А. Г. КУРОШ

ЛЕКЦИИ ПО ОБЩЕЙ АЛГЕБРЕ

ИЗДАНИЕ ВТОРОЕ

ИЗДАТЕЛЬСТВО «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
Москва 1973

517.1
К 93
УДК 512.8

К $\frac{0223—1797}{042(02)\text{-}73}$ 47-73

ОГЛАВЛЕНИЕ

ОТ РЕДАКТОРА

Вышедшие в 1962 году своим первым изданием «Лекции по общей алгебре» А. Г. Куроша подводили итог громадной работы одного из крупнейших современных алгебраистов по пропаганде идей и методов абстрактной, теоретико-множественной («общей», как любил говорить А. Г. Курош) алгебры среди широких кругов математиков.

Книга сразу стала библиографической редкостью. Ее автор в последние годы своей жизни мечтал о широком пополнении книги. Об этом говорится в введении к ротапринтному изданию Московского университета «А. Г. Курош. Общая алгебра (лекции 1969/70 учебного года). Москва — 1970» его автором следующее: «В 1962 г. вышла из печати моя книга «Лекции по общей алгебре», позже появились ее переводы на английский, немецкий, французский, польский, чешский, японский и китайский языки. Настоящий курс не опирается на эту книгу и имеет с нею сравнительно немного перекрытий, хотя идейно к ней весьма близок. Надеюсь, что в будущем я смогу объединить материал этой книги и этого курса в одну новую книгу».

К сожалению, этому не суждено было сбыться...

Настоящее издание книги было предпринято уже после ухода ее автора из жизни (Александр Геннадиевич Курош скончался 18 мая 1971 года). Оно полностью воспроизводит, без каких-либо существенных изменений, текст первого издания; исправлены лишь отдельные неточности и опечатки.

Однако, в интересах читателя, широко пополнен «Указатель литературы», помещенный в конце книги. За последние 10 лет бурное развитие общей алгебры сопровождалось еще более бурно возраставшим потоком книг по алгебре во всем мире. Положение сложилось таким, что пришлось почти полностью отказаться от дополнительного включения в «Указатель»

журнальных статей (даже и обзорного характера), а также книг ротапринтного и препринтного изданий. (Некоторое предпочтение в этом отношении дано лишь двум направлениям в алгебре, особенно увлекшим А. Г. Куроша в последние годы его жизни, — теории категорий и теории универсальных алгебр.)

Правда, в значительной степени этот урон компенсируется перечислением в «Указателе» всех обзоров по алгебре, вышедших в серии сборников «Итоги науки, ВИНИТИ АН СССР», каждый из которых снабжен весьма подробной библиографией.

Наконец, в интересах прежде всего более молодых читателей книги, в «Указатель литературы» включено несколько книг по теории множеств, математической логике и топологии, а также по некоторым приложениям алгебры.

О. Н. Головин

ПРЕДИСЛОВИЕ

На рубеже двадцатых и тридцатых годов нашего века широкие круги математиков обнаружили, что в алгебре, одной из старейших ветвей математики, произошла радикальная перестройка. Эта перестройка, а именно превращение алгебры в теоретико-множественную, аксиоматическую науку, имеющую основным объектом изучения алгебраические операции, производимые над элементами произвольной природы, была подготовлена, конечно, всем предшествующим развитием алгебры. Началась она еще в конце девятнадцатого века, продолжалась, постепенно усиливаясь, в первых десятилетиях двадцатого века, но лишь выход в 1930 и 1931 гг. двухтомной «Современной алгебры» Ван-дер-Вардена сделал идеи, результаты и методы этой «новой» алгебры доступными всем математикам-неалгебраистам.

Общеизвестно, сколь значительным, а иногда и решающим, было в дальнейшем влияние этой современной алгебры на развитие многих областей математики, из которых в первую очередь назовем топологию и функциональный анализ. Одновременно в последние три десятилетия продолжалось интенсивное и даже бурное развитие самой алгебры, обнаружились ее многочисленные новые связи со смежными разделами науки, и в результате лицо современной или, как мы предпочитаем говорить, общей алгебры стало сейчас совсем иным, чем оно было тридцать лет тому назад.

За эти десятилетия весьма далеко идущее развитие испытали те более старые ветви общей алгебры — теория полей и теория ассоциативных и ассоциативно-коммутативных колец, — которым была в основном посвящена книга Ван-дер-Вардена. Еще более решительной была перестройка теории групп, старейшей среди всех ветвей общей алгебры. Вместе с тем теория колец в значительной мере стала сейчас теорией неассоциативных колец, включающей в себя в качестве составной

части теорию лиевых колец и алгебр. Возникла и заняла весьма заметное место топологическая алгебра, развилась параллельная ей теория упорядоченных алгебраических образований. Появилась и быстро развилась теория структур, в самые последние годы возникла параллельная ей теория категорий, имеющая, несомненно, очень большое будущее. В рамках классических разделов общей алгебры оформились такие самостоятельные направления, как гомологическая алгебра, уже нашедшая многочисленные выходы в топологию и алгебраическую геометрию, проективная алгебра, включившая в себя основное содержание проективной геометрии, и дифференциальная алгебра, открывающая общей алгебре непосредственные выходы в теорию дифференциальных уравнений. Теории полугрупп и квазигрупп перестали быть просто теориями «обобщенных» групп и нашли собственные пути развития и собственные области приложений. Возникла, наконец, общая теория универсальных алгебр и еще более общая, переплетающаяся с математической логикой, теория моделей.

Казалось бы, что основные идеи и важнейшие результаты, накопленные к настоящему времени общей алгеброй, должны были бы в той же мере входить в научный багаж всякого культурного математика, как это было в тридцатых годах, когда экзамен по современной алгебре сдавался большинством аспирантов-математиков. На самом деле, однако, это далеко не так — знакомство широких кругов математиков с достижениями общей алгебры остается сейчас в значительной мере на уровне начала тридцатых годов.

Причину этого указать легко. Основным пособием, по которому молодые математики изучают общую алгебру, у нас остается книга Ван-дер-Вардена, хотя эта книга, безусловно замечательная и сыгравшая в истории математики двадцатого века выдающуюся роль, уже так далека от современного состояния алгебры, что сам автор, выпуская ее четвертое издание, назвал ее просто «Алгеброй».

В зарубежной литературе имеются и другие книги, более свежие. Некоторые из них, несколько модернизируя материал, изложенный в книге Ван-дер-Вардена, в основном дополняют и развивают его в сторону личных научных интересов автора. Получаются полезные книги, не дающие, однако, правильного представления о современном состоянии общей алгебры. Кроме того, это обычно книги большого объема, адресующиеся скорее к алгебраистам, чем к математикам всех специальнос-

тей. Книги другого типа представляют собой по существу свод основных алгебраических понятий и их простейших свойств. Полезные в качестве справочных пособий, такие книги не дают читателю возможности почувствовать все своеобразие и глубину современной алгебраической науки — самые глубокие и самые значительные результаты в них или отсутствуют совсем, или же формулируются среди упражнений.

Для того, чтобы показать математикам современное лицо общей алгебры, более подошла бы книга иного характера. Не очень большая по объему, она должна была бы адресоваться к читателю, владеющему университетским курсом высшей алгебры и желающему пополнить свое алгебраическое образование, но, быть может, не предполагающему выбирать алгебру своей научной специальностью. Этим не исключается, конечно, возможность того, что и алгебраист в вопросах, далеких от своих специальных интересов, мог бы найти в этой книге кое-что для себя полезное.

Эта книга не должна и не могла бы заменить монографий по отдельным разделам общей алгебры. Не должна она быть и коллекцией вводных глав из этих монографий. Задачей книги был бы показ основных разделов современной общей алгебры, преимущественно в их взаимной связи, причем изложение доводилось бы до отдельных глубоких теорем и нацеливалось бы на эти теоремы. Отбор весьма небольшого числа таких теорем в каждом из основных разделов общей алгебры неизбежно определялся бы субъективными оценками автора книги. Сами эти теоремы вовсе не должны были бы излагаться в наибольшей общности, достигнутой к настоящему времени.

Содержание этой книги было бы, понятно, весьма мозаичным, и читателю пришлось бы, следуя за автором, иногда в пределах одного параграфа переходить из одной ветви общей алгебры в другую. Разбивка материала на главы была бы столь условной, что о схеме зависимости глав не могло бы быть речи.

О желательности появления книги такого характера мне привелось говорить в 1951 г. на Всесоюзном совещании по алгебре и теории чисел (см. Успехи матем. наук **7**: 3 (1952), стр. 167), а писать ее я начал в 1956 г. За четыре года, прошедших с этого времени, работа над книгой неоднократно прерывалась и возобновлялась, план книги много раз менялся, многие параграфы писались по нескольку раз, написанный

материал переставлялся, переделывался, выбрасывался. Иными словами, работа приобретала такой характер, что все чаще и чаще приходилось вспоминать новеллу Бальзака «Неведомый шедевр»... Было разумно поэтому завершить работу, не стремясь довести книгу до того состояния, которое соответствовало бы изложенной выше программе. Читатель без труда обнаружит, в чем именно книга отступает от этой программы.

Замечу, что название книги полностью оправдывается тем, что в основе ее лежат три больших специальных курса по общей алгебре, прочитанные мною за последние десять лет в Московском университете.

В книгу местами включены формулировки некоторых результатов, в самой книге не доказываемых и не используемых. Предполагается, что эти формулировки, выделенные из общего текста звездочками, читателем не будут пропускаться. Вряд ли нужно специально подчеркивать, что включение в книгу этих дополнительных указаний не означает доведения соответствующих мест книги до самых последних результатов, к настоящему времени полученных.

Ссылки на журнальную литературу, встречающиеся в тексте книги, в общем довольно случайны и не могут рассматриваться как материал по истории алгебры в двадцатом веке. С другой стороны, к книге приложен достаточно полный указатель книг по различным разделам общей алгебры, вышедших за последние тридцать лет. В него включены и некоторые обзорные статьи.

Ввиду большой многоплановости и мозаичности книги в ней пришлось весьма часто делать ссылки на предшествующий материал, хотя ясно, что в большинстве случаев читатель будет находить эти ссылки для себя излишними. Ссылка V.3.6 означает: глава пятая, параграф 3, пункт 6.

И первоначальный план книги, и ряд ее глав, притом некоторые в различных редакциях, я имел удовольствие докладывать на семинаре по общей алгебре Московского университета. Я приношу моим товарищам по семинару за их интерес к моей работе, за советы и критику свою искреннюю благодарность. Я горячо благодарю также Олега Николаевича Головина, взявшего на себя большой труд редактирования книги, внимательно прочитавшего рукопись и сделавшего много полезных замечаний.

Москва,
май 1960 г.

А. Курош

ГЛАВА ПЕРВАЯ

ОТНОШЕНИЯ

§ 1. Множества

1. В основе общей алгебры лежат понятия и методы теории множеств. Читатель, приступающий к изучению общей алгебры, не нуждается, конечно, в том, чтобы ему напоминали определения таких теоретико-множественных понятий, как *подмножество, дополнение* подмножества в множестве, *пустое множество, пересечение* и *объединение* множеств. Отметим, что для обозначения пересечения и объединения множеств мы будем употреблять соответственно символы $\bigcap$ и $\bigcup$, для обозначения принадлежности подмножества и элемента к множеству — соответственно символы $\subset$ и $\in$, а дополнение подмножества A в множестве M будем обозначать через $M \setminus A$.

Операции пересечения и объединения множеств связаны между собою следующими двойственными друг другу законами дистрибутивности: для любых трех множеств A, B, C

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \tag{1}$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C). \tag{2}$$

Докажем хотя бы второе из этих тождеств. Так как $B \cap C \subseteq B$, то

$$A \cup (B \cap C) \subseteq A \cup B;$$

аналогично

$$A \cup (B \cap C) \subseteq A \cup C,$$

и поэтому левая часть равенства (2) содержится в его правой части. С другой стороны, если элемент x содержится

в правой части равенства (2), то одновременно

$$x \in A \cup B, \quad x \in A \cup C. \tag{3}$$

Если $x \in A$, то x содержится в левой части равенства (2). Если же x к A не принадлежит, то из (3) следует, что x принадлежит и к B, и к C, т. е. содержится в пересечении $B \cap C$, а поэтому x снова содержится в левой части равенства (2). Вся правая часть равенства (2) входит, следовательно, в его левую часть. Равенство (2) доказано.

2. Читатель знаком, далее, с понятием *отображения, или соответствия, или однозначной функции.* Если φ — отображение множества A в множество B, т. е. на все B или на его подмножество, то будем употреблять символ φ: $A \to B$, а образ элемента $a \in A$ при отображении φ будем обозначать через $a\varphi$.

Если φ: $A \to B$, ψ: $B \to C$, то последовательное выполнение отображений φ и ψ приводит к вполне определенному отображению множества A в множество C, которое мы обозначим через $\varphi\psi$ и назовем *произведением* отображения φ на отображение ψ. Таким образом, для всех a из A

$$a(\varphi\psi) = (a\varphi)\psi. \tag{4}$$

Это умножение отображений можно назвать частичным: если даны два любых отображения, φ: $A \to B$ и ψ: $A' \to B'$, то произведение $\varphi\psi$ существует не всегда; оно существует тогда и только тогда, когда для всех $a \in A$ $a\varphi \in A'$. Отсюда следует, что *для отображений любого множества A в себя произведение всегда существует.*

Умножение отображений ассоциативно: если даны отображения

$$\varphi\colon A \to B, \quad \psi\colon B \to C, \quad \chi\colon C \to D, \tag{5}$$

то

$$(\varphi\psi)\chi = \varphi(\psi\chi). \tag{6}$$

Действительно, если a — произвольный элемент из A, то ввиду (4)

$$a[(\varphi\psi)\chi] = [a(\varphi\psi)]\chi = [(a\varphi)\psi]\chi = (a\varphi)(\psi\chi) = a[\varphi(\psi\chi)].$$

Ввиду равенства (6) результат последовательного выполнения отображений (5) можно записать через $\varphi\psi\chi$.

3. *Тождественное отображение* множества A в себя условимся обозначать через ε_A; таким образом,

$$a\varepsilon_A = a \text{ для всех } a \in A.$$

Тождественное отображение играет при умножении отображений роль единицы, так как для любых отображений $\varphi\colon A \to B$ и $\psi\colon C \to A$

$$\varepsilon_A \varphi = \varphi, \qquad \psi \varepsilon_A = \psi.$$

Читатель знаком с понятием *взаимно однозначного отображения* множества A на множество B (т. е. взаимно однозначного соответствия между этими множествами). Очевидно, что отображение $\varphi\colon A \to B$ тогда и только тогда будет взаимно однозначным отображением A на B, если для него существует обратное отображение, т. е. отображение $\varphi^{-1}\colon B \to A$, удовлетворяющее условиям

$$\varphi\varphi^{-1} = \varepsilon_A, \qquad \varphi^{-1}\varphi = \varepsilon_B.$$

Как известно, если существует взаимно однозначное отображение множества A на множество B, то множества A и B называются *равномощными* или, как говорят, они имеют одну и ту же *мощность*. При этом мощность конечного множества совпадает с числом его элементов, множества, равномощные с множеством всех натуральных чисел, называются *счетными*, а о множествах, равномощных с множеством всех действительных чисел, говорят, что они имеют *мощность континуума*.

4. При изучении бесконечных множеств весьма часто приходится использовать следующую аксиому выбора:

Если дано множество M, то существует функция φ, сопоставляющая каждому непустому подмножеству A из M один определенный элемент $\varphi(A)$ этого подмножества.

Иными словами, функция φ *отмечает* по одному элементу в каждом из непустых подмножеств множества M.

Вопрос о логических основах этой аксиомы и о законности ее использования принадлежит к числу самых трудных и спорных вопросов обоснования теории множеств. Мы не смогли бы, однако, обойтись без аксиомы выбора. Для счетных множеств она может быть, впрочем, легко доказана: если элементы множества M пронумерованы натуральными числами, то мы получим требуемую функцию, если в каждом

подмножестве A из M отметим тот его элемент, который имеет наименьший номер.

В I. 6.3 будут приведены некоторые утверждения, равносильные аксиоме выбора.

§ 2. Бинарные отношения

1. Если дано множество M, то его *квадратом* $M \times M$ называется множество всех упорядоченных пар (a, b), где $a, b \in M$. Пусть R — любое подмножество из $M \times M$. Оно следующим образом определяет в множестве M *бинарное отношение*, которое мы также будем обозначать символом R (в конкретных случаях для записи отношений используются различные специальные символы): если $a, b \in M$, то говорят, что элемент a находится в отношении R к элементу b, и записывают это через aRb в том и только в том случае, если пара (a, b) принадлежит к подмножеству R; таким образом, записи

$$aRb \text{ и } (a, b) \in R$$

равносильны.

Изучение бинарных отношений в множестве M не отличается, следовательно, от изучения подмножеств множества $M \times M$. Можно говорить, в частности, о *включении* бинарного отношения R в бинарное отношение R', $R \subseteq R'$, а также о *пересечении* и *объединении* бинарных отношений. *Дополнением* к бинарному отношению R является бинарное отношение $\bar{R}$, определяемое подмножеством $\bar{R} = (M \times M) \setminus R$; иными словами, $a\bar{R}b$ тогда и только тогда, если $(a, b) \notin R$.

2. С другой стороны, то обстоятельство, что бинарные отношения задаются множествами упорядоченных пар элементов из M, делает алгебру бинарных отношений более богатой, чем простая алгебра подмножеств произвольного множества. Так, пусть в множестве M заданы произвольные бинарные отношения R и S. Назовем их *произведением* RS бинарное отношение, определяемое следующим образом: $a(RS)b$ тогда и только тогда, когда в M существует хотя бы один такой элемент c, что aRc и cSb.

Умножение бинарных отношений ассоциативно,

$$(RS)T = R(ST),$$

так как элемент a тогда и только тогда находится в каждом из отношений $(RS)T$ и $R(ST)$ к элементу b, если сущест-

вуют такие элементы c и d, что

$$aRc,\ cSd,\ dTb.$$

Умножение бинарных отношений не является, однако, коммутативным; бинарные отношения R и S лишь иногда будут *перестановочными*,

$$RS = SR.$$

Если в множестве M даны бинарные отношения R_i (i пробегает множество индексов I) и S, то

$$\left(\bigcup_{i\in I} R_i\right) S = \bigcup_{i\in I} R_i S,\quad S\left(\bigcup_{i\in I} R_i\right) = \bigcup_{i\in I} SR_i. \tag{1}$$

Действительно, $a\left[\left(\bigcup_{i\in I} R_i\right) S\right] b$ равносильно существованию такого элемента c, что $a\left(\bigcup_{i\in I} R_i\right) c$ и cSb. Это равносильно, однако, существованию такого индекса i_0, что $aR_{i_0}c$ и cSb, т. е. $a(R_{i_0}S)b$, и поэтому $a\left(\bigcup_{i\in I} R_iS\right) b$.

Заметим, что в равенствах (1) объединения нельзя заменить пересечениями.

Из (1) следует, что *если даны бинарные отношения R, R' и S, причем $R \subseteq R'$, то*

$$RS \subseteq R'S,\quad SR \subseteq SR'. \tag{2}$$

Действительно, включение $R \subseteq R'$ равносильно равенству $R \cup R' = R'$, из которого вытекает равенство

$$(R \cup R')S = RS \cup R'S = R'S,$$

равносильное включению $RS \subseteq R'S$.

3. Для всякого бинарного отношения R в множестве M существует *обратное отношение* R^{-1}, определяемое следующим образом: $aR^{-1}b$ тогда и только тогда, когда bRa. Ясно, что

$$(R^{-1})^{-1} = R$$

и что из $R \subseteq S$ следует $R^{-1} \subseteq S^{-1}$.

Если в множестве M даны бинарные отношения R_i, $i\in I$, S и T, то

$$\left(\bigcap_{i\in I} R_i\right)^{-1} = \bigcap_{i\in I} R_i^{-1}, \tag{3}$$

$$\left(\bigcup_{i\in I} R_i\right)^{-1} = \bigcup_{i\in I} R_i^{-1}, \tag{4}$$

$$(ST)^{-1} = T^{-1}S^{-1}. \tag{5}$$

Действительно, $a\left(\bigcap_{i\in I} R_i\right)^{-1} b$ означает, что $b\left(\bigcap_{i\in I} R_i\right) a$, т. е. bR_ia для всех $i\in I$, откуда $aR_i^{-1}b$ для всех $i\in I$, и поэтому $a\left(\bigcap_{i\in I} R_i^{-1}\right) b$. Аналогично доказывается и равенство (4). Наконец, $a(ST)^{-1}b$ означает, что $b(ST)a$, т. е. существует такой элемент c, что bSc и cTa, а поэтому $aT^{-1}c$ и $cS^{-1}b$, откуда $a(T^{-1}S^{-1})b$.

4. *Единичное отношение* E определяется следующим образом: aEb тогда и только тогда, если $a=b$; иными словами, отношение E задается множеством всех пар вида (a, a), $a\in M$. Очевидно, что $E^{-1}=E$ и что для любого бинарного отношения R

$$RE = ER = R.$$

Отметим также *пустое отношение* O, определяемое пустым подмножеством множества $M\times M$. Ясно, что для любого бинарного отношения R в множестве M

$$O\subseteq R \text{ и } RO = OR = O.$$

5. В ближайших параграфах мы встретимся с такими бинарными отношениями R, заданными в множестве M, которые обладают некоторыми из следующих четырех свойств:

Рефлексивность: aRa для всех $a\in M$; иными словами, $E\subseteq R$.

Транзитивность: если aRb и bRc, то aRc; иными словами, $RR\subseteq R$.

Симметричность: если aRb, то bRa; иными словами, $R^{-1}=R$.

Антисимметричность: если aRb и bRa, то $a=b$; иными словами, $R\cap R^{-1}\subseteq E$.

Если бинарное отношение R обладает любым из указанных четырех свойств, то обратное отношение R^{-1} обладает этим же свойством.

В самом деле, если $E \subseteq R$, то

$$E = E^{-1} \subseteq R^{-1}.$$

Если $RR \subseteq R$, то

$$R^{-1}R^{-1} = (RR)^{-1} \subseteq R^{-1}.$$

Если $R^{-1} = R$, то

$$(R^{-1})^{-1} = R = R^{-1}.$$

Наконец, если $R \cap R^{-1} \subseteq E$, то

$$R^{-1} \cap (R^{-1})^{-1} = R^{-1} \cap R \subseteq E.$$

6. Пусть в множестве M выбрано подмножество N. Бинарное отношение R, заданное в M, естественным образом *индуцирует* бинарное отношение R^N в множестве N: если $a, b \in N$, то aR^Nb тогда и только тогда, когда в M справедливо aRb. Иными словами, учитывая, что $N \times N$ является подмножеством множества $M \times M$,

$$R^N = R \cap (N \times N).$$

Легко проверяются следующие равенства:

$$(R^N)^{-1} = (R^{-1})^N, \quad \left(\bigcap_{i \in I} R_i\right)^N = \bigcap_{i \in I} R_i^N, \quad \left(\bigcup_{i \in I} R_i\right)^N = \bigcup_{i \in I} R_i^N.$$

7. Понятие бинарного отношения допускает различные обобщения. Так, рассмотрим *n-ю степень* M^n множества M, т. е. множество всех упорядоченных систем $(a_1, a_2, \ldots, a_n)$ из n элементов множества M. Тогда любое подмножество R множества M^n определяет в множестве M *n-арное отношение* (при $n = 3$ — *тернарное отношение*). Множества, в которых задано некоторое число таких отношений, называются *моделями* и являются предметом самостоятельной теории.

§ 3. Отношения эквивалентности

1. Важным типом бинарных отношений являются *отношения эквивалентности*, т. е. бинарные отношения, обладающие свойствами рефлексивности, транзитивности и симметричности (см. I.2.5). Из многочисленных

известных читателю конкретных примеров таких отношений напомним хотя бы равенство дробей и сравнимость целых чисел по некоторому модулю. Для записи отношений эквивалентности чаще всего используются символы $\sim$ и $\equiv$.

2. Отношения эквивалентности, определенные на множестве M, весьма тесно связаны с *разбиениями множества M на непересекающиеся классы.* Под разбиением следует понимать такой выбор в множестве M системы непустых подмножеств (классов этого разбиения), что всякий элемент из M принадлежит к одному и только одному из этих подмножеств.

Всякое разбиение π множества M определяет в M отношение эквивалентности.

Действительно, если $a, b \in M$ и если мы положим $a \sim b$ в том и только в том случае, когда a и b принадлежат к одному классу разбиения π, то получим в M бинарное отношение, удовлетворяющее, очевидно, всем требованиям определения отношения эквивалентности.

Обратно, *всякое отношение эквивалентности R, заданное в множестве M, определяет разбиение этого множества.*

В самом деле, назовем классом элемента a и обозначим через K_a множество всех тех элементов x из M, для которых aRx. Из рефлексивности отношения R вытекает включение $a \in K_a$, т. е. система классов K_a, $a \in M$, покрывает все множество M. Далее, симметричность отношения R показывает, что из $b \in K_a$ следует $a \in K_b$, транзитивность же отношения R приводит к тому, что если $b \in K_a$, то из $c \in K_b$ следует $c \in K_a$, т. е. $K_b \subseteq K_a$. Эти последние замечания приводят вместе к тому, что если $b \in K_a$, то $K_b = K_a$, т. е. класс определяется любым своим элементом. Если, наконец, K_a и K_b — два произвольных класса с непустым пересечением, содержащим, например, элемент c, то $K_a = K_c$ и $K_b = K_c$, т. е. классы K_a и K_b совпадают. Мы доказали, что система всех различных классов вида K_a является разбиением множества M.

Очевидно, что переход от разбиения π множества M к определяемому им отношению эквивалентности, а затем к определяемому последним разбиению множества M приводит снова к разбиению π. *Между отношениями эквивалентности в множестве M и разбиениями множества M на непересекающиеся классы установлено, следовательно, взаимно однозначное соответствие.*

3. *Если в множестве M заданы отношения эквивалентности R_i, $i \in I$, то их пересечение также будет отношением эквивалентности.*

В самом деле, из aR_ia для всех $i \in I$ следует $a\left(\bigcap_{i\in I} R_i\right)a$. Далее, если $a\left(\bigcap_{i\in I} R_i\right)b$ и $b\left(\bigcap_{i\in I} R_i\right)c$, то aR_ib и bR_ic для всех $i \in I$, откуда aR_ic для всех $i \in I$, а поэтому $a\left(\bigcap_{i\in I} R_i\right)c$. Наконец, если $a\left(\bigcap_{i\in I} R_i\right)b$, то aR_ib для всех $i \in I$, т. е. bR_ia для всех $i \in I$, откуда $b\left(\bigcap_{i\in I} R_i\right)a$.

Без труда проверяется, что если отношениям эквивалентности R_i, $i \in I$, соответствуют разбиения π_i множества M, $i \in I$, то отношению эквивалентности $\bigcap_{i\in I} R_i$ соответствует разбиение, классами которого служат все непустые пересечения классов, взятых по одному в каждом из разбиений π_i, $i \in I$. Это разбиение мы назовем *пересечением разбиений* π_i, $i \in I$.

Если в множестве M заданы отношения эквивалентности R_i, $i \in I$, то их объединение, понимаемое в смысле объединения бинарных отношений, уже не будет, вообще говоря, отношением эквивалентности. *В множестве M существует, однако, такое отношение эквивалентности, которое включает в себя все отношения R_i, $i \in I$* (в смысле включения бинарных отношений), *но само включается в любое другое отношение эквивалентности, включающее в себя все R_i, $i \in I$.* Это отношение эквивалентности может быть названо *объединением* отношений эквивалентности R_i, $i \in I$.

Для доказательства определим в множестве M бинарное отношение S следующим образом: aSb тогда и только тогда, когда в M можно хотя бы одним способом выбрать такую конечную систему элементов

$$a = c_0,\ c_1,\ c_2,\ \ldots,\ c_{n-1},\ c_n = b, \tag{1}$$

что для $k = 1, 2, \ldots, n$ существует хотя бы один такой индекс $i_k \in I$, для которого $c_{k-1}R_{i_k}c_k$. Отношение S является, очевидно, рефлексивным, транзитивным и симметричным. Если же T — любое отношение эквивалентности, включающее в себя

все R_i, $i \in I$, и если aSb, причем этим элементам соответствует система элементов (1), то из $c_{k-1}R_{i_k}c_k$ следует $c_{k-1}Tc_k$, $k = 1, 2, \ldots, n$, а поэтому ввиду транзитивности отношения T имеет место aTb.

* Произведение RS двух отношений эквивалентности R и S тогда и только тогда является отношением эквивалентности, если отношения R и S перестановочны, $RS = SR$. Если это имеет место, то объединение отношений эквивалентности R и S совпадает с их произведением как бинарных отношений [Шик, Spisy vyd. přírodověde fakult. Masarykovy univ. (1954), № 3, 97—102]. *

4. Множество классов разбиения, соответствующего данному отношению эквивалентности R в множестве M, мы будем обозначать через M/R и называть *фактор-множеством* множества M по отношению эквивалентности R. Отображение множества M на фактор-множество M/R, сопоставляющее всякому элементу $a \in M$ тот класс разбиения, соответствующего R, в котором лежит элемент a, называется *естественным отображением* M на M/R.

Между отношениями эквивалентности, имеющимися в множестве M, и отображениями этого множества на некоторые другие множества существует тесная связь, являющаяся прототипом так называемых «теорем о гомоморфизмах», с которыми мы неоднократно будем встречаться в следующих главах книги. Именно, если дано отображение φ множества M на некоторое множество N, то ему соответствует вполне определенное отношение эквивалентности R в множестве M (т. е. разбиение этого множества): для элементов a, $b \in M$ полагаем aRb в том и только в том случае, если $a\varphi = b\varphi$. Сопоставляя каждому элементу x из N класс тех элементов из M, которые имеют x своим образом при отображении φ, *мы получаем взаимно однозначное отображение* ξ *множества* N *на множество* M/R, *причем произведение* $\varphi\xi$ *совпадает с естественным отображением* M *на* M/R.

§ 4. Частичная упорядоченность

1. Другим очень важным типом бинарных отношений являются *отношения частичной упорядоченности,* т. е. бинарные отношения, обладающие свойствами рефлексивности, транзитивности и антисимметричности.

Множество M с заданной в нем частичной упорядоченностью называется *частично упорядоченным*. Для записи частичной упорядоченности будет употребляться символ $\leqslant$; если $a, b \in M$ и $a \leqslant b$, то, в зависимости от обстоятельств, будем говорить, что *a меньше или равно b, a содержится в b, a предшествует b.*

Если $a \leqslant b$ и $a \neq b$, то будем писать $a < b$ и говорить, что *a меньше b, a строго содержится* в b и т. д. Бинарное отношение $<$ уже не будет, конечно, рефлексивным. Через $\geqslant$ и $>$ будут записываться отношения, обратные к отношениям $\leqslant$ и $<$, т. е., например, $a \geqslant b$ (*a больше или равно b, a содержит b, a следует за b*) тогда и только тогда, когда $b \leqslant a$.

Пусть в множестве M задана частичная упорядоченность. Элементы a и b этого множества будут называться *сравнимыми*, если $a \leqslant b$ или $b \leqslant a$. Далеко не всякие два элемента из M обязаны быть сравнимыми — именно по этой причине мы говорим о «частичной» упорядоченности. Так, мы получим *тривиальную* частичную упорядоченность множества M, если положим, что $a \leqslant b$ лишь при $a = b$; различные элементы из M будут в этом случае несравнимыми. Частично упорядоченное множество, в котором любые два элемента сравнимы, называется *упорядоченным множеством* или *линейно упорядоченным множеством*, или *цепью*.

2. В различных разделах математики упорядоченные и частично упорядоченные множества встречаются чрезвычайно часто. В качестве первых примеров упорядоченных множеств можно указать множество натуральных чисел и множество точек прямой линии (т. е. множество всех действительных чисел), оба в их естественной упорядоченности. Примерами частично (но не линейно) упорядоченных множеств служат:

множество $\tilde{N}$ всех подмножеств некоторого данного множества N с отношением теоретико-множественного включения $\subseteq$ в качестве отношения частичной упорядоченности;

множество всех непрерывных действительных функций, определенных на отрезке $[0, 1]$, если $f \leqslant g$ означает, что для всех x из этого отрезка $f(x) \leqslant g(x)$;

множество всех натуральных чисел, если $a \leqslant b$ понимать в том смысле, что b делится нацело на a.

* Всякая частичная упорядоченность данного множества M может быть продолжена до линейной упорядоченности этого множества, т. е. может быть включена в линейную упорядоченность (в смысле включения бинарных отношений, см. I.2.1) [Шпильрайн, Fund. Math. **16** (1930), 386—389]. *

3. Пусть между частично упорядоченными множествами M и M' установлено взаимно однозначное соответствие φ,

$$a\varphi = a', \quad a \in M, \quad a' \in M'.$$

Если из $a \leqslant b$, где $a, b \in M$, всегда следует $a\varphi \leqslant b\varphi$ и обратно, то φ называется *изоморфизмом* между M и M', а сами множества M и M' — *изоморфными* частично упорядоченными множествами. Очевидно, что в тех случаях, когда частичная упорядоченность является самостоятельным объектом изучения, а природа элементов, из которых составлены рассматриваемые множества, не играет роли, изомофные множества можно считать тождественными.

4. Мы знаем (см. I.2.6), что частичная упорядоченность, заданная в множестве M, индуцирует во всяком подмножестве этого множества некоторое бинарное отношение; легко видеть, что оно также будет частичной упорядоченностью. Будем говорить, что частично упорядоченное множество M *изоморфно вкладывается* в частично упорядоченное множество N, если существует изоморфное отображение множества M на некоторое подмножество N' множества N, причем N' рассматривается с частичной упорядоченностью, индуцированной в нем частичной упорядоченностью множества N.

5. Следующая теорема подчеркивает особую роль первого из указанных в I.4.2 примеров частично упорядоченного множества.

Всякое частично упорядоченное множество M изоморфно вкладывается в множество $\tilde{N}$ всех подмножеств некоторого множества N, частично упорядоченное по включению. В качестве множества N можно взять, например, само M.

В самом деле, поставим в соответствие каждому элементу a из M подмножество A, составленное из всех таких элементов $x \in M$, что $x \leqslant a$. Пусть $a, b \in M$, а A, B — соответствующие им подмножества. Если $A = B$, то $b \leqslant a$,

$a \leqslant b$, откуда $a = b$. Этим доказано, что соответствие $a \to A$ является взаимно однозначным отображением множества M в множество $\tilde{M}$ всех его подмножеств. Если, далее, $a \leqslant b$, то из $x \leqslant a$ будет следовать $x \leqslant b$, т. е. $A \subseteq B$. Обратно, если $A \subseteq B$, то $a \in B$, т. е. $a \leqslant b$. Таким образом, соответствие $a \to A$ является изоморфным вложением M в $\tilde{M}$.

6. Как вытекает из доказанного в I.2.5, *отношение, обратное к отношению частичной упорядоченности, само будет частичной упорядоченностью.*

Частично упорядоченные множества M и M' называются *инверсно изоморфными*, если одно из них изоморфно другому, взятому с обратной частичной упорядоченностью, т. е. если между ними существует такое взаимно однозначное соответствие φ,

$$a\varphi = a', \quad a \in M, \quad a' \in M',$$

что $a \leqslant b$, где $a, b \in M$, тогда и только тогда, когда $a\varphi \geqslant b\varphi$.

§ 5. Условие минимальности

1. Элемент a частично упорядоченного множества M называется *минимальным элементом* этого множества, если в M нет ни одного элемента x, удовлетворяющего условию $x < a$. Ясно, что M может содержать много различных минимальных элементов, но может также не иметь ни одного такого элемента.

Так, множество $\tilde{N}$ всех подмножеств некоторого множества N обладает единственным минимальным элементом — это будет пустое подмножество. В множестве всех непустых подмножеств множества N минимальными элементами являются все подмножества, состоящие из одного элемента. Наконец, если множество N бесконечное, то множество всех его бесконечных подмножеств вообще не имеет минимальных элементов.

Понятие минимального элемента будет сейчас использовано в определении одного специального класса частично упорядоченных множеств, более широкого, чем класс конечных частично упорядоченных множеств. Это будет класс

частично упорядоченных множеств, удовлетворяющих следующим *условиям, между собою эквивалентным:*

Условие минимальности. *Всякое непустое подмножество N частично упорядоченного множества M обладает хотя бы одним минимальным (в N) элементом.*

Условие обрыва убывающих цепей [1]). *Всякая строго убывающая цепь элементов частичо упорядоченного множества M,*

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

обрывается на конечном месте. Иными словами, для всякой убывающей цепи элементов

$$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n \geqslant \ldots$$

существует такой индекс n, на котором эта цепь стабилизуется, т. е.

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

Условие индуктивности. *Все элементы частично упорядоченного множества M обладают некоторым свойством $\mathfrak{E}$, если этим свойством обладают все минимальные элементы этого множества (в случае, когда они существуют) и если из справедливости свойства $\mathfrak{E}$ для всех элементов, строго предшествующих некоторому элементу a, может быть выведена справедливость этого свойства для самого элемента a.*

2. Докажем эквивалентность указанных трех условий.

Из условия минимальности вытекает условие индуктивности.

В самом деле, пусть частично упорядоченное множество M удовлетворяет условию минимальности и пусть в нем для некоторого свойства $\mathfrak{E}$ выполняются посылки условия индуктивности. Если тем не менее в M существуют элементы, которые не обладают свойством $\mathfrak{E}$, то пусть a будет одним из минимальных среди таких элементов — существование элемента a вытекает из условия минимальности. Элемент a не может быть минимальным во всем M, что следует из

---

[1]) Понятие убывающей цепи, о котором идет речь в этом условии, является частным случаем общего понятия цепи, введенного в I.4.1.

первой посылки условия индуктивности, а так как все элементы, строго предшествующие a, свойством $\mathfrak{E}$ уже обладают, то, по второй посылке условия индуктивности, и сам элемент a должен обладать свойством $\mathfrak{E}$, т. е. мы приходим к противоречию.

Из условия индуктивности вытекает условие обрыва убывающих цепей.

Пусть, в самом деле, частично упорядоченное множество M удовлетворяет условию индуктивности. Применим это условие к следующему свойству: элемент a обладает свойством $\mathfrak{E}$, если всякая строго убывающая цепь элементов, начинающаяся от элемента a, обрывается на конечном месте. Этим свойством обладают, очевидно, все минимальные элементы множества M, если они существуют. С другой стороны, пусть все элементы, строго предшествующие элементу a, обладают нашим свойством $\mathfrak{E}$. В этом случае второй член любой строго убывающей цепи, начинающейся от элемента a, будет обладать свойством $\mathfrak{E}$, а поэтому рассматриваемая цепь должна обрываться, т. е. элемент a также обладает свойством $\mathfrak{E}$. Из условия индуктивности теперь следует, что нашим свойством $\mathfrak{E}$ обладают вообще все элементы множества M, т. е. в M обрывается всякая строго убывающая цепь — она начинается, понятно, с некоторого элемента.

Из условия обрыва убывающих цепей вытекает условие минимальности.

Для доказательства предположим, что частично упорядоченное множество M условию минимальности не удовлетворяет, а именно пусть его непустое подмножество N не имеет минимальных элементов. Пользуясь аксиомой выбора (см. I.1.4), отметим по одному элементу в каждом непустом подмножестве из N, а затем следующим образом построим последовательность элементов

$$a_n, \qquad n = 1, 2, \ldots \tag{1}$$

В качестве a_1 возьмем элемент, отмеченный в самом подмножестве N. Если элемент a_n уже построен и $a_n \in N$, то в качестве a_{n+1} берем элемент, отмеченный в непустом (так как N не имеет минимальных элементов) множестве элементов из N, строго предшествующих a_n. Последовательность (1) является, очевидно, бесконечной строго убывающей цепью, т. е. множество M не может удовлетворять условию обрыва убывающих цепей.

3. Условие индуктивности позволяет проводить не только доказательства по индукции, но и *построения по индукции.* Именно, пусть M — частично упорядоченное множество с условием минимальности и пусть мы хотим определить на этом множестве функцию $\varphi(x)$, относящую всякому элементу x из M некоторый элемент вспомогательного множества S. Будем считать при этом, что функция $\varphi(x)$ должна удовлетворять некоторым *рекуррентным соотношениям,* т. е. соотношениям, однозначно определяющим для всякого $a \in M$ значение $\varphi(a)$ по значениям $\varphi(b)$ для всех b, строго меньших a. Докажем, что *существует, и притом единственная, функция* $\varphi(x)$, *определенная на всем множестве* M, *удовлетворяющая указанным рекуррентным соотношениям и принимающая произвольные заданные значения на всех минимальных элементах множества* M.

Начнем с доказательства единственности. Пусть на M существуют две различные функции, $\varphi(x)$ и $\psi(x)$, удовлетворяющие нашим условиям. В непустом множестве тех элементов x, для которых $\varphi(x) \neq \psi(x)$, существует, ввиду условия минимальности, хотя бы один минимальный элемент a. Этот элемент не может быть минимальным во всем M, так как на минимальных элементах множества M функции $\varphi(x)$ и $\psi(x)$ по условию совпадают. Существуют, следовательно, такие элементы b, что $b < a$, причем для всех этих элементов $\varphi(b) = \psi(b)$. Рекуррентные соотношения однозначно определяют, однако, значения рассматриваемых функций для $x = a$ по их значениям для всех $b < a$, а поэтому $\varphi(a) = \psi(a)$, т. е. мы пришли к противоречию.

Переходим к доказательству существования искомой функции $\varphi(x)$, предполагая, что на минимальных элементах ее значения уже заданы. Будем говорить, что элемент $a \in M$ обладает свойством $\mathfrak{E}$, если на множестве A всех таких x, что $x \leqslant a$, может быть определена функция $\varphi_a(x)$, удовлетворяющая заданным рекуррентным соотношениям и принимающая заданные значения на минимальных элементах из M, содержащихся в a.

Все минимальные элементы из M обладают, очевидно, свойством $\mathfrak{E}$. С другой стороны, если a и b обладают свойством $\mathfrak{E}$ и $b < a$, то, применяя доказанную выше единственность искомой функции вместо M к множеству B тех x, для которых $x \leqslant b$, мы получим, что для всех этих x

$$\varphi_b(x) = \varphi_a(x).$$

Отсюда следует, что если все элементы b, строго предшествующие данному элементу a, обладают свойством $\mathfrak{E}$, то этим свойством обладает и сам элемент a: мы получим функцию $\varphi_a(x)$, удовлетворяющую всем требованиям, если для всякого b, $b < a$, положим

$$\varphi_a(b) = \varphi_b(b),$$

а в качестве $\varphi_a(a)$ возьмем то значение, которое однозначно определяется рекуррентными соотношениями.

На основании условия индуктивности, выполняющегося в множестве M, можно теперь утверждать, что все элементы этого множества обладают свойством $\mathfrak{E}$. Полагая, наконец, для всех $a \in M$

$$\varphi(a) = \varphi_a(a),$$

мы определим функцию $\varphi(x)$, обладающую всеми нужными свойствами, и этим закончим доказательство теоремы.

4. Линейно упорядоченное множество, удовлетворяющее условию минимальности, а поэтому и двум другим условиям, с ним эквивалентным, называется *вполне упорядоченным*. Примером вполне упорядоченного множества служит множество натуральных чисел в его естественной упорядоченности. Всякое подмножество вполне упорядоченного множества само вполне упорядочено. Из определения вполне упорядоченного множества следует, что оно обладает единственным минимальным элементом.

Во вполне упорядоченном множестве для всякого элемента a существует элемент, непосредственно следующий за a (за единственным возможным исключением, если a является максимальным (см. I.5.5) элементом). Элемент a может не иметь, однако, непосредственно предшествующего элемента; в этом случае он называется *предельным элементом*.

Частично упорядоченное множество тогда и только тогда удовлетворяет условию минимальности, если все его цепи (т. е. линейно упорядоченные подмножества) вполне упорядочены.

Действительно, если частично упорядоченное множество M удовлетворяет условию минимальности, то это же верно для всех его подмножеств, в частности для всех цепей. Обратное утверждение вытекает из того, что в формулировке условия

обрыва убывающих цепей, эквивалентного условию минимальности, используются лишь цепи множества M.

5. В частично упорядоченном множестве M можно перейти к обратной частичной упорядоченности. Минимальные элементы этой обратной упорядоченности называются *максимальными элементами* множества M в его исходной упорядоченности, а убывающие цепи в обратной упорядоченности называются *возрастающими цепями* множества M. Вообще, этим путем для всякого понятия (или утверждения), связанного с частичной упорядоченностью, можно получить двойственное понятие (утверждение).

Пусть частично упорядоченное множество M удовлетворяет условию минимальности. Беря в M обратную частичную упорядоченность, мы получим частично упорядоченное множество, удовлетворяющее *условию максимальности*. Для множеств с условием максимальности остается справедливым, после замены отношения $\leqslant$ на отношение $\geqslant$ и обратно, все, сказанное выше о множествах с условием минимальности.

§ 6. Теоремы, равносильные аксиоме выбора

1. Пусть N — подмножество частично упорядоченного множества M. Всякий элемент a из M (не обязательно содержащийся в N), удовлетворяющий условию $a \geqslant x$ для всех $x \in N$, называется *верхней гранью* подмножества N в множестве M. Двойственным является понятие *нижней грани*.

2. С другой стороны, если M — частично упорядоченное множество, то множество всех его цепей само будет частично упорядоченным при помощи теоретико-множественного включения. Максимальные элементы этого последнего множества, если они существуют, естественно называть *максимальными цепями* множества M.

3. Эти понятия используются в формулировке двух из следующих трех теорем, *каждая из которых*, как будет сейчас доказано, *эквивалентна аксиоме выбора* (см. I.1.4).

Теорема Цермело. *Всякое множество можно вполне упорядочить.*

Теорема Хаусдорфа. *Всякая цепь частично упорядоченного множества содержится в некоторой максимальной цепи.*

Теорема Куратовского — Цорна. *Если всякая цепь частично упорядоченного множества M обладает верхней гранью, то всякий элемент множества M меньше (или равен) некоторого максимального элемента.*

4. Докажем эквивалентность этих теорем и аксиомы выбора. *Из аксиомы выбора следует теорема Цермело.*

Будем называть *отрезком* некоторого вполне упорядоченного множества A всякое его подмножество B, содержащее вместе с любым своим элементом b все такие $x \in A$, что $x \leqslant b$. Множество элементов, строго предшествующих некоторому элементу a из A, будет истинным отрезком множества A (т. е. отрезком, отличным от самого A), и этим исчерпываются все истинные отрезки: если B — такой отрезок, то B состоит из всех элементов, строго предшествующих минимальному элементу дополнения $A \setminus B$, т. е. *определяется* этим элементом. Пустое подмножество мы также будем считать истинным отрезком множества A; он определяется минимальным элементом этого множества.

Перейдем к доказательству теоремы. Пусть дано произвольное множество M. На основании аксиомы выбора отметим в каждом его непустом подмножестве N по одному элементу $\varphi(N)$. Будем называть непустое подмножество A из M *отмеченным*, если оно может быть вполне упорядочено, причем так, что для всякого $a \in A$

$$a = \varphi(M \setminus A'),$$

где A' — отрезок множества A в указанной полной упорядоченности, определяемый элементом a. Отмеченные подмножества в M существуют; таково, например, подмножество, состоящее из одного элемента $\varphi(M)$.

Пусть A и B — два отмеченных подмножества, для которых выбраны полные упорядоченности, обладающие свойством, указанным в предыдущем абзаце. Тогда оба эти подмножества имеют $\varphi(M)$ в качестве первого элемента и поэтому обладают непустыми совпадающими отрезками. Объединение C всех совпадающих отрезков этих двух подмножеств будет, очевидно, отрезком в каждом из них; это наибольший среди совпадающих отрезков. Если бы отрезок C был отличен и от A, и от B, то, по определению отмеченного подмножества, отрезок C определялся бы и в A, и в B элементом $\varphi(M \setminus C)$,

а тогда A и B обладали бы бо́льшим, чем C, совпадающим отрезком, состоящим из C и элемента $\varphi(M \setminus C)$. Это противоречие с определением C показывает, что одно из двух отмеченных подмножеств A и B является отрезком другого.

Отсюда следует, что объединение L всех отмеченных подмножеств из M само будет отмеченным. Действительно, если a и b из L принадлежат соответственно к отмеченным подмножествам A и B, то они оба лежат в большем из этих подмножеств, например в A. Полагая $a \geqslant b$ в L, если $a \geqslant b$ в этом A, мы получим в L линейную упорядоченность, которая будет даже полной упорядоченностью: всякая убывающая цепочка элементов в L целиком содержится в некотором отмеченном подмножестве A и поэтому должна обрываться. Наконец, если $a \in L$, то a содержится в некотором отмеченном подмножестве A и определяет в L и в A один и тот же отрезок A', причем $a = \varphi(M \setminus A')$. Этим доказана отмеченность множества L.

Для окончания доказательства теоремы остается указать, что если бы L было отлично от M, то, в противоречие с определением L, мы получили бы большее, чем L, отмеченное подмножество, присоединяя к L элемент $\varphi(M \setminus L)$ и считая этот элемент следующим за всеми элементами из L.

Из теоремы Цермело следует теорема Хаусдорфа.

Пусть в частично упорядоченном множестве M взята произвольная цепь A. Если $A = M$, то доказывать нечего, в противном же случае будем считать, на основании теоремы Цермело, множество $B = M \setminus A$ вполне упорядоченным; эта полная упорядоченность никак не связана с частичной упорядоченностью B как подмножества множества M.

Отнесем первый элемент множества B к *первому классу*, если он в множестве M сравним (см. I.4.1) с каждым элементом из A, и ко *второму классу* в противоположном случае. Пусть теперь b — произвольный элемент из B и пусть каждый из элементов множества B, строго предшествующих элементу b в смысле заданной в B полной упорядоченности, уже отнесен к первому или ко второму классу. Тогда мы отнесем элемент b к первому классу, если он в M сравним как с каждым элементом из A, так и с каждым из тех элементов, ему предшествующих в B, которые отнесены к первому классу; в противоположном же случае элемент b будет отнесен ко второму классу.

Мы проводим, таким образом, индуктивное построение по вполне упорядоченному множеству B, и поэтому можно считать (см. 1.5.3), что всякий элемент из B однозначным образом отнесен к первому или второму классу. Множество C, содержащее все элементы цепи A и все элементы первого класса из B, будет в множестве M цепью, так как любые два элемента из C сравнимы в M между собой. Эта цепь будет в M максимальной, так как всякий элемент второго класса из B несравним хотя бы с одним элементом из C. Теорема доказана.

Из теоремы Хаусдорфа следует теорема Куратовского — Цорна.

В самом деле, пусть дано такое частично упорядоченное множество M, в котором всякая цепь обладает верхней гранью, и пусть $a \in M$. Цепь, состоящая из одного элемента a, по теореме Хаусдорфа содержится в некоторой максимальной цепи C. Если элемент c — верхняя грань цепи C, то $a \leqslant c$. С другой стороны, элемент c максимален в M: если существует такой элемент b, что $c < b$, то для всех $x \in C$ ввиду $x \leqslant c$ будет $x < b$, т. е., присоединяя к цепи C элемент b, мы получим бо́льшую цепь в противоречие с максимальностью цепи C. Теорема доказана.

Из теоремы Куратовского — Цорна следует аксиома выбора.

Пусть дано произвольное множество M. Рассмотрим такие системы непустых подмножеств из M, на которых возможно задание (хотя бы одним способом) функции, отмечающей в каждом подмножестве A данной системы один из его элементов $\varphi(A)$. Системы такого рода существуют — таковы, например, системы, состоящие из одного непустого множества. Обозначим через Φ множество всех функций указанного вида, заданных на всевозможных системах подмножеств, на которых задание таких функций возможно.

Пусть φ и ψ — две функции, принадлежащие к Φ и заданные соответственно на системах подмножеств S и T. Положим $\varphi \leqslant \psi$, если $S \subseteq T$ и на системе S функции φ и ψ совпадают. Этим в множестве Φ определяется частичная упорядоченность. Возьмем в Φ произвольную цепь Γ (в смысле этой частичной упорядоченности), состоящую из функций φ_α, заданных соответственно на системах S_α. На системе $T = \bigcup\limits_\alpha S_\alpha$

может быть определена функция ψ, совпадающая на каждой системе S_α с функцией φ_α. Ясно, что ψ принадлежит к Φ и служит верхней гранью для цепи Γ.

К множеству Φ применима, следовательно, теорема Куратовского — Цорна, а поэтому Φ обладает максимальными элементами. Пусть χ будет один из этих элементов. Если бы система U, на которой определена функция χ, не содержала непустого подмножества A из M, то на системе, полученной из U присоединением A, можно было бы определить функции, строго бо́льшие, чем χ: это была бы всякая функция, совпадающая с χ на системе U и отмечающая в подмножестве A один из его элементов. Полученное противоречие с максимальностью функции χ показывает, что система U совпадает на самом деле с системой всех непустых подмножеств множества M. Теорема доказана.

* Утверждение, что всякое множество может быть линейно упорядочено, является более слабым, чем аксиома выбора [Мостовский, Fund. Math. **32** (1939), 201 — 252]. *

ГЛАВА ВТОРАЯ

ГРУППЫ И КОЛЬЦА

§ 1. Группоиды, полугруппы, группы

1. В основе всех понятий, изучаемых в различных отделах алгебры, лежит понятие *алгебраической операции*. Ограничимся пока рассмотрением *бинарных* операций. В самом широком понимании это будет закон, по которому некоторым упорядоченным парам элементов данного множества M (т. е. некоторым элементам из квадрата множества M, см. I.2.1) ставятся в соответствие элементы из M, один или много. Если мы назовем эту операцию *умножением* и будем употреблять для нее обычную мультипликативную запись, то равенство

$$ab = c \tag{1}$$

будет иметь тот смысл, что для пары элементов a, b из M произведение определено и что одним из значений этого произведения служит элемент c.

Понятие бинарной алгебраической операции, рассматриваемое в этом широком смысле, равносильно понятию заданного в множестве M тернарного отношения (см. I.2.7).

Действительно, если в M задана бинарная операция, то мы введем в M тернарное отношение R, полагая, что $R(a, b, c)$ тогда и только тогда, когда имеет место равенство (1). Обратно, если в M задано тернарное отношение R, то будем считать, что равенство (1) имеет место тогда и только тогда, когда справедливо $R(a, b, c)$.

2. В дальнейшем *бинарная алгебраическая операция* будет пониматься, как правило, в более узком смысле:

произведение должно быть определено для любой упорядоченной пары элементов и должно быть однозначным. Всякое непустое множество, в котором задана алгебраическая операция этого типа, называется *группоидом*.

Это понятие все еще слишком широко. Более узким будет имеющее разнообразные применения понятие *полугруппы*, т. е. группоида, в котором выполняется *закон ассоциативности*: для любых элементов a, b и c

$$(ab)\,c = a\,(bc). \tag{2}$$

Равенство (2) придает однозначный смысл произведению abc любых трех элементов полугруппы. Отсюда легко следует, что при всех n произведение $a_1a_2 \ldots a_n$ любых n элементов, взятых в указанном порядке, также будет однозначно определенным элементом полугруппы.

3. Еще более узким является понятие группы, одно из самых важных алгебраических понятий. *Группой* называется полугруппа, в которой выполнимы обратные операции, т. е. для любых элементов a и b каждое из уравнений

$$ax = b, \qquad ya = b \tag{3}$$

обладает решением, притом единственным.

Заметим, что единственность решений каждого из уравнений (3) позволяет производить в группе *левосторонние* и *правосторонние сокращения*: если

$$ab_1 = ab_2 \text{ или } b_1a = b_2a,$$

то $b_1 = b_2$.

Решения x и y уравнений (3) в случае произвольной группы не обязаны совпадать. Дело в том, что алгебраическая операция не предполагается нами коммутативной, т. е. произведение может зависеть от порядка сомножителей. Группа (или полугруппа, или группоид), для любых двух элементов a, b которой выполняется *закон коммутативности*

$$ab = ba,$$

называется *коммутативной* или *абелевой*.

4. *Всякая группа G обладает однозначно определенным элементом e, удовлетворяющим условию*

$$ae = ea = a$$

для всех элементов $a \in G$.

Действительно, из определения группы следует существование в G для любого элемента a такого элемента e'_a, что $ae'_a = a$, причем этот элемент e'_a однозначно определен. Если b — любой другой элемент группы G, а y — элемент группы, удовлетворяющий равенству $ya = b$, то, ввиду закона ассоциативности,

$$be'_a = (ya)\,e'_a = y\,(ae'_a) = ya = b,$$

откуда $e'_b = e'_a$. Элемент e'_a не зависит, следовательно, от элемента a; обозначим его через e'. Таким образом,

$$ae' = a \text{ для всех } a \in G. \tag{4}$$

Аналогично доказывается существование и единственность такого элемента e'', что

$$e''a = a \text{ для всех } a \in G. \tag{5}$$

Применяя, однако, равенства (4) и (5) к произведению $e''e'$, мы получаем $e''e' = e''$ и $e''e' = e'$, откуда $e'' = e'$. Теорема доказана.

Элемент e, существование и единственность которого утверждаются в этой теореме, называется *единицей* группы G и обычно обозначается символом 1.

Для всякого элемента a группы G существует такой однозначно определенный элемент a^{-1}, что

$$aa^{-1} = a^{-1}a = 1.$$

Действительно, из определения группы вытекает существование таких однозначно определенных элементов a' и a'', что

$$aa' = 1, \quad a''a = 1.$$

Однако, применяя закон ассоциативности, мы получаем

$$a''aa' = a''\,(aa') = a'' \cdot 1 = a'',$$

$$a''aa' = (a''a)\,a' = 1 \cdot a' = a',$$

откуда $a'' = a'$.

Элемент a^{-1} называется *обратным элементом* для a. Ясно, что обратным для a^{-1} служит сам элемент a и что $1^{-1} = 1$. Легко видеть также, что для любых элементов $a_1, a_2, \ldots, a_n$

$$(a_1a_2 \ldots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \ldots a_2^{-1}a_1^{-1}.$$

5. Следующая теорема часто облегчает проверку того, что данная полугруппа является группой:

Полугруппа G тогда и только тогда будет группой, если в G существует по меньшей мере одна правая единица e, обладающая свойством

$$ae = a \text{ для всех } a \in G,$$

причем это e можно выбрать так, что для всякого $a \in G$ существует по меньшей мере один правый обратный элемент a^{-1}, удовлетворяющий условию

$$aa^{-1} = e.$$

В одну сторону эта теорема доказана в предшествующем пункте. Пусть теперь дана полугруппа G, удовлетворяющая условиям теоремы. Покажем, что элемент e будет и левой единицей для G. Если $a \in G$ и a^{-1} — один из его правых обратных элементов, то

$$eaa^{-1} = ee = e = aa^{-1}.$$

Умножая обе части этого равенства справа на один из элементов, правых обратных для a^{-1}, и используя однозначность произведения в полугруппе, мы получим

$$eae = ae,$$

откуда $ea = a$, что мы и хотели показать.

Если теперь e' — любая правая единица для G, e'' — любая левая единица, то, как и в доказательстве первой теоремы предшествующего пункта, мы получим, что $e'' = e'$, т. е. докажем существование и единственность в G единицы e.

Пусть, далее, снова $a \in G$ и a^{-1} — один из правых обратных элементов для a. Умножая равенство $aa^{-1} = e$ слева на a^{-1}, мы получим

$$a^{-1}aa^{-1} = a^{-1}.$$

Умножая это последнее равенство справа на один из правых обратных элементов для a^{-1}, мы приходим к равенству

$$a^{-1}ae = e,$$

откуда $a^{-1}a = e$. Элемент a^{-1} оказался и левым обратным для a.

Теперь, как и в доказательстве второй теоремы предшествующего пункта, легко проверяется, что любой левый обратный элемент для a равен любому правому обратному

элементу. Отсюда следует существование в G для всякого элемента a однозначно определенного обратного элемента a^{-1}.

Для завершения доказательства теоремы укажем, что решениями уравнений (3) служат соответственно элементы

$$x = a^{-1}b \quad \text{и} \quad y = ba^{-1}.$$

Единственность этих решений следует из того, что если, например, $ax_1 = ax_2$, то, умножая это равенство слева на a^{-1}, мы получим $x_1 = x_2$.

6. Иногда, в частности при изучении абелевых групп, используется не мультипликативная, а аддитивная запись: групповая операция называется *сложением,* сумма записывается через $a+b$, единица группы называется *нулем* и обозначается символом 0, а вместо обратного элемента говорят о *противоположном элементе* и обозначают его через $-a$.

При аддитивной записи для абелевых групп обратная операция — в этом случае она будет, конечно, единственной — называется *вычитанием.* Решение уравнения

$$a + x = b$$

называется *разностью* и записывается в виде $b - a$. Ясно, что

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

и поэтому

$$b - (a_1 + a_2) = b - a_1 - a_2.$$

7. Многочисленные важные примеры абелевых групп дают нам обычные операции над числами. Так, беря все целые числа — положительные, нуль и отрицательные — и рассматривая в этом множестве операцию сложения, мы получаем абелеву группу, называемую *аддитивной группой целых чисел.* Абелеву группу по сложению составляют также все рациональные числа — *это аддитивная группа рациональных чисел.* Можно говорить и об аддитивных группах всех действительных и всех комплексных чисел.

Если же взять лишь натуральные числа, то они составляют по сложению полугруппу, называемую *аддитивной полугруппой натуральных чисел,* но не группу, так как вычитание здесь не всегда выполнимо.

При составлении из чисел групп по умножению следует помнить, что ни в одну из них не войдет число нуль, так как деление на нуль невозможно. Мультипликативную группу составляют, например, все отличные от нуля рациональные

числа, равно как и лишь строго положительные рациональные числа. С другой стороны, по умножению полугруппами, но не группами, будут системы всех целых чисел, всех целых неотрицательных чисел и всех натуральных чисел.

Как пример конечной абелевой группы назовем *мультипликативную группу корней n-й степени из единицы.* Порядок этой группы — а *порядком* конечной группы называется число ее элементов — равен n.

8. Перейдем к примерам некоммутативных групп и полугрупп. Назовем *преобразованием* множества M любое отображение этого множества в себя (т. е. на некоторое его подмножество). Частным случаем преобразования является *подстановка*, т. е. взаимно однозначное отображение множества M на себя.

В I.1.2. введено умножение отображений, понимаемое как их последовательное выполнение, и доказана ассоциативность этой операции. В применении к случаю преобразований мы получаем, что относительно операции последовательного выполнения все преобразования данного множества M составляют полугруппу; она называется *симметрической полугруппой на множестве M.*

Так как последовательное выполнение двух подстановок множества M снова будет подстановкой, то можно говорить и о полугруппе подстановок на M. *Тождественная подстановка*, оставляющая на месте каждый элемент из M, является единицей этой полугруппы. С другой стороны, если x — произвольная подстановка, переводящая всякий элемент a из M в элемент ax, то обратное преобразование, переводящее ax в a для всех $a \in M$, также будет подстановкой; она служит для x *обратной подстановкой.* Таким образом, ввиду II. 1.5, по операции последовательного выполнения все подстановки данного множества M составляют группу; она называется *симметрической группой на множестве M.*

Если множество M конечно и состоит из n элементов, то симметрическая группа на M, называемая *симметрической группой n-й степени* и обозначаемая через S_n, будет конечной и имеет порядок $n!$. Конечной будет и симметрическая полугруппа на конечном множестве M.

Другим примером некоммутативной группы является совокупность всех невырожденных квадратных матриц порядка n (где $n \geqslant 2$) с действительными элементами, рассматриваемая относительно операции умножения матриц.

§ 2. Кольца, тела, поля

1. Вторым важнейшим алгебраическим понятием, наряду с понятием группы, является понятие кольца. *Кольцом* называется множество R, в котором заданы две бинарные алгебраические операции (в смысле II.1.2) — сложение и умножение, причем по сложению это должна быть абелева группа — *аддитивная группа кольца* R, — а умножение должно быть связано со сложением *законами дистрибутивности*:

$$a(b+c)=ab+ac, \qquad (b+c)a=ba+ca. \tag{1}$$

На само умножение в общем случае не накладывается никаких ограничений, т. е. кольцо R по умножению является лишь группоидом — это будет *мультипликативный группоид кольца* R. Если умножение в кольце ассоциативно, то мы называем кольцо *ассоциативным кольцом* и говорим о его *мультипликативной полугруппе;* если же умножение в кольце и ассоциативно, и коммутативно, то кольцо называется *ассоциативно-коммутативным.*

Во всяком кольце законы дистрибутивности выполняются и для разности, т. е.

$$a(b-c)=ab-ac, \qquad (b-c)a=ba-ca. \tag{2}$$

Действительно, по II.1.6,

$$c+(b-c)=b.$$

Умножая обе части этого равенства слева на a, а затем применяя в левой части равенства первый из законов дистрибутивности (1), мы получим

$$ac+a(b-c)=ab,$$

откуда, снова по II. 1.6, вытекает первое из равенств (2).

2. *Всякая абелева группа G служит аддитивной группой некоторого кольца*: достаточно предположить, что групповая операция группы G записывается аддитивно, а затем ввести в G *нулевое умножение*, т. е. положить

$$ab=0$$

для любых a и b из G. Выполнение законов дистрибутивности (1) очевидно. Это *нулевое кольцо* с аддитивной группой G будет, конечно, ассоциативно-коммутативным. В теории

колец нулевые кольца играют роль, параллельную той роли, которую в теории групп играют абелевы группы.

Первым примером ненулевого ассоциативно-коммутативного кольца служит *кольцо целых чисел.* В качестве примера ассоциативного, но не коммутативного кольца напомним *кольцо квадратных матриц* порядка n (где $n \geqslant 2$) с действительными элементами: операциями в этом кольце служат вводимые в курсе высшей алгебры сложение и умножение матриц.

Укажем, наконец, один пример неассоциативного кольца. Это будет *кольцо векторов трехмерного евклидова пространства,* причем операциями служат обычное сложение векторов и определяемое в курсе аналитической геометрии векторное умножение векторов. Легко проверяется, что это умножение не будет ни ассоциативным, ни коммутативным, но что со сложением оно связано законами дистрибутивности (1).

Читатель легко проверит также (или же найдет в учебниках по векторной алгебре), что в построенном нами кольце для любых векторов a, b, c выполняются следующие равенства:

$$a^2 = 0 \tag{3}$$

и *тождество Якоби*

$$(ab)\,c + (bc)\,a + (ca)\,b = 0. \tag{4}$$

Заметим, что из (3) вытекает *закон антикоммутативности*

$$ba = -ab.$$

Действительно, так как

$$a^2 = b^2 = (a+b)^2 = 0,$$

то

$$0 = (a+b)^2 = a^2 + ab + ba + b^2 = ab + ba.$$

3. Всякое кольцо, удовлетворяющее условиям (3) и (4), называется *лиевым кольцом.* Лиевы кольца составляют важный класс колец, в общем случае неассоциативных; к ним принадлежат, впрочем, все нулевые кольца.

Между ассоциативными и лиевыми кольцами существует следующая любопытная связь:

Если R — произвольное ассоциативное кольцо, то, сохраняя аддитивную группу этого кольца, а операцию

умножения ab заменяя операцией коммутирования

$$a \circ b = ab - ba,$$

мы получим лиево кольцо $R^{(-)}$.

В самом деле, проверим справедливость законов дистрибутивности; можно проверить хотя бы первый из законов (1)

$$a \circ (b+c) = a(b+c) - (b+c)a = ab + ac - ba - ca = \\ = (ab - ba) + (ac - ca) = a \circ b + a \circ c.$$

Таким образом, множество R, рассматриваемое с операциями сложения и коммутирования, оказывается кольцом; обозначим его через $R^{(-)}$. Остается проверить справедливость равенств (3) и (4):

$$a \circ a = aa - aa = 0,$$

$$(a \circ b) \circ c + (b \circ c) \circ a + (c \circ a) \circ b = (ab - ba)c - c(ab - ba) + \\ + (bc - cb)a - a(bc - cb) + (ca - ac)b - b(ca - ac) = 0.$$

Кольцо $R^{(-)}$ оказалось лиевым.

4. *Если в ассоциативном кольце R сохранить его аддитивную группу, а операцию умножения ab заменить операцией симметрирования*

$$a \cdot b = ab + ba,$$

то будет получено кольцо $R^{(+)}$, в котором для любых элементов a, b выполняются равенства

$$a \cdot b = b \cdot a, \tag{5}$$

$$[(a \cdot a) \cdot b] \cdot a = (a \cdot a) \cdot (b \cdot a). \tag{6}$$

В самом деле, проверим хотя бы первый из законов дистрибутивности (1):

$$a \cdot (b+c) = a(b+c) + (b+c)a = ab + ac + ba + ca = \\ = (ab + ba) + (ac + ca) = a \cdot b + a \cdot c.$$

Проверим теперь справедливость равенств (5) и (6):

$$a \cdot b = ab + ba = ba + ab = b \cdot a,$$

$$[(a \cdot a) \cdot b] \cdot a = [(aa + aa)b + b(aa + aa)]a + \\ + a[(aa + aa)b + b(aa + aa)] = aaba + \\ + aaba + baaa + baaa + aaab + aaab + \\ + abaa + abaa = (aa + aa)(ba + ab) + \\ + (ba + ab)(aa + aa) = (a \cdot a) \cdot (b \cdot a).$$

Всякое кольцо, удовлетворяющее условиям (5) и (6), называется *йордановым*. В общем случае оно неассоциативное; к йордановым кольцам принадлежат, впрочем, все ассоциативно-коммутативные кольца.

5. *Во всяком кольце R любое произведение, в котором хотя бы один из сомножителей равен нулю, само равно нулю. Иными словами,*

$$a \cdot 0 = 0 \cdot a = 0 \tag{7}$$

для всех элементов a кольца R.

В самом деле, если x — произвольный вспомогательный элемент кольца R, то, ввиду (2),

$$a \cdot 0 = a(x - x) = ax - ax = 0.$$

Если a и b — любые элементы произвольного кольца R, то

$$(-a)b = a(-b) = -ab, \tag{8}$$

$$(-a)(-b) = ab. \tag{9}$$

Действительно,

$$ab + (-a)b = [a + (-a)]b = 0 \cdot b = 0.$$

Так же проверяется и вторая половина равенства (8). С другой стороны, используя (8), получаем

$$(-a)(-b) = -[a(-b)] = -(-ab) = ab,$$

чем доказано и (9).

6. Заметим, что обращение утверждения, выражаемого равенством (7), справедливое в случае числовых колец, в общем случае не имеет места: существуют кольца, обладающие *делителями нуля*, т. е. такими отличными от нуля элементами a и b, произведение которых равно нулю:

$$ab = 0.$$

Примерами таких колец помимо любого нулевого кольца, являются к о л ь ц а м а т р и ц. Мы уже упоминали кольцо действительных квадратных матриц. Вообще, если R — произвольное кольцо, то можно рассмотреть всевозможные квадратные матрицы порядка n с элементами из R. Определяя для них обычным способом сложение и умножение, мы получим, как

легко проверить, кольцо, даже ассоциативное, если ассоциативно исходное кольцо R. Нулем этого кольца служит *нулевая матрица*, составленная из нулей. Построенное кольцо называется *полным кольцом матриц* порядка n над кольцом R и обозначается через R_n.

Если $n \geqslant 2$, а кольцо R состоит не только из одного нуля, то полное кольцо матриц R_n обладает делителями нуля.

Действительно, если a — отличный от нуля элемент из R, то матрицы

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 \\ 0 & \dots & 0 & a \end{pmatrix}$$

отличны от нулевой матрицы, но их произведение равно нулю.

Примерами колец с делителями нуля являются также полные кольца функций. Пусть даны произвольное множество M и произвольное кольцо R. Рассмотрим множество всевозможных *функций* на M со значениями в R, т. е. всевозможных отображений f множества M в кольцо R; образ элемента $x \in M$ при отображении f будем обозначать здесь через $f(x)$. Это множество функций превращается в кольцо, если сумма и произведение функций будут определены, как обычно, равенствами

$$(f+g)(x) = f(x) + g(x),$$
$$(fg)(x) = f(x) \cdot g(x),$$

т. е. при помощи сложения и умножения значений заданных функций для всех x из M. Легко проверяется, что все требования, входящие в определение кольца, выполняются и что полученное кольцо будет ассоциативным или коммутативным, если только ассоциативно или соответственно коммутативно исходное кольцо R.

Построенное кольцо называется *полным кольцом функций* на множестве M со значениями в кольце R. Если M — множество точек числовой прямой, а R — совокупность действительных чисел, то наше кольцо будет обычным кольцом всех действительных функций действительного переменного.

Всякое полное кольцо функций на множестве M, содержащем не менее двух элементов, со значениями в кольце R, состоящем не из одного нуля, обладает делителями нуля.

В самом деле, роль нуля в этом кольце играет *нулевая функция*, тождественно (т. е. для всех x из M) равная нулю. Если же мы разобьем множество M на два непустых непересекающихся подмножества A и B, то существуют, очевидно, такие ненулевые функции f и g, что f принимает нулевые значения на A, а g — на B. Ясно, что произведение fg будет нулевой функцией.

7. Ассоциативно-коммутативное кольцо без делителей нуля называется *областью целостности*; таковы, в частности, всевозможные числовые кольца. Важные примеры областей целостности можно получить, используя следующую конструкцию.

Если R—произвольное ассоциативно-коммутативное кольцо, то можно рассмотреть всевозможные *многочлены*

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n, \qquad n \geqslant 0,$$

относительно *неизвестного x с коэффициентами* $a_0, a_1, \ldots, a_n$ из R; если $a_n \neq 0$, то n будет *степенью* этого многочлена. Определяя сложение и умножение многочленов так же, как это делается в курсе высшей алгебры, мы получим, как нетрудно проверить, кольцо, называемое *кольцом многочленов* $R[x]$ от неизвестного x над кольцом R; это кольцо также будет ассоциативно-коммутативным. Нулем кольца многочленов служит многочлен, все коэффициенты которого равны нулю.

Аналогично определяется кольцо многочленов $R[x_1, x_2, \ldots, x_n]$ от любого конечного числа неизвестных; оно будет при этом просто кольцом многочленов от одного неизвестного x_n над кольцом $R[x_1, \ldots, x_{n-1}]$. Можно говорить и о кольце многочленов над R от любого бесконечного множества неизвестных, считая при этом, что каждый отдельный многочлен зависит лишь от некоторого конечного числа неизвестных.

Если R — область целостности, то любое кольцо многочленов над R также будет областью целостности.

Справедливость этого утверждения для кольца многочленов $R[x]$ от одного неизвестного вытекает из того, что если многочлены f и g отличны от нуля, а в R нет делителей нуля, то степень произведения fg равна сумме степеней сомножителей, т. е. это произведение также отлично от нуля. Переход к случаю любого конечного числа неизвестных

достигается простой индукцией, а в случае колец многочленов от бесконечного множества неизвестных достаточно учесть, что всякий многочлен записывается через конечное число неизвестных.

8. Над произвольным ассоциативно-коммутативным кольцом R можно рассматривать не только многочлены, но и (формальные) *степенные ряды*

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_k x^k + \ldots = \sum_{k=0}^{\infty} a_k x^k \qquad (10)$$

от неизвестного x. Определение операций переносится с многочленов на степенные ряды без всяких затруднений:

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k + b_k) x^k,$$

$$\sum_{k=0}^{\infty} a_k x^k \cdot \sum_{l=0}^{\infty} b_l x^l = \sum_{m=0}^{\infty} c_m x^m,$$

где

$$c_m = \sum_{k+l=m} a_k b_l.$$

Как и в случае многочленов, проверяется, что мы получаем ассоциативно-коммутативное кольцо; оно называется *кольцом степенных рядов* от неизвестного x над кольцом R и обозначается через $R\{x\}$.

Переход к кольцам степенных рядов над R от любого конечного числа, а затем и от бесконечного множества неизвестных совершается так же, как для колец многочленов, причем в случае бесконечного множества неизвестных целесообразно наложить требование, что каждый степенной ряд зависит лишь от конечного числа неизвестных.

Если R — *область целостности, то любое кольцо степенных рядов над* R *также будет областью целостности.*

Достаточно рассмотреть случай кольца $R\{x\}$ от одного неизвестного. Если мы назовем *нижней степенью* степенного ряда (10) число n в том случае, когда

$$a_0 = a_1 = \ldots = a_{n-1} = 0, \quad a_n \neq 0,$$

то всякий ненулевой степенной ряд будет обладать нижней степенью. Ввиду отсутствия в R делителей нуля нижняя

степень произведения двух степенных рядов равна сумме нижних степеней сомножителей. Отсюда следует наше утверждение.

9. Понятие *единицы*, введенное в II.1.4 для случая группы, переносится, конечно, на случай любого группоида или кольца R: это будет такой элемент 1, что для всех элементов a из R

$$a \cdot 1 = 1 \cdot a = a.$$

Если единица в кольце R существует, то только одна. Ее может, однако, и не быть, как показывает пример кольца четных чисел.

Всякое лиево кольцо (см. II.2.3), *состоящее не только из одного нуля, является кольцом без единицы.*

Действительно, пусть лиево кольцо L обладает единицей 1. Тогда, по (3), полагая $a = 1$, получаем $1^2 = 0$. Таким образом, $1 = 0$, откуда, ввиду (7), вытекает, что кольцо L состоит лишь из нуля.

Если кольцо R обладает единицей, то единицами обладают также всевозможные кольца матриц над R, кольца функций со значениями в R, а в ассоциативно-коммутативном случае и кольца многочленов и кольца степенных рядов над R от любого числа неизвестных.

Действительно, единицей кольца матриц служит единичная матрица, по главной диагонали которой стоит 1, а все элементы вне диагонали равны нулю. Единицей кольца функций является функция, тождественно равная 1. Наконец, единицей кольца многочленов (или кольца степенных рядов) служит многочлен (степенной ряд), все коэффициенты которого равны нулю, кроме a_0, равного 1.

10. Всякое кольцо является по умножению группоидом а ассоциативное кольцо — полугруппой. Никакое кольцо, состоящее не только из нуля, не может быть по умножению группой, как вытекает из мультипликативного свойства нуля (7). Может оказаться, однако, что все отличные от нуля элементы кольца составляют группу по умножению. Такое кольцо — оно непременно будет ассоциативным — называется *телом*, а группа по умножению его отличных от нуля элементов — *мультипликативной группой* этого тела.

Тело с коммутативным умножением называется *полем*. Основные примеры полей — поле рациональных чисел, поле

действительных чисел и поле комплексных чисел. Пример некоммутативного тела будет указан в V. 6.8.

Из определения тела следует, что *тело не содержит делителей нуля*. Далее, *всякое тело обладает единицей* — действительно, единица мультипликативной группы этого тела служит, ввиду (7), единицей для всего тела. Наконец, *во всяком теле каждое из уравнений*

$$ax = b, \quad ya = b, \quad \text{где } a \neq 0, \tag{11}$$

обладает решением, притом единственным.

Действительно, если $b \neq 0$, то оба уравнения (11) обладают однозначно определенными решениями в мультипликативной группе тела, а нуль не может удовлетворять ни одному из этих уравнений. Если же $b = 0$, то нуль служит решением для каждого из уравнений (11) и никаких других решений нет ввиду отсутствия делителей нуля.

Обратно, *ассоциативное кольцо R будет телом, если в нем каждое из уравнений вида* (11) *при любом $a \neq 0$ и произвольном b обладает хотя бы одним решением.*

Покажем прежде всего, что в R нет делителей нуля. Если $a \neq 0$ и $b \neq 0$, но $ab = 0$, то обозначим через e одно из решений уравнения $ax = a$, а через c — одно из решений уравнения $bx = e$. Тогда

$$0 = 0 \cdot c = abc = ae = a,$$

что противоречит условию.

Отсюда следует, что множество отличных от нуля элементов кольца R будет мультипликативной полугруппой. Оно будет даже группой, так как уравнения (11) обладают при $a \neq 0$ и $b \neq 0$ решениями в самом этом множестве, а единственность этих решений следует из отсутствия в R делителей нуля: если, например, $ax_1 = ax_2$ и $a \neq 0$, то $a(x_1 - x_2) = 0$ и поэтому $x_1 = x_2$. Теорема доказана.

С вопросом о перенесении понятия тела на случай неассоциативных колец мы встретимся в II.6.1.

§ 3. Подгруппы, подкольца

1. Непустое подмножество A группоида G называется *подгруппоидом* в G, если произведение любых двух элементов из A само принадлежит к A. Если G — полугруппа, то подгруппоид A естественно назвать *подполугруппой*. Если же

G — группа, то *подгруппой* этой группы мы назовем такую подполугруппу A, которая сама является группой относительно операции, определенной в группе G; для этого достаточно, чтобы подполугруппа A вместе со всяким своим элементом a содержала и его обратный элемент a^{-1}.

Не всякая подполугруппа некоторой группы обязана быть подгруппой этой группы, как показывает пример аддитивной полугруппы натуральных чисел, являющейся подполугруппой, но не подгруппой, аддитивной группы всех целых чисел.

Заметим, что имеет смысл говорить и о подгруппах любой полугруппы. Так, симметрическая группа на произвольном множестве M (см. II.1.8) является подгруппой симметрической полугруппы на этом же множестве.

2. *Подкольцом* кольца R называется всякое подмножество A этого кольца, само являющееся кольцом относительно операций, определенных в R. Иными словами, A должно быть подгруппой аддитивной группы кольца R и подгруппоидом мультипликативного группоида этого кольца: законы дистрибутивности, будучи справедливыми в R, выполняются, конечно, и в A.

Можно говорить, в частности, о подкольце тела или поля. Так, кольцо целых чисел является подкольцом поля рациональных чисел.

Аналогично определяются понятия *подтела и подполя*. Можно говорить при этом о подтеле (подполе) не только тела, но и любого кольца. Так, в кольце многочленов $P[x]$ над произвольным полем P многочлены нулевой степени, к которым добавлен нуль, составляют подполе.

3. Подгруппами всякой группы G являются, в частности, сама эта группа и *единичная подгруппа* E, составленная из одной единицы. Аналогично подкольцами всякого кольца R служат само это кольцо и *нуль-подкольцо*, составленное из одного нуля.

Для получения более интересных примеров подгрупп введем понятие о степенях элементов. Пусть G — произвольная полугруппа и a — ее элемент. Ассоциативность умножения позволяет обычным путем определить *положительные степени* a^n элемента a, $n = 1, 2, \ldots$, причем, как обычно,

$$a^k \cdot a^l = a^{k+l}, \tag{1}$$

$$(a^k)^l = a^{kl}. \tag{2}$$

Из (1) следует, что все положительные степени элемента a составляют в полугруппе G абелеву подполугруппу, называемую *циклической подполугруппой* элемента a.

