nu, \text{ где } \nu \text{ — 0-арная операция из } \Omega, \\ f(u_1(a_1, \ldots, a_s), \ldots, u_n(a_1, \ldots, a_s)), & \text{если } w = f(u_1, \ldots, u_n), \text{ где } n \geqslant 1 \\ & \text{и } f \text{ — } n\text{-арная операция из } \Omega \end{cases}$$

(в последнем случае, разумеется, предполагается, что для слов u, вес которых меньше веса слова w, элементы $u(a_1, \ldots, a_s) \in A$ уже определены).

Элемент $w(a_1, \ldots, a_s) \in A$ и называется *результатом подстановки элементов $a_1, \ldots, a_s$ в слово w*. Наглядно это означает, что мы заменяем буквы x_i элементами a_i, а символы ν элементами $\nu(A)$ и выполняем операции из Ω в порядке, предписанном строением слова w.

Предложение 5. *Если A — алгебра сигнатуры Ω, порожденная множеством X, и W — абсолютно свободная алгебра сигнатуры Ω со свободной порождающей систе-*

мой X, то множество A совпадает с множеством B результатов всевозможных подстановок элементов множества X, рассматриваемых как элементы алгебры A, во все слова из W и

$$\operatorname{Card} A \leqslant \max\{\operatorname{Card} X,\ \operatorname{Card}\Omega,\ \aleph_0\}.$$

Доказательство. Заметим сначала, что B содержит результаты подстановки элементов множества X в слова веса 0, т. е. элементы $\nu(A)$, где ν — 0-арные операции из Ω, и элементы множества X, рассматриваемые как элементы алгебры A. Если f — n-арная операция из Ω, $n \geqslant 1$, и $u_1, \ldots, u_n \in B$, то можно считать, что $u_i = u_i(x_1, \ldots, x_s)$, где $x_i \in X \subseteq A$ и $u_i \in W$. Но тогда $w = f(u_1, \ldots, u_n) \in W$ и, следовательно, $w(x_1, \ldots, x_s) \in B$, если x_i считать элементами алгебры A. Таким образом, B — подалгебра алгебры A, содержащая X, откуда $A = B$. Далее, обозначим через W_m множество слов веса m сигнатуры Ω в алфавите X и положим

$$\mathfrak{m} = \max\{\operatorname{Card} X,\ \operatorname{Card}\Omega,\ \aleph_0\}.$$

Пусть, наконец, Ω_n — множество n-арных операций, входящих в сигнатуру Ω. Напомним, что $\mathfrak{n}'\mathfrak{n}''$, где $\mathfrak{n}' = \operatorname{Card} Y'$ и $\mathfrak{n}'' = \operatorname{Card} Y''$, по определению, означает $\operatorname{Card}(Y' \times Y'')$. По теореме I.2.2,

$$\operatorname{Card} W_0 = \operatorname{Card}(X \cup \Omega) \leqslant \operatorname{Card}(X \times \Omega) \leqslant \mathfrak{m}^2 = \mathfrak{m}.$$

Используя индуктивное предположение, теорему I.2.2 и предложения I.2.3(а) и I.2.3(в), получаем

$$\operatorname{Card}(W_{m-1}^n \times \Omega_n) \leqslant \mathfrak{m}^2 = \mathfrak{m}.$$

По тем же соображениям отсюда вытекает

$$\operatorname{Card} W_m \leqslant \operatorname{Card}\Big(\bigcup_{1 \leqslant n < \infty} (W_{m-1}^n \times \Omega_n) \cup W_{m-1}\Big) \leqslant \mathfrak{m}\aleph_0 \leqslant \mathfrak{m}^2 = \mathfrak{m}$$

и, следовательно,

$$\operatorname{Card} A \leqslant \operatorname{Card}\Big(\bigcup_{0 \leqslant n < \infty} W_n\Big) \leqslant \mathfrak{m}\aleph_0 \leqslant \mathfrak{m}^2 = \mathfrak{m}.$$

Из предложения 5 непосредственно вытекает:

Следствие. *Если A — алгебра, порожденная множеством X, φ и ψ — гомоморфизмы алгебры A в алгебру B и $\varphi(x) = \psi(x)$ для всех $x \in X$, то $\varphi = \psi$.*

Предложение 6. *Если A — алгебра сигнатуры Ω, W — абсолютно свободная алгебра сигнатуры Ω со свобод-*

ной порождающей системой X *и* φ*—отображение множества* X *в алгебру* A*, то существует единственный гомоморфизм* ψ*:* $W \to A$ *такой, что* $\psi(x) = \varphi(x)$ *для всех* $x \in X$.

Доказательство. Если $w \in W$, то обозначим через $\psi(w)$ результат подстановки в слово w элементов $\varphi(x)$ вместо x для всех $x \in X$. Легко понять, что ψ — гомоморфизм, обладающий нужными свойствами. Его единственность вытекает из следствия предложения 5.

Предложение 7. *Каждая алгебра* A *сигнатуры* Ω *изоморфна фактор-алгебре некоторой абсолютно свободной алгебры сигнатуры* Ω.

Доказательство. Пусть W — абсолютно свободная алгебра сигнатуры Ω со свободной порождающей системой A. В силу предложения 6, тождественное отображение A на A продолжается до гомоморфного наложения W на A. Остается принять во внимание теорему о гомоморфизме (предложение 2).

Будем говорить, что алгебра B *разложена в подпрямое произведение алгебр* A_ι, $\iota \in \Im$, если существует гомоморфное вложение φ алгебры B в прямое произведение $\prod_{\iota \in \Im} A_\iota$, причем, если π_ι — естественные проекции на A_ι, то $\operatorname{Im} \varphi\pi_\iota = A_\iota$ для всех $\iota \in \Im$. Разложение в подпрямое произведение называется *тривиальным*, если $\varphi\pi_\iota$ для некоторого $\iota \in \Im$ оказывается изоморфизмом. Подчеркнем, что, в отличие от прямого произведения, существование подпрямого разложения алгебры почти ничего не говорит о ее строении.

Примеры. 1. Если $B = \prod_{\iota \in \Im} A_\iota$, то можно положить $\varphi = 1_B$.

2. B — произвольная алгебра, $A_i = B$ для всех $i \in \mathbf{N}$ и $\varphi(b) = (b, b, \ldots)$ для всех $b \in B$. Это тривиальное разложение.

3. B — кольцо $\mathbf{Z}$, $\Im = \mathbf{N}$, $A_m = \mathbf{Z}/\mathbf{Z}m$, $m = 1, 2, \ldots$,

$$\varphi(n) = (\pi_1(n), \pi_2(n), \pi_3(n), \ldots),$$

где π_m — естественный гомоморфизм $\mathbf{Z}$ на $\mathbf{Z}/\mathbf{Z}m$.

4. Пусть $R = \Delta[x_1, x_2, \ldots]$ — кольцо многочленов без свободного члена от счетного множества перемеиных над полем Δ, I_i — идеал кольца R, порожденный элементом x_i, φ_i: $R \to R/I_i$ — естественный гомоморфизм. Положим

$$\varphi(f) = (\pi_1(f), \pi_2(f), \ldots)$$

для всякого $f \in R$. Это подпрямое разложение нетривиально, хотя каждое из колец R/I_i изоморфно R.

Предложение 8. *Если A — универсальная алгебра, $\Xi \subseteq \Theta(A)$ и $\bigcap\limits_{\theta \in \Xi} \theta = 0_A$, то отображение* φ: $A \to \prod\limits_{\theta \in \Xi} A/\theta$, *где*

$$\varphi(a) = (\ldots, \theta(a), \ldots),$$

осуществляет подпрямое разложение алгебры A.

Доказательство. Нетрудно проверить, что φ — гомоморфизм алгебры A в $\prod\limits_{\theta \in \Xi} A/\theta$ и что $\operatorname{Im} \varphi\theta = A/\theta$ для всех $\theta \in \Xi$. Если $\varphi(a') = \varphi(a'')$, то $\theta(a') = \theta(a'')$ для всех $\theta \in \Xi$. Отсюда

$$(a', a'') \in \bigcap_{\theta \in \Xi} \theta = 0_A,$$

т. е. $a' = a''$. Таким образом, φ оказывается вложением, т. е. осуществляет подпрямое разложение алгебры A.

Алгебра B называется *подпрямо неразложимой*, если любое ее представление в виде подпрямого произведения тривиально.

Предложение 9. *Алгебра B подпрямо неразложима тогда и только тогда, когда пересечение всех ее ненулевых конгруэнций является ненулевой конгруэнцией.*

Доказательство. Если φ: $B \to \prod\limits_{\iota \in \Im} A_\iota$ — нетривиальное разложение в подпрямое произведение и π_ι — естественные проекции, то $\operatorname{Ker} \varphi\pi_\iota \neq 0_B$ для всех $\iota \in \Im$. Если $(b', b'') \in \bigcap\limits_{\iota \in \Im} \operatorname{Ker} \varphi\pi_\iota$, то $(b'\varphi)\pi_\iota = (b''\varphi)\pi_\iota$ для всех $\iota \in \Im$. Отсюда $b'\varphi = b''\varphi$ и, поскольку, φ — вложение, то $b' = b''$. Таким образом,

$$\bigcap_{0_B \neq \theta \in \Theta(B)} \theta \subseteq \bigcap_{\iota \in \Im} \operatorname{Ker} \varphi\pi_\iota = 0_B.$$

Наоборот, если $\bigcap\limits_{0_B \neq \theta \in \Theta(B)} \theta = 0_B$, то рассмотрим прямое произведение $\prod\limits_{0_B \neq \theta \in \Theta(B)} B/\theta$ и положим

$$\varphi(b) = (\ldots, \theta(b), \ldots)$$

для всех $b \in B$. В силу предложения 8, φ осуществляет подпрямое разложение алгебры B. Если $0_B \neq \theta \in \Theta(B)$, то найдутся $b', b'' \in B$ такие, что $b' \neq b''$, но $\theta(b') = \theta(b'')$.

Отсюда $b'\varphi\theta = b''\varphi\theta$, т. е. $\operatorname{Ker}\varphi\theta \neq 0_B$. Этим доказана нетривиальность полученного разложения.

Из предложения 9 вытекает, в частности, подпрямая неразложимость следующих алгебр: 1) групп, содержащих наименьшую ненулевую нормальную подгруппу (например, абелевых групп порядка p^n, где p — простое число); 2) колец, обладающих наименьшим ненулевым идеалом (например, простых колец, тел, полей, колец вычетов по модулю p^n, где p — простое число).

Теорема 1. *Всякая универсальная алгебра A разлагается в подпрямое произведение подпрямо неразложимых алгебр.*

Доказательство. Если алгебра A подпрямо неразложима, то все ясно. В противном случае, по предложению 9, пересечение ненулевых конгруэнций алгебры A равно 0_A. Другими словами, если $a, b \in A$ и $a \neq b$, то множество

$$\Xi_{a,b} = \{\theta \mid \theta \in \Theta(A),\ \theta \neq 0_A,\ (a, b) \notin \theta\}$$

непусто. Если C — цепь из $\Xi_{a,b}$, то положим

$$\theta_C = \{(x, y) \mid x, y \in A,\ \exists \theta \in C,\ (x, y) \in \theta\}.$$

Тогда для любой n-арной операции f из сигнатуры алгебры A, где $n \geqslant 1$, и любых $(x_i, y_i) \in \theta_C$, $i = 1, \ldots, n$, имеем $(x_i, y_i) \in \theta_i$ для подходящих $\theta_i \in C$. Поскольку C — цепь, имеем $\theta_i \subseteq \theta_{i_0}$ для некоторого i_0 и всех i. Следовательно, $(x_i, y_i) \in \theta_{i_0}$ для всех i, откуда

$$(f(x_1, \ldots, x_n),\ f(y_1, \ldots, y_n)) \in \theta_{i_0},$$

а значит,

$$f((x_1, y_1), \ldots, (x_n, y_n)) = (f(x_1, \ldots, x_n), f(y_1, \ldots, y_n)) \in \theta_C.$$

Следовательно, θ_C — подалгебра алгебры $A \times A$. Ее рефлексивность и симметричность очевидны. Если $(x, y), (y, z) \in \theta_C$, то $(x, y) \in \theta'$ и $(y, z) \in \theta''$, где $\theta', \theta'' \in C$. Поскольку $\theta' \subseteq \theta''$ или $\theta'' \subseteq \theta'$, то (x, y) и (y, z) одновременно принадлежат θ' или θ''. Но тогда $(x, z) \in \theta'$ или θ'', а значит, $(x, z) \in \theta_C$. Таким образом, $\theta_C \in \Theta(A)$, причем $(a, b) \notin \theta_C$. Следовательно, $\theta_C \in \Xi_{a,b}$, причем $\theta_C \supseteq \theta$ для всех $\theta \in C$. По лемме Куратовского — Цорна (см. теорема I.1.2), $\Xi_{a,b}$ содержит максимальный элемент, скажем, $\theta_{a,b}$. Если $x, y \in A$ и $x \neq y$, то $(x, y) \notin \theta_{x,y}$ и, следовательно, $(x, y) \notin \bigcap_{a \neq b} \theta_{a,b}$. Таким образом, $\bigcap_{a \neq b} \theta_{a,b} = 0_A$, и, по предложению 8,

алгебра A разлагается в подпрямое произведение алгебр $A/\theta_{a,b}$. Убедимся, что алгебра $B = A/\theta_{a,b}$ подпрямо неразложима для любых различных $a, b \in A$. В самом деле, если $0_B \neq \bar{\theta} \in \Theta(B)$, то, по предложению 4, $\bar{\theta} = \theta/\theta_{a,b}$, где $\theta_{a,b} \subseteq \theta \in \Theta(A)$. В силу определения конгруэнции $\theta_{a,b}$, $(a, b) \in \theta$. Поэтому, если $\bar{\theta}_0 = \bigcap_{0_B \neq \bar{\theta} \in \Theta(B)} \bar{\theta}$ и $\bar{\theta}_0 = \theta_0/\theta_{a,b}$, то $(a, b) \in \theta_0$. Отсюда $\theta_0 \neq \theta_{a,b}$ и, следовательно, $\bar{\theta}_0 \neq 0_B$. Остается лишь принять во внимание предложение 9.

Упражнения

1. Пусть A — множество, а Ω — множество всех отображений множества A в себя, рассматриваемых как унарные операции. Доказать, что $\varnothing$ и A являются единственными подалгебрами алгебры (A, Ω).

2. Пусть A — линейное пространство над полем P, T — подмножество множества линейных преобразований пространства A и $\Omega = \{+, -, 0\} \cup P \cup T$. Найти все подалгебры алгебры (A, Ω) в следующих случаях: а) T — все линейные преобразования; б) T — все обратимые линейные преобразования; в) T — все линейные преобразования вида $\lambda 1_A$, где $\lambda \in P$.

3. Если все операции алгебры A унарны или 0-арны, то теоретико-множественное объединение любых двух подалгебр является подалгеброй.

4. Объединение возрастающей цепи подалгебр любой алгебры является подалгеброй.

5. Пусть A — абелева группа, а Ω состоит из 0-арной операции 0 и бинарной операции вычитания. Доказать, что подалгебрами алгебры (A, Ω) являются все подгруппы группы A и только они.

6. Пусть A, B и C — произвольные алгебры сигнатуры Ω, а E — одноэлементная алгебра той же сигнатуры. Доказать: а) $A \times B \cong B \times A$; б) $(A \times B) \times C \cong A \times (B \times C)$; в) $A \times E \cong A$.

7. Если $A_{\iota\varkappa}$, $\iota \in \Im$, $\varkappa \in \Im_\iota$, — алгебры сигнатуры Ω, то

$$\prod_{\iota \in \Im,\ \varkappa \in \Im_\iota} A_{\iota\varkappa} \cong \prod_{\iota \in \Im} \left(\prod_{\varkappa \in \Im_\iota} A_{\iota\varkappa} \right).$$

8. Если A_ι, $\iota \in \Im$, — алгебры сигнатуры Ω, $A = \prod_{\iota \in \Im} A_\iota$, $\pi_\iota \colon A \to A_\iota$ — естественные проекции и каждая из алгебр A_ι содержит одноэлементную подалгебру, то существуют гомоморфизмы $\sigma_\iota \colon A_\iota \to A$ такие, что $\sigma_\iota \pi_\iota = 1_{A_\iota}$. Построить пример, показывающий, что требование существования одноэлементных подалгебр существенно.

9. На множестве $A = \{0, 1\}$ определим унарные операции f и g, положив $f(0) = 0 = g(1)$ и $f(1) = 1 = g(0)$. Доказать, что (A, f) и (A, g) не изоморфны, но $(A, f) \times (A, g) \cong (A, g) \times (A, g)$.

10. Пусть A — алгебра, $\theta', \theta'' \in \Theta(A)$ и $\theta = \sup\{\theta', \theta''\}$. Доказать, что $(a, b) \in \theta$ тогда и только тогда, когда существует цепочка $a = x_0, x_1, \ldots, x_{2n} = b$ элементов из A такая, что $(x_{2k}, x_{2k+1}) \in \theta'$ и $(x_{2k+1},$

$x_{2k+2}) \in \theta''$ при $k=0, 1, \ldots, n-1$. Обобщить этот результат для $\sup \Xi$, где $\Xi \subseteq \Theta(A)$.

11. Пусть A—алгебра, B—ее подалгебра, $\theta \in \Theta(A)$ и

$$C = \{x \mid x \in A,\ \exists b \in B\ (x, b) \in \theta\}.$$

Доказать, что C—подалгебра алгебры A.

12. Если A' и A''—алгебры сигнатуры Ω, $\theta' \in \Theta(A')$ и $\theta'' \in \Theta(A'')$, то $\theta' \times \theta'' \in \Theta(A' \times A'')$ и $(A' \times A'')/(\theta' \times \theta'') \cong (A'/\theta') \times (A''/\theta'')$.

13. Если A—группа, θ', $\theta'' \in \Theta(A)$, $\theta' \cap \theta'' = 0_A$ и $\sup\{\theta', \theta''\} = A \times A$, то $A \cong (A/\theta') \times (A/\theta'')$.

14. Пусть A—алгебра сигнатуры Ω. Если $n \geqslant 1$, f—n-арная операция из Ω и $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n \in A$, то унарная операция $u(x) = f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n)$ называется i-м *редуктом* операции f. Пусть $\overline{\Omega}$—множество всех редуктов всех операций $f \in \Omega$. Доказать, что всякая конгруэнция алгебры $(A, \overline{\Omega})$ является конгруэнцией алгебры (A, Ω) и наоборот.

15. Пусть W—абсолютно свободная алгебра сигнатуры Ω со свободной порождающей системой X, $x_0 \in X$ и W'—множество всех слов из W, отличных от x_0. Доказать, что W'—максимальная подалгебра алгебры W и что всякая максимальная подалгебра алгебры W может быть получена таким способом.

16. Доказать, что группа автоморфизмов абсолютно свободной алгебры сигнатуры Ω со свободной порождающей системой X изоморфна группе всех взаимно однозначных отображений множества X на себя.

17. Пусть B—пересечение всех максимальных подалгебр алгебры A, порожденной множеством X, и $b \in B \cap X$. Доказать, что множество $X \setminus \{b\}$ порождает алгебру A.

18. Доказать, что абсолютно свободный *унар* (т. е. алгебра с одной унарной операцией) с одноэлементной свободной порождающей системой изоморфен унару $(\mathbf{N}, f)$, где $f(n) = n+1$, и что моноид эндоморфизмов этого унара изоморфен аддитивному мононду неотрицательных целых чисел. Установить, что абсолютно свободный унар со счетной свободной порождающей системой изоморфен объединению счетного множества попарно не пересекающихся унаров $(\mathbf{N}, f)$.

19. Найти все подпрямо неразложимые абелевы группы.

20. Доказать, что унар (A, f) подпрямо неразложим тогда и только тогда, когда он имеет вид или $A = \{y_0, y_1, y_2, \ldots\}$, где $f(y_i) = y_{i-1}$ для $i \geqslant 1$ и $f(y_0) = y_0$, или $A = \{x_1, \ldots, x_m, y\}$, где m—единица или степень простого числа, $f(x_i) = x_{i+1}$, если $1 \leqslant i < m$, $f(x_m) = x_1$ и $f(y) = y$, или A—подалгебра $\{x_1, \ldots, x_m\}$ указанной выше алгебры.

21. Пусть A_i, $i = 1, 2, \ldots$,—изоморфные друг другу алгебры, содержащие собственные одноэлементные подалгебры, и $A = \prod_{i \in \mathbf{N}} A_i$. Доказать, что A допускает разложение в прямое произведение алгебр, изоморфных A, не являющееся тривиальным разложением в подпрямое произведение.

§ 2. Многообразия

Формальное выражение $u = v$, где u и v—слова сигнатуры Ω в счетном алфавите X, называется *тождеством* сигнатуры Ω. Скажем, что в алгебре A *выполняется тож-*

дество $u = v$, если после замены букв любыми элементами алгебры A и осуществления входящих в слова u и v операций слева и справа получается один и тот же элемент алгебры A. Другими словами, если тождество имеет вид

$$u(x_1, \ldots, x_m) = v(x_1, \ldots, x_m),$$

где $x_i \in X$, то для любых $a_1, \ldots, a_m \in A$ в алгебре A имеет место равенство

$$u(a_1, \ldots, a_m) = v(a_1, \ldots, a_m).$$

Класс $\mathfrak{M}$ алгебр сигнатуры Ω называется *многообразием*, если существует множество Σ тождеств сигнатуры Ω такое, что алгебра сигнатуры Ω принадлежит классу $\mathfrak{M}$ тогда и только тогда, когда в ней выполняются все тождества из множества Σ. Многочисленные примеры многообразий приведены в § 3. Примеры классов, не являющихся многообразиями, будут указаны после доказательства приводимой ниже теоремы 1.

Пусть $\mathfrak{K}$ — непустой класс алгебр сигнатуры Ω, а X — непустое множество. Алгебра F из класса $\mathfrak{K}$ называется *свободной алгеброй класса* $\mathfrak{K}$ *со свободной порождающей системой* X, если: 1) существует отображение $\varkappa$ множества X в алгебру F; 2) алгебра F порождается множеством $\operatorname{Im}\varkappa$; 3) (свойство универсальности) если A — алгебра из $\mathfrak{K}$ и φ — отображение множества X в алгебру A, то существует гомоморфизм ψ: $F \to A$ такой, что $\varkappa\psi = \varphi$. Подчеркнем, что в свойстве 1) не требуется, чтобы отображение $\varkappa$ было вложением. Однако имеет место:

Предложение 1. *Если* F *— свободная алгебра класса* $\mathfrak{K}$, *содержащего не только одноэлементные алгебры, то отображение* $\varkappa$ *является вложением.*

Доказательство. Допустим, что $x, y \in X$, $x \neq y$, $\varkappa(x) = \varkappa(y)$ и алгебра $A \in \mathfrak{K}$ содержит различные элементы a и b. Тогда ясно, что для отображения φ: $X \to A$, где

$$\varphi(z) = \begin{cases} a, & \text{если } z = x, \\ b, & \text{если } z \neq x, \end{cases}$$

невозможно найти гомоморфизм ψ, указанный в свойстве 3).

Предложение 2. *Если класс* $\mathfrak{K}$ *замкнут относительно подалгебр* (т. е. вместе со всякой алгеброй содержит все ее непустые подалгебры) *и прямых произведений* (т. е. вместе с любым множеством алгебр содержит и их

прямое произведение), *то для любого непустого множества* X *класс* $\mathfrak{K}$ *содержит свободную алгебру со свободной порождающей системой* X.

Доказательство. Рассмотрим множество Ξ' всех попарно не изоморфных алгебр из класса $\mathfrak{K}$, мощность которых не превосходит $\mathfrak{m} = \aleph_0 (\operatorname{Card} X)(\operatorname{Card} \Omega)$. Пусть Ξ — множество всех пар $(A_\alpha, \varphi_\alpha)$, где $A_\alpha \in \Xi'$, а φ_α — отображение множества X в алгебру A_α. Рассмотрим прямое произведение $H = \prod_{(A_\alpha, \varphi_\alpha) \in \Xi} A_\alpha$ и отображение $\varkappa$: $X \to H$, где

$$\varkappa(x) = (\ldots, \varphi_\alpha(x), \ldots).$$

Пусть F — подалгебра алгебры H, порожденная множеством $\operatorname{Im}\varkappa$. По условию, $F \in \mathfrak{K}$. Ясно, что F обладает свойствами 1) и 2) из определения свободной алгебры. Допустим, что A — алгебра из $\mathfrak{K}$ и φ — отображение из X в A. Ввиду предложения 1.5, $\operatorname{Im}\varphi$ порождает подалгебру A' мощности, не превосходящей $\mathfrak{m}$. Следовательно, для некоторой пары $(A_\alpha, \varphi_\alpha) \in \Xi$ имеем $\varphi_\alpha = \varphi\chi$, где χ: $A' \to A_\alpha$ — изоморфизм. Положив $\psi = \pi_\alpha \chi^{-1}$, где π_α — естественная проекция H на A_α, для любого $x \in X$ получим

$$x\varkappa\psi = x\varkappa\pi_\alpha\chi^{-1} = x\varphi_\alpha\chi^{-1} = x\varphi\chi\chi^{-1} = x\varphi,$$

т. е. $\varkappa\psi = \varphi$.

Класс алгебр называется *абстрактным*, если вместе с любой алгеброй он содержит и все алгебры, изоморфные ей.

Теорема 1. *Непустой абстрактный класс алгебр* $\mathfrak{M}$ *сигнатуры* Ω *является многообразием в том и только в том случае, когда* $\mathfrak{M}$ *замкнут относительно подалгебр, фактор-алгебр* (т. е. вместе со всякой алгеброй содержит и все ее фактор-алгебры) *и прямых произведений.*

Доказательство. Необходимость указанных свойств легко усматривается из соответствующих определений. Допустим теперь, что класс $\mathfrak{M}$ обладает перечисленными свойствами. Если $\mathfrak{M}$ содержит лишь одноэлементные алгебры, то $\mathfrak{M}$ — многообразие, определяемое тождеством $x = y$. Так что будем считать, что $\mathfrak{M}$ содержит не только одноэлементные алгебры. По предложению 2, класс $\mathfrak{M}$ содержит свободную алгебру F со счетной свободной порождающей системой $X = \{x_1, x_2, \ldots\}$, причем, по предложению 1, $X \subseteq F$. Пусть W — абсолютно свободная алгебра сигнатуры Ω с той же свободной порождаю-

щей системой. По предложению 1.6, тождественное отображение множества X на себя продолжается до гомоморфизма φ: $W \longrightarrow F$. Положим

$$\Sigma = \{u = v \mid u,\ v \in W,\ (u, v) \in \operatorname{Ker}\varphi\}$$

и рассмотрим многообразие $\mathfrak{M}'$, определенное этой системой тождеств. Если $A \in \mathfrak{M}$, $(u(x_1, \ldots, x_s) = v(x_1, \ldots, x_s)) \in \Sigma$ и $a_1, \ldots, a_s \in A$, то по свойству универсальности свободной алгебры существует гомоморфизм ψ: $F \longrightarrow A$ такой, что $\psi(x_i) = a_i$, $i = 1, \ldots, s$. Но в алгебре F справедливо равенство $u(x_1, \ldots, x_s) = v(x_1, \ldots, x_s)$ и, следовательно

$$u(a_1, \ldots, a_s) = \psi(u(x_1, \ldots, x_s)) = \psi(v(x_1, \ldots, x_s)) = v(a_1, \ldots, a_s).$$

Этим доказано, что $A \in \mathfrak{M}'$, т. е. что $\mathfrak{M} \subseteq \mathfrak{M}'$. Допустим теперь, что $A \in \mathfrak{M}'$. В силу предложения 1.7, $A \cong V/\theta$, где V — абсолютно свободная алгебра сигнатуры Ω со свободной порождающей системой Y. Пусть π: $V \longrightarrow A$ — естественный гомоморфизм (рис. 1). По предложению 2, существует свободная алгебра G класса $\mathfrak{M}$ со свободной порождающей системой Y, а предложения 1.7 и 1 обеспечивают существование такого гомоморфного наложения ψ: $V \longrightarrow G$, что $y\psi = y$ для всех $y \in Y$. По теореме о гомоморфизме (предложение 1.2), $G \cong V/\operatorname{Ker}\psi$. Если

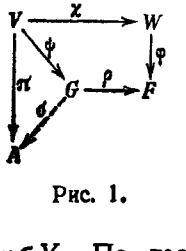


Рис. 1.

$$(u(y_1, \ldots, y_s),\ v(y_1, \ldots, y_s)) \in \operatorname{Ker}\psi,$$

то, воспользовавшись предложением 1.6, найдем гомоморфизм χ: $V \longrightarrow W$ такой, что $\chi(y_i) = x_i$. По свойству универсальности, существует гомоморфизм ρ: $G \longrightarrow F$ такой, что $\rho(y_i) = \varphi(x_i) = x_i$ для $i = 1, \ldots, s$. Поэтому в алгебре F справедливы равенства

$$u(x_1, \ldots, x_s) = (u(y_1, \ldots, y_s))\psi\rho = (v(y_1, \ldots, y_s))\psi\rho = v(x_1, \ldots, x_s),$$

т. е. $(u = v) \in \Sigma$. Но тогда в алгебре A имеет место

$$u(y_1\pi, \ldots, y_s\pi) = v(y_1\pi, \ldots, y_s\pi),$$

откуда

$$u(y_1, \ldots, y_s)\pi = v(y_1, \ldots, y_s)\pi,$$

т. е.

$$(u(y_1, \ldots, y_s),\ v(y_1, \ldots, y_s)) \in \operatorname{Ker}\pi.$$

Таким образом, $\operatorname{Ker}\psi \subseteq \operatorname{Ker}\pi$, и, по предложению 1.3, существует такой гомоморфизм $\sigma\colon G \to A$, что $\psi\sigma = \pi$. При этом σ — наложение, поскольку π — наложение. По теореме о гомоморфизме (предложение 1.2), $A \cong G/\operatorname{Ker}\sigma$, и, поскольку $\mathfrak{M}$ замкнуто относительно гомоморфных образов, то $A \in \mathfrak{M}$. Таким образом, $\mathfrak{M}' \subseteq \mathfrak{M}$, а значит, $\mathfrak{M} = \mathfrak{M}'$.

Теорема 2 (Фудзивара). *Пусть F — свободная алгебра многообразия $\mathfrak{M}$ сигнатуры Ω, содержащего неодноэлементные алгебры, X и Y — свободные порождающие системы алгебры F и множество X бесконечно. Тогда X и Y — равномощные множества.*

Доказательство. Если $\operatorname{Card} X \neq \operatorname{Card} Y$, то можно считать, что $\operatorname{Card} X > \operatorname{Card} Y$. Предложение 1 позволяет предполагать, что $X, Y \subseteq F$. Поскольку X порождает F, то, по предложению 1.5, для каждого $y \in Y$ имеет место равенство $y = w_y$, где w_y — некоторое слово сигнатуры Ω в алфавите X. Пусть Z — множество всех букв алфавита X, встречающихся хотя бы в одном из слов w_y. Если Y конечно, то, ввиду предложения I.2.3(г),

$$\operatorname{Card} Z < \aleph_0 \leqslant \operatorname{Card} X.$$

Если же Y бесконечно, то произвольным образом перенумеруем буквы, входящие в каждое из слов w_y. Далее для каждой буквы $x \in Z$ выберем одно из содержащих ее слов w_y и положим $\varphi(x) = (y, i)$, где i — номер буквы x в выбранном слове w_y. Ясно, что φ — вложение множества Z в прямое произведение $Y \times \mathbf{Z}$. Поэтому, учитывая предложения I.2.3(в) и (г) и теорему I.2.2, получаем

$$\operatorname{Card} Z \leqslant \operatorname{Card}(Y \times \mathbf{Z}) \leqslant \operatorname{Card}(Y \times Y) = \operatorname{Card} Y < \operatorname{Card} X.$$

Таким образом, в обоих случаях найдется буква $x_0 \in X \setminus Z$. Но $x_0 = v(y_1, \ldots, y_m)$, где v — некоторое слово сигнатуры Ω в алфавите Y. Отсюда

$$x_0 = v(w_{y_1}, \ldots, w_{y_m}) = u(x_1, \ldots, x_s),$$

где u — слово сигнатуры Ω в алфавите X, зависящее от букв $x_1, \ldots, x_s$, отличных от x_0. Пусть теперь A — алгебра из $\mathfrak{M}$, содержащая более одного элемента. Выберем $a \in A$ и $b \neq u(a, \ldots, a)$. Рассмотрим отображение $\varphi\colon X \to A$, где

$$\varphi(x) = \begin{cases} a, & \text{если } x \neq x_0, \\ b, & \text{если } x = x_0. \end{cases}$$

По свойству универсальности, φ продолжается до гомоморфизма ψ: $F \to A$. Тогда

$$b = \varphi(x_0) = \psi(x_0) = \psi(u(x_1, \ldots, x_s)) =$$
$$= u(\psi(x_1), \ldots, \psi(x_s)) = u(\varphi(x_1), \ldots, \varphi(x_s)) =$$
$$= u(a, \ldots, a) \neq b.$$

Противоречие.

Убедимся, что требование бесконечности множества X в теореме Фудзивары существенно. В самом деле, рассмотрим многообразие $\mathfrak{M}$ сигнатуры $\{\cdot, f, g\}$, где $\cdot$ — бинарная, а f и g — унарные операции, определяемые тождествами $f(x)g(x) = x$, $f(xy) = x$ и $g(xy) = y$. Это многообразие содержит двухэлементную алгебру $A = \{a, b\}$, где $ab = a = aa$, $ba = b = bb$, $f(a) = a = g(b)$, $f(b) = b = g(a)$. Пусть F и G — свободные алгебры многообразия $\mathfrak{M}$ со свободными порождающими системами $\{x\}$ и $\{u, v\}$ соответственно. Свойство универсальности обеспечивает существование таких гомоморфизмов φ: $F \to G$ и ψ: $G \to F$, что $x\varphi = uv$, $u\psi = f(x)$ и $v\psi = g(x)$. Тогда

$$x(\varphi\psi) = (uv)\psi = u\psi \cdot v\psi = f(x)g(x) = x,$$
$$u(\psi\varphi) = (f(x))\varphi = f(x\varphi) = f(uv) = u$$

и

$$v(\psi\varphi) = (g(x))\varphi = g(x\varphi) = g(uv) = v.$$

Отсюда $\varphi\psi = 1_F$ и $\psi\varphi = 1_G$, по следствию предложения 1.5, а значит, φ и ψ — изоморфизмы.

Подобный пример может быть найден и в многообразии модулей (см. § 3).

Если A — универсальная алгебра и $\theta', \theta'' \in \Theta(A)$, то положим

$$\theta' \circ \theta'' = \{(a, b) \mid a, b \in A, \exists x \in A\, (a, x) \in \theta' \& (x, b) \in \theta''\}.$$

Конгруэнции θ' и θ'' называются *перестановочными*, если $\theta' \circ \theta'' = \theta'' \circ \theta'$.

Предложение 3. *Если θ' и θ'' — перестановочные конгруэнции алгебры A, то $\theta' \circ \theta'' \in \Theta(A)$ и $\sup\{\theta', \theta''\} = \theta' \circ \theta''$.*

Доказательство. Ясно, что $(a, a) \in \theta' \circ \theta''$ для всех $a \in A$. Если $(a, b) \in \theta' \circ \theta''$, то, в силу перестановочности, $(a, x) \in \theta''$ и $(x, b) \in \theta'$ для некоторого $x \in A$, и, следовательно, $(b, a) \in \theta' \circ \theta''$, ввиду симметричности подмножеств θ' и θ''. Если (a, b), $(b, c) \in \theta' \circ \theta''$, то для подходящих $x, y \in A$ имеем $(a, x), (b, y) \in \theta'$ и $(x, b), (y, c) \in \theta''$. Отсюда

$(y, x) \in \theta' \circ \theta'' = \theta'' \circ \theta'$ и, следовательно, $(y, z) \in \theta''$ и $(z, x) \in \theta'$ для некоторого $z \in A$. Тогда $(a, z) \in \theta'$ и $(z, c) \in \theta''$, т. е. $(a, c) \in \theta' \circ \theta''$. Таким образом, подмножество $\theta' \circ \theta''$ рефлексивно, симметрично и транзитивно. Пусть $n \geqslant 1$, f — n-арная операция из сигнатуры алгебры A и $(x_i, y_i) \in \theta' \circ \theta''$, $i = 1, \ldots, n$. Тогда $(x_i, z_i) \in \theta'$ и $(z_i, y_i) \in \theta''$ для подходящих $z_i \in A$. Отсюда

$$(f(x_1, x_2, \ldots, x_n), f(z_1, x_2, \ldots, x_n)) \in \theta',$$
$$(f(z_1, x_2, \ldots, x_n), f(y_1, x_2, \ldots, x_n)) \in \theta'',$$
$$(f(y_1, x_2, \ldots, x_n), f(y_1, z_2, \ldots, x_n)) \in \theta',$$
$$(f(y_1, z_2, x_3, \ldots, x_n), f(y_1, y_2, x_3, \ldots, x_n)) \in \theta'',$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(f(y_1, \ldots, y_{n-1}, x_n), f(y_1, \ldots, y_{n-1}, z_n)) \in \theta',$$
$$(f(y_1, \ldots, y_{n-1}, z_n), f(y_1, \ldots, y_{n-1}, y_n)) \in \theta''.$$

Следовательно,

$$(f(x_1, x_2, \ldots, x_n), f(y_1, x_2, \ldots, x_n)) \in \theta' \circ \theta'',$$
$$(f(y_1, x_2, \ldots, x_n), f(y_1, y_2, \ldots, x_n)) \in \theta' \circ \theta'',$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(f(y_1, \ldots, y_{n-1}, x_n), f(y_1, y_2, \ldots, y_n)) \in \theta' \circ \theta''.$$

В силу установленной выше транзитивности множества $\theta' \circ \theta''$ отсюда вытекает

$$(f(x_1, x_2, \ldots, x_n), f(y_1, y_2, \ldots, y_n)) \in \theta' \circ \theta'',$$

что доказывает включение $\theta' \circ \theta'' \in \Theta(A)$. Далее, ясно, что $\theta', \theta'' \leqslant \theta' \circ \theta''$. Если же $\theta \in \Theta(A)$, $\theta', \theta'' \leqslant \theta$ и $(x, y) \in \theta' \circ \theta''$, то $(x, z) \in \theta'$ и $(z, y) \in \theta''$ для некоторого $z \in A$. Отсюда (x, z), $(x, y) \in \theta$, а значит, $(x, y) \in \theta$. Этим доказано, что $\theta' \circ \theta'' = \sup\{\theta', \theta''\}$.

Теорема 3 (Мальцев). *Конгруэнции любой алгебры многообразия $\mathfrak{M}$ сигнатуры Ω попарно перестановочны тогда и только тогда, когда абсолютно свободная алгебра сигнатуры Ω со свободной порождающей системой $\{x, y, z\}$ содержит такое слово $w(x, y, z)$, что во всех алгебрах из $\mathfrak{M}$ справедливы тождества $w(x, x, z) = z$ и $w(x, z, z) = x$.*

Доказательство. Если конгруэнции всех алгебр из $\mathfrak{M}$ перестановочны, то рассмотрим свободную алгебру F многообразия $\mathfrak{M}$ со свободной порождающей системой $\{x, y, z\}$ и гомоморфизмы φ' и φ'' алгебры F в свободную алгебру G многообразия $\mathfrak{M}$ со свободной порождающей системой $\{u, v\}$, где $\varphi'(x) = \varphi'(y) = \varphi''(x) = u$ и

$\varphi'(z)=\varphi''(y)=\varphi''(z)=v$. Тогда $(x,\ z)\in \operatorname{Ker}\varphi'\circ\operatorname{Ker}\varphi''=$ $=\operatorname{Ker}\varphi''\circ\operatorname{Ker}\varphi'$ и, следовательно, $(x, w)\in\operatorname{Ker}\varphi''$ и $(w, z)\in$ $\in\operatorname{Ker}\varphi'$ для некоторого слова $w=w(x,\ y,\ z)$. Отсюда

$$w(u,\ u,\ v)=\varphi'(w(x,\ y,\ z))=\varphi'(w)=\varphi'(z)=v$$

и

$$w(u,\ v,\ v)=\varphi''(w(x,\ y,\ z))=\varphi''(w)=\varphi''(x)=u.$$

Теперь, найдя гомоморфизм ψ алгебры G в алгебру F, для которого $\psi(u)=x$ и $\psi(v)=z$, получим

$$z=\psi(v)=\psi(w(u,\ u,\ v))=w(x,\ x,\ z)$$

и

$$x=\psi(u)=\psi(w(u,\ v,\ v))=w(x,\ z,\ z),$$

что и требовалось. Если, наоборот, указанное в формулировке слово w существует, $A\in\mathfrak{M}$, θ', $\theta''\in\Theta(A)$ и $(a,\ b)\in\theta'\circ\theta''$, то $(a,\ c)\in\theta'$ и $(c,\ b)\in\theta''$ для некоторого $c\in A$. Отсюда, поскольку $a=w(a, b, b)$, имеем $(a, w(a, c, b))\in$ $\in\theta''$, а поскольку $b=w(a,\ a,\ b)$, то $(w(a,\ c,\ b),\ b)\in\theta'$. Следовательно, $(a, b)\in\theta''\circ\theta'$. Таким образом, $\theta'\circ\theta''\subseteq\theta''\circ\theta'$. Обратное включение доказывается аналогично.

Следствие 1. *Если сигнатура многообразия $\mathfrak{M}$ содержит групповые операции, то конгруэнции любой алгебры из $\mathfrak{M}$ перестановочны.*

Для доказательства достаточно заметить, что для групповых операций слово $w(x,\ y,\ z)=xy^{-1}z$ удовлетворяет условиям теоремы 3.

В частности,

Следствие 2. *Конгруэнции любого мультиоператорного кольца перестановочны.*

Во всех предыдущих рассмотрениях сигнатура алгебр предполагалась фиксированной. Заметим, однако, что при заданной сигнатуре Ω каждое слово $w=w(x_1,\ \ldots,\ x_m)$ сигнатуры Ω в счетном алфавите можно рассматривать как m-арную операцию. Так что каждую алгебру сигнатуры Ω можно рассматривать как алгебру сигнатуры $W(\Omega)$, где $W(\Omega)$ — множество слов сигнатуры Ω в счетном алфавите. Таким образом, с каждым многообразием $\mathfrak{M}$ сигнатуры Ω связано многообразие $W(\mathfrak{M})$ сигнатуры $W(\Omega)$. Многообразия $\mathfrak{M}$ и $\mathfrak{M}'$ сигнатур Ω и Ω' соответственно называются *эквивалентными в смысле Мальцева*, если $W(\mathfrak{M})=W'(\mathfrak{M}')$. В гл. III (теоремы 4.2 и 4.3) будет доказана эквивалентность в смысле Мальцева многообразий булевых колец

и булевых алгебр. В качестве другого примера установим следующий результат:

Теорема 4. *Многообразие* $\mathfrak{M}$ *сигнатуры* $\Omega = \{0, -\}$, *где* 0 — *нульарная, а* $-$ — *бинарная операция, определяемое тождествами*: (а) $x - x = 0$; (б) $0 - (0 - x) = x$; (в) $(x - y) - z = (x - z) - y$, *эквивалентно в смысле Мальцева многообразию абелевых групп в сигнатуре* $\{+, -, 0\}$, *где* $+$ — *бинарная,* $-$ — *унарная, а* 0 — 0-*арная операции.*

Доказательство. Если A — абелева группа, то, положив $a - b = a + (-b)$, нетрудно убедиться в справедливости свойств (а) — (в). Допустим теперь, что A — алгебра сигнатуры $\{0, -\}$, удовлетворяющая тождествам (а) и (в). Положим $-a = 0 - a$ и $a + b = a - (0 - b)$. Тогда из (а) вытекает

$$(-x) + x = (0 - x) - (0 - x) = 0,$$

из (б) —

$$0 + x = 0 - (0 - x) = x,$$

из (б) и (в) —

$$x + y = x - (0 - y) = (0 - (0 - x)) - (0 - y) =$$
$$= (0 - (0 - y)) - (0 - x) = y - (0 - x) = y + x.$$

Отсюда, используя (в), выводим

$$(x + y) + z = (y + x) + z = (y - (-x)) - (-z) =$$
$$= (y - (-z)) - (-x) = (y + z) + x = x + (y + z).$$

Упражнения

1. Свободные алгебры класса $\mathfrak{K}$ с равномощными свободными порождающими системами изоморфны.

2. Если F — свободная алгебра класса $\mathfrak{K}$ со свободной порождающей системой X и F' — подалгебра в F, порожденная подмножеством $X' \subseteq X$, то F' — свободная алгебра класса $\mathfrak{K}$ со свободной порождающей системой X'.

3. Доказать, что для всякого класса $\mathfrak{K}$ алгебр сигнатуры Ω существует наименьшее многообразие $\mathfrak{M}$, содержащее $\mathfrak{K}$, и что каждая алгебра из $\mathfrak{M}$ изоморфна фактор-алгебре подалгебры подпрямого произведения некоторых алгебр из $\mathfrak{K}$.

4. Пусть F — свободная алгебра класса $\mathfrak{K}$ со свободной порождающей системой X, θ — эквивалентность на X (т. е. конгруэнция множества X с пустой сигнатурой) и $\overline{\theta}$ — наименьшая конгруэнция из $\Theta(F)$, содержащая θ. Доказать, что свободная алгебра класса $\mathfrak{K}$ со свободной порождающей системой X/θ изоморфна фактор-алгебре $F/\overline{\theta}$.

5. Пусть W — абсолютно свободная алгебра сигнатуры Ω со свободной порождающей системой X, $\mathfrak{M}$ — многообразие сигнатуры Ω, θ — совокупность всех тождеств, справедливых на всех алгебрах из $\mathfrak{M}$,

рассматриваемая как подмножество алгебры $W \times W$. Доказать: а) $\theta \in \Theta(W)$; б) если φ — эндоморфизм алгебры W и $(\omega', \omega'') \in \theta$, то $(\varphi(\omega'), \varphi(\omega'')) \in \theta$; в) фактор-алгебра W/θ изоморфна свободной алгебре многообразия $\mathfrak{M}$ со свободной порождающей системой X.

6. Пусть $\mathfrak{M}$ — многообразие сигнатуры $\{f, 0\}$, где f — унарная, а 0 — нульарная операции, определяемое тождеством $f(0) = 0$. Доказать, что каждая свободная алгебра многообразия $\mathfrak{M}$ является объединением абсолютно свободного и одноэлементного унаров (см. упр. 18 § 1) без общих элементов.

7. Если конгруэнции алгебры перестановочны, то перестановочны и конгруэнции любой ее фактор-алгебры.

8. Пусть (A, f) — *связный унар* (т. е. для любых $x, y \in A$ имеем $f^k(x) = f^l(y)$ для подходящих k и l). Доказать, что конгруэнции унара A перестановочны тогда и только тогда, когда или $A = \{x_0, x_1, \ldots, x_n\}$, где $f(x_i) = x_{i-1}$ при $i \geqslant 1$ и $f(x_0) = x_0$, или $A = \{x_0, x_1, x_2, \ldots\}$, где $f(x_i) = x_{i-1}$ при $i \geqslant 1$ и $f(x_0) = x_0$, или $A = \{y_1, \ldots, y_n\}$, где $f(y_i) = y_{i+1}$, если $1 \leqslant i < n$, и $f(y_n) = y_1$.

9. Пусть A_ι, $\iota \in \mathfrak{I}$, алгебры из многообразия $\mathfrak{M}$. Алгебра $A \in \mathfrak{M}$ называется *копроизведением алгебр* A_ι, если существуют гомоморфизмы $\varkappa_\iota$: $A_\iota \longrightarrow A$, объединение $\bigcup_{\iota \in \mathfrak{I}} \operatorname{Im} \varkappa_\iota$ порождает алгебру A и для любой алгебры $B \in \mathfrak{M}$ и любых гомоморфизмов φ_ι: $A_\iota \longrightarrow B$ существует такой гомоморфизм φ: $A \longrightarrow B$, что $\varkappa_\iota \varphi = \varphi_\iota$ для всех $\iota \in \mathfrak{I}$. Доказать: а) для любого множества алгебр многообразия $\mathfrak{M}$ существует их копроизведение; б) всякая свободная алгебра многообразия $\mathfrak{M}$ изоморфна копроизведению свободных алгебр многообразия $\mathfrak{M}$ с одноэлементным свободным порождающим множеством; в) копроизведение абелевых групп [модулей] изоморфно их прямой сумме.

10. Многообразие сигнатуры $\{1, :\}$, где 1 — нульарная, а $:$ — бинарная операции, определяемое тождествами $(x:x) = 1$, $1:(1:x) = x$ и $(x:z):(y:z) = x:y$, эквивалентно в смысле Мальцева многообразию групп в сигнатуре $\{\cdot, {}^{-1}, 1\}$.

Указание. Положить $a:b = ab^{-1}$. Затем доказать, что $a:1 = a$, и $((1:a):b):(1:b) = 1:a$, после чего положить $ab = a:(1:b)$ и $a^{-1} = 1:a$.

§ 3. Свободные алгебры классических алгебраических систем

В таблице 1 приведен ряд многообразий. Бо́льшая часть из них хорошо известна, о некоторых пойдет речь в последующих главах. В силу предложения 1.7, свободная алгебра многообразия $\mathfrak{M}$ сигнатуры Ω является фактор-алгеброй абсолютно свободной алгебры сигнатуры Ω. Поэтому для получения описания свободной алгебры многообразия $\mathfrak{M}$ достаточно в каждом классе соответствующей конгруэнции отметить некоторое слово. Поскольку определение группоида никаких тождеств не содержит, свободный группоид — это абсолютно свободная алгебра сигнатуры, содержащей в точности одну бинарную операцию.

ТАБЛИЦА 1

	Название	Сигнатура					Тождества	Примечание
		Число операций	n-арные операции					
			$n=0$	1	2	3		
1.	Группоиды	1			$\cdot$			
2.	Полугруппы	1			$\cdot$		(1) $(xy)z=x(yz)$;	
3.	Моноиды	2	1		$\cdot$		(1) и (2) $x1=1x=x$;	
4.	Группы	3	1	$^{-1}$	$\cdot$		(1), (2) и (3) $x^{-1}x=xx^{-1}=1$;	
5.	Абелевы группы	3	0	—	$+$		(1′) $(x+y)+z=x+(y+z)$; (2′) $x+0=0+x=x$; (3′) $x+(-x)=0$; (4′) $x+y=y+x$;	
6.	Кольца (не обязательно ассоциативные)	4	0	—	$+$, $\cdot$		(1′)—(4′) (5) $(x+y)z=xz+yz$; (6) $x(y+z)=xy+xz$;	
7.	Ассоциативное кольцо	4	0	—	$+$, $\cdot$		(1′)—(4′), (5), (6), (1)	
8.	Ассоциативное кольцо с единицей	5	0, 1	—	$+$, $\cdot$		(1′)—(4′), (5), (6), (1) и (2);	

ТАБЛИЦА 1 (продолжение)

	Название	Сигнатура					Тождества	Примечание
		Число операций	n-арные операции					
			$n=0$	1	2	3		
9.	Ассоциативное коммутативное кольцо с единицей	5	0, 1	—	$+$, $\cdot$		(1′)—(4′), (5), (6), (1), (2) и (4) $xy=yx$;	
10.	Кольцо Ли	4	0	—	$+$, $\cdot$		(1′)—(4′), (5), (6), (7) $xx=0$; (8) $(xy)z+(yz)x+(zx)y=0$;	см. § V. 4
11.	Структура (решетка)	2			$+$, $\cdot$		(1), (4), (1′), (4′), (9′) $xx=x$; (9′) $x+x=x$; (10) $x(x+y)=x$; (10′) $x+xy=x$;	см. § III. 1
12.	Полуструктура	1			$\cdot$		(1), (4), (9);	
13.	Булева алгебра	5	0, 1	$'$	$+$, $\cdot$		(1), (4), (1′), (4′), (9) (9′), (10), (10′), (5), (11) $x0=0$; (11′) $x+1=1$; (12) $xx'=0$; (12′) $x+x'=1$; (13) $x''=x$	см. § III. 4
14.	Правый модуль над ассоциативным кольцом R с единицей	$3+\|R\|$	0	—, λ, где $\lambda\in R$	$+$		(1′)—(4′), (14) $(x+y)\lambda=x\lambda+y\lambda$; (15) $x(\lambda+\mu)=x\lambda+x\mu$; (16) $x(\lambda\mu)=(x\lambda)\mu$;	Тождества (15) и (16) означают $\|R\times R\|$ тождеств, а (14) —

							(17) $x1 = x$;	$\|R\|$ тождеств. То же относится к приводимому ниже тождеству (18)
15.	Линейная алгебра над коммутативным ассоциативным кольцом R с единицей (не обязательно ассоциативная)	$4+\|R\|$	0	—, λ, где $\lambda \in R$	$+$, $\cdot$		(1′)—(4′), (5), (6), (14)—(17), (18) $\lambda(xy) = (\lambda x)\, y = x\,(\lambda y)$	
16.	Ассоциативная линейная алгебра над коммутативным ассоциативным кольцом Φ с единицей	$4+\|\Phi\|$	0	—, λ, где $\lambda \in \Phi$	$+$, $\cdot$		(1′)—(4′), (5), (6), (1), (14)—(18);	
17.	Унар	1		f				
18.	Груда	1				$(\ ,\ ,\ )$	(19) $((x, y, z), u, v) = (x, y, (z, u, v))$; (20) $(x, x, y) = y$; (21) $(x, y, y) = x$;	
19.	Полугруда	1				$(\ ,\ ,\ )$	(19) и (22) $((x, y, z), u, v) = (x, (u, z, y), v)$	

Поэтому элементами свободного группоида со свободной порождающей системой X служат строки вида

$$w = x_1 \dots x_m,$$

где $x_i \in X$ и имеется в виду некоторое распределение скобок, описывающее порядок, в котором следует осуществлять умножение. Такие строки будем называть *неассоциативными словами* в алфавите X. Число m называется *длиной* слова w и обозначается через $l(w)$. Убрав в неассоциативном слове скобки, получаем последовательность $x_1 \dots x_n$, которая называется *ассоциативным словом* в алфавите X. Определив произведение ассоциативных слов $x_1 \dots x_m$ и $y_1 \dots y_n$ как $x_1 \dots x_m y_1 \dots y_n$, нетрудно убедиться, что возникает полугруппа.

Более того, положив $\varkappa(x) = x$ для всех $x \in X$, легко видеть, что F оказывается свободной полугруппой со свободной порождающей системой X. При рассмотрении свободного моноида возникают ассоциативные слова, где некоторые из x равны 1. Однако свойство единицы позволяет эти элементы выбросить. Таким образом, элементами свободного моноида со свободной порождающей системой X служат ассоциативные слова в алфавите X и символ 1. Последний часто отождествляется с пустым словом. Условимся считать, что длина пустого слова равна нулю.

Пусть снова X — непустое множество. Рассмотрим множество

$$X^{\pm 1} = \{x^\varepsilon \mid x \in X,\ \varepsilon = \pm 1\}$$

и свободный моноид M со свободной порождающей системой $X^{\pm 1}$. Слово $x^\varepsilon x^{-\varepsilon}$, где $x \in X$ и $\varepsilon = \pm 1$, назовем для краткости *плохим*. Переход от слова $u \in M$ к новому слову из M путем выбрасывания некоторого плохого подслова назовем *редукцией*. Поскольку каждая редукция уменьшает длину слова, то после некоторого конечного числа редукций возникнет *групповое слово*, т. е. слово, не содержащее плохих подслов.

Лемма. *Групповое слово, возникающее из слова $w \in M$ с помощью цепочки редукций, определяется однозначно.*

В самом деле, утверждение леммы тривиально, если $l(w) \leqslant 2$. Пусть $l(w) \geqslant 3$ и найдутся две цепочки редукций, приводящие к групповым словам u и v соответственно. Равенство $u = v$ вытекает из индуктивного предположения, если в обеих цепочках первая редукция применена

к одному и тому же плохому подслову. Если это не так, то для некоторых x, $y \in X$ и ε, $\delta = \pm 1$ имеем или

$$w = w' x^{\varepsilon} x^{-\varepsilon} x^{\varepsilon} w''$$

и первая редукция первой цепочки уничтожает $x^{\varepsilon}x^{-\varepsilon}$, а первая редукция второй — $x^{-\varepsilon}x^{\varepsilon}$, или же

$$w = w' x^{\varepsilon} x^{-\varepsilon} w_0 y^{\delta} y^{-\delta} w''$$

и первая редукция первой цепочки уничтожает $x^{\varepsilon}x^{-\varepsilon}$, а первая редукция второй — $y^{\delta}y^{-\delta}$. В первом случае первые редукции обеих цепочек приводят w к одному и тому же слову $w'x^{\varepsilon}w''$, что позволяет применить индуктивное предположение. Во втором случае после первых редукций возникают слова

$$u' = w' w_0 y^{\delta} y^{-\delta} w''$$

и

$$v' = w' x^{\varepsilon} x^{-\varepsilon} w_0 w''.$$

Если в первом из них применить редукцию к подслову $y^{\delta}y^{-\delta}$, а во втором — к подслову $x^{\varepsilon}x^{-\varepsilon}$, то возникает одно и то же слово $s = w'w_0w''$, приводящееся, в силу индуктивного предположения, к однозначно определенному групповому слову s_0. Таким образом, слово u' цепочками редукций приводится к групповым словам u и s_0. В силу индуктивного предположения, $u = s_0$. Аналогичное рассуждение, примененное к слову v', дает $v = s_0$. Таким образом, $u = v$, что и требовалось.

Ввиду леммы, каждому слову $u \in M$ отвечает единственное групповое слово $\mathrm{gr}(u)$. Положим

$$\theta = \{(u, v) \mid u, v \in M, \ \mathrm{gr}(u) = \mathrm{gr}(v)\}.$$

Нетрудно проверить, что θ — эквивалентность. Допустим, что (u', v'), $(u'', v'') \in \theta$. Легко выводимые из леммы равенства

$$\mathrm{gr}(u'u'') = \mathrm{gr}(\mathrm{gr}(u')\,\mathrm{gr}(u''))$$

и

$$\mathrm{gr}(v'v'') = \mathrm{gr}(\mathrm{gr}(v')\,\mathrm{gr}(v''))$$

показывают, что $(u'u'', v'v'') \in \theta$. Следовательно, θ — конгруэнция.

Предложение 1. *$F = M/\theta$ — свободная группа со свободной порождающей системой X.*

Доказательство. Поскольку

$$(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1},\ 1) \in \theta,$$

то F оказывается группой. Если положить $\varkappa(x) = \theta(x^1)$ для всех $x \in X$, то $\varkappa$ — отображение множества X в F и $\operatorname{Im}\varkappa$ порождает F как группу. Пусть G — группа, и φ — отображение множества X в G. Продолжим φ до отображения $\varphi^{\pm}$: $X^{\pm} \to G$, полагая $\varphi^{\pm}(x^{\varepsilon}) = \varphi(x)^{\varepsilon}$ для любых $x \in X$ и $\varepsilon = \pm 1$. Поскольку M — свободный моноид, существует гомоморфизм ψ': $M \to G$ такой, что $\psi'(x^{\varepsilon}) = \varphi^{\pm}(x^{\varepsilon})$ для любых $x \in X$ и $\varepsilon = \pm 1$. Равенство

$$\begin{aligned}\psi'(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1}) &= \\ = \psi'(x_1^{\varepsilon_1}) \dots \psi'(x_n^{\varepsilon_n})\, \psi'(x_n^{-\varepsilon_n}) \dots \psi'(x_1^{-\varepsilon_1}) &= \\ = \varphi^{\pm}(x_1^{\varepsilon_1}) \dots \varphi^{\pm}(x_n^{\varepsilon_n})\, \varphi^{\pm}(x_n^{-\varepsilon_n}) \dots \varphi^{\pm}(x_1^{-\varepsilon_1}) &= \\ = \varphi(x_1)^{\varepsilon_1} \dots \varphi(x_n)^{\varepsilon_n}\, \varphi(x_n)^{-\varepsilon_n} \dots \varphi(x_1)^{-\varepsilon_1} = 1 = \psi'(1)\end{aligned}$$

показывают, что $\theta \leqslant \operatorname{Ker}\psi'$. В силу предложения 1.3, $\psi' = \theta\psi$, где θ: $M \to F$ — естественный гомоморфизм, а ψ: $F \to G$. Если $x \in X$, то

$$x\varkappa\psi = x^1\theta\psi = x^1\psi' = x^1\varphi^{\pm} = x\varphi,$$

т. е. F обладает свойством универсальности.

Подмножество $\mathscr{E}$ правого модуля F над ассоциативным кольцом R называется *базой*, если каждый элемент a из F единственным способом представляется в форме $a = \sum_{e \in \mathscr{E}} e\lambda_e$, где $\lambda_e \in R$, причем почти все λ_e равны 0. Нетрудно заметить, что база содержит лишь ненулевые элементы. Отметим также, что правый R-модуль R обладает одноэлементной базой $\{1\}$.

Предложение 2. *Правый R-модуль свободен в многообразии всех правых R-модулей тогда и только тогда, когда он обладает базой. При этом база совпадает со свободной порождающей системой.*

Доказательство. Поскольку всякое отображение базы в какой-либо правый R-модуль однозначно продолжается до гомоморфизма модулей, то легко понять, что наличие базы влечет свободу. Наоборот, если F — свободный модуль со свободной порождающей системой $\mathscr{E}$, то каждый элемент из F представляется в форме $\sum_{e \in \mathscr{E}} e\lambda_e$, поскольку $\mathscr{E}$ порождает F. Для доказательства единствен-

ности этого представления рассмотрим прямое произведение $\prod_{e\in\mathscr{E}} R_e$, где R_e изоморфен правому R-модулю R, и отображение $\varphi\colon \mathscr{E} \to \prod_{e\in\mathscr{E}} R_e$, где для $e\in\mathscr{E}$ и естественных проекций π_f на R_f имеет место

$$\pi_f(e) = \begin{cases} 1, & \text{если } f = e, \\ 0, & \text{если } f \neq e. \end{cases}$$

Если в F справедливо равенство $\sum e\lambda_e = \sum e\mu_e$, где $\lambda_{e_0} \neq \mu_{e_0}$ для некоторого $e_0 \in \mathscr{E}$, то, продолжив φ до гомоморфизма $\bar{\varphi}$, придем к невозможному равенству

$$\lambda_{e_0} = \pi_{e_0}\left(\sum e\lambda_e\right) = \pi_{e_0}\left(\sum e\mu_e\right) = \mu_{e_0}.$$

Другое описание свободного правого R-модуля дает

Предложение 3. *Пусть G — прямое произведение* $\mathfrak{m}$ *экземпляров кольца R, рассматриваемого как правый R-модуль, и F — подмодуль модуля G, состоящий из всех строк, почти все координаты которых равны* 0. *Тогда строки, у которых на одном месте стоит* 1, *а на остальных местах — нули, образуют базу модуля F, и F изоморфен свободному правому R-модулю со свободной порождающей системой мощности* $\mathfrak{m}$.

Доказательство. Первое утверждение почти очевидно, а второе вытекает из предложения 2.

Поскольку каждую абелеву группу можно рассматривать как $\mathbf{Z}$-модуль, предложения 2 и 3 дают описание свободных абелевых групп.

Заметим, что, в отличие от линейных пространств, число элементов базы свободного модуля, вообще говоря, не определяется однозначно. Правда, согласно теореме 2.2, соответствующий пример может быть найден лишь в случае, когда одна из баз (а значит и все базы) конечна. Для получения такого примера рассмотрим кольцо эндоморфизмов R свободной абелевой группы с базой $\{e_1, e_2, \ldots\}$. Как уже отмечалось, правый R-модуль R обладает одноэлементной базой $\{1\}$. С другой стороны, определим f, $g \in R$, положив

$$e_i f = \begin{cases} e_n, & \text{если } i = 2n, \\ 0, & \text{если } i = 2n+1, \end{cases} \quad \text{и} \quad e_i g = \begin{cases} 0, & \text{если } i = 2n, \\ e_n, & \text{если } i = 2n+1. \end{cases}$$

Кроме того, для каждого $\varphi \in R$ определим λ_φ, $\mu_\varphi \in R$ равенствами $e_i\lambda_\varphi = e_{2i}\varphi$ и $e_i\mu_\varphi = e_{2i+1}\varphi$. Тогда

$$e_i(f\lambda_\varphi + g\mu_\varphi) = (e_i f)\lambda_\varphi + (e_i g)\mu_\varphi = \begin{cases} e_n\lambda_\varphi = e_{2n}\varphi = e_i\varphi, & \text{если } i = 2n, \\ e_n\mu_\varphi = e_{2n+1}\varphi = e_i\varphi, & \text{если } i = 2n+1, \end{cases}$$

для всех i, откуда

$$\varphi = f\lambda_\varphi + g\mu_\varphi.$$

Если

$$\varphi = f\lambda' + g\mu' = f\lambda'' + g\mu'',$$

где λ', μ', λ'', $\mu'' \in R$, то положим $\lambda = \lambda' - \lambda''$ и $\mu = \mu'' - \mu'$. Тогда $f\lambda = g\mu$. Отсюда $e_{2n}(f\lambda) = (e_{2n}g)\mu = 0$ и $e_{2n+1}(f\lambda) = 0$, т. е. $f\lambda = 0$. Следовательно, $e_i\lambda = (e_{2i}f)\lambda = 0$ для всех i, т. е. $\lambda = 0$. Аналогично проверяется, что $\mu = 0$. Таким образом, множество $\{f, g\}$ также оказывается базой правого R-модуля R.

Предложение 4. *Всякий ненулевой правый модуль над любым телом K свободен и все его базы равномощны.*

Доказательство. Пусть F — ненулевой правый K-модуль. Подмножество модуля F назовем *линейно независимым*, если всякое его конечное подмножество линейно независимо в обычном смысле (ЭА, с. 155). Поскольку объединение возрастающей системы линейно независимых множеств линейно независимо, то, по лемме Куратовского—Цорна (теорема I.1.2), F содержит максимальное линейно независимое подмножество $\mathscr{E}$. Если $x \in F \setminus \mathscr{E}$, то $\{x\} \cup \mathscr{E}$ — линейно зависимое множество и, следовательно,

$$x\lambda_0 + e_1\lambda_1 + \ldots + e_m\lambda_m = 0,$$

где $\lambda_i \in K$, $e_i \in \mathscr{E}$ и не все λ_i обращаются в нуль. Ясно, что при этом $\lambda_0 \neq 0$. Отсюда

$$x = e_1(-\lambda_1\lambda_0^{-1}) + \ldots + e_m(-\lambda_m\lambda_0^{-1}),$$

т. е. любой элемент из F является линейной комбинацией элементов из $\mathscr{E}$. Единственность такого представления легко выводится из линейной независимости. Таким образом, модуль F обладает базой и, по предложению 2, свободен. В силу теоремы 2.2, второе утверждение является следствием следующей леммы:

Лемма. *Если $\{e_1, \ldots, e_n\}$ — база правого модуля F над телом K, то всякое подмножество из F, содержащее $n+1$ элемент, линейно зависимо.*

Доказательство проведем индукцией по n. Если $n=1$ и $a_1, a_2 \in F$, то $a_i = e_1\lambda_{11}$ и $a_2 = e_1\lambda_{12}$, где $\lambda_{11}, \lambda_{12} \in K$ и, скажем, $\lambda_{11} \neq 0$. Тогда

$$a_1(-\lambda_{11}^{-1}\lambda_{12}) + a_2 1 = e_1(-\lambda_{12} + \lambda_{12}) = 0,$$

что и требовалось. Если $n \geqslant 2$ и $a_1, \ldots, a_{n+1} \in F$, то

$$a_j = e_1\lambda_{1j} + \ldots + e_n\lambda_{nj} \quad (j = 1, 2, \ldots, n+1),$$

где $\lambda_{ij} \in K$. Изменив, если нужно, нумерацию, будем иметь $\lambda = \lambda_{n\,n+1} \neq 0$. Положим

$$b_j = a_j - a_{n+1}\lambda^{-1}\lambda_{nj} \quad (j = 1, 2, \ldots, n).$$

Легко видеть, что $b_1, \ldots, b_n$ принадлежит подмодулю F', порожденному элементами $e_1, \ldots, e_{n-1}$, и что последние образуют базу модуля F'. В силу индуктивного предположения,

$$b_1\mu_1 + \ldots + b_n\mu_n = 0,$$

где $\mu_j \in K$ и хотя бы один из них отличен от нуля. Отсюда

$$a_1\mu_1 + \ldots + a_n\mu_n - a_{n+1}(\lambda^{-1}\lambda_{n1} + \ldots + \lambda^{-1}\lambda_{nn}) = 0,$$

что доказывает линейную зависимость множества $\{a_1, \ldots, a_{n+1}\}$.

Предложение 4 позволяет говорить о *размерности модуля* над телом.

Пусть Φ — ассоциативное коммутативное кольцо с единицей. Многообразие линейных Φ-алгебр называется *мультипликативным*, если оно определяется множеством тождеств вида $u = v$, где u и v — неассоциативные слова. К числу мультипликативных многообразий относятся ассоциативные алгебры (определяются тождеством $(xy)z = x(yz)$, ассоциативные коммутативные алгебры ($(xy)z = x(yz)$ и $xy = yx$), алгебры с единицей ($x1 = x = 1x$). Поскольку всякое кольцо является алгеброй над кольцом целых чисел, то можно говорить и о мультипликативных многообразиях колец.

Предложение 5. *Пусть Φ — ассоциативное коммутативное кольцо с единицей, $\mathfrak{M}$ — многообразие группоидов [с единицей], определяемое множеством Σ тождеств вида*

$$x_1 \ldots x_n = x_{\sigma(1)} \ldots x_{\sigma(n)},$$

где σ — подстановка на множестве $\{1, \ldots, n\}$, а в правой и левой частях подразумевается некоторая расстановка скобок (возможно, различная). *Пусть, далее, F — свободный*

Ф-модуль, базой которого служит свободный группоид M [с единицей] многообразия $\mathfrak{G}$ со свободной порождающей системой X. Умножение, имеющееся в M, по дистрибутивности распространяется на F. Тогда F становится свободной линейной Ф-алгеброй мультипликативного многообразия $\mathfrak{M}$ линейных Ф-алгебр [с единицей], определяемого множеством тождеств Σ, со свободной порождающей системой X.

Доказательство. Непосредственный подсчет показывает, что F — линейная Ф-алгебра, принадлежащая многообразию $\mathfrak{M}$. Очевидно, что она обладает свойствами 1) и 2) из определения свободной универсальной алгебры. Пусть, далее, A — произвольная алгебра из многообразия $\mathfrak{M}$, $A^\times$ — ее мультипликативный группоид [с единицей] и $\varphi\colon X \to A$ — отображение. Поскольку M — свободный группоид [с единицей] многообразия $\mathfrak{G}$, то φ продолжается до гомоморфизма $\varphi'\colon M \to A^\times$ группоидов [с единицей]. Положив

$$\psi\left(\sum_{u\in M}\lambda_u u\right) = \sum_{u\in M}\lambda_u \varphi'(u),$$

нетрудно проверить, что $\psi\colon F \to A$ — гомоморфизм линейных Ф-алгебр [с единицей].

Следствие. *Кольцо многочленов над полем P от множества неизвестных X является свободной ассоциативной коммутативной P-алгеброй с единицей со свободной порождающей системой X.*

Упражнения

1. Любое многообразие абелевых групп определяется тождеством вида $nx=0$, где $n\in\mathbf{N}$.

2. Конечная абелева p-группа изоморфна свободной группе некоторого многообразия абелевых групп тогда и только тогда, когда она изоморфна прямой сумме некоторого множества экземпляров циклической группы порядка p^k для некоторого k.

3. Описать наименьшее многообразие абелевых групп, содержащее: а) циклическую группу порядка m; б) циклические группы порядков m и n; в) группу $\mathbf{Z}$.

4. Доказать, что в классе всех ассоциативных нильпотентных линейных алгебр над полем P не существует свободной алгебры (напомним, что линейная алгебра R называется *нильпотентной*, если существует такое $n\in\mathbf{N}$, что $a_1a_2\ldots a_n=0$ для любых $a_1, \ldots, a_n\in R$).

5. Описать свободную алгебру в классе всех ассоциативных линейных алгебр над полем P, определяемом тождеством $x_1x_2\ldots x_n=0$ для некоторого n.

6. Описать наименьшее многообразие коммутативных ассоциативных колец, содержащее поле вычетов по модулю p.

7. Многообразия групп [ассоциативных колец] образуют полную структуру, антиизоморфную структуре всех нормальных подгрупп [идеалов] свободной группы [свободного ассоциативного кольца] F со счетной свободной порождающей системой, замкнутых относительно всех эндоморфизмов группы [кольца] F.

8. Пусть $\mathfrak{M}$ — многообразие унаров, определяемое тождеством $f(x)=f(y)$. Доказать, что свободный удар этого многообразия с m-элементной свободной порождающей системой содержит $m+1$ элемент. Обобщить этот результат на многообразие, определяемое тождеством $f^n(x)=f^n(y)$ для некоторого n.

9. Описать свободные унары многообразия, определяемого тождеством $x=f^n(x)$ для некоторого n.

10. Любое многообразие унаров определяется либо тождеством $f^k(x)=f^l(x)$ для некоторых k и l, либо тождеством $f^m(x)=f^m(y)$ для некоторого m.

11. Найти наименьшее многообразие унаров, содержащее унар

а) $\{a, b, c\}$, где $f(a)=b$, $f(b)=c$ и $f(c)=a$; б) $\{a, b\}$, где $f(a)=b=f(b)$; в) $\{a_1, a_2, \ldots\}$, где $f(a_i)=a_{i+1}$.

12. Если A — группа и $(x, y, z)=xy^{-1}z$, то $(A, (\ ,\ ,\ ))$ — груда.

13. Пусть A — груда и $a\in A$. Положим $xy=(x, a, y)$ и $x^{-1}=(a, x, a)$. Доказать, что $(A, \{\cdot, {}^{-1}, a\})$ — группа.

14. Пусть A — множество всех подмножеств прямого произведения $U\times V$ двух миожеств. Если φ, ψ, $\chi\in A$, то положим

$$(\varphi, \psi, \chi)=\{(u, v)\mid u\in U,\ v\in V,\ \exists x\in U,\ \exists y\in V\,(((u, y)\in\varphi)\ \&\ ((x, y)\in\psi)\ \&\ ((x, v)\in\chi))\}.$$

Доказать, что $(A, (\ ,\ ,\ ))$ — полугруда.

15. Доказать, что всякая груда является полугрудой.

ЛИТЕРАТУРА

Житомирский Г. И. Основные понятия универсальной алгебры.— Саратов: Изд-во Саратовск. ун-та, 1981.

Кон П. Универсальная алгебра.—М.: Мир, 1968.