Если же G — группа, то мы положим $a^0 = 1$, а затем введем *отрицательные степени* элемента a. Именно, если n — любое натуральное число, то легко проверяется равенство

$$a^n(a^{-1})^n = 1,$$

из которого вытекает, что

$$(a^{-1})^n = (a^n)^{-1}. \tag{3}$$

Элемент, равный обеим частям равенства (3), мы и обозначим через a^{-n}. Равенства (1) и (2) остаются справедливыми для любых степеней элемента a группы G, а поэтому все степени элемента a, включая нулевую и отрицательные, составляют в группе G абелеву подгруппу, называемую *циклической подгруппой* элемента a и обозначаемую через $\{a\}$.

При аддитивной записи групповой операции вместо степеней элемента следует говорить о *кратных* этого элемента.

4. Степени элемента a группы G, имеющие различные показатели, не обязаны быть различными элементами этой группы, как вытекает хотя бы из существования конечных групп. Если все степени элемента a действительно различны, то a называется *элементом бесконечного порядка*, а в противном случае — *элементом конечного порядка*. В этом втором случае существуют такие целые числа k и l, что $k > l$, но

$$a^k = a^l.$$

Отсюда $a^{k-l} = 1$, причем $k - l > 0$, т. е. существуют равные единице степени элемента a с натуральными показателями. Наименьший среди таких показателей называется *порядком* элемента a.

Если a — элемент конечного порядка n, то степени

$$1 = a^0,\ a,\ a^2,\ \ldots,\ a^{n-1} \tag{4}$$

будут, очевидно, различными элементами группы. Всякая другая степень a^k элемента a, положительная или отрицательная, равна одному из элементов (4). Действительно, если

$$k = nq + r,\ 0 \leqslant r < n,$$

то, ввиду (1), (2) и равенства $a^n = 1$,

$$a^k = (a^n)^q a^r = a^r.$$

Отсюда следует, что *порядок n элемента конечного порядка a совпадает с порядком* (см. II.1.7) *его циклической подгруппы* $\{a\}$.

Группа, все элементы которой имеют конечные порядки, не обязательно ограниченные в совокупности, называется *периодической*. С другой стороны, группа называется *группой без кручения*, если все ее элементы, кроме 1, бесконечного порядка.

5. В случае колец возникает естественный вопрос об аналоге циклической подгруппы, т. е. о минимальном подкольце, содержащем данный элемент. Пусть R — произвольное (не обязательно ассоциативное) кольцо и a — его элемент. Всякое подкольцо кольца R, содержащее a, содержит также всевозможные произведения по n множителей, равных a ($n = 1, 2, 3, \ldots$); эти произведения играют роль положительных степеней элемента a. Ввиду возможной неассоциативности умножения во всяком таком произведении должны быть некоторым образом распределены скобки, причем так, чтобы каждый раз перемножались лишь два элемента кольца. Для $n = 3$ таких произведений будет два — $(aa)a$ и $a(aa)$, для $n = 4$ — пять, и т. д.

Всякое подкольцо, содержащее a, содержит и всевозможные суммы любого конечного числа указанных произведений, взятых с любыми целыми коэффициентами. Элементы кольца R, записываемые в виде таких сумм (быть может, и неоднозначно), сами составляют, однако, подкольцо в R; это и будет искомое *подкольцо, порожденное элементом a*.

Из сказанного следует, что если кольцо R ассоциативно, то подкольцо, порожденное элементом a, состоит из всех тех элементов кольца R, которые хотя бы одним способом записываются в виде суммы (с целыми коэффициентами) положительных степеней элемента a. Это подкольцо будет, таким образом, коммутативным.

6. Всякая подгруппа группы G содержит единицу этой группы, всякое подкольцо кольца R — нуль этого кольца. Пересечение любой системы подгрупп группы G (любой системы подколец кольца R) будет, следовательно, непустым.

Пересечение любой системы подгрупп группы G является подгруппой этой группы. Аналогично, пересечение любой системы подколец кольца R будет подкольцом этого кольца, пересечение любой системы подполугрупп некоторой полугруппы, если оно не пусто, будет подполугруппой, и т. д.

Докажем хотя бы первое утверждение. Пусть в группе G взята произвольная система подгрупп A_α, где α пробегает некоторое множество индексов, и пусть D — пересечение этих подгрупп. Если b и c — любые элементы из D, то их произведение bc содержится в каждой из подгрупп A_α, т. е. содержится в D. С другой стороны, для любого $b \in D$ элемент b^{-1} принадлежит к каждой из подгрупп A_α, а поэтому $b^{-1} \in D$. Множество D будет, следовательно, подгруппой группы G.

7. Пусть G будет или группой, или кольцом, или телом, или полугруппой, или алгебраической системой какого-либо другого из встречавшихся нам типов. Если M — любое подмножество из G, то существует минимальная подгруппа (соответственно подкольцо, подтело и т. д.), содержащая подмножество M, — *подгруппа, порожденная множеством* M; обозначается она через $\{M\}$. Именно, это будет пересечение всех подгрупп группы G, целиком содержащих M; по меньшей мере одна такая подгруппа существует, а именно — сама G.

Легко проверить, обобщая данное в II.3.3 определение циклических подгрупп, что *подгруппа $\{M\}$ состоит из тех и только тех элементов группы G, которые хотя бы одним способом могут быть записаны в виде некоторого произведения степеней конечного числа элементов из M.*

Аналогично, обобщая сказанное в II.3.5, мы получим, что *подкольцо, порожденное в кольце R множеством M, состоит из всех тех элементов кольца R, которые хотя бы одним способом могут быть записаны в виде суммы (с целыми коэффициентами) произведений конечного числа элементов из M*; в неассоциативном случае эти произведения рассматриваются, конечно, с некоторым распределением скобок.

8. Применяя сказанное выше к случаю, когда в группе G задана некоторая система подгрупп A_i, $i \in I$, а множество M

является объединением всех A_i, мы придем к понятию *подгруппы, порожденной заданной системой подгрупп*; обозначается она через $\{A_i,\ i \in I\}$ в общем случае, через $\{A, B\}$, если речь идет об объединении двух подгрупп A и B, и т. д. Аналогичный смысл имеет понятие *подкольца, порожденного в кольце заданной системой подколец.*

9. Если G — или группа, или кольцо, и т. д., то в G существуют такие подмножества M — само G, например, — что

$$\{M\} = G.$$

Всякое такое подмножество M называется *системой образующих* для G.

Если G обладает хотя бы одной конечной системой образующих, то говорят, что G — *группа* (или полугруппа, или кольцо) *с конечным числом образующих*. Система образующих может состоять, в частности, из одного элемента. Группы, обладающие одним образующим элементом, т. е. совпадающие с одной из своих циклических подгрупп, называются *циклическими группами*. Полное обозрение циклических групп будет дано в следующем параграфе.

§ 4. Изоморфизм

1. Понятие изоморфизма может быть введено для каждого из рассматриваемых в этой главе типов алгебраических систем, причем оно играет здесь ту же роль, что и для частично упорядоченных множеств (см. I.4.3): изоморфные группы, например, могут рассматриваться как тождественные, как два экземпляра одной и той же группы всякий раз, когда изучается сама групповая операция, а природа элементов, из которых группы составлены, не играет роли.

Переходим к определениям. Группоиды G и G' называются *изоморфными*, если существует такое взаимно однозначное отображение φ группоида G на группоид G', что для любых элементов $a,\ b \in G$

$$(ab)\varphi = a\varphi \cdot b\varphi.$$

Само отображение φ с этими свойствами называется *изоморфным отображением*. Ясно, что свойство группоидов быть изоморфными симметрично (отображение, обратное изо-

морфному, само будет изоморфным) и транзитивно; оно и рефлексивно — достаточно рассмотреть тождественное отображение группоида на себя. Изоморфизм группоидов G и G' записывается обычно символом

$$G \simeq G'.$$

Этот же символ будет использоваться нами для записи изоморфизма и в случае других алгебраических образований.

Понятно, что при изоморфном отображении сохраняются все свойства группоида, формулируемые на языке операции, заданной в этом группоиде, в частности такие, как ассоциативность, коммутативность, существование единицы и обратных элементов. Покажем на простом примере, как доказываются такого рода утверждения. Пусть G — коммутативный группоид, а φ — его изоморфное отображение на группоид G'. Если a' и b' — любые элементы из G', а a и b — такие элементы из G, что

$$a\varphi = a', \quad b\varphi = b',$$

то

$$(ab)\varphi = a'b', \quad (ba)\varphi = b'a',$$

и из равенства $ab = ba$ и однозначности отображения вытекает равенство $a'b' = b'a'$.

Отсюда следует, что *изоморфным образом полугруппы, группы или абелевой группы будет полугруппа или соответственно группа, или абелева группа.*

Два кольца называются *изоморфными*, если между ними можно установить взаимно однозначное соответствие, являющееся изоморфизмом как для аддитивных групп, так и для мультипликативных группоидов этих колец. Ясно, что при изоморфизме сохраняется свойство кольца быть ассоциативным, коммутативным, лиевым или йордановым, а также свойство быть телом.

Укажем один интересный пример изоморфизма групп: *мультипликативная группа положительных действительных чисел изоморфна аддитивной группе всех действительных чисел.* В самом деле, ставя в соответствие каждому положительному числу его логарифм по некоторому фиксированному основанию, мы получим взаимно однозначное отображение первой из указанных групп на вторую. Изоморфность этого отображения вытекает из того, что логарифм произведения равен сумме логарифмов сомножителей.

2. Переходя к обещанному в II.3.9 обозрению всех циклических групп, начнем с некоторых примеров. Аддитивная группа целых чисел служит примером бесконечной циклической группы, так как всякое целое число кратно числу 1. С другой стороны, мультипликативная группа корней n-й степени из единицы служит примером конечной циклической группы порядка n, как вытекает из существования первообразного корня n-й степени из единицы.

Все бесконечные циклические группы изоморфны аддитивной группе целых чисел и поэтому изоморфны между собой. Все конечные циклические группы порядка n изоморфны мультипликативной группе корней n-й степени из единицы и поэтому изоморфны между собой.

Докажем первое из этих утверждений. Если G — бесконечная циклическая группа с образующим элементом a, то соответствие

$$a^k \to k$$

будет взаимно однозначным отображением группы G на всю аддитивную группу целых чисел. Изоморфность этого отображения вытекает из II.3.3, формула (1).

Для доказательства второго утверждения достаточно установить соответствие между степенями (с одинаковыми показателями) образующего элемента заданной циклической группы и соответствующего первообразного корня из единицы.

В силу этой теоремы для того, чтобы получить, например, обозрение всех подгрупп бесконечной циклической группы, достаточно рассмотреть аддитивную группу целых чисел.

Все ненулевые подгруппы аддитивной группы целых чисел исчерпываются совокупностями чисел, кратных некоторому натуральному числу n.

Ясно, в самом деле, что все целые числа, кратные натуральному числу n, составляют подгруппу, а именно циклическую подгруппу числа n, причем при различных n эти подгруппы различны. С другой стороны, если A — любая ненулевая подгруппа аддитивной группы целых чисел, то она не может состоять лишь из отрицательных чисел, так как вместе со всяким числом должна содержать и число, ему противоположное. Пусть n — наименьшее натуральное число, содержащееся в подгруппе A. Если a — любое число из A,

то пусть

$$a = qn + r, \quad 0 \leqslant r < n.$$

Тогда

$$r = a - qn \in A,$$

а поэтому, ввиду выбора числа n, $r = 0$, т. е. $a = qn$, что и требовалось доказать.

Таким образом, *всякая подгруппа бесконечной циклической группы сама является циклической.* Это же верно и для конечных циклических групп.

3. Говорят, что группоид G *изоморфно вкладывается* в группоид G', если существует изоморфное отображение группоида G на некоторый подгруппоид группоида G'. Это понятие переносится, конечно, и на случай колец.

Всякое кольцо R изоморфно вкладывается в полное кольцо матриц R_n (см. II.2.6).

В самом деле, *скалярные матрицы*, т. е. матрицы, имеющие на главной диагонали один и тот же элемент a, а вне этой диагонали нули, составляют в R_n подкольцо, изоморфное кольцу R.

Всякое кольцо R изоморфно вкладывается в полное кольцо функций на данном множестве M со значениями в R (см. II.2.6).

Действительно, функции, принимающие для всех x из M одно и тоже значение $a \in R$, составляют в кольце функций подкольцо, изоморфное кольцу R.

Для произвольного ассоциативно-коммутативного кольца R кольцо многочленов $R[x]$ изоморфно вкладывается в кольцо степенных рядов $R\{x\}$ (см. II.2.8).

В самом деле, степенные ряды, имеющие не более конечного числа отличных от нуля коэффициентов, составляют в $R\{x\}$ подкольцо, изоморфное кольцу $R[x]$.

4. Несколько больше усилий требует доказательство следующей теоремы:

Всякое кольцо R изоморфно вкладывается в кольцо с единицей. Если при этом кольцо R ассоциативно или коммутативно, то его можно вложить соответственно в ассоциативное или коммутативное кольцо с единицей.

Доказательство. Рассмотрим множество всевозможных пар вида (a, k), где $a \in R$, k — целое число. Определим

сумму и произведение таких пар равенствами:

$$(a,\ k)+(b,\ l)=(a+b,\ k+l), \tag{1}$$

$$(a,\ k)(b,\ l)=(ab+la+kb,\ kl). \tag{2}$$

По сложению мы получаем, очевидно, абелеву группу. Так как

$$\begin{aligned}[(a,\ k)+(b,\ l)](c,\ m)&=(a+b,\ k+l)(c,\ m)=\\&=((a+b)c+m(a+b)+(k+l)c,\ (k+l)m)=\\&=(ac+ma+kc+bc+mb+lc,\ km+lm)=\\&=(ac+ma+kc,\ km)+(bc+mb+lc,\ lm)=\\&=(a,\ k)(c,\ m)+(b,\ l)(c,\ m)\end{aligned}$$

и так же проверяется второй закон дистрибутивности, то нами построено кольцо. Из (2) следует, что

$$(a,\ k)(0,\ 1)=(0,\ 1)(a,\ k)=(a,\ k),$$

т. е. пара (0, 1) служит единицей этого кольца. Наконец, ввиду (1) и (2),

$$(a,\ 0)+(b,\ 0)=(a+b,\ 0),$$

$$(a,\ 0)(b,\ 0)=(ab,\ 0),$$

т. е. пары вида $(a, 0)$ составляют в нашем кольце пар подкольцо, изоморфное кольцу R.

Этим доказано первое утверждение теоремы. Второе утверждение легко следует из (2).

Заметим, что построенное нами кольцо вовсе не является единственным (или минимальным) кольцом с единицей, содержащим (в смысле изоморфного вложения) заданное кольцо R — так, уже само кольцо R могло обладать единицей.

5. *Всякий группоид изоморфно вкладывается в мультипликативный группоид некоторого кольца, причем ассоциативный или коммутативный группоид может быть вложен в кольцо, обладающее таким же свойством.*

Для доказательства рассмотрим всевозможные суммы вида

$$\sum_{a\in G} k_a a, \tag{3}$$

где a пробегает все элементы данного группоида G, а коэффициенты k_a являются целыми числами, причем не более конечного числа этих коэффициентов отлич-

но от нуля. Следующим образом определим сложение и умножение сумм вида (3):

$$\sum_{a\in G} k_a a + \sum_{a\in G} l_a a = \sum_{a\in G} (k_a + l_a)\, a, \tag{4}$$

$$\sum_{a\in G} k_a a \cdot \sum_{b\in G} l_b b = \sum_{c\in G} m_c c, \tag{5}$$

где m_c является суммой всех отличных от нуля произведений $k_a l_b$ для таких a и b, что $ab = c$. Ясно, что правые части равенств (4) и (5) являются суммами вида (3); так, равенство (5) имеет тот смысл, что конечные суммы, входящие в качестве множителей в левую часть этого равенства, должны перемножаться почленно, далее,

$$k_a a \cdot l_b b = (k_a l_b)(ab),$$

причем произведение ab следует понимать в смысле операции, заданной в группоиде G, а затем выполняется приведение подобных членов.

По сложению мы получаем, конечно, абелеву группу. Проверка законов дистрибутивности, а также доказательство того, что из ассоциативности или коммутативности умножения в группоиде G следует это же для умножения сумм вида (3), несколько громоздки, но не представляют никаких принципиальных трудностей, и их проведение предоставляется читателю.

Таким образом, всевозможные суммы вида (3) составляют кольцо относительно операций, определенных равенствами (4) и (5). Те суммы вида (3), у которых $k_a = 1$ для какого-то одного элемента a из G, а все остальные коэффициенты равны нулю, составляют, как вытекает из (5), подгруппоид мультипликативного группоида этого кольца, изоморфный заданному группоиду G. Теорема доказана.

Построенное нами кольцо называется *целочисленным группоидным кольцом* группоида G. Если группоид G является полугруппой или группой, то говорят соответственно о *целочисленном полугрупповом кольце* и *целочисленном групповом кольце*.

6. *Всякая группа G изоморфно вкладывается в симметрическую группу на некотором множестве M* (см. II.1.8). *В качестве M можно взять при этом множество элементов самой группы G.*

В самом деле, поставим в соответствие каждому элементу a группы G преобразование этой группы, переводящее любой элемент x из G в элемент xa. Так как из $x \neq y$ следует $xa \neq ya$ и, кроме того, для любого x из G имеет место равенство

$$(xa^{-1})\, a = x,$$

то преобразование $x \to xa$ отображает G на себя взаимно однозначно, т. е. является подстановкой. Далее, если $a \neq b$, то и подстановки, соответствующие этим элементам, будут различными, так как, например, $1 \cdot a \neq 1 \cdot b$. Наконец, равенство

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

показывает, что подстановка, соответствующая произведению ab, совпадает с результатом последовательного выполнения подстановок, соответствующих элементам a и b.

Всякая полугруппа G изоморфно вкладывается в симметрическую полугруппу на некотором множестве M (см. II.1.8).

Для доказательства изоморфно вложим полугруппу G, используя II.4.5, в мультипликативную полугруппу некоторого ассоциативного кольца R, изоморфно вложим затем это кольцо, по II.4.4, в ассоциативное кольцо $\bar{R}$ с единицей и обозначим через $\bar{G}$ мультипликативную полугруппу этого последнего кольца. Так как в $\bar{G}$ существует такой элемент 1, что из $a \neq b$ следует $1 \cdot a \neq 1 \cdot b$, то, почти дословно повторяя доказательство предшествующей теоремы, мы получим, что полугруппа $\bar{G}$ изоморфно вкладывается в симметрическую полугруппу на самом множестве $\bar{G}$. Этим достигается искомое вложение и для заданной полугруппы G.

Заметим, что возможность вложения любого группоида (и, в частности, любой полугруппы) в группоид (полугруппу) с единицей можно было бы доказать и непосредственно, без перехода к кольцам.

§ 5. Вложение полугрупп в группы и колец в тела

1. Не всякая полугруппа G может быть изоморфно вложена в какую-либо группу — необходимым условием для этого является выполнимость в G *закона сокращения* (см. II.1.3):

Из $ac = bc$, а также из $ca = cb$ следует $a = b$.

Пример полугруппы, не удовлетворяющей этому условию, построить очень легко.

Аналогично не всякое ассоциативное кольцо R может быть изоморфно вложено в какое-либо тело — для этого необходимо (см. II.2.10) отсутствие в R делителей нуля.

Указанные необходимые условия в общем случае вовсе не являются достаточными.

* Необходимые и достаточные условия для вложимости полугруппы в группу выражаются в виде бесконечного множества требований вида: «из данной системы равенств следует такое-то равенство»; они не могут быть записаны при помощи конечного числа таких требований [А. И. Мальцев, Мат. сб. **6** (1939), 331—336; **8** (1940), 251—264].

Существуют ассоциативные кольца без делителей нуля, которые не могут быть вложены в тело [А. И. Мальцев, Math. Ann. **113** (1937), 686—691]. *

2. Целью этого параграфа является доказательство того, что приведенные выше необходимые условия для вложимости полугруппы в группу и ассоциативного кольца в тело будут в коммутативном случае и достаточными. Начнем с доказательства следующего вспомогательного утверждения:

Пусть в абелевой полугруппе G выделена подполугруппа S, причем в G можно выполнять сокращение на элементы из S, т. е. из $ax=bx$, где $x\in S$, $a, b\in G$, всегда следует $a=b$. Тогда полугруппу G можно изоморфно вложить в такую абелеву полугруппу $\bar{G}$ с единицей, что всякий элемент из S обладает в $\bar{G}$ обратным элементом.

Рассмотрим множество всевозможных *дробей* вида $\frac{a}{x}$, где $a\in G$, $x\in S$, понимая под этим просто упорядоченную пару элементов a, x. Дроби $\frac{a}{x}$ и $\frac{b}{y}$ будем считать равными,

$$\frac{a}{x}=\frac{b}{y},$$

в том и только в том случае, если $ay=bx$. Это отношение равенства будет, очевидно, рефлексивным и симметричным. Оно и транзитивно, так как если также

$$\frac{b}{y}=\frac{c}{z},$$

т. е. $bz = cy$, то

$$ayz = bxz = cyx,$$

откуда, после сокращения на $y \in S$, получаем $az = cx$ или

$$\frac{a}{x} = \frac{c}{z}.$$

Таким образом (см. I. 3.2), все множество дробей распадается на непересекающиеся классы равных дробей. Множество этих классов обозначим через $\bar{G}$.

Определим *умножение дробей* равенством

$$\frac{a}{x} \cdot \frac{b}{y} = \frac{ab}{xy}. \tag{1}$$

Это определение имеет смысл, так как $xy \in S$.

Если

$$\frac{a}{x} = \frac{a_1}{x_1}, \quad \frac{b}{y} = \frac{b_1}{y_1}, \tag{2}$$

т. е.

$$ax_1 = a_1x, \quad by_1 = b_1y, \tag{3}$$

то

$$abx_1y_1 = a_1b_1xy,$$

откуда

$$\frac{ab}{xy} = \frac{a_1b_1}{x_1y_1}.$$

Таким образом, заменяя в левой части равенства (1) множители равными им дробями, мы получим произведение, равное правой части равенства (1).

Это позволяет рассматривать равенство (1) как определение умножения классов равных дробей. Ассоциативность и коммутативность этого умножения очевидны, а поэтому $\bar{G}$ превращено нами в абелеву полугруппу.

Все дроби вида $\frac{z}{z}$, $z \in S$, равны между собой. С другой стороны, если

$$\frac{a}{x} = \frac{z}{z},$$

то $az = zx$, т. е., после сокращения на z, $a = x$. Дроби вида $\frac{z}{z}$ составляют, следовательно, отдельный класс. Этот класс

играет роль единицы полугруппы $\bar{G}$. Действительно, так как дроби можно *сокращать* на общий множитель, принадлежащий к S:

$$\frac{az}{xz} = \frac{a}{x}, \quad z \in S,$$

ввиду $(az)x = a(xz)$, то

$$\frac{a}{x} \cdot \frac{z}{z} = \frac{az}{xz} = \frac{a}{x}.$$

Если a — фиксированный элемент из G, то все дроби вида $\frac{ax}{x}$ равны между собой: из $(ax)y = (ay)x$ следует

$$\frac{ax}{x} = \frac{ay}{y}.$$

С другой стороны, если

$$\frac{ax}{x} = \frac{b}{y},$$

то $axy = bx$, т. е. $b = ay$. Наконец, если

$$\frac{ax}{x} = \frac{by}{y},$$

то $axy = byx$, откуда $a = b$. Таким образом, ставя в соответствие каждому элементу a из G класс равных между собою дробей вида $\frac{ax}{x}$, мы получаем взаимно однозначное отображение полугруппы G в полугруппу $\bar{G}$. Изоморфность этого отображения вытекает из равенства

$$\frac{ax}{x} \cdot \frac{by}{y} = \frac{(ab)(xy)}{xy}.$$

Для завершения доказательства заметим, что элементу $z \in S$ соответствует класс дробей вида $\frac{zy}{y}$. Существование в полугруппе $\bar{G}$ обратного элемента для этого класса вытекает из следующего замечания:

Класс дробей, равных дроби $\frac{x}{y}$, *где* $x, y \in S$, *обладает в полугруппе* $\bar{G}$ *обратным элементом. Им служит класс дробей, равных дроби* $\frac{y}{x}$.

Действительно,

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{yx} = \frac{t}{t}, \quad t \in S.$$

3. Из доказанного выше утверждения и последнего замечания предшествующего пункта вытекает теорема (случай $S = G$):

Всякая абелева полугруппа с законом сокращения может быть изоморфно вложена в абелеву группу.

Так, применяя изложенную конструкцию к аддитивной полугруппе натуральных чисел, являющейся абелевой полугруппой с законом сокращения, читатель получит обычное вложение этой полугруппы в аддитивную группу целых чисел.

4. *Пусть в ассоциативно-коммутативном кольце R выделено множество N элементов, отличных от нуля и не являющихся делителями нуля. Тогда кольцо R можно изоморфно вложить в такое ассоциативно-коммутативное кольцо $\bar{R}$ с единицей, что всякий элемент из N обладает в $\bar{R}$ обратным элементом.*

Заметим сперва, что подполугруппа S мультипликативной полугруппы кольца R, порожденная множеством N (см. II. 3. 7), также не содержит ни нуля, ни делителей нуля. Действительно, S состоит из всевозможных произведений элементов из N. Однако, если $a \neq 0$, $b \neq 0$ и оба эти элемента не являются делителями нуля, то $ab \neq 0$ и из $(ab)c = 0$ следует $bc = 0$ и поэтому $c = 0$.

Таким образом, в мультипликативной полугруппе кольца R можно выполнять сокращение на элементы из S, а поэтому по II.5.2 эта полугруппа вкладывается в такую коммутативную полугруппу $\bar{R}$ с единицей, в которой всякий элемент из S и, в частности, из N обладает обратным элементом. Будем считать, что полугруппа $\bar{R}$ получена конструкцией, указанной в II.5.2.

Желая превратить $\bar{R}$ в кольцо, определим *сложение дробей* вида $\frac{a}{x}$, $a \in R$, $x \in S$, равенством

$$\frac{a}{x} + \frac{b}{y} = \frac{ay + bx}{xy}. \tag{4}$$

Это определение имеет смысл, так как $xy \in S$.

Если имеют место равенства (2) и поэтому (3), то

$$(ay + bx)\, x_1 y_1 = ayx_1y_1 + bxx_1y_1 = a_1xyy_1 + b_1yxx_1 =$$

$$= (a_1y_1 + b_1x_1)\, xy,$$

т. е.

$$\frac{ay+bx}{xy} = \frac{a_1y_1+b_1x_1}{x_1y_1}.$$

Таким образом, равенство (4) можно рассматривать как определение сложения классов равных дробей, т. е. сложения в $\bar{R}$. Коммутативность этого сложения очевидна, а ассоциативность легко проверяется на основании (4).

Все дроби вида $\frac{0}{z}$ равны между собою и составляют полный класс равных дробей. Этот класс играет в $\bar{R}$ роль нуля, так как

$$\frac{a}{x} + \frac{0}{z} = \frac{az}{xz} = \frac{a}{x}.$$

Далее, всякий элемент из $\bar{R}$ обладает противоположным элементом, так как

$$\frac{a}{x} + \frac{(-a)}{x} = \frac{ax+(-a)x}{x^2} = \frac{0}{x^2}.$$

Мы получаем, следовательно, что $\bar{R}$ будет по сложению абелевой группой.

Сложение и умножение связаны в $\bar{R}$ законом дистрибутивности:

$$\frac{a}{x}\cdot\frac{c}{z} + \frac{b}{y}\cdot\frac{c}{z} = \frac{ac}{xz} + \frac{bc}{yz} = \frac{acyz+bcxz}{xyz^2} = \frac{acy+bcx}{xyz} =$$

$$= \frac{ay+bx}{xy}\cdot\frac{c}{z} = \left(\frac{a}{x}+\frac{b}{y}\right)\cdot\frac{c}{z}.$$

Таким образом, $\bar{R}$ оказывается ассоциативно-коммутативным кольцом. Как мы знаем, отображение, переводящее каждый элемент $a \in R$ в класс равных между собою дробей вида $\frac{ax}{x}$, изоморфно по умножению. Оно изоморфно и по сложению, как показывает равенство

$$\frac{ax}{x} + \frac{by}{y} = \frac{axy+byx}{xy} = \frac{(a+b)xy}{xy}.$$

Доказательство теоремы закончено. Кольцо $\bar{R}$, построенное нами, называется *кольцом дробей* кольца R по множеству неделителей нуля N (или по мультипликативной полугруппе неделителей нуля S). Как мы знаем из II.5.2, *в кольце дробей $\bar{R}$ обратными элементами обладают не только*

все элементы из S, но и вообще все элементы, представимые дробями вида $\frac{x}{y}$, где $x, y \in S$.

5. Применим полученные результаты к случаю, когда R является областью целостности (см. II. 2.7). В этом случае можно положить $N = R \setminus 0$, причем $S = N$. Мы приходим к очень важной теореме:

Всякая область целостности R изоморфно вкладывается в поле.

Действительно, в этом случае в виде $\frac{x}{y}$, где $x, y \in S$, записывается всякий элемент из $\bar{R}$, отличный от нуля, т. е. всякий такой элемент обладает в $\bar{R}$ обратным элементом. Кольцо $\bar{R}$ будет, следовательно, полем; это — *поле дробей* области целостности R.

* Пусть ассоциативное кольцо R без делителей нуля удовлетворяет следующему условию, в коммутативном случае всегда выполняющемуся: для любых элементов a и b из R, отличных от нуля, в R можно найти такие отличные от нуля элементы x и y, что $ax = by$. Тогда R изоморфно вкладывается в тело [Орэ, Ann. of Math. **32** (1931), 463—477]. *

6. Установленная выше теорема существования поля дробей дополняется следующей теоремой единственности:

Пусть R — область целостности, $\bar{R}$ — ее поле дробей; пусть, с другой стороны, R является подкольцом некоторого поля P, причем подполе поля P, порожденное множеством R, совпадает с самим P. Тогда между $\bar{R}$ и P существует изоморфное соответствие φ, тождественно отображающее кольцо R на себя, причем это соответствие φ однозначно определено.

Условимся элемент a кольца R, рассматриваемый как элемент поля P, обозначить через a'. Таким образом, соответствие $a \to a'$ есть тождественное отображение кольца R на себя.

Докажем сначала, что если изоморфное отображение φ поля $\bar{R}$ на поле P, тождественное на R, существует, то оно однозначно определено. Действительно, если $\frac{a}{b}$ — произвольная дробь, то из

$$b \cdot \frac{a}{b} = a$$

следует

$$b\varphi \cdot \left(\frac{a}{b}\right)\varphi = a\varphi,$$

т. е., ввиду $a\varphi = a'$, $b\varphi = b'$,

$$b' \cdot \left(\frac{a}{b}\right)\varphi = a'.$$

Таким образом, изоморфизм φ переводит элемент $\frac{a}{b}$ поля $\bar{R}$ в частное элементов a' и b' поля P и поэтому определен однозначно.

Переходим к доказательству основного утверждения теоремы. Поставим в соответствие элементу $\frac{a}{b}$ поля $\bar{R}$ частное $\frac{a'}{b'}$ элементов a' и b' поля P, причем положим $\frac{a'}{b'} = \left(\frac{a}{b}\right)\varphi$. Если $\frac{a}{b} = \frac{c}{d}$, т. е. $ad = bc$, то в P справедливо равенство $a'd' = b'c'$, а поэтому, ввиду равенства $b' \cdot \frac{a'}{b'} = a'$, будет

$$b'd' \cdot \frac{a'}{b'} = a'd' = b'c',$$

откуда

$$d' \cdot \frac{a'}{b'} = c',$$

т. е. $\frac{a'}{b'} = \frac{c'}{d'}$. Отображение φ не зависит, следовательно, от выбора записи элемента поля $\bar{R}$ в виде дроби, т. е. является однозначным отображением поля $\bar{R}$ в поле P. Оно будет даже взаимно однозначным отображением, так как если в поле P имеет место равенство $\frac{a'}{b'} = \frac{c'}{d'}$, то $a'd' = b'c'$, а поэтому в кольце R будет $ad = bc$, откуда в поле $\bar{R}$ вытекает равенство $\frac{a}{b} = \frac{c}{d}$.

Изоморфность отображения φ следует из того, что равенства (1) и (4), определяющие умножение и сложение дробей, заведомо справедливы для частных в произвольном поле P.

Мы получили изоморфное отображение поля дробей $\bar{R}$ в поле P. Оно будет тождественным на кольце R, так как для любого $a \in R$

$$\left(\frac{ab}{b}\right)\varphi = \frac{a'b'}{b'} = a' \in P.$$

Наконец, мы знаем, что изоморфным образом поля всегда является поле. Следовательно, те элементы поля P, которые записываются в виде частных элементов из R, составляют в поле P подполе, содержащее все кольцо R и поэтому, по условию теоремы, совпадающее с P. Нами построено, следовательно, изморфное отображение φ поля $\bar{R}$ на все поле P, тождественное на R.

7. Полем дробей для кольца целых чисел служит поле рациональных чисел.

Если P — произвольное поле, то кольцо многочленов $P[x]$ является областью целостности (см. II.2.7) и поэтому вкладывается в поле дробей. Это поле обозначается через $P(x)$ и называется *полем рациональных дробей* от неизвестного x над полем P. Его элементы имеют вид дробей $\frac{f(x)}{g(x)}$, где $f(x)$ и $g(x)$ — многочлены из $P[x]$, причем $g(x) \neq 0$, а равенство этих дробей и операции над ними определяются в соответствии с II. 5.2 и II. 5.4.

Аналогичный смысл имеет понятие поля рациональных дробей $P(x_1, x_2, \ldots, x_n)$ от нескольких неизвестных.

* Поле дробей для кольца степенных рядов $P\{x\}$ над полем P (см. II. 2.8) изоморфно *полю «лорановых» степенных рядов* над P, т. е. рядов вида

$$a_n x^n + a_{n+1} x^{n+1} + \ldots, \tag{5}$$

где n может быть больше, равно или меньше нуля, а все коэффициенты принадлежат к P; ряд (5) в общем случае содержит, следовательно, конечное число членов с отрицательными степенями неизвестного x и бесконечно много членов с его положительными степенями. Операции над этими рядами выполняются по правилам, естественно обобщающим правила операций в кольце $P\{x\}$. *

§ 6. Неассоциативные тела, квазигруппы. Изотопия

1. Понятие тела можно перенести на неассоциативный случай несколькими неэквивалентными способами. Так, можно рассматривать такие кольца, в которых для любых элементов a и b, где $a \neq 0$, уравнения

$$ax = b, \quad ya = b \tag{1}$$

обладают решениями, не обязательно однозначно определенными. Всякое такое кольцо мы будем называть *кольцом с делением*; из нашего определения вытекает, что кольцо с делением может обладать делителями нуля.

Кольцо с делением, в котором уравнения (1) обладают однозначными решениями, назовем *квазителом*. Делителей нуля квазитело содержать не может, и поэтому отличные от нуля элементы квазитела составляют по умножению группоид. Это будет *квазигруппа*, т. е. группоид, в котором для любых элементов a и b однозначно разрешимы уравнения (1).

Наконец, термин *тело* мы сохраним для квазитела, обладающего единицей. Отличные от нуля элементы тела составляют по умножению квазигруппу с единицей, т. е. *лупу*.

* Всякое (не обязательно ассоциативное) кольцо без делителей нуля вкладывается в квазитело [Б. Нейман, Proc. London Math. Soc. **1** (1951), 241 — 256]. *

2. Существуют квазитела, на являющиеся телами, и квазигруппы, не являющиеся лупами. Дело в том, что хотя в квазигруппе G для всякого элемента a уравнения

$$ax = a, \qquad ya = a \tag{2}$$

однозначно разрешимы, но эти решения не обязаны совпадать и не обязаны служить соответственно правой или левой единицей для других элементов из G.

Всякое подквазигруппа A лупы G с единицей e является подлупой с той же единицей e.

Действительно, для всякого $a \in A$ уравнения (2) обладают в G единственным решением e, которое должно, следовательно, содержаться в подквазигруппе A.

3. На квазигруппы и в особенности на лупы переносится ряд результатов, относящихся к группам. Мы не будем этого дальше касаться и введем лишь одно обобщение понятия изоморфизма, играющее в теории квазигрупп заметную роль.

Пусть дан группоид G с умножением $a \cdot b$ и пусть φ, ψ и χ — произвольные взаимно однозначные отображения множества G на себя, не обязательно различные. Мы получим на множестве G новый группоид, если для любых $a, b \in G$ положим

$$a \circ b = (a\varphi \cdot b\psi)\chi. \tag{3}$$

Этот новый группоид не обязан быть изоморфным старому, но в какой-то мере они близки.

В соответствии с этим группоид G с умножением $a \circ b$ называется *изотопным* группоиду G' с умножением $a' \cdot b'$, если существуют такие три взаимно однозначных отображения φ, ψ и χ^{-1} G на G', что для любых a, $b \in G$

$$(a \circ b)\chi^{-1} = a\varphi \cdot b\psi. \tag{4}$$

Ясно, что *при* $\varphi = \psi = \chi^{-1}$ *мы получаем изоморфное отображение* G *на* G'.

Легко проверяется, что отношение изотопии рефлексивно, транзитивно и симметрично.

Во многих случаях удобно считать, что обе операции, $a \circ b$ и $a \cdot b$, заданы на одном и том же множестве G и что φ, ψ и χ, входящие в (3) или (4), являются некоторыми взаимно однозначными отображениями этого множества на себя.

4. *Всякий группоид, изотопный квазигруппе, сам является квазигруппой.*

В самом деле, пусть на множестве G заданы группоид с умножением $a \circ b$ и квазигруппа с умножением $a \cdot b$, причем они изотопны, т. е. имеет место (3). Докажем, что, например, уравнение

$$a \circ x = b \tag{5}$$

имеет однозначное решение для любых a, $b \in G$. Мы знаем, что уравнение

$$a\varphi \cdot y = b\chi^{-1}$$

обладает однозначно определенным решением c. Положим $x = c\psi^{-1}$. Тогда

$$a \circ x = a \circ c\psi^{-1} = (a\varphi \cdot c)\chi = (b\chi^{-1})\chi = b.$$

С другой стороны, если x' — любое решение уравнения (5), то

$$a\varphi \cdot x'\psi = b\chi^{-1},$$

откуда $x'\psi = c$, т. е. $x' = c\psi^{-1}$.

5. *Всякая квазигруппа изотопна лупе* [А л б е р т, Trans. Amer. Math. Soc. **54** (1943), 507 — 519].

Действительно, фиксируем в квазигруппе G с умножением $a \cdot b$ произвольный элемент e. Тогда в G существует такой

элемент f, что

$$e \cdot f = e. \tag{6}$$

Пусть a — произвольный элемент из G. Обозначим через $a\varphi$ и $a\psi$ такие однозначно определенные элементы, что

$$a\varphi \cdot f = a, \qquad e \cdot a\psi = a. \tag{7}$$

Отображения $a \to a\varphi$ и $a \to a\psi$, где a пробегает все множество G, будут взаимно однозначными отображениями G на себя. Так, если $a\varphi = b\varphi$, то $a\varphi \cdot f = b\varphi \cdot f$, т. е. $a = b$. С другой стороны, если c — произвольный элемент из G, то

$$c = (c \cdot f)\varphi.$$

Отсюда следует, что, полагая для всех a, $b \in G$

$$a \circ b = a\varphi \cdot b\psi, \tag{8}$$

мы определим на G новый группоид, изотопный с исходной квазигруппой; роль χ здесь играет тождественное отображение, т. е. это будет, как говорят, *главный изотоп*. Ввиду доказанного в предшествующем пункте полученный группоид будет сам квазигруппой. Он будет даже лупой, так как единицей для него служит элемент e. В самом деле, так как по (6) и (7)

$$e\varphi = e, \quad e\psi = f,$$

то, ввиду (8) и (7),

$$a \circ e = a\varphi \cdot f = a,$$

$$e \circ a = e \cdot a\psi = a.$$

Теорема доказана.

6. *Если группоид с единицей изотопен полугруппе, то они изоморфны и поэтому оба ассоциативны и оба обладают единицей* [Брак, Trans. Amer. Math. Soc. **60** (1946), 245 — 354; Хьюз, J. London Math. Soc. **32** (1957), 510 — 511].

Действительно, пусть на множестве G заданы группоид с умножением $a \cdot b$, обладающий единицей e, и полугруппа с умножением $a \circ b$, причем они изотопны,

$$a \circ b = (a\varphi \cdot b\psi)\chi,$$

где φ, ψ, χ — взаимно однозначные отображения множества G на себя. Так как для любых a, b, $c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c),$$

то

$$[(a\varphi \cdot b\psi)\chi\varphi \cdot c\psi]\chi = [a\varphi \cdot (b\varphi \cdot c\psi)\chi\psi]\chi,$$

откуда

$$(a\varphi \cdot b\psi)\chi\varphi \cdot c\psi = a\varphi \cdot (b\varphi \cdot c\psi)\chi\psi. \tag{9}$$

Полагая в этом равенстве $a\varphi = c\psi = e$, мы для всех $b \in G$ получаем

$$b\psi\chi\varphi = b\varphi\chi\psi. \tag{10}$$

Полагая в (9), далее, $a\varphi = e$ и используя (10), получаем

$$b\varphi\chi\psi \cdot c\psi = (b\varphi \cdot c\psi)\chi\psi$$

или, заменяя $b\varphi$ на a и $c\psi$ на b,

$$a\chi\psi \cdot b = (a \cdot b)\chi\psi \tag{11}$$

для всех a, $b \in G$. Наконец, полагая в (9) $c\psi = e$ и используя (10), получаем

$$(a\varphi \cdot b\psi)\chi\varphi = a\varphi \cdot b\psi\chi\varphi$$

или, заменяя $a\varphi$ на a и $b\psi$ на b,

$$(a \cdot b)\chi\varphi = a \cdot b\chi\varphi \tag{12}$$

для всех a, $b \in G$.

Используя (11), (12) и (10), мы приходим к следующему равенству: для любых a, $b \in G$

$$(a \circ b)\psi\chi\varphi = (a\varphi \cdot b\psi)\chi\psi\chi\varphi = (a\varphi\chi\psi \cdot b\psi)\chi\varphi = a\psi\chi\varphi \cdot b\psi\chi\varphi.$$

Это равенство показывает, что произведение $\psi\chi\varphi$, являющееся взаимно однозначным отображением множества G на себя, будет изоморфизмом между заданными полугруппой и группоидом. Теорема доказана.

Из этой теоремы вытекает теорема Алберта (Trans. Amer. Math. Soc. **54** (1943), 507—519): *Если лупа изотопна группе, то они изоморфны.* Отсюда, в частности, следует, что изотопные группы всегда изоморфны, и поэтому для применения изотопии в теории групп нет оснований.

7. Понятие изотопии можно перенести в теорию неассоциативных колец. Именно, рассматривая кольца с одной и той же аддитивной группой G, определим *изотопию колец* равенством (3), как и выше, но будем считать, что отображения φ, ψ и χ являются изоморфными отобра-

жениями группы G на себя (т. е. ее автоморфизмами в смысле III. 3.1). Из результатов, полученных выше, и методов, использованных при их доказательстве, вытекают теперь следующие результаты:

Всякое кольцо, изотопное квазителу, само является квазителом.

В самом деле, пусть на аддитивной абелевой группе G заданы кольцо с умножением $a \circ b$ и изотопное ему квазитело с умножением $a \cdot b$. Если $a \circ b = 0$, то

$$(a\varphi \cdot b\psi)\chi = 0,$$

а так как при изоморфизме χ группы G нуль остается на месте, то

$$a\varphi \cdot b\psi = 0.$$

Поэтому один из сомножителей равен нулю, например $a\varphi = 0$, откуда $a = 0$, т. е. заданное кольцо не содержит делителей нуля. Таким образом, на множестве $G \setminus 0$ заданы группоид и квазигруппа, а так как отображения φ, ψ и χ можно рассматривать как взаимно однозначные отображения этого множества на себя, то остается применить II. 6.4.

Всякое квазитело изотопно (неассоциативному) телу.

В самом деле, если дано квазитело K с умножением $a \cdot b$, то, по II. 6.5, мультипликативная квазигруппа его отличных от нуля элементов изотопна лупе с умножением $a \circ b$, определенным равенством (8), где взаимно однозначные отображения φ и ψ множества $K \setminus 0$ определяются равенствами (7). Дополнительно положим $0\varphi = 0\psi = 0$, что согласуется с (7), и докажем, что φ и ψ являются теперь изоморфными отображениями аддитивной группы тела K на себя. Так, из

$$(a\varphi + b\varphi) \cdot f = a\varphi \cdot f + b\varphi \cdot f = a + b$$

следует

$$(a + b)\varphi = a\varphi + b\varphi.$$

Полагая дополнительно $a \circ 0 = 0 \circ a = 0$ для всех $a \in K$, определяем умножение $\circ$ для всех элементов из K, причем единица e построенной выше лупы будет единицей и для этого умножения. Остается доказать дистрибутивность этого умножения относительно сложения. Так, по (8),

$$(a + b) \circ c = (a + b)\varphi \cdot c\psi = (a\varphi + b\varphi) \cdot c\psi =$$
$$= a\varphi \cdot c\psi + b\varphi \cdot c\psi = a \circ c + b \circ c.$$

Теорема доказана.

Если кольцо с единицей изотопно ассоциативному кольцу, то они изоморфны.

Действительно, пусть на аддитивной абелевой группе G заданы кольцо с умножением $a \cdot b$, обладающее единицей e, и ассоциативное кольцо с умножением $a \circ b$, причем для любых a, $b \in G$ имеет место равенство (3), где φ, ψ и χ — изоморфные отображения группы G на себя. Тогда произведение $\psi\chi\varphi$, являющееся, очевидно, изоморфным отображением группы G на себя, будет, в силу доказанного в II. 6.6, изоморфизмом между заданными кольцами.

* Ассоциативное кольцо с единицей может обладать неассоциативным изотопом. Существуют ассоциативные кольца без единицы, между собою изотопные, но не изоморфные [Альберт, Ann. of Math. **43** (1942), 685—707]. *

§ 7. Нормальные делители, идеалы

1. Пусть дана группа G и в ней подгруппа H. Если a — произвольный элемент из G, то совокупность aH всевозможных произведений вида ah, где h пробегает подгруппу H, называется *левым смежным классом* группы G по подгруппе H, определяемым элементом a. Ясно, что $a \in aH$, так как подгруппа H содержит единицу.

Если элемент b содержится в классе aH, то $bH = aH$, т. е. *всякий левый смежный класс группы G по подгруппе H определяется любым из своих элементов.* Действительно, если $b = ah_0$, $h_0 \in H$, то для любых h', $h'' \in H$

$$bh' = a(h_0h') \text{ и } ah'' = b(h_0^{-1}h''),$$

т. е. $bH \subseteq aH$ и $aH \subseteq bH$.

Отсюда следует, что *два любых левых смежных класса группы G по подгруппе H или совпадают, или же имеют пустое пересечение.* Мы получаем разбиение группы G на непересекающиеся левые смежные классы по подгруппе H. Оно называется *левосторонним разложением* группы G по подгруппе H. Одним из классов этого разложения будет сама подгруппа H: если $a \in H$, то $aH = H$.

2. Аналогичным путем можно получить *правостороннее разложение* группы G по подгруппе H, составленное из *правых смежных классов* Ha, $a \in G$. В некоммутативном случае правостороннее разложение G по H действительно мо-

жет отличаться от левостороннего. Эти оба разложения состоят, однако, из одного и того же числа классов: отображение, переводящее каждый элемент a группы G в элемент a^{-1}, является взаимно однозначным отображением G на себя, переводящим всякий левый смежный класс aH в правый смежный класс Ha^{-1} и обратно.

Число смежных классов в любом из двух разложений группы G по подгруппе H, если оно конечно, называется *индексом* подгруппы H в группе G.

3. Если G — конечная группа порядка n, а H — ее подгруппа порядка k и индекса j, то всякий смежный класс aH состоит ровно из k элементов, а поэтому

$$n = kj.$$

Отсюда вытекает

Теорема Лагранжа. *Порядок и индекс любой подгруппы конечной группы являются делителями порядка самой группы.*

Из этой теоремы следует, ввиду II. 3.4, что *порядок любого элемента конечной группы является делителем порядка группы.* Из теоремы Лагранжа следует также, что *всякая конечная группа, порядок которой является простым числом, будет циклической.* Действительно, эта группа должна совпадать с циклической подгруппой, порожденной любым ее элементом, отличным от 1.

4. Подгруппа H называется *нормальным делителем* (или *инвариантной подгруппой*) группы G, если левостороннее разложение группы G по подгруппе H совпадает с правосторонним, т. е. если для любого $a \in G$ имеет место равенство (понимаемое в смысле совпадения обоих подмножеств в G)

$$aH = Ha. \tag{1}$$

Можно говорить, следовательно, просто о *разложении группы G по нормальному делителю H.*

Укажем некоторые другие определения нормального делителя, равносильные приведенному выше.

Элементы x и y группы G называются *сопряженными* в G, если в G можно найти такой элемент a, что

$$y = a^{-1}xa,$$

т. е. y получается из x *трансформированием* элементом a.

Подгруппа H группы G тогда и только тогда будет нормальным делителем в G, если H вместе со всяким своим элементом содержит и все элементы, сопряженные с ним в G.

Действительно, если H — нормальный делитель в G, h — любой элемент из H, a — любой элемент из G, то, по (1), в H существует такой элемент h', что

$$ah' = ha, \tag{2}$$

откуда

$$a^{-1}ha = h' \in H. \tag{3}$$

Обратно, если для любых $h \in H$ и $a \in G$ в H существует элемент h', удовлетворяющий равенствам (3) и поэтому (2), то $Ha \subseteq aH$. Это включение справедливо при всех a, в частности при a^{-1}, т. е. $Ha^{-1} \subseteq a^{-1}H$, откуда следует $aH \subseteq Ha$, а поэтому на самом деле имеет место равенство (1).

Подгруппы U и V группы G называются *сопряженными* в G, если в G существует такой элемент a, трансформирование которым подгруппы U переводит ее в V, т. е.

$$a^{-1}Ua = V.$$

Заметим, что множество $a^{-1}Ua$ при любой подгруппе U и любом $a \in G$ будет подгруппой, притом изоморфной с U.

Действительно, если $u_1, u_2 \in U$, то

$$(a^{-1}u_1a)(a^{-1}u_2a) = a^{-1}(u_1u_2)a;$$

с другой стороны, из

$$a^{-1}u_1a = a^{-1}u_2a$$

следует $u_1 = u_2$, а поэтому отображение $u \to a^{-1}ua$, $u \in U$, будет изоморфным отображением U на $a^{-1}Ua$ и, следовательно, $a^{-1}Ua$ является подгруппой.

Всякий нормальный делитель группы G совпадает со всеми подгруппами, сопряженными с ним в G. Обратно, если подгруппа H группы G содержит все подгруппы, сопряженные с нею в G, то она будет нормальным делителем.

В самом деле, из (1) вытекает равенство

$$a\,^{1}Ha = H, \tag{4}$$

что доказывает первое утверждение теоремы. С другой стороны, если

$$a^{-1}Ha \subset H,$$

причем включение строгое, то

$$H \subset aHa^{-1} = (a^{-1})^{-1} Ha^{-1}.$$

Таким образом, если подгруппа H должна содержать *все* подгруппы, с нею сопряженные, то она непременно совпадает с ними, т. е. при любом $a \in G$ имеет место равенство (4), а поэтому и вытекающее из него равенство (1).

5. *Пересечение любого множества нормальных делителей группы G само является нормальным делителем в G.*

Действительно, если D есть пересечение нормальных делителей A_i, $i \in I$, то D будет подгруппой в G (см. II. 3.6), и, кроме того, всякий элемент, сопряженный с элементом из D, содержится в каждом из нормальных делителей A_i и поэтому принадлежит к D.

Подгруппа, порожденная любой системой нормальных делителей группы G (см. II. 3.8), *сама будет нормальным делителем в G.*

Пусть, в самом деле, заданы нормальные делители A_i, $i \in I$, и пусть B будет подгруппа, ими порожденная. Как указано в II. 3.7, всякий элемент b из B может быть записан в виде

$$b = a_1 a_2 \ldots a_n,$$

где $a_j \in A_{i_j}$, $j = 1, 2, \ldots, n$. Если g — любой элемент из G, то

$$g^{-1}bg = (g^{-1}a_1 g)(g^{-1}a_2 g) \ldots (g^{-1}a_n g),$$

а так как

$$g^{-1}a_j g \in A_{i_j},\ j = 1, 2, \ldots, n,$$

то

$$g^{-1}bg \in B.$$

6. Все подгруппы абелевой группы будут в ней, конечно, нормальными делителями. С другой стороны, для всякой группы G нормальными делителями служат единичная подгруппа E и сама группа G. Группа, не имеющая нормальных делителей, отличных от нее самой и от E, называется *простой*.

Простыми абелевыми группами являются конечные циклические группы простых порядков и только они.

Действительно, если абелева группа G простая, то она вообще не содержит нетривиальных подгрупп, а так как циклические подгруппы в ней должны существовать, то она сама будет циклической. Бесконечная циклическая группа обладает, однако, нетривиальными подгруппами — в аддитивной группе целых чисел содержится в качестве истинной подгруппы группа четных чисел. Далее, если группа $G=\{a\}$ — циклическая конечного порядка n, то при составном числе n, $n=kl$, подгруппа $\{a^k\}$ будет иметь порядок l, т. е. отлична и от G, и от E. Если же, однако, группа $G=\{a\}$ имеет простой порядок p, то она не может иметь нетривиальных подгрупп, как вытекает из теоремы Лагранжа.

7. Существуют и некоммутативные простые группы, как конечные, так и бесконечные. Рассмотрим, например, в симметрической группе n-й степени S_n (см. II.1.8) подмножество A_n четных подстановок. Как доказывается в учебниках по высшей алгебре, четность подстановки n-й степени совпадает с четностью числа сомножителей в любом разложении этой подстановки в произведение транспозиций. Отсюда вытекает, что произведение четных подстановок n-й степени всегда четно, а так как подстановка, обратная к четной, сама четная, то мы получаем, что A_n *будет подгруппой группы* S_n.

Группа A_n называется *знакопеременной группой n-й степени* и имеет порядок $\frac{1}{2}n!$. Заметим, что она будет в S_n не только подгруппой, но даже нормальным делителем: индекс A_n в S_n равен двум, причем оба разложения группы S_n по подгруппе A_n совпадают, состоя из двух классов — сама подгруппа A_n и класс нечетных подстановок.

Группа A_3 имеет порядок 3 и поэтому является циклической группой простого порядка, т. е. простой. Группа A_4 не будет простой — легко проверяется, что четные подстановки [1])

$$(12)(34),\ (13)(24),\ (14)(23)$$

---

[1]) Напомним, что при записи подстановки через циклы за каждым символом пишется тот символ, в который он переходит при рассматриваемой подстановке. Цикл закрывается, когда мы доходим до

составляют вместе с единицей нормальный делитель этой группы.

Знакопеременная группа n-й степени A_n является при $n \geqslant 5$ простой.

Покажем сперва, что циклы (ijk) длины 3, являющиеся, как легко видеть, четными подстановками, составляют для группы A_n систему образующих (см. II. 3.9). Действительно, всякая четная подстановка разлагается в произведение четного числа транспозиций, а поэтому и в произведение циклов длины 3, так как

$$(ij)(ik) = (ijk),$$

$$(ij)(kl) = (ijk)(ilk).$$

Докажем, далее, что всякий нормальный делитель H группы A_n, содержащий хотя бы один цикл (ijk) длины 3, содержит и любой другой цикл $(i'j'k')$ длины 3 и поэтому, как показано выше, совпадает с A_n. Действительно, если символы l и m отличны от i, j и k, то подстановка n-й степени

$$\alpha = \begin{pmatrix} i & j & k & l & m & \dots \\ i' & j' & k' & l' & m' & \dots \end{pmatrix},$$

которую можно сделать четной, транспонируя, если нужно, символы l' и m' в нижней строке, такова, что

$$\alpha^{-1}(ijk)\alpha = (i'j'k').$$

Остается показать, что всякий нормальный делитель H группы A_n, $n \geqslant 5$, отличный от E, со-

---

символа, переходящего в первый символ цикла. Символы, остающиеся при нашей подстановке на месте, при разложении в циклы опускаются. Так,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix} = (143)(26).$$

С другой стороны,

$$(12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

если, конечно, известно, что это подстановка 4-й степени. Напомним также, что четность подстановки совпадает с четностью разности между числом символов, действительно переставляемых этой подстановкой, и числом циклов в ее разложении.

держит хотя бы один цикл длины 3. Возьмем в H такой отличный от 1 элемент α, который оставляет неподвижными возможно больше символов. Если подстановка α не является циклом длины 3, то она будет иметь один из следующих двух видов:

1) Разложение α в циклы содержит хотя бы один цикл, длина которого не меньше трех:

$$\alpha = (ijk \ldots) \ldots$$

При этом α, будучи четной подстановкой, не может быть циклом $(ijkl)$ длины 4, а поэтому α перемещает по меньшей мере два символа, отличных от i, j и k; пусть это будут l и m.

2) Подстановка α разлагается в произведение независимых циклов длины 2, которых будет не меньше двух:

$$\alpha = (ij)(kl) \ldots$$

В этом случае, так как $n \geqslant 5$, существует символ m, отличный от i, j, k и l.

Пусть $\beta = (klm)$. Тогда $\beta^{-1}\alpha\beta \in H$, так как $\beta \in A_n$, и поэтому

$$\gamma = \beta^{-1}\alpha\beta\alpha^{-1} \in H.$$

Подстановка γ отлична от 1, так как в случае 1) подстановка $\beta^{-1}\alpha\beta$ переводит символ j не в символ k, как это делает α, а в символ l; в случае же 2) подстановка $\beta^{-1}\alpha\beta$ переводит символ l в символ m, а не в символ k, как это производится подстановкой α.

С другой стороны, подстановка γ оставляет на месте в первом случае все символы, оставляемые на месте подстановкой α, так как все они отличны от k, l и m, а во втором случае — все символы, остающиеся на месте при α, кроме, быть может, символа m. Легко проверяется, однако, что в первом случае подстановка γ дополнительно оставляет на месте символ i, а во втором случае — символы i и j. Таким образом, в обоих случаях при γ остается больше неподвижных символов, чем при α. Это противоречие с выбором подстановки α показывает, что α должно быть циклом длины 3, т. е. доказывает теорему.

Заметим, что знакопеременными группами A_n, $n \geqslant 5$, далеко не исчерпываются все конечные некоммутативные простые группы.

8. В следующей главе будет показано, что та роль, которую в теории групп играет понятие нормального делителя, в теории колец принадлежит понятию идеала.

Подмножество A произвольного кольца R называется *идеалом* в R, если оно является подгруппой аддитивной группы кольца R — для этого достаточно, чтобы разность любых двух элементов из A принадлежала к A — и если, кроме того, для любых элементов $a \in A$ и $r \in R$ оба произведения ar и ra содержатся в A.

Из этого определения следует, что всякий идеал кольца R будет в R подкольцом. Легко видеть, далее, что пересечение любой системы идеалов кольца R само будет идеалом. С другой стороны, *подгруппа аддитивной группы кольца R, порожденная данной системой идеалов A_i, $i \in I$, также будет идеалом*: эта подгруппа состоит из всевозможных конечных сумм элементов из идеалов A_i, но умножение такой суммы слева или справа на любой элемент кольца R снова приводит к сумме такого же вида.

В II. 4. 2 дано описание всех подгрупп аддитивной группы целых чисел. *Все эти подгруппы (включая нулевую) и, конечно, только они являются идеалами в кольце целых чисел*, так как произведение числа, кратного n, на любое целое число само кратно n.

9. Во всяком кольце R идеалами будут само R и *нуль-идеал* O, состоящий из одного нуля. Кольцо, не содержащее других идеалов, кроме этих двух, называется *простым*.

Всякое тело и вообще всякое кольцо с делением (см. II. 6.1) *является простым кольцом.*

Действительно, пусть дано кольцо с делением K. Если в нем задан идеал A, отличный от O, и если $a \in A$, $a \neq 0$, то, ввиду разрешимости в K уравнений (1) из II. 6.1, к A будет принадлежать любой элемент b из R, т. е. $A = R$.

Полное кольцо матриц K_n любого порядка n над любым кольцом с делением K является простым кольцом.

Пусть, в самом деле, в кольце K_n задан ненулевой идеал A. Если $\alpha = (a_{ij})$ — ненулевая матрица, принадлежащая к A, то пусть, например, $a_{kl} \neq 0$. Условимся обозначать через $\bar{x}_{ij}$ матрицу из K_n, у которой на месте (i, j) стоит элемент x из K, а все остальные места заняты нулями. Предположим, далее, что b — произвольный элемент из K, а s и t — произвольные индексы, $1 \leqslant s, t \leqslant n$. Ввиду разрешимости в K

уравнений (1) из II. 6.1 в K существуют такие элементы x и y, что

$$y(a_{kl}x) = b.$$

Применяя правило умножения матриц, получаем, что

$$\bar{y}_{sk}(\alpha\bar{x}_{lt}) = \bar{b}_{st}.$$

Таким образом, все матрицы вида $\bar{b}_{st}$ принадлежат к идеалу A, а так как всякая матрица из K_n представима в виде суммы матриц этого вида, то $A = K_n$, что и требовалось доказать.

10. Если в определении идеала отказаться от требования, что для любого a из идеала A и любого r из кольца R оба произведения ar и ra принадлежат к A, и требовать это лишь для произведения ar и л и произведения ra, то мы придем к понятию *одностороннего идеала*, а именно *правого идеала*, если $ar \in A$ для всех $a \in A$ и $r \in R$, и *левого идеала*, если $ra \in A$. В коммутативном случае, равно как и в антикоммутативном, в частности в лиевых и в йордановых кольцах (см. II.2.3 и II.2.4), всякий односторонний идеал будет, конечно, идеалом (или, как иногда говорят, *двусторонним идеалом*).

Так как в приведенном выше доказательстве простоты любого кольца с делением достаточно было использовать разрешимость лишь одного из уравнений (1) из II.6.1, то можно утверждать, что *никакое кольцо с делением K не содержит односторонних идеалов, отличных от K и O.*

Если ассоциативное кольцо R не содержит других односторонних идеалов, кроме R и O, и не является кольцом с нулевым умножением (см. II.2.2), *то оно будет телом.*

В самом деле, назовем *левым аннулятором* кольца R всякий такой элемент a, что $ar = 0$ для всех $r \in R$. Левые аннуляторы составляют в ассоциативном кольце R идеал, даже двусторонний. Этот идеал в нашем случае равен нулю — если бы он равнялся R, то кольцо R было бы нулевым. Таким образом, для любого ненулевого элемента a множество aR всевозможных произведений вида ar, $r \in R$, являющееся в ассоциативном кольце правым идеалом, будет отлично от O и поэтому $aR = R$. Отсюда следует, что для любого элемента $b \in R$ в R разрешимо уравнение $ax = b$. Аналогично доказывается разрешимость в R всякого уравнения вида $ya = b$, $a \neq 0$, а поэтому, по II.2.10, R будет телом.

Из сказанного легко вытекает, что *ненулевое ассоциативно-коммутативное кольцо будет простым тогда и только тогда, если оно является полем.* С другой стороны, так как в нулевом кольце всякая подгруппа аддитивной группы будет идеалом, то, ввиду II.7.6, *нулевые простые кольца исчерпываются нулевыми кольцами на циклических аддитивных группах простых порядков.*

11. Определения идеала и одностороннего идеала легко переносятся на случай любого группоида — достаточно исключить из этих определений упоминания об аддитивной группе. Всякий идеал, а также левый или правый идеал кольца будут, очевидно, соответственно идеалом, левым или правым идеалом мультипликативного группоида этого кольца. Обратное, однако, не имеет места: в кольце целых чисел совокупность чисел, кратных хотя бы одному из чисел 2 и 3, не будет идеалом, хотя и будет идеалом мультипликативной полугруппы этого кольца.

§ 8. Гауссовы полугруппы

1. Как известно, в кольце целых чисел C и в кольце многочленов $P[x]$ над любым полем P имеют место совершенно параллельные теории делимости. В настоящем и следующем параграфах будут установлены причины этого параллелизма.

Пусть дана абелева полугруппа G с единицей 1, удовлетворяющая закону сокращения (см. II.5.1). *Делители единицы этой полугруппы,* т. е. такие элементы ε, для которых в G существует обратный элемент ε^{-1},

$$\varepsilon\varepsilon^{-1} = 1,$$

составляют в ней подгруппу, так как и произведение делителей единицы, и элемент, обратный к делителю единицы, сами будут делителями единицы. С другой стороны, *если произведение элементов* $a_1, a_2, \ldots, a_n \in G$ *является делителем единицы,*

$$a_1 a_2 \ldots a_n = \varepsilon,$$

то каждый из элементов a_i, $i = 1, 2, \ldots, n$, *сам будет делителем единицы.* Действительно,

$$a_i^{-1} = a_1 \ldots a_{i-1} a_{i-1} \ldots a_n \varepsilon^{-1}, \quad i = 1, 2, \ldots, n.$$

2. Если элементы $a, b \in G$ таковы, что $a = bc$, то элемент b называется *делителем* элемента a; говорят также, что a *делится* на b. Элементы a и b называются *ассоциированными*, если каждый из них служит делителем для другого,

$$a = bc, \quad b = ad. \tag{1}$$

Так как из (1) следует

$$a = a(cd),$$

т. е., ввиду закона сокращения,

$$cd = 1,$$

то *и c и d будут делителями единицы.* С другой стороны, для любого делителя единицы ε *элементы a и εa ассоциированы между собой*, так как

$$a = \varepsilon^{-1}(\varepsilon a).$$

Отсюда же следует, что *всякий делитель единицы служит делителем для любого элемента полугруппы G.*

Отношение ассоциированности является, очевидно, отношением эквивалентности, и поэтому вся полугруппа G распадается на *классы ассоциированных элементов*; одним из этих классов будет группа делителей единицы. С другой стороны, отношение «b служит делителем для a» рефлексивно и транзитивно. Вместе с тем для любых делителей единицы ε_1 и ε_2 из

$$a = bc$$

следует

$$\varepsilon_1 a = (\varepsilon_2 b)(\varepsilon_1 \varepsilon_2^{-1} c),$$

т. е. $\varepsilon_2 b$ служит делителем для $\varepsilon_1 a$. Мы получим, таким образом, *частичную упорядоченность* в множестве классов ассоциированных элементов полугруппы G, если для классов A, B положим $B \leqslant A$ в том случае, когда хотя бы один (и, следовательно, всякий) элемент из B служит делителем хотя бы для одного (и, следовательно, для всякого) элемента из A. Класс делителей единицы будет минимальным элементом этого множества (см. I.5.1), притом единственным.

3. Элемент $p \in G$, не являющийся делителем единицы, называется *неприводимым*, если его делителями служат, помимо делителей единицы, лишь элементы, с ним самим

ассоциированные, т. е. если из

$$p = ab$$

всегда следует, что один из элементов a, b является делителем единицы, а поэтому другой ассоциирован с p. *Вместе с p неприводимыми будут, очевидно, все элементы, с p ассоциированные.* Классы ассоциированных неприводимых элементов, если такие элементы в полугруппе G вообще существуют, будут в точности минимальными элементами частично упорядоченного множества классов ассоциированных элементов, отличных от класса делителей единицы.

Элемент $p \in G$, не являющийся делителем единицы, называется *простым*, если произведение ab может делиться на p лишь в том случае, когда хотя бы один из элементов a, b делится на p. *Всякий элемент, ассоциированный с простым элементом p, будет, очевидно, простым.* Индукцией по n легко доказывается также, что *если произведение $a_1 a_2 \dots a_n$ делится на простой элемент p, то на p делится хотя бы один из элементов a_i, $i = 1, 2, \dots, n$.*

Всякий простой элемент p является неприводимым.

Действительно, если

$$p = ab,$$

то, ввиду простоты p, хотя бы один из сомножителей, например a, делится на p. Однако p делится в свою очередь на a, т. е. p и a ассоциированы, а поэтому элемент b будет делителем единицы.

Заметим, что обратное утверждение в общем случае не имеет места.

4. Если a, $b \in G$, то элемент $d \in G$ называется *наибольшим общим делителем* элементов a и b и записывается через

$$d = (a, b), \tag{2}$$

если d служит для a и b общим делителем и если d сам делится на любой другой общий делитель элементов a и b.

Если также $d' = (a, b)$, то d и d' должны делиться друг на друга, т. е. они ассоциированы. С другой стороны, если $d = (a, b)$ и ε_1, ε_2, ε_3 — произвольные делители единицы, то и

$$\varepsilon_1 d = (\varepsilon_2 a, \varepsilon_3 b),$$

т. е. замена в равенстве (2) всех входящих в него элементов любыми элементами, с ними ассоциированными, не нарушает этого равенства. Иными словами, если A, B, D — соответственно классы элементов, ассоциированных с a, b и d, то равенство (2) можно переписать в виде

$$D = (A,\ B).$$

Класс D будет единственным максимальным элементом (см. I.5.5) в частично упорядоченном множестве всех таких классов X, что $X \leqslant A$ и $X \leqslant B$, а символ (A, B) следует рассматривать как обозначение для этого класса.

Конечно, элементы $a,\ b \in G$ могут, вообще говоря, не иметь наибольшего общего делителя. Однако, *если a делится на b, то (a, b) существует, причем*

$$(a,\ b) = b.$$

5. *Если наибольший общий делитель существует для любой пары элементов $a,\ b \in G$, то всякий неприводимый элемент полугруппы G будет простым.*

Докажем сперва, что при наших предположениях для любых $a,\ b,\ c \in G$

$$(ac,\ bc) = (a,\ b)\,c. \tag{3}$$

В самом деле, так как a делится на (a, b), то ac делится на $(a, b)\,c$. Аналогично и bc делится на $(a, b)\,c$, а поэтому левая часть равенства (3) делится на правую,

$$(ac,\ bc) = (a,\ b)\,cd. \tag{4}$$

Отсюда

$$ac = (ac,\ bc)\,u = (a,\ b)\,cdu,$$

т. е., в силу закона сокращения,

$$a = (a,\ b)\,du. \tag{5}$$

Аналогично

$$b = (a,\ b)\,dv. \tag{6}$$

Из (5) и (6) следует, что элемент $(a,b)\,d$ служит общим делителем для a и b, а так как он сам делится на (a, b), то элемент d должен быть делителем единицы. Этим доказано, что от равенства (4) можно перейти к равенству (3).

Покажем теперь, что для любых трех элементов $a, b, c \in G$

$$((a, b), c) = (a, (b, c)). \tag{7}$$

Действительно, элемент $((a, b), c)$ служит общим делителем для (a, b) и c, а поэтому общим делителем и для элементов a, b, c. С другой стороны, всякий общий делитель этих трех элементов служит общим делителем для (a, b) и c, а поэтому он будет делителем и для $((a, b), c)$. Это же самое можно утверждать и для элемента $(a, (b, c))$, а поэтому левая и правая части равенства (7) ассоциированы, что по существу и выражается равенством (7).

Назовем, далее, элементы $a, b \in G$ *взаимно простыми*, если их общими делителями служат лишь делители единицы; это можно записать равенством

$$(a, b) = 1.$$

Если $(a, b) = 1$ *и* $(a, c) = 1$, *то и* $(a, bc) = 1$.

Действительно, так как a служит делителем для ac, то

$$(a, ac) = a.$$

Далее, из $(a, b) = 1$ следует, ввиду (3),

$$(ac, bc) = c.$$

Поэтому, ввиду (7),

$$(a, bc) = ((a, ac), bc) = (a, (ac, bc)) = (a, c) = 1.$$

Переходим к доказательству самой теоремы. Пусть p — неприводимый элемент полугруппы G и пусть произведение ab делится на p. Если бы ни a, ни b на p не делились, то, ввиду неприводимости p, общими делителями для a и p (а также для b и p) служили бы лишь делители единицы, т. е. a и p (а также b и p) были бы взаимно просты,

$$(a, p) = 1, \quad (b, p) = 1.$$

Но тогда, как доказано выше, мы имели бы и

$$(ab, p) = 1,$$

хотя по условию ab делится на p, а p не является делителем единицы. Этим противоречием доказана простота элемента p.

6. Пусть, как и раньше, G будет абелева полугруппа с 1, удовлетворяющая закону сокращения. Если

$$a = b_1 b_2 \dots b_k \tag{8}$$

и если элементы $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k$ таковы, что

$$\varepsilon_1 \varepsilon_2 \dots \varepsilon_k = 1$$

— все эти элементы будут, следовательно, делителями единицы, — то имеет место также равенство

$$a = (\varepsilon_1 b_1)(\varepsilon_2 b_2) \dots (\varepsilon_k b_k). \tag{9}$$

Два разложения элемента a в произведение нескольких элементов, (8) и

$$a = c_1 c_2 \dots c_l, \tag{10}$$

будут называться *ассоциированными разложениями*, если $l = k$ и если, быть может, после изменения нумерации множителей во втором из этих разложений элементы b_i и c_i ассоциированы, $i = 1, 2, \dots, k$, т. е. (10) имеет вид (9).

Абелева полугруппа G с единицей, удовлетворяющая закону сокращения, называется *гауссовой полугруппой*, если всякий ее элемент a, не являющийся делителем единицы, разлагается в произведение неприводимых элементов, причем любые два таких разложения элемента a между собою ассоциированы.

К числу гауссовых полугрупп принадлежат все абелевы группы — они не содержат элементов, не являющихся делителями единицы. Гауссовой будет и мультипликативная полугруппа отличных от нуля целых чисел. Делителями единицы в этой полугруппе служат числа 1 и —1, а неприводимыми элементами являются все простые числа, взятые со знаком + или —. Мультипликативная полугруппа отличных от нуля многочленов от неизвестного x с коэффициентами из поля P также принадлежит к числу гауссовых полугрупп. Ее делителями единицы являются все отличные от нуля элементы поля P, а неприводимые элементы совпадают с неприводимыми многочленами.

7. *Абелева полугруппа G с единицей, удовлетворяющая закону сокращения, тогда и только тогда будет гауссовой, если она удовлетворяет любому из следующих*

эквивалентных между собою наборов условий: (α, β′), (α, β″), *где условия* α, β′ *и* β″ *таковы*:

(α) *частично упорядоченное множество классов ассоциированных элементов полугруппы* G (см. II. 8.2) *удовлетворяет условию минимальности* (см. I. 5.1);

(β′) *любые два элемента полугруппы* G *обладают наибольшим общим делителем*;

(β″) *всякий неприводимый элемент полугруппы* G *является простым.*

Так как, по II. 8.5, из (β′) следует (β″), то эта теорема сводится на доказываемые ниже два утверждения.

8. *Всякая гауссова полугруппа* G *удовлетворяет условиям* (α) *и* (β′).

В самом деле, назовем *длиной* элемента a гауссовой полугруппы G число множителей в любом разложении элемента a в произведение неприводимых множителей. Если $a=bc$, причем b — *истинный* делитель для a, т. е. ни b, ни c не являются делителями единицы, то мы получим разложение элемента a в произведение неприводимых множителей, перемножая разложения такого рода, взятые для элементов b и c. Таким образом, длина элемента a равна сумме длин элементов b и c, а поэтому длина истинного делителя элемента a строго меньше длины самого a. Отсюда следует, что всякая такая последовательность

$$a_1, a_2, \ldots, a_n, \ldots$$

элементов полугруппы G, что a_{n+1} является истинным делителем для a_n, $n=1, 2, \ldots$, обрывается на конечном месте. Этим доказана справедливость условия (α).

С другой стороны, пусть a, $b \in G$ и пусть

$$p_1, p_2, \ldots, p_n \tag{11}$$

будет такой набор неприводимых элементов, что всякий неприводимый делитель как элемента a, так и элемента b ассоциирован с одним и только одним элементом из (11); отсюда следует, что среди элементов (11) нет ассоциированных. Элементы a и b можно записать теперь в виде

$$a=\varepsilon p_1^{k_1}p_2^{k_2}\ldots p_n^{k_n},\quad b=\varepsilon' p_1^{l_1}p_2^{l_2}\ldots p_n^{l_n},$$

где ε, ε' — делители единицы, а некоторые из показателей $k_1, k_2, \ldots, k_n, l_1, l_2, \ldots, l_n$ могут равняться нулю. Так как

любой делитель c элемента a может быть записан в виде

$$c = \varepsilon'' p_1^{s_1} p_2^{s_2} \dots p_n^{s_n},$$

где ε'' — делитель единицы и $0 \leqslant s_i \leqslant k_i$, $i = 1, 2, \dots, n$, и аналогичное утверждение справедливо для делителей элемента b, то наибольшим общим делителем элементов a и b будет служить элемент

$$\alpha = p_1^{m_1} p_2^{m_2} \dots p_n^{m_n},$$

где $m_i = \min(k_i, l_i)$, $i = 1, 2, \dots, n$. Таким образом, выполняется и условие (β').

9. *Всякая абелева полугруппа G с единицей, удовлетворяющая закону сокращения и условиям* (α) *и* (β''), *является гауссовой.*

Нам нужно доказать, что всякий элемент $a \in G$, не являющийся делителем единицы, обладает разложением в произведение неприводимых элементов и что это разложение определено однозначно с точностью до ассоциированности. Сперва заметим, что если это утверждение выполняется для a, то оно выполняется и для любого элемента, ассоциированного с a. Это позволяет, ввиду (α) и I. 5.1, доказывать наше утверждение индукцией по частично упорядоченному множеству классов ассоциированных элементов полугруппы G.

Это утверждение заведомо выполняется для неприводимых элементов, т. е. для элементов из минимальных классов, отличных от класса делителей единицы. Будем считать поэтому все доказанным для всех истинных делителей элемента a. Если a не является неприводимым элементом, то

$$a = bc,$$

где b и c — истинные делители для a. В силу индуктивного предположения

$$b = p_1 p_2 \dots p_k, \qquad c = p_{k+1} p_{k+2} \dots p_n,$$

где все p_i, $i = 1, 2, \dots, n$, неприводимы. Отсюда

$$a = p_1 p_2 \dots p_k p_{k+1} p_{k+2} \dots p_n. \tag{12}$$

Пусть, далее,

$$a = q_1 q_2 \dots q_s \tag{13}$$

будет любое другое разложение элемента a в произведение неприводимых множителей. Так как, по (β''), неприводимый элемент q_1 является простым, то, по II.8.3, хотя бы один из элементов p_i, $i = 1, 2, \ldots, n$, должен делиться на q_1. Пусть это будет элемент p_1. Он, однако, неприводим, а поэтому элементы p_1 и q_1 ассоциированы,

$$p_1 = \varepsilon q_1. \tag{14}$$

Отсюда, ввиду закона сокращения,

$$(\varepsilon p_2) p_3 \ldots p_n = q_2 q_3 \ldots q_s. \tag{15}$$

Левая и правая части равенства (15) являются разложениями на неприводимые множители для истинного делителя элемента a, а поэтому, по индуктивному предположению, они ассоциированы. Отсюда и из (14) вытекает, однако, ассоциированность разложений (12) и (13) элемента a — действительно, из ассоциированности элемента εp_2 с элементом q_2, например, следует ассоциированность элементов p_2 и q_2.

§ 9. Гауссовы кольца

1. Напомним, что если R — область целостности (см. II. 2.7), то множество $R/0$ будет по умножению абелевой полугруппой, удовлетворяющей закону сокращения.

Область целостности R с единицей называется *гауссовым кольцом*, если мультипликативная полугруппа отличных от нуля элементов из R является гауссовой полугруппой.

К числу гауссовых колец тривиальным образом принадлежат все поля. Однако не всякая область целостности с единицей будет гауссовым кольцом.

* Совокупность комплексных чисел вида $a + b\sqrt{-3}$, где a и b — любые целые числа, будет областью целостности с единицей, но не гауссовым кольцом. Так,

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$$

будут в этом кольце два неассоциированных разложения числа 4 в произведение неприводимых множителей. *

2. Пусть дана область целостности R с единицей. Если $a \in R$, то множество

$$(a) = aR,$$

т. е. совокупность элементов вида ar, $r \in R$, будет идеалом в R (см. II.7.8.). Это *главный идеал*, порожденный элементом a. Ясно, что a содержится в идеале (a), так как $a = a \cdot 1$. Если в R все идеалы главные, т. е. всякий идеал из R порождается некоторым элементом, то R называется *кольцом главных идеалов*.

Всякое кольцо главных идеалов R является гауссовым кольцом.

Ввиду II.8.7 достаточно доказать, что в мультипликативной полугруппе отличных от нуля элементов из R выполняются условия (α) и (β').

Если элемент a делится на элемент b, $a = bc$, то $a \in (b)$ и поэтому $(a) \subseteq (b)$; верно и обратное. Таким образом, если в последовательности ненулевых элементов

$$a_1, a_2, \ldots, a_n, \ldots \tag{1}$$

каждый элемент a_n делится на a_{n+1}, $n = 1, 2, \ldots$, то соответствующие главные идеалы будут составлять возрастающую последовательность,

$$(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n) \subseteq \ldots \tag{2}$$

Легко проверяется, что теоретико-множественное объединение этой возрастающей последовательности идеалов само будет идеалом в R, т. е., в силу наших предположений об R, некоторым главным идеалом; обозначим его через (b). Элемент b, принадлежа к объединению возрастающей последовательности (2), должен содержаться в некотором идеале (a_n) и поэтому во всех идеалах (a_i) при $i \geqslant n$. Для всех этих i будет, следовательно, $(b) \subseteq (a_i)$, что вместе с $(a_i) \subseteq (b)$ дает $(a_i) = (b)$. Таким образом, элементы a_i и b служат делителями друг для друга, т. е. ассоциированы. Этим доказано, что в последовательности (1) ассоциированы между собою все элементы a_i при $i \geqslant n$, т. е. условие (α) выполняется.

С другой стороны, если a, $b \in R$, то совокупность элементов вида $ar + bs$, где r и s независимо пробегают все кольцо R, будет идеалом и, следовательно, главным идеалом; обозначим его через (d). Тогда

$$(d) \supseteq (a), \qquad (d) \supseteq (b),$$

так как

$$a = a \cdot 1 + b \cdot 0 \in (d), \qquad b = a \cdot 0 + b \cdot 1 \in (d),$$

и поэтому элемент d служит общим делителем для a и b. Если же c — любой общий делитель для a и b, то

$$(c) \supseteq (a), \quad (c) \supseteq (b),$$

а поэтому идеал (c) содержит всякий элемент, имеющий вид $ar + bs$, т. е. $(c) \supseteq (d)$, откуда следует, что c служит делителем и для d. Мы получаем, что d является наибольшим общим делителем для a и b. Этим доказано, что условие (β') также выполняется.