Курош А. Г. Лекции по общей алгебре.—М.: Наука, 1973.

Курош А. Г. Общая алгебра (лекции 1969/70 учебного года).—М.: Наука, 1974.

Мальцев А. И. Алгебраические системы.—М.: Наука, 1970.

Grätzer G. Universal algebra.—Berlin; Heidelberg; N. Y.: Springer-Verlag, 1979.

Jonsson B. Topics in universal algebra.—Berlin; Heidelberg; N. Y.: Springer-Verlag, 1972 (Lect. Notes Math., v. 250).

Wille R. Kongruenzklassengeometrien.—Berlin; Heidelberg; N. Y., Springer-Verlag, 1970 (Lect. Notes Math., Bd. 113).

ГЛАВА III

СТРУКТУРЫ (РЕШЕТКИ)

В этой главе сначала отмечается, что на структуры можно смотреть и как на частично упорядоченные множества и как на универсальные алгебры. Далее рассматриваются дедекиндовы (модулярные) и дистрибутивные структуры, а также булевы алгебры. Для дедекиндовых структур доказываются теорема о композиционных рядах и теорема об атомности дедекиндовой структуры, удовлетворяющей условию минимальности. Для дистрибутивных структур описано их представление структурами подмножеств. Наконец, охарактеризована булева алгебра всех подмножеств некоторого множества и установлена связь между булевыми алгебрами и булевыми кольцами. Как следствие получена теорема о строении конечных булевых алгебр.

§ 1. Основные свойства

Частично упорядоченное множество называется *структурой* (или *решеткой*), если каждое его двухэлементное подмножество обладает как точной верхней, так и точной нижней гранью. Разумеется, каждая полная структура является структурой. Структурой оказывается и каждая цепь. В частности, целые числа с обычным порядком образуют структуру, не являющуюся полной структурой. Приводимая ниже теорема 1 показывает, что на структуру можно смотреть как на универсальную алгебру с двумя бинарными операциями. Более того, структуры образуют многообразие в классе таких алгебр.

Теорема 1. *Если L — структура, то, полагая*

$$a+b=\sup\{a, b\}$$

и

$$ab=\inf\{a, b\},$$

получаем две операции на L, причем

(1) $(a+b)+c=a+(b+c)$;	(1′) $(ab)c=a(bc)$;
(2) $a+b=b+a$;	(2′) $ab=ba$;
(3) $a+a=a$;	(3′) $aa=a$;
(4) $(a+b)a=a$;	(4′) $ab+a=a$.

Наоборот, если L — множество с операциями $+$ и $\cdot$, обладающими приведенными выше 8 свойствами, то определение

$$a \leqslant b, \text{ если } a=ab,$$

превращает L в структуру, причем

$$\inf\{a, b\}=ab$$

и

$$\sup\{a, b\}=a+b.$$

Доказательство. Допустим, что L — структура Как было отмечено на с. 8, $a+b$ и ab — однозначно определенные элементы структуры L. Другими словами, $+$ и $\cdot$ действительно являются операциями на множестве L. Справедливость свойств (1) и (1′) вытекает из предложения I.3.3. Свойства (2), (2′), (3) и (3′) очевидны. Для доказательства свойства (4) заметим, что $a \leqslant a+b$ и, следовательно, $a \in \{a, a+b\}^{\nabla}$. Но если $x \in \{a, a+b\}^{\nabla}$, то $x \leqslant a$, т. е. a — наибольший элемент нижнего конуса $\{a, a+b\}^{\nabla}$, и по определению $a=(a+b)a$. Двойственным рассуждением устанавливается свойство (4′).

Допустим теперь, что L — множество с бинарными операциями, подчиненными указанным 8 условиям, и $\leqslant$ определено, как в формулировке. Рефлексивность отношения $\leqslant$ вытекает из равенства $aa=a$. Если $a \leqslant b$ и $b \leqslant c$, то $a=ab$ и $b=bc$. Учитывая ассоциативность умножения, получаем

$$a=ab=a(bc)=(ab)c=ac,$$

т. е. $a \leqslant c$. Таким образом, отношение $\leqslant$ транзитивно. Если $a \leqslant b$ и $b \leqslant a$, то $a=ab$ и $b=ba$, откуда $a=b$, в силу коммутативности умножения. Таким образом, $\leqslant$ — порядок. Из равенств $(ab)a=a(ab)=(aa)b=ab$ и $(ab)b=a(bb)=ab$ вытекает, что $ab \in \{a, b\}^{\nabla}$. Если $x \in \{a, b\}^{\nabla}$, то $x \leqslant a$ и $x \leqslant b$, т. е. $x=xa$ и $x=xb$. Отсюда

$$x(ab)=(xa)b=xb=x,$$

т. е. $x \leqslant ab$. Следовательно, ab — наибольший элемент нижнего конуса $\{a, b\}^\nabla$, т. е. $ab = \inf\{a, b\}$. Далее, используя (2) и (4), получаем $a(a+b) = a$ и

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

откуда $a+b \in \{a, b\}^\triangle$. Если $x \in \{a, b\}^\triangle$, то $ax = a$ и $bx = b$, откуда по (4′), (2) и (2′) приходим к

$$x = x + xa = x + ax = x + a$$

и

$$x = x + xb = x + bx = x + b.$$

Но тогда, учитывая (3), (1), (2), (2′) и (4), имеем

$$(a+b)x = (a+b)(x+x) = (a+b)(x+a+x+b) = \\ = (a+b)(x+(a+b)) = a+b,$$

т. е.

$$a+b \leqslant x.$$

Таким образом, $a+b$ — наименьший элемент верхнего конуса $\{a, b\}^\triangle$, т. е.

$$a+b = \sup\{a, b\}.$$

Замечание. Если в соответствии с теоремой 1 от структуры перейти к множеству с двумя операциями, а от него к структуре в соответствии с той же теоремой 1, то, как нетрудно проверить, возникает исходная структура. То же самое имеет место и при переходе от множества с операциями к структуре, а затем снова к множеству с операциями.

Отметим несколько полезных технических утверждений:

Предложение 1. *Для любых элементов a, b, c и d структуры L справедливо*: (а) *если* $a, b \leqslant c$, *то* $a+b \leqslant c$; (б) *если* $c \leqslant a, b$, *то* $c \leqslant ab$; (в) *если* $a \leqslant b$ *и* $c \leqslant d$, *то* $a+c \leqslant b+d$ *и* $ac \leqslant bd$; (г) $ac+bc \leqslant (a+b)c$.

Доказательство. Свойства (а) и (б) легко вывести из определения операций $+$ и $\cdot$, учитывая, что $a+b$ [ab] — наименьший [наибольший] элемент верхнего [нижнего] конуса $\{a, b\}^\triangle$ [$\{a, b\}^\nabla$]. Для доказательства (в) достаточно заметить, что $a \leqslant b$ и $c \leqslant d$ влечет $a \leqslant b \leqslant b+d$ и $c \leqslant d \leqslant b+d$, т. е. $b+d \in \{a, c\}^\triangle$. Аналогично устанавливается, что $ac \in \{b, d\}^\nabla$. Наконец, используя очевидные неравенства $ac \leqslant c$, $bc \leqslant c$, $ac \leqslant a \leqslant a+b$ и $bc \leqslant b \leqslant a+b$, а также (а) и (б), последовательно по-

лучаем

$$ac+bc\leqslant c,\ ac+bc\leqslant a+b \text{ и } ac+bc\leqslant(a+b)c.$$

Если a и b — элементы структуры L и $a\leqslant b$, то множество

$$[a,\ b]=\{x\mid x\in L,\ a\leqslant x\leqslant b\}$$

называется *интервалом*. Из предложения 1 вытекает, что всякий интервал является подструктурой структуры L.

Гомоморфизм структур, рассматриваемых как универсальные алгебры, является изотонным отображением. Действительно, если φ — гомоморфизм структур и $a\leqslant b$, то, согласно теореме 1, $a=ab$. Отсюда $\varphi(a)=\varphi(a)\varphi(b)$, т. е. $\varphi(a)\leqslant\varphi(b)$. Однако произвольное изотонное отображение одной структуры в другую не обязано быть гомоморфизмом. Например, пусть L — структура подмножеств множества $M=\{1, 2, \ldots, n\}$, где $n\geqslant 3$, L' — структура целых чисел с обычным порядком и $\varphi(A)=$(число точек подмножества A). Изотонность этого отображения очевидна. Однако

$$\varphi(\sup_L(\{1, 2\}, \{3\}))=\varphi(\{1, 2, 3\})=3\neq 2=$$
$$=\sup_{L'}\{2, 1\}=\sup_{L'}\{\varphi(\{1, 2\}),\ \varphi(\{3\})\}.$$

Тем не менее, изоморфизм φ частично упорядоченных множеств L и L' оказывается изоморфизмом универсальных алгебр. Действительно, ясно, что $\varphi(a+b)\in\{\varphi(a), \varphi(b)\}^{\triangle}$. Если, далее, $\varphi(x)\in\{\varphi(a),\ \varphi(b)\}^{\triangle}$, то $x\in\{a, b\}^{\triangle}$. Отсюда $x\geqslant a+b$ и, следовательно, $\varphi(x)\geqslant\varphi(a+b)$. Таким образом, $\varphi(a+b)$ — наименьший элемент верхнего конуса $\{\varphi(a),\ \varphi(b)\}^{\triangle}$, т. е. $\varphi(a+b)=\varphi(a)+\varphi(b)$. Аналогично проверяется, что $\varphi(ab)=\varphi(a)\varphi(b)$.

Упражнения

1. Если a, b, c, d — элементы структуры, то

$$ac+bc+ad+bd\leqslant(a+b)(c+d).$$

2. Доказать равносильность следующих свойств элементов a и b произвольной структуры: (а) $a\leqslant b$; (б) $a\leqslant ab$; (в) $a+b\leqslant b$.

3. Всякий минимальный [максимальный] элемент структуры является наименьшим [наибольшим].

4. Если a, b, c — элементы структуры и $a+b+c=abc$, то $a=b=c$.

5. Во всякой структуре справедливо равенство

$$(ab+ac)(ab+bc)=ab.$$

6. Доказать равносильность следующих свойств структуры L: а) L — цепь; б) все непустые подмножества из L являются подструктурами; в) какова бы ни была структура P, всякое изотонное отображение частично упорядоченного множества L в P является структурным гомоморфизмом; г) $a=bc$ влечет $a=b$ или $a=c$.

§ 2. Дедекиндовы (модулярные) структуры

Структура L называется *дедекиндовой* (или *модулярной*) если для любых $a, b, c \in L$, где $a \leqslant c$, справедлив *модулярный закон*

$$(a+b)c = a+bc.$$

Предложение 1. *Если конгруэнции универсальной алгебры A перестановочны, то структура ее конгруэнций $\Theta(A)$ дедекиндова.*

Доказательство. Ввиду предложений II.2.3 и 1.1(г), достаточно доказать, что в случае перестановочности конгруэнций из $\Theta(A)$ для любых $\theta, \theta', \theta'' \in \Theta(A)$, удовлетворяющих условию $\theta' \subseteq \theta$, имеет место $(\theta' \circ \theta'') \cap \theta \leqslant \theta' \circ (\theta \cap \theta'')$. Но если пара (a, b) из $A \times A$ принадлежит левой части этого неравенства, то $(a, b) \in \theta$ и для некоторого $c \in A$ имеет место $(a, c) \in \theta'$ и $(c, b) \in \theta''$. Поскольку $\theta' \subseteq \theta$, отсюда вытекает, что $(c, a) \in \theta$ и, следовательно, $(c, b) \in \theta$. Таким образом, $(c, b) \in \theta \cap \theta''$, а значит, $(a, b) \in \theta' \circ (\theta \cap \theta'')$.

В силу следствия 2 теоремы II.2.3, конгруэнции групп, колец и модулей перестановочны. Нетрудно проверить, что в этих случаях структуры конгруэнций изоморфны структурам нормальных подгрупп, идеалов и подмодулей соответственно. Таким образом, все результаты о дедекиндовых структурах применимы и для этих важных структур.

Предложение 2. *Следующие свойства структуры L эквивалентны:*

(1) *L дедекиндова;*

(2) *$a(ab+c) = ab+ac$ для любых $a, b, c \in L$;*

(3) *если $a \leqslant b$ и для некоторого $c \in L$ справедливо $a+c = b+c$ и $ac = bc$, то $a = b$.*

Доказательство. Допустим, что справедливо свойство (1). Тогда для любых $a, b, c \in L$ имеем $ab \leqslant a$ и, следовательно,

$$a(ab+c) = (ab+c)a = ab+ac.$$

Если же, кроме того, выполнены условия свойства (3), то

$$b = (b + c)\, b = (a + c)\, b = a + cb = a + ac = a.$$

Таким образом, справедливы импликации (1) $\Rightarrow$ (2) и (1) $\Rightarrow$ (3). Если выполнено (2) и $a \leqslant c$, то имеем

$$(a + b)\, c = (ac + b)\, c = ac + bc = a + bc,$$

т. е. (2) $\Rightarrow$ (1). Допустим, наконец, что справедливо свойство (3). Если a, b, $c \in L$ и $a \leqslant c$, то, используя предложение 1.1, получаем

$$a + b \leqslant (a + b)\, c + b \leqslant a + b$$

и

$$bc \leqslant (a + bc)\, b \leqslant (c + bc)\, b = bc.$$

Отсюда

$$(a + b)\, c + b = a + b = (a + bc) + b$$

и

$$[(a + b)\, c]\, b = bc = (a + bc)\, b.$$

Но, по предложению 1.1(г),

$$(a + b)\, c \geqslant a + bc.$$

Поэтому, применяя (3), получаем

$$(a + b)\, c = a + bc,$$

так что импликация (3) $\Rightarrow$ (1) также справедлива.

Замечание. Свойство (2) предложения 2 показывает, что дедекиндовы структуры образуют многообразие универсальных алгебр сигнатуры $(+, \cdot)$.

Цепь $a_0 \leqslant a_1 \leqslant \ldots \leqslant a_n$, принадлежащая структуре с нулем 0 и единицей 1, называется *композиционным рядом*, если $a_0 = 0$, $a_n = 1$ и все интервалы $[a_{i-1}, a_i]$ простые, т. е. $a_{i-1} \leqslant x \leqslant a_i$ влечет $x = a_{i-1}$ или a_i. Число n называется *длиной композиционного ряда*.

Теорема 1. *Все композиционные ряды дедекиндовой структуры* (если они существуют) *имеют одинаковую длину.*

Теорема 1 является непосредственным следствием следующего утверждения:

Предложение 3. *Если дедекиндова структура L имеет композиционный ряд длины n, то она не содержит цепей, состоящих из $n + 2$ элементов.*

Доказательство. Предварительно установим следующий факт:

Лемма. *Если a и b — элементы дедекиндовой структуры L, то интервалы $[ab, a]$ и $[b, a+b]$ изоморфны. При этом изоморфизм осуществляется отображениями*

$$\varphi(x) = x + b \quad (ab \leqslant x \leqslant a)$$

и

$$\psi(y) = ay \quad (b \leqslant y \leqslant a + b).$$

Для доказательства достаточно заметить, что φ и ψ — изотонные отображения, причем

$$\psi(\varphi(x)) = a(x+b) = x + ab = x$$

и

$$\varphi(\psi(y)) = ay + b = (a+b)\,y = y.$$

Вернемся к доказательству предложения. Если $n = 1$, то L является двухэлементной цепью, и предложение, очевидно, справедливо. Поэтому допустим, что $n > 1$, что $0 = a_0 < a_1 < \ldots < a_n = 1$ — композиционный ряд структуры L и что L содержит цепь

$$b_0 < b_1 < \ldots < b_{n+1},$$

все элементы которой различны. Не ограничивая общности, можно считать, что $b_0 = 0$. Рассмотрим цепь

$$a_1 \leqslant a_1 + b_1 \leqslant \ldots \leqslant a_1 + b_{n+1}.$$

Так как эта цепь принадлежит структуре $[a_1, 1]$, обладающей композиционным рядом

$$a_1 < a_2 < \ldots < a_n = 1,$$

то, в силу индуктивного предположения, для некоторого номера i имеем

$$a_1 + b_{i-1} = a_1 + b_i.$$

Разумеется, можно считать, что i — наименьший из таких номеров. Если $i = 1$, т. е. $a_1 = a_1 + b_1$, то $0 < b_1 \leqslant a_1$, откуда $a_1 = b_1$ в силу простоты интервала $[0, a_1]$. Следовательно, $[a_1, 1]$ содержит цепь $b_1 < \ldots < b_{n+1}$, что противоречит индуктивному предположению. Пусть теперь $i > 1$. Если

$$a_1 b_{i-1} = a_1 b_i,$$

то свойство (3) предложения 1 приводит к неверному равенству $b_i = b_{i-1}$. В противном случае, поскольку

$a_1b_{i-1} \leqslant a_1b_i$, а a_1b_{i-1} и a_1b_i принадлежат простому интервалу $[0, a_1]$, имеем $a_1b_{i-1}=0$ и $a_1b_i=a_1$. Отсюда $a_1 \leqslant b_i$ и, следовательно, $b_i=a_1+b_i=a_1+b_{i-1}$. Согласно лемме, существует изоморфизм φ интервала $[0, b_{i-1}]=[a_1b_{i-1}, b_{i-1}]$ на $[a_1, a_1+b_{i-1}]=[a_1, b_i]$. Но тогда структура $[a_1, 1]$ содержит цепь

$$a_1=\varphi(b_0)<\varphi(b_1)<\ldots<\varphi(b_{i-1})=b_i<b_{i+1}<\ldots<b_{n+1},$$

что противоречит индуктивному предположению.

Структура L с нулем и единицей называется *структурой с дополнениями*, если для каждого $a \in L$ найдется $b \in L$ такой, что $a+b=1$ и $ab=0$. Этот элемент b называется *дополнением* элемента a. Дополнение, вообще говоря, не определяется однозначно. Например, в структуре

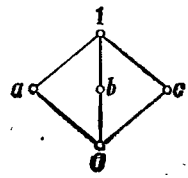


Рис. 2.

{0, 1, a, b, c | a, b и c попарно не сравнимы}

(рис. 2) как b, так и c являются дополнениями элемента a. Если $xy=0$, то вместо $x+y$ часто пишут $x \bigoplus y$, так что y служит дополнением элемента x, если $x \bigoplus y=1$.

Предложение 4. *Если L — дедекиндова структура с дополнениями и $a \leqslant b$, то $a \bigoplus c=b$ для некоторого $c \in L$.*

Доказательство. Если $a \bigoplus x=1$, то, положив $c=xb$ и учитывая модулярный закон, будем иметь

$$b=(a+x)b=a+xb=a+c$$

и

$$ac=axb=0.$$

Элемент p структуры L с нулем 0 называется *атомом*, если $p \neq 0$ и $0 \leqslant x \leqslant p$, где $x \in L$, влечет, что $x=0$ или p. Структура L с нулем 0 называется *атомной*, если для всякого ненулевого $a \in L$ существует атом $p \leqslant a$.

Предложение 5. *Каждый ненулевой элемент полной атомной дедекиндовой структуры L с дополнениями представляется как точная верхняя грань некоторого множества атомов.*

Доказательство. Пусть $0 \neq a \in L$, $A=\{p \mid p$ — атом, $p \leqslant a\}$ и $b=\sup A$. Ясно, что $a \geqslant b$. Если $a \neq b$, то, в силу предложения 4, $a=b \bigoplus c$, где $c \neq 0$. По условию найдется атом q такой, что $q \leqslant c \leqslant a$. Но тогда

$q \in A$, откуда $q \leqslant bc = 0$. Полученное противоречие показывает, что $a = \sup A$.

Предложение 6. *Если дедекиндова структура с дополнениями удовлетворяет условию минимальности, то каждый ее элемент представляется как сумма конечного множества атомов.*

Доказательство. Предварительно установим:

Лемма. *Если дедекиндова структура с дополнениями удовлетворяет условию минимальности, то оно удовлетворяет условию максимальности.*

Для доказательства рассмотрим цепочку

$$0 = a_0 \leqslant a_1 \leqslant a_2 \leqslant \ldots$$

и положим $a'_0 = 1$. Допустим, что построены элементы $a'_1, \ldots, a'_{n-1}$ так, что $a'_1 \geqslant a'_2 \geqslant \ldots \geqslant a'_{n-1}$ и $a_i \oplus a'_i = 1$ для $i = 0, 1, \ldots, n-1$. Ввиду модулярного закона

$$a_n = a_n(a_{n-1} + a'_{n-1}) = a_{n-1} + a_n a'_{n-1}.$$

В силу предложения 4, $a_n a'_{n-1} \oplus a'_n = a'_{n-1}$ для некоторого $a'_n \in L$. Отсюда

$$a_n + a'_n = a_{n-1} + a_n a'_{n-1} + a'_n = a_{n-1} + a'_{n-1} = 1$$

и, поскольку $a'_n \leqslant a'_{n-1}$,

$$a_n a'_n = a_n a'_n a'_{n-1} = (a_n a'_{n-1})\, a'_n = 0.$$

В силу условия минимальности, $a'_m = a'_{m+1}$ для некоторого m. Но тогда, учитывая модулярный закон, получим

$$a_{m+1} = a_{m+1}(a_m + a'_m) = a_m + a_{m+1} a'_m = a_m + a_{m+1} a'_{m+1} = a_m.$$

Возвращаясь к доказательству теоремы, заметим, что из условия минимальности вытекает, что рассматриваемая структура L атомна. Пусть U — множество всех ее атомов и $0 \neq a \in L$. Рассмотрим совокупность S всевозможных конечных сумм атомов, принадлежащих пересечению $U \cap a^{\nabla}$. Ввиду леммы, множество S содержит максимальный элемент, скажем $s = p_1 + \ldots + p_n$, где $p_i \in U \cap a^{\nabla}$. Очевидно, $s \leqslant a$. В силу предложения 4, $a = s \oplus t$ для некоторого t. Если $t = 0$, то все доказано. Если же $t \neq 0$, то $p \leqslant t$ для некоторого $p \in U$. Разумеется, $p \in U \cap a^{\nabla}$. В силу выбора s, $p + s = s$, а значит, $p \leqslant s$ и, следовательно, $p \leqslant st = 0$. Противоречие.

Упражнения

1. Доказать, что дедекиндовость структуры L равносильна каждому из следующих свойств: а) $a+b(a+c)=(a+b)(a+c)$; б) $(a+bc)\times\times(b+c)=a(b+c)+bc$; в) если $a\leqslant c$ и $d\leqslant b$, то $a+b(c+d)=(a+b)c+d$; г) если $a\leqslant c\leqslant a+b$, то $a+bc=c$; д) если $a\leqslant b\leqslant c+d$, $ac=bc$ и $(a+c)d=(b+c)d$, то $a=b$; е) L не содержит подструктур, изображенных на рис. 3.

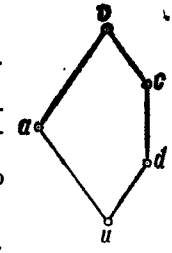


Рис. 3.

2. Если a, b, c—элементы дедекиндовой структуры с нулем и $(a+b)c=0$, то $a(b+c)=ab$.

3. Во всякой дедекиндовой структуре справедливо равенство $(ab+ac)(ab+bc)=ab$, а из соотношения $(a+b)c=bc$ вытекает, что $a(b+c)=ab$.

4. В дедекиндовой структуре с нулем равенство $(a_1+\ldots+a_n)b=0$ влечет $(a_1+b)\ldots(a_n+b)=a_1a_2\ldots a_n+b$.

5. Если $a_1, \ldots, a_n$, $b_1, \ldots, b_n$—элементы дедекиндовой структуры и $a_i\leqslant b_j$ при $i\neq j$, то

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

6. Элементы a и b дедекиндовой структуры с 0 и 1 обладают дополнениями, если дополнения имеют элементы ab и $a+b$.

7. Если C—вполне упорядоченное подмножество дедекиндовой структуры L с дополнениями, то L содержит цепь C^*, двойственную цепи C и состоящую из дополнений к ее элементам.

§ 3. Дистрибутивные структуры

Структура D называется *дистрибутивной*, если $(a+b)c=ac+bc$ для любых $a, b, c\in D$. Примерами дистрибутивных структур служат цепи и любая структура всех подмножеств любого множества (ср. ЭА, с. 142).

Предложение 1. *Следующие свойства структуры D эквивалентны*:

(1) *D дистрибутивна*;

(2) $ab+c=(a+c)(b+c)$ *для любых* $a, b, c\in D$;

(3) $ab+ac+bc=(a+b)(a+c)(b+c)$ *для любых* $a, b, c\in D$;

(4) *если для некоторого* $c\in D$ *справедливо* $a+c=b+c$ *и* $ac=bc$, *то* $a=b$.

Доказательство. (1)$\Rightarrow$(2). Имеем

$$(a+c)(b+c)=(a+c)b+c=ab+bc+c=ab+c.$$

(2)$\Rightarrow$(3). Действительно,

$$ab+ac+bc=ab+(ac+bc)=$$
$$=(a+ac+bc)(b+ac+bc)=(a+bc)(b+ac)=$$
$$=(a+b)(a+c)(b+a)(b+c)=(a+b)(a+c)(b+c).$$

(3) $\Rightarrow$ (1). Если $a \leqslant c$, то $ac = a = a + ab = ab + ac$. Поэтому

$$ac + bc = ab + ac + bc = (a + b)(a + c)(b + c) = \\ = (a + b)c(b + c) = (a + b)c.$$

В силу предложения 2.1, этим доказана дедекиндовость структуры D. Далее, положим

$$u = ab + ac + bc$$

и

$$v = (a + b)(a + c)(b + c).$$

Замечая, что $ac + bc \leqslant c$, и используя модулярный закон, получаем

$$cu = c(ab + (ac + bc)) = abc + ac + bc = ac + bc$$

и

$$cv = c(a + b)(a + c)(b + c) = (a + b)c.$$

Но $u = v$ по условию. Поэтому

$$(a + b)c = cv = cu = ac + bc.$$

(1) $\Rightarrow$ (4). Если $a + c = b + c$ и $ac = bc$, то, применяя (1), получим

$$a = a(a + c) = a(b + c) = ab + ac = ab + bc = \\ = (a + c)b = (b + c)b = b.$$

(4) $\Rightarrow$ (3). Положим $u = ab + ac + bc$, $v = (a + b)(a + c)(b + c)$, $p = ac + b(a + c)$, $q = bc + a(b + c)$ и $r = ab + c(a + b)$. Согласно предложению 2.2, из свойства (4) вытекает справедливость модулярного закона. Поэтому

$$p + r = [ac + b(a + c)] + [ab + c(a + b)] = \\ = b(a + c) + c(a + b) = (a + b)[b(a + c) + c] = \\ = (a + b)(a + c)(b + c) = v,$$

$$q + r = [bc + a(b + c)] + [ab + c(a + b)] = \\ = a(b + c) + c(a + b) = (a + b)[a(b + c) + c] = \\ = (a + b)(b + c)(a + c) = v,$$

$$pr = [ac + b(a + c)][ab + c(a + b)] = \\ = ab + [ac + b(a + c)]c(a + b) = \\ = ab + [ac + b(a + c)c](a + b) = u$$

и

$$qr=[bc+a(b+c)][ab+c(a+b)]=$$
$$=ab+[bc+a(b+c)]c(a+b)=$$
$$=ab+[bc+a(b+c)c](a+b)=u.$$

В силу (4) имеем $p=q$. Но тогда

$$p=p+q=[ac+b(a+c)]+[bc+a(b+c)]=$$
$$=b(a+c)+a(b+c)=(a+c)[b+a(b+c)]=v$$

и

$$p=pq=[ac+b(a+c)][bc+a(b+c)]=$$
$$=bc+[ac+b(a+c)a](b+c)=$$
$$=bc+[ac+b(a+c)a](b+c)=u.$$

Таким образом, имеем $u=p=v$, что и требовалось.

Теорема 1. *Всякая дистрибутивная структура D изоморфна некоторой структуре множеств* (т. е. подструктуре структуры всех подмножеств некоторого множества).

Доказательство. Предварительно установим следующий факт:

Лемма. *Подпрямо неразложимая дистрибутивная структура D содержит не более двух элементов.*

Действительно, допустим, что D содержит различные элементы a, b и c. Эти элементы могут быть выбраны так, что $a\leqslant b\leqslant c$. В самом деле, если $a\not\leqslant b$ и $b\not\leqslant a$, то ab, a и $a+b$ различны и $ab\leqslant a\leqslant a+b$. В противном случае можно считать, что $a<b$. Если $ac\neq a$, то $ac<a<b$. Если $b+c\neq b$, то $a<b<b+c$. Если же $ac=a$ и $b+c=b$, то $a<c<b$. Итак, пусть $a\leqslant b\leqslant c$. Положим $U=b^{\Delta}$ и $V=b^{\nabla}$ и определим отображение φ: $D\to U\times V$, положив $x\varphi=(x+b,\ xb)$ для всякого $x\in D$. Для любых $x,\ y\in D$ имеем

$$(x+y)\varphi=(x+y+b,\ (x+y)b)=(x+b,\ xb)+(y+b,\ yb)=$$
$$=x\varphi+y\varphi$$

и

$$xy\varphi=(xy+b,\ xyb)=(x+b,\ xb)(y+b,\ yb)=x\varphi\cdot y\varphi.$$

Кроме того, если $x\varphi=y\varphi$, то $x+b=y+b$ и $xb=yb$, откуда $x=y$ в силу предложения 1. Таким образом, φ оказывается гомоморфным вложением структуры D в $U\times V$. При этом, если π_U и π_V—естественные проекции $U\times V$

на U и V соответственно, то

$$a\varphi\pi_U = a + b = b = b + b = b\varphi\pi_U$$

и

$$b\varphi\pi_V = bb = b = bc = c\varphi\pi_V.$$

Следовательно, ни $\varphi\pi_U$, ни $\varphi\pi_V$ не являются изоморфизмами. Это означает, что нами построено нетривиальное разложение структуры D в подпрямое произведение. Значит, D не является подпрямо неразложимой.

Возвращаясь к доказательству теоремы, заметим, что в силу леммы и теоремы II.1.1, структура D разлагается в подпрямое произведение двухэлементных цепей D_α. Разумеется, можно считать, что $D \subseteq \prod_{\alpha \in I} D_\alpha$. Обозначим через L структуру всех подмножеств множества I, а через π_α — естественную проекцию $\prod D_\alpha$ на D_α. Для каждого $x \in D$ положим

$$\varphi(x) = \{\alpha \mid \alpha \in I,\ x\pi_\alpha = 1\}.$$

Если $\varphi(x) = \varphi(y)$, то $x = y$, ибо $x\pi_\alpha = 1 = y\pi_\alpha$ для всех $\alpha \in \varphi(x)$ и $x\pi_\alpha = 0 = y\pi_\alpha$ для всех $\alpha \notin \varphi(x)$. Следовательно, φ — вложение. Остается доказать, что $\varphi(x+y) = \varphi(x) \cup \varphi(y)$ и $\varphi(xy) = \varphi(x) \cap \varphi(y)$. Но эти равенства являются следствием импликаций

$$\begin{aligned}\alpha \in \varphi(x) \cup \varphi(y) &\Leftrightarrow ((\alpha \in \varphi(x)) \vee (\alpha \in \varphi(y))) \Leftrightarrow \\ &\Leftrightarrow ((\pi_\alpha(x) = 1) \vee (\pi_\alpha(y) = 1)) \Leftrightarrow \\ &\Leftrightarrow (\pi_\alpha(x) + \pi_\alpha(y) = \pi_\alpha(x+y) = 1) \Leftrightarrow \\ &\Leftrightarrow (\alpha \in \varphi(x+y))\end{aligned}$$

и

$$\begin{aligned}\alpha \in \varphi(x) \cap \varphi(y) &\Leftrightarrow ((\alpha \in \varphi(x)) \,\&\, (\alpha \in \varphi(y))) \Leftrightarrow \\ &\Leftrightarrow ((\pi_\alpha(x) = 1) \,\&\, (\pi_\alpha(y) = 1)) \Leftrightarrow \\ &\Leftrightarrow (\pi_\alpha(x) \cdot \pi_\alpha(y) = \pi_\alpha(xy) = 1) \Leftrightarrow \\ &\Leftrightarrow (a \in \varphi(xy)).\end{aligned}$$

Ясно, что дистрибутивный закон естественным образом распространяется на любые конечные суммы элементов дистрибутивной структуры. Если же эта структура полна, то можно говорить и о дистрибутивности бесконечных сумм. Самым сильным требованием в этом нап-

равлении являются *абсолютная* inf-*дистрибутивность*

$$\inf_{\alpha\in A}\sup_{\beta\in B_\alpha}\{a_{\alpha\beta}\}=\sup_{\varphi\in\Phi}\inf_{\alpha\in A}\{a_{\alpha\varphi(\alpha)}\}.$$

и *абсолютная* sup-*дистрибутивность*

$$\sup_{\alpha\in A}\inf_{\beta\in B_\alpha}\{a_{\alpha\beta}\}=\inf_{\varphi\in\Phi}\sup_{\alpha\in A}\{a_{\alpha\varphi(\alpha)}\},$$

где Φ—множество всех таких отображений φ множества A в объединение $\bigcup\limits_{\alpha\in A}B_\alpha$, что $\varphi(\alpha)\in B_\alpha$ для всех $\alpha\in A$.

Предложение 2. *Множество подмножеств произвольного множества, замкнутое относительно бесконечных объединений и пересечений, образует полную структуру, в которой справедливы как абсолютная* inf-*дистрибутивность, так и абсолютная* sup-*дистрибутивность.*

Доказательство. Если $x\in\bigcap\limits_{\alpha\in A}\bigcup\limits_{\beta\in B_\alpha}X_{\alpha\beta}$, то $x\in\bigcup\limits_{\beta\in B_\alpha}X_{\alpha\beta}$ для каждого α н, следовательно, $x\in X_{\alpha\varphi(\alpha)}$ для некоторого $\varphi(\alpha)\in B_\alpha$. Тогда $x\in\bigcap\limits_{\alpha\in A}X_{\alpha\varphi(\alpha)}\subseteq$ $\subseteq\bigcup\limits_{\varphi\in\Phi}\bigcap\limits_{\alpha\in A}X_{\alpha\varphi(\alpha)}$. Наоборот, если $x\in\bigcup\limits_{\alpha\in\Phi}\bigcap\limits_{\alpha\in A}X_{\alpha\varphi(\alpha)}$, то $x\in\bigcap\limits_{\alpha\in A}X_{\alpha\varphi(\alpha)}$ для некоторого $\varphi\in\Phi$. Таким образом, для каждого $\alpha\in A$ существует такой индекс $\beta\in B_\alpha$, что $x\in X_{\alpha\beta}$ и, следовательно, $x\in\bigcup\limits_{\beta\in B_\alpha}X_{\alpha\beta}$ для всех $\alpha\in A$. Последнее означает, что $x\in\bigcap\limits_{\alpha\in A}\bigcup\limits_{\beta\in B_\alpha}X_{\alpha\beta}$, чем и завершается доказательство абсолютной inf-дистрибутивности. Пусть теперь $x\in\bigcup\limits_{\alpha\in A}\bigcap\limits_{\beta\in B_\alpha}X_{\alpha\beta}$. Тогда для некоторого $\alpha\in A$ и всех $\beta\in B_\alpha$ имеем $x\in X_{\alpha\beta}$. Поэтому $x\in X_{\alpha\varphi(\alpha)}\subseteq\bigcup\limits_{\alpha\in A}X_{\alpha\varphi(\alpha)}$ для всех $\varphi\in\Phi$ и, значит, $x\in\bigcap\limits_{\varphi\in\Phi}\bigcup\limits_{\alpha\in A}X_{\alpha\varphi(\alpha)}$. «Обратный ход» завершает установление абсолютной sup-дистрибутивности.

Упражнения

1. Доказать, что дистрибутивность структуры L равносильна каждому из следующих свойств: а) неравенство $a\leqslant b$ имеет место тогда и только тогда, когда $ac\leqslant bc$ и $a+c\leqslant b+c$ для некоторого $c\in L$; б) $(a+b)(c+ab)=ab+ac+bc$ для любых $a, b, c\in L$; в) $(a+b)c\leqslant$ $\leqslant a+bc$ для любых $a, b, c\in L$.

2. В дистрибутивной структуре соотношения $ab \leqslant x \leqslant a+b$ и $x = ax+bx+ab$ выполняются одновременно.

3. Дистрибутивная структура, обладающая композиционным рядом, конечна.

4. Подструктура дистрибутивной структуры, порожденная конечным множеством, конечна.

5. Непустое подмножество I дистрибутивной структуры D называется *идеалом*, если $a, b \in I$ влечет $a+b \in I$ и $ad \in I$ для любого $d \in D$. Идеал I называется *простым*, если $ab \in I$ влечет $a \in I$ или $b \in I$. Доказать, что нижний конус a^{∇} является простым идеалом тогда и только тогда, когда $a = bc$ влечет $a = b$ или $a = c$.

6. Идеал дистрибутивной структуры D называется *максимальным*, если он является максимальным элементом частично упорядоченного множества идеалов, отличных от D. Доказать, что всякий максимальный идеал дистрибутивной структуры с единицей прост. Убедиться, что конечные подмножества бесконечного множества образуют структуру, не содержащую максимальных идеалов.

§ 4. Булевы алгебры

Дистрибутивная структура B с дополнениями называется *булевой алгеброй*. Из предложения 3.1 вытекает, что каждый элемент $a \in B$ обладает в точности одним дополнением a'. Таким образом, можно считать, что наряду с двумя бинарными операциями в булевой алгебре определена еще одна унарная операция. Булевой алгеброй является структура всех подмножеств фиксированного множества. Примером дистрибутивной структуры, не являющейся булевой алгеброй, служит цепь, содержащая более двух элементов.

Предложение 1. *Во всякой булевой алгебре B для любых $a, b \in B$ справедливы равенства:*

(а) $(a+b)' = a'b'$;
(б) $(ab)' = a'+b'$;
(в) $a'' = a$;
(г) $0' = 1,\ 1' = 0$.

Если же B полна, то для любого подмножества $A \subseteq B$ справедливо:

(д) $a \cdot \sup A = \sup(aA)$;
(е) $a + \inf A = \inf(a+A)$.

Доказательство. Равенство (в) сразу следует из единственности дополнения. Поскольку $0+1=1$ и $0 \cdot 1 = 0$, то по той же причине справедливо (г). Учитывая предложение 3.1, получаем

$$(a+b)+a'b' = (a+b+a')(a+b+b') = 1 \cdot 1 = 1$$

и

$$(a+b)(a'b')=aa'b'+ba'b'=0+0=0.$$

В силу единственности дополнения, отсюда вытекает (а). Учитывая (а) и (в), получаем

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

Далее, если B полна, то, очевидно, $a\cdot\sup A\in(aA)^{\Delta}$. Если же $v\in(aA)^{\Delta}$, то, в силу свойства (2) предложения 3.1,

$$a'+v\geqslant a'+ax=(a'+a)(a'+x)=a'+x\geqslant x$$

для всех $x\in A$. Отсюда $a'+v\geqslant\sup A$ и, следовательно,

$$a\cdot\sup A\leqslant a(a'+v)=av\leqslant v.$$

Таким образом,

$$a\cdot\sup A=\sup(aA),$$

т. е. справедливо (д). Равенство (е) устанавливается двойственными рассуждениями.

Теорема 1. *Следующие свойства полной булевой алгебры B эквивалентны*:

(1) *B изоморфна структуре всех подмножеств некоторого множества M;*

(2) *B абсолютно* sup-*дистрибутивна*;

(3) *B абсолютно* inf-*дистрибутивна*;

(4) *B атомна.*

Доказательство. Справедливость импликаций (1)$\Rightarrow$(2) и (1)$\Rightarrow$(3) вытекает из предложения 3.2.

(3)$\Rightarrow$(4). Обозначим через Φ множество всех отображений алгебры B в двухэлементное множество $\{0, 1\}$. Для любых $b\in B$ и $\varphi\in\Phi$ положим $b=b^0$, $b'=b^1$, $\theta_\varphi=\inf\limits_{b\in B}\{b^{\varphi(b)}\}$ и $\Phi'=\{\varphi\mid\varphi\in\Phi,\ \theta_\varphi\neq 0\}$. Если $0<x\leqslant\theta_\varphi$, то $x\leqslant x^{\varphi(x)}$. Если $\varphi(x)=1$, то $x\leqslant xx'=0$, вопреки условию. Следовательно, $\varphi(x)=0$. Отсюда $x\leqslant\theta_\varphi\leqslant x^0=x$, т. е. $x=\theta_\varphi$. Таким образом, θ_φ—атом для всякого $\varphi\in\Phi'$. Используя (2), получаем

$$1=\inf_{b\in B}(b+b')=\inf_{b\in B}\sup_{i\in\{0,1\}}\{b^i\}=\sup_{\varphi\in\Phi}\inf_{b\in B}\{b^{\varphi(b)}\}=$$
$$=\sup_{\varphi\in\Phi}\theta_\varphi=\sup_{\varphi\in\Phi'}\theta_\varphi.$$

Если, далее, $0\neq b\in B$, то ввиду предложения 1(д) имеем

$$b=b\sup_{\varphi\in\Phi'}\theta_\varphi=\sup_{\varphi\in\Phi'}b\theta_\varphi.$$

Для некоторого $\varphi \in \Phi'$ имеем $0 < b\theta_\varphi \leqslant \theta_\varphi$. Поскольку θ_φ — атом, отсюда вытекает, что $b\theta_\varphi = \theta_\varphi$. Следовательно, $\theta_\varphi \leqslant b$, что и требовалось.

(4) $\Rightarrow$ (1). Пусть M — множество всех атомов алгебры B и P — структура всех подмножеств множества M. Если $b \in B$, то положим

$$\varphi(b) = \begin{cases} \{p \mid p \in M,\ p \leqslant b\}, & \text{если } b \neq 0, \\ \varnothing, & \text{если } b = 0. \end{cases}$$

Тогда φ отображает B в P. Определим отображение ψ: $P \to B$, положив

$$\psi(X) = \begin{cases} \sup X, & \text{если } X \neq \varnothing, \\ 0, & \text{если } X = \varnothing. \end{cases}$$

В силу предложения 2.5, $\psi(\varphi(b)) = b$ для всех $b \in B$, т. е. $\varphi\psi = 1_B$. С другой стороны, если $X \in P$, то $X \subseteq \varphi(\psi(X))$, а если $y \in \varphi(\psi(X))$, то $y \leqslant \sup X$. В силу предложения 1(д), имеем

$$y = y\psi(X) = y \sup X = \sup(yX),$$

откуда

$$0 < xy \leqslant x,\ y$$

для некоторого $x \in X$. Поскольку x и y — атомы, отсюда вытекает, что

$$y = xy = x \in X.$$

Таким образом, $X = \varphi(\psi(X))$, т. е. $\psi\varphi = 1_P$. Ясно, что φ и ψ изотонны.

(2) $\Rightarrow$ (1). Достаточно заметить, что эта импликация двойственна уже доказанной импликации (3) $\Rightarrow$ (1).

Из теоремы 1 непосредственно вытекает

Следствие (теорема Стоуна). *Конечная булева алгебра изоморфна структуре всех подмножеств некоторого конечного множества.*

Существуют и безатомные булевы алгебры. Соответствующий пример можно найти в конце § 8 книги: Скорняков Л. А. Элементы теории структур.—М.: Наука, 1982.

Остановимся на связи булевых алгебр с кольцами.

Кольцо R называется *булевым*, если $a^2 = a$ для всех $a \in R$.

Предложение 2. *Булево кольцо коммутативно, и* $a + a = 0$ (т. е. $a = -a$) *для всех элементов* a.

Доказательство. Во-первых,

$$a+a=(a+a)^2=a^2+a^2+a^2+a^2=a+a+a+a,$$

откуда $a+a=0$. Во-вторых,

$$a+b=(a+b)^2=a^2+ab+ba+b^2=a+b+ab+ba.$$

Отсюда $ab+ba=0$. Учитывая доказанное выше, получаем

$$ab=ab+(ba+ba)=(ab+ba)+ba=ba.$$

Теорема 2. *Пусть B — булева алгебра. Для любых $a, b\in B$ положим*

$$a\# b=ab'+a'b$$

и

$$a\circ b=ab.$$

Тогда B становится булевым кольцом с единицей.

Доказательство. Равенство $a^2=a$, ассоциативность умножения, наличие единицы и коммутативность обеих операций очевидны. Далее, учитывая предложение 1, имеем

$$\begin{aligned}(a\# b)\# c&=(ab'+a'b)\,c'+(ab'+a'b)'\,c=\\&=ab'c'+a'bc'+(a'+b)\,(a+b')\,c=\\&=ab'c'+a'bc'+a'b'c+bac=\\&=a\,(b'c'+bc)+a'\,(bc'+b'c)=\\&=a\,(b'+c)\,(b+c')+a'\,(bc'+b'c)=\\&=a\,(bc'+b'c)'+a'\,(bc'+b'c)=a\# (b\# c),\end{aligned}$$

$$a\# 0=a0'+a'0=a\cdot 1=a$$

и

$$a\# a=aa'+a'a=0,$$

т. е. B оказывается абелевой группой по сложению. Наконец,

$$\begin{aligned}(a\# b)\circ c&=(ab'+a'b)\,c=ab'c+a'bc=\\&=ac\,(b'+c')+(a'+c')\,bc=(ac)\,(bc)'+(ac)'\,(bc)=\\&=a\circ c\# b\circ c.\end{aligned}$$

Теорема 3. *Пусть R — булево кольцо с единицей относительно операций $\#$ и $\circ$. Положим*

$$a+b=a\# b\# a\circ b$$

и

$$ab = a \circ b.$$

Тогда R становится булевой алгеброй B. Кольцо, полученное из алгебры B с помощью теоремы 2, совпадает с R. Применение только что описанной конструкции к кольцу, полученному в теореме 2, приводит к исходной булевой алгебре.

Доказательство. Ассоциативность операций $+$ и $\cdot$, а также равенство $aa = a$ проверяются непосредственным подсчетом. Коммутативность булева кольца, установленная в предложении 2, обеспечивает коммутативность этих операций. Кроме того, $a \# a = 0$ по предложению 2. Поэтому

$$a + a = a \# a \# a \circ a = a,$$

$$(a + b)\, a = (a \# b \# a \circ b) \circ a = a \circ a \# a \circ b \# a \circ b \circ a =$$

$$= a \circ a \# a \circ b \# a \circ b = a$$

и

$$a + ab = a \# a \circ b \# a \circ (a \circ b) = a \# a \circ b \# a \circ b = a.$$

В силу теоремы 1.1, B оказывается структурой. Ясно, что $a1 = a$ и $a0 = 0$ для всех $a \in B$, т. е. структура B обладает нулем и единицей. Из равенств

$$a(1 \# a) = a \circ 1 \# a \circ a = a \# a = 0$$

и

$$a + (1 \# a) = a \# 1 \# a \# a \circ (1 \# a) =$$

$$= a \# 1 \# a \# a \# a = 1$$

вытекает, что B—структура с дополнениями. Ее дистрибутивность проверяется следующим образом:

$$(a + b)\, c = (a \# b \# ab) \circ c = ac \# bc \# ac \circ bc = ac + bc.$$

Заключительные утверждения теоремы вытекают из равенств

$$ab' + a'b =$$

$$= a \circ (1 \# b) \# (1 \# a) \circ b \# a \circ (1 \# b) \circ b \circ (1 \# a) =$$

$$= a \# ab \# b \# ab \# ab \# aba \# abb \# abab = a \# b$$

и

$$a \# b \# a \circ b = (ab' + a'b)(ab)' + (ab' + a'b)' ab =$$
$$= (ab' + a'b)(a' + b') + (a' + b)(a + b') ab =$$
$$= ab' + a'b + ab = ab' + ab + a'b + ab =$$
$$= a(b' + b) + (a' + a) b = a + b.$$

Упражнения

1. Для элементов булевой алгебры a и b равносильны следующие утверждения: а) $a \leqslant b$; б) $ab' = 0$; в) $a' + b = 1$.

2. Все идеалы булевой алгебры B имеют вид a^{∇}, где $a \in B$, тогда и только тогда, когда она конечна.

3. Дистрибутивная структура с 0 и 1 является булевой алгеброй тогда и только тогда, когда каждый ее собственный простой идеал максимален.

4. Идеал I булевой алгебры B максимален тогда и только тогда, когда для любого $a \in B$ идеал I содержит a в том и только в том случае, когда $a' \notin I$.

5. Совокупность элементов дистрибутивной структуры с 0 и 1, обладающих дополнениями, образует подструктуру, являющуюся булевой алгеброй.

6. Дедекиндова структура, в которой каждый элемент обладает в точности одним дополнением, является булевой алгеброй.

7. Каждая дистрибутивная структура является подструктурой некоторой булевой алгебры.

8. Булева алгебра, удовлетворяющая условию минимальности или максимальности, конечна.

9. Всякая конгруэнция булевой алгебры является конгруэнцией соответствующего булева кольца, и наоборот.

10. Булево кольцо является полем тогда и только тогда, когда оно двухэлементно.

11. Идемпотенты любого коммутативного кольца образуют булево кольцо относительно операции

$$e \# f = e + f - 2ef, \quad e \circ f = ef.$$

12. Если a, b, c—элементы булева кольца, причем $a \# b \# c = 0$ и $a \circ b \# a \circ c \# b \circ c = 1$, то в соответствующей булевой алгебре справедливы равенства: $a + b = 1$, $a' + b' = c$ и $ab = 1 \# a \# b$.

ЛИТЕРАТУРА

Биркгоф Г. Теория решеток.—М.: Наука, 1983.
Владимиров Д. А. Булевы алгебры.—М.: Наука, 1969.
Гретцер Г. Общая теория решеток.—М.: Мир, 1982.
Салий В. Н. Лекции по теории решеток.—Саратов: Изд-во Саратовск. ун-та, 1970.
Салий В. Н. Решетки с единственными дополнениями.—М.: Наука, 1983.
Сикорский Р. Булевы алгебры.—М.: Мир, 1969.
Скорняков Л. А. Дедекиндовы структуры с дополнениями и регулярные кольца.—М.: Физматгиз, 1961.

Скорияков Л. А. Элементы теории структур.—М.: Наука, 1982.
Blyth T., Janowitz M. F. Residuation theory.—Oxford: Pergamon Press, 1972.
Gierz G., Hofmann K. H., Keimel K., Lawson J. D., Mislove M., Scott D. S. A compendium of continuous lattices.—Berlin; Heidelberg; N. Y.: Springer-Verlag, 1980.
Kalmbach G. Orthomodular lattices.—London: Academic Press, 1983.
Maeda F. Kontinuerliche Geometrien.—Berlin; Göttingen; Heidelberg: Springer-Verlag, 1958.
Maeda F., Maeda S. Theory of symmetric lattices.—Berlin; N. Y.: Springer-Verlag, 1970.
von Neumann J. Continuos geometry.—New Jersey: Princenton, 1960.

ГЛАВА IV

АССОЦИАТИВНЫЕ КОЛЬЦА И МОДУЛИ НАД НИМИ

В этой главе под словом «кольцо» всегда понимается ассоциативное кольцо. При рассмотрении модулей всегда предполагается, что кольцо обладает единицей, а все модули унитарны. Изложение начинается с примера кольца без делителей нуля, не вложимого в тело. Построение этого примера дает повод познакомиться с техникой работы со свободными ассоциативными кольцами. В дальнейшем содержании можно выделить две линии: строение колец и основы гомологической алгебры. В рамках первой из них рассматриваются регулярные кольца, обсуждаются условия обрыва цепей односторонних идеалов и вводится квазирегулярный радикал Джекобсона. Из конкретных результатов здесь можно выделить регулярность кольца матриц над регулярным кольцом, теорему Гильберта о базисе, теоремы о строении простых колец с минимальным одиосторонним идеалом и классически полупростых колец, а также теорему о простоте тензорного произведения простых алгебр. Основным результатом, относящимся к гомологической алгебре, является теорема, дающая теоретико-модульную характеризацию классически полупростых колец. Попутно рассмотрены проективные и инъективные модули и, в частности, приведен критерий Бэра инъективности модуля. В заключение доказана теорема о строении конечно порожденных абелевых групп.

§ 1. Вложение в тело

Хорошо известно, что всякое коммутативное кольцо без делителей нуля вкладывается в поле — его поле частных. В некоммутативном случае достаточным условием для вложимости кольца R без делителей нуля в тело (даже в тело частных!) является условие Оре: для любых $a, b \in R$, где $b \neq 0$, существуют $u, v \in R$ такие, что $v \neq 0$ и $av = bu$ (см. упр. 3). Впрочем, для вложения кольца в тело оно не необходимо (см. упр. 4). Более того, на первый взгляд

можно ожидать, что произвольное кольцо без делителей нуля вкладывается в тело (интересно заметить, что без предположения ассоциативности умножения это действительно так). Однако на самом деле имеет место:

Теорема 1 (Мальцев). *Существует кольцо без делителей нуля, не вложимое в тело.*

Доказательство. Пусть F — свободное кольцо со свободной порождающей системой $\{a, b, c, d, x, y, u, v\}$. Его элементами служат линейные комбинации ассоциативных слов в этом алфавите с целыми коэффициентами (см. с. 63). Рассмотрим идеал I кольца F, порожденный элементами $ax-by$, $cx-dy$ и $au-bv$. Слова by, dy, bv назовем для краткости *плохими*, а слова, не содержащие плохих подслов, *хорошими*. Элемент из F, являющийся линейной комбинацией хороших слов, назовем *каноническим*.

Лемма 1. *Пусть p и q — различные плохие слова и*

$$p' = \begin{cases} ax, & \text{если } p = by, \\ cx, & \text{если } p = dy, \\ au, & \text{если } p = bv. \end{cases}$$

Для каждого $f \in F$ существует элемент $g \in F$, выражающийся через слова, имеющие ту же длину, что и слова, входящие в запись элемента f, но не содержащие подслова p, и такой, что $f - g \in F(p' - p)F$. Если слова, входящие в запись элемента f, не содержали подслова q, то g можно выбрать обладающим тем же свойством.

Доказательство достаточно провести в предположении, что f — слово. Допустим, для определенности, что $p = by$. Тогда $q = dy$ или bv. Обозначим через m число подслов by, входящих в f. Если $m = 0$, то можно положить $g = f$. Если $m \geqslant 1$, то можно записать $f = f'(by)f''$, где f' и f'' — некоторые слова, возможно, пустые. Тогда слово $f'(ax)f''$ имеет ту же длину, что и f, но содержит лишь $m-1$ подслов by, а если f не содержало подслов dy или bv, то таких подслов нет и в $f'axf''$. В силу индуктивного предположения, $f'axf'' - g \in F(p' - p)F$ для некоторого g, обладающего нужными свойствами. Отсюда

$$f - g = (f'axf'' - g) - (f''axf'' - f) =$$
$$= (f'axf'' - g) - f'(ax - by)f'' \in F(p' - p)F.$$

Трехкратным применением леммы 1 устанавливается

Лемма 2. *Для каждого* $f \in F$ *существует такой канонический элемент* g, *что* $f - g \in I$.

Лемма 3. *Если* $s_1, \ldots, s_m$ — *различные канонические слова,* $k_t \in \mathbf{Z}$ *и* $f = \sum k_t s_t \in I$, *то* $f = 0$.

Действительно, если $f \in I$, то

$$f = \sum_h w'_h (ax - by) f'_h + \sum_i w''_i (cx - dy) f''_i + \sum_j w'''_j (au - bv) f'''_j, \qquad (*)$$

где w'_h, w''_i, w'''_j — слова, а f'_h, f''_i, $f'''_j \in F$. Воспользовавшись леммой 1, можно записать

$$w'''_j - \bar{w}'''_j = \sum_p w'_{jp} (ax - by) f'_{jp} + \sum_q w''_{jq} (cx - dy) f''_{jq},$$

где $\bar{w}'''_j$ является линейной комбинацией слов, не содержащих подслов by и dy. Отсюда

$$f = \sum_h w'_h (ax - by) f'_h + \sum_{j,\,p} w'_{jp} (ax - by) [f'_{jp} (au - bv) f'''_j] + \sum_i w''_i (cx - dy) f''_i + \sum_{j,\,q} w''_{jq} (cx - dy) [f''_{jq} (au - bv) f'''_j] + \sum_j \bar{w}'''_j (au - bv) f'''_j.$$

Этот результат дает возможность предполагать, что слова w'''_j в равенстве (*) не содержат подслов by и dy. Далее запишем $w'''_j = w_j (bv) \tilde{w}_j$, где слово w_j не содержит подслова bv. Тогда

$$w'''_j (au - bv) f'''_j = w_j au \tilde{w}_j (au - bv) f'''_j - w_j (au - bv) [\tilde{w}_j (au - bv) f'''_j].$$

Применив те же рассуждения к слову $w_j au \tilde{w}_j$, а затем к другим вновь появляющимся словам, можно добиться, что слова w'''_j в равенстве (*) не будут содержать и подслова bv. Аналогичные рассуждения приводят к возможности предполагать, что слова w''_i и слова, входящие в запись элемента f'''_j, не содержат подслов by и dy, а в словах w'_h и словах, входящих в запись элементов f''_i, нет подслова by. Наконец, можно предполагать, что $w'_h \neq w'_k$, если $h \neq k$. Допустим, что $f'_{h_0} \neq 0$ для некоторого h. Если теперь w — слово, входящее в запись элемента f'_{h_0}, то первая сумма правой части равенства (*) содержит

слово $w_{h_0} by w$. Поскольку слова s_t не содержат подслова by, то это слово должно сократиться. Однако оно не может сократиться ни со словами, встречающимися в двух других суммах, ибо они не содержат подслова by, ни со словами из первой суммы, ибо все w_h различны. Таким образом, имеем $f'_h = 0$ для каждого h, т. е. первая сумма исчезает. После этого аналогичные рассуждения, использующие подслово dy, приводят к исчезновению второй суммы. Те же рассуждения со словом bv доказывают исчезновение третьей суммы, т. е. $f = 0$.

Рассмотрим фактор-кольцо $R = F/I$. Смежный класс из R, содержащий $f \in F$, обозначим через $[f]$.

Из леммы 3 вытекает

Лемма 4. *Если f и g — канонические элементы и $[f] = [g]$, то $f = g$.*

Лемма 5. *Если f, g, h — канонические слова и $[f][g] = [h]$, то*

$$(\text{длина } h) = (\text{длина } f) + (\text{длина } g).$$

В самом деле, ввиду леммы 4, это очевидно, если fg — каноническое слово. В противном случае имеем или $f = f'b$ и $g = yg'$, или $f = f'd$ и $g = yg'$, или $f = f'b$ и $g = vg'$, где f' и g' — некоторые слова. Но тогда

$$[f][g] = [f'byg'] = [f' axg'],$$

или

$$[f][g] = [f' dy g'] = [f' cx g'],$$

или

$$[f][g] = [f' bv g'] = [f' au\ g'],$$

причем справа стоят канонические слова, в силу леммы 3 совпадающие с h.

Лемма 6. *R — кольцо без делителей нуля.*

Для доказательства обозначим через h_0 линейную комбинацию самых длинных слов, входящих в запись элемента $h \in F$, и положим $h_1 = h - h_0$. Допустим, что f, $g \in F$ и $[f][g] = [0]$. В силу леммы 2, элементы f и g можно считать каноническими. По той же лемме существуют такие канонические элементы h' и h'', что

$$[h'] = [f_0 g_0]$$

и

$$[h''] = [f_0 g_1 + f_1 g_0 + f_1 g_1].$$

Тогда

$$[h'+h'']=[f_0+f_1][g_0+g_1]=[f][g]=[0].$$

Согласно лемме 3, $h'+h''=0$. Но ввиду леммы 5, слова, входящие в запись элементов h' и h'', имеют различную длину. Поэтому $h'=0$. С другой стороны, положим

$$f_0=p'a+p''b+p'''c+p^{IV}d+p^{V}$$

и

$$g_0=xq'+yq''+uq'''+vq^{IV}+q^{V},$$

где слова, входящие в p^V не кончаются на a, b, c или d, а слова, входящие в q^V, не начинаются на x, y, u или v. Кроме того, пусть

$$h=\underline{p'\,ax\,q'}+p''\,bx\,q'+\underline{\underline{p'''\,cx\,q'}}+p^{IV}\,dx\,q'+p^{V}\,xq'+$$
$$+p'\,ay\,q''+\underline{p''\,ax\,q''}+p'''\,cy\,q''+\underline{\underline{p^{IV}\,cx\,q''}}+p^{V}\,yq''+$$
$$+\underline{\underline{p'\,au\,q'''}}+p''\,bu\,q'''+p'''\,cu\,q'''+p^{IV}\,du\,q'''+p^{V}\,uq'''+$$
$$+p'\,av\,q^{IV}+\underline{\underline{p''\,au\,q^{IV}}}+p'''\,cv\,q^{IV}+p^{IV}\,dv\,q^{IV}+p^{V}\,vq^{IV}+$$
$$+p'\,aq^{V}+p''bq^{V}+p'''\,cq^{V}+p^{IV}\,dq^{V}+p^{V}q^{V}.$$

Тогда $[h]=[f_0g_0]=[0]$ и, ввиду леммы 3, $h=0$. Поскольку слова p', p'', p''' и p^{IV} имеют одну и ту же длину, а (длина p^V) = (длина p') + 1, то подобные члены могут иметь лишь подчеркнутые слагаемые выписанного представления элемента h. Поэтому $p^V\neq 0$ влечет $q'=\ldots=q^V=0$, т. е. $[g]=[0]$. Если же $p^V=0$, то предположим, что $p'\neq 0$. Из невозможности сокращения получаем, что $q''=q^{IV}=q^V=0$. Но тогда $p''\,ax\,q''=0$, а значит, и $p'\,ax'q'=0$, так как этому члену теперь не с чем сокращаться. Отсюда $q'=0$. Аналогично, из $q^{IV}=0$ вытекает, что $q'''=0$. Таким образом, опять имеем $[g]=[0]$. Далее, имея $p'=p^V=0$, допустим, что $p''\neq 0$, и, рассматривая второй столбец записи элемента h, убедимся, что $[g]=0$. К тому же выводу приводят аналогичные рассуждения, если предположить, что $p'''\neq 0$ или $p^{IV}\neq 0$. Таким образом, если $[g]\neq[0]$, то $p'=\ldots=p^V=0$, т. е. $[f]=[0]$.

Возвращаясь к доказательству теоремы, допустим, что кольцо R вложено в тело K. Ввиду леммы 3, $[a]$, $[b]$, $[x]$, $[cu-dv]\neq 0$. Следовательно, в теле K существуют элементы $[a]^{-1}$, $[x]^{-1}$ и $[b]^{-1}$. Из равенств

$$[a][u]=[b][v],\quad [c][x]=[d][y]$$

и

$$[a][x]=[b][y]$$

вытекает

$$[u]=[a]^{-1}[b][v], \quad [c]=[d][y][x]^{-1}$$

и

$$[y][x]^{-1}[a]^{-1}[b]=[1].$$

Отсюда

$$[c][u]=[d][y][x]^{-1}[a]^{-1}[b][v]=[d][1][v]=[d][v].$$

Таким образом,

$$[0]\neq[cu-dv]=[c][u]-[d][v]=[0].$$

Полученное противоречие показывает, что P не вложимо в тело. Остается заметить, что, согласно лемме 6, в P нет делителей нуля.

Построение изложенного примера (решившего, кстати сказать, известную в свое время проблему ван-дер-Вардена) вызвало многочисленные исследования, связанные с поисками критериев вложимости кольца в тело. Подробное обсуждение этого вопроса можно найти в книгах Кон П. Свободные кольца и их связи.—М.: Мир, 1975, § 7.6, и Бокуть Л. А. Ассоциативные кольца. Т. II.—Новосибирск: Изд-во НГУ, 1981.

Упражнения

1. Пусть F—свободное кольцо со свободной порождающей системой $\{x, y\}$ и I—его идеал, порожденный элементом x^2-y^2. Доказать, что F/I—кольцо без делителей нуля. Найти все делители нуля кольца F/H, где H—идеал, порожденный элементом $x^2-xy-yx+y^2$.

2. Доказать, что всякое кольцо R вкладывается в такое кольцо Q, что каждый элемент из R является левым делителем нуля, всякий идемпотент кольца Q принадлежит R и, кроме того, xR, $Rx\neq 0$ для всякого ненулевого $x\in Q$. Указание. Превратить R во вполне упорядоченное миожество и применить трансфиинитиую индукцию.

3. Доказать, что условие Оре (см. с. 87) достаточно для вложения кольца R без делителей нуля в тело. Указание. На множестве Q пар (a, b), где $a, b\in R$ и $b\neq 0$, ввести операции $(a, b)+(c, d)=(av+cu, bv)$, где $bv=du$ и $v\neq 0$, и $(a, b)(c, d)=(au, dv)$, где $bu=cv$ и $v\neq 0$, а также отношение θ, где $((a, b), (c, d))\in\theta$, если найдутся $u, v\in R$ такие, что $v\neq 0$, $au=cv$ и $bu=dv$. Доказать, что θ—эквивалентность, что на фактор-миожестве Q/θ, исходя из операций $+$ и $\cdot$, естественным образом определяются сложение и умножение и что Q/θ с этими операциями оказывается искомым телом.

4. Пусть P—поле, G—линейно упорядочениая группа (см. гл. VII) и R—множество всех формальных сумм вида $\sum\lambda_g g$, где $\lambda_g\in P$,

$g \in G$ и множество $\{g \mid \lambda_g \neq 0\}$ вполне упорядочено. Доказать, что при естественном определении операций R становится телом. Указание Заметить, что $(1+w)^{-1} = 1 - w + w^2 - w^3 + \ldots$ для любого $w \in R$.

5. Доказать, что свободная ассоциативная алгебра с единицей над полем, обладающая двухэлементной свободной порождающей системой $\{x, y\}$, не удовлетворяет условию Оре, но вложимо в тело. Указание. Использовать упр. 4 и упр. 2 из § 1 гл. VII, взяв в качестве G свободную группу с двухэлементной свободной порождающей системой.

§ 2. Регулярные кольца

Кольцо R с единицей называется *регулярным*, если уравнение $axa = a$ разрешимо в R для всякого $a \in R$. Примерами регулярных колец могут служить тела и прямые произведения тел, а также булевы кольца (см. § 4 гл. III). Регулярными оказываются кольца матриц над телом (см. следствие теоремы 2), кольца эндоморфизмов линейных пространств над телом или полем без предположения конечности размерности (см. упр. 3) и кольца функций (см. упр. 2). Регулярные кольца тесно связаны с дедекиндовыми структурами с дополнениями (см. Скорняков Л. А. Дедекиндовы структуры с дополнениями и регулярные кольца.— М.: Физматгиз, 1961).

Теорема 1. *Следующие свойства кольца R с единицей эквивалентны*:

(1) *R регулярно*;

(2) *каждый главный правый идеал кольца R порождается идемпотентом*;

(2′) *каждый главный левый идеал кольца R порождается идемпотентом*;

(3) *главные правые идеалы кольца R образуют подструктуру структуры всех его правых идеалов, обладающую дополнениями*;

(3′) *главные левые идеалы кольца R образуют подструктуру структуры всех его левых идеалов, обладающую дополнениями*;

(4) *каждый конечно порожденный правый идеал кольца R выделяется прямым слагаемым*;

(4′) *каждый конечно порожденный левый идеал кольца R выделяется прямым слагаемым*;

(5) *каждый конечно порожденный правый идеал кольца R порождается идемпотентом*;

(5′) *каждый конечно порожденный левый идеал кольца R порождается идемпотентом.*

Доказательство. (1)$\Rightarrow$(2). Если $a, x \in R$ и $axa=a$, то, положив $e=ax$, получим

$$e^2 = ax\,ax = ax = e$$

и

$$a = axa = ea$$

Следовательно,

$$eR \subseteq aR \subseteq eR,$$

т. е. $aR=eR$.

(2)$\Rightarrow$(1). Если $a \in R$ и $aR=eR$, где $e^2=e \in R$, то $e=ax$ и $a=ey$ для некоторых $x, y \in R$. Отсюда $ea=e^2y=a$ и, следовательно, $a=ea=axa$.

Импликации (1)$\Rightarrow$(2′) и (2′)$\Rightarrow$(1) доказываются аналогично.

(1)$\Rightarrow$(3). Пусть $e^2=e \in R$ и $f^2=f \in R$. В силу доказанного выше, можно считать, что кольцо R обладает свойствами (2) и (2′). Поэтому найдутся $g^2=g \in R$ и $h^2=h \in R$ такие, что

$$(f-ef)\,R = gR \qquad (*)$$

и

$$R(f-ef) = Rh. \qquad (**)$$

Ввиду свойства (2), свойство (3) является следствием утверждений

(а) $eR+fR=(e+g)\,R$,

(б) $eR \cap fR = (f-fh)\,R$

и

в) $eR \oplus (1-e)\,R = R$,

которые сейчас будут доказаны.

(а) Действительно, $g=(f-ef)\,x$ для некоторого $x \in R$. Отсюда

$$eg = e(f-ef)\,x = 0$$

и, следовательно,

$$e = (e+g)-(e+g)\,g \in (e+g)\,R.$$

Далее, из равенства (*) нетрудно вывести, что $f-ef=g(f-ef)$. Поэтому

$$f=ef+g(f-ef)=ef+g(f-ef)+e(f-ef)=$$
$$=ef+(e+g)(f-ef)\in(e+g)R.$$

Таким образом,

$$eR+fR\subseteq(e+g)R\subseteq eR+fR.$$

(б) В самом деле, из (**) нетрудно получить, что

$$f-ef=(f-ef)h=fh-efh,$$

откуда

$$f-fh=ef-efh\in eR$$

Кроме того,

$$f-fh\in fR.$$

Таким образом,

$$f-fh\in eR\cap fR.$$

С другой стороны, если $x\in eR\cap fR$, то $x=eu=fv$ для некоторых $u, v\in R$, откуда $x=ex=fx$, а значит

$$(f-ef)x=x-x=0.$$

Кроме того, ввиду (**), $h=w(f-ef)$ для некоторого $w\in R$. Поэтому

$$fx=fx-fw(f-ef)x=fx-fhx=(f-fh)x\in(f-fh)R,$$

т. е.

$$eR\cap fR\subseteq(f-fh)R.$$

(в) Достаточно заметить, что $1\in eR+(1-e)R$ и $eR\cap(1-e)R=0$ (ср. ЭА, теорема II.6.2).

(3)$\Rightarrow$(4). Достаточно заметить, что, согласно (3), каждый конечно порожденный правый идеал кольца R оказывается главным.

(4)$\Rightarrow$(5). Хорошо известно, что правый идеал, выделяющийся прямым слагаемым, порождается идемпотентом (ЭА, с. 128, теорема II.6.1).

(5)$\Rightarrow$(2). Тривиально.

Таким образом, установлена эквивалентность свойств (1)—(5). Теперь рассмотрим кольцо R° с той же аддитивной группой, что и R, и с умножением $\circ$, определенным равенством $x\circ y=yx$. Свойства (2′)—(5′) для коль-

ца R означают свойства (2)—(5) для кольца R°, а свойство (1) выполняется для этих колец одновременно. Поэтому уже доказанная эквивалентность свойств (1)—(5) в кольце R° означает эквивалентность свойств (1), (2′)—(5′) в кольце R.

Теорема 2. *Кольцо матриц над регулярным кольцом регулярно.*

Доказательство. Пусть R—регулярное кольцо. Обозначим через R_n кольцо $n\times n$-матриц над R, а через R^n—множество n-мерных строк над R. Напомним, что как R, так и R^n являются правыми R-модулями, причем R^n—свободный модуль. Базу последнего образуют строки

$$e_i=(\underbrace{0,\ \ldots,\ 0}_{i-1},\ 1,\ 0,\ \ldots,\ 0)\qquad (i=1,\ \ldots,\ n)$$

(см. предложение II.3.3). Если M—правый R-модуль, то через $\mathfrak{L}(M)$ обозначим структуру всех его подмодулей.

Лемма 1. *Каждый конечно порожденный подмодуль из $\mathfrak{L}(R^n)$ обладает дополнениями в структуре $\mathfrak{L}(R^n)$.*

Доказательство будем вести индукцией по n. При $n=1$ можно воспользоваться свойством (4) теоремы 1. Пусть теперь $n\geqslant 2$. Запишем

$$M=a_1R+\ldots+a_mR,$$

где

$$a_i=(\alpha_{i1},\ \ldots,\ \alpha_{in})\in R^n.$$

В силу свойств (2) и (3) теоремы 1,

$$\alpha_{11}R+\ldots+\alpha_{m1}R=\varepsilon R,$$

где $\varepsilon^2=\varepsilon\in R$. Отсюда

$$\varepsilon=\alpha_{11}\xi_1+\ldots+\alpha_{m1}\xi_m \qquad (*)$$

для некоторых $\xi_i\in R$ и

$$\varepsilon a_{i1}=\alpha_{i1}$$

для всех i. Положим

$$c=(a_1\xi_1+\ldots+a_m\xi_m)\,\varepsilon,$$
$$b_i=a_i-c\alpha_{i1}\qquad (i=1,\ \ldots,\ m)$$

и

$$M'=b_1R+\ldots+b_mR,$$

Ввиду (*)

$$c=(\varepsilon, \ldots),$$

откуда

$$b_i=(\alpha_{i1}-\varepsilon\alpha_{i1}, \ldots)=(0, \ldots).$$

Следовательно,

$$M'\subseteq F=\{(0, \alpha_2, \ldots, \alpha_n)\mid \alpha_i\in R\}.$$

Модуль F, очевидно, изоморфен R^{n-1}. Поэтому, в силу индуктивного предположения,

$$F=M'\oplus N' \qquad (**)$$

для некоторого подмодуля $N'\subseteq F$. Далее, положим

$$d=(1-\varepsilon, 0, \ldots, 0).$$

Если

$$u=(\nu_1, \ldots, \nu_n)\in R^n,$$

то

$$u-c\nu_1-d\nu_1\in F,$$

откуда, в силу (**)

$$u-c\nu_1-d\nu_1=u'+v',$$

где $u'\in M'$, $v'\in N'$. Для некоторых $\eta_i\in R$ имеем

$$u'=b_1\eta_1+\ldots+b_m\eta_m=$$
$$=a_1\eta_1+\ldots+a_m\eta_m-c(\alpha_{11}\eta_1+\ldots+\alpha_{m1}\eta_m).$$

Следовательно,

$$u=(a_1\eta_1+\ldots+a_m\eta_m)+c(\nu_1-\alpha_{11}\eta_1-\ldots-\alpha_{m1}\eta_m)+$$
$$+d\nu_1+v',$$

т. е.

$$R^n=(M'+cR)+(dR+N').$$

При этом, если $u\in M$, то при подходящих $\zeta_i\in R$ имеем

$$u=a_1\zeta_1+\ldots+a_m\zeta_m=$$
$$=b_1\zeta_1+\ldots+b_m\zeta_m+c(\alpha_{11}\zeta_1+\ldots+\alpha_{m1}\zeta_m),$$

откуда

$$M=M'+cR$$

и, значит,

$$R^n = M + (dR + N').$$

Если

$$v \in M \cap (dR + N'),$$

то

$$v = u' + c\lambda = d\mu + v',$$

где $\lambda, \mu \in R$, $u' \in M'$ и $v' \in N'$. Сравнивая первые координаты, получаем

$$\varepsilon\lambda = 0 + \varepsilon\lambda = (1 - \varepsilon)\mu + 0 = (1 - \varepsilon)\mu.$$

Отсюда

$$(1 - \varepsilon)\mu = \varepsilon\lambda = \varepsilon(1 - \varepsilon)\mu = 0$$

и, следовательно,

$$c\lambda = c\varepsilon\lambda = 0$$

и

$$d\mu = d(1 - \varepsilon)\mu = d0 = 0.$$

Но тогда

$$u' = v' \in M' \cap N' = 0,$$

т. е. $v = 0$. Таким образом,

$$R^n = M \oplus (dR + N'),$$

что и требовалось.

Лемма 2. *Если $M \in \mathfrak{L}(R^n)$, то обозначим через $\Phi(M)$ совокупность всех матриц из R_n, столбцы которых принадлежат M, а если $I \in \mathfrak{L}(R_n)$, где R_n рассматривается как правый R_n-модуль, то через $\Psi(I)$ обозначим подмодуль, состоящий из всех столбцов, принадлежащих матрицам, лежащим в I. Тогда Φ и Ψ — взаимно обратные изоморфизмы структур $\mathfrak{L}(R^n)$ и $\mathfrak{L}(R_n)$, причем правый идеал I конечно порожден тогда и только тогда, когда конечно порожден подмодуль $\Psi(I)$.*

Действительно, стандартный подсчет показывает, что $\Phi(M)$ — правый идеал кольца R_n. Чтобы убедиться, что $\Psi(I)$ — подмодуль в R^n, следует установить, что вместе с каждой матрицей правый идеал I содержит матрицу, первым столбцом которой служит любой наперед заданный из ее столбцов, а остальные столбцы нулевые. Это

также делается с помощью стандартных вычислений. Ясно, что Φ и Ψ—изотонные отображения. Используя определение и приведенные выше соображения, нетрудно усмотреть, что $\Psi(\Phi(M))=M$ для любого $M\in\mathfrak{L}(R^n)$ и $\Phi(\Psi(I))=I$ для любого $I\in\mathfrak{L}(R_n)$, а также сохранение при отображениях Φ и Ψ конечной порожденности.

Если теперь I—главный правый идеал кольца R_n, то, по лемме 2, $\Psi(I)$—конечно порожденный подмодуль в $\mathfrak{L}(R^n)$. Согласно лемме 1, $R^n=\Psi(I)\oplus N$ для некоторого $N\in\mathfrak{L}(R^n)$. Еще раз применив лемму 2, получаем

$$R_n=\Phi(\Psi(I))\oplus\Phi(N)=I\oplus\Phi(N),$$

т. е. для R_n выполнено свойство (4) теоремы 1.

Следствие. *Кольцо матриц над телом регулярно.*

Упражнения

1. Элемент a регулярного кольца обратим тогда и только тогда, когда как $ab=0$, так и $ba=0$ влечет $b=0$.

2. Кольцо всех действительных функций на отрезке [0, 1] регулярно.

3. Кольцо линейных преобразований линейного пространства (не обязательно конечномерного) над полем (и даже над телом) регулярно.

4. Центр регулярного кольца является регулярным кольцом.

5. Все идемпотенты регулярного кольца центральны в том и только в том случае, когда в этом кольце нет ненулевых нильпотентных элементов.

6. Если I—идеал регулярного кольца, то уравнение $axa=a$ разрешимо в I для всякого $a\in I$.

7. Регулярное кольцо является телом тогда и только тогда, когда 0 и 1 являются единственными его идемпотентами.

8. Регулярное кольцо, все идемпотенты которого центральны, вкладывается в прямое произведение тел. Структура идеалов такого кольца дистрибутивна.

9. Если I—идеал (левый, правый или двусторонний) регулярного кольца R и для любых $a,\ b\in R$ справедлива импликация

$$(ab\in I)\Rightarrow((a\in I)\vee(b\in I)),$$

то I—максимальный идеал.

§ 3. Нётеровы кольца

Первые исследования в теории колец были связаны с описанием строения конечномерных алгебр с единицей над полем. Ясно, что, скажем, правые идеалы таких алгебр удовлетворяют как условию максимальности, так и условию минимальности. Как выяснилось в дальнейшем, эти условия достаточны для получения ряда содержательных теорем о строении колец. Итак, правый R-мо-

дуль называется *нётеровым* [*артиновым*], если частично упорядоченное множество всех подмодулей этого модуля удовлетворяет условию максимальности [минимальности]. Кольцо R с единицей называется *нётеровым* [*артиновым*] справа, если оно нётерово [артиново], как правый R-модуль. Наиболее популярный пример нётерова кольца — кольцо целых чисел. Нётеровым являются кольца многочленов над полем и, как уже отмечалось, любые конечномерные алгебры с единицей. Последние оказываются и артиновыми кольцами. Кольцо целых чисел не артиново, ибо содержит бесконечную убывающую цепь идеалов

$$\mathbf{Z} \supsetneq 2\mathbf{Z} \supsetneq 4\mathbf{Z} \supsetneq \ldots \supsetneq 2^n\mathbf{Z} \supsetneq \ldots$$

Как нётеровыми, так и артиновыми является любое конечное кольцо, а также кольцо матриц над телом. Кольцо действительных функций на отрезке $[0, 1]$ не является ни артиновым, ни нётеровым. Для доказательства достаточно рассмотреть идеалы

$$I_n = \left\{ f \mid f(x) = 0, \quad \text{если} \quad 0 \leqslant x \leqslant \frac{1}{n} \right\}$$

и

$$J_n = \left\{ f \mid f(x) = 0, \quad \text{если} \quad \frac{1}{n} \leqslant x \leqslant 1 \right\}$$

для $n = 1, 2, \ldots$.

Предложение 1. *Правый R-модуль A является нётеровым тогда и только тогда, когда все его подмодули конечно порождены.*

Доказательство. Если подмодуль B нётерова модуля A не конечно порожден, то найдется последовательность $b_1, b_2, \ldots$ элементов модуля B такая, что для каждого i элемент b_{i+1} не принадлежит подмодулю B_i, порожденному элементами $b_1, \ldots, b_i$. Но тогда цепь подмодулей $B_1, B_2, \ldots$ окажется строго возрастающей, что противоречит нётеровости модуля A. Наоборот, если все подмодули модуля A конечно порождены, но A содержит возрастающую цепь подмодулей $A_1 \subseteq A_2 \subseteq \ldots$, то объединение $B = \bigcup_{1 \leqslant i \leqslant \infty} A_i$ оказывается подмодулем и, следовательно, порождается некоторым конечным множеством $b_1, \ldots, b_m$. Каждое b_i принадлежит $A_{n(i)}$ для некоторого $n(i)$ и, если $n = \max_{1 \leqslant i \leqslant n} \{n(i)\}$, то $b_i \in A_n$ для всех i. Но

тогда

$$A_n \subseteq A_{n+k} \subseteq B \subseteq A_n.$$

для всех k, т. е. цепь $A_1, A_2, \ldots$ обрывается.

Предложение 2. *Пусть B—подмодуль правого R-модуля A. Тогда модуль A оказывается нётеровым [артиновым] тогда и только тогда, когда нётеровыми [артиновыми] являются модули B и A/B.*

Доказательство. Если A нётеров [артинов], то нётеровость [артиновость] модуля B очевидна, а нётеровость [артиновость] фактор-модуля A/B вытекает из предложений II.1.1, II.1.4. Доказательству обратного утверждения предпошлем следующую лемму:

Лемма. *Если A, B, C—подмодули правого R-модуля M, $A+C=B+C$, $A \cap C = B \cap C$ и $A \subseteq B$, то $A=B$.*

Для доказательства достаточно вспомнить, что, ввиду следствия 2 теоремы II.2.3 и предложения III.2.1, структура подмодулей модуля M дедекиндова, и применить свойство (3) предложения III.2.2.

Допустим теперь, что B и A/B—нётеровы [артиновы] модули, а $C_1 \subseteq C_2 \subseteq \ldots$ $[C_1 \supseteq C_2 \supseteq \ldots]$ — возрастающая [убывающая] цепь подмодулей модуля A. Рассмотрим возрастающие [убывающие] цепи

$$B \cap C_1 \subseteq B \cap C_2 \subseteq \ldots \quad [B \cap C_1 \supseteq B \cap C_2 \supseteq \ldots]$$

и

$$\pi(C_1) \subseteq \pi(C_2) \subseteq \ldots \quad [\pi(C_1) \supseteq \pi(C_2) \supseteq \ldots],$$

где π: $A \to A/B$—естественный гомоморфизм. Тогда найдется такой номер n, что $B \cap C_n = B \cap C_{n+k}$ и $\pi(C_n) = \pi(C_{n+k})$ для любого k. Из второго равенства нетрудно вывести, что $C_n + B = C_{n+k} + B$. Поскольку $C_n \subseteq C_{n+k}$ $[C_n \supseteq C_{n+k}]$, то, в силу леммы, $C_n = C_{n+k}$. Таким образом, произвольная возрастающая [убывающая] цепь подмодулей модуля A обрывается, т. е. A—нётеров [артинов] модуль.

Предложение 3. *Прямая сумма конечного числа нётеровых [артиновых] модулей нётерова [артинова].*

Доказательство. Пусть $A_1, \ldots, A_m$—нётеровы [артиновы] модули, а $A = A_1 \oplus \ldots \oplus A_m$—их прямая сумма. Если $m=1$, то справедливость предложения тривиальна. Если $m \geqslant 2$, то положим $B = A_1 \oplus \ldots \oplus A_{m-1}$. Тогда $A = B \oplus A_m$, и, следовательно, $A/A_m \cong B$ (ЭА, следствие теоремы II.5.16). Учитывая индуктивное предположение,

замечаем, что B и A_m — нётеровы [артиновы] модули, после чего остается лишь сослаться на предложение 2.

Предложение 4. *Конечно порожденные правые модули над нётеровым* [*артиновым*] *справа кольцом* R *нётеровы* [*артиновы*].

Доказательство. В силу определения свободного модуля любой конечно порожденный правый R-модуль A изоморфен фактор-модулю F/K, где F — конечно порожденный свободный правый R-модуль. Из предложений 3 и II.3.3 вытекает, что F — нётеров [артинов] модуль, после чего остается лишь воспользоваться предложением 2.

Пусть R — кольцо с единицей. Формальную бесконечную сумму

$$a_0+a_1x+a_2x^2+\ldots,$$

где $a_i\in R$, а x — некоторый символ, назовем *степенным рядом*. Множество $R[[x]]$ всех степенных рядов превращается в кольцо, если сложение и умножение определить равенствами

$$(a_0+a_1x+a_2x^2+\ldots)+(b_0+b_1x+b_2x^2+\ldots)=$$
$$=(a_0+b_0)+(a_1+b_1)\,x+(a_2+b_2)\,x^2+\ldots$$

и

$$(a_0+a_1x+a_2x^2+\ldots)\,(b_0+b_1x+b_2x^2+\ldots)=$$
$$=(c_0+c_1x+c_2x^2+\ldots),$$

где

$$c_i=a_0b_i+a_1b_{i-1}+a_2b_{i-2}+\ldots+a_{i-1}b_1+a_ib_0.$$

Это кольцо называется *кольцом степенных рядов над* R *от переменного* x. Степенной ряд, у которого почти все коэффициенты равны нулю, называется *многочленом*. Если $f=a_0+a_1x+\ldots$ — многочлен, $a_n\neq 0$ и $a_i=0$ при $i>n$, то число n называется *степенью многочлена* f, а a_n — его *старшим коэффициентом*. Нетрудно проверить, что многочлены образуют подкольцо кольца $R[[x]]$, которое называется *кольцом многочленов над* R *от переменного* x и обозначается через $R[x]$. *Кольцо многочленов над* R *от переменных* $x_1, \ldots, x_n$ определяется по индукции равенством

$$R[x_1, \ldots, x_n]=R[x_1, \ldots, x_{n-1}][x_n].$$

Нетрудно доказать, что для любой перестановки σ множества $\{1, \ldots, n\}$ имеет место изоморфизм

$$R[x_1, \ldots, x_n] \cong R[x_{\sigma(1)}, \ldots, x_{\sigma(n)}].$$

Теорема 1 (теорема Гильберта о базисе). *Кольцо многочленов от n переменных над нётеровым справа кольцом с единицей нётерово.*

Доказательство. Очевидно, достаточно доказать теорему для случая одного переменного, а затем использовать индукцию. Итак, пусть R — нётерово справа кольцо с единицей, $R' = R[x]$ — кольцо многочленов от x над ним и I — правый идеал кольца R'. Обозначим через H дополненное нулем множество старших коэффициентов всех многочленов, входящих в I. Если $\lambda, \mu \in H$, то I содержит многочлены $f = \lambda x^m + \ldots$ и $g = \mu x^n + \ldots$ Пусть, для определенности, $m \geqslant n$. Тогда многочлен $f + gx^{m-n}$ принадлежит идеалу I, а его старший коэффициент равен $\lambda + \mu$, т. е. $\lambda + \mu \in H$. Ясно также, что $\lambda\xi \in H$ для всех $\xi \in R$. Таким образом, H — правый идеал кольца R и, в силу предложения 1, порождается конечным множеством, скажем, $\{\lambda_1, \ldots, \lambda_s\}$. Тогда I содержит многочлеины $f_i = \lambda_i x^{n_i} + \ldots$, $i = 1, \ldots, s$. Пусть $n = \max\{n_1, \ldots, n_m\}$ и $g_i = f_i x^{n-n_i}$. Рассмотрим множество

$$L = \{f \mid f \in I, \quad (\text{степень } f) < n\}$$

и подмодуль M правого R-модуля $R[x]$, порожденный множеством $\{1, x, x^2, \ldots, x^{n-1}\}$. Легко видеть, что L является подмодулем модуля M. В силу предложений 1 и 4, L порождается конечным множеством, скажем $\{q_1, \ldots, q_t\}$. Убедимся, что R'-модуль I порождается множеством

$$\{g_1, \ldots, g_s, q_1, \ldots, q_t\},$$

т. е. что каждый многочлен f из I принадлежит правому идеалу I_0, порожденному этим множеством. Это ясно, если (степень f) $< n$. Допустим, что (степень f) $= m \geqslant n$ и $f = \lambda x^m + \ldots$ Тогда $\lambda \in H$ и, следовательно,

$$\lambda = \lambda_1\xi_1 + \ldots + \lambda_s\xi_s$$

для некоторых $\xi_i \in R$. Положим

$$f' = f - g_1\xi_1 x^{m-n} - \ldots - g_s\xi_s x^{m-n},$$

Поскольку $f' \in I$ и (степень $f') < m$, то $f' \in I_0$ в силу индуктивного предположения. Но тогда

$$f = f' + g_1\xi_1 x^{m-n} + \ldots + g_s\xi_s x^{m-n} \in I_0,$$

ибо $g_i \in I_0$.

Следствие. *Кольцо многочленов от конечного множества переменных над полем, телом или кольцом целых чисел нётерово.*

Упражнения

1. Подмодули A и B модуля C нётеровы [артиновы] тогда и только тогда, когда нётеровы [артиновы] модули $A+B$ и $A \cap B$.

2. Кольцо матриц над нётеровым [артиновым] слева кольцом нётерово [артиново] слева.

3. Нётеров [артинов] модуль разлагается в прямую сумму подмодулей, не разложимых в прямую сумму.

4. Эндоморфизм φ нётерова [артинова] модуля является автоморфизмом тогда и только тогда, когда φ — наложение [вложение].

5. Доказать, что для любой перестановки σ множества $\{1, \ldots, n\}$ справедливы изоморфизмы колец

$$R[[x_1, \ldots, x_n]] \cong R[[x_{\sigma(1)}, \ldots, x_{\sigma(n)}]]$$

и

$$R[x_1, \ldots, x_n] \cong R[x_{\sigma(1)}, \ldots, x_{\sigma(n)}]$$

(по определению, $R[[x_1, \ldots, x_n]] = R[[x_1, \ldots, x_{n-1}]][[x_n]]$).

6. Если R — кольцо, а H — его подмножество, то полагаем

$$\mathrm{Ann}_r H = \{x \mid x \in R,\ Hx = 0\}$$

и

$$\mathrm{Ann}_l H = \{x \mid x \in R,\ xH = 0\}.$$

Доказать, что $\mathrm{Ann}_r L$ — правый, а $\mathrm{Ann}_l H$ — левый идеалы. Установить равенства

$$\mathrm{Ann}_r(\mathrm{Ann}_l(\mathrm{Ann}_r H)) = \mathrm{Ann}_r H$$

и

$$\mathrm{Ann}_l(\mathrm{Ann}_r(\mathrm{Ann}_l H)) = \mathrm{Ann}_l H.$$

Идеалы вида $\mathrm{Ann}_r H$ и $\mathrm{Ann}_l H$ называются *аннуляторными*. Доказать, что кольцо удовлетворяет условию минимальности для левых аннуляторных идеалов тогда и только тогда, когда оно удовлетворяет условию максимальности для правых аннуляторных идеалов.

7. Доказать, что подкольцо кольца, удовлетворяющего условию минимальности [максимальности] для аннуляторных идеалов, само удовлетворяет тому же условию.

8. Пусть R — кольцо матриц вида $\begin{Vmatrix} a & 0 \\ b & m \end{Vmatrix}$, где m — целое, а a и b —

рациональные числа. Доказать, что R йётерово справа, не нётерово слева и не артиново ни справа, ни слева.

Указание. Убедиться, что матрицы, у которых $a=m=0$, образуют двусторонний идеал I, являющийся минимальным правым идеалом, но не конечно порожденным левым идеалом. Затем доказать правую нётеровость фактор-кольца R/I. Для доказательства неартиновости рассмотреть множество матриц, у которых $a=0$.

9. Пусть R — кольцо матриц вида $\begin{Vmatrix} a & 0 \\ b & r \end{Vmatrix}$, где r — рациональное число, а a и b — действительные числа. Доказать, что R нётерово и артиново справа, но ни йётерово, ни артиново слева.

10. Пусть P — поле рациональных функций от t над полем Δ и R — линейное пространство над P с базой $\{1, e\}$. Для любых f, f', g, $g' \in R$ положим

$$(f(t)+g(t)e)(f'(t)+g'(t)e)=f(t)f'(t)+(f(t)g'(t)+g(t)f'(t^2))e.$$

Доказать, что R — кольцо, у которого структура правых идеалов обладает композиционным рядом длины 2, а структура левых идеалов — композиционным рядом длины 3.

11. Пусть P — множество всех рациональных чисел, знаменателями которых служат степени фиксированного простого числа p. Доказать, что кольцо с аддитивной группой $P/\mathbf{Z}$ и нулевым умножением артиново, но не нётерово.

Замечание. Можно доказать, что всякое артиново слева кольцо с единицей йётерово (Джекобсон Н. Теория колец.— М.: ИЛ, 1947, с. 136, теорема 29).

§ 4. Тензорное произведение

Пусть A — правый, а B — левый R-модули. В свободной абелевой группе F со свободной порождающей системой $A\times B$ рассмотрим подгруппу K, порожденную всеми элементами вида

$$(a'+a'',\ b)-(a',\ b)-(a'',\ b),$$
$$(a,\ b'+b'')-(a,\ b')-(a,\ b'')$$

и

$$(a\xi,\ b)-(a,\ \xi b),$$

где $a,\ a',\ a''\in A,\ b,\ b',\ b''\in B$ и $\xi\in R$. Фактор-группа F/K называется *тензорным произведением* R-*модулей* A и B и обозначается через $A\otimes_R B$. Обозначим через τ естественный гомоморфизм F на $A\otimes_R B$ и положим $a\otimes b=\tau(a,\ b)$. Подчеркнем, что каждый элемент из $A\otimes_R B$ представляется как линейная комбинация элементов вида $a\otimes b$ с целыми коэффициентами. Из равенств

$$a\otimes 0+a\otimes 0=a\otimes(0+0)=a\otimes 0$$

вытекает, что $a \otimes 0 = 0$, где 0 в правой части равенства обозначает нуль группы $A \otimes_R B$, при любом $a \in A$. Аналогично устанавливается, что $0 \otimes b = 0$ для любого $b \in B$.

Пример: $\mathbf{Z}/\mathbf{Z}m \otimes_{\mathbf{Z}} \mathbf{Z}/\mathbf{Z}n = 0$, если НОД $(m, n) = 1$.

Действительно, $um + vn = 1$ для некоторых u, $v \in \mathbf{Z}$, откуда

$$[x]_m \otimes [y]_n = [umx + vnx]_m \otimes [y]_n = [vx]_m n \otimes [y]_n = [vx]_m \otimes n[y]_n = [vx]_m \otimes [ny]_n = [vx]_m \otimes [0]_n = 0,$$

где $[z]_k$ — класс вычетов по модулю k, содержащий z.

Пусть A — правый, а B — левый R-модули. Отображение φ множества $A \times B$ в абелеву группу G называется *билинейным*, если для любых a, a' $a'' \in A$, b, b', $b'' \in B$ и $\lambda \in R$ справедливы равенства

$$\varphi(a' + a'', b) = \varphi(a', b) + \varphi(a'', b),$$
$$\varphi(a, b' + b'') = \varphi(a, b') + \varphi(a, b'')$$

и

$$\varphi(a\lambda, b) = \varphi(a, \lambda b).$$

Теорема 1. *Пусть A — правый, а B — левый R-модули. Абелева группа T изоморфна тензорному произведению $A \otimes_R B$ тогда и только тогда, когда существует такое билинейное отображение σ прямого произведения $A \times B$ в T, что $\operatorname{Im}\sigma$ порождает группу T и для любой абелевой группы T' и любого билинейного отображения φ: $A \times B \to T'$ найдется такой гомоморфизм абелевых групп ψ: $T \to T'$, что $\varphi = \sigma\psi$.*

Доказательство. Непосредственно из определения тензорного произведения вытекает, что указанное там отображение τ индуцирует билинейное отображение σ множества $A \times B$ в абелеву группу $A \otimes_R B$. Если, далее, T' — абелева группа и φ: $A \times B \to T'$ — билинейное отображение, то, по определению свободной абелевой группы, φ совпадает с ограничением на $A \times B$ некоторого гомоморфизма абелевых групп $\bar{\varphi}$: $F \to T'$. В силу билинейности отображения φ, $\bar{\varphi}(K) = 0$ и, в силу предложения II.1.3, $\bar{\varphi} = \tau\psi$ для некоторого гомоморфизма ψ: $A \otimes_R B \to T'$. Отсюда $\varphi = \sigma\psi$, что и требовалось. Допустим теперь, что абелева группа T удовлетворяет условиям теоремы. Тогда найдутся гомоморфизмы абелевых групп ψ: $T \to A \otimes_R B$ и ψ': $A \otimes_R B \to T$ такие, что $\tau = \sigma\psi$ и $\sigma =$

$= \tau\psi'$. Отсюда $\tau = \tau\psi'\psi$ и $\sigma = \sigma\psi\psi'$. Поскольку τ — наложение, а $\operatorname{Im}\sigma$ порождает группу T, то, в силу следствия предложения II.1.5, эти равенства влекут $1_{A\otimes_R B} = \psi\psi'$ и $1_T = \psi'\psi$, т. е. ψ оказывается изоморфизмом.

Предложение 1. *Если A — правый R-модуль, то абелевы группы $A\otimes_R R$ и A изоморфны.*

Доказательство. Определим σ: $A\times R \to A$, положив $\sigma(a, \lambda) = a\lambda$ для любых $a \in A$ и $\lambda \in R$. Без труда проверяется, что σ — билинейное наложение $A\times R$ на A. Если, далее, T' — абелева группа и φ: $A\times R \to T'$ — билинейное отображение, то, положив $\psi(a) = \varphi(a, 1)$, нетрудно заметить, что ψ — гомоморфизм группы A в группу T'. При этом

$$(a, \lambda)\sigma\psi = (a\lambda)\psi = \varphi(a\lambda, 1) = \varphi(a, \lambda)$$

для любых $a \in A$ и $\lambda \in R$, т. е. $\varphi = \sigma\psi$. Остается лишь применить теорему 1.

Предложение 2. *Если $A = \dot{\sum\limits_{\iota\in\mathfrak{I}}} A_\iota$ — прямая сумма правых [левых] R-модулей, то для любого левого [правого] R-модуля B имеет место изоморфизм абелевых групп*

$$\Big(\dot{\sum_{\iota\in\mathfrak{I}}} A_\iota\Big)\otimes_R B \cong \dot{\sum_{\iota\in\mathfrak{I}}} (A_\iota\otimes_R B)$$
$$\Big[B\otimes_R\Big(\dot{\sum_{\iota\in\mathfrak{I}}} A_\iota\Big) \cong \dot{\sum_{\iota\in\mathfrak{I}}} (B\otimes_R A_\iota)\Big].$$

Доказательство. Пусть $T = \dot{\sum\limits_{\iota\in\mathfrak{I}}} (A_\iota\otimes_R B)$ и p_ι — естественная проекция модуля A на A_ι. Определим отображение φ: $A\otimes_R B \to T$, положив

$$\varphi(w) = (\ldots, \textstyle\sum p_\iota(a_k)\otimes b_k, \ldots),$$

если $w = \sum\limits_k a_k\otimes b_k \in A\otimes_R B$. Корректность этого определения вытекает из равенств

$$\varphi((a'+a'')\otimes b - a'\otimes b - a''\otimes b) =$$
$$= (\ldots, p_\iota(a'+a'')\otimes b - p_\iota(a')\otimes b - p_\iota(a'')\otimes b, \ldots) = 0,$$
$$\varphi(a\otimes(b'+b'') - a\otimes b' - a\otimes b'') =$$
$$= (\ldots, p_\iota(a)\otimes(b'+b'') - p_\iota(a)\otimes b' - p_\iota(a)\otimes b'', \ldots) = 0$$

и

$$\varphi(a\xi\otimes b - a\otimes\xi b) =$$
$$= (\ldots, p_\iota(a\xi)\otimes b - p_\iota(a)\otimes\xi b, \ldots) = 0,$$

где a, a', $a''\in A$, b, b', $b''\in B$ и $\xi\in R$. Ясно, что φ — гомоморфизм абелевых групп. Допуская некоторую вольность, можно считать, что $A_\iota\subseteq A$ и $A_\iota\otimes_R B\subseteq T$. Тогда каждый элемент из T представляется как сумма элементов вида $a_\iota\otimes b$, где $a_\iota\in A_\iota$ и $b\in B$, и $\varphi(a_\iota\otimes b)=a_\iota\otimes b$. Следовательно, φ оказывается наложением. Если $\varphi(w)=0$, где $w=\sum_k a_k\otimes b_k$, то

$$\sum_k p_\iota(a_k)\otimes b_k=0$$

для всех ι. Допуская, как и выше, некоторую вольность, можем записать

$$a_k=\sum_{\iota\in\mathfrak{I}} p_\iota(a_k).$$

Отсюда

$$w=\sum_k a_k\otimes b_k=\sum_k\Big(\sum_\iota p_\iota(a_k)\Big)\otimes b_k=\sum_\iota\Big(\sum_k p_\iota(a_k)\otimes b_k\Big)=0,$$

т. е. φ оказывается изоморфизмом. Второе утверждение доказывается аналогично.

Из предложений 1, 2 и II.3.3 вытекает

Предложение 3. *Если A — правый, R-модуль, а F — свободный левый R-модуль с базой $\mathfrak{E}$ и $A_e=A$ для всех $e\in\mathfrak{E}$, то отображение*

$$\varphi\colon A\otimes_R F\longrightarrow\dot{\sum_{e\in\mathfrak{E}}} A_e,$$

где

$$\varphi\Big(a\otimes\sum_{e\in\mathfrak{E}}\lambda_e e\Big)=\sum_{e\in\mathfrak{E}} a\lambda_e,$$

является изоморфизмом абелевых групп.

Если R и S — кольца с единицей, то абелева группа A называется *R-S-бимодулем*, если A является левым R-модулем и правым S-модулем, причем

$$(\lambda a)\xi=\lambda(a\xi)$$

для любых $\lambda\in R$, $a\in A$ и $\xi\in S$. Всякий правый [левый] R-модуль является $\mathbf{Z}$-R-бимодулем [R-$\mathbf{Z}$-бимодулем]. Кольцо R оказывается как R-S-, так и S-R-бимодулем для всякого подкольца S кольца R, содержащего единицу кольца R. Всякий правый модуль A над коммутативным

кольцом R можно считать R-R-бимодулем, если положить $\lambda a = a\lambda$ для любых $\lambda \in R$ и $a \in A$ (ср. ЭА, с. 108).

Предложение 4. *Если A — S-R-бимодуль, а B — R-T-бимодуль, то определения*

$$\xi(a \otimes b) = \xi a \otimes b$$

и

$$(a \otimes b)\rho = a \otimes b\rho,$$

где $\xi \in S$, $a \in A$, $b \in B$ и $\rho \in T$, превращает абелеву группу $A \otimes_R B$ в S-T-бимодуль.

Доказательство. Корректность первого из определений вытекает из соотношений

$$\xi[(a' + a'') \otimes b - a' \otimes b - a'' \otimes b] = \xi(a' + a'') \otimes b - \xi a' \otimes b - \xi a'' \otimes b = (\xi a' + \xi a'') \otimes b - \xi a' \otimes b - \xi a'' \otimes b \in K,$$

$$\xi[a \otimes (b' + b'') - a \otimes b' - a \otimes b''] = \xi a \otimes (b' + b'') - \xi a \otimes b' - \xi a \otimes b'' \in K$$

и

$$\xi[a\lambda \otimes b - a \otimes \lambda b] = \xi(a\lambda) \otimes b - \xi a \otimes \lambda b = (\xi a)\lambda \otimes b - \xi a \otimes \lambda b \in K,$$

где a, a', $a'' \in A$, b, b', $b'' \in B$, $\xi \in S$, $\lambda \in R$, а K — подгруппа, рассмотренная при определении тензорного произведения. После этого без труда проверяется, что $A \otimes_R B$ превращается в левый S-модуль. Аналогично устанавливается, что $A \otimes_R B$ — правый T-модуль. Остается заметить, что

$$(\xi(a \otimes b))\rho = \xi a \otimes b\rho = (\xi(a \otimes b))\rho$$

для любых $\xi \in S$, $a \in A$, $b \in B$, $\rho \in T$.

Напомним, что абелева группа D называется *делимой группой без кручения*, если всякое уравнение $nx = a$, где $a \in D$ и $0 \neq n \in \mathbf{Z}$, имеет в D единственное решение.

В главе VII понадобится

Предложение 5. *Если D — делимая абелева группа без кручения, то отображение φ: $D \to D \otimes_{\mathbf{Z}} \mathbf{Q}$, где $\mathbf{Q}$ — поле рациональных чисел и $\varphi(a) = a \otimes 1$ для всех $a \in D$, является изоморфизмом абелевых групп.*

Доказательство. Ясно, что φ — гомоморфизм абелевых групп. Определим отображение $\bar{\psi}$: $D \times \mathbf{Q} \to D$

равенством $n\bar{\psi}\left(a, \frac{m}{n}\right) = ma$. Это возможно, поскольку D — делимая группа без кручения. Импликации

$$\left.\begin{array}{l} \frac{m}{n} = \frac{r}{s} \Rightarrow ms = rn \\ \left((ms)\,\bar{\psi}\left(a, \frac{r}{s}\right) = mra = rn\bar{\psi}\left(a, \frac{m}{n}\right)\right) \end{array}\right\} \Rightarrow$$

$$\Rightarrow \bar{\psi}\left(a, \frac{r}{s}\right) = \bar{\psi}\left(a, \frac{m}{n}\right)$$

обеспечивают корректность этого определения. Билинейность отображения $\bar{\psi}$ вытекает из равенств

$$n\left(\bar{\psi}\left(a', \frac{m}{n}\right) + \bar{\psi}\left(a'', \frac{m}{n}\right)\right) = ma' + ma'' = m(a' + a''),$$

$$nr\left(\bar{\psi}\left(a, \frac{m}{n}\right) + \bar{\psi}\left(a, \frac{r}{s}\right)\right) = msa + nra = (ms + nr)a$$

и

$$n\bar{\psi}\left(ak, \frac{m}{n}\right) = m(ka) = (km)a = n\bar{\psi}\left(a, k\frac{m}{n}\right),$$

где k, m, n, r, $s \in \mathbf{Z}$ и a, a', $a'' \in D$. В силу теоремы 1, существует такой гомоморфизм абелевых групп ψ: $D \otimes_{\mathbf{Z}} \mathbf{Q} \to D$, что $\psi\left(a \otimes \frac{m}{n}\right) = \bar{\psi}\left(a, \frac{m}{n}\right)$ для любых $a \in D$ и $\frac{m}{n} \in \mathbf{Q}$. Следовательно, если $\varphi(a') = \varphi(a'')$, т. е. $a' \otimes 1 = a'' \otimes 1$, то

$$a' = 1a' = \bar{\psi}(a', 1) = \psi(a' \otimes 1) = \psi(a'' \otimes 1) = \bar{\psi}(a'', 1) = 1a'' = a''.$$

Значит, φ — гомоморфное вложение. Наконец, если $a \otimes \frac{m}{n} \in D \otimes_{\mathbf{Z}} \mathbf{Q}$, то $a = nb$ для некоторого $b \in D$. Отсюда

$$\varphi(mb) = bm \otimes 1 = b \otimes n \cdot \frac{m}{n} = bn \otimes \frac{m}{n} = a \otimes \frac{m}{n},$$

т. е. φ — наложение.

Пусть теперь R и S — алгебры над коммутативным кольцом Δ с единицей. В силу предложения 4 и предшествующего ему замечания, тензорное произведение $R \otimes_{\Delta} S$ можно рассматривать как Δ-модуль. Определим на этом модуле умножение, положив

$$(a \otimes b)(c \otimes d) = ac \otimes bd$$

для любых a, $c \in A$ и b, $d \in B$. Чтобы доказать корректность этого определения, заметим, что для любых x, a, a', $a'' \in A$, y, b, b', $b'' \in B$ и $\xi \in \Delta$ справедливы соотношения

$$(x \otimes y)[(a' + a'') \otimes b - a' \otimes b - a'' \otimes b] = \\ = x(a' + a'') \otimes yb - xa' \otimes yb - xa'' \otimes yb = 0,$$

$$(x \otimes y)[a \otimes (b' + b'') - a \otimes b' - a \otimes b''] = \\ = xa \otimes y(b' + b'') - xa \otimes yb' - xa \otimes yb'' = 0$$

и

$$(x \otimes y)[a\xi \otimes b - a \otimes \xi b] = x(a\xi) \otimes yb - xa \otimes y(\xi b) = \\ = (xa)\xi \otimes yb - xa \otimes \xi(yb) = 0$$

и что аналогичный результат верен для умножения на $x \otimes y$ справа. Поэтому, если $a \otimes b = a' \otimes b'$ и $c \otimes d = c' \otimes d'$, то $(a \otimes b)(c \otimes d) = (a' \otimes b')(c \otimes d) = (a' \otimes b') \times (c' \otimes d')$. Проверка свойств, входящих в определение кольца, не составляет труда. Кроме того, если a, $c \in R$, b, $d \in S$ и $\lambda \in \Delta$, то

$$\lambda((a \otimes b)(c \otimes d)) = \lambda(ac) \otimes bd, \\ (\lambda(a \otimes b))(c \otimes d) = (\lambda a) c \otimes bd$$

и

$$(a \otimes b)(\lambda(c \otimes d)) = a(\lambda c) \otimes bd.$$

Таким образом, $R \otimes_\Delta S$ становится Δ-алгеброй, которая называется *тензорным произведением алгебр* R и S.

Предложение 5. *Алгебры* $R \otimes_\Delta S$ *и* $S \otimes_\Delta R$ *изоморфны.*

Доказательство. Достаточно заметить, что равенство $\varphi(a \otimes b) = b \otimes a$, где $a \in R$, $b \in S$, корректно определяет искомый изоморфизм φ.

Упражнения

1. Какова бы ни была абелева группа A, группы $A \otimes_{\mathbf{Z}} (\mathbf{Z}/\mathbf{Z}_n)$ и A/nA изоморфны.

2. Абелевы группы $\mathbf{Z}/\mathbf{Z}m \otimes_{\mathbf{Z}} \mathbf{Z}/\mathbf{Z}n$ и $\mathbf{Z}/\mathbf{Z}d$, где $d = \text{НОД}(m, n)$, изоморфны.

3. Доказать изоморфизм абелевых групп $\mathbf{Z}/6\mathbf{Z} \otimes_{\mathbf{Z}} \mathbf{Z}/6\mathbf{Z}$ и $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$.

4. Пусть A — правый R-модуль, B — R-S-бимодуль и C — правый S-модуль. Доказать, что определение

$$f\lambda(b) = f(\lambda b),$$

где $f \in \mathrm{Hom}_S(B, C)$, $\lambda \in R$ и $b \in B$, превращает $\mathrm{Hom}_S(B, C)$ в правый R-модуль и что отображение

$$\varphi\colon \mathrm{Hom}_R(A, \mathrm{Hom}_S(B, C)) \longrightarrow \mathrm{Hom}_S((A \otimes_R B), C),$$

где $\varphi(f)(a \otimes b) = f(a)(b)$, является изоморфизмом абелевых групп.

5. Если A — правый R-модуль, то A и $A \otimes_R R$ изоморфны как правые R-модули (ср. предложение 1).

6. Пусть $\mathbf{C}$ — поле комплексных чисел, рассматриваемое как алгебра над полем действительных чисел $\mathbf{R}$. Доказать, что $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C}$ и $\mathbf{C} \times \mathbf{C}$ изоморфны как $\mathbf{R}$-алгебры.

7. Если A, B, C — модули [алгебры] над коммутативным кольцом Δ с единицей, то $(A \otimes_\Delta B) \otimes_\Delta C \cong A \otimes_\Delta (B \otimes_\Delta C)$ — изоморфизм Δ-модулей [Δ-алгебр].

8. Если Δ — коммутативное кольцо с единицей, то

$$\Delta[x_1, \ldots, x_m] \otimes_\Delta \Delta[y_1, \ldots, y_n] \text{ и } \Delta[x_1, \ldots, x_m, y_1, \ldots, y_n]$$

изоморфны как Δ-алгебры.

9. Если Δ_n — алгебра $n \times n$-матриц над коммутативным кольцом Δ с единицей, то $\Delta_m \otimes_\Delta \Delta_n$ и Δ_{mn} изоморфны как Δ-алгебры.

10. Если R — алгебра над коммутативным кольцом Δ с единицей, то R_n и $R \otimes_\Delta \Delta_n$ изоморфны как Δ-алгебры.

11. Пусть R-алгебра с единицей над коммутативным кольцом Δ с единицей, A и B — подалгебры алгебры R, причем: а) $1 \in A \cap B$; б) если $a \in A$ и $b \in B$, то $ab = ba$; в) $A \cup B$ порождает R как Δ-алгебру; г) если $\varphi\colon A \longrightarrow S$ и $\psi\colon B \longrightarrow S$ — гомоморфизмы алгебр A и B в некоторую Δ-алгебру S, $\varphi(c) = \psi(c)$ для любого $c \in A \cap B$ и $\varphi(a)\psi(b) = \psi(b)\varphi(a)$ для любых $a \in A$ и $b \in B$, то существует гомоморфизм $\chi\colon R \longrightarrow S$ такой, что $\chi(a) = \varphi(a)$ для всех $a \in A$ и $\chi(b) = \psi(b)$ для всех $b \in B$. Доказать, что R и $A \otimes_\Delta B$ изоморфны как Δ-алгебры.

§ 5. Простые кольца

Напомним, что *простым кольцом* называется кольцо, не являющееся кольцом с нулевым умножением и не содержащее двусторонних идеалов, отличных от $\{0\}$ и всего кольца. Простыми кольцами являются поля, тела и кольца матриц над ними (ЭА, с. 103, теоремы II.4.10). Всякое ненулевое фактор-кольцо простого кольца, очевидно, изоморфно ему. Поэтому переход от простого кольца как к идеалам, так и к фактор-кольцам не приводит к проще устроенным кольцам. Этим объясняется особый интерес к их строению (ср. теорема 2 § 6).

Теорема 1. *Простое кольцо R с единицей, содержащее минимальный правый идеал M, изоморфно кольцу матриц над некоторым телом.*

Доказательство. Предварительно докажем следующие три леммы:

Лемма 1. *Если кольцо эндоморфизмов линейного пространства над телом просто, то пространство конечномерно.*

Для доказательства достаточно заметить, что множество эндоморфизмов, имеющих конечномерный образ, образует двусторонний идеал.

Лемма 2. *Если D — кольцо с единицей e и уравнение $ax=e$ разрешимо в D для каждого ненулевого $a\in D$, то D — тело.*

В самом деле, если $0\neq a\in D$, то, по условию, $ax=e$ и $xy=e$ для некоторых x, $y\in D$. Отсюда

$$xa=xae=xaxy=xey=xy=e.$$

Таким образом, x оказывается двусторонним обратным для a, что и требовалось.

Пусть теперь $0\neq a\in M$. Обозначим через RaR совокупность всевозможных сумм вида $\sum_i x_i a y_i$, где x_i, $y_i\in R$. Легко видеть, что RaR — двусторонний идеал кольца R и $0\neq a\in RaR$. Поскольку R — простое кольцо, то $R=RaR$. Если $M^2=0$, то

$$aR=aRaR=(aR)^2\subseteq M^2=0,$$

что невозможно. Таким образом, M не является правым идеалом с нулевым умножением и, следовательно, $M=eR$, где $e^2=e\in M$ (ЭА, с. 129, теорема II.6.3).

Лемма 3. *$D=eRe$ — тело с единицей e.*

Действительно, если $0\neq ere\in eRe$, то

$$0\neq ereR\subseteq M.$$

Отсюда, поскольку M минимален, вытекает $ereR=M$. Следовательно, $e=eres$ для некоторого $s\in R$. Но тогда

$$e=e^2=eresе=(ere)(ese),$$

и остается лишь использовать лемму 2.

Возвращаясь к доказательству теоремы, замечаем, что $\lambda a\in M$ для любых $\lambda\in D$ и $a\in M$. После этого нетрудно проверить, что M превращается в левое линейное пространство над телом D. Если $a\in M$ и $r\in R$, то положим

$$a\Phi(r)=ar.$$

Поскольку

$$(a'+a'')\Phi(r)=(a'+a'')r=a'r+a''r=a'\Phi(r)+a''\Phi(r)$$

и

$$(\lambda a)\Phi(r)=(\lambda a)r=\lambda(ar)=\lambda(a\Phi(r))$$

для любых $\lambda\in D$ и a', a'', $a\in M$, то Φ отображает R в кольцо эндоморфизмов левого D-пространства M. Из равенства

$$a\Phi(r'r'')=a(r'r'')=(ar')r''=(a\Phi(r'))\Phi(r'')=a(\Phi(r')\Phi(r'')),$$

где $a\in M$, r', $r''\in R$, вытекает, что Φ — кольцевой гомоморфизм. Если $\operatorname{Ker}\Phi=R$, то

$$a=a\cdot 1=a\Phi(1)=0$$

для любого $a\in M$, что невозможно. Ввиду простоты кольца R, получаем, что $\operatorname{Ker}\Phi=0$, т. е. Φ оказывается вложением. Пусть теперь φ — эндоморфизм D-пространства M. Ввиду равенства $R=ReR$, имеем

$$1=\sum_i x_i e y_i$$

для некоторых x_i, $y_i\in R$. Положим

$$r=\sum_i x_i e\varphi(ey_i).$$

Тогда для любого $a\in M$ имеем $a=ea$ и, следовательно, $ax_ie\in D$. Отсюда

$$a\Phi(r)=ar=\sum_i ax_ie\varphi(ey_i)=$$

$$=\varphi\left(\sum_i ax_iey_i\right)=\varphi\left(a\sum_i x_iey_i\right)=\varphi(a)=a\varphi.$$

Таким образом, $\Phi(r)=\varphi$, т. е. Φ оказывается наложением. Итак, Φ — изоморфизм кольца R на кольцо эндоморфизмов D-пространства M. Остается заметить, что, в силу леммы 1, D-пространство M должно быть конечномерным и что кольцо эндоморфизмов конечномерного D-пространства изоморфно кольцу матриц над D (ср. ЭА, с. 166, теорема III.1.15).

Алгебра R с единицей над коммутативным кольцом Δ с единицей называется *центральной*, если ее центр совпадает с Δ (напомним, что в рассматриваемом случае $\Delta\subseteq R$ — ср. ЭА, с. 177, теорема III.2.1).

Теорема 2. *Тензорное произведение простой *) алгебры S с единицей над полем P и центральной простой алгебры R над тем же полем является простой алгеброй.*

Доказательство. Справедливость теоремы является непосредственным следствием следующей леммы:

Лемма: *Если R — центральная простая алгебра с единицей над полем P, а S — алгебра с единицей над тем же полем, то каждый идеал I алгебры $R \otimes_P S$ имеет вид $I = R \otimes H$, где H — идеал алгебры S.*

Для доказательства зафиксируем базу $\mathfrak{E}$ алгебры S. Можно предполагать, что $I \neq 0$. Поэтому среди ненулевых элементов идеала I найдется элемент d, имеющий наиболее короткую запись вида

$$d = \sum_{i=1}^{n} a_i \otimes e_i,$$

где $0 \neq a_i \in R$ и $e_i \in \mathfrak{E}$. Ввиду простоты алгебры R,

$$1 = \sum_j u_j a_1 v_j$$

для подходящих u_j, $v_j \in R$. Отсюда

$$d' = \sum_j (u_j \otimes 1)\, d\, (v_j \otimes 1) = 1 \otimes e_1 + c_2 \otimes e_2 + \ldots + c_n \otimes e_n,$$

где

$$c_i = \sum_j u_j a_i v_j.$$

Если $c_{i_0} \notin P$ для некоторого $i_0 \geqslant 2$, то $c_{i_0} x - x c_{i_0} \neq 0$ для некоторого $x \in R$, поскольку R центральна. Но

$$(1 \otimes e_1)(x \otimes 1) = x \otimes e_1 = (x \otimes 1)(1 \otimes e_1).$$

Поэтому из предложения 4.3 вытекает

$$d'' = d'(x \otimes 1) - (x \otimes 1) d' = \sum_{i=2}^{n} (c_i x - x c_i) \otimes e_i \neq 0.$$

Поскольку d'' лежит в I и имеет более короткую запись, чем d, то возникает противоречие. Таким образом, $c_i \in P$

*) Вообще говоря, идеал кольца R, являющегося Δ-алгеброй, является идеалом алгебры R лишь при условии, что он является подмодулем. Однако при наличии в кольце R единицы это дополнительное условие выполняется автоматически (ср. ЭА, с. 178, теорема III.2.3). Поэтому в рассматриваемом случае простота алгебры R означает простоту кольца R.

для всех i. Но тогда $c_i \otimes e_i = 1 \otimes c_i e_i$, откуда

$$1 \otimes \left(e_1 + \sum_{i=2}^{n} c_i e_i \right) = d' \in I.$$

Поэтому

$$H = \{y \mid y \in S,\ 1 \otimes y \in I\} \neq 0.$$

Нетрудно проверить, что H — идеал алгебры S. Из равенства

$$r \otimes y = (r \otimes 1)(1 \otimes y),$$

где $r \in R, y \in H$, вытекает, что $R \otimes H \subseteq I$. Выберем в идеале H некоторую базу $\mathfrak{B}'$ и дополним ее множеством $\mathfrak{B}''$ до базы алгебры S. Если $I \neq R \otimes H$, то найдем элемент $d \in I \setminus R \otimes H$, имеющий самую короткую запись вида

$$d = \sum_{i=1}^{n'} a_i \otimes e_i' + \sum_{j=1}^{n''} b_j \otimes e_j'',$$

где $0 \neq a_i, b_j \in R$, $e_i' \in \mathfrak{B}'$ и $e_j'' \in \mathfrak{B}''$. Тогда элемент $d - \sum_{i=1}^{n''} a_i \otimes e_i' \in I \setminus R \otimes H$ и имеет более короткую запись указанного вида. Следовательно, $a_i = 0$ для всех i, т. е.

$$d = \sum_{j=1}^{n''} b_j \otimes e_j''.$$

Как и выше, находим $u_k, v_k \in R$ так, что

$$\sum_k u_k b_1 v_k = 1,$$

и рассматриваем

$$d' = \sum_k (u_k \otimes 1)\, d\, (v_k \otimes 1) = 1 \otimes e_1'' + \sum_{j=2}^{n''} c_j \otimes e_j'',$$

где $c_j \in R$. Если $c_j \notin P$ для некоторого $j \geqslant 2$, то, как и выше, приходим к противоречию с выбором элемента d. Если же $c_j \in P$ для всех $j \geqslant 2$, то

$$d' = 1 \otimes \left(e_1'' + \sum_{j=2}^{n''} c_j e_j'' \right).$$

Поскольку $d' \in I$, то $e_1'' + \sum_{j=2}^{n''} c_j e_j'' \in H$, что невозможно.

Упражнения

1. Центр простого кольца с единицей является полем.
2. Кольцо матриц над простым кольцом просто.
3. Артиново справа простое кольцо с единицей, не содержащее идемпотентов, отличных от 0 и 1, является телом.
4. Если R — кольцо, а R_2 — кольцо 2×2-матриц над R, то

$$\begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} R_2 \begin{Vmatrix} 1 & 0 \\ 0 & 0 \end{Vmatrix} \cong R.$$

5. Пусть F — свободная ассоциативная алгебра с единицей над полем действительных чисел со свободной порождающей системой $\{x, y\}$ и I — ее идеал, порожденный элементом $xy - yx - 1$. Доказать, что фактор-кольцо F/I — нётерово слева и справа простое кольцо.
6. Пусть A и B — алгебры над коммутативным кольцом Δ с единицей. Тогда: а) центр алгебры $A \otimes_\Delta B$ порождается как подалгебра элементами вида $u \otimes v$, где u и v принадлежат центрам алгебр A и B соответственно. В частности,

$$(\text{центр } A \otimes_\Delta B) \cong (\text{центр } A) \otimes_\Delta (\text{центр } B);$$

б) если K и L — левые идеалы алгебр A и B соответственно, то аддитивная группа, порожденная элементами вида $u \otimes v$, где $u \in K$ и $v \in L$, является левым идеалом алгебры $A \otimes_\Delta B$; в) если K и L — двусторонние идеалы алгебр A и B соответственно, то аддитивная группа I, порожденная элементами вида $u \otimes v$, где $u \in K$ и $v \in L$, оказывается двусторонним идеалом алгебры $A \otimes_\Delta B$ и $(A \otimes_\Delta B)/I \cong (A/K) \otimes_\Delta (B/L)$ (подразумевается изоморфизм Δ-алгебр).
7. Если $\mathbf{K}$ — тело кватернионов, рассматриваемое как алгебра над полем действительных чисел $\mathbf{R}$, то $\mathbf{K} \otimes_{\mathbf{R}} \mathbf{K}$ и $\mathbf{R}_4$ изоморфны как $\mathbf{R}$-алгебры.

§ 6. Радикал и классически полупростые кольца

Одной из основных задач алгебры является описание строения алгебраических систем. В принципе этого можно достичь, выделяя те или иные классы таких систем, из которых могут быть сконструированы остальные более сложно устроенные системы. В случае колец для решения подобной задачи может быть использовано понятие радикала, рассматриваемое, впрочем, и в других теориях.

Назовем *радикалом* отображение τ класса всех колец в себя, обладающее следующими свойствами:

(1) $\tau(R)$ — идеал кольца R;

(2) $\tau(\tau(R)) = \tau(R)$;

(3) если $\varphi\colon R \to R'$ — гомоморфное наложение колец, то $\varphi(\tau(R)) \subseteq \tau(R')$;

(4) $\tau(R/\tau(R)) = 0$.

Пусть τ — радикал. Кольцо R называется τ-*радикальным*, если $\tau(R) = R$, и τ-*полупростым*, если $\tau(R) = 0$.

Тривиальными примерами радикала служат отображения $\mathfrak{r}(R)=0$ для всех R и $\mathfrak{r}(R)=R$ для всех R. В первом случае все кольца оказываются $\mathfrak{r}$-полупростыми, а $\{0\}$ — единственным $\mathfrak{r}$-радикальным кольцом. Прямо противоположная ситуация наблюдается во втором случае. Менее тривиальный пример доставляет определение

$$\mathfrak{r}(R)=\{x \mid x\in R,\quad nx=0 \quad \text{для некоторого} \quad n\in \mathbf{Z}\}.$$

В этом случае справедливость свойств (1)—(3) также очевидна, а проверка свойства (4) является нетрудным упражнением. Примером $\mathfrak{r}$-полупростого кольца в этом случае может служить поле действительных чисел, а примером $\mathfrak{r}$-радикального — любое кольцо вычетов.

Для построения более интересного радикала введем новую бинарную операцию $\circ$ (она называется *присоединенным умножением*), положив

$$a\circ b=a+b+ab.$$

Непосредственный счет показывает, что $(a\circ b)\circ c=a\circ(b\circ c)$ и $a\circ 0=0\circ a=a$ для любых a, b и c. Элемент a называется *квазирегулярным*, если существует элемент a' такой, что $a\circ a'=a'\circ a=0$. Правый идеал называется *квазирегулярным*, если квазирегулярны все его элементы. Ясно, что нулевой правый идеал квазирегулярен.

Теорема 1. *Пусть R — кольцо и $\mathfrak{r}(R)$ — сумма всех его правых квазирегулярных идеалов. Тогда $\mathfrak{r}$ оказывается радикалом.*

Доказательство. Сначала установим несколько лемм.

Лемма 1. *Если $b\circ y=0$ и $(a+ay)\circ z=0$, то*

$$(a+b)\circ y\circ z=0.$$

Действительно,

$$\begin{aligned}(a+b)\circ(y+z+yz)&=\\ &=a+b+y+z+yz+ay+az+ayz+by+bz+byz=\\ &=b\circ y+(a+ay)\circ z+(b\circ y)z=0.\end{aligned}$$

Лемма 2. *Если I — правый идеал и уравнение $a\circ x=0$ разрешимо в R для всех $a\in I$, то I квазирегулярен.*

В самом деле, если $a\in I$, то по условию $a\circ x=0$ для некоторого $x\in R$. Но $x=-a-ax\in I$ и, следовательно,

$x \circ y = 0$ для некоторого $y \in R$. Отсюда

$$x \circ a = x \circ a \circ x \circ y = x \circ y = 0,$$

что доказывает квазирегулярность элемента a.

Лемма 3. *Если* $xy \circ z = 0$, *то* $yx \circ u = 0$ *для некоторого* $u \in R$.

Для доказательства положим $u = -yx - yzx$ и заметим, что

$$yx \circ u = yx - yx - yzx - (yx)^2 - yxyzx =$$
$$= -y(xy + z + (xy)z)x = -y(xy \circ z)x = 0.$$

Лемма 4. *Если* I_1 *и* I_2 — *квазирегулярные правые идеалы, то правый идеал* $I_1 + I_2$ *также квазирегулярен.*

Действительно, если $a \in I_1$ и $b \in I_2$, то $b \circ y = 0$ для некоторого $y \in R$. Поскольку $a + ay \in I_1$, то $(a + ay) \circ z = 0$ для некоторого $z \in R$. В силу леммы 1, $(a + b) \circ (y \circ z) = 0$, и квазирегулярность правого идеала $I_1 + I_2$ вытекает из леммы 2.

Лемма 5. *Правый идеал* $\mathfrak{r}(R)$ *квазирегулярен.*

Для доказательства достаточно заметить, что каждый элемент из $\mathfrak{r}(R)$ принадлежит сумме конечного числа квазирегулярных правых идеалов, и, используя лемму 4, провести индукцию.

Лемма 6. $\mathfrak{r}(R)$ — *двусторонний идеал.*

Действительно, если $x \in R$ и $b \in x\mathfrak{r}(R)$, то $b = xa$, где $a \in \mathfrak{r}(R)$. Но $ax \in \mathfrak{r}(R)$, и, в силу леммы 5, $ax \circ z = 0$ для некоторого $z \in R$. По лемме 3, $xa \circ u = 0$ для некоторого $u \in R$. Таким образом, правый идеал $x\mathfrak{r}(R)$ удовлетворяет условиям леммы 2 и, следовательно, квазирегулярен. Поэтому $x\mathfrak{r}(R) \subseteq \mathfrak{r}(R)$ для всех $x \in R$, т. е. $\mathfrak{r}(R)$ — левый идеал. Но $\mathfrak{r}(R)$ — правый идеал по определению.

Лемма 7. $\mathfrak{r}(R)$ — *квазирегулярное кольцо, т. е.* $\mathfrak{r}(\mathfrak{r}(R)) = \mathfrak{r}(R)$.

Действительно, по лемме 5 для любого $a \in \mathfrak{r}(R)$ имеем $a \circ a' = a' \circ a = 0$ для некоторого $a' \in R$. При этом $a' = -a - aa' \in \mathfrak{r}(R)$ ибо $\mathfrak{r}(R)$ — правый идеал. Таким образом, $\mathfrak{r}(R)$ — квазирегулярное кольцо и, следовательно, $\mathfrak{r}(\mathfrak{r}(R)) = \mathfrak{r}(R)$.

Лемма 8. *Если* φ: $R \to R'$ — *гомоморфное наложение, то* $\varphi(\mathfrak{r}(R)) \subseteq \mathfrak{r}(R')$.

Достаточно заметить, что при гомоморфном наложении образом квазирегулярного идеала служит квазирегулярный идеал, и учесть лемму 6.

Лемма 9. $\tau(R/\tau(R))=0$.

Для доказательства обозначим через π естественный гомоморфизм R на $R/\tau(R)$. Пусть $\bar{J}=\tau(R/\tau(R))$ и $I=\pi^{-1}(\bar{J})$. Если $a\in I$, то $\pi(a\circ x)=\pi(a)\circ\pi(x)=\pi(0)$ для некоторого $x\in R$, поскольку $\bar{J}$, в силу леммы 7, квазирегулярен. Следовательно, $a\circ x\in\tau(R)$, а значит,

$$a\circ(x\circ y)=(a\circ x)\circ y=0$$

для некоторого $y\in R$ в силу леммы 5. По лемме 2, правый идеал I квазирегулярен. Следовательно, $I\subseteq\tau(R)$, т. е. $\bar{J}$ — нулевой идеал.

Справедливость теоремы является непосредственным следствием лемм 6—9.

Радикал τ, возникающий согласно теореме 1, называется *квазирегулярным радикалом* или *радикалом Джекобсона*. Идеал $\tau(R)$ называется *квазирегулярным радикалом кольца* R.

Предложение 1. *Пусть R — кольцо и J — его квазирегулярный радикал. Тогда*

(а) *J равен сумме всех квазирегулярных левых идеалов кольца R;*

(б) *если H — правый [левый] ниль-идеал кольца* (т. е. $\forall x\in H\exists n\ (x^n=0)$), *то $H\subseteq J$;*

(в) *если $a\in R$, $b\in J$ и $ab=a$ [$ba=a$], то $a=0$;*

(г) *если R — кольцо с единицей, то J совпадает с пересечением всех максимальных правых [левых] идеалов кольца R;*

д) *если R артиново справа [слева], то J нильпотентен* (т. е. найдется такое n, что произведение любых n элементов из J равно нулю).

Доказательство. (а) Пусть J' — сумма всех квазирегулярных левых идеалов кольца R. Переходя к инверсному кольцу, т. е. рассматривая на множестве R операцию $x\circ y=yx$ и применяя теорему 1, убеждаемся, что J' — двусторонний квазирегулярный идеал. Следовательно, $J'\subseteq J$. Переход к инверсному кольцу позволяет доказать обратное включение.

(б) Если $x\in H$ и $x^n=0$, то положим

$$y=(-x)+(-x)^2+\ldots+(-x)^{n-1}.$$

Тогда

$$y\circ x=x\circ y=x+[-x+(-x)^2+\ldots+(-x)^{n-1}]+$$
$$+x[-x+(-x)^2+\ldots+(-x)^{n-1}]=0.$$

Таким образом, H оказывается квазирегулярным правым [левым] идеалом. Остается принять во внимание (а).

(в) Поскольку $-b \in J$, то $(-b)+x+(-b)x=0$ для некоторого $x \in R$. Если $ab=a$, то

$$a=ab=a(x-bx)=ax-abx=ax-ax=0.$$

Случай, когда $ba=a$, рассматривается аналогично.

(г) Обозначим через W пересечение всех максимальных правых идеалов кольца R. Если $J \not\subseteq W$, то $J \not\subseteq M$ для некоторого максимального правого идеала M кольца R. Отсюда $R=J+M$ и, следовательно, $1=x+y$, где $x \in J$ и $y \in M$. Но $-x+z+(-x)z=0$ для некоторого $z \in R$. Отсюда

$$x=z-xz=(1-x)z=yz \in M$$

и, следовательно, $1 \in M$, что невозможно. Таким образом, $J \subseteq W$. Пусть, далее, $w \in W$. Если $(1+w)R \neq R$, то $(1+W)R$ содержится в некотором максимальном правом идеале M и, в частности, $1+w \in M$. Поскольку $w \in M$, то $1 \in M$, что невозможно. Следовательно, $(1+w)R=R$, т. е. $1=(1+w)r$ для некоторого $r \in R$. Отсюда

$$w+(r-1)+w(r-1)=w+r-1+wr-w=0,$$

и W квазирегулярен по лемме 2 теоремы 1. Этим доказано, что $W \subseteq J$. Второе утверждение доказывается переходом к инверсному кольцу.

(д) В силу правой артиновости кольца R для некоторого n имеем

$$J^n=J^{n+1}=\ldots=J^{2n},$$

где, как обычно, для $X, Y \subseteq R$ под XY понимается совокупность всевозможных сумм $\sum_i x_i y_i$, где $x_i \in X$, $y_i \in Y$. Положив $V=J^n$, заметим, что $V=V^2$. Если $V=0$, то все доказано. В противном случае оказывается непустым множество

$$\mathfrak{M}=\{I \mid I-\text{правый идеал в } R,\ I \subseteq J,\ IV \neq 0\},$$

ибо $V \in \mathfrak{M}$. Ввиду правой артиновости кольца R, множество $\mathfrak{M}$ содержит минимальный элемент, скажем, I_0. Поскольку $I_0 \in \mathfrak{M}$, то найдется такой элемент $a \in I_0$, что $aV \neq 0$. Но тогда

$$(aV)V=aV^2=aV \neq 0,$$

т. е. $aV \in \mathfrak{M}$. Поскольку $aV \subseteq I_0$, то, в силу выбора правого идеала I_0, имеем $aV = I_0$. Отсюда $a = av$ для некоторого $v \in V$, что, ввиду (в), влечет $a = 0$ хотя выше было отмечено, что $aV \neq 0$. Справедливость утверждеиия (д) для артинова слева кольца устанавливается переходом к инверсному кольцу.

Кольцо называется *классическим полупростым*, если оно изоморфно прямой сумме конечного числа полных колец матриц над некоторыми телами.

Теорема 2 (Веддербарн—Артин). *Для кольца R с единицей эквивалентны следующие утверждения*:

(1) *R — классически полупростое кольцо*;

(2) *R — артиново справа [слева] кольцо с нулевым квазирегулярным радикалом*;

(3) *R разлагается в прямую сумму минимальных правых [левых] идеалов* (т. е. *R вполне приводимо справа [слева]*);

(4) *Для каждого правого [левого] идеала H кольца R найдется такой идемпотент $e \in R$, что $H = eR$ [$H = Re$]*, (т. е. H порождается идемпотентом);

(5) *Для каждого правого [левого] идеала H' кольца R найдется такой правый [левый] идеал H', что $R = H \oplus H'$.*

(6) *R — артиново справа [слева] регулярное кольцо*;

(7) *R — нётерово справа [слева] регулярное кольцо.*

Доказательство. Достаточно доказать правый вариант, ибо левый выводится из него переходом к инверсному кольцу, поскольку при этом переходе справедливость свойства (1), очевидно, сохраняется.

(1) $\Rightarrow$ (6). Кольцо матриц над телом D, будучи конечномерным пространством над D, оказывается артиновым справа, поскольку его правые идеалы являются подпространствами. После этого правая артиновость кольца R вытекает из предложения 3.3. Регулярность кольца матриц над телом вытекает из теоремы 2.2. Регулярность конечной прямой суммы регулярных колец проверяется без труда.

(6) $\Rightarrow$ (2). Если J — квазирегулярный радикал артинова справа регулярного кольца и $0 \neq x \in J$, то, в силу теоремы 2.1, $xR = eR$, где $e^2 = e \in xR \subseteq J$. Но тогда $e = 0$ по предложению 1 (в), а значит, $x = 0$, что невозможно.

(2) $\Rightarrow$ (3). Для сокращения речи условимся называть идемпотент e кольца R *минимальным*, если eR — минимальный правый идеал. В силу правой артиновости, R содержит минимальный правый идеал M. Поскольку

квазирегулярный радикал кольца R равен нулю, то, ввиду предложения 1 (б), $M^2 \neq 0$. Но тогда $M = eR$, где $e^2 = e \in R$ (см. ЭА, с. 129, теорема II.6.3). Таким образом, кольцо R содержит минимальные идемпотенты. Другими словами, если определить *ортогональную систему* как множество ненулевых попарно ортогональных минимальных идемпотентов *), то в R существуют ортогональные системы. Совокупность всех таких ортогональных систем образует частично упорядоченное множество относительно обычного включения. Поскольку объединение возрастающей последовательности ортогональных систем снова оказывается ортогональной системой, то, согласно теореме I.1.2, существует максимальная ортогональная система, скажем, $\mathfrak{Z}$. Если $\mathfrak{Z}$ бесконечна, то в ней содержится счетная подсистема, скажем, $\{e_1, e_2, \ldots\}$. Положим

$$H_i = \sum_{k=i}^{\infty} e_k R.$$

Тогда

$$H_1 \supseteq H_2 \supseteq \ldots$$

и, в силу правой артиновости, $H_n = H_{n+1}$ для некоторого n. Отсюда $e_n \in H_{n+1}$, т. е.

$$e_n = \sum_{k=n+1}^{m} e_k r_k,$$

где $r_k \in R$. Следовательно,

$$0 \neq e_n = e_n^2 = e_n \sum_{k=n+1}^{m} e_k r_k = 0,$$

ибо $e_n e_k = 0$, если $k > n$. Таким образом,

$$\mathfrak{Z} = \{e_1, \ldots, e_n\}.$$

Положим

$$e = e_1 + \ldots + e_n.$$

Учитывая ортогональность идемпотентов e_i, нетрудно подсчитать, что $e^2 = e$ и $e_i e = e_i = e e_i$ для каждого i. Допустим, что $e \neq 1$. Тогда правый идеал $(1-e)R \neq 0$ и,

*) Напомним, что идемпотенты e и f называются *ортогональными*, если $ef = fe = 0$.

в силу правой артиновости кольца R, содержит минимальный правый идеал, порождаемый, как уже отмечалось, некоторым минимальным идемпотентом f. Поскольку $f \in (1-e)R$, то $f=(1-e)r$ для некоторого $r \in R$. Отсюда

$$e_i f = e_i e f = e_i e (1-e) r = e_i 0 r = 0.$$

Если $fe=0$, то

$$f e_i = f e e_i = 0 e_i = 0$$

для каждого i и, вопреки допущению, максимальная система $\mathfrak{Z}$ вкладывается в бóльшую ортогональную систему $\mathfrak{Z} \cup \{f\}$. Таким образом, $fe \neq 0$, но $ef=0$. Рассмотрим элемент $g=f(1-e)$. Равенство

$$g^2 = f(1-e)f(1-e) = f(f-ef)(1-e) = \\ = f^2(1-e) = f(1-e) = g$$

показывает, что g — идемпотент. Если $g=0$, то $f=fe$, откуда

$$0 \neq f = f^2 = fef = f0 = 0,$$

что невозможно. Если же $g \neq 0$, то из соотношения $0 \neq gR \subseteq fR$ и минимальности правого идеала fR вытекает, что $gR=fR$. Следовательно, g — минимальный идемпотент. Но

$$e_i g = e_i f (1-e) = 0 (1-e) = 0$$

и

$$g e_i = f(1-e) e_i = f(1-e) e e_i = f 0 e_i = 0,$$

и мы опять сумели вложить максимальную ортогональную систему $\mathfrak{Z}$ в бóльшую ортогональную систему $\mathfrak{Z} \cup \{g\}$. Полученное противоречие показывает, что $e=1$, откуда

$$R = 1R = e_1 R \oplus \ldots \oplus e_n R$$

(см. ЭА, с. 128, теорема II.6.2).

Импликации (3) $\Rightarrow$ (4), (4) $\Rightarrow$ (5) и (5) $\Rightarrow$ (4) вытекают из элементарных свойств правых [левых] идеалов (см. ЭМ, с. 130, теорема II.6.6; с. 128, теоремы II.6.2 и II.6.1).

(4) $\Rightarrow$ (1). Пусть R обладает свойством (4).

Из предложения 3.1 вытекает

Лемма 1. *R нетерово справа.*

Ввиду леммы 1, каждый ненулевой правый идеал I кольца R содержит максимальный подмодуль H. В силу уже доказанной импликации (4) $\Rightarrow$ (5), структура правых

идеалов кольца R является структурой с дополнениями. С другой стороны, из предложения III.2.1 и следствия 2 теоремы II.2.3 вытекает, что эта структура дедекиндова. Отсюда, учитывая предложение III.2.4, выводим, что $I = H \oplus M$ для некоторого правого идеала M кольца R. Поскольку $M \cong I/H$ (ЭА, с. 120, следствие теоремы II.5.16), то M — минимальный правый идеал (ЭА, с. 121, теорема II.5.19). Таким образом, доказана

Лемма 2. *Каждый ненулевой правый идеал кольца R содержит минимальный правый идеал.*

Лемма 3. *Каждый двусторонний идеал I кольца R порождается центральным идемпотентом.*

В самом деле, согласно (4), $I = eR$, где $e^2 = e \in R$. Поскольку I — двусторонний идеал, то для любого $r \in R$ имеем $re \in I = eR$ и, следовательно, $re = er'$ для некоторого $r' \in R$. Отсюда

$$(1-e)\,re = (1-e)\,er' = 0 \qquad (*)$$

для любого $r \in R$. Согласно (4), $er\,(1-e)\,R = gR$, где $g^2 = g \in R$, а значит, $er\,(1-e) = ger\,(1-e)$ и $g = er\,(1-e)\,s$ для некоторого $s \in R$. Ввиду (*),

$$g = g^2 = er\,(1-e)\,ser\,(1-e)\,s = 0$$

и, следовательно,

$$er - ere = er\,(1-e) = ger\,(1-e) = 0. \qquad (**)$$

Учитывая (*) и (**), получаем

$$er - re = (e + (1-e))\,(er - re) =$$
$$= er + (1-e)\,er - ere - (1-e)\,re = 0$$

для любого $r \in R$, т. е. e оказывается центральным идемпотентом.

Далее, для сокращения речи условимся называть идемпотент e *простым*, если e централен и eR — простое кольцо.

Лемма 4. *Каждый ненулевой идеал I кольца R содержит простой идемпотент.*

Действительно, по лемме 1, среди двусторонних идеалов кольца R, лежащих в I, содержится максимальный, скажем M. В силу леммы 3, $I = eR$ и $M = fR$, где e и f — центральные идемпотенты. Разумеется, $ef = f$. Поэтому $e - f$ — центральный идемпотент, и $I = M \oplus (e-f)\,R$ (ср. ЭА, с. 128, теорема II.6.1). Если H — ненулевой двусторонний идеал кольца $(e-f)\,R$, то H — ненулевой двусторонний идеал кольца R (ЭА, с. 131, теорема II.6.7(1)). Поскольку

$M \subset M \oplus H$, то $M \oplus H = I$. Но тогда $e-f = fr + x$, где $r \in R$ и $x \in H$. Умножая слева на $e-f$, получим

$$e-f = (e-f)\,x \in H,$$

т. е. $H = (e-f)\,R$. Таким образом, $(e-f)\,R$ — простое кольцо, т. е. $e-f$ — простой идемпотент.

Лемма 4 показывает, что, определив *ортогональную систему* как множество попарно ортогональных простых идемпотентов, мы получим, что в кольце R существуют ортогональные системы. Совокупность всех таких ортогональных систем образует частично упорядоченное множество по включению. Поскольку объединение возрастающей последовательности ортогональных систем снова оказывается ортогональной системой, то, по теореме I.1.2, найдется максимальная ортогональная система, скажем, $\mathfrak{I}$. Если $\mathfrak{I}$ бесконечна, то в ней содержится счетная подсистема $\{e_1, e_2, \ldots\}$. Положим

$$H_m = \sum_{i=1}^{m} e_i R.$$

Тогда

$$H_1 \subseteq H_2 \subseteq \ldots$$

и, в силу леммы 1, $H_n = H_{n+1}$ для некоторого n. Отсюда $e_{n+1} \in H_n$, т. е.

$$e_{n+1} = \sum_{i=1}^{n} e_i r_i,$$

где $r_i \in R$. Поскольку $e_{n+1} e_i = 0$ при $i \leqslant n$, то

$$0 \neq e_{n+1} = e_{n+1}^2 = e_{n+1} \sum_{i=1}^{n} e_i r_i = 0.$$

Таким образом,

$$\mathfrak{I} = \{e_1, \ldots, e_n\}.$$

Положим

$$e = e_1 + \ldots + e_n.$$

Если $e \neq 1$, то, по лемме 4, идеал $(1-e)\,R$ содержит простой идемпотент, скажем, g. Поскольку g централен, $e_i e = e_i = e e_i$ для любого i и $g = (1-e)\,g$, то $g e_i = e_i g = 0$ для всех i. Таким образом, максимальная ортогональная

система $\mathfrak{I}$ вкладывается в бо́льшую ортогональную систему $\mathfrak{I} \cup \{g\}$, что невозможно. Следовательно, $e = 1$, а значит,

$$R = e_1 R \oplus \ldots \oplus e_n R,$$

где $e_i R$ — простое кольцо с единицей e_i, содержащее в силу леммы 2 минимальный правый идеал (см. ЭА, с. 128, теорема II.6.1, с. 131, теорема II.6.7 (1)). В силу теоремы 5.1, $e_i R$ изоморфно кольцу матриц над некоторым телом.

(4) $\Rightarrow$ (7). Тривиально.

(7) $\Rightarrow$ (4). Достаточно вспомнить, что, согласно теореме 2.1, все конечно порожденные правые идеалы регулярного кольца порождаются идемпотентами и что, по предложению 3.1, все правые идеалы нётерова справа кольца конечно порождены.