3. Область целостности R с единицей называется *евклидовым кольцом*, если всякому элементу $a \in R$, отличному от нуля, поставлено в соответствие неотрицательное целое число $n(a)$, причем выполняется следующее требование: для любых элементов a, $b \in R$, где $b \neq 0$, в кольце R можно так подобрать элементы q и r, что

$$a = bq + r,$$

причем или $r = 0$, или же $n(r) < n(b)$.

Всякое евклидово кольцо является кольцом главных идеалов и, следовательно, гауссовым кольцом.

В самом деле, пусть в евклидовом кольце R взят идеал A. Если $A = O$, то $A = (0)$. Если же $A \neq O$, то пусть a_0 будет один из тех ненулевых элементов из A, что $n(a_0) \leqslant n(a)$, каков бы ни был ненулевой элемент $a \in A$. Тогда для произвольного $a \in A$ можно, по условию, найти в R такие элементы q и r, что

$$a = a_0 q + r,$$

причем если $r \neq 0$, то $n(r) < n(a_0)$. Однако

$$r = a - a_0 q \in A,$$

и мы приходим к противоречию с выбором элемента a_0. Поэтому $r = 0$, т. е. $a = a_0 q$, чем доказано, что A является главным идеалом, порожденным элементом a_0.

К числу евклидовых колец принадлежат кольцо целых чисел C, а также кольцо многочленов $P[x]$ над полем P: в первом кольце роль $n(a)$ играет абсолютная величина $|a|$ числа a, а во втором — степень многочлена a. *Кольца C и $P[x]$ будут, следовательно, кольцами главных идеалов и гауссовыми кольцами.*

* Во всяком евклидовом кольце для разыскания наибольшего общего делителя двух элементов можно применять известный читателю алгоритм Евклида.

Существуют кольца главных идеалов, не являющиеся евклидовыми кольцами [Моцкин, Bull. Amer. Math. Soc. **55** (1949), 1142—1146]. *

4. Мы закончим параграф доказательством следующей теоремы:

Если R — гауссово кольцо, то кольцо многочленов $R[x]$ также будет гауссовым.

Мы знаем из II.2.7, что кольцо $R[x]$ будет в нашем случае областью целостности с единицей. Нужно доказать, ввиду II.8.7, что в мультипликативной полугруппе отличных от нуля элементов из $R[x]$ выполняются условия (α) и (β') из II.8.7.

Начнем с замечания, что *в кольце $R[x]$ делителями единицы служат делители единицы кольца R и только они.* Отметим, далее, что так как для ненулевых элементов гауссова кольца R выполняется условие (β') из II.8.7, то, ввиду (7) из II. 8.5, *можно говорить о наибольшем общем делителе любой конечной системы ненулевых элементов из R, причем он определен однозначно с точностью до ассоциированности.* Ясно, что это остается справедливым и в том случае, когда к рассматриваемой системе добавлено несколько элементов, равных нулю.

Многочлен $\varphi(x)$ называется *примитивным*, если наибольший общий делитель системы его коэффициентов является делителем единицы и поэтому может быть принят равным 1. Многочлен, ассоциированный с примитивным многочленом, сам, очевидно, примитивен. Среди многочленов нулевой степени примитивными будут делители единицы и только они.

Если $f(x)$ — произвольный ненулевой многочлен и a — наибольший общий делитель его коэффициентов, то

$$f(x) = a\varphi(x), \tag{3}$$

где многочлен $\varphi(x)$ примитивен. Если имеет место также равенство

$$f(x) = b\psi(x),$$

где $b \in R$, а $\psi(x)$ — примитивный многочлен, то b, будучи делителем для всех коэффициентов многочлена $f(x)$, служит

делителем и для a,

$$a = bc.$$

Поэтому, ввиду отсутствия в $R[x]$ делителей нуля,

$$\psi(x) = c\varphi(x),$$

откуда, ввиду примитивности $\psi(x)$, элемент c должен быть делителем единицы.

Этим доказано, что *в записи вида* (3) *для многочлена* $f(x)$ *и элемент* a *из* R, *и примитивный многочлен* $\varphi(x)$ *определены однозначно с точностью до множителя, являющегося делителем единицы, т. е. с точностью до ассоциированности.* Будем называть запись вида (3) *канонической записью* многочлена $f(x)$.

5. Лемма Гаусса. *Произведение примитивных многочленов само примитивно.*

В самом деле, пусть даны примитивные многочлены

$$f(x) = a_0x^k + a_1x^{k-1} + \ldots + a_ix^{k-i} + \ldots + a_k,$$
$$g(x) = b_0x^l + b_1x^{l-1} + \ldots + b_jx^{l-j} + \ldots + b_l$$

и пусть их произведение

$$f(x)g(x) = c_0x^{k+l} + c_1x^{k+l-1} + \ldots + c_{i+j}x^{(k+l)-(i+j)} + \ldots + c_{k+l}$$

не является примитивным. Отсюда следует, так как кольцо R гауссово, что коэффициенты $c_0, c_1, \ldots, c_{k+l}$ обладают общим неприводимым делителем p. Так как многочлены $f(x)$ и $g(x)$ примитивны, то ни у одного из них все коэффициенты не могут делиться на p. Пусть a_i и b_j будут коэффициенты этих многочленов с наименьшими индексами, не делящиеся на p. Однако

$$c_{i+j} = a_ib_j + a_{i-1}b_{j+1} + a_{i-2}b_{j+2} + \ldots + a_{i+1}b_{j-1} + a_{i+2}b_{j-2} + \ldots \quad (4)$$

Так как, по условию, все коэффициенты $a_{i-1}, a_{i-2}, \ldots$ и $b_{j-1}, b_{j-2}, \ldots$ делятся на p, то на p делятся как левая часть равенства (4), так и все слагаемые правой части, кроме первого. Отсюда следует, что на p делится и произведение a_ib_j, а так как неприводимый элемент p является в гауссовом кольце R простым (см. II.8.7.), то на p должен делиться хотя бы один из элементов a_i, b_j в противоречие с их выбором. Лемма доказана.

Отсюда следует, что *если даны ненулевые многочлены* $f_i(x)$, $i=1, 2, \ldots, n$, *с каноническими записями*

$$f_i(x)=a_i\varphi_i(x), \quad i=1, 2, \ldots, n,$$

и если

$$f(x)=\prod_{i=1}^{n} f_i(x), \quad a=\prod_{i=1}^{n} a_i, \quad \varphi(x)=\prod_{i=1}^{n} \varphi_i(x),$$

то

$$f(x)=a\varphi(x)$$

будет канонической записью многочлена $f(x)$. Отсюда следует, что *если произведение нескольких многочленов равно примитивному многочлену, то каждый из сомножителей будет примитивным многочленом.* Отметим также, что *если даны многочлены* $f(x)$ *и* $g(x)$ *с каноническими записями*

$$f(x)=a\varphi(x), \quad g(x)=b\psi(x)$$

и если $f(x)$ *делится на* $g(x)$, *то* a *делится на* b, *а* $\varphi(x)$ *делится на* $\psi(x)$.

6. Пусть в кольце $R[x]$ дана такая последовательность ненулевых многочленов

$$f_1(x), f_2(x), \ldots, f_n(x), \ldots, \tag{5}$$

что $f_n(x)$ делится на $f_{n+1}(x)$, $n=1, 2, \ldots$ Если

$$f_n(x)=a_n\varphi_n(x), \quad n=1, 2, \ldots,$$

— канонические записи этих многочленов, то в каждой из последовательностей

$$a_1, a_2, \ldots, a_n, \ldots, \tag{6}$$

$$\varphi_1(x), \varphi_2(x), \ldots, \varphi_n(x), \ldots \tag{7}$$

всякий элемент делится на следующий.

Так как кольцо R гауссово и так как, с другой стороны, в последовательности (7) степени многочленов идут не возрастая, то найдется натуральное число N со следующими свойствами: 1) все элементы $a_n \in R$ при $n \geqslant N$ между собою ассоциированы; 2) все многочлены $\varphi_n(x)$ имеют при $n \geqslant N$ одну и ту же степень, т. е. отличаются друг от друга множителями из R, которые, ввиду примитивности

многочленов $\varphi_n(x)$, должны быть делителями единицы. Отсюда следует, что все многочлены $f_n(x)$ из (5) будут при $n \geqslant N$ ассоциированными между собою, а поэтому для отличных от нуля многочленов из $R[x]$ выполняется условие (α).

7. Пусть теперь неприводимый многочлен $p(x)$ служит делителем для произведения $f(x)g(x)$. Если

$$f(x) = a\varphi(x), \qquad g(x) = b\psi(x)$$

— канонические записи многочленов $f(x)$ и $g(x)$, то

$$f(x)g(x) = (ab)[\varphi(x)\psi(x)]$$

будет канонической записью произведения $f(x)g(x)$. С другой стороны, для многочлена $p(x)$ также существует каноническая запись, а поэтому, ввиду его неприводимости, $p(x)$ будет или неприводимым элементом p кольца R, или же неприводимым примитивным многочленом $\pi(x)$.

В первом случае элемент p служит делителем для произведения ab, а поэтому, ввиду того, что кольцо R гауссово, p будет делителем хотя бы для одного из элементов a, b, например для a. В этом случае элемент p будет делителем и для многочлена $a\varphi(x) = f(x)$.

8. Остается более трудный второй случай. Здесь многочлен $\pi(x)$ будет служить делителем для произведения примитивных многочленов $\varphi(x)\psi(x)$.

Как известно из II. 5.5, область целостности R вкладывается в поле дробей; обозначим его через Q. Всякий многочлен из кольца $R[x]$ будет, конечно, многочленом и из кольца $Q[x]$. С другой стороны, если $q(x)$ — произвольный ненулевой многочлен из $Q(x)$, то, приводя дроби, служащие его коэффициентами, к общему знаменателю и вынося за скобки этот знаменатель, а затем и наибольший общий делитель числителей, мы придем к записи

$$q(x) = \frac{a}{b}\varphi(x), \tag{8}$$

где $\varphi(x)$ — примитивный многочлен из $R[x]$.

Если

$$q(x) = \frac{c}{d}\psi(x)$$

— другая запись вида (8) для $q(x)$, т. е. многочлен $\psi(x)$ принадлежит к $R[x]$ и примитивен, то

$$(ad)\varphi(x) = (bc)\psi(x), \tag{9}$$

а поэтому левая и правая части равенства (9) будут каноническими записями одного и того же многочлена из кольца $R[x]$, т. е. между собою ассоциированы. Таким образом, *примитивный многочлен* $\varphi(x)$ *определен для многочлена* $q(x)$ *однозначно с точностью до ассоциированности.* Назовем запись вида (8) *канонической записью* многочлена $q(x)$ из $Q[x]$.

Если даны ненулевые многочлены $q_1(x)$, $q_2(x)$ *из* $Q[x]$ *с каноническими записями*

$$q_i(x) = \frac{a_i}{b_i}\varphi_i(x), \quad i = 1, 2, \tag{10}$$

то

$$q_1(x)\,q_2(x) = \frac{a_1a_2}{b_1b_2}[\varphi_1(x)\varphi_2(x)] \tag{11}$$

будет, в силу леммы Гаусса, канонической записью для произведения $q_1(x)\,q_2(x)$.

Неприводимый примитивный многочлен $\pi(x)$ *остается неприводимым и в кольце* $Q[x]$. Действительно, если

$$\pi(x) = q_1(x)\,q_2(x),$$

где $q_1(x)$, $q_2(x) \in Q[x]$ и имеют канонические записи (10), то, по (11), $\pi(x)$ ассоциирован с произведением $\varphi_1(x)\,\varphi_2(x)$. Поэтому один из многочленов $\varphi_i(x)$, $i = 1, 2$, должен иметь степень 0; это же верно для соответствующего $q_i(x)$.

Мы знаем из II.9.3, что кольцо $Q[x]$ является гауссовым. Отсюда следует, так как $\pi(x)$ служит делителем для произведения $\varphi(x)\psi(x)$, что один из этих сомножителей, например $\varphi(x)$, делится на $\pi(x)$ в кольце $Q[x]$,

$$\varphi(x) = \pi(x)\,q(x), \quad q(x) \in Q[x].$$

Если $q(x)$ имеет каноническую запись

$$q(x) = \frac{c}{d}\chi(x),$$

то из примитивности многочленов $\varphi(x)$ и $\pi(x)$ следует, что $\varphi(x)$ ассоциировано с произведением $\pi(x)\chi(x)$, а поэтому

$\varphi(x)$ делится на $\pi(x)$ уже в кольце $R[x]$. На $\pi(x)$ делится, следовательно, и многочлен $f(x)=a\varphi(x)$.

Таким образом, в кольце $R[x]$ выполняется и условие (β''). Теорема II.9.4 доказана.

9. Из этой теоремы немедленно следует, что *кольцо многочленов $R[x_1, x_2, \ldots, x_n]$ от любого конечного числа неизвестных над любым гауссовым кольцом R само будет гауссовым.* В частности, гауссовым является кольцо многочленов $P[x_1, x_2, \ldots, x_n]$ над любым полем P.

Теперь легко показать, что *существуют гауссовы кольца, не являющиеся кольцами главных идеалов.* Так, в кольце многочленов $R=P[x, y]$ над полем P множество A многочленов без свободного члена будет идеалом, отличным от R. Этот идеал не является, однако, главным, так как общими делителями входящих в него многочленов x и y служат лишь отличные от нуля элементы из P.

§ 10. Дедекиндовы кольца

1. Как и в предшествующем параграфе, будем рассматривать область целостности R с единицей. Напомним (см. II.5.5 и II.5.6), что область целостности R содержится в однозначно определенном поле дробей.

Если A и B — идеалы из R, то их *произведением* AB называется идеал, порожденный всевозможными произведениями вида ab, где $a\in A$, $b\in B$. Легко видеть, что идеал AB состоит из тех и только тех элементов кольца R, которые хотя бы одним способом могут быть записаны в виде

$$\sum_{i=1}^{n} a_i b_i, \quad a_i \in A, \quad b_i \in B. \tag{1}$$

Из ассоциативности операций в R сейчас же вытекает ассоциативность умножения идеалов. Можно говорить, следовательно, о *полугруппе идеалов* кольца R; коммутативность этой полугруппы очевидна.

Так как всякий элемент вида (1) принадлежит и к пересечению идеалов A и B, то

$$AB \subseteq A \cap B.$$

С другой стороны, из $B\subseteq B'$ следует, очевидно,

$$AB \subseteq AB'. \tag{2}$$

2. Идеал C называется *простым*, если из включения $xy \in C$, $x, y \in R$, всегда следует, что хотя бы один из элементов x, y содержится в C. Этому определению удовлетворяют, очевидно, идеалы R и O. В дальнейшем, говоря о простых идеалах, мы будем эти два идеала исключать из рассмотрения.

Идеал C тогда и только тогда будет простым, если для любых идеалов A, B из $AB \subseteq C$ следует, что или $A \subseteq C$, или $B \subseteq C$.

В самом деле, пусть $AB \subseteq C$, но $A \not\subseteq C$, $B \not\subseteq C$. Существуют, следовательно, такие $a \in A$, $b \in B$, которые не содержатся в C, хотя $ab \in C$. Идеал C не является, таким образом, простым. Обратно, если идеал C не простой, то существуют a и b, лежащие вне C, но $ab \in C$. Переходя к главным идеалам, получаем, что $(a) \not\subseteq C$, $(b) \not\subseteq C$, но $(a)(b) \subseteq C$.

Будем понимать ниже под *максимальным идеалом* нашего кольца R всякий максимальный среди истинных (т. е. отличных от R) идеалов.

Всякий максимальный идеал M является простым.

Действительно, пусть $a \notin M$, $b \notin M$, но

$$ab \in M. \tag{3}$$

Идеал (M, a), порожденный идеалом M и элементом a, совпадает с R. Он состоит, однако, из элементов, записываемых в виде $m + xa$, $m \in M$, $x \in R$, и поэтому может быть записан в виде $M + Ra$. Аналогично $(M, b) = R$ и этот идеал может быть записан в виде $M + Rb$. Поэтому, ввиду (3), мы приходим к противоречию:

$$R = RR = (M + Ra)(M + Rb) \subseteq M.$$

3. *В кольце главных идеалов* (см. II.9.2) *простые идеалы совпадают с идеалами вида (p), где p — простой элемент* (см. II.8.3)

Действительно, если $xy \in (p)$, то

$$xy = pz, \qquad z \in R,$$

а поэтому, по определению простого элемента, хотя бы один из элементов x, y делится на p, т. е. содержится в идеале (p). Если же элемент q не простой, то, по II.8.7, он приводим, $q = ab$, где ни a, ни b не являются делителями единицы.

Отсюда $ab \in (q)$; однако, например, если $a \in (q)$, то

$$a = qc = abc,$$

откуда, ввиду отсутствия делителей нуля, $bc = 1$, т. е. b оказалось бы делителем единицы.

В кольце главных идеалов всякий идеал, отличный от всего кольца и от нуля, является произведением конечного числа простых идеалов.

Действительно, если элемент a не является делителем единицы и не равен нулю, то существует разложение a в произведение простых множителей,

$$a = p_1 p_2 \dots p_n,$$

а тогда

$$(a) = (p_1)(p_2) \dots (p_n).$$

Область целостности R с единицей называется *дедекиндовым кольцом*, если всякий идеал из R, отличный от самого R и от O, представим в виде произведения конечного числа простых идеалов. Ниже будет указана некоторая характеризация дедекиндовых колец.

4. Пусть R — область целостности с 1, P — ее поле дробей. Подгруппу A аддитивной группы поля P назовем *дробным идеалом* кольца R, если выполняются следующие два условия: 1) если $a \in A$, $x \in R$, то $ax \in A$; 2) все элементы из A можно записать в виде дробей с общим знаменателем, т. е.

$$A = \frac{1}{d} A_0, \qquad A_0 \subseteq R, \qquad d \in R, \qquad d \neq 0. \tag{4}$$

Ясно, что A_0 будет идеалом в R и что при этом условии равенство (4) можно считать определением дробного идеала.

К числу дробных идеалов принадлежат идеалы самого кольца R или, как мы будем сейчас говорить, его *целые идеалы*. С другой стороны, *главным дробным идеалом* будет называться дробный идеал вида $\frac{1}{b}(a)$, где (a) — главный целый идеал. Этот главный дробный идеал содержит, в частности, элемент $\frac{a}{b}$ поля P и порождается этим элементом, а поэтому его можно было бы записать в виде $\left(\frac{a}{b}\right)$.

Вообще, так как пересечение любого множества дробных идеалов является дробным идеалом, то можно говорить о дробном идеале, *порожденном* данным конечным множеством элементов из P: так как все эти элементы можно записать в виде дробей с общим знаменателем d, то все они лежат в дробном идеале $\frac{1}{d}R$, а поэтому можно говорить о пересечении всех дробных идеалов, содержащих заданные элементы.

5. На дробные идеалы переносится и определение произведения идеалов, причем если

$$A=\frac{1}{c}A_0, \qquad B=\frac{1}{d}B_0,$$

то

$$AC=\frac{1}{cd}A_0B_0,$$

т. е. *это произведение является дробным идеалом* Так как умножение остается ассоциативным (и коммутативным) и так как произведение ненулевых дробных идеалов само отлично от нуля, то можно говорить о *полугруппе ненулевых дробных идеалов* кольца R. Единицей этой полугруппы служит само R.

Нашей целью является доказательство следующей теоремы.

Область целостности R с единицей тогда и только тогда будет дедекиндовым кольцом, если его полугруппа ненулевых дробных идеалов является группой.

6. Пусть R — снова область целостности с единицей. Ее дробный идеал A называется *обратимым*, если существует такой дробный идеал A^{-1}, что

$$AA^{-1}=R.$$

Всякий ненулевой главный дробный идеал обратим, так как

$$\left(\frac{a}{b}\right)^{-1}=\left(\frac{b}{a}\right).$$

Всякий обратимый дробный идеал порождается конечным числом элементов.

В самом деле, если $AA^{-1}=R$, то для единицы существует запись вида

$$1=\sum_{i=1}^{n}a_ia_i', \quad a_i\in A, \quad a_i'\in A^{-1}, \quad i=1, 2, \ldots, n.$$

Отсюда для любого $a \in A$ будет

$$a = \sum_{i=1}^{n} a_i (a_i' a),$$

а так как $a_i' a \in R$, $i = 1, 2, \ldots, n$, то

$$A = (a_1, a_2, \ldots, a_n).$$

Если

$$B = A_1 A_2 \ldots A_n$$

и если дробный идеал B обратим, то каждый из дробных идеалов A_i, $i = 1, 2, \ldots, n$, также будет обратимым, так как

$$A_i \left[\left(\prod_{j \neq i} A_j \right) B^{-1} \right] = R.$$

7. *Если простые идеалы $C_1, C_2, \ldots, C_n$, рассматриваемые как дробные идеалы, обратимы, то*

$$A = C_1 C_2 \ldots C_n \tag{5}$$

будет единственным представлением целого идеала A в виде произведения простых идеалов.

Будем вести доказательство индукцией по n. Если $n = 1$, то покажем, что представление идеала C_1 в виде произведения двух целых идеалов, отличных от R,

$$C_1 = B_1 B_2,$$

вообще невозможно. Именно, так как идеал C_1 простой, то, по II.10.2, будет, например, $B_1 \subseteq C_1$. Отсюда, так как, по условию, идеал C_1 обратим, а включение (2) имеет место и в случае дробного идеала A,

$$B_2 = RB_2 = C_1^{-1} C_1 B_2 \supseteq C_1^{-1} B_1 B_2 = C_1^{-1} C_1 = R,$$

что невозможно.

Переходим к общему случаю. Пусть идеал A обладает как представлением (5), так и представлением

$$A = D_1 D_2 \ldots D_k, \tag{6}$$

где идеалы D_j, $j = 1, 2, \ldots, k$, простые. Пусть C_i — один из минимальных среди идеалов C_i, $i = 1, 2, \ldots, n$. Так как A содержится в простом идеале C_1, то, ввиду (6) и II.10.2, будет, например, $D_1 \subseteq C_1$. Аналогично существует такое i, что

$C_i \subseteq D_1$. Отсюда, ввиду минимальности C_1, следует

$$C_i = D_1 = C_1.$$

Приравнивая теперь правые части равенств (5) и (6), умноженные на C_1^{-1}, мы получаем

$$C_2 \dots C_n = D_2 \dots D_k,$$

откуда, по индуктивному предположению, $n = k$ и, после возможной перенумерации, $C_i = D_i$, $i = 2, \dots, n$.

8. *В дедекиндовом кольце R всякий простой идеал максимален и обратим.*

Предположим сперва, что простой идеал C обратим, и докажем его максимальность. Пусть существует такой элемент $a \in R$, лежащий вне C, что идеал $(C, a) = C + Ra$ отличен от R. Тогда тем более отличен от R идеал $C + Ra^2$, так как $C + Ra^2 \subseteq C + Ra$, и, ввиду дедекиндовости кольца, для этих двух идеалов существуют разложения в произведения простых идеалов,

$$C + Ra = \prod_{i=1}^{n} C_i, \qquad C + Ra^2 = \prod_{j=1}^{k} D_j. \tag{7}$$

Сейчас нам необходимо построить кольцо, которое в III.2.6 будет названо фактор-кольцом кольца R по идеалу C. Разложим аддитивную группу кольца R в смежные классы по подгруппе C. Если $C + x$ и $C + y$ — два любых смежных класса, то, умножая любой элемент первого класса на любой элемент второго, мы получим (так как C — идеал) элемент смежного класса $C + xy$. Это позволяет говорить об умножении смежных классов. Можно говорить и о сложении смежных классов, так как сумма любого элемента из $C + x$ с любым элементом из $C + y$ лежит в смежном классе $C + (x + y)$. Легко проверяется, что множество смежных классов по C составляет относительно этих операций кольцо $\bar{R}$; его нулем служит C, а единицей $C + 1$.

В нашем случае кольцо $\bar{R}$ не имеет делителей нуля, так как из $x \notin C$, $y \notin C$ и

$$(C + x)(C + y) = C$$

следовало бы $xy \in C$ в противоречие с простотой идеала C. К кольцу $\bar{R}$ применимы, следовательно, результаты предшествующих пунктов.

Так как, по (7), $C \subseteq C_i$, $i = 1, 2, \ldots, n$, то простой идеал C_i распадается на смежные классы по C, которые, как легко проверяется, составляют в $\bar{R}$ простой идеал $\bar{C}_i$; аналогично вводятся простые идеалы $\bar{D}_j$, $j = 1, 2, \ldots, k$. Если положим $\bar{a} = C + a$, то из (7) для главного идеала $\bar{R}\bar{a}$ вытекает разложение

$$\bar{R}\bar{a} = \prod_{i=1}^{n} \bar{C}_i,$$

а поэтому

$$(\bar{R}\bar{a})^2 = \bar{R}\bar{a}^2 = \prod_{i=1}^{n} \bar{C}_i^2 = \prod_{j=1}^{k} \bar{D}_j. \tag{8}$$

Все простые множители, входящие в разложения (8) для главного и поэтому, по II.10.6, обратимого идеала $\bar{R}\bar{a}^2$, сами обратимы, и, следовательно, по II.10.7, разложения (8) совпадают. Отсюда вытекает, что $k = 2n$ и, после перенумерации,

$$C_i = D_{2i-1} = D_{2i}, \qquad i = 1, 2, \ldots, n.$$

Таким образом,

$$C + Ra^2 = (C + Ra)^2,$$

откуда

$$C \subset (C + Ra)^2 \subseteq C^2 + Ra.$$

Для всякого $x \in C$ существуют, следовательно, такие $y \in C^2$ и $z \in R$, что

$$x = y + za.$$

Отсюда $za \in C$, а так как идеал C простой и $a \notin C$, то $z \in C$. Таким образом,

$$C \subseteq C^2 + Ca,$$

а так как обратное включение очевидно, то

$$C = C^2 + Ca.$$

Умножая обе части на идеал C^{-1}, существующий ввиду обратимости C, получаем

$$R = C + Ra$$

— противоречие с предположением. Максимальность идеала C доказана.

Докажем теперь обратимость всякого простого идеала C. Пусть $x \in C$, $x \neq 0$. Тогда

$$Rx = \prod_{i=1}^{n} C_i,$$

где идеалы C_i, $i = 1, 2, \ldots, n$, простые и, по II.10.6, обратимые (так как идеал Rx главный и поэтому обратимый), т. е., по доказанному выше, они максимальны. Так как, однако, $Rx \subseteq C$ и идеал C простой, то хотя бы для одного i будет $C_i \subseteq C$, т. е., ввиду максимальности C_i, $C_i = C$, а поэтому идеал C обратим.

9. Из результатов двух предшествующих пунктов вытекает следующее важное утверждение:

В дедекиндовом кольце всякий идеал, отличный от R и O, обладает единственным разложением в произведение простых идеалов.

10. Покажем теперь, что *всякий ненулевой дробный идеал A дедекиндова кольца R разлагается в произведение положительных или отрицательных степеней простых идеалов и поэтому обратим.*

Действительно, пусть $A = \frac{1}{d} A_0$. Тогда

$$A_0 = \prod_{i=1}^{n} C_i, \qquad Rd = \prod_{j=1}^{k} D_j,$$

где все C_i и D_j простые, а так как все простые идеалы D_j, $j = 1, 2, \ldots, k$, обратимы, то

$$A = A_0 (Rd)^{-1} = \prod_{i=1}^{n} C_i \cdot \prod_{j=1}^{k} D_j^{-1}.$$

Этим в одну сторону доказана основная теорема II.10.5.

11. Докажем обратное утверждение этой теоремы. Если ненулевые дробные идеалы области целостности R с единицей составляют по умножению группу и поэтому обратимы, то, по II.10.6, каждый (целый) идеал из R порождается конечным числом элементов. Отсюда следует, что *в R выполняется условие максимальности для идеалов:*

объединение B возрастающей цепочки идеалов

$$A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq \ldots$$

само будет идеалом и поэтому порождается конечным числом элементов. Найдется такое n, что все эти элементы уже лежат в A_n, а тогда

$$B = A_n = A_{n+1} = \ldots$$

Утверждение, что кольцо R дедекиндово, будет, ввиду II.10.2, доказано, если мы покажем, что *всякий целый идеал из R, отличный от R и O, является произведением максимальных идеалов.* Если это не так, то пусть A будет одним из максимальных среди тех идеалов, которые не могут быть так представлены. Он не будет максимальным идеалом кольца R, но, ввиду условия максимальности, существует содержащий его максимальный идеал M. Так как $A \subseteq M$ и $M^{-1}M = R$, то $M^{-1}A \subseteq R$, т. е. $M^{-1}A$ является целым идеалом. Из

$$A = RA = M(M^{-1}A) \tag{9}$$

следует

$$A \subseteq M^{-1}A.$$

Если бы это включение было строгим, то идеал $M^{-1}A$ разлагался бы в произведение максимальных идеалов, а тогда, по (9), и для A существовало бы такое представление против предположения. Поэтому $M^{-1}A = A$, т. е.

$$A = MA. \tag{10}$$

Приведем это к противоречию, показав, что существует такой элемент $z \in M$, что произведение элемента $1 - z$ на любой элемент из A равно нулю, хотя $z \neq 1$, а в R нет делителей нуля.

Пусть идеал A порождается элементами $x_1, x_2, \ldots, x_n$,

$$A = (x_1, x_2, \ldots, x_n).$$

Положим

$$A_i = (x_i, x_{i+1}, \ldots, x_n), \qquad i = 1, 2, \ldots, n,$$

и $A_{n+1} = O$ и докажем существование такого $z_i \in M$, $i = 1, 2, \ldots, n+1$, что

$$(1 - z_i)A \subseteq A_i. \tag{11}$$

Так как $A_1 = A$, то можно взять $z_1 = 0$. Пусть z_i со свойством (11) уже найдено. Тогда, ввиду (10),

$$(1 - z_i)A = (1 - z_i)MA \subseteq MA_i,$$

а так как всякий элемент идеала MA_i можно представить в виде суммы произведений элементов $x_i, x_{i+1}, \ldots, x_n$ на некоторые элементы из M, то

$$(1 - z_i) x_i = \sum_{j=i}^{n} z_{ij} x_j, \qquad z_{ij} \in M.$$

Отсюда

$$(1 - z_i - z_{ii}) x_i \in A_{i+1},$$

и поэтому

$$(1 - z_{i+1}) A \subseteq A_{i+1},$$

где

$$1 - z_{i+1} = (1 - z_i)(1 - z_i - z_{ii});$$

ясно, что $z_{i+1} \in M$. Элемент z_{n+1} и будет искомым элементом z. Теорема доказана.

* Область целостности R с единицей тогда и только тогда будет дедекиндовым кольцом, если удовлетворяются следующие условия: 1) условие максимальности для идеалов; 2) всякий простой идеал максимален; 3) кольцо R *целозамкнуто* в своем поле дробей P, т. е. всякий элемент из P, являющийся корнем многочлена с коэффициентами из R и со старшим коэффициентом 1, сам принадлежит к R. *

ГЛАВА ТРЕТЬЯ

УНИВЕРСАЛЬНЫЕ АЛГЕБРЫ. ГРУППЫ С МУЛЬТИОПЕРАТОРАМИ

§ 1. Универсальные алгебры. Гомоморфизмы

1. Параллелизм между теорией групп и теорией колец, неоднократно проявлявшийся в предшествующей главе, обнаруживается и во многих других разделах этих теорий. Во многих случаях оказывается целесообразным не рассматривать группы и кольца отдельно, а строить единую теорию, из которой результаты, относящиеся к группам и к кольцам, вытекали бы в качестве простых следствий. Именно с этой целью было начато изучение алгебраических образований с произвольным числом алгебраических операций, притом не обязательно бинарных.

2. Пусть дано множество G. Будем говорить, что в G определена *n-арная алгебраическая операция* ω (где n — целое неотрицательное число), если любой упорядоченной системе из n элементов $a_1, a_2, \ldots, a_n$ множества G сопоставлен однозначно определенный элемент этого же множества; этот результат применения операции ω к указанной системе элементов будет записываться через $a_1 a_2 \ldots a_n \omega$. В некоторых случаях приходится отказываться от требования, чтобы n-арная операция ω была определена для любых упорядоченных систем из n элементов, т. е. эта операция будет лишь *частичной*. Требование однозначности операции будет, однако, обычно сохраняться, и поэтому понятие n-арной операции является лишь частным случаем понятия $(n+1)$-арного отношения (ср. II.1.1).

При $n=2$ мы приходим к привычному нам понятию бинарной операции (см. II.1.2), при $n=3$ получаем *тернарную*

операцию, и т. д. С другой стороны, при $n=1$ мы будем говорить об *унарной операции*. Эта операция сопоставляет всякому элементу $a \in G$ однозначно определенный элемент $a\omega \in G$, т. е. является некоторым однозначным отображением множества G в себя. Наконец, случай $n=0$, т. е. случай *нульарной операции*, означает, что в множестве G фиксируется некоторый определенный элемент, который не зависит от выбора в G каких-либо элементов или систем элементов. Так, беря единицу группы, мы применяем к этой группе нульарную операцию; такими же операциями в случае кольца будет взятие его нуля или единицы (если последняя существует).

3. Множество G называется *универсальной алгеброй*, если в нем задана некоторая система Ω n-арных алгебраических операций, причем для различных операций $\omega \in \Omega$ числа n могут быть как различными, так и совпадающими. Эта система операций может быть и бесконечной — примерами универсальных алгебр такого рода служат векторные пространства над бесконечными полями: здесь имеется одна бинарная операция, а именно сложение, бесконечное множество унарных операций, а именно умножений на элементы основного поля, и одна нульарная, фиксирующая нулевой элемент.

В предшествующей главе мы встречали много различных видов универсальных алгебр — группоиды, группы, квазигруппы, кольца и т. д. Заметим, что мы умеем двумя способами рассматривать группу как универсальную алгебру: с одной стороны, это множество с тремя бинарными операциями — умножением и левым и правым делениями; с другой стороны, это множество с одной бинарной операцией — умножением, с одной унарной операцией — взятием обратного элемента и с одной нульарной оцерацией — взятием единицы. К вопросу о различных способах задания одной и той же алгебраической системы в качестве универсальной алгебры мы вернемся еще в III.6.6.

Заметим также, что тела можно будет считать универсальными алгебрами лишь в том случае, если к рассмотрению будут допущены частичные алгебраические операции, так как именно таковы и левое и правое деление в теле, и взятие обратного элемента.

4. Пусть дана универсальная алгебра G с системой операций Ω. Подмножество $A \subseteq G$ будет называться *подалгеброй* универсальной алгебры G, если для любой операции $\omega \in \Omega$ из $a_1, a_2, \ldots, a_n \in A$, где n — арность операции ω, всегда следует

$$a_1 a_2 \ldots a_n \omega \in A.$$

Частными случаями этого понятия являются, очевидно, подгруппоид группоида, подгруппа группы, подкольцо кольца. Отметим, впрочем, что если кольцо R обладает единицей и если оно рассматривается как универсальная алгебра, в число операций которой включена нульарная операция взятия единицы, то подалгебрами будут лишь те подкольца кольца R (см. II.3.2), которые содержат единицу кольца R, а не любые подкольца, даже если они обладают своей собственной единицей.

Так же, как в II.3.6, доказывается, что *пересечение любой системы подалгебр универсальной алгебры G, если оно не пусто, будет подалгеброй этой алгебры.*

Отсюда следует, что *если в универсальной алгебре G взято произвольное непустое подмножество M, то существует однозначно определенная подалгебра $\{M\}$, минимальная среди подалгебр, целиком содержащих M.* Это будет пересечение всех подалгебр из G, содержащих M, — одной из таких подалгебр будет само G. Если $\{M\} = G$, то M будет *системой образующих* для G.

5. Универсальные алгебры G и G', в которых заданы соответственно системы операций Ω и Ω', называются *однотипными*, если можно установить такое взаимно однозначное соответствие между системами Ω и Ω', при котором любая операция $\omega \in \Omega$ и соответствующая ей операция $\omega' \in \Omega'$ будут n-арными с о д н и м и т е м ж е n. Можно считать, следовательно, что в однотипных универсальных алгебрах задана о д н а и т а ж е система операций Ω.

Однотипные универсальные алгебры G и G' с одной и той же системой операций Ω называются *изоморфными*, если существует такое взаимно однозначное отображение φ алгебры G на алгебру G', что для любой n-арной операции $\omega \in \Omega$ и любых элементов $a_1, a_2, \ldots, a_n \in G$

$$(a_1 a_2 \ldots a_n \omega)\varphi = (a_1\varphi)(a_2\varphi)\ldots(a_n\varphi)\omega. \qquad (1)$$

Понятие изоморфизма универсальных алгебр играет в точности ту же роль, какую оно играло для групп, колец или частично упорядоченных множеств. Сейчас будет введено одно его обобщение, а именно понятие гомоморфизма, очень важное для всей дальнейшей теории. Именно, сохраняя требование (1), но считая, что φ является лишь однозначным (а не обязательно взаимно однозначным) отображением алгебры G в алгебру G' (т. е. не обязательно на всю эту алгебру), мы приходим к определению *гомоморфного отображения* одной универсальной алгебры в другую, ей однотипную.

Из определения гомоморфизма легко следует, что *произведение гомоморфизмов* (в смысле I.1.2) *само будет гомоморфизмом*. Действительно, если даны однотипные алгебры G, G', G'' с одной и той же системой операций Ω и гомоморфизмы φ: $G \to G'$ и ψ: $G' \to G''$, то для любой n-арной операции $\omega \in \Omega$ и любых элементов $a_1, a_2, \ldots, a_n \in G$ будет

$$(a_1a_2 \ldots a_n\omega)(\varphi\psi) = [(a_1a_2 \ldots a_n\omega)\varphi]\psi =$$
$$= [(a_1\varphi)(a_2\varphi) \ldots (a_n\varphi)\omega]\psi = [(a_1\varphi)\psi][(a_2\varphi)\psi] \ldots [(a_n\varphi)\psi]\omega =$$
$$= [a_1(\varphi\psi)][a_2(\varphi\psi)] \ldots [a_n(\varphi\psi)]\omega,$$

чем и доказано, что произведение $\varphi\psi$ будет гомоморфизмом алгебры G в алгебру G''.

Из (1) следует также, что если $G\varphi$ есть образ алгебры G при гомоморфном отображении φ в алгебру G', то $G\varphi$ *будет подалгеброй алгебры* G'.

Если $G\varphi = G'$, то мы говорим о гомоморфном отображении *на* G' и называем G' *гомоморфным образом* алгебры G.

6. Применим понятие гомоморфизма к случаю группоидов и колец. Ясно, что в случае бинарного умножения равенство (1) превращается в равенство

$$(ab)\varphi = a\varphi \cdot b\varphi \tag{2}$$

и что универсальная алгебра, однотипная с группоидом, сама будет группоидом. Легко проверяется, как и в случае изоморфизма (см. II.4.1), что при гомоморфном отображении группоида G на группоид G' сохраняются такие свойства операции, заданной в G, как коммутативность и ассоциативность.

Пусть φ — *гомоморфное отображение группоида* G *на группоид* G'. *Если* G *обладает единицей* e, *то* $e\varphi$ *будет единицей в* G'. *Если, сверх того, элемент* $b \in G$ *является одним из* (*правых*) *обратных элементов для* $a \in G$, *то* $b\varphi$ *будет одним из* (*правых*) *обратных элементов для* $a\varphi$.

Действительно, для $a \in G$ из $ae = ea = a$ и (2) следует $a\varphi \cdot e\varphi = e\varphi \cdot a\varphi = a\varphi$, а так как элемент $a\varphi$ пробегает весь группоид G', когда a пробегает группоид G, то $e\varphi$ действительно будет единицей в G'. С другой стороны, из $ab = e$ и (2) следует $a\varphi \cdot b\varphi = e\varphi$.

Таким образом, *гомоморфный образ полугруппы или группы будет полугруппой и соответственно группой.*

Рассмотрим теперь гомоморфное отображение φ кольца R на однотипную ему универсальную алгебру R'. Из сказанного выше следует, что R' будет абелевой группой по сложению и группоидом по умножению. Докажем, что в R' выполняются законы дистрибутивности. Если $a', b', c' \in R'$, а элементы $a, b, c \in R$ таковы, что $a\varphi = a'$, $b\varphi = b'$, $c\varphi = c'$, то из равенства

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

справедливого в кольце R, следует равенство

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

Так же проверяется и второй закон дистрибутивности.

Таким образом, *гомоморфный образ кольца будет кольцом.* Из сказанного выше следует, что при гомоморфизме колец нуль переходит в нуль и что гомоморфным образом ассоциативного или коммутативного кольца будет кольцо с таким же свойством.

7. Существует некоторый способ обозрения всех гомоморфных отображений данной универсальной алгебры G. Введем сперва следующее понятие.

Рассмотрим универсальную алгебру G с системой операций Ω. Отношение эквивалентности π (см. I. 3.1), заданное в G, называется *конгруенцией* в G, если для любой n-арной операции $\omega \in \Omega$ и любых элементов

$$a_i,\ a_i' \in G, \qquad i = 1, 2, \ldots, n,$$

из

$$a_i \pi a_i', \qquad i = 1, 2, \ldots, n,$$

следует

$$(a_1a_2\dots a_n\omega)\,\pi\,(a_1'a_2'\dots a_n'\omega).$$

Иными словами, если взяты произвольные классы A_1, $A_2,\dots,$ A_n разбиения, определяемого отношением эквивалентности π (см. I.3.2), то класс B, содержащий элемент $a_1a_2\dots a_n\omega$, где $a_i\in A_i$, $i=1,2,\dots,n$, не зависит от выбора элементов a_i в их классах A_i, $i=1,2,\dots,n$. Это позволяет определить n-арную операцию ω в фактор-множестве G/π (см. I.3.4), полагая

$$A_1A_2\dots A_n\omega=B. \tag{3}$$

Так как это справедливо для всех операций $\omega\in\Omega$, то в результате G/π превращается в универсальную алгебру с той же системой операций Ω, что и исходная алгебра G. Эта алгебра G/π называется *фактор-алгеброй* универсальной алгебры G по конгруенции π.

Определение (3) операций в фактор-алгебре G/π и определение гомоморфизма (1) показывают, что естественное отображение алгебры G на фактор-алгебру G/π (см. I.3.4) будет гомоморфизмом. Он называется *естественным гомоморфизмом* G на G/π.

Из существования естественного гомоморфизма G на G/π и сказанного в предшествующем пункте следует, что *фактор-алгебры группоидов, групп, колец сами будут соответственно группоидами, группами, кольцами.* Можно говорить, следовательно, о *фактор-группоиде* (или *фактор-группе*, или *фактор-кольце*) G/π группоида (группы, кольца) G по некоторой конгруенции π.

8. Обращением сказанного в предшествующем пункте служит следующая теорема о гомоморфизмах, дающая обозрение всех гомоморфных отображений универсальных алгебр.

Если G — универсальная алгебра с системой операций Ω, а φ — ее гомоморфное отображение на однотипную универсальную алгебру G', $G\varphi=G'$, то в G существует такая конгруенция π, что алгебра G' изоморфна фактор-алгебре G/π. Больше того, существует такое изоморфное отображение ψ алгебры G' на фактор-алгебру G/π, что произведение $\varphi\psi$ совпадает с естественным гомоморфизмом G на G/π.

В самом деле, мы получим разбиение алгебры G на непересекающиеся классы, относя в один класс такие элементы из G, образы которых при гомоморфизме φ совпадают. Отношение эквивалентности π, определяемое этим разбиением, будет в алгебре G конгруенцией. Действительно, для любой n-арной операции $\omega \in \Omega$ из

$$a_i\varphi = \bar{a}_i\varphi, \qquad i = 1, 2, \ldots, n,$$

следует, по (1),

$$(a_1a_2 \ldots a_n\omega)\,\varphi = (a_1\varphi)(a_2\varphi)\ldots(a_n\varphi)\,\omega = \\ = (\bar{a}_1\varphi)(\bar{a}_2\varphi)\ldots(\bar{a}_n\varphi)\,\omega = (\bar{a}_1\bar{a}_2\ldots\bar{a}_n\omega)\,\varphi,$$

т. е. элементы $a_1a_2\ldots a_n\omega$ и $\bar{a}_1\bar{a}_2\ldots\bar{a}_n\omega$ также принадлежат к одному классу разбиения π.

Существует, следовательно, фактор-алгебра G/π. Ставя в соответствие всякому элементу $a' \in G'$ класс A разбиения π, составленный из всех прообразов элемента a' при гомоморфизме φ, мы получим взаимно однозначное отображение ψ алгебры G' на фактор-алгебру G/π. Докажем, что ψ является изоморфизмом.

Пусть n-арная операция ω — любая операция из Ω, а a'_i, $i = 1, 2, \ldots, n$, — любые элементы из G'. Полагая

$$a'_i\psi = A_i, \quad i = 1, 2, \ldots, n,$$

и выбирая элементы $a_i \in A_i$, $i = 1, 2, \ldots, n$, откуда

$$a_i\varphi = a'_i, \quad i = 1, 2, \ldots, n,$$

мы получим, по (1),

$$(a_1a_2 \ldots a_n\omega)\,\varphi = a'_1a'_2 \ldots a'_n\omega. \tag{4}$$

Так как, по (3),

$$a_1a_2 \ldots a_n\omega \in A_1A_2 \ldots A_n\omega,$$

то из (4) следует

$$(a'_1a'_2 \ldots a'_n\omega)\,\psi = A_1A_2 \ldots A_n\omega = (a'_1\psi)(a'_2\psi) \ldots (a'_n\psi)\,\omega,$$

что и доказывает изоморфность отображения ψ.

Наконец, если a — произвольный элемент алгебры G и если

$$a\varphi = a', \qquad a'\psi = A,$$

то, ввиду определения отображения ψ, $a \in A$. Этим показано, что произведение $\varphi\psi$ совпадает с естественным гомоморфизмом G на G/π. Теорема о гомоморфизмах доказана.

§ 2. Группы с мультиоператорами

1. Как мы увидим ниже, существует весьма тесная связь между конгруенциями и, следовательно, гомоморфизмами групп и колец, с одной стороны, и нормальными делителями групп и идеалами колец, с другой стороны. Эта связь не может быть в полной мере распространена на случай любых универсальных алгебр, в частности на случай группоидов или полугрупп. Она целиком сохраняется, однако, для одного специального класса универсальных алгебр, введенного недавно Хиггинсом (Proc. London Math. Soc. **6** (1956), 366 — 416) и представляющего собою весьма удачное объединение классов групп и колец.

Пусть дана группа G. Эта группа не обязана быть коммутативной, но нам будет удобно использовать для нее аддитивную запись; в частности, нулевой элемент этой группы будет, как обычно, обозначаться символом 0. Группа G будет называться *группой с системой мультиоператоров* Ω или, короче, *Ω-группой*, если в G задана помимо сложения еще некоторая система n-арных алгебраических операций Ω (при некоторых n, удовлетворяющих условию $n \geqslant 1$), причем для всех $\omega \in \Omega$ должно выполняться условие

$$00 \ldots 0\omega = 0, \tag{1}$$

где слева элемент 0 стоит n раз, если операция ω n-арна.

Ясно, что при пустой системе операций Ω мы получаем понятие группы. С другой стороны, понятие Ω-группы превращается в понятие кольца, если *аддитивная группа* этой Ω-группы — условимся так называть группу по сложению — коммутативна и если система операций Ω состоит из одного бинарного умножения, связанного со сложением законами дистрибутивности; условие (1) отсюда, как мы знаем, следует.

2. Ω-группу G можно считать универсальной алгеброй относительно операций аддитивной группы и операций из Ω. Всякая подалгебра этой алгебры (см. III.1.4) будет подгруппой аддитивной группы и поэтому содержит 0, условие (1) продолжает выполняться, и поэтому она сама является Ω-группой. Будем говорить поэтому не о подалгебрах, а об *Ω-подгруппах* Ω-группы G.

Отсюда, ввиду III.1.4, следует, что *пересечение любой системы* Ω*-подгрупп* Ω*-группы* G *само будет* Ω*-подгруппой* и, в частности, содержит элемент 0. С другой стороны, Ω*-подгруппой будет и подалгебра* $\{M\}$, порожденная непустым подмножеством M Ω-группы G.

Заметим, что, ввиду (1), нулевая подгруппа аддитивной группы будет Ω-подгруппой.

3. Если Ω-группа G гомоморфизмом φ (см. III.1.5) отображается на однотипную ей универсальную алгебру G', то это будет, в частности, гомоморфизм для аддитивной группы Ω-группы G, а поэтому алгебра G' по операциям, соответствующим операциям аддитивной группы Ω-группы G, сама будет группой. Будем считать эту группу записанной аддитивно и ее нуль обозначать через $0'$. Так как φ — гомоморфизм, а $0\varphi = 0'$, то для любой операции $\omega \in \Omega$ будет, ввиду (1),

$$0'0' \ldots 0'\omega = 0'.$$

Таким образом, *всякий гомоморфный образ* Ω*-группы сам будет* Ω*-группой.* В частности, *фактор-алгебры* Ω*-групп* (см. III.1.7) *сами являются* Ω*-группами.* Можно говорить поэтому об Ω*-фактор-группе* G/π Ω-группы G по конгруенции π.

4. Непустое подмножество A Ω-группы G называется *идеалом* в G, если выполняются следующие два условия:

1) A является нормальным делителем аддитивной группы;

2) для всякой n-арной операции $\omega \in \Omega$, любого элемента $a \in A$ и любых элементов $x_1, x_2, \ldots, x_n \in G$ должно при $i = 1, 2, \ldots, n$ иметь место включение

$$-(x_1x_2 \ldots x_n\omega) + x_1 \ldots x_{i-1}(a + x_i)\, x_{i+1} \ldots x_n\omega \in A. \quad (2)$$

Для групп определенное сейчас понятие идеала совпадает с понятием нормального делителя, так как, ввиду пустоты системы операций Ω, условие 2) отпадает.

Для колец наше новое понятие идеала совпадает с понятием (двустороннего) идеала, введенным в II.7.8.

Действительно, в этом случае условие 1) требует, чтобы A было подгруппой аддитивной группы кольца, условие же 2) превращается для операции умножения и любых $a \in A$, $x_1, x_2 \in G$ при $i = 1$ в

$$-x_1x_2 + (a + x_1)\, x_2 = -x_1x_2 + ax_2 + x_1x_2 = ax_2 \in A,$$

а при $i=2$ в

$$-x_1x_2+x_1(a+x_2)=-x_1x_2+x_1a+x_1x_2=x_1a\in A,$$

что и требовалось доказать.

Заметим, что включение (2) может быть переписано в виде

$$x_1\ldots x_{i-1}(a+x_i)x_{i+1}\ldots x_n\omega\in x_1x_2\ldots x_n\omega+A, \quad (3)$$
$$i=1,\ 2,\ \ldots,\ n,$$

где справа стоит смежный класс по нормальному делителю A, порожденный элементом $x_1x_2\ldots x_n\omega$. Применяя включение (3) несколько раз, мы приходим к следующему утверждению:

Для любого идеала A Ω-группы G, любой n-арной операции $\omega\in\Omega$, любых элементов $a_1,\ a_2,\ \ldots,\ a_n\in A$ и любых элементов $x_1,\ x_2,\ \ldots,\ x_n\in G$ имеет место включение

$$(a_1+x_1)(a_2+x_2)\ldots(a_n+x_n)\omega\in x_1x_2\ldots x_n\omega+A. \quad (4)$$

Отсюда следует, что *всякий идеал A Ω-группы G является ее Ω-подгруппой.* Действительно, A будет подгруппой аддитивной группы в силу условия 1), а из (4) для любой n-арной операции $\omega\in\Omega$ и любых $a_1,\ a_2,\ \ldots,\ a_n\in A$ следует при $x_1=x_2=\ldots=x_n=0$, ввиду равенства (1),

$$a_1a_2\ldots a_n\omega\in A.$$

Ясно, что идеалами Ω-группы G будут, в частности, само G и нулевая подгруппа O. Если в G нет других идеалов, то это будет *простая* Ω-группа.

Без труда проверяется, что *пересечение любой системы идеалов Ω-группы G само будет идеалом,* а поэтому можно говорить и об идеале, *порожденном* любой системой элементов M.

Заметим, что *идеал, порожденный системой идеалов A_i, $i\in I$, Ω-группы G, совпадает с порожденной этими идеалами подгруппой B аддитивной группы.*

Действительно, из II.7.5. мы знаем, что $B=\{A_i,\ i\in I\}$ является нормальным делителем аддитивной группы и что всякий элемент из B записывается в виде

$$b=a_1+a_2+\ldots+a_k,\quad a_j\in A_{i_j},\ j=1,\ 2,\ \ldots,\ k. \quad (5)$$

Пусть даны n-арная операция $\omega\in\Omega$, элемент $b\in B$ с записью (5) и элементы $x_1,\ x_2,\ \ldots,\ x_n\in G$. Так как $A_{i_1},\ A_{i_2},\ \ldots,\ A_{i_k}$

являются идеалами, то, используя (3) и (5), мы получим

$$x_1 \dots x_{i-1}(b + x_i)x_{i+1} \dots x_n\omega \in x_1x_2 \dots x_n\omega + B,$$

что и требовалось доказать.

Идеал $B = \{A_i,\ i \in I\}$ будет называться *суммой* идеалов A_i, $i \in I$.

5. Сейчас будет доказана теорема, выясняющая роль понятия идеала в теории Ω-групп. Заметим, что, говоря о *разложении Ω-группы G по идеалу A*, мы будем понимать под этим разложение аддитивной группы этой Ω-группы по A как по нормальному делителю.

Все конгруенции в произвольной Ω-группе G исчерпываются ее разложениями по различным идеалам.

В самом деле, пусть A будет произвольный идеал Ω-группы G. Для любых a_1, $a_2 \in A$ и x_1, $x_2 \in G$ существует, в силу определения нормального делителя, такой элемент $a_3 \in A$, что

$$a_1 + x_2 = x_2 + a_3,$$

а поэтому

$$(x_1 + a_1) + (x_2 + a_2) = (x_1 + x_2) + (a_3 + a_2) \in (x_1 + x_2) + A.$$

С другой стороны, для любой n-арной операции $\omega \in \Omega$, любых элементов $a_1, a_2, \dots, a_n \in A$ и $x_1, x_2, \dots, x_n \in G$ имеет место включение (4). Эти включения показывают, что разложение G в смежные классы по A действительно является конгруенцией в Ω-группе G.

Пусть теперь в G дана произвольная конгруенция π. Обозначим через A тот класс разбиения π, в котором содержится нуль аддитивной группы; элементы $a \in A$ характеризуются, следовательно, тем, что имеет место $a\pi 0$. Если a_1, $a_2 \in A$, то $a_1\pi 0$, $a_2\pi 0$, а поэтому, по определению конгруенции,

$$(a_1 + a_2)\,\pi\,(0 + 0), \quad \text{т. е.} \quad (a_1 + a_2)\,\pi\,0,$$

откуда $a_1 + a_2 \in A$. Далее, если $a \in A$, то

$$[0 + (-a)]\,\pi\,[a + (-a)],$$

т. е. $-a\pi 0$, откуда $-a \in A$. Наконец, если $a \in A$, $x \in G$, то

$$(-x + a + x)\,\pi\,(-x + 0 + x),$$

т. е. $(-x + a + x)\pi 0$, откуда $-x + a + x \in A$. Этим доказано, что A является нормальным делителем аддитивной группы.

Если теперь даны n-арная операция $\omega \in \Omega$, элемент $a \in A$ и элементы $x_1, x_2, \ldots, x_n \in G$, то

$$(a + x_i)\,\pi\,(0 + x_i), \quad \text{т. е.} \quad (a + x_i)\,\pi\,x_i,$$

откуда

$$[x_1 \ldots x_{i-1}(a + x_i)\,x_{i+1} \ldots x_n\omega]\,\pi\,(x_1x_2 \ldots x_n\omega),$$

а поэтому

$$-x_1x_2 \ldots x_n\omega + x_1 \ldots x_{i-1}(a + x_i)\,x_{i+1} \ldots x_n\omega \in A,$$
$$i = 1, 2, \ldots, n.$$

Мы получаем, что класс A будет даже идеалом Ω-группы G.

Рассмотрим, наконец, произвольный класс B разбиения π. Если $b \in B$, $a \in A$, т. е. $a\pi 0$, то

$$(b + a)\,\pi\,(b + 0), \quad \text{т. е.} \quad (b + a)\,\pi\,b,$$

откуда для смежного класса $b + A$ следует включение

$$b + A \subseteq B.$$

С другой стороны, если b' — произвольный элемент из класса B, то из $b'\pi b$ следует $(-b + b')\,\pi 0$ или

$$-b + b' \in A, \quad \text{т. е.} \quad b' \in b + A.$$

Этим доказано равенство $B = b + A$, т. е. доказано, что всякий класс разбиения π является смежным классом по идеалу A. Теорема доказана.

6. В силу этой теоремы мы будем говорить в дальнейшем не об Ω-фактор-группе G/π Ω-группы G по некоторой конгруенции π, а об *Ω-фактор-группе по идеалу A* и обозначать ее через G/A. Идеал A будет, очевидно, нулем этой Ω-фактор-группы.

Применяя все сказанное к случаю групп, мы получаем, что *все конгруенции в группе G исчерпываются ее разложениями по различным нормальным делителям.* Можно говорить, следовательно, о *фактор-группе группы G по нормальному делителю A* и обозначать ее через G/A.

С другой стороны, *все конгруенции в кольце R исчерпываются его разложениями по различным (двусторонним) идеалам,* а поэтому мы будем говорить о *фактор-кольце кольца R по идеалу A* и обозначать его через R/A.

Из доказанной выше теоремы вытекает еще одно замечание. Если φ — гомоморфное отображение Ω-группы G на Ω-группу G', то *ядром* гомоморфизма φ называется совокупность тех элементов из G, которые при φ отображаются в нуль Ω-группы G'. Из теоремы III.2.5 и из теоремы о гомоморфизмах III.1.8. следует:

Ядрами гомоморфизмов Ω-группы служат ее идеалы и только они. Гомоморфный образ Ω-группы определяется с точностью до изоморфизма ядром рассматриваемого гомоморфизма.

7. Рассмотрим некоторые простейшие, но важные примеры.

Всякий гомоморфный образ циклической группы сам, является циклической группой.

Действительно, если G' — образ циклической группы $G = \{a\}$ при гомоморфизме φ, причем $a\varphi = a'$, то для любого элемента $g' \in G'$ можно найти прообраз $a^k \in G$, а поэтому

$$g' = a^k\varphi = (a\varphi)^k = a'^k,$$

т. е. $G' = \{a'\}$.

Найдем теперь все гомоморфные образы бесконечной циклической группы, в качестве которой, по II.4.2, можно взять аддитивную группу целых чисел. В II.4.2 дано обозрение подгрупп этой группы, причем все они будут, конечно, нормальными делителями. Если $\{n\}$ — подгруппа, составленная из чисел, кратных натуральному числу n, то два числа тогда и только тогда будут принадлежать к одному смежному классу по этой подгруппе, если их разность нацело делится на n, т. е. если эти числа при делении на n дают один и тот же остаток. Так как остатками при делении целых чисел на n могут служить лишь числа $0, 1, 2, \ldots, n-1$, то фактор-группа аддитивной группы целых чисел по подгруппе $\{n\}$ будет конечной группой порядка n, притом, как показано выше, циклической. Число n было произвольным, а поэтому, учитывая описание циклических групп, данное в II.4.2, мы приходим к следующему результату:

Гомоморфными образами бесконечной циклической группы служат всевозможные циклические группы и только они.

8. Найдем теперь все гомоморфные образы кольца целых чисел C. Как отмечено в II.7.8, все подгруппы аддитивной

группы этого кольца служат в нем идеалами, а поэтому нам остается рассмотреть фактор-кольца по этим идеалам.

Фактор-кольцо по нуль-идеалу изоморфно, конечно, самому кольцу C. Фактор-кольцо кольца C по идеалу чисел, кратных натуральному числу n, мы обозначим через C_n и назовем *кольцом вычетов по модулю n*. Из сказанного в предыдущем пункте следует, что это кольцо конечно и состоит из n элементов, что его аддитивная группа циклическая и что в смежных классах, составляющих это кольцо, в качестве представителей можно выбрать числа $0, 1, 2, \ldots, n-1$. В соответствии с этим сами элементы кольца C_n могут быть обозначены через $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}$.

Из определения операций в фактор-кольце (ср. III.1.7) вытекают следующие правила оперирования в кольце C_n: если $0 \leqslant k, \ l < n$ и $k+l = nq_1 + r_1, \ kl = nq_2 + r_2$, где $0 \leqslant r_1, r_2 < n$, то

$$\overline{k} + \overline{l} = \overline{r}_1, \quad \overline{k} \cdot \overline{l} = \overline{r}_2.$$

В частности, элемент $\overline{0}$ будет нулем кольца C_n, элемент $\overline{1}$ — его единицей.

Кольцо C_n обладает делителями нуля при составном числе n, но является полем, если число n простое.

В самом деле, если $n = kl, \ 1 < k, \ l < n$, то элементы k и l кольца C_n отличны от нуля $\overline{0}$ этого кольца, но $\overline{k} \cdot \overline{l} = \overline{0}$. Если же число n простое, $n = p \geqslant 2$, то всякое число k, удовлетворяющее неравенствам $1 \leqslant k \leqslant p-1$, будет с p взаимно простым. Существуют, следовательно, такие целые числа l и m, что имеет место равенство

$$kl + pm = 1,$$

причем число l можно выбрать так, что $1 \leqslant l \leqslant p-1$. Отсюда следует, что в кольце вычетов C_p выполняется равенство

$$\overline{k} \cdot \overline{l} = \overline{1},$$

т. е. всякий элемент из C_p, отличный от нуля, обладает в кольце C_p обратным элементом, а поэтому это кольцо будет полем.

Кольца вычетов C_p по простым модулям p, $p = 2, 3, 5, \ldots$, являются первыми примерами конечных полей, причем они играют в теории полей и тел весьма важную роль, как будет сейчас показано.

9. Пусть дано тело K, не обязательно ассоциативное (см. II.6.1). Пересечение всех подтел тела K само будет подтелом, которое мы временно назовем простым подтелом тела K. Нашей целью является описание строения этого подтела.

Назовем *центром* произвольного кольца R совокупность элементов a из R, перестановочных с каждым элементом кольца R, т. е.

$$ax = xa \tag{6}$$

для всех $x \in R$, и, кроме того, удовлетворяющих для всех $x, y \in R$ условиям

$$(ax)\,y = a\,(xy), \qquad (xy)\,a = x\,(ya), \tag{7}$$

а поэтому и условию

$$(xa)\,y = x\,(ay),$$

так как, по (6) и (7),

$$(xa)\,y = (ax)\,y = a\,(xy) = (xy)\,a = x\,(ya) = x\,(ay).$$

Нуль кольца R, а также его единица, если она существует, принадлежат, понятно, к центру этого кольца.

Центр кольца R является ассоциативно-коммутативным подкольцом. Центр тела является подполем.

Действительно, если элементы a и b входят в центр кольца R, то для любых $x, y \in R$

$$(a \pm b)\,x = ax \pm bx = xa \pm xb = x\,(a \pm b),$$

$$[(a \pm b)\,x]\,y = (ax \pm bx)\,y = (ax)\,y \pm (bx)\,y =$$

$$= a\,(xy) \pm b\,(xy) = (a \pm b)\,(xy);$$

так же проверяется и второе из условий (7). С другой стороны,

$$(ab)\,x = a\,(bx) = a\,(xb) = (ax)\,b = (xa)\,b = x\,(ab),$$

$$[(ab)\,x]\,y = [a\,(bx)]\,y = a\,[(bx)\,y] = a\,[b\,(xy)] = (ab)\,(xy).$$

Таким образом, центр кольца R оказался подкольцом, притом, очевидно, ассоциативно-коммутативным.

Если же R — тело с единицей e и a — элемент из его центра, причем $a \neq 0$, то, решая уравнения $ax = e$ и $ya = e$ и учитывая, что a содержится в центре, мы найдем одно-

значно определенный обратный элемент a^{-1}, одновременно левый и правый. Тогда для любых $x, y \in R$

$$a^{-1}x = (a^{-1}x)(aa^{-1}) = [(a^{-1}x)\,a]\,a^{-1} = [a^{-1}(xa)]\,a^{-1} =$$
$$= [a^{-1}(ax)]\,a^{-1} = [(a^{-1}a)\,x]\,a^{-1} = xa^{-1},$$
$$(a^{-1}x)y = (a^{-1}a)\,[(a^{-1}x)y] = a^{-1}\{a\,[(a^{-1}x)y]\} =$$
$$= a^{-1}\{[a\,(a^{-1}x)]\,y\} = a^{-1}\{[(aa^{-1})\,x]\,y\} = a^{-1}(xy);$$

так же проверяется и второе из условий (7). Этим доказано, что элемент a^{-1} принадлежит к центру тела R, а поэтому центр будет полем.

10. Вообще говоря, центр кольца может случайно состоять лишь из одного нуля. Если же K — тело с единицей e, то его центр непременно содержит e, а также все кратные ne, где n — любое целое число. Все эти кратные составляют в K ассоциативно-коммутативное подкольцо $C^{(K)}$, содержащееся во всех подтелах тела K, а поэтому и в его простом подтеле. С другой стороны, простое подтело должно содержаться в центре тела K, так как центр является подполем, а поэтому *простое подтело ассоциативно и коммутативно.* В дальнейшем можно говорить, следовательно, не о простом подтеле, а о *простом подполе* тела K.

Простое подполе тела K изоморфно или полю рациональных чисел, или же одному из полей вычетов C_p по простому модулю p.

Для доказательства рассмотрим отображение $n \to ne$ кольца целых чисел C на кольцо $C^{(K)}$. Это отображение будет гомоморфным, а поэтому, как показано в III.2.8, кольцо $C^{(K)}$ изоморфно или кольцу целых чисел C, или же некоторому кольцу вычетов C_n, даже некоторому полю вычетов C_p по простому модулю p, так как в теле K нет делителей нуля. В последнем случае поле C_p и будет искомым простым подполем тела K. Если же имеет место первый случай, то центр тела K, являющийся полем и содержащий подкольцо $C^{(K)}$, изоморфное кольцу целых чисел, будет содержать и поле дробей этого подкольца, изоморфное (см. II.5.7) полю рациональных чисел. Это поле и будет простым подполем тела K.

11. Если простое подполе тела K изоморфно полю рациональных чисел, то говорят, что тело K *без характеристики*

(или что оно имеет *характеристику нуль*); таковы, в частности, все числовые поля. Если же простое подполе тела K изоморфно полю вычетов C_p по простому модулю p, то K называется телом *конечной характеристики* или *простой характеристики*, а именно *характеристики* p.

Всякий отличный от нуля элемент тела K без характеристики (характеристики p) имеет в аддитивной группе этого тела бесконечный порядок (порядок p).

Действительно, если тело K без характеристики и $a \in K$, $a \neq 0$, то из $na = 0$ следовало бы $(ne) \cdot a = 0$, т. е. $ne = 0$, так как в K нет делителей нуля, откуда $n = 0$. Если же характеристика тела K равна p, то для любого a из K будет

$$pa = (pe)\, a = 0 \cdot a = 0,$$

а поэтому, если $a \neq 0$, порядок этого элемента будет равен простому числу p.

12. Вернемся к рассмотрению произвольной Ω-группы G. Возьмем в ней идеал A и Ω-фактор-группу по нему $G' = G/A$. Пусть B' — произвольная Ω-подгруппы Ω-группы G', а B — ее полный прообраз в G при естественном гомоморфизме G на G', т. е. совокупность тех элементов из G, которые лежат в смежных классах, составляющих B'. Докажем, что *B будет в G Ω-подгруппой.*

В самом деле, если $x, y \in B$, т. е. $x + A, y + A \in B'$, то

$$(x + y) + A = (x + A) + (y + A) \in B',$$

$$-x + A = -(x + A) \in B',$$

т. е. $x + y \in B$, $-x \in B$. С другой стороны, для n-арной операции $\omega \in \Omega$ и элементов $x_1, x_2, \ldots, x_n \in B$ из включений $x_i + A \in B'$, равенств $x_i + A = A + x_i$, $i = 1, 2, \ldots, n$, и включения (4) следует равенство

$$x_1 x_2 \ldots x_n \omega + A = (x_1 + A)(x_2 + A) \ldots (x_n + A)\, \omega \in B',$$

а поэтому $x_1 x_2 \ldots x_n \omega \in B$.

Ω-подгруппа B, построенная нами, содержит, конечно, идеал A. Обратно, *если дана произвольная Ω-подгруппа B Ω-группы G, содержащая идеал A, то ее образ B' при естественном гомоморфизме Ω-группы G на Ω-группу $G' = G/A$ будет Ω-подгруппой, причем B служит для B' полным прообразом.*

Действительно, естественный гомоморфизм G на G' индуцирует гомоморфизм B в G', а поэтому, в силу сказанного в III.1.5, B' будет Ω-подгруппой в G'. С другой стороны, из $B \supseteq A$ следует, что всякий элемент из G, входящий в смежный класс по идеалу A, принадлежащий к B', будет содержаться в B.

Нами доказана следующая теорема:

Относя всякой Ω-подгруппе Ω-фактор-группы $G' = G/A$ ее полный прообраз при естественном гомоморфизме G на G', мы получаем взаимно однозначное соответствие, сохраняющее отношение включения, между всеми Ω-подгруппами Ω-группы G' и всеми теми Ω-подгруппами Ω-группы G, которые содержат идеал A.

13. Дополним этот результат следующей теоремой:

При соответствии, указанном в предшествующей теореме, идеалу одной из Ω-групп G, G' соответствует идеал другой Ω-группы, причем Ω-фактор-группы по соответствующим друг другу идеалам изоморфны между собой.

В самом деле, если B' является идеалом Ω-группы $G' = G/A$, а B — его полным прообразом в G, то последовательное выполнение естественных гомоморфизмов G на G' и G' на $G'' = G'/B'$ будет, как следует из сказанного в III.1.5, гомоморфизмом G на G''. Ядро этого гомоморфизма (см. III.2.6) составляют те элементы из G, которые при отображении G на G' отображаются в B', т. е. элементы, составляющие Ω-подгруппу B. Отсюда следует, ввиду III.2.6, III.2.5 и III.1.8, что B будет идеалом Ω-группы G и что Ω-фактор-группы G/B и G'/B' изоморфны между собой.

Пусть теперь B будет идеалом Ω-группы G, а B' — его образом при естественном гомоморфизме G на G'. Если $b \in B$, $x \in G$, то $b + A \in B'$, $x + A \in G'$. Так как

$$-x + b + x \in B,$$

то

$$-(x + A) + (b + A) + (x + A) = (-x + b + x) + A \in B',$$

т. е. B' является нормальным делителем аддитивной группы Ω-группы G'. Если же дана n-арная операция $\pi \in \Omega$ и произвольные элементы $b \in B$ и $x_1, x_2, \ldots, x_n \in G$, т. е.

$b+A \in B'$, $x_i+A \in G'$, $i=1, 2, \ldots, n$, то из

$$-x_1x_2 \ldots x_n\omega + x_1 \ldots x_{i-1}(b+x_i)x_{i+1} \ldots x_n\omega = b_0 \in B,$$
$$i=1, 2, \ldots, n,$$

следует

$$-(x_1+A)(x_2+A) \ldots (x_n+A)\,\omega + (x_1+A) \ldots$$
$$\ldots (x_{i-1}+A)[(b+A)+(x_i+A)](x_{i+1}+A) \ldots (x_n+A)\,\omega =$$
$$= b_0 + A \in B', \qquad i=1, 2, \ldots, n.$$

Этим доказано, что B' будет идеалом в G'.

Заметим, что в последней части доказательства мы не пользовались предположением, что $B \supseteq A$.

§ 3. Автоморфизмы, эндоморфизмы. Поле p-адических чисел

1. Пусть G — универсальная алгебра. Всякое изоморфное отображение алгебры G на себя называется *автоморфизмом*. Так, G всегда обладает *тождественным автоморфизмом* — это будет тождественное отображение G на себя. Примерами нетривиальных автоморфизмов служат автоморфизм аддитивной группы целых чисел, переводящий всякое целое число k в число $-k$, а также автоморфизм поля комплексных чисел, переводящий всякое комплексное число $a+bi$ в число $a-bi$.

Результат последовательного выполнения автоморфизмов алгебры G снова будет автоморфизмом. По этому умножению, ассоциативному ввиду I.1.2, все автоморфизмы алгебры G составляют группу, так как единицей служит тождественный автоморфизм, а обратное отображение для любого автоморфизма также будет автоморфизмом; эта группа называется *группой автоморфизмов* универсальной алгебры G.

* Всякая группа изоморфна группе всех автоморфизмов некоторой универсальной алгебры [Биркгоф, Revista Unione Mat. Argentina **11** (1946), 155—157].

Всякая группа изоморфно вкладывается в группу автоморфизмов некоторой абелевой группы. *

2. Пусть дана некоммутативная полугруппа G, обладающая единицей, и в ней выбран *делитель единицы* ε, т. е. элемент, для которого в G существует обратный элемент ε^{-1},

одновременно левый и правый (ср. II.8.1). Трансформируя полугруппу G элементом ε, т. е. отображая всякий элемент x из G в элемент $\varepsilon^{-1}x\varepsilon$, мы получаем автоморфизм полугруппы G, называемый ее *внутренним автоморфизмом*. Действительно, из

$$\varepsilon^{-1}x\varepsilon = \varepsilon^{-1}y\varepsilon$$

следует $x = y$, т. е. рассматриваемое отображение взаимно однозначно. Далее, из

$$x = \varepsilon^{-1}(\varepsilon x\varepsilon^{-1})\varepsilon$$

вытекает, что это будет отображение на всю полугруппу G. Наконец, равенство

$$\varepsilon^{-1}(xy)\varepsilon = \varepsilon^{-1}x\varepsilon \cdot \varepsilon^{-1}y\varepsilon$$

доказывает изоморфность этого отображения.

Ясно, что коммутативная полугруппа с единицей, в частности всякая абелева группа, обладает единственным внутренним автоморфизмом, а именно тождественным.

Легко проверяется, что произведение трансформирований полугруппы с единицей элементами ε и δ совпадает с трансформированием элементом $\varepsilon\delta$, а обратным для трансформирования элементом ε служит трансформирование элементом ε^{-1}. Отсюда следует, что *внутренние автоморфизмы полугруппы с единицей составляют подгруппу в группе всех автоморфизмов этой полугруппы.*

Подгруппа внутренних автоморфизмов будет даже нормальным делителем в группе всех автоморфизмов рассматриваемой полугруппы G. В самом деле, пусть даны произвольный автоморфизм φ полугруппы G и ее внутренний автоморфизм α, порожденный делителем единицы ε. Тогда для любого $x \in G$

$$x(\varphi^{-1}\alpha\varphi) = [\varepsilon^{-1}(x\varphi^{-1})\varepsilon]\varphi =$$
$$= (\varepsilon^{-1})\varphi \cdot (x\varphi^{-1})\varphi \cdot (\varepsilon\varphi) = (\varepsilon\varphi)^{-1}x(\varepsilon\varphi),$$

т. е. автоморфизм $\varphi^{-1}\alpha\varphi$ является внутренним и порождается делителем единицы $\varepsilon\varphi$.

С другой стороны, если G — группа и, следовательно, все элементы из G являются делителями единицы, то мы получаем гомоморфное отображение всей группы G на группу ее внутренних автоморфизмов, ставя в соответствие всякому элементу из G порождаемый им внутренний автоморфизм. Ядром

этого гомоморфизма (см. III.2.6) служит совокупность элементов из G, перестановочных с каждым элементом этой группы; она называется *центром* группы G. Из теоремы о гомоморфизмах вытекает, что *центр группы G является нормальным делителем, а группа внутренних автоморфизмов группы G изоморфна фактор-группе группы G по ее центру.*

3. Понятие внутреннего автоморфизма переносится на случай любого ассоциативного кольца с единицей. Именно, *всякий внутренний автоморфизм мультипликативной полугруппы ассоциативного кольца R с единицей будет автоморфизмом самого этого кольца,* так как

$$\varepsilon^{-1}(x+y)\varepsilon = \varepsilon^{-1}x\varepsilon + \varepsilon^{-1}y\varepsilon.$$

Такой автоморфизм естественно назвать *внутренним автоморфизмом* кольца R.

4. Всякое гомоморфное отображение универсальной алгебры G в себя называется ее *эндоморфизмом.* К числу эндоморфизмов принадлежат, в частности, все автоморфизмы, а также все изоморфные отображения G в себя и все гомоморфные отображения G на себя.

Результат последовательного выполнения эндоморфизмов снова будет эндоморфизмом, а поэтому все эндоморфизмы составляют по этому умножению, ассоциативному ввиду I.1.2, полугруппу, называемую *полугруппой эндоморфизмов* универсальной алгебры G.

Эта полугруппа эндоморфизмов обладает единицей — ею служит тождественный автоморфизм. Делителями единицы полугруппы эндоморфизмов являются автоморфизмы и только они, так как только в случае автоморфизмов возможно однозначное обратное отображение.

Полезно отметить, что тождественный автоморфизм универсальной алгебры G играет роль единицы не только для эндоморфизмов этой алгебры: он является, очевидно, левой единицей для всех гомоморфных отображений алгебры G в любые другие алгебры, а также является правой единицей для всех гомоморфных отображений некоторых алгебр в алгебру G.

5. Займемся сейчас рассмотрением гомоморфных отображений Ω-групп. Если φ и ψ — два гомоморфизма

Ω-группы G в Ω-группу G', то отображение

$$a(\varphi+\psi)=a\varphi+a\psi, \quad a\in G, \tag{1}$$

в общем случае не является гомоморфизмом. Оно тогда и только тогда будет гомоморфизмом (см. III.1.5), если для любых $a, b\in G$

$$(a+b)(\varphi+\psi)=a(\varphi+\psi)+b(\varphi+\psi),$$

т. е. если

$$b\varphi+a\psi=a\psi+b\varphi, \tag{2}$$

и если для любой n-арной операции $\omega\in\Omega$ и любых $a_1, a_2, \ldots, a_n\in G$

$$(a_1a_2\ldots a_n\omega)(\varphi+\psi)=[a_1(\varphi+\psi)][a_2(\varphi+\psi)]\ldots[a_n(\varphi+\psi)]\omega,$$

т. е. если

$$(a_1\varphi)(a_2\varphi)\ldots(a_n\varphi)\omega+(a_1\psi)(a_2\psi)\ldots(a_n\psi)\omega=$$
$$=(a_1\varphi+a_1\psi)(a_2\varphi+a_2\psi)\ldots(a_n\varphi+a_n\psi)\omega. \tag{3}$$

Если условия (2) и (3) выполняются, то гомоморфизмы φ и ψ называются *суммируемыми*, а гомоморфизм $\varphi+\psi$ — их *суммой*.

Условие (2) показывает для случая группы без мультиоператоров, что *гомоморфизмы φ и ψ группы G в группу G' тогда и только тогда суммируемы, если подгруппы $G\varphi$ и $G\psi$ группы G' поэлементно перестановочны.* Если же рассматриваются гомоморфизмы φ и ψ кольца R в кольцо R', то условие (2) выполняется автоматически, а условие (3) превращается в условие: для любых $a, b\in R$

$$a\varphi\cdot b\varphi+a\psi\cdot b\psi=(a\varphi+a\psi)(b\varphi+b\psi),$$

т. е.

$$a\varphi\cdot b\psi+a\psi\cdot b\varphi=0.$$

6. Нами определено частичное сложение гомоморфизмов Ω-группы G в Ω-группу G'. Это сложение коммутативно, так как из (2) для всех $a\in G$ следует

$$a\varphi+a\psi=a\psi+a\varphi,$$

т. е., ввиду (1), $\varphi+\psi=\psi+\varphi$. Оно и ассоциативно, так как для всех $a\in G$

$$a[(\varphi+\psi)+\chi]=a[\varphi+(\psi+\chi)]=a\varphi+a\psi+a\chi.$$

Отсюда следует, что если сумма $\sum_{i=1}^{n} \varphi_i$ гомоморфизмов $\varphi_i\colon G \to G'$, $i = 1, 2, \ldots, n$, является гомоморфизмом, то она однозначно определена. Заметим, что можно говорить и о *сумме бесконечного семейства гомоморфизмов* $\varphi_i\colon G \to G'$, $i \in I$, если дополнительно предположить, что для любого $a \in G$ лишь конечное число элементов $a\varphi_i$, $i \in I$, отлично от нуля.

Если гомоморфизмы φ *и* ψ Ω-*группы* G *в* Ω-*группу* G' *суммируемы, то для любых* Ω-*групп* H *и* F *и любых гомоморфизмов* $\sigma\colon H \to G$ *и* $\tau\colon G' \to F$ *гомоморфизмы* $\sigma\varphi$ *и* $\sigma\psi$, *а также* $\varphi\tau$ *и* $\psi\tau$ (см. III.1.5) *будут суммируемыми и*

$$\sigma(\varphi + \psi) = \sigma\varphi + \sigma\psi, \quad (\varphi + \psi)\tau = \varphi\tau + \psi\tau. \tag{4}$$

Действительно, если $a \in H$, то

$$a[\sigma(\varphi + \psi)] = (a\sigma)(\varphi + \psi) = (a\sigma)\varphi + (a\sigma)\psi =$$
$$= a(\sigma\varphi) + a(\sigma\psi) = a(\sigma\varphi + \sigma\psi),$$

т. е. отображение $\sigma\varphi + \sigma\psi$ будет гомоморфизмом и имеет место первое из равенств (4). Столь же просто доказывается и второе утверждение теоремы. Заметим, что из существования сумм, стоящих в правых частях равенств (4), не вытекает существование сумм, стоящих в их левых частях.

7. Ввиду равенства $0 + 0 = 0$, где 0 — нуль Ω-группы, и равенства (1) из III.2.1 отображение, переводящее всякий элемент Ω-группы G в нуль Ω-группы G', будет гомоморфизмом; это *нулевой гомоморфизм* G в G'.

Немедленно проверяются следующие утверждения: всякий гомоморфизм $\varphi\colon G \to G'$ суммируем с нулевым гомоморфизмом, причем сумма равна φ; если гомоморфизмы $\varphi, \psi\colon G \to G'$ суммируемы и

$$\varphi + \psi = \varphi,$$

то гомоморфизм ψ нулевой; наконец, для любых Ω-групп H и F и любых гомоморфизмов $\sigma\colon H \to G$ и $\tau\colon G' \to F$ произведение σ на нулевой гомоморфизм G в G' равно нулевому гомоморфизму H в G', а произведение нулевого гомоморфизма G в G' на τ равно нулевому гомоморфизму G в F.