Упражнения

1. Найти квазирегулярный радикал следующих колец: а) кольцо вычетов по модулю n; б) кольцо многочленов над полем; в) фактор-кольцо кольца многочленов над полем по идеалу, порожденному многочленом f; г) кольцо степенных рядов над полем; д) кольцо верхних треугольных матриц над полем.

2. Пусть $\mathfrak{r}$ — квазирегулярный радикал. Доказать: а) $\mathfrak{r}(R) = 0$, если R — регулярное кольцо; б) если R_n — кольцо $n \times n$-матриц над R, то $\mathfrak{r}(R_n) = (\mathfrak{r}(R))_n$; в) $\mathfrak{r}(R \oplus S) = \mathfrak{r}(R) \oplus \mathfrak{r}(S)$ (имеется в виду кольцевая прямая сумма); г) $\mathfrak{r}(I) = I \cap \mathfrak{r}(R)$ для всякого идеала I кольца R.

3. Кольцо матриц над классически полупростым кольцом классически полупросто.

4. Если идеал I кольца R и фактор-кольцо R/I $\mathfrak{r}$-радикальны, то R также $\mathfrak{r}$-радикально.

5. Классически полупростое кольцо без делителей нуля является телом.

6. Если все идемпотенты классически полупростого кольца центральны, то оно разлагается в прямую сумму тел.

7. Артиново кольцо без нильпотентных элементов изоморфно прямой сумме тел.

8. Коммутативное кольцо с нулевым квазирегулярным радикалом разлагается в подпрямое произведение полей.

9. Если пересечение максимальных двусторонних идеалов кольца R равно нулю, то R разлагается в подпрямое произведение простых колец.

10. Следующие свойства кольца R эквивалентны: (1) R не содержит левых идеалов, отличных от $\{0\}$ и R; (2) R не содержит правых идеалов, отличных от $\{0\}$ и R; (3) R — или тело, или одноэлементное кольцо, или абелева группа простого порядка с нулевым умножением.

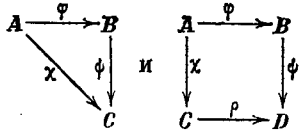
11. Центр классически полупростого кольца является прямой суммой полей.

§ 7. Гомологическая алгебра

В этом параграфе рассматриваются правые модули над кольцом R с единицей. Широко используется язык точных последовательностей. Именно, строка

$$A \xrightarrow{\varphi} B \xrightarrow{\psi} C,$$

где A, B и C — модули, а φ и ψ — гомоморфизмы, называется *точной последовательностью*, если $\operatorname{Im}\varphi = \operatorname{Ker}\psi$. Нетрудно заметить, что точность последовательности $0 \xrightarrow{} A \xrightarrow{\varphi} B$ $[A \xrightarrow{\psi} B \xrightarrow{} 0]$ означает, что φ—вложение [ψ—наложение]. Последовательность $0 \to A \to B \to C \to 0$ называется точной, если точны последовательности $0 \to A \to B$, $A \to B \to C$ и $B \to C \to 0$. Фигуры



где A, B, C, D — модули, а φ, ψ, χ, ρ — гомоморфизмы, называются *коммутативными диаграммами*, если $\varphi\psi = \chi$ и $\varphi\psi = \chi\rho$ соответственно.

Предложение 1. *Следующие свойства точной последовательности*

$$0 \xrightarrow{} A \xrightarrow{\iota} B \xrightarrow{\pi} C \xrightarrow{} 0$$

эквивалентны:

(1) $\iota\varphi = 1_A$ *для некоторого* φ: $B \to A$;

(2) $\psi\pi = 1_C$ *для некоторого* ψ: $C \to B$;

(3) $B = (\operatorname{Im}\iota) \oplus H$ *для некоторого подмодуля* $H \subseteq B$;

(4) *существует такой эндоморфизм* f *модуля* B, *что* $f^2 = f$ *и* $\operatorname{Im} f = \operatorname{Im}\iota$.

Доказательство. (1) $\Rightarrow$ (4). Положим $f = \varphi\iota$. Тогда $\operatorname{Im} f \subseteq \operatorname{Im}\iota$. Кроме того,

$$f^2 = \varphi\iota\varphi\iota = \varphi 1_A \iota = \varphi\iota = f.$$

Наконец, если $a \in A$, то

$$a\iota = a 1_A \iota = a\iota\varphi\iota = a\iota f \in \operatorname{Im} f,$$

т. е. $\operatorname{Im}\iota \subseteq \operatorname{Im} f$.

(4) $\Rightarrow$ (3). Положим $H=\{x-xf \mid x\in B\}$. Легко проверить, что H — подмодуль. При этом $b=bf+(b-bf)$ для каждого $b\in B$, т. е.

$$B=\operatorname{Im} f+H=\operatorname{Im}\iota+H.$$

Если $x\iota=y-yf$, где $x,\ y\in B$, то $x\iota=zf$ для некоторого $z\in B$, откуда

$$zf=zf^2=(y-yf)f=yf-yf^2=0$$

Таким образом, $\operatorname{Im}\iota\cap H=0$, т. е. $B=\operatorname{Im}\iota\oplus H$.

(3) $\Rightarrow$ (1). Достаточно положить $(a\iota+h)\varphi=a$ для любых $a\in A$ и $h\in H$.

(1) $\Rightarrow$ (2). Для каждого $c\in C$ положим $c\psi=b-b\varphi\iota$, где $b\pi=c$. Определение корректно, ибо $b\pi=b'\pi$ влечет $b-b'=a\iota$ для некоторого $a\in A$, откуда

$$(b-b\varphi\iota)-(b'-b'\varphi\iota)=(b-b')-(b-b')\varphi\iota=a\iota-a\iota\varphi\iota=0.$$

Простой счет показывает, что ψ — гомоморфизм. Если $c\in C$, то, поскольку $\iota\pi=0$, получим

$$c\psi\pi=(b-b\varphi\iota)\pi=c-b\varphi\iota\pi=c,$$

т. е. $\psi\pi=1_C$.

(2) $\Rightarrow$ (4). Положим $f=1_B-\pi\psi$. Тогда

$$f^2=1_B-\pi\psi-\pi\psi+\pi\psi\pi\psi=f.$$

Если $a\in A$, то

$$a\iota=a\iota-a\iota\pi\psi=(a\iota)f,$$

т. е. $\operatorname{Im}\iota\subseteq\operatorname{Im}f$. С другой стороны, для любого $b\in B$ имеем

$$(bf)\pi=b(1_B-\pi\psi)\pi=b\pi-b\pi 1_C=0.$$

Следовательно,

$$bf\in\operatorname{Ker}\pi=\operatorname{Im}\iota,$$

т. е. $\operatorname{Im}f\subseteq\operatorname{Im}\iota$.

Точная последовательность, обладающая свойствами, перечисленными в предложении 1, называется *расщепляющейся*.

Модуль P называется *проективным*, если всякая диаграмма

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow & & \\ A & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

с точной строкой дополняется до коммутативной некоторым гомоморфизмом $P \to A$. Меняя в этом определении направление стрелок, приходим к следующему определению: модуль Q называется *инъективным*, если всякая диаграмма

$$\begin{array}{ccccc} 0 & \to & A & \to & B \\ & & \downarrow & & \\ & & Q & & \end{array}$$

с точной строкой дополняется до коммутативной некоторым гомоморфизмом $B \to Q$.

Вопрос о существовании проективных модулей решается следующим предложением:

Предложение 2. *Следующие свойства модуля P эквивалентны:*

(1) *P проективен;*

(2) *всякая точная последовательность $0 \to A \to B \to P \to 0$ расщепляется;*

(3) *существует такой свободный модуль F, что $F = P \oplus H$ для некоторого подмодуля $H \subseteq F$.*

Доказательство. (1) $\Rightarrow$ (2). Согласно (1), диаграмма

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & & \downarrow 1_P & & \\ 0 & \to & A & \to & B & \xrightarrow{\pi} & P & \to & 0 \end{array}$$

дополняется до коммутативной некоторым гомоморфизмом ψ: $P \to B$. Следовательно, $\psi\pi = 1_P$, т. е. справедливо свойство (2) предложения 1.

(2) $\Rightarrow$ (3). Поскольку P является гомоморфным образом некоторого свободного модуля F, то возникает точная последовательность

$$0 \to \operatorname{Ker}\pi \xrightarrow{\iota} F \xrightarrow{\pi} P \to 0,$$

где ι — естественное вложение. Согласно предложению 1,

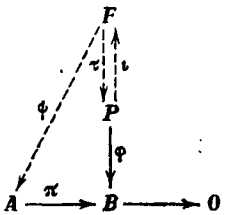
$$F = \operatorname{Ker}\pi \oplus P',$$

откуда

$$P \cong F/\operatorname{Ker}\pi \cong P'$$

см. ЭА, с. 120, следствие теоремы II.5.16).

(3) $\Rightarrow$ (1). Пусть $F = P \oplus H$, где F — свободный модуль с базой $\mathscr{E}$. Естественное вложение P в F обозначим через ι, а естественную проекцию F на P через τ. Тогда $\iota\tau = 1_P$. Рассмотрим диаграмму



с точной строкой. Поскольку π — наложение, то для каждого $e \in \mathscr{E}$ можно выбрать в A такой элемент $e\psi$, что $(e\psi)\pi = e\tau\varphi$. Возникающее таким образом отображение ψ базы $\mathscr{E}$ в модуль A может быть продолжено до гомоморфизма модуля F в A, который мы также обозначим через ψ. Для любого $x \in P$ имеем

$$x\iota = \sum_{e \in \mathscr{E}} e\lambda_e,$$

где $\lambda_e \in R$. Отсюда

$$x(\iota\psi)\pi = \sum_{e \in \mathscr{E}} ((e\psi)\pi)\lambda_e = \sum_{e \in \mathscr{E}} (e\tau\varphi)\lambda_e =$$
$$= \left(\sum_{e \in \mathscr{E}} e\lambda_e\right)\tau\varphi = x\iota\tau\varphi = x1_P\varphi = x\varphi.$$

Таким образом, $(\iota\psi)\pi = \varphi$, что доказывает проективность модуля P.

Из предложения 2, в частности, следует, что всякий свободный модуль проективен. Поэтому каждый модуль оказывается гомоморфным образом проективного. Естественно ожидать, что всякий модуль вкладывается в инъективный. Однако этот факт, да и само существование инъективных модулей устанавливается далеко не тривиальными рассуждениями. Приступим к решению этой задачи.

Теорема 1 (Критерий Бэра). *Если всякая диаграмма*

$$\begin{array}{ccc} I & \xrightarrow{\varkappa} & R \\ \downarrow & & \\ Q & & \end{array}$$

где ι — естественное вложение правого идеала I в кольцо R, дополняется до коммутативной некоторым гомоморфизмом $R \to Q$, то правый R-модуль Q инъективен.

Доказательство. Рассмотрим диаграмму

$$\begin{array}{ccc} 0 \longrightarrow A & \xrightarrow{\iota} & B \\ & \downarrow{\scriptstyle \varphi} & \\ & Q & \end{array}$$

с точной строкой. Пусть $A_0 = \operatorname{Im}\iota$. Рассмотрим множество $\mathfrak{P}$ всех пар (A', φ'), где $A_0 \subseteq A' \subseteq B$, $\varphi'\colon A' \to Q$ и $a\iota\varphi' = a\varphi$ для всех $a \in A$. Множество $\mathfrak{P}$ непусто, ибо $(A_0, \iota^{-1}\varphi) \in \mathfrak{P}$. Положим

$$(A', \varphi') \leqslant (A'', \varphi''),$$

если $A' \subseteq A''$ и $a'\varphi' = a'\varphi''$ для всех $a' \in A'$. Легко проверяется, что это определение превращает $\mathfrak{P}$ в частично упорядоченное множество. Если $\{(A_\alpha, \varphi_\alpha)\}$ — возрастающая цепь из $\mathfrak{P}$, то рассмотрим пару $(\bar{A}, \bar{\varphi})$, где $\bar{A} = \bigcup A_\alpha$ и $\bar{a}\bar{\varphi} = \bar{a}\varphi_\alpha$, если $\bar{a} \in A_\alpha$. Легко проверить, что $\bar{\varphi}$ не зависит от выбора индекса α и является гомоморфизмом $\bar{A}$ в Q. Ясно, что $a\iota\bar{\varphi} = a\varphi$. Таким образом, $(\bar{A}, \bar{\varphi}) \in \mathfrak{P}$. При этом $(\bar{A}, \bar{\varphi}) \geqslant (A_\alpha, \varphi_\alpha)$ для всех α. Этим доказано, что верхний конус любой цепи из $\mathfrak{P}$ не пуст. По лемме Куратовского — Цорна (теорема I.1.2), частично упорядоченное множество $\mathfrak{P}$ содержит максимальный элемент (A^0, φ^0). Если $A^0 = B$, то все доказано. Если же $A^0 \neq B$, то выберем элемент $b \in B \setminus A^0$. Тогда

$$I = \{\lambda \mid \lambda \in R,\ b\lambda \in A^0\}$$

— правый идеал кольца R. Определим гомоморфизм $f\colon I \to Q$, положив $\lambda f = (b\lambda)\varphi^0$, и найдем продолжающий его гомоморфизм $g\colon R \to Q$. Пусть $1g = q \in Q$. Рассмотрим подмодуль $\bar{B} = A^0 + bR$ модуля B. Если $a \in A^0$ и $\lambda \in R$, то положим

$$(a + b\lambda)\psi = a\varphi^0 + q\lambda.$$

Если

$$a + b\lambda = a' + b\lambda',$$

то

$$b(\lambda - \lambda') = a' - a \in A^0,$$

т. е. $\lambda - \lambda' \in I$. Отсюда

$$(a' - a)\varphi^0 = (b(\lambda - \lambda'))\varphi^0 = (\lambda - \lambda')f = (1(\lambda - \lambda'))g = \\ = q(\lambda - \lambda'),$$

т. е.

$$(a + b\lambda)\psi = a\varphi^0 + q\lambda = a'\varphi^0 + q\lambda' = (a' + b\lambda')\psi.$$

Таким образом, ψ оказывается гомоморфизмом модуля $\overline{B}$ в Q. Легко видеть, что $a\iota\psi = a\iota\varphi_0 = a\varphi$ для всех $a \in A$. Следовательно, $(\overline{B}, \psi) \in \mathfrak{P}$. Но это невозможно, поскольку $(\overline{B}, \psi) > (A^0, \varphi^0)$.

Теорема 1 позволяет дать описание инъективных абелевых групп:

Предложение 3. *Абелева группа Q является инъективным $\mathbf{Z}$-модулем тогда и только тогда, когда она делима* (т. е. уравнение $xm = q$ разрешимо в ней для любых $0 \neq m \in \mathbf{Z}$ и $q \in Q$).

В самом деле, если всякое уравнение вида $xm = q$ разрешимо в Q и дана диаграмма

$$\begin{array}{ccc} 0 \to I & \to & \mathbf{Z} \\ & & \downarrow \varphi \\ & & Q \end{array}$$

с точной строкой, то $I = 0$ или $I = m\mathbf{Z}$. Если $I = 0$, то возможность замкнуть данную диаграмму до коммутативной очевидна. Если $I = m\mathbf{Z}$ и $m\varphi = q$, где $m \neq 0$, то $xm = q$ для некоторого $x \in Q$. Ясно, что существует такой гомоморфизм ψ: $\mathbf{Z} \to Q$, что $1\psi = x$. Тогда для любого $k \in \mathbf{Z}$ имеем

$$(mk)\psi = (1\psi)mk = x(mk) = qk = (m\varphi)k = (mk)\varphi,$$

и инъективность $\mathbf{Z}$-модуля Q вытекает из теоремы 1. Наоборот, если Q — инъективный $\mathbf{Z}$-модуль и дано уравнение $xm = q$, то, очевидно, существует такой гомоморфизм φ: $m\mathbf{Z} \to Q$, что $m\varphi = q$. Ввиду инъективности модуля Q, найдется гомоморфизм ψ: $\mathbf{Z} \to Q$ такой, что $m\varphi = m\psi$. Отсюда

$$(1\psi)m = m\psi = m\varphi = q,$$

что и требовалось.

Теорема 2. *Всякий правый R-модуль можно вложить в инъективный правый R-модуль.*

Доказательство. Сначала установим две леммы.

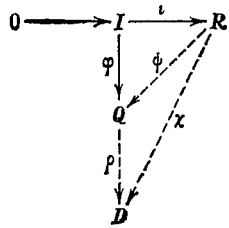
Лемма 1. *Если D — делимая абелева группа, то абелева группа $Q = \mathrm{Hom}_{\mathbf{Z}}(R, D)$ становится инъективным правым R-модулем, если для любых $\lambda, \xi \in R$ и $f \in Q$ положить*

$$\xi(f\lambda) = (\lambda\xi) f.$$

В самом деле, ясно, что $f\lambda \in Q$. Кроме того, если $\mu \in R$, то

$$\xi(f(\lambda\mu)) = ((\lambda\mu)\xi) f = (\lambda(\mu\xi)) f = (\mu\xi)(f\lambda) = \xi((f\lambda)\mu),$$

т. е. $f(\lambda\mu) = (f\lambda)\mu$. Проверка остальных требований, входящих в определение модуля, столь же тривиальна. Далее, рассмотрим диаграмму



с точной строкой. Определим отображение ρ: $Q \to D$, положив $f\rho = 1f$ для всех $f \in Q$. Если $f, g \in Q$, то

$$(f+g)\rho = 1(f+g) = 1f + 1g = f\rho + g\rho,$$

т. е. ρ — гомоморфизм абелевых групп. Поскольку D делима, то, согласно предложению 3, найдется такой групповой гомоморфизм χ: $R \to D$, что $\iota\chi = \varphi\rho$. Теперь определим отображение ψ: $R \to Q$, положив

$$\xi(\lambda\psi) = (\lambda\xi)\chi$$

для любых $\xi, \lambda \in R$. Поскольку

$$(\xi+\eta)(\lambda\psi) = (\lambda(\xi+\eta))\chi = (\lambda\xi)\chi + (\lambda\eta)\chi = \xi(\lambda\psi) + \eta(\lambda\psi)$$

для любых $\xi, \eta \in R$, то $\lambda\psi$ действительно лежит в Q. Более того, если $\xi, \lambda, \mu \in R$, то

$$\xi((\lambda+\mu)\psi) = ((\lambda+\mu)\xi)\chi = (\lambda\xi)\chi + (\mu\xi)\chi = \\ = \xi(\lambda\psi) + \xi(\mu\psi) = \xi(\lambda\psi + \mu\psi)$$

и, если вспомнить определение произведения $f\mu$ в Q,

$$\xi((\lambda\mu)\psi) = ((\lambda\mu)\xi)\chi = (\lambda(\mu\xi))\chi = (\mu\xi)(\lambda\psi) = \xi((\lambda\psi)\mu).$$

Таким образом, $(\lambda+\mu)\psi = \lambda\psi + \mu\psi$ и $(\lambda\mu)\psi = (\lambda\psi)\mu$, т. е. ψ — гомоморфизм правых R-модулей. Если $\eta \in I$ и $\xi \in R$, то, поскольку $\eta\xi \in I$, имеем

$$\xi(\eta(\iota\psi)) = \xi(\eta\psi) = (\eta\xi)\chi = (\eta\xi)(\iota\chi) =$$
$$= ((\eta\xi)\varphi)\rho = 1((\eta\xi)\varphi) = 1((\eta\varphi)\xi) = (\xi\cdot 1)(\eta\varphi) = \xi\eta\varphi.$$

Следовательно, $\eta(\iota\psi) = \eta\varphi$ для любых $\eta \in I$, т. е. $\iota\psi = \varphi$, что и требовалось.

Лемма 2. *Всякая абелева группа вкладывается в делимую.*

Действительно, любая абелева группа A изоморфна фактор-группе F/K, где F — свободная абелева группа, т. е., по предложению II.3.3, прямая сумма некоторого множества экземпляров группы $\mathbf{Z}$. Ясно, что F можно вложить в делимую группу D, являющуюся прямой суммой такого же множества экземпляров аддитивной группы рациональных чисел, и что D/K — также делимая группа. Остается заметить, что F/K естественным образом вкладывается в D/K.

Вернемся к доказательству теоремы. Если A — произвольный R-модуль, то, рассматривая его как абелеву группу и воспользовавшись леммой 2, найдем гомоморфное вложение абелевой группы A в некоторую делимую абелеву группу D. Лемма 1 позволяет рассмотреть инъективный модуль $Q = \mathrm{Hom}_{\mathbf{Z}}(R, D)$. Если $a \in A$ и $\xi \in R$, то положим

$$\xi(a\iota) = a\xi.$$

Легко видеть, что ι — гомоморфизм R-модуля A в R-модуль Q, ибо

$$\xi((a\lambda)\iota) = (a\lambda)\xi = a(\lambda\xi) = (\lambda\xi)(a\iota) = \xi((a\iota)\lambda)$$

для любого $\lambda \in R$. При этом, если $a\iota = 0$, то

$$a = a1 = 1(a\iota) = 0.$$

Отсюда $a = 0$, т. е. ι оказывается гомоморфным вложением.

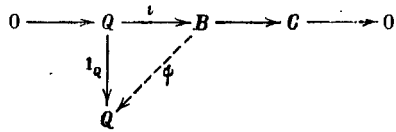
Предложение 4. *Следующие свойства модуля Q эквивалентны:*

(1) *Q инъективен;*

(2) *всякая точная последовательность $0 \longrightarrow Q \longrightarrow B \longrightarrow C \longrightarrow 0$ расщепляема.*

(3) *существует такой инъективный модуль* $\overline{Q}$, *что* $\overline{Q} = Q \oplus H$ *для некоторого подмодуля* $H \subseteq \overline{Q}$.

Доказательство. (1)$\Rightarrow$(2). Согласно (1), диаграмма



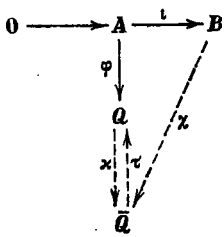
дополняется до коммутативной некоторым гомоморфизмом ψ: $B \to Q$. Следовательно, $\iota\psi = 1_Q$, т. е. справедливо свойство (1) предложения 1.

(2)$\Rightarrow$(3). Поскольку Q вкладывается, по теореме 2, в некоторый инъективный модуль $\overline{Q}$, то возникает точная последовательность

$$0 \to Q \to \overline{Q} \to \overline{Q}/Q \to 0.$$

Согласно предложению 1, $\overline{Q} = Q \oplus H$, что и требовалось.

(3)$\Rightarrow$(1). Пусть $\overline{Q} = Q \oplus H$, где $\overline{Q}$ — инъективный модуль. Естественное вложение Q в $\overline{Q}$ обозначим через $\varkappa$, а естественную проекцию $\overline{Q}$ на Q — через τ. Тогда $\varkappa\tau = 1_Q$. Рассмотрим диаграмму



Поскольку модуль $\overline{Q}$ инъективный, то $\varphi\varkappa = \iota\chi$ для некоторого χ: $B \to \overline{Q}$. Отсюда

$$\iota(\chi\tau) = \varphi\varkappa\tau = \varphi 1_Q = \varphi,$$

что и доказывает инъективность модуля Q.

Теорема 3. *Следующие свойства кольца* R *с единицей эквивалентны:*

(1) *R классически полупростое;*

(2) *все правые идеалы кольца R инъективны как правые R-модули;*

(3) *все правые R-модули инъективны;*

(4) *все правые R-модули проективны.*

Доказательство. (1)$\Rightarrow$(3). Пусть A — произвольный R-модуль. Рассмотрим диаграмму

$$\begin{array}{ccc} 0 \longrightarrow H & \longrightarrow & R \\ & & \downarrow{\scriptstyle \varphi} \\ & & A \end{array}$$

где $0 \longrightarrow H \longrightarrow R$ — точная последовательность. Согласно свойству (5) теоремы 6.2, $H \oplus H' = R$ для некоторого правого идеала H'. Положим $\psi = \pi\varphi$, где π — естественная проекция R на H. Для любого $x \in H$ имеем

$$x\psi = x\pi\varphi = x\varphi,$$

и модуль A инъективен по критерию Бэра (теорема 1).

(3)$\Rightarrow$(4). Достаточно заметить, что, согласно предложению 4, любая точная последовательность

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

расщепляется, каков бы ни был модуль C, и применить предложение 2.

(4)$\Rightarrow$(2). Достаточно заметить, что, каков бы ни был правый идеал H кольца R, по предложению 2 расщепляется всякая точная последовательность

$$0 \longrightarrow H \longrightarrow B \longrightarrow C \longrightarrow 0,$$

и применить предложение 4.

(2)$\Rightarrow$(1). В силу предложения 4, для любого правого идеала H кольца R точная последовательность

$$0 \longrightarrow H \xrightarrow{\iota} R \longrightarrow R/H \longrightarrow 0,$$

где ι — естественное вложение, расщепляется. В силу предложения 1, $H \oplus H' = R$ для некоторого правого идеала H'. Таким образом, R удовлетворяет условию (5) теоремы 6.2.

Поскольку классически полупростое кольцо характеризуется как правыми, так и соответствующими левыми свойствами, то теорема 3 остается справедливой и для левых модулей. Отметим также, что теорема 3 служит примером результата, относящегося к гомологической клас-

сификации колец, ибо в ней устанавливается связь между свойствами кольца и свойствами модулей над ним.

Поскольку каждая абелева группа является модулем над кольцом целых чисел, именно здесь уместна

Теорема 4. *Всякая конечно порожденная абелева группа разлагается в прямую сумму свободной и конечной подгрупп.*

Доказательство. Напомним, что элемент a абелевой группы называется *периодическим*, если $ma=0$ для некоторого натурального m.

Лемма. *Конечно порожденная абелева группа A, не содержащая ненулевых периодических элементов, свободна.*

Действительно, пусть $\{a_1, \ldots, a_n\}$ — наименьшее по количеству элементов подмножество, порождающее группу A. Тогда $A \cong F/H$, где F — свободная абелева группа с базой длины n. Если $H=\{0\}$, то A свободна. Если же $H \neq \{0\}$, то для каждой базы $\mathscr{E}$ группы F, содержащей n элементов, обозначим через $k(\mathscr{E})$ наименьший положительный коэффициент, встречающийся при записи элементов из H в этой базе. Пусть $\mathscr{E}=\{e_1, \ldots, e_n\}$ — база с наименьшим числом $k(\mathscr{E})$. Для некоторого $h \in H$, изменив, если нужно, нумерацию, имеем

$$h = k(\mathscr{E})\, e_1 + k_2 e_2 + \ldots + k_n e_n,$$

где $k_i \in \mathbf{Z}$. Запишем $k_i = k(\mathscr{E})\, q_i + r_i$, где $0 \leqslant r_i < k(\mathscr{E})$. Тогда система

$$\{e_1 + q_2 e_2 + \ldots + q_n e_n,\ e_2,\ \ldots,\ e_n\}$$

также служит базой для F. Однако

$$h = k(\mathscr{E})\,(e_1 + q_2 e_2 + \ldots + q_n e_n) + r_2 e_2 + \ldots + r_n e_n,$$

и если $r_i \neq 0$ для некоторого i, то мы вступаем в противоречие с выбором базы $\mathscr{E}$. Следовательно,

$$h = k(\mathscr{E})\,(e_1 + q_2 e_2 + \ldots + q_n e_n).$$

Если $e_1 + q_2 e_2 + \ldots + q_n e_n \in H$, то, обозначив через π естественный гомоморфизм F на F/H, для любого $a \in A$ при подходящих $l_i \in \mathbf{Z}$ будем иметь

$$a = \pi(l_1 e_1 + l_2 e_2 + \ldots + l_n e_n) = \\ = (l_2 - l_1 q_2)\,\pi(e_2) + \ldots + (l_n - l_1 q_n)\,\pi(e_n).$$

Таким образом, A порождается элементами $\pi(e_2), \ldots, \pi(e_n)$, что противоречит выбору числа n. Следовательно,

$$u = e_1 + q_2 e_2 + \ldots + q_n e_n \notin H,$$

но

$$k(\mathfrak{E})\, u \in H.$$

Таким образом, $\pi(u)$ — ненулевой периодический элемент в A, что невозможно.

Если теперь A — произвольная конечно порожденная абелева группа, то обозначим через T совокупность ее периодических элементов. Нетрудно проверить, что T — подгруппа и что фактор-группа A/T ненулевых периодических элементов не содержит. Из леммы и предложения 2 вытекает, что

$$A \cong T \oplus A/T,$$

причем A/T свободна. Группа T, будучи гомоморфным образом конечно порожденной группы A, конечно порождена. Наконец, нетрудно сообразить, что конечно порожденная периодическая абелева группа конечна.

Напомним, что строение конечных абелевых групп хорошо известно (см., например, ЭА, с. 232).

Упражнения

1. Пусть

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \varphi\downarrow & & \psi\downarrow & & \chi\downarrow & & \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

— коммутативная диаграмма с точными строками. Доказать, что ψ является вложением [наложением], если φ и χ — вложения [наложения].

2. Если R — внешняя прямая сумма двух тел, то каждое из этих тел является проективным, но не свободным правым модулем.

3. Прямая сумма [прямое произведение] проективных [инъективных] модулей проективна [инъективно] (ср. предложения VIII.1.13 и VIII.1.14).

4. Если R — нётерово справа, то прямая сумма любого множества инъективных модулей инъективна.

5. Если все правые идеалы кольца R проективны, то фактор-модуль любого инъективного правого R-модуля инъективен.

6. Всякая проективная абелева группа свободна.

7. Пусть Q — множество всех корней из единицы степеней p^n, где p — фиксированное простое число, а n пробегает все натуральные числа. Доказать, что Q — инъективная абелева группа.

8. В какую инъективную абелеву группу вкладываются группы $\mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/n\mathbf{Z}$?

9. Доказать, что кольца вычетов инъективны как модули над собой.

10. Все базы свободной абелевой группы содержат одно и то же число элементов. То же самое для свободного модуля над произвольным коммутативным кольцом (ср. пример на с. 61).

11. Все ненулевые правые R-модули свободны тогда и только тогда, когда R — тело.

12. Пусть P — проективный правый R-модуль и $\varphi\colon A \longrightarrow B$ — вложение левых R-модулей. Доказать, что отображение $\overline{\varphi}\colon P \otimes_R A \longrightarrow P \otimes_R B$, определяемое равенством $\overline{\varphi}(u \otimes a) = u \otimes \varphi(a)$ для любых $u \in P$ и $a \in A$, является вложением абелевых групп. Получить тот же результат для случая, когда $R = \mathbf{Z}$, а P — произвольная абелева группа, не содержащая ненулевых элементов конечного порядка.

13. Если $A = \dot{\sum\limits_{\iota \in \Im}} A_\iota$ — прямая сумма правых R-модулей, то для любого правого R-модуля B имеет место изоморфизм групп:

$$\operatorname{Hom}_R\left(\dot{\sum_{\iota \in \Im}} A_\iota,\ B\right) \cong \prod_{\iota \in \Im} \operatorname{Hom}_R(A_\iota,\ B).$$

14. Если A — правый R-модуль, а $B = \prod\limits_{\iota \in \Im} B_\iota$ — прямое произведение правых R-модулей, то имеет место изоморфизм абелевых групп:

$$\operatorname{Hom}_R\left(A,\ \prod_{\iota \in \Im} B_\iota\right) \cong \prod_{\iota \in \Im} \operatorname{Hom}_R(A,\ B_\iota).$$

ЛИТЕРАТУРА

Андрунакиевич В. А., Рябухин Ю. М. Радикалы алгебр и структурная теория.— М.: Наука, 1979.

Атья М., Макдональд И. Введение в коммутативную алгебру.— М.: Мир, 1972.

Бовди А. А. Групповые кольца.— Ужгород: Изд-во Ужгородск. ун-та, 1974.

Бокуть Л. А. Ассоциативные кольца. Т.1.— Новосибирск: Изд-во НГУ, 1977; т.II, Новосибирск, Изд-во НГУ, 1981.

Бурбаки Н. Алгебра. Модули, кольца, формы.— М.: Наука, 1966.

Бурбаки Н. Коммутативная алгебра.— М.: Мир, 1971.

Ван дер Варден Б. Л. Алгебра.— М.: Наука, 1979.

Джекобсон Н. Теория колец.— М.: ИЛ, 1947.

Джекобсон Н. Строение колец.— М.: ИЛ, 1961.

Дрозд Ю. А., Кириченко В. В. Конечномерные алгебры.— Кнев: Вища школа, 1980.

Залесский А. Е., Михалев А. В. Групповые кольца.— В кн.: Итоги науки и техники. Современные проблемы математики.— М.: Изд-во ВИНИТИ, 1973, Т.2, с. 5—118.

Зарисский О., Самюэль Н. Коммутативная алгебра. Т.1, 2.— М.: ИЛ, 1963.

Калужнин Л. А. Введение в общую алгебру.— М.: Наука, 1973.

Картан А., Эйленберг С. Гомологическая алгебра.— М.: ИЛ, 1960.

Кириченко В. В. Кольца и модули.— Киев: Изд-во Киевск. ун-та, 1981.

Каш Ф. Модули и кольца.— М.: Мир, 1981.

Кон П. Свободные кольца и их связи.— М.: Мир, 1975.

Курош А. Г. Лекции по общей алгебре.— М.: Наука, 1973.

Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр.— М.: Наука, 1969.

Ламбек И. Кольца и модули.— М.: Мир, 1971.
Ленг С. Алгебра.— М.: Мир, 1968.
Маклейн С. Гомология.— М.: Мир, 1966.
Мишина А. П., Скорняков Л. А. Абелевы группы и модули.— М.: Наука, 1969.
Скорняков Л. А. Дедекиндовы структуры с дополнениями и регулярные кольца.— М.: Физматгиз, 1961.
Фейс К., Алгебра: кольца, модули и категории. Т.I.— М.: Мир, 1977; Т.II.— М.: Мир, 1979.
Фукс Л. Бесконечные абелевы группы. Т.I.— М.: Мир, 1974; Т.II.— М.: Мир, 1977.
Херстейн И. Некоммутативные кольца.— М.: Мир, 1972.
Brandal W. Commutative rings whose finitely generated modules decompose.— Berlin; Heidelberg; N. Y.: Springer-Verlag, 1979 (Lect. Notes Math., v. 723).
Chatters A. W., Hajarnavis C. R. Rings with chain conditions.— Boston: London; Melbourne: Pitman, 1980.
Cozzens J., Faith C. Simple Noetherian rings.— Cambridge: Cambridge Univ. Press, 1975.
Dicks W. Groups, trees and projective modules.— Berlin; Heidelberg; N. Y.: Springer-Verlag, 1980 (Lect. Notes Math., v. 790).
Goodearl K. R. Von Neumann regular rings.— London; San Francisco; Melburn: Pitman, 1979.
Herstein I. N. Rings with involution.— Chicago; London: Chicago Univ. Press, 1976.
Jategaonkar A. V. Left principal ideal rings.— Berlin; Heidelberg; N. Y.: Springer-Verlag, 1970 (Lect. Notes Math.; v. 123).
Lam T. Y. Serre's conjecture.— Berlin; Heidelberg; N. Y.: Springer-Verlag, 1978 (Lect. Notes Math., v. 635).
Montgomery S. Fixed rings of finite automorphism group of associative rings.— Berlin; Heidelberg; N. Y.: Springer-Verlag, 1980 (Lect. Notes Math., v. 818).
von Neumann J. Continuous geometry.— New Jersey: Princenton, 1960.
Passman D. S. The algebraic structure of group rings.— N. Y.: Wiley-Interscionce, 1977.
Stenström B. Rings of quotients. An introduction to methods of ring theory.— Berlin: Springer-Verlag, 1975.

Литературу по топологическим и упорядоченным кольцам см. в гл. VII, а по кольцам Ли и другим неассоциативным кольцам — в гл. V.

ГЛАВА V

ГРУППЫ И АЛГЕБРЫ ЛИ

Объединение в одной главе, казалось бы, совсем разных алгебраических систем не случайно. В конце главы устанавливается очень тесная связь между нильпотентными группами и нильпотентными алгебрами Ли. Кроме того, доказываются теорема о подгруппах свободной группы, теорема о строении конечных нильпотентных групп, теорема об одновременном приведении всех матриц разрешимой линейной группы к треугольному виду и теорема о представлении алгебр Ли как ассоциативных алгебр с операцией коммутирования.

§ 1. Подгруппы свободной группы

Описание строения свободной группы было дано в гл. II.

Теорема 1. *Неодноэлементная подгруппа свободной группы свободна.*

Замечание. Этот результат носит в некотором смысле исключительный характер, так как для большинства алгебраических систем аналогичное утверждение места не имеет. Среди других исключений: группоиды, неассоциативные кольца и алгебры Ли.

Доказательство. Пусть F — свободная группа со свободной порождающей системой X и H — ее неодноэлементная подгруппа. Напомним, что элементами группы F служат редуцированные слова в алфавите $X \cup X^{-1}$, т. е. слова, в которых x и x^{-1} не стоят рядом ни для какого $x \in X \cup X^{-1}$. При этом два таких слова равны тогда и только тогда, когда они имеют одинаковую запись, т. е. состоят из одних и тех же букв, записанных в одном и том же порядке.

Лемма 1. *Группа F содержит подмножество W редуцированных слов, обладающее следующими свойствами:* (а) $1 \in W$; (б) *каждый правый смежный класс по подгруппе H содержит в точности один элемент из W;* (в) *если $w \in W$, то W содержит все начальные отрезки слова w.*

Для доказательства положим $W_0=\{1\}$ и допустим, что построена возрастающая цепочка $W_0 \subseteq W_1 \subseteq \ldots \subseteq W_{n-1}$ подмножеств из F с соблюдением следующих свойств: ($а_i$) $1 \in W_i$; ($б_i$) каждый правый смежный класс по подгруппе H, содержащий редуцированное слово длины, не превосходящей i, содержит в точности один элемент из W_i; ($в_i$) если $w \in W_i$, то w — редуцированное слово, и W_i содержит все его начальные отрезки. Пусть, далее, $\mathfrak{R}$ — множество всех правых смежных классов по подгруппе H, содержащих редуцированные слова длины n, но не содержащих слов меньшей длины. Если $K \in \mathfrak{R}$, то $K=Hv$, где v — редуцированное слово длины n. Если $v=v'x$, где $x \in X \cup X^{-1}$ и v' — начальный отрезок слова v, то, согласно ($б_{n-1}$), $Hv'=Hw$, где $w \in W_{n-1}$. Положим $w_K=wx$. Слово w_K редуцированное, ибо в противном случае оно как элемент группы F равно слову u длины, меньшей, чем n. Но тогда $K=Hv'x=Hw_K=Hu$, что противоречит выбору смежного класса K. Положив

$$W_n=W_{n-1} \cup \{w_K \mid K \in \mathfrak{R}\},$$

нетрудно убедиться в справедливости свойств ($а_n$), ($б_n$) и ($в_n$). Ясно, что множество $W=\bigcup\limits_{1 \leqslant i < \infty} W_i$ обладает нужными свойствами.

Если теперь $w \in W$ и $x \in X \cup X^{-1}$, то, по свойству (б),

$$\{v\}=W \cap Hwx.$$

Положим

$$h_{w,x}=wxv^{-1}.$$

Поскольку $wx=hv$ для некоторого $h \in H$, то

$$h_{w,x}=h \in H. \qquad (*)$$

Лемма 2. *Множество*

$$\Xi=\{h_{w,x} \mid w \in W,\ x \in X,\ h_{w,x} \neq 1\}$$

порождает H.

Действительно, пусть $h \in H$ и

$$h=x_1 \ldots x_n$$

— его запись в виде редуцированного слова в алфавите $X \cup X^{-1}$. Положим (здесь мы не различаем одноэлемент-

ное множество и образующий его элемент)

$$v_1 = W \cap Hx_1,$$
$$v_2 = W \cap Hv_1x_2,$$
$$v_3 = W \cap Hv_2x_3,$$
$$\dots\dots\dots\dots$$
$$v_n = W \cap Hv_{n-1}x_n.$$

Тогда

$$h_{1,\,x_1}h_{v_1,\,x_2}\dots h_{v_{n-1}x_n} =$$
$$= x_1v_1^{-1}v_1x_2v_2^{-1}v_2x_3v_3^{-1}\dots v_{n-1}x_nv_n^{-1} = x_1x_2\dots x_nv_n^{-1} = hv_n^{-1}.$$

Ввиду (*), отсюда следует, что

$$v_n = h_{v_{n-1}x_n}^{-1}\dots h_{1,\,x_1}^{-1}h \in H.$$

Но тогда, в силу свойств (а) и (б) из леммы 1,

$$v_n = W \cap H = 1$$

и, следовательно,

$$h = h_{1,\,x_1}\dots h_{v_{n-1},\,x_n}.$$

Лемма 3. *Если* $h_{w,\,x} \neq 1$, *то слово* wxv^{-1} *редуцированное.*

Действительно, поскольку w и v — редуцированные слова, то сокращение в слове wxv^{-1} возможно лишь в случаях, когда $w = w'x^{-1}$ или $v = v'x$. В первом случае, в силу леммы 1 (в), имеем $w' \in W$. Поскольку $v \in W$ и $v = h^{-1}wx = h^{-1}w'$, где $h \in H$, то, учитывая лемму 1 (б), получаем $v = w'$. Таким образом,

$$h_{w,\,x} = wxv^{-1} = w'v^{-1} = 1,$$

вопреки условию. Во втором случае, по лемме 1 (в), $v' \in W$. Из равенства $v'x = v = h^{-1}wx$, где $h \in H$, получаем $v' = h^{-1}w$, что, как и выше, влечет $v' = w$. Отсюда

$$h_{w,\,x} = wxv^{-1} = v'xv^{-1} = vv^{-1} = 1,$$

что противоречит условию.

Лемма 4. *Если* w_1, w_2, v_1, $v_2 \in W$, x_1, $x_2 \in X \cup X^{-1}$, h_1, $h_2 \in H$, $h_1w_1x_1 = v_1$, $h_2w_2x_2 = v_2$, $u_1 = w_1x_1v_1^{-1} \neq 1$, $u_2 = w_2x_2v_2^{-1} \neq 1$, u_1 *и* u_2 *редуцированы и редуцированное слово, возникающее из слова* $x_1v_1^{-1}w_2x_2$, *не содержит* x_1 *или* x_2, *то* $w_1 = v_2$, $x_1 = x_2^{-1}$ *и* $v_1 = w_2$.

Для доказательства сначала допустим, что при осуществлении редукций в слове $x_1v_1^{-1}w_2x_2$ буква x_1 исчезает не позже, чем x_2. Поскольку u_1, а значит, и $x_1v_1^{-1}$ редуцированы, то перед этим должно исчезнуть v_1^{-1}. Следовательно, или $w_2=v_1$ и $x_2=x_1^{-1}$, или же w_2 имеет редуцированную запись $w_2=v_1x_1^{-1}w'$. В первом случае, используя условие леммы, получаем

$$h_1w_1=v_1x_1^{-1}=w_2x_2=h_2^{-1}v_2,$$

откуда $w_1=v_2$, ввиду леммы 1 (б). Во втором случае, согласно лемме 1 (в), имеем $v_1x_1^{-1}\in W$. С другой стороны, $h_1w_1=v_1x_1^{-1}$, и, согласно лемме 1.(б), $w_1=v_1x_1^{-1}$, что, вопреки условию, влечет $u_1=1$. Допустим теперь, что буква x_2 исчезает раньше буквы x_1. Тогда, учитывая редуцированность слова u_2, а, значит, и слова w_2x_2, получаем, что v_1^{-1} имеет редуцированную запись $v_1^{-1}=v'x_2^{-1}w_2^{-1}$. Следовательно, v_1 имеет редуцированную запись $v_1=w_2x_2v'^{-1}$. Ввиду (в), $h_2^{-1}v_2=w_2x_2\in W$, откуда, согласно (б), $w_2x_2=v_2$ и, следовательно, $w_2x_2v_2^{-1}=1$, вопреки условию.

Лемма 5. *Если* $h_{w_i,\,x_i}\in\Xi$ *для* $i=1,\ \ldots,\ n$, $\varepsilon_i=\pm1$ *и*

$$h_{w_1,\,x_1}^{\varepsilon_1}\ldots h_{w_n,\,x_n}^{\varepsilon_n}=1,$$

то $h_{w_i,\,x_i}=h_{w_{i+1},\,x_{i+1}}$ *и* $\varepsilon_i=-\varepsilon_{i+1}$ *для некоторого* i.

Для доказательства положим:

$$\bar{w}_i=\begin{cases}w_i, & \text{если } \varepsilon_i=1,\\ v_i, & \text{если } \varepsilon_i=-1,\end{cases}\qquad \bar{v}_i=\begin{cases}v_i, & \text{если } \varepsilon_i=1,\\ w_i, & \text{если } \varepsilon_i=-1,\end{cases}$$

$$\bar{x}_i=\begin{cases}x_i, & \text{если } \varepsilon_i=1,\\ x_i^{-1}, & \text{если } \varepsilon_i=-1.\end{cases}$$

По условию, после осуществления ряда редукций все буквы слова

$$s=\bar{w}_1\bar{x}_1\bar{v}_1^{-1}\ldots\bar{w}_n\bar{x}_n\bar{v}_n^{-1}$$

исчезают. Ввиду леммы 3, эти редукции должны начинаться с редукций одного из слов

$$\bar{w}_i\bar{x}_i\bar{v}_i^{-1}\bar{w}_{i+1}\bar{x}_{i+1}\bar{v}_{i+1}^{-1},$$

в результате которых должна исчезнуть буква $\bar{x}_i$ или $\bar{x}_{i+1}$. Но тогда из лемм 3 и 4 вытекает, что $\bar{w}_i=\bar{v}_{i+1}$, $\bar{x}_i=\bar{x}_{i+1}^{-1}$ и

$\bar{v}_i = \bar{w}_{i+1}$. Поскольку $x_i,\ x_{i+1} \in X$, это, в свою очередь, влечет $\varepsilon_i = -\varepsilon_{i+1}$ и $h_{w_i, x_i} = h_{w_{i+1}, x_{i+1}}$.

Возвращаясь к доказательству теоремы, обозначим через Y некоторое множество, равномощное Ξ, и пусть $\varphi\colon Y \to \Xi$ — взаимно однозначное отображение. Если теперь G — свободная группа со свободной порождающей системой Y, то φ может быть продолжено до гомоморфизма ψ группы G в группу H. Ввиду леммы 2, ψ — гомоморфное наложение. Если

$$\psi(y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n}) = 1$$

для некоторого редуцированного слова $s = y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n}$ из G, то

$$\psi(y_1)^{\varepsilon_1} \dots \psi(y_n)^{\varepsilon_n} = 1.$$

Поскольку $\psi(y_i) \in \Xi$, то, согласно лемме 5, $\psi(y_i) = \psi(y_{i+1})$ и $\varepsilon_i = -\varepsilon_{i+1}$ для некоторого i. Отсюда $y_i = y_{i+1}$, что противоречит редуцированности слова $y_1^{\varepsilon_1} \dots y_n^{\varepsilon_n}$.

Упражнения

1. Вывести из теоремы 1 аналогичную теорему для абелевых групп (ср. упр. 6 из гл. IV).

2. Пусть F — свободная группа со свободной порождающей системой $\{x, y\}$. Доказать, что множество $\{x^n y x^n \mid n = 1, 2, \dots\}$ является свободной порождающей системой для порождаемой им подгруппы.

3. Указать систему свободных порождающих для подгруппы свободной группы, состоящей из всех редуцированных слов четной длины.

4. Тот же вопрос для коммутанта свободной группы.

5. Подгруппа свободной группы с бесконечной системой свободных порождающих, имеющая конечный индекс, не может быть конечно порождена.

§ 2. Нильпотентные группы

Если a и b — элементы группы G, то элемент

$$[a, b] = a^{-1}b^{-1}ab$$

называется *коммутатором*. По индукции определяется *длинный коммутатор*

$$[a_1, \dots, a_n] = [[a_1, \dots, a_{n-1}], a_n].$$

Предложение 1. *Если a, b, c и g — элементы группы G, то*:

(а) $[a, b]^{-1} = [b, a]$;

(б) $[ab, c] = [a, c][a, c, b][b, c]$;

(в) $[a, bc] = [a, c][a, b][a, b, c]$;

(г) $g^{-1}[a, b]g = [g^{-1}ag, g^{-1}bg]$;

(д) $[a, b, c^a][c, a, b^c][b, c, a^b] = 1$,

где $x^g = g^{-1}xg$.

Доказательство. (а) Имеем

$$[a, b][b, a] = a^{-1}b^{-1}abb^{-1}a^{-1}ba = 1.$$

(б) Запишем

$$[a, c][a, c, b][b, c] = [a, c][a, c]^{-1}b^{-1}[a, c]bb^{-1}c^{-1}bc = \\ = b^{-1}a^{-1}c^{-1}acc^{-1}bc = (ab)^{-1}c^{-1}(ab)c = [ab, c].$$

(в) Имеем

$$[a, c][a, b][a, b, c] = a^{-1}c^{-1}ac[a, b][a, b]^{-1}c^{-1}[a, b]c = \\ = a^{-1}c^{-1}aa^{-1}b^{-1}abc = a^{-1}(bc)^{-1}a(bc) = [a, bc].$$

(г) Замечаем, что

$$g^{-1}[a, b]g = g^{-1}a^{-1}gg^{-1}b^{-1}gg^{-1}agg^{-1}bg = [g^{-1}ag, g^{-1}bg].$$

(д) Учитывая (а), запишем

$$[a, b, c^a][c, a, b^c][b, c, a^b] = \\ = b^{-1}a^{-1}baa^{-1}c^{-1}aa^{-1}b^{-1}aba^{-1}ca \cdot \\ \cdot a^{-1}c^{-1}acc^{-1}b^{-1}cc^{-1}a^{-1}cac^{-1}bc \cdot \\ \cdot c^{-1}b^{-1}cbb^{-1}a^{-1}bb^{-1}c^{-1}bcb^{-1}ab = 1.$$

Если H и K — нормальные подгруппы группы G, то множество всевозможных произведений коммутаторов вида $[x, y]$, где или $x \in H$ и $y \in K$, или $x \in K$ и $y \in H$, называется *взаимным коммутантом* подгрупп H и K и обозначается через $[H, K]$. Множество $G' = [G, G]$ называется *коммутантом* группы G.

Предложение 2. *Если H и K — нормальные подгруппы группы G, то взаимный коммутант $[H, K]$ — нормальная подгруппа в G и $[H, K] \subseteq H \cap K$. В частности, коммутант группы G является ее нормальной подгруппой.*

Доказательство. Из предложения 1 (а) вытекает, что взаимный коммутант является подгруппой. Ее нормальность легко получить, воспользовавшись предложе-

нием 1(г). Если $x \in H$ и $y \in K$, то $[x, y] = x^{-1}y^{-1}xy \in H$, ибо x^{-1}, $y^{-1}xy \in H$. Следовательно, $[H, K] \subseteq H$. Аналогично проверяется, что $[H, K] \subseteq K$.

Если G — группа, то положим $G_1 = G$ и по индукции определим

$$G_{i+1} = [G_i, G].$$

В силу предложения 2, все G_i — нормальные подгруппы в G.

Предложение 3. $[G_i, G_j] \subseteq G_{i+j}$.

Доказательство. При $j = 1$ нужное включение вытекает из определения. Если $j \geqslant 2$, $x \in G_i$, $y \in G_{j-1}$ и $z \in G$, то, полагая $u = yxy^{-1}$ и используя индуктивное предположение и предложения 1(а), 1(д) и 2, получим

$$[x, [y, z]] = [[y, z], u^y]^{-1} = [y, z, u^y]^{-1} = [u, y, z^u][z, u, y^z] \in [[G_i, G_{j-1}], G][[G, G_i], G_{j-1}] \subseteq G_{i+(j-1)+1} \cdot G_{(i+1)+(j-1)} = G_{i+j}.$$

Пусть снова G — группа. Через $\mathfrak{Z}_1(G)$ обозначим ее центр, а через $\mathfrak{Z}_{i+1}(G)$ — полный прообраз центра факторгруппы $G/\mathfrak{Z}_i(G)$. Кроме того, пусть $\mathfrak{Z}_0(G) = \{1\}$.

Предложение 4. (а) $\mathfrak{Z}_i(G/\mathfrak{Z}_1(G)) = \mathfrak{Z}_{i+1}(G)/\mathfrak{Z}_1(G)$; (б) *если* $g \in \mathfrak{Z}_2(G)$, *то* $[x, g^k] = [x, g]^k$ *для любого* $x \in G$ *и любого натурального* k; (в) *если* $z^m = 1$ *для всех* $z \in \mathfrak{Z}_1(G)$, *то* $g^m \in \mathfrak{Z}_i(G)$ *для всех* $g \in \mathfrak{Z}_{i+1}(G)$ *при любом* i.

Доказательство. (а) Для $i \leqslant 1$ это ясно. Если $i \geqslant 2$, то положим $\bar{G} = G/\mathfrak{Z}_1(G)$ и условимся обозначать через $\bar{x}$ смежный класс в фактор-группе $\bar{G}$, содержащий элемент $x \in G$. Если $x \in \mathfrak{Z}_{i+1}(G)$, то, по определению, смежный класс $x\mathfrak{Z}_i(G)$ лежит в $\mathfrak{Z}_1(G/\mathfrak{Z}_i(G))$. Следовательно, $[x, g] \in \mathfrak{Z}_i(G)$ для любого $g \in G$. В силу индуктивного предположения

$$[\bar{x}, \bar{g}] \in \mathfrak{Z}_i(G)/\mathfrak{Z}_1(G) = \mathfrak{Z}_{i-1}(\bar{G}).$$

Таким образом, смежный класс $\bar{x}\mathfrak{Z}_{i-1}(\bar{G})$ лежит в $\mathfrak{Z}_1(\bar{G}/\mathfrak{Z}_{i-1}(\bar{G}))$, т. е. $\bar{x} \in \mathfrak{Z}_i(\bar{G})$. Следовательно,

$$\mathfrak{Z}_{i+1}(G)/\mathfrak{Z}_1(G) \subseteq \mathfrak{Z}_i(\bar{G}).$$

Допустим теперь, что $\bar{x} \in \mathfrak{Z}_i(\bar{G})$. В силу индуктивного предположения, для любого $g \in G$ имеем

$$[\bar{x}, \bar{g}] \in \mathfrak{Z}_{i-1}(\bar{G}) = \mathfrak{Z}_i(G)/\mathfrak{Z}_1(G).$$

Отсюда $[x, g] \in \mathfrak{Z}_i(G)$ и, следовательно, смежный класс $x\mathfrak{Z}_i(G)$ лежит в $\mathfrak{Z}_1(G/\mathfrak{Z}_i(G))$. Таким образом, $x \in \mathfrak{Z}_{i+1}(G)$, а значит, $\bar{x} \in \mathfrak{Z}_{i+1}(\bar{G})$. Тем самым доказано, что $\mathfrak{Z}_i(\bar{G}) \subseteq \mathfrak{Z}_{i+1}(G)/\mathfrak{Z}_1(G)$.

(б) При $k = 1$ нужное равенство тривиально. Если $k \geqslant 2$, то заметим, что $g \in \mathfrak{Z}_2(G)$ влечет $[x, g] \in \mathfrak{Z}_1(G)$ и, следовательно, $[x, g, y] = 1$ для любых $x, y \in G$. Используя этот результат, предложение 1(в) и индуктивное предположение, получаем

$$[x, g^k] = [x, g^{k-1}][x, g][x, g, g^{k-1}] = \\ = [x, g]^{k-1}[x, g] = [x, g]^k.$$

(в) Если $g \in \mathfrak{Z}_1(G)$, то, по условию, $g^m = 1 \in \mathfrak{Z}_0(G)$, т. е. при $i = 0$ утверждение (в) справедливо. Допустим теперь, что $g \in \mathfrak{Z}_{i+1}(G)$, где $i \geqslant 1$, и что $\bar{x}$ имеет тот же смысл, что и в доказательстве части (а). Согласно (а), $\bar{g} \in \mathfrak{Z}_i(\bar{G})$ и, в силу индуктивного предположения,

$$\bar{g}^m \in \mathfrak{Z}_{i-1}(\bar{G}) = \mathfrak{Z}_i(G)/\mathfrak{Z}_1(G),$$

откуда $g^m \in \mathfrak{Z}_i(G)$.

Говорят, что группа G *обладает нижним* [*верхним*] *центральным рядом длины* n, если $G_{n+1} = \{1\}$ [$\mathfrak{Z}_n(G) = G$].

Теорема 1. *Следующие свойства группы* G *эквивалентны*;

(1) $[g_1, \ldots, g_{n+1}] = 1$ *для любых* $g_1, \ldots, g_{n+1} \in G$;

(2) G *обладает нижним центральным рядом длины* n;

(3) G *обладает верхним центральным рядом длины* n.

Доказательство. (1)$\Rightarrow$(2). Простая индукция показывает, что каждый элемент из G_{n+1} представляется как произведение коммутаторов длины $n+1$.

(2)$\Rightarrow$(1). Достаточно заметить, что, согласно предложению 3, $[\underbrace{G, \ldots, G}_{n+1 \text{ раз}}] = G_{n+1} = \{1\}$.

(1)$\Rightarrow$(3). Для $n = 1$ очевидно. Если $n \geqslant 2$, то $[g_1, \ldots, g_n] \in \mathfrak{Z}_1(G)$ для любых $g_1, \ldots, g_n \in G$. Применив предложение 4(а) и индуктивное предположение, получаем

$$G/\mathfrak{Z}_1(G) = \mathfrak{Z}_{n-1}(G/\mathfrak{Z}_1(G)) = \mathfrak{Z}_n(G)/\mathfrak{Z}_1(G),$$

откуда $G = \mathfrak{Z}_n(G)$.

(3)$\Rightarrow$(1). Для $n = 1$ очевидно. Если $n \geqslant 2$, то, ввиду предложения 4(а), имеем

$$\mathfrak{Z}_{n-1}(G/\mathfrak{Z}_1(G)) = \mathfrak{Z}_n(G)/\mathfrak{Z}_1(G) = G/\mathfrak{Z}_1(G).$$

В силу индуктивного предположения, $[g_1, \ldots, g_n] \in \mathfrak{Z}_1(G)$ для любых $g_1, \ldots, g_n \in G$, откуда $[g_1, \ldots, g_n, g_{n+1}] = 1$ для любого $g_{n+1} \in G$.

Группа, обладающая одним из свойств (1)—(3) теоремы 1, называется *нильпотентной группой ступени n*. Ясно, что нильпотентная группа ступени n является нильпотентной группой любой большей ступени. В частности, абелева группа оказывается нильпотентной группой ступени n для любого $n \geqslant 2$.

Предложение 5. *Если ассоциативное кольцо R с единицей 1 содержит нильпотентное подкольцо S степени n* (т. е. $s_1 \ldots s_n = 0$ для любых $s_1, \ldots, s_n \in S$), *то множество G всех элементов вида $1+s$, где $s \in S$, образует нильпотентную группу ступени n.*

Доказательство. Равенство

$$(1+s)(1-s+s^2-\ldots+(-1)^{n-1}s^{n-1}) = 1,$$

где $s \in S$, показывает, что G — действительно группа. Отсюда же следует, что если $s \in S^k$ (т. е. s представляется как целочисленная линейная комбинация k-элементных произведений элементов из S), то

$$(1+s)^{-1} = 1-s+u,$$

где $u \in S^{2k}$. Поэтому, если $s \in S^k$ и $t \in S$, то

$$\begin{aligned}[1+s,\ 1+t] &= (1-s+u)(1+t)^{-1}(1+s)(1+t) = \\ &= (1-s+u)(1+(1+t)^{-1}s(1+t)) = \\ &= (1-s+u)(1+(1-t+v)s(1+t)) = \\ &= (1-s+u)(1+s-ts+vs+st-tst+vst),\end{aligned}$$

где $v \in S^2$. Ясно, что

$$w = -ts+vs+st-tst+vst \in S^{k+1},$$

и, следовательно,

$$\begin{aligned}[1+s,\ 1+t] &= (1-s+u)(1+s+w) = \\ &= 1-s^2+(1-s)w+u(1+s+w).\end{aligned}$$

Таким образом,

$$[1+s,\ 1+t] = 1+r,$$

где

$$r = -s^2+(1-s)w+u(1+s+w) \in S^{k+1}.$$

Отсюда, используя индукцию, нетрудно вывести, что

$$[1+s_1, \ldots, 1+s_n] \in 1+S^n = \{1\}$$

для любых $s_1, \ldots, s_n \in S$, а это и требовалось.

Пример. Пусть R — кольцо всех нижних треугольных матриц (т. е. матриц, у которых над главной диагональю стоят только нули) над некоторым полем. Нетрудно проверить, что матрицы из R, у которых главная диагональ заполнена нулями, образуют нильпотентное подкольцо (даже идеал). В силу предложения 5, матрицы из R, у которых главная диагональ заполнена единицами, образуют нильпотентную группу ступени n.

Если H — подгруппа группы G, то множество

$$C(H) = \{x \mid x \in G,\ xh = hx \text{ для всех } h \in H\}$$

называется *централизатором подгруппы* H в группе G. Нетрудно проверить, что $C(H)$ — подгруппа в G.

Предложение 6. *Пусть H — нормальная подгруппа группы G. Тогда*: (а) *$C(H)$ — нормальная подгруппа в G*; (б) *$\mathfrak{Z}_1(H)$ — нормальная подгруппа в G*; (в) *если H конечна, то $C(H)$ имеет конечный индекс в G*; (г) *если G нильпотентна, а H — максимальная абелева нормальная подгруппа в G, то $C(H) = H$.*

Доказательство. (а) Если $h \in H$, $c \in C(H)$ и $g \in G$, то $ghg^{-1} \in H$. Отсюда

$$hg^{-1}cg = g^{-1}ghg^{-1}cg = g^{-1}cghg^{-1}g = g^{-1}cgh,$$

т. е. $g^{-1}cg \in C(H)$.

(б) Достаточно заметить, что $\mathfrak{Z}_1(H) = H \cap C(H)$, и применить (а).

(в) Пусть $H = \{h_1, \ldots, h_m\}$, $\bar{H} = \underbrace{H \times \ldots \times H}_{m \text{ раз}}$ и $C = C(H)$.

Определим отображение φ: $G/C \longrightarrow \bar{H}$, положив

$$\varphi(Cg) = (g^{-1}h_1g, \ldots, g^{-1}h_mg).$$

Определение это корректно, ибо $Cg_1 = Cg_2$ влечет $g_1g_2^{-1} \in C$, откуда

$$g_1^{-1}h_ig_1 = g_1^{-1}h_ig_1g_2^{-1}g_2 = g_1^{-1}g_1g_2^{-1}h_ig_2 = g_2^{-1}h_ig_2$$

для всех i. Если $\varphi(Cg_1) = \varphi(Cg_2)$, то $g_1^{-1}h_ig_1 = g_2^{-1}h_ig_2$ для любого i. Отсюда $g_2g_1^{-1}h_i = h_ig_2g_1^{-1}$ для всех i, т. е.

$g_2g_1^{-1} \in C$, а значит, $Cg_1 = Cg_2$. Следовательно, φ — вложение, откуда $|G/C| \leqslant |\bar{H}| = m^m$.

(г) Ясно, что $H \subseteq C(H)$. Обозначим $C(0) = C(H)$ и, по индукции, $C(i+1) = [C(i), G]$. Если $C(0) \neq H$, то, ввиду нильпотентности группы G, найдется такой номер i, что $C(i) \not\subseteq H$, но $C(i+1) \subseteq H$. Если $x \in C(i) \setminus H$, то множество $H \cup \{x\}$ порождает абелеву подгруппу $\bar{H}$, ибо $x \in C(i) \subseteq C(H)$, в силу предложения 2. Если $a \in \bar{H}$, то $a = x^k h$, где $h \in H$. Тогда для любого $g \in G$ имеем

$$g^{-1}ag = g^{-1}x^k hg = x^k x^{-k} g^{-1} x^k g g^{-1} hg = \\ = x^k [x^k, g]\, g^{-1}hg \in x^k H = \bar{H}.$$

Следовательно, $\bar{H}$ оказывается абелевой нормальной подгруппой в G, что противоречит выбору H.

Если H — подгруппа группы G, то множество

$$N(H) = \{x \mid x \in G,\ xH = Hx\}$$

называется *нормализатором* подгруппы H в группе G. Нетрудно проверить, что $N(H)$ — подгруппа в G и что H — нормальная подгруппа в $N(H)$.

Предложение 7. *Если H — подгруппа нильпотентной группы G ступени n и $N(H) = H$, то $H = G$.*

Доказательство. По теореме 1, $\mathfrak{Z}_n(G) = G$. Если $H \neq G$, то для некоторого номера i имеем $\mathfrak{Z}_i(G) \subseteq H$, но $\mathfrak{Z}_{i+1}(G) \not\subseteq H$. Если $z \in \mathfrak{Z}_{i+1}(G) \setminus H$, то

$$hz\mathfrak{Z}_i(G) = zh\mathfrak{Z}_i(G) = \mathfrak{Z}_i(G)\, zh = \mathfrak{Z}_i(G)\, hz$$

для любого $h \in H$. Отсюда $zh = xhz$ и $hz = zhy$ для некоторых x, $y \in \mathfrak{Z}_i(G) \subseteq H$. Следовательно, $zH = Hz$, откуда $z \in N(H) = H$, вопреки выбору z.

Напомним, что *p-группой*, где p — простое число, называется группа, все элементы которой имеют порядок, равный какой-либо степени числа p.

Предложение 8. *Конечная p-группа G нильпотентна.*

Доказательство. Убедимся сначала, что $|G| = p^m$ для некоторого m. Действительно, если q — простое число, входящее в разложение числа $|G|$, то по первой теореме Силова (ЭА, с. 214, теорема IV.2.3), G содержит подгруппу порядка q и, следовательно, $q = p$. Далее, если $m = 1$, то G коммутативна и, следовательно, нильпотентна. Пусть $m \geqslant 2$. Для каждого $g \in G$ обозначим через $K(g)$ его класс сопряженности. Напомним, что $|K(g)| = 1$ в том

и только в том случае, когда $g \in \mathfrak{Z}_1(G)$. Представив G в виде объединения классов сопряженности (см. ЭА, с. 88, теорема II.3.21), получим

$$p^m = |\mathfrak{Z}_1(G)| + |K(g_1)| + \ldots + |K(g_t)|,$$

где $|K(g_i)| \neq 1$. Но все числа $|K(g_i)|$ делятся на p (см. ЭА, с. 213, теорема IV.2.1) и, следовательно, $|\mathfrak{Z}_1(G)| = p^k$, где $1 \leqslant k \leqslant m$. По индуктивному предположению, группа $G/\mathfrak{Z}_1(G)$ нильпотентна. Ввиду теоремы 1 и предложения 4(а), для некоторого натурального n имеем

$$\mathfrak{Z}_{n+1}(G)/\mathfrak{Z}_1(G) = \mathfrak{Z}_n(G/\mathfrak{Z}_1(G)) = G/\mathfrak{Z}_1(G).$$

Отсюда $\mathfrak{Z}_{n+1}(G) = G$, и нильпотентность группы G вытекает из теоремы 1.

Теорема 2. *Конечная группа G нильпотентна тогда и только тогда, когда она изоморфна прямому произведению p-групп* (по различным p).

Доказательство. Достаточность легко получить, используя предложение 8 и свойство (1) из теоремы 1. Допустим теперь, что G — нильпотентная группа и

$$|G| = p_1^{k_1} \ldots p_m^{k_m},$$

где p_i — различные простые числа. По теореме Силова (ЭА, с. 214, теорема IV.2.3) для каждого i группа G содержит подгруппу P_i порядка $p_i^{k_i}$.

Лемма 1. *P_i — нормальная подгруппа группы G.*

Действительно, если $x \in N(N(P_i))$, то

$$x^{-1}P_i x \subseteq x^{-1}N(P_i)\,x = N(P_i)$$

и $|x^{-1}P_i x| = p^{k_i}$. Таким образом, P_i и $x^{-1}P_i x$ — это две максимальные p_i-подгруппы группы $N(P_i)$ (т. е. ее силовские p_i-подгруппы). По второй теореме Силова (Кострикин А. И. Введение в алгебру. — М.: Наука, 1977, с. 333, теорема 2), $P_i = y^{-1}x^{-1}P_i xy$ для некоторого $y \in N(P_i)$. Следовательно, $xy \in N(P_i)$, откуда $x \in N(P_i)$, а значит, $N(N(P_i)) = N(P_i)$. По предложению 7, $N(P_i) = G$, что и означает нормальность подгруппы P_i в G.

Лемма 2. *Для каждого i*

$$P_i \cap (P_1 \ldots P_{i-1}P_{i+1} \ldots P_m) = \{1\}.$$

Для доказательства выберем x, принадлежащий указанному в формулировке пересечению, и положим

$r=|G|/p_i^{k_i}$. Тогда $x^{p_i^{k_i}}=1=x^r$. Но $up_i^{k_i}+vr=1$ для некоторых целых u и v. Поэтому

$$x=x^{up_i^{k_i}+vr}=\left(x^{p_i^{k_i}}\right)^u(x^r)^v=1.$$

Лемма 3. *Если* $i\neq j$, $x\in P_i$ *и* $y\in P_j$, *то* $xy=yx$.

Действительно, по лемме 1, $x^{-1}y^{-1}x\in P_j$ и $y^{-1}xy\in P_i$. Ввиду леммы 2, отсюда вытекает

$$[x, y]=(x^{-1}y^{-1}x)\,y=x^{-1}(y^{-1}xy)\in P_i\cap P_j=\{1\},$$

что и требовалось.

Теперь заметим, что, ввиду леммы 1, $P_1\ldots P_m$ — подгруппа в G. Из лемм 2 и 3 нетрудно вывести, что

$$P_1\ldots P_m\cong P_1\times\ldots\times P_m.$$

Равенство

$$|P_1\times\ldots\times P_m|=p_1^{k_1}\ldots p_m^{k_m}=|G|$$

показывает, что

$$G=P_1\ldots P_m,$$

чем и завершается доказательство теоремы.

Упражнения

1. Элемент нильпотентной группы без периодических элементов сопряжен со своим обратным тогда и только тогда, когда он равен 1.

2. Подгруппа некоммутативной нильпотентной группы G ступени n, порожденная некоторым элементом и коммутантом G', имеет ступень нильпотентности $n-1$.

3. Совокупность периодических элементов нильпотентной группы образует подгруппу.

4. Любая нормальная подгруппа нильпотентной группы G имеет нетривиальное пересечение с $\mathfrak{Z}_1(G)$.

5. В нильпотентной группе G без периодических элементов для любых $x, y\in G$ справедлива импликация

$$(x^my^n=y^nx^m)\Rightarrow(xy=yx).$$

6. Если нильпотентная группа G не содержит периодических элементов, то таких элементов нет и в фактор-группах $\mathfrak{Z}_{i+1}(G)/\mathfrak{Z}_i(G)$.

7. Конечно порожденная нильпотентная группа с конечным центром конечна.

8. Подгруппа конечно порожденной нильпотентной группы конечно порождена.

9. Периодические элементы конечно порожденной нильпотентной

группы образуют конечную подгруппу. Указание. Использовать предыдущее упражнение.

10. Нильпотентная группа порядка pq, где p и q — простые числа, коммутативна. То же для групп порядка $p^k q^l$, где $k, l \leqslant 2$.

§ 3. Линейные группы

Линейной группой степени n называется подгруппа G группы невырожденных линейных преобразований n-мерного линейного пространства V над некоторым полем. На протяжении всего этого параграфа пространство V считается зафиксированным. Подпространство U пространства V называется *G-инвариантным* подпространством или *G-подпространством*, если $g(x) \in U$ для любых $x \in U$ и $g \in G$. Линейная группа называется *неприводимой*, если V не содержит G-инвариантных подпространств, отличных от $\{0\}$ и V. В противном случае группа G называется *приводимой*. Взаимно однозначное линейное отображение $\varphi\colon U \to U'$, где U и U' — G-инвариантные подпространства, называется *изоморфизмом*, если $\varphi(g(x)) = g(\varphi(x))$ для любых $x \in U$ и $g \in G$.

Цоколем G-подпространства W называется сумма всех минимальных G-подпространств. Цоколь называется *однородным*, если он разлагается в прямую сумму попарно изоморфных минимальных G-подпространств.

Предложение 1. *Цоколь G-подпространства W представляется как прямая сумма минимальных G-подпространств. Если он однороден, то все входящие в него минимальные G-подпространства попарно изоморфны.*

Доказательство. Воспользовавшись леммой Куратовского — Цорна (теорема I.1.2), найдем максимальное подмножество минимальных G-подпространств, образующих прямую сумму. Если S — их сумма и $S \neq W$, то найдется минимальное G-подпространство $M \not\subseteq S$. Тогда $0 \subseteq M \cap S \subset S$. В силу минимальности подпространства M, $M \cap S = 0$. Следовательно, сумма $M \oplus S$ также прямая, что противоречит выбору суммы S. Если, далее, S однороден и M — минимальное G-подпространство, то существует ненулевой гомоморфизм φ G-подпространства M в одно из прямых слагаемых. В силу минимальности, соотношения $\operatorname{Ker}\varphi \neq M$ и $\operatorname{Im}\varphi \neq 0$ влекут соответственно, что φ — вложение и наложение.

Предложение 2. *Пусть H — нормальная подгруппа линейной группы G, а M_1 и M_2 — изоморфные минималь-*

ные H-подпространства. Тогда $g(M_1)$ и $g(M_2)$ — изоморфные минимальные H-подпространства для любого $g \in G$.

Доказательство. Если $0 \neq b \in g(M_1)$ и $y \in g(M_1)$, то $b = g(a)$ и $y = g(x)$ для некоторых a, $x \in M_1$. Поэтому для любого $h \in H$ получаем

$$h(y) = xgh = xghg^{-1}g = g(xghg^{-1}) \in g(M_1),$$

поскольку $g^{-1}hg \in H$. Следовательно, $g(M_1)$ — H-подпространство. Более того, поскольку $x = h(a)$ для некоторого $h \in H$, то

$$y = g(h(a)) = ahg = agg^{-1}hg = bg^{-1}hg,$$

что доказывает минимальность H-подпространства $g(M_1)$. Если, наконец, φ: $M_1 \to M_2$ — изоморфизм H-подпространств, то $g^{-1}\varphi g$ осуществляет изоморфизм H-подпространств $g(M_1)$ и $g(M_2)$.