8. Рассмотрим гомоморфизмы некоторой группы G (без мультиоператоров) в абелеву группу G'; будем считать

первую группу записанной мультипликативно, а вторую аддитивно. В этом случае, ввиду (2), любые два гомоморфизма суммируемы. С другой стороны, для любого гомоморфизма $\varphi\colon G \to G'$ отображение $-\varphi$, определяемое равенством

$$a(-\varphi) = -a\varphi, \quad a \in G,$$

будет в этом случае гомоморфизмом, так как для любых $a, b \in G$

$$(ab)(-\varphi) = -(ab)\varphi = -(a\varphi + b\varphi) = (-a\varphi) + (-b\varphi) = \\ = a(-\varphi) + b(-\varphi).$$

Этот гомоморфизм будет противоположным для φ, так как для $a \in G$

$$a[\varphi + (-\varphi)] = a\varphi + a(-\varphi) = a\varphi - a\varphi = 0,$$

т. е. $\varphi + (-\varphi)$ равно нулевому гомоморфизму.

Таким образом, *гомоморфизмы любой группы G в абелеву группу G' составляют по сложению абелеву группу.*

Рассмотрим, в частности, эндоморфизмы абелевой группы G. Они составляют по сложению абелеву группу, а по умножению полугруппу с единицей (см. III.3.4), причем справедливы законы дистрибутивности (4). Мы получаем, что *эндоморфизмы абелевой группы G составляют относительно операций сложения и умножения эндоморфизмов ассоциативное кольцо с единицей.* Это кольцо называется *кольцом эндоморфизмов* абелевой группы G.

Всякое ассоциативное кольцо изоморфно вкладывается в кольцо эндоморфизмов некоторой абелевой группы.

Ввиду II.4.4 можно считать, что рассматриваемое ассоциативное кольцо R обладает единицей 1. Если a — любой элемент из R, то отображение, переводящее всякий элемент x из R в элемент xa, будет эндоморфизмом аддитивной группы кольца R, так как

$$(x + y)a = xa + ya.$$

Сумме и произведению элементов из R соответствуют сумма и произведение соответствующих эндоморфизмов, как показывают равенства

$$x(a + b) = xa + xb,$$

$$x(ab) = (xa)b.$$

Наконец, различным элементам из R соответствуют различные эндоморфизмы, так как из $a \neq b$ следует $1 \cdot a \neq 1 \cdot b$.

9. *Кольцо эндоморфизмов бесконечной циклической группы изоморфно кольцу целых чисел С.*

В самом деле, если a — образующий элемент заданной группы, записанной аддитивно, и если эндоморфизм φ переводит элемент a в элемент ka, где k — некоторое целое число, то

$$(na)\varphi = nka, \tag{5}$$

т. е. эндоморфизм φ вполне определяется заданием числа k. Обратно, отображение φ нашей группы, определяемое равенством (5), действительно будет эндоморфизмом. Таким образом, между эндоморфизмами бесконечной циклической группы $\{a\}$ и целыми числами установлено взаимно однозначное соответствие. Изоморфность этого соответствия вытекает из того, что если

$$a\varphi = ka, \quad a\psi = la,$$

то

$$a(\varphi + \psi) = a\varphi + a\psi = ka + la = (k + l)\,a,$$

$$a(\varphi\psi) = (a\varphi)\psi = (ka)\psi = (kl)\,a.$$

Так как в кольце целых чисел лишь числа 1 и -1 обладают обратными, то *группа автоморфизмов бесконечной циклической группы $\{a\}$ является циклической группой второго порядка,* причем состоит из тождественного автоморфизма и автоморфизма, переводящего всякий элемент группы в его противоположный.

* Кольцо эндоморфизмов конечной циклической группы порядка n изоморфно кольцу вычетов C_n по модулю n.

Кольцо эндоморфизмов аддитивной группы рациональных чисел изоморфно полю рациональных чисел. Таким образом, всякий ненулевой эндоморфизм этой группы является автоморфизмом. *

10. В теории абелевых групп очень большую роль играет *группа типа p^∞,* где p — простое число: это мультипликативная группа всех тех комплексных чисел, которые являются корнями из единицы некоторой степени p^n, $n = 1, 2, \ldots$ Как известно, группа корней из единицы степени p^n, где n фиксировано, будет циклической порядка p^n с образующим элементом

$$a_n = \cos\frac{2\pi}{p^n} + i\sin\frac{2\pi}{p^n}.$$

Группа типа p^∞ будет, следовательно, абелевой и бесконечной, а именно объединением возрастающей последовательности циклических подгрупп $\{a_n\}$, $n = 1, 2, \ldots$ Система элементов

$$a_n, \quad n = 1, 2, \ldots, \tag{6}$$

служит для этой группы системой образующих. Если мы условимся употреблять для группы типа p^∞ аддитивную запись вместо мультипликативной, то образующие элементы (6) будут связаны равенствами

$$pa_1 = 0, \quad pa_{n+1} = a_n, \quad n = 1, 2, \ldots \tag{7}$$

Найдем кольцо эндоморфизмов группы типа p^∞. Если φ — эндоморфизм этой группы, то он вполне определяется заданием образов всех образующих элементов (6). Так как элемент a_n имеет порядок p^n, то и порядок элемента $a_n\varphi$ не может превосходить числа p^n. Все такие элементы лежат, однако, в циклической подгруппе $\{a_n\}$, а поэтому

$$a_n\varphi = k_n a_n, \quad n = 1, 2, \ldots, \tag{8}$$

где

$$0 \leqslant k_n < p^n. \tag{9}$$

Далее, равенства (7), справедливые для элементов (6), должны выполняться и для их образов при эндоморфизме φ, а поэтому

$$p(a_{n+1}\varphi) = a_n\varphi,$$

откуда

$$p(k_{n+1}a_{n+1}) = k_{n+1}a_n = k_n a_n.$$

Отсюда следует, что разность $k_{n+1} - k_n$ должна нацело делиться на порядок p^n элемента a_n, или, используя символику, принятую в теории чисел,

$$k_{n+1} \equiv k_n \pmod{p^n}. \tag{10}$$

Таким образом, всякому эндоморфизму φ группы типа p^∞ соответствует последовательность целых неотрицательных чисел

$$(k_1, k_2, \ldots, k_n, \ldots), \tag{11}$$

подчиненных условиям (9) и (10). Двум различным эндоморфизмам соответствуют при этом различные последовательности вида (11), так как хотя бы один из образующих элементов (6) имеет при этих эндоморфизмах различные образы.

Обратно, всякая последовательность вида (11), подчиненная условиям (9) и (10), соответствует некоторому эндоморфизму φ группы типа p^∞. Именно, на основании равенств (8) можно определить отображение φ для всех элементов нашей группы, причем легко проверяется, что это отображение будет эндоморфизмом.

Если в группе типа p^∞ взяты два эндоморфизма, φ и ψ, заданные соответственно последовательностями (11) и

$$(l_1,\ l_2,\ \ldots,\ l_n,\ \ldots), \tag{12}$$

то

$$a_n(\varphi+\psi)=(k_n+l_n)\,a_n,$$

$$a_n(\varphi\psi)=(k_nl_n)\,a_n.$$

Из справедливости для последовательностей (11) и (12) условий типа условия (10) следует, что

$$k_{n+1}+l_{n+1}\equiv k_n+l_n \pmod{p^n},$$

$$k_{n+1}l_{n+1}\equiv k_nl_n \pmod{p^n};$$

эти сравнения не нарушатся, если их левые части будут заменены положительными вычетами по модулю p^{n+1} (т. е. остатками от деления на p^{n+1}), а правые — по модулю p^n, чем достигается выполнение и условий (9).

Таким образом, кольцо эндоморфизмов группы типа p^∞ изоморфно кольцу последовательностей целых неотрицательных чисел вида (11), удовлетворяющих условиям (9) и (10), причем сложение и умножение этих последовательностей производятся покомпонентно с последующим переходом на каждом n-м месте к вычету по модулю p^n. Это коммутативное кольцо называется *кольцом целых p-адических чисел*. Его нулем служит последовательность (0, 0, ..., 0, ...), соответствующая нулевому эндоморфизму группы типа p^∞, а единицей — последовательность (1, 1, ..., 1, ...), соответствующая тождественному автоморфизму этой группы.

11. Для целых p-адических чисел возможна и другая запись. Пусть целое p-адическое число α задано последовательностью целых неотрицательных чисел (11), подчиненной условиям (9) и (10). Если мы положим

$$a_0=k_1,\quad a_n=\frac{k_{n+1}-k_n}{p^n},\quad n=1,\ 2,\ \ldots, \tag{13}$$

то все a_n, $n=0, 1, 2, \ldots$, будут целыми, а именно будут некоторыми положительными вычетами по модулю p, т. е.

$$0 \leqslant a_n < p, \quad n=0, 1, 2, \ldots \tag{14}$$

Так как, по (13),

$$k_n = a_0 + a_1 p + a_2 p^2 + \ldots + a_{n-1} p^{n-1}, \quad n=1, 2, \ldots, \tag{15}$$

то целому p-адическому числу α можно поставить в соответствие бесконечный ряд

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_n p^n + \ldots; \tag{16}$$

различным целым p-адическим числам соответствуют при этом, очевидно, различные ряды вида (16). Обратно, если произвольный ряд вида (16), коэффициенты которого целые и подчинены условиям (14), то, определяя числа k_n равенствами (15), мы получим последовательность вида (11), удовлетворяющую условиям (9) и (10).

Между всеми целыми p-адическими числами и всеми рядами вида (16), коэффициенты которых являются вычетами по модулю p, мы установили взаимно однозначное соответствие. Используя (15), легко перенести операции, определенные для целых p-адических чисел, на ряды вида (16): если число α задается рядом (16), а число β — рядом

$$b_0 + b_1 p + b_2 p^2 + \ldots + b_n p^n + \ldots,$$

также удовлетворяющим условиям (14), то

$$\alpha + \beta = c_0 + c_1 p + c_2 p^2 + \ldots + c_n p^n + \ldots,$$

где все коэффициенты c_n являются вычетами по модулю p, причем

$$c_0 = a_0 + b_0 - pq_0,$$

$$c_n = a_n + b_n + q_{n-1} - pq_n, \quad n=1, 2, \ldots;$$

с другой стороны,

$$\alpha\beta = d_0 + d_1 p + d_2 p^2 + \ldots + d_n p^n + \ldots,$$

где коэффициенты d_n также будут вычетами по модулю p, причем

$$d_0 = a_0 b_0 - ps_0,$$

$$d_n = \sum_{k+l=n} a_k b_l + s_{n-1} - ps_n, \quad n=1, 2, \ldots$$

12. Из этого описания умножения немедленно следует, ввиду простоты числа p, что *кольцо целых p-адических чисел не содержит делителей нуля* и поэтому, по II.5.5, для него существует поле дробей, называемое *полем p-адических чисел*. Это поле можно построить следующим образом.

Рассмотрим всевозможные ряды вида

$$a_k p^k + a_{k+1} p^{k+1} + \ldots + a_n p^n + \ldots, \qquad (17)$$

где все коэффициенты a_n являются вычетами по модулю p, а k больше, равно или меньше нуля; ряд (17) может содержать, следовательно, конечное число членов с отрицательными степенями числа p. Если при этом не все коэффициенты ряда (17) равны нулю, то будем считать, что $a_k \neq 0$; с другой стороны, ряды с нулевыми коэффициентами все считаются между собою тождественными.

Перенося естественным путем определение операций над рядами вида (16) на ряды вида (17), мы получим, что эти последние ряды составляют ассоциативно-коммутативное кольцо, единицей которого служит такой ряд вида (17), у которого $a_0 = 1$, а все остальные коэффициенты равны нулю. Это кольцо будет даже полем: если ряд (17) отличен от нуля, т. е. $a_k \neq 0$, то обратным для него будет ряд

$$b_{-k} p^{-k} + b_{-k+1} p^{-k+1} + \ldots + b_n p^n + \ldots,$$

коэффициенты которого, являющиеся вычетами по модулю p, последовательно находятся из следующих уравнений, разрешимых ввиду простоты числа p:

$$\begin{aligned}
a_k b_{-k} - p s_{-k} &= 1, \\
a_k b_{-k+1} + a_{k+1} b_{-k} + s_{-k} - p s_{-k+1} &= 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
a_k b_n + a_{k+1} b_{n-1} + \ldots + a_{n+2k} b_{-k} + s_{n-1} - p s_n &= 0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Те ряды вида (17), у которых $k \geqslant 0$, составляют в построенном нами поле подкольцо, изоморфное кольцу целых p-адических чисел. Само это поле служит для него полем дробей: всякий ряд вида (17) после умножения (в смысле нашего определения этой операции) на некоторую положительную степень числа p (которая является, конечно, целым p-адическим числом) превращается в ряд вида (16), т. е. в целое p-адическое число.

§ 4. Нормальные и композиционные ряды

1. *Если в* Ω*-группе* G *даны идеал* A *и* Ω*-подгруппа* B*, то порожденная ими* Ω*-подгруппа* $\{A, B\}$ *состоит из тех элементов из* G*, которые хотя бы одним способом могут быть записаны в виде* $a+b$*, где* $a \in A$*,* $b \in B$*, а поэтому имеет смысл запись*

$$\{A, B\} = A + B. \tag{1}$$

Ясно, в самом деле, что всякий элемент вида $a+b$ принадлежит к $\{A, B\}$. Покажем, что эти элементы сами составляют Ω-подгруппу, которая содержит, понятно, и A и B. Действительно, если $a, a' \in A$, $b, b' \in B$, то $b+a'-b \in A$, так как A является нормальным делителем аддитивной группы. Поэтому

$$(a+b)+(a'+b') = [a+(b+a'-b)]+(b+b') = a''+b'',$$

где $a'' \in A$, $b'' \in B$. Далее, $0 = 0+0$, но нуль содержится и в A, и в B. Если же дан элемент $a+b$, то противоположным для него будет элемент $a'-b$, где $a' = -b-a+b \in A$. Наконец, для любой n-арной операции $\omega \in \Omega$ и любых элементов

$$a_1, a_2, \ldots, a_n \in A \quad \text{и} \quad b_1, b_2, \ldots, b_n \in B,$$

в силу (4) из III.2.4, имеем

$$(a_1+b_1)(a_2+b_2)\ldots(a_n+b_n)\omega \in b_1 b_2 \ldots b_n \omega + A,$$

но

$$b_1 b_2 \ldots b_n \omega = b \in B,$$

так как B является Ω-группой, а $b+A = A+b$.

2. Следующая теорема об изоморфизме весьма часто используется.

Если A *и* B *—* Ω*-подгруппы* Ω*-группы* G*, причем* A *является идеалом в* Ω*-подгруппе* $\{A, B\}$*, то пересечение* $A \cap B$ *будет идеалом в* B *и имеет место изоморфизм*

$$\{A, B\}/A \simeq B/(A \cap B). \tag{2}$$

Действительно, равенство (1) показывает, что всякий смежный класс Ω-группы $\{A, B\}$ по идеалу A содержит хотя бы один элемент из B. Таким образом, при естественном гомоморфном отображении $\{A, B\}$ на $\{A, B\}/A$ Ω-подгруппа B будет гомоморфно отображаться на всю эту Ω-фактор-группу.

Ядром указанного гомоморфизма (см. III.2.6) служит, очевидно, пересечение $A \cap B$. Оно будет, следовательно, идеалом в B, а справедливость изоморфизма (2) вытекает из теорем III.1.8 и III.2.5.

3. Сейчас будет доказана лемма Цасенхауза, обобщающая теорему об изоморфизме и существенно используемая ниже в доказательстве теоремы Шрейера.

Если в Ω*-группе* G *даны* Ω*-подгруппы* A, A', B *и* B', *причем* A' *и* B' *являются соответственно идеалами в* A *и в* B, *то* $A'+(A\cap B')$ *и* $B'+(B\cap A')$ *будут соответственно идеалами в* $A'+(A\cap B)$ *и в* $B'+(B\cap A)$ *и имеет место изоморфизм*

$$A'+(A\cap B)/A'+(A\cap B')\simeq B'+(B\cap A)/B'+(B\cap A'). \quad (3)$$

Эта лемма превращается, очевидно, в теорему об изоморфизме при $A\supseteq B$ и $B'=O$.

Для доказательства леммы положим

$$C=A\cap B.$$

Так как B' — идеал в B, а $C\subseteq B$, то, по теореме об изоморфизме,

$$C\cap B'=A\cap B\cap B'=A\cap B'$$

будет идеалом в C. Это же верно и для пересечения $B\cap A'$, а поэтому и для суммы C' этих двух идеалов (см. III.2.4),

$$C'=(A\cap B')+(B\cap A'). \quad (4)$$

Положим

$$D=C/C'.$$

С другой стороны, так как A' является идеалом в A, то, по III.4.1,

$$\{A',\ A\cap B\}=A'+(A\cap B)=A'+C.$$

Произвольный элемент этой суммы имеет вид $a'+c$, где $a'\in A'$, $c\in C$. Поставим ему в соответствие смежный класс (т. е. элемент группы D) $C'+c$. Если элемент $a'+c$ обладает другой записью этого же вида,

$$a'+c=a_1'+c_1,\qquad a_1'\in A',\qquad c_1\in C,$$

то

$$-a_1'+a'=c_1-c\in A'\cap C\subseteq A'\cap B\subseteq C',$$

а поэтому

$$c_1 = (-a_1' + a') + c \in C' + c.$$

Мы получаем однозначное отображение Ω-группы $A' + C$ в Ω-группу D, даже на всю эту Ω-группу, так как всякий элемент $c \in C$, принадлежащий, конечно, к $A' + C$, отображается при этом в свой смежный класс $C' + c$. Это отображение гомоморфно: так как A' — идеал в $A' + C$, то

$$(a_1' + c_1) + (a_2' + c_2) = a_3' + (c_1 + c_2), \quad a_3' \in A',$$

и, по (4) из III.2.4, для любой n-арной операции $\omega \in \Omega$

$$(a_1' + c_1)(a_2' + c_2) \dots (a_n' + c_n)\,\omega = a_0' + c_1 c_2 \dots c_n \omega,$$

где $a_0' \in A'$, а $c_1 c_2 \dots c_n \omega \in C$, так как C является Ω-группой.

Ядром построенного гомоморфизма служит сумма $A' + (A \cap B')$. Действительно, эта сумма входит в ядро, так как $A \cap B' \subseteq C'$. С другой стороны, если элемент $a' + c \in A' + C$ отображается при рассматриваемом гомоморфизме в C', то $c \in C'$, и поэтому, по (4), можно записать:

$$c = u + v, \text{ где } u \in B \cap A', \ v \in A \cap B'$$

— ясно, что при записи суммы двух идеалов слагаемые можно писать в любом порядке. Таким образом,

$$a' + c = (a' + u) + v \in A' + (A \cap B').$$

Отсюда следует, что $A' + (A \cap B')$ будет идеалом в $A' + C = A' + (A \cap B)$ и, кроме того, имеет место изоморфизм

$$A' + (A \cap B)/A' + (A \cap B') \simeq D.$$

По соображениям симметрии можно утверждать, что $B' + (B \cap A')$ будет идеалом в $B' + (B \cap A)$ и

$$B' + (B \cap A)/B' + (B \cap A') \simeq D.$$

Изоморфизм (3) этим доказан.

4. Конечная система вложенных друг в друга Ω-подгрупп Ω-группы G,

$$G = A_0 \supset A_1 \supset A_2 \supset \dots \supset A_k = O, \tag{5}$$

начинающаяся с самой G и оканчивающаяся нулем, называется *нормальным рядом* этой Ω-группы, если всякая Ω-подгруппа A_i, $i = 1, 2, \dots, k$, является истинным идеалом в A_{i-1}

(хотя и не обязательно в A_j при $j<i-1$). Число k называется *длиною* нормального ряда (5), а Ω-фактор-группы

$$G/A_1,\ A_1/A_2,\ldots,\ A_{k-1}/A_k=A_{k-1}$$

— *факторами* этого ряда.

Всякая Ω-группа G обладает нормальными рядами — таков ряд $G\supset O$, а также, если в G имеется нетривиальный идеал A, ряд $G\supset A\supset O$.

Нормальный ряд

$$G=B_0\supset B_1\supset B_2\supset\ldots\supset B_l=O$$

называется *уплотнением* ряда (5), если всякая Ω-подгруппа A_i, $i=1,\ 2,\ldots,\ k-1$, совпадает с одной из Ω-подгрупп B_j; ясно, что $l\geqslant k$.

Наконец, два нормальных ряда Ω-группы G называются *изоморфными*, если их длины равны, а между факторами можно установить такое взаимно однозначное соответствие, что соответствующие факторы будут изоморфными Ω-группами. При этом не предполагается, что указанное соответствие сохраняет взаимное расположение факторов, т. е. i-й фактор первого ряда не обязан быть изоморфным i-му же фактору второго ряда.

5. Теорема Шрейера. *Всякие два нормальных ряда произвольной Ω-группы G обладают изоморфными уплотнениями.*

В самом деле, пусть в G даны нормальные ряды

$$G=A_0\supset A_1\supset A_2\supset\ldots\supset A_k=O, \tag{6}$$

$$G=B_0\supset B_1\supset B_2\supset\ldots\supset B_l=O. \tag{7}$$

Положим

$$A_{ij}=A_i+(A_{i-1}\cap B_j),\qquad i=1,\ 2,\ldots,\ k,\qquad j=0,\ 1,\ldots,\ l;$$

$$B_{ji}=B_j+(B_{j-1}\cap A_i),\qquad j=1,\ 2,\ldots,\ l,\qquad i=0,\ 1,\ldots,\ k.$$

Эти записи имеют смысл в силу III.4.1, так как, например, A_i является идеалом, а $A_{i-1}\cap B_j$ — Ω-подгруппой в A_{i-1}. Отметим, что для $i=1,\ 2,\ldots,\ k$ и $j=1,\ 2,\ldots,\ l$ имеют место включения

$$A_{i-1}=A_{i0}\supseteq A_{i,\,j-1}\supseteq A_{ij}\supseteq A_{il}=A_i,$$

$$B_{j-1}=B_{j0}\supseteq B_{j,\,i-1}\supseteq B_{ji}\supseteq B_{jk}=B_j.$$

Ввиду леммы Цасенхауза (см. III.4.3) A_{ij} и B_{ji} будут соответственно идеалами в $A_{i,\,j-1}$ и $B_{j,\,i-1}$, а соответствующие

Ω-фактор-группы изоморфны:

$$A_{i,j-1}/A_{ij} \simeq B_{j,i-1}/B_{ji}. \tag{8}$$

Если мы вставим в ряд (6) между A_{i-1} и A_i, $l=1, 2, \ldots, \ldots, k$, все A_{ij}, $j=1, 2, \ldots, l-1$, то получим, вообще говоря, для ряда (6) *уплотнение с повторениями*, так как равенство $A_{i,j-1}=A_{ij}$ случайно может иметь место. Аналогично получается уплотнение с повторениями и для ряда (7). Эти уплотнения, ввиду (8), изоморфны.

Для окончания доказательства остается перейти к уплотнениям без повторений. Если $A_{i,j-1}=A_{ij}$, т. е.

$$A_{i,j-1}/A_{ij}=O,$$

то, по (8), и $B_{j,i-1}=B_{ji}$. Отсюда следует, что, не нарушая изоморфизма рассматриваемых уплотнений, можно одновременно исключить из них все повторения. Теорема доказана.

* *Возрастающим нормальным рядом* Ω-группы G называется система ее Ω-подгрупп A_α, удовлетворяющая следующим условиям:

1. Индексы α составляют вполне упорядоченное множество (см. I.5.4) с первым элементом 0 и последним элементом μ.

2. $A_0=O$, $A_\mu=G$.

3. Если $\alpha<\beta$, то $A_\alpha \subset A_\beta$.

4. Если индекс, непосредственно следующий за α, обозначим через $\alpha+1$, то для всех α A_α является идеалом в $A_{\alpha+1}$.

5. Если индекс α предельный, то A_α является теоретико-множественным объединением всех A_β, $\beta<\alpha$.

Любые два возрастающих нормальных ряда произвольной Ω-группы G обладают изоморфными уплотнениями, также являющимися возрастающими нормальными рядами [*А. Г. Курош*, Мат. сб. **16** (1945), 59—72]. Пример бесконечной циклической группы показывает, что для бесконечных у б ы в а ю щ и х нормальных рядов аналогичная теорема не имеет места. *

6. Нормальный ряд Ω-группы, не имеющий уплотнений, отличных от него самого, называется *композиционным рядом* этой Ω-группы. Ввиду III.2.13 *нормальный ряд Ω-группы тогда и только тогда будет композиционным, если все его факторы являются простыми Ω-группами* (см. III.2.4).

Из теоремы Шрейера вытекают следующие две теоремы:

Теоремы Жордана — Гельдера. *Если Ω-группа G обладает композиционными рядами, то всякие два ее композиционных ряда изоморфны.*

Если Ω-группа G обладает композиционными рядами, то всякий ее нормальный ряд может быть уплотнен до композиционного ряда и поэтому имеет длину, не превосходящую длины композиционных рядов этой Ω-группы.

Для доказательства этой второй теоремы достаточно применить теорему Шрейера к данному нормальному ряду и к одному из композиционных рядов рассматриваемой группы.

Применяя введенные понятия к случаю групп без мультиоператоров, заметим, что композиционными рядами обладают как все конечные, так и некоторые бесконечные группы. Однако ни бесконечная циклическая группа, ни группа типа p^∞ (см. III.3.10) композиционных рядов не имеют.

7. *Инвариантным рядом* Ω-группы G называется упорядоченная по включению конечная система идеалов самой Ω-группы G, начинающаяся с G и оканчивающаяся нулем. Это понятие является частным случаем понятия нормального ряда, а поэтому для него имеют смысл понятия изоморфизма рядов и уплотнения ряда, введенные в III.4.4. Инвариантный ряд, не имеющий уплотнений, отличных от него самого и также являющихся инвариантными рядами, называется *главным рядом*. Имеют место теоремы:

Всякие два инвариантных ряда произвольной Ω-группы могут быть уплотнены до изоморфных инвариантных рядов.

Если Ω-группа обладает главными рядами, то всякие два ее главных ряда изоморфны, а любой инвариантный ряд может быть уплотнен до главного ряда.

Легко проверяется, что эти теоремы могут быть доказаны теми же методами, как и соответствующие теоремы для нормальных рядов. Они, впрочем, немедленно вытекают из теорем, доказанных выше, если воспользоваться следующей конструкцией. Пусть дана Ω-группа G. Расширим систему мультиоператоров Ω до системы Ω′, добавляя к Ω некоторую, в общем случае бесконечную, систему унарных операций. Именно, к Ω добавляются все внутренние автоморфизмы аддитивной группы G, а также все отображения G в себя, определяемые следующим образом: для любой n-арной

операции $\omega \in \Omega$, любых элементов $x_1, x_2, \ldots, x_n \in G$ и любого числа i, $1 \leqslant i \leqslant n$, берется отображение, переводящее всякий элемент $a \in G$ в элемент

$$-x_1x_2\ldots x_n\omega + x_1\ldots x_{i-1}(a + x_i)x_{i+1}\ldots x_n\omega.$$

Все добавленные унарные операции переводят нуль в нуль, т. е. удовлетворяют условию (1) из III.2.1, а поэтому G является Ω'-группой. В силу определения идеала (см. III.2.4) *Ω'-подгруппами в G будут идеалы Ω-группы G и только они*, а поэтому нормальные (композиционные) ряды Ω'-группы G совпадают с инвариантными (главными) рядами Ω-группы G.

§ 5. Абелевы, нильпотентные и разрешимые Ω-группы

1. Пусть в Ω-группе G взяты Ω-подгруппы A и B. *Взаимным коммутантом* $[A, B]$ этих Ω-подгрупп называется идеал Ω-подгруппы $\{A, B\}$, порожденный в ней множеством всех элементов следующих двух видов:

$$[a, b] = -a - b + a + b, \qquad a \in A,\ b \in B, \tag{1}$$

— этот элемент называется *коммутатором* элементов a и b, — и

$$[a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n; \omega] = -a_1a_2\ldots a_n\omega - b_1b_2\ldots b_n\omega + (a_1 + b_1)(a_2 + b_2)\ldots(a_n + b_n)\omega, \tag{2}$$

где ω — n-арная операция из Ω, $a_1, a_2, \ldots, a_n \in A$, $b_1, b_2, \ldots, b_n \in B$.

Таким образом, в случае группы G без мультиоператоров взаимный коммутант $[A, B]$ двух подгрупп A, $B \subseteq G$ является нормальным делителем, порожденным в подгруппе $\{A, B\}$ всевозможными коммутаторами $[a, b]$, где $a \in A$, $b \in B$. Если же рассматривается кольцо R, то $[a, b]$ всегда равно нулю, а элементы (2) принимают вид

$$[a_1, a_2; b_1, b_2] = -a_1a_2 - b_1b_2 + (a_1 + b_1)(a_2 + b_2) = a_1b_2 + b_1a_2 = [a_1, 0; 0, b_2] + [0, a_2; b_1, 0].$$

В этом случае, следовательно, взаимный коммутант $[A, B]$ двух подколец A, $B \subseteq R$ является идеалом, порожденным в подкольце $\{A, B\}$ всевозможными произведениями ab и ba, где $a \in A$, $b \in B$.

Из определения идеала немедленно следует, что если в Ω-группе G взята Ω-подгруппа A, а в ней некоторое подмножество M, то идеал, порожденный множеством M в A, содержится в идеале, порожденном M в G. Отсюда вытекает, что *если в Ω-группе G даны Ω-подгруппы A', B', A, B, причем $A' \subseteq A$, $B' \subseteq B$, то*

$$[A', B'] \subseteq [A, B].$$

* В группе без мультиоператоров взаимный коммутант $[A, B]$ совпадает с подгруппой, порожденной всеми коммутаторами $[a, b]$, $a \in A$, $b \in B$. *

2. *Для любых Ω-подгрупп A и B Ω-группы G имеет место равенство*

$$[A, B] = [B, A]. \tag{3}$$

Действительно, для любых $b \in B$, $a \in A$

$$[b, a] = -a + [-a, b] + a \in [A, B], \tag{4}$$

так как $[A, B]$ по сложению является нормальным делителем в $\{A, B\}$. С другой стороны, для любой n-арной операции $\omega \in \Omega$ и любых $b_1, b_2, \ldots, b_n \in B$, $a_1, a_2, \ldots, a_n \in A$

$$b_1 b_2 \ldots b_n \omega \in B, \qquad a_1 a_2 \ldots a_n \omega \in A$$

и поэтому, ввиду (4),

$$[b_1 b_2 \ldots b_n \omega,\ a_1 a_2 \ldots a_n \omega] \in [A, B].$$

Далее

$$b_i + a_i = [-b_i, -a_i] + a_i + b_i, \qquad i = 1, 2, \ldots, n,$$

а так как, по (4),

$$[-b_i, -a_i] \in [A, B], \qquad i = 1, 2, \ldots, n,$$

и $[A, B]$ является идеалом в $\{A, B\}$, то, в силу (4) из III.2.4,

$$(b_1 + a_1)(b_2 + a_2) \ldots (b_n + a_n)\,\omega = \\ = (a_1 + b_1)(a_2 + b_2) \ldots (a_n + b_n)\,\omega + d,$$

где $d \in [A, B]$. Мы получаем, что

$$[b_1, b_2, \ldots, b_n; a_1, a_2, \ldots, a_n; \omega] = [b_1 b_2 \ldots b_n \omega,\ a_1 a_2 \ldots a_n \omega] + \\ + [a_1, a_2, \ldots, a_n; b_1, b_2, \ldots, b_n; \omega] + d \in [A, B]. \tag{5}$$

Из (4) и (5) вытекает включение

$$[B,\ A] \subseteq [A,\ B],$$

из которого по соображениям симметрии следует равенство (3).

3. Как показывает определение, взаимный коммутант $[A, G]$ любой Ω-подгруппы A с самой Ω-группой G является идеалом в G. Это справедливо, в частности, для

$$G' = [G,\ G].$$

Этот идеал называется *коммутантом* Ω-группы G.

Для группы G без мультиоператоров коммутант G' будет, следовательно, нормальным делителем, порожденным всеми коммутаторами $[a, b]$, $a, b \in G$. Для кольца R коммутант является идеалом, порожденным всеми произведениями ab, $a, b \in R$; в теории колец этот идеал называется обычно *квадратом* кольца R.

Ω-подгруппа A Ω-группы G тогда и только тогда является идеалом в G, если

$$[A,\ G] \subseteq A. \tag{6}$$

Действительно, если A — идеал в G, то для всех $a \in A$, $x \in G$ в A содержится элемент $-x+a+x$, а поэтому и элемент $[a, x]$. С другой стороны, ввиду (4) из III.2.4, для всякой n-арной операции $\omega \in \Omega$ и всех $a_1, a_2, \ldots, a_n \in A$, $x_1, x_2, \ldots, x_n \in G$ в A содержится элемент

$$-x_1x_2\ldots x_n\omega + (a_1+x_1)(a_2+x_2)\ldots(a_n+x_n)\,\omega,$$

а поэтому и элемент

$$[a_1,\ a_2, \ldots,\ a_n;\ x_1,\ x_2, \ldots,\ x_n;\ \omega].$$

Идеал A содержит, следовательно, и идеал, порожденный всеми указанными элементами, т. е. идеал $[A, G]$.

Обратно, если выполняется (6), то A содержит, в частности, все коммутаторы $[a, x]$, $a \in A$, $x \in G$, откуда $-x+a+x \in A$, т. е. условие 1) из III.2.4 выполняется. Выполняется и условие 2); действительно, (2) из III.2.4 следует из

$$[0, \ldots,\ 0,\ a,\ 0, \ldots,\ 0;\ x_1,\ x_2, \ldots,\ x_n;\ \omega] \in A,$$

так как $0\ldots0a0\ldots0\omega \in A$.

Из этой теоремы вытекает, ввиду включения

$$[A,\ G] \subseteq [G,\ G] = G',$$

что *всякая Ω-подгруппа A Ω-группы G, содержащая коммутант G', будет в G идеалом.*

4. Ω-группа G называется *абелевой*, если ее коммутант равен нулю,

$$[G,\ G]=O.$$

Это означает, в частности, что для всех $a,\ b\in G$

$$[a,\ b]=0,$$

откуда следует

$$a+b=b+a, \tag{7}$$

т. е. *абелева Ω-группа имеет абелеву аддитивную группу.* С другой стороны, для всякой n-арной операции $\omega\in\Omega$ и любых $a_1,\ a_2,\ldots,\ a_n,\ b_1,\ b_2,\ldots,\ b_n\in G$ будет

$$[a_1,\ a_2,\ldots,\ a_n;\ b_1,\ b_2,\ldots,\ b_n;\ \omega]=0,$$

т. е., ввиду (7),

$$(a_1+b_1)(a_2+b_2)\ldots(a_n+b_n)\,\omega=a_1a_2\ldots a_n\omega+b_1b_2\ldots b_n\omega. \tag{8}$$

Для групп без мультиоператоров это понятие превращается в понятие обычной абелевой группы, а для колец — в понятие кольца с нулевым умножением, так как условие (8) равносильно для колец условию $ab=0$ для всех a и b.

Всякая Ω-подгруппа A абелевой Ω-группы G является в G идеалом, так как $A\supseteq G'=O$.

Всякая Ω-подгруппа A и всякая Ω-фактор-группа G/A абелевой Ω-группы G сами абелевы, так как из справедливости в G условий (7) и (8) вытекает их справедливость и в A, и в G/A.

5. *Ω-фактор-группа G/A Ω-группы G тогда и только тогда абелева, если идеал A содержит коммутант G' Ω-группы G,*

$$A\supseteq G'. \tag{9}$$

Действительно, абелевость Ω-фактор-группы G/A означает, что для всех $x,\ y\in G$

$$[x+A,\ y+A]=A$$

и для всякой n-арной операции $\omega\in\Omega$ и любых $x_1,\ x_2,\ldots,\ x_n,\ y_1,\ y_2,\ldots,\ y_n\in G$

$$[x_1+A,\ x_2+A,\ldots,\ x_n+A;\ y_1+A,\ y_2+A,\ldots,\ y_n+A;\ \omega]=A.$$

Это равносильно, однако, включениям

$$[x, y] \in A,$$

$$[x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n; \omega] \in A,$$

т. е. равносильно включению (9).

В частности, *абелевой будет Ω-фактор-группа G/G' Ω-группы G по ее коммутанту.*

6. Нормальный ряд

$$G = A_0 \supset A_1 \supset A_2 \supset \ldots \supset A_k = O \tag{10}$$

Ω-группы G (см. III.4.4) называется *центральным рядом,* если

$$[A_i, G] \subseteq A_{i+1}, \quad i = 0, 1, \ldots, k-1. \tag{11}$$

Заметим, что из (11) вытекает для всех i включение

$$[A_i, G] \subseteq A_i,$$

а поэтому, по III.5.3, все A_i будут идеалами в G, т. е. всякий центральный ряд является инвариантным рядом (см. III.4.7).

Ω-группа G называется *нильпотентной,* если она обладает хотя бы одним центральным рядом. К числу нильпотентных Ω-групп принадлежит, в частности, всякая абелева Ω-группа G, так как для нее ряд $G \supset O$ служит центральным рядом.

Нижней центральной цепью произвольной Ω-группы G называется убывающая цепь идеалов

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_i \supseteq \ldots, \tag{12}$$

где

$$G_{i+1} = [G_i, G], \quad i = 0, 1, 2, \ldots \tag{13}$$

Заметим, что если уже доказано, что G_i является идеалом, то идеал G_{i+1} будет содержаться в G_i.

Ω-группа G тогда и только тогда нильпотентна, если ее нижняя центральная цепь (12) *после конечного числа шагов достигает нулевой подгруппы, т. е. $G_k = O$ при некотором k.*

В самом деле, если $G_k = O$, то цепь (12) превращается, ввиду (13), в конечный центральный ряд. Обратно, пусть Ω-группа G обладает центральным рядом (10). Тогда $G_0 =$

$= G = A_0$. Если уже доказано, что $G_i \subseteq A_i$, то, по (13) и (11),

$$G_{i+1} = [G_i,\ G] \subseteq [A_i,\ G] \subseteq A_{i+1}.$$

Отсюда следует, что

$$G_k \subseteq A_k = O,$$

т. е. $G_k = O$.

Всякая Ω-подгруппа A нильпотентной Ω-группы G сама нильпотентна.

Действительно, пусть

$$A = A_0 \supseteq A_1 \supseteq A_2 \supseteq \ldots \supseteq A_i \supseteq \ldots$$

будет нижняя центральная цепь Ω-группы A. Тогда

$$A_0 = A \subseteq G = G_0.$$

Пусть уже доказано, что $A_i \subseteq G_i$. Тогда

$$A_{i+1} = [A_i,\ A] \subseteq [G_i,\ G] = G_{i+1}.$$

Из $G_k = O$ следует теперь $A_k = O$.

Всякий гомоморфный образ $H = G\varphi$ нильпотентной Ω-группы G сам нильпотентен.

Действительно, пусть (12) и

$$H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_i \supseteq \ldots$$

будут соответственно нижними центральными цепями Ω-групп G и H. Тогда

$$H_0 = H = G\varphi = G_0\varphi.$$

Пусть уже доказано, что

$$H_i \subseteq G_i\varphi. \tag{14}$$

Если $a' \in H_i$, $b' \in H$, то существуют, ввиду (14), такие $a \in G_i$ и $b \in G$, что $a\varphi = a'$, $b\varphi = b'$, а поэтому, в силу определения гомоморфизма,

$$[a,\ b]\varphi = [a',\ b']. \tag{15}$$

Аналогично для любой n-арной операции $\omega \in \Omega$ и любых $a'_1, a'_2, \ldots, a'_n \in H_i$, $b'_1, b'_2, \ldots, b'_n \in H$ существуют такие $a_1, a_2, \ldots, a_n \in G_i$ и $b_1, b_2, \ldots, b_n \in G$, что $a_i\varphi = a'_i$, $b_i\varphi = b'_i$, $i = 1, 2, \ldots, n$, а поэтому

$$[a_1, a_2, \ldots, a_n;\ b_1, b_2, \ldots, b_n;\ \omega]\varphi = \\ = [a'_1, a'_2, \ldots, a'_n;\ b'_1, b'_2, \ldots, b'_n;\ \omega]. \tag{16}$$

Так как, в силу замечания, сделанного в конце III.2.13, образ $G_{i+1}\varphi$ идеала G_{i+1} является идеалом в H, то, ввиду (15) и (16),

$$H_{i+1} = [H_i, H] \subseteq G_{i+1}\varphi.$$

Отсюда и из $G_k = O$ следует $H_k = O$.

7. Нормальный ряд

$$G = A_0 \supset A_1 \supset A_2 \supset \ldots \supset A_k = O \tag{17}$$

Ω-группы G называется *разрешимым рядом,* если все факторы

$$A_i/A_{i+1}, \qquad i = 0, 1, \ldots, k-1,$$

этого ряда являются абелевыми Ω-группами, т. е., ввиду III.5.5, если

$$[A_i, A_i] \subseteq A_{i+1}, \qquad i = 0, 1, \ldots, k-1. \tag{18}$$

Ω-группа G называется *разрешимой,* если она обладает хотя бы одним разрешимым рядом.

Всякая нильпотентная Ω-группа G разрешима.

Действительно, если в G задан центральный ряд (10), то, ввиду (11),

$$[A_i, A_i] \subseteq [A_i, G] \subseteq A_{i+1}, \qquad i = 0, 1, \ldots, k-1,$$

что и требовалось доказать.

Цепью коммутантов Ω-группы G называется убывающая цепь Ω-подгрупп

$$G = G^{(0)} \supseteq G' \supseteq G'' \supseteq \ldots \supseteq G^{(i)} \supseteq \ldots, \tag{19}$$

где

$$G^{(i+1)} = [G^{(i)}, G^{(i)}], \qquad i = 0, 1, 2, \ldots \tag{20}$$

Ω-группа G тогда и только тогда разрешима, если ее цепь коммутантов (19) *после конечного числа шагов достигает нуля, т. е. $G^{(k)} = O$ при некотором k.*

В самом деле, если $G^{(k)} = O$, то цепь (19) превращается, ввиду (20), в конечный разрешимый ряд. Обратно, пусть Ω-группа G обладает разрешимым рядом (17). Тогда $G^{(0)} = G = A_0$. Если уже доказано, что $G^{(i)} \subseteq A_i$, то, по (20) и (18),

$$G^{(i+1)} = [G^{(i)}, G^{(i)}] \subseteq [A_i, A_i] \subseteq A_{i+1}.$$

Отсюда следует, что

$$G^{(k)} \subseteq A_k = O,$$

т. е. $G^{(k)} = O$.

Всякая Ω-подгруппа A разрешимой Ω-группы G сама разрешима.

В самом деле, пусть

$$A = A^{(0)} \supseteq A' \supseteq A'' \supseteq \ldots \supseteq A^{(i)} \supseteq \ldots$$

будет цепь коммутантов Ω-группы A. Тогда

$$A^{(0)} = A \subseteq G = G^{(0)}.$$

Если уже доказано, что $A^{(i)} \subseteq G^{(i)}$, то

$$A^{(i+1)} = [A^{(i)}, A^{(i)}] \subseteq [G^{(i)}, G^{(i)}] = G^{(i+1)}.$$

Из $G^{(k)} = O$ следует теперь $A^{(k)} = O$.

Всякий гомоморфный образ разрешимой Ω-группы G сам разрешим.

Достаточно доказать это утверждение для Ω-факторгруппы G/A. Так как всякое уплотнение разрешимого ряда само разрешимо, то, по теореме Шрейера III.4.5, для нормального ряда $G \supset A \supset O$ существует в нашем случае разрешимое уплотнение, которое, по III.2.12 и III.2.13, определяет разрешимый ряд в G/A.

8. И в случае групп, и в случае неассоциативных, в частности лиевых, колец разрешимость оказывается существенно шире нильпотентности. Иное положение в случае ассоциативных колец:

Всякое разрешимое ассоциативное кольцо нильпотентно.

Заметим сперва, что *если даны ассоциативное кольцо R и натуральное число n, то идеал, порожденный в R множеством всевозможных произведений по n элементов из R, совпадает с подгруппой, порожденной этим множеством в аддитивной группе кольца R.* В самом деле, указанная подгруппа состоит из нуля и всевозможных сумм конечного числа произведений по n элементов. Умножая такую сумму слева или справа на любой элемент из R, мы получим сумму нескольких произведений по $n+1$ элементу каждое. Заменяя, однако, в каждом из членов этой суммы одну пару соседних сомножителей их произведением, мы снова придем к сумме произведений по n элементов.

Отсюда легко выводятся следующие два утверждения.

В ассоциативном кольце R i-й член цепи коммутантов $R^{(i)}$ совпадает с идеалом, порожденным в R множеством всевозможных произведений по 2^i элементов из R.

Для $i=1$ это известно нам из III.5.3. Пусть утверждение уже доказано для i, т. е. $R^{(i)}$ состоит из сумм произведений по 2^i элементов. Тогда $R^{(i+1)}$ является, ввиду (20), подгруппой аддитивной группы кольца R, порожденной всевозможными произведениями пар элементов из $R^{(i)}$, т. е., ввиду законов дистрибутивности, порожденной всевозможными произведениями по 2^{i+1} элементов.

В ассоциативном кольце R i-й член нижней центральной цепи R_i совпадает с идеалом, порожденным в R множеством всевозможных произведений по $i+1$ элементу из R.

Для $i=1$ это верно. Пусть наше утверждение уже доказано для i, т. е. R_i состоит из сумм произведений по $i+1$ элементу. Тогда R_{i+1} является, ввиду (13) и III.5.1, идеалом, порожденным в R произведениями элементов из R_i на любые элементы из R, слева или справа, т. е., ввиду законов дистрибутивности, порожденным всевозможными произведениями по $i+2$ элемента.

Таким образом, для ассоциативного кольца R

$$R^{(i)}=R_{2^i-1} \quad i=0,\ 1,\ 2,\ldots,$$

а поэтому из $R^{(k)}=O$ следует $R_{2^k-1}=O$, что и требовалось доказать.

§ 6. Примитивные классы универсальных алгебр

1. Вернемся к изучению произвольных универсальных алгебр. Понятие однотипности алгебр (см. III.1.5) является слишком общим для того, чтобы выделять разумные классы алгебраических образований. Так, далеко не всякая универсальная алгебра с одной бинарной операцией (умножение), одной унарной операцией (взятие обратного элемента) и одной нульарной операцией (взятие единицы) будет группой, хотя она и однотипна с группами. Группы выделяются среди всех этих алгебр тем, что в них, как мы хорошо знаем, имеют место следующие тождественные соотношения: для любых x, y, z

$$(xy)z=x(yz), \qquad x\cdot 1=x, \qquad xx^{-1}=1.$$

Мы хотим определить понятие тождественного соотношения для случая универсальных алгебр с любой фиксированной системой операций Ω.

2. Пусть дано некоторое непустое вспомогательное множество X, элементы которого будут называться *свободными элементами* и обозначаться через x с индексами, а также через y, z и т. д. С другой стороны, всем нульарным операциям из Ω, если такие существуют, сопоставим некоторые символы, которые будут называться *символами нульарных операций*.

Определим понятие *слова*. Прежде всего, словами будут считаться все свободные элементы и все символы нульарных операций. Если же мы уже знаем, что выражения $w_1, w_2, \ldots, w_n$ являются словами, то для любой n-арной операции $\omega \in \Omega$, где $n \geqslant 1$, формальное выражение

$$w_1 w_2 \ldots w_n \omega \tag{1}$$

также будет считаться словом.

Таким образом, всякое слово будет конечным выражением, в котором участвуют свободные элементы, символы нульарных операций и символы ω для n-арных операций из Ω, $n \geqslant 1$, причем с любым числом повторений; при этом символ n-арной операции ω всегда «действует» на n предшествующих ему слов.

Так, пусть в Ω входят тернарная операция ω, унарные операции ω' и ω'' и нульарная операция с символом 0. Тогда словами будут, например, выражения

$$[(x\omega')\,0\,y\omega]\,x\,(y\omega'')\,\omega \text{ или } (xyz\omega)(x\omega')(y\omega')\,\omega.$$

Понятно, что эти слова можно было бы записать без всяких скобок:

$$x\omega' 0 y\omega x y\omega'' \omega, \quad xyz\omega x\omega' y\omega' \omega.$$

Будем называть слова $w_1, w_2, \ldots, w_n$ *подсловами* слова (1). Будем считать, далее, что свойство быть подсловом транзитивно, и поэтому подслова слов $w_1, w_2, \ldots, w_n$ будут подсловами и для слова (1), и т. д. В частности, подсловами слова (1) будут все входящие в его запись свободные элементы и символы нульарных операций. Условимся считать также, что всякое слово является своим собственным подсловом.

Ясно, что понятие слова по существу зависит от системы операций Ω. Рассматривая универсальные алгебры с системой операций Ω, мы будем, разумеется, использовать лишь слова, имеющие смысл в Ω.

3. Пусть даны слова w_1 и w_2, относящиеся к системе операций Ω. Обозначим через $x_1, x_2, \ldots, x_k$ все различные свободные элементы, встречающиеся хотя бы в одном из этих слов, а через $0_1, 0_2, \ldots, 0_l$ — все встречающиеся хотя бы в одном из этих слов символы нульарных операций. Будем говорить, что в универсальной алгебре G с системой операций Ω выполняется *тождественное соотношение*

$$w_1 = w_2, \tag{2}$$

если равенство (2) имеет место в G при замене свободных элементов x_i, $i = 1, 2, \ldots, k$, произвольными элементами $a_i \in G$, не обязательно различными. При этом символы 0_j, $j = 1, 2, \ldots, l$, заменяются, понятно, теми элементами из G, взятие которых означает в G соответствующую нульарную операцию, и, вообще, операции из Ω выполняются по правилам оперирования в алгебре G.

Если дано множество тождественных соотношений Λ, то все универсальные алгебры с системой операций Ω, в которых выполняются все тождественные соотношения из Λ, составляют *примитивный класс* алгебр. Условимся обозначать этот примитивный класс той же буквой Λ, что и определяющее его множество тождественных соотношений.

Так, примитивный класс составляют группы, рассматриваемые как алгебры с одной бинарной, одной унарной и одной нульарной операциями. Абелевы группы составляют более узкий примитивный класс — здесь накладывается дополнительное тождественное соотношение $xy = yx$. Еще более узкий примитивный класс мы получим, налагая тождественное соотношение $x^2 = 1$.

Кольца, ассоциативные кольца, ассоциативно-коммутативные кольца, лиевы кольца, йордановы кольца также будут примитивными классами универсальных алгебр.

Весь класс однотипных между собою универсальных алгебр с системой операций Ω также можно считать примитивным классом, а именно для пустого множества тождественных соотношений. Примитивным классом будет и класс Ω-групп с данной системой операций Ω — он определяется тождественными соотношениями, входящими в определение группы, и соотношениями (1) из III. 2.1. С другой стороны, множество тождественных соотношений Λ может оказаться таким, что из него следует тождественное соотношение $x = y$, т. е. соот-

ветствующий примитивный класс состоит из одной-единственной алгебры, содержащей лишь один элемент.

4. *Всякий примитивный класс универсальных алгебр вместе со всякой своей алгеброй содержит все ее подалгебры и все ее гомоморфные образы.*

Ясно, что если в алгебре G выполняется тождественное соотношение (2), то оно выполняется, в частности, и для элементов из любой подалгебры. С другой стороны, пусть в G выполняется тождественное соотношение (2) и пусть задан гомоморфизм φ алгебры G на одноипную алгебру H. Обозначим через w_1'', w_2'' те элементы из H, которые получаются после подстановки в слова w_1 и w_2 вместо свободных элементов x_i, $i = 1, 2, \ldots, k$, некоторых элементов $b_i \in H$, $i = 1, 2, \ldots, k$. Выберем в алгебре G такие элементы a_i, $i = 1, 2, \ldots, k$, что $a_i\varphi = b_i$ для всех i, и обозначим через w_1', w_2' те элементы из G, которые получаются после подстановки a_i вместо x_i, $i = 1, 2, \ldots, k$, в слова w_1 и w_2. Из определения гомоморфизма следует, что

$$w_j'\varphi = w_j'', \qquad j = 1, 2,$$

а так как $w_1' = w_2'$, то и $w_1'' = w_2''$ что и требовалось доказать.

5. Понятие слова может быть использовано и для других целей. Рассмотрим универсальную алгебру G с системой операций Ω и возьмем произвольное слово

$$w = w(x_1, x_2, \ldots, x_n)$$

в этих операциях относительно свободных элементов x_1, $x_2, \ldots, x_n$, $n \geqslant 1$. Заменим k из этих элементов, $0 \leqslant k \leqslant n$, например элементы x_{n-k+1}, x_{n-k+2}, $\ldots$, x_n, некоторыми фиксированными элементами $b_1, b_2, \ldots, b_k \in G$. Выражение

$$w(x_1, x_2, \ldots, x_{n-k}, b_1, b_2, \ldots, b_k), \tag{3}$$

которое будет при этом получено, следующим образом определяет в множестве G $(n-k)$-арную операцию: системе элементов $a_1, a_2, \ldots, a_{n-k} \in G$ эта операция сопоставляет однозначно определенный элемент

$$w(a_1, a_2, \ldots, a_{n-k}, b_1, b_2, \ldots, b_k).$$

Все операции, которые этим путем могут быть в G получены, называются *производными операциями* алгебры G.

Понятно, что различные выражения вида (3) могут случайно определять в G одну и ту же производную операцию. Производная операция будет называться *главной*, если $k = 0$, т. е. если в слове w не производится никакой предварительной замены части свободных элементов элементами из G. К числу главных производных операций алгебры Ω принадлежат, в частности, операции из самой системы Ω.

6. Пусть на множестве G заданы две универсальные алгебры, соответственно с системами операций Ω и Ω'. Будем говорить, что эти две алгебры определяют на G одну и ту же *алгебраическую систему*, если в G всякая операция из Ω' является производной от операций системы Ω и обратно; сами такие системы операций Ω и Ω' назовем *эквивалентными* в G.

Если алгебры G и H однотипны относительно системы операций Ω и если в G мы перейдем к эквивалентной системе операций Ω', то в H такой переход в общем случае не имеет смысла — если производная операция была получена в G заменой в некотором слове части свободных элементов фиксированными элементами из G, то в H эта операция не может быть однозначно определена. Отсюда следует, что понятие гомоморфизма относится лишь к данной системе операций Ω и может потерять смысл при переходе к эквивалентной системе операций Ω'. Это же имеет место и для понятия подалгебры — достаточно учесть, что те элементы b_1, b_2, ..., b_k, которые участвуют в выражении (3), не обязаны принадлежать к рассматриваемой подалгебре (относительно операций из Ω).

Читатель без труда проверит, что положение будет иным, если всякая операция любой из систем Ω, Ω' является главной производной операцией от другой системы. Отсюда следует, что те два способа рассмотрения группы как универсальной алгебры, которые указаны в III. 1.3, с точки зрения гомоморфизмов и подгрупп действительно равносильны, что, впрочем, мы знали и ранее.

§ 7. Свободные универсальные алгебры

1. Множество всевозможных слов относительно системы операций Ω и множества свободных элементов X можно рассматривать как алгебру с системой операций Ω. Именно, если даны n-арная операция $\omega \in \Omega$, $n \geqslant 1$, и слова w_1,

$w_2, \ldots, w_n$, то слово $w_1 w_2 \ldots w_n \omega$ будет считаться результатом применения операции ω к заданным словам. Применение же любой нульарной операции из Ω будет пониматься как взятие символа этой нульарной операции, принадлежащего, как мы знаем, к множеству слов.

Обозначим эту *алгебру слов* через $S(\Omega, X)$. Понятно, что в ней не выполняется никакое нетривиальное тождественное соотношение, т. е. соотношение вида

$$w_1 = w_2, \tag{1}$$

где w_1 и w_2 — различные слова. Понятно также, что множество X служит для этой алгебры системой образующих (см. III.1.4). Если же дано подмножество $X' \subset X$, то оно порождает в $S(\Omega, X)$ подалгебру, являющуюся алгеброй слов $S(\Omega, X')$.

2. Рассмотрим теперь произвольную систему тождественных соотношений Λ. Слова v' и v'' будут называться *эквивалентными* относительно Λ, если от одного к другому можно перейти конечным числом преобразований следующего вида: пусть в системе Λ содержится соотношение (1); заменим входящие в него свободные элементы x_i, $i = 1, 2, \ldots k$, некоторыми словами, после чего левая и правая части соотношения (1) превращаются в слова $\overline{w}_1$ и $\overline{w}_2$; если $\overline{w}_1$ (или $\overline{w}_2$) служит подсловом слова v', то оно заменяется в слове v' на $\overline{w}_2$ (или соответственно на $\overline{w}_1$).

Это отношение будет, очевидно, рефлексивным, транзитивным и симметричным, т. е. в алгебру $S(\Omega, X)$ введено отношение эквивалентности. *Это будет даже конгруенция* (см. III.1.7), так как если дано слово $w_1 w_2 \ldots w_n \omega$, полученное из слов $w_1, w_2 \ldots, w_n$ применением операции ω, то замена слов w_i, $i = 1, 2, \ldots, n$, словами, им эквивалентными, может быть осуществлена применением к данному слову конечного числа преобразований описанного выше вида.

Фактор-алгебра алгебры $S(\Omega, X)$ по построенной нами конгруенции (см. III.1.7) будет обозначаться символом $S(\Omega, X, \Lambda)$ и называться *свободной алгеброй* примитивного класса Λ, а множество X — ее *системой свободных образующих*. Конечно, на самом деле системой образующих для этой алгебры служит не само множество X, а множество соответствующих классов эквивалентных слов; мы будем

обозначать его, однако, той же буквой X. Всякая алгебра, изоморфная алгебре $S(\Omega, X, \Lambda)$, также будет называться свободной, а множество образов элементов из X при этом изоморфизме — системой свободных образующих.

Из определения свободной алгебры $S(\Omega, X, \Lambda)$ следует, что в ней выполняются все тождественные соотношения из Λ, т. е. *алгебра* $S(\Omega, X, \Lambda)$ *принадлежит к примитивному классу* Λ.

3. *Пусть в универсальной алгебре G примитивного класса Λ выбрана система образующих M. Алгебра G тогда и только тогда будет свободной алгеброй в примитивном классе Λ, а M — ее системой свободных образующих, если выполняется следующее условие: для любой алгебры H класса Λ и любого однозначного отображения φ множества M в алгебру H существует, притом единственное, гомоморфное отображение G в H, совпадающее с φ на множестве M.*

Положим сперва, что $G = S(\Omega, X, \Lambda)$, $M = X$ и уже задано отображение φ множества X в алгебру H. Отображение $\bar{\varphi}$ всей алгебры $S(\Omega, X, \Lambda)$ в алгебру H определим следующим образом: на множестве X оно совпадает с φ; символы нульарных операций $\bar{\varphi}$ отображает в те элементы из H, взятие которых означает в H соответствующую нульарную операцию; наконец, если для слов $w_1, w_2, \ldots, w_n$ образы при $\bar{\varphi}$ уже однозначно определены, а операция $\omega \in \Omega$ n-арна, то полагаем

$$(w_1 w_2 \ldots w_n \omega)\bar{\varphi} = (w_1\bar{\varphi})(w_2\bar{\varphi}) \ldots (w_n\bar{\varphi})\omega; \qquad (2)$$

ясно, что образ слова $w_1 w_2 \ldots w_n \omega$ при отображении $\bar{\varphi}$ может быть определен лишь равенством (2), если мы хотим, чтобы это отображение было гомоморфным.

Заметим, что применение отображения $\bar{\varphi}$ к слову, эквивалентному слову $w_1 w_2 \ldots w_n \omega$ в смысле III. 7.2, дает элемент, равный в алгебре H правой части равенства (2), так как в H выполняются все тождественные соотношения из Λ. Таким образом, отображение $\bar{\varphi}$ определено для элементов алгебры $S(\Omega, X, \Lambda)$; его гомоморфность и однозначная определенность следуют из (2).

Пусть теперь даны алгебра G и ее система образующих M, удовлетворяющие условию нашей теоремы. Возьмем в качестве алгебры H такую свободную алгебру $S(\Omega, X, \Lambda)$, что множества M и X равномощны, т. е. существует взаимно однозначное отображение φ множества M на X. По условию, существует гомоморфизм ψ: $G \to S(\Omega, X, \Lambda)$, совпадающий с φ на M. С другой стороны, из сказанного выше следует, что существует гомоморфизм χ: $S(\Omega, X, \Lambda) \to G$, совпадающий на X с φ^{-1}.

Произведение $\chi\psi$ будет эндоморфизмом алгебры $S(\Omega, X, \Lambda)$, тождественным на системе образующих X, а произведение $\psi\chi$ — эндоморфизмом алгебры G, тождественным на системе образующих M. Из условия единственности, предположенного для алгебры G и уже доказанного для $S(\Omega, X, \Lambda)$, следует, что эти эндоморфизмы будут тождественными автоморфизмами указанных алгебр. Отсюда вытекает, что каждый из гомоморфизмов ψ, χ будет в действительности изоморфизмом между алгебрами G и $S(\Omega, X, \Lambda)$, что и требовалось доказать.

4. Из доказанной теоремы вытекает следующий результат, выясняющий истинное значение понятия свободной алгебры:

Всякая алгебра G примитивного класса Λ является гомоморфным образом некоторой свободной алгебры этого класса.

В самом деле, возьмем в G любую систему образующих M и рассмотрим такую свободную алгебру $S(\Omega, X, \Lambda)$, что существует отображение φ множества X на множество M, т. е. мощность X больше или равна мощности M. Тогда, по доказанному, отображение φ можно продолжить до гомоморфизма $\bar{\varphi}$: $S(\Omega, X, \Lambda) \to G$, причем это будет гомоморфизм на всю алгебру G, так как образ алгебры $S(\Omega, X, \Lambda)$ при $\bar{\varphi}$ содержит все множество M.

5. Ясно, что если множества X и Y равномощны, то свободные алгебры $S(\Omega, X, \Lambda)$ и $S(\Omega, Y, \Lambda)$ будут изоморфными. На вопрос, следует ли, обратно, из изоморфизма указанных свободных алгебр равномощность множеств свободных образующих X и Y, ответ в общем случае будет отрицательным, как показывает отмеченный в III. 6.3 примитивный класс,

состоящий из одной одноэлементной алгебры; этот класс, в котором выполняются, конечно, любые тождественные соотношения, условимся называть *абсолютно вырожденным*.

Справедливы следующие теоремы Фудзивары [Proc. Japan. Acad. **31** (1955), 135—136]:

Если примитивный класс Λ *не является абсолютно вырожденным и если свободные алгебры* $S(\Omega, X, \Lambda)$ *и* $S(\Omega, Y, \Lambda)$ *изоморфны, причем хотя бы одно из множеств* X, Y *бесконечно, то эти множества равномощны.*

Пусть это не так и пусть, например, мощность множества X больше мощности множества Y [1]). Можно считать, что рассматриваемые алгебры не только изоморфны, но даже совпадают,

$$S(\Omega, X, \Lambda) = S(\Omega, Y, \Lambda) = S. \tag{3}$$

Всякий элемент из Y записывается, следовательно, в виде слова относительно конечного числа свободных образующих из X. Фиксируя для каждого $y \in Y$ одну такую запись и собирая все элементы из X, которые используются в этих записях для всех $y \in Y$, мы получим подмножество $X' \subset X$, имеющее заведомо меньшую мощность, чем X: оно конечно, если конечно множество Y, и имеет мощность, не превосходящую мощности Y, если Y бесконечно. Можно выбрать, следовательно, элемент $x_0 \in X \setminus X'$.

Элемент x_0 записывается в виде слова от конечного числа элементов из Y. Записывая в свою очередь эти элементы через элементы из X', мы получим, что x_0 равно в алгебре S некоторому слову w_0 от элементов из X',

$$x_0 = w_0.$$

Это равенство означает эквивалентность слов x_0 и w_0 в алгебре слов (см. III.7.2), т. е. оно получено применением тождественных соотношений из Λ. Но тогда, учитывая, что в слово w_0 свободный элемент x_0 не входит, мы могли бы при помощи тех же тождественных соотношений получить в алгебре S равенство $a = w_0$, где a — произвольный элемент из S. Таким образом, в S все элементы равны между собой, т. е. из тождественных соотношений Λ вытекает тождественное соотношение $x = y$, а поэтому примитивный класс Λ оказывается абсолютно вырожденным против предположения. Теорема доказана.

[1]) Здесь используется основанное на аксиоме выбора утверждение, что всякие две мощности можно сравнивать по величине.

6. *Пусть систему тождественных соотношений* Λ *можно расширить до такой системы* Λ^*, *что примитивный класс* Λ^* *не является абсолютно вырожденным, но конечные множества свободных образующих порождают в нем конечные свободные алгебры. Тогда в классе* Λ *изоморфные свободные алгебры обладают равномощными системами свободных образующих.*

Пусть, в самом деле, в классе Λ даны изоморфные свободные алгебры с системами свободных образующих X и Y. Как и выше, можно считать, что эти алгебры совпадают, т. е. имеют место равенства (3). Кроме того, в силу предшествующей теоремы оба множества X, Y можно считать конечными.

Предположим, что X содержит больше элементов, чем Y. Наложим на алгебру S тождественные соотношения из системы $\Lambda^* \setminus \Lambda$, т. е. перейдем к фактор-алгебре S^* по соответствующей конгруенции. Это будет, очевидно, свободная алгебра в примитивном классе Λ^*, причем она в силу условий теоремы конечна, так как имеет своими системами свободных образующих конечные множества X и Y.

Пусть подмножество $X' \subset X$ содержит столько же элементов, как и Y. Тогда подалгебра $\{X'\}$ алгебры S^*, являясь свободной алгеброй $S(\Omega, X', \Lambda^*)$, должна в действительности состоять из стольких же элементов, как и S^*, т. е. она совпадает со всей алгеброй S^*. Отсюда следует, что всякий элемент $x_0 \in X \setminus X'$ записывается в виде слова от элементов из X', что, однако, как и в доказательстве предшествующей теоремы, приводит к противоречию.

7. Класс группоидов является примитивным классом относительно одной бинарной операции и пустого множества тождественных соотношений; будем, как обычно, называть эту операцию умножением и записывать в виде *ab*. *Свободный группоид* с множеством X свободных образующих совпадает с группоидом слов. *Словом* в этом случае будет всякая конечная упорядоченная система элементов из X,

$$x_1 x_2 \dots x_n, \quad n \geqslant 1,$$

с любыми повторениями, причем в этой системе задано *распределение скобок*: каждый из символов x_i, $i = 1, 2, \dots, n$, считается взятым в скобки, а затем скобки расставлены так, что каждый раз «перемножаются» лишь две скобки.

Произведение двух слов означает, что заданные слова берутся в скобки и пишутся одно за другим.

Конечно, записывая слова в группоидах, можно писать, например,

$$((x_1x_2)\,x_1)\,(x_3x_2),$$

а не

$$((((x_1)\,(x_2))\,(x_1))\,((x_3)\,(x_2))).$$

8. Класс полугрупп является примитивным классом с тождественным соотношением ассоциативности. В этом случае *слово* относительно множества X свободных образующих может быть записано в виде

$$x_1x_2 \ldots x_n, \quad n \geqslant 1, \tag{4}$$

уже без всяких скобок. *Произведение* двух слов (4) означает теперь, что заданные слова записываются одно за другим без скобок.

Утверждение, что нами построена *свободная полугруппа* с множеством X свободных образующих, будет обосновано лишь после того, как мы покажем, что различные слова вида (4) будут в этой полугруппе различными элементами. Однако умножение слов, определенное в предшествующем абзаце, превращает, очевидно, множество всех слов вида (4) в полугруппу с множеством образующих X. Эта полугруппа является гомоморфным образом свободной полугруппы с множеством X свободных образующих, а так как в ней различные слова вида (4) являются различными элементами, то это же верно и для свободной полугруппы. На самом деле указанный гомоморфизм является, конечно, изоморфизмом.

Использование степеней элементов позволяет записывать слова в полугруппах короче: вместо слова $x_1x_1x_1x_2x_1x_2x_2$ можно писать $x_1^3x_2x_1x_2^2$.

9. Рассмотрим теперь примитивный класс всех групп с операциями умножения, взятия обратного элемента и взятия единицы. Тождественные соотношения позволяют записать всякое *слово* относительно множества X свободных образующих или в виде 1 — это слово, не содержащее ни одного свободного элемента, называется *пустым*, — или же в виде

$$w = x_1^{\varepsilon_1}x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}, \quad n \geqslant 1, \tag{5}$$

где x_i, $i=1, 2, \ldots, n$, — элементы из X, не обязательно различные, $\varepsilon_i = \pm 1$, $i=1, 2, \ldots, n$, причем если $x_i = x_{i+1}$, то и $\varepsilon_i = \varepsilon_{i+1}$; иными словами, в (5) не могут стоять рядом элемент $x \in X$ и его обратный элемент x^{-1}. Число n назовем *длиной* слова (5).

Различные слова вида (5) *являются различными элементами свободной группы с множеством* X *свободных образующих и не равны в этой группе пустому слову.*

Для доказательства построим группу, элементами которой служат пустое слово и всевозможные слова вида (5). Умножение слов определим в соответствии с тем, как оно выполнялось бы в свободной группе. Именно, пустое слово должно играть роль единицы. Если же даны два слова вида (5),

$$w_1 = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}, \qquad w_2 = y_1^{\eta_1} y_2^{\eta_2} \ldots y_m^{\eta_m},$$

где, понятно, $y_i \in X$, $i=1, 2, \ldots, m$, то записываем эти слова одно за другим,

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n} y_1^{\eta_1} y_2^{\eta_2} \ldots y_m^{\eta_m}.$$

Если при этом $x_n = y_1$ и $\varepsilon_n = -\eta_1$, то выполняем *сокращение*. После этого станут соседними элементы $x_{n-1}^{\varepsilon_{n-1}}$ и $y_2^{\eta_2}$, и, быть может, снова придется выполнить сокращение. Так продолжаем до такого первого места k, что или $x_{n-k} \neq y_{k+1}$, или $x_{n-k} = y_{k+1}$, но и $\varepsilon_{n-k} = \eta_{k+1}$. Тогда полагаем

$$w_1 w_2 = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_{n-k}^{\varepsilon_{n-k}} y_{k+1}^{\eta_{k+1}} y_{k+2}^{\eta_{k+2}} \ldots y_m^{\eta_m}. \tag{6}$$

Ясно, что справа в (6) стоит слово вида (5), если $n \neq m$ или же $n=m$, но $k<n$, в противном же случае справа будет стоять пустое слово. Мы получаем, следовательно, что *обратным* для слова (5) будет слово

$$w^{-1} = x_n^{-\varepsilon_n} \ldots x_2^{-\varepsilon_2} x_1^{-\varepsilon_1}.$$

Введенное нами умножение слов ассоциативно.

Будем доказывать равенство

$$w_1 (w_2 w_3) = (w_1 w_2) w_3 \tag{7}$$

индукцией по длине слова w_2, причем все слова w_1, w_2, w_3 можно считать отличными от пустого слова.

Пусть сперва $w_2 = y^{\eta}$, где $y \in X$, $\eta = \pm 1$. Если последний символ слова w_1 и первый символ слова w_3 таковы, что хотя бы один из них отличен от $y^{-\eta}$, то хотя бы в одном

из произведений w_1w_2, w_2w_3 сокращения не будут выполняться и поэтому равенство (7) имеет место. Если же

$$w_1 = x_1^{\varepsilon_1} \dots x_{n-1}^{\varepsilon_{n-1}} y^{-\eta}, \quad w_3 = y^{-\eta} z_2^{\delta_2} \dots z_s^{\delta_s},$$

то

$$x_1^{\varepsilon_1} \dots x_{n-1}^{\varepsilon_{n-1}} y^{-\eta} z_2^{\delta_2} \dots z_s^{\delta_s}$$

будет словом вида (5), равным как левой, так и правой части равенства (7).

Пусть теперь $w_2 = w_2' \cdot y_m^{\eta_m}$, где слово w_2' имеет вид

$$w_2' = y_1^{\eta_1} \dots y_{m-1}^{\eta_{m-1}}.$$

Считая равенство (7) доказанным для случая, когда длина слова w_2 меньше m, получаем

$$\begin{aligned} w_1(w_2w_3) &= w_1\left[\left(w_2' \cdot y_m^{\eta_m}\right) w_3\right] = w_1\left[w_2'\left(y_m^{\eta_m} w_3\right)\right] = \\ &= (w_1w_2')\left(y_m^{\eta_m} w_3\right) = \left[\left(w_1w_2'\right) y_m^{\eta_m}\right] w_3 = \\ &= \left[w_1\left(w_2' y_m^{\eta_m}\right)\right] w_3 = (w_1w_2)\, w_3, \end{aligned}$$

что и требовалось доказать.

Мы построили группу из слов вида (5) и пустого слова, причем множество X служит для нее системой образующих. Эта группа является гомоморфным образом свободной группы с множеством X свободных образующих. Поэтому указанные слова являются различными и в свободной группе, что и требовалось доказать. *Построенная нами группа сама оказывается, следовательно, свободной группой с системой свободных образующих X.*

Слова вида (5) можно, понятно, записывать короче, используя, как и в случае полугрупп, степени элементов, на этот раз и отрицательные.

Свободная группа с одним свободным образующим x будет, очевидно, бесконечной циклической группой $\{x\}$. Если же множество свободных образующих X содержит больше одного элемента, то порожденная им свободная группа некоммутативна, так как слова xy и yx, где $x, y \in X$, будут в ней различными элементами.

В III.8.12 будет дано описание подгрупп свободной группы.

10. В примитивном классе всех абелевых групп, записываемых аддитивно, *словами* относительно множества X свободных образующих будут суммы конечного числа различных элементов из X, взятых с некоторыми целыми коэффициентами, отличными от нуля, а также пустое слово 0. Определим *сложение* таких слов как сложение коэффициентов при одинаковых элементах $x \in X$; если при этом в одно из слов элемент x не входит, то считаем коэффициент при нем равным нулю. Немедленно проверяется, что мы получаем абелеву группу, которая и будет свободной абелевой группой с множеством X свободных образующих.

11. Перейдем к рассмотрению примитивного класса всех колец. Рассуждая так же, как в случае полугрупп или групп, мы получим, что аддитивная группа *свободного кольца* с множеством X свободных образующих является свободной абелевой группой (см. III.7.10) относительно множества свободных образующих $\bar{X}$, которое в свою очередь является свободным мультипликативным группоидом с множеством X свободных образующих (см. III.7.7). Умножение в свободном кольце сводится, в силу закона дистрибутивности, на умножение элементов из $\bar{X}$, которое производится по правилу умножения слов в свободном группоиде (см. III.7.7).

Все сказанное остается справедливым и для *свободного ассоциативного кольца* с множеством X свободных образующих. Множество $\bar{X}$ будет в этом случае, однако, свободной полугруппой с множеством X свободных образующих (см. III.7.8), и умножение элементов из $\bar{X}$ производится по правилу умножения слов в свободной полугруппе.

Наконец, *свободное ассоциативно-коммутативное кольцо* с множеством X свободных образующих является просто кольцом многочленов от элементов из X с целыми коэффициентами.

Заметим, что далеко не для всякого примитивного класса универсальных алгебр удается получить такую однозначную («каноническую») запись элементов свободных алгебр этого класса, какая получена в рассмотренных выше случаях.

12. *Свободные абелевы группы (а также свободные группы, свободные кольца, свободные ассоциативные или ассоциативно-коммутативные кольца) изоморфны тогда и только тогда, если их системы свободных образующих равномощны.*

Действительно, накладывая на абелевы группы тождественное соотношение $2x = 0$, мы получаем примитивный класс тех абелевых групп, все ненулевые элементы которых имеют порядок 2. Возьмем конечную систему свободных образующих X, состоящую из элементов $x_1, x_2, \ldots, x_n$. Тогда словом в рассматриваемом случае будет выражение вида

$$k_1x_1 + k_2x_2 + \ldots + k_nx_n,$$

где все k_i, $i = 1, 2, \ldots, n$, равны единице или нулю. Сложение слов сводится на сложение коэффициентов при одинаковых элементах x_i, выполняемое по модулю 2, т. е. $1 + 1 = 0$. Мы получаем, что в рассматриваемом примитивном классе свободные группы, порожденные конечными системами свободных образующих, сами конечны.

К этому же примитивному классу мы придем, накладывая на класс групп тождественные соотношения $xy = yx$ и $x^2 = 1$ (легко видеть, впрочем, что первое из них вытекает из второго). По существу этот же примитивный класс получается при наложении на указанные в формулировке теоремы классы колец тождественных соотношений

$$xy = 0, \quad 2x = 0.$$

Для доказательства теоремы теперь остается сослаться на вторую теорему Фудзивары (III.7.6).

13. Рассмотрим произвольный примитивный класс Ω-групп. Всякая Ω-группа G этого класса является, по III.7.4, гомоморфным образом некоторой свободной Ω-группы S этого же класса, т. е., по III.2.6 и III.1.8, изоморфна Ω-фактор-группе свободной Ω-группы S по некоторому идеалу A. Пусть элементы s_i, где i пробегает множество индексов I, порождают A как идеал Ω-группы S. Соответствующие элементы в G равны нулю. Система равенств

$$s_i = 0, \quad i \in I, \tag{8}$$

где s_i считаются записанными через свободные образующие свободной Ω-группы S, вполне определяет идеал A в свободной Ω-группе S, т. е. определяет Ω-фактор-группу S/A, а поэтому с точностью до изоморфизма определяет исходную Ω-группу G. Система равенств (8) называется *системой определяющих соотношений* для Ω-группы G.

Таким образом, всякая Ω-группа, в частности всякая группа и всякое кольцо, может быть задана системой определяющих соотношений в некоторой системе образующих. Это задание, конечно, отнюдь не является однозначным.

Пример. Симметрическая группа 3-й степени S_3 (см. II.1.8) может быть задана в классе групп двумя образующими a, b и определяющими соотношениями

$$a^3 = 1, \quad b^2 = 1, \quad abab = 1. \tag{9}$$

Действительно, подстановки

$$a = \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \qquad b = \begin{pmatrix} 123 \\ 213 \end{pmatrix}$$

порождают всю группу S_3 и удовлетворяют соотношениям (9). С другой стороны, из (9) следует равенство $ba = a^2b$, а поэтому всякий элемент группы, заданной определяющими соотношениями (9), может быть записан в виде $a^k b^l$, где $k = 0,1,2$, $l = 0,1$, т. е. эта группа состоит не более чем из шести элементов; порядок группы S_3 равен, однако, шести.

§ 8. Свободные произведения групп

1. Указанное в III.7.3 характерное свойство свободных алгебр данного примитивного класса Λ подсказывает следующее определение. Если A_i, $i \in I$, — семейство алгебр класса Λ, то назовем алгебру G класса Λ *свободным объединением* этого семейства, если $A_i \subset G$, $i \in I$, и если для любой алгебры H класса Λ и любого набора гомоморфизмов φ_i алгебр A_i в алгебру H, $i \in I$, существует, притом единственный, гомоморфизм φ алгебры G в алгебру H, совпадающий с φ_i на подалгебре A_i, $i \in I$.

Если свободным объединением алгебр A_i, $i \in I$, служат как алгебра G, так и алгебра G', то между G и G' существует изоморфизм, продолжающий тождественные автоморфизмы подалгебр A_i, $i \in I$.

Действительно, указанные тождественные автоморфизмы можно рассматривать как гомоморфизмы φ_i подалгебр A_i алгебры G, $i \in I$, в алгебру G', а также как гомоморфизмы ψ_i подалгебр A_i алгебры G', $i \in I$, в алгебру G. Они индуцируют, следовательно, гомоморфизмы $\varphi\colon G \to G'$ и $\psi\colon G' \to G$. Произведение $\varphi\psi$ является тем единственным гомоморфизмом G

в себя, который определяется изоморфными вложениями всех A_i в G в качестве подалгебр, т. е. это будет тождественный автоморфизм алгебры G. Аналогично $\psi\varphi$ является тождественным автоморфизмом алгебры G', а поэтому φ и ψ будут обратными друг другу изоморфизмами.

Свободное объединение G алгебр A_i, $i \in I$, совпадает с подалгеброй, порожденной в G всеми A_i, $i \in I$.

Пусть, в самом деле, подалгебры A_i, $i \in I$, порождают в G подалгебру G_0 (см. III.1.4). Если заданы алгебра H класса Λ и гомоморфизмы φ_i: $A_i \to H$, $i \in I$, то определяемый этими гомоморфизмами гомоморфизм φ: $G \to H$ индуцирует гомоморфизм φ_0: $G_0 \to H$, совпадающий с φ_i на подалгебре A_i, $i \in I$. Это будет единственный гомоморфизм G_0 в H с указанным свойством. Действительно, без труда проверяется, что подалгебра G_0 состоит из тех и только из тех элементов алгебры G, которые хотя бы одним способом выражаются через элементы подалгебр A_i, $i \in I$, при помощи операций алгебры G, применяемых конечное число раз. Гомоморфизмы φ_i, $i \in I$, могут порождать, следовательно, лишь один гомоморфизм алгебры G_0.

Таким образом, алгебра G_0 сама оказалась свободным объединением алгебр A_i, $i \in I$. Тогда существует, как доказано, изоморфизм φ алгебры G_0 на алгебру G, продолжающий тождественные автоморфизмы алгебр A_i, $i \in I$. Но, ввиду сказанного в предшествующем абзаце, эти тождественные автоморфизмы могут порождать лишь тождественный автоморфизм алгебры G_0, а поэтому $G_0 = G$.

2. Группа G называется *свободным произведением* своих подгрупп A_i, $i \in I$, если эти подгруппы порождают вместе всю группу G и если всякий отличный от 1 элемент $g \in G$ обладает единственным разложением в произведение вида

$$g = a_1 a_2 \ldots a_n, \quad n \geqslant 1, \tag{1}$$

где $a_k \in A_{i_k}$ и $a_k \neq 1$, $k = 1, 2, \ldots, n$, причем рядом не могут стоять элементы из одной и той же подгруппы A_i, т. е.

$$i_k \neq i_{k+1}, \quad k = 1, 2, \ldots, n-1.$$

Произведение с этими свойствами, стоящее в (1) справа, будем называть *несократимой записью* элемента g. Число n назовем *длиной* этого элемента и обозначим ее через $\lambda(g)$.

Индексы i_1 и i_n будем называть соответственно *первым индексом* и *последним индексом* элемента g. Дополнительно положим $\lambda(1) = 0$.

Для записи свободного произведения будем использовать символ

$$G = \prod_{i \in I}^{*} A_i$$

или, если число свободных множителей конечно,

$$G = A_1 * A_2 * \ldots * A_n.$$

Сопоставление с III.7.9 показывает, что *свободная группа является свободным произведением бесконечных циклических групп.*

Если группа G является свободным произведением подгрупп A_i, $i \in I$, то G будет свободным объединением групп A_i в примитивном классе групп.