Предложение 3. *Если G — абелева линейная группа над полем $\mathbf{C}$ комплексных чисел, то всякое неприводимое G-подпространство M одномерно.*

Доказательство. Напомним, что линейное преобразование называется *растяжением*, если все ненулевые векторы являются его собственными векторами с одним и тем же собственным значением (это значит, что в любой базе этому линейному преобразованию отвечает матрица вида λE, где $0 \neq \lambda \in \mathbf{C}$). Если все линейные преобразования из группы G являются растяжениями, то все одномерные подпространства M G-инвариантны, и одномерность пространства является следствием его инвариантности. Поэтому можно допустить, что G содержит линейное преобразование g_0, не являющееся растяжением. Разумеется, M содержит собственный вектор e линейного преобразования g_0. Пусть $g_0(e) = \lambda e$, где $\lambda \in \mathbf{C}$. Положим

$$W = \{x \mid x \in M,\ g_0(x) = \lambda x\}.$$

Если $w \in W$ и $g \in G$, то

$$g_0(g(w)) = g(g_0(w)) = \lambda g(w),$$

т. е. $g(w) \in W$. Следовательно, W — G-подпространство, откуда $W = M$. Таким образом, все ненулевые векторы из M оказываются собственными векторами для g_0 с собственным значением λ, т. е., вопреки допущению, g_0 оказывается растяжением.

Группа G называется *ограниченной*, если существует такое натуральное $k \geqslant 1$, что $g^k = 1$ для всех $g \in G$.

Предложение 4. *Ограниченная нильпотентная линейная группа G над полем комплексных чисел конечна.*

Доказательство. Пусть n — степень группы G и $g^k = 1$ для всех $g \in G$. Если $n = 1$, то G — подгруппа группы всех корней k-й степени из 1 и, следовательно, конечна. Если $n \geqslant 2$ и G приводима, то $V = V_1 \oplus V_2$, где V_1 и V_2 — ненулевые подпространства, скажем, размерности r и s соответственно, причем V_1 — G-инвариантно. Пусть $u_i\colon V_i \to V$ — естественные вложения, а $\pi_i\colon V \to V_i$ — проекции с ядром V_j, где $j \neq i$. Если $g \in G$, то обозначим через $\Phi_1(g)$ ограничение g на V_1 и положим $\Phi_2(g) = u_2 g \pi_2$. Поскольку V_1 — G-инвариантно, то Φ_1 — гомоморфизм группы G на ограниченную нильпотентную линейную группу G_1 степени $r < n$ и $u_1 g \pi_2 = 0$ для всех $g \in G$. Поэтому из равенства

$$\pi_1 u_1 + \pi_2 u_2 = 1_V$$

вытекает

$$g\pi_2 = \pi_1 u_1 g \pi_2 + \pi_2 u_2 g \pi_2 = \pi_2 u_2 g \pi_2.$$

Следовательно,

$$\Phi_2(g')\,\Phi_2(g'') = u_2 g' \pi_2 u_2 g'' \pi_2 = u_2 g' g'' \pi_2 = \Phi_2(g'g'')$$

для любых $g', g'' \in G$, т. е. Φ_2 — гомоморфизм группы G на ограниченную нильпотентную линейную группу G_2 степени $s < n$. В силу индуктивного предположения, G_1 и G_2 — конечные группы. Поэтому гомоморфизмы Φ_1 и Φ_2 определяют гомоморфизм Φ группы G в конечную группу $G_1 \times G_2$. Если $g \in \operatorname{Ker}\Phi$, то матрица этого линейного преобразования в базе, являющейся объединением баз подпространств V_1 и V_2 (координаты образа базисного вектора служат строками матрицы), имеет вид

$$\begin{Vmatrix} E & 0 \\ C & E \end{Vmatrix}.$$

Тогда

$$\begin{Vmatrix} E & 0 \\ 0 & E \end{Vmatrix} = \begin{Vmatrix} E & 0 \\ C & E \end{Vmatrix}^k = \begin{Vmatrix} E & 0 \\ kC & E \end{Vmatrix}.$$

Отсюда $C = 0$ и, следовательно, $\operatorname{Ker}\Phi = \{E\}$, что обеспечивает конечность группы G. Допустим теперь, что G неприводима, и рассмотрим максимальную абелеву нормальную подгруппу H в G. В силу предложения 2, цоколь H-пространства V является G-пространством и,

следовательно, совпадает с V. Но в силу предложения 3, неприводимые H-пространства одномерны. В силу предложения 1, V — прямая сумма одномерных H-пространств, и в базе пространства V, являющейся объединением баз этих подпространств, все матрицы, отвечающие линейным преобразованиям из H, оказываются диагональными. Поскольку $g^k = 1$ для всех $g \in G$, то на диагоналях должны стоять корни k-й степени из 1 и, следовательно, H конечна. По предложению 2.6(в) конечен индекс ее централизатора C в G. Остается заметить, что, в силу предложения 2.6(г), $H = C$, т. е. индекс подгруппы H в группе G конечен.

Напомним, что группа G называется *разрешимой*, если ряд ее коммутантов $G \supseteq G' \supseteq G'' \supseteq \ldots \supseteq G^{(k)} \supseteq \ldots$, где $G^{(k)} = (G^{(k-1)})'$, обрывается на конечном шаге, т. е. $G^{(n)} = \{1\}$ для некоторого n (ср. ЭА, с. 216).

Теорема 1 (Колчин — Мальцев). *Каждая разрешимая линейная группа G степени n над полем комплексных чисел* $\mathbf{C}$ *содержит такую подгруппу K конечного индекса, что при подходящем выборе базы все матрицы, отвечающие линейным преобразованиям из K, оказываются нижними треугольными.*

Замечание. Другими словами, заключение теоремы 1 утверждает, что матрицы из K одновременно приводятся к нижнему треугольному виду. В этом случае говорят также, что группа K *триангулируема*.

Доказательство. Поскольку для $n = 1$ теорема тривиально справедлива, то можно предполагать, что для линейных групп степени, меньшей n, теорема верна.

Лемма. *Если K и L — подгруппы конечного индекса в группе G, то подгруппа $K \cap L$ также имеет конечный индекс в G.*

Действительно, пусть $a_1, \ldots, a_p$ — представители всех левых смежных классов по подгруппе K. Далее, выберем представители $b_1, \ldots, b_q$ левых смежных классов по подгруппе L, причем, если смежный класс содержит элементы из K, то в качестве его представителя возьмем один из этих элементов. Если теперь $g \in G$, то для подходящего номера i имеем $g = a_i k$, где $k \in K$, а для подходящего номера j получаем $k = b_j l$, где $l \in L$. В силу выбора элемента b_j, $b_j \in K$. Отсюда $l = b_j^{-1} k \in K \cap L$ и, следовательно, $g = a_i b_j l \in a_i b_j (K \cap L)$. Таким образом, множество

$$\{a_i b_j \mid i = 1, \ldots, p;\ j = 1, \ldots, q\}$$

содержит представители всех левых смежных классов по подгруппе $K \cap L$, что и требовалось.

Дальнейшее доказательство теоремы сводится к рассмотрению ряда случаев.

Случай 1. G приводима.

При этом предположении $V = V_1 \oplus V_2$, где V_1 и V_2 — ненулевые подпространства, скажем, размерности r и s соответственно, причем V_1 — G-инвариантно. Тогда в базе, являющейся объединением баз подпространств V_1 и V_2, каждому линейному преобразованию $g \in G$ отвечает матрица

$$A(g) = \left\| \begin{array}{c|c} A_1(g) & 0 \\ \hline * & A_2(g) \end{array} \right\| \begin{matrix} \}r \\ \}s \end{matrix}.$$

Пусть G_i, $i = 1, 2$, — множество линейных преобразований пространства V_i, отвечающих матрицам $A_i(g)$, где g пробегает группу G. Нетрудно проверить, что G_i — группа и что A_i — гомоморфное наложение группы G на G_i. Будучи линейными группами степени, меньшей n, G_1 и G_2 содержат триангулируемые подгруппы $\overline{K}_1$ и $\overline{K}_2$ соответственно, имеющие конечный индекс, по индуктивному предположению. Это означает, что для подходящих $r \times r$-матрицы T_1 и $s \times s$-матрицы T_2 группы $T_1^{-1}\overline{K}_1 T_1$ и $T_2^{-1}\overline{K}_2 T_2$ (здесь под $\overline{K}_1$ и $\overline{K}_2$ понимаются группы матриц, соответствующих линейным преобразованиям из $\overline{K}_1$ и $\overline{K}_2$ в выбранной выше базе) состоят из нижних треугольных матриц. Пусть K_1 и K_2 — полные прообразы подгрупп $\overline{K}_1$ и $\overline{K}_2$ в G, а

$$T = \left\| \begin{array}{cc} T_1 & 0 \\ 0 & T_2 \end{array} \right\|.$$

Тогда для любого $g \in K_1 \cap K_2$ имеем

$$T^{-1}A(g)T = \left\| \begin{array}{c|c} T_1^{-1} & 0 \\ \hline 0 & T_2^{-1} \end{array} \right\| \cdot \left\| \begin{array}{c|c} A_1(g) & 0 \\ \hline * & A_2(g) \end{array} \right\| \cdot \left\| \begin{array}{c|c} T_1 & 0 \\ \hline 0 & T_2 \end{array} \right\| =$$

$$= \left\| \begin{array}{c|c} T_1^{-1}A_1(g)\,T_1 & 0 \\ \hline * & T_2^{-1}A_2(g)\,T_2 \end{array} \right\| = \left\| \begin{array}{c|c} \diagdown & 0 \\ \hline * & \diagdown \end{array} \right\|.$$

Поскольку K_1 и K_2, очевидно, имеют конечный индекс в G, то по лемме, $K = K_1 \cap K_2$ — искомая триангулируемая подгруппа конечного индекса.

Случай 2. G неприводима и содержит такую нормальную подгруппу H, что цоколь S H-пространства V неоднороден.

Согласно предложению 1, цоколь S представляется в виде прямой суммы минимальных H-подпространств. Объединяя изоморфные прямые слагаемые, запишем

$$S = S_1 \oplus \ldots \oplus S_m,$$

где S_i — однородные H-подпространства. По предположению, $m \geqslant 2$. Из предложений 1 и 2 вытекает, что каждое линейное преобразование $g \in G$ осуществляет перестановку слагаемых $S_1, \ldots, S_m$. Следовательно, существует гомоморфизм φ группы G в симметрическую группу $\mathfrak{S}_m$. Ясно, что $\overline{K} = \operatorname{Ker}\varphi$ имеет конечный индекс в G и что S_i — $\overline{K}$-подпространства. Согласно случаю 1, $\overline{K}$ содержит триангулируемую подгруппу K конечного индекса. Ясно, что K имеет конечный индекс в G.

Случай 3. G неприводима, унимодулярна (т. е. в любой базе определители всех матриц, отвечающих линейным преобразованиям из G, равны 1) и для любой нормальной подгруппы H группы G цоколь H-пространства V однороден.

В силу предложения 2, для любой нормальной подгруппы H из G цоколь H-пространства V G-инвариантен, и, следовательно, совпадает с V. В частности, если H абелева, то, в силу предложения 3, V разлагается в прямую сумму изоморфных друг другу одномерных H-подпространств. Поэтому матрицы, отвечающие линейным преобразованиям из H, оказываются скалярными. Ввиду унимодулярности группы G, они имеют вид λE, где λ — корень n-й степени из 1. Следовательно, H — конечная группа. Далее, воспользовавшись разрешимостью группы G, выпишем ряд коммутантов

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(r)} \supseteq G^{(r+1)} = \{1\}.$$

Будучи абелевой нормальной подгруппой в G, группа $G^{(r)}$ оказывается, как отмечено выше, конечной. Допустим, что установлена конечность групп $G^{(r)}$, $G^{(r-1)}$, ..., $G^{(r-k)}$. Обозначим через C централизатор группы $G^{(r-k)}$ в группе $G^{(r-k-1)}$. Поскольку $C = G^{(r-k-1)} \cap \overline{C}$, где $\overline{C}$ — централизатор подгруппы $G^{(r-k)}$ в G, то, ввиду предложения 2.6(а), C — нормальная подгруппа в G. По предложению 2.6(б), нормальным в G оказывается и ее центр Z.

Как уже отмечалось, группа Z должна быть конечной. Кроме того,

$$[[C, C], C] \subseteq [[G^{(r-k-1)}, G^{(r-k-1)}], C] = [G^{(r-k)}, C] = \{1\},$$

т. е. группа C нильпотентна. Из теоремы 2.1 и предложения 2.4(в) вытекает ограниченность группы C. Поэтому, по предложению 4, она должна быть конечной. С другой стороны, из предложения 2.6(в) вытекает конечность фактор-группы $G^{(r-k-1)}/C$. Поскольку

$$|G^{(r-k-1)}| = |G^{(r-k-1)}/C| \cdot |C|,$$

то $G^{(r-k-1)}$ оказывается конечной группой. Таким образом, группа G конечна и теорема тривиально справедлива.

Случай 4. G неприводима и для любой нормальной подгруппы H из G цоколь H-пространства V однороден.

Пусть Δ — группа всех растяжений. Положим $\overline{G} = \Delta G$. Тогда

$$\overline{G}/\Delta = \Delta G/\Delta \cong G/\Delta \cap G.$$

Поскольку Δ коммутативна, а $G/\Delta \cap G$ разрешима, то разрешимой оказывается и группа $\overline{G}$ (ЭА, с. 216, теорема IV.2.5). Используя возможность извлекать корни n-й степени из 1, запишем $\overline{G} = \Delta G_1$, где G_1 — унимодулярная группа. Будучи нормальной подгруппой разрешимой группы $\overline{G}$, группа G_1 разрешима. Если G_1 не удовлетворяет условиям случаев 1 и 2, то мы оказываемся в условиях случая 3. Таким образом, G_1 содержит триангулируемую подгруппу K_1 конечного индекса, т. е. множество G_1/K_1 левых смежных классов группы G_1 по подгруппе K_1 конечно. Положим $K = \Delta K_1 \cap G$ и рассмотрим отображение Φ множества левых смежных классов G/K в G_1/K_1, где

$$\Phi(gK) = |g|^{-1} g K_1,$$

причем $|g|$ — определитель матрицы, соответствующий линейному преобразованию g в какой-нибудь базе. Если $a, b \in G$ и $|a|^{-1} a = |b|^{-1} bk$, где $k \in K_1$, то

$$b^{-1}a = |a| \cdot |b|^{-1} k \in \Delta K_1 \cap G = K,$$

т. е. $a \in bK$. Таким образом, Φ оказывается вложением и, следовательно, подгруппа K имеет конечный индекс в G. Но эта подгруппа, будучи подгруппой триангулируемой группы ΔK_1, триангулируема.

Упражнения

1. Если H — нормальная подгруппа линейной группы G и U — G-инвариантное подпространство осиовного пространства V, то UH — G-инвариантное подпространство.

2. Центр неприводнмой линейной группы над алгебраическн замкнутым полем состоит из скалярных матриц.

3. Разрешимая линейная группа над полем комплексных чисел содержит нормальную подгруппу с нильпотентным коммутантом, имеющую конечный индекс.

§ 4. Кольца и алгебры Ли

Кольцом называется абелева группа R, на которой определена операция умножения, связанная со сложением дистрибутивными законами

$$(a+b)\,c = ac + bc$$

и

$$a\,(b+c) = ab + ac$$

для любых a, b, $c \in R$. Кольцо R называется *алгеброй* над коммутативным ассоциативным кольцом Φ с единицей, если R — модуль над Φ и для любых $a, b \in R$ и $\lambda \in \Phi$ имеет место

$$\lambda\,(ab) = (\lambda a)\,b = a\,(\lambda b).$$

Каждое кольцо можно рассматривать как алгебру над кольцом целых чисел.

Кольцо [алгебра] называется *кольцом Ли* [*алгеброй Ли*], если для любых его элементов a, b и c справедливы равенства

$$aa = 0$$

и

$$(ab)\,c + (bc)\,a + (ca)\,b = 0 \quad \text{(тождество Якоби)}.$$

Возводя $a+b$ в квадрат и применяя первое соотношение, получаем

$$ab + ba = 0 \quad \text{(антикоммутативность)}.$$

Всякое ассоциативное кольцо [алгебра] A превращается в кольцо Ли [алгебру Ли] $A^{(-)}$, если, сохранив сложение, определить новое умножение $[\ ,\ ]$ равенством

$$[a,\ b] = ab - ba.$$

Действительно, $[a, a]=0$ и, как показывает прямой счет,

$$[[a, b], c]+[[b, c], a]+[[c, a], b]=0.$$

Кольцо Ли образуют векторы трехмерного пространства с обычным сложением и векторным умножением. Кольцом Ли является и всякое кольцо с нулевым умножением. Оба эти утверждения проверяются непосредственным подсчетом.

Пусть X—линейно упорядоченное множество и $W(X)$ — множество всех ассоциативных слов в алфавите X (см. § 3 гл. II). Напомним, что через $l(w)$ обозначается длина слова w. Длина пустого слова считается равной нулю. На множестве $W(X)$ определим порядок, полагая

$$x_1 \ldots x_m \leqslant y_1 \ldots y_n,$$

если для некоторого i имеем $x_1=y_1, \ldots, x_{i-1}=y_{i-1}$ и либо $x_i < y_i$, либо $i=n+1$. Без труда проверяется, что это действительно порядок, т. е. справедливы свойства рефлексивности, транзитивности и антисимметричности. Столь же просто убедиться, что множество $W(X)$ линейно упорядочено. Подчеркнем, что слово, совпадающее с начальным отрезком другого слова, считается, в соответствии с данным определением, бо́льшим последнего.

Ассоциативное слово w в линейно упорядоченном алфавите X называется *правильным*, если для всякого представления $w=uv$, где $u, v \neq \varnothing$, справедливо неравенство $vu < w$.

Наряду с ассоциативными будут рассматриваться и неассоциативные слова в линейно упорядоченном алфавите X. Если w—неассоциативное слово в этом алфавите, то через $\bar{w}$ будем обозначать ассоциативное слово, полученное из w удалением всех скобок. Неассоциативное слово w в алфавите X называется *правильным*, если: (*i*) $\bar{w}$—правильное ассоциативное слово; (*ii*) если $w=uv$, то u и v—правильные неассоциативные слова и $\bar{u} > \bar{v}$; (*iii*) если $w=(u'u'')v$ и $u', u'' \neq \varnothing$, то $\bar{u}'' \leqslant \bar{v}$.

Предложение 1. *Если* $w=x_1 \ldots x_n$ — *правильное ассоциативное слово в линейно упорядоченном алфавите* X, *то* $x_1 \geqslant x_i$ *для всех* i, *а если* $n \geqslant 2$, *то* $x_1 > x_n$.

Доказательство. Если $x_1 < x_i$, то

$$w=x_1 \ldots x_n < (x_i \ldots x_n)(x_1 \ldots x_{i-1}),$$

что противоречит определению правильности. Если же $x_1 = x_i$ для всех i, то $w = vu$ для любого представления $w = uv$, что опять несовместимо с правильностью. Поэтому, допустив, что $x_1 = x_m$, и положив $x_1 = a$, для некоторого i получим $w = a^k x_i \ldots x_{i+t} a^m$, где $x_i < a$, k, $m \geqslant 1$, $l \geqslant 0$. Отсюда

$$a^m (a^k x_i \ldots x_{i+l}) > a^k x_i \ldots x_{i+t} a^m = w,$$

вопреки правильности слова w.

Предложение 2. *Пусть X — линейно упорядоченный алфавит, a, $d \in X$, $d < a$ и Y — алфавит, полученный присоединением к X новой буквы z. Для любого $x \in X$ полагаем $x < z$, если $x < a$, и $z < x$, если $a \leqslant x$. Тогда*

(а) *Y — линейно упорядоченное множество.*

Если, далее, u — слово в алфавите X (ассоциативное или неассоциативное), *то через $\tilde{u}$ обозначается слово в алфавите Y, полученное из u заменой всех подслов ad на z. Наоборот, если w — слово в алфавите Y* (ассоциативное или неассоциативное), *то через $\nu(w)$ обозначается слово в алфавите X, полученное из w заменой буквы z словом ad. Тогда:*

(б) *Для любого слова u в алфавите X* (ассоциативного или неассоциативного), *не содержащего подслова ad,*

$$\nu(\tilde{u}) = u.$$

(в) *Для любого слова w в алфавите Y* (ассоциативного или неассоциативного)

$$\widetilde{\nu(w)} = w.$$

(г) *Для любого неассоциативного слова w в алфавите Y*

$$\overline{\nu(w)} = \nu(\overline{w}).$$

(д) *Если u и v — ассоциативные слова в алфавите X, причем или v не начинается с d, или u не кончается на a, то*

$$\widetilde{uv} = \tilde{u}\tilde{v}.$$

(е) *Если u и v — ассоциативные слова в алфавите X, не содержащие букв, меньших d, то $u < v$ тогда и только тогда, когда $\tilde{u} < \tilde{v}$.*

(ж) *Если u — ассоциативное слово в алфавите X, не содержащее букв, меньших d, то u и $\tilde{u}$ являются правильными ассоциативными словами одновременно.*

(з) *Если* u *и* v *— ассоциативные слова в алфавите* Y, *не содержащие подслов* ad *и букв, меньших* d, *то* $u < v$ *тогда и только тогда, когда* $\nu(u) < \nu(v)$.

(и) *Если* u *— ассоциативное слово в алфавите* Y, *не содержащее подслова* ad *и букв, меньших* d, *то* u *и* $\nu(u)$ *являются правильными ассоциативными словами одновременно.*

(к) *Если* w *— правильное неассоциативное слово в алфавите* Y, *причем* $\overline{w}$ *не содержит подслова* ad *и букв, меньших* d, *то* $\nu(w)$ *— правильное неассоциативное слово в алфавите* X.

(л) *Если* u *— правильное неассоциативное слово в алфавите* X, *не содержащее букв, меньших* d, *то*

$$\tilde{\bar{u}} = \bar{\tilde{u}}.$$

Доказательство. Утверждения (а) — (д) очевидны.

(е) Пусть $u < v$. Допустим, что $u = vs$. Если s не начинается с d или v не кончается на a, то, ввиду (д), $\tilde{u} = \tilde{v}\tilde{s}$, откуда $\tilde{u} < \tilde{v}$. В противном случае получаем то же самое, заметив, что $s = ds'$, $\tilde{v} = \tilde{v}'a$, $\tilde{u} = \tilde{v}'z\tilde{s}'$ и $z < a$. Поэтому обратимся к случаю, когда $u = wxu'$, $v = wyv'$, где $x, y \in X$ и $x < y$. Если w кончается на a и $x = d$, то $y \neq d$ и $w = w'a$. Учитывая (д), получаем

$$\tilde{u} = \widetilde{w'adu'} = \tilde{w}'z\tilde{u}' \quad \text{и} \quad \tilde{v} = \widetilde{w'ayu'} = \tilde{w}'a\widetilde{yu'}.$$

Отсюда $\tilde{u} < \tilde{v}$, ибо, по определению, $z < a$. Если w не кончается на a или $x \neq d$, то заметим, что из неравенства $x < y$ и ограничений, наложенных на u и v, вытекает, что $y \neq d$. Поэтому, снова используя (д), получаем

$$\tilde{u} = \tilde{w}\widetilde{xu'} = \begin{cases} \tilde{w}x\tilde{u}', & \text{если } x \neq a \text{ или } u' \text{ не} \\ & \text{начинается с } d, \qquad (1_u) \\ \tilde{w}z\tilde{u}'' & \text{в противном случае} \qquad (2_u) \end{cases}$$

и

$$\tilde{v} = \tilde{w}\widetilde{yv'} = \begin{cases} \tilde{w}y\tilde{v}', & \text{если } y \neq a \text{ или } v' \text{ не} \\ & \text{начинается с } d, \qquad (1_v) \\ \tilde{w}z\tilde{u}'' & \text{в противном случае.} \qquad (2_v) \end{cases}$$

Рассматривая все комбинации возникших возможностей, получаем:

(1_u) и (1_v): $\tilde{u} < \tilde{v}$, ибо $x < y$.

(1_u) и (2_v): имеем $x < y = a$, откуда $x < z$ и, следовательно, $\tilde{u} < \tilde{v}$.

(2_u) и (1_v): имеем $a = x < y$, откуда $z < y$ и, следовательно, $\tilde{u} < \tilde{v}$.

(2_u) и (2_v): невозможно, ибо $x \neq y$.

Пусть теперь $\tilde{u} < \tilde{v}$. Если $\tilde{u} = \tilde{v}s$, то, очевидно, $u < v$. Допустим, что $\tilde{u} = \tilde{w}x\tilde{u}'$, $\tilde{v} = \tilde{w}y\tilde{v}'$, где $x, y \in Y$ и $x < y$. Если $x, y \in X$, то, очевидно, $u < v$. Если $x = z$, то $u = wadu'$, $v = wyv'$ и $z < y$. Отсюда, по определению, $a \leqslant y$. При $a < y$ сразу получаем, что $u < v$. В случае же, когда $a = y$, замечаем, что v' не начинается с d (иначе было бы $\tilde{v} = \tilde{w}z\tilde{v}''$), т. е. $v' = tv''$, где $d \neq t \in X$. Отсюда $v = watv''$ и, следовательно, $u < v$, поскольку $d < t$.

(ж) Если $l(u) = 1$ или $u = ad$, то справедливость утверждения очевидна. В противном случае $l(\tilde{u}) \geqslant 2$. Если u — правильное ассоциативное слово и $\tilde{u} = w'w''$, где w' и w'' — слова в алфавите Y, то, в силу (б),

$$u = \nu(\tilde{u}) = \nu(w')\nu(w'').$$

В силу правильности слова u, отсюда вытекает

$$\nu(w'')\nu(w') < u.$$

Кроме того, ввиду предложения 1, слово u, а значит, и $\nu(w')$ не начинается с d. Поэтому, применяя (в), (д) и (е), получаем

$$w''w' = \widetilde{\nu(w'')}\,\widetilde{\nu(w')} = \widetilde{\nu(w'')\nu(w')} < \tilde{u}.$$

Этим доказана правильность слова $\tilde{u}$. Наоборот, если правильно слово $\tilde{u}$ и $u = u'u''$, то по тем же соображениям

$$\widetilde{u''u'} = \tilde{u}''\tilde{u}' < \tilde{u},$$

откуда $u''u' < u$, что и требовалось.

(з) В силу (в) и (е) справедлива эквивалентность

$$(\nu(u) < \nu(v)) \Leftrightarrow (u = \widetilde{\nu(u)} < \widetilde{\nu(v)} = v).$$

(и) Вытекает из (в) и (ж).

(к) Очевидно, если w не содержит буквы z. В противном случае при $l(w) = 1$ замечаем, что $w = z$ и $\nu(w) = ad$ — правильное слово, а при $l(w) = 2$ возникают две возможности: $w = xz$ или $w = zx$, где $x \in X$. В первом случае, ввиду правильности слова w, имеем $x > z$, и цепочка

импликаций

$$(x > z) \Rightarrow (a \leqslant x) \Rightarrow (x \geqslant ad)$$

обеспечивает правильность неассоциативного слова $\nu(w) = x(ad)$. Во втором случае правильность неассоциативного слова $\nu(w) = (ad)x$ вытекает из имеющего по условию место неравенства $d \leqslant x$ и цепочки импликаций

$$(z > x) \Rightarrow (x < a) \Rightarrow (ad > x).$$

Если $l(w) \geqslant 3$, то $w = uv$, где u и v — правильные неассоциативные слова в алфавите Y, причем $\bar{u} > \bar{v}$. Тогда $\nu(w) = \nu(u)\nu(v)$. В силу индуктивного предположения, $\nu(u)$ и $\nu(v)$ — правильные неассоциативные слова в алфавите X. Согласно (г) и (и), $\overline{\nu(w)} = \nu(\bar{w})$ — правильное ассоциативное слово, а из (г) и (з) вытекает

$$\overline{\nu(u)} = \nu(\bar{u}) > \nu(\bar{v}) = \overline{\nu(v)}.$$

Если $l(u) \geqslant 2$, то $u = u'u''$ и $\bar{u}'' \leqslant \bar{v}$. Тогда $\nu(w) = (\nu(u') \times \times \nu(u''))\nu(v)$ и $\overline{\nu(u'')} < \overline{\nu(v)}$ в силу (г) и (з), как и выше. Этим доказана правильность неассоциативного слова $\nu(w)$ при $l(u) \geqslant 2$. Если $l(u) = 1$, то при $u \neq z$ имеем $l(\nu(u)) = 1$, и слово $\nu(w)$ опять оказывается правильным. Если же $u = z$, то $\nu(w) = (ad)\nu(v)$ и $d \leqslant \overline{\nu(v)}$, ибо $\overline{\nu(v)}$, будучи правильным ассоциативным словом, или имеет длину 1, или, в силу предложения 1, не начинается с d. Так что и в этом случае $\nu(w)$ — правильное неассоциативное слово.

(л) Если $l(u) = 1$, то все ясно. Если $l(u) = 2$, то при $u \neq ad$ имеем $\bar{\bar{u}} = u = \tilde{u}$, откуда $\tilde{\bar{u}} = \bar{\tilde{u}}$. Если же $u = ad$, то $\bar{\bar{u}} = z = \bar{z} = \tilde{\bar{u}}$. Допустим теперь, что $l(u) \geqslant 3$. Тогда $u = sv$, где s и v — правильные неассоциативные слова. Если $v \neq d$, то, в силу предложения 1, v не начинается с d. Поэтому, учитывая индуктивное предположение и утверждение (д), получаем

$$\bar{\bar{u}} = \bar{\bar{sv}} = \bar{\bar{s}}\,\bar{\bar{v}} = \tilde{\bar{s}}\,\tilde{\bar{v}} = \tilde{\bar{sv}} = \tilde{\bar{u}}. \qquad (*)$$

Обратимся к случаю, когда $v = d$. Поскольку $l(u) \geqslant 3$, то $s = s's''$, где s' и s'' — правильные неассоциативные слова и $\bar{s}'' \leqslant d$. Если $s'' \neq d$, то, по предложению 1, s'' начинается с буквы, большей d, и, следовательно, $\bar{s}'' > d$. Таким образом, $s'' = d$, т. е. s не кончается на a, что

позволяет получить цепочку равенств (*) с помощью тех же самых соображений.

Предложение 3. *Всякое ассоциативное слово w в линейно упорядоченном алфавите X единственным образом представляется в форме*

$$w = w_1 \dots w_r,$$

где $w_1 \leqslant w_2 \leqslant \dots \leqslant w_r$ и каждое из подслов w_i является правильным ассоциативным словом.

Доказательство. Справедливость предложения тривиальна, если $l(w) = 1$. Если $l(w) = 2$, то $w = xy$, где $x, y \in X$. При $x > y$ слово w оказывается правильным, а при $x \leqslant y$ можно положить $w_1 = x$ и $w_2 = y$. Пусть теперь $l(w) \geqslant 3$ и d — наименьшая из букв, входящих в слово w. Если $w = dw'$, то, в силу индуктивного предположения, $w' = w_2 \dots w_r$, где w_i — однозначно определенные правильные ассоциативные слова и $w_2 \leqslant \dots \leqslant w_r$. Если $l(w_2) = 1$, то $d \leqslant w_2$, в силу выбора d. Если $l(w_2) \geqslant 2$, то, согласно предложению 1, w_2 не начинается с d, откуда $d < w_2$. Следовательно, в обоих случаях можно положить $w_1 = d$. Для доказательства единственности достаточно заметить, что, ввиду предложения 1, никакой начальный отрезок слова w, отличный от d, правильным ассоциативным словом быть не может. Обратимся к случаю, когда w не начинается с d. Тогда w содержит подслово ad, где $d < a$. Применительно к этим буквам используем обозначения Y, $\tilde{u}$ и $\nu(w)$, введенные в предложении 2. Тогда $l(\tilde{w}) < l(w)$ и, в силу индуктивного предположения,

$$\tilde{w} = w_1 \dots w_r,$$

где w_i — правильные ассоциативные слова в алфавите Y и $w_1 \leqslant \dots \leqslant w_r$. Ввиду предложения 2 (б),

$$w = \nu(\tilde{w}) = \nu(w_1) \dots \nu(w_r).$$

Из предложения 2 (и) вытекает правильность слов $\nu(w_i)$, а из предложения 2 (з) — справедливость неравенств

$$\nu(w_1) \leqslant \dots \leqslant \nu(w_r).$$

Если

$$w = s_1 \dots s_m,$$

где s_i — правильные ассоциативные слова, $s_1 \leqslant \ldots \leqslant s_m$ и w не начинается с d, то с d не начинается и слово s_1. Но тогда d не может стоять и в начале слов $s_2, \ldots, s_m$. По предложению 2 (д),

$$\tilde{w} = \tilde{s}_1 \ldots \tilde{s}_m.$$

По предложению 2 (ж), $\tilde{s}_i$ — правильные ассоциативные слова, а, в силу предложения 2 (е), $\tilde{s}_1 \leqslant \ldots \leqslant \tilde{s}_m$. Из индуктивного предположения получаем $m = r$ и $w_i = \tilde{s}_i$ для всех i. Отсюда, ввиду предложения 2 (б),

$$\nu(w_i) = \nu(\tilde{s}_i) = s_i$$

для всех i, чем и завершается доказательство единственности нужного представления.

Предложение 4. *Если u — правильное ассоциативное слово в линейно упорядоченном алфавите X, то существует единственное правильное неассоциативное слово $\omega(u)$ такое, что $\overline{\omega(u)} = u$.*

Доказательство. Если $l(u) \leqslant 2$, то можно положить $\omega(u) = u$. Если $l(u) \geqslant 3$, то обозначим через d наименьшую букву, входящую в u. Ввиду предложения 1, u не начинается с d. Следовательно, u содержит подслово ad, где $d < a$. Применительно к этой паре будем использовать обозначения Y, $\tilde{u}$ и $\nu(w)$, введенные в предложении 2. В силу предложения 2 (ж), $\tilde{u}$ — правильное ассоциативное слово в алфавите Y, причем $2 \leqslant l(\tilde{u}) < l(u)$. В силу индуктивного предположения, $\tilde{u} = \omega(\tilde{u})$, где $\omega(\tilde{u})$ — правильное неассоциативное слово в алфавите Y. Положим

$$\omega(u) = \nu(\omega(\tilde{u})).$$

В силу предложения 2 (к), $\omega(u)$ — правильное неассоциативное слово в алфавите X, а из предложений 2 (г) и 2 (б) вытекает

$$\overline{\omega(u)} = \overline{\nu(\omega(\tilde{u}))} = \nu(\overline{\omega(\tilde{u})}) = \nu(\tilde{u}) = u.$$

Если, далее, v — правильное неассоциативное слово в алфавите X и $\overline{v} = u$, то ввиду предложения 2 (л)

$$\tilde{v} = \tilde{\overline{v}} = \tilde{u} = \overline{\omega(\tilde{u})}.$$

В силу индуктивного предположения, отсюда вытекает, что $\tilde{v} = \omega(\tilde{u})$, после чего предложение 2 (б) дает

$$v = \nu(\tilde{v}) = \nu(\omega(\tilde{u})) = \omega(u).$$

Ассоциативная алгебра A с единицей над коммутативным ассоциативным кольцом Φ с единицей называется *универсальной обертывающей* алгебры Ли L над тем же кольцом, если существует гомоморфное вложение $\sigma\colon L \to A^{(-)}$ и для любой ассоциативной алгебры B с единицей над кольцом Φ и любого гомоморфизма $\varphi\colon L \to B^{(-)}$ существует гомоморфизм $\psi\colon A \to B$ такой, что $\sigma\psi = \varphi$.

Теорема 1 (Пуанкаре — Биркгоф — Витт). *Всякая алгебра Ли L над любым полем P обладает универсальной обертывающей.*

Доказательство. Пусть X — база линейного пространства L. В силу аксиомы о полном упорядочении, можно считать, что множество X вполне упорядочено. Пусть, далее, F — свободная алгебра Ли над полем P со свободной порождающей системой X и $\pi\colon F \to L$ — гомоморфизм алгебр Ли, где $\pi(x) = x$ для всех $x \in X$. Положим $T = \operatorname{Ker}\pi$ и обозначим через G свободную ассоциативную алгебру с единицей над полем P со свободной порождающей системой X. Умножение в алгебрах F и G условимся обозначать символами $\circ$ и $\cdot$ соответственно.

Наряду с введенным ранее, нам понадобится новый порядок на множестве $W(X)$ всех ассоциативных слов в алфавите X. Именно, если $u, v \in W(X)$, то условимся писать $u \trianglelefteq v$ и говорить, что *u младше v* или что *v старше u*, если или $l(u) < l(v)$, или $l(u) = l(v)$ и $u \leqslant v$. Нетрудно проверить, что это определение превращ ет множество $W(X)$ в линейно упорядоченное множество.

Легко проверяется

Лемма 1. *Если u, u', v, $v' \in W(X)$, $u \trianglelefteq u'$ и $v \trianglelefteq v'$, то $uv \trianglelefteq u'v'$.*

Лемма 2. *$(W(X), \trianglelefteq)$ — вполне упорядоченное множество.*

Для доказательства достаточно установить, что вполне упорядочены множества

$$W_n = \{w \mid w \in W(X),\ l(w) = n\}, \qquad n = 1, 2, \ldots$$

Но при $n = 1$ это вытекает из полной упорядоченности множества X. Если же $n \geqslant 2$ и $\varnothing \neq M \subseteq W_n$, то среди

первых букв слов, принадлежащих M, найдем наименьшую, скажем, x_0. Пусть M_0 — множество, состоящее из всех слов, принадлежащих M и начинающихся с x_0, а $\tilde{M}_0$ — множество слов, получающихся из слов, принадлежащих M_0, отбрасыванием стоящей в начале буквы x_0. В силу индуктивного предположения, $\tilde{M}_0$ содержит самое младшее слово, скажем, w_0. Тогда нетрудно проверить, что $x_0 w_0$ оказывается самым младшим словом множества M.

Лемма 3. *F совпадает с линейной оболочкой множества $\mathfrak{W}$ всех правильных неассоциативных слов в алфавите X.*

Будем доказывать, что каждое неассоциативное слово w в алфавите X как элемент алгебры F равно линейной комбинации слов из $\mathfrak{W}$. Если $l(w)=1$, то справедливость этого утверждения тривиальна. Если $l(w)\geqslant 2$, то $w=u\circ v$. При этом индуктивное предположение позволяет считать, что $u, v\in\mathfrak{W}$. Ввиду антикоммутативности, можно предполагать, что $\bar{u}\geqslant\bar{v}$. Если $\bar{u}=\bar{v}$, то, по предложению 4, $u=v$, откуда $w=0$, по определению кольца Ли. Так что можно считать, что $\bar{u}>\bar{v}$. Теперь будем вести индукцию по длине слова u. Если $l(u)=1$, т. е. $u\in X$, то при $l(v)=1$ сразу замечаем, что $\bar{w}=\overline{uv}$ — правильное ассоциативное слово, а $w=u\circ v$ — правильное неассоциативное слово. Если же $l(v)\geqslant 2$, то, учитывая предложение 1, запишем $\bar{v}=u^k y s$, где $k\geqslant 0$, $y\in X$ и $u>y$. Убедимся, что w — правильное неассоциативное слово. Поскольку $l(u)=1$ и $\bar{u}>\bar{v}$, то для этого достаточно установить, что $\bar{w}=u^{k+1}ys$ — правильное ассоциативное слово. Если это не так, то

$$\bar{w}=w'w''\leqslant w''w'$$

для некоторых ассоциативных слов w' и w''. Возможны два случая:

1) $w'=u^l$, где $1\leqslant l\leqslant k+1$;
2) $w'=u^{k+1}ys'$, где $s's''=s$.

Но в первом случае получаем невозможное соотношение

$$w''w'=u^{k+1-l}ysu^l<u^{k+1}ys=\bar{w}\leqslant w''w',$$

ибо $y<u$. Во втором же случае имеем

$$s''u^{k+1}ys'=w''w'\geqslant\bar{w}=u^{k+1}ys'.$$

Поскольку, в силу предложения 1, все буквы слова s'' не превосходят u, отсюда вытекает, что

$$s'' = u^{k+1}s'''.$$

Но тогда

$$\bar{v} = (u^k y s')\, s'' < u^{k+1}s'''u^k y s' = s''\,(u^k y s'),$$

вопреки правильности слова $\bar{v}$. Допустим теперь, что $l(u) \geqslant 2$, т. е. $u = u' \circ u''$. Поскольку u — правильное неассоциативное слово, то такими же будут слова u' и u''. Из тождества Якоби и антикоммутативности вытекает

$$w = (u' \circ u'') \circ v = -(u'' \circ v) \circ u' - (v \circ u') \circ u'' = \\ = u' \circ (u'' \circ v) + u'' \circ (v \circ u').$$

Поскольку $l(u')$, $l(u'') < l(u)$, то, в силу индуктивного предположения, слова $u' \circ (u'' \circ v)$ и $u'' \circ (v \circ u')$, а значит и w, представляются в виде линейной комбинации слов из $\mathfrak{W}$.

Если $0 \neq g \in G$, то самое старшее из ассоциативных слов, входящих в запись элемента g с ненулевым коэффициентом, назовем *лидером* элемента g и будем обозначать через $\varkappa(g)$.

Лемма 4. *Если* $f, g \in G$, *то* $\varkappa(fg) = \varkappa(f)\,\varkappa(g)$.

Для доказательства достаточно заметить, что $\varkappa(f)\,\varkappa(g)$ отлично от всех других слов, входящих в запись элемента fg, и применить лемму 1.

Для элементов $f, g \in G$ положим

$$[f, g] = fg - gf.$$

По свойству универсальности свободной алгебры, тождественное отображение множества X на себя продолжается до гомоморфизма σ' алгебры Ли F в алгебру Ли $G^{(-)}$. Тогда для любого $w \in \mathfrak{W}$ имеем

$$\sigma'(w) = \begin{cases} \bar{w}, & \text{если } l(w) = 1, \\ [\sigma'(u), \sigma'(v)], & \text{если } w = u \circ v. \end{cases}$$

Лемма 5. *Если* w — *правильное неассоциативное слово в алфавите* X, *то*

$$\sigma'(w) = \bar{w} + f,$$

где f — *линейная комбинация слов длины* $l(w)$ *и* $\varkappa(f) \lhd \bar{w}$.

В самом деле, все ясно, если $l(w)=1$. Если $l(w)\geqslant 2$, то $w=u\circ v$, где u и v — правильные неассоциативные слова. В силу индуктивного предположения,

$$\sigma'(u)=\bar{u}+f \quad \text{и} \quad \sigma'(v)=\bar{v}+g,$$

где f и g обладают указанными в формулировке свойствами. Отсюда

$$\sigma'(w)=\bar{w}+(\bar{u}g+fg+f\bar{v}-\bar{v}\bar{u}-\bar{v}f-g\bar{u}-gf).$$

Ввиду правильности слова $\bar{w}$, имеем $\bar{w}>\bar{v}\bar{u}$. Но слова $\bar{w}$ и $\bar{v}\bar{u}$ имеют одинаковую длину и, следовательно, $\bar{v}\bar{u}\vartriangleleft\bar{w}$. Кроме того, из лемм 1 и 4 вытекает, что

$$\varkappa(\bar{u}g),\ \varkappa(fg),\ \varkappa(f\bar{v}),\ \varkappa(\bar{v}f),\ \varkappa(g\bar{u}),\ \varkappa(gf)\vartriangleleft\bar{w}.$$

Следовательно, лидер скобки младше $\bar{w}$, что и требовалось.

Лемма 6. *$\mathfrak{W}$ — база линейного пространства F.*

Для доказательства, ввиду леммы 3, достаточно установить, что множество $\mathfrak{W}$ линейно независимо. Но если

$$\lambda_1 w_1+\ldots+\lambda_n w_n=0,$$

где $0\neq\lambda_i\in P$ и w_i — различные элементы из $\mathfrak{W}$, то

$$\lambda_1\sigma'(w_1)+\ldots+\lambda_n\sigma'(w_n)=0.$$

Предложение 4 позволяет считать, что $\bar{w}_i\vartriangleleft\bar{w}_1$ для $i\geqslant 2$. Применяя лемму 5, получим $\lambda_1\bar{w}_1+g=0$, где $\varkappa(g)\vartriangleleft\bar{w}_1$. Разумеется, в свободной ассоциативной алгебре G это невозможно.

Лемма 7. *Идеал T обладает базой $\mathfrak{B}$ со следующими свойствами:*

(i) *если b', $b''\in\mathfrak{B}$ и $b'\neq b''$, то $\varkappa(\sigma'(b'))\neq\varkappa(\sigma'(b''))$;*

(ii) *если w — правильное ассоциативное слово в алфавите X и $l(w)\geqslant 2$, то $w=\varkappa(\sigma'(b))$ для некоторого $b\in\mathfrak{B}$.*

Для доказательства снова рассмотрим множество $\mathfrak{W}$ всех правильных неассоциативных слов в алфавите X. Если u — правильное ассоциативное слово в алфавите X и $l(u)\geqslant 2$, то в силу предложения 4, $u=\bar{\omega}(u)$ для некоторого $\omega(u)\in\mathfrak{W}$. Поскольку X — база линейного пространства L, то

$$\omega(u)=f+\lambda_1 x_1+\ldots+\lambda_m x_m,$$

где $f \in T$, $\lambda_i \in P$ и $x_i \in X$. Ввиду леммы 6 и предложения 4,

$$f = \mu_1 w_1 + \ldots + \mu_n w_n,$$

где $0 \neq \mu_j \in P$, $w_j \in \mathfrak{W}$ и $\bar{w}_j \lhd \bar{w}_1$ для $j \geqslant 2$. Поскольку $l(u) \geqslant 2$, то $l(w_1) \geqslant 2$. Поэтому, учитывая лемму 5, получаем

$$u = \overline{\omega(u)} = \varkappa(\sigma'(\omega(u))) =$$
$$= \varkappa(\mu_1 \sigma'(w_1) + \ldots + \mu_n \sigma'(w_n) + \lambda_1 x_1 + \ldots + \lambda_m x_m) =$$
$$= \bar{w}_1 = \varkappa(\mu_1 \sigma'(w_1) + \ldots + \mu_n \sigma'(w_n)) = \varkappa(\sigma'(f)).$$

Этим доказано, что каждое правильное ассоциативное слово длины $\geqslant 2$ представимо в форме $\varkappa(\sigma'(f))$ для некоторого $f \in T$. Следовательно, каждому такому слову w можно сопоставить элемент $f_w \in T$ так, что $\varkappa(\sigma'(f_w)) = w$. Пусть $\mathfrak{B}$ — совокупность выбранных элементов. Если

$$\lambda_1 b_1 + \ldots + \lambda_n b_n = 0,$$

где $0 \neq \lambda_i \in P$, $b_i \in \mathfrak{B}$ и $b_i \neq b_j$ при $i \neq j$, то можно считать, что

$$\varkappa(\sigma'(b_i)) \lhd \varkappa(\sigma'(b_1))$$

для $i \geqslant 2$. Тогда

$$\varkappa(\lambda_1 \sigma'(b_1) + \ldots + \lambda_n \sigma'(b_n)) = \varkappa(\sigma'(b_1)) \neq 0,$$

хотя

$$\lambda_1 \sigma'(b_1) + \ldots + \lambda_n \sigma'(b_n) = \sigma'(\lambda_1 b_1 + \ldots + \lambda_n b_n) = 0.$$

Полученное противоречие доказывает линейную независимость множества $\mathfrak{B}$. Если T' — линейная оболочка этого множества, то, очевидно, $T' \subseteq T$. Если $T' \neq T$, то рассмотрим множество

$$\{w \mid w = \varkappa(\sigma'(f)) \text{ для некоторого } f \in T \setminus T'\}$$

и, воспользовавшись леммой 2, выберем в нем самый младший элемент, скажем w_0. Поскольку X — база алгебры L, то $l(w_0) \geqslant 2$. В силу уже доказанного, $w_0 = \varkappa(\sigma'(b_0))$ для некоторого $b_0 \in \mathfrak{B}$. С другой стороны, $w_0 = \varkappa(\sigma'(f_0))$ для некоторого $f_0 \in T \setminus T'$. Тогда для некоторого $\lambda \in P$ имеем

$$\varkappa(\sigma'(f_0 - \lambda b_0)) \lhd w_0,$$

откуда $f_0 - \lambda b_0 \in T'$, а значит, $f_0 \in T'$, вопреки выбору элемента f_0. Таким обрааом, $\mathfrak{B}$ оказывается искомой базой.

Лемма 8. *$K=\sigma'(T)\,G$ — двусторонний идеал алгебры G.*

В самом деле, ясно, что K — правый идеал. Если $x\in X$, и $f\in T$, то

$$x\sigma'(f)=[x,\ \sigma'(f)]+\sigma'(f)\,x=\sigma'(x\circ f)+\sigma'(f)\,x\in K,$$

ибо $x\circ f\in T$, что и доказывает лемму.

Лемма 9. *Если $f\in F$ и $\sigma'(f)\in K$, то $f\in T$.*

Для доказательства допустим, что множество

$$\Xi=\{w\mid w=\varkappa(\sigma'(f)),\ \text{где}\ f\in F\setminus T\ \text{и}\ \sigma'(f)\in K\}$$

не пусто. Ввиду леммы 2, Ξ содержит самый младший элемент, скажем w_0. Пусть $w_0=\varkappa(\sigma'(f_0))$, где $f_0\in F\setminus T$ и $\sigma'(f_0)\in K$. Вспомнив, что $F=\sum\limits_{x\in X}Px+T$, и воспользовавшись леммой 7, запишем

$$f_0=\lambda_1x_1+\ldots+\lambda_mx_m+\mu_1b_1+\ldots+\mu_nb_n,$$

где $0\neq\lambda_i,\ \mu_j\in P$, $x_i\in X$, $b_j\in\mathfrak{B}$ и $\varkappa(\sigma'(b_j))\vartriangleleft\varkappa(\sigma'(b_1))$ для $j\geqslant 2$. Отсюда

$$w_0=\varkappa(\sigma'(f_0))=\varkappa(\sigma'(b_1))$$

и, следовательно,

$$\varkappa(\sigma'(f_0-\lambda b_1))\vartriangleleft w_0$$

для некоторого $\lambda\in P$. В силу выбора слова w_0,

$$\varkappa(\sigma'(f_0-\lambda b_1))\notin\Xi.$$

Но, $\sigma'(f_0-\lambda b_1)\in K$ и, следовательно, $f_0-\lambda b_1\in T$. Отсюда $f_0\in T$, что противоречит выбору элемента f_0.

Вернемся к доказательству теоремы. Учитывая лемму 8, рассмотрим фактор-алгебру $A=G/K$ и обозначим через τ естественный гомоморфизм алгебры G на A. Поскольку $T\sigma'\tau=0$, то, в силу предложения II.1.3, $\sigma'\tau=\pi\sigma$ для некоторого $\sigma\colon L\to A^{(-)}$ (рис. 4). Если $f\in F$ и $f\pi\sigma=0$, то $f\sigma'\tau=0$ и, следовательно, $\sigma'(f)\in K$. По лемме 9, $f\in T$, откуда $f\pi=0$, а значит, σ — вложение. Пусть теперь B — ассоциативная алгебра с единицей над полем P и $\varphi\colon L\to B^{(-)}$ — гомоморфизм алгебр Ли. Поскольку G — свободная ассоциативная алгебра с единицей над P, то существует гомоморфизм ψ': $G\to B$ такой, что $x\psi'=x\pi\varphi$ для всех $x\in X$. Поскольку $x\sigma'=x$, то $x\sigma'\psi'=x\pi\varphi$ для всех $x\in X$ и, по следствию

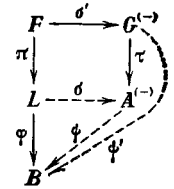


Рис. 4.

предложения II.1.5, $\sigma'\psi' = \pi\varphi$. Отсюда $T\sigma'\psi' = T\pi\varphi = 0$, т. е. $\sigma'(T) \subseteq \operatorname{Ker}\psi'$. Поэтому

$$K = \sigma'(T)\, G \subseteq \operatorname{Ker}\psi'$$

и, по предложению II.1.3, $\psi' = \tau\psi$ для некоторого ψ: $A \to B$. Таким образом,

$$\pi\sigma\psi = \sigma'\tau\psi = \sigma'\psi' = \pi\varphi,$$

откуда $\sigma\psi = \varphi$, поскольку π — наложение.

Упражнения

1. Если $x_1 \ldots x_n$ — слово в линейно упорядоченном алфавите X, $x_1 \geqslant x_2 \geqslant \ldots \geqslant x_n$ и $x_1 \neq x_n$, то $x_1 \ldots x_n$ — правильное ассоциативное слово.

2. Выяснить, при каких условиях произведение двух правильных ассоциативных слов является правильным ассоциативным словом.

3. Если w — правильное неассоциативное, а u — правильное ассоциативное слово в алфавите X, $x \in X$ и $\tilde{w} = ux^k$, то $w = (\ldots(\underbrace{(u \circ x) \circ x) \ldots \circ x}_{k \text{ раз}}) \circ x$.

4. Свободная алгебра Ли над коммутативным ассоциативным кольцом с единицей обладает универсальной обертывающей. Замечание: В общем случае этот результат неверен (см. Ширшов А. И. — УМН, 1953, **8**, № 5, с. 173—175).

5. Линейное отображение d ассоциативной алгебры A в себя называется *дифференцированием*, если $d(ab) = d(a)\, b + a\, d(b)$ для любых $a, b \in A$. Доказать, что дифференцирования образуют алгебру Ли относительно операции $[\ ,\ ]$.

6. Матрицы второго порядка с нулевым следом образуют алгебру Ли относительно операции $[\ ,\ ]$. Указать базу ее универсальной обертывающей.

7. Доказать, что универсальная обертывающая алгебры Ли с нулевым умножением изоморфна алгебре многочленов.

8. Доказать, что алгебра Ли трехмерных векторов с векторным умножением вкладывается в алгебру $\mathbf{K}^{(-)}$, где $\mathbf{K}$ — тело кватернионов.

§ 5. Нильпотентные алгебры Ли и нильпотентные группы

Пусть L — кольцо Ли, операцию умножения в котором будем обозначать символом $\circ$. По индукции определим n-е *каноническое произведение*

$$(a_1, \ldots, a_n) = (a_1, \ldots, a_{n-1}) \circ a_n.$$

Кольцо L называется *нильпотентным индекса* n, если

$$(a_1, \ldots, a_n) = 0$$

для любых $a_i \in L$. Заметим, что, как и ступень нильпотентности группы, индекс нильпотентности кольца Ли не определяется однозначно.

Предложение 1. *Если кольцо Ли L нильпотентно индекса n, то при любой расстановке скобок произведение n элементов на L обращается в нуль.*

Этот результат является следствием более общего утверждения:

Предложение 2. *Пусть L — кольцо Ли и L^m — множество целочисленных линейных комбинаций m-х канонических произведений из L. Тогда при любой расстановке скобок произведение m элементов из L лежит в L^m.*

Доказательство. Предварительно установим следующую лемму:

Лемма. $L^i \circ L^j \subseteq L^{i+j}$ *при любых* i *и* j.

В самом деле, при $j=1$ это вытекает из определения. Если же $j \geqslant 2$, то, используя индуктивное предположение, для любых $a \in L^i$, $b \in L^{j-1}$ и $c \in L$ получаем

$$a \circ (b \circ c) = (c \circ b) \circ a = -(b \circ a) \circ c - (a \circ c) \circ b = \\ = (a \circ b) \circ c - (a \circ c) \circ b \in L^{i+j-1} \circ L + L^{i+1} \circ L^{j-1} \subseteq L^{i+j}.$$

Утверждение предложения тривиально при $m=2$. Если же $m \geqslant 2$, то, ввиду леммы и индуктивного предположения, при $i+j=m$, получаем

$$u \circ v \in L^i \circ L^j \subseteq L^m,$$

где u и v — произведения соответственно i и j элементов из L с произвольной расстановкой скобок.

Теорема 1. *Пусть G — нильпотентная группа ступени n и*

$$G = G_1 \supseteq G_2 \supseteq \ldots \supseteq G_n \supseteq G_{n+1} = \{1\}$$

— ее нижний центральный ряд. Внешняя прямая сумма абелевых групп

$$L = G/G_2 \oplus G_2/G_3 \oplus \ldots \oplus G_{n-1}/G_n \oplus G_n$$

оказывается нильпотентной алгеброй Ли индекса n, если произведение $[a]_i \circ [b]_j$, где $[a]_i \in G_i/G_{i+1}$ и $[b]_j \in G_j/G_{j+1}$, определены равенством

$$[a]_i \circ [b]_j = \begin{cases} [a, b]_{i+j}, & \text{если } i+j \leqslant n, \\ [1]_n, & \text{если } i+j > n. \end{cases}$$

Доказательство. Убедимся, что умножение определено корректно. В самом деле, если $[a]_l=[c]_i$ и $[b]_j=[d]_j$, то $a=cu$ и $b=dv$, где $u\in G_{i+1}$ и $v\in G_{j+1}$. В силу предложений 2.1(б), 2.1(в)

$$[a, b]=[cu, dv]=[c, dv][c, dv, u][u, dv]=$$
$$=[c, v][c, d][c, d, v][c, dv, u][u, v][u, d][u, d, v].$$

Учитывая предложение 2.3, получаем

$$[c, d]\in G_{i+j},\ [c, v]\in G_{i+j+1},\ [c, d]^{-1}[c, v][c, d]\in G_{i+j+1},$$
$$[c, d, v],\ [c, dv, u],\ [u, v],\ [u, d],\ [u, d, v]\in G_{i+j+1}.$$

Следовательно,

$$[c, d]^{-1}[a, b]=$$
$$=([c, d]^{-1}[c, v][c, d])[c, d, v][c, dv, u][u, v][u, d][u, d, v]\in$$
$$\in G_{i+j+1},$$

т. е.

$$[[a, b]]_{i+j}=[[c, d]]_{i+j},$$

что и требовалось. Для проверки дистрибутивности, очевидно, достаточно установить справедливость включения

$$[a, c][b, c][ab, c]^{-1}\in G_{k+l+1}$$

для любых $a, b\in G_k$ и $c\in G_l$. Оно, в свою очередь, является следствием следующих соотношений, вытекающих из предложений 2.1(б) и 2.3:

$$[ab, c]=[a, c][a, c, b][b, c]$$

и

$$[a, c][b, c][ab, c]^{-1}=[a, c][b, c][b, c]^{-1}[a, c, b]^{-1}[a, c]^{-1}=$$
$$=[a, c][a, c, b]^{-1}[a, c]^{-1}\in G_{k+l+1}.$$

Если $a_i\in G_i$, $i=0, 1, \ldots, n$ и

$$([a_0], [a_1], \ldots, [a_n])\circ([a_0], [a_1], \ldots, [a_n])=$$
$$=([b_0], [b_1], \ldots, [b_n]),$$

то

$$b_k=\prod_{i+j=k}[a_i, a_j]\cdot u,$$

где $u\in G_{k+1}$. Поскольку $[a_i, a_i]=1$ и, по предложению 2.1(а), $[a_i, a_j][a_j, a_i]=1$, то $b_k=u\in G_{k+1}$ для всех k. Остается вспомнить, что $([1], [1], \ldots, [1])$ — нуль кольца L. На-

конец, для доказательства тождества Якоби достаточно для любых $a_i, b_i, c_i \in G_i$, $i = 0, 1, \ldots, n$, установить включение

$$\prod_{k+l+m=i} [[a_k, b_l], c_m] \cdot \prod_{k+l+m=i} [[b_l, c_m], a_k] \cdot \prod_{k+l+m=i} [[c_m, a_k], b_l] \in G_{i+1},$$

которое, как легко видеть, является следствием включения

$$[[a, b], c][[b, c], a][[c, a], b] \in G_{k+l+m+1}$$

для любых $a \in G_k$, $b \in G_l$ и $c \in G_m$. Для доказательства последнего, воспользовавшись предложением 2.1(в), запишем

$$[[a, b], c^a] = [[a, b], c[c, a]] = \\ = [[a, b], [c, a]][[a, b], c][[a, b], c, [c, a]],$$

где $c^a = a^{-1}ca$. Аналогично, имеют место равенства

$$[[b, c], a^b] = [[b, c], [a, b]][[b, c], a][[b, c], a, [a, b]]$$

и

$$[[c, a], b^c] = [[c, a], [b, c]][[c, a], b][[c, a], b, [b, c]].$$

В силу предложения 2.3, коммутаторы $[[a, b], [c, a]]$, $[[a, b], c, [c, a]]$, $[[b, c], [a, b]]$, $[[b, c], a, [a, b]]$, $[[c, a], [b, c]]$ и $[[c, a], b, [b, c]]$ принадлежат $G_{k+l+m+1}$. Поскольку $G_{k+l+m+1}$ — нормальная подгруппа в G_{k+l+m}, то, перемножая выписанные выше равенства и принимая во внимание предложение 2.1(д), получаем требуемое включение. Нильпотентность кольца L является непосредственным следствием предложения 2.3.

Упражнения

1. Доказать, что нильпотентная алгебра Ли может быть вложена в алгебру Ли, возникающую из нильпотентной ассоциативной алгебры.
2. Доказать, что кольцо Ли, соответствующее прямому произведению нильпотентных групп, изоморфно прямому произведению колец Ли, соответствующих сомножителям.
3. Построить кольцо Ли, соответствующее группе кватернионов.

ЛИТЕРАТУРА

Адян С. И. Проблема Бернсайда и тождества в группах.—М.: Наука, 1975.

Бахтурин Ю. А. (Bachturin J. A.) Lectures on Lie algebras.—Berlin: Akademie-Verlag, 1978.

Борель А. Линейные алгебраические группы.—М.: Мир, 1972.

Бурбаки Н. Группы и алгебры Ли. Гл. I—III.—М.: Мир, 1976. Гл. IV—VI.—М.: Мир, 1972. Гл. VII—VIII—М.: Мир, 1978.

Винберг Э. Б., Онищик А. Л. Семинар по алгебраическим группам и группам Ли.—М.: Изд-во МГУ, 1969.

Вовси С. М. (Vovsi S. M.) Triangular products of group representations and their applications. — Boston; Basel; Stuttgart: Birkhäuser, 1981.
Горчаков Ю. М. Группы с конечными классами сопряженных элементов. — М.: Наука, 1978.
Гото М., Гроссханс Ф. Полупростые алгебры Ли. — М.: Мир, 1981.
Джекобсон Н. Алгебры Ли. — М.: Мир, 1964.
Диксмье Ж. Универсальные обертывающие алгебры. — М.: Мир, 1978.
Жевлаков К. А., Слинько А. М., Шестаков И. П., Ширшов А. И. Кольца, близкие к ассоциативным. — М.: Наука, 1978. .
Капланский И. Алгебры Ли и локально компактные группы. — М.: Мир, 1974.
Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1982.
Кон П. Универсальная алгебра. — М.: Мир, 1968.
Курош А. Г. Теория групп. — М.: Наука, 1967.
Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр. — М.: Наука, 1969.
Линдон Р., Шупп П. Комбинаторная теория групп. — М.: Мир, 1980.
Магнус В., Каррас К., Солитэр Д. Комбинаторная теория групп. — М.: Наука, 1974.
Мерзляков Ю. И. Рациональные группы. — М.: Наука, 1980.
Наймарк М. А. Теория представлений групп. — М.: Наука, 1976.
Неймаи Х. Многообразия групп. — М.: Мир, 1969.
Плоткин Б. И. Группы автоморфизмов алгебраических систем. — М.: Наука, 1966.
Постников М. М. Группы и алгебры Ли. — М.: Наука, 1982.
Серр Ж.-П. Алгебры Ли и группы Ли. — М.: Мир, 1969.
Судзуки М. Строение группы и строение структуры ее подгрупп. — М.: ИЛ, 1960.
Супруненко Д. А. Разрешимые и нильпотентные линейные группы. — Минск: Изд-во БГУ, 1958.
Супруненко Л. А. Группы матриц. — М.: Наука, 1972.
Теория алгебр Ли. Топология групп Ли. Семинар «Софус Ли»: Сб. статей. — М.: ИЛ, 1962.
Холл М. Теория групп. — М.: ИЛ, 1962.
Черников С. Н. Группы с заданными свойствами систем подгрупп. — М.: Наука, 1980.
Шевалле К. Теория групп Ли. — М.: ИЛ, 1948.
Шеметков Л. А. Формации конечных групп. — М.: Наука, 1978.
Шмидт О. Ю. Абстрактная теория групп. — М.; Л.: ГТТИ, 1933.
Serre J.-P. Arbres, amalgames, SL_2. — Astérisque, 1977.
Warfield R. B. Nilpotent groups. — Berlin; Heidelberg; N. Y.: Springer-Verlag, 1976 (Lect. Notes Math., v. 513).
Wehrfritz B.A.P. Infinite linear groups. An account of the group-theoretic properties of infinite groups of matrices. — Berlin: Springer-Verlag, 1973.

Литературу по топологическим и упорядоченным группам см. в гл. VII, по абелевым группам и групповым кольцам — в гл. IV.

ГЛАВА VI

ПОЛЯ И ТЕЛА

В этой главе доказывается теорема о строении расширений данного поля, описываются конечные поля и приводится основная теорема теории Галуа. Далее излагается описание конечномерных алгебр с делением над полем действительных чисел и доказывается теорема о коммутативности конечных тел.

§ 1. Строение полей

Напомним, что *полем* называется коммутативное и ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратим. Примерами полей служат действительные и комплексные числа с обычными операциями и кольца вычетов по простому модулю. Совокупность рациональных функций над любыми полями и фактор-кольцо кольца многочленов над полем по идеалу, порожденному неприводимым многочленом, также оказываются полями.

Поле $\overline{P}$ называется *расширением* поля P, если P — подполе в $\overline{P}$. Расширение $\overline{P}$ называется *алгебраическим*, если для всякого $\gamma \in \overline{P}$ найдется ненулевой многочлен f над полем P такой, что $f(\gamma) = 0$.

Предложение 1. *Если $\overline{P}$ — расширение поля P, R — подкольцо кольца $\overline{P}$, содержащее P, и R конечномерно как линейное пространство над P, то все элементы, принадлежащие R, алгебраичны над P.*

Доказательство. Пусть $\gamma \in R$. Поскольку R конечномерно над P, то при достаточно большом n множество $\{1, \gamma, \gamma^2, \ldots, \gamma^n\}$ оказывается линейно зависимым. Следовательно,

$$\gamma^m + \alpha_1 \gamma^{m-1} + \ldots + \alpha_m = 0$$

для некоторых $\alpha_1, \ldots, \alpha_m \in P$ для подходящего $m \leqslant n$. Таким образом, γ служит корнем многочлена $f = x^m + \alpha_1 x^{m-1} + \ldots + \alpha_m$ над P, т. е. γ алгебраичен над P.

Предложение 2. *Если P' — алгебраическое расширение поля P, а P'' — алгебраическое расширение поля P', то P'' — алгебраическое расширение поля P.*

Доказательство. Если $\gamma \in P''$, то

$$\gamma^n + \beta_1 \gamma^{n-1} + \ldots + \beta_n = 0 \qquad (*)$$

для некоторых $\beta_1, \ldots, \beta_n \in P'$. Для каждого из этих β_i найдутся такие $\alpha_{i1}, \ldots, \alpha_{im_i} \in P$, что

$$\beta_i^{m_i} + \alpha_{i1}\beta_i^{m_i-1} + \ldots + \alpha_{im_i} = 0. \qquad (**)$$

Рассматривая поле P'' как линейное пространство над полем P, выделим в нем линейное подпространство R, натянутое на множество произведений

$$\{\beta_1^{s_1}\beta_2^{s_2} \ldots \beta_n^{s_n}\gamma^s \mid 0 \leqslant s_i < m_i, \quad 0 \leqslant s < n\}.$$

Учитывая равенства (*) и (**), нетрудно показать, что R — подкольцо. Поскольку R конечномерно над P, то, согласно предложению 1, все его элементы и, в частности, γ алгебраичны над P.

Предложение 3. *Если P и P' — поля, R — подкольцо поля P, U — подполе поля P, порожденное кольцом R и φ: $R \to P'$ — гомоморфное вложение, то существует такое гомоморфное вложение ψ поля U в P, что $\psi(r) = \varphi(r)$ для всех $r \in R$.*

Доказательство. Простые вычисления показывают, что любой элемент из U представляется в форме rs^{-1}, где $r, s \in R$ и $s \neq 0$. Для любого $rs^{-1} \in U$ положим

$$\psi(rs^{-1}) = \varphi(r)\varphi(s)^{-1}.$$

Это определение корректно, поскольку $s \neq 0$ влечет $\varphi(s) \neq 0$, а из $rs^{-1} = r_1 s_1^{-1}$ вытекает $rs_1 = r_1 s$ и, следовательно,

$$\varphi(r)\varphi(s_1) = \varphi(r_1)\varphi(s),$$

т. е.

$$\varphi(r)\varphi(s)^{-1} = \varphi(r_1)\varphi(s_1)^{-1}.$$

После этого стандартные вычисления показывают, что ψ является гомоморфным вложением с нужным свойством.

Поле P называется *алгебраически замкнутым*, если всякий многочлен над P имеет корень, принадлежащий P. Это равносильно разложимости на линейные множители всякого отличного от константы многочлена над P.

Теорема 1. *Для всякого поля P существует алгебраически замкнутое алгебраическое расширение $\overline{P}$. При этом, каково бы ни было алгебраически замкнутое алгебраическое расширение $\overline{P}'$ поля P, существует изоморфизм полей φ: $\overline{P} \to \overline{P}'$ такой, что $\varphi(a) = a$ для всех $a \in P$* (т. е. $\overline{P}$ определяется однозначно с точностью до изоморфизма над P).

Доказательство. Сначала установим несколько лемм.

Лемма 1. *Пусть P — произвольное поле, $P[x]$ — кольцо многочленов от одного неизвестного над P, I — идеал кольца $P[x]$, порожденный неприводимым многочленом g, $\overline{P} = P[x]/I$. Тогда $\overline{P}$ — поле, естественный гомоморфизм π: $P[x] \to \overline{P}$ осуществляет гомоморфное вложение поля P в $\overline{P}$ и $\pi(x)$ служит корнем многочлена g* (точнее, многочлена, полученного из g заменой его коэффициентов на их образы при вложении π). *При этом $\overline{P}$ алгебраично над P.*

Действительно, если $\pi(f)$ — ненулевой элемент кольца $\overline{P}$, то f не делится на g и, ввиду неприводимости многочлена g, НОД$(f, g) = 1$. Поэтому $fu + gv = 1$ для некоторых $u, v \in P[x]$. Поскольку $gv \in I$, отсюда вытекает

$$\pi(f)\pi(u) = \pi(1) - \pi(gv) = \pi(1),$$

что доказывает обратимость элемента $\pi(f)$. Следовательно, $\overline{P}$ — поле. Если $\alpha, \beta \in P$ и $\alpha \neq \beta$, то $\alpha - \beta$ не делится на g, откуда $\pi(\alpha) \neq \pi(\beta)$. Если, далее,

$$g = x^n + \alpha_1 x^{n-1} + \ldots + \alpha_n,$$

то, отождествляя $\pi(\alpha_i)$ с α_i, получаем

$$0 = \pi(0) = \pi(g) = \pi(x)^n + \pi(\alpha_1)\pi(x)^{n-1} + \ldots + \pi(\alpha_n) = \\ = \pi(x)^n + \alpha_1\pi(x)^{n-1} + \ldots + \alpha_n.$$

Таким образом, $\pi(x)$ оказывается корнем многочлена g. Наконец, $\overline{P}$ как линейное пространство над P порождается элементами $1, \pi(x), \pi(x^2), \ldots, \pi(x^{n-1})$. Следовательно, $\overline{P}$ конечномерно над P и, согласно предложению 1, алгебраично.

Лемма 2. *Алгебраическое расширение P' алгебраически замкнутого поля P совпадает с P.*

Действительно, если $\gamma \in P'$, то $f(\gamma) = 0$ для некоторого многочлена f над P. Можно считать, что f непри-

водим над P. Но из алгебраической замкнутости поля P вытекает, что f линеен, и, следовательно, $\gamma \in P$.

Лемма 3. *Для всякого поля P существует такое алгебраическое расширение P', что всякий отличный от константы многочлен над P имеет корень в поле P'.*

Для доказательства превратим множество всех неприводимых многочленов над полем P во вполне упорядоченное множество, скажем, $\{f_\alpha \mid \alpha < \Omega\}$. Положим $P_0 = P$ и допустим, что для всех $\beta < \alpha$ построены алгебраические расширения P_β поля P так, что f_β имеет корень в поле P_β и $P_{\beta'}$ является подполем в $P_{\beta''}$, если $\beta' < \beta'' < \alpha$. Рассмотрим поле $\tilde{P} = \bigcup_{\beta<\alpha} P_\beta$. Если f_α имеет корень в $\tilde{P}$, то положим $P_\alpha = \tilde{P}$. В противном случае запишем $f_\alpha = g_1 \dots g_m$, где g_i—неприводимые многочлены над $\tilde{P}$, и рассмотрим фактор-кольцо $P_\alpha = \tilde{P}[x]/(g_1)$, где (g_1)—идеал в $\tilde{P}[x]$, порожденный многочленом g_1. Из леммы 1 и предложения 2 вытекает, что P_α—поле, являющееся алгебраическим расширением поля $\tilde{P}$ и содержащее корень многочлена g_1, а значит, и корень многочлена f_α. Ясно, что $P' = \bigcup_{\alpha<\Omega} P_\alpha$ является искомым расширением поля P.

Возвращаясь к доказательству теоремы, положим $P^{(0)} = P$ и допустим, что построены алгебраические расширения $P^{(0)}, P^{(1)}, \dots, P^{(m-1)}$ поля P так, что всякий многочлен над $P^{(i-1)}$ имеет корень в $P^{(i)}$. Воспользовавшись леммой 3, построим алгебраическое расширение $P^{(m)}$ поля $P^{(m-1)}$, в котором каждый многочлен над $P^{(m-1)}$ имеет корень. По предложению 2, $P^{(m)}$ алгебраично над P. Легко видеть, что $\overline{P} = \bigcup_{0\leqslant i<\infty} P^{(i)}$ оказывается алгебраически замкнутым алгебраическим расширением поля P. Допустим теперь, что $\overline{P}'$—произвольное алгебраически замкнутое алгебраическое расширение поля P. Рассмотрим множество $\mathfrak{P}$ всех пар (U, φ), где U—подполе поля $\overline{P}$, содержащее P, а φ—гомоморфное вложение поля U в поле $\overline{P}'$, причем $\varphi(\alpha) = \alpha$ для всех $\alpha \in P$. Множество $\mathfrak{P}$ непусто, ибо $(P, 1_P) \in \mathfrak{P}$. Положим

$$(U', \varphi') \leqslant (U'', \varphi''),$$

если $U' \subseteq U''$ и $\varphi''(u) = \varphi'(u)$ для всех $u \in U'$. Легко проверяется, что это определение превращает $\mathfrak{P}$ в частично упорядоченное множество. Если $\{(U_\varkappa, \varphi_\varkappa)\}$—возрастаю-

щая цепь из $\mathfrak{P}$, то рассмотрим пару $(\overline{U}, \overline{\varphi})$, где $\overline{U} = \bigcup_{\varkappa} U_\varkappa$ и $\overline{\varphi}(u) = \varphi_\varkappa(u)$, если $u \in U_\varkappa$. Легко проверить, что $\overline{\varphi}(u)$ не зависит от выбора $\varkappa$ и является гомоморфным вложением поля $\overline{U}$ в $\overline{P}^0$. При этом, $(U_\varkappa, \varphi_\varkappa) \leqslant (\overline{U}, \overline{\varphi})$ для всех $\varkappa$. Следовательно, верхний конус любой цепи из $\mathfrak{P}$ не пуст. По лемме Куратовского — Цорна (теорема I.1.1) частично упорядоченное множество $\mathfrak{P}$ содержит максимальный элемент $(\overline{U}, \overline{\varphi})$. Если $\overline{U} \neq \overline{P}$, то выберем $\gamma \in \overline{P} \setminus \overline{U}$. Поскольку γ является корнем некоторого многочлена над P и $P \subseteq \overline{U}$, то можно считать γ корнем некоторого многочлена f над $\overline{U}$. При этом многочлен f можно выбрать неприводимым над $\overline{U}$. Рассмотрим многочлен $\overline{f} = \overline{\varphi}(f)$, т. е. многочлен над $\overline{P}'$, коэффициентами которого служат образы коэффициентов многочлена f при отображении $\overline{\varphi}$. Поскольку φ — вложение, то $\overline{f}$ неприводим над полем $\operatorname{Im}\overline{\varphi}$. В силу алгебраической замкнутости поля $\overline{P}'$, $\overline{f}(\gamma') = 0$ для некоторого $\gamma' \in \overline{P}'$. Обозначим через R подкольцо поля $\overline{P}$, порожденное полем $\overline{U}$ и элементом γ. Если $r \in R$, то

$$r = u_0\gamma^n + u_1\gamma^{n-1} + \ldots + u_n,$$

где $u_i \in \overline{U}$. Положим

$$\varphi(r) = \overline{\varphi}(u_0)\,\gamma'^n + \overline{\varphi}(u_1)\,\gamma'^{n-1} + \ldots + \overline{\varphi}(u_n).$$

Если

$$g = u_0x^n + u_1x^{n-1} + \ldots + u_n$$

— многочлен над полем $\overline{U}$ и $g(\gamma) = 0$, то, поскольку f неприводим над U, имеем $g = fh$ для некоторого многочлена h над U. Поскольку $\overline{f}(\gamma') = 0$, то

$$\varphi(g(\gamma)) = \overline{\varphi}(g)(\gamma') = \overline{\varphi}(f)(\gamma')\,\overline{\varphi}(h)(\gamma') = \overline{f}(\gamma')\,\overline{\varphi}(h)(\gamma') = 0.$$

Этим доказано, что φ — корректно определенное отображение кольца R в поле $\overline{P}'$. Если $\varphi(r) = 0$, то γ' оказывается корнем многочлена

$$\overline{g}(x) = \varphi(u_0)\,x^n + \varphi(u_1)\,x^{n-1} + \ldots + \varphi(u_n)$$

над полем $\operatorname{Im}\varphi$. В силу неприводимости многочлена $\overline{f}$ над $\operatorname{Im}\varphi$, отсюда вытекает, что $\overline{g} = \overline{f}\,\overline{h}$ для некоторого мно-

гочлена $\bar{h}$ над $\operatorname{Im}\varphi$. Отсюда

$$r = g(\gamma) = f(\gamma)\,h(\gamma) = 0.$$

Таким образом, $\varphi(r) = 0$ влечет $r = 0$. Нетрудно проверить, что φ — кольцевой гомоморфизм. Следовательно, φ — гомоморфное вложение кольца R в поле $\overline{P}'$. Согласно предложению 3, φ может быть продолжено до гомоморфного вложения ψ в поле $\overline{P}'$ подполя $V \subseteq \overline{P}$, порожденного кольцом R. Тогда $(V, \psi) \in \mathfrak{P}$ и $(\overline{U}, \overline{\varphi}) \lneq (V, \psi)$, вопреки выбору пары $(\overline{U}, \overline{\varphi})$. Таким образом, $\overline{U} = \overline{P}$, т. е. $\overline{\varphi}$ — гомоморфное вложение поля $\overline{P}$ в поле $\overline{P}'$. Поле $\operatorname{Im}\overline{\varphi}$, будучи изоморфным полю $\overline{P}$, алгебраически замкнуто, а поле $\overline{P}'$, будучи алгебраическим расширением поля P, является алгебраическим расширением поля $\operatorname{Im}\overline{\varphi}$. Согласно лемме 2, $\operatorname{Im}\overline{\varphi} = \overline{P}'$, что и завершает доказательство.

Теорема 2 (Штейниц). *Всякое расширение P' поля P изоморфно алгебраическому расширению или самого поля P, или поля рациональных функций над ним.*

Доказательство. Подмножество M поля P' назовем *алгебраически независимым*, если $f(a_1, \ldots, a_n) \neq 0$ для любых $a_1, \ldots, a_n \in M$ и любого ненулевого многочлена f от n неизвестных над P. Поскольку алгебраическая независимость одноэлементного подмножества $\{a\}$ означает неалгебраичность элемента a над P, то отсутствие в поле P' алгебраически независимых подмножеств означает его алгебраичность над P. В противном случае, применяя лемму Куратовского—Цорна (теорема I.1.2) к частично упорядоченному множеству алгебраически независимых подмножеств из P', найдем в нем максимальный элемент M. Пусть R — алгебра многочленов над полем P от множества неизвестных M. По следствию предложения II.3.5, R — свободная ассоциативная коммутативная P-алгебра с единицей со свободной порождающей системой M. Поэтому естественное отображение множества M в поле P' продолжается до гомоморфизма φ кольца R в поле P'. Ввиду алгебраической независимости множества M, φ оказывается вложением и, согласно предложению 3, продолжается до гомоморфного вложения поля Q рациональных функций над P от множества неизвестных M в поле P'. Отождествим Q с $\operatorname{Im}\psi$ и возьмем $\gamma \in P' \setminus Q$. В силу вы-

бора множества M, множество $M \cup \{\gamma\}$ алгебраически независимым не является. Следовательно, $f(\gamma, a_1, \ldots, a_n) = 0$ для некоторого ненулевого многочлена f от $n+1$ неизвестного над P и подходящих $a_1, \ldots, a_n \in M$. При этом в f имеется одночлен с ненулевым коэффициентом, содержащий γ. Но тогда простые вычисления показывают, что γ является корнем многочлена с коэффициентом из поля Q, т. е. алгебраичен над Q. Таким образом, P' — алгебраическое расширение поля Q, что и требовалось.

Теорема 3. (а) *Порядок любого конечного поля равен* p^n, *где* p — *простое число.* (б) *Для любого числа* $q = p^n$, *где* p — *простое число, существует поле порядка* q. (в) *Мультипликативная группа любого конечного поля циклическая.* (г) *Конечные поля одного и того же порядка изоморфны.*

Доказательство. (а) Если P — конечное поле, характеристики p (напомним, что p — простое число), то элементы 0, 1, 2, ..., $p-1$ образуют подполе P_0, изоморфное поле вычетов по модулю p. Ясно, что P — конечномерное линейное пространство над P_0 и если n — размерность этого пространства, то $|P| = p^n$.

(б) Пусть P_0 — поле вычетов по модулю p. По теореме 1 существует алгебраически замкнутое алгебраическое расширение $\overline{P}$ поля P_0. Убедимся, что для любых $a, b \in \overline{P}$ и любого натурального k имеет место

$$(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k}. \qquad (*)$$

Действительно, любой биномиальный коэффициент

$$C_p^i = \frac{p(p-1)\ldots(p-i+1)}{1 \cdot 2 \ldots (p-1)}$$

делится на p, ибо p взаимно просто с любым числом, стоящим в знаменателе. Отсюда $C_p^i a^{p-i} b^i = 0$ и, следовательно,

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} C_p^i a^{p-i} b^i + b^p = a^p + b^p.$$

Если $k > 1$, то, учитывая индуктивное предположение, получим

$$(a+b)^{p^k} = ((a+b)^{p^{k-1}})^p = (a^{p^{k-1}} + b^{p^{k-1}})^p = a^{p^k} + b^{p^k}.$$

Если $p = 2$, то $b = -b$ и $b^{p^k} = -b^{p^k}$. Если же $p > 2$, то $(-b)^{p^k} = -b^{p^k}$, откуда

$$(a-b)^{p^k} = a^{p^k} + (-b)^{p^k} = a^{p^k} - b^{p^k}.$$

Далее заметим, что многочлен $x^q - x$ над полем $\overline{P}$ не имеет кратных корней. В самом деле, кратные корни этого многочлена отличны от 0 и должны быть кратными корнями многочлена $x^{q-1} - 1$. Однако этот многочлен кратных корней не имеет, ибо единственным корнем его производной $(q-1)\,x^{q-2}$ служит 0, не являющийся корнем для $x^{q-1} - 1$. Таким образом, обозначив через P множество всех корней многочлена $x^q - x$, принадлежащих $\overline{P}$, и принимая во внимание алгебраическую замкнутость поля $\overline{P}$, будем иметь $|P| = q$. Далее, если $a, b \in P$, то, используя (*), получаем $0, 1 \in P$,

$$(a \pm b)^q - (a \pm b) = (a^q - a) \pm (b^q - b) = 0,$$
$$(ab)^q - ab = a^q b^q - ab = ab - ab = 0$$

и если $b \neq 0$, то

$$\left(\frac{a}{b}\right)^q - \frac{a}{b} = \frac{a^q}{b^q} - \frac{a}{b} = \frac{a}{b} - \frac{a}{b} = 0,$$

откуда следует, что P — поле.

(в) Пусть P' — произвольное конечное поле. В силу (а), $|P'| = q = p^n$, где p — простое число. Допустим, что мультипликативная группа G этого поля не является циклической. Из описания строения конечных абелевых групп (ЭА, с. 232) вытекает, что G содержит пару примарных циклических слагаемых, отвечающих одному и тому же простому числу r. Если r^s и r^t — порядки этих слагаемых, то порожденная ими подгруппа H содержит r^{s+t} элементов. Если $s \leqslant t$, то каждый из этих элементов является корнем многочлена $x^{r^t} - 1$ над полем P'. Таким образом, многочлен степени r^t имеет в поле P' более, чем r^t, различных корней. Полученное противоречие доказывает, что G — циклическая группа.

(г) Пусть P' — конечное поле порядка $q = p^n$. Согласно (в)

$$P' = \{0, 1, g, g^2, \ldots, g^{q-2}\}$$

для некоторого $g \in P'$. Далее, характеристика поля P', очевидно, равна p. Следовательно, P' содержит подполе P_0, изоморфное полю вычетов по модулю p. Разумеется, можно рассматривать P' как линейное пространство над P_0. Допустим, что система

$$\mathscr{E} = \{1, g, g^2, \ldots, g^{m-1}\}$$

линейно независима над P_0, а $\mathfrak{B} \cup \{g^m\}$ линейно зависима. Тогда g^m принадлежит линейной оболочке L системы $\mathfrak{B}$ над P_0. Если $g^{m+i} \in L$, то

$$g^{m+i+1} = gg^{m+i} \in gL \subseteq P_0 g^m + L \subseteq L.$$

Таким образом, $P' = L$, т. е. $\mathfrak{B}$ оказывается базой поля P' над P_0. Поскольку $|P_0| = p$, то $|L| = p^m$ и, следовательно, $m = n$. Таким образом, поле P' содержит такой элемент g, что система

$$\{1, g, g^2, \ldots, g^{n-1}\}$$

служит базой поля P' над P_0. Поскольку этот вывод справедлив для любого поля порядка q, то построенное при доказательстве утверждения (б) поле P также обладает базой

$$\{1, a, a^2, \ldots, a^{n-1}\}$$

для подходящего $a \in P$. Легко видеть, что отображение φ, определяемое равенством

$$\varphi(w) = \alpha_0 + \alpha_1 g + \ldots + \alpha_{n-1} g^{n-1},$$

если

$$w = \alpha_0 + \alpha_1 a + \ldots + \alpha_{n-1} a^{n-1},$$

где $\alpha_i \in P_0$, оказывается изоморфизмом поля P на поле P'.

Применяя (в) к полю вычетов по модулю p, получаем:

Следствие. *Для любого простого числа p существует такое целое число k, что $2 \leqslant k < p$ и множество остатков от деления чисел k, k^2, ..., k^{p-1} на p совпадает с множеством* $\{1, 2, \ldots, p-1\}$.

Упражнения

1. Конечно порожденная коммутативная алгебраическая алгебра с единицей над полем P имеет конечную размерность (алгебра над полем P называется *алгебраической*, если все ее элементы являются корнями многочленов над P).

2. Пусть P — конечное расширение поля Δ, а R — поле рациональных функций над Δ. Доказать, что тензорное произведение $P \otimes_\Delta R$ изоморфно полю рациональных функций над P.

3. Убедиться, что тензорное произведение двух полей рациональных функций над одним и тем же полем полем не является.

4. Пусть n — нечетное число и расширение P поля Δ характеристики, отличной от 2, содержит все корни степени n из единицы. Доказать, что P содержит все корни из единицы степени $2n$.

5. Каждое подполе поля порядка p^n имеет порядок p^m, где m делит n.

6. Если P' — алгебраическое расширение поля P и каждый отличный от константы многочлен над P имеет корень в P', то P' — алгебраически замкнутое поле. Используя этот результат, упростить доказательство теоремы 1.

§ 2. Теория Галуа

Начнем с некоторых результатов, относящихся к телам, имея в виду использовать их также и в следующем параграфе. Поскольку, согласно теореме II.3.4, каждый ненулевой левый модуль над телом D свободен, будем говорить о левых линейных пространствах над телом D или, короче, о левых D-пространствах. Размерность левого линейного пространства L над телом D условимся обозначать через $(L: D)$. Через $\mathrm{Aut}\, P$ будем обозначать группу автоморфизмов поля P.

Предложение 1. *Если k — подтело тела L, а L — подтело тела P, то*

$$(P:k)=(P:L)\,(L:k).$$

Доказательство. Пусть $(P:L)=r$, $(L:k)=s$, $\{a_1, \ldots, a_s\}$ — база k-пространства L и $\{b_1, \ldots, b_r\}$ — база L-пространства P. Положим $c_{ij}=a_jb_i$, $i=1, \ldots, r$, $j=1, \ldots, s$. Если $a\in P$, то

$$a=\sum_{i=1}^{r}\lambda_i b_i$$

для некоторых $\lambda_i\in L$. Но

$$\lambda_i=\sum_{j=1}^{s}\alpha_{ij}a_j$$

для некоторых $\alpha_{ij}\in k$ и, следовательно,

$$a=\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_{ij}c_{ij}.$$

Таким образом, элементы c_{ij} порождают P как левое линейное пространство над k. Эти элементы линейно независимы над k. Действительно, если

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_{ij}c_{ij}=0$$

для некоторых $\alpha_{ij}\in k$, то, положив $\lambda_i=\sum_{j=1}^{s}\alpha_{ij}a_j$,

будем иметь $\lambda_i \in L$ и

$$\sum_{i=1}^{r} \lambda_i b_i = \sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_{ij} a_j b_i = \sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_{ij} c_{ij} = 0.$$

Поскольку $b_1, \ldots, b_r$ линейно независимы над L, то

$$\sum_{j=1}^{s} \alpha_{ij} a_j = \lambda_i = 0$$

для всех i, что влечет $\alpha_{ij} = 0$ для всех j, ввиду линейной независимости элементов $a_1, \ldots, a_s$ над k. Таким образом, $(P:k) = rs$, что и требовалось.

Основным предметом дальнейшего рассмотрения служат конечномерные расширения фиксированного поля k, которые для краткости будем называть *конечными*. Напомним, что, согласно предложению 1.1, все конечные расширения являются алгебраическими. Зафиксируем некоторое алгебраическое замыкание $\bar{k}$ поля k, т. е. алгебраически замкнутое алгебраическое расширение поля k, существующее согласно теореме 1,1, и будем рассматривать расширения поля k, лежащие в $\bar{k}$. Из теоремы 1.1 и предложения 1.2 нетрудно вывести, что это равносильно рассмотрению произвольных алгебраических расширений поля k. Если P — подполе поля $\bar{k}$ и $\alpha_1, \ldots, \alpha_m \in \bar{k}$, то наименьшее расширение поля P, содержащее эти элементы, условимся обозначать через $P(\alpha_1, \ldots, \alpha_m)$. Если P — расширение поля L, то положим

$$G_L(P) = \{\varphi \mid \varphi \in \mathrm{Aut}\, P,\ \varphi(\xi) = \xi \text{ для всех } \xi \in L\}.$$

Ясно, что $G_L(P)$ — подгруппа группы $\mathrm{Aut}\, P$.

Предложение 2. *Пусть P — расширение поля L, $f \in L[x]$, n — степень многочлена f, $\alpha \in P$ и $f(\alpha) = 0$. Тогда*: (а) *если f неприводим над L и*

$$L(\alpha) = \{g(\alpha) \mid g \in L[x] \text{ и } (\text{степень } g) < n\},$$

то $L(\alpha)$ — поле и $(L(\alpha):L) = n$; (б) *если $\varphi \in G_L(P)$, то $\varphi(\alpha)$ — корень многочлена f*; (в) *если многочлен f неприводим, φ_0 — изоморфизм поля L на некоторое подполе L' поля P, $\tilde{\varphi}: L[x] \to L'[x]$ — изоморфизм колец многочленов, индуцированный изоморфизмом φ_0, и β — корень многочлена $\tilde{\varphi}(f)$, то существует один и только один изоморфизм $\bar{\varphi}$ поля $L(\alpha)$ на поле $L'(\beta)$ такой, что $\beta = \bar{\varphi}(\alpha)$ и $\bar{\varphi}(\xi) = \varphi_0(\xi)$ для всех $\xi \in L$*; (г) *если β — корень многочлена f и f непри-*

водим над L, то существует один и только один изоморфизм φ поля $L(\alpha)$ на поле $L(\beta)$ такой, что $\beta=\varphi(\alpha)$ и $\varphi(\xi)=\xi$ для всех $\xi\in L$; (д) если поле P алгебраически замкнуто, а многочлен f неприводим, то всякий изоморфизм φ поля L на некоторое подполе L' поля P может быть продолжен до изоморфизма $\bar{\varphi}$ расширения $L(\alpha)$ на некоторое подполе поля P.

Доказательство. (а) Пусть $R=\{g(\alpha)\mid g\in L[x]\}$. Ясно, что R — подкольцо поля P. Если $g(\alpha)\neq 0$, то НОД$(f, g)=1$. Следовательно, $uf+vg=1$ для некоторых $u, v\in L[x]$, откуда $v(\alpha)g(\alpha)=1$. Таким образом, R оказывается полем. Деля с остатком на f, нетрудно заметить, что все R можно получить, ограничившись рассмотрением многочленов g, степень которых меньше n. Поэтому в качестве базы поля $L(\alpha)$ над L можно взять $1, \alpha, \ldots, \alpha^{n-1}$.

(б) Пусть

$$f=\alpha_0x^n+\ldots+\alpha_n,$$

где $\alpha_i\in L$. Если $f(\alpha)=0$ и $\varphi\in G_L(P)$, то

$$\alpha_0\varphi(\alpha)^n+\ldots+\alpha_{n-1}\varphi(\alpha)+\alpha_n=$$
$$=\varphi(\alpha_0\alpha^n+\ldots+\alpha_{n-1}\alpha+\alpha_n)=0.$$

(в) Ввиду (а), каждый элемент из $L(\alpha)$ представляется в форме $g(\alpha)$, где g — многочлен над L степени, меньшей, чем n. Поскольку f неприводим, α не может быть корнем многочлена степени, меньшей, чем n. Поэтому вышеупомянутое представление оказывается однозначным. После этого ясно, что равенство

$$\bar{\varphi}(g(\alpha))=\tilde{\varphi}(g)(\beta)$$

определяет единственный искомый изоморфизм $\bar{\varphi}$.

(г) Вытекает из (в) при $\varphi_0=1_L$.

(д) Пусть $\tilde{\varphi}$: $L[x]\to L'[x]$ — изоморфизм колец многочленов, индуцированный изоморфизмом φ. Поскольку P алгебраически замкнуто, то многочлен $\tilde{\varphi}(f)$ имеет в P некоторый корень β, и остается лишь применить (в).

Предложение 3 (теорема о примитивном элементе). *Если P — конечное расширение поля k характеристики 0, то $P=k(\gamma)$ для некоторого $\gamma\in P$, причем $h(\gamma)=0$ для некоторого неприводимого многочлена h над k.*

Доказательство. По условию, $P=k(\alpha_1, \ldots, \alpha_n)$, где $\alpha_i\in\bar{k}$. Следовательно, существует цепочка расширений

$$k\subseteq k(\alpha_1)\subseteq k(\alpha_1)(\alpha_2)\subseteq\ldots\subseteq k(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)=P.$$

Поэтому достаточно рассмотреть случай, когда $P = k(\alpha, \beta)$. По предложению 1.1, расширение P алгебраично над k. Поэтому $f(\alpha) = 0$ и $g(\beta) = 0$, где f и g — неприводимые многочлены над k. Пусть $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$ и $\beta = \beta_1, \beta_2, \ldots$ $\ldots, \beta_n$ — все корни многочленов f и g соответственно. Все они лежат в $\bar{k}$. Поскольку k бесконечно, найдется $\zeta \in k$ такой, что

$$\alpha_i + \zeta\beta_j \neq \alpha + \zeta\beta$$

для всех пар $(i, j) \neq (1, 1)$. Положим $\gamma = \alpha + \zeta\beta$ и рассмотрим многочлен

$$F(x) = f(\gamma - \zeta x)$$

над полем $k(\gamma)$. Равенство

$$F(\beta) = f(\gamma - \zeta\beta) = f(\alpha) = 0$$

показывает, что β является общим корнем многочленов F и g. Однако если $j \neq 1$, то предположение $F(\beta_j) = 0$ влечет

$$f(\gamma - \zeta\beta_j) = F(\beta_j) = 0.$$

Следовательно, $\gamma - \zeta\beta_j = \alpha_i$ для некоторого i, что противоречит выбору ζ. Таким образом, β — единственный общий корень многочленов F и g, откуда НОД $(F, g) = x - \beta$, ибо над полем характеристики 0 неприводимые многочлены кратных корней не имеют. Поскольку коэффициенты многочленов F и g лежат в поле $k(\gamma)$, то $\beta \in k(\gamma)$. Но тогда и $\alpha = \gamma - \zeta\beta \in k(\gamma)$, откуда $P \subseteq k(\gamma)$. Обратное включение очевидно. Существование неприводимого многочлена вытекает из предложения 1.1.

Расширение P поля L называется *нормальным*, если всякий неприводимый многочлен над L, имеющий корень в P, разлагается над P на линейные множители. В этом случае будем также говорить, что поле P *нормально над* L.

Предложение 4. *Следующие свойства конечного расширения P поля L характеристики 0 равносильны:* (1) *P нормально над L;* (2) *$P = L(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — все корни некоторого неприводимого многочлена над полем L;* (3) *$P = L(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — все корни некоторого многочлена над полем L. При этом $|G_L(P)| = (P:L)$.*

Доказательство. Допустим, что P нормально над L. По предложению 3, $P = L(\alpha)$, где $\alpha \in P$. При этом α — корень некоторого неприводимого многочлена $f \in L[x]$. Пусть $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ — все корни этого многочлена.

В силу нормальности расширения P, все они лежат в P. Следовательно, $P=L(\alpha_1, \ldots, \alpha_n)$. Кроме того, если $\varphi \in G_L(P)$, то, в силу предложения 2(б), $\varphi(\alpha)=\alpha_i$ для некоторого i. Если φ, $\psi \in G_L(P)$ и $\varphi(\alpha)=\psi(\alpha)$, то $\varphi=\psi$, по предложению 2(г). Отсюда $|G_L(P)|=n$, что вместе с предложением 2(а) дает $|G_L(P)|=n=(P:L)$. Этим доказана импликация (1)$\Rightarrow$(2). Импликация (2)$\Rightarrow$(3) тривиальна. Остается доказать, что (3)$\Rightarrow$(1). Допустим, что $P=L(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — все корни многочлена $f \in L[x]$. В силу предложения 3, $P=L(\gamma)$ для некоторого $\gamma \in P$, причем $h(\gamma)=0$ для некоторого неприводимого многочлена h над L. Если g — неприводимый многочлен из $L[x]$, $g(\alpha)=0$, где $\alpha \in P$, и $g(\beta)=0$ для некоторого $\beta \in \bar{k}$, то, согласно предложению 2(в), существует изоморфизм $\varphi_0: L(\alpha) \to L(\beta)$, причем $\beta=\varphi_0(\alpha)$ и $\varphi_0(\xi)=\xi$ для всех $\xi \in L$. По предложению 2(д), φ_0 может быть продолжен до изоморфизма φ поля $P=L(\gamma)$ на некоторое подполе P' поля $\bar{k}$. По предложению 2(б), $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$ — все корни многочлена f. Отсюда $\varphi(P)=P$ и, следовательно, $\beta \in \varphi(P)=P$, что и требовалось.

Из предложения 4 вытекает

Следствие. *Если L — конечное расширение поля k характеристики 0, P — конечное расширение поля L и P нормально над k, то P нормально над L.*

Теорема 1 (основная теорема теории Галуа). *Пусть P — конечное нормальное расширение поля k характеристики 0, $\mathfrak{L}$ — структура всех расширений поля k, лежащих в P, $\mathfrak{H}$ — структура всех подгрупп группы $G=G_k(P)$, Φ — отображение структуры $\mathfrak{L}$ в структуру $\mathfrak{H}$, определяемое равенством*

$$\Phi(L)=G_L(P),$$

и Ψ — отображение структуры $\mathfrak{H}$ в структуру $\mathfrak{L}$, определяемое равенством

$$\Psi(H)=\{\xi \mid \xi \in P,\ \chi(\xi)=\xi \text{ для всех } \chi \in H\},$$

Тогда Φ оказывается антиизоморфизмом структуры $\mathfrak{L}$ на структуру $\mathfrak{H}$, а Ψ — обратным к нему антиизоморфизмом. Подгруппа $G_L(P)$ группы G нормальна в том и только в том случае, когда L — нормальное расширение поля k. При этом

$$G_k(L) \cong G_k(P)/G_L(P).$$

Доказательство. Ясно, что Φ и Ψ — антиизотонные отображения. Если $L \in \mathfrak{L}$ и $H \in \mathfrak{H}$, то, очевидно, $L \subseteq \Psi\Phi(L)$ и $H \subseteq \Phi\Psi(H)$. Отсюда

$$\Phi(L) \subseteq \Phi\Psi\Phi(L) \subseteq \Phi(L),$$

т. е.

$$G_L(P) = \Phi(L) = \Phi\Psi\Phi(L) = G_{\Psi\Phi(L)}(P)$$

для всех $L \in \mathfrak{L}$. В силу предложений 1 и 4 и следствия последнего, отсюда вытекает
$(\Psi\Phi(L):k) =$

$$= \frac{(P:k)}{(P:\Psi\Phi(L))} = \frac{(P:k)}{|G_{\Psi\Phi(L)}(P)|} = \frac{(P:k)}{|G_L(P)|} = \frac{(P:k)}{(P:L)} = (L:k)$$

и, следовательно,

$$L = \Psi\Phi(L). \qquad (*)$$

Если $H \in \mathfrak{H}$, то положим $L = \Psi(H)$. По предложению 3, $P = L(\alpha)$ для некоторого $\alpha \in P$, причем $h(\alpha) = 0$ для некоторого неприводимого многочлена h над L. Пусть $H = \{\varphi_1, \ldots, \varphi_s\}$, причем $\varphi_1 = 1_P$. Учитывая формулы Виета, замечаем, что все коэффициенты многочлена

$$g(x) = (x-\alpha)(x-\varphi_2(\alpha)) \ldots (x-\varphi_s(\alpha))$$

остаются на месте при любом автоморфизме из H и, следовательно, принадлежат $L = \Psi(H)$. При этом $g(\alpha) = 0$, а значит, h делит g. С помощью предложений 2(а) и 4 отсюда выводим, что

$$|G_L(P)| = (P:L) = (\text{степень } h) \leqslant (\text{степень } g) = s.$$

Но $H \subseteq G_L(P)$ и, следовательно,

$$H = G_L(P) = \Phi(L) = \Phi\Psi(H).$$

Таким образом, Φ и Ψ — взаимно обратные отображения, что доказывает антиизоморфизм структур $\mathfrak{L}$ и $\mathfrak{H}$.

Если теперь H — нормальная подгруппа в G, $L = \Psi(H)$ и неприводимый многочлен f степени s имеет корень $\alpha \in L$, то, по предложению 2(г), для любого другого корня β многочлена f имеем $\alpha\varphi = \beta$ для некоторого $\varphi \in G$. Если $\chi \in H$, то $\varphi\chi\varphi^{-1} \in H$ и, поскольку $\alpha \in L$, получаем

$$\beta\chi = \alpha\varphi\chi = \alpha\varphi\chi\varphi^{-1}\varphi = \alpha\varphi = \beta.$$

Следовательно, $\beta \in \Psi(H) = L$, т. е. L — нормальное расширение.

Наконец, если L — нормальное расширение поля k, лежащее в P, то, по предложению 4, $L=k(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — все корни некоторого неприводимого многочлена над k. Если $g \in G$, то, согласно предложению 2 (б), g переставляет корни этого многочлена. Поэтому, обозначив через $\pi(g)$ ограничение автоморфизма g на поле L, получим, что $\pi(g) \in G_k(L)$. Ясно, что π — гомоморфизм группы G в группу $G_k(L)$. Пусть теперь $\varphi \in G_k(L)$. По предложению 3, $P=L(\gamma)$, где γ — корень неприводимого многочлена над L. По предложению 2 (в), найдется автоморфизм $\bar{\varphi} \in G_k(P)=G$ такой, что $\pi(\bar{\varphi})=\varphi$ и $\bar{\varphi}(\gamma)=\gamma$. Следовательно, π — гомоморфное наложение. Ясно, что $\operatorname{Ker}\pi = G_L(P)$. Таким образом, $G_L(P)$ — нормальная подгруппа группы G и $G/G_L(P) \cong G_k(P)$.

Замечание. В случае, когда характеристика поля k отлична от нуля, теорема 1 остается в силе, если вместо нормальных расширений говорить о расширениях, порожденных всеми корнями неприводимого многочлена, не имеющего кратных корней. Примером неприводимого многочлена, удовлетворяющего этому условию, может служить многочлен x^2+x+1 над полем вычетов по модулю 2.

Группой Галуа многочлена f над полем k называется группа $G_k(P)$, где P — расширение поля k, полученное присоединением к k всех корней многочлена f.

Если f — многочлен над полем рациональных чисел $\mathbf{Q}$, то разрешимость уравнения $f=0$ в радикалах естественно трактовать как возможность получить расширение P поля $\mathbf{Q}$, содержащее все корни многочлена f, в виде последнего члена цепочки

$$\mathbf{Q}=P_1 \subseteq P_2 \subseteq \ldots \subseteq P_n=P,$$

где P_{i+1} получено из P_i присоединением некоторого корня уравнения $x^{m_i}-a_i$ для некоторого $a_i \in P_i$.

Теорема 2. *Если уравнение $f(x)=0$, где f — неприводимый многочлен над полем рациональных чисел $\mathbf{Q}$, разрешимо в радикалах, то группа Галуа многочлена f разрешима.*

Доказательство. Предварительно установим ряд лемм.

Лемма 1. *Если $s \leqslant n$, то*

$$C_n^s + C_{n-1}^s + \ldots + C_s^s = C_{n+1}^{s+1}.$$

Действительно, если $n=1$, то имеем $C_1^1=C_2^2$. Если $n \geqslant 2$, то, используя хорошо известное равенство $C_{i-1}^s +$

$+C_{i-1}^{s-1}=C_i^s$, где $i>s$, и индуктивное предположение, получаем

$$\sum_{i=s}^{n} C_i^s = C_s^s + \sum_{i=s+1}^{n} C_{i-1}^s + \sum_{i=s+1}^{n} C_{i-1}^{s-1} =$$

$$= \sum_{i=s}^{n-1} C_i^s + \sum_{i=s}^{n-1} C_i^{s-1} = C_n^{s+1} + C_n^s = C_{n+1}^{s+1}.$$

Лемма 2. *Многочлен*

$$\Phi(x) = x^{p-1} + x^{p-2} + \ldots + x + 1,$$

где p — простое число, неприводим над полем $\mathbf{Q}$.

В самом деле, если $\Phi(x)$ приводим, то приводим и многочлен $\Phi(x+1)$. Но, ввиду леммы 1,

$$\Phi(x+1) = \sum_{k=0}^{p-1} \sum_{i=0}^{k} C_k^i x^i = \sum_{i=0}^{p-1} (C_{p-1}^i + C_{p-2}^i + \ldots + C_i^i)\, x^i =$$

$$= \sum_{i=0}^{p-1} C_p^{i+1} x^i = x^{p-1} + C_p^{p-1} x^{p-2} + \ldots + C_p^2 x + p,$$

и возникает противоречие с критерием Эйзенштейна (Кострикин А. И. Введение в алгебру.— М.: Наука, 1977, с. 231—232).

Лемма 3. *Если p — простое число и ζ — первообразный корень степени p из* 1, *то $G = G_{\mathbf{Q}}(\mathbf{Q}(\zeta))$ — циклическая группа.*

Действительно, корни многочлена $f = x^{p-1} + x^{p-2} + \ldots + 1$ совпадают, очевидно, с множеством $\zeta, \zeta^2, \ldots, \zeta^{p-1}$. По следствию теоремы 1.3, найдется такое целое число k, что остатки от деления чисел $k, k^2, \ldots, k^{p-1}$ на p заполняют множество $\{1, 2, \ldots, p-1\}$. В силу предложения 2(г) и леммы 2, $\varphi_0(\zeta) = \zeta^k$ для некоторого $\varphi_0 \in G$. Если теперь $\varphi \in G$, то $\varphi(\zeta) = \zeta^s$, где $1 \leqslant s < p$. В силу выбора числа k, $k^m = pq + s$ для некоторого m. Отсюда

$$\varphi(\zeta) = \zeta^s = \zeta^{k^m} = \varphi_0^m(\zeta),$$

и, следовательно, $\varphi = \varphi_0^m$ в силу предложения 2(г).

Лемма 4. *Если ζ — первообразный корень степени n из* 1, *то $G_{\mathbf{Q}}(\mathbf{Q}(\zeta))$ — разрешимая группа.*

Доказательство будем вести индукцией по числу t простых сомножителей числа n. Если $t=1$, то можно воспользоваться леммой 3. Если $t \geqslant 2$, то запишем $n = mp$, где p — простое число. Пусть ξ и η — первообразные

корни из 1 степеней m и p соответственно. Ясно, что $\mathbf{Q}(\zeta)=\mathbf{Q}(\xi)(\eta)$. В силу предложения 4, $\mathbf{Q}(\xi)$ — нормальное расширение поля $\mathbf{Q}$. Поэтому, используя теорему 1, получаем

$$G_{\mathbf{Q}}(\mathbf{Q}(\xi)) \cong G_{\mathbf{Q}}(\mathbf{Q}(\zeta))/G_{\mathbf{Q}(\xi)}(\mathbf{Q}(\zeta)). \qquad (*)$$

Далее, если $\varphi \in G_{\mathbf{Q}(\xi)}(\mathbf{Q}(\zeta))$, то $\varphi(\eta) \in \mathbf{Q}(\eta)$. Следовательно, обозначив через φ_0 ограничение автоморфизма φ на поле $\mathbf{Q}(\eta)$, будем иметь $\varphi_0 \in G_{\mathbf{Q}}(\mathbf{Q}(\eta))$. Если $\varphi, \psi \in G_{\mathbf{Q}(\xi)}(\mathbf{Q}(\zeta))$ и $\varphi_0=\psi_0$, то $\varphi(\eta)=\psi(\eta)$ и, поскольку $\varphi(\xi)=\xi=\psi(\xi)$, то $\varphi(\zeta)=\psi(\zeta)$. В силу предложения 2(г), $\varphi=\psi$. Таким образом, $G_{\mathbf{Q}(\xi)}(\mathbf{Q}(\zeta))$ изоморфна подгруппе группы $G_{\mathbf{Q}}(\mathbf{Q}(\eta))$, разрешимой по лемме 3. Следовательно, $G_{\mathbf{Q}(\xi)}(\mathbf{Q}(\zeta))$ также разрешима. Из индуктивного предположения вытекает разрешимость группы $G_{\mathbf{Q}}(\mathbf{Q}(\xi))$. Вместе с изоморфизмом (*) это дает разрешимость группы $G_{\mathbf{Q}}(\mathbf{Q}(\zeta))$ (ЭА, с. 216, теорема IV.2.5).

Лемма 5. *Пусть* $\alpha \in \mathbf{Q}$, β — *комплексное число*, $\beta^n=\alpha$ *и* E — *конечное расширение поля* $\mathbf{Q}$, *содержащее первообразный корень* ζ *степени* n *из* 1. *Тогда* $G_E(E(\beta))$ — *циклическая группа.*

Для доказательства выберем неприводимый многочлен g над E, корнем которого служит β. Этот многочлен, разумеется, делит $x^n-\alpha$ и, следовательно, его корни принадлежат множеству $\{\beta, \beta\zeta, \beta\zeta^2, \ldots, \beta\zeta^{n-1}\}$. Если g линеен, то $\beta \in E$ и $G_E(E(\beta))=\{1\}$. В противном случае возьмем $k \geqslant 1$ так, что $g(\beta\zeta^k)=0$, но $g(\beta\zeta^i) \neq 0$, если $1 \leqslant i < k$. В силу предложения 2(г), существует $\varphi_0 \in G = G_E(E(\beta))$ такой, что $\varphi_0(\beta)=\beta\zeta^k$. Используя индукцию, получаем

$$\varphi_0^t(\beta)=\varphi_0(\varphi_0^{t-1}(\beta))=\varphi_0(\beta\zeta^{(t-1)k})=\beta\zeta^{k+(t-1)k}=\beta\zeta^{kt} \qquad (*)$$

для любого натурального t. Если теперь $\varphi \in G$, то, по предложению 2(б), $\varphi(\beta)=\beta\zeta^s$ для некоторого s. Записав $s=kq+r$, где $0 \leqslant r < k$, и используя (*), получим

$$\varphi(\beta)=\beta\zeta^s=\beta\zeta^{kq}\zeta^r=\varphi_0^q(\beta)\,\zeta^r.$$

Отсюда

$$\beta\varphi\varphi_0^{-q}=\beta\zeta^r$$

и, поскольку $\varphi\varphi_0^{-q} \in G$, то $g(\beta\zeta^r)=0$. В силу выбора числа k, $r=0$, т. е. $\varphi(\beta)=\varphi_0^q(\beta)$. В силу предложения 2(г), $\varphi=\varphi_0^q$, т. е. G — циклическая группа, порожденная автоморфизмом φ_0.

Вернемся к доказательству теоремы. Корнями многочлена f служат комплексные числа, скажем, $\alpha_1, \ldots, \alpha_n$. По определению, разрешимость уравнения $f(x)=0$ в радикалах означает существование цепочки расширений

$$\mathbf{Q}=P_1\subseteq P_2\subseteq\ldots\subseteq P_s=\mathbf{Q}(\alpha_1, \ldots, \alpha_n),$$

где каждое P_{i+1} получается из P_i присоединением всех корней многочлена $x^{m_i}-a_i$ для некоторого $a_i\in P_i$. Пусть $E=\mathbf{Q}(\zeta)$, где ζ — первообразный корень из 1 степени $m=m_1\ldots m_n$, а $P=E(a_1, \ldots, a_s)$. Разумеется, E содержит все корни из 1 степеней $m_1, \ldots, m_n$. Рассмотрим цепочку расширений

$$E=P_1'\subseteq P_2'\subseteq\ldots\subseteq P_s'=P,$$

где P_{i+1}' получается из P_i' присоединением всех корней многочлена $x^{m_i}-a_i$. По предложению 4, P_{i+1}' — нормальное расширение поля P_i' и, в силу теоремы 1,

$$G_E(P_i')\cong G_E(P_{i+1}')/G_{P_i'}(P_{i+1}').$$

По лемме 5, $G_{P_i'}(P_{i+1}')$ — разрешимая группа. По индукции можно считать разрешимой группу $G_E(P_i')$. Но тогда разрешима и группа $G_E(P_{i+1}')$ (ЭА, с. 216, теорема IV.2.5). Таким образом, установлена разрешимость группы $G_E(P)$. Группа $G_{\mathbf{Q}}(E)$ разрешима по лемме 4. Из предложения 4 и теоремы 1 вытекает существование изоморфизмов

$$G_{\mathbf{Q}}(P_s)\cong G_{\mathbf{Q}}(P)/G_{P_s}(P)$$

и

$$G_{\mathbf{Q}}(E)\cong G_{\mathbf{Q}}(P)/G_E(P).$$

Следовательно, разрешима группа $G_{\mathbf{Q}}(P)$ (цит. выше). Но тогда разрешима и ее фактор-группа $G_{\mathbf{Q}}(P_s)$ (там же).

Теорема 2 позволяет указать уравнение пятой степени, не разрешимое в радикалах. Предварительно установим:

Предложение 6. *Если подгруппа H симметрической группы $\mathfrak{S}_5$ содержит хотя бы одну транспозицию и транзитивна* (т. е. для любых $i, j\in\{1, 2, 3, 4, 5\}$ существует $\sigma\in H$ такая, что $\sigma(i)=j$), *то* $H=\mathfrak{S}_5$.

Доказательство. Пусть T — транзитивная подгруппа группы $\mathfrak{S}_5$.

Лемма 1. *Если* $(ij)\in T$ *и* $\sigma\in T$, *то* $(\sigma(i)\ \sigma(j))\in T$.

Для доказательства достаточно заметить, что

$$\sigma^{-1}(ij)\sigma=(\sigma(i)\ \sigma(j)).$$

Лемма 2. *Если T содержит некоторую транспозицию (st), то для любого i найдется j такое, что $(ij)\in T$.*

В самом деле, $\sigma(s)=i$ для некоторого $\sigma\in T$. Если $j=\sigma(t)$, то $(ij)\in T$ по лемме 1.

Лемма 3. *Если символ s принадлежит четырем транспозициям, лежащим в T, то $T=\mathfrak{S}_5$.*

Действительно, если i, j и s различны, то

$$\sigma=(sij)=(si)(sj)\in T.$$

Но $(si)\in T$ и, по лемме 1,

$$(ij)=(\sigma(s)\ \sigma(i))\in T.$$

Таким образом, H содержит все транспозиции и, следовательно, совпадает с $\mathfrak{S}_5$ (ЭА, с. 86, теорема II.3.17).

Лемма 4. *Если символ s принадлежит трем транспозициям, лежащим в T, то $T=\mathfrak{S}_5$.*

Действительно, если $(si)\in T$ для всех $i\neq s$, то применима лемма 3. Допустим, что $(si)\notin T$. По лемме 2, $(ij)\in T$ для некоторого $j\neq i$. Но $(sj)\in T$ и, ввиду леммы 1, $(si)\in T$. Противоречие.

Лемма 5. *Если символ s принадлежит двум транспозициям, лежащим в T, то $T=\mathfrak{S}_5$.*

Для доказательства допустим, что (si), $(sj)\in T$, где $i\neq j$. Пусть $k\neq i$, j, s. Если T содержит (ki), (kj) или (ks), то, ввиду леммы 1, $(ks)\in T$ и применима лемма 4. В противном случае выберем $\sigma\in T$ так, что $\sigma(s)=k$. Ввиду леммы 1, как $\sigma(i)$, так и $\sigma(j)$ отличны от i, j, k и s что, разумеется, невозможно.

Возвращаясь к доказательству предложения, допустим, что $(st)\in H$. Пусть $\{i, j, k, s, t\}=\{1, 2, 3, 4, 5\}$. По лемме 2, H содержит транспозиции (ip), (jq) и (kr) для подходящих p, q, r. Если p, q, r не все различны, то $H=\mathfrak{S}_5$ по лемме 5. К тому же выводу придем и в случае, когда множество $\{p, q, r\}$ содержит s или t. Таким образом, $\{i, j, k\}=\{p, q, r\}$. Следовательно, $p=j$ или $p=k$. Но тогда опять оказывается применимой лемма 5.

Предложение 7. *Группа $\mathfrak{S}_5$ не разрешима.*

Доказательство. Если бы $\mathfrak{S}_5$ была разрешимой, то была бы разрешимой и ее нормальная подгруппа $\mathfrak{A}_5$ (ЭА, с. 216, теорема IV.2.5), что противоречит простоте последней (ЭА, с. 223, теорема IV.2.9).

Теорема 3. *Уравнение* $x^5-4x+2=0$ *над полем рациональных чисел* $\mathbf{Q}$ *не разрешимо в радикалах.*

Доказательство. По критерию Эйзенштейна (Кострикин А. И. Введение в алгебру.— М.: Наука, 1977, с. 231—232), многочлен $f=x^5-4x+2$ неприводим над $\mathbf{Q}$. По правилу знаков Декарта (там же, с. 286, теорема 2), f имеет один отрицательный корень и не более двух положительных. Поскольку $f(0), f(2)>0$, а $f(1)<0$, то f имеет в точности 3 действительных корня. Итак, пусть $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$ — корни многочлена f, причем $\alpha_1=\overline{\alpha_2}\neq\alpha_2$, а $\alpha_3, \alpha_4, \alpha_5$ — действительные числа. Пусть $P=\mathbf{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$. Можно считать, что P — подполе поля комплексных чисел. Поскольку переход к комплексно сопряженному числу индуцирует автоморфизм из $G_{\mathbf{Q}}(P)$, меняющий местами α_1 и α_2 и оставляющий на месте остальные корни, то $(12)\in G_{\mathbf{Q}}(P)$. В силу предложения 2 (г), группа $G_{\mathbf{Q}}(P)$ транзитивна. Следовательно, $G_{\mathbf{Q}}(P)=\mathfrak{S}_5$ по предложению 6. Остается лишь сопоставить теорему 2 и предложение 7.

Упражнения

1. Пусть $\bar{k}$ — алгебраическое замыкание поля k характеристики 0, P' и P'' — конечные нормальные расширения поля k, принадлежащие $\bar{k}$, и P — подполе поля $\bar{k}$, порожденное объединением $P'\cup P''$. Доказать, что существует изоморфизм поля P на поле $P'\otimes_{P'\cap P''}P''$, оставляющий на месте все элементы из P''.

2. Пусть $\bar{\mathbf{Q}}$ алгебраическое замыкание поля $\mathbf{Q}$ и k — максимальное подполе поля $\bar{\mathbf{Q}}$, не содержащее $\sqrt{2}$. Доказать, что $G_k(P)$ — циклическая группа для любого конечного расширения P поля k.

3. Пусть $\bar{k}$ — алгебраическое замыкание поля k характеристики 0, σ — автоморфизм поля $\bar{k}$, оставляющий на месте все элементы из k, и $L=\{x\mid x\in\bar{k},\ \sigma(x)=x\}$. Доказать, что $G_L(P)$ — циклическая группа для любого конечного расширения P поля L.

4. Пусть $\mathbf{Q}$ — поле рациональных чисел и $\omega^4=2$. Доказать, что $\mathbf{Q}(\omega)$ не является нормальным расширением поля $\mathbf{Q}$.

5. Определить группу Галуа следующих многочленов над полем рациональных чисел: а) x^3-x-1; б) x^2-2; в) x^4-5; г) x^4+2; д) $(x^2-2)(x^3-3)(x^2-5)(x^2-7)$.

6. Любое конечное расширение поля рациональных чисел содержит лишь конечное число корней из единицы.

§ 3. Тела

Пусть Δ — коммутативное кольцо с единицей. Кольцо R называется *алгеброй над* Δ или, короче, Δ-*алгеброй*, если R является модулем над Δ и для любых $\lambda\in\Delta$ и

$r, s \in R$ справедливо

$$\lambda(rs) = (\lambda r)s = r(\lambda s).$$

Если есть опасность перепутать алгебру с универсальной алгеброй, то употребляют термин «линейная алгебра». Ясно, что линейные алгебры образуют многообразие универсальных алгебр, сигнатура которого состоит из кольцевых операций и множества Δ унарных операций. Каждое кольцо является алгеброй над кольцом $\mathbf{Z}$. Другой важный частный случай возникает, если Δ — поле. В этом случае R оказывается линейным пространством над Δ. Алгебра R называется *конечномерной*, если конечна размерность этого линейного пространства. Алгебра над полем Δ, являющаяся телом, называется *алгеброй с делением*. Над полем действительных чисел известны следующие алгебры с делением: поля действительных и комплексных чисел и тело кватернионов, которое можно представить как подкольцо кольца матриц второго порядка над полем комплексных чисел, состоящее из всех матриц вида

$$\begin{Vmatrix} u & v \\ -\bar{v} & \bar{u} \end{Vmatrix}$$

(см. ЭА, с. 101—103). Этот список оказывается исчерпывающим, поскольку справедлива:

Теорема 1 (Фробениус). *Всякая конечномерная алгебра A с делением над полем $\mathbf{R}$ действительных чисел изоморфна или полю действительных чисел, или полю комплексных чисел, или телу кватернионов.*

Доказательство. Ясно, что отображение $\alpha \mapsto \alpha 1$ осуществляет гомоморфное вложение поля $\mathbf{R}$ в алгебру A. Поэтому можно считать, что $\mathbf{R} \subseteq A$ (ср. ЭА, теорема III.2.1). Если $\dim A = 1$, то $A = \mathbf{R}$. Так что в дальнейшем будем предполагать, что $n = \dim A \geqslant 2$.

Лемма 1. *Для всякого $a \in A \setminus \mathbf{R}$ найдутся $\alpha, \beta \in \mathbf{R}$ такие, что $a^2 + 2\alpha a + \beta = 0$.*

Действительно, элементы $1, a, a^2, \ldots, a^n$ линейно зависимы, т. е.

$$\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_n a^n = 0$$

для некоторых $\alpha_i \in \mathbf{R}$, среди которых имеются ненулевые. Более того, легко понять, что $\alpha_i \neq 0$ для некоторого $i \neq 0$. Таким образом, степень многочлена

$$f(t) = \alpha_0 + \alpha_1 t + \alpha_2 t^2 + \ldots + \alpha_n t^n$$

отлична от нуля. Но всякий многочлен над полем $\mathbf{R}$ разлагается в произведение многочленов степени $\leqslant 2$, т. е.

$$f(t)=g_1(t)\dots g_m(t),$$

где (степень $g_i)\leqslant 2$. Поскольку степени элемента a перестановочны друг с другом, то

$$g_1(a)\dots g_m(a)=f(a)=0.$$

Поскольку в теле нет делителей нуля (см. ЭА, с. 95, теорема II.4.5), то $g_i(a)=0$ для некоторого i. Если (степень $g_i)=1$, то, вопреки предположению, $a\in\mathbf{R}$. Так что (степень $g_i)=2$, а это и доказывает лемму.

Лемма 2. *Если* $a\in A\setminus\mathbf{R}$, $\alpha,\beta\in\mathbf{R}$ *и* $a^2+2\alpha a+\beta=0$, *то* $\alpha^2-\beta<0$.

В самом деле, если $\alpha^2-\beta\geqslant 0$, то многочлен $t^2+2\alpha t+\beta$ имеет действительные корни, скажем, γ' и γ''. Но тогда

$$(a-\gamma')(a-\gamma'')=a^2+2\alpha a+\beta=0,$$

откуда $a=\gamma'$ или γ'', вопреки условию.

Лемма 3. *Если* $1, e_1, \dots, e_m$ *— линейно независимые элементы из* A, *то можно найти элемент* $f\in A$ *такой, что* $f^2=-1$, *а система*

$$\{1, e_1, \dots, e_{i-1}, f, e_{i+1}, \dots, e_m\} \qquad (*)$$

остается линейно независимой.

Действительно, по лемме 1, $e_i^2+2\alpha e_i+\beta=0$ для некоторых $\alpha,\beta\in\mathbf{R}$. По лемме 2, $\alpha^2-\beta<0$. Поскольку

$$(e_i+\alpha)^2+(\beta-\alpha^2)=0,$$

то, положив

$$f=\frac{1}{\sqrt{\beta-\alpha^2}}(e_i+\alpha),$$

получим $f^2=-1$. Кроме того, нетрудно убедиться в линейной независимости системы (*).

Лемма 4. *Пусть* $1, a, b$ *— линейно независимые элементы из* A *и* $a^2=b^2=-1$. *Тогда найдется* $c\in\mathbf{R}a+\mathbf{R}b$ *такой, что* $c^2=-1$, $ac+ca=0$ *и система* $\{1, a, c, ac\}$ *линейно независима.*

В самом деле, по лемме 1

$$(a+b)^2=\alpha(a+b)+\beta$$

и

$$(a-b)^2=\gamma(a-b)+\delta,$$

где $\alpha, \beta, \gamma, \delta \in \mathbf{R}$. Отсюда

$$-1+ab+ba-1=\alpha(a+b)+\beta$$

и

$$-1-ab-ba-1=\gamma(a-b)+\delta.$$

Складывая эти равенства, получаем

$$(\beta+\delta+4)+(\alpha+\gamma)a+(\alpha-\gamma)b=0.$$

Поскольку 1, a и b линейно независимы, то

$$\beta+\delta+4=\alpha+\gamma=\alpha-\gamma=0,$$

откуда $\alpha=\gamma=0$ и, следовательно,

$$ab+ba=\beta+2.$$

Положим $\xi=(\beta+2)/2$. Тогда

$$(b+\xi a)^2=-1+\xi(ab+ba)-\xi^2=-1+2\xi^2-\xi^2=-1+\xi^2.$$

Если $b+\xi a \in \mathbf{R}$, то возникает противоречие с линейной независимостью системы $\{1, a, b\}$. Поэтому, в силу леммы 2, $-1+\xi^2=-\eta^2$, где $0 \neq \eta \in \mathbf{R}$. Положим

$$c=\frac{1}{\eta}(b+\xi a).$$

Нетрудно проверить, что $\{1, a, c\}$ — линейно независимая система. При этом

$$c^2=\frac{1}{\eta^2}(b+\xi a)^2=-1$$

и

$$ac+ca=\frac{1}{\eta}(ab-\xi+ba-\xi)=\frac{1}{\eta}(2\xi-\xi-\xi)=0.$$

Если, наконец,

$$ac=\alpha+\beta a+\gamma c,$$

где $\alpha, \beta, \gamma \in \mathbf{R}$, то, умножая справа на c, получаем

$$-a=\alpha c+\beta ac-\gamma.$$

Следовательно,

$$-a=\alpha c+\alpha\beta+\beta^2 a+\beta\gamma c-\gamma,$$

откуда, ввиду линейной независимости системы $\{1, a, c\}$, $\beta^2 = -1$. Противоречие.

Лемма 5. *Если* $a, b \in A$, $a^2 = b^2$ *и* $ab = ba$, *то* $a = b$ *или* $a = -b$.

Действительно,

$$(a-b)(a+b) = a^2 - ba + ab - b^2 = 0,$$

откуда $a = b$ или $a = -b$.

Возвращаясь к доказательству теоремы, допустим, что $\dim A = 2$. В силу леммы 3, можно найти базу $\{1, e\}$, где $e^2 = -1$. Тогда

$$(\alpha + \beta e)(\gamma + \delta e) = (\alpha\gamma - \beta\delta) + (\alpha\delta + \beta\gamma)e \qquad (\alpha, \beta, \gamma, \delta \in \mathbf{R}),$$

и отображение $\alpha + \beta e \mapsto \alpha + \beta i$ осуществляет изоморфизм алгебры A на поле комплексных чисел. Если же $\dim A \geqslant 3$, то леммы 3 и 4 позволяют найти элементы a и c, указанные в лемме 4. Если $\{1, a, c, ac\}$ — база алгебры A, то, как нетрудно подсчитать, таблица умножения этих элементов имеет вид

	1	a	c	ac
1	1	a	c	ac
a	a	-1	ac	$-c$
c	c	$-ac$	-1	a
ac	ac	c	$-a$	-1

и отображение

$$\alpha + \beta a + \gamma c + \delta(ac) \mapsto \begin{Vmatrix} \alpha + \beta i & \gamma + \delta i \\ -\gamma + \delta i & \alpha - \beta i \end{Vmatrix}$$

оказывается изоморфизмом алгебры A на тело кватернионов (см. ЭА, с. 102). Допустим, наконец, что $\dim A \geqslant 5$. Тогда в силу лемм 3 и 4, найдутся элементы $a, c, d \in A$ такие, что $\{1, a, c, ac, d\}$ — линейно независимая система, $a^2 = c^2 = d^2 = -1$ и $ac + ca = 0$. Еще раз применив лемму 4, найдем $u \in A$ такой, что $u = \xi a + \eta d$ для некоторых $\xi, \eta \in \mathbf{R}$, $u^2 = -1$, $ua + au = 0$ и система $\{1, a, u, au\}$ линейно независима, а затем $v \in A$, удовлетворяющий условиям $v = \zeta c + \chi u$, где $\zeta, \chi \in \mathbf{R}$, $v^2 = -1$ и $cv + vc = 0$, причем $\{1, c, v, cv\}$ — линейно независимая система. Тогда $\eta\chi \neq 0$ и, кроме того,

$$(cv)^2 = cvcv = -c^2v^2 = -1,$$
$$a(cv) = ac(\zeta c + \chi u) = -\zeta a + \chi acu,$$
$$(cv)a = c(\zeta c + \chi u)a = -\zeta a + \chi cua$$

и

$$acu = -cau = cua.$$

Следовательно,

$$a(cv) = (cv)a.$$

По лемме 5, $a = cv$ или $a = -cv$. Отсюда

$$a = \pm c(\zeta c + \chi u) = \mp\zeta \pm \chi\xi ca \pm \chi\eta cd.$$

Умножая слева на c, получаем

$$-ac = ca = \mp\zeta c \mp \chi\xi a \mp \chi\eta d,$$

что противоречит линейной независимости системы $\{1, a, c, ac, d\}$.

Докажем теперь коммутативность всякого конечного тела. С этой целью выделим в поле комплексных чисел множество Ω_n всех корней степени n из 1, не являющихся корнями из 1 меньшей степени. Многочлен

$$\Phi_n(x) = \prod_{\omega \in \Omega_n} (x - \omega)$$

называется *n-м круговым многочленом.*

Предложение 1. *Круговые многочлены Φ_n суть многочлены с целочисленными коэффициентами, старший из которых равен единице.*

Доказательство. Поскольку $\Phi_1 = x - 1$, можно вести индукцию по n. Пусть $n \geqslant 2$ и ϑ — множество всех отличных от n делителей числа n. Тогда

$$x^n - 1 = \Phi_n(x) \prod_{d \in \vartheta} \Phi_d(x).$$

В силу индуктивного предположения,

$$\prod_{d \in \vartheta} \Phi_d(x) = x^k + a_1 x^{k-1} + \ldots + a_k,$$

где a_i — целые числа. Записав

$$\Phi_n(x) = b_0 x^l + b_1 x^{l-1} + \ldots + b_l,$$

заметим, что $k + l = n$, $b_0 = 1$,

$$\begin{aligned} &b_1 + a_1 = 0, \\ &b_2 + a_1 b_1 + a_2 = 0, \\ &\quad\ldots\ldots\ldots\ldots \\ &b_l + a_1 b_{l-1} + \ldots + a_{l-1} b_1 + a_l = 0, \end{aligned}$$

где $a_i=0$, если $i>k$. Отсюда ясно, что b_j — целые числа.

Теорема 2 (Веддербарн). *Всякое конечное тело коммутативно.*

Доказательство. Пусть K — конечное тело и P — его центр. Ясно, что P — поле и что K можно рассматривать как линейное пространство над P. Пусть n — размерность этого пространства. Согласно теореме 1.3 (а), $|P|=q=p^m$, где p — простое число. Тогда $|K|=q^n$. Ясно, что $P^*=P\setminus\{0\}$ — центр группы $K^*=K\setminus\{0\}$. Пусть $g_1, \ldots, g_r$ — представители всех неодноэлементных классов сопряженности группы K^*,

$$C_i=\{x \mid x\in K,\ xg_i=g_ix\}$$

и $C_i^*=C_i\setminus\{0\}$. Если K_i — класс сопряженности, содержащий элемент g_i, то

$$q^n-1=|K^*|=|K_i|\cdot|C_i^*|$$

(см. ЭА, с. 213, теорема IV.2.1). Представляя K^* в виде объединения классов сопряженности (см. ЭА, с. 88, теорема II.3.21), получаем

$$q^n-1=|K^*|=|P^*|+|K_1|+\ldots+|K_r|=$$
$$=q-1+\sum_{i=1}^{r}\frac{q^n-1}{|C_i^*|}. \qquad (*)$$

Далее, нетрудно проверить, что C_i — подтело тела K, содержащее поле P. Тогда K можно рассматривать как левое линейное пространство над телом C_i, а C_i — как линейное пространство над полем P. Если s_i и t_i — размерности этих пространств (см. предложение II.3.4), то

$$|C_i|=q^{t_i}$$

и

$$n=s_it_i,$$

согласно предложению 2.1. Отсюда

$$|C_i^*|=q^{t_i}-1. \qquad (**)$$

Обозначим через ϑ_m множество всех отличных от m делителей числа m. Напомним, что, по определению кругового многочлена,

$$x^n-1=\Phi_n(x)\prod_{d\in\vartheta_n}\Phi_d(x). \qquad (***)$$

Отсюда

$$\frac{x^n-1}{x^{t_i}-1}=\frac{\Phi_n(x)\prod\limits_{d\in\vartheta_n}\Phi_d(x)}{\Phi_{t_i}(x)\prod\limits_{d\in\vartheta_{t_i}}\Phi_d(x)}=\Phi_n(x)\Psi_i(x),$$

где Ψ_i — некоторый многочлен. Вместе с (*), (**) и (***) эти равенства дают

$$q-1=\Phi_n(q)\prod_{d\in\vartheta_n}\Phi_d(q)-\sum_{i=1}^{r}\Phi_n(q)\Psi_i(q)=$$

$$=\Phi_n(q)\left[\prod_{d\in\vartheta_n}\Phi_d(q)-\sum_{i=1}^{r}\Psi_i(q)\right]. \qquad (****)$$

Заметим еще, что многочлены $\Phi_d(x)$, где $d\in\vartheta_n$, и $\Psi_i(x)$, $i=1, 2, \ldots, r$, разлагаются в произведение множителей вида $x-\omega$, где ω — корень из 1. Поскольку корни из 1 — целые алгебраические числа, то целым алгебраическим оказывается и число

$$\gamma=\prod_{d\in\vartheta_n}\Phi_d(q)-\sum_{i=1}^{r}\Psi_i(q)=\frac{q-1}{\Phi_n(q)}$$

(см. ЭА, с. 209, теорема IV.1.16). Но по предложению 1, $\Phi_n(q)$ — обычное целое число. Следовательно, γ оказывается рациональным числом, а значит, и обычным целым (ЭА, с. 209, теорема IV.1.15). Поэтому, в силу (****), $|q-1|\geqslant|\Phi_n(q)|$.

Пусть теперь Ω — множество всех первообразных корней степени n из 1. Если $n\geqslant 2$, то найдется $\omega_0\in\Omega$ такой, что 0, q и ω_0 не лежат на одной прямой комплексной плоскости. Тогда

$$|q-\omega_0|>q-|\omega_0|=q-1,$$

откуда

$$|\Phi_n(q)|=\prod_{\omega\in\Omega}|q-\omega|>(q-1)^{|\Omega|}\geqslant q-1.$$

Противоречие.

Упражнения

1. Если тело D является центральной конечномерной алгеброй над полем k и P — максимальное подполе тела D, то $(D:k)=(P:k)^2$.

2. Пусть K — линейное пространство над полем рациональных чисел $\mathbf{Q}$ с базой $\{1, i, j, k\}$. Убедиться, что задание умножения

таблицей

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	2	$-2i$
k	k	j	$2i$	2

превращает K в тело и что $\mathbf{Q}(i)$ и $\mathbf{Q}(j)$ — неизоморфные максимальные подполя этого тела.

3. Если тело K является конечномерным пространством над своим алгебраически замкнутым подполем P, то $K=P$.

4. Всякое конечное простое кольцо с единицей изоморфно кольцу матриц над полем.

5. Всякое конечное регулярное кольцо изоморфно прямой сумме колец матриц над полями.

6. Всякое тело является алгеброй или над полем рациональных чисел, или над полем вычетов по простому модулю.

ЛИТЕРАТУРА

Артин Э. Геометрическая алгебра.— М.: Наука, 1969.
Ван дер Варден Б. Л. Алгебра.— М.: Наука, 1979.
Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр.— М.: Наука, 1969.
Постников М. М. Теория Галуа.— М.: Физматгиз, 1963.
Херстейн И. Некоммутативные кольца.— М.: Мир, 1972.

ГЛАВА VII

АЛГЕБРЫ С ДОПОЛНИТЕЛЬНОЙ СТРУКТУРОЙ (В СМЫСЛЕ БУРБАКИ)

В этой главе рассматриваются упорядоченные группы, нормированные кольца и топологические кольца. Кроме основных понятий, здесь изложено доказательство теоремы Гельдера об архимедовых линейно упорядоченных группах, охарактеризованы линейно упорядочиваемые абелевы группы, описаны нормирования поля рациональных чисел и даны критерии нормируемости топологических тел и полей.

§ 1. Упорядочеиные группы

Группа G называется *частично упорядоченной*, если G — частично упорядоченное множество и для любых $a, b, g \in G$ справедлива импликация

$$(a \leqslant b) \Rightarrow ((ag \leqslant bg) \,\&\, (ga \leqslant gb)).$$

Если дополнительно G оказывается цепью, то группа G называется *линейно упорядоченной*. Примерами линейно упорядоченных групп служат аддитивные группы целых, рациональных и действительных чисел. Всякую группу можно рассматривать как частично упорядоченную группу с тривиальным порядком. Аддитивная группа действительных функций, определенных на отрезке $[0, 1]$, становится частично упорядоченной, если положить $f \leqslant g$ в случае, когда $f(x) \leqslant g(x)$ для всех $x \in [0, 1]$. Другие примеры приведены в упражнениях.

Предложение 1. *Если G — частично упорядоченная группа, $a, b \in G$ и $a \leqslant b$, то $b^{-1} \leqslant a^{-1}$.*

Доказательство. Умножая неравенство $a \leqslant b$ слева на a^{-1} и справа на b^{-1}, последовательно получаем $1 \leqslant a^{-1}b$ и $b^{-1} \leqslant a^{-1}$.

Если G — частично упорядоченная группа, то множество

$$K = \{u \mid u \in G,\ u \geqslant 1\}$$

называется *положительным конусом*. Задание положи-

тельного конуса однозначно определяет порядок, ибо, как легко проверить, $a \leqslant b$ тогда и только тогда, когда $a^{-1}b \in K$. Положим

$$K^{-1} = \{u^{-1} \mid u \in K\}.$$

Предложение 2. *Подмножество K группы G является положительным конусом некоторого порядка, превращающего G в частично упорядоченную группу, тогда и только тогда, когда $K \cap K^{-1} = \{1\}$, $KK \subseteq K$ и $g^{-1}Kg \subseteq K$ для всех $g \in G$. Линейность этого порядка равносильна равенству $K \cup K^{-1} = G$.*

Доказательство. Если K — положительный конус, то для любых $u, v \in K$ и $g \in G$ имеем

$$uv \geqslant 1 \cdot 1 = 1$$

$$g^{-1}ug \geqslant g^{-1}g = 1,$$

т. е. $KK \subseteq K$ и $g^{-1}Kg \subseteq K$. Если $u \in K \cap K^{-1}$, то ввиду предложения 1, $u = (u^{-1})^{-1} \leqslant 1 \leqslant u$, откуда $u = 1$. В случае линейного порядка $g \notin K$ влечет $g \leqslant 1$, откуда $g \in K^{-1}$ в силу предложения 1. Допустим теперь, что группа G содержит подмножество K с указанными в формулировке свойствами, и для любых $a, b \in G$ положим $a \leqslant b$, если $a^{-1}b \in K$. Поскольку $1 \in K$, то отношение $\leqslant$ рефлексивно. Если $a \leqslant b$ и $b \leqslant a$, то $a^{-1}b, b^{-1}a \in K$. Отсюда $a^{-1}b \in K \cap K^{-1} = \{1\}$, т. е. $a = b$. Если $a \leqslant b$ и $b \leqslant c$, то $a^{-1}b, b^{-1}c \in K$, откуда $a^{-1}c \in KK \subseteq K$, т. е. $a \leqslant c$. Таким образом, $\leqslant$ — порядок. Если $a \leqslant b$, то для любого $g \in G$ имеем

$$(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in K$$

и

$$(ag)^{-1}(bg) = g^{-1}a^{-1}bg \in g^{-1}Kg \in K,$$

т. е. $ga \leqslant gb$ и $ag \leqslant bg$. Таким образом, G — частично упорядоченная группа. Ясно, что $u \in K$ равносильно $1 \cdot u \in K$, что, в свою очередь, означает, что $1 \leqslant u$. Следовательно, K совпадает с положительным конусом этой группы. Если $K \cup K^{-1} = G$, то для любых $a, b \in G$ имеем $a^{-1}b \in K$ или $b^{-1}a \in K$. Следовательно, $a \leqslant b$ или $b \leqslant a$, т. е. порядок оказывается линейным.

Следствие. *Если G — линейно упорядоченная группа, $g \in G$ и $g^n = 1$, где $n \geqslant 2$, то $g = 1$.*

Для доказательства достаточно предположить, что $g^{n-1} \neq 1$, и заметить, что, ввиду предложений 1 и 2, $g^{n-1} \in K \cap K^{-1} = \{1\}$.

Естественна задача описания *линейно упорядочиваемых групп*, т. е. групп, которые могут быть превращены в линейно упорядоченные. В качестве примера подобного результата приведем:

Теорема 1. *Абелева группа линейно упорядочиваема тогда и только тогда, когда она не содержит отличных от* 0 *элементов конечного порядка.*

Доказательство. Отсутствие в линейно упорядочиваемой группе ненулевых элементов конечного порядка вытекает из следствия предложения 2. Если же G — абелева группа, не содержащая таких элементов, то, воспользовавшись леммой 2 из доказательства теоремы IV.7.2, вложим ее в делимую группу Q. Периодические элементы группы Q образуют подгруппу T. При этом Q/T — делимая группа и $T \cap G = \{0\}$. Поэтому можно считать, что G принадлежит делимой абелевой группе, не содержащей периодических элементов, отличных от 0, т. е. делимой группе без кручения. В силу предложений IV.4.4 и IV.4.5, всякая такая группа может рассматриваться как линейное пространство над полем рациональных чисел $\mathbf{Q}$. Теперь справедливость теоремы является непосредственным следствием следующего утверждения:

Всякое линейное пространство L над полем $\mathbf{Q}$ *может быть превращено в линейно упорядоченную группу.*

Для доказательства, воспользовавшись аксиомой о полном упорядочении, предположим, что база $\mathfrak{S}$ линейного пространства L (при $L \neq \{0\}$ все очевидно) вполне упорядочена. Рассмотрим множество K, состоящее из нуля и всех таких элементов $\sum_{e \in \mathfrak{S}} \lambda_e e \in L$, что $\lambda_{e_0} > 0$, где e_0 — наименьший элемент множества $\{e \mid e \in \mathfrak{S},\ \lambda_e \neq 0\}$. Ясно, что $K \cap (-K) = \{0\}$, $K + K \subseteq K$ и $K \cup (-K) = L$. Остается принять во внимание предложение 2.

Линейно упорядоченная группа G называется *архимедовой*, если для любых $a, b \in G$, где $a \neq 1$, найдется такое целое число n, что $b \leqslant a^n$. Примером архимедовой линейно упорядоченной группы служит аддитивная группа действительных чисел. Убедимся, что, по существу, других таких групп нет.

Теорема 2 (Гельдер). *Всякая архимедова линейно упорядоченная группа G изоморфна* (как частично упорядоченная группа) *некоторой подгруппе аддитивной группы действительных чисел* $\mathbf{R}$.

Доказательство. Допустим, что G содержит элемент $g > 1$, для которого справедлива следующая импликация:

$$(1 \leqslant x < g) \Rightarrow (x = 1). \qquad (*)$$

Если $1 \neq a \in G$, то, ввиду предложения 1, $a^{\varepsilon} > 1$, где $\varepsilon = 1$ или -1. Из архимедовости вытекает существование такого $n \in \mathbf{Z}$, что $g^n \leqslant a^{\varepsilon} < g^{n+1}$. Отсюда $1 \leqslant a^{\varepsilon} g^{-n} < g$ и, в силу (*), $a = g^{n\varepsilon}$. Таким образом, G оказывается циклической группой, порожденной элементом g. При этом из предложения 2 и его следствия вытекает, что $g^n \geqslant 1$ тогда и только тогда, когда $n \geqslant 0$, а значит, $g^m \leqslant g^n$ в том и только в том случае, когда $m \leqslant n$. Следовательно, равенство $\varphi(g^n) = n$ определяет гомоморфное вложение группы G в $\mathbf{R}$, причем $g^m \leqslant g^n$ тогда и только тогда, когда $\varphi(m) \leqslant \varphi(n)$. Полученный результат позволяет предполагать, что группа G обладает следующим свойством:

если $g \in G$ и $g > 1$, то $g > x > 1$ для некоторого $x \in G$.

Если $g \leqslant x^2$, то

$$(gx^{-1})^2 = gx^{-1}gx^{-1} \leqslant gx^{-1}x^2x^{-1} = g$$

и, ввиду предложения 1, $g^{-1} < x^{-1} < 1$, откуда $1 < gx^{-1} < g$. Таким образом, для каждого $g \in G$ найдется элемент $z \in G$, обладающий следующими свойствами:

$$1 < z < g, \quad z^2 \leqslant g \qquad (**)$$

(этим элементом будет x или gx^{-1}).

Лемма 1. *G—коммутативная группа.*

Для доказательства обозначим через $\mathfrak{Z}(G)$ центр группы G и допустим, что $b \notin \mathfrak{Z}(G)$. Можно считать, что $b > 1$ и что $ab \neq ba$ для некоторого $a > 1$. Разумеется, $a \notin \mathfrak{Z}(G)$. Поэтому можно считать, что $ba < ab$. Положим $g = aba^{-1}b^{-1}$. Тогда $g = ab(ba)^{-1} > 1$. Для этого g выберем элемент z, указанный в (**). В силу архимедовости, найдутся такие натуральные числа m и n, что $z^m \leqslant a < z^{m+1}$ и $z^n \leqslant b < z^{n+1}$. Отсюда, учитывая предложение 1, получаем

$$z^2 \leqslant g = aba^{-1}b^{-1} < z^{m+1}z^{n+1}z^{-m}z^{-n} = z^2.$$

Полученное противоречие доказывает, что $G = \mathfrak{Z}(G)$, т. е. что G коммутативна.

Лемма 2. *Если* $a, b \in G$, $a < b$ *и* $m > 0$, *то* $a^m < b^m$.