В самом деле, если для набора гомоморфизмов φ_i подгрупп A_i в некоторую группу H, $i \in I$, существует такой гомоморфизм φ группы G в H, что $\varphi = \varphi_i$ на подгруппе A_i, $i \in I$, то, по (1), для всех $g \in G$

$$g\varphi = a_1\varphi_{i_1} \cdot a_2\varphi_{i_2} \ldots a_n\varphi_{i_n}, \tag{2}$$

т. е. φ определено однозначно. Легко проверяется, с другой стороны, что если (2) считать определением отображения φ группы G в группу H, то φ будет гомоморфизмом.

Эта теорема допускает обращение, как немедленно следует, ввиду теоремы, доказываемой в следующем пункте, из результатов настоящего и предшествующего пунктов.

3. Докажем, что *для любого семейства групп A_i, $i \in I$, существует свободное произведение этого семейства групп*, т. е., точнее, свободное произведение групп, изоморфных заданным.

Будем называть *словом* формально написанное выражение

$$a_1 a_2 \ldots a_n, \quad n \geqslant 1, \tag{3}$$

где $a_k \in A_{i_k}$, $a_k \neq 1$, $k = 1, 2, \ldots, n$, и $i_k \neq i_{k+1}$, $k = 1, 2, \ldots, n-1$.

Введем также *пустое слово* (случай $n = 0$). Множество всех слов обозначим через M, а симметрическую группу на этом множестве (см. II.1.8) — через S.

Всякий элемент $a \in A_i$ следующим образом определяет отображение $\bar{a}$ множества M в себя: пустое слово переходит в слово a длины 1, откуда следует, что при $a \neq b$, $a, b \in A_i$, будет $\bar{a} \neq \bar{b}$; с другой стороны, для слова вида (3) полагаем

$$(a_1a_2 \dots a_n)\bar{a} = \begin{cases} a_1a_2 \dots a_na, & \text{если } i_n \neq i; \\ a_1a_2 \dots (a_na), & \text{если } i_n = i \text{ и } a_na \neq 1; \\ a_1a_2 \dots a_{n-1}, & \text{если } i_n = i \text{ и } a_na = 1. \end{cases}$$

Отсюда следует, в частности, что единице группы A_i соответствует тождественное отображение множества M на себя.

Легко проверяется, что

$$\overline{ab} = \bar{a}\bar{b}, \quad a, b \in A_i,$$

где произведение справа понимается в смысле умножения отображений, а поэтому отображение $\overline{a^{-1}}$ обратно отображению $\bar{a}$. Таким образом, всякое отображение $\bar{a}$ будет подстановкой в множестве M и, следовательно, отображения $\bar{a}$, взятые для всех $a \in A_i$, составляют в группе S подгруппу $\bar{A}_i$, изоморфную группе A_i.

Обозначим через G подгруппу группы S, порожденную всеми подгруппами $\bar{A}_i$, $i \in I$. Группа G будет свободным произведением подгрупп $\bar{A}_i$, $i \in I$: всякий элемент из G, отличный от единицы, может быть записан в виде произведения

$$\bar{a}_1\bar{a}_2 \dots \bar{a}_n, \tag{4}$$

где $a_1a_2 \dots a_n$ — слово, причем эта запись единственная, так, как подстановка (4) переводит пустое слово как раз в слово $a_1a_2 \dots a_n$.

4. Докажем следующую теорему о подгруппах свободного произведения групп [А. Г. Курош, Math. Ann. **109** (1934), 647—660]:

Если

$$G = \prod_{i \in I}^{*} A_i, \tag{5}$$

то всякая подгруппа U группы G является свободным произведением подгрупп, сопряженных в G (см. II.74) *с некоторыми подгруппами свободных множителей A_i, и некоторой свободной подгруппы.*

Для того, чтобы указать более развернутую формулировку этой теоремы, введем следующее понятие. Элементы $x, y \in G$ назовем *эквивалентными по двойному модулю* (A_i, U), если

$$y = a_i x u, \qquad a_i \in A_i, \qquad u \in U.$$

Так как A_i и U — подгруппы, то мы получаем разбиение группы G на непересекающиеся классы вида $A_i x U$, которое назовем *разложением* (A_i, U).

Заметим, что если D — класс из разложения (A_i, U), то D вместе со всяким своим элементом x содержит и весь левый смежный класс xU, т. е. состоит из нескольких левых классов по U.

Развернутая формулировка теоремы о подгруппах такова:

Если имеет место (5) *и* $U \subset G$, *то во всех классах* D *каждого из разложений* (A_i, U), $i \in I$, *можно так выбрать по одному представителю*

$$s = s(i, D),$$

что

$$U = \prod_{i \in I,\ D \in (A_i, U)}^{*} (U \cap s^{-1} A_i s) * F, \tag{6}$$

где F — *свободная подгруппа. Выбор представителей возможен при этом такой, что для всех* $i \in I$ *единица будет представителем своего класса* $A_i U$, *т. е. все пересечения* $U \cap A_i$, $i \in I$, *отличные от* E, *входят свободными множителями в разложение* (6).

5. Доказательство этой теоремы, приводимое ниже, принадлежит Маклейну [Mathematika **5** (1958), 13—19].

Лемма 1. *Существуют такие, зависящие от* $i \in I$, *выборы систем представителей* $r_i(C)$ *во всех левых смежных классах* C *по подгруппе* U, *что выполняются следующие требования*:

1) $r_i(U) = 1$;

2) *если* $a_i \in A_i$, *то* $r_i(a_i C) = a_i' r_i(C)$, *где* $a_i' \in A_i$;

3) *если* $r_i(C) = a_i s$, *где* $a_i \in A_i$ (a_i *может при этом равняться единице*), *а* $s \neq 1$ *и первый индекс* j *элемента* s *отличен от* i, *то*

$$r_i(sU) = r_j(sU) = s.$$

Будем вести выбор представителей $r_i(C)$ индукцией по минимальной длине $\lambda(A_i C)$ элементов того класса $A_i C$

разложения по двойному модулю (A_i, U), в состав которого входит C. Будем считать при этом, что выполняется также следующее требование

4) $\lambda(r_i(C)) \leqslant 1 + \lambda(A_iC)$.

Если $\lambda(A_iC) = 0$, т. е. $A_iC = A_i \cdot 1 \cdot U = A_iU$, то в C имеются элементы из A_i и в качестве $r_i(C)$ берем любой из этих элементов, полагая лишь $r_i(U) = 1$. Требования 1), 2) и 4) проверяются без затруднений, а требование 3) в рассматриваемом случае бессодержательно.

Пусть теперь класс D разложения (A_i, U) таков, что $\lambda(D) = n \geqslant 1$. Если $g \in D$ и $\lambda(g) = n$, то $D = A_igU$, а первый индекс j элемента g отличен от i, так как иначе в классе D нашелся бы элемент, длина которого меньше n. Так как $\lambda(A_jgU) < n$, то по индуктивному предположению, уже выбран представитель $r_j(gU) = s$, причем, по 4), $\lambda(s) \leqslant n$. Так как $D = A_isU$, то $n = \lambda(D) \leqslant \lambda(s)$ и, следовательно, $\lambda(s) = n$, а поэтому первый индекс k элемента s отличен от i, причем, по индуктивному предположению (условие 3)), $r_k(sU) = s$.

Выбираем теперь представителей $r_i(C)$ для всех C, входящих в состав D. Именно, если $C = sU$, то полагаем $r_i(C) = s$; для всякого другого $C \subseteq D$ в качестве $r_i(C)$ берем один из содержащихся в C элементов a_is, $a_i \in A_i$. Ясно, что требования 2), 3) и 4) выполняются, а требование 1) к случаю $n \geqslant 1$ не имеет отношения.

Лемма доказана. Одновременно мы получили, что в каждом классе $D \in (A_i, U)$ среди представителей $r_i(C)$ для всех левых классов C, входящих в D, имеется ровно один такой представитель s, который или равен 1, или же его первый индекс отличен от i. Именно этот представитель выбирается в качестве $s(i, D)$. Еще раз отметим, что для всякого класса C, входящего в D, представитель $r_i(C)$ отличается от $s(i, D)$ левым множителем, принадлежащим к A_i.

6. Лемма 2. *Подгруппа U порождается всеми элементами $r_i^{-1}(C)\, r_j(C)$, где $i, j \in I$, а C пробегает левые смежные классы по U, и всеми пересечениями $U \cap (s^{-1}A_is)$, где $s = s(i, D)$, $D \in (A_i, U)$, $i \in I$.*

Заметим сперва, что представители $r_i(C)$ и $r_j(C)$ оба принадлежат к C, т. е. отличаются друг от друга правым множителем из U, а поэтому $r_i^{-1}(C)\, r_j(C) \in U$.

Возьмем теперь произвольный элемент $g \in G$, его произвольную (не обязательно несократимую) запись вида

$$g = a_1 a_2 \ldots a_n, \quad a_k \in A_{i_k}, \quad k = 1, 2, \ldots, n, \tag{7}$$

и любой левый класс C по U. Тогда легкая проверка, которую целесообразно вести снизу вверх, показывает справедливость следующего равенства, в правой части которого стоит произведение элементов, взятых в квадратные скобки:

$$\begin{aligned} r_{i_1}^{-1}(gC) \cdot g \cdot r_{i_n}(C) &= r_{i_1}^{-1}(gC) \cdot a_1 a_2 \ldots a_n \cdot r_{i_n}(C) = \\ &= [r_{i_1}^{-1}(gC) \cdot a_1 \cdot r_{i_1}(a_2 \ldots a_n C)] \cdot \\ &\quad \cdot \ldots \ldots \ldots \ldots \ldots \ldots \\ &\quad \cdot [r_{i_{n-2}}^{-1}(a_{n-1} a_n C) \cdot r_{i_{n-1}}(a_{n-1} a_n C)] \cdot \\ &\quad \cdot [r_{i_{n-1}}^{-1}(a_{n-1} a_n C) \cdot a_{n-1} \cdot r_{i_{n-1}}(a_n C)] \cdot \\ &\quad \cdot [r_{i_{n-1}}^{-1}(a_n C) \cdot r_{i_n}(a_n C)] \cdot [r_{i_n}^{-1}(a_n C) \cdot a_n \cdot r_{i_n}(C)]. \end{aligned}$$

В каждой строчке первый множитель имеет вид

$$r_i^{-1}(C')\, r_j(C').$$

Рассмотрим любой из вторых множителей,

$$x = r_{i_k}^{-1}(a_k a_{k+1} \ldots a_n C) \cdot a_k \cdot r_{i_k}(a_{k+1} \ldots a_n C), \quad k = 1, 2, \ldots, n,$$

и покажем, что он содержится в пересечении $U \cap s^{-1} A_{i_k} s$, где $s = s(l_k, D)$, $D \in (A_{i_k}, U)$ и $C' \subseteq D$, причем

$$C' = a_{k+1} \ldots a_n C.$$

Действительно, так как

$$r_{i_k}(a_k C') = a_{i_k} s, \quad r_{i_k}(C') = a'_{i_k} s,$$

где $a_{i_k}, a'_{i_k} \in A_{i_k}$, то

$$x = s^{-1}\left(a_{i_k}^{-1} a_k a'_{i_k}\right) s \in s^{-1} A_{i_k} s.$$

С другой стороны, если $C = cU$, то

$$r_{i_k}(a_k a_{k+1} \ldots a_n C) = a_k a_{k+1} \ldots a_n c u_1, \; u_1 \in U,$$

$$r_{i_k}(a_{k+1} \ldots a_n C) = a_{k+1} \ldots a_n c u_2, \; u_2 \in U,$$

а поэтому $x = u_1^{-1} u_2 \in U$.

Заметим теперь, что если $C = U$ и $g \in U$, то

$$r_{i_1}(gC) = r_{i_n}(C) = 1,$$

и поэтому полученное выше основное равенство превращается в выражение для g, доказывающее нашу лемму.

7. Введем в рассмотрение символы $[C, i, j]$ для любых $i, j \in I$ и любых левых классов C по U. Обозначим через F группу, которая имеет множество всех этих символов своей системой образующих и задается в этих образующих системой определяющих соотношений (см. III.7.13), состоящей из всевозможных равенств следующих типов:

(а) $[C, i, j][C, j, k] = [C, i, k]$,

(б) $[U, i, j] = 1$,

(в) $[sU, i, j] = 1$, если $s = s(i, D)$, а j — первый индекс элемента s.

Лемма 3. *Группа F является свободной группой.*

В самом деле, из (а) следует равенство

$$[C, i, j] = [C, i, k] \cdot [C, j, k]^{-1},$$

а поэтому в системе образующих можно оставить лишь символы $[C, i, k]$ с фиксированным вторым индексом k. Определяющими соотношениями в этих образующих являются равенства следующих типов:

(а′) $[C, k, k] = 1$,

(б′) $[U, i, k] = 1$,

(в′) $[sU, i, k] = [sU, j, k]$, где $s = s(i, D)$, а j — первый индекс элемента s.

Выбрасывая, наконец, все образующие, равные 1, и оставляя в каждом классе равных между собою образующих лишь по одному представителю, мы получим для F систему образующих, не связанных никакими нетривиальными соотношениями, т. е. систему свободных образующих.

8. Сопоставим каждой группе $U \cap s^{-1}A_i s$, где $s = s(i, D)$, $D \in (A_i, U)$, $i \in I$, изоморфную ей группу $B_{i,D}$ и фиксируем определенный изоморфизм $\sigma_{i,D}\colon B_{i,D} \to (U \cap s^{-1}A_i s)$. С другой стороны, сопоставим каждому элементу $[C, i, j]$ группы F элемент $r_i^{-1}(C) r_j(C)$ подгруппы U. Так как после такой замены равенства (а), (б) и (в) не нарушаются (см. 1) и 3) из леммы 1), то этим определяется гомоморфизм σ_F группы F в группу U.

Возьмем теперь, в соответствии с III.8.3, группу

$$B = \prod_{i \in I,\ D \in (A_i, U)}^{*} B_{i,D} * F. \tag{8}$$

Набор всех гомоморфизмов $\sigma_{i,D}$ *и* σ_F *индуцирует, по* III.8.2, *однозначно определенный гомоморфизм* σ *группы* B *в группу* U, даже, по лемме 2, на U.

9. Вернемся к рассмотрению основной формулы из III.8.6, дающей выражение для элемента $r_{i_1}^{-1}(gC)\cdot g\cdot r_{i_n}(C)$. Если в правой части этой формулы всякий множитель вида $r_i^{-1}(C)r_j(C)$ заменим соответствующим элементом $[C, i, j]$ из F, а всякий множитель из подгруппы вида $U\cap s^{-1}A_j s$ — соответствующим ему при изоморфизме $\sigma_{i,D}^{-1}$ элементом из $B_{i,D}$, то получим вполне определенный элемент группы B, который обозначим через $m(g, C)$.

Лемма 4. *Элемент* $m(g, C)$ *не зависит от выбора записи* (7) *для элемента* g *и обладает следующими свойствами*:

$$m(gh, C) = m(g, hC)\cdot[hC, i, j]\cdot m(h, C), \tag{9}$$

где i *— последний индекс элемента* g, j *— первый индекс элемента* h;

$$m(1, C) = 1, \tag{10}$$

$$m(g^{-1}, C) = m^{-1}(g, g^{-1}C). \tag{11}$$

Все эти утверждения без труда вытекают из определения элемента $m(g, C)$. Нужно лишь учесть, что элемент g обладает единственной несократимой записью относительно свободного разложения (5) и что от одной записи вида (7) для элемента g можно перейти к любой другой такой записи конечным числом следующих преобразований и преобразований, к ним обратных: если $i_k = i_{k+1}$ и $a_k a_{k+1} = a' \in A_{i_k}$, то в (7) отрезок $a_k a_{k+1}$ заменяется элементом a' при $a' \neq 1$ и выбрасывается при $a' = 1$.

Равенство (9) при $C = U$ и $g, h \in U$ показывает, ввиду (б) из III.8.7, что *отображение* τ, *сопоставляющее каждому элементу* $g\in U$ *элемент* $m(g, U)\in B$, *будет гомоморфизмом* U *в* B.

Лемма 5. *Произведение* $\tau\sigma$ *является тождественным отображением группы* U *на себя.*

Действительно, из определения гомоморфизма σ и элемента $m(g, C)$ следует, что

$$m(g, C)\sigma = r_{i_1}^{-1}(gC)\cdot g\cdot r_{i_n}(C), \tag{12}$$

а поэтому для $g \in U$, ввиду 1) из леммы 1,

$$g(\tau\sigma) = m(g, U)\,\sigma = g.$$

10. Лемма 6. *Если* $r = r_i(C)$, *то* $m(r, U) = 1$.

Доказательство ведем индукцией по $\lambda(r)$, так как для $r = 1$ утверждение леммы следует из (10). Пусть $r = ag$, где $a \in A_j$, $\lambda(g) = \lambda(r) - 1$ и поэтому или $g = 1$, или же первый индекс k элемента g отличен от j. Если $j \neq i$, то, по 3) из леммы 1, $r_j(C) = r$, а поэтому, снова по 3) из леммы 1, будет $r_j(gU) = g$. Отсюда по индуктивному предположению

$$m(g, U) = 1. \tag{13}$$

Пусть $g \neq 1$. Тогда, по (9),

$$m(r, U) = m(ag, U) = m(a, gU) \cdot [gU, j, k] \cdot m(g, U).$$

Однако, из $j \neq k$ следует (см. последний абзац в III.8.5), что $g = s(j, D)$, где $D = A_j gU$, а поэтому, по (в) из III.8.7,

$$[gU, j, k] = 1.$$

Отсюда и из (13) следует, что

$$m(r, U) = m(a, gU).$$

Это равенство справедливо, очевидно, и при $g = 1$. Так как, наконец, $a \in A_j$, то, по определению элемента $m(g, C)$,

$$m(r, U) = m(a, gU) = \left[r_i^{-1}(rU) \cdot a \cdot r_j(gU)\right] \sigma_{i,D}^{-1} =$$

$$= \left(r^{-1} ag\right) \sigma_{i,D}^{-1} = 1.$$

11. Лемма 7. *Произведение* $\sigma\tau$ *является тождественным отображением группы* B *на себя.*

Достаточно, ввиду (8), найти образы при $\sigma\tau$ для элементов вида $[C, i, j]$ и для элементов из подгрупп $B_{i,D}$.

Если $b = [C, i, j]$, то

$$b(\sigma\tau) = \left(b\sigma_F\right)\tau = \left[r_i^{-1}(C)\, r_j(C)\right]\tau.$$

Положим $r_i(C) = r$, $r_j(C) = r_0$ и обозначим первые индексы этих элементов соответственно через k и k_0. Тогда, ввиду $r^{-1}r_0 \in U$ и (9),

$$b(\sigma\tau) = (r^{-1}r_0)\,\tau = m(r^{-1}r_0, U) =$$

$$= m(r^{-1}, r_0U)\,[r_0U, k, k_0]\, m(r_0, U).$$

Но, по лемме 6 и (11),

$$m(r_0, U) = 1,$$

$$m(r^{-1}, r_0U) = m^{-1}(r, r^{-1}r_0U) = m^{-1}(r, U) = 1$$

и поэтому, так как $r_0U = C$,

$$b(\sigma\tau) = [C, k, k_0].$$

Если $k = i$, $k_0 = j$, то $b(\sigma\tau) = b$. Если $k_0 \neq j$, то, так как $r_0 = r_j(C)$, то $r_0 = s(j, D)$ для соответствующего D. Поэтому, по (в) из III.8.7, $[r_0U, j, k_0] = 1$, а тогда, по (а) из III.8.7,

$$b(\sigma\tau) = [C, k, k_0] = [C, k, j][C, j, k_0] = [C, k, j].$$

Если, наконец, и $k \neq i$, то аналогичные рассмотрения позволяют заменить k через i, т. е. снова $b(\sigma\tau) = b$.

Пусть теперь $b \in B_{i, D}$. Тогда

$$b\sigma = b\sigma_{i, D} = s^{-1}as, \tag{14}$$

где $a \in A_i$, $s = s(i, D)$. В то же время $b\sigma \in U$, а поэтому

$$asU = sU. \tag{15}$$

Отсюда, ввиду (9), если через j обозначим первый индекс элемента s, $j \neq i$,

$$b(\sigma\tau) = (s^{-1}as)\tau = m(s^{-1}as, U) =$$
$$= m(s^{-1}, asU) \cdot [asU, j, i] \cdot m(a, sU) \cdot [sU, i, j] \cdot m(s, U).$$

Но, по лемме 6 и (11)

$$m(s, U) = 1,$$

$$m(s^{-1}, asU) = m^{-1}(s, s^{-1}asU) = m^{-1}(s, U) = 1.$$

С другой стороны, по (в), (а) и (а′) из III.8.7 и (15),

$$[sU, i, j] = 1,$$

$$[asU, j, i] = [sU, j, i] = [sU, i, j]^{-1} = 1.$$

Мы получаем, ввиду (14) и (15), что

$$b(\sigma\tau) = m(a, sU) = \left[r_i^{-1}(asU) \cdot a \cdot r_i(sU)\right]\sigma_{i, D}^{-1} =$$
$$= (s^{-1}as)\sigma_{i, D}^{-1} = b,$$

что и требовалось доказать.

12. Из лемм 5 и 7 вытекает, что каждое из отображений σ и τ является изоморфизмом между U и B. Этим, ввиду (8), определения σ и леммы 3, доказано основное утверждение теоремы о подгруппах. Ее второе утверждение доказано при выборе представителей $s(i, D)$ в III.8.5.

Так как всякая подгруппа, сопряженная внутри некоторой группы с подгруппой бесконечной циклической группы, сама является бесконечной циклической группой, а свободное произведение свободных групп само будет свободной группой, то из доказанной теоремы вытекает

Теорема Нильсена — Шрейера. *Всякая подгруппа свободной группы, отличная от единичной подгруппы, сама свободна.*

13. Отметим следующее очевидное свойство свободных произведений:

Если

$$G = \prod_{i \in I}^{*} A_i \tag{16}$$

и

$$A_i = \prod_{j \in J_i}^{*} A_{ij}, \qquad i \in I,$$

то

$$G = \prod_{i \in I,\ j \in J_i}^{*} A_{ij}. \tag{17}$$

Свободное разложение (17) называется *продолжением* свободного разложения (16).

Два свободных разложения группы G,

$$G = \prod_{i \in I}^{*} A_i * F_1 = \prod_{j \in J}^{*} B_j * F_2,$$

называются *изоморфными*, если F_1 и F_2 являются изоморфными свободными группами, а между свободными множителями A_i и B_j можно установить такое взаимно однозначное соответствие, что соответствующие множители сопряжены в группе G.

Справедлива следующая теорема [А. Г. Курош, Math. Ann. **109** (1934), 647 — 660; Бэр и Леви, Comp. Math. **3** (1936), 391 — 398]:

Два любых свободных разложения произвольной группы обладают изоморфными продолжениями.

В самом деле, если

$$G=\prod_{i\in I}^{*} A_i=\prod_{j\in J}^{*} B_j, \tag{18}$$

то, применяя теорему о подгруппах, получаем

$$B_j=\prod_{i\in I,\ D\in(A_i,\ B_j)}^{*}(B_j\cap s^{-1}A_is)*F_j,\qquad s=s(i,\ D),\qquad j\in J;$$

$$A_i=\prod_{j\in J,\ D'\in(B_j,\ A_i)}^{*}(A_i\cap t^{-1}B_jt)*F_i',\qquad t=s(j,\ D'),\qquad i\in I.$$

Этим определяются продолжения свободных разложений (18), и мы хотим доказать их изоморфность.

Фиксируем пару индексов $i\in I, j\in J$ и заметим, что если $D\in(A_i,\ B_j)$, то совокупность D^{-1} элементов, обратных ко всем элементам из D, будет классом разложения $(B_j,\ A_i)$, причем этим путем между классами указанных двух разложений устанавливается взаимно однозначное соответствие. Докажем сопряженность в G подгрупп $B_j\cap s^{-1}A_is$ и $A_i\cap t^{-1}B_jt$, где $s=s(i,\ D)$, $t=s(j,\ D^{-1})$. Так как

$$D^{-1}=B_jtA_i=(A_isB_j)^{-1}=B_js^{-1}A_i,$$

то

$$t=b_js^{-1}a_i,\quad b_j\in B_j,\quad a_i\in A_i.$$

Поэтому

$$A_i\cap t^{-1}B_jt=A_i\cap a_i^{-1}sb_j^{-1}B_jb_js^{-1}a_i=$$
$$=A_i\cap a_i^{-1}sB_js^{-1}a_i=a_i^{-1}s(s^{-1}A_is\cap B_j)s^{-1}a_i.$$

Для окончания доказательства остается отметить, что нормальный делитель, порожденный в группе некоторой системой подгрупп, не меняется, если каждая из этих подгрупп заменяется подгруппой, с нею сопряженной, а затем воспользоваться следующим свойством свободного произведения:

Если $G=A*B$ и A порождает в G нормальный делитель $\bar{A}$, то B изоморфно фактор-группе $G/\bar{A}$.

В самом деле, нормальный делитель $\bar{A}$ состоит из тех и только тех элементов из G, для которых произведение элементов из B, входящих в их несократимую запись (с сохранением их взаимного порядка) равно 1. Отсюда следует, что всякий смежный класс G по $\bar{A}$ содержит ровно один элемент из B.

ГЛАВА ЧЕТВЕРТАЯ

СТРУКТУРЫ

§ 1. Структуры, полные структуры

1. Параллелизм между теорией групп и теорией колец привел к введению в алгебру, наряду с понятием Ω-группы, и некоторых других понятий. Одно из них, а именно понятие структуры, подсказано тем, что и множества всех подгрупп или всех нормальных делителей некоторой группы, и множества всех подколец или всех идеалов (двусторонних, левых или правых) некоторого кольца частично упорядочены по теоретико-множественному включению, причем эта частичная упорядоченность обладает некоторыми дополнительными свойствами.

Частично упорядоченное множество S называется *структурой*, если оно удовлетворяет следующим двум условиям:

I_1. Для всякой пары элементов a, $b \in S$ в S существует такой элемент $c = a \cap b$, *пересечение* элементов a и b, что

$$c \leqslant a, \qquad c \leqslant b,$$

причем если некоторый элемент c' также обладает свойствами $c' \leqslant a$, $c' \leqslant b$, то $c' \leqslant c$.

I_2. Для всякой пары элементов a, $b \in S$ в S существует такой элемент $d = a \cup b$, *объединение* элементов a и b, что

$$d \geqslant a, \qquad d \geqslant b,$$

причем если некоторый элемент d' также обладает свойствами $d' \geqslant a$, $d' \geqslant b$, то $d' \geqslant d$.

Ясно, что и пересечение $a \cap b$, и объединение $a \cup b$ элементов a и b определены однозначно. Ясно также, что частично упорядоченное множество, инверсно изоморфное структуре

(см. 1.4.6.), само будет структурой, причем понятия пересечения и объединения двойственны друг другу (см. 1.5.5).

Мы видим, что можно говорить о *структуре подгрупп* и *структуре нормальных делителей* некоторой группы G, а также о *структуре подколец, структуре идеалов, структуре левых (правых) идеалов* некоторого кольца R. Во всех этих случаях пересечением подгрупп (или подколец) A и B является их теоретико-множественное пересечение $A \cap B$, а роль объединения играет подгруппа (подкольцо) $\{A, B\}$, порожденная этими подгруппами (подкольцами). Можно говорить, вообще, о *структуре подалгебр* данной универсальной алгебры, а также о *структуре* Ω*-подгрупп* и о *структуре идеалов* данной Ω-группы.

Укажем некоторые другие примеры структур. Так, все подмножества множества M составляют структуру по теоретико-множественному включению, причем пересечение и объединение имеют теоретико-множественный смысл; эта *структура подмножеств* M будет в дальнейшем использоваться.

Всякое линейно упорядоченное множество L *является структурой,* причем если $a, b \in L$ и $a \leqslant b$, то

$$a \cap b = a, \qquad a \cup b = b.$$

Множество натуральных чисел будет структурой, если в качестве отношения порядка принять отношение делимости. Роль пересечения играет здесь наибольший общий делитель, а объединением будет наименьшее общее кратное.

2. Структуры могут рассматриваться как частный случай универсальных алгебр. Именно, понятие структуры может быть определено без использования частичной упорядоченности, а лишь при помощи свойств бинарных операций пересечения и объединения:

Множество S *с двумя бинарными операциями* $a \cap b$ *и* $a \cup b$ *тогда и только тогда будет структурой, если эти операции удовлетворяют следующим тождественным соотношениям*:

II_1. $a \cap a = a$, $a \cup a = a$;

II_2. $a \cap b = b \cap a$, $a \cup b = b \cup a$;

II_3. $(a \cap b) \cap c = a \cap (b \cap c)$, $(a \cup b) \cup c = a \cup (b \cup c)$;

II_4. $a \cap (a \cup b) = a$, $a \cup (a \cap b) = a$.

Предположим сперва, что дана структура S, т. е. что операции $a \cap b$ и $a \cup b$ определены условиями I_1 и I_2. Тогда

выполнение свойств II_1 и II_2 очевидно. Проверим свойство II_3, например для пересечения. Так как, по I_1,

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

то, снова по I_1,

$$(a \cap b) \cap c \leqslant b \cap c,$$
$$(a \cap b) \cap c \leqslant a \cap (b \cap c).$$

Аналогично

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

а поэтому имеет место II_3.

С другой стороны, ясно, ввиду I_1, что

$$a \cap (a \cup b) \leqslant a;$$

однако $a \leqslant a$ и, по I_2, $a \leqslant a \cup b$, а поэтому, по I_1,

$$a \leqslant a \cap (a \cup b).$$

Отсюда следует справедливость II_4.

Пусть теперь дано множество S с двумя бинарными операциями, обладающими свойствами II_1—II_4. Если $a, b \in S$, то равенства

$$a \cap b = a, \qquad a \cup b = b \tag{1}$$

одновременно выполняются или не выполняются. Действительно, если $a \cap b = a$, то, по II_4 и II_2,

$$a \cup b = (a \cap b) \cup b = b;$$

если же $a \cup b = b$, то, по II_4,

$$a \cap b = a \cap (a \cup b) = a.$$

Если равенства (1) для элементов a и b имеют место, то положим $a \leqslant b$. Этим в множество S введена частичная упорядоченность. Действительно, $a \leqslant a$ ввиду II_1. Далее, если $a \leqslant b$ и $b \leqslant c$, т. е. $a \cap b = a$, $b \cap c = b$, то, в силу II_3,

$$a \cap c = (a \cap b) \cap c = a \cap (b \cap c) = a \cap b = a,$$

т. е. $a \leqslant c$. Наконец, если $a \leqslant b$ и $b \leqslant a$, т. е. $a \cap b = a$, $b \cap a = b$, то, ввиду II_2, $a = b$.

Покажем, что выполняется условие I_1. Из $(a \cap b) \cap a = a \cap (a \cap b) = (a \cap a) \cap b = a \cap b$ следует $a \cap b \leqslant a$. Анало-

гично $a \cap b \leqslant b$. Если же в S взят произвольный элемент c', удовлетворяющий условиям $c' \leqslant a$, $c' \leqslant b$, т. е. $c' \cap a = c'$, $c' \cap b = c'$, то

$$c' \cap (a \cap b) = (c' \cap a) \cap b = c' \cap b = c',$$

откуда $c' \leqslant a \cap b$. Элемент $a \cap b$ является, следовательно, пересечением элементов a и b в смысле условия I_1. Аналогичным образом доказывается, что элемент $a \cup b$ будет объединением элементов a и b в смысле условия I_2.

3. Полученное нами второе определение понятия структуры показывает, что *структуры составляют примитивный класс универсальных алгебр с двумя бинарными операциями* (см. III.6.3). Это определение по существу должно считаться основным, как следует из приводимых ниже определений подструктуры и изоморфного вложения структур.

Именно, подмножество T структуры S называется *подструктурой* этой структуры, если оно является подалгеброй структуры S, рассматриваемой как универсальная алгебра в смысле определения IV.1.2. Иными словами, T вместе со всякими своими элементами a и b содержит их пересечение $a \cap b$ и их объединение $a \cup b$, понимаемые в смысле операций в структуре S, т. е. T само является структурой относительно операций, определенных в S.

Следует учесть, что подмножество T структуры S может оказаться структурой по той частичной упорядоченности, которая индуцируется в T частичной упорядоченностью, заданной в S, не являясь подструктурой в смысле данного выше определения. Так, хотя в структуре подгруппы группы G упорядоченность теоретико-множественная, однако эта структура не будет подструктурой в структуре всех подмножеств множества G, так как объединения в этих двух структурах имеют разный смысл. Аналогично структура подколец кольца R не будет подструктурой структуры подгрупп аддитивной группы этого кольца.

Структура нормальных делителей группы G является подструктурой структуры всех подгрупп этой группы, как показано в II.7.5. Вообще, из сказанного в III.2.4 следует, что *структура идеалов Ω-группы G будет подструктурой как в структуре всех Ω-подгрупп этой Ω-группы, так и в структуре подгрупп ее аддитивной группы.*

4. Взаимно однозначное отображение φ структуры S в структуру S' называется *изоморфным отображением* или *изоморфным вложением* S в S', если для любых $a, b \in S$

$$(a \cap b)\varphi = a\varphi \cap b\varphi, \qquad (a \cup b)\varphi = a\varphi \cup b\varphi.$$

Иными словами, это будет изоморфизм структур, рассматриваемых как универсальные алгебры (см. III.1.5).

Изоморфное вложение φ структуры S в структуру S' является изоморфным вложением S в S' в смысле изоморфизма частично упорядоченных множеств (см. I.4.4). Действительно, пусть $a, b \in S$. Если $a \leqslant b$, т. е. $a \cap b = a$, то

$$(a \cap b)\varphi = a\varphi \cap b\varphi = a\varphi,$$

откуда $a\varphi \leqslant b\varphi$. Проводя эти рассуждения в обратном порядке и используя взаимную однозначность отображения φ, мы получим, что из $a\varphi \leqslant b\varphi$ следует $a \leqslant b$.

Примеры, приведенные выше, показывают, что обратное утверждение не имеет места: если даны частично упорядоченные множества S и S' и φ — изоморфное отображение S в S', то в том случае, когда S и S' являются структурами, φ не обязано быть изоморфным отображением структуры S в структуру S'. Положение будет, впрочем, иным, если рассматриваются изоморфные отображения S *на* S':

Если даны структуры S и S', то всякое изоморфное отображение S на S', понимаемое в смысле частичной упорядоченности, будет изоморфным отображением структуры S на структуру S'.

Действительно, если $a, b \in S$, то из $a \cap b \leqslant a$ следует $(a \cap b)\varphi \leqslant a\varphi$; аналогично $(a \cap b)\varphi \leqslant b\varphi$. Если же элемент $c' \in S'$ таков, что $c' \leqslant a\varphi$ и $c' \leqslant b\varphi$, и если c — тот элемент из S, для которого $c\varphi = c'$, то $c \leqslant a$ и $c \leqslant b$, т. е. $c \leqslant a \cap b$, откуда $c\varphi \leqslant (a \cap b)\varphi$. Этим доказано, что

$$(a \cap b)\varphi = a\varphi \cap b\varphi.$$

Так же проводится доказательство и для объединения.

Заметим, что на структуры можно перенести также понятие гомоморфизма и вообще все, что относится к произвольным примитивным классам универсальных алгебр; в частности, в соответствии с III.7.2, имеет смысл понятие свободной структуры с данным множеством X свободных образующих.

5. Как следует из I.2.1, бинарные отношения на множестве M составляют структуру, совпадающую со структурой всех подмножеств множества $M \times M$. Отношения эквивалентности на множестве M также составляют структуру, как доказано в I.3.3. Эта *структура отношений эквивалентности* не является, однако, подструктурой структуры бинарных отношений.

* Всякая структура изоморфно вкладывается в структуру отношений эквивалентности, определенных в некотором множестве [Уитмэн, Bull. Amer. Math. Soc. **52** (1946), 507—522].

Структура отношений эквивалентности, определенных в произвольно заданном множестве, изоморфно вкладывается в структуру подгрупп некоторой группы [Биркгоф, Proc. Cambr. Philos. Soc. **31** (1935), 433—454].

Таким образом, всякая структура изоморфно вкладывается в структуру подгрупп некоторой группы. *

6. Многие из структур, отмечавшихся выше — структура подмножеств множества M, структура подгрупп группы G, структура подколец кольца R (и, вообще, структура Ω-подгрупп Ω-группы G), структура отношений эквивалентности на множестве M, — обладают тем свойством, что пересечения и объединения определены в них не только для двух и поэтому, в силу ассоциативности, для любого конечного числа элементов, но и для любых бесконечных подмножеств. Иными словами, эти структуры являются полными структурами в смысле следующего определения:

Частично упорядоченное множество S называется *полной структурой*, если для любого непустого подмножества $A \subseteq S$ в S существуют элементы c и d со следующими свойствами:

I_1'. Для всех $a \in A$ выполняется неравенство $c \leqslant a$, причем если некоторый элемент c' также удовлетворяет условию $c' \leqslant a$ для всех $a \in A$, то $c' \leqslant c$.

I_2'. Для всех $a \in A$ выполняется неравенство $d \geqslant a$, причем если некоторый элемент d' также удовлетворяет условию $d' \geqslant a$ для всех $a \in A$, то $d' \geqslant d$.

Однозначно определенные элементы c и d называются соответственно *пересечением* и *объединением* элементов подмножества A. Записываться они будут следующим образом:

$$c = \bigcap_{a \in A} a, \qquad d = \bigcup_{a \in A} a$$

или, если элементы из A обозначены через a_α, где индекс α пробегает некоторое множество M,

$$c = \bigcap_{\alpha \in M} a_\alpha, \qquad d = \bigcup_{\alpha \in M} a_\alpha.$$

Ясно, что полная структура является и просто структурой.

7. Пересечение всех элементов полной структуры S называется *нулем* этой структуры и будет обозначаться символом 0. Этот элемент однозначно определяется любым из следующих трех условий: для всех $a \in S$

$$1)\ 0 \leqslant a; \quad 2)\ 0 \cap a = 0; \quad 3)\ 0 \cup a = a.$$

Объединение всех элементов полной структуры называется *единичным элементом* этой структуры и будет обозначаться символом 1. Этот элемент однозначно определяется любым из следующих трех условий: для всех $a \in S$

$$1')\ 1 \geqslant a; \quad 2')\ 1 \cup a = 1; \quad 3')\ 1 \cap a = a.$$

Нулем и единичным элементом (или одним из них) могут обладать, понятно, и структуры, не являющиеся полными.

Роль нуля и единичного элемента в структуре подгрупп группы G играют соответственно единичная подгруппа и сама группа G, в структуре подколец кольца R — нуль-подкольцо и само кольцо R, в структуре подмножеств множества M — пустое подмножество и само множество M. В структуре натуральных чисел, упорядоченных по делимости, а также в цепи натуральных чисел с их естественной упорядоченностью, нулем служит число 1, а единичный элемент отсутствует.

8. *Частично упорядоченное множество S тогда и только тогда будет полной структурой, если оно обладает единичным элементом и если в нем существует пересечение элементов для каждого непустого подмножества.*

В доказательстве нуждается лишь утверждение, что если в S существуют единичный элемент и все пересечения, то существуют и объединения. Пусть A — непустое подмножество из S. В S существуют такие элементы b, что $b \geqslant a$ для всех $a \in A$; таким элементом во всяком случае является 1. Пусть

B будет непустое множество всех этих элементов b, а d — их пересечение,

$$d = \bigcap_{b \in B} b.$$

Докажем, что d является объединением элементов подмножества A. В самом деле, если $a \in A$, то $a \leqslant b$ для всех $b \in B$, а поэтому $a \leqslant d$. С другой стороны, если элемент $s \in S$ таков, что $s \geqslant a$ для всех $a \in A$, то $s \in B$, а поэтому $d \leqslant s$. Таким образом,

$$d = \bigcup_{a \in A} a.$$

Так как свойство частично упорядоченного множества быть полной структурой (как и свойство быть структурой) сохраняется при инверсном изоморфизме (см. I.4.6), то в доказанной сейчас теореме можно было бы требовать существование нуля и объединений для всех непустых подмножеств.

* Назовем отображение φ частично упорядоченного множества M в частично упорядоченное множество N *монотонным*, если для $a, b \in M$ из $a \leqslant b$ всегда следует $a\varphi \leqslant b\varphi$. Структура S тогда и только тогда будет полной структурой, если для любого монотонного отображения φ структуры S в себя существуют неподвижные элементы, т. е. такие элементы a, что $a\varphi = a$ [Тарский, Pacif. J. Math. **5** (1955), 285—309; Дэйвис, Pacif. J. Math. **5** (1955), 311—319]. *

9. В I.4.5 было доказано, что всякое частично упорядоченное множество M изоморфно вкладывается в полную структуру $\tilde{M}$ всех своих подмножеств. Сейчас мы хотим доказать следующую теорему:

Всякая структура может быть изоморфно вложена (в смысле изоморфизма структур, см. IV.1.4) *в полную структуру.*

Эта теорема вытекает, впрочем, из следующего утверждения, усиливающего теорему I.4.5:

Всякое частично упорядоченное множество M изоморфно вкладывается в некоторую полную структуру S, причем так, что для всякого подмножества $A \subseteq M$, для

которого в M существуют пересечение или объединение, они сохраняются при этом вложении φ, т. е.

$$\left(\bigcap_{a\in A} a\right)\varphi = \bigcap_{a\in A} a\varphi, \quad \left(\bigcup_{a\in A} a\right)\varphi = \bigcup_{a\in A} a\varphi. \tag{2}$$

Ясно, что вложение M в $\tilde{M}$, построенное в I.4.5, не удовлетворяет поставленным требованиям. Мы поступим следующим образом. Будем считать, прежде всего, что множество M обладает нулем 0, так как иначе его можно было бы присоединить к M. Непустое подмножество $X \subseteq M$ назовем *идеалом* в M, если: 1) X вместе со всяким своим элементом x содержит и все такие элементы $y \in M$, что $y \leqslant x$; 2) для всякого $X' \subseteq X$, для которого в M существует объединение, это объединение содержится в X.

Множество S всех идеалов множества M частично упорядочено по теоретико-множественному включению. Так как S обладает единичным элементом — M будет, очевидно, идеалом в самом себе — и так как теоретико-множественное пересечение любого множества идеалов содержит нуль и удовлетворяет всем требованиям, входящим в определение идеала, то множество S будет, по IV.1.8, полной структурой.

Для любого элемента $a \in M$ множество (a) всех таких элементов $b \in M$, что $b \leqslant a$, будет идеалом; это *главный идеал*, порожденный элементом a. Ставя в соответствие всякому $a \in M$ порожденный им главный идеал (a), мы получим, как и в I.4.5, изоморфное вложение φ частично упорядоченного множества M в полную структуру S.

Предположим теперь, что для подмножества $A \subseteq M$ в M существует пересечение

$$c = \bigcap_{a\in A} a.$$

Тогда $c \leqslant a$ и поэтому $(c) \subseteq (a)$ для всех $a \in A$. Если же теоретико-множественное пересечение всех главных идеалов (a), $a \in A$, содержит элемент x, то $x \leqslant a$ для всех $a \in A$ и поэтому $x \leqslant c$. Таким образом,

$$(c) = \bigcap_{a\in A} (a),$$

что доказывает первое из равенств (2).

Наконец, пусть для подмножества $A \subseteq M$ в M существует объединение

$$d = \bigcup_{a \in A} a.$$

Тогда $(d) \supseteq (a)$ для всех $a \in A$. Если же некоторый идеал X содержит все $a \in A$, то, по определению идеала, он содержит и их объединение d, а поэтому $(d) \subseteq X$. Таким образом,

$$(d) = \bigcup_{a \in A} (a).$$

Этим доказано и второе из равенств (2), т. е. закончено доказательство теоремы.

Читатель без труда проверит, что конструкция, использованная в этом доказательстве, в применении к упорядоченному множеству рациональных чисел по существу дает обычное пополнение системы рациональных чисел дедекиндовыми сечениями.

10. *Частично упорядоченное множество S тогда и только тогда будет полной структурой, если S обладает нулем и если в S всякий идеал является главным.*

Действительно, если S — полная структура, то для любого идеала X существует объединение a всех его элементов, причем, в силу определения идеала, $a \in X$, а поэтому $X = (a)$. Обратно, пусть в частично упорядоченном множестве S существует нуль и всякий идеал является главным. Главным идеалом будет, в частности, и само S, а поэтому в S существует единичный элемент. Если же A — непустое подмножество из S, то совокупность X всех таких элементов $x \in S$, что $x \leqslant a$ для всех $a \in A$, содержит 0 и является идеалом. Этот идеал должен быть главным, $X = (b)$, и элемент b будет пересечением подмножества A. Ввиду IV.1.8 S оказалось полной структурой.

Таким образом, применение к полным структурам конструкции, изложенной в предшествующем пункте, не может дать ничего нового.

§ 2. Дедекиндовы структуры

1. Среди аксиом $II_1 - II_4$, определяющих структуру (см. IV.1.2), лишь аксиома II_4 связывает операции пересечения и объединения. Эта связь очень слаба. Некоторые структуры, например структура всех подмножеств некоторого множества,

дополнительно удовлетворяют условию дистрибутивности

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c) \tag{1}$$

(см. I.1.1). Структуры, удовлетворяющие этому условию для любых a, b и c, называются *дистрибутивными* и будут изучаться в § 6 настоящей главы. Однако структуры нормальных делителей групп и тем более структуры всех подгрупп, как правило, не являются дистрибутивными.

Желание выделить по возможности узкий класс структур, к которому принадлежали бы структуры нормальных делителей произвольных групп (хотя и не обязательно структуры всех подгрупп), приводит к следующему определению:

Структура S называется *дедекиндовой* (или *модулярной*), если для любых $a, b, c \in S$, удовлетворяющих условию $a \geqslant b$, выполняется равенство

$$a \cap (b \cup c) = b \cup (a \cap c). \tag{2}$$

Всякая дистрибутивная структура является дедекиндовой, так как из $a \geqslant b$ вытекает $a \cap b = b$ и поэтому при условии $a \geqslant b$ из (1) следует (2).

Всякая подструктура T дедекиндовой структуры S (см. IV.1.3) *сама дедекиндова*, так как равенство (2) должно выполняться, в частности, для элементов $a, b, c \in T$, удовлетворяющих условию $a \geqslant b$.

Свойство дедекиндовости сохраняется, само собою разумеется, при изоморфизме структур. С другой стороны, *структура, инверсно изоморфная дедекиндовой структуре, сама дедекиндова*, так как, меняя в определении дедекиндовой структуры символ $\geqslant$ на символ $\leqslant$ и переставляя символы $\cap$ и $\cup$, мы придем к тому же определению с переставленными лишь буквами a и b.

2. *Структура всех нормальных делителей произвольной группы является дедекиндовой.*

Действительно, пусть в группе G даны нормальные делители A, B и C, причем $A \supseteq B$. Нужно доказать, учитывая (1) из III.4.1, что

$$A \cap BC = B(A \cap C). \tag{3}$$

Так как $B \subseteq A$ и $B \subseteq BC$, то B содержится в левой части равенства (3). Там же содержится и $A \cap C$, так как

$C \subseteq BC$. Отсюда следует включение

$$A \cap BC \supseteq B(A \cap C). \tag{4}$$

С другой стороны, любой элемент, содержащийся в нормальном делителе $A \cap BC$, является элементом $a \in A$, допускающим в то же время запись

$$a = bc, \tag{5}$$

где $b \in B$, $c \in C$. Отсюда $c = b^{-1}a \in A$, так как $B \subseteq A$, т. е.

$$c \in (A \cap C).$$

Поэтому, ввиду (5), всякий элемент левой части равенства (3) содержится в его правой части, что вместе с включением (4) доказывает это равенство.

Идеалы произвольной Ω*-группы составляют, в силу сказанного в* III.2.4, *подструктуру структуры нормальных делителей аддитивной группы этой* Ω*-группы, т. е. составляют дедекиндову структуру.* Отсюда следует, что *структура всех идеалов произвольного кольца будет дедекиндовой.*

Отметим, что структура всех подгрупп некоммутативной группы, как правило, не является дедекиндовой.

3. Существует много различных определений дедекиндовой структуры, равносильных приведенному выше. Укажем некоторые из них.

Структура S *тогда и только тогда дедекиндова, если для любых* a, b, $c \in S$

$$a \cap [(a \cap b) \cup c] = (a \cap b) \cup (a \cap c). \tag{6}$$

Действительно, если структура S дедекиндова, то, так как $a \geqslant a \cap b$, (6) следует из (2). Обратно, если в структуре S выполняется условие (6), то для $a \geqslant b$ из (6) следует (2), так как в этом случае $a \cap b = b$.

Мы видим, таким образом, что *дедекиндовы структуры составляют примитивный класс универсальных алгебр.*

4. *Структура* S *тогда и только тогда дедекиндова, если из того, что элементы* a, b, $c \in S$ *удовлетворяют условиям*

$$a \leqslant b, \quad a \cap c = b \cap c, \quad a \cup c = b \cup c, \tag{7}$$

следует $a = b$.

Действительно, если структура S дедекиндова и элементы a, b, c удовлетворяют условиям (7), то

$$a = a \cup (a \cap c) = a \cup (b \cap c) = b \cap (a \cup c) = b \cap (b \cup c) = b.$$

Пусть теперь выполняются посылки обратного утверждения и пусть в S даны элементы a, b, c, причем $a \geqslant b$. Легко проверяется (см. вывод неравенства (4)), что, какова бы ни была структура S, из $a \geqslant b$ следует

$$a \cap (b \cup c) \geqslant b \cup (a \cap c). \tag{8}$$

Вместе с тем

$$[a \cap (b \cup c)] \cap c = a \cap [(b \cup c) \cap c] = a \cap c, \tag{9}$$

а так как при $a \geqslant b$

$$a \geqslant b \cup (a \cap c),$$

то

$$a \cap c \geqslant [b \cup (a \cap c)] \cap c \geqslant (a \cap c) \cap c = a \cap c,$$

т. е.

$$[b \cup (a \cap c)] \cap c = a \cap c. \tag{10}$$

Из (9) и (10) следует, что при $a \geqslant b$

$$[a \cap (b \cup c)] \cap c = [b \cup (a \cap c)] \cap c. \tag{11}$$

Переходя от равенства (11) к двойственному равенству, т. е. переставляя символы $\cap$ и $\cup$, а также меняя местами буквы a и b, мы получим

$$[a \cap (b \cup c)] \cup c = [b \cup (a \cap c)] \cup c, \tag{12}$$

причем неравенство $a \geqslant b$ сохраняется, так как символ $\geqslant$ мы также должны заменить на $\leqslant$. Мы видим, что (8), (11) и (12) имеют вид условий (7), а поэтому, в силу сделанных предположений, при $a \geqslant b$ имеет место равенство (2), что и требовалось доказать.

5. В теорию дедекиндовых структур можно было бы перенести известные нам из III.4.7 свойства инвариантных и главных рядов Ω-групп. Мы не будем этого делать в полном объеме и ограничимся результатами, необходимыми для дальнейшего.

Пусть дана дедекиндовая стуктура S, обладающая нулем и единичным элементом. Упорядоченная конечная система

элементов,

$$0 = a_0 < a_1 < a_2 < \ldots < a_{k-1} < a_k = 1, \tag{13}$$

называется *нормальным рядом* этой структуры [1]); число k— *длина* этого ряда. Нормальный ряд

$$0 = b_0 < b_1 < b_2 < \ldots < b_{l-1} < b_l = 1 \tag{14}$$

называется *уплотнением* ряда (13), если всякий элемент a_i, $i = 0, 1, \ldots, k$, равен одному из элементов b_j, $0 \leqslant j \leqslant l$.

6. *Всякие два нормальных ряда дедекиндовой структуры S обладают уплотнениями одинаковой длины.*

Пусть, в самом деле, в S заданы произвольные нормальные ряды (13) и (14). Положим, в некоторой мере повторяя то, что мы делали в III.4.5,

$$a_{ij} = a_i \cup (a_{i+1} \cap b_j), \quad i = 0, 1, \ldots, k-1, \quad j = 0, 1, \ldots, l;$$
$$b_{ji} = b_j \cup (b_{j+1} \cap a_i), \quad j = 0, 1, \ldots, l-1, \quad i = 0, 1, \ldots, k.$$

Так как

$$a_{i0} = a_i, \quad a_{il} = a_{i+1}$$

и

$$a_{ij} \leqslant a_{i,j+1}, \quad j = 0, 1, \ldots, l-1,$$

то элементы a_{ij} составляют нормальный ряд, быть может с повторениями, являющийся уплотнением ряда (13). Аналогично элементы b_{ji} составляют уплотнение ряда (14). Эти два новых ряда имеют одну и ту же длину kl, и поэтому остается показать, что они обладают равным числом повторений.

Действительно, пусть

$$a_{ij} = a_{i,j+1}. \tag{15}$$

Используя последовательно определение элемента $a_{i,j+1}$, равенство (15), неравенство $a_{ij} \leqslant a_{i+1}$, определение элемента a_{ij} и, наконец, определение (2) дедекиндовой структуры вместе с неравенством $a_{i+1} \cap b_j \leqslant b_{j+1}$, мы получим:

$$a_{i+1} \cap b_{j+1} = a_{i,j+1} \cap (a_{i+1} \cap b_{j+1}) = a_{ij} \cap (a_{i+1} \cap b_{j+1}) =$$
$$= a_{ij} \cap b_{j+1} = [a_i \cup (a_{i+1} \cap b_j)] \cap b_{j+1} = (a_i \cap b_{j+1}) \cup (a_{i+1} \cap b_j).$$

[1]) Такова принятая здесь терминология, хотя было бы последовательнее говорить об инвариантных рядах.

Этот результат вместе с определением элементов b_{ji} и $b_{j,\,i+1}$ и очевидным неравенством $a_{i+1} \cap b_j \leqslant b_j$ приводит к равенствам

$$b_{ji} = b_j \cup (b_{j+1} \cap a_i) = b_j \cup (b_{j+1} \cap a_i) \cup (a_{i+1} \cap b_j) =$$
$$= b_j \cup (a_{i+1} \cap b_{j+1}) = b_{j,\,i+1}.$$

Мы доказали, что повторения в построенных нами уплотнениях нормальных рядов (13) и (14) находятся во взаимно однозначном соответствии, т. е. могут быть одновременно удалены. Теорема доказана.

7. Будем называть *главным рядом* дедекиндовой структуры такой ее нормальный ряд, который не может быть уплотнен без повторений. Как и в III.4.6, из доказанной выше теоремы вытекают следующие результаты:

Если дедекиндова структура обладает главными рядами, то все ее главные ряды имеют одинаковую длину.

Если дедекиндова структура обладает главными рядами, то всякий ее нормальный ряд может быть уплотнен до главного ряда.

Отсюда следует, что *всякая подструктура T дедекиндовой структуры S, обладающей главными рядами, сама обладает главными рядами.* В самом деле, если главные ряды структуры S имеют длину k, то длины цепей подструктуры T не могут превосходить k. Если

$$c_0 < c_1 < \ldots < c_l \tag{16}$$

— одна из цепей максимальной длины, содержащихся в T, то c_0 и c_l будут соответственно нулем и единичным элементом структуры T, а (16) — одним из главных рядов этой структуры.

8. Полученные результаты позволяют указать еще одну форму определения дедекиндовой структуры:

Структура S тогда и только тогда дедекиндова, если во всякой ее подструктуре, обладающей главными рядами, все главные ряды имеют одинаковую длину.

Действительно, если структура S дедекиндова, то достаточно сослаться на IV.2.1 и IV.2.7. Если же структура S не дедекиндова, то из IV.2.4 следует существование в S таких элементов a, b, c, что выполняются условия (7), но $a \neq b$. Легко проверяется, что при этих условиях элементы a, b, c, $a \cap c$ и $a \cup c$ составляют подструктуру структуры S, причем

последние два элемента служат соответственно нулем и единичным элементом этой подструктуры. Построенная подструктура обладает, однако, двумя главными рядами различной длины, а именно рядами

$$a \cap c < a < b < a \cup c,$$

$$a \cap c < c < a \cup c.$$

9. *Дедекиндова структура S тогда и только тогда обладает главными рядами, если она удовлетворяет условиям обрыва убывающих и возрастающих цепей* (см. I.5.1 и I.5.5).

Действительно, если дедекиндова структура S обладает главными рядами длины k, то длины ее нормальных рядов не превосходят k. Однако всякая конечная цепь структуры S после добавления, если нужно, нуля и единичного элемента превращается в нормальный ряд этой структуры. Этим доказано, что в S не может быть бесконечных цепей.

Обратно, пусть в структуре S выполняются условия обрыва убывающих и возрастающих цепей, а поэтому и условия, им эквивалентные (см. I.5.1). Ввиду условия минимальности в S существуют минимальные элементы, а так как пересечение двух минимальных элементов должно совпадать с каждым из них, то в действительности в S существует лишь один такой элемент; он будет нулем нашей структуры. Аналогично в S существует и единичный элемент.

Если $a \in S$ и $a \neq 1$, то в непустом множестве таких элементов x, что $x > a$, существуют минимальные элементы, т. е., как говорят, элементы, *покрывающие* элемент a. Пользуясь аксиомой выбора, для каждого a, $a \neq 1$, отметим один из покрывающих его элементов; обозначим его через a'. Цепь

$$0 = a_0 < a_1 < a_2 < \ldots < a_n < \ldots, \tag{17}$$

где

$$a_n = a'_{n-1}, \qquad n = 1, 2, \ldots,$$

по условию должна обрываться. Существует, следовательно, такое n, что $a_n = 1$, т. е. цепь (17) будет главным рядом структуры S.

10. Если в произвольной структуре S взяты элементы a и b, причем $a \geqslant b$, то совокупность таких элементов x, что $a \geqslant x \geqslant b$, будет в S подструктурой, имеющей b своим нулем

и a — единичным элементом. Обозначим эту подструктуру через a/b.

Если в дедекиндовой структуре S взяты произвольные элементы a и b, то подструктуры $(a \cup b)/a$ и $b/(a \cap b)$ изоморфны.

Действительно, если $x \in b/(a \cap b)$, т. е.

$$a \cap b \leqslant x \leqslant b,$$

то положим

$$x\varphi = x \cup a.$$

Ясно, что $a \leqslant x\varphi \leqslant a \cup b$, т. е. $x\varphi \in (a \cup b)/a$.

Если бы существовал такой элемент y, $a \cap b \leqslant y \leqslant b$, отличный от x, что $y\varphi = x\varphi$, то элемент $z = x \cup y$ был бы заведомо отличен хотя бы от одного из элементов x, y, например от первого, т. е. $z > x$. Однако

$$a \cap b \leqslant z \leqslant b,$$

и поэтому, ввиду $a \cup a = a$,

$$z \cup a = x \cup y \cup a = (x \cup a) \cup (y \cup a) = x\varphi \cup y\varphi = x\varphi = x \cup a,$$
$$z \cap a = a \cap b = x \cap a,$$

что противоречит дедекиндовости структуры S ввиду IV.2.4.

С другой стороны, если $x' \in (a \cup b)/a$, т. е.

$$a \leqslant x' \leqslant a \cup b,$$

то, в силу дедекиндовости структуры,

$$x' = (a \cup b) \cap x' = a \cup (b \cap x'),$$

а так как

$$a \cap b \leqslant b \cap x' \leqslant b,$$

то

$$x' = (b \cap x')\varphi.$$

Отображение φ оказалось взаимно однозначным отображением подструктуры $b/(a \cap b)$ на всю подструктуру $(a \cup b)/a$. Докажем изоморфность этого отображения. Если x, $y \in b/(a \cap b)$, то из $x \leqslant y$ следует $x \cup a \leqslant y \cup a$, т. е. $x\varphi \leqslant y\varphi$. С другой стороны, если $x\varphi \leqslant y\varphi$, т. е. $x \cup a \leqslant y \cup a$, то

$$(x \cup y) \cup a = (x \cup a) \cup (y \cup a) = y \cup a.$$

т. е. $(x \cup y)\varphi = y\varphi$, откуда, ввиду взаимной однозначности

отображения φ, $x \cup y = y$, т. е. $x \leqslant y$. Теперь остается сослаться на последний результат из IV.1.4.

11. Пусть дедекиндова структура S обладает главными рядами. Тогда для любого $a \in S$ подструктура $a/0$ также обладает главными рядами; обозначим длину этих рядов $l(a)$.

Для любых элементов a и b дедекиндовой структуры S, обладающей главными рядами, имеет место равенство

$$l(a \cup b) = l(a) + l(b) - l(a \cap b). \tag{18}$$

В самом деле, выше доказано, что подструктуры $(a \cup b)/a$ и $b/(a \cap b)$ изоморфны. Их главные ряды имеют, следовательно, одну и ту же длину. Эта длина для первой подструктуры равна, однако, числу $l(a \cup b) - l(a)$, для второй — числу $l(b) - l(a \cap b)$.

§ 3. Прямые объединения. Теорема Шмидта — Орэ

1. В теории групп весьма употребительна одна конструкция, называемая прямым произведением групп или, в случае аддитивной записи групповой операции, их прямой суммой. В теории колец аналогичную роль играет двусторонняя прямая сумма колец. Изучение этих понятий приводит к совершенно параллельным теориям, которые в действительности являются частными проявлениями одной теории, относящейся к дедекиндовым структурам. Именно в этой общности мы и будем вести изложение, а в следующем параграфе дополним его замечаниями, относящимися специально к группам, кольцам или Ω-группам.

2. Пусть дана дедекиндова структура S, обладающая нулем. Элемент $a \in S$ называется *прямым объединением* элементов $b_1, b_2, \ldots, b_k \in S$ и будет записываться в виде

$$a = b_1 \times b_2 \times \ldots \times b_k, \tag{1}$$

если a является объединением этих элементов,

$$a = b_1 \cup b_2 \cup \ldots \cup b_k, \tag{2}$$

и если для $i = 1, 2, \ldots, k$

$$(b_1 \cup \ldots \cup b_{i-1} \cup b_{i+1} \cup \ldots \cup b_k) \cap b_i = 0. \tag{3}$$

Если структура S полная (см. IV.1.6), то можно определить и бесконечные прямые объединения: элемент a

будет *прямым объединением* элементов b_i, где i пробегает некоторое множество индексов I, если

$$a = \bigcup_{i \in I} b_i \tag{4}$$

и если для всех $i \in I$

$$b_i \cap \bar{b}_i = 0, \tag{5}$$

где

$$\bar{b}_i = \bigcup_{j \in I,\ j \neq i} b_j.$$

3. Приступим к изучению основных свойств прямых объединений в дедекиндовой структуре S с нулем. Мы ограничимся при этом случаем к о н е ч н ы х прямых объединений. Дедекиндовость структуры S, в самом определении IV.3.2 не игравшая никакой роли, во многих местах будет теперь существенно использована.

В определении IV.3.2 *условие* (3) *может быть заменено следующим условием, ему равносильным:*

$$(b_1 \cup \ldots \cup b_{i-1}) \cap b_i = 0, \quad i = 2, 3, \ldots, k. \tag{6}$$

Ясно, что (6) следует из (3). Для доказательства того, что из (6) следует (3), мы будем индукцией по l доказывать, что пересечение каждого из l элементов $b_1, b_2, \ldots, b_l$, $2 \leqslant l \leqslant k$, с объединением остальных $l-1$ элементов этой системы равно нулю. Действительно, для $l=2$ это утверждение следует из (6) при $i=2$. Пусть наше утверждение уже доказано для $l-1$. Из (6) следует равенство

$$(b_1 \cup \ldots \cup b_{l-1}) \cap b_l = 0. \tag{7}$$

Если же $j < l$, то применение неравенства

$$b_j \leqslant b_1 \cup \ldots \cup b_{l-1},$$

дедекиндовости структуры S, равенства (7) и индуктивного предположения дает

$$\begin{aligned}(b_1 \cup \ldots \cup b_{j-1} \cup b_{j+1} \cup \ldots \cup b_l) \cap b_j &= \\ = [(b_1 \cup \ldots \cup b_{j-1} \cup b_{j+1} \cup \ldots \cup b_{l-1}) \cup b_l] \cap (b_1 \cup \ldots \cup b_{l-1}) \cap b_j &= \\ = (b_1 \cup \ldots \cup b_{j-1} \cup b_{j+1} \cup \ldots \cup b_{l-1}) \cap b_j = 0.&\end{aligned}$$

Наше утверждение доказано, следовательно, для всех l, в том числе и для $l=k$, что и приводит к условию (3).

4. Пользуясь условием (6), читатель немедленно докажет следующие свойства прямого объединения:

Если $a = b_1 \times b_2 \times \ldots \times b_k$ *и* $b_1 \cup b_2 \cup \ldots \cup b_l = c$, $l < k$, *то* $a = c \times b_{l+1} \times \ldots \times b_k$.

Если $a = b_1 \times b_2 \times \ldots \times b_k$ *и* $b_1 = c_1 \times c_2 \times \ldots \times c_l$, *то* $a = c_1 \times c_2 \times \ldots \times c_l \times b_2 \times \ldots \times b_k$.

Учитывая, что в определении IV.3.2 нумерация элементов $b_1, b_2, \ldots, b_k$ не играет роли, мы придем, применяя несколько раз второе из указанных сейчас утверждений, к такому результату:

Если

$$a = b_1 \times b_2 \times \ldots \times b_k \tag{8}$$

и если элементы b_i, *все или некоторые, сами разложены в прямое объединение,*

$$b_i = c_{i1} \times c_{i2} \times \ldots \times c_{il_i}, \quad 1 \leqslant l_i, \quad i = 1, 2, \ldots, k,$$

то элемент a *будет прямым объединением всех элементов* c_{ij}, $1 \leqslant j \leqslant l_i$, $i = 1, 2, \ldots, k$. Это новое прямое разложение элемента a называется *продолжением* прямого разложения (8).

С другой стороны, из определения прямого объединения следует, что *если в прямом разложении* (8) *мы возьмем элементы* $b_1, b_2, \ldots, b_l$, $l < k$, *и положим* $b_1 \cup b_2 \cup \ldots \cup b_l = c$, *то*

$$c = b_1 \times b_2 \times \ldots \times b_l.$$

Отсюда и из первого из утверждений настоящего пункта вытекает следующий результат:

Если дано прямое разложение (8) *элемента* a *и если система элементов* $b_1, b_2, \ldots, b_k$ *разбита на непересекающиеся подсистемы, то, заменяя каждую из подсистем объединением входящих в нее элементов, мы получим новое прямое разложение элемента* a, *для которого разложение* (8) *служит продолжением.*

5. *Пусть дано прямое разложение* (8) *элемента* a. *Если выбраны элементы* b'_i, $0 \leqslant b'_i \leqslant b_i$, $i = 1, 2, \ldots, k$, *и если*

$$a' = b'_1 \cup b'_2 \cup \ldots \cup b'_k,$$

то

$$a' = b'_1 \times b'_2 \times \ldots \times b'_k. \tag{9}$$

Если $b'_i < b_i$ *хотя бы для одного* i, *то* $a' < a$.

В самом деле, для $i = 1, 2, \ldots, k$

$$(b'_1 \cup \ldots \cup b'_{i-1} \cup b'_{i+1} \cup \ldots \cup b'_k) \cap b'_i \leqslant$$
$$\leqslant (b_1 \cup \ldots \cup b_{i-1} \cup b_{i+1} \cup \ldots \cup b_k) \cap b_i = 0,$$

чем доказано утверждение (9). С другой стороны, если $a' = a$, то, используя дедекиндовость структуры S, получаем для $i = 1, 2, \ldots, k$:

$$b_i = b_i \cap a = b_i \cap a' = b_i \cap (b'_1 \cup b'_2 \cup \ldots \cup b'_k) =$$
$$= b'_i \cup [b_i \cap (b'_1 \cup \ldots \cup b'_{i-1} \cup b'_{i+1} \cup \ldots \cup b'_k)] = b'_i,$$

так как

$$b_i \cap (b'_1 \cup \ldots \cup b'_{i-1} \cup b'_{i+1} \cup \ldots \cup b'_k) \leqslant$$
$$\leqslant b_i \cap (b_1 \cup \ldots \cup b_{i-1} \cup b_{i+1} \cup \ldots \cup b_k) = 0.$$

6. *Если* $a = b \times c$ *и элемент* a' *удовлетворяет условиям* $b \leqslant a' \leqslant a$, *то*

$$a' = b \times (a' \cap c).$$

Действительно, ввиду условия дедекиндовости,

$$a' = a' \cap a = a' \cap (b \cup c) = b \cup (a' \cap c).$$

С другой стороны,

$$b \cap (a' \cap c) \leqslant b \cap c = 0.$$

7. Заметим, что если дедекиндова структура S обладает главными рядами и если $a = b \times c$, то, по (18) из IV.2.11,

$$l(a) = l(b) + l(c). \tag{10}$$

Вообще, если $a = b_1 \times b_2 \times \ldots \times b_k$, то

$$l(a) = l(b_1) + l(b_2) + \ldots + l(b_k). \tag{11}$$

8. В тех случаях, когда используется понятие прямого объединения, важную роль играет обычно вопрос об изоморфизме различных прямых разложений данной группы (или данного кольца). Этот вопрос явился предметом многочисленных исследований, преимущественно в рамках теории дедекиндовых структур. Мы ограничимся изложением одного частного, но важного результата, явившегося началом этих исследований.

Введем одно вспомогательное понятие. Пусть дана дедекиндова структура S, обладающая нулем 0 и единичным

элементом 1, и пусть дано прямое разложение

$$1 = a_1 \times a_2 \times \ldots \times a_k. \tag{12}$$

Положим, как обычно, что

$$\bar{a}_i = a_1 \cup \ldots \cup a_{i-1} \cup a_{i+1} \cup \ldots \cup a_k, \quad i = 1, 2, \ldots, k, \tag{13}$$

откуда, по IV.3.4,

$$1 = a_i \times \bar{a}_i, \qquad i = 1, 2, \ldots, k. \tag{14}$$

Если $b \in S$, то назовем *компонентой* этого элемента в сомножителе a_i прямого разложения (12) элемент

$$b^i = a_i \cap (b \cup \bar{a}_i). \tag{15}$$

9. *Элемент b содержится в объединении всех своих компонент относительно прямого разложения* (12),

$$b \leqslant b^1 \cup b^2 \cup \ldots \cup b^k.$$

Действительно, используя (15), а также несколько раз применяя определение дедекиндовой структуры, получаем:

$$\begin{aligned}
&b^1 \cup b^2 \cup \ldots \cup b^k = [a_1 \cap (b \cup \bar{a}_1)] \cup [a_2 \cap (b \cup \bar{a}_2)] \cup \ldots \\
&\ldots \cup [a_k \cap (b \cup \bar{a}_k)] = \{a_1 \cup [a_2 \cap (b \cup \bar{a}_2)] \cup \ldots \\
&\ldots \cup [a_k \cap (b \cup \bar{a}_k)]\} \cap (b \cup \bar{a}_1) = \\
&= \{a_1 \cup a_2 \cup [a_3 \cap (b \cup \bar{a}_3)] \cup \ldots \cup [a_k \cap (b \cup \bar{a}_k)]\} \cap (b \cup \bar{a}_1 \cap \\
&\cap (b \cup \bar{a}_2) = \ldots\ldots\ldots\ldots\ldots\ldots\ldots = \\
&= (a_1 \cup a_2 \cup \ldots \cup a_k) \cap (b \cup \bar{a}_1) \cap (b \cup \bar{a}_2) \cap \ldots \cap (b \cup \bar{a}_k) = \\
&= (b \cup \bar{a}_1) \cap (b \cup \bar{a}_2) \cap \ldots \cap (b \cup \bar{a}_k) \geqslant b.
\end{aligned}$$

Заметим, что в этом доказательстве мы использовали такие неравенства, как, например,

$$a_i \cap (b \cup \bar{a}_i) \leqslant a_i \leqslant b \cup \bar{a}_1, \qquad i \neq 1.$$

10. Назовем элементы a и b нашей структуры S *прямо подобными*, если в S существует такой элемент c, что

$$1 = a \times c = b \times c.$$

Два прямых разложения единичного элемента структуры S назовем *прямо подобными*, если они состоят из одинакового числа сомножителей и если между этими прямыми сомножителями

можно установить такое взаимно однозначное соответствие, что соответствующие сомножители прямо подобны в S.

Назовем, наконец, ненулевой элемент a структуры S *неразложимым*, если он не может быть разложен в прямое объединение двух элементов, отличных от нуля.

11. Если дано прямое разложение

$$1 = a_1 \times a_2 \times \ldots \times a_k$$

единичного элемента структуры S, то, полагая

$$c_l = a_1 \times a_2 \times \ldots \times a_l, \quad l \leqslant k,$$

мы получим в S нормальный ряд длины k:

$$0 = c_0 < c_1 < c_2 < \ldots < c_k = 1.$$

Отсюда следует, ввиду IV.2.7, что *если дедекиндова структура S обладает главными рядами и если длина этих рядов равна n, то всякое прямое разложение единичного элемента состоит не более чем из n сомножителей и, следовательно, может быть продолжено* (см. IV.3.4) *до прямого разложения с неразложимыми сомножителями.*

12. Нашей целью является доказательство следующей теоремы [О. Ю. Шмидт, Math. Zeitschr. **29** (1928), 34—41; Оре, Ann. of Math. **37** (1936), 265—292]:

В дедекиндовой структуре S, обладающей главными рядами, любые два разложения единичного элемента в прямое объединение неразложимых элементов прямо подобны (см. IV.3.10).

Эта теорема вытекает, впрочем, из следующей теоремы:

Если в дедекиндовой структуре S, обладающей главными рядами, даны два любых разложения единичного элемента в прямое объединение неразложимых элементов,

$$1 = a_1 \times a_2 \times \ldots \times a_k, \tag{16}$$

$$1 = b_1 \times b_2 \times \ldots \times b_l, \tag{17}$$

то всякий сомножитель любого из этих разложений может быть замещен некоторым сомножителем из другого разложения.

При этом под возможностью *замещения* элемента a_1 в разложении (16) некоторым сомножителем b_j из разложения (17) следует понимать существование прямого разложения

$$1 = b_j \times a_2 \times \ldots \times a_k,$$

т. е., в силу (14),

$$1 = b_j \times \bar{a}_1. \tag{18}$$

Первая из указанных теорем действительно вытекает из второй. В самом деле, *если элемент* b_j *из* (17) *замещает элемент* a_1 *в* (16), *то*, как показывают равенства (14) (для $i = 1$) и (18), *элементы* a_1 *и* b_j *прямо подобны в* S. Пусть уже построено прямое разложение

$$1 = b_{j_1} \times \ldots \times b_{j_m} \times a_{m+1} \times \ldots \times a_k, \tag{19}$$

где $1 \leqslant m < k$, причем $b_{j_1}, \ldots, b_{j_m}$ являются различными сомножителями из разложения (17) и элементы a_i и b_{j_i}, $i = 1, 2, \ldots, m$, прямо подобны в S. Применим вторую теорему к прямым разложениям (19) и (17). Элемент a_{m+1} должен замещаться в (19) некоторым сомножителем $b_{j_{m+1}}$ из (17), а поэтому a_{m+1} и $b_{j_{m+1}}$ прямо подобны. При этом индекс j_{m+1} отличен от всех индексов $j_1, \ldots, j_m$, так как из

$$1 = b_{j_1} \times \ldots \times b_{j_m} \times b_{j_{m+1}} \times a_{m+2} \times \ldots \times a_k$$

следует

$$b_{j_i} \cap b_{j_{m+1}} = 0, \qquad i = 1, 2, \ldots, m.$$

Продолжая так далее, мы придем к прямому разложению

$$1 = b_{j_1} \times b_{j_2} \times \ldots \times b_{j_k},$$

откуда $k \leqslant l$. Сопоставляя с прямым разложением (17), мы получаем, что на самом деле $k = l$ и что прямые разложения (16) и (17) прямо подобны.

13. Доказательство второй теоремы мы будем вести индукцией по длине главных рядов рассматриваемых структур, так как главный ряд длины 1 имеет лишь структура, состоящая из двух элементов, нуля и единицы, а для этой структуры доказываемая теорема, очевидно, справедлива.

Пусть нужно заместить элемент a_1 из прямого разложения (16). Обозначим через a_1^i компоненту (см. IV.3.8) элемента a_1 в прямом сомножителе b_i разложения (17). Предположим

сперва, что хотя бы при одном i элемент a_1^i отличен от b_1. Тогда, полагая

$$g = a_1^1 \cup a_1^2 \cup \ldots \cup a_1^l,$$

в силу IV.3.5, получаем

$$g = a_1^1 \times a_1^2 \times \ldots \times a_1^l, \tag{20}$$

причем $g < 1$. Так как, по IV.3.9, $a_1 \leqslant g$, то, по IV.3.6,

$$g = a_1 \times d, \tag{21}$$

где

$$d = g \cap (a_2 \times \ldots \times a_k). \tag{22}$$

По индуктивному предположению для структуры $g/0$ теорема уже доказана. Поэтому, продолжая разложения (21) и (20) до прямых разложений с неразложимыми сомножителями — обозначим эти разложения через (21′) и (20′), — можно будет заместить неразложимый элемент a_1 в (21′) некоторым неразложимым сомножителем c_1 из (20′), т. е.

$$g = c_1 \times d. \tag{23}$$

Для определенности пусть $c_1 \leqslant a_1^1$.

Из (23), (22) и неравенства $c_1 \leqslant g$ следует

$$0 = c_1 \cap d = c_1 \cap g \cap (a_2 \times \ldots \times a_k) = c_1 \cap (a_2 \times \ldots \times a_k),$$

т. е. объединение

$$h = c_1 \cup (a_2 \times \ldots \times a_k)$$

будет прямым,

$$h = c_1 \times a_2 \times \ldots \times a_k.$$

Из прямого подобия элементов a_1 и c_1 в g следует, ввиду (10) из IV.3.7, что $l(a_1) = l(c_1)$, а поэтому, по (11) из IV.3.7, $l(h) = l(1)$, откуда $h = 1$.

Таким образом,

$$1 = c_1 \times a_2 \times \ldots \times a_k.$$

Однако $c_1 \leqslant a_1^1 \leqslant b_1$, а так как элемент b_1 неразложимый, то, в силу IV.3.6,

$$c_1 = a_1^1 = b_1 \tag{24}$$

и поэтому

$$1 = b_1 \times a_2 \times \ldots \times a_k.$$

Мы получаем, что элемент a_1 замещается в прямом разложении (16) элементом b_1; элементы a_1 и b_1 будут, следова-

тельно, прямо подобными. Заметим, кроме того, что, по (24), компонента элемента a_1 в сомножителе b_1 прямого разложения (17) совпадает с b_1.

Покажем, что в рассматриваемом случае элемент b_1 в свою очередь замещается в прямом разложении (17) элементом a_1. Действительно, так как, по (24), $a_1^1 = b_1$, т. е., по (15),

$$b_1 \cap (a_1 \cup \bar{b}_1) = b_1,$$

то

$$b_1 \leqslant a_1 \cup \bar{b}_1,$$

а поэтому

$$a_1 \cup \bar{b}_1 = 1.$$

С другой стороны, из прямого подобия элементов a_1 и b_1 следует $l(a_1) = l(b_1)$, а поэтому, в силу (18) из IV.2.11 и (10) из IV.3.7,

$$l(1) = l(b_1) + l(\bar{b}_1) = l(a_1) + l(\bar{b}_1),$$

откуда

$$a_1 \cap \bar{b}_1 = 0.$$

Этим доказано существование прямого разложения

$$1 = a_1 \times \bar{b}_1 = a_1 \times b_2 \times \ldots \times b_l.$$

14. Предположим теперь, что компоненты элемента a_1 во всех сомножителях b_i разложения (17) совпадают с самими b_i и в то же время компонента в сомножителе a_1 разложения (16) хотя бы для одного b_i, например для b_1, совпадает с a_1. В этом случае, как мы знаем из рассмотрений предшествующего абзаца,

$$a_1 \cup \bar{b}_1 = 1, \qquad b_1 \cup \bar{a}_1 = 1. \tag{25}$$

Из (16), (17) и (25) следует, ввиду (18) из IV.2.11 и (10) из IV.3.7, что

$$l(1) = l(a_1) + l(\bar{a}_1) = l(b_1) + l(\bar{b}_1),$$

$$l(1) \leqslant l(a_1) + l(\bar{b}_1), \qquad l(1) \leqslant l(b_1) + l(\bar{a}_1).$$

Сопоставляя эти равенства и неравенства, получаем

$$l(a_1) = l(b_1), \quad l(\bar{a}_1) = l(\bar{b}_1)$$

и, следовательно,

$$a_1 \cap \bar{b}_1 = b_1 \cap \bar{a}_1 = 0,$$

т. е.

$$1 = a_1 \times b_2 \times \ \dots \ \times b_l = b_1 \times a_2 \times \ \dots \ \times a_k.$$

15. Остается рассмотреть тот случай, когда компоненты элемента a_1 во всех сомножителях b_i разложения (17) совпадают с самими b_i, но компоненты всех b_i, $i = 1, 2, \dots, l$, в сомножителе a_1 разложения (16) отличны от a_1. В этом случае все прямые сомножители разложения (17) находятся в тех же условиях, в каких находился элемент a_1 в рассмотренном выше первом случае. Сомножители b_i, $i = 1, 2, \dots, l$, можно, таким образом, последовательно замещать в разложении (17) сомножителями из разложения (16). Как мы знаем из IV.3.12, при этом последовательном замещении найдется такое b_i, которое замещается элементом a_1. Но тогда, как показано в IV. 3.13, компонента элемента b_i в прямом сомножителе a_1 разложения (16) должна совпадать с a_1 против предположения.

Это противоречие показывает, что рассматриваемый последний случай вообще невозможен. Теорема доказана.

§ 4. Прямые разложения Ω-групп

1. Как мы знаем, структура нормальных делителей произвольной группы, структура идеалов произвольного кольца и, вообще, структура идеалов произвольной Ω-группы являются и дедекиндовыми, и полными. Применяя определения IV.3.2 к этим структурам, причем к тому случаю, когда в качестве a берется сама группа, само кольцо или, вообще, сама Ω-группа (т. е. единичные элементы указанных структур), мы получим определение разложения группы в *прямое произведение ее нормальных делителей* и разложения кольца или Ω-группы в *прямую сумму их идеалов*.

2. Эти теоретико-структурные определения могут быть переформулированы на языке операций, заданных в группе, кольце или Ω-группе. Сделаем это сразу для Ω-группы.

Пусть в Ω-группе G заданы Ω-подгруппы B_i, $i \in I$. Обозначим через $\bar{B}_i$ Ω-подгруппу, порожденную в G всеми B_j, где $j \in I$, $j \neq i$. Ω-группа G есть *прямая сумма своих Ω-подгрупп* B_i, $i \in I$, если выполняются следующие условия α) и β):

α) Взаимный коммутант (см. III. 5.1) Ω-подгрупп B_i и $\bar{B}_i$ равен нулю для всех $i \in I$,

$$[B_i, \bar{B}_i] = O, \quad i \in I. \tag{1}$$

Отметим сразу же, что из условия α) следует равенство

$$[B_i, B_j] = O \text{ при } i \neq j. \tag{2}$$

Поэтому равны нулю, в частности, все коммутаторы $[b_i, b_j]$, где $b_i \in B_i$, $b_j \in B_j$, т. е. при $i \neq j$ любые элементы, взятые по одному из подгрупп B_i и B_j, между собою перестановочны.