Действительно, ясно, $a^m \leqslant b^m$. Если $a^m = b^m$, то, ввиду леммы 1,

$$1 = a^m b^{-m} = (ab^{-1})^m.$$

Поскольку $ab^{-1} \neq 1$, это противоречит следствию предложения 2.

Теперь зафиксируем в G элемент $a > 1$ и для любого $b \in G$ рассмотрим множества

$$U_b = \left\{ \frac{m}{n} \,\middle|\, m,\ n \in \mathbf{Z},\ n > 0,\ a^m \leqslant b^n \right\}$$

и

$$V_b = \left\{ \frac{m}{n} \,\middle|\, m,\ n \in \mathbf{Z},\ n > 0,\ a^m > b^n \right\}.$$

Ввиду архимедовости группы G, оба они непустые. Более того, если $\frac{m}{n} \in U_b$, $\frac{r}{s} \in V_b$ и $\frac{m}{n} \geqslant \frac{r}{s}$, то $ms \geqslant rn$, откуда, ввиду леммы 2, вытекает

$$b^{ns} = (b^s)^n < (a^r)^n = a^{rn} \leqslant a^{ms} = (a^m)^s \leqslant (b^n)^s = b^{ns}.$$

Таким образом, $\frac{m}{n} < \frac{r}{s}$ для любых $\frac{m}{n} \in U_b$ и $\frac{r}{s} \in V_b$, т. е. пара (U_b, V_b) образует дедекиндово сечение на множестве рациональных чисел. Пусть $\varphi(b)$ — действительное число, определяемое этим сечением. Если $\frac{m}{n} \in U_b$ и $\frac{r}{s} \in U_c$, то $a^m \leqslant b^n$ и $a^r \leqslant c^s$. Отсюда, учитывая лемму 1, получаем

$$a^{ms+nr} \leqslant b^{ns} c^{ns} = (bc)^{ns},$$

т. е.

$$U_b + U_c \subseteq U_{bc}.$$

Аналогично проверяется, что

$$V_b + V_c \subseteq V_{bc}.$$

По свойству дедекиндовых сечений,

$$U_b + U_c = U_{bc},$$

т. е.

$$\varphi(bc) = \varphi(b) + \varphi(c).$$

Таким образом, φ — гомоморфизм группы G в группу $\mathbf{R}$. Если $\varphi(b) = 0$, то $\varphi(b^{-1}) = 0$. Поэтому можно считать,

что $b > 1$. Отсюда $a \leqslant b^n$ для некоторого $n > 0$, т. е. $\frac{1}{n} \in U_b$, в то время как $\varphi(b) = 0$ означает, что U_b не содержит положительных чисел. Таким образом, φ—гомоморфное вложение. Если $b \leqslant c$ и $\frac{m}{n} \in U_b$, то $a^m \leqslant b^n \leqslant c^n$, откуда $\frac{m}{n} \in U_c$. Следовательно, $U_b \subseteq U_c$, а значит, $\varphi(b) \leqslant \varphi(c)$, т. е. φ—изотонное отображение. Если $\varphi(b) < \varphi(c)$, то

$$\varphi(b^{-1}c) = -\varphi(b) + \varphi(c) > 0.$$

Следовательно, $\frac{1}{n} \in U_{b^{-1}c}$ для некоторого n. Отсюда

$$1 < a \leqslant (b^{-1}c)^n.$$

Ясно, что неравенство $b^{-1}c \leqslant 1$ влечет $(b^{-1}c)^n \leqslant 1$. Поэтому $b^{-1}c > 1$, откуда $b < c$, чем и завершается доказательство теоремы.

Упражнения

1. Убедиться, что приведенная ниже таблица дает примеры частично упорядоченных групп ($\mathbf{R}$—множество всех действительных чисел). Какие из этих групп являются линейно упорядоченными?

	Группа	Порядок
1.	$\mathbf{R} \times \mathbf{R}$ относительно сложения.	$(a, b) \leqslant (c, d)$, если или $a < c$, или $a = c$ и $b \leqslant d$.
2.	Мультипликативная группа положительных рациональных чисел.	$a \leqslant b$, если a/b—целое число.
3.	Отображения плоскости на себя, определяемые равенствами вида $\varphi(x) = ax + b$, где $a, b \in \mathbf{R}$ и $a > 0$, с обычным умножением отображений.	$\varphi \leqslant \psi$, если $\varphi = ax + b$, $\psi = cx + d$, причем или $a < c$, или $a = c$ и $b \leqslant d$.
4.	Матрица вида $\begin{Vmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{Vmatrix}$, где $a, b, c \in \mathbf{R}$, с операцией умножения.	$\begin{Vmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{Vmatrix} \leqslant \begin{Vmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{Vmatrix}$, если или $a < a'$, или $a = a'$ и $b < b'$, или $a = a'$, $b = b'$ и $c \leqslant c'$.
5.	$\mathbf{R} \times \mathbf{R}$ с операцией сложения	$(a, b) \leqslant (c, d)$, если $a = c$ и $b \leqslant d$.

2. Всякая свободная группа линейно упорядочиваема. Указание. Взять в качестве положительного конуса множество всех слов вида $x_1^{k_1}\dots x_m^{k_m}$, где $k_1+\dots+k_m\geqslant 0$.

3. Подмножество H частично упорядоченной группы G называется *выпуклым*, если $a\leqslant x\leqslant b$ и $a,\ b\in H$ влечет $x\in H$. Если H — выпуклая нормальная подгруппа частично упорядоченной группы G, то определение: $aH\leqslant bH$, если существуют $u\in aH$ и $v\in bH$ такие, что $u\leqslant v$, превращает фактор-группу G/H в частично упорядоченную группу. Сформулировать и доказать для частично упорядоченных групп аналог теоремы о гомоморфизме.

4. Если частично упорядочеиная группа содержит наибольший или наименьший элемент, то она одноэлементна.

5. Линейно упорядоченная группа, в которой каждое ограниченное подмножество имеет как точную верхнюю, так и точную нижнюю грани (напомним, что непустое подмножество A частично упорядоченного множества P называется *ограниченным*, если найдутся $b,\ c\in P$ такие, что $b\leqslant x\leqslant c$ для всех $x\in A$), или одноэлементна, или изоморфна аддитивной группе всех целых или всех действительных чисел.

6. Частично упорядоченная группа называется *l-группой* (или *структурно упорядоченной группой*), если ее частично упорядоченное множество является структурой. Операции взятия точной верхней и точной нижней граней в этой структуре будем обозначать символами $\vee$ и $\wedge$ соответственно. Заметим, что l-группа является универсальной алгеброй сигнатуры $\{\cdot,\ ^{-1},\ 1,\ \vee,\ \wedge\}$. Выяснить, какие из частично упорядочеиных групп упражнения 1 являются l-группами. Доказать:

а) Частично упорядоченная коммутативная группа является l-группой тогда и только тогда, когда ее положительный конус является структурой (отиосительно индуцнрованиого порядка) и порождает группу;

б) в любой l-группе выполняются тождества

$$a\,(x\wedge y)^{-1}\,b=(ax^{-1}b)\vee(ay^{-1}b)$$

и

$$a\,(a\wedge b)^{-1}\,b=a\vee b.$$

в) В любой коммутативной l-группе справедливо тождество

$$ab=(a\vee b)\,(a\wedge b).$$

г) Всякая коммутативная l-группа является дистрибутивной структурой.

7. При любых натуральных m и n для любых элементов a и b линейно упорядочениой группы справедлива импликация

$$(a^mb^n=b^na^m)\Rightarrow(ab=ba).$$

8. Структурно упорядоченная группа является линейно упорядоченной тогда и только тогда, когда для любых ее элементов a и b справедлива имплнкация

$$(a,\ b>1)\Rightarrow(a\wedge b>1).$$

§ 2. Нормированные кольца

Ассоциативное кольцо R называется *нормированным*, если каждому $a \in R$ поставлено в соответствие неотрицательное действительное число $\|a\|$ (оно называется *нормой* элемента a) причем:

(1) $\|a\| = 0$ тогда и только тогда, когда $a = 0$;

(2) $\|a+b\| \leqslant \|a\| + \|b\|$ для любых a, $b \in R$;

(3) $\|ab\| = \|a\| \cdot \|b\|$ для любых a, $b \in R$.

В качестве примеров нормированных колец можно указать поля действительных и компексных чисел, где $\|a\|$—модуль числа a. Непосредственно из определения вытекает, что нормированное кольцо не содержит делителей нуля и что $\|1\| = 1$ (достаточно в (3) положить $a = b = 1$), откуда $\|1\| = \|-1\|$ (следует положить в (3) $a = b = -1$). Теперь, полагая в (3) $b = -1$, получим $\|a\| = \|-a\|$. Наконец, из (2) вытекает

$$\|a\| = \|(a-b)+b\| \leqslant \|a-b\| + \|b\|,$$

откуда

$$\|a\| - \|b\| \leqslant \|a-b\|.$$

Вместе с $\|b\| - \|a\| \leqslant \|b-a\| = \|a-b\|$ это дает

$$|\|a\| - \|b\|| \leqslant \|a-b\|.$$

Всякое кольцо без делителей нуля становится нормированным, если положить $\|0\| = 0$ и $\|a\| = 1$ при $a \neq 0$. Такую норму назовем *тривиальной*. Норма называется *неархимедовой*, если вместо (2) выполняется более сильное условие

$$(2') \qquad \|a+b\| \leqslant \max\{\|a\|, \|b\|\}.$$

В качестве примера кольца с неархимедовой нормой рассмотрим кольцо целых чисел, зафиксируем простое число p и для каждого целого числа $m \neq 0$ положим $\|m\| = 2^{-k}$, где k—количество сомножителей p, входящих в m. Кроме того, пусть $\|0\| = 0$. Справедливость свойств (1) и (3) очевидна. Если $m = p^k m'$, $n = p^l n'$, НОД$(m', p) =$ $=$ НОД$(n', p) = 1$ и $k \leqslant l$, то

$$m+n = p^k (m' + p^{l-k} n'),$$

откуда $\|m+n\| \leqslant 2^{-k}$, причем $2^{-k} \geqslant 2^{-l}$, т. е. выполнено свойство (2'). Введенную норму можно распространить

на поле рациональных чисел, положив

$$\left\|\frac{m}{n}\right\| = \frac{\|m\|}{\|n\|}.$$

Сохранение свойств (1) и (3) очевидно. Кроме того,

$$\left\|\frac{m}{n}+\frac{s}{t}\right\| = \frac{\|mt+sn\|}{\|nt\|} \leqslant \max\left\{\frac{\|mt\|}{\|nt\|}, \frac{\|sn\|}{\|nt\|}\right\} = \max\left\{\left\|\frac{m}{n}\right\|, \left\|\frac{s}{t}\right\|\right\},$$

т. е. свойство (2′) также сохраняется. Определенная таким образом норма называется *p-адической*. Приведенными примерами, по существу, исчерпываются все возможности для нормирования поля рациональных чисел. Именно, имеет место:

Теорема 1. *Если* $\|\ \|$*—нетривиальная норма на поле рациональных чисел, то или*

$$\|\ \| = |\ |^{\rho},$$

где $0 < \rho \leqslant 1$, *или*

$$\|\ \| \leqslant |\ |^{\sigma},$$

где $|\ |$*—p-адическая норма для некоторого простого числа* p, *а* $\sigma > 0$.

Доказательство. Установим сначала несколько лемм.

Лемма 1. $\|n\| \leqslant n$ *для любого натурального* n.

Действительно, вспоминая, что $\|1\| = 1$, и, используя (2), получаем

$$\|n\| = \|\underbrace{1+\ldots+1}_{n \text{ раз}}\| \leqslant \underbrace{\|1\|+\ldots+\|1\|}_{n \text{ раз}} = n.$$

Лемма 2. *Если* α, β *и* γ*—положительные действительные числа и* $\gamma^n \leqslant n\alpha+\beta$ *для каждого натурального* n, *то* $\gamma \leqslant 1$.

Для доказательства допустим, что $\gamma = 1+\delta$, где $\delta > 0$. Если $n \geqslant 2$, то

$$\gamma^n = (1+\delta)^n = 1+n\delta+C_n^2\delta^2+\ldots > n\delta+\frac{n(n-1)}{2}\delta^2.$$

Кроме того, для достаточно больших n имеем

$$n\delta > \beta \quad \text{и} \quad \frac{1}{2}(n-1)\delta^2 > \alpha.$$

Отсюда

$$\gamma^n > \beta + n\alpha,$$

что противоречит условию.

Лемма 3. *Если* $\|n\| \leqslant 1$ *для всех натуральных* n, *то норма* $\|\ \|$ *неархимедова.*

В самом деле, при выполнении условий леммы для любого натурального n и любых рациональных чисел a и b имеем

$$\begin{aligned}\|a+b\|^n &= \|(a+b)^n\| = \\ &= \|a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \ldots + C_n^{n-1}ab^{n-1} + b^n\| \leqslant \\ &\leqslant \|a\|^n + \|C_n^1\|\|a\|^{n-1}\|b\| + \|C_n^2\|\|a\|^{n-2}\|b\|^2 + \ldots \\ &\quad \ldots + \|C_n^{n-1}\|\|a\|\|b\|^{n-1} + \|b\|^n \leqslant \\ &\leqslant \|a\|^n + \|a\|^{n-1}\|b\| + \|a\|^{n-2}\|b\|^2 + \ldots \\ &\quad \ldots + \|a\|\|b\|^{n-1} + \|b\|^n \leqslant (n+1)M^n,\end{aligned}$$

где $M = \max\{\|a\|, \|b\|\}$. Отсюда $\left(\frac{\|a+b\|}{M}\right)^n \leqslant n1 + 1$, что, ввиду леммы 2, влечет

$$\frac{\|a+b\|}{M} \leqslant 1,$$

т. е.

$$\|a+b\| \leqslant M = \max\{\|a\|, \|b\|\}.$$

Лемма 4. *Если* k *и* l *— натуральные числа, причем* $k, l > 1$, *то*

$$\|l\| \leqslant \max\left\{1, \|k\|^{\frac{\log l}{\log k}}\right\},$$

где логарифм берется по произвольному основанию, большему 1.

Для доказательства запишем

$$l^n = c_0 + c_1 k + \ldots + c_m k^m,$$

где n — натуральное число, $0 \leqslant c_i < k$ и $c_m \neq 0$. Отсюда

$$k^m \leqslant l^n,$$

а значит,

$$m \leqslant n\frac{\log l}{\log k}.$$

Положив $M=\max\{1, \|k\|\}$ и используя лемму 1, получим

$$\|l^n\| \leqslant \|c_0\| + \|c_1\| \cdot \|k\| + \ldots + \|c_m\| \cdot \|k\|^m < \\ < k(1 + \|k\| + \ldots + \|k\|^m) \leqslant k(m+1) M^m.$$

Отсюда

$$\|l\|^n < k\left(n \frac{\log l}{\log k} + 1\right) M^{n \frac{\log l}{\log k}},$$

а значит,

$$\left(\frac{\|l\|}{M^{\frac{\log l}{\log k}}}\right)^n < nk \frac{\log l}{\log k} + k.$$

В силу произвольности n, можно применить лемму 2, дающую

$$\|l\| \leqslant M^{\frac{\log l}{\log k}} = \max\left\{1, \|k\|^{\frac{\log l}{\log k}}\right\}.$$

Вернемся к доказательству теоремы. Допустим сначала, что $\|m\| > 1$ для некоторого натурального m. Если $\|n\| \leqslant 1$ для некоторого натурального $n > 1$, то, в силу леммы 4, получаем

$$1 < \|m\| \leqslant \max\left\{1, \|n\|^{\frac{\log m}{\log n}}\right\} \leqslant 1.$$

Следовательно, $\|n\| > 1$ для всех натуральных $n > 1$. Еще раз применив лемму 4, для любых m и n получаем

$$\|m\| \leqslant \|n\|^{\frac{\log m}{\log n}}.$$

Отсюда

$$\|m\|^{\frac{1}{\log m}} \leqslant \|n\|^{\frac{1}{\log n}},$$

что, ввиду равноправия m и n, дает

$$\|m\|^{\frac{1}{\log m}} = \|n\|^{\frac{1}{\log n}}.$$

Если $\|2\| = 2^\rho$, то для любого натурального $m > 1$ имеем

$$\|m\| = \|2\|^{\frac{\log m}{\log 2}} = \left(2^{\frac{\log m}{\log 2}}\right)^\rho = m^\rho.$$

Поэтому $\|m\| = |m|^\rho$ для всякого целого m, а значит $\|a\| = |a|^\rho$ для всякого рационального числа a. При этом

$0 < \rho \leqslant 1$, ибо, ввиду леммы 1,

$$1 < \|2\| = 2^{\rho} = \|2\| \leqslant 2.$$

Допустим теперь, что $\|m\| \leqslant 1$ для всех натуральных m. По лемме 3, $\|\ \|$ — неархимедова норма. Поэтому множество

$$I = \{m \mid m \in \mathbf{Z},\ \|m\| < 1\}$$

оказывается идеалом в кольце $\mathbf{Z}$. Этот идеал прост, ибо $\|mn\| < 1$, очевидно, влечет $\|m\| < 1$ или $\|n\| < 1$. Следовательно, $I = \mathbf{Z}p$, где p — простое число. Разумеется $\|p\| = 2^{-\sigma}$ для некоторого $\sigma > 0$. Каждое рациональное число a единственным способом представляется в виде $a = \frac{m}{n} p^k$, где $m, n, k \in \mathbf{Z}$, $n > 0$ и $\mathrm{HOD}(m, p) = \mathrm{HOD}(n, p) = 1$. Тогда $m, n \notin I$ и, следовательно, $\|m\| = \|n\| = 1$. Таким образом,

$$\|a\| = \|p\|^k = 2^{-\sigma k} = |a|^{\sigma},$$

т. е. $\|\ \| = |\ |^{\sigma}$.

Элемент a нормированного кольца R называется *пределом* последовательности $a_1, a_2, \ldots$, где $a_i \in R$ (в обозначениях, $\lim\limits_{i \to \infty} a_i = a$), если для каждого $\varepsilon > 0$ найдется такой номер n, что $\|a - a_i\| < \varepsilon$ для всех $i > n$.

Предложение 1. *Пусть* $a = \lim\limits_{i \to \infty} a_i$ *и* $b = \lim\limits_{i \to \infty} b_i$. *Тогда*: (а) $\lim\limits_{i \to \infty} (a_i + b_i) = a + b$; (б) $\lim\limits_{i \to \infty} \|a_i\| = \|a\|$; (в) $\lim\limits_{i \to \infty} a_i b_i = ab$.

Доказательство. (а) Если $\varepsilon > 0$, то для достаточно больших i имеем $\|a - a_i\|, \|b - b_i\| < \frac{\varepsilon}{2}$, откуда $\|(a + b) - (a_i + b_i)\| < \varepsilon$.

(б) Сразу следует из неравенства $|\|a\| - \|a_i\|| \leqslant \|a - a_i\|$, установленного в начале параграфа.

(в) Ввиду (б), $\|a_i\|, \|b_i\| < C$ для всех i и подходящего числа C. Для достаточно больших i имеем $\|a - a_i\|, \|b - b_i\| < \frac{\varepsilon}{2C}$, откуда

$$\|ab - a_i b_i\| \leqslant \|a - a_i\| \cdot \|b\| + \|a_i\| \cdot \|b - b_i\| < \frac{\varepsilon}{2C} C + \frac{\varepsilon}{2C} C = \varepsilon.$$

Последовательность $a_1, a_2, \ldots$ элементов нормированного кольца называется *последовательностью Коши*, если для любого $\varepsilon > 0$ найдется такой номер n, что $i, j > n$ влечет $\|a_i - a_j\| < \varepsilon$.

Предложение 2. *Если* $a_1, a_2, \ldots$ *— последовательность Коши, то* $\lim\limits_{i\to\infty}\|a_i\|=\alpha$ *для некоторого действительного числа* α *и множество* $\{\|a_i\|\,|\,i=1, 2, \ldots\}$ *ограничено.*

Доказательство. Как уже отмечалось, непосредственным следствием определения нормированного кольца является неравенство $|\|a_i\|-\|a_j\||\leqslant\|a_i-a_j\|$. Поэтому последовательность действительных чисел $\|a_1\|, \|a_2\|, \ldots$ является последовательностью Коши. Хорошо известно, что всякая такая последовательность ограничена и имеет предел.

Нормированное кольцо R называется *полным*, если всякая последовательность Коши элементов из R имеет предел. Полное кольцо $\hat{R}$ называется *пополнением* нормированного кольца R, если $R\subseteq\hat{R}$ и каждый элемент из $\hat{R}$ является пределом некоторой последовательности элементов из R.

Теорема 2. *Каждое нормированное кольцо* R *обладает пополнением* $\hat{R}$. *Если* R *— коммутативное кольцо, тело или поле, то* $\hat{R}$ *является коммутативным кольцом, телом или полем соответственно.*

Доказательство. Установим сначала справедливость второго утверждения. Если R коммутативно и $a, b\in\hat{R}$, то $a=\lim\limits_{i\to\infty}a_i$ и $b=\lim\limits_{i\to\infty}b_i$, где $a_i,\ b_i\in R$. Тогда

$$ab-ba=\lim_{i\to\infty}(a_ib_i-b_ia_i)=0.$$

Если R — тело и $0\neq a\in\hat{R}$, то $a=\lim\limits_{i\to\infty}a_i$, где $a_i\in R$. Тогда $\lim\limits_{i\to\infty}\|a_i\|=\|a\|\neq 0$, это позволяет считать, что $\|a_i\|\geqslant\alpha$ для некоторого $\alpha>0$ при любом i. Если $\varepsilon>0$, то выберем n так, что

$$\|a_i-a_j\|<\varepsilon\alpha^2$$

для любых $i, j>n$. Поскольку $\|a_i\|\cdot\|a_i^{-1}\|=1$ для всех i, то отсюда вытекает

$$\|a_i^{-1}-a_j^{-1}\|=\|a_i^{-1}(a_j-a_i)a_j^{-1}\|=$$
$$=\frac{1}{\|a_i\|\cdot\|a_j\|}\|a_i-a_j\|<\frac{1}{\alpha^2}\varepsilon\alpha^2=\varepsilon.$$

Следовательно, $a_1^{-1}, a_2^{-1}, \ldots$ — последовательность Коши и, в силу полноты кольца $\hat{R}$, $b=\lim\limits_{i\to\infty}a_i^{-1}$ для некоторого

$b \in \hat{R}$. Ясно, что

$$ab = \lim_{i \to \infty} a_i a_i^{-1} = 1 = \lim_{i \to \infty} a_i^{-1} a_i = ba,$$

т. е. $\hat{R}$ — тело. Если R — поле, то, в силу доказанного, $\hat{R}$ — коммутативное тело, т. е. поле.

Существование пополнения является непосредственным следствием следующего предложения:

Предложение 3. *Последовательности Коши из нормированного кольца R образуют подкольцо R_K^∞ кольца R^∞ последовательностей из R. При этом:*

(1) *Отображение* φ, *где*

$$\varphi(a) = (a, a, \ldots)$$

для каждого $a \in R$, является гомоморфным вложением кольца R в R_K^∞;

(2) *Множество*

$$I = \{\bar{a} \mid \bar{a} \in R_K^\infty,\ \forall \varepsilon > 0\, \exists n\, \forall i > n\, (\|a_i\| < \varepsilon)\}$$

является идеалом кольца R_K^∞, причем $\varphi(R) \cap I = 0$.

(3) *Фактор-кольцо $\hat{R} = R_K^\infty / I$ является пополнением кольца R, если определить норму равенством*

$$\|\bar{a} + I\| = \lim_{i \to \infty} \|a_i\|$$

для каждой $\bar{a} = (a_1, a_2, \ldots) \in R_K^\infty$.

Доказательство. Если $\bar{a}, \bar{b} \in R_K^\infty$ и $\varepsilon > 0$, то найдем такой номер n, что $i, j > n$ влечет $\|a_i - a_j\|, \|b_i - b_j\| < \frac{\varepsilon}{2}$. Тогда

$$\|(a_i + b_i) - (a_j + b_j)\| \leqslant \|a_i - a_j\| + \|b_i - b_j\| < \varepsilon,$$

т. е. $\bar{a} + \bar{b} \in R_K^\infty$. Далее, ввиду предложения 2, для некоторого $C > 0$ имеем $\|a_i\|, \|b_j\| < C$ для любых i и j. Если теперь $\varepsilon > 0$, то выберем номер n так, что $\|a_i - a_j\|$, $\|b_i - b_j\| < \frac{\varepsilon}{2C}$ для любых $i, j > n$. Тогда

$$\|a_i b_i - a_j b_j\| = \|a_i (b_i - b_j) + (a_i - a_j) b_j\| \leqslant$$
$$\leqslant \|a_i\| \cdot \|b_i - b_j\| + \|a_i - a_j\| \cdot \|b_j\| < C \frac{\varepsilon}{2C} + \frac{\varepsilon}{2C} C = \varepsilon,$$

т. е. $\bar{a}\bar{b} \in R_K^\infty$. Итак, R_K^∞ — подкольцо в R^∞. Ясно, что φ — гомоморфное вложение и что $\bar{a}, \bar{b} \in I$ влечет $\bar{a} + \bar{b} \in I$.

Если же $\bar{a}\in I$ и $\bar{b}\in R_K^\infty$, то, как уже отмечалось, числа $\|b_i\|$ ограничены некоторым $C>0$. Поэтому, взяв $\varepsilon>0$, найдем номер n такой, что $\|a_i\|<\frac{\varepsilon}{C}$ для всех $i>n$. Тогда

$$\|a_ib_i\|=\|a_i\|\|b_i\|=\frac{\varepsilon}{C}C=\varepsilon$$

и

$$\|b_ia_i\|=\|b_i\|\|a_i\|<C\frac{\varepsilon}{C}=\varepsilon$$

для всех $i>n$, т. е. $\bar{a}\bar{b}$, $\bar{b}\bar{a}\in I$. Наконец, если $a\in R$ и $\varphi(a)\in I$, то $\|a\|<\varepsilon$ для любого $\varepsilon>0$, откуда $\|a\|=0$, а значит, и $a=0$. Таким образом, φ индуцирует гомоморфное вложение кольца R в кольцо $\hat{R}$.

Убедимся теперь, что $\hat{R}$ — нормированное кольцо. Для сокращения записи положим $[\bar{a}]=\bar{a}+I$ для каждого $\bar{a}\in R_K^\infty$. Если $[\bar{a}]=[\bar{b}]$, то $\lim\limits_{i\to\infty}\|a_i-b_i\|=0$ и, учитывая неравенство $|\|a_i\|-\|b_i\||<\|a_i-b_i\|$, получаем, что $\lim\limits_{i\to\infty}\|a_i\|=\lim\limits_{i\to\infty}\|b_i\|$. Этим доказана корректность определения нормы в кольце $\hat{R}$. Далее, ясно, что $\|[\bar{0}]\|=0$. Если же $\|[\bar{a}]\|=0$, то $\lim\limits_{i\to\infty}\|a_i\|=0$, откуда $[\bar{a}]=0$. Кроме того,

$$\|[\bar{a}]+[\bar{b}]\|=\|[\bar{a}+\bar{b}]\|=\lim_{i\to\infty}\|a_i+b_i\|\leqslant\lim_{i\to\infty}(\|a_i\|+\|b_i\|)=$$
$$=\lim_{i\to\infty}\|a_i\|+\lim_{i\to\infty}\|b_i\|=\|[\bar{a}]\|+\|[\bar{b}]\|,$$

$$\|[\bar{a}][\bar{b}]\|=\|[\bar{a}\bar{b}]\|=\lim_{i\to\infty}\|a_ib_i\|=\lim_{i\to\infty}\|a_i\|\cdot\|b_i\|=$$
$$=\lim_{i\to\infty}\|a_i\|\lim_{i\to\infty}\|b_i\|=\|[\bar{a}]\|\cdot\|[\bar{b}]\|$$

и $\|[\varphi(a)]\|=\|a\|$ для всех $a\in R$. Так что $\hat{R}$ — нормированное кольцо, причем R вкладывается в него как подкольцо с сохранением нормы. Если $[\bar{a}]\in\hat{R}$, то для любого $\varepsilon>0$ при подходящем числе n для любых i, $j>n$ имеем $\|a_j-a_i\|<\frac{\varepsilon}{2}$. Поэтому, если $i>n$, то

$$\|[\bar{a}]-[\varphi(a_i)]\|=\lim_{j\to\infty}\|a_j-a_i\|\leqslant\frac{\varepsilon}{2}<\varepsilon,$$

т. е. $[\bar{a}]=\lim\limits_{i\to\infty}[\varphi(a_i)]$. Таким образом, остается лишь доказать полноту кольца $\hat{R}$. С этой целью назовем последовательность Коши $b=(b_1, b_2, \ldots)$ *приведенной*, если $\|b_k-b_{k+s}\|<\frac{1}{2^{k+1}}$ для любых k, $s\geqslant 1$.

Лемма. *Если* $\bar{a}=(a_1, a_2, \ldots)$ — *последовательность Коши из* R_K^∞, *то* $[\bar{a}]=[\bar{b}]$, *где* $\bar{b}$ — *подходящая приведенная последовательность Коши.*

Для доказательства выберем числа $m_1<m_2<\ldots$ так, что

$$\|a_{m_j}-a_{m_j+r}\|<\frac{1}{2^{j+1}}$$

для всех $r\geqslant 0$ и положим

$$\bar{b}=(a_{m_1}, a_{m_2}, \ldots).$$

Тогда

$$\|\bar{a}-\bar{b}\|=\lim_{k\to\infty}\|a_k-a_{m_k}\|=0,$$

ибо $m_k\geqslant k$ и $\bar{a}$ — последовательность Коши. Отсюда $\bar{a}-\bar{b}\in I$ и, следовательно, $[\bar{a}]=[\bar{b}]$.

Пусть теперь

$$\alpha=([\bar{a}_1], [\bar{a}_2], \ldots)$$

— последовательность Коши в кольце $\hat{R}$ и

$$\bar{a}_i=(a_{i1}, a_{i2}, \ldots).$$

Ввиду леммы, последовательности $\bar{a}_i$ можно считать приведенными. Выберем числа $m_1<m_2<\ldots$ так, что

$$\|[\bar{a}_{m_k}]-[\bar{a}_{m_k+s}]\|<\frac{1}{2^{k+1}} \qquad (*)$$

для всех $s\geqslant 0$, и докажем, что

$$\|a_{m_k i}-a_{m_k+s\,j}\|<\frac{1}{2^{k-1}} \qquad (**)$$

для любых $s>0$ и i, $j\geqslant k$. В самом деле, поскольку

$$\|[\bar{a}_{m_k}]-[\bar{a}_{m_k+s}]\|=\lim_{h\to\infty}\|a_{m_k h}-a_{m_k+s\,h}\|,$$

то для некоторого $h > k$ получаем

$$\left|\|[\bar{a}_{m_k}]-[\bar{a}_{m_k+s}]\|-\|a_{m_k h}-a_{m_k+s\,h}\|\right| < \frac{1}{2^{k+1}}.$$

Учитывая приведенность последовательностей $\bar{a}_i$ и неравенство (*), получаем

$$\begin{aligned}\|a_{m_k i}-a_{m_k+s\,j}\| &\leqslant \|a_{m_k i}-a_{m_k h}\|+\\ &+\left|\|a_{m_k h}-a_{m_k+s\,h}\|-\|[\bar{a}_{m_k}]-[\bar{a}_{m_k+s}]\|\right|+\\ &+\|[\bar{a}_{m_k}]-[\bar{a}_{m_k+s}]\|+\|a_{m_k+s\,h}-a_{m_k+s\,j}\|<\\ &<\frac{1}{2^{k+1}}+\frac{1}{2^{k+1}}+\frac{1}{2^{k+1}}+\frac{1}{2^{k+1}}=\frac{1}{2^{k-1}},\end{aligned}$$

что доказывает (**). Из (**) вытекает, что

$$\|a_{m_k m_k}-a_{m_k+s\,m_k+s}\|<\frac{1}{2^{k-1}},$$

т. е. последовательность

$$\bar{a}=(a_{11},\ a_{22},\ \ldots)$$

оказывается последовательностью Коши в кольце R. Еще раз используя (**), получаем, что

$$\|[\bar{a}]-[\bar{a}_{m_k}]\|=\lim_{j\to\infty}\|a_{jj}-a_{m_k j}\|\leqslant\frac{1}{2^{k-1}},$$

откуда при $i > m_k$, используя (*), выводим

$$\|[\bar{a}]-[\bar{a}_i]\|\leqslant\|[\bar{a}]-[\bar{a}_{m_k}]\|+\|[\bar{a}_{m_k}]-[\bar{a}_i]\|<\frac{1}{2^{k-2}}.$$

Следовательно, $[\bar{a}]=\lim\limits_{i\to\infty}[\bar{a}_i]$, что доказывает полноту кольца $\hat{R}$.

Упражнения

1. Доказать, что определение $\|f\|=2^{\text{степень } f}$ превращает кольцо многочленов над полем в нормированное кольцо (предполагается, что (степень 0) $=-\infty$).

2. Если R — неархимедово нормированное кольцо, то ряд $a_0+a_1+a_2+\ldots$, где $a_i\in R$, сходится тогда и только тогда, когда $\lim\limits_{i\to\infty} a_i=0$.

3. Если $\hat{R}$ — пополненне нормированного кольца R, то всякий гомоморфизм φ кольца R в полное нормированное кольцо R', удов-

летворяющий условию $\|\varphi(a)\| \leqslant \|a\|$ для всех $a \in R$, однозначно продолжается до гомоморфизма кольца $\hat{R}$ в R'.

4. Доказать, что пополнение нормированного кольца определяется однозначно с точностью до изоморфизма.

5. Пополнение кольца целых чисел с p-адической нормой называется *кольцом целых p-адических чисел*. Доказать, что кольцо изоморфно кольцу степенных рядов $a_0 + a_1 p + a_2 p^2 + \ldots$, где $0 \leqslant a_i < p$. Указание. Представить описанным способом целые числа и заметить, что в последовательности Коши целых чисел каждый из коэффициентов при p стабилизируется на конечном шаге.

6. Пополнение поля рациональных чисел с p-адической нормой называется *полем p-адических чисел*. Доказать, что это поле изоморфно полю рядов вида $a_m p^m + a_{m+1} p^{m+1} + \ldots$, где m, $a_i \in \mathbf{Z}$, $a_m \neq 0$ и $0 \leqslant a_i < p$.

7. Если в определении p-адической нормы отказаться от требования простоты числа p, то возникает *псевдо-норма*, т. е. вместо (3) выполняется $\|ab\| \leqslant \|a\| \cdot \|b\|$.

8. Ранг матрицы является псевдо-нормой кольца матриц над полем.

9. Доказать аналог теоремы 2 для колец с псевдо-нормой.

§ 3. Топологические кольца

Напомним, что множество M называется *топологическим пространством* (точнее, отделимым топологическим пространством), если на полной структуре всех подмножеств множества M определен оператор замыкания τ, причем $\tau(X \cup Y) = \tau(X) \cup \tau(Y)$ для любых X, $Y \subseteq M$ и $\tau\{x\} = \{x\}$ для любого $x \in M$. Каждый такой оператор замыкания называется *топологией* на множестве M. Топология называется *дискретной*, если $\tau(X) = X$ для всех $X \subseteq M$. Подмножества X, для которых $\tau(X) = X$, называются *замкнутыми* (в частности, в случае дискретной топологии все подмножества замкнуты), а дополнения замкнутых множеств — *открытыми*. *Окрестностью* элемента $x \in M$ называется всякое множество, которое содержит открытое множество, включающее в себя элемент x. Отображение φ топологического пространства M в топологическое пространство M' называется *непрерывным*, если для любого $x \in M$ и любой окрестности U' элемента $\varphi(x)$ найдется такая окрестность U элемента x, что $\varphi(U) \subseteq U'$.

Предложение 1. *Для совпадения двух топологий на множестве M необходимо и достаточно, чтобы совпадали множества открытых [замкнутых множеств этих топологий.*

Доказательство. Необходимость условия очевидна. Достаточность вытекает из следствия предложения I.3.4.

Предложение 2. *Система* Σ *подмножеств множества* M *совпадает с системой всех замкнутых подмножеств для некоторой топологии на* M *тогда и только тогда, когда* Σ *обладает следующими свойствами*: (i) $M \in \Sigma$; (ii) *если* $A_\iota \in \Sigma$, $\iota \in \mathfrak{I}$, *то* $\bigcap_{\iota \in \mathfrak{I}} A_\iota \in \Sigma$; (iii) *если* $A, B \in \Sigma$, *то* $A \cup B \in \Sigma$; (iv) *все одноэлементные подмножества множества* M *принадлежат* Σ.

Доказательство. Справедливость свойств (i) и (ii) для системы замкнутых множеств вытекает из предложения I.3.5, а свойства (iii) и (iv) являются непосредственным следствием определения. Если, наоборот, задана система Σ со свойствами (i)—(iv), то для каждого $X \subseteq M$ положим

$$\tau(X) = \bigcap_{X \subseteq A \in \Sigma} A.$$

В силу предложения I.3.5, τ — оператор замыкания. Поэтому из включений $X \subseteq X \cup Y$ и $Y \subseteq X \cup Y$ вытекает, что

$$\tau(X) \cup \tau(Y) \subseteq \tau(X \cup Y)$$

для любых X, $Y \subseteq M$. С другой стороны, имея $\tau(X)$, $\tau(Y) \in \Sigma$ и учитывая (iii), получаем

$$\tau(X \cup Y) \subseteq \tau(X) \cup \tau(Y).$$

Следовательно,

$$\tau(X \cup Y) = \tau(X) \cup \tau(Y).$$

Наконец, $\tau(\{x\}) = \{x\}$ для всех $x \in M$, ввиду (iv).

Из предложения 2 и определения открытого множества вытекает:

Предложение 3. *Система* Σ *подмножеств множества* M *совпадает с системой всех открытых подмножеств для некоторой топологии на* M *тогда и только тогда, когда* Σ *обладает следующими свойствами*: (i*) $\varnothing \in \Sigma$; (ii*) *если* $U_\iota \in \Sigma$, $\iota \in \mathfrak{I}$, *то* $\bigcup_{\iota \in \mathfrak{I}} U_\iota \in \Sigma$; (iii*) *если* $U, V \in \Sigma$, *то* $U \cap V \in \Sigma$; (iv*) *все дополнения одноэлементных подмножеств множества* M *принадлежат* Σ.

Предложение 4. *Подмножество* U *топологического пространства* M *открыто в том и только в том*

случае, когда для любого $x \in U$ найдется окрестность элемента x, принадлежащая U.

Доказательство. Если U открыто, то оно является окрестностью любого из своих элементов. Наоборот, если выполнены условия предложения, то для любого $x \in U$ можно найти его окрестность W_x, принадлежащую U. По определению окрестности, $x \in U_x \subseteq W_x$ для некоторого открытого множества U_x. Отсюда

$$U \subseteq \bigcup_{x \in U} U_x \subseteq \bigcup_{x \in U} W_x \subseteq U.$$

Следовательно, $U = \bigcup_{x \in U} U_x$, и U открыто по предложению 3 (ii*).

Система Σ окрестностей элемента x топологического пространства называется *базой окрестностей элемента x*, если каждая окрестность этого элемента содержит некоторую окрестность из Σ.

Предложение 5. *Пусть каждому элементу x множества M поставлена в соответствие некоторая система Σ_x подмножеств множества M. Для существования на множестве M такой топологии, что для каждого $x \in M$ система Σ_x является базой окрестностей элемента x, необходимо и достаточно, чтобы для каждого $x \in M$ была справедлива импликация*

$$((U \in \Sigma_x) \,\&\, (V \in \Sigma_x)) \Rightarrow (\exists W \in \Sigma_x\, (W \subseteq U \cap V))$$

и

$$\bigcap_{U \in \Sigma_x} U = \{x\}.$$

Доказательство. Если M — топологическое пространство и Σ_x — база окрестностей элемента $x \in M$, то

$$\{x\} \subseteq \bigcap_{U \in \Sigma_x} U \subseteq \bigcap_{x \neq y \in M} (M \setminus \{y\}) = M \setminus \Big(\bigcup_{x \neq y \in M} \{y\}\Big) = \{x\},$$

т. е.

$$\bigcap_{U \in \Sigma_x} U = \{x\}.$$

Если же $U, V \in \Sigma_x$, то для подходящих открытых множеств U' и V' имеем $x \in U' \subseteq U$ и $x \in V' \subseteq V$. В силу предложения 3 (iii*), $U' \cap V'$ — открытое множество и, поскольку $x \in U' \cap V'$, — окрестность элемента x. Поэтому $W \subseteq U' \cap V' \subseteq U \cap V$ для некоторого $W \in \Sigma_x$. Допустим теперь, что системы Σ_x обладают указанными в форму-

лировке свойствами. Обозначим через Σ^0 систему всех подмножеств W множества M, обладающих следующим свойством: если $x \in W$, то $x \in U \subseteq W$ для некоторого $U \in \Sigma_x$. Ясно, что Σ^0 обладает свойством (i*) из предложения 3. Если $x \in \bigcup_{\iota \in \Im} W_\iota$, где $W_\iota \in \Sigma^0$, то $x \in W_{\iota_0}$ для некоторого $\iota_0 \in \Im$. Но тогда

$$x \in U \subseteq W_{\iota_0} \subseteq \bigcup_{\iota \in \Im} W_\iota$$

для некоторого $U \in \Sigma_x$. Следовательно, $\bigcup_{\iota \in \Im} W_\iota \in \Sigma^0$, т. е. Σ^0 обладает свойством (ii*) из предложения 3. Если W', $W'' \in \Sigma^0$ и $x \in W' \cap W''$, то $x \in U' \subseteq W'$ и $x \in U'' \subseteq W''$ для подходящих U', $U'' \in \Sigma_x$. Но по условию $U \subseteq U' \cap U''$ для некоторого $U \in \Sigma_x$ и, следовательно, $x \in U \subseteq W' \cap W''$. Таким образом, $W' \cap W'' \in \Sigma^0$, т. е. выполнено свойство (iii*). Если $a \in M$ и $x \in M \setminus \{a\}$, то, согласно первому свойству системы Σ^0, $x \in U$ и $a \notin U$ для некоторого $U \in \Sigma_x$. Следовательно, $M \setminus \{a\} \in \Sigma^0$, т. е. выполнено свойство (iv*). Остается принять во внимание предложение 3.

Универсальная алгебра A называется *топологической*, если A — топологическое пространство и все операции алгебры A непрерывны, т. е. если f — n-арная операция, $a = f(a_1, \ldots, a_n)$, $n \geqslant 1$ и U — окрестность элемента a, то найдутся такие окрестности U_i элементов a_i, $i = 1, \ldots, n$, что

$$f(U_1, \ldots, U_n) \subseteq U.$$

В частности, кольцо R называется *топологическим*, если R — топологическое пространство и выполнены следующие условия:

(1) если a, $b \in R$ и W — окрестность элемента $a+b$, то найдутся окрестности U и V элементов a и b соответственно такие, что $U+V \subseteq W$;

(2) если $a \in R$ и U — окрестность элемента $-a$, то $-V \subseteq U$ для некоторой окрестности V элемента a;

(3) если a, $b \in R$ и W — окрестность элемента ab, то найдутся окрестности U и V элементов a и b соответственно такие, что $UV \subseteq W$.

Предложение 6. *Если Σ_0 — база окрестностей нуля топологического кольца R, то Σ_0 обладает следующими свойствами:*

(1) $\bigcap_{U \in \Sigma_0} U = \{0\}$;

(2) *если* $U, V \in \Sigma_0$, *то* $W \subseteq U \cap V$ *для некоторого* $W \in \Sigma_0$;
(3) *если* $U \in \Sigma_0$, *то* $V + V \subseteq U$ *для некоторого* $V \in \Sigma_0$;
(4) *если* $U \in \Sigma_0$, *то* $-V \subseteq U$ *для некоторого* $V \in \Sigma_0$;
(5) *если* $U \in \Sigma_0$, *то* $VV \subseteq U$ *для некоторого* $V \in \Sigma_0$;
(6) *если* $a \in R$ *и* $U \in \Sigma_0$, *то для некоторого* $V \in \Sigma_0$ *имеет место* $aV \cup Va \subseteq U$.

Наоборот, если в кольце R *выделена система подмножеств* Σ_0, *обладающая свойствами* (1)—(6), *то на множестве* R *существует одна и только одна топология, превращающая* R *в топологическое кольцо и имеющая систему* Σ_0 *базой окрестностей нуля. При этом для каждого* $a \in R$ *система*

$$\Sigma_a = \{a + U \mid U \in \Sigma_0\}$$

служит базой окрестностей элемента a.

Доказательство. Если Σ_0 — база окрестностей нуля, то справедливость свойств (1) и (2) вытекает из предложения 5, а свойства (3)—(6) являются следствиями определения топологического кольца, поскольку $0+0=0$, $-0=0$, $0 \cdot 0 = 0$ и $0 \cdot a = a \cdot 0 = 0$ для всякого $a \in R$. Допустим теперь, что система Σ_0 обладает свойствами (1)—(6). Если $a \in R$ и $x \in \bigcap_{U \in \Sigma_0} (a + U)$, то $x - a \in \bigcap_{U \in \Sigma_0} U = \{0\}$, откуда $x = a$. Кроме того, согласно (2), для любых $U, V \in \Sigma_0$ имеем $W \subseteq U \cap V$ для некоторого $W \in \Sigma_0$. Тогда

$$a + W \subseteq (a + U) \cap (a + V)$$

для любого $a \in R$. Таким образом, система

$$\Sigma = \{\Sigma_a \mid a \in R\}$$

удовлетворяет условиям предложения 5 и потому оказывается объединением баз окрестностей элементов кольца R для некоторой топологии τ на нем. Пусть $a, b \in R$. Если W' — окрестность элемента $a + b$ в топологии τ, то $a + b + W \subseteq W'$ для некоторого $W \in \Sigma_0$. По свойству (3), можно найти $U \in \Sigma_0$ так, что $U + U \subseteq W$. Тогда

$$(a + U) + (b + U) \subseteq a + b + (U + U) \subseteq a + b + W \subseteq W'.$$

Если теперь W' — окрестность элемента $-a$ в топологии τ, то $-a + W \subseteq W'$ для некоторого $W \in \Sigma_0$. Свойство (4) позволяет выбрать $U \in \Sigma_0$ так, что $-U \subseteq W$, откуда

$$-(a + U) \subseteq -a + (-U) \subseteq -a + W \subseteq W'.$$

Наконец, если W' — окрестность элемента ab и $ab+W\subseteq \subseteq W'$, где $W\in\Sigma_0$, то, дважды воспользовавшись свойством (3), найдем T', $T''\in\Sigma_0$ такие, что $T'+T'\subseteq W$ и $T''+T''\subseteq T'$. Согласно (2), $V\subseteq T'\cap T''$ для некоторого $V\in\Sigma_0$. Тогда $V+V+V\subseteq W$. Теперь, используя (5) и (6), выберем V', V'', $V'''\in\Sigma_0$ так, что $aV'\subseteq V$, $V''b\subseteq V$ и $V'''V'''\subseteq V$. По свойству (2), в Σ_0 найдется множество $U\subseteq V'\cap V''\cap V'''$. Тогда

$$(a+U)(b+U)\subseteq ab+aV'+V''b+V'''V'''\subseteq$$
$$\subseteq ab+(V+V+V)\subseteq ab+W\subseteq W'.$$

Следовательно, R с топологией τ оказывается топологическим кольцом. Ясно, что Σ_0 — база окрестностей нуля в этой топологии, а Σ_a — база окрестностей элемента a. Если τ' — другая топология на R, превращающая R в топологическое кольцо и имеющая Σ_0 базой окрестностей нуля, то для любой окрестности W элемента $a\in R$ в этой топологии, ввиду равенства $a+0=a$, имеем $a+U\subseteq W$ для некоторого $U\in\Sigma_0$. Следовательно, Σ_a — база окрестностей элемента a в топологии τ'. Ввиду предложения 4, из совпадения баз окрестностей элементов в топологиях τ и τ' вытекает совпадение их систем открытых множеств, что, в силу предложения 1, влечет совпадение самих топологий.

Предложение 7. *Если R — топологическое кольцо с единицей, a — его обратимый элемент и U — открытое множество, то aU и Ua — открытые множества.*

Доказательство. Пусть $x\in aU$, т. е. $x=au$, где $u\in U$. Согласно предложению 6, $u+W\subseteq U$ для некоторой окрестности нуля W. По свойству (7) предложения 6, $a^{-1}V\subseteq W$ для некоторой окрестности нуля V. Поэтому

$$x+V=a(u+a^{-1}V)\subseteq a(u+W)\subseteq aU$$

и множество aU открыто, в силу предложений 4 и 6. Для множества Ua доказательство проводится аналогично.

Элемент a топологического кольца называется *топологически нильпотентным*, если $a^n\longrightarrow 0$ при $n\longrightarrow\infty$, т. е. если для любой окрестности нуля U найдется такой номер n, что $a^i\in U$ при всех $i>n$. Обратимый элемент a топологического кольца называется *нейтральным*, если ни a, ни a^{-1} не являются топологически нильпотентными элементами. Подмножество X топологического кольца называется *ограниченным справа*, если для

любой окрестности нуля U найдется такая окрестность нуля V, что $XV \subseteq U$.

Предложение 8. *Пусть R — нормированное кольцо с единицей. Тогда* (а) *система подмножеств U_n, $n=1, 2, \ldots$, где*

$$U_n = \left\{x \mid x \in R,\ \|x\| < \frac{1}{n}\right\},$$

является базой окрестностей нуля топологии, превращающей R в топологическое кольцо; (б) *элемент $a \in R$ топологически нильпотентен тогда и только тогда, когда $\|a\| < 1$*; (в) *обратимый элемент $a \in R$ нейтрален тогда и только тогда, когда $\|a\| = 1$*; (г) *объединение множеств топологически нильпотентных и нейтральных элементов ограничено справа и слева.*

Доказательство. (а) Поскольку $\|a\| = 0$ равносильно $a = 0$, то $\bigcap_{n=1}^{\infty} U_n = 0$, т. е. выполнено свойство (1) предложения 6. Свойство (2) справедливо, поскольку $U_m \subseteq U_n$, если $m > n$. Включение $U_{2n} + U_{2n} \subseteq U_n$ обеспечивает выполнение свойства (3), а равенство $\|-a\| = \|a\|$ — свойства (4). Свойство (5) является следствием включений $U_n U_n \subseteq U_{n^2} \subseteq U_n$. Для доказательства свойства (6) выберем n так, что $\|a\| < n$. Тогда

$$aU_{n^2} \cup U_{n^2}a \subseteq U_n.$$

Таким образом, утверждение (а) является следствием предложения 6.

(б) Ясно, что равенство $\lim_{n\to\infty} a^n = 0$ равносильно $\lim_{n\to\infty} \|a\|^n = 0$, что, в свою очередь, равносильно неравенству $\|a\| < 1$.

(в) Вытекает из (б).

(г) Если x — топологически нильпотентный или нейтральный элемент, то, согласно (б) и (в), $\|x\| \leqslant 1$. Поэтому $xU_n \cup U_n x \subseteq U_n$ для любого такого x.

Тело K назовем *топологическим телом*, если оно является топологическим кольцом и для любого ненулевого $a \in K$ и любой окрестности U элемента a^{-1} найдется такая окрестность V элемента a, что $0 \notin V$ и $V^{-1} \subseteq V$. Другими словами, требуется, чтобы операция взятия обратного также была непрерывна. Топологическое тело [кольцо] называется *нормируемым*, если на нем можно задать норму так, что топология, возникающая в силу предложения 8(а), совпадает с исходной.

Теорема 1. *Топологическое тело K нормируемо тогда и только тогда, когда множество его топологически нильпотентных элементов открыто и ограничено справа, а при умножении топологически нильпотентного или нейтрального элемента на топологически нильпотентный получается топологически нильпотентный элемент.*

Доказательство. Обозначим через T и N соответственно множества топологически нильпотентных и нейтральных элементов тела K. Положим $L=T\cup N$. Если тело K нормируемо, то выполнение указанных в формулировке свойств вытекает из предложений 8(б), 8(в) и 8(г). Допустим теперь, что K обладает перечисленными в формулировке свойствами. Если топология дискретна, то требованиям теоремы удовлетворяет тривиальная норма. Поэтому в дальнейшем будем предполагать, что топология на K не дискретна.

Обозначим через $K^\times$ мультипликативную группу тела K.

Лемма 1. *$g^{-1}Tg\subseteq T$ для любого $g\in K^\times$.*

Для доказательства зафиксируем окрестность нуля U и возьмем $t\in T$. Из равенства $g^{-1}0g=0$ и определения топологического кольца вытекает существование такой окрестности нуля V, что $g^{-1}Vg\subseteq U$. Теперь выберем n так, что $t^i\in V$ при всех $i>n$. Тогда

$$(g^{-1}tg)^i=g^{-1}t^ig\subseteq g^{-1}Vg\subseteq U,$$

т. е. $g^{-1}tg\in T$.

Лемма 2. *N — нормальная подгруппа группы $K^\times$.*

В самом деле, ясно, что $1\in N$ и что $a^{-1}\in N$, если $a\in N$. Если $a,\ b\in N$ и $ab\notin N$, то $ab\in T$ или $(ab)^{-1}\in T$. Если $ab\in T$, то, по условию теоремы,

$$b=a^{-1}ab\in NT\subseteq T.$$

Аналогично приходим к противоречию, предположив, что $b^{-1}a^{-1}=(ab)^{-1}\in T$. Если, далее, $a\in N$, $g\in K^\times$ и $g^{-1}ag\notin N$, то $g^{-1}ag\in T$ или $g^{-1}a^{-1}g\in T$. Но тогда, в силу леммы 1, имеем

$$a=g(g^{-1}ag)g^{-1}\in gTg^{-1}\subseteq T$$

или

$$a^{-1}=g(g^{-1}a^{-1}g)g^{-1}\in gTg^{-1}\subseteq T,$$

что невозможно.

Учитывая лемму 2, положим $G=K^\times/N$ и обозначим через π естественный гомоморфизм группы $K^\times$ на G.

Лемма 3. $TL\subseteq T$.

Действительно, $TT\subseteq T$ по условию. Если же $t\in T$ и $a\in N$, то, учитывая лемму 2 и условие теоремы, получаем

$$ta=tat^{-1}t\in NT\subseteq T.$$

Лемма 4. $LL\subseteq L$.

В самом деле, ввиду леммы 3, леммы 2 и условия теоремы,

$$LL=(T\cup N)L\subseteq TL\cup NT\cup NN\subseteq T\cup N=L.$$

Лемма 5. *G — архимедова линейно упорядоченная группа с положительным конусом $\pi(L)$.*

Действительно, по лемме 4 имеем $\pi(L)\pi(L)\subseteq\pi(L)$, а из лемм 1 и 2 для любого $g\in K^\times$ вытекает

$$\pi(g)^{-1}\pi(L)\pi(g)=\pi(g^{-1}(N\cup T)g)\subseteq\pi(N\cup T)=\pi(L).$$

Если $g\in K^\times$ и

$$\pi(g)\in\pi(L)\cap\pi(L)^{-1},$$

то $g=ac=b^{-1}d$, где a, $b\in L$ и c, $d\in N$. Если $g\notin N$, то $a\notin N$, откуда $a\in T$. Следовательно,

$$b^{-1}=acd^{-1}\in TN\subseteq TL\subseteq T,$$

по лемме 3. Еще раз применив лемму 3, получаем

$$1=b^{-1}b\in TL\subseteq T,$$

что невозможно. Таким образом,

$$\pi(L)\cap\pi(L^{-1}=\pi(1).$$

Если $x\notin L$, то, по определению множества N, $x^{-1}\in T\subseteq L$. Следовательно, $x\in L^{-1}$, т. е.

$$\pi(L)\cup\pi(L)^{-1}=G.$$

По предложению 1.2, G оказывается линейно упорядоченной группой с положительным конусом $\pi(L)$. Если, далее, a, $b\in K^\times$ и $a\notin N$, то $a\in T$ или $a^{-1}\in T$. Поскольку T открыто и $b^{-1}0=0$, то, по определению топологического кольца, $b^{-1}U\subseteq T$ для некоторой окрестности нуля U. С другой стороны, $a^n\in U$ или $a^{-n}\in U$ для подходящего n. Отсюда

$$b^{-1}a^n\in b^{-1}U\subseteq T\subseteq L$$

или

$$b^{-1}a^{-n} \in b^{-1}U \subseteq T \subseteq L,$$

что, как было отмечено после определения положительного конуса, влечет $\pi(b) \leqslant \pi(a)^n$ или $\pi(b) \leqslant \pi(a)^{-n}$, т. е. G — архимедова группа.

Из леммы 5 и теоремы 1.2 вытекает возможность отождествить G с подгруппой аддитивной группы действительных чисел. Для каждого $a \in K$ положим

$$\varphi(a) = \begin{cases} 2^{-\pi(a)}, & \text{если } a \neq 0, \\ 0, & \text{если } a = 0. \end{cases}$$

Лемма 6. *Функция* φ *обладает следующими свойствами:*

(i) $\varphi(a) = 0$ *тогда и только тогда, когда* $a = 0$;

(ii) $\varphi(ab) = \varphi(a)\varphi(b)$ *для любых* $a, b \in K$;

(iii) $\varphi(a) = 1$ *тогда и только тогда, когда* $a \in N$;

(iv) $\varphi(a^{-1}) = 1/\varphi(a)$, *если* $0 \neq a \in K$;

(v) $\varphi(a) < 1$ *тогда и только тогда, когда* $a \in T$;

(vi) *если* U *— окрестность нуля в* K, $0 \neq b \in K$ *и* $Tb \subseteq U$, *то для любого* $a \in K$ *справедлива импликация*

$$(\varphi(a) < \varphi(b)) \Rightarrow (a \in U);$$

(vii) *существует такое натуральное число* n, *что*

$$\varphi(a+b) \leqslant 2n \max\{\varphi(a), \varphi(b)\}$$

для любых $a, b \in K$.

Доказательство. Справедливость свойств (i)—(v) является непосредственным следствием определения функции φ и леммы 5. При выполнении условий свойства (vi), используя (ii) и (iv), получаем

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)/\varphi(b) < 1.$$

Ввиду (v), отсюда вытекает, что $ab^{-1} \in T$ и, следовательно,

$$a \in Tb \subseteq U.$$

Для доказательства свойства (vii) сначала установим вспомогательное утверждение:

Существует такое натуральное число n, *что*

$$\varphi(1+c) \leqslant n(1+\varphi(c)) \qquad (*)$$

для любого $c \in K$.

В самом деле, если такого n не существует, то для каждого натурального k найдется элемент $c_k \in K$, удов-

летворяющий неравенству

$$\varphi(1+c_k) > k(1+\varphi(c_k)).$$

Тогда

$$\frac{1}{\varphi(1+c_k)} + \frac{\varphi(c_k)}{\varphi(1+c_k)} = \frac{1+\varphi(c_k)}{\varphi(1+c_k)} < \frac{1}{k}$$

и, следовательно,

$$\lim_{k\to\infty}\left(\frac{1}{\varphi(1+c_k)} + \frac{\varphi(c_k)}{\varphi(1+c_k)}\right) = 0.$$

Поскольку $1/\varphi(1+c_k) > 0$ и $\varphi(c_k)/\varphi(1+c_k) \geqslant 0$, то отсюда вытекает, что

$$\lim_{k\to\infty}\frac{1}{\varphi(1+c_k)} = \lim_{k\to\infty}\frac{\varphi(c_k)}{\varphi(1+c_k)} = 0.$$

Теперь рассмотрим такие окрестности нуля U и V, что $1 \notin U$ и $V+V \subseteq U$. Поскольку, по условию, T ограничено справа, то имеем $TW \subseteq V$ для некоторой окрестности нуля W. Поскольку топология на K, по предположению, не дискретна, W содержит элемент $w \neq 0$. Ввиду (i), $\varphi(w) \neq 0$ и, следовательно, для некоторого натурального числа k_0, учитывая (ii) и (iv), получаем

$$\varphi((1+c_{k_0})^{-1}) = \frac{1}{\varphi(1+c_{k_0})} < \varphi(w)$$

и

$$\varphi(c_{k_0}(1+c_{k_0})^{-1}) = \frac{\varphi(c_{k_0})}{\varphi(1+c_{k_0})} < \varphi(w).$$

Отсюда, вспоминая, что $Tw \subseteq TW \subseteq V$, и применяя (vi), выводим, что

$$(1+c_{k_0})^{-1},\ c_{k_0}(1+c_{k_0})^{-1} \in V.$$

Но тогда

$$1 = (1+c_{k_0})^{-1} + c_{k_0}(1+c_{k_0})^{-1} \in V+V \subseteq U,$$

что противоречит выбору окрестности U.

Возвращаясь к доказательству справедливости свойства (vii), заметим, что при $a=0$ оно, очевидно, имеет место. Поэтому допустим, что $a \neq 0$. Из (ii), (iv) и (*)

вытекает, что

$$\varphi(a+b)=\varphi(a(1+a^{-1}b))=\varphi(a)\varphi(1+a^{-1}b)\leqslant$$
$$\leqslant n\varphi(a)(1+\varphi(a^{-1}b))=n\varphi(a)\left(1+\frac{\varphi(b)}{\varphi(a)}\right)=$$
$$=n(\varphi(a)+\varphi(b)).$$

Но поскольку $\varphi(a)$, $\varphi(b)\geqslant 0$, то имеем

$$\varphi(a)+\varphi(b)\leqslant 2\max\{\varphi(a),\ \varphi(b)\},$$

и, следовательно,

$$\varphi(a+b)\leqslant 2n\max\{\varphi(a),\ \varphi(b)\}.$$

Лемма 7. *Если* $\alpha>0$ *и* $(2n)^{\alpha}\leqslant 2$, *где* n *— натуральное число, указанное в лемме* 6 (vii), *то функция*

$$\|a\|=\varphi(a)^{\alpha}$$

является нормой на теле K.

Действительно, учитывая лемму 6(i), получаем, что $\|a\|=0$ тогда и только тогда, когда $a=0$. Ввиду леммы 6(ii),

$$\|ab\|=\varphi(ab)^{\alpha}=\varphi(a)^{\alpha}\varphi(b)^{\alpha}=\|a\|\cdot\|b\|$$

для любых a, $b\in K$. Ввиду леммы 6 (vii), для любых a, $b\in K$ имеет место

$$\|a+b\|=\varphi(a+b)^{\alpha}\leqslant(2n\max\{\varphi(a),\ \varphi(b)\})^{\alpha}=$$
$$=(2n)^{\alpha}\max\{\varphi(a)^{\alpha},\ \varphi(b)^{\alpha}\}\leqslant 2\max\{\|a\|,\ \|b\|\}.$$

Стандартная индукция позволяет получить

$$\|a_1+\ldots+a_{2^k}\|\leqslant 2^k\max\{\|a_1\|,\ \ldots,\ \|a_{2^k}\|\}\qquad(*)$$

для любых $a_1,\ \ldots,\ a_{2^k}\in K$. В частности, ввиду леммы 6 (iii),

$$\|2^k\|\leqslant 2^k.\qquad(**)$$

Пусть теперь m — произвольное натуральное число. Выберем натуральное число $k(m)$ так, что $2^{k(m)}\leqslant m<2^{k(m)+1}$. Индукцией по $k(m)$ будем доказывать неравенство

$$\|m\|\leqslant 2m.\qquad(***)$$

Оно очевидно при $k(m)=0$. Если $k(m)\geqslant 1$, то, ввиду (*),

$$\|m\|=\|(m-2^{k(m)})+2^{k(m)}\|\leqslant 2\max\{\|m-2^{k(m)}\|,\ \|2^{k(m)}\|\}.$$

Если $\|m-2^{k(m)}\| \leqslant \|2^{k(m)}\|$, то

$$\max\{\|m-2^{k(m)}\|,\ \|2^{k(m)}\|\} = \|2^{k(m)}\|$$

и, ввиду (**),

$$\|m\| \leqslant 2\|2^{k(m)}\| \leqslant 2\cdot 2^{k(m)} \leqslant 2m,$$

т. е. (***) имеет место. Если же $\|m-2^{k(m)}\| > \|2^{k(m)}\|$, то

$$\max\{\|m-2^{k(m)}\|,\ \|2^{k(m)}\|\} = \|m-2^{k(m)}\|$$

и, значит,

$$\|m\| \leqslant 2\|m-2^{k(m)}\|.$$

Поскольку $2^{k(m)} \leqslant m < 2^{k(m)+1}$, то $0 \leqslant m-2^{k(m)} < 2^{k(m)}$. При $m-2^{k(m)}=0$, учитывая (**), получаем

$$\|m\| = \|2^{k(m)}\| \leqslant 2^{k(m)} = m < 2m.$$

Если же $m-2^{k(m)} > 0$, то найдется натуральное число $q < k(m)$, для которого $2^q \leqslant m-2^{k(m)} < 2^{q+1}$. Кроме того, из неравенства $m < 2^{k(m)+1}$ следует, что $2m < 2^{k(m)+2}$, т. е. $2m-2^{k(m)+2} < 0$. Поэтому, используя индуктивное предположение, получаем

$$\|m\| \leqslant 2\|m-2^{k(m)}\| \leqslant 2\cdot 2(m-2^{k(m)}) = 2m+2m-2^{k(m)+2} < 2m.$$

Теперь докажем, что

$$\|1+a\| \leqslant 1+\|a\| \qquad (****)$$

для любого $a \in K$.

В самом деле, поскольку 1 и a коммутируют, то

$$(1+a)^{2^n-1} = \sum_{i=0}^{2^n-1} C^i_{2^n-1} a^i,$$

причем стоящая в правой части сумма содержит 2^n слагаемых. Ввиду равенства $\|ab\| = \|a\|\cdot\|b\|$ и неравенства (***),

$$\|C^i_{2^n-1}a^i\| = \|C^i_{2^n-1}\|\cdot\|a^i\| \leqslant 2C^i_{2^n-1}\|a\|^i.$$

Используя эти неравенства и (*), получаем

$$\|1+a\|^{2^n-1} = \|(1+a)^{2^n-1}\| \leqslant$$
$$\leqslant 2^n \max\{\|C^i_{2^n-1}a^i\|,\ i=0,\ 1,\ 2,\ \ldots,\ 2^n-1\} \leqslant$$
$$\leqslant 2^{n+1}\max\{C^i_{2^n-1}\|a\|^i,\ i=0,\ 1,\ 2,\ \ldots,\ 2^n-1\} \leqslant$$
$$\leqslant 2^{n+1}(1+\|a\|)^{2^n-1}.$$

Отсюда

$$\|1+a\| \leqslant 2^{\frac{n+1}{2^n-1}}(1+\|a\|)$$

и, поскольку $\lim\limits_{n\to\infty} 2^{\frac{n+1}{2^n-1}} = 1$,

$$\|1+a\| \leqslant \lim_{n\to\infty} 2^{\frac{n+1}{2^n-1}}(1+\|a\|) = 1+\|a\|.$$

Наконец, докажем, что

$$\|a+b\| \leqslant \|a\|+\|b\|$$

для любых a, $b \in K$.

Это ясно, если $a=0$. Поэтому допустим, что $a \neq 0$. Учитывая равенство

$$1 = \|1\| = \|aa^{-1}\| = \|a\| \cdot \|a^{-1}\|$$

и (****), получим

$$\|a+b\| = \|a(1+a^{-1}b)\| = \|a\| \cdot \|1+a^{-1}b\| \leqslant$$
$$\leqslant \|a\|(1+\|a^{-1}b\|) = \|a\|\left(1+\frac{\|b\|}{\|a\|}\right) = \|a\|+\|b\|.$$

Лемма 8. *U_n—окрестность нуля для каждого n.*

В самом деле, поскольку топология не дискретна, а T, по условию, открыто, найдется ненулевой $t \in T$. Ввиду леммы 6(v), $\|t\| < 1$. Поэтому, если задано n, то для подходящего k имеем $\|t^k\| = \|t\|^k < \frac{1}{n}$. Отсюда $t^k T \subseteq U_n$, а, ввиду предложения 7, $t^k T$—открытое множество.

Лемма 9. *Если U—окрестность нуля, то $U_n \subseteq U$ для некоторого n.*

Для доказательства заметим, что, поскольку T, по условию, ограничено справа, то $TV \subseteq U$ для некоторой окрестности нуля V. Ввиду недискретности топологии, найдется ненулевой $v \in V$. Выберем натуральное число n так, что $\frac{1}{n} < \varphi(v)^\alpha$. Тогда, используя лемму 6(vi), получим

$$U_n = \left\{x \mid x \in K,\ \varphi(x)^\alpha < \frac{1}{n}\right\} \subseteq \{x \mid x \in K,\ \varphi(x) < \varphi(v)\} \subseteq U.$$

Итак, если недискретное топологическое тело K удовлетворяет условиям теоремы, то построим функцию φ, указанную в лемме 6. Если n—натуральное число, упоминаемое в свойстве (vii), то для подходящего положи-

тельного действительного числа α имеем $(2n)^{\alpha} < 2$. После этого лемма 7 обеспечивает существование нормы на теле K. Согласно предложению 8 (а), эта норма определяет на R топологию. Из лемм 8 и 9 вытекает, что база окрестностей нуля этой топологии служит базой окрестностей нуля исходной топологии. Следовательно, эти топологии совпадают по предложению 6.

Теорема 2. *Топологическое поле нормируемо тогда и только тогда, когда множество его топологически нильпотентных элементов открыто, а объединение множеств топологически нильпотентных и нейтральных элементов ограничено.*

Доказательство. Если P—нормированное поле, то множество его топологически нильпотентных элементов открыто по теореме 1, а объединение множеств топологически нильпотентных и нейтральных элементов ограничено по предложению 8 (г). Наоборот, если выполнены условия теоремы, то множество T его топологически нильпотентных элементов открыто и ограничено. Пусть, далее, $b \in T$ и a принадлежит объединению L множеств топологически нильпотентных и нейтральных элементов. Легко видеть, что при возведении в степень топологически нильпотентного элемента получается топологически нильпотентный элемент. Поэтому $a^k \in L$ и $b^k \in T$ для любого $k > 0$. Если теперь задана окрестность нуля U, то, ввиду ограниченности множества L, имеем $LV \subseteq U$ для подходящей окрестности нуля V. Если n_0 таково, что $b^n \in V$ для всех $n > n_0$, то

$$(ab)^n = a^n b^n \in LV \subseteq V.$$

Следовательно, $ab \in T$, т. е. $LT \subseteq T$. Таким образом, оказываются выполненными условия теоремы 1.

Упражнения

1. Если U—открытое подмножество топологического кольца R и $a \in R$, то $a+U$—открытое множество.
2. Если U и V—открытые подмножества топологического кольца, то множество $U+V$ также открыто.
3. Если U и V—открытые подмножества топологического тела, то UV—открытое миожество, но для топологического кольца это не всегда так.
4. Центр топологяческого кольца замкнут.
5. Левый [правый] аннулятор любого подмножества топологического кольца замкнут.
6. Всякая открытая подгруппа аддитивной группы топологического кольца замкнута.

7. Кольцо с неархимедовой нормой обладает базой окрестностей нуля, состоящей из подгрупп.

8. Если на кольце R задана псевдо-норма (см. упр. 7—9 из § 2), то система $\{U_n \mid n = 1, 2, \ldots\}$, где $U_n = \left\{x \mid x \in R, \|x\| < \frac{1}{n}\right\}$, образует базу окрестностей нуля топологии, превращающей R в топологическое кольцо.

ЛИТЕРАТУРА

Арнаутов В. И., Водинчар М. И., Михалев А. В. Введение в теорию топологических колец и модулей.—Кишинев: Штиинца, 1981.

Биркгоф Г. Теория решеток.—М.: Наука, 1983.

Бурбаки Н. Общая топология. Основные структуры.—М.: Наука, 1968.

Бурбаки Н. Общая топология. Числа и связанные с ними группы и пространства.—М.: Физматгиз, 1958.

Бурбаки Н. Общая топология. Использование вещественных чисел в общей топологии. Функциональные пространства. Сводка результатов.—М.: Наука, 1975.

Бурбаки Н. Алгебра. Многочлены и поля. Упорядоченные группы.—М.: Наука, 1965.

ван дер Варден, Б. Л. Алгебра.—М.: Наука, 1976.

Вейль А. Интегрирование в топологических группах и его применение.—М.: ИЛ, 1950.

Гельфанд И. М., Райков Д. А., Шилов Г. Е. Коммутативные нормированные кольца.—М.: Физматгиз, 1960.

Гринлиф Ф. Инвариантные средние на топологических группах.—М.: Мир, 1973.

Кокорин А. И., Копытов В. М. Линейно упорядоченные группы.—М.: Наука, 1972.

Копытов В. М. Решеточно упорядоченные группы.—М.: Наука, 1983.

Курош А. Г. Лекции по общей алгебре.—М.: Наука, 1973.

Моррис С. Двойственность Понтрягина и строение локально компактных абелевых групп.—М.: Мир, 1980.

Мухин Ю. Н. Локально компактные группы.—Свердловск: Изд-во Уральск. ун-та, 1981.

Наймарк М. А. Нормированные кольца.—М.: Наука, 1968.

Наймарк М. А. Теория представлений групп.—М.: Наука, 1976.

Понтрягин Л. С. Непрерывные группы.—М.: Наука, 1973.

Фукс Л. Частично упорядоченные алгебраические системы.—М.: Мир, 1965.

Gillman L., Jerison M. Rings of continuous functions.—Berlin; N. Y.; Heidelberg: Springer-Verlag, 1976.

Литературу по группам Ли см. в гл. V.

ГЛАВА VIII

КАТЕГОРИИ

Возникновение теории категорий связано с наблюдением, что совокупности всех групп, или всех колец, или всех модулей над фиксированным кольцом, рассматриваемые вместе с соответствующими гомоморфизмами, обладают рядом общих свойств. Многие из этих свойств сохраняются и при рассмотрении всех множеств с произвольными отображениями, всех частично упорядоченных множеств с изотонными отображениями, всех топологических пространств с непрерывными отображениями и т. п. Уже из этого перечисления видно, что язык теории категорий, в рамках которой формализируется то общее, что имеется в названных теориях, весьма емок. Выяснилось, что он оказывается полезным и во многих других самых разнообразных ситуациях. Подчеркнем, что в отличие от теории универсальных алгебр, теория категорий изучает не отдельные алгебраические (и не только алгебраические) системы, а совокупность алгебраических систем. Как правило, на языке теории категорий можно выразить те свойства алгебраических систем, в которых не фигурируют отдельные элементы. В настоящей главе излагаются те из основных понятий теории категории, роль которых представляется особенно важной для изучения конкретных алгебраических систем. В качестве основных результатов называем характеризацию категории модулей над кольцом и доказательство эквивалентности категорий модулей над кольцом R и над кольцом матриц над ним.

§ 1. Основные понятия

Категорией $\mathfrak{K}$ называется пара, состоящая из класса $\mathrm{Ob}\mathfrak{K}$, элементы которого называются *объектами*, и класса множеств $H_{\mathfrak{K}}(A, B)$, где $A, B \in \mathrm{Ob}\mathfrak{K}$, причем выполняются следующие свойства:

(0) Если A, A', B, $B' \in \mathrm{Ob}\mathfrak{K}$ и $A \neq A'$ или $B \neq B'$, то

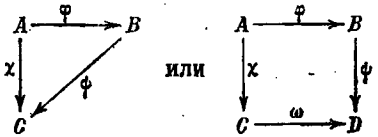
$$H_{\mathfrak{K}}(A, B) \cap H_{\mathfrak{K}}(A', B') = \varnothing;$$

(1) для любых $\varphi \in H_{\mathfrak{K}}(A, B)$ и $\psi \in H_{\mathfrak{K}}(B, C)$ определено произведение $\varphi\psi \in H_{\mathfrak{K}}(A, C)$;

(2) если $\varphi \in H_{\mathfrak{K}}(A, B)$, $\psi \in H_{\mathfrak{K}}(B, C)$ и $\chi \in H_{\mathfrak{K}}(C, D)$, то $(\varphi\psi)\chi = \varphi(\psi\chi)$;

(3) для любого $A \in \mathrm{Ob}\mathfrak{K}$ существует элемент $\mathrm{I}_A \in H_{\mathfrak{K}}(A, A)$ такой, что для любых $\varphi \in H_{\mathfrak{K}}(B, A)$ и $\psi \in H_{\mathfrak{K}}(A, C)$ имеет место $\varphi \mathrm{I}_A = \varphi$ и $\mathrm{I}_A \psi = \psi$.

Элементы множества $H_{\mathfrak{K}}(A, B)$ называются *морфизмами*. *Началом* каждого из этих морфизмов служит, по определению, объект A, а *концом* — объект B. Морфизм I_A называется *единичным морфизмом* объекта A. Вместо $\varphi \in H_{\mathfrak{K}}(A, B)$ часто будет писаться $\varphi\colon A \to B$ или $A \xrightarrow{\varphi} B$. Выражение «*диаграмма*



коммутативна» означают справедливость равенств $\varphi\psi = \chi$ или $\varphi\psi = \chi\omega$ соответственно. Примеры категорий приведены в таблице 1.

Морфизм $\varphi\colon A \to B$ называется *мономорфизмом* [*эпиморфизмом*], если каковы бы ни были ψ, $\chi \in H_{\mathfrak{K}}(C, A)$ [ψ, $\chi \in H_{\mathfrak{K}}(B, D)$] равенство $\psi\varphi = \chi\varphi$ [$\varphi\psi = \varphi\chi$] влечет за собой $\psi = \chi$.

Предложение 1. *В любой категории универсальных алгебр всякое гомоморфное вложение является мономорфизмом.*

Доказательство тривиально (ср. ЭА, с. 49, теорема II.1.3).

Предложение 2. *Если объектами категории $\mathfrak{K}$ служат алгебры класса $\mathfrak{M}$, обладающего свободной алгеброй F с одноэлементной свободной порождающей системой $\{x\}$, то всякий мономорфизм категории $\mathfrak{K}$ является гомоморфным вложением.*

Доказательство. Если $\varphi\colon A \to B$ — мономорфизм категории $\mathfrak{K}$, $a', a'' \in A$, $a' \neq a''$ и $\varphi(a') = \varphi(a'')$, то существуют морфизмы ψ, $\chi \in H_{\mathfrak{K}}(F, A)$ такие, что $\psi(x) = a'$ и

ТАБЛИЦА 1

	Обозначение или название	Объекты	Морфизмы	Произведение морфизмов
1.	SET	Множества	Отображения	Произведение отображений
2.	GROUP	Группы	Гомоморфизмы	»
3.	ABEL	Абелевы группы	»	»
4.	RING	Кольца	»	»
5.	RING-1	Кольца с единицей	Гомоморфизмы, переводящие 1 в 1	»
6.	R-Mod	Левые R-модули	Гомоморфизмы	»
7.	TOP	Топологические пространства	Непрерывные отображения	»

Продолжение

	Обозначение или название	Объекты	Морфизмы	Произведение морфизмов
8.	Ord-P	Элементы частично упорядоченного множества P	$H_{\text{Ord-}P}(a, b) = \begin{cases} (a, b), & \text{если } a \leqslant b \\ \varnothing, & \text{если } a \not\leqslant b \end{cases}$	$(a, b)(b, c) = (a, c)$
9.	REL	Непустые множества	$H_{\text{REL}}(A, B) = \{\rho \mid \rho \subseteq A \times B, \forall a \in A \exists b \in B\, (a, b) \in \rho\}$	$\rho \circ \sigma = \{(a, b) \mid \exists x\, (a, x) \in \rho\ \&\ (x, b) \in \sigma\}$
10.	Универсальные алгебры	Универсальные алгебры одной и той же сигнатуры, принадлежащие некоторому классу $\mathfrak{M}$	Гомоморфизмы	Произведение отображений
11.	Моноид R	Точка w	Элементы моноида R	Произведение элементов моноида R
12.	Кольцо R	»	Элементы кольца R	Произведение элементов кольца R

$\chi(x) = a''$. Тогда $\varphi(\psi(x)) = \varphi(\chi(x))$, откуда $\psi\varphi = \chi\varphi$, по следствию предложения II.1.5. По определению мономорфизма, получаем $\psi = \chi$, что противоречит определению этих морфизмов.

Предложение 3. *В любой категории универсальных алгебр всякое гомоморфное наложение является эпиморфизмом.*

Доказательство тривиально (ср. ЭА, с. 49, теорема II.1.1).

Однако аналог предложения 2, вообще говоря, места не имеет. В самом деле, пусть $\mathfrak{K}$ — категория коммутативных колец без делителей нуля с обычными гомоморфизмами в качестве морфизмов, а φ: $\mathbf{Z} \to \mathbf{Q}$ — естественное вложение кольца целых чисел в поле рациональных чисел. Если R — произвольный объект категории $\mathfrak{K}$, $\psi, \chi \in H_{\mathfrak{K}}(\mathbf{Q}, R)$, $\varphi\psi = \varphi\chi$ и $\psi \neq \chi$, то $\psi\left(\frac{m}{n}\right) \neq \chi\left(\frac{m}{n}\right)$ для некоторых m, $n \in \mathbf{Z}$. Но тогда

$$\psi(m) = \psi(\varphi(m)) = m\varphi\psi = m\varphi\chi = \chi(\varphi(m)) = \chi(m),$$

откуда

$$\psi(n)\,\psi\left(\frac{m}{n}\right) = \psi(m) = \chi(m) = \chi(n)\,\chi\left(\frac{m}{n}\right) = \psi(n)\,\chi\left(\frac{m}{n}\right).$$

Отсюда, поскольку $\psi\left(\frac{m}{n}\right) \neq \chi\left(\frac{m}{n}\right)$ и в R нет делителей нуля, получаем $\psi(n) = 0$, а значит, $\psi(m) = \chi(m) = 0$. Поэтому

$$\psi\left(\frac{m}{n}\right) = \psi(m)\,\psi\left(\frac{1}{n}\right) = 0 = \chi(m)\,\chi\left(\frac{1}{n}\right) = \chi\left(\frac{m}{n}\right).$$

Противоречие.

Предложение 4. *В категории левых модулей над кольцом R всякий эпиморфизм является наложением.*

Доказательство. Пусть $\varphi \in \mathrm{Hom}_R(A, B)$, φ — эпиморфизм и $C = \mathrm{Im}\,\varphi$. Если ψ — естественный гомоморфизм модуля B на фактор-модуль B/C, а χ — нулевой гомоморфизм модуля B в B/C, то $\varphi\psi = \varphi\chi$. Отсюда, поскольку φ — эпиморфизм, получаем $\psi = \chi$, что возможно лишь при $B = C$.

Ввиду предложения 4, эпиморфизм оказывается наложением в категории абелевых групп. Более того, имеет место:

Предложение 5. *В категории групп всякий эпиморфизм является наложением.*

Доказательство. Пусть $\varphi \in H_{\mathrm{GROUP}}(A, B)$, φ — эпиморфизм и $C = \operatorname{Im}\varphi$. Если подгруппа C нормальна, то можно рассмотреть фактор-группу B/C. Пусть ψ — естественный гомоморфизм группы B на B/C, а χ отображает все элементы из B в единицу фактор-группы B/C. Тогда $\varphi\psi = \varphi\chi$, откуда $\psi = \chi$, что возможно лишь при $B = C$. Таким образом, можно предполагать, что подгруппа C не нормальна. Поскольку всякая подгруппа индекса 2 нормальна, то можно предполагать, что фактор-множество B/C содержит, по крайней мере, три различных смежных класса, скажем C, uC и vC. Пусть S — группа всех взаимно однозначных отображений множества B на себя. Определим $\sigma \in S$, положив

$$\sigma(b) = \begin{cases} vu^{-1}b, & \text{если } b \in uC, \\ uv^{-1}b, & \text{если } b \in vC, \\ b & \text{в остальных случаях.} \end{cases}$$

Далее, определим морфизмы $\psi, \chi \in H_{\mathrm{GROUP}}(B, S)$ равенствами

$$x\psi(b) = xb$$

и

$$x\chi(b) = \sigma^{-1}(\sigma(x)\, b)$$

для любых b, $x \in B$. Тогда для любого $a \in A$ имеем

$$x\chi(\varphi(a)) = \sigma^{-1}(\sigma(x)\,\varphi(a)) =$$

$$= \begin{cases} \sigma^{-1}(vu^{-1}x\varphi(a)) = x\varphi(a) = x\psi(\varphi(a)), & \text{если } x \in uC, \\ \sigma^{-1}(uv^{-1}x\varphi(a)) = x\varphi(a) = x\psi(\varphi(a)), & \text{если } x \in vC, \\ x\varphi(a) = x\psi(\varphi(a)) & \text{в остальных случаях.} \end{cases}$$

Следовательно,

$$a\varphi\chi = \chi(\varphi(a)) = \psi(\varphi(a)) = a\varphi\psi$$

для всех $a \in A$, т. е. $\varphi\chi = \varphi\psi$. В то же время

$$v\psi(u^{-1}) = vu^{-1} \neq 1$$

и

$$v\chi(u^{-1}) = \sigma^{-1}(\sigma(v)\, u^{-1}) = \sigma^{-1}(uu^{-1}) = \sigma^{-1}(1) = 1,$$

т. е. $\psi \neq \chi$.

Предложение 6. *Если произведение морфизмов* $\varphi\psi$ *является эпиморфизмом* [*мономорфизмом*], *то* ψ — *эпиморфизм* [φ — *мономорфизм*].

Доказательство. Если $\varphi\psi$ — эпиморфизм и $\psi\chi' = \psi\chi''$, то $\varphi\psi\chi' = \varphi\psi\chi''$, откуда $\chi' = \chi''$, т. е. ψ оказывается эпиморфизмом. Если $\varphi\psi$ — мономорфизм и $\chi'\varphi = \chi''\varphi$, то $\chi'\varphi\psi = \chi''\varphi\psi$, откуда $\chi' = \chi''$, т. е. φ — мономорфизм.

Морфизм $\varphi\colon A \to B$ называется *изоморфизмом*, если существует морфизм $\psi\colon B \to A$ такой, что $\varphi\psi = I_A$ и $\psi\varphi = I_B$. Нетрудно показать, что морфизм ψ определяется однозначно. Это позволяет обозначить его через φ^{-1}. Подчеркнем еще, что, ввиду предложения 6, изоморфизм является мономорфизмом и эпиморфизмом одновременно. Однако приведенный выше пример показывает, что обратное утверждение имеет место не всегда.

Морфизм $\varphi\colon A \to B$ называется *ретракцией* [*коретракцией*], если существует морфизм $\psi\colon B \to A$, такой, что $\psi\varphi = I_B$ [$\varphi\psi = I_A$]. Объект A называется *ретрактом* [*коретрактом*] объекта B, если существует коретракция [ретракция] $\varphi\colon A \to B$.

Поскольку I_A является мономорфизмом и эпиморфизмом, из предложения 6 вытекает:

Предложение 7. *Всякая ретракция* [*коретракция*] *является эпиморфизмом* [*мономорфизмом*].

С любой категорией $\mathfrak{K}$ связана *двойственная* ей категория $\mathfrak{K}^{op}$. Объектами и морфизмами категории $\mathfrak{K}^{op}$ служат соответственно, объекты и морфизмы категории $\mathfrak{K}$, но произведение морфизмов определяется формулой $\varphi \circ \psi = \psi\varphi$. Другими словами, при переходе от $\mathfrak{K}$ к $\mathfrak{K}^{op}$ следует изменить на противоположное направление всех стрелок, изображающих морфизмы. Ясно, что каждое теоретико-категорное высказывание выражается как некоторое высказывание на языке умножения морфизмов или, что то же самое, как некоторое высказывание о диаграммах. Заменив в этом высказывании исходное умножение на умножение $\circ$ (т. е. изменив в нем направление стрелок), мы получим новое высказывание, называемое *двойственным*. Например, определения мономорфизма и эпиморфизма двойственны друг другу. То же самое можно сказать о ретракции и коретракции. Ясно, что если какое-то теоретико-категорное утверждение справедливо в категории $\mathfrak{K}$, то двойственное ему утверждение справедливо в категории $\mathfrak{K}^{op}$. В частности, отсюда вытекает, что если какое-то утверждение справедливо в любой категории, то в любой категории

имеет место и двойственное утверждение. Это, например, позволяет ограничиться доказательством лишь одного из утверждений предложения 6. Рассмотренный факт носит название *принципа двойственности* и часто используется для сокращения изложения. Так, например, объект P категории $\mathfrak{K}$ называется *проективным*, если для любого эпиморфизма $\pi \in H_{\mathfrak{K}}(A, B)$ и любого морфизма $\varphi \in H_{\mathfrak{K}}(P, B)$ существует морфизм $\psi \in H_{\mathfrak{K}}(P, A)$ такой, что $\varphi = \psi\pi$ (рис. 5, *а*)), а *инъективный* объект определяется по принципу двойственности (рис. 5, *б*)) (ср. § 7 гл. IV).

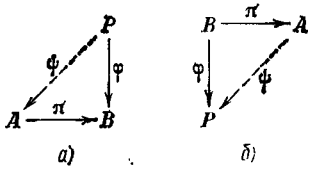


Рис. 5.

Пусть A_ι, $\iota \in \mathfrak{I}$,— семейство объектов категории $\mathfrak{K}$. Объект A называется *произведением объектов* A_ι *с проекциями* p_ι: $A \dashrightarrow A_\iota$, если для любого множества морфизмов φ_ι: $B \longrightarrow A_\iota$ существует один и только один морфизм φ: $B \longrightarrow A$ такой, что $\varphi p_\iota = \varphi_\iota$ для всех $\iota \in \mathfrak{I}$. Двойственно, объект A называется *копроизведением объектов* A_ι *с инъекциями* u_ι: $A_\iota \longrightarrow A$, если для любого множества морфизмов φ_ι: $A_\iota \longrightarrow B$ существует один и только одии морфизм φ: $A \longrightarrow B$ такой, что $u_\iota\varphi = \varphi_\iota$. Произведение объектов A_ι с проекциями p_ι обозначается через $\prod\limits_{\iota \in \mathfrak{I}} (A_\iota, p_\iota)$, а для копроизведения с инъекциями u_ι используется символ $\coprod\limits_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$.

Предложение 8. *Если* $A = \prod\limits_{\iota \in \mathfrak{I}} (A_\iota, p_\iota)$, $\varphi, \psi \in H_{\mathfrak{K}}(B, A)$ *и* $\varphi p_\iota = \psi p_\iota$ *для всех* $\iota \in \mathfrak{I}$, *то* $\varphi = \psi$.

Доказательство. Положив $\varphi_\iota = \psi p_\iota$, заметим, что справедливы равенства $\varphi p_\iota = \varphi_\iota = \psi p_\iota$ для всех $\iota \in \mathfrak{I}$, и воспользуемся единственностью морфизма φ, упоминаемой в определении произведения.

В силу принципа двойственности справедливо:

Предложение 9. *Если* $A = \coprod\limits_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$, $\varphi, \psi \in H_{\mathfrak{K}}(A, B)$ *и* $u_\iota\varphi = u_\iota\psi$ *для всех* $\iota \in \mathfrak{I}$, *то* $\varphi = \psi$.

Предложение 10. *Если* $A = \prod\limits_{\iota \in \mathfrak{I}} (A_\iota, p_\iota)$ *и* $A' = \prod\limits_{\iota \in \mathfrak{I}} (A_\iota, p'_\iota)$, *то существует изоморфизм* φ: $A \longrightarrow A'$ *такой, что* $\varphi p'_\iota = p_\iota$ *и* $\varphi^{-1} p_\iota = p'_\iota$ *для всех* $\iota \in \mathfrak{I}$.

Доказательство. По определению, существуют морфизмы $\varphi\colon A' \to A$ и $\psi\colon A' \to A$ такие, что $\varphi p'_\iota = p_\iota$ и $\psi p_\iota = p'_\iota$ для всех $\iota \in \mathfrak{I}$. Отсюда

$$\varphi\psi p_\iota = \varphi p'_\iota = p_\iota = \mathrm{I}_A p_\iota$$

и

$$\psi\varphi p'_\iota = \psi p_\iota = p'_\iota = \mathrm{I}_{A'} p'_\iota,$$

что, в силу предложения 8, влечет $\varphi\psi = \mathrm{I}_A$ и $\psi\varphi = \mathrm{I}_{A'}$.

В силу принципа двойственности справедливо:

Предложение 11. *Если* $A = \coprod\limits_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$ *и* $A' = \coprod\limits_{\iota \in \mathfrak{I}} (A_\iota, u'_\iota)$, *то существует изоморфизм* $\varphi\colon A' \to A$ *такой, что* $u'_\iota \varphi = u_\iota$ *и* $u_\iota \varphi^{-1} = u'_\iota$ *для всех* $\iota \in \mathfrak{I}$.

Предложения 10 и 11 показывают, что как произведение, так и копроизведение определяются однозначно с точностью до изоморфизма.

В категориях универсальных алгебр произведение в смысле теории категорий совпадает, как легко проверить, с прямым произведением (см. § 1 гл. II). Поскольку всякое множество можно рассматривать как алгебру с пустым множеством операций (или с одной унарной операцией $f(x) = x$), то то же самое верно и для категории множеств. Допустим теперь, что $a = \prod\limits_{\iota \in \mathfrak{I}} (a_\iota, p_\iota)$ в категории Ord-P (пример 8 из таблицы 1). Существование морфизмов p_ι означает, что $a \leqslant a_\iota$ для всех $\iota \in \mathfrak{I}$, т. е. что $a \in \{a_\iota \mid \iota \in \mathfrak{I}\}^\nabla$. Если же $b \in \{a_\iota \mid \iota \in \mathfrak{I}\}^\nabla$, то, по определению, существуют морфизмы $\varphi_\iota\colon b \to a_\iota$, а значит, и морфизм $\varphi\colon b \to a$, т. е. $b \leqslant a$. Таким образом, a — наибольший элемент нижнего конуса $\{a_\iota \mid \iota \in \mathfrak{I}\}^\nabla$, т. е. $a = \inf_P \{a_\iota \mid \iota \in \mathfrak{I}\}$ (см. § 1 гл. I). Аналогичные соображения показывают, что копроизведение в категории Ord-P совпадает с точной верхней гранью. В категории SET (пример 1 из таблицы 1) копроизведение $A = \coprod\limits_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$, как нетрудно проверить, совпадает с объединением множеств A_ι, рассматриваемых как попарно не пересекающиеся. Отметим важное для дальнейшего.

Предложение 12. *В категории левых модулей над кольцом* R *копроизведение совпадает с прямой суммой.*

Доказательство. Пусть A — прямая сумма модулей A_ι, $\iota \in \mathfrak{I}$. Обозначим через u_ι естественное гомоморф-

ное вложение модуля A_ι в A. Тогда для любых гомоморфизмов φ_ι модулей A_ι в некоторый модуль B равенством

$$\varphi(\ldots, a_\iota, \ldots) = \sum_{\iota \in \mathfrak{I}} \varphi_\iota(a_\iota)$$

(определение корректно, ибо $a_\iota = 0$ почти для всех ι) определяется единственный гомоморфизм $\varphi\colon A \to B$, удовлетворяющий равенствам $u_\iota \varphi = \varphi_\iota$ для всех $\iota \in \mathfrak{I}$.

Другие примеры произведений и копроизведений могут быть найдены в упражнениях.

Предложение 13. *Копроизведение проективных объектов проективно.*

Доказательство. Пусть P_ι, $\iota \in \mathfrak{I}$, — семейство проективных объектов и P — их копроизведение с каноническими инъекциями $u_\iota\colon P_\iota \to P$. Если $\pi\colon A \to B$ — эпиморфизм и $\varphi\colon P \to B$ — морфизм, то для каждого $\iota \in \mathfrak{I}$ найдется морфизм $\psi_\iota\colon P_\iota \to A$ такой, что $\psi_\iota \pi = u_\iota \varphi$. По определению копроизведения, существует морфизм $\psi\colon P \to A$ такой, что $u_\iota \psi = \psi_\iota$ для всех $\iota \in \mathfrak{I}$. Отсюда

$$u_\iota \psi \pi = \psi_\iota \pi = u_\iota \varphi$$

для всех $\iota \in \mathfrak{I}$ и, следовательно, $\psi\pi = \varphi$ по предложению 9.

По принципу двойственности справедливо:

Предложение 14. *Произведение инъективных объектов инъективно.*

Категория $\mathfrak{K}$ называется *категорией с произведениями* [*с копроизведениями*], если для любого семейства ее объектов существует их произведение [копроизведение].

Объект U категории $\mathfrak{K}$ называется *образующим* [*кообразующим*], если для любого $A \in \mathrm{Ob}\mathfrak{K}$ множество $H_{\mathfrak{K}}(U, A)$ [$H_{\mathfrak{K}}(A, U)$] непусто и для любых A, $B \in \mathrm{Ob}\mathfrak{K}$ и любых различных морфизмов φ, $\psi \in H_{\mathfrak{K}}(A, B)$ существует такой морфизм $\chi \in H_{\mathfrak{K}}(U, A)$ [$\chi \in H_{\mathfrak{K}}(B, U)$], что $\chi\varphi \neq \chi\psi$ [$\varphi\chi \neq \psi\chi$].

Предложение 15. *Пусть $\mathfrak{K}$ — категория с копроизведениями. Объект $U \in \mathrm{Ob}\mathfrak{K}$ является образующим категории $\mathfrak{K}$ тогда и только тогда, когда для любого объекта $A \in \mathrm{Ob}\mathfrak{K}$ существует эпиморфизм $\pi\colon F \to A$, где F — копроизведение некоторого множества экземпляров объекта U.*

Доказательство. Пусть U — образующий и $A \in \mathrm{Ob}\mathfrak{K}$. Тогда $H_{\mathfrak{K}}(U, A) \neq \varnothing$ и, следовательно, существует копроизведение $F = \coprod_{\omega \in H_{\mathfrak{K}}(U, A)} (U_\omega, u_\omega)$, где $U_\omega = U$ для всех ω. По определению копроизведения, существует морфизм $\pi\colon F \to A$ такой, что $u_\omega \pi = \omega$ для всех ω. Если $\pi\psi = \pi\chi$, но

ТАБЛИЦА 2

	$\mathfrak{K}$	$\mathfrak{K}'$	$T(A)$	$T(\varphi)$, где $\varphi\colon A \longrightarrow B$	Примечания
1.	Универсальные алгебры	SET	Множество A	φ	Этот функтор называется *забывающим*
2.	GROUP	ABEL	A/A^*, где A^* — коммутант группы A	$T(\varphi)(aA') = \varphi(a)B'$	Определение $T(\varphi)$ корректно, так как $\varphi(A') \subseteq B'$
3.	ABEL	ABEL	Подгруппа всех периодических элементов из A	φ	Определение $T(\varphi)$ корректно, так как $\varphi(T(A)) \subseteq T(B)$
4.	R-Mod	ABEL	$\mathrm{Hom}_R(U, A)$, где U — фиксированный левый R-модуль	$fT(\varphi) = f\varphi$	

Продолжение

	$\mathfrak{K}$	$\mathfrak{K}'$	$T(A)$	$T(\varphi)$, где $\varphi\colon A \longrightarrow B$	Примечания
5.	R-Mod	ABEL	$U \otimes_R A$, где U — фиксированный правый R-модуль	$(u \otimes a)\, T(\varphi) = u \otimes a\varphi$, где $u \in U$, $a \in A$	
6.	Моноид R	SET	Некоторое множество $T(A)$ (напомним, что Моноид R содержит лишь один объект A)	T — гомоморфизм моноида R в моноид отображений множества $T(A)$ в себя	При различном выборе множества $T(A)$ получаем различные функторы
7.	Булевы алгебры	RING	Булево кольцо, соответствующее булевой алгебре A (см. теорему III.4.2)	φ	
8.	GROUP	RING′	Целочисленное групповое кольцо $\mathbf{Z}A$	$(ka)\, T(\varphi) = k(a\varphi)$, где $k \in \mathbf{Z}$, $a \in A$.	

$\psi \neq \chi$, то, по определению образующего, $\omega\psi \neq \omega\chi$ для некоторого ω: $U \to A$. С другой стороны,

$$\omega\psi = u_\omega \pi\psi = u_\omega \pi\chi = \omega\chi.$$

Полученное противоречие показывает, что π — эпиморфизм. Допустим теперь, что для объекта U выполнены условия предложения, φ, $\psi \in H_{\mathfrak{K}}(A, B)$ и $\varphi \neq \psi$. По условию, существует эпиморфизм π: $F \to A$, где $F = \coprod_{\iota \in \mathfrak{I}} (U_\iota, u_\iota)$ и $U_\iota = U$ для всех $\iota \in \mathfrak{I}$. Тогда $\pi\varphi \neq \pi\psi$ и, в силу предложения 9, $u_\iota \pi\varphi \neq u_\iota \pi\psi$ для некоторого $\iota \in \mathfrak{I}$. Положив $\chi = u_\iota \pi$, получим $\chi\varphi \neq \chi\psi$, где $\chi \in H_{\mathfrak{K}}(U, A)$, что и требовалось.

В категории непустых множеств образующим является, как нетрудно видеть, любое непустое множество, а в категории R-Mod — левый R-модуль R. Некоторые другие примеры указаны в упражнениях.

Функтор T категории $\mathfrak{K}$ в категорию $\mathfrak{K}'$ определяется как отображение класса объектов категории $\mathfrak{K}$ в класс объектов категории $\mathfrak{K}'$ и класса морфизмов категории $\mathfrak{K}$ в класс морфизмов категории $\mathfrak{K}'$, обладающее следующими свойствами:

(0) если $\varphi \in H_{\mathfrak{K}}(A, B)$, то $T(\varphi) \in H_{\mathfrak{K}'}(T(A), T(B))$;

(1) если $\varphi \in H_{\mathfrak{K}}(A, B)$ и $\psi \in H_{\mathfrak{K}}(B, C)$, то $T(\varphi\psi) = T(\varphi) T(\psi)$;

(2) $T(1_A) = 1_{T(A)}$ для любого $A \in \mathrm{Ob}\mathfrak{K}$.

Ряд примеров функторов указан в таблице 2, а также в упражнениях. Для дальнейшего будет важен функтор $H(A, -)$ из произвольной категории $\mathfrak{K}$ в категорию множеств SET, связанный с фиксированным объектом A из $\mathfrak{K}$. Именно, каждому $B \in \mathrm{Ob}\mathfrak{K}$ ставится в соответствие множество $H_{\mathfrak{K}}(A, B)$, а $H(A, \varphi)$, где $\varphi \in H_{\mathfrak{K}}(B, C)$, определяется равенством

$$H(A, \varphi)(f) = f\varphi$$

для любого $f \in H_{\mathfrak{K}}(A, B)$. Проверка свойств (1) и (2) тривиальна.

Упражнения

1. В категории унаров все эпиморфизмы являются наложениями.

2. В категории полугрупп существуют эпиморфизмы, не являющиеся наложениями.

3. В категории частично упорядоченных множеств всякий мономорфизм является вложением, а каждый эпиморфизм — наложением. Указание (ко второй части). Если φ: $A \to B$ — изотонное отобра-

женне частнчно упорядоченных множеств, не являющееся наложеннем, то рассмотреть множество $C=\{1, 2, 3, 6\}$, упорядоченное по делимости, выбрать $b_0 \in B \setminus \operatorname{Im}\varphi$ и положнть

$$\psi(x)=\begin{cases}6, \text{ если } x > b_0,\\ 2, \text{ если } x \text{ и } b_0\\ \quad \text{не сравнимы},\\ 3, \text{ если } x=b_0,\\ 1, \text{ если } x < b_0,\end{cases} \quad \text{и} \quad \chi(x)=\begin{cases}6, \text{ если } x > b_0,\\ 3, \text{ если } x=b_0\\ \quad \text{или } x \text{ и } b_0,\\ \quad \text{не сравнимы},\\ 1, \text{ если } x < b_0.\end{cases}$$

4. Описать мономорфизмы и эпиморфизмы в категорни REL (см. табл. 1).

5. Всякий объект категории непустых множеств проективеи и инъективен.

6. В категории колец [полугрупп] одноэлементное кольцо [полугруппа] является единственным инъективным объектом.

7. Описать инъективные унары.

8. Если $\mathfrak{K}$—категория всех универсальных алгебр некоторого многообразия $\mathfrak{M}$ и всякнй эпиморфизм из $\mathfrak{K}$ является наложением, то свободная алгебра многообразия $\mathfrak{M}$ является проективным объектом категории $\mathfrak{K}$.

9. Всякая проективная абелева группа свободна.

10. Ретракт [коретракт] инъективного [проективного] объекта инъективен [проективен].

11. Копроизведение в категории унаров совпадает с объединением сомножителей, рассматриваемых как попарно не пересекающиеся множества.

12. Копроизведение в категории групп совпадает со свободным произведением (Курош А. Г. Теория групп.—М.: Наука, 1967, § 33). Обобщить этот результат для произвольного многообразия универсальных алгебр.

13. Произведением в категории топологических пространств с непрерывными отображениями в качестве морфизмов служит тихоновское произведение (Александров П. С. Введение в теорию множеств и общую топологию.—М.: Наука, 1977, гл. 6, § 4).

14. В категорин $\mathfrak{K}$ из упр. 8 всякая свободная алгебра является образующим.

15. В категории непустых множеств всякое непустое множество является образующим, а всякое множество, содержащее более одного элемента,—кообразующим.

16. Если U—образующий и π: $V \longrightarrow U$—эпиморфизм, то V—образующий. В частности, ретракт образующего является образующим.

17. Пусть $\mathfrak{K}$—произвольная категория, $B \in \operatorname{Ob}\mathfrak{K}$, $T=H_{\mathfrak{K}}(-, B)$ и $T(\varphi)(f)=f\varphi$ для любых $\varphi \in H_{\mathfrak{K}}(A'', B)$ и $f \in H_{\mathfrak{K}}(A', A'')$. Доказать, что T—функтор из категории, двойственной категории $\mathfrak{K}$, в категорию множеств.

18. Построить функтор T из категории SET в категорию REL (см. табл. 1) так, что $T(A)=T(B)$ влечет $A=B$ для всех $A, B \in \operatorname{Ob}$ SET, а из $T(\varphi)=T(\psi)$ вытекает $\varphi=\psi$ для любых морфизмов φ и ψ категории SET.

19. Модуль P проективен тогда и только тогда, когда $\operatorname{Hom}(P, \varphi)$ является эпиморфизмом для каждого эпиморфнзма φ.

20. Модуль Q инъективен тогда и только тогда, когда $\operatorname{Hom}(\varphi, Q)$ является эпиморфизмом для каждого мономорфизма φ.

§ 2. Аддитивные категории

Категория $\mathfrak{K}$ называется *аддитивной* *), если для любых ее объектов A и B множество $H_{\mathfrak{K}}(A, B)$ является абелевой группой и для любых $\varphi, \psi \in H_{\mathfrak{K}}(A, B)$, $\chi \in H_{\mathfrak{K}}(D, A)$ и $\omega \in H_{\mathfrak{K}}(B, C)$, где C, D — произвольные объекты из $\mathfrak{K}$, справедливы равенства

$$\chi(\varphi+\psi)=\chi\varphi+\chi\psi$$

и

$$(\varphi+\psi)\omega=\varphi\omega+\psi\omega.$$

Легко проверяется, что при тех же обозначениях $\chi 0_{AB}=0_{AB}=0_{AB}\omega$, где 0_{AB} — нуль абелевой группы $H_{\mathfrak{K}}(A, B)$. Часто вместо 0_{AB} будем писать просто 0. При рассмотрении аддитивных категорий естественно рассматривать *аддитивные функторы*, т. е. такие функторы T, что $T(\varphi+\psi)=T(\varphi)+T(\psi)$ для любых $\varphi, \psi \in H_{\mathfrak{K}}(A, B)$. Заметим, что категория, двойственная аддитивной, очевидным образом аддитивна. Важнейшим примером аддитивной категории является категория модулей над кольцом R (левых или правых) и, в частности, категория абелевых групп. Категория «Кольцо R» (пример 12 из таблицы 1) также является аддитивной.

Предложение 1. *Если* $A=\prod\limits_{\iota\in\Im}(A_\iota, p_\iota)$ — *произведение в аддитивной категории* $\mathfrak{K}$, *то для любого объекта* U *из* $\mathfrak{K}$ *существует изоморфизм абелевых групп* Γ: $\prod\limits_{\iota\in\Im}H_{\mathfrak{K}}(U, A_\iota)\longrightarrow H_{\mathfrak{K}}(U, A)$, *причем*

$$\Gamma(\ldots, \varphi_\iota, \ldots)p_\iota=\varphi_\iota$$

и

$$\Gamma^{-1}(\varphi)=(\ldots, \varphi p_\iota, \ldots)$$

для любых $\iota\in\Im$, φ_ι: $U\longrightarrow A_\iota$ *и* φ: $U\longrightarrow A$.

Доказательство. Если $G=\prod\limits_{\iota\in\Im}H_{\mathfrak{K}}(U, A_\iota)$ и $\overline{\varphi}\in G$, то, как отмечалось в § 1,

$$\overline{\varphi}=(\ldots, \varphi_\iota, \ldots),$$

*) Часто в определении аддитивной категории дополнительно требуют существования копроизведений для конечного множества объектов, а категории, аддитивные в смысле предложенного определения, называют *предаддитивными*.

где $\varphi_\iota \in H_{\mathfrak{K}}(U, A_\iota)$. По определению произведения, существует единственный морфизм $\Gamma(\overline{\varphi}) \in H_{\mathfrak{K}}(U, A)$ такой, что $\Gamma(\overline{\varphi})\, p_\iota = \varphi_\iota$ для всех $\iota \in \mathfrak{I}$. Если

$$\overline{\psi} = (\ldots, \psi_\iota, \ldots) \in G,$$

то, очевидно $\Gamma(\overline{\varphi}) = \Gamma(\overline{\psi})$ влечет $\overline{\varphi} = \overline{\psi}$. Кроме того,

$$\Gamma(\overline{\varphi} + \overline{\psi})\, p_\iota = \varphi_\iota + \psi_\iota = (\Gamma(\overline{\varphi}) + \Gamma(\overline{\psi}))\, p_\iota,$$

откуда $\Gamma(\overline{\varphi} + \overline{\psi}) = \Gamma(\overline{\varphi}) + \Gamma(\overline{\psi})$, в силу предложения 1.6. Следовательно, Γ: $G \to H_{\mathfrak{K}}(U, A)$—гомоморфное вложение групп. Наконец, если $\varphi \in H_{\mathfrak{K}}(U, A)$, то

$$\overline{\varphi} = (\ldots, \varphi p_\iota, \ldots) \in G$$

и $\Gamma(\overline{\varphi})\, p_\iota = \varphi p_\iota$ для всех $\iota \in \mathfrak{I}$. Отсюда, ввиду предложения 1.6, $\Gamma(\overline{\varphi}) = \varphi$, т. е. Γ оказывается наложением. Этим же доказано, что

$$\Gamma^{-1}(\varphi) = (\ldots, \varphi p_\iota, \ldots).$$

Если $\mathfrak{I}' \subseteq \mathfrak{I}$, то по определению произведения и копроизведения существуют однозначно определенные морфизмы

$$p(\mathfrak{I}, \mathfrak{I}'): \prod_{\iota \in \mathfrak{I}} (A_\iota, p_\iota) \to \prod_{\iota \in \mathfrak{I}'} (A_\iota, p'_\iota)$$

и

$$u(\mathfrak{I}', \mathfrak{I}): \coprod_{\iota \in \mathfrak{I}'} (A_\iota, u'_\iota) \to \coprod_{\iota \in \mathfrak{I}} (A_\iota, u_\iota),$$

удовлетворяющие условиям $p(\mathfrak{I}, \mathfrak{I}')\, p'_\iota = p_\iota$ и $u'_\iota u(\mathfrak{I}', \mathfrak{I}) = u_\iota$ для всех $\iota \in \mathfrak{I}'$.

Предложение 2. *Пусть* $\{A_\iota, \iota \in \mathfrak{I}\}$—*семейство объектов аддитивной категории* $\mathfrak{K}$, $\mathfrak{I}_0$—*конечное подмножество множества* $\mathfrak{I}$, $A = \coprod_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$, $A^0 = \coprod_{\iota \in \mathfrak{I}_0} (A_\iota, u^0_\iota)$, $P = \prod_{\iota \in \mathfrak{I}} (A_\iota, p_\iota)$, $P^0 = \prod_{\iota \in \mathfrak{I}_0} (A_\iota, p^0_\iota)$ *и* $\theta = \sum_{\iota \in \mathfrak{I}_0} p^0_\iota u^0_\iota$. *Тогда существует морфизм* σ: $A \to P$, *обладающий следующими свойствами*:

(а) $u_\iota \sigma p_\varkappa = \begin{cases} 1_{A_\iota}, & \text{если } \iota = \varkappa, \\ 0_{A_\iota A_\varkappa}, & \text{если } \iota \neq \varkappa; \end{cases}$

(б) *если* $\mathfrak{I}' \subseteq \mathfrak{I}$ *и* $A' = \coprod_{\iota \in \mathfrak{I}'} (A_\iota, u'_\iota)$, *то и* $(\mathfrak{I}', \mathfrak{I})\, \sigma p_\varkappa = 0_{A' A_\varkappa}$ *для любого* $\varkappa \notin \mathfrak{I}'$.

(в) $u(\mathfrak{I}_0, \mathfrak{I})\, \sigma p(\mathfrak{I}, \mathfrak{I}_0)\, \theta = \mathrm{I}_{A^0}$ (рис. 6).

Доказательство. Для любых $\iota, \varkappa \in \mathfrak{I}$ положим

$$\sigma_{\iota\varkappa} = \begin{cases} \mathrm{I}_{A_\iota}, & \text{если } \iota = \varkappa, \\ 0_{A_\iota A_\varkappa}, & \text{если } \iota \neq \varkappa. \end{cases}$$

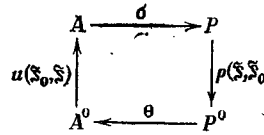


Рис. 6.

По определению копроизведения, существует морфизм $\sigma_\varkappa$: $A \longrightarrow A_\varkappa$ такой, что $u_\iota \sigma_\varkappa = \sigma_{\iota\varkappa}$. Используя определение произведения, найдем морфизм σ: $A \longrightarrow P$, где $\sigma p_\varkappa = \sigma_\varkappa$ для всех $\varkappa \in \mathfrak{I}$. Тогда

$$u_\iota \sigma p_\varkappa = u_\iota \sigma_\varkappa = \sigma_{\iota\varkappa},$$

что доказывает свойство (а). Кроме того, для любых $\iota \in \mathfrak{I}'$ и $\varkappa \notin \mathfrak{I}'$ имеем

$$u'_\iota u(\mathfrak{I}', \mathfrak{I})\, \sigma p_\varkappa = u_\iota \sigma p_\varkappa = 0_{A_\iota A_\varkappa} = u'_\iota 0_{A' A_\varkappa}.$$

Ввиду предложения 1.7, отсюда вытекает, что

$$u(\mathfrak{I}', \mathfrak{I})\, \sigma p_\varkappa = 0_{A' A_\varkappa}.$$

Далее замечаем, что, ввиду (а), для каждого $\varkappa \in \mathfrak{I}_0$ имеет место

$$u^0_\varkappa u(\mathfrak{I}_0, \mathfrak{I})\, \sigma p(\mathfrak{I}, \mathfrak{I}_0)\, \theta = \sum_{\iota \in \mathfrak{I}_0} u_\varkappa \sigma p(\mathfrak{I}, \mathfrak{I}_0)\, p^0_\iota u^0_\iota = \sum_{\iota \in \mathfrak{I}_0} u_\varkappa \sigma p_\iota u^0_\iota = u^0_\varkappa = u^0_\varkappa \mathrm{I}_{A_0},$$

после чего остается лишь использовать предложение 1.7.

Объект U категории $\mathfrak{K}$ с копроизведениями называется *малым*, если для любого морфизма φ: $U \longrightarrow \coprod_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$ найдется такое конечное подмножество $\mathfrak{I}_0 \subseteq \mathfrak{I}$, что $\varphi = \varphi' u(\mathfrak{I}_0, \mathfrak{I})$, где φ': $U \longrightarrow \coprod_{\iota \in \mathfrak{I}_0} (A_\iota, u^0_\iota)$.

Предложение 3. *Всякий конечно порожденный левый R-модуль является малым объектом категории левых R-модулей. Всякий малый проективный объект этой категории является конечно порожденным модулем.*

Доказательство. Если A — левый R-модуль, порожденный элементами $a_1, \ldots, a_n$, и φ: $A \longrightarrow \coprod_{\iota \in \mathfrak{I}} A_\iota$, то,

учитывая предложение 1.12, замечаем, что для некоторого конечного множества $\mathfrak{I}_0 \subseteq \mathfrak{I}$ имеем $\varphi(a_i) \in \coprod_{\iota \in \mathfrak{I}_0} A_\iota$ для всех i. Следовательно, A мал. Допустим теперь, что проективный левый R-модуль P является малым объектом категории R-Mod. Рассмотрим гомоморфное наложение $\psi\colon F \to P$, где F — свободный левый R-модуль. В силу предложения IV.7.2, $\varphi\psi = 1_P$ для некоторого $\varphi\colon P \to F$. Но, согласно предложению II.3.3, $F = \coprod_{\iota \in \mathfrak{I}} R_\iota$, где $R_\iota = R$ для всех $\iota \in \mathfrak{I}$. Следовательно $\varphi = \varphi' u(\mathfrak{I}_0, \mathfrak{I})$, где $\varphi'\colon P \to \coprod_{\iota \in \mathfrak{I}_0} R_\iota$ и $\mathfrak{I}_0$ — конечное подмножество в $\mathfrak{I}$. Из равенства

$$\varphi' u(\mathfrak{I}_0, \mathfrak{I})\psi = 1_P$$

и предложения 1.6 вытекает, что $u(\mathfrak{I}_0, \mathfrak{I})\psi$ — эпиморфизм. Ввиду предложения 1.4, $u(\mathfrak{I}_0, \mathfrak{I})\psi$ — наложение, и конечная порожденность модуля P очевидна.

Предложение 4. *Если $A = \coprod_{\iota \in \mathfrak{I}} (A_\iota, u_\iota)$ — копроизведение объектов аддитивной категории $\mathfrak{K}$ с произведениями, то для любого малого объекта U категории $\mathfrak{K}$ абелевы группы $H_{\mathfrak{K}}(U, A)$ и $\coprod_{\iota \in \mathfrak{I}} H_{\mathfrak{K}}(U, A_\iota)$ изоморфны.*

Доказательство. Положим $L = \coprod_{\iota \in \mathfrak{I}} H_{\mathfrak{K}}(U, A_\iota)$ и $G = \prod_{\iota \in \mathfrak{I}} H_{\mathfrak{K}}(U, A_\iota)$, и пусть P и σ имеют тот же смысл, что и в предложении 2.

Лемма 1. *Если $\varphi\colon U \to A$, то $\varphi\sigma p_\iota = 0_{UA_\iota}$ почти для всех $\iota \in \mathfrak{I}$.*

В самом деле, поскольку U мал, то $\varphi = \varphi' u(\mathfrak{I}_0, \mathfrak{I})$, где $\mathfrak{I}_0$ — конечное подмножество множества $\mathfrak{I}$. Учитывая предложение 2(б), получаем

$$\varphi\sigma p_\varkappa = \varphi' u(\mathfrak{I}_0, \mathfrak{I})\sigma p_\varkappa = \varphi' 0_{A^0 A_\varkappa} = 0_{UA_\varkappa}$$

для всех $\varkappa \notin \mathfrak{I}_0$.

Лемма 2. *Если $\bar{\varphi}\colon U \to P$ и $\bar{\varphi} p_\iota = 0_{UA_\iota}$ почти для всех ι, то $\bar{\varphi} = \varphi\sigma$ для некоторого $\varphi\colon U \to A$.*

В самом деле, пусть $\mathfrak{I}_0 = \{\iota \mid \iota \in \mathfrak{I},\ \bar{\varphi} p_\iota \neq 0\}$. По условию, $\mathfrak{I}_0$ конечно. Пусть A^0, P^0 и θ имеют тот же смысл, что и в предложении 2. Положим

$$\varphi = \bar{\varphi} p(\mathfrak{I}, \mathfrak{I}_0)\theta u(\mathfrak{I}_0, \mathfrak{I}).$$

Учитывая предложение 2(а), для каждого $\varkappa \in \mathfrak{I}$ получаем $\varphi\sigma p_\varkappa = \sum_{\iota \in \mathfrak{I}_0} \bar{\varphi} p(\mathfrak{I}, \mathfrak{I}_0)\, p_\iota^0 u_\iota^0 u(\mathfrak{I}_0, \mathfrak{I})\, \sigma p_\varkappa = \sum_{\iota \in \mathfrak{I}_0} \bar{\varphi} p_\iota u_\iota \sigma p_\varkappa = \bar{\varphi} p_\varkappa$, что, в силу предложения 1.6, влечет $\varphi\sigma = \bar{\varphi}$.

Вернемся к доказательству предложения. Пусть Γ: $G \to H_{\mathfrak{R}}(U, P)$ — изоморфизм абелевых групп, указанный в предложении 1. Для каждого $\varphi \in H_{\mathfrak{R}}(U, A)$ положим $\Delta(\varphi) = \Gamma^{-1}(\varphi\sigma)$. В силу предложения 1,

$$\Delta(\varphi) = (\ldots, \varphi\sigma p_\iota, \ldots),$$

и, по лемме 1, $\Delta(\varphi) \in L$. Таким образом, Δ: $H_{\mathfrak{R}}(U, A) \to L$ — гомоморфизм абелевых групп. Если $f \in L$, то $f = (\ldots, \varphi_\iota, \ldots)$, где $\varphi_\iota \in H_{\mathfrak{R}}(U, A_\iota)$, причем $\varphi_\iota = 0$ почти для всех $\iota \in \mathfrak{I}$. По предложению 1, $\Gamma(f)\, p_\iota = \varphi_\iota$, причем $\Gamma(f) \in H_{\mathfrak{R}}(U, P)$. Следовательно, по лемме 2, $\Gamma(f) = \varphi\sigma$ для некоторого $\varphi \in H_{\mathfrak{R}}(U, A)$. Отсюда

$$\Delta(\varphi) = \Gamma^{-1}(\varphi\sigma) = \Gamma^{-1}(\Gamma(f)) = f,$$

т. е. Δ оказывается наложением. Допустим теперь, что $\varphi \in H_{\mathfrak{R}}(U, A)$ и $\Delta(\varphi) = 0$. Тогда $\varphi\sigma = 0$. Поскольку объект U мал, то $\varphi = \varphi' u(\mathfrak{I}_0, \mathfrak{I})$, где $\mathfrak{I}_0$ — конечное подмножество в $\mathfrak{I}$ и φ': $U \to \coprod_{\iota \in \mathfrak{I}_0} (A_\iota, u_\iota^0)$. Ввиду предложения 2(в),

$$0 = \varphi\sigma p(\mathfrak{I}, \mathfrak{I}_0)\, \theta = \varphi' u(\mathfrak{I}_0, \mathfrak{I})\, \sigma p(\mathfrak{I}, \mathfrak{I}_0)\, \theta = \varphi'.$$

Следовательно, $\varphi = 0$, т. е. Δ — вложение.

Ядром морфизма φ: $A \to B$ аддитивной категории $\mathfrak{R}$ называется такой мономорфизм $\varkappa$: $K \to A$, что $\varkappa\varphi = 0$ и для любого морфизма $\varkappa'$: $K' \to A$ (рис. 7), удовлетворяющего равенству $\varkappa'\varphi = 0$, найдется такой морфизм: ω: $K' \to K$, что $\omega\varkappa = \varkappa'$. Нетрудно заметить, что в категории R-Mod ядром является естественное вложение обычного ядра (см. ЭА, с. 112). Двойственным образом определяется *коядро*. Ядро морфизма φ условимся обозначать через $\operatorname{Ker}\varphi$, а коядро — через $\operatorname{Coker}\varphi$.

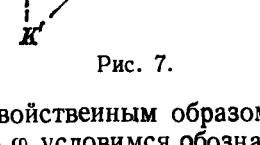


Рис. 7.

Категории $\mathfrak{R}$ и $\mathfrak{R}'$ называются *эквивалентными*, если существует функтор T: $\mathfrak{R} \to \mathfrak{R}'$, обладающий следующими свойствами:

(1) если $\varphi, \psi \in H_{\mathfrak{R}}(A, B)$ и $T(\varphi) = T(\psi)$, то $\varphi = \psi$;

(2) если $A, B \in \operatorname{Ob}\mathfrak{R}$ и $\bar{\varphi} \in H_{\mathfrak{R}'}(T(A), T(B))$, то $\bar{\varphi} = T(\varphi)$ для некоторого $\varphi \in H_{\mathfrak{R}}(A, B)$;

(3) если $\overline{A} \in \mathrm{Ob}\,\mathfrak{K}'$, то найдутся объект $A \in \mathrm{Ob}\,\mathfrak{K}$ и изоморфизм θ: $T(A) \to \overline{A}$ категории $\mathfrak{K}'$;

(4) если $\mathfrak{K}$ и $\mathfrak{K}'$ — аддитивные категории, то T — аддитивный функтор.

Предложение 5. *Пусть $\mathfrak{K}$ — аддитивная категория, обладающая следующими свойствами:*

(1) *В $\mathfrak{K}$ существует копроизведение любого множества объектов;*

(2) *$\mathfrak{K}$ содержит малый проективный образующий U;*

(3) *каждый эпиморфизм категории $\mathfrak{K}$ служит коядром некоторого мономорфизма;*

(4) *каждый морфизм категории $\mathfrak{K}$ представляется в виде произведения эпиморфизма и мономорфизма;*

(5) *всякий мономорфизм служит ядром некоторого морфизма.*

Тогда $\mathfrak{K}$ эквивалентна категории левых $H_{\mathfrak{K}}(U, U)$-модулей.

Доказательство. Обозначим через R кольцо $H_{\mathfrak{K}}(U, U)$. Поскольку для любых $\lambda \in H_{\mathfrak{K}}(U, U)$ и $a \in H_{\mathfrak{K}}(U, A)$ определено произведение $\lambda a \in H_{\mathfrak{K}}(U, A)$, то каждая абелева группа $H_{\mathfrak{K}}(U, A)$ естественным образом превращается в левый R-модуль. Более того, $T = \mathrm{Hom}(U, —)$ (см. конец § 1) оказывается аддитивным функтором из категории $\mathfrak{K}$ в категорию левых R-модулей R-Mod.

Лемма 1. *Если $\varphi, \psi \in H_{\mathfrak{K}}(A, B)$ и $T(\varphi) = T(\psi)$, то $\varphi = \psi$.*

Действительно, если $\varphi \neq \psi$, то, поскольку U — образующий, $f\varphi \neq f\psi$ для некоторого $f \in H_{\mathfrak{K}}(U, A) = T(A)$. Отсюда

$$T(\varphi)(f) = f\varphi \neq f\psi = T(\psi)(f),$$

т. е. $T(\varphi) \neq T(\psi)$.

Лемма 2. *Если $B \in \mathrm{Ob}\,\mathfrak{K}$ и $\Phi \in \mathrm{Hom}_R(T(U), T(B))$, то $\Phi = T(\varphi)$ для некоторого $\varphi \in H_{\mathfrak{K}}(U, B)$.*

Для доказательства положим $\varphi = \Phi(1_U)$. Тогда для любого $\lambda \in R = T(U)$ имеем

$$\Phi(\lambda) = \Phi(\lambda 1_U) = \lambda\Phi(1_U) = \lambda\varphi = T(\varphi)(\lambda),$$

откуда $\Phi = T(\varphi)$.

Лемма 3. *Если $A, B \in \mathrm{Ob}\,\mathfrak{K}$ и $\Phi \in \mathrm{Hom}_R(T(A), T(B))$, то $\Phi = T(\varphi)$ для некоторого $\varphi \in H_{\mathfrak{K}}(A, B)$.*

В самом деле, согласно предложению 1.15, существует эпиморфизм π: $F \to A$, где $F = \coprod_{\iota \in \mathfrak{I}} (U_\iota, u_\iota)$ и $U_\iota = U$ для

всех $\iota \in \mathfrak{I}$. По условию, эпиморфизм π служит коядром некоторого мономорфизма $\varkappa$: $K \to F$ (рис. 8). Положим

$$\Phi_\iota = T(u_\iota)\, T(\pi)\, \Phi.$$

В силу леммы 2, $\Phi_\iota = T(\varphi_\iota)$ для некоторого $\varphi_\iota \in H_\mathfrak{K}(U, B)$. По определению копроизведения существует морфизм $\bar{\varphi}$: $F \to B$ такой, что $u_\iota \bar{\varphi} = \varphi_\iota$ для всех $\iota \in \mathfrak{I}$. Если $\varkappa\bar{\varphi} \neq 0$, то, поскольку U — образующий, $\rho\varkappa\bar{\varphi} \neq 0$ для некоторого $\rho \in H_\mathfrak{K}(U, K)$. Тогда $\rho\varkappa \in H_\mathfrak{K}(U, F)$. Поскольку U мал, то $\rho\varkappa = \rho' u(\mathfrak{I}_0, \mathfrak{I})$, где $\mathfrak{I}_0$ — конечное подмножество множества $\mathfrak{I}$. Учитывая предложение 2(в), получаем

$$\begin{aligned}
\rho\varkappa\bar{\varphi} &= \rho' u(\mathfrak{I}_0, \mathfrak{I})\,\bar{\varphi} = \rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p(\mathfrak{I}, \mathfrak{I}_0)\,\theta u(\mathfrak{I}_0, \mathfrak{I})\,\bar{\varphi} = \\
&= \sum_{\iota \in \mathfrak{I}_0} \rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p(\mathfrak{I}, \mathfrak{I}_0)\, p^0_\iota u^0_\iota u(\mathfrak{I}_0, \mathfrak{I})\,\bar{\varphi} = \\
&= \sum_{\iota \in \mathfrak{I}_0} \rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p_\iota u_\iota \bar{\varphi} = \sum_{\iota \in \mathfrak{I}_0} \rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p_\iota \varphi_\iota = \\
&= \sum_{\iota \in \mathfrak{I}_0} (\rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p_\iota)\, T(\varphi_\iota) = \\
&= \sum_{\iota \in \mathfrak{I}_0} \rho^\flat u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p_\iota\, (T(u_\iota)\, T(\pi)\, \Phi) = \\
&= \sum_{\iota \in \mathfrak{I}_0} \Phi(\rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p_\iota\, (T(u_\iota)\, T(\pi))) = \\
&= \sum_{\iota \in \mathfrak{I}_0} \Phi(\rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p_\iota u_\iota \pi) = \\
&= \sum_{\iota \in \mathfrak{I}_0} \Phi(\rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p(\mathfrak{I}, \mathfrak{I}_0)\, p^0_\iota u^0_\iota u(\mathfrak{I}_0, \mathfrak{I})\,\pi) = \\
&= \Phi(\rho' u(\mathfrak{I}_0, \mathfrak{I})\,\sigma p(\mathfrak{I}, \mathfrak{I}_0)\,\theta u(\mathfrak{I}_0, \mathfrak{I})\,\pi) = \\
&= \Phi(\rho' u(\mathfrak{I}_0, \mathfrak{I})\,\pi) = \Phi(\rho\varkappa\pi) = 0,
\end{aligned}$$

ибо $\varkappa\pi = 0$. Противоречие. Следовательно, $\varkappa\bar{\varphi} = 0$ и, по определению коядра, $\bar{\varphi} = \pi\varphi$ для некоторого $\varphi \in H_\mathfrak{K}(A, B)$.

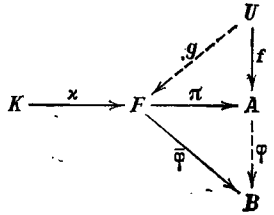


Рис. 8.

Если теперь $f \in T(A) = H_\mathfrak{K}(U, A)$, то, поскольку U проек-

тивен, а π—эпиморфизм, $f=g\pi$ для некоторого $g\in H_{\mathfrak{R}}(U, F)$. Используя малость объекта U, запишем $g=g'u(\mathfrak{I}_0, \mathfrak{I})$, где $\mathfrak{I}_0$—конечное подмножество множества $\mathfrak{I}$. Предложение 2(в) позволяет записать

$$\begin{aligned} f=g\pi=g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\pi=g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p(\mathfrak{I},\ \mathfrak{I}_0)\,\theta u(\mathfrak{I}_0,\ \mathfrak{I})\,\pi= \\ =\sum_{\iota\in\mathfrak{I}_0} g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p(\mathfrak{I},\ \mathfrak{I}_0)\,p_\iota^0 u_\iota^0 u(\mathfrak{I}_0,\ \mathfrak{I})\,\pi= \\ =\sum_{\iota\in\mathfrak{I}_0} g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p(\mathfrak{I},\ \mathfrak{I}_0)\,p_\iota^0 u_\iota\pi= \\ =\sum_{\iota\in\mathfrak{I}_0}(g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p(\mathfrak{I},\ \mathfrak{I}_0)\,p_\iota^0)\,T(u_\iota\pi)=\sum_{\iota\in\mathfrak{I}_0}(g\sigma p_\iota)\,T(u_\iota\pi). \end{aligned}$$

Отсюда

$$\begin{aligned} \Phi(f)=\sum_{\iota\in\mathfrak{I}_0} g\sigma p_\iota(T(u_\iota\pi)\,\Phi)=\sum_{\iota\in\mathfrak{I}_0}(g\sigma p_\iota)\,\Phi_\iota= \\ =\sum_{\iota\in\mathfrak{I}_0}(g\sigma p_\iota)\,T(\varphi_\iota)=\sum_{\iota\in\mathfrak{I}_0} g\sigma p_\iota\varphi_\iota. \end{aligned}$$

С другой стороны, с помощью того же предложения 2(в) получаем

$$\begin{aligned} T(\varphi)(f)=f\varphi=g\pi\varphi=g\overline{\varphi}=g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\overline{\varphi}= \\ =g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p(\mathfrak{I},\ \mathfrak{I}_0)\,\theta u(\mathfrak{I}_0,\ \mathfrak{I})\,\overline{\varphi}= \\ =\sum_{\iota\in\mathfrak{I}_0} g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p(\mathfrak{I},\ \mathfrak{I}_0)\,p_\iota^0 u_\iota^0 u(\mathfrak{I}_0,\ \mathfrak{I})\,\overline{\varphi}= \\ =\sum_{\iota\in\mathfrak{I}_0} g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p_\iota u_\iota\overline{\varphi}= \\ =\sum_{\iota\in\mathfrak{I}_0} g'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p_\iota\varphi_\iota=\sum_{\iota\in\mathfrak{I}_0} g\sigma p_\iota\varphi_\iota. \end{aligned}$$

Таким образом, $\Phi(f)=T(\varphi)(f)$ для всех $f\in T(A)$, т. е. $\Phi=T(\varphi)$.

Лемма 4. *Если* $F=\coprod_{\iota\in\mathfrak{I}}(U_\iota, u_\iota)$, *где* $U_\iota=U$ *для всех* $\iota\in\mathfrak{I}$, *то* $T(F)$—*свободный левый* R-*модуль со свободной порождающей системой* $\mathscr{E}=\{u_\iota\mid\iota\in\mathfrak{I}\}$.

Для доказательства, ввиду предложения II.3.2, достаточно установить, что $\mathscr{E}$—база модуля $T(F)$. Но для любого $f\in T(F)=H_{\mathfrak{R}}(U, F)$, поскольку U мал, имеем $f=f'u(\mathfrak{I}_0, \mathfrak{I})$ для некоторого конечного подмножества $\mathfrak{I}_0$ множества $\mathfrak{I}$. Поскольку

$$\lambda_\iota=f'u(\mathfrak{I}_0,\ \mathfrak{I})\,\sigma p_\iota\in H_{\mathfrak{R}}(U,\ U)=R,$$

используя предложение 2(в), получаем

$$f = f'u(\mathfrak{I}_0, \mathfrak{I}) = f'u(\mathfrak{I}_0, \mathfrak{I})\sigma p(\mathfrak{I}, \mathfrak{I}_0)\theta u(\mathfrak{I}_0, \mathfrak{I}) =$$
$$= \sum_{\iota \in \mathfrak{I}_0} f'u(\mathfrak{I}_0, \mathfrak{I})\sigma p(\mathfrak{I}, \mathfrak{I}_0)\, p_\iota^0 u_\iota^0 u(\mathfrak{I}_0, \mathfrak{I}) =$$
$$= \sum_{\iota \in \mathfrak{I}_0} f'u(\mathfrak{I}_0, \mathfrak{I})\sigma p_\iota u_\iota = \sum_{\iota \in \mathfrak{I}_0} \lambda_\iota u_\iota.$$

Если же $\sum_{\iota \in \mathfrak{I}_0} \lambda_\iota u_\iota = 0$, где $\mathfrak{I}_0$ — конечное подмножество множества $\mathfrak{I}$ и $\lambda_\iota \in R = \mathrm{Hom}_{\mathfrak{K}}(U, U)$, то, ввиду предложения 2(а), для каждого $\varkappa \in \mathfrak{I}_0$ получаем

$$0 = \left(\sum_{\iota \in \mathfrak{I}_0} \lambda_\iota u_\iota\right)\sigma p_\varkappa = \sum_{\iota \in \mathfrak{I}_0} \lambda_\iota u_\iota \sigma p_\varkappa = \lambda_\varkappa.$$

Лемма 5. *Если* ω*—эпиморфизм из* $H_{\mathfrak{K}}(A, B)$, *то* $T(\omega)$*—эпиморфизм категории* R-Mod.

Для доказательства рассмотрим в категории R-Mod точную последовательность

$$T(A) \xrightarrow{T(\omega)} T(B) \xrightarrow{\Pi} M \longrightarrow 0.$$

Если $M = 0$, то все доказано. В противном случае найдем ненулевой гомоморфизм Φ: $R \longrightarrow M$ (рис. 9). Поскольку Π — эпиморфизм, то $\Phi = \Psi\Pi$ для некоторого Ψ: $R \longrightarrow T(B)$. Ввиду леммы 2, $\Psi = T(\psi)$ для некоторого $\psi \in H_{\mathfrak{K}}(U, B)$ (рис. 9). Поскольку U проективен, а ω — эпиморфизм, то

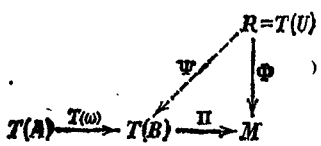


Рис. 9.

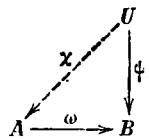


Рис. 10.

$\psi = \chi\omega$ для некоторого $\chi \in H_{\mathfrak{K}}(U, A)$ (рис. 10). Отсюда

$$\Phi = \Psi\Pi = T(\psi)\,\Pi = T(\chi)\,T(\omega)\,\Pi = 0,$$

вопреки выбору гомоморфизма Φ.

Лемма 6. *Для всякого левого* R*-модуля* M *найдется объект* $A \in \mathrm{Ob}\,\mathfrak{K}$ *такой, что модули* M *и* $T(A)$ *изоморфны.*

Для доказательства заметим, что, ввиду леммы 4, в категории R-Mod существует точная последовательность

$$T(G) \xrightarrow{\Phi} T(F) \xrightarrow{\Pi} M \longrightarrow 0,$$

где F и G — копроизведения некоторого множества экземпляров объекта U. В силу леммы 3, $\Phi = T(\varphi)$ для некоторого $\varphi \in H_{\mathfrak{R}}(G, F)$. По условию, $\varphi = \pi\varkappa$, где π — эпиморфизм, а $\varkappa$ — мономорфизм (рис. 11). Из условия же вытекает, что $\varkappa$ — ядро некоторого морфизма χ, причем $\chi = \tau\rho$, где τ: $F \to C$ — эпиморфизм, а ρ — мономорфизм. Из равенства $(\varkappa\tau)\rho = \varkappa\chi = 0$ вытекает, что $\varkappa\tau = 0$, ибо ρ — мономорфизм. Поэтому

$$\Phi T(\tau) = T(\varphi)\,T(\tau) = T(\varphi\tau) = T(\pi\varkappa\tau) = 0$$

и, в силу предложения II.1.3, существует гомоморфизм X: $M \to T(C)$ такой, что $\Pi X = T(\tau)$ (рис. 12). Из леммы 5 и предложений 1.4 и 1.6 вытекает, что X — наложение. Если X не является вложением, то $mX = 0$ для некоторого

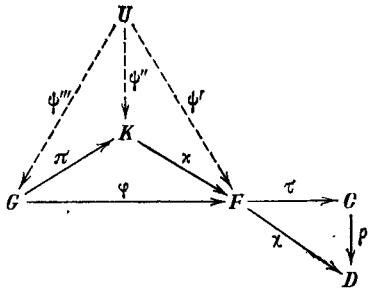


Рис. 11.

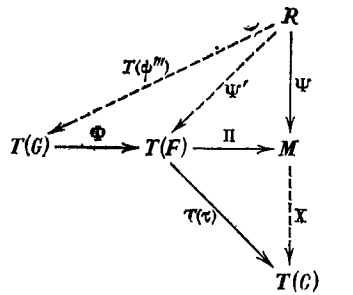


Рис. 12.

ненулевого $m \in M$. Положив $1\Psi = m$, определим гомоморфизм Ψ: $R \to M$ такой, что $\Psi \neq 0$, но $\Psi X = 0$. Поскольку Π — эпиморфизм, то $\Psi = \Psi'\Pi$ для некоторого $\Psi' \in \mathrm{Hom}_R(R, T(F))$, а в силу леммы 3, $\Psi' = T(\psi')$ для некоторого $\psi' \in H_{\mathfrak{R}}(U, F)$. Отсюда

$$T(\psi'\chi) = T(\psi')\,T(\tau)\,T(\rho) = \Psi'\Pi X T(\rho) = \Psi X T(\rho) = 0,$$

что, ввиду леммы 1, дает $\psi'\chi = 0$. Но $\varkappa = \mathrm{Ker}\,\chi$. Поэтому $\psi' = \psi''\varkappa$ для некоторого $\psi'' \in H_{\mathfrak{R}}(U, K)$. Но π — эпиморфизм, а объект U проективен. Следовательно, $\psi'' = \psi'''\pi$, для некоторого $\psi''' \in H_{\mathfrak{R}}(U, G)$. Отсюда

$$\psi' = \psi''\varkappa = \psi'''\pi\varkappa = \psi'''\varphi,$$

а значит

$$\Psi = \Psi'\Pi = T(\psi')\,\Pi = T(\psi''')\,T(\varphi)\,\Pi = T(\psi''')\,\Phi\Pi = 0.$$

Полученное противоречие завершает доказательство леммы.

Справедливость предложения является следствием леммы 1, 3 и 6.

Поскольку в категории R-Mod свойства (1)—(5), очевидно, справедливы, непосредственным следствием предложения 5 является:

Теорема 1. *Аддитивная категория $\mathfrak{K}$ эквивалентна категории всех левых модулей над некоторым кольцом тогда и только тогда, когда в $\mathfrak{K}$ существует копроизведение любого множества объектов, $\mathfrak{K}$ содержит малый проективный образующий U, каждый морфизм категории $\mathfrak{K}$ обладает ядром, каждый морфизм категории $\mathfrak{K}$ представляется в виде произведения эпиморфизма и мономорфизма и всякий мономорфизм служит ядром некоторого морфизма.*

Теорема 2. *Пусть R—ассоциативное кольцо с единицей и R_n—кольцо $n\times n$-матриц над ним. Тогда категории всех лезых R- и R_n-модулей эквивалентны.*

Доказательство. Пусть E_{ij}—матрица из R_n, у которой на месте (i, j) стоит 1 и на остальных местах—нули, и $E_i=E_{ii}$. Нетрудно проверить, что

$$R_n=R_nE_1\oplus\ \dots\ \oplus R_nE_n$$

(ср. ЭА, с. 130, теорема 5). Более того, левые R_n-модули R_nE_i изоморфны между собой. В самом деле, для каждой $X\in R_n$ положим

$$\Phi(XE_1)=XE_{1i}.$$

Если $XE_1=YE_1$, то

$$XE_{1i}=XE_1E_{1i}=YE_1E_{1i}=YE_{1i}.$$

Следовательно, Ф—корректно определенное отображение модуля R_nE_1 в R_nE_i, являющееся, как легко проверить, гомоморфизмом левых R_n-модулей. Если $XE_{1i}=YE_{1i}$, то, умножая справа на E_{i1}, получим $XE_1=YE_1$, т. е. Ф оказывается вложением. Равенство

$$E_i=E_{i1}E_{1i}=\Phi(E_{i1}E_1)$$

показывает, что Ф—наложение. Таким образом,

$$R_n=\underbrace{U\oplus\ \dots\ \oplus U}_{n\text{ раз}},$$

где $U\cong R_nE_1$, и, ввиду предложений 1.12 и II.1.3 каждый

свободный левый R_n-модуль изоморфен копроизведению некоторого множества экземпляров модуля U. Поскольку каждый левый R_n-модуль изоморфен фактор-модулю свободного, то из предложений 1.3 и 1.15 вытекает, что U — образующий категории R_n-Mod. Будучи конечно порожденным, этот модуль, по предложению 3, оказывается малым объектом категории R_n-Mod. Ввиду предложения IV.7.2, R_nE_1 — проективный R_n-модуль. Поэтому, согласно предложению 5, категория R_n-Mod эквивалентна категории $\mathrm{Hom}_{R_n}(U, U)$-Mod. Таким образом, для завершения доказательства остается установить справедливость следующего утверждения:

Лемма. *Кольца* $\mathrm{Hom}_{R_n}(U, U)$ *и* R *изоморфны.*

Для доказательства леммы рассмотрим отображение Γ кольца R в кольцо $\mathrm{Hom}_{R_n}(U, U)$, определяемое равенством

$$E_1\Gamma(\lambda) = E_1\lambda.$$

Поскольку

$$E_1(\Gamma(\lambda)\,\Gamma(\mu)) = (E_1\lambda)\,\Gamma(\mu) = ((\lambda E)\,E_1)\,\Gamma(\mu) = \\ = \lambda E \cdot E_1\mu = E_1\lambda\mu = E_1\Gamma(\lambda\mu)$$

для любых $\lambda, \mu \in R$, то Γ — гомоморфизм колец. Импликация

$$(E_1\lambda = E_1\mu) \Rightarrow (\lambda = \mu)$$

показывает, что Γ — вложение. Если, наконец, $f \in \in \mathrm{Hom}_{R_n}(U, U)$ и

$$E_1 f = E_{11}\lambda_1 + \ldots + E_{n1}\lambda_n,$$

то

$$E_1 f = E_1^2 f_1 = E_1(E_1 f) = E_1\lambda_1 = E_1\Gamma(\lambda_1).$$

Следовательно, $f = \Gamma(\lambda_1)$, т. е. Γ оказывается наложением.

Из теоремы 2 вытекает, что любой класс колец, определяемый свойствами категории модулей над ним, замкнут относительно перехода к кольцам матриц. В частности, из теоремы IV.7.3 вытекает:

Следствие. *Кольцо матриц над классически полупростым кольцом классически полупросто.*

Упражнения

1. Если A — правый R-модуль, то положим $T(B) = A \otimes_R B$ (см. § 4, гл. IV). Определить $T(\varphi)$ для морфизмов категории R-Mod так, чтобы T стал аддитивным функтором из категории R-Mod в категорию абелевых групп.

2. Копроизведение конечного множества малых объектов аддитивной категории является малым объектом.

3. Ретракт малого объекта аддитивной категории мал.

4. Модуль, не представимый как объединение счетного множества своих собственных подмодулей, мал. Указание. Сначала рассмотреть гомоморфизм в копроизведение счетного множества модулей. При рассмотрении копроизведения с произвольным множеством слагаемых построить последовательность гомоморфизмов на конечные копроизведения с возрастающим числом слагаемых.

5. Пусть R — кольцо, структура левых идеалов которого изоморфна цепи действительных чисел из отрезка $[0, 1]$. Доказать, что максимальный левый идеал этого кольца мал, но не конечно порожден. Построить пример такого кольца (ср. Klatt G. B., Levy L. S.—Trans. Amer. Math. Soc., 1969, 137, 407—419.

6. Доказать, что кообразующим в категории абелевых групп служит прямое произведение аддитивной группы рациональных чисел и групп типа p^∞ для всех простых чисел p (Фукс Л. Бесконечные абелевы группы. Т. 1.— М.: Мир, 1974, гл. 1, § 3).

7. Кольцо R регулярно тогда и только тогда, когда справедливо следующее свойство: если P и P' — малые проективные объекты категории R-Mod, A — произвольный левый R-модуль, φ: $A \to P$ — мономорфизм и π: $P' \to A$ — эпиморфизм, то φ — коретракция. Указание. При выполнении указанного свойства следует устаиовить справедливость свойства (4) теоремы IV.2.1. Если же R регулярно, то можно вложить P в конечно порожденный свободный модуль и воспользоваться леммой 1 теоремы IV.2.2.

8. Используя теорему 2 и упражнение 7, дать новое доказательство теоремы IV.2.2.

ЛИТЕРАТУРА

Букур И., Деляну А. Введение в теорию категорий и функторов.— М.: Мир, 1972.

Картан А., Эйленберг С. Гомологическая алгебра.— М.: ИЛ, 1960.

Маклейн С. Гомология.— М.: Мир, 1966.

Фейс К., Алгебра: кольца, модули и категории. Т. I.— М.: Мир, 1977, Т.II.— М.: Мир, 1979.

Цаленко М. Ш., Шульгейфер Е. Г. Основы теории категорий.— М.: Наука, 1974.

Mitchell B. Rings with several objects. Adv. Math., 1972, 8, p. 1—161.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