β) Всякий ненулевой элемент $a \in G$ однозначно (с точностью до порядка слагаемых) записывается в виде суммы конечного числа ненулевых элементов, взятых по одному в некоторых из Ω-подгрупп B_i, т. е.

$$a = b_1 + b_2 + \ldots + b_k, \tag{3}$$

где $b_l \in B_{i_l}$, $l = 1, 2, \ldots, k$, и $i_l \neq i_m$ при $l \neq m$.

3. Докажем *равносильность этих двух определений.* Пусть Ω-группа G является прямым объединением своих идеалов B_i, $i \in I$, в смысле IV.3.2. Тогда, по III.2.4, $\bar{B}_i$, $i \in I$, также будет идеалом. Поэтому, по III.5.3,

$$[B_i, \bar{B}_i] \subseteq [B_i, G] \subseteq B_i,$$
$$[B_i, \bar{B}_i] \subseteq [G, \bar{B}_i] \subseteq \bar{B}_i,$$

а так как $B_i \cap \bar{B}_i = O$ по (5) из IV.3.2, то условие α) доказано.

С другой стороны, равенство (4) из IV.3.2 (где в качестве a берется само G) и последняя теорема из III.2.4 показывают, ввиду вытекающей из α) перестановочности элементов, взятых в различных подгруппах B_i, что для любого элемента $a \in G$ существует запись вида (3). Пусть этих записей две, а именно (3) и

$$a = b'_1 + b'_2 + \ldots + b'_k;$$

без ограничения общности — достаточно добавить к обеим записям, если нужно, несколько слагаемых, равных нулю, — можно считать, что в них одно и то же число слагаемых и что b'_l, $l = 1, 2, \ldots, k$, содержится в той же Ω-подгруппе B_{i_l},

что и b_l. Если при этом, например, $b_1 \neq b_1'$, т. е. $-b_1' + b_1 \neq 0$, то

$$-b_1' + b_1 = b_2' + \ldots + b_k' - (b_2 + \ldots + b_k) \in B_{i_1} \cap \bar{B}_{i_1},$$

что противоречит равенству (5) из IV.3.2.

Пусть теперь Ω-группа G является прямой суммой своих Ω-подгрупп B_i, $i \in I$, в смысле определения IV.4.2. Докажем, что всякая Ω-подгруппа B_i является в G идеалом.

Если $x \in B_i$ и $a \in G$, то для a существует запись вида (3), а так как элементы из различных B_j, $j \in I$, между собою перестановочны, то

$$-a + x + a = -b_i + x + b_i \in B_i;$$

этим доказано, что B_i является нормальным делителем аддитивной группы.

С другой стороны, из равенства (1) следует, ввиду (2) из III.5.1, что для любой n-арной операции $\omega \in \Omega$ и любых элементов $b_1, b_2, \ldots, b_n \in B_i$ и $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_n \in \bar{B}_i$

$$(b_1 + \bar{b}_1)(b_2 + \bar{b}_2) \ldots (b_n + \bar{b}_n)\omega = b_1 b_2 \ldots b_n\omega + \bar{b}_1 \bar{b}_2 \ldots \bar{b}_n\omega. \tag{4}$$

Пусть теперь заданы n-арная операция $\omega \in \Omega$, элементы $a_1, a_2, \ldots, a_n \in G$, элемент $b \in B_i$ и число k, $1 \leqslant k \leqslant n$. Ввиду β) существует запись

$$a_j = b_j + \bar{b}_j, \quad b_j \in B_i, \quad \bar{b}_j \in \bar{B}_i, \quad j = 1, 2, \ldots, n. \tag{5}$$

Используя (4), (5) и перестановочность элементов из подгрупп B_i и $\bar{B}_i$, получаем

$$\begin{aligned}
&-a_1 \ldots a_n\omega + a_1 \ldots a_{k-1}(b + a_k) a_{k+1} \ldots a_n\omega = \\
&= -(b_1 + \bar{b}_1) \ldots (b_n + \bar{b}_n)\omega + (b_1 + \bar{b}_1) \ldots \\
&\ldots (b_{k-1} - \bar{b}_{k-1})(b + b_k + \bar{b}_k)(b_{k+1} + \bar{b}_{k+1}) \ldots \\
&\ldots (b_n + \bar{b}_n)\omega = -\bar{b}_1 \ldots \bar{b}_n\omega - b_1 \ldots b_n\omega + \\
&+ b_1 \ldots b_{k-1}(b + b_k) b_{k+1} \ldots b_n\omega + \bar{b}_1 \ldots \bar{b}_n\omega \in B_i.
\end{aligned}$$

Этим доказано, что все B_i, $i \in I$, являются идеалами в G. Из условия β) следует, далее, что идеалы B_i порождают вместе всю Ω-группу G. Наконец, если бы пересечение $B_i \cap \bar{B}_i$ содержало ненулевой элемент a, то для него мы

имели бы две различных записи вида (3) в противоречие с β): в одной из них из подгруппы B_i берется элемент a, а из других подгрупп — нули, в другой же элемент a представляется в виде суммы элементов, взятых по одному в нескольких подгруппах B_j, где $j \neq i$. Теорема доказана.

4. *Для групп условие* α) *из определения* IV.4.2 *может быть заменено условием*:

α′) любые элементы, взятые по одному из любых двух подгрупп B_i и B_j, при $i \neq j$ перестановочны между собой.

Для колец условие α) *может быть заменено условием*:

α″) произведение любых элементов, взятых по одному из любых двух подколец B_i и B_j, при $i \neq j$ равно нулю.

Из сказнного в III.5.1 и включения

$$[B_i, B_j] \subseteq [B_i, \overline{B}_i], \qquad i \neq j,$$

вытекает, что из α) следуют соответственно α′) и α″). С другой стороны, в случае групп из α′) следует перестановочность элементов из B_i и $\overline{B}_i$, т. е., снова по III.5.1, следует α). В случае же колец из β) следует, что всякий элемент из $\overline{B}_i$ обладает записью вида (3) со слагаемыми, взятыми в некоторых из подгрупп B_j, $j \neq i$. Поэтому, в силу законов дистрибутивности, из α″) вытекает, что если $x \in B_i$, $y \in \overline{B}_i$, то

$$xy = yx = 0,$$

а это, по III.5.1, влечет за собою α).

5. Пусть нормальные делители A и B группы G прямо подобны в смысле IV.3.10, т. е. существует такой нормальный делитель C, что имеют место прямые разложения

$$G = A \times C = B \times C. \tag{6}$$

Тогда A и B изоморфны фактор-группе G/C, т. е. изоморфны между собой. При этом изоморфизме сопоставляются такие элементы $a \in A$ и $b \in B$, что

$$a = bc, \quad c \in C,$$

причем *элемент c принадлежит к центру группы G* (см. III.3.2), а поэтому указанный изоморфизм между A и B называется *центральным*.

В самом деле, в силу второго из разложений (6) элемент c перестановочен с каждым элементом из B. С другой стороны, для любого $c' \in C$ из первого из разложений (6) следует равенство

$$ac' = c'a,$$

т. е.

$$(bc)\,c' = c'\,(bc),$$

откуда, ввиду сказанного выше, следует

$$cc' = c'c.$$

Элемент c перестановочен, следовательно, с элементами как из B, так и из C, а поэтому и со всеми элементами группы G.

Аналогично, если даны прямо подобные идеалы A и B кольца R, т. е. имеют место разложения в прямую сумму

$$R = A + C = B + C, \tag{7}$$

то A *и* B *изоморфны фактор-кольцу* R/C, *а поэтому изоморфны между собой.* При этом изоморфизме соответствуют друг другу такие элементы $a \in A$ и $b \in B$, что

$$a = b + c, \quad c \in C, \tag{8}$$

причем *элемент* c *принадлежит к аннулятору кольца* R, а поэтому указанный изоморфизм между A и B можно назвать *аннуляторным.* Отметим, что *аннулятором* кольца R называется совокупность таких элементов $a \in R$, что

$$ax = xa = 0$$

для всех $x \in R$.

Докажем, что элемент c из (8) обладает этим свойством. Из второго из разложений (7) следует, что для всех $b' \in B$, $c' \in C$

$$b'c' = c'b' = 0, \tag{9}$$

в частности

$$b'c = cb' = 0. \tag{10}$$

С другой стороны, из первого из разложений (7) следует, что для любого $c' \in C$

$$ac' = c'a = 0,$$

т. е., по (8),

$$(b + c)\,c' = c'\,(b + c) = 0,$$

откуда, в силу (9),

$$cc' = c'c = 0. \tag{11}$$

Из (10) и (11) следует, ввиду второго из разложений (7), принадлежность c к аннулятору кольца R.

Из доказанного следует, что прямо подобные прямые разложения в группах и кольцах (см. IV. 3.10) будут соответственно *центрально изоморфными* и *аннуляторно изоморфными*. Обратное, понятно, не утверждается.

6. Из теоремы Шмидта — Орэ (см. IV.3.12) вытекают теперь следующие теоремы:

Если группа G обладает главными рядами, то любые ее два прямых разложения с неразложимыми сомножителями центрально изоморфны.

Если кольцо R обладает главными рядами, то любые его два прямых разложения с неразложимыми слагаемыми аннуляторно изоморфны.

* Если все гомоморфные образы группы (кольца) G, лежащие в ее центре (в его аннуляторе), удовлетворяют условию минимальности для подгрупп (подколец), то любые два прямых разложения G, причем число прямых сомножителей (слагаемых) может быть и бесконечным, обладают центрально (аннуляторно) изоморфными продолжениями. Условия этой теоремы выполняются, в частности, в том случае, когда центр (аннулятор) G или фактор-группа G по коммутанту (фактор-кольцо по квадрату) удовлетворяют условию минимальности [А. Г. Курош, Изв. АН СССР, сер. матем. **10** (1946), 47—72]. *

§ 5. Полные прямые суммы универсальных алгебр

1. Пусть дано семейство универсальных алгебр G_i с одной и той же системой операций Ω и относящихся к одному и тому же примитивному классу Λ (см. III.6.3); индекс i пробегает некоторое множество I, конечное или бесконечное. Рассмотрим множество G, элементами которого являются всевозможные системы $a = (a_i)$ элементов, взятых по одному в каждой из алгебр G_i, т. е. $a_i \in G_i$, $i \in I$. Элемент a_i будет называться i-й *компонентой* (или компонентой в алгебре G_i) элемента a.

Множество G можно превратить в универсальную алгебру с системой операций Ω, полагая, что операции из Ω

выполняются в G покомпонентно: если даны n-арная операция $\omega \in \Omega$ и n элементов из G,

$$a^{(k)} = (a_i^{(k)}), \quad k = 1, 2, \ldots, n,$$

то

$$a'a'' \ldots a^{(n)}\omega = (a_i' a_i'' \ldots a_i^{(n)}\omega).$$

Это определение операций показывает, что в алгебре G будут выполняться все тождественные соотношения из Λ.

Алгебра G называется *полной прямой суммой* алгебр G_i, $i \in I$, и будет записываться в виде

$$G = \widetilde{\sum_{i \in I}} G_i. \tag{1}$$

Можно говорить, в частности, о группе, являющейся полной прямой суммой (или полным прямым произведением) данного семейства групп, и т. д.

2. Подалгебра A алгебры G, представленной в виде (1) называется *подпрямой суммой* алгебр G_i, $i \in I$, если для всякого $i \in I$ i-е компоненты всех элементов из A исчерпывают всю алгебру G_i. Ясно, что к числу таких подалгебр принадлежит сама алгебра G, но в G существуют, вообще говоря, и истинные подалгебры с этим свойством.

Если алгебра A является подпрямой суммой алгебр G_i, $i \in I$, то для всякого $i \in I$ мы получим гомоморфное отображение φ_i алгебры A на алгебру G_i, сопоставляя всякому элементу

$$a = (a_i) \in A$$

его i-ю компоненту a_i. Как мы знаем из III.1.8, гомоморфизм φ_i определяет на алгебре A конгруенцию π_i, причем алгебры G_i и A/π_i изоморфны.

Пересечение конгруенций π_i, $i \in I$ (см. I.3.3), *является нулевой конгруенцией, т. е. разбиением алгебры A на отдельные элементы.*

Действительно, если в A даны два различных элемента, то хотя бы при одном i они имеют различные i-е компоненты, а поэтому принадлежат к различным классам конгруенции π_i.

3. Справедлива обратная теорема:

Если в универсальной алгебре A задана система конгруенций π_i, $i \in I$, с нулевым пересечением, то алгебра A

изоморфна подпрямой сумме фактор-алгебр A/π_i, $i \in I$.

Для доказательства обозначим через G полную прямую сумму алгебр A/π_i, $i \in I$,

$$G = \sum_{i \in I}^{\sim} A/\pi_i.$$

Отобразим алгебру A в алгебру G, сопоставляя каждому элементу $a \in A$ тот элемент из G, i-я компонента которого для всякого $i \in I$ является классом конгруенции π_i, содержащим элемент a. Это отображение будет гомоморфизмом, так как в алгебре G операции производятся покомпонентно, а в алгебре A/π_i, $i \in I$, применение операций к классам конгруенции π_i определяется через применение операций к элементам из A, выбранным по одному в этих классах.

Полученный гомоморфизм будет даже изоморфизмом, так как из условия, что пересечение конгруенций π_i должно быть нулевым, следует, что для любых двух различных элементов из A найдется хотя бы одно такое $i \in I$, что эти элементы лежат в разных классах конгруенции π_i, а поэтому их образы в G имеют разные i-е компоненты. Наконец, та подалгебра алгебры G, на которую алгебра A изоморфно отображается, будет подпрямой суммой алгебр A/π_i, $i \in I$, так как для всех $i \in I$ любой класс конгруенции π_i, т. е. любой элемент алгебры A/π_i, служит i-й компонентой образов в G всех своих элементов.

В случае Ω-групп конгруенции задаются идеалами, как мы знаем из III. 2.5, причем легко видеть, что пересечение конгруенций определяется пересечением соответствующих идеалов. Таким образом, *представления любой* Ω*-группы* (*в частности, группы, кольца*) *в виде подпрямой суммы взаимно однозначно соответствуют системам ее идеалов* (*нормальных делителей*) *с нулевым пересечением.*

4. Универсальная алгебра A называется *подпрямо неразложимой,* если в ней любая система ненулевых конгруенций обладает ненулевым пересечением. Из сказанного в IV. 5.2 и IV. 5.3 следует, что это будет тогда и только тогда, если при любом представлении алгебры A в виде подпрямой суммы некоторых алгебр G_i, $i \in I$, хотя бы для одного i гомоморфизм φ_i, отображающий всякий элемент из A в его i-ю компоненту, будет изоморфизмом между A и G_i.

Имеет место следующая теорема [Биркгоф, Bull. Amer. Math. Soc. **50** (1944), 764—768]:

Всякая универсальная алгебра A разлагается в подпрямую сумму подпрямо неразложимых алгебр, принадлежащих к тому же примитивному классу, что и алгебра A.

Для доказательства рассмотрим любую пару различных элементов $x, y \in A$ и обозначим через $M(x, y)$ множество всех конгруенций на алгебре A, *разделяющих* эти элементы, т. е. таких, что x и y для каждой из этих конгруенций принадлежат к различным классам. Множество $M(x, y)$ не является пустым, так как в нем содержится нулевая конгруенция (см. IV. 5.2). Покажем, что это множество, частично упорядоченное в соответствии с I. 2.1, обладает максимальными элементами.

Для этого, в силу теоремы Куратовского — Цорна (см. I. 6.3), достаточно показать, что всякая цепь множества $M(x, y)$ обладает верхней гранью. Пусть конгруенции $\pi_i \in M(x, y)$, где i пробегает упорядоченное множество I, составляют цепь, т. е. $\pi_i < \pi_j$ при $i < j$. Тогда бинарное отношение π^*, определяемое условием, что $b\pi^* c$ тогда и только тогда, если существует такое $i \in I$, что $b\pi_i c$, будет, очевидно, отношением эквивалентности. Оно будет и конгруенцией: если в A взяты элементы $b_1, b_2, \ldots, b_n$ и $c_1, c_2, \ldots, c_n$, причем $b_j \pi^* c_j$, $j = 1, 2, \ldots, n$, то существуют такие $i_1, i_2, \ldots, i_n \in I$, что $b_j \pi_{i_j} c_j$, $j = 1, 2, \ldots, n$. Если i_0 — наибольший из индексов $i_1, i_2, \ldots, i_n$, то $b_j \pi_{i_0} c_j$, $j = 1, 2, \ldots, n$. Пусть ω — любая n-арная операция, заданная в алгебре A. Так как π_{i_0} является конгруенцией, то

$$(b_1 b_2 \ldots b_n \omega)\, \pi_{i_0}\, (c_1 c_2 \ldots c_n \omega),$$

а поэтому и

$$(b_1 b_2 \ldots b_n \omega)\, \pi^*\, (c_1 c_2 \ldots c_n \omega),$$

т. е. π^* действительно является конгруенцией. Эта конгруенция разделяет элементы x и y, так как они разделялись каждой из конгруенций π_i, $i \in I$, и служит, очевидно, верхней гранью для заданной цепи конгруенций.

Фиксируем теперь для каждой пары различных элементов $x, y \in A$ одну из максимальных конгруенций, их разделяющих; обозначим ее через $\pi(x, y)$. Пересечение всех этих конгруенций является нулевым, так как любая пара

различных элементов из A разделяется хотя бы одной из этих конгруенций. Поэтому, по теореме IV. 5.3, алгебра A является подпрямой суммой всех фактор-алгебр $A/\pi(x, y)$.

Остается показать, что каждая фактор-алгебра $A/\pi(x, y)$ подпрямо неразложима. Для этого заметим, что между всеми конгруенциями этой фактор-алгебры и всеми теми конгруенциями алгебры A, которые содержат конгруенцию $\pi(x, y)$, существует естественное взаимно однозначное соответствие, сохраняющее отношение включения. Однако пересечение всех конгруенций алгебры A, строго больших чем $\pi(x, y)$, само строго больше этой конгруенции, так как все указанные конгруенции не разделяют элементов x и y, в то время как $\pi(x, y)$ их разделяет. Отсюда следует, что пересечение всех ненулевых конгруенций алгебры $A/\pi(x, y)$ само будет ненулевым. Теорема доказана.

5. Рассмотрим теперь полную прямую сумму Ω-групп G_i, $i \in I$,

$$G = \widetilde{\sum_{i \in I}} G_i.$$

Из сказанного в IV. 5.1 следует, что G само будет Ω-группой того же примитивного класса, к которому принадлежат все G_i, $i \in I$. Ее нулем будет служить элемент, всякая компонента которого равна нулю соответствующей Ω-группы G_i.

Подмножество G' Ω-группы G, состоящее из всех тех элементов $a = (a_i)$, у которых лишь конечное число компонент a_i, $i \in I$, отлично от нуля, будет в G Ω-подгруппой, так как покомпонентное применение к элементам из G' сложения или вычитания, а также операций из Ω не выводит за пределы G'.

Ω-группа G' называется *прямой суммой* Ω-групп G_i, $i \in I$. Основанием для этого служит следующая теорема:

Ω-группа G' является прямой суммой (в смысле определений IV. 3.2 *и* IV. 4.2) *своих идеалов G'_i, $i \in I$, соответственно изоморфных Ω-группам G_i.*

Для доказательства обозначим через G'_i подмножество тех элементов из G', у которых все компоненты, кроме, быть может, i-й, равны нулю. Ввиду покомпонентного выполнения операций это G'_i будет в G' Ω-подгруппой и даже идеалом, причем оно изоморфно, очевидно, Ω-группе G_i.

Заметим, далее, что всякий элемент из G' имеет лишь конечное число ненулевых компонент и поэтому может быть представлен в виде суммы конечного числа элементов, каждый из которых обладает лишь одной ненулевой компонентой. Отсюда следует, что G' является суммой (см. III. 2.4) всех идеалов G'_i, $i \in I$. С другой стороны, сумма $\bar{G}'_i$ всех идеалов G'_j, где $j \in I$ и $j \neq i$, состоит из тех и только тех элементов из G', i-я компонента которых равна нулю. Ясно, наконец, что

$$G'_i \cap \bar{G}'_i = O,$$

т. е. все требования, входящие в определение IV. 3.2, выполняются.

6. Мы имеем, следовательно, для понятия прямой суммы Ω-групп три равносильных определения: теоретико-структурное определение IV. 3.2, «внутреннее» определение IV. 4.2 и «внешнее» определение IV. 5.5, являющееся конструкцией, позволяющей говорить о прямой сумме любых наперед заданных Ω-групп. Заметим, что понятие полной прямой суммы бесконечного числа прямых слагаемых не является теоретико-структурным.

§ 6. Дистрибутивные структуры

1. В IV. 2.1 структура S была названа дистрибутивной, если в ней тождественно выполняется равенство

$$a \cap (b \cup c) = (a \cap b) \cup (a \cap c). \tag{1}$$

Покажем, что *тождество* (1) *равносильно двойственному ему тождеству*

$$a \cup (b \cap c) = (a \cup b) \cap (a \cup c). \tag{2}$$

Действительно, применяя (1) и определение структуры IV. 1.2, получаем:

$$a \cup (b \cap c) = [a \cup (a \cap c)] \cup (b \cap c) = a \cup [(a \cap c) \cup (b \cap c)] =$$
$$= a \cup [(a \cup b) \cap c] = [(a \cup b) \cap a] \cup [(a \cup b) \cap c] = (a \cup b) \cap (a \cup c).$$

Двойственные рассмотрения позволяют вывести (1) из (2).

Если структура S дистрибутивна, то в ней для любых элементов a, b, c из

$$a \cap c = b \cap c, \qquad a \cup c = b \cup c$$

следует $a = b$. Действительно,

$$a = a \cup (a \cap c) = a \cup (b \cap c) = (a \cup b) \cap (a \cup c) =$$
$$= (a \cup b) \cap (b \cup c) = b \cup (a \cap c) = b \cup (b \cap c) = b.$$

* Доказанное сейчас свойство дистрибутивных структур может быть принято в качестве их определения. *

2. Как мы знаем из I. 1.1, структура всех подмножеств любого множества дистрибутивна. Это же справедливо и для любых подструктур таких структур, т. е., как мы будем говорить, для любых *структур множеств*. Оказывается, что этим по существу исчерпываются все дистрибутивные структуры.

Всякая дистрибутивная структура изоморфна некоторой структуре множеств.

3. Дистрибутивные структуры составляют примитивный класс универсальных алгебр, и поэтому к ним применима теорема IV. 5.4: всякая дистрибутивная структура является подпрямой суммой подпрямо неразложимых дистрибутивных структур.

Примером подпрямо неразложимой дистрибутивной структуры служит структура T, состоящая из двух элементов — нуля и единицы. Дистрибутивность этой структуры очевидна. Если бы структура T была подпрямо разложимой, то она была бы подструктурой полной прямой суммы структур T_i, $i \in I$, причем существовали бы гомоморфизмы $\varphi_i : T \to T_i$, $i \in I$, не являющиеся изоморфизмами. Но в этом случае всякая структура T_i, $i \in I$, состояла бы из одного элемента, а тогда и прямая сумма этих структур была бы одноэлементной и не могла бы содержать T.

Всякая подпрямо неразложимая дистрибутивная структура, состоящая не только из одного элемента, изоморфна структуре T.

В самом деле, пусть дана дистрибутивная структура S. Если она состоит из двух элементов, то изоморфна, очевидно,

структуре T. Если же в S содержится не менее трех элементов, то найдется элемент a, отличный как от нуля, так и от единицы, если в S имеются нуль или единица. Обозначим через U подструктуру всех элементов x из S, удовлетворяющих условию $x \leqslant a$, а через V — подструктуру таких $x \in S$, что $x \geqslant a$. Ввиду условий, наложенных на выбор элемента a, каждая из подструктур U, V состоит не только из одного элемента a.

Обозначим через $U+V$ полную прямую сумму структур U и V в смысле IV.5.1: ее элементами служат пары (u, v), $u \in U$, $v \in V$, операции над которыми производятся покомпонентно. Сопоставим всякому $x \in S$ пару $(x \cap a,\ x \cup a) \in \in U+V$. Это отображение S в $U+V$ взаимно однозначно, так как для x, $y \in S$ из

$$x \cap a = y \cap a, \quad x \cup a = y \cup a$$

следует, как доказано в IV.6.1, $x = y$.

Это отображение является даже изоморфным, так как

$$((x \cup y) \cap a, (x \cup y) \cup a) = ((x \cap a) \cup (y \cap a), (x \cup a) \cup (y \cup a)) = \\ = (x \cap a,\ x \cup a) \cup (y \cap a,\ y \cup a);$$

$$((x \cap y) \cap a, (x \cap y) \cup a) = ((x \cap a) \cap (y \cap a), (x \cup a) \cap (y \cup a)) = \\ = (x \cap a,\ x \cup a) \cap (y \cap a,\ y \cup a).$$

Можно считать, следовательно, S подструктурой структуры $U+V$. Так как элементу $x \in U$ соответствует пара (x, a), а элементу $x \in V$ — пара (a, x), то мы получаем, что гомоморфизмы, отображающие всякий элемент из S соответственно в его первую или вторую компоненты, будут отображать S на все U и соответственно на все V и не являются изоморфизмами. Структура S оказалась, следовательно, подпрямо разложимой.

4. Докажем теперь основную теорему IV.6.2. Если дана дистрибутивная структура S, то, по сказанному выше, она является подпрямой суммой структур T_i, $i \in I$, где всякое T_i состоит из двух элементов — нуля 0_i и единицы 1_i (одноэлементные прямые слагаемые можно, конечно, исключить из рассмотрения). Обозначим через M множество всех единиц 1_i, $i \in I$, и сопоставим всякому элементу $a \in S$ подмножество A множества M, состоящее из всех тех единиц 1_i, которые являются i-ми компонентами в записи a как элемента

полной прямой суммы структур T_i, $i \in I$. Ясно, что если $a \neq b$, то и соответствующие им множества будут различными. С другой стороны, из покомпонентного выполнения операций в полной прямой сумме структур T_i, $i \in I$, и свойств единицы и нуля сейчас же следует, что элементу $a \cup b$ соответствует теоретико-множественное объединение $A \cup B$ множеств A и B, и элементу $a \cap b$ — теоретико-множественное пересечение $A \cap B$ этих множеств. Теорема доказана.

Заметим, что *если дистрибутивная структура S обладает нулем и единицей, то в полученном выше представлении множествами нулю будет соответствовать пустое подмножество множества M, а единице — само M.* Заметим также, что *если структура S конечная, то,* как показывает доказательство теоремы IV. 5.4, она будет подпрямой суммой конечного числа подпрямо неразложимых структур, а поэтому *она будет изоморфной некоторой структуре подмножеств конечного множества.*

5. Дистрибутивная структура S с нулем и единицей называется *булевой структурой* (или *булевой алгеброй*), если всякий элемент $a \in S$ обладает *дополнением* $\bar{a}$, где $\bar{a} \in S$ и

$$a \cap \bar{a} = 0, \qquad a \cup \bar{a} = 1.$$

Всякий элемент $a \in S$ обладает единственным дополнением, как вытекает из доказанного в IV. 6.1.

Структура всех подмножеств некоторого множества является булевой структурой, так как для всякого подмножества A существует теоретико-множественное дополнение $\bar{A}$. Структуру множеств (см. IV. 6.2), содержащую вместе со всяким подмножеством и его теоретико-множественное дополнение, будем называть *булевой структурой множеств.*

Всякая булева структура S изоморфна некоторой булевой структуре множеств.

Эта теорема уже доказана по существу в предшествующем пункте. Именно, если элементу $a \in S$ соответствует подмножество $A \subseteq M$, то дополнению $\bar{a}$ будет соответствовать теоретико-множественное дополнение $\bar{A}$ множества A в M: записи элементов a и $\bar{a}$ в полной прямой сумме структур T_i,

$i \in I$, таковы, что если i-я компонента в одной из них есть 1_i, то в другой она будет 0_i, и обратно.

6. *Всякая конечная булева структура S изоморфна структуре всех подмножеств некоторого конечного множества.*

Действительно, полученные выше результаты позволяют считать структуру S булевой структурой подмножеств конечного множества M. Обозначим через N множество всех тех подмножеств из M, которые являются минимальными отличными от нуля элементами структуры S.

Всякое подмножество A, являющееся элементом структуры S, совпадает с объединением A_0 всех содержащихся в нем подмножеств, входящих в N. В самом деле, в противном случае пересечение $A \cap \bar{A}_0$ было бы непустым элементом из S (так как $\bar{A}_0 \in S$), т. е. содержало бы хотя бы одно из входящих в N подмножеств в противоречие с определением множества A_0.

Теперь легко видеть, что, сопоставляя всякому $A \in S$ множество всех содержащихся в нем элементов из N, мы получаем взаимно однозначное и даже изоморфное отображение структуры S на структуру всех подмножеств множества N.

7. Ассоциативное кольцо R с единицей называется *булевым кольцом*, если все его элементы идемпотентны, т. е.

$$a^2 = a, \qquad a \in R. \tag{3}$$

Всякое булево кольцо коммутативно и удовлетворяет тождеству

$$2a = 0. \tag{4}$$

Действительно, для любых a, $b \in R$ из (3) следует

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b,$$

откуда

$$ab + ba = 0. \tag{5}$$

Полагая в (5) $b = a$ и учитывая (3), мы получаем (4), т. е. $a = -a$, а тогда (5) можно переписать в виде

$$ab - ba = 0.$$

* Всякую булеву структуру можно превратить в булево кольцо, если положить

$$a+b=(a\cap\bar{b})\cup(\bar{a}\cap b),\qquad ab=a\cap b.$$

Обратно, всякое булево кольцо можно превратить в булеву структуру, если положить

$$a\cup b=a+b-ab,\qquad a\cap b=ab.$$

Этим путем между булевыми структурами и булевыми кольцами устанавливается взаимно однозначное соответствие [Стоун, Trans. Amer. Math. Soc. **40** (1936), 37—111]. *

ГЛАВА ПЯТАЯ

ОПЕРАТОРНЫЕ ГРУППЫ И КОЛЬЦА. МОДУЛИ. ЛИНЕЙНЫЕ АЛГЕБРЫ

§ 1. Операторные группы и кольца

1. Как известно, действительное векторное пространство является абелевой группой по сложению, в которой дополнительно определено умножение векторов на действительные числа, связанное известными аксиомами со сложением векторов. Умножение на действительные числа имеет смысл также и в кольце действительных функций действительного переменного, и в кольце действительных квадратных матриц данного порядка. Эти и многие другие примеры привели к введению операторных алгебраических образований.

Если дан группоид (в частности, полугруппа или группа) G, то в нем можно выбрать произвольную систему эндоморфизмов Σ (см. III. 3.4) и рассматривать лишь те подгруппоиды, которые отображаются в себя при всех эндоморфизмах из Σ. Обобщая эту идею, обозначим через Σ некоторое множество, составленное из элементов $\alpha, \beta, \ldots$, и будем говорить, что группоид G является Σ-*операторным*, а множество Σ называть его *областью операторов*, если всякому элементу $\alpha \in \Sigma$ поставлен в соответствие некоторый эндоморфизм группоида G. Различным элементам из Σ может соответствовать при этом один и тот же эндоморфизм. Оператор α можно считать символом соответствующего ему эндоморфизма, так что для любых $a, b \in G$ и любого $\alpha \in \Sigma$

$$(ab)\alpha = a\alpha \cdot b\alpha. \tag{1}$$

Если G — Σ-операторная группа с единицей e, то из (1) следует

$$e\alpha = e, \qquad \alpha \in \Sigma.$$

Таким образом, *операторная группа является частным случаем мультиоператорной группы* (см. III.2.1): все мультиоператоры унарны и для каждого из них выполняется условие (1).

2. Подгруппоид A Σ-операторного группоида G называется Σ-*допустимым*, если при всех эндоморфизмах, соответствующих операторам из Σ, он отображается в себя, т. е. для всех $\alpha \in \Sigma$

$$A\alpha \subseteq A.$$

Любой оператор $\alpha \in \Sigma$ порождает, следовательно, некоторый эндоморфизм во всяком Σ-допустимом подгруппоиде A, что позволяет считать этот подгруппоид операторным с той же областью операторов Σ.

Пересечение любой системы Σ-допустимых подгруппоидов, если оно не пусто, само будет, конечно, Σ-допустимым. С другой стороны, используя (1) и II.3.8, можно легко показать, что подгруппоид, порожденный некоторой системой Σ-допустимых подгруппоидов, сам будет Σ-допустимым.

Операторные группоиды G и G' с одной и той же областью операторов Σ называются Σ-*операторно изоморфными*, если существует такое изоморфное отображение φ группоида G на группоид G', называемое Σ-*операторным изоморфизмом*, что для любых $a \in G$ и $\alpha \in \Sigma$

$$(a\alpha)\varphi = (a\varphi)\alpha. \tag{2}$$

При помощи равенства (2) определяются и Σ-*операторные гомоморфизмы*. Можно говорить, в частности, о Σ-*операторных эндоморфизмах* и *автоморфизмах* Σ-операторного группоида G.

Из (2) вытекает, что *эндоморфизм* φ Σ-*операторного группоида* G *тогда и только тогда будет* Σ-*операторным, если он перестановочен* (*в полугруппе эндоморфизмов*, см. III.3.4) *со всеми эндоморфизмами, соответствующими операторам из* Σ.

Заметим, что если множество Σ пусто или же состоит лишь из одного тождественного автоморфизма группоида G, то изучение G как Σ-операторного группоида равносильно изучению его как группоида без операторов.

3. Пусть даны полугруппа Σ и Σ-операторный группоид G. Будем говорить, что G является *группоидом с*

полугруппой операторов Σ, если для любого $a \in G$ и любых $\alpha, \beta \in \Sigma$

$$a(\alpha\beta) = (a\alpha)\beta. \tag{3}$$

Заметим, что условие (3) заведомо выполняется, если в качестве Σ взята подполугруппа полугруппы всех эндоморфизмов группоида G.

Произвольное множество Σ *можно так вложить в полугруппу* Γ, *что всякий* Σ*-операторный группоид будет группоидом с полугруппой операторов* Γ. *При этом* Σ*-допустимые подгруппоиды будут и* Γ*-допустимыми, а* Σ*-операторно изоморфные группоиды останутся и* Γ*-операторно изоморфными.*

В качестве множества Γ можно взять множество всевозможных *слов* вида

$$\alpha_1\alpha_2 \ldots \alpha_n, \tag{4}$$

т. е. конечных упорядоченных систем элементов из Σ, где $n \geqslant 1$, а элементы $\alpha_1, \alpha_2, \ldots, \alpha_n$ не обязаны быть различными. Определяя умножение слов равенством

$$(\alpha_1\alpha_2 \ldots \alpha_n)(\beta_1\beta_2 \ldots \beta_s) = \alpha_1\alpha_2 \ldots \alpha_n\beta_1\beta_2 \ldots \beta_s, \tag{5}$$

мы превращаем Γ в полугруппу. Ставя в соответствие слову (4) эндоморфизм Σ-операторного группоида G, являющийся произведением эндоморфизмов, соответствующих операторам $\alpha_1, \alpha_2, \ldots, \alpha_n$, мы делаем группоид G Γ-операторным, причем требование (3) будет, ввиду (5), удовлетворяться. Все остальные утверждения теоремы также будут, очевидно, справедливыми.

4. Пусть G — аддитивно записанная абелева группа, а R — ассоциативное кольцо. Группа G называется *абелевой группой с кольцом операторов* R или R*-модулем*, если G является R-операторной группой, т. е. для любых $a, b \in G$ и $\alpha \in R$ имеет место равенство (1), записываемое теперь в виде

$$(a + b)\alpha = a\alpha + b\alpha, \tag{6}$$

и если, кроме того, для любых $a \in G$ и $\alpha, \beta \in R$ выполняются равенства

$$a(\alpha + \beta) = a\alpha + a\beta, \tag{7}$$

$$a(\alpha\beta) = (a\alpha)\beta. \tag{8}$$

Естественность этого понятия вытекает из того, что *всякая абелева группа будет модулем относительно любого подкольца своего кольца эндоморфизмов,* так как, по III.3.8, в этом случае условия (6) — (8) выполняются.

Этот пример подсказывает следующее дополнительное требование: если кольцо R обладает единицей ε, то будем рассматривать такие R-модули, что ε служит для них *тождественным оператором*; иными словами, оператору ε соответствует тождественный автоморфизм группы G,

$$a\varepsilon = a, \qquad a \in G. \tag{9}$$

R-модули со свойством (9) называются *унитарными* R-модулями.

* Если R — ассоциативное кольцо с единицей, то изучение произвольных R-модулей полностью сводится на изучение унитарных R-модулей и таких R-модулей, в которых операторы из R действуют тривиально, т. е. для любого a из модуля и α из R

$$a\alpha = 0.$$

Произвольное множество Σ можно так вложить в ассоциативное кольцо R с единицей, что всякая Σ-операторная абелева группа будет унитарным R-модулем, Σ-допустимые подгруппы останутся R-допустимыми, т. е. будут *подмодулями* R-модуля, а Σ-операторно изоморфные абелевы группы останутся изоморфными R-модулями. *

5. Рассмотрим некоторые примеры.

Для произвольной группы G группа ее внутренних автоморфизмов (см. III.3.2) служит группой операторов, так как, как мы знаем, условия (1) и (3) выполняются. Допустимыми подгруппами относительно этой области операторов будут нормальные делители группы G и только они.

Для группы G группой операторов служит также группа всех ее автоморфизмов, а полугруппой операторов — полугруппа всех эндоморфизмов (см. III. 3.4). Подгруппы, допустимые относительно этих областей операторов, называются соответственно *характеристическими* и *вполне характеристическими.*

Действительное n-мерное векторное пространство является унитарным модулем над полем действительных чисел. Подмодулями этого модуля служат линейные подпространства, а операторными эндоморфизмами (см. V.1.2) — линейные преобразования.

6. Если в произвольном кольце R взят элемент a, то отображение $x \to xa$, $x \in R$, будет эндоморфизмом аддитивной группы кольца R, как вытекает из закона дистрибутивности; этот эндоморфизм называется *правым умножением*. Аддитивную группу кольца R можно считать, следовательно, операторной с самим множеством R в качестве области операторов; допустимыми подгруппами будут при этом правые идеалы кольца R (см. II.7.10) и только они. Аналогично определяются *левые умножения*, т. е. R еще раз выступает в качестве области операторов для своей аддитивной группы, причем в этом случае допустимыми подгруппами будут левые идеалы. Наконец, объединяя эти две области операторов, мы получим для аддитивной группы кольца R такую область операторов, при которой допустимыми подгруппами будут лишь (двусторонние) идеалы.

Если кольцо R ассоциативно, то оно, рассматриваемое как множество правых умножений, будет служить для своей аддитивной группы даже кольцом операторов в смысле V. 1.4, так как условиия (7), (8) и, в случае кольца с единицей, (9) заведомо выполняются. Если же рассматривать R как множество левых умножений, то равенство (8) выполняться не будет. В этом случае, как показывает справедливое в R равенство

$$(bc)\,a = b\,(ca),$$

кольцом операторов для аддитивной группы кольца R можно считать кольцо, антиизоморфное кольцу R. Отметим, что кольца R и R' называются *антиизоморфными*, если существует такой изоморфизм φ между аддитивными группами этих колец, что для всех a, $b \in R$

$$(ab)\,\varphi = b\varphi \cdot a\varphi.$$

7. При определении понятия операторов для колец можно, конечно, использовать, по аналогии со случаем групп, эндоморфизмы кольца. Примеры, а именно умножение на число в кольце функций и в кольце матриц, подсказывают и другой путь, — рассмотрение тех эндоморфизмов φ аддитивной группы кольца R, которые перестановочны (в смысле умножения эндоморфизмов) с правыми и левыми умножениями (см. V.1.6), т. е. удовлетворяют условию (для всех a, $b \in R$)

$$(ab)\,\varphi = (a\varphi)\,b = a\,(b\varphi). \qquad (10)$$

Именно этот путь мы и избираем. Таким образом, если Σ — множество с элементами $\alpha, \beta, \ldots$, то кольцо R называется *Σ-операторным*, если Σ-операторна его аддитивная группа и если, кроме того, для любых $a, b \in R$ и любого $\alpha \in \Sigma$

$$(ab)\alpha = (a\alpha)b = a(b\alpha). \tag{11}$$

Понятия *Σ-допустимого подкольца*, *Σ-допустимого идеала*, *Σ-операторного изоморфизма* и *Σ-операторного гомоморфизма* определяются по аналогии с тем, как это делалось в случае групп.

Если Σ-операторное кольцо R обладает единицей, то эндоморфизмы, соответствующие операторам из Σ, сами являются умножениями (одновременно правыми и левыми) на элементы кольца R, перестановочные со всеми элементами из R, а поэтому все идеалы и все односторонние идеалы кольца R будут Σ-допустимыми.

Действительно, для всех $a \in R$ и $\alpha \in \Sigma$

$$a\alpha = (a \cdot 1)\alpha = a \cdot (1\alpha),$$
$$a\alpha = (1 \cdot a)\alpha = (1\alpha) \cdot a,$$

откуда

$$a \cdot (1\alpha) = (1\alpha) \cdot a, \qquad a \in R.$$

Заметим, не развивая этого далее, что определение Σ-операторного кольца без труда переносится на случай любой мультиоператорной группы.

8. *Те эндоморфизмы аддитивной группы кольца R, которые удовлетворяют условию* (10), *составляют подкольцо в кольце всех эндоморфизмов этой группы.* Действительно, если эндоморфизмы φ и ψ обладают свойством (10), то, например,

$$(ab)(\varphi \pm \psi) = (ab)\varphi \pm (ab)\psi = (a\varphi)b \pm (a\psi)b =$$
$$= (a\varphi \pm a\psi)b = [a(\varphi \pm \psi)]b,$$
$$(ab)(\varphi\psi) = [(ab)\varphi]\psi = [(a\varphi)b]\psi = [(a\varphi)\psi]b = [a(\varphi\psi)]b.$$

Этим оправдывается следующее понятие. Если Σ — некоторое ассоциативное кольцо, то кольцо R называется *операторным с кольцом операторов* Σ, если оно Σ-операторно и если, сверх того, кольцо Σ служит для аддитивной группы кольца R кольцом операторов в смысле V.1.4.

Заметим, что если n — целое число, то отображение $a \to na$, определенное для всех элементов a кольца R, будет эндоморфизмом аддитивной группы этого кольца, причем выполняются также условия (7), (8), (9) и (11). Таким образом, *всякое кольцо R можно считать операторным с кольцом целых чисел в качестве кольца операторов.* Все подкольца кольца R будут при этом допустимыми, все изоморфизмы — операторными.

9. Пусть эндоморфизмы φ и ψ аддитивной группы кольца R удовлетворяют условию (10). Если $\varphi\psi \neq \psi\varphi$, то существует такой элемент $a \in R$, что

$$a\varphi\psi \neq a\psi\varphi.$$

Тогда для любого $x \in R$ мы получим, используя (10):

$$(a\varphi\psi)x = (a\varphi \cdot x)\psi = a\varphi \cdot x\psi = (a \cdot x\psi)\varphi =$$
$$= [(ax)\psi]\varphi = (a\psi \cdot x)\varphi = (a\psi\varphi)x.$$

Отсюда следует, что отличный от нуля элемент

$$b = a\varphi\psi - a\psi\varphi$$

удовлетворяет равенству

$$bx = 0$$

для всех $x \in R$, т. е. служит для кольца R *левым аннулятором.* Так же проверяется, что b будет для R и *правым аннулятором,* поэтому и вообще *аннулятором,* т. е. (см. IV.4.5)

$$bx = xb = 0$$

для всех $x \in R$.

Конечно, кольца, обладающие аннуляторами, существуют — так, всякое нулевое кольцо (см. II.2.2) состоит только из аннуляторов. Можно считать тем не менее достаточно оправданным, если мы, изучая кольца с кольцом операторов Σ, будем предполагать это кольцо Σ не только ассоциативным, но и коммутативным.

10. Σ-операторные группы (Σ-операторные кольца) составляют при данном Σ примитивный класс мультиоператорных групп. К тому, что было сказано в главе третьей, в частности о гомоморфизмах мультиоператорных групп, мы добавим лишь несколько замечаний.

Идеалы Σ-операторных групп (колец), рассматриваемых как мультиоператорные группы, совпадают с их Σ-допустимыми нормальными делителями (Σ-допустимыми идеалами).

В самом деле, если G — Σ-операторная группа, то для ее нормального делителя A включения $a\alpha \in A$ для всех $a \in A$, $\alpha \in \Sigma$ имеют место тогда и только тогда, если для всех $a \in A$, $x \in G$, $\alpha \in \Sigma$

$$(x\alpha)^{-1}(a\alpha)(x\alpha) = (x\alpha)^{-1}(ax)\alpha \in A.$$

Последнее включение является, однако, переписанным для нашего случая включением (2) из III.2.4.

С другой стороны, если A — подгруппа аддитивной группы Σ-операторного кольца R, то для всех $a \in A$, $x \in R$, $\alpha \in \Sigma$ включения $a\alpha \in A$ и

$$-x\alpha + a\alpha + x\alpha = -x\alpha + (a + x)\alpha \in A$$

равносильны; последнее включение снова является, однако, включением (2) из III.2.4. Мы знаем, вместе с тем, что для кольца, рассматриваемого как мультиоператорная группа, понятие идеала совпадает с понятием (двустороннего) идеала.

11. *Операторные эндоморфизмы Σ-операторной абелевой группы G составляют подкольцо в кольце всех эндоморфизмов этой группы* (см. III.3.8). Это без труда следует из определения сложения и умножения эндоморфизмов, если использовать характеризацию операторных эндоморфизмов, указанную в V.1.2. Полученное подкольцо называется *кольцом операторных эндоморфизмов* Σ-операторной абелевой группы G.

Так, кольцом операторных эндоморфизмов для n-мерного действительного векторного пространства (см. V.1.5) служит кольцо линейных преобразований, изоморфное, как известно из курса высшей алгебры, кольцу действительных квадратных матриц порядка n.

12. *Пусть G будет группа (кольцо) с произвольной областью операторов Σ, а H — ее допустимый нормальный делитель (его допустимый идеал). Тогда факторгруппу (фактор-кольцо) G/H можно сделать операторной с областью операторов Σ, причем так, что естественный гомоморфизм G на G/H будет Σ-операторным.*

Действительно, если G — группа, то для любых $a \in G$, $h \in H$ и $\alpha \in \Sigma$

$$(ah)\alpha = a\alpha \cdot h\alpha = a\alpha \cdot h',$$

где $h' \in H$ ввиду допустимости H. Это позволяет определить действие оператора α на элемент aH фактор-группы G/H равенством

$$(aH)\alpha = a\alpha \cdot H. \tag{12}$$

Справедливость условия (1) из V.1.1 проверяется без затруднений:

$$(aH \cdot bH)\alpha = (abH)\alpha = (ab)\alpha \cdot H = (a\alpha \cdot b\alpha)H =$$
$$= (a\alpha \cdot H)(b\alpha \cdot H) = (aH)\alpha \cdot (bH)\alpha.$$

Группа G/H оказалась Σ-операторной; последнее утверждение теоремы непосредственно следует из (12).

Если же G — кольцо, то равенство (12), определяющее действие операторов в G/H, перепишется в виде

$$(a + H)\alpha = a\alpha + H.$$

Проверим справедливость условия (11) из V.1.7:

$$[(a + H)(b + H)]\alpha = (ab + H)\alpha = (ab)\alpha + H = a\alpha \cdot b + H =$$
$$= (a\alpha + H)(b + H) = (a + H)\alpha \cdot (b + H).$$

Так же проверяется и вторая половина условия (11). Теорема доказана.

Читатель без труда проверит, что *если G является группой с полугруппой операторов Σ, или абелевой группой с кольцом операторов Σ, или же кольцом с кольцом операторов Σ, то это же можно утверждать и для G/H, где H — Σ-допустимый нормальный делитель или идеал.*

§ 2. Свободные модули. Абелевы группы

1. Все модули, рассматриваемые ниже, являются унитарными модулями над ассоциативным кольцом R с единицей; выполняются, следовательно, тождества (6) — (9) из V.1.4. Все эти модули составляют относительно операций абелевой группы и операторов из R примитивный класс универсальных алгебр (III.6.3), а поэтому можно говорить о *свободных R-модулях* (III.7.2). Систему свободных образующих свободного R-модуля будем называть его *базой*.

Применяя определение абелевой группы и упомянутые выше тождества (6) — (9), мы сейчас же получаем, что всякий элемент свободного R-модуля S с базой X записывается в виде конечной суммы

$$x_1\alpha_1 + x_2\alpha_2 + \ldots + x_n\alpha_n, \tag{1}$$

где $x_1, x_2, \ldots, x_n$ — различные элементы из X, $\alpha_1, \alpha_2, \ldots, \alpha_n \in R$ и отличны от нуля, $n \geqslant 0$. Покажем, что *эта запись однозначна*, после чего будем говорить о ней как о *записи* рассматриваемого элемента в базе X.

Для доказательства сопоставим каждому $x \in X$ R-модуль R_x, изоморфный кольцу R, рассматриваемому как правый модуль над самим собою (см. V.1.6), и возьмем, в соответствии с IV.5.5, прямую сумму S' всех этих модулей R_x, $x \in X$. Если элемент модуля R_x, соответствующий единице кольца R, мы обозначим через x, то, по IV.4.2, всякий элемент модуля S' однозначно записывается в виде (1). Доказываемое нами утверждение вытекает теперь из того, что, по III.7.3, существует гомоморфизм S в S', переводящий всякий элемент $x \in X$ в элемент x соответствующего модуля R_x.

Одновременно мы доказали, что *всякий свободный R-модуль является прямой суммой некоторого множества R-модулей, изоморфных самому R как правому R-модулю, и обратно.*

2. Правый идеал B ассоциативного кольца R с единицей назовем *главным*, если существует такой элемент $\beta \in B$, что всякий элемент из B хотя бы одним способом записывается в виде $\beta\alpha$, $\alpha \in R$. Будем записывать в этом случае $B = (\beta)$.

Если все правые идеалы кольца R являются главными и R не содержит делителей нуля, то всякий ненулевой подмодуль свободного R-модуля сам будет свободным R-модулем.

В самом деле, пусть в свободном R-модуле S с базой X взят ненулевой подмодуль U. Множество элементов $Y \subseteq U$ назовем *допустимым*, если выполняются следующие требования:

1) подмодуль $\{Y\}$, порожденный множеством Y, является свободным и имеет Y своей базой;

2) если X_Y есть множество всех элементов из X, входящих в записи в базе X для каких-либо элементов из Y, то

$$\{X_Y\} \cap U = \{Y\}.$$

Вопрос о существовании допустимых множеств оставим пока открытым, но отметим, что если они существуют и если дана цепь из допустимых множеств, то ее объединение также будет допустимым. Поэтому, по теореме Куратовского — Цорна (I.6.3), существуют максимальные среди допустимых множеств. Пусть Y будет одно из них.

Теорема будет доказана, ввиду 1), если мы покажем, что $\{Y\} = U$. Пусть

$$\{Y\} \subset U; \tag{2}$$

это будет иметь место и в том случае, когда допустимые множества отсутствуют, если заменим подмодуль $\{Y\}$ нулевым подмодулем. Покажем, что (2) приводит к противоречию.

Ввиду условия 2) в записи любого элемента из U, лежащего вне $\{Y\}$, должны встречаться элементы из X, лежащие вне X_Y. Пусть минимальное возможное число таких элементов будет n, $n \geqslant 1$, и пусть в $U \setminus \{Y\}$ существуют элементы, в записях которых встречаются элементы $x_1, x_2, \ldots, x_n$ из $X \setminus X_Y$ и только они. Коэффициенты при x_n в записях всех этих элементов составляют, после добавления к ним нуля, правый идеал кольца R, т. е., по условию, главный правый идеал (β).

Обозначим через z тот из рассматриваемых элементов из $U \setminus \{Y\}$, в записи которого коэффициент при x_n есть как раз β, и покажем, что, в противоречие с максимальностью Y, после добавления к Y элемента z мы снова получаем допустимое множество.

Действительно, если бы не выполнялось условие 1), то элементы из подмодуля $\{Y, z\}$ обладали бы неоднозначной записью через элементы множества $Y \cup z$, а тогда нашелся бы такой отличный от нуля элемент $\alpha \in R$, что

$$z\alpha \in \{Y\}.$$

Это невозможно, однако, так как в запись элемента z входят с ненулевыми коэффициентами элементы $x_1, x_2, \ldots, x_n \in X \setminus X_Y$, а тогда, ввиду отсутствия в кольце R делителей нуля, они имеют ненулевые коэффициенты и в записи элемента $z\alpha$.

С другой стороны, для проверки условия 2) возьмем любой элемент $t \in \{X_Y \cup z\} \cap U$. В его запись в базе X входят некоторые элементы из X_Y, а также элементы $x_1, x_2, \ldots, x_n$, причем коэффициент при x_n содержится в правом идеале (β), т. е. имеет вид $\beta\gamma$, $\gamma \in R$. Отсюда следует, что в запись разности $t - z\gamma$ элемент x_n уже не входит, а тогда, ввиду минимальности числа n, не входят и элементы $x_1, x_2, \ldots, x_{n-1}$, т. е.

$$t - z\gamma \in \{X_Y\} \cap U = \{Y\},$$

откуда

$$t \in \{Y, z\}.$$

Теорема доказана.

3. Всякая абелева группа является модулем над кольцом целых чисел, и это кольцо есть кольцо главных идеалов (см. II.9.3). Применяя к этому случаю полученные выше результаты и учитывая, что аддитивная группа кольца целых чисел является бесконечной циклической группой, получаем:

Всякая свободная абелева группа (см. III.7.10) *является прямой суммой бесконечных циклических групп.* Число этих циклических прямых слагаемых (или мощность их множества) не зависит, по III.7.12, от выбора прямого разложения и называется *рангом* этой свободной абелевой группы.

Всякая ненулевая подгруппа свободной абелевой группы сама свободна.

В свободной абелевой группе S конечного ранга n ранг всякой подгруппы конечен и не превосходит n.

В самом деле, пусть $x_1, x_2, \ldots, x_n$ будет база группы S. Возьмем в S любые k элементов $y_1, y_2, \ldots, y_k$, где $k > n$. Тогда

$$y_i = c_{i_1}x_1 + c_{i_2}x_2 + \ldots + c_{i_n}x_n, \qquad i = 1, 2, \ldots, k.$$

Система из k целочисленных n-мерных векторов

$$(c_{i_1}, c_{i_2}, \ldots, c_{i_n}), \qquad i = 1, 2, \ldots, k,$$

ввиду $k > n$ линейно зависима, как известно, а поэтому можно подобрать такие целые числа l_i, не все равные нулю, $i = 1, 2, \ldots, k$, что

$$l_1y_1 + l_2y_2 + \ldots + l_ky_k = 0.$$

Элементы $y_1, y_2, \ldots, y_k$ не могут входить, следовательно, в базу какой-либо подгруппы группы S.

4. Докажем следующую основную теорему об абелевых группах с конечным числом образующих:

Всякая абелева группа с конечным числом образующих является прямой суммой конечного числа циклических групп.

Доказательство этой теоремы, излагаемое ниже, принадлежит Радо [Journ. London Math. Soc. **26** (1951), 74—75].

Пусть абелева группа G обладает системами из n образующих. Рассмотрим всевозможные такие системы, допуская, что в них могут встречаться и равные элементы, и элементы, равные нулю. Пусть

$$a_1,\ a_2,\ \ldots,\ a_n \tag{3}$$

— одна из этих систем образующих, причем положим, обозначая через $o(a)$ порядок элемента a, что

$$o(a_1) \leqslant o(a_2) \leqslant \ldots \leqslant o(a_n). \tag{4}$$

Таким образом, если в (3) встречаются нули, то они стоят в начале, а если входят элементы бесконечного порядка, то они стоят в конце.

Систему (3) можно выбрать так, что система чисел (4) будет в лексикографическом смысле минимальной из возможных, т. е. если $b_1,\ b_2,\ \ldots,\ b_n$ — другая система образующих и

$$o(b_1) \leqslant o(b_2) \leqslant \ldots \leqslant o(b_n),$$

то нет такого i, $1 \leqslant i \leqslant n$, что

$$o(b_1) = o(a_1),\ \ldots,\ o(b_{i-1}) = o(a_{i-1}),\ o(b_i) < o(a_i).$$

Покажем, что если система образующих (3) выбрана указанным способом, то группа G будет прямой суммой циклических подгрупп $\{a_1\}, \{a_2\}, \ldots, \{a_n\}$. Если это не так, то запись элементов группы G в виде суммы элементов из указанных циклических подгрупп не будет однозначной, а поэтому можно получить равенство

$$k_1a_1 + k_2a_2 + \ldots + k_na_n = 0, \tag{5}$$

в котором не все слагаемые равны нулю. Пусть

$$k_1a_1 = \ldots = k_{j-1}a_{j-1} = 0, \tag{6}$$

но $k_ja_j \neq 0$, $j \geqslant 1$; можно считать, очевидно, что

$$0 < k_j < o(a_j). \tag{7}$$

Обозначим через k наибольший общий делитель чисел k_j, k_{j+1}, ..., k_n, т. е.

$$k_i = km_i, \qquad i = j,\ j+1,\ \ldots,\ n, \tag{8}$$

и числа m_j, m_{j+1} ..., m_n в совокупности взаимно просты. Докажем следующее вспомогательное утверждение:

5. *Если даны абелева группа* $A = \{a_j, a_{j+1}, \ldots, a_n\}$ *и система взаимно простых целых чисел* $m_j, m_{j+1}, \ldots, m_n$, *то в* A *можно так выбрать новую систему образующих,*

$$A = \{b_j, b_{j+1}, \ldots, b_n\}, \tag{9}$$

что

$$b_j = m_j a_j + m_{j+1} a_{j+1} + \ldots + m_n a_n. \tag{10}$$

Будем доказывать это индукцией по сумме абсолютных величин

$$m = |m_j| + |m_{j+1}| + \ldots + |m_n|,$$

так как при $m = 1$ утверждение тривиально. Если $m > 1$, то хотя бы два из системы взаимно простых чисел m_j, $m_{j+1}, \ldots, m_n$ должны быть отличными от нуля. Пусть, например,

$$|m_j| \geqslant |m_{j+1}| > 0.$$

Тогда или $|m_j + m_{j+1}| < |m_j|$ или $|m_j - m_{j+1}| < |m_j|$, т. е. для одного из двух знаков будет

$$|m_j \pm m_{j+1}| + |m_{j+1}| + \ldots + |m_n| < m. \tag{11}$$

Так как

$$A = \{a_j, a_{j+1} \mp a_j, a_{j+2}, \ldots, a_n\},$$

то, учитывая (11) и применяя индуктивное предположение, мы получим (9), где

$$b_j = (m_j \pm m_{j+1})\, a_j + m_{j+1}(a_{j+1} \mp a_j) + \\ + m_{j+2} a_{j+2} + \ldots + m_n a_n = m_j a_j + m_{j+1} a_{j+1} + \ldots + m_n a_n,$$

что и требовалось доказать.

6. Возвращаясь к доказательству основной теоремы и применяя доказанное утверждение, мы получим для группы G новую систему образующих,

$$G = \{a_1, \ldots, a_{j-1}, b_j, b_{j+1}, \ldots, b_n\},$$

где b_j удовлетворяет равенству (10). Из (5), (6) и (8) следует, однако, что $kb_j = 0$, а поэтому, ввиду (7),

$$o(b_j) \leqslant k \leqslant k_j < o(a_j),$$

что противоречит выбору системы образующих (3). Теорема доказана.

7. *Бесконечная циклическая группа неразложима в прямую сумму* (см. IV.3.10), так как, по II.4.2, всякие две ее ненулевые подгруппы имеют ненулевое пересечение.

Конечная циклическая группа $\{a\}$ *порядка* p^n, *где* p — *простое число, также неразложима,* так как все ее ненулевые подгруппы исчерпываются циклическими подгруппами элементов a, pa, p^2a, ..., $p^{n-1}a$, которые вложены друг в друга. Назовем такие циклические группы *примарными.*

Конечная циклическая группа $\{a\}$, *имеющая порядок*

$$m = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k},$$

где $p_1, p_2, \dots, p_k$ — *различные простые числа и* $k \geqslant 2$, *разлагается в прямую сумму примарных циклических групп, имеющих соответственно порядки* $p_1^{n_1}, p_2^{n_2}, \dots, p_k^{n_k}$.

Действительно, введем обозначение

$$q_i = p_1^{n_1} \dots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \dots p_k^{n_k}, \qquad i = 1, 2, \dots, k.$$

Тогда циклическая подгруппа $\{q_i a\}$ имеет порядок $p_i^{n_i}$, $i = 1, 2, \dots, k$. Сумма этих подгрупп будет, по IV.3.2, их прямой суммой, так как порядки всех элементов суммы подгрупп $\{q_j a\}$, $j \neq i$, взаимно просты с числом p_i, и поэтому пересечение этой последней суммы с подгруппой $\{q_i a\}$ равно нулю. Так как, однако, порядок прямой суммы конечного числа конечных групп равен произведению порядков прямых слагаемых, то порядок прямой суммы всех подгрупп $\{q_i a\}$, $i = 1, 2, \dots, k$, равен m, т. е. эта прямая сумма совпадает со всей группой $\{a\}$.

Отсюда, ввиду IV.3.4, вытекает следующее усиление основной теоремы:

Всякая абелева группа с конечным числом образующих является прямой суммой конечного числа неразложимых циклических групп, частью бесконечных, частью конечных примарных.

8. В IV.4.5 было введено понятие изоморфизма прямых разложений (прилагательное «центральный» для абелевых групп можно, конечно, опустить).

Всякие два разложения абелевой группы G с конечным числом образующих в прямую сумму неразложимых циклических групп изоморфны.

Действительно, пусть эти разложения будут

$$\begin{aligned} G &= \{a_1\} + \ldots + \{a_k\} + \{b_1\} + \ldots + \{b_s\}, \\ G &= \{a_1'\} + \ldots + \{a_l'\} + \{b_1'\} + \ldots + \{b_t'\}, \end{aligned} \tag{12}$$

где элементы a имеют конечные порядки, элементы b бесконечного порядка. Без труда проверяется, что в абелевой группе совокупность элементов конечных порядков является подгруппой, которая называется *периодической частью* этой группы. Если F — периодическая часть нашей группы G, то

$$F = \{a_1\} + \ldots + \{a_k\} = \{a_1'\} + \ldots + \{a_l'\}, \tag{13}$$

так как всякий элемент из G, в запись которого в одном из разложений (12) хотя бы один из элементов b входит с отличным от нуля коэффициентом, будет непременно бесконечного порядка.

Группа F конечная и поэтому обладает главными рядами, а тогда изомофизм прямых разложений (13) вытекает, по IV.4.6, из теоремы Шмидта — Орэ. С другой стороны, свободные абелевы группы $\{b_1\} + \ldots + \{b_s\}$ и $\{b_1'\} + \ldots + \{b_t'\}$ соответственно рангов s и t изоморфны, по IV.4.5, фактор-группе G/F, т. е. изоморфны между собой, а тогда $s = t$ (см. V.2.3).

* Всякие два разложения произвольной абелевой группы в прямую сумму неразложимых циклических групп изоморфны, если группа обладает такими разложениями (быть может с бесконечным множеством прямых слагаемых).

Всякая подгруппа прямой суммы циклических групп сама разлагается в прямую сумму циклических групп [Л. Я. Куликов, Мат. сб. **16** (1945), 129 — 162]. *

9. Абелева группа называется *примарной* по простому числу p, если порядок всякого ее элемента есть степень числа p.

Элемент a примарной (по p) абелевой группы G имеет конечную *высоту* n, $n \geqslant 0$, если уравнение

$$p^k x = a$$

разрешимо в G тогда и только тогда, когда $k \leqslant n$.

* Всякая периодическая (см. II.3.4) абелева группа разлагается в прямую сумму примарных групп по различным простым числам.

Примарная абелева группа G тогда и только тогда разлагается в прямую сумму циклических групп, если она является объединением возрастающей последовательности

$$A_1 \subseteq A_2 \subseteq \ldots \subseteq A_n \subseteq \ldots$$

таких своих подгрупп, что у каждой из них отличные от нуля элементы имеют конечные и в совокупности ограниченные высоты (в G) [Л. Я. Куликов, там же].

Всякая примарная абелева группа с ограниченными в совокупности порядками элементов разлагается в прямую сумму циклических групп [Прюфер, Math. Zeitschr. **17** (1923), 35—61].

Всякая счетная примарная абелева группа, все ненулевые элементы которой имеют конечные высоты, разлагается в прямую сумму циклических групп [Прюфер, там же].*

§ 3. Векторные пространства над телами

1. Изучим R-модули в том частном случае, когда ассоциативное кольцо R является телом, не обязательно коммутативным. Всякий унитарный модуль над ассоциативным телом K называется *векторным* (или *линейным*) *пространством* над этим телом. Следует помнить, что умножение элементов векторного пространства на элементы тела K подчинено условиям (6)—(9) из V. 1.4.

Подмодули (т. е. K-допустимые подгруппы) векторного пространства называются его *линейными подпространствами*. *Изоморфизм* векторных пространств над телом K всегда понимается, в соответствии с V.1.2, как их K-операторный изоморфизм.

2. *Для любого подпространства A векторного пространства V над телом K существует дополнение, т. е. такое подпространство B пространства V, что*

$$A \cap B = O, \quad \{A, B\} = V.$$

Иными словами, пространство V будет прямой суммой подпространств A и B,

$$V = A + B.$$

Действительно, рассмотрим все те подпространства векторного пространства V, пересечения которых с A равны нулю. Множество M всех таких подпространств не пусто, так как содержит нулевое подпространство. Далее, это множество частично упорядочено по теоретико-множественному включению, причем оно удовлетворяет условиям теоремы Куратовского — Цорна (см. I. 6.3).

В самом деле, если в M дана любая цепь L, то объединение C подпространств C_i, составляющих эту цепь (i пробегает некоторое множество индексов), само будет подпространством в V: если $x, y \in C$, то существуют такие i и j, что $x \in C_i$, $y \in C_j$, а поэтому, полагая, например, $C_i \subseteq C_j$, получим $x, y \in C_j$, т. е. $x \pm y \in C_j$ и, следовательно, $x \pm y \in C$; с другой стороны, из $x \in C_i$ следует $x\alpha \in C_i$ для всех $\alpha \in K$, а поэтому $x\alpha \in C$. Из $C_i \cap A = O$ для всех i следует, очевидно, что $C \cap A = O$, а поэтому подпространство C служит верхней гранью в множестве M для цепи L.

В множестве M существуют, таким образом, максимальные элементы. Пусть подпространство B будет одним из этих максимальных элементов. Тогда $A \cap B = O$, как вытекает из определения множества M. Покажем, что $\{A, B\} = V$.

Если $x \in V$, $x \notin B$, то подпространство $\{B, x\}$ состоит из всех элементов вида $b + x\alpha$, где $b \in B$, $\alpha \in K$. Это подпространство строго больше B, а поэтому, ввиду максимальности B в M, пересечение $A \cap \{B, x\}$ содержит отличный от нуля элемент $a = b + x\alpha$. Так как $\alpha \neq 0$ — иначе было бы $a \in B$ в противоречие с равенством $A \cap B = O$, — то $x = a\alpha^{-1} - b\alpha^{-1} \in \{A, B\}$, что и требовалось доказать.

Дополнение для подпространства A может быть выбрано в пространстве V, вообще говоря, многими способами. Все эти дополнения изоморфны, однако, между собою, так как, по теореме об изоморфизме III. 4.2 или по IV. 4.5, все они изоморфны фактор-пространству V/A.

3. Понятие линейной зависимости, играющее очень большую роль в теории конечномерных векторных пространств над полем, изучаемой в курсе высшей алгебры, переносится и на рассматриваемый сейчас общий случай. Именно, конечная система элементов

$$a_1, a_2, \ldots, a_k \tag{1}$$

векторного пространства V над телом K называется *линейно зависимой*, если в K существуют такие элементы $\alpha_1, \alpha_2, \ldots, \alpha_k$,

не все равные нулю, что

$$a_1\alpha_1 + a_2\alpha_2 + \ldots + a_k\alpha_k = 0,$$

и *линейно независимой* в противоположном случае. Как обычно, линейная зависимость системы (1) равносильна тому, что хотя бы один элемент из (1) линейно выражается через другие элементы этой системы (с коэффициентами из тела K).

Все основные свойства линейной зависимости, устанавливаемые в курсе высшей алгебры, без всяких затруднений распространяются на случай произвольных векторных пространств над любыми ассоциативными телами. Мы не будем поэтому приводить доказательств этих свойств и ограничимся лишь формулировкой важнейших из них:

Если в векторном пространстве V над телом K заданы две конечные системы элементов,

$$a_1,\ a_2,\ \ldots,\ a_k$$

и

$$b_1,\ b_2,\ \ldots,\ b_l,$$

из которых первая линейно независимая и, кроме того, всякий ее элемент линейно выражается через вторую систему, то $k \leqslant l$.

Отсюда вытекает, что *если в векторном пространстве V над телом K заданы две конечные линейно независимые системы элементов, причем любой элемент каждой из этих систем линейно выражается через другую систему, то эти две системы состоят из одного и того же числа элементов.*

4. Некоторая, не обязательно конечная, система элементов X векторного пространства V над телом K называется *линейно зависимой,* если в X содержится хотя бы одна конечная линейно зависимая подсистема элементов, и *линейно независимой,* если все конечные подсистемы системы X линейно независимы. Ясно, что всякая линейно независимая система является подмножеством и что всякая ее часть сама линейно независима.

Пространство V обладает линейно независимыми подмножествами; таковы, например, подмножества, состоящие из одного ненулевого элемента. Множество M всех линейно независимых подмножеств пространства V частично упорядочено по включению, причем удовлетворяет условиям теоремы

Куратовского — Цорна (см. I.6.3). Именно, если в M дана цепь L, то объединение X линейно независимых подмножеств X_i, составляющих эту цепь, само будет линейно независимым: если в X взята конечная система элементов

$$x_1, x_2, \ldots, x_k, \tag{2}$$

то существует такое линейно независимое подмножество X_j, входящее в цепь L, которое содержит всю систему (2), а поэтому система (2) должна быть линейно независимой. Подмножество X служит, следовательно, верхней гранью цепи L в множестве M.

Этим доказано, что *векторное пространство V над телом K обладает максимальными линейно независимыми подмножествами, причем всякое линейно независимое подмножество этого пространства содержится в некотором максимальном.*

Всякое максимальное линейно независимое подмножество векторного пространства V называется *базой* этого пространства.

5. *Подмножество X, составленное из элементов x_i (i пробегает некоторое множество индексов), тогда и только тогда будет базой векторного пространства V над телом K, если всякий отличный от нуля элемент a из V обладает однозначной записью*

$$a = x_{i_1}\alpha^1 + x_{i_2}\alpha^2 + \ldots + x_{i_k}\alpha^k, \tag{3}$$

где $x_{i_1}, x_{i_2}, \ldots, x_{i_k} \in X$, $\alpha^1, \alpha^2, \ldots, \alpha^k$ — отличные от нуля элементы тела K, а $k \geqslant 1$.

Действительно, пусть X — база пространства V, но отличный от нуля элемент a из V не может быть записан в виде (3); отсюда, в частности, вытекает, что $a \notin X$. Тогда, добавляя элемент a к любой конечной подсистеме множества X, мы получим линейно независимую систему, а поэтому, добавляя a ко всей базе X, мы вновь получим линейно независимое множество в противоречие с определением базы. Если же элемент a обладает двумя различными записями через базу X, а именно (3) и

$$a = x_{j_1}\beta^1 + x_{j_2}\beta^2 + \ldots + x_{j_l}\beta^l,$$

то объединение конечных подсистем $x_{i_1}, \ldots, x_{i_k}$ и $x_{j_1}, \ldots, x_{j_l}$ базы X будет линейно зависимым, что снова

противоречит определению базы. Проверка обратного утверждения теоремы столь же проста и предоставляется читателю.

Вместо записи (3) для всех элементов a векторного пространства V можно употреблять, конечно, однозначно определенную запись

$$a = \sum_{x_i \in X} x_i \alpha^i, \qquad \alpha^i \in K, \tag{3'}$$

в которой не более конечного числа коэффициентов α^i отлично от нуля. Ввиду V.1.4 сложение элементов, записанных в виде (3'), сводится к сложению коэффициентов при одинаковых x_i, а умножение элемента a на элемент β тела K равносильно умножению всех коэффициентов α^i из (3') на β справа.

Ввиду IV.4.2 можно сказать, что *векторное пространство V над телом K с базой X является прямой суммой векторных пространств xK, $x \in X$.*

6. *Все базы векторного пространства V над телом K имеют одну и ту же мощность.*

Пусть, в самом деле, в пространстве V взяты базы X и Y. Если хотя бы одна из них, например X, конечна и состоит из m элементов, то, как немедленно следует из V.3.3, база Y также конечна и также состоит из m элементов.

Пусть, однако, обе базы X, Y бесконечны и имеют соответственно мощности $\mathfrak{m}$ и $\mathfrak{n}$, причем предположим, что $\mathfrak{m} < \mathfrak{n}$. Всякий элемент x базы X обладает, по V.3.5, записью вида (3) через конечную систему элементов Y_x из базы Y. Объединение Y' всех таких конечных подсистем Y_x, где x пробегает всю базу X, будет истинным подмножеством базы Y, так как оно, как объединение множества конечных множеств, имеющего мощность $\mathfrak{m}$, само имеет мощность $\mathfrak{m}$. Пусть y — любой элемент из $Y \setminus Y'$. По V.3.5 он линейно выражается через конечную систему элементов $x_1, x_2, \ldots, x_k$ из X, а поэтому и через конечную подсистему $\bigcup_{i=1}^{k} Y_{x_i}$ множества Y', что противоречит, однако, линейной независимости базы Y. Теорема доказана.

Мощность любой базы векторного пространства V называется *размерностью* этого пространства. Если, в частности, эта мощность конечна, то мы говорим о *конечномерном* пространстве. Так, векторное пространство xK одномерно.

7. *Для всякой мощности* $\mathfrak{m}$, *конечной или бесконечной, существует векторное пространство над телом* K, *имеющее размерность* $\mathfrak{m}$.

Пусть X — любое множество мощности $\mathfrak{m}$. Тогда прямая сумма одномерных векторных пространств xK для всех $x \in X$ (ее существование вытекает из IV.5.5) будет искомым векторным пространством. Здесь xK есть совокупность элементов вида $x\alpha$, $\alpha \in K$, с естественными определениями операций сложения и умножения на элемент из K.

Векторные пространства V *и* W *над телом* K *изоморфны тогда и только тогда, когда они имеют одну и ту же размерность.*

В самом деле, если существует изоморфное отображение φ пространства V на пространство W и если X — база пространства V, то $X\varphi$ будет базой пространства W. Этим в одну сторону теорема доказана.

Пусть, с другой стороны, пространства V и W обладают соответственно базами X и Y, имеющими одну и ту же мощность. Фиксируем некоторое взаимно однозначное отображение φ базы X на базу Y,

$$x\varphi \in Y \text{ для всех } x \in X,$$

и следующим образом распространим его на все пространство V: если элемент a из V имеет запись (3′) через базу X, то положим

$$a\varphi = \sum_{x_i \in X} (x_i\varphi)\,\alpha^i.$$

Мы получаем, очевидно, взаимно однозначное отображение пространства V на все пространство W; изоморфность этого отображения следует из сказанного в V.3.5.

Мы видим, что теоремы настоящего пункта дают исчерпывающее описание всех векторных пространств над любым телом K.

§ 4. Кольца линейных преобразований

1. Операторные эндоморфизмы векторного пространства V над телом K называются *линейными преобразованиями* этого пространства. По V.1.11 линейные преобразования составляют подкольцо в кольце всех эндоморфизмов абелевой группы V. Будем обозначать кольцо линейных преобразований через $R(V, K)$.

Мы хотим показать, что заданием этого кольца определяется и тело K, и само пространство V. Для того чтобы точнее сформулировать это утверждение, введем следующее понятие, обобщающее понятие изоморфизма двух векторных пространств над одним и тем же телом.

Пусть даны векторные пространства V над телом K и W над телом L. Будем говорить, что между этими пространствами установлено *полулинейное соответствие* σ, если существует изоморфизм σ тела K на тело L и изоморфизм, который также обозначим через σ, группы V на группу W, причем для всех $a \in V$, $\alpha \in K$

$$(a\alpha)\sigma = a\sigma \cdot \alpha\sigma.$$

Таким образом, если $K = L$ и σ является тождественным автоморфизмом тела K, то полулинейное соответствие превращается в изоморфизм векторных пространств V и W над телом K.

2. *Если векторные пространства V над телом K и W над телом L находятся в полулинейном соответствии σ, то кольца линейных преобразований $R(V, K)$ и $R(W, L)$ этих пространств изоморфны.*

В самом деле, пусть $\varphi \in R(V, K)$. Тогда $\sigma^{-1}\varphi\sigma$ будет отображением W в себя, являющимся линейным преобразованием, так как, учитывая, что φ является линейным преобразованием, для любых b, $b' \in W$, $\beta \in L$ получим

$$(b + b')(\sigma^{-1}\varphi\sigma) = b(\sigma^{-1}\varphi\sigma) + b'(\sigma^{-1}\varphi\sigma),$$

$$(b\beta)(\sigma^{-1}\varphi\sigma) = (b\sigma^{-1} \cdot \beta\sigma^{-1})\varphi\sigma = (b\sigma^{-1}\varphi \cdot \beta\sigma^{-1})\sigma = b(\sigma^{-1}\varphi\sigma) \cdot \beta.$$

Соответствие $\varphi \to \sigma^{-1}\varphi\sigma$ является гомоморфным отображением кольца $R(V, K)$ в кольцо $R(W, L)$, так как для любого $b \in W$ и любых φ, $\psi \in R(V, K)$

$$b[\sigma^{-1}(\varphi + \psi)\sigma] = b[\sigma^{-1}\varphi\sigma + \sigma^{-1}\psi\sigma],$$
$$b[\sigma^{-1}(\varphi\psi)\sigma] = b(\sigma^{-1}\varphi\sigma)(\sigma^{-1}\psi\sigma).$$

Это будет отображение на все кольцо $R(W, L)$, так как если $\varphi' \in R(W, L)$, то

$$\varphi' = \sigma^{-1}(\sigma\varphi'\sigma^{-1})\sigma, \qquad \sigma\varphi'\sigma^{-1} \in R(V, K).$$

Это соответствие будет, наконец, изоморфизмом, так как если преобразование $\sigma^{-1}\varphi\sigma$ нулевое, т. е. для всех $b \in W$

$$b(\sigma^{-1}\varphi\sigma) = 0,$$

то для всех $a \in V$

$$a\varphi = (a\sigma)(\sigma^{-1}\varphi\sigma)\sigma^{-1} = 0\sigma^{-1} = 0,$$

т. е. линейное преобразование φ также будет нулевым.

Будем говорить, что построенный нами изоморфизм между кольцами $R(V, K)$ и $R(W, L)$ *индуцируется* полулинейным соответствием σ.

3. Справедливо обратное утверждение (см., например, книгу Р. Бэра «Линейная алгебра и проективная геометрия»):

* Всякий изоморфизм между кольцами линейных преобразований $R(V, K)$ и $R(W, L)$ индуцируется некоторым полулинейным соответствием между пространствами V и W. *

Мы будем доказывать, впрочем, следующее более слабое утверждение:

Задание, с точностью до изоморфизма, кольца линейных преобразований $R(V, K)$ определяет, также с точностью до изоморфизма, и тело K, и пространство V (т. е. определяет размерность этого пространства).

4. Фиксируем в пространстве V базу X с элементами x_i, $i \in I$. Как обычно, линейное преобразование φ вполне определяется, ввиду (2) из V.1.2, заданием образов $x_i\varphi$ всех элементов базы X. Сопоставим преобразованию φ бесконечную матрицу, строки и столбцы которой пронумерованы всевозможными индексами $i \in I$, причем в i-м столбце ставим коэффициенты записи элемента $x_i\varphi$ в базе X; понятно, что лишь конечное число этих коэффициентов отлично от нуля.

Обратно, всякая матрица указанного вида, содержащая в каждом столбце лишь конечное число ненулевых элементов, соответствует некоторому линейному преобразованию. *Множество K_I всех таких матриц будет кольцом при обычном определении операций над матрицами, и это кольцо антиизоморфно кольцу $R(V, K)$* (см. V.1.6). Мы проверим лишь следующие два утверждения:

Если $A, B \in K_I$, то и $AB \in K_I$. Действительно, если $i \in I$ и i-й столбец матрицы B имеет ненулевые элементы лишь в строках с номерами $j_1, j_2, \ldots, j_n$, то рассмотрим столбцы с этими же номерами в матрице A. В них содержится лишь конечное число ненулевых элементов, которые расположены

в конечном числе строк, а поэтому в i-м столбце произведения AB будет лишь конечное число ненулевых элементов.

Если $\varphi, \psi \in R(V, K)$ и им соответствуют матрицы $(\beta_{ji}), (\gamma_{kj}) \in K_I$, то произведению $\varphi\psi$ соответствует матрица $(\gamma_{kj})\cdot(\beta_{ji})$.

Действительно, для всех $i \in I$ из

$$x_i\varphi = \sum_{j \in I} x_j\beta_{ji},$$

$$x_j\psi = \sum_{k \in I} x_k\gamma_{kj}$$

следует

$$x_i(\varphi\psi) = \sum_{j \in I} (x_j\psi)\beta_{ji} = \sum_{k \in I} x_k\left(\sum_{j \in I} \gamma_{kj}\beta_{ji}\right).$$

5. Нам нужно, следовательно, доказать, что задание кольца K_I как абстрактного кольца определяет и тело K (с точностью до изоморфизма), и мощность множества индексов I.

Фиксируем конечную систему индексов

$$j_1, j_2, \ldots, j_n \in I, \quad n \geqslant 1, \tag{1}$$

и систему отличных от нуля элементов $\lambda_t^s \in K$, $s, t = 1, 2, \ldots, n$, подчиненных следующим условиям:

$$\lambda_s^s = 1; \quad \lambda_s^t = (\lambda_t^s)^{-1}; \quad \lambda_t^s\lambda_u^t = \lambda_u^s. \tag{2}$$

Обозначим через

$$S = S(j_1, j_2, \ldots, j_n; \lambda_t^s, s, t = 1, 2, \ldots, n) \tag{3}$$

совокупность матриц из K_I, у которых лишь строки с номерами из (1) могут быть ненулевыми, причем для $s, t = 1, 2, \ldots, n$ j_s-я строка получается умножением слева j_t-й строки на λ_t^s.

Множество S является минимальным правым идеалом кольца K_I.

Утверждение, что S будет правым идеалом в K_I, проверяется без затруднений. Этот идеал состоит не только из нуля — одну строку с номером из (1) в матрице из S можно, очевидно, задать произвольно.

Для доказательства минимальности идеала S введем обозначение, которым будем пользоваться и дальше: если $\alpha \in K$, то через $(\alpha)_{ji}$ обозначим матрицу из K_I, у которой на месте (j, i) стоит элемент α, а все остальные элементы равны нулю.

Возьмем в S любую ненулевую матрицу A; пусть у нее на месте (j, i), где j из системы (1), стоит элемент $\alpha \neq 0$. Умножая A справа на матрицу $(\alpha^{-1})_{ii}$, мы получим матрицу из S с одним ненулевым i-м столбцом, причем на месте (j, i) стоит единица. Умножая, наконец, полученную матрицу справа на некоторую матрицу из K_l, у которой лишь i-я строка может быть ненулевой, можно получить, очевидно, любую матрицу из S.

Идеалами вида (3) *исчерпываются все минимальные правые идеалы кольца* K_l.

Действительно, возьмем в K_l произвольный ненулевой правый идеал T, а в нем матрицу с ненулевым i-м столбцом. Умножая эту матрицу справа на $(1)_{ii}$, мы получим матрицу A из T, содержащую лишь один этот ненулевой i-й столбец. Пусть отличные от нуля элементы этого столбца будут

$$\alpha_{j_1 i},\ \alpha_{j_2 i},\ \ldots,\ \alpha_{j_n i}.$$

Положим

$$\lambda_l^s = \alpha_{j_s i}\alpha_{j_l i}^{-1},\ s, t = 1, 2, \ldots, n;$$

условия (2) выполняются. Теперь легко видеть, что содержащийся в T правый идеал, порожденный матрицей A, есть идеал S из (3).

6. *Все минимальные правые идеалы кольца* K_l, *рассматриваемые как правые модули над* K_l, *изоморфны между собой.*

Действительно, пусть S и S' будут два идеала вида (3). Отметим по одному индексу, j и j', из относящихся к этим идеалам систем индексов (1). Всякая матрица из S вполне определяется своей j-й строкой, которая может быть произвольной; это же относится к S' и j'. Мы получим, следовательно, взаимно однозначное соответствие между S и S', если сопоставим друг другу матрицы, j-я и соответственно j'-я строки которых совпадают. Это соответствие является на самом деле изоморфизмом K_l-модулей S и S'.

Отсюда следует, *что изоморфны между собою и кольца операторных эндоморфизмов минимальных правых идеалов кольца* K_l, *рассматриваемых как* K_l*-модули.* Покажем, что *эти кольца антиизоморфны телу* K.

Не нарушая общности, рассмотрим такой идеал S вида (3), для которого $n = 1$, т. е. система (1) состоит из одного

индекса j. Ясно, что умножение слева всех элементов всех матриц из S на элемент $\alpha \in K$ будет K_I-операторным эндоморфизмом идеала S.

Пусть теперь φ будет любой K_I-операторный эндоморфизм идеала S. Так как $(1)_{jj} \in S$, то найдем $(1)_{jj}\varphi$. Если бы эта матрица, содержащая одну ненулевую j-ю строку, имела отличный от нуля элемент на месте (j, l), $j \neq i$, то мы получили бы, в противоречие с K_I-операторностью эндоморфизма φ, что

$$((1)_{jj} \cdot (1)_{ii})\varphi = 0\varphi = 0,$$

$$((1)_{jj}\varphi) \cdot (1)_{ii} \neq 0.$$

Таким образом,

$$(1)_{jj}\varphi = (\alpha)_{jj}, \quad \alpha \in K.$$

Всякая матрица A из S равна, однако, своему произведению слева на $(1)_{jj}$, а поэтому

$$A\varphi = ((1)_{jj}A)\varphi = (1)_{jj}\varphi \cdot A = (\alpha)_{jj}A.$$

Последнее произведение означает, однако, что все элементы матрицы A умножаются слева на α.

Мы получаем, что все K_I-операторные эндоморфизмы идеала S исчерпываются умножениями слева на элементы тела K. При этом сумме эндоморфизмов соответствует сумма соответствующих элементов из K, а произведению, так как умножение на $\alpha \in K$ производится слева, — произведение элементов из K в обратном порядке.

Этим доказано, что тело K определяется с точностью до изоморфизма заданием кольца $R(V, K)$ как абстрактного кольца. Именно, тело K антиизоморфно кольцу R'-операторных эндоморфизмов любого минимального правого идеала кольца $R'(= K_I)$, антиизоморфного кольцу $R(V, K)$.

7. Переходим к вопросу о мощности множества индексов I. Предположим сначала, что множество I конечно и состоит из индексов 1, 2, ..., n. Совокупность $S(j)$ матриц из K_I, лишь j-я строка которых может быть отличной от нуля, $j = 1, 2, \ldots, n$, будет, по V.4.5, минимальным правым идеалом кольца K_I. Эти идеалы составляют прямую сумму (см. IV.3.2), совпадающую со всем кольцом K_I, а поэтому в K_I, как

в правом K_I-модуле, имеется композиционный ряд длины n (см. III.4.6)

$$O \subset S(1) \subset S(1)+S(2) \subset \ldots \subset \sum_{j=1}^{n} S(j) = K_I.$$

Число n инвариантно определяется, следовательно, ввиду теоремы Жордана — Гельдера, самим K_I-модулем K_I.

Рассмотрим теперь случай б е с к о н е ч н о г о множества I. Назовем систему минимальных правых идеалов кольца K_I *независимой*, если правый идеал, порожденный всеми идеалами этой системы, является их прямой суммой. Система идеалов $S(j)$ (см. выше), взятых для всех $j \in I$, будет независимой системой, притом даже максимальной, так как всякий идеал S вида (3) содержится в прямой сумме идеалов $S(j)$, где j — из системы (1), и поэтому не может быть добавлен к системе всех идеалов $S(j)$, $j \in I$, без нарушения ее независимости. Мощность системы идеалов $S(j)$ совпадает, понятно, с мощностью множества I.

Мощность любой независимой системы минимальных правых идеалов кольца K_I не больше мощности множества I.

В самом деле, если дана система идеалов вида (3), то множество связанных с ними систем индексов (1) будет частью множества всех конечных подмножеств (бесконечного) множества I, и поэтому его мощность не превосходит мощности I. С другой стороны, из тех же результатов о композиционных рядах (см. III.4.6) следует, что независимая система идеалов вида (3), связанных с данной системой индексов (1), может быть лишь конечной.

Таким образом, и мощность множества I (т. е. размерность векторного пространства V) однозначно определяется заданием кольца $R(V, K)$ как абстрактного кольца. Именно, э т а м о щ н о с т ь я в л я е т с я м а к с и м а л ь н о й м о щ н о с т ь ю н е з а в и с и м о й с и с т е м ы м и н и м а л ь н ы х п р а в ы х и д е а л о в к о л ь ц а, а н т и и з о м о р ф н о г о к о л ь ц у $R(V, K)$. Теорема доказана.

8. Если в кольце R взято множество M, то назовем *правым аннулятором* этого множества совокупность таких элементов $r \in R$, что $xr = 0$ для всех $x \in M$. Правый аннулятор любого множества будет, очевидно, правым идеалом кольца R. Аналогично определяется *левый аннулятор*.

* Ассоциативное кольцо R тогда и только тогда изоморфно кольцу $R(V, K)$ всех линейных преобразований некоторого векторного пространства V над некоторым телом K, если оно удовлетворяет следующим условиям: 1) R обладает единицей; 2) R обладает минимальными односторонними идеалами, которые все содержатся в каждом ненулевом двустороннем идеале; 3) если правый аннулятор левого идеала равен нулю, то этот левый идеал содержит все минимальные левые идеалы; 4) сумма любых двух правых (левых) аннуляторов сама является таким же аннулятором [Вулфсон, Amer. Journ. Math. **75** (1953), 358—386]. *

§ 5. Простые кольца. Теорема Джекобсона

1. Из сказанного в II.7.9 следует, что полное кольцо матриц данного порядка n над ассоциативным телом K (т. е. кольцо всех линейных преобразований n-мерного векторного пространства над K) будет простым кольцом. Сейчас мы хотим изучить один много более широкий класс простых ассоциативных колец.

Рассмотрим произвольное векторное пространство V над ассоциативным телом K. Образ $V\varphi$ этого пространства при линейном преобразовании φ будет, очевидно, линейным подпространством (см. V.3.1). Говорят, что φ есть линейное преобразование *конечного ранга*, если подпространство $V\varphi$ конечномерно. Ясно, что сумма и разность линейных преобразований конечного ранга, а также произведение линейных преобразований, хотя бы одно из которых является преобразованием конечного ранга, сами будут преобразованиями конечного ранга, а поэтому множество $R'(V, K)$ всех таких преобразований будет подкольцом и даже идеалом кольца всех линейных преобразований $R(V, K)$.

Подкольцо R_0 кольца $R(V, K)$ называется *плотным кольцом линейных преобразований*, если для любой линейно независимой конечной системы элементов $x_1, x_2, \ldots, x_n \in V$ и произвольной системы элементов $y_1, y_2, \ldots, y_n \in V$ в кольце R_0 найдется такое линейное преобразование φ, что

$$x_i\varphi = y_i, \qquad i = 1, 2, \ldots, n.$$

2. *Всякое плотное кольцо линейных преобразований конечного ранга является простым кольцом.*

Действительно, пусть R_0 — плотное кольцо линейных преобразований конечного ранга в векторном пространстве V над телом K и пусть R_0 обладает ненулевым идеалом A. Докажем, что *для всякого конечномерного подпространства L можно найти в идеале A проекцию V на L*, т. е. такое преобразование $a \in A$, что $Va = L$ и для всякого $y \in L$ имеет место $ya = y$.

Пусть сперва подпространство L одномерно, $L = xK$, $x \neq 0$. Возьмем $a \in A$, $a \neq 0$. Подпространство Va конечномерно; пусть $y_1, y_2, \ldots, y_n$ будет его база. Тогда существует такое $x_1 \in V$, что $x_1 a = y_1$. Ввиду плотности R_0 существует такое $\varphi \in R_0$, что

$$y_1\varphi = x_1, \quad y_2\varphi = \ldots = y_n\varphi = 0. \tag{1}$$

Так как A — идеал, то $a\varphi = a' \in A$ и, по (1), $Va' = x_1 K$, причем $x_1 a' = x_1$. Существуют, далее, такие $\varphi_1, \varphi_2 \in R_0$, что

$$x\varphi_1 = x_1, \qquad x_1\varphi_2 = x.$$

Поэтому

$$V(\varphi_1 a' \varphi_2) = xK = L,$$
$$x(\varphi_1 a' \varphi_2) = x,$$

а так как $\varphi_1 a' \varphi_2 \in A$, то это и будет искомая проекция.

Пусть теперь наше утверждение уже доказано для подпространств размерности $n-1$ и пусть подпространство L n-мерно, $n > 1$. Возьмем в нем $(n-1)$-мерное подпространство L'; по предположению, существует проекция $a' \in A$ пространства V на подпространство L'. Тогда $La' = L'$. Ядро L'' этого преобразования является одномерным подпространством, $L''a' = O$, и

$$L = L' + L''.$$

Существует проекция $a'' \in A$ пространства V на подпространство L''. Тогда

$$a = a' + a'' - a'a'' \in A$$

и будет искомой проекцией V на L. В самом деле, для всех $x \in V$

$$xa = xa' + xa'' - (xa')\,a'' \in L;$$

если $x \in L'$, то

$$xa = x + xa'' - xa'' = x;$$

если $x \in L''$, то $xa' = 0$ и

$$xa = xa'' = x.$$

Доказательство теоремы проходит теперь без затруднений. Для любого $\varphi \in R_0$ подпространство $V\varphi$ конечномерно и, по доказанному, существует $a \in A$, являющееся проекцией V на $V\varphi$. Поэтому $\varphi a = \varphi$, откуда $\varphi \in A$, т. е. $A = R_0$.

3. *Всякое плотное кольцо линейных преобразований конечного ранга обладает минимальными правыми идеалами.*

В самом деле, пусть R_0 — снова плотное кольцо линейных преобразований конечного ранга в векторном пространстве V над телом K и пусть L — любое одномерное подпространство из V. Применяя доказанное выше утверждение к случаю $A = R_0$, можно утверждать существование такого $a \in R_0$, которое является проекцией V на L. Обозначим через L' совокупность таких $y' \in V$, что $y'a = 0$. Тогда $L \cap L' = O$ и

$$V = L + L'. \tag{2}$$

Обозначим через A совокупность таких $a' \in R_0$, что $L'a' = O$. Ясно, что $a \in A$, т. е. A состоит не только из нуля, и что A будет правым идеалом кольца R_0. Докажем, что этот идеал минимальный. Пусть a_1 и a_2 — любые ненулевые элементы из A. Если $L = xK$, то $xa_1 \neq 0$, так как иначе было бы $Va_1 = O$, т. е. $a_1 = 0$. Поэтому, ввиду плотности кольца R_0, существует такое $\varphi \in R_0$, что

$$(xa_1)\varphi = xa_2, \tag{3}$$

а так как

$$L'a_1 = L'a_2 = O,$$

то, ввиду (2) и (3),

$$a_1\varphi = a_2,$$

т. е. правый идеал A порождается своим произвольным ненулевым элементом a_1.

4. Обращением полученных результатов служит следующая теорема Джекобсона [Trans. Amer. Math. Soc. **57** (1945), 228—245]:

Всякое ненулевое (см. II.2.2) *простое кольцо R, обладающее минимальными правыми идеалами, изоморфно плот-*

ному кольцу линейных преобразований конечного ранга некоторого векторного пространства над некоторым телом.

Возьмем в нашем кольце R минимальный правый идеал A. Умножение идеала A справа на элемент $r \in R$ определяет эндоморфизм аддитивной группы A. Так как сумме (произведению) элементов из R соответствует сумма (произведение) соответствующих эндоморфизмов, то мы имеем гомоморфизм кольца R в кольцо эндоморфизмов аддитивной группы A.

Из простоты кольца R следует, что этот гомоморфизм будет или изоморфизмом, или же отображением в нуль. Последнее, однако, невозможно. Из $AR = O$ (т. е. $ar = 0$ для всех $a \in A$, $r \in R$) следовало бы $A^2 = O$, а тогда ненулевой двусторонний идеал

$$B = RA + A,$$

т. е. совокупность элементов вида

$$\sum_{i=1}^{n} r_i a_i + a, \quad r_i \in R, \quad a_i, a \in A, \quad i = 1, 2, \ldots, n$$

(при всевозможных натуральных n), обладал бы свойством $B^2 = O$. Из простоты кольца R вытекает, однако, $B = R$, а гогда $R^2 = O$ в противоречие с тем, что кольцо R по условию ненулевое.

5. Можно считать, следовательно, что R является некоторым кольцом эндоморфизмов (т. е. подкольцом кольца всех эндоморфизмов) аддитивной группы идеала A. Так как правый идеал A минимальный, то в группе A нет нетривиальной подгруппы, допустимой (см. V.1.2) относительно всех эндоморфизмов из R, т. е., как говорят, кольцо эндоморфизмов R *неприводимо.*

Лемма Шура. *Если задано некоторое неприводимое кольцо эндоморфизмов R абелевой группы A, то совокупность K тех эндоморфизмов группы A, которые перестановочны (в смысле умножения эндоморфизмов) с каждым эндоморфизмом из R, будет телом.*

Ясно, в самом деле, что K является подкольцом кольца всех эндоморфизмов группы A и содержит тождественный автоморфизм группы A. Пусть теперь $\alpha \in K$ и $\alpha \neq 0$. Тогда $A\alpha \neq O$ и так как подгруппа $A\alpha$ выдерживает умножение справа на все элементы из R, а кольцо эндоморфизмов R

неприводимое, то $A\alpha = A$. Ядро эндоморфизма α будет R-допустимой подгруппой, т. е., ввиду неприводимости кольца R, оно равно нулю. Эндоморфизм α оказался, следовательно, автоморфизмом, а тогда существует обратный автоморфизм α^{-1}, перестановочный, как и α, со всеми эндоморфизмами из R; поэтому $\alpha^{-1} \in K$.

Применяя лемму Шура к доказываемой нами теореме, мы получаем, что аддитивная группа идеала A является векторным пространством над телом K, а так как всякий эндоморфизм из R перестановочен с каждым эндоморфизмом из K, то R будет некоторым кольцом линейных преобразований этого векторного пространства.

6. *Кольцо R является плотным кольцом линейных преобразований.*

Пусть сперва в A даны элементы a и a', причем $a \neq 0$. Множество aR является правым идеалом кольца R. Если $aR = O$, то множество всех $x \in A$, для которых $xR = O$, будет состоять не только из одного нуля, а так как это правый идеал в R, то, ввиду минимальности A, он совпадает с A. Отсюда следует, однако, $AR = O$, что, как показано в V.5.4, невозможно. Поэтому $aR = A$, а тогда существует такое $r \in R$, что $ar = a'$.

Пусть теперь в A даны линейно независимые над K элементы $a_1, a_2, \ldots, a_n$ и произвольные элементы $a_1', a_2', \ldots, a_n'$, $n > 1$. Предположим, что уже доказано существование таких элементов $r_i \in R$, $i = 1, 2, \ldots, n$, что

$$a_i r_i \neq 0, \quad a_j r_i = 0 \quad \text{при } j = 1, \ldots, i-1, i+1, \ldots, n.$$

По доказанному выше, существуют такие $r_i' \in R$, $i = 1, 2, \ldots, n$, что

$$a_i r_i r_i' = a_i'.$$

Поэтому элемент

$$r = \sum_{i=1}^{n} r_i r_i' \in R$$

обладает тем свойством, что

$$a_i r = a_i', \quad i = 1, 2, \ldots, n.$$

7. Нам нужно, следовательно, доказать, что *для любой линейно независимой над K системы элементов $a_1, a_2, \ldots$*

..., $a_n \in A$, $n > 1$, *существует такой элемент* $r \in R$, *что*

$$a_1 r = \ldots = a_{n-1} r = 0, \qquad a_n r \neq 0.$$

Пусть сперва $n = 2$. Предположим, что из $a_1 r = 0$ всегда следует $a_2 r = 0$. Для всякого $a \in A$ существует такое $r \in R$, что $a = a_1 r$. Если также $a = a_1 r'$, то $a_1 (r - r') = 0$, а поэтому, по предположению, и $a_2 (r - r') = 0$, откуда $a_2 r = a_2 r'$. Мы определим, следовательно, однозначное отображение α группы A в себя, если для $a = a_1 r$ положим

$$a\alpha = a_2 r.$$

Отображение α является эндоморфизмом группы A, так как из $a = a_1 r$, $b = a_1 r'$ следует $a + b = a_1 (r + r')$ и поэтому

$$(a + b)\alpha = a_2 (r + r') = a_2 r + a_2 r' = a\alpha + b\alpha.$$

Эндоморфизм α перестановочен с каждым эндоморфизмом $r_0 \in R$, так как из $a = a_1 r$ следует $ar_0 = a_1 (rr_0)$, откуда

$$(ar_0)\alpha = a_2 (rr_0) = (a\alpha) r_0.$$

Этим доказано, что $\alpha \in K$. Так как

$$(a_1\alpha) r = (a_1 r)\alpha = a_2 r, \quad r \in R,$$

то

$$(a_1\alpha - a_2) r = 0, \qquad r \in R,$$

а поэтому, как мы знаем из V.5.6, $a_1\alpha - a_2 = 0$ в противоречие с линейной независимостью над K системы элементов a_1, a_2.

8. Пусть теперь n произвольное и для $n - 1$ утверждение V.5.7 уже доказано. Существует, следовательно, такое $r' \in R$, что

$$a_1 r' = \ldots = a_{n-2} r' = 0, \qquad a_{n-1} r' \neq 0;$$

обозначим через R' множество всех таких r'. Если элементы $a_{n-1} r'$ и $a_n r'$ линейно независимы над K, то, по доказанному, существует такое $r'' \in R$, что

$$a_{n-1} r' r'' = 0, \qquad a_n r' r'' \neq 0,$$

и можно положить $r = r' r''$.

Пусть, однако,

$$a_{n-1} r' = (a_n r')\beta, \qquad \beta \in K, \ \beta \neq 0. \tag{4}$$

Используя снова индуктивное предположение, можно найти такое $r_0 \in R$, что

$$a_1 r_0 = \ldots = a_{n-2} r_0 = 0, \qquad (a_{n-1} - a_n \beta) r_0 \neq 0. \tag{5}$$

Если $a_n r_0 = 0$, $a_{n-1} r_0 \neq 0$, то найдется такое $r_1 \in R$, что $a_{n-1} r_0 r_1 = a_{n-1} r'$, а тогда можно положить $r = r' - r_0 r_1$, так как $a_n r = a_n r' \neq 0$. Если $a_{n-1} r_0 = 0$, $a_n r_0 \neq 0$, то будет просто $r = r_0$. Если $a_{n-1} r_0$ и $a_n r_0$ линейно независимы, то, так как $r_0 \in R'$, существование искомого r выше уже доказано.

Остается рассмотреть случай

$$a_{n-1} r_0 = (a_n r_0)\gamma, \qquad \gamma \in K, \ \gamma \neq 0; \tag{6}$$

из (5) следует $\beta \neq \gamma$. Существует такое $r_2 \in R$, что

$$a_{n-1} r_0 r_2 = a_{n-1} r'. \tag{7}$$

Тогда, по (6), (7) и (4),

$$a_n r_0 r_2 = a_{n-1} r_0 \gamma^{-1} r_2 = (a_{n-1} r_0 r_2)\gamma^{-1} = a_{n-1} r' \gamma^{-1} = a_n r' \beta \gamma^{-1},$$

откуда

$$a_n (r' \beta \gamma^{-1} - r_0 r_2) = 0. \tag{8}$$

Теперь можно положить $r = r' - r_0 r_2$: ясно, что

$$a_1 r = \ldots = a_{n-1} r = 0;$$

если бы было и $a_n r = 0$, то, ввиду (8), мы имели бы

$$a_n r' = a_n r' \beta \gamma^{-1},$$

а так как $\beta \gamma^{-1} \neq 1$, то получили бы $a_n r' = 0$, что не имеет места.

9. *Кольцо R состоит из линейных преобразований конечного ранга.*

Достаточно доказать, что R содержит хотя бы одно ненулевое линейное преобразование конечного ранга, так как тогда пересечение R с идеалом $R'(A, K)$ кольца $R(A, K)$ (см. V.5.1) будет отличным от нуля идеалом кольца R и, ввиду простоты кольца R, будет совпадать с R.

Мы знаем из V.5.4, что $A^2 \neq O$. Отсюда и из минимальности правого идеала A следует, что для любого данного ненулевого $a \in A$ будет $aA = A$. Существует, в частности, такое $e \in A$, $e \neq 0$, что $ae = a$. Отсюда

$$a(e^2 - e) = 0,$$

а поэтому $e^2 = e$, так как элементы из A, аннулирующие a справа, составляют правый идеал; элемент e является, следовательно, *идемпотентом*. Ясно, что $A = eR$.

Рассматривая теперь e как принадлежащее к кольцу R линейное преобразование векторного пространства A над телом K, покажем, что оно конечного ранга. Именно, подпространство Ae одномерно. Действительно, если бы в нем содержались линейно независимые над K элементы a' и a'', то, ввиду идемпотентности e,

$$a'e = a', \quad a''e = a''. \tag{9}$$

В соответствии с V.5.7 существует такое $r \in R$, что

$$a'r = 0, \qquad a''r \neq 0.$$

Отсюда

$$a'(er) = 0, \qquad a''(er) \neq 0,$$

т. е. $er \neq 0$. Так как $er \in A$, то множество элементов из A аннулирующих a' справа, состоит не только из нуля. Это множество является правым идеалом и поэтому совпадает с A, что противоречит, однако, первому из равенств (9). Теорема Джекобсона доказана.

$*$ Если R_i, $i = 1, 2$, является плотным кольцом линейных преобразований конечного ранга в векторном пространстве V_i над телом K_i и если существует изоморфизм τ между кольцами R_1 и R_2, то между пространствами V_1 и V_2 существует такое полулинейное соответствие σ (см. V.4.1), что для всех $a \in V_1$, $r \in R_1$

$$(ar)\sigma = a\sigma \cdot r\tau.$$

Полные кольца матриц конечных порядков над телами и только они являются ненулевыми простыми ассоциативными кольцами, удовлетворяющими условию минимальности для правых идеалов. $*$

§ 6. Линейные алгебры. Алгебра кватернионов и алгебра Кэли

1. Переходя к операторным кольцам (см. V.1.7), естественно в качестве частного случая рассмотреть кольца, допускающие в качестве кольца операторов (см. V.1.8) некоторое ассоциативное тело. При этом, учитывая сказанное

в V.1.9, мы будем предполагать, что это тело коммутативно, т. е. является полем.

Кольцо R, имеющее поле P своим кольцом операторов, называется *линейной алгеброй* над полем P. Обычно, впрочем, говорят просто об *алгебре* над полем, так как нет опасности смешать это понятие с понятием универсальной алгебры. Если при этом R является ассоциативным телом, то принято говорить об (ассоциативной) *алгебре с делением.*

В неассоциативном случае в соответствии с терминологией, введенной в II.6.1, мы будем называть *алгеброй с делением* всякое кольцо с делением, являющееся алгеброй над данным полем. Аналогичный смысл имеет понятие *алгебры с однозначным делением.* Если же алгеброй над полем является тело, то, как будет показано ниже, это всего лишь означает, что в центре нашего тела выделено некоторое подполе; впрочем, иногда мы будем все же говорить об *алгебре с однозначным делением и с единицей.*

Все сказанное в V.1.7 применимо и к случаю алгебр. Так, *изоморфизмы и гомоморфизмы* алгебр над полем P следует понимать как их P-операторные изоморфизмы и гомоморфизмы. P-допустимые подкольца алгебры называются ее *подалгебрами.* Под *идеалом* алгебры всегда понимается ее P-допустимый идеал. Понятен также смысл термина *факторалгебра.*

Аддитивная группа всякой алгебры R над полем P является векторным пространством над этим полем, как немедленно вытекает из определения алгебры. Векторные пространства поддаются изучению много легче, чем, например, произвольные абелевы группы без операторов. По этой причине теория алгебр во многих отношениях проще и разработана заметно дальше, чем параллельная ей теория колец без операторов.

2. В III.2.9 было введено понятие центра кольца; напомним, что единица кольца, если она существует, содержится в его центре.

Если кольцо R обладает единицей e и если в центре кольца R лежит подполе P, содержащее e, то R будет алгеброй над P.

Действительно, если произведение элементов из R на элементы поля P понимать в смысле умножения, заданного в кольце R, то выполненность всех требований, входящих

в определение алгебры, немедленно вытекает из свойств операций в кольце и определения центра.

Так, поле комплексных чисел является алгеброй с делением над полем действительных чисел. Кольцо многочленов $P[x]$ над полем P будет алгеброй над этим полем, так как многочлены нулевой степени составляют в $P[x]$ подполе, изоморфное полю P и содержащее единицу кольца. Всякое тело будет алгеброй над своим центром, так как последний, как показано в III.2.9, является полем.

Если алгебра R над полем P обладает единицей e, то в центре этой алгебры лежит подполе, содержащее e и изоморфное полю P.

Для доказательства обозначим через P' совокупность элементов вида $e\alpha$, где $\alpha \in P$. Ввиду (7) и (8) из V.1.4 и (11) из V.1.7

$$e(\alpha \pm \beta) = e\alpha \pm e\beta,$$

$$e(\alpha\beta) = (ee)(\alpha\beta) = [(ee)\alpha]\beta = (e\alpha \cdot e)\beta = e\alpha \cdot e\beta.$$

Отсюда следует, что отображение $\alpha \to e\alpha$ будет гомоморфным отображением P на P', притом даже изоморфным, так как P — поле и, ввиду (9) из V.1.4,

$$1 \to e \cdot 1 = e \neq 0,$$

где 1 — единица поля P.

Докажем, наконец, что подполе P' содержится в центре алгебры R. В самом деле, для любых x, $y \in R$

$$(e\alpha)x = (ex)\alpha = (xe)\alpha = x(e\alpha),$$

$$[(e\alpha)x]y = [(ex)\alpha]y = x\alpha \cdot y = (xy)\alpha = [e(xy)]\alpha = (e\alpha)(xy),$$

$$(xy)(e\alpha) = [(xy)e]\alpha = (xy)\alpha = x \cdot y\alpha = x[(ye)\alpha] = x[y(e\alpha)].$$

Теорема доказана.

3. Пусть дана алгебра R над полем P и пусть в аддитивном векторном пространстве этой алгебры выбрана база X, составленная из элементов x_i (где i пробегает некоторое множество индексов). Всякий элемент a из R обладает однозначной записью вида (3′) из V.3.5, т. е. вида

$$a = \sum_{x_i \in X} x_i \alpha^i, \quad \alpha^i \in P,$$

причем сложение элементов из R и их умножение на элемент β поля P сводятся на сложение соответственных коэффициентов и на умножение коэффициентов на β.

Если x_i, $x_j \in X$, то произведение $x_i x_j$, будучи элементом из R, также обладает записью через базу X,

$$x_i x_j = \sum_{x_k \in X} x_k \varepsilon_{ij}^k, \tag{1}$$

причем при данных i и j лишь конечное число коэффициентов ε_{ij}^k может быть отлично от нуля. *Система элементов ε_{ij}^k поля P полностью определяет умножение в алгебре R.* Действительно, для любых α, $\beta \in P$

$$(x_i\alpha)(x_j\beta) = (x_i x_j)(\alpha\beta) = \sum_{x_k \in X} x_k (\varepsilon_{ij}^k \alpha\beta).$$

Если же в R даны произвольные элементы

$$a = \sum_{x_i \in X} x_i \alpha^i, \quad b = \sum_{x_j \in X} x_j \beta^j, \tag{2}$$

то, учитывая, что лишь конечное число коэффициентов a^i и β^j может быть отлично от нуля, на основании законов дистрибутивности получаем

$$ab = \sum_{x_i \in X} \sum_{x_j \in X} (x_i\alpha^i)(x_j\beta^j) = \sum_{i,\ j,\ k} x_k (\varepsilon_{ij}^k \alpha^i \beta^j). \tag{3}$$

Понятно, что при переходе от базы X к другой базе алгебры R числа ε_{ij}^k меняются, т. е. алгебра R будет в этой новой базе определяться «*таблицей умножения*», отличной от (1).

4. *Если в векторном пространстве V над полем P выбрана база X, составленная из элементов x_i, $i \in I$, а в поле P взяты произвольные элементы ε_{ij}^k, i, j, $k \in I$, то существует алгебра над полем P, имеющая V своим аддитивным векторным пространством и задаваемая в базе X таблицей умножения* (1) *с этими коэффициентами ε_{ij}^k.*

Действительно, если для любых элементов a, $b \in V$, записываемых в базе X в виде (2), мы определим произведение формулой (3), то, как легко проверить, будут выполняться и законы дистрибутивности, и требование (11) из V.1.7, а элементы базы X будут перемножаться в соответствии с (1).

Ясно, что алгебра, построенная этим путем, в общем случае (т. е. если выбор чисел ε_{ij}^k не подчинен дополнительным ограничениям) не будет ни ассоциативной, ни коммутативной. Легко проверить, используя законы дистрибутивности, запись элементов алгебры через базу и свойства умножения в поле, что *если в алгебре R над полем P выбрана база X, то для того чтобы эта алгебра была ассоциативной, коммутативной или лиевой* (см. II.2.3), *не только необходимо* (*что очевидно*), *но и достаточно, чтобы для любых x_i, x_j, $x_k \in X$ выполнялись соответственно равенства*

$$(x_i x_j) x_k = x_i (x_j x_k)$$

или

$$x_i x_j = x_j x_i,$$

или, наконец,

$$x_i x_j = -x_j x_i, \quad (x_i x_j) x_k + (x_j x_k) x_i + (x_k x_i) x_j = 0.$$

5. Применим результаты V.3.7 и V.6.4 к построению одного специального типа алгебр. Возьмем произвольный группоид G и произвольное поле P, а затем построим векторное пространство над P, имеющее множество G своей базой. Определяя произведение для элементов этой базы как их произведение в группоиде G, мы получим алгебру, называемую *группоидной алгеброй* группоида G над полем P. Читатель сравнит, конечно, это понятие с понятием целочисленного группоидного кольца из II.4.5.

Группоидная алгебра будет ассоциативной, если группоид G является полугруппой или, в частности, группой. В этом случае говорят о *полугрупповой* и соответственно *групповой алгебре*.

Так, алгебра многочленов $P[x]$ над полем P будет полугрупповой алгеброй: ее базой служит совокупность степеней $x^0 = 1$, x, x^2, ..., x^n, ... неизвестного x, составляющая по умножению полугруппу, изоморфную аддитивной полугруппе целых неотрицательных чисел.

6. Если аддитивное векторное пространство алгебры R над полем P конечномерно (см. V.3.6), то и сама алгебра называется *конечномерной*; ее *размерность* иногда называется также *рангом*.

Так, кольцо матриц P_n над полем P (см. II.2.6) является, ввиду V.6.2, алгеброй над этим полем, так как центр кольца P_n

содержит совокупность скалярных матриц (см. II.4.3), содержащую единичную матрицу и изоморфную полю P. Алгебра матриц P_n имеет при этом конечную размерность n^2, так как ее базу составляют матрицы e_{ij}, $i, j = 1, 2, \ldots, n$, у которых на месте (i, j) стоит 1, а на всех остальных местах — нули. Таблица умножения алгебры P_n в этой базе такова:

$$e_{ij} \cdot e_{jk} = e_{ik},$$
$$e_{ij} \cdot e_{kl} = 0 \quad \text{при} \quad j \neq k.$$

7. Как уже было отмечено в V.6.2, поле комплексных чисел K является алгеброй с делением над полем действительных чисел или, как мы будем говорить, *действительной* алгеброй с делением. Эта алгебра имеет размерность 2, так как числа 1 и i составляют ее базу. Алгебра K имеет в этой базе следующую таблицу умножения:

$$1^2 = 1, \quad 1 \cdot i = i \cdot 1 = i, \quad i^2 = -1.$$

8. Построим теперь четырехмерную действительную ассоциативную алгебру с делением Q, называемую *алгеброй кватернионов*. Это будет алгебра с базой 1, i, j, k и следующей таблицей умножения:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

(4)

При разыскании в этой таблице произведения, например i на j, следует брать пересечение строки с номером i со столбцом с номером j, т. е. $ij = k$.

Из таблицы умножения (4) сразу следует, что элемент 1 является единицей алгебры Q и что эта алгебра некоммутативна. *Алгебра Q будет, однако, ассоциативной*: так как элементы i, j, k входят в таблицу умножения (4) равноправным (с точностью до знаков) образом, то, ввиду V.6.4, достаточно проверить справедливость равенств

$$(ii)\,i = i\,(ii), \quad (ii)\,j = i\,(ij), \quad (ij)\,i = i\,(ji), \quad (ji)\,i = j\,(ii), \quad (ij)\,k = i\,(jk),$$

что предоставляется читателю.

9. Всякий *кватернион* (т. е. элемент алгебры Q) α обладает однозначной записью

$$\alpha = a + ib + jc + kd$$

с действительными коэффициентами a, b, c, d. Кватернион

$$\bar{\alpha} = a - ib - jc - kd$$

называется *сопряженным* кватерниону α. Легко проверяется, что

$$\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}, \quad \overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta} \tag{5}$$

и что

$$\alpha\bar{\alpha} = \bar{\alpha}\alpha = a^2 + b^2 + c^2 + d^2. \tag{6}$$

Неотрицательное действительное число

$$n(\alpha) = \alpha\bar{\alpha} = \bar{\alpha}\alpha, \tag{7}$$

равное нулю лишь при $\alpha = 0$, называется *нормой* кватерниона α. Легко проверить, что

$$n(\alpha\beta) = n(\alpha) \cdot n(\beta), \tag{8}$$

а поэтому *алгебра кватернионов не содержит делителей нуля*. Действительно, ввиду (7) и (5),

$$n(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\bar{\beta}\bar{\alpha} = (\alpha\bar{\alpha}) \cdot n(\beta) = n(\alpha) \cdot n(\beta).$$

Если $\alpha \neq 0$ и поэтому $n(\alpha) \neq 0$, то, по (7),

$$\alpha \cdot \left(\frac{1}{n(\alpha)}\bar{\alpha}\right) = \left(\frac{1}{n(\alpha)}\bar{\alpha}\right) \cdot \alpha = 1.$$

Для всякого отличного от нуля кватерниона α существует, следовательно, обратный кватернион, а поэтому *алгебра кватернионов является телом.*

10. Построим, наконец, одну восьмимерную действительную неассоциативную алгебру с однозначным делением и с единицей, называемую *алгеброй Кэли.*

Рассмотрим всевозможные выражения вида $\alpha + \beta e$, где α и β — кватернионы, а e — новый символ; в частности, вместо $\alpha + \beta e$ при $\beta = 0$ мы будем писать просто α, а при $\alpha = 0$ — просто βe. Определяя для рассматриваемых выражений сложение и умножение на действительное число a равенствами

$$(\alpha + \beta e) + (\gamma + \delta e) = (\alpha + \gamma) + (\beta + \delta) e, \tag{9}$$

$$(\alpha + \beta e)\, a = (\alpha a) + (\beta a)\, e, \tag{10}$$

мы получаем восьмимерное действительное векторное пространство с базой

$$1,\ i,\ j,\ k,\ e,\ ie,\ je,\ ke. \tag{11}$$

Определим в этом пространстве умножение равенством

$$(\alpha+\beta e)(\gamma+\delta e)=(\alpha\gamma-\bar{\delta}\beta)+(\delta\alpha+\beta\bar{\gamma})e. \tag{12}$$

Легко проверяется дистрибутивность этого умножения относительно сложения (9), а также, ввиду (10), справедливость равенств

$$[(\alpha+\beta e)(\gamma+\delta e)]\,a=[(\alpha+\beta e)\,a]\,(\gamma+\delta e)=$$

$$=(\alpha+\beta e)\,[(\gamma+\delta e)\,a].$$

Таблица умножения полученной алгебры Кэли в базе (11) без труда выводится из (12). Это будет следующая таблица:

	1	i	j	k	e	ie	je	ke
1	1	i	j	k	e	ie	je	ke
i	i	-1	k	$-j$	ie	$-e$	$-ke$	je
j	j	$-k$	-1	i	je	ke	$-e$	$-ie$
k	k	j	$-i$	-1	ke	$-je$	ie	$-e$
e	e	$-ie$	$-je$	$-ke$	-1	i	j	k
ie	ie	e	$-ke$	je	$-i$	-1	$-k$	j
je	je	ke	e	$-ie$	$-j$	k	-1	$-i$
ke	ke	$-je$	ie	e	$-k$	$-j$	i	-1

Мы видим, что элементы вида $\alpha=\alpha+0e$ составляют в алгебре Кэли подалгебру, изоморфную алгебре кватернионов. С другой стороны, из (9) и (12) вытекает, что в записи $\alpha+\beta e$ элементов алгебры Кэли и сложение, и умножение можно понимать в смысле операций, определенных в этой алгебре.

Алгебра Кэли не является ни коммутативной, ни ассоциативной. Так,

$$(ij)\,e=ke,\qquad i\,(je)=-ke.$$

11. Если $\xi=\alpha+\beta e$ — элемент алгебры Кэли, то назовем *сопряженным* ему элемент

$$\bar{\xi}=\bar{\alpha}-\beta e.$$

На основании (12) и (5) легко проверяется, что для любых элементов ξ и η алгебры Кэли

$$\overline{\xi\eta} = \overline{\eta}\,\overline{\xi}, \quad \overline{\xi+\eta} = \overline{\xi} + \overline{\eta} \tag{13}$$

и что для $\xi = \alpha + \beta e$

$$\xi\overline{\xi} = \overline{\xi}\xi = \alpha\overline{\alpha} + \beta\overline{\beta} = n(\alpha) + n(\beta). \tag{14}$$

Это неотрицательное действительное число, равное нулю лишь при $\xi = 0$, называется *нормой* элемента ξ и обозначается через $n(\xi)$.

Если $\xi = \alpha + \beta e$, $\eta = \gamma + \delta e$, то из (12) и (14) следует, ввиду (5), что

$$n(\xi\eta) = (\alpha\gamma - \overline{\delta}\beta)(\overline{\gamma}\overline{\alpha} - \overline{\beta}\delta) + (\delta\alpha + \beta\overline{\gamma})(\overline{\alpha}\overline{\delta} + \gamma\overline{\beta}) =$$

$$= n(\alpha)\,n(\gamma) + n(\beta)\,n(\delta) + n(\alpha)\,n(\delta) + n(\beta)\,n(\gamma) + a - b,$$

где

$$a = \delta\alpha\gamma\overline{\beta} + \overline{\beta}\gamma\overline{\alpha}\overline{\delta},$$

$$b = \alpha\gamma\overline{\beta}\delta + \overline{\delta}\overline{\beta}\overline{\alpha}\overline{\gamma}.$$

Так как, по (5), вторые слагаемые в выражениях для a и b сопряжены с первыми слагаемыми, то a и b будут действительными числами. Если $\delta = 0$, то, очевидно, $a = b = 0$ и поэтому $a - b = 0$. Если же $\delta \neq 0$ и поэтому $n(\delta) \neq 0$, то, ввиду действительности числа a,

$$an(\delta) = \overline{\delta}a\delta = bn(\delta),$$

откуда $a = b$, т. е. снова $a - b = 0$.

Таким образом,

$$n(\xi\eta) = [n(\alpha) + n(\beta)]\,[n(\gamma) + n(\delta)] = n(\xi)\,n(\eta). \tag{15}$$

Отсюда следует, что *алгебра Кэли не содержит делителей нуля.*

12. Равенство (12) показывает, что элемент $1 = 1 + 0e$ является единицей алгебры Кэли.

С другой стороны, если даны элементы $\xi = \alpha + \beta e$ и $\eta = \gamma + \delta e$, причем $\xi \neq 0$, то уравнение

$$\xi\zeta = \eta \tag{16}$$

обладает решением, притом единственным ввиду отсутствия делителей нуля. Именно,

$$\zeta = \frac{1}{n(\xi)}\bar{\xi}\eta = \frac{1}{n(\xi)}[(\bar{\alpha}\gamma + \bar{\delta}\beta) + (\delta\bar{\alpha} - \beta\bar{\gamma})e].$$

Читатель без труда проверит, используя (12) и (5), что элемент ζ действительно удовлетворяет уравнению (16). Аналогично единственным решением уравнения

$$\zeta\xi = \eta, \quad \xi \neq 0,$$

служит элемент

$$\zeta = \frac{1}{n(\xi)}\eta\bar{\xi}.$$

Мы получаем, что *алгебра Кэли является (неассоциативным) телом.*

§ 7. Альтернативные кольца. Теорема Артина

1. Алгебру кватернионов и алгебру Кэли вовсе не следует считать случайными примерами действительных алгебр с делением — их особая роль устанавливается во многих теоремах, некоторые из которых будут доказаны или упомянуты в следующем параграфе, а также в §§ 6 и 10 следующей главы.

Укажем сначала одну простую классификацию всех колец. Закон ассоциативности связывает, как известно, три элемента, а поэтому *всякое кольцо, все подкольца которого, порожденные тремя элементами, ассоциативны, само будет ассоциативным.* Более широкий класс колец составляют *альтернативные кольца,* т. е. те кольца, в которых ассоциативны все подкольца, порожденные д в у м я элементами. Еще более широким будет класс *колец с ассоциативными степенями,* т. е. тех колец, в которых ассоциативны все подкольца, порожденные о д н и м элементом; этот класс не исчерпывает, конечно, всех колец.

2. Если a, b, c — элементы некоторого кольца R, то назовем *ассоциатором* этих элементов элемент

$$[a, b, c] = (ab)c - a(bc). \tag{1}$$

Очевидно, что

$$[a, b, c] = 0$$

тогда и только тогда, если для элементов a, b, c выполняется закон ассоциативности

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

Из (1) следует, что

$$[a+a', b, c] = [a, b, c] + [a', b, c]; \tag{2}$$

аналогичные равенства справедливы и для мест, занимаемых в ассоциаторе элементами b и c. С другой стороны,

$$[-a, b, c] = -[a, b, c].$$

На основании (1) легко проверяется следующее равенство, справедливое для любых элементов a, b, c, $d \in R$:

$$[ab, c, d] - [a, bc, d] + [a, b, cd] = a[b, c, d] + [a, b, c]d. \tag{3}$$

3. Теорема Артина. *Кольцо R тогда и только тогда альтернативно, если для любых a, $b \in R$ имеют место равенства*

$$(aa)b = a(ab), \quad (ba)a = b(aa)\ ^{1}). \tag{4}$$

Очевидно, что в альтернативном кольце условия (4) выполняются. Будем считать поэтому, что дано кольцо R, в котором для любых элементов a и b выполняются равенства (4); эти равенства могут быть записаны в виде

$$[a, a, b] = 0, \quad [b, a, a] = 0. \tag{5}$$

4. *В кольце R для любых a и b справедливо равенство*

$$[a, b, a] = 0. \tag{6}$$

Действительно, ввиду (5) и (2),

$$0 = [a, a+b, a+b] = [a, a, a] + [a, a, b] + [a, b, a] + [a, b, b] = [a, b, a].$$

Если в кольце R элементы a, b, c подвергнуты некоторой перестановке, то ассоциатор $[a, b, c]$ не меняется, если эта перестановка четная, и меняет знак, если она нечетная.

---

[1]) Читатель может принять тождества (4) в качестве определения альтернативного кольца и без ущерба для дальнейшего опустить доказательство теоремы Артина. Мы видим, что альтернативные кольца составляют примитивный класс универсальных алгебр (см. III.6.3).

Достаточно, как известно, рассмотреть лишь случай транспозиций двух элементов. Ввиду (5) и (2)

$$0=[a,\ b+c,\ b+c]=[a,\ b,\ b]+[a,\ b,\ c]+[a,\ c,\ b]+$$
$$+[a,\ c,\ c]=[a,\ b,\ c]+[a,\ c,\ b],$$

откуда

$$[a,\ b,\ c]=-[a,\ c,\ b].$$

Аналогично доказываются равенства

$$[a,\ b,\ c]=-[b,\ a,\ c]$$

и, ввиду (6),

$$[a,\ b,\ c]=-[c,\ b,\ a].$$

5. Если A, B, C — подмножества нашего кольца R, то условимся писать

$$[A,\ B,\ C]=O,$$

если $[a,\ b,\ c]=0$ для всех $a\in A$, $b\in B$, $c\in C$.

Подмножество A кольца R назовем *α-множеством*, если

$$[A,\ A,\ R]=O, \tag{7}$$

и поэтому, на основании доказанного выше,

$$[A,\ R,\ A]=O,\quad [R,\ A,\ A]=O. \tag{8}$$

Из (5) следует, что множество, состоящее из одного элемента, будет α-множеством.

Подкольцо кольца R, порожденное α-множеством A, само будет α-множеством, т. е., короче, будет α-подкольцом.

Действительно, из (2) следует, что, добавляя к множеству A всевозможные суммы и разности его элементов, мы снова получим α-множество. Покажем, что это же имеет место и тогда, когда к A добавляются произведения всевозможных пар его элементов. В самом деле, если a_1, a_2, a_3, $a_4\in A$, то, ввиду (3),

$$[a_1a_2,\ x,\ a_3]-[a_1,\ a_2x,\ a_3]+[a_1,\ a_2,\ xa_3]=$$
$$=a_1[a_2,\ x,\ a_3]+[a_1,\ a_2,\ x]a_3,$$

откуда, ввиду (7) и (8),

$$[a_1a_2,\ x,\ a_3]=0. \tag{9}$$

Далее, снова по (3),

$$[a_1a_2,\ x,\ a_3a_4]-[a_1,\ a_2x,\ a_3a_4]+[a_1,\ a_2,\ x(a_3a_4)]=$$
$$=a_1[a_2,\ x,\ a_3a_4]+[a_1,\ a_2,\ x](a_3a_4),$$

откуда, ввиду (7), (8) и (9),

$$[a_1a_2,\ x,\ a_3a_4]=0.$$

Таким образом, если мы, начиная от множества A, будем поочередно добавлять к построенному α-множеству или все суммы и разности его элементов, или же все произведения пар его элементов, мы получим в R возрастающую последовательность α-множеств. Объединение этой последовательности будет, конечно, α-множеством и вместе с тем оно будет совпадать с подкольцом, порожденным множеством A.

Из этого результата вытекает, что *всякое подкольцо кольца R, порожденное одним элементом, будет α-подкольцом и поэтому будет ассоциативным.*

6. Если A и B будут α-подкольцами кольца R, то обозначим через C множество всех таких элементов c из R, что

$$[A,\ B,\ c]=O.$$

Ясно, что

$$C\supseteq(A\cup B) \tag{10}$$

и что C замкнуто относительно сложения и вычитания.

Если $c\in C$, то для любых $a'\in A$ и $b'\in B$ имеют место включения

$$a'c,\ ca',\ b'c,\ cb'\in C.$$

Действительно, если $a\in A$, $b\in B$, то, по (3),

$$[aa',\ c,\ b]-[a,\ a'c,\ b]+[a,\ a',\ cb]=a[a',\ c,\ b]+[a,\ a',\ c]b,$$
$$[bc,\ a',\ a]-[b,\ ca',\ a]+[b,\ c,\ a'a]=b[c,\ a',\ a]+[b,\ c,\ a']a$$

или, учитывая, что A является α-подкольцом, а $c\in C$,

$$[a,\ a'c,\ b]=0,$$
$$[b,\ ca',\ a]=0,$$

т. е. $a'c\in C$, $ca'\in C$. Так же доказываются и два других включения.

Ввиду II.3.7 любой элемент подкольца $\{A,\ B\}$ представим в виде суммы произведений вида $w=x_1x_2\ldots x_n$, где всякое x_i, $i=1,\ 2,\ \ldots,\ n$, принадлежит к A или к B; назовем n *длиной* этого произведения, $n=l(w)$. В произведении w некоторым способом распределены скобки, причем всякая скобка является произведением ровно двух меньших скобок. Произведение w длины n назовем *нормальным элементом*, если

всякая скобка длины k, $2 \leqslant k \leqslant n$, входящая в состав этого произведения, является произведением скобки длины $k-1$ на элемент из A или из B, слева или справа. Таким образом, произведение $(ab)(b'a')$ не будет нормальным, а произведение $b'[(ab)a']$ нормально.

Из доказанного выше следует, ввиду (10), что всякий нормальный элемент w принадлежит к множеству C, т. е. для всех $a \in A$, $b \in B$

$$[a, b, w] = 0. \tag{11}$$

7. *Всякое произведение нормальных элементов представимо в виде суммы нормальных элементов.*

Достаточно доказать это для произведения двух нормальных элементов v и w. Будем вести доказательство индукцией по длине элемента v, так как при $l(v) = 1$ нормальность произведения vw очевидна.

Если $v = v'a$, $l(v') = l(v) - 1$, $a \in A$, то

$$vw = (v'a)w = v'(aw) + [v', a, w] =$$
$$= v'(aw) - [v', w, a] = v'(aw) - (v'w)a + v'(wa),$$

но каждое из трех слагаемых полученной суммы представимо, по индуктивному предположению, в виде суммы нормальных элементов. На этот случай сводится и случай $v = av'$:

$$vw = (av')w = a(v'w) + [a, v', w] =$$
$$= a(v'w) - (v', a, w) = a(v'w) - (v'a)w + v'(aw).$$

Отсюда следует, что *всякий элемент из* $\{A, B\}$ *представим в виде суммы нормальных элементов.*

8. *Если* v, w *— нормальные элементы, то для любых* $a \in A$, $b \in B$

$$[a, v, w] = [b, v, w] = 0. \tag{12}$$

Если $l(v) = 1$, то (12) следует из (11). Будем поэтому вести доказательство индукцией по длине элемента v. Если $v = b'v'$, где $l(v') = l(v) - 1$, $b' \in B$, то, по (3),

$$[b'v', w, a] - [b', v'w, a] + [b', v', wa] =$$
$$= b'[v', w, a] + [b', v', w]a.$$

Отсюда, используя индуктивное предположение, а также (11) и результат, доказанный в предшествующем пункте, мы по-

лучаем

$$[b'v', w, a] = [v, w, a] = [a, v, w] = 0.$$

В случаях $v = v'a'$, $v = a'v'$ и $v = v'b'$ также применяется тождество (3), причем в качестве элементов a, b, c, d нужно соответственно брать w, v', a', a или a, a', v', w, или, наконец, v', b', w, a.

9. *Если u, v, w — нормальные элементы, то*

$$[u, v, w] = 0. \tag{13}$$

Ввиду (12) можно вести доказательство индукцией по длине элемента u. Если $u = u'a$, $l(u') = l(u) - 1$, $a \in A$, то, по (3),

$$[u'a, v, w] - [u', av, w] + [u', a, vw] = u'[a, v, w] + [u', a, v]w$$

или, используя индуктивное предположение и результат из V 7.7,

$$[u'a, v, w] = [u, v, w] = 0.$$

Так же рассматриваются и другие возможные случаи.

Отсюда, учитывая, что всякий элемент подкольца $\{A, B\}$ является суммой нормальных элементов, мы получаем, что *подкольцо $\{A, B\}$, порожденное α-подкольцами A и B, будет ассоциативным.* Если же в качестве A и B мы возьмем подкольца, каждое из которых порождено одним элементом, то получим, ввиду последнего результата из V.7.5, что *всякое подкольцо кольца R, порожденное двумя элементами, ассоциативно*, и этим закончим доказательство теоремы Артина.

*Если аддитивная группа кольца R не содержит отличных от нуля элементов конечного порядка, то R тогда и только тогда будет кольцом с ассоциативными степенями, если для всякого элемента a из R

$$(aa)a = a(aa), \qquad [(aa)a]a = (aa)(aa).$$

[А л б е р т, Summa Bras. Math. **2** (1948), 21—33; см. также А. Т. Г а й н о в, Успехи мат. наук **12**:3 (1957), 141—146].*

10. Докажем теперь, *что алгебра Кэли альтернативна.*

Достаточно проверить, ввиду теоремы Артина, что в алгебре Кэли выполняются равенства (4). Проверим хотя бы первое из них. Если

$$\xi = \alpha + \beta e, \quad \eta = \gamma + \delta e,$$

то, по (12) из V.6.10,

$$(\xi\xi)\,\eta = [(\alpha^2 - \bar{\beta}\beta)\,\gamma - \bar{\delta}\,(\beta\alpha + \beta\bar{\alpha})] + [\delta\,(\alpha^2 - \bar{\beta}\beta) + (\beta\alpha + \beta\bar{\alpha})\bar{\gamma}]\,e,$$

$$\xi\,(\xi\eta) = [\alpha\,(\alpha\gamma - \bar{\delta}\beta) - (\overline{\delta\alpha + \beta\bar{\gamma}})\,\beta] + [(\delta\alpha + \beta\bar{\gamma})\alpha + \beta\,(\overline{\alpha\gamma - \bar{\delta}\beta})]\,e.$$

Правые части этих равенств будут, однако, совпадать, как легко показать на основании (5) из V.6.9, если учесть, что и $\alpha + \bar{\alpha}$, и $\beta\bar{\beta} = \bar{\beta}\beta$ являются действительными числами и поэтому перестановочны с любым кватернионом.

§ 8. Обобщенная теорема Фробениуса

1. *Поле действительных чисел и поле комплексных чисел являются единственными конечномерными действительными ассоциативно-коммутативными алгебрами без делителей нуля.*

Тело кватернионов является единственной конечномерной действительной ассоциативной, но не коммутативной алгеброй без делителей нуля.

Алгебра Кэли является единственной конечномерной действительной альтернативной, но не ассоциативной алгеброй без делителей нуля.

Объединение первых двух теорем называется *теоремой Фробениуса*; объединение всех трех теорем мы будем называть *обобщенной теоремой Фробениуса.*

2. Докажем сперва следующую общую теорему:

Всякая конечномерная алгебра R без делителей нуля над произвольным полем P является алгеброй с однозначным делением.

Докажем однозначную разрешимость хотя бы первого из уравнений

$$ax = b, \quad ya = b, \tag{1}$$

где $a \neq 0$. Обозначим через aR совокупность элементов вида ar для всевозможных r из R. Ясно, что aR будет линейным подпространством аддитивного векторного пространства алгебры R. Если это подпространство отлично от всей алгебры R, то оно имеет строго меньшую размерность. Взяв, следовательно, любую базу

$$x_1, x_2, \ldots, x_n$$

алгебры R, мы получим, что элементы

$$ax_1,\ ax_2,\ \ldots,\ ax_n$$

линейно зависимы, т. е. в поле P существуют такие элементы $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n$, не все равные нулю, что

$$(ax_1)\alpha_1+(ax_2)\alpha_2+\ldots+(ax_n)\alpha_n=0.$$

Отсюда, однако, следует

$$a(x_1\alpha_1+x_2\alpha_2+\ldots+x_n\alpha_n)=0,$$

где оба множителя отличны от нуля, что противоречит отсутствию в алгебре R делителей нуля.

Мы получаем, что $aR=R$. Существует, следовательно, такой элемент $r\in R$, что

$$ar=b,$$

т. е. первое из уравнений (1) действительно оказалось разрешимым. Единственность его решения вытекает из отсутствия в алгебре R делителей нуля. Теорема доказана.

Для дальнейшего отметим, что в альтернативной алгебре ассоциативно не только всякое подкольцо, порожденное двумя элементами, но даже всякая подалгебра с двумя образующими — достаточно учесть, как выражаются элементы указанной подалгебры через элементы подкольца, порожденного этими же двумя образующими.

Всякая альтернативная конечномерная алгебра с однозначным делением R над произвольным полем P обладает единицей.

В ассоциативном случае утверждение этой теоремы немедленно следует из II.2.10. Если же алгебра R лишь альтернативна, то всякая ее подалгебра с двумя образующими будет ассоциативной конечномерной алгеброй без делителей нуля, т. е., по предшествующей теореме, алгеброй с делением и, следовательно, обладает единицей. Пусть, однако, две такие подалгебры обладают различными единицами, e_1 и e_2. Подалгебра, порожденная этими двумя элементами, сама будет ассоциативной алгеброй с делением, и мы приходим к противоречию, так как в ассоциативном теле не может быть двух различных ненулевых *идемпотентных элементов*, т. е. элементов, равных своему квадрату.

3. Мы можем теперь, приступая к доказательству обобщенной теоремы Фробениуса, считать, что нам дана действи-

тельная альтернативная (в частности, ассоциативная или даже ассоциативно-коммутативная) алгебра с однозначным делением R конечной размерности n, обладающая единицей.

Как показано в V.6.2, в центре алгебры R содержится подполе D, изоморфное полю действительных чисел — это будет совокупность элементов, кратных единице 1 алгебры R.

Если элемент a алгебры R лежит вне подполя D, то порожденная им подалгебра $\{a\}$ содержит это подполе и изоморфна полю комплексных чисел.

В самом деле, ввиду альтернативности алгебры R, подалгебра $\{a\}$ ассоциативна, т. е. можно в обычном смысле говорить о степенях элемента a. Так как алгебра R имеет размерность n, то элементы

$$1,\ a,\ a^2,\ \ldots,\ a^n$$

линейно зависимы. Существует, следовательно, такой многочлен $f(x)$ с действительными коэффициентами, степени не выше n, который обращается в нуль элементом a. Из основной теоремы алгебры комплексных чисел следует, что $f(x)$ разлагается на линейные и неприводимые квадратные множители с действительными коэффициентами, а так как в алгебре R нет делителей нуля, то элемент a обращает в нуль один из этих множителей; обозначим его через $\varphi(x)$.

Так как a лежит вне подполя D и поэтому не может удовлетворять никакому уравнению первой степени с действительными коэффициентами, то

$$\varphi(x) = x^2 + \beta x + \gamma, \quad \gamma \neq 0. \tag{2}$$

Таким образом,

$$a^2 + \beta a + \gamma = 0, \tag{3}$$

т. е. $\gamma \in \{a\}$ и поэтому в подалгебре $\{a\}$ содержится все подполе D. Из (3) следует, что подалгебра $\{a\}$ двумерна и что ее базу составляют элементы 1, a, причем

$$a^2 = -\gamma - \beta a.$$

Обозначим, с другой стороны, через α комплексное число, являющееся корнем квадратного трехчлена (2). Число α не является действительным, а поэтому числа 1, α составляют базу алгебры комплексных чисел. Таблица умножения, определяющая алгебру комплексных чисел в этой базе, совпадает, очевидно, с таблицей умножения, определяющей подалгебру $\{a\}$ в базе 1, a. Отсюда, по V.6.3, вытекает изоморфизм подалгебры $\{a\}$ с полем комплексных чисел.

4. *Если элементы a и b алгебры R лежат вне подполя D и порождают различные подалгебры $\{a\}$, $\{b\}$, то подалгебра $\{a, b\}$ изоморфна алгебре кватернионов.*

Так как подалгебра $\{a\}$ изоморфна полю комплексных чисел, то в ней можно выбрать базу 1, i, причем

$$i^2 = -1. \tag{4}$$

Аналогично в подалгебре $\{b\}$ существует база 1, j_0, где

$$j_0^2 = -1. \tag{5}$$

Ясно, что $\{i\} = \{a\}$, $\{j_0\} = \{b\}$, откуда $\{i, j_0\} = \{a, b\}$ и, так как $j_0 \notin \{a\}$, элементы 1, i, j_0 линейно независимы.

Каждый из элементов $i + j_0$, $i - j_0$ лежит поэтому вне подполя D и, следовательно, должен удовлетворять некоторому неприводимому квадратному многочлену с действительными коэффициентами, а тогда квадраты этих элементов должны выражаться через их первые степени и единицу. Существуют, следовательно, такие действительные числа α, β, γ, δ, что

$$\begin{aligned}(i + j_0)^2 &= -2 + (ij_0 + j_0 i) = \alpha(i + j_0) + \beta,\\ (i - j_0)^2 &= -2 - (ij_0 + j_0 i) = \gamma(i - j_0) + \delta.\end{aligned} \tag{6}$$

Складывая эти равенства, получаем

$$-4 = (\alpha + \gamma) i + (\alpha - \gamma) j_0 + (\beta + \delta),$$

откуда, ввиду линейной независимости элементов 1, i, j_0, следует $\alpha + \gamma = \alpha - \gamma = 0$, т. е. $\alpha = \gamma = 0$. Из (6) мы получаем теперь, что элемент $ij_0 + j_0 i$ будет действительным числом, которое обозначим через 2μ; именно,

$$ij_0 + j_0 i = 2\mu = \beta + 2 = -(\delta + 2). \tag{7}$$

Так как квадратные трехчлены, которым удовлетворяют элементы $i + j_0$ и $i - j_0$, неприводимы, то, ввиду $\alpha = \gamma = 0$, должно быть $\beta < 0$, $\delta < 0$, откуда, по (7),

$$-1 < \mu < 1.$$

Число

$$\nu = \frac{1}{\sqrt{1 - \mu^2}} \tag{8}$$

будет, следовательно, отличным от нуля действительным числом.

Рассмотрим теперь лежащий в подалгебре $\{a, b\}$ элемент

$$j = \mu\nu i + \nu j_0.$$

Так как $\nu \neq 0$, то элементы 1, i, j линейно независимы, а на основании (7) и (8) легко проверяются равенства

$$j^2 = -1, \tag{9}$$

$$ij + ji = 0. \tag{10}$$

Введем обозначение

$$k = ij = -ji. \tag{11}$$

Если бы имело место равенство

$$k = \alpha + \beta i + \gamma j$$

с действительными коэффициентами α, β, γ, то, умножая обе его части справа на i, мы получили бы, ввиду (11),

$$j = \alpha i - \beta - \gamma k = \alpha i - \beta - \gamma(\alpha + \beta i + \gamma j).$$

Приравнивая здесь, однако, коэффициенты при j, мы пришли бы к равенству

$$1 = -\gamma^2,$$

что невозможно, так как число γ действительное.

Элементы 1, i, j, k оказываются, следовательно, линейно независимыми. Эти элементы лежат в ассоциативной (ввиду альтернативности алгебры R) подалгебре $\{a, b\}$ и даже порождают эту подалгебру. Поэтому, на основании (4), (9) и (11), без труда проверяется, что для элементов 1, i, j, k выполняются все равенства (4) из V.6.8. Так, например,

$$k^2 = (ij)(-ji) = -i(j^2)i = i^2 = -1,$$

$$jk = j(-ji) = -(j^2)i = i.$$

Этим показано, что элементы 1, i, j, k составляют базу порождаемой ими подалгебры $\{a, b\}$ и что эта подалгебра изоморфна алгебре кватернионов.

Таким образом, первая из теорем V.8.1 уже доказана.

5. Если бы доказательство второй из теорем V.8.1 было нашей конечной целью, то нам осталось бы проделать весьма немногое. Пусть рассматриваемая алгебра R ассоциативна и пусть в ней найдена подалгебра $\{a, b\}$, изоморфная алгебре кватернионов, и лежащий вне ее элемент c. Обозначим через 1, i, j, k базу подалгебры $\{a, b\}$ с обычной для алгебры кватернионов таблицей умножения — будем называть такую базу *канонической*. С другой стороны, подалгебра $\{c\}$ при наших предположениях изоморфна полю комплексных

чисел и поэтому в ней содержится такой элемент e, что

$$e^2 = -1,$$

причем $\{e\} = \{c\}$.

Повторяя рассуждения, использованные при выводе равенства (7), можно утверждать существование таких действительных чисел α, β, γ, что

$$ie + ei = \alpha, \quad je + ej = \beta, \quad ke + ek = \gamma.$$

Отсюда, используя ассоциативность алгебры R, получаем

$$ek = (ei)\,j = \alpha j - i\,(ej) = \alpha j - \beta i + (ij)\,e =$$
$$= \alpha j - \beta i + ke = \alpha j - \beta i + \gamma - ek,$$

т. е.

$$2ek = \alpha j - \beta i + \gamma,$$

или, после умножения справа на k,

$$-2e = \alpha i + \beta j + \gamma k.$$

Это приводит, однако, к включению $e \in \{a, b\}$, что невозможно. Вторая из теорем V.8.1 доказана.

6. Возвращаемся к доказательству обобщенной теоремы Фробениуса.

Если элементы a, b и c алгебры R таковы, что $\{a, b\}$, $\{a, c\}$ и $\{b, c\}$ являются различными подалгебрами, изоморфными телу кватернионов, то подалгебра $\{a, b, c\}$ изоморфна алгебре Кэли.

Так как подалгебра $\{a, b\}$ изоморфна телу кватернионов, то она обладает канонической базой $1, i, j, k$. С другой стороны, в подалгебре $\{c\}$ содержится такой элемент e_0, что

$$e_0^2 = -1,$$

причем $\{e_0\} = \{c\}$.

Подалгебра $\{i, e_0\}$ изоморфна телу кватернионов, так как из $\{i\} = \{e_0\}$ следовало бы $c \in \{a, b\}$. Поэтому, как показано в V.8.4, существует такой элемент

$$e_1 = \alpha_1 i + \beta_1 e_0 \tag{12}$$

с действительными α_1 и β_1, причем $\beta_1 \neq 0$, что элементы 1, i, e_1, ie_1 составляют каноническую базу подалгебры $\{i, e_0\}$.

Из $\{j\} = \{e_1\}$ следовало бы, ввиду (12), что $e_0 \in \{a, b\}$, что невозможно. Подалгебра $\{j, e_1\}$ изоморфна, следова-

тельно, телу кватернионов и поэтому в ней существует такой элемент

$$e_2 = \alpha_2 j + \beta_2 e_1 \tag{13}$$

с действительными α_2 и β_2, причем $\beta_2 \neq 0$, что элементы 1, j, e_2, je_2 составляют каноническую базу подалгебры $\{j, e_2\}$.

Покажем, что *подалгебра* $\{i, e_2\}$ *также изоморфна телу кватернионов и имеет систему элементов* 1, i, e_2, ie_2 *своей канонической базой.* Действительно, из $\{i\} = \{e_2\}$ следовало бы, ввиду (13) и (12), что $e_1 \in \{a, b\}$, откуда и $e_0 \in \{a, b\}$, что невозможно. Этим доказано первое утверждение. Так как, далее, уже известно, что

$$i^2 = e_2^2 = -1,$$

то для доказательства второго утверждения достаточно, как мы знаем из V.8.4, установить справедливость равенства

$$ie_2 + e_2 i = 0.$$

Учитывая, однако, что имеют место равенства

$$ij + ji = 0, \quad ie_1 + e_1 i = 0,$$

мы получаем

$$ie_2 + e_2 i = i(\alpha_2 j + \beta_2 e_1) + (\alpha_2 j + \beta_2 e_1) i =$$
$$= \alpha_2 (ij + ji) + \beta_2 (ie_1 + e_1 i) = 0.$$

7. Как и выше, подалгебра $\{k, e_2\}$ изоморфна телу кватернионов и обладает канонической базой 1, k, e, ke, где

$$e = \alpha_3 k + \beta_3 e_2 \tag{14}$$

с действительными α_3 и β_3, причем $\beta_3 \neq 0$. Отметим, что $\{k, e_2\} = \{k, e\}$. Таким же путем, как в предшествующем пункте, проверяется, что подалгебры $\{i, e\}$ и $\{j, e\}$ также изоморфны телу кватернионов и имеют своими каноническими базами соответственно системы элементов 1, i, e, ie и 1, j, e, je.

8. *Система элементов*

$$1, i, j, k, e, ie, je, ke \tag{15}$$

линейно независима.

Действительно, если бы она была линейно зависимой, то в подалгебре $\{i, j\} = \{a, b\}$ существовали бы такие эле-

менты u, v, причем $v \neq 0$, что

$$u = ve. \tag{16}$$

Так как подалгебра $\{v\}$ изоморфна полю комплексных или действительных чисел, то элемент v^{-1} содержится в ней и поэтому в ассоциативной подалгебре $\{v, e\}$. Отсюда

$$v^{-1}(ve) = (v^{-1}v)\, e = e,$$

т. е. из (16) мы получили бы

$$e = v^{-1}u \in \{a, b\},$$

что невозможно.

9. *Для элементов* (15) *выполняется таблица умножения алгебры Кэли* (см. V.6.10).

Мы знаем, что системы элементов

$$(1, i, j, k),\ (1, i, e, ie),\ (1, j, e, je),\ (1, k, e, ke) \tag{17}$$

являются каноническими базами порождаемых ими подалгебр, изоморфных алгебре кватернионов. Ввиду этого в указанной таблице остается проверить немного мест. Покажем на нескольких типичных случаях, как это делается.

Так как подалгебра $\{e+i, j\}$ ассоциативна, то

$$[j(e+i)](e+i) = j[(e+i)(e+i)],$$

откуда, используя сказанное выше о системах (17), получаем

$$-j + (je)\, i - ke - j = -2j,$$

т. е.

$$(je)\, i = ke. \tag{18}$$

Далее, из равенства

$$(e+i)[j(e+i)] = [(e+i)j](e+i)$$

получаем, используя (18), что

$$i(je) = -ke. \tag{19}$$

Наконец, из ассоциативности подалгебры $\{k, i+je\}$ вытекает равенство

$$[(i+je)(i+je)]\, k = (i+je)[(i+je)\, k],$$

из которого, используя равенства (18), (19) и аналогично доказываемое равенство

$$(je)\, k = -ie,$$

мы получаем

$$(je)(ie) = k.$$

Этим путем будет показано, что элементы (15) составляют базу порождаемой ими подалгебры $\{a, b, c\}$ и что эта подалгебра изоморфна алгебре Кэли.

Условимся базу подалгебры Кэли, удовлетворяющую таблице умножения из V.6.10, называть *канонической.*

10. Предположим, наконец, что алгебра R содержит как подалгебру, изоморфную алгебре Кэли и имеющую своей канонической базой систему элементов

$$1,\ i,\ j,\ k,\ e,\ ie,\ je,\ ke,$$

так и некоторый элемент, лежащий вне этой подалгебры. Тогда, обобщая рассмотрения, проведенные в предшествующих пунктах, мы нашли бы в алгебре R такой элемент f, что каждая из следующих систем элементов порождала бы подалгебру, изоморфную алгебре Кэли, и служила бы для нее канонической базой:

$$\begin{array}{llll} 1, & i, & j, k, & f, if, \quad jf, kf; \\ 1, & i, & e, ie, & f, if, \quad ef, (ie)f; \\ 1, & j, & e, je, & f, jf, \quad ef, (je)f; \\ 1, & je, & i, ke, & f, (je)f, if, (ke)f. \end{array}$$

Соответствующие построения весьма громоздки, но не представляют принципиальных трудностей и поэтому могут быть предоставлены читателю.

Из каноничности указанных баз вытекают следующие равенства:

$$\begin{array}{ll} e^2 = -1, & (if)^2 = -1, \\ (jf)(if) = k, & k(if) = -jf, \\ e(if) = (ie)f, & (if)e = -(ie)f, \\ (jf)e = -(je)f, & [(je)f]e = jf, \\ \multicolumn{2}{c}{[(je)f](if) = -ke.} \end{array}$$

Используя эти равенства, мы из равенства

$$(jf)[(e+if)(e+if)] = [(jf)(e+if)](e+if),$$

справедливого ввиду альтернативности алгебры R, получаем

$$-2(jf) = [-(je)f + k](e+if) = -2(jf) + 2ke,$$

т. е. $ke = 0$, что невозможно.

Полученное противоречие заканчивает доказательство обобщенной теоремы Фробениуса.

* Всякое альтернативное тело или ассоциативно, или же, рассматриваемое как алгебра над своим центром (см. V.6.2), конечномерно, а именно, имеет размерность 8 и является так называемой алгеброй Кэли — Диксона, т. е. некоторым обобщением алгебры Кэли на случай произвольного основного поля [Л. А. Скорняков, Укр. мат. журнал **2**:1 (1950), 70—85; Брак и Клейнфилд, Proc. Amer. Math. Soc. **2** (1951), 878—890]. *

11. Теорема Фробениуса не может быть обобщена на случай неальтернативных алгебр, так как существует, например, весьма много различных конечномерных действительных алгебр с ассоциативными степенями, являющихся алгебрами с однозначным делением.

* Размерность конечномерной действительной алгебры без делителей нуля может принимать лишь значения $n = 1$, 2, 4 или 8 [Милнор, Bull. Amer. Math. Soc. **64** (1958), 87—89]. *

12. Рассуждения, параллельные тем, которые использованы в V.8.3, немедленно приводят к следующей теореме:

Единственной конечномерной алгеброй с ассоциативными степенями над полем комплексных чисел, обладающей единицей, но не содержащей делителей нуля, является само поле комплексных чисел.

§ 9. Теорема Биркгофа — Витта о лиевых алгебрах

1. В II.2.3 доказано, что, заменяя в ассоциативном кольце R операцию умножения ab операцией коммутирования

$$a \circ b = ab - ba,$$

мы получаем лиево кольцо $L(R)$.

Если кольцо R является Σ-операторным (см. V.1.7), *то и кольцо $L(R)$ будет Σ-операторным.*

Так как указанные кольца имеют одну и ту же аддитивную группу, то нужно проверить лишь справедливость условия (11) из V.1.7. Если $a, b \in R$, $\alpha \in \Sigma$, то

$$(a \circ b)\alpha = (ab - ba)\alpha = (ab)\alpha - (ba)\alpha =$$
$$= (a\alpha)b - b(a\alpha) = (a\alpha) \circ b.$$

Так же проверяется и равенство

$$(a \circ b)\alpha = a \circ (b\alpha).$$

В частности, *если R является алгеброй над полем P, то и $L(R)$ будет алгеброй над этим же полем.*

2. Для случая алгебр некоторым обращением результата из II.2.3 служит следующая теорема [Биркгоф, Ann. of Math. **38** (1937), 526—532; Витт, J. reine und angew. Math. **177** (1937), 152—160]:

Для всякой левой алгебры L над любым полем P существует такая ассоциативная алгебра R над этим же полем, что алгебра L изоморфно вкладывается в алгебру $L(R)$.

Доказательство. Выбираем базу алгебры L над полем P. Считая эту базу, в соответствии с теоремой Цермело (см. I.6.3), вполне упорядоченной, запишем ее в виде

$$e_1, e_2, \ldots, e_\alpha, \ldots \tag{1}$$

Если для записи умножения в алгебре L будет употребляться символ $\times$, то

$$e_\alpha \times e_\beta = \sum_\gamma c_{\alpha\beta}^\gamma e_\gamma; \tag{2}$$

ясно, что при данных α и β лишь конечное число коэффициентов $c_{\alpha\beta}^\gamma$ может быть отлично от нуля.

Будем называть *словом* всякую упорядоченную конечную систему элементов из базы (1), не обязательно различных. Если дано слово

$$w = e_{\alpha_1} e_{\alpha_2} \ldots e_{\alpha_k} \tag{3}$$

длины k, $k \geqslant 1$, — элементы, составляющие это слово, мы записываем друг за другом, не разделяя запятыми, — то, как обычно, назовем *инверсией* в этом слове всякую пару e_{α_i}, e_{α_j} входящих в него элементов, для которой $i < j$, но $\alpha_i > \alpha_j$ в смысле упорядоченности базы (1).

Будем рассматривать, далее, *суммы слов*, т. е. конечные неупорядоченные системы слов, не обязательно различных, взятых с некоторыми отличными от нуля коэффициентами из поля P. В записи сумм слов мы будем формально соединять слова знаком $+$.

Наибольшую длину слов, входящих в данную сумму слов s, назовем *степенью* этой суммы. Если n — степень суммы слов s, то обозначим через l_i, $i=n, n-1, \ldots, 2$, общее число инверсий в словах длины i, входящих в s; если же в s слова длины i не входят совсем, то положим $l_i=0$. Ясно, что l_1 можно не рассматривать. Символ

$$\sigma=(l_n, l_{n-1}, \ldots, l_2) \tag{4}$$

называется *высотой* суммы слов s.

3. Считая n фиксированным, введем в множество высот вида (4), т. е. степени n, лексикографическую упорядоченность: если

$$\sigma'=(l'_n, l'_{n-1}, \ldots, l'_2),$$

то будем считать $\sigma<\sigma'$, если есть такое i, что $l_i<l'_i$, но (при $i<n$) $l_n=l'_n, \ldots, l_{i+1}=l'_{i+1}$.

Лексикографическая упорядоченность высот степени n делает множество этих высот вполне упорядоченным.

Очевидно, что это будет линейная упорядоченность. Рассмотрим строго убывающую последовательность высот

$$\sigma_1>\sigma_2>\ldots>\sigma_k>\ldots, \tag{5}$$

где

$$\sigma_k=(l_{kn}, l_{k,n-1}, \ldots, l_{k2}), \qquad k=1, 2 \ldots$$

Ясно, что

$$l_{1n}\geqslant l_{2n}\geqslant\ldots\geqslant l_{kn}\geqslant\ldots,$$

и поэтому существует такое k_1, что

$$l_{k_1 n}=l_{k_1+1,\ n}=\ldots$$

Отсюда следует, что

$$l_{k_1,\ n-1}\geqslant l_{k_1+1,\ n-1}\geqslant\ldots,$$

и поэтому существует такое k_2, $k_2\geqslant k_1$, что

$$l_{k_2,\ n-1}=l_{k_2+1,\ n-1}=\ldots$$

Продолжая далее для $n-2, \ldots, 2$, мы докажем, что последовательность (5) обрывается.

4. Пусть в сумму слов s входит с коэффициентом $a\in P$ слово $w=w_1e_\beta e_\alpha w_2$, где $\beta>\alpha$ в смысле упорядоченности базы (1), w_1, w_2 — некоторые слова, из которых одно или

оба могут отсутствовать. Назовем *редукцией* суммы слов s замену в s слагаемого aw суммой слов

$$aw_1e_\alpha e_\beta w_2 + \sum_\gamma (ac^\gamma_{\beta\alpha})\, w_1 e_\gamma w_2.$$

Редукция не меняет, очевидно, степень суммы слов s, но понижает ее высоту.

Отсюда следует, ввиду полной упорядоченности множества высот, что всякую сумму слов s можно превратить последовательными редукциями в сумму слов высоты $(0, 0, \ldots, 0)$, т. е. в сумму слов без инверсий или, как мы будем говорить, *нормальных слов*. В полученной сумме слов мы совершим затем приведение подобных членов, что может уменьшить, конечно, степень этой суммы, но не нарушит ее свойства быть суммой нормальных слов, и этим приведем сумму слов s *к нормальному виду*.

5. Лемма. *Всякая сумма слов приводится к одному единственному нормальному виду, не зависящему от выполняемой последовательности редукций.*

Утверждение леммы выполняется для сумм высоты $(0, 0, \ldots, 0)$, так как в этом случае совершается лишь приведение подобных членов. Это позволяет вести доказательство индукцией по вполне упорядоченному множеству высот.

Пусть сумма слов s двумя последовательностями редукций приводится соответственно к нормальным видам s_1 и s_2. Если обе цепочки редукций начинаются с одной и той же редукции, переводящей s в s', то, так как высота суммы s' меньше высоты суммы s, можно применить индуктивное предположение и поэтому $s_1 = s_2$.

Пусть, с другой стороны, начальные редукции обоих цепочек редукций относились к различным словам суммы s, причем они переводили s соответственно в s' и s''. В сумме s' можно выполнить начальную редукцию второй цепочки редукций, после чего придем к некоторой сумме слов s'''; эту же сумму слов s''' мы получим, выполняя в s'' начальную редукцию первой цепочки. Приводя s''' некоторым способом к нормальному виду s_3 и учитывая, что высоты сумм s' и s'' меньше высоты суммы s, мы получим, что $s_1 = s_3$, $s_2 = s_3$, т. е. $s_1 = s_2$.

Эти же рассуждения применимы и к тому случаю, когда начальные редукции обеих цепочек редукций относятся к ука-

занным двум местам слова

$$w_1 e_\beta e_\alpha w_3 e_\delta e_\gamma w_2, \quad \beta > \alpha, \ \delta > \gamma, \tag{6}$$

коэффициент которого мы опускаем; слово w_3 может, конечно, и отсутствовать. В этом случае, однако, для перехода от сумм s' и s'' к одной и той же сумме s''' необходимо выполнить начальную редукцию второй (первой) цепочки во всех тех словах суммы s' (суммы s''), которые появились вместо слова (6).

6. Остается рассмотреть случай, когда начальные редукции обеих цепочек редукций относятся к указанным двум местам слова

$$w_1 e_\gamma e_\beta e_\alpha w_2, \quad \gamma > \beta > \alpha. \tag{7}$$

Пусть, как и выше, s' и s'' будут суммы слов, полученные после этих начальных редукций. Если начальная редукция первой цепочки относилась к месту (γ, β), то в слове той же длины, появившемся вместо слова (7) после этой редукции, можно выполнить еще редукцию на месте (γ, α), а затем и на месте (β, α). В результате от суммы s' мы придем к сумме s_1''', которая будет отличаться от исходной суммы s тем, что вместо слова (7) стоит сумма

$$w_1 e_\alpha e_\beta e_\gamma w_2 + \sum_\delta c^\delta_{\gamma\beta} w_1 e_\delta e_\alpha w_2 + \\ + \sum_\delta c^\delta_{\gamma\alpha} w_1 e_\beta e_\delta w_2 + \sum_\delta c^\delta_{\beta\alpha} w_1 e_\delta e_\gamma w_2. \tag{8}$$

Аналогично от суммы s'' можно перейти несколькими редукциями к сумме s_2''', отличающейся от суммы s тем, что слово (7) заменено суммой

$$w_1 e_\alpha e_\beta e_\gamma w_2 + \sum_\delta c^\delta_{\beta\alpha} w_1 e_\gamma e_\delta w_2 + \\ + \sum_\delta c^\delta_{\gamma\alpha} w_1 e_\delta e_\beta w_2 + \sum_\delta c^\delta_{\gamma\beta} w_1 e_\alpha e_\delta w_2. \tag{9}$$

7. Сравним суммы (8) и (9). В них входят соответственно слагаемые

$$c^\delta_{\gamma\beta} w_1 e_\delta e_\alpha w_2 \quad \text{и} \quad c^\delta_{\gamma\beta} w_1 e_\alpha e_\delta w_2. \tag{10}$$

Если $\delta = \alpha$, то слагаемые (10) совпадают. Если $\delta > \alpha$, то в первом из этих слагаемых возможна редукция, переводящая его во второе слагаемое, к которому прибавлена сумма

$\sum_{\varepsilon} c_{\gamma\beta}^{\delta} c_{\delta\alpha}^{\varepsilon} w_1 e_\varepsilon w_2$. Если же $\alpha > \delta$, то редукция во втором из слагаемых (10) переводит его в сумму первого слагаемого и суммы $\sum_{\varepsilon} c_{\gamma\beta}^{\delta} c_{\alpha\delta}^{\varepsilon} w_1 e_\varepsilon w_2$.

Аналогичные рассмотрения применимы и к другим слагаемым сумм (8) и (9). Отсюда следует, что эти суммы после соответствующих редукций могут быть превращены в такие суммы — обозначим их через (8′) и (9′), — которые отличаются друг от друга лишь словами вида $w_1 e_\varepsilon w_2$. Легко видеть, однако, что сумма коэффициентов при данном слове $w_1 e_\varepsilon w_2$ в сумме (8′) равна

$$\sum_{\delta > \alpha} c_{\gamma\beta}^{\delta} c_{\delta\alpha}^{\varepsilon} + \sum_{\delta < \beta} c_{\gamma\alpha}^{\delta} c_{\beta\delta}^{\varepsilon} + \sum_{\delta > \gamma} c_{\beta\alpha}^{\delta} c_{\delta\gamma}^{\varepsilon}, \tag{11}$$

а в сумме (9′) —

$$\sum_{\delta < \alpha} c_{\gamma\beta}^{\delta} c_{\alpha\delta}^{\varepsilon} + \sum_{\delta > \beta} c_{\gamma\alpha}^{\delta} c_{\delta\beta}^{\varepsilon} + \sum_{\delta < \gamma} c_{\beta\alpha}^{\delta} c_{\gamma\delta}^{\varepsilon}. \tag{12}$$

Эти две суммы коэффициентов равны между собой. Действительно, применяя к справедливому в алгебре L равенству

$$(e_\gamma \times e_\beta) \times e_\alpha + (e_\beta \times e_\alpha) \times e_\gamma + (e_\alpha \times e_\gamma) \times e_\beta = 0$$

таблицу умножения (2) и приравнивая нулю коэффициент при e_ε, мы получим равенство

$$\sum_{\delta} \left(c_{\gamma\beta}^{\delta} c_{\delta\alpha}^{\varepsilon} + c_{\beta\alpha}^{\delta} c_{\delta\gamma}^{\varepsilon} + c_{\alpha\gamma}^{\delta} c_{\delta\beta}^{\varepsilon} \right) = 0.$$

Отсюда следует равенство нулю разности сумм (11) и (12), если учесть, что для любых α, β и δ из

$$e_\alpha \times e_\beta = -e_\beta \times e_\alpha$$

следует равенство

$$c_{\alpha\beta}^{\delta} = -c_{\beta\alpha}^{\delta}, \tag{13}$$

а из

$$e_\alpha \times e_\alpha = 0$$

— равенство

$$c_{\alpha\alpha}^{\delta} = 0.$$

Теперь можно утверждать, что существуют цепочки редукций, приводящие суммы слов s_1''' и s_2''' к одному и тому же

нормальному виду s_3. Дальнейшие рассмотрения идут так же, как в предшествующих случаях. Доказательство леммы закончено.

8. Построим теперь над полем P алгебру R, базой которой служит множество всех нормальных слов (см. V. 9.4). Произведением нормальных слов w_1 и w_2 будем считать тот нормальный вид, к которому приводится слово w_1w_2. Ввиду леммы это произведение однозначно и ассоциативно.

Перейдем от полученной ассоциативной алгебры R к соответствующей лиевой алгебре $L(R)$, обозначая умножение в последней символом $\circ$. Найдем ее подалгебру, порожденную всеми элементами e_α, которые, будучи нормальными словами, входят в базу алгебр R и $L(R)$. Для этого покажем, что при любых α и β

$$e_\alpha \circ e_\beta = e_\alpha \times e_\beta.$$

Действительно, если $\alpha = \beta$, то

$$e_\alpha \circ e_\alpha = 0 = e_\alpha \times e_\alpha.$$

Если $\alpha > \beta$, то, ввиду (2),

$$e_\alpha \circ e_\beta = e_\alpha e_\beta - e_\beta e_\alpha = e_\beta e_\alpha + \sum_\gamma c_{\alpha\beta}^\gamma e_\gamma - e_\beta e_\alpha =$$
$$= \sum_\gamma c_{\alpha\beta}^\gamma e_\gamma = e_\alpha \times e_\beta.$$

Если же $\alpha < \beta$, то, ввиду (13),

$$e_\alpha \circ e_\beta = e_\alpha e_\beta - e_\beta e_\alpha = e_\alpha e_\beta - e_\alpha e_\beta - \sum_\gamma c_{\beta\alpha}^\gamma e_\gamma =$$
$$= \sum_\gamma c_{\alpha\beta}^\gamma e_\gamma = e_\alpha \times e_\beta.$$

Таким образом, в алгебре $L(R)$ мы нашли подалгебру, изоморфную алгебре L. Теорема Биркгофа — Витта доказана.

* Если L — конечномерная лиева алгебра над полем без характеристики (см. III. 2.11), то существует такая конечномерная ассоциативная алгебра R над этим же полем, что L изоморфно вкладывается в $L(R)$ [И. Д. Адо, Изв. Каз. физ.-мат. о-ва **7** (1934—1935), 1—43; см. также И. Д. Адо, Успехи мат. наук **2**:6 (1947), 159—173; Хариш-Чандра, Ann. of Math. **50** (1949), 68—76].

Теорема, аналогичная теореме Биркгофа — Витта, справедлива для лиевых колец без операторов [Лазар, C. R., Paris

234:8 (1952), 788—791]. На лиевы кольца с произвольной областью операторов эта теорема не может быть распространена [А. И. Ширшов, Успехи мат. наук **8**:5 (1953), 173—175]. ⁎

§ 10. Дифференцирования. Дифференциальные кольца

1. В V. 1.7, вводя понятие операторного кольца, мы использовали не эндоморфизмы кольца R, т. е. не такие эндоморфизмы φ аддитивной группы этого кольца, которые удовлетворяют условию

$$(ab)\varphi = a\varphi \cdot b\varphi, \qquad a,\ b \in R,$$

а те эндоморфизмы φ аддитивной группы, которые перестановочны со всеми правыми и левыми умножениями, т. е. удовлетворяют условию

$$(ab)\varphi = (a\varphi)\,b = a\,(b\varphi), \qquad a,\ b \in R.$$

Выбор именно этих преобразований можно, конечно, оправдать историческими соображениями. Однако во многих вопросах существенно используются и такие эндоморфизмы δ аддитивной группы кольца R, для которых выполняется условие

$$(ab)\delta = (a\delta)\,b + a\,(b\delta), \qquad a,\ b \in R. \tag{1}$$

Это условие аналогично правилу дифференцирования произведения, а так как δ, как эндоморфизм аддитивной группы кольца R, удовлетворяет и условию

$$(a+b)\delta = a\delta + b\delta, \qquad a,\ b \in R, \tag{2}$$

аналогичному правилу дифференцирования суммы, то δ называется *дифференцированием* кольца R.

Если кольцо R операторное, в частности алгебра над некоторым полем, то в определении дифференцирования естественно предполагать, что δ — операторный эндоморфизм аддитивной группы. Иными словами, δ должно удовлетворять помимо условий (1) и (2) также условию

$$(a\alpha)\delta = (a\delta)\alpha, \tag{3}$$

где $a \in R$, α — произвольный оператор.

Нулевой эндоморфизм любого кольца R (см. III. 3.7) является, очевидно, его дифференцированием. Примером не-

тривиального дифференцирования служит обычное дифференцирование в кольце многочленов $P[x]$ от одного неизвестного над полем P.

2. Если G — произвольная абелева группа, то ее кольцо эндоморфизмов (III. 3.8) ассоциативно. Заменяя в этом кольце операцию умножения операцией

$$\varphi \circ \psi = \varphi\psi - \psi\varphi,$$

мы получаем, по II. 2.3, лиево кольцо, которое назовем *лиевым кольцом эндоморфизмов* абелевой группы G.

Совокупность дифференцирований произвольного кольца R является подкольцом в лиевом кольце эндоморфизмов аддитивной группы кольца R.

В самом деле, если δ_1 и δ_2 — дифференцирования кольца R, то эндоморфизм аддитивной группы $\delta_1 + \delta_2$ также будет дифференцированием, так как для любых a, $b \in R$

$$\begin{aligned}(ab)(\delta_1+\delta_2) &= (ab)\delta_1 + (ab)\delta_2 = (a\delta_1)b + a(b\delta_1) + (a\delta_2)b + \\ &+ a(b\delta_2) = (a\delta_1 + a\delta_2)b + a(b\delta_1 + b\delta_2) = \\ &= [a(\delta_1+\delta_2)]b + a[b(\delta_1+\delta_2)].\end{aligned}$$

Выше уже отмечено, далее, что нулевой эндоморфизм является дифференцированием. Эндоморфизм $-\delta$, противоположный дифференцированию δ, сам будет дифференцированием, так как для a, $b \in R$

$$\begin{aligned}(ab)(-\delta) &= -[(ab)\delta] = -[(a\delta)b + a(b\delta)] = \\ &= [a(-\delta)]b + a[b(-\delta)].\end{aligned}$$

Наконец, лиево произведение

$$\delta_1 \circ \delta_2 = \delta_1\delta_2 - \delta_2\delta_1$$

дифференцирований δ_1, δ_2 само будет дифференцированием, так как для a, $b \in R$

$$\begin{aligned}(ab)(\delta_1 \circ \delta_2) &= (ab)(\delta_1\delta_2 - \delta_2\delta_1) = [(ab)\delta_1]\delta_2 - [(ab)\delta_2]\delta_1 = \\ &= [(a\delta_1)b + a(b\delta_1)]\delta_2 - [(a\delta_2)b + a(b\delta_2)]\delta_1 = \\ &= [(a\delta_1)b]\delta_2 + [a(b\delta_1)]\delta_2 - [(a\delta_2)b]\delta_1 - [a(b\delta_2)]\delta_1 = \\ &= [(a\delta_1)\delta_2]b + (a\delta_1)(b\delta_2) + (a\delta_2)(b\delta_1) + a[(b\delta_1)\delta_2] - \\ &- [(a\delta_2)\delta_1]b - (a\delta_2)(b\delta_1) - (a\delta_1)(b\delta_2) - a[(b\delta_2)\delta_1] = \\ &= [a(\delta_1 \circ \delta_2)]b + a[b(\delta_1 \circ \delta_2)].\end{aligned}$$

Теорема доказана.

Заметим, что если R — алгебра над полем P, то и кольцо операторных эндоморфизмов аддитивной группы кольца R будет алгеброй над P: если φ — такой эндоморфизм, $\alpha \in P$ и $a \in R$, то следует положить

$$a(\varphi\alpha) = (a\varphi)\alpha = (a\alpha)\varphi. \tag{4}$$

Алгеброй над P будет и лиево кольцо операторных эндоморфизмов аддитивной группы кольца R, так как, ввиду (4),

$$a[(\varphi_1 \circ \varphi_2)\alpha] = [a(\varphi_1\varphi_2 - \varphi_2\varphi_1)]\alpha =$$
$$= [a(\varphi_1\alpha)]\varphi_2 - (a\varphi_2)(\varphi_1\alpha) = a[(\varphi_1\alpha) \circ \varphi_2],$$

т. е.

$$(\varphi_1 \circ \varphi_2)\alpha = (\varphi_1\alpha) \circ \varphi_2$$

и, аналогично,

$$(\varphi_1 \circ \varphi_2)\alpha = \varphi_1 \circ (\varphi_2\alpha).$$

Наконец, *лиево кольцо дифференцирований алгебры R будет подалгеброй этой лиевой алгебры эндоморфизмов*, так как если δ — дифференцирование, $\alpha \in P$, то для a, $b \in R$

$$(ab)(\delta\alpha) = [(ab)\delta]\alpha = [(a\delta)b + a(b\delta)]\alpha = [a(\delta\alpha)]b + a[b(\delta\alpha)].$$

Это замечание переносится, понятно, на случай колец с произвольной системой операторов.

3. Пусть дано ассоциативное кольцо R. Если $r \in R$, то определим отображение δ_r, полагая для всех $a \in R$

$$a\delta_r = ar - ra. \tag{5}$$

Это отображение будет дифференцированием, так как для a, $b \in R$

$$(a+b)\delta_r = (a+b)r - r(a+b) = a\delta_r + b\delta_r,$$

$$(ab)\delta_r = abr - rab = abr - rab + arb - arb = (a\delta_r)b + a(b\delta_r).$$

Оно называется *внутренним дифференцированием* кольца R, определяемым элементом r. Ясно, что среди ассоциативных колец ассоциативно-коммутативные кольца и только они не имеют внутренних дифференцирований, отличных от нулевого эндоморфизма.

4. Если R — лиево кольцо и $r \in R$, то правое умножение на r, т. е. отображение δ_r, определяемое равенством

$$a\delta_r = ar, \tag{6}$$

где $a \in R$, является дифференцированием кольца R. В самом деле, из V.1.6 мы знаем, что δ_r будет эндоморфизмом аддитивной группы кольца R. С другой стороны, если $a, b \in R$, то, используя тождество Якоби и закон антикоммутативности (см. II. 2.2), получаем:

$$(ab)\,\delta_r = (ab)\,r = -(br)\,a - (ra)\,b = (ar)\,b + a\,(br) = \\ = (a\delta_r)\,b + a\,(b\delta_r).$$

Дифференцирование δ_r называется *внутренним дифференцированием* лиева кольца R, определяемым элементом r. Очевидно, что среди лиевых колец нулевые кольца и только они не имеют внутренних дифференцирований, отличных от нулевого эндоморфизма ω.

Внутренние дифференцирования составляют идеал в лиевом кольце всех дифференцирований лиева кольца R, так как

$$\delta_r - \delta_s = \delta_{r-s},$$
$$\delta_r \circ \delta' = \delta_{r\delta'},$$

где $r, s \in R$, δ' — произвольное дифференцирование.

Действительно, если $a \in R$, то

$$a\,(\delta_r - \delta_s) = ar - as = a\delta_{r-s},$$

$$a\,(\delta_r \circ \delta') = a\,(\delta_r\delta' - \delta'\delta_r) = (ar)\,\delta' - (a\delta')\,r = \\ = (a\delta')\,r + a\,(r\delta') - (a\delta')\,r = a\delta_{r\delta'}.$$

Отображение

$$r \to \delta_r, \qquad r \in R,$$

является гомоморфизмом лиева кольца R на лиево кольцо его внутренних дифференцирований.

В самом деле, если $a, r, s \in R$, то

$$a\delta_{r+s} = a\,(r+s) = ar + as = a\delta_r + a\delta_s = a\,(\delta_r + \delta_s),$$

$$a\delta_{rs} = a\,(rs) = -(rs)\,a = (sa)\,r + (ar)\,s = (ar)\,s - (as)\,r = \\ = a\,(\delta_r\delta_s - \delta_s\delta_r) = a\,(\delta_r \circ \delta_s).$$

Ядром этого гомоморфизма служит, очевидно, совокупность аннуляторов кольца R (см. V.1.9).

Результаты этого пункта весьма напоминают результаты из III.3.2 о внутренних автоморфизмах групп.

5. Если R — ассоциативное кольцо, а L — лиево кольцо, соответствующее ему в смысле II.2.3, то *всякое дифференцирование* δ *кольца* R *будет дифференцированием и в* L. Действительно,

$$(a \circ b)\delta = (ab - ba)\delta = (a\delta)b + a(b\delta) - (b\delta)a - b(a\delta) =$$
$$= (a\delta \circ b) + (a \circ b\delta).$$

Обратное, вообще говоря, не имеет места. Однако *внутренние дифференцирования кольца* R *будут внутренними дифференцированиями и в кольце* L *и обратно.* В самом деле, (5) можно переписать в виде

$$a\delta_r = a \circ r;$$

с другой стороны, (6) должно быть записано теперь в виде

$$a\delta_r = a \circ r$$

и поэтому

$$a\delta_r = ar - ra.$$

Из результатов этого и предшествующего пунктов вытекает, что *внутренние дифференцирования ассоциативного кольца* R *составляют идеал в лиевом кольце всех дифференцирований кольца* R.

Заметим, что все результаты, полученные в этих последних пунктах, справедливы для колец с произвольной областью операторов и, в частности, для алгебр.

* Понятие внутреннего дифференцирования может быть распространено со случая ассоциативных и лиевых колец на случай произвольных колец, причем так, что внутренние дифференцирования будут составлять идеал в лиевом кольце всех дифференцирований [Шэфер, Bull. Amer. Math. Soc. **55** (1949), 769 — 776]. *

6. Вполне аналогичным понятию операторного кольца является понятие дифференциального кольца. Кольцо R называется *дифференциальным кольцом с системой дифференцирований* Δ, если задано множество Δ и всякому элементу $\delta \in \Delta$ поставлено в соответствие некоторое дифференцирование кольца R; при этом не предполагается, что

различным элементам из Δ должны соответствовать различные дифференцирования. Отметим, не давая точных формулировок, что можно было бы считать Δ лиевым кольцом и определить понятие дифференциального кольца с лиевым кольцом дифференцирований Δ.

Если R — дифференциальное кольцо с системой дифференцирований Δ, то под *дифференциальным подкольцом (идеалом)* кольца R следует понимать такое подкольцо (идеал) A из R, что для всех $a \in A$, $\delta \in \Delta$

$$a\delta \in A.$$

Естественным образом определяются также понятия *изоморфизма* и *гомоморфизма* дифференциальных колец с одной и той же системой дифференцирований Δ.

7. Рассмотрим дифференциальное кольцо R с одним дифференцированием δ, причем условимся употреблять запись, привычную из курса математического анализа: если $a \in R$, то

$$a\delta = a'.$$

Равенства (1) и (2) перепишутся теперь в виде

$$(ab)' = a'b + ab', \tag{7}$$

$$(a+b)' = a' + b', \tag{8}$$

откуда, в частности,

$$0' = 0, \tag{9}$$

$$(-a)' = -a'. \tag{10}$$

Если кольцо R обладает единицей e, то, по (7), для $a \in R$

$$a' = (ae)' = a'e + ae' = a' + ae',$$

т. е. $ae' = 0$. Кольцо с единицей не может, однако, обладать аннулятором, отличным от нуля, и поэтому

$$e' = 0. \tag{11}$$

Пусть R — поле, a, $b \in R$, $a \neq 0$ и c — решение уравнения $ax = b$. Тогда

$$b' = (ac)' = a'c + ac',$$

откуда

$$c' = a^{-1}b' - a^{-1}a'c = a^{-2}(ab' - a'b). \tag{12}$$

8. Элемент a кольца R называется *константой* относительно рассматриваемого дифференцирования, если

$$a' = 0.$$

Из (7)—(11) следует, что *константы составляют в R подкольцо, содержащее единицу, если R — кольцо с единицей.* Таким образом, в кольце целых чисел нет никаких дифференцирований, отличных от нулевого эндоморфизма. Это же справедливо для поля рациональных чисел, так как, ввиду (12), *в поле константы составляют подполе.*

9. Пусть R — ассоциативно-коммутативное дифференциальное кольцо с одним дифференцированием. Рассмотрим кольцо многочленов

$$\bar{R} = R[x,\ x',\ x'',\ \ldots,\ x^{(n)},\ \ldots]$$

над кольцом R от счетного множества неизвестных (см. II. 2.7). Полагая

$$(x)' = x',\ (x^{(n)})' = x^{(n+1)},\quad n = 1,\ 2,\ \ldots,$$

можно, опираясь на (7) и (8) и используя однозначность записи элемента из $\bar{R}$ в виде многочлена, распространить дифференцирование, заданное в R, на все кольцо $\bar{R}$. Проверка того, что при этом будут выполнены все требования, входящие в определение дифференцирования, предоставляется читателю.

В полученном дифференциальном кольце $\bar{R}$ дифференциальное подкольцо, порожденное подкольцом R и элементом x, совпадает со всем $\bar{R}$. По этой причине кольцо $\bar{R}$, рассматриваемое с введенным нами дифференцированием, называется *кольцом дифференциальных многочленов над кольцом R от одного неизвестного x.*

Эта конструкция без труда переносится на случай нескольких неизвестных, а также нескольких дифференцирований.

* Кольцо $\bar{R}$ не содержит никаких констант, отличных от констант кольца R. В частности, если кольцо R рассматривалось с нулевым дифференцированием, то R и будет служить подкольцом констант кольца $\bar{R}$. *

ГЛАВА ШЕСТАЯ

УПОРЯДОЧЕННЫЕ И ТОПОЛОГИЧЕСКИЕ ГРУППЫ И КОЛЬЦА. НОРМИРОВАННЫЕ КОЛЬЦА

§ 1. Упорядоченные группы

1. Как правило, те основные алгебраические образования, с которыми обычно приходится иметь дело математикам, не являются группами, кольцами или полями в чистом виде. Уже рассмотренные нами операторные группы и кольца и дифференциальные кольца представляют собою некоторое приближение к тем конкретным алгебраическим системам, какие встречаются в неалгебраических исследованиях. В настоящей главе мы пойдем другими путями, но в этом же направлении. Начнем с рассмотрения упорядоченных образований.

Аддитивные группы целых чисел, рациональных чисел и действительных чисел одновременно являются и группами, и линейно упорядоченными множествами (см. I.4.1). Аддитивная группа действительных функций действительного переменного x, определенных для всех значений x, превращается в частично упорядоченное множество, если положить, что $f \leqslant g$ тогда и только тогда, когда $f(x) \leqslant g(x)$ для всех значений x.

Во всех этих группах упорядоченность и групповая операция связаны следующим образом: неравенство между элементами группы не нарушается, если к обеим его частям прибавить один и тот же элемент. Это приводит к следующему определению, причем мы перейдем к мультипликативной записи:

Группоид G называется *линейно упорядоченным* (соответственно *частично упорядоченным*), если для его элементов задана линейная (соответственно частичная) упорядоченность,

причем из $a \leqslant b$ следует $ax \leqslant bx$ и $xa \leqslant xb$ для всех $x \in G$.

Из этого определения вытекает, что если для элементов a, b, c, d частично (в частности, линейно) упорядоченного группоида G имеют место неравенства

$$a \leqslant b, \quad c \leqslant d,$$

то

$$ac \leqslant bd. \tag{1}$$

Очевидно, что если A — подгруппоид группоида G, то частичная упорядоченность группоида G индуцирует частичную упорядоченность в A.

Частично упорядоченные группоиды G и G' называются *изоморфными*, если существует взаимно однозначное отображение G на G', являющееся изоморфизмом и в смысле алгебраической операции и в смысле частичной упорядоченности (см. II. 4.1 и I. 4.3). Всякий группоид можно считать частично упорядоченным, рассматривая его тривиальную частичную упорядоченность (см. I. 4.1).

2. Назовем *монотонным преобразованием* частично упорядоченного множества M такое отображение φ множества M в себя, что из $a \leqslant b$ всегда следует $a\varphi \leqslant b\varphi$. Произведение монотонных преобразований само будет монотонным, т. е. эти преобразования составляют подполугруппу в симметрической полугруппе на множестве M (см. II. 1.8), причем подполугруппу с единицей, так как тождественное преобразование монотонно.

Если φ, ψ — монотонные преобразования множества M, то положим $\varphi \leqslant \psi$, если $x\varphi \leqslant x\psi$ для всех $x \in M$. Этим полугруппа монотонных преобразований частично упорядочивается: если χ — любое монотонное преобразование, то из $x\varphi \leqslant x\psi$ следует $x(\varphi\chi) \leqslant x(\psi\chi)$ для всех $x \in M$, т. е. $\varphi\chi \leqslant \psi\chi$; с другой стороны, из $(x\chi)\varphi \leqslant (x\chi)\psi$ для всех $x \in M$ следует $x(\chi\varphi) \leqslant x(\chi\psi)$, т. е. $\chi\varphi \leqslant \chi\psi$.

Справедлива следующая теорема Кришнана [Bull. Soc. Math. Fr. **78** (1950), 235 — 263]:

Всякая частично упорядоченная полугруппа G с единицей изоморфно вкладывается в частично упорядоченную полугруппу монотонных преобразований самого частично упорядоченного множества G.

Действительно, поставим в соответствие всякому элементу $a \in G$ преобразование φ_a, полагая для всех $x \in G$

$$x\varphi_a = xa.$$

Так как из $x \leqslant y$ следует $xa \leqslant ya$, то преобразование φ_a монотонно. С другой стороны, из II. 4.6 мы знаем, что благодаря наличию в G единицы отображение $a \to \varphi_a$, $a \in G$, является изоморфным отображением полугруппы G в симметрическую полугруппу на G, т. е., следовательно, в полугруппу монотонных преобразований множества G. Наконец, если $a \leqslant b$, то для всех x будет $xa \leqslant xb$, т. е. $\varphi_a \leqslant \varphi_b$; обратно, из $\varphi_a \leqslant \varphi_b$ следует, в частности, $1 \cdot a \leqslant 1 \cdot b$, т. е. $a \leqslant b$. Теорема доказана.

Из этой теоремы следует, что *всякая частично упорядоченная группа G изоморфно вкладывается в частично упорядоченную группу монотонных подстановок самого частично упорядоченного множества G.*

3. Элемент a частично упорядоченной группы G называется *положительным*, если $a \geqslant 1$ (или, при аддитивной записи, если $a \geqslant 0$), и *отрицательным*, если $a \leqslant 1$. В линейно упорядоченной группе всякий элемент или положителен или отрицателен.

Из (1) следует, что произведение положительных элементов частично упорядоченной группы G положительно, т. е. положительные элементы составляют в G подполугруппу, которую мы назовем *полугруппой положительных элементов* частично упорядоченной группы G. Впрочем, и отрицательные элементы составляют подполугруппу.

Частичная упорядоченность группы G полностью определяется заданием полугруппы положительных элементов, так как $a \leqslant b$ тогда и только тогда, когда $1 \leqslant ba^{-1}$.

Подполугруппа P группы G тогда и только тогда служит полугруппой положительных элементов при некоторой частичной упорядоченности группы G, если выполняются следующие условия:

1) $1 \in P$;

2) *если* $a \in P$ *и* $a^{-1} \in P$, *то* $a = 1$;

3) *если* $a \in P$, $x \in G$, *то* $x^{-1}ax \in P$.

Действительно, если P — полугруппа положительных элементов частично упорядоченной группы G, то 1) $1 \leqslant 1$;

2) из $a^{-1} \geqslant 1$ следует $1 \geqslant a$, а так как дано, что $a \geqslant 1$, то $a = 1$; 3) из $a \geqslant 1$ следует $x^{-1}ax \geqslant x^{-1}x = 1$.

Обратно, пусть подполугруппа P группы G обладает свойствами 1) — 3). Положим $a \leqslant b$, если $ba^{-1} \in P$, а поэтому, ввиду 3), и $a^{-1}b = a^{-1}(ba^{-1})a \in P$. Это будет частичная упорядоченность группы G:

$a \leqslant a$, так как, по 1), $aa^{-1} = 1 \in P$;

если $a \leqslant b$ и $b \leqslant a$, т. е. $ba^{-1} \in P$ и $ab^{-1} = (ba^{-1})^{-1} \in P$, то, по 2), $ba^{-1} = 1$, т. е. $b = a$;

если $a \leqslant b$ и $b \leqslant c$, т. е. $ba^{-1} \in P$ и $cb^{-1} \in P$, то $ca^{-1} = (cb^{-1})(ba^{-1}) \in P$, т. е. $a \leqslant c$;

наконец, если $a \leqslant b$, т. е. $ba^{-1} \in P$, то $(bx)(ax)^{-1} = ba^{-1} \in P$, т. е. $ax \leqslant bx$, и, ввиду 3), $(xb)(xa)^{-1} = x(ba^{-1})x^{-1} \in P$, т. е. $xa \leqslant xb$.

При этой частичной упорядоченности положительными будут элементы из P и только они, так как $a \geqslant 1$ тогда и только тогда, если $a \cdot 1^{-1} = a \in P$. Теорема доказана.

Подполугруппа P группы G тогда и только тогда определяет линейную упорядоченность этой группы, если она удовлетворяет помимо условий 1) — 3) *также условию* 4) *для любого $a \in G$ или $a \in P$, или $a^{-1} \in P$.*

В самом деле, если группа G линейно упорядочена и элемент a не является положительным, то $a < 1$, откуда следует $1 < a^{-1}$, т. е. элемент a^{-1} положителен. Обратно, пусть подполугруппа P удовлетворяет условиям 1) — 4) и $a, b \in G$. Если $ba^{-1} \in P$, то $a \leqslant b$ в смысле частичной упорядоченности, определяемой полугруппой P. Если же $ba^{-1} \notin P$, то, по 4), $(ba^{-1})^{-1} = ab^{-1} \in P$, т. е. $b \leqslant a$.

* Частично упорядоченное множество M называется *направленным*, если для любых $a, b \in M$ существует такой элемент $c \in M$, что

$$a \leqslant c, \quad b \leqslant c.$$

Можно говорить, следовательно, о *направленной группе*. Частично упорядоченная группа тогда и только тогда будет направленной, если она совпадает с подгруппой, порожденной всеми ее положительными элементами. *

4. В частично упорядоченной группе G из $a \geqslant 1$ следует $a^n \geqslant 1$ для всех натуральных n. Поэтому, ввиду свойства 2) полугруппы положительных элементов, *всякий строго положительный элемент* a (т. е. такой, что $a > 1$

должен иметь бесконечный порядок: если $a^n = 1$, $n > 1$, то $a^{n-1} = a^{-1}$. Отсюда следует (определения см. в II. 3.4):

Всякая линейно упорядоченная группа является группой без кручения.

Периодическая группа не допускает никаких частичных упорядочений, кроме тривиального.

5. Если в группе G заданы два частичных упорядочения, соответственно с полугруппами положительных элементов P_1 и P_2, то второе частичное упорядочение назовем *продолжением* первого, если $P_2 \supset P_1$, т. е. если из $a \leqslant b$ в первом упорядочении всегда следует это же неравенство во втором упорядочении.

Множество всех подполугрупп группы G, удовлетворяющих условиям 1) — 3) из VI. 1.3, частично упорядочено по включению. Объединение любой цепи из таких подполугрупп само будет подполугруппой со свойствами 1) — 3), а поэтому, по теореме Куратовского — Цорна, всякая подполугруппа со свойствами 1) — 3) содержится в максимальной такой подполугруппе, т. е. *всякая частичная упорядоченность группы G продолжается до максимальной* (*далее не продолжаемой*) *частичной упорядоченности.*

Если группа G допускает линейные упорядоченности, то всякая ее линейная упорядоченность максимальна.

Это очевидное утверждение мы дополним одним критерием того, когда все максимальные упорядоченности группы G линейны [Охниси, Osaka Math. J. **2** (1950), 161 — 164].

6. Начнем с некоторых замечаний о подполугруппах группы G, обладающих свойствами 1) — 3). Если P — такая подполугруппа, то множество P^{-1} всех элементов p^{-1}, где $p \in P$, также будет, очевидно, подполугруппой со свойствами 1) — 3). Отметим, что

$$P \cap P^{-1} = 1, \tag{2}$$

так как иначе будет нарушено свойство 2).

Лемма 1. *Если P и Q — подполугруппы группы G, обладающие свойствами* 1) — 3), *и*

$$P \cap Q^{-1} = 1, \tag{3}$$

то множество PQ всех элементов группы G, представимых в виде pq, $p \in P$, $q \in Q$, само будет подполугруппой со свойствами 1) — 3).

Действительно,

$$(p_1q_1)(p_2q_2) = (p_1 \cdot q_1p_2q_1^{-1})(q_1q_2) = p_3q_3, \tag{4}$$

где $p_3 \in P$, $q_3 \in Q$. Этим доказано, что PQ — подполугруппа.

Далее, $1 = 1 \cdot 1 \in PQ$. С другой стороны, если $pq = 1$, то $p = q^{-1}$, откуда, ввиду (3), следует $p = q = 1$. Из

$$(p_1q_1)(p_2q_2) = 1$$

будет вытекать поэтому (см. (4)), что $p_3 = q_3 = 1$, т. е., так как полугруппы P и Q обладают свойством 2),

$$q_1 = q_2 = p_1 = q_1p_2q_1^{-1} = p_2 = 1.$$

Наконец, для любого $x \in G$

$$x^{-1}(pq)x = (x^{-1}px)(x^{-1}qx) = p'q' \in PQ.$$

Лемма доказана.

Пересечение любой системы подполугрупп группы G, обладающих свойствами 1) — 3), само будет, очевидно, подполугруппой с этими же свойствами. Отсюда следует, что если элемент a вообще содержится хотя бы в одной такой подполугруппе, то существует минимальная подполугруппа со свойствами 1) — 3), содержащая элемент a; обозначим ее через P_a.

7. *Тогда и только тогда все максимальные упорядоченности группы G линейны, если:*

I. *P_a существует для всякого $a \in G$.*

II. *Из $b, c \in P_a$, $a \in G$, и $b \neq 1$, $c \neq 1$, следует, что*

$$P_b \cap P_c \neq 1.$$

Доказательство. Если группа G допускает линейную упорядоченность с полугруппой положительных элементов P, то $a \in P$ или $a \in P^{-1}$, а поэтому свойство I выполняется.

Пусть теперь всякая частичная упорядоченность группы G продолжается до линейной. Если $b, c \in P_a$, $b \neq 1$, $c \neq 1$, но $P_b \cap P_c = 1$, то, по лемме 1, $P_bP_c^{-1}$ будет подполугруппой со свойствами 1) — 3). Частичная упорядоченность, определяемая этой подполугруппой, по условию может быть продолжена до линейной, определяемой подполугруппой положительных элементов P. Таким образом,

$$b \in P, \qquad c^{-1} \in P,$$

а поэтому $c \in P^{-1}$. Мы приходим к противоречию с тем, что или $a \in P$, т. е. $P_a \subseteq P$, и поэтому $P_a \cap P^{-1} = 1$, или же $a \in P^{-1}$, т. е. $P_a \subseteq P^{-1}$, и тогда $P_a \cap P = 1$. Этим доказано, что выполняется и свойство II.

Предположим теперь, что группа G обладает свойствами I и II и что в G взяты элемент a и подполугруппа P со свойствами 1) — 3).

Лемма 2. *Если* $P \cap P_a \neq 1$, *то* $P \cap P_a^{-1} = 1$.

В самом деле, пусть $x \in P \cap P_a$, $x \neq 1$, и вместе с тем $y \in P \cap P_a^{-1}$, $y \neq 1$. Тогда $x^{-1} \in P_{a^{-1}}$, $y \in P_a^{-1} = P_{a^{-1}}$, а поэтому, по II,

$$P_{x^{-1}} \cap P_y \neq 1.$$

Однако $x^{-1} \in P^{-1}$, $y \in P$, т. е. $P_{x^{-1}} \subseteq P^{-1}$, $P_y \subseteq P$, а поэтому $P^{-1} \cap P \neq 1$, что противоречит (2). Лемма доказана.

Для окончания доказательства теоремы возьмем в группе G любую подполугруппу P, определяющую максимальную упорядоченность. Если эта упорядоченность еще не линейная, то условие 4) из VI. 1.3 не выполняется, т. е. существует такой элемент $a \in G$, что $a \notin P$ и $a^{-1} \notin P$. В силу условия I подполугруппа P_a существует, причем, ввиду леммы 2, можно считать (заменяя, если нужно, a на a^{-1}), что $P \cap P_a^{-1} = 1$. Поэтому, по лемме 1, произведение PP_a будет подполугруппой со свойствами 1) — 3), притом строго большей чем P, что противоречит, однако, выбору подполугруппы P. Теорема доказана.

8. Из доказанного критерия вытекает следующая теорема Е. П. Шимбиревой [Мат. сб. **20** (1947), 145 — 178]:

Все максимальные упорядоченности абелевой группы без кручения линейны.

В самом деле, если a — отличный от 1 элемент абелевой группы без кручения G, то подполугруппа P_a состоит из всех степеней a^n, $n = 0, 1, 2, \ldots$ Так как, кроме того, всегда $P_1 = 1$, то условие I выполняется. Выполняется и условие II, так как если $b = a^k$, $c = a^l$, $k \geqslant 1$, $l \geqslant 1$, то $a^{kl} \neq 1$ и $a^{kl} \in P_b \cap P_c$.

Частным случаем этой теоремы является теорема Леви [Rend. Palermo **35** (1913), 225 — 236]:

Всякая абелева группа без кручения может быть линейно упорядочена.

* Существуют, притом в различных формах, необходимые и достаточные условия для того, чтобы группу можно было линейно упорядочить [Ивасава, J. Math. Soc. Jap. **1** (1948), 1 — 9; А. И. Мальцев, Изв. АН СССР, серия матем. **13** (1949), 473 — 482; В. Д. Поддерюгин, Изв. АН СССР, серия матем. **21** (1957), 199 — 208]. *

§ 2. Упорядоченные кольца

1. Все упорядоченные группы, перечисленные во втором абзаце VI.1.1, являются аддитивными группами некоторых колец или полей. Эти примеры упорядоченных колец (полей) подсказывают следующее определение, которое можно было бы сформулировать сразу для любой группы с мультиоператорами (см. III.2.1):

Кольцо R называется *линейно (частично) упорядоченным*, если линейно (частично) упорядочена его аддитивная группа (см. VI.1.1), и поэтому, по VI.1.3, можно говорить о положительных элементах, и если, сверх того, произведение положительных элементов положительно, т. е. из $a \geqslant 0$, $b \geqslant 0$ следует $ab \geqslant 0$.

Из этого определения следует, что тривиальная частичная упорядоченность аддитивной группы любого кольца будет (тривиальной же) частичной упорядоченностью самого кольца.

Требование о произведении положительных элементов, входящее в наше определение, равносильно, очевидно, тому, что если $a \leqslant b$ и $c \geqslant 0$, то $ac \leqslant bc$ и $ca \leqslant cb$. Отметим, далее, что так как из $a \geqslant 0$ следует $-a \leqslant 0$ — достаточно прибавить $-a$ к обеим частям первого неравенства, — и, обратно, из $a \leqslant 0$ следует $-a \geqslant 0$, то справедливо следующее *правило знаков*:

если $a \leqslant 0$, $b \geqslant 0$, то $ab \leqslant 0$ и $ba \leqslant 0$;
если $a \leqslant 0$, $b \leqslant 0$, то $ab \geqslant 0$.

Отсюда следует, что было бы невозможно определить упорядоченное кольцо как кольцо, в котором задана такая упорядоченность, по которой и аддитивная группа, и мультипликативный группоид этого кольца являются упорядоченными в смысле VI. 1.1.

Отметим, что в случае колец без делителей нуля условие о произведении положительных элементов, входящее в опре-

деление упорядоченного кольца, можно изложить в следующей редакции: произведение строго положительных элементов строго положительно, т. е. из $a>0$, $b>0$ следует $ab>0$. Это равносильно тому, что если $a<b$ и $c>0$, то $ac<bc$ и $ca<cb$.

Укажем, наконец, что *изоморфизм* упорядоченных колец определяется по существу так же, как в VI. 1.1 для упорядоченных группоидов.

2. Ввиду VI.1.3 любая частичная упорядоченность кольца R определяется аддитивной полугруппой положительных элементов P: $a\leqslant b$ тогда и только тогда, если $b-a\in P$. Из VI.1.3 и определения упорядоченного кольца следует:

Подполугруппа P аддитивной группы кольца R тогда и только тогда служит полугруппой положительных элементов при некоторой частичной упорядоченности этого кольца, если выполняются следующие условия:

1′) $0\in P$;

2′) *если* $a\in P$ *и* $-a\in P$, *то* $a=0$;

3′) *если* $a\in P$ *и* $b\in P$, *то* $ab\in P$.

Частичная упорядоченность кольца R, определяемая аддитивной полугруппой P со свойствами 1′)—3′), *тогда и только тогда будет линейной, если выполняется также условие*:

4′) *для любого* $a\in R$ *или* $a\in P$, *или* $-a\in P$.

3. Если $a_1, a_2, \ldots, a_n$ — отличные от нуля элементы кольца R, то под их *произведением* будем понимать сейчас всякое произведение (в неассоциативном случае — с некоторым распределением скобок), всякий множитель которого является одним из a_i, $i=1, 2, \ldots, n$, причем каждое a_i может встречаться в этом произведении несколько раз, в том числе не встречаться ни одного раза. Произведение элементов $a_1, a_2, \ldots, a_n$ будет называться *четным*, если каждое a_i, $i=1, 2, \ldots, n$, входит в него четное число раз. Наконец, говоря о *сумме произведений* некоторых элементов, мы будем считать, что все эти произведения входят в рассматриваемую сумму со знаком плюс.

Справедлива следующая теорема [см. Йонсон, Proc. Amer. Math. Soc. **3** (1952), 414—416; В. Д. Поддерюгин, Успехи мат. наук **9**:4 (1954), 211—216]:

Кольцо R тогда и только тогда является кольцом без делителей нуля, допускающим линейную упорядоченность, если всякая сумма четных произведений его элементов отлична от нуля.

В самом деле, пусть R — линейно упорядоченное кольцо без делителей нуля и пусть дано некоторое четное произведение его элементов. Это произведение не изменится, если все входящие в него отрицательные множители будут заменены противоположными элементами, а поэтому оно равно произведению строго положительных элементов, т. е., ввиду отсутствия делителей нуля, само строго положительно. Строго положительной и поэтому отличной от нуля будет, следовательно, и всякая сумма четных произведений.

4. Наоборот, если кольцо R таково, что любая сумма четных произведений его элементов отлична от нуля, то R не может содержать делителей нуля, так как из $ab=0$, $a\neq 0$, $b\neq 0$, следовало бы, что равно нулю четное произведение $(ab)(ab)$.

Назовем подмножество Q нашего кольца R *правильным*, если оно удовлетворяет следующим требованиям:

а) $0\notin Q$;

б) если $a\in Q$, то $-a\notin Q$;

в) если $a_1, a_2, \ldots, a_n\in Q$, $n\geqslant 0$, и $x_1, x_2, \ldots, x_k$ — отличные от нуля элементы из R, $k\geqslant 0$, причем $n+k>0$, а σ — некоторая сумма произведений всех этих элементов, то существует хотя бы одна такая замена элементов x_j элементами x_j', где

$$x_j'=x_j \quad \text{или} \quad x_j'=-x_j, \quad j=1, 2, \ldots, k, \tag{1}$$

после которой сумма σ будет отлична от нуля.

Лемма 1. *Пустое множество является правильным.*

В самом деле, пусть сумма σ произведений отличных от нуля элементов $x_1, x_2, \ldots, x_k\in R$, $k\geqslant 1$, остается равной нулю при любой замене вида (1). Если элемент x_1 входит в каждый член этой суммы нечетное число раз, то σx_1 будет суммой, каждый член которой содержит множитель x_1 уже четное число раз, причем эта сумма снова остается равной нулю, какая бы замена вида (1) ни была выполнена.

Пусть, с другой стороны, некоторые члены суммы σ содержат множитель x_1 четное число раз, а другие — нечетное.

Обозначим сумму первых через σ_1, сумму вторых — через σ_2:

$$\sigma = \sigma_1 + \sigma_2.$$

Таким образом, сумма $\sigma_1 + \sigma_2$ равна нулю при любой замене вида (1). Это же верно, следовательно, и для суммы, получающейся из нее после замены x_1 на $-x_1$ — эту сумму можно записать, очевидно, в виде $\sigma_1 - \sigma_2$, — а поэтому и и для суммы $2\sigma_1$, каждый член которой содержит множитель x_1 уже четное число раз.

Проделывая эти преобразования последовательно для каждого из элементов $x_1, x_2, \ldots, x_k$, мы придем, наконец, к равной нулю сумме четных произведений этих элементов, что противоречит, однако, нашим предположениям. Лемма доказана.

Лемма 2. *Если правильное множество Q не содержит ни элемента a, ни элемента $-a$, где $a \neq 0$, то хотя бы одно из объединений $Q \cup a$, $Q \cup (-a)$ будет правильным.*

Пусть существует, в самом деле, такая сумма σ_1 произведений некоторых элементов из Q, элемента a и отличных от нуля элементов

$$x_1, x_2, \ldots, x_k, \tag{2}$$

которая равна нулю, какая бы замена вида (1) для элементов (2) ни была выполнена. Пусть, с другой стороны, существует такая сумма σ_2 произведений некоторых элементов из Q, элемента a и отличных от нуля элементов

$$y_1, y_2, \ldots, y_l, \tag{3}$$

которая остается равной нулю, если элемент a заменяется на $-a$, а элементы (3) подвергаются любой замене вида (1). Тогда $\sigma_1\sigma_2$ будет такой суммой произведений некоторых элементов из Q и элементов

$$a, x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_l, \tag{4}$$

которая равна нулю при всякой замене вида (1), примененной к элементам (4). Это противоречит, однако, правильности множества Q. Лемма доказана.

5. Объединение всякой цепи правильных подмножеств нашего кольца R будет, очевидно, правильным. Поэтому, по теореме Куратовского — Цорна, в R существуют максимальные

правильные подмножества. Пусть Q — одно из них. В силу леммы 2 для всякого $a \in R$, $a \neq 0$, или a, или $-a$ принадлежит к Q.

Если $a, b \in Q$, *то и* $a+b \in Q$. Действительно, $a+b \neq 0$ ввиду б) из определения правильного множества. Если бы множество Q содержало элемент $c = -(a+b)$, то имело бы место равенство

$$a+b+c=0$$

в противоречие с правильностью множества Q.

Если $a, b \in Q$, *то и* $ab \in Q$. Действительно, $ab \neq 0$ ввиду а) из определения правильного множества и отсутствия делителей нуля. Если бы множество Q содержало элемент $d = -ab$, то имело бы место равенство

$$ab+d=0$$

в противоречие с правильностью множества Q.

Отсюда следует, что объединение $P = Q \cup 0$ будет аддитивной подполугруппой кольца R, удовлетворяющей всем условиям 1′) —4′) из VI. 2.2. Этим теорема VI. 2.3 доказана.

6. Из этой теоремы следует:

Коммутативно-ассоциативное кольцо тогда и только тогда является областью целостности, допускающей линейную упорядоченность, если никакая сумма квадратов его элементов, отличных от нуля, не будет равна нулю.

Отсюда вытекает, что поле комплексных чисел не допускает линейной упорядоченности: в этом поле имеет место равенство

$$1^2+i^2=0.$$

* Поле степенных рядов над упорядоченным полем P (см. II. 5.7), а поэтому и поле рациональных дробей над таким полем P — могут быть линейно упорядочены. *

7. *Если линейно упорядоченное кольцо* R *обладает единицей, то оно обладает подкольцом, изоморфным кольцу целых чисел с его обычной упорядоченностью.*

В самом деле, единица должна быть строго положительной, так как она совпадает со своим квадратом. Строго положительны, следовательно, и все положительные кратные единицы, которые все различны в силу VI. 1.4.

Отсюда следует, *что обычная упорядоченность кольца целых чисел является его единственной возможной линейной упорядоченностью.*

* Кольцо целых чисел является единственным линейно упорядоченным кольцом без делителей нуля и с единицей, упорядоченное подмножество положительных элементов которого вполне упорядочено (см. I. 5.4). *

8. *Упорядоченность области целостности R может быть распространена, и притом единственным способом, на ее поле дробей $\bar{R}$.*

Предположим сперва, что упорядоченность кольца R уже распространена на поле $\bar{R}$. Если $\frac{a}{b} > 0$, то, так как из $b \neq 0$ следует $b^2 > 0$, мы получаем, что

$$\frac{a}{b} \cdot b^2 = ab > 0.$$

Обратно, если $ab > 0$ в R, то, так как $(b^{-1})^2 > 0$, будет

$$ab \cdot (b^{-1})^2 = \frac{a}{b} > 0.$$

Отсюда уже вытекает единственность возможного распространения упорядоченности с R на $\bar{R}$.

Для доказательства существования такого распространения положим, что $\frac{a}{b} > 0$ тогда и только тогда, если $ab > 0$. Если $\frac{a}{b} = \frac{c}{d}$, т. е. $ad = bc$ (см. II. 5.2), то $abd^2 = b^2cd$. Поэтому, ввиду $d^2 > 0$, $b^2 > 0$, из $ab > 0$ будет следовать $cd > 0$, т. е. $\frac{c}{d} > 0$; наше определение строгой положительности в поле $\bar{R}$ является, следовательно, законным.

Если $a, b \in R$, причем $a \neq 0$, $b \neq 0$, то лишь один из элементов ab, $(-a)b$ будет в R строго положительным, а поэтому или $\frac{a}{b} > 0$, или же $-\frac{a}{b} = \frac{-a}{b} > 0$ (см. II. 5.4), причем эти случаи исключают друг друга.

Если $\frac{a}{b} > 0$, $\frac{c}{d} > 0$, т. е. $ab > 0$, $cd > 0$, то $abd^2 > 0$, $b^2cd > 0$, откуда

$$(ad + bc)\, bd = abd^2 + b^2cd > 0,$$

т. е. (см. II. 5.4)

$$\frac{a}{b}+\frac{c}{d}>0.$$

При тех же предположениях будет

$$(ac)(bd)=(ab)(cd)>0,$$

т. е. (см. II. 5.2)

$$\frac{a}{b}\cdot\frac{c}{d}>0.$$

Этим доказано, что множество P, состоящее из нуля и всех строго положительных элементов поля $\bar{R}$, удовлетворяет всем условиям из VI. 2.2, т. е. определяет в $\bar{R}$ линейную упорядоченность. Эта упорядоченность является распространением заданной линейной упорядоченности кольца R, так как, по II. 5.2,

$$a=\frac{ab}{b},\quad b\neq 0,$$

но из $a>0$ следует $(ab)b=ab^2>0$ и обратно.

Из этой теоремы и VI. 2.7 вытекает, что *обычная упорядоченность поля рациональных чисел является его единственной возможной линейной упорядоченностью.*

Так как аддитивная группа любого линейно упорядоченного тела K является, по VI.1.4, группой без кручения, то K будет телом без характеристики (см. III. 2.11), т. е., ввиду сказанного выше, *всякое линейно упорядоченное тело K содержит в качестве простого подполя поле рациональных чисел с его обычной упорядоченностью.*

9. *Упорядоченное множество Q строго положительных элементов любого линейно упорядоченного ассоциативного тела K составляет по умножению линейно упорядоченную группу.*

Действительно, из VI. 2.7 мы знаем, что единица тела K принадлежит к Q. Далее, если $a\in Q$, т. е. $a>0$, то и $a^{-1}\in Q$, так как из $a^{-1}<0$ следовало бы, по VI. 2.1, что $aa^{-1}=1<0$. Множество Q оказывается, следовательно, мультипликативной группой. Остальные утверждения теоремы следуют из определения упорядоченности кольца без делителей нуля (см. VI. 2.1).

* Всякая линейно упорядоченная группа может быть изоморфно вложена в линейно упорядоченную мультипликативную группу строго положительных элементов некоторого линейно упорядоченного ассоциативного тела [А. И. Мальцев, Докл. АН СССР **60** (1948), 1499—1501; Нейман, Trans. Amer. Math. Soc. **66** (1949), 202—252]. *

§ 3. Архимедовы группы и кольца

1. Подмножество N частично упорядоченного множества M называется *выпуклым*, если оно вместе со всякими своими сравнимыми элементами a и b, $a<b$, содержит и все элементы x множества M, удовлетворяющие неравенствам $a\leqslant x\leqslant b$.

Подгруппа A частично упорядоченной группы G тогда и только тогда будет выпуклой, если в ней вместе со всяким положительным элементом a содержатся все положительные элементы x группы G, удовлетворяющие неравенству $x\leqslant a$.

В самом деле, неравенства $a\leqslant x\leqslant b$ и $1\leqslant a^{-1}x\leqslant a^{-1}b$ равносильны.

Пусть G и G' — частично упорядоченные группы, P и P' — их полугруппы положительных элементов, φ — отображение G на G'. Отображение φ мы назовем *монотонным гомоморфизмом*, если оно является гомоморфизмом в теоретико-групповом смысле и если, сверх того, $P\varphi=P'$. Этим не утверждается, конечно, что P служит для P' полным прообразом — достаточно вспомнить 2) из VI. 1.3.

Ядро A монотонного гомоморфизма φ является выпуклым нормальным делителем.

Пусть, в самом деле, $a\in A$, $a\geqslant 1$ и $x\in G$, $1\leqslant x\leqslant a$. Из $x\geqslant 1$ и определения гомоморфизма φ следует

$$x\varphi\geqslant 1'. \tag{1}$$

С другой стороны, так как $x^{-1}a\geqslant 1$ и $a\varphi=1'$, то

$$1'\leqslant(x^{-1}a)\varphi=(x\varphi)^{-1}(a\varphi)=(x\varphi)^{-1}. \tag{2}$$

Из (1) и (2) следует $x\varphi=1'$, т. е. $x\in A$.

Если A — выпуклый нормальный делитель частично упорядоченной группы G, то фактор-группу $G'=G/A$ можно так частично упорядочить, что естественное

гомоморфное отображение G на G' будет монотонным гомоморфизмом.

Действительно, если P — полугруппа положительных элементов группы G, то обозначим через P' совокупность смежных классов по A, содержащих хотя бы по одному элементу из P. Теорема будет доказана, если мы покажем, что P' является подполугруппой группы G' и обладает свойствами 1) — 3) из VI.1.3. Требует проверки, впрочем, лишь свойство 2), так как остальные утверждения очевидны.

Пусть $p \in P$, т. е. $pA \in P'$, и пусть вместе с тем $(pA)^{-1} = p^{-1}A \in P'$. Существует, следовательно, такой элемент $p_0 = p^{-1}a$, что $p_0 \in P$, $a \in A$. Поэтому $pp_0 = a$, т. е. $a \geqslant 1$, а так как $1 \leqslant p_0$, то

$$p \leqslant pp_0 = a.$$

Отсюда, ввиду неравенства $1 \leqslant p$ и выпуклости A, следует $p \in A$, т. е. $pA = A$, что и требовалось доказать.

2. Выпуклыми подгруппами любой частично упорядоченной группы G являются сама группа G и единичная подгруппа E. Из определения выпуклой подгруппы следует, что пересечение любого множества выпуклых подгрупп и объединение любой цепи выпуклых подгрупп сами будут выпуклыми.

Выпуклые подгруппы линейно упорядоченной группы G составляют цепь по теоретико-множественному включению.

Пусть, в самом деле, в группе G взяты выпуклые подгруппы A и B, причем в B содержится элемент b, лежащий вне A; без ограничения общности можно считать, что $b > 1$. Если бы в A существовал такой элемент a, что $b < a$, то, ввиду выпуклости A, было бы $b \in A$ против предположения. Таким образом, все положительные элементы подгруппы A будут меньше b, т. е., ввиду выпуклости B, все они принадлежат к B, а поэтому $A \subset B$. Теорема доказана.

Если a — строго положительный элемент линейно упорядоченной группы G, то множество A, состоящее из всех таких элементов x, что $1 \leqslant x \leqslant a^n$ при некотором натуральном n, и элементов, им обратных, будет минимальной выпуклой подгруппой, содержащей элемент a.

Все указанные элементы действительно должны принадлежать ко всякой выпуклой подгруппе, содержащей a. Пусть,

далее,

$$\left.\begin{aligned} 1 \leqslant x \leqslant a^k, \\ 1 \leqslant y \leqslant a^l \end{aligned}\right\} \tag{3}$$

при некоторых натуральных k и l. Тогда, по (1) из VI. 1.1,

$$1 \leqslant xy \leqslant a^{k+l},$$

т. е. $xy \in A$, а поэтому и $(xy)^{-1} = y^{-1}x^{-1} \in A$. С другой стороны, из (3) следует

$$a^{-l} \leqslant y^{-1} \leqslant 1,$$

а поэтому

$$a^{-l} \leqslant xy^{-1} \leqslant a^k.$$

Таким образом, если $1 \leqslant xy^{-1}$, то $xy^{-1} \in A$. Если же $xy^{-1} < 1$, то

$$1 < (xy^{-1})^{-1} \leqslant a^l,$$

т. е. $(xy^{-1})^{-1} \in A$, а тогда и $xy^{-1} \in A$. Теперь очевидно, что A является подгруппой, притом содержащей a и выпуклой.

3. Строго положительные элементы a и b линейно упорядоченной группы G называются относящимися к одному *архимедову классу*, если они порождают одну и ту же выпуклую подгруппу группы G. Все строго положительные элементы распадаются, следовательно, на непересекающиеся архимедовы классы. Удобно считать также, что элемент 1 составляет отдельный архимедов класс.

Множество архимедовых классов группы G линейно упорядочивается в соответствии с естественной линейной упорядоченностью скачков (т. е. пар соседних подгрупп) в цепи выпуклых подгрупп группы G.

Линейно упорядоченная группа G называется *архимедовой*, если в ней нет выпуклых подгрупп, отличных от G и E. Из последней из теорем VI.3.2 следует:

Линейно упорядоченная группа G тогда и только тогда будет архимедовой, если для любой пары a, b ее строго положительных элементов можно указать такое натуральное число $n = n(a, b)$, что $a^n > b$.

Примерами архимедовых групп служат подгруппы аддитивной группы действительных чисел с их естественной упорядоченностью.

4. Теорема Гельдера. *Всякая архимедова группа коммутативна и изоморфна некоторой подгруппе аддитивной группы действительных чисел с ее естественной упорядоченностью.*

Пусть архимедова группа G обладает минимальным строго положительным элементом a. Если b — любой строго положительный элемент из G, то существует такое натуральное число n, что

$$a^n \leqslant b < a^{n+1}.$$

Отсюда

$$1 \leqslant ba^{-n} < a,$$

а поэтому $ba^{-n} = 1$, т. е. $b = a^n$. Все строго положительные элементы группы G исчерпываются, следовательно, степенями элемента a, а так как, по VI.1.1,

$$1 < a < a^2 < \ldots < a^n < \ldots,$$

то G оказывается изоморфной аддитивной группе целых чисел с ее естественной упорядоченностью.

Предположим теперь, что среди строго положительных элементов архимедовой группы G нет минимального. В этом случае для всякого $a > 1$ существует такое $b > 1$, что $b^2 \leqslant a$. Действительно, существует такой элемент c, что

$$1 < c < a,$$

откуда $1 < c^{-1}a$. Если $c^2 \leqslant a$, то $b = c$. Если же $c^2 > a$, то $1 > c^{-1}ac^{-1}$, т. е. $a > (c^{-1}a)^2$ и поэтому $b = c^{-1}a$.

Для доказательства коммутативности группы G достаточно показать перестановочность любой пары ее строго положительных элементов a, b. Если $ab \neq ba$, то без ограничения общности можно положить, что

$$c = a^{-1}b^{-1}ab > 1.$$

Как доказано, существует такой элемент d, что $1 < d$ и $d^2 \leqslant c$. Можно считать при этом, что $d < a$ и $d < b$, а поэтому существуют такие натуральные числа k и l, что

$$d^k \leqslant a < d^{k+1}, \quad d^l \leqslant b < d^{l+1}.$$

Отсюда

$$ab < d^{k+l+2},$$

$$a^{-1}b^{-1} \leqslant d^{-(k+l)},$$

т. е.

$$c < d^2,$$

а так как, по условию, $d^2 \leqslant c$, то мы приходим к противоречию. Коммутативность группы G доказана.

5. Нам удобно перейти теперь к аддитивной записи операции в группе G. Фиксируем в G некоторый строго положительный элемент e и поставим в соответствие всякому элементу $a \in G$ класс U_a всех таких рациональных чисел $\frac{m}{n}$, $n > 0$, для которых

$$me \leqslant na. \tag{4}$$

Если $\frac{m}{n} \in U_a$ и $\frac{p}{q} \leqslant \frac{m}{n}$, то и $\frac{p}{q} \in U_a$, так как из (4) и $pn \leqslant qm$ следует

$$(pn)\, e \leqslant (qm)\, e \leqslant (qn)\, a,$$

откуда

$$pe \leqslant qa.$$

В частности, если $\frac{m}{n} \in U_a$ и $\frac{p}{q} = \frac{m}{n}$, то и $\frac{p}{q} \in U_a$, т. е. класс U_a на самом деле можно считать множеством рациональных чисел.

Класс U_a содержит не все рациональные числа: ввиду архимедовости группы G существует такое натуральное число m, что $me > a$, а поэтому $m \notin U_a$. Класс U_a является, следовательно, первым классом некоторого сечения в системе рациональных чисел, т. е. определяет, в силу дедекиндовой теории действительных чисел, некоторое действительное число α. Положим

$$\alpha = a\theta.$$

6. Если $a \leqslant b$, то $a\theta \leqslant b\theta$, так как из (4) и $a \leqslant b$ следует

$$me \leqslant nb,$$

т. е. $U_a \subseteq U_b$.

Докажем, далее, что

$$(a + b)\,\theta = a\theta + b\theta. \tag{5}$$

Действительно, если

$$\frac{m}{n} \in U_a, \quad \frac{p}{q} \in U_b,$$

т. е.

$$me \leqslant na, \quad pe \leqslant qb,$$

то

$$(mq + np)\, e \leqslant nq\,(a + b),$$

откуда

$$\frac{mq+np}{nq} = \frac{m}{n} + \frac{p}{q} \in U_{a+b}.$$

С другой стороны, таким же путем может быть показано, что если

$$\frac{m}{n} \notin U_a, \quad \frac{p}{q} \notin U_b,$$

то и

$$\frac{m}{n} + \frac{p}{q} \notin U_{a+b},$$

откуда следует (5).

Отображение θ является, следовательно, монотонным гомоморфным отображением группы G на некоторую подгруппу аддитивной группы действительных чисел. При этом гомоморфизме в нуль переходит лишь нуль группы G: если $a > 0$, то, ввиду архимедовости группы G, существует такое натуральное число m, что $ma > e$, т. е. $\frac{1}{m} \in U_a$, а поэтому $a\theta > 0$. Гомоморфизм θ будет, следовательно, изоморфизмом, притом сохраняющим отношение порядка. Теорема доказана.

Отметим, что подгруппа $G\theta$ аддитивной группы действительных чисел, на которую нами изоморфно отображена аддитивная группа G, содержит число 1, так как $e\theta = 1$.

7. Лемма. *Если A и B — подгруппы аддитивной группы действительных чисел с ее естественной упорядоченностью, а φ — монотонный гомоморфизм A на B, то существует такое действительное число r, $r \geqslant 0$, что для всех $a \in A$*

$$a\varphi = ar. \tag{6}$$

Действительно, если существует такое $a \in A$, $a > 0$, что $a\varphi = 0$, то и $(na)\varphi = 0$ для всех натуральных n, т. е. $B = A\varphi = 0$. В этом случае $r = 0$.

Предположим поэтому, что φ является изоморфизмом. Если $a_1, a_2 \in A$, $a_1 > 0$, $a_2 > 0$, то и $a_1\varphi > 0$, $a_2\varphi > 0$. Если $\frac{a_1\varphi}{a_2\varphi} < \frac{a_1}{a_2}$, то существует такое положительное рациональное

число $\frac{m}{n}$, что

$$\frac{a_1\varphi}{a_2\varphi} < \frac{m}{n} < \frac{a_1}{a_2}. \tag{7}$$

Отсюда $na_1 > ma_2$, т. е. $n(a_1\varphi) > m(a_2\varphi)$, хотя из (7) следует $n(a_1\varphi) < m(a_2\varphi)$. К такому же противоречию мы придем и в предположении, что $\frac{a_1\varphi}{a_2\varphi} > \frac{a_1}{a_2}$. Таким образом,

$$\frac{a_1\varphi}{a_2\varphi} = \frac{a_1}{a_2},$$

а тогда

$$r = \frac{a\varphi}{a}, \quad a \in A, \quad a > 0.$$

Действительно, если $a' < 0$, то

$$a'\varphi = -(-a')\varphi = -(-a')r = a'r,$$

т. е. число r удовлетворяет условию (6) для всех элементов из A. Лемма доказана.

Назовем гомоморфизм φ линейно упорядоченной группы G на линейно упорядоченную группу G' *инверсным гомоморфизмом*, если из $a \in G$, $a \geqslant 0$ следует $a\varphi \leqslant 0$. *Доказанная нами лемма справедлива и тогда, если* φ *— инверсный гомоморфизм; в этом случае, однако,* $r \leqslant 0$.

В самом деле, если φ — инверсный гомоморфизм A на B, то отображение $-\varphi$, где

$$a(-\varphi) = -a\varphi, \quad a \in A,$$

будет монотонным гомоморфизмом. Существует, следовательно, такое действительное число r, $r \geqslant 0$, что

$$a(-\varphi) = ar, \quad a \in A,$$

но тогда

$$a\varphi = -[a(-\varphi)] = -ar = a(-r), \quad a \in A,$$

где $-r \leqslant 0$.

8. Линейно упорядоченное кольцо R называется *архимедовым*, если его аддитивная группа является архимедовой. Справедлива следующая теорема [Я. В. Хион, Успехи мат. наук **9**:4 (1954), 237—242; Таллини, Atti Accad. Naz. Lincei, Rend. **18** (1955), 367—373]:

Всякое архимедово кольцо R ассоциативно и коммутативно. Больше того, оно или является нулевым кольцом на некоторой подгруппе аддитивной группы действительных чисел, или же изоморфно некоторому подкольцу поля действительных чисел с его естественной упорядоченностью.

Действительно, на основании теоремы Гельдера (см. VI.3.4) можно считать, что аддитивная группа кольца R уже является подгруппой аддитивной группы действительных чисел. Однако, умножение в R не будет, вообще говоря, совпадать с обычным умножением действительных чисел и, в отличие от последнего, мы будем записывать его через $a \cdot b$.

Если $a \in R$, то преобразование $x \to x \cdot a$, $x \in R$, будет эндоморфизмом аддитивной группы кольца R, монотонным при $a \geqslant 0$ и инверсным при $a \leqslant 0$. Поэтому, по VI.3.7, существует такое действительное число r_a, что

$$x \cdot a = x r_a, \quad x \in R,$$

причем из $a \geqslant 0$ следует $r_a \geqslant 0$.

Так как для всех $x \in R$

$$x \cdot (a+b) = x \cdot a + x \cdot b = x r_a + x r_b = x (r_a + r_b),$$

т. е. $r_{a+b} = r_a + r_b$, то отображение $a \to r_a$ будет монотонным гомоморфизмом аддитивной группы кольца R в аддитивную группу действительных чисел. Поэтому, по лемме, существует такое действительное число s, $s \geqslant 0$, что для всех $a \in R$

$$r_a = as.$$

Если $s = 0$, то $r_a = 0$ для всех a, т. е. R будет нулевым кольцом. Если же $s > 0$, то отображение $a \to r_a$ будет монотонным изоморфизмом аддитивной группы. Вместе с тем из

$$a \cdot b = a r_b = a (bs) = (ab) s$$

следует

$$r_{a \cdot b} = (a \cdot b) s = [(ab) s] s = (as)(bs) = r_a r_b.$$

Таким образом, при $s > 0$ соответствие $a \to r_a$ отображает кольцо R монотонно и изоморфно на некоторое подкольцо поля действительных чисел с его естественной упорядоченностью. Теорема доказана.

§ 4. Нормированные кольца

1. В поле действительных чисел определено понятие абсолютной величины, в поле комплексных чисел — понятие модуля. Вспоминая привычные свойства этих понятий и учитывая, в частности, что и абсолютная величина и модуль являются неотрицательными действительными числами, а поле действительных чисел линейно упорядочено, мы приходим к следующему общему определению:

Пусть W — линейно упорядоченное кольцо (см. VI.2.1). Некоторое кольцо R будет называться *нормированным кольцом со значениями нормы в кольце* W, если всякому элементу $a \in R$ поставлен в соответствие некоторый элемент $w(a) \in W$ — *норма* элемента a, — причем выполняются следующие условия:

1. $w(0) = 0$; $w(a) > 0$ при $a \neq 0$;
2. $w(ab) = w(a)\,w(b)$;
3. $w(a - b) \leqslant w(a) + w(b)$.

Из 3 и 1 следует, что для всех $b \in R$ будет $w(-b) \leqslant w(b)$, а так как $b = -(-b)$, то

3_1. $w(-b) = w(b)$, $b \in R$.

Отсюда вытекает

3_2. $w(a + b) \leqslant w(a) + w(b)$.

Помимо полей действительных и комплексных чисел *примерами нормированных тел с действительной нормой могут служить тело кватернионов и алгебра Кэли.* Именно, в этих телах в качестве нормы элемента α нужно взять квадратный корень из той нормы $n(\alpha)$, которая введена соответственно в V.6.9 и V.6.11. Так определенная норма будет совпадать с длиною вектора α соответственно в четырех- и восьмимерном евклидовом пространстве, а поэтому условие 3 выполняется. Выполнение условия 1 очевидно, справедливость же условия 2 вытекает из равенств (8) и (15) § 6 гл. V.

Всякое линейно упорядоченное кольцо R можно нормировать со значениями нормы в самом кольце R.

Действительно, назовем *абсолютной величиной* $|a|$ элемента $a \in R$ положительный из числа элементов a и $-a$. Абсолютная величина удовлетворяет требованиям, входящим в определение нормы. В самом деле, выполнение условия 1

очевидно. Условие 2 легко следует из правила знаков (см. VI.2.1):

если $a \geqslant 0$, $b \geqslant 0$, то $|a| \cdot |b| = ab = |ab|$;
если $a \leqslant 0$, $b \geqslant 0$, то $|a| \cdot |b| = (-a)b = -ab = |ab|$;
если $a \leqslant 0$, $b \leqslant 0$, то $|a| \cdot |b| = (-a)(-b) = ab = |ab|$.

Покажем, что выполняется и условие 3. Если $a \geqslant b \geqslant 0$, то $b \geqslant -b$ и $a+b \geqslant a-b$, а поэтому

$$|a-b| = a-b \leqslant a+b = |a|+|b|.$$

Если $a \geqslant 0 \geqslant b$, то

$$|a-b| = a-b = a+(-b) = |a|+|b|.$$

Если $0 \geqslant a \geqslant b$, то $-a \geqslant a$ и $-a-b \geqslant a-b$, а поэтому

$$|a-b| = a-b \leqslant -a-b = |a|+|b|.$$

Если $b \geqslant a \geqslant 0$, то $a \geqslant -a$ и $a+b \geqslant b-a$, а поэтому

$$|a-b| = -(a-b) = b-a \leqslant a+b = |a|+|b|.$$

Если $b \geqslant 0 \geqslant a$, то

$$|a-b| = b-a = b+(-a) = |a|+|b|.$$

Если, наконец, $0 \geqslant b \geqslant a$, то $b \leqslant -b$ и $b-a \leqslant -a-b$, а поэтому

$$|a-b| = b-a \leqslant -a-b = |a|+|b|.$$

Теорема доказана.

2. Во всех примерах, рассмотренных выше, все положительные элементы кольца W служат нормами некоторых элементов кольца R. В этом случае мы будем говорить, что W является *кольцом значений* нормы.

Пусть R — нормированное кольцо с кольцом значений W. *Если кольцо R обладает единицей* 1, *то $w(1)$ служит единицей кольца W.* Действительно, если $a \in R$, то

$$w(a) = w(a \cdot 1) = w(a) \cdot w(1),$$

т. е. $w(1)$ служит единицей для всех положительных элементов из W, а поэтому и для элементов, им противоположных.

Кольца R и W одновременно обладают или не обладают делителями нуля.

В самом деле, если $a, b \in R$, $a \neq 0$, $b \neq 0$, но $ab = 0$, то $w(a) > 0$, $w(b) > 0$, но

$$w(a)\, w(b) = w(ab) = 0.$$

Обратно, если кольцо W обладает делителями нуля, то в нем можно найти такие строго положительные элементы α, β, что $\alpha\beta = 0$. Тогда в R существуют такие элементы a, b, что $w(a) = \alpha$, $w(b) = \beta$, и поэтому $a \neq 0$, $b \neq 0$. Однако

$$w(ab) = w(a)\, w(b) = \alpha\beta = 0,$$

откуда $ab = 0$.

Если кольцо R коммутативно или ассоциативно, то это же можно утверждать и для кольца W.

В самом деле, справедливость закона коммутативности или ассоциативности для положительных элементов кольца W немедленно следует из условия 2 в определении нормированного кольца, все же другие элементы кольца W являются противоположными для положительных элементов.

Из этих же соображений вытекает и следующее утверждение:

Если R является кольцом с делением (или кольцом с однозначным делением, или телом), то это же верно и для W.

3. Если линейно упорядоченное кольцо W обладает единицей 1, то любое кольцо R допускает следующее *тривиальное нормирование* со значениями в W:

$$w(0) = 0, \quad w(a) = 1 \text{ для всех } a \in R,\ a \neq 0.$$

Ясно, что все условия 1—3 из VI.4.1 выполняются. Выполняется даже следующее условие, более сильное, чем условие 3:

3′. $w(a - b) \leqslant \max(w(a), w(b))$.

Отсюда, как и раньше, следует

3′$_1$. $w(-b) = w(b)$,

а поэтому

$$w(a + b) = w[a - (-b)] \leqslant \max(w(a), w(-b)) = \max(w(a), w(b)),$$

т. е.

3′$_2$. $w(a + b) \leqslant \max(w(a), w(b))$.

Нормирование, подчиненное условиям 1, 2 и 3′, называется *неархимедовым*, в противоположность *архимедову нормированию*, при котором условие 3′ не выполняется и

имеет место лишь условие 3. Перечисленные в VI.4.1 обычные нормирования полей действительных и комплексных чисел, тела кватернионов и алгебры Кэли являются архимедовыми. Таково же и указанное в VI.4.1 нормирование линейно упорядоченного кольца.

4. В определении неархимедова нормирования, т. е. в аксиомах 1, 2 и 3′, используются лишь упорядоченность и умножение положительных элементов кольца W. Это определение можно дословно перенести поэтому на случай нормирования кольца R элементами некоторого линейно упорядоченного мультипликативного группоида G с нулем, т. е. с таким элементом 0, что для всех $x \in G$, $0 \leqslant x$,

$$x \cdot 0 = 0 \cdot x = 0.$$

Именно в таком смысле будут пониматься дальше *неархимедовы нормирования* кольца R. Мы будем при этом говорить о нормировании кольца R с *группоидом значений* G, если всякий элемент из G служит нормой некоторого элемента из R.

Пусть в кольце R задано неархимедово нормирование $w(a)$ с группоидом значений G. В этом случае имеют место результаты, аналогичные указанным в VI.4.2 и доказываемые теми же рассуждениями. Можно отметить, впрочем, что в рассматриваемом нами случае норма определяет гомоморфное отображение мультипликативного группоида кольца R на группоид G.

Если кольцо R обладает единицей 1, *то* $w(1)$ *служит единицей группоида* G.

Кольцо R и группоид G одновременно обладают или не обладают делителями нуля — смысл понятия делителей нуля в группоиде с нулем очевиден.

Если кольцо R ассоциативно, то группоид G будет полугруппой. Из коммутативности кольца R следует коммутативность G.

Если R является ассоциативным телом, то отличные от нуля элементы из G составляют группу по умножению, заданному в G.

5. Пусть R — линейно упорядоченное кольцо, G — упорядоченное множество архимедовых классов его аддитивной группы (см. VI.3.3); класс, содержащий элемент $a \in R$, $a \geqslant 0$, будем обозначать через $\bar{a}$. Если a, $b \in R$, $a \geqslant 0$, $b \geqslant 0$,

откуда $ab \geqslant 0$, то положим

$$\bar{a}\bar{b} = \overline{ab}. \tag{1}$$

Равенство (1) *превращает множество* G *в линейно упорядоченный группоид с нулем, называемый группоидом архимедовых классов кольца* R.

Действительно, если $\bar{a}_1 = \bar{a}_2$, то пусть, например, $a_1 \leqslant a_2$. Существует, однако, такое натуральное число n, что $a_2 \leqslant na_1$, а поэтому ввиду $b \geqslant 0$,

$$a_1 b \leqslant a_2 b \leqslant n(a_1 b),$$

откуда $\overline{a_1 b} = \overline{a_2 b}$. Этим доказано, что равенство (1) на самом деле является определением умножения в множестве G.

Далее, если $\bar{a}_1 < \bar{a}_2$, то $a_1 < a_2$, а поэтому для любого $b \geqslant 0$

$$a_1 b \leqslant a_2 b, \quad ba_1 \leqslant ba_2,$$

откуда для любого $\bar{b} \in G$

$$\bar{a}_1 \bar{b} \leqslant \bar{a}_2 \bar{b}, \quad \bar{b}\bar{a}_1 \leqslant \bar{b}\bar{a}_2.$$

Таким образом, группоид G оказывается линейно упорядоченным (см. VI.1.1).

Наконец, класс $\bar{0}$ будет, очевидно, нулем линейно упорядоченного группоида G.

Справедлива следующая теорема [Я. В. Хион, Изв. АН СССР, серия матем. **21** (1957), 311—328]:

Всякое линейно упорядоченное кольцо R *допускает неархимедово нормирование со своим группоидом архимедовых классов в качестве группоида значений.*

В самом деле, для каждого $a \in R$ возьмем в качестве $w(a)$ тот архимедов класс, к которому принадлежит абсолютная величина $|a|$ (см. VI.4.1). Условие 1 выполняется очевидным образом, справедливость условия 2 следует из справедливости этого условия для абсолютной величины и равенства (1). Покажем, что выполняется и условие 3′. Действительно, ввиду $|-b| = |b|$ и VI.4.1,

$$|a-b| = |a+(-b)| \leqslant |a| + |b| \leqslant 2 \max(|a|, |b|),$$

а поэтому

$$|\overline{a-b}| \leqslant \max(|\bar{a}|, |\bar{b}|),$$

т. е.

$$w(a-b) \leqslant \max(w(a), w(b)).$$

6. Пусть в кольце R задана неархимедова норма со значениями в линейно упорядоченном группоиде G с нулем. Перейдем в группоиде G от мультипликативной записи операции, как до сих пор предполагалось, к аддитивной записи и, кроме того, заменим упорядоченность в G на инверсную (ср. I.4.6). Элемент 0 естественно обозначить теперь символом ∞, причем для всех $x \in G$

$$\infty \geqslant x, \qquad x + \infty = \infty + x = \infty. \tag{2}$$

Неархимедово нормирование, заданное в кольце R, превращается этим путем в так называемое *логарифмическое нормирование* со значениями в аддитивном группоиде G, причем условия 1, 2 и 3′ принимают вид:

1_0. $w(0) = \infty$, $w(a) < \infty$ при $a \neq 0$;

2_0. $w(ab) = w(a) + w(b)$;

$3'_0$. $w(a - b) \geqslant \min\,(w(a), w(b))$.

Обратный переход также, конечно, возможен.

Если в R было задано неархимедово нормирование с (неотрицательными) действительными значениями, то полученное из него логарифмическое нормирование также можно считать действительным, а именно со значениями в упорядоченной аддитивной группе действительных чисел, пополненной символом ∞. В самом деле, описанное выше преобразование группоида значений нормы можно в рассматриваемом случае получить, заменив всякое положительное действительное число α числом $-\ln \alpha$.

Возьмем поле P и рассмотрим в качестве R любое из следующих трех колец: *кольцо многочленов* $P[x]$ (см. II.2.7), *кольцо степенных рядов* $P\{x\}$ (см. II.2.8), *поле лорановых степенных рядов* (см. II.5.7). Если $a \in R$, $a \neq 0$, то пусть $w(a)$ будет показатель наименьшей степени неизвестного x, входящей в запись многочлена (ряда) a с отличным от нуля коэффициентом; положим, кроме того, $w(0) = \infty$. *Этим в кольце R вводится целочисленное логарифмическое нормирование* — проверка условий 1_0, 2_0, $3'_0$ не представляет затруднений.

7. Возвращаясь к общему понятию нормирования (см. VI.4.1), отметим, что иногда условие 2 заменяется более слабым условием

$2'$. $w(ab) \leqslant w(a)\,w(b)$.

В этом случае говорят о *псевдонормировании.*

Важные примеры псевдонормированных колец представляют некоторые кольца функций. Так, рассмотрим кольцо всех непрерывных действительных функций $f(x)$, определенных на отрезке [0, 1] числовой прямой. Полагая

$$w(f) = \max_{x \in [0,1]} |f(x)|,$$

мы вводим в это кольцо действительную псевдонорму, так как условия 1, 2′ (но не 2) и 3 выполняются.

§ 5. Логарифмические нормирования полей

1. Логарифмические нормирования существенно используются в теории полей и теории областей целостности, причем их применения основываются, в частности, на излагаемых в этом параграфе понятиях и результатах.

Пусть в поле P задано логарифмическое нормирование w (см. VI.4.6) с группоидом значений G. Из результатов, указанных в VI.4.4, и определения логарифмической нормы вытекает, что G будет аддитивно записанной линейно упорядоченной абелевой группой, пополненной символом ∞.

Обозначим через R_w множество всех тех элементов $a \in P$, для которых $w(a) \geqslant 0$. Ввиду 1_0, 2_0 и $3_0'$ R_w будет подкольцом поля P; оно называется *кольцом нормирования* w в поле P.

Так как норма w определяет гомоморфное отображение мультипликативной группы поля P на группу G, то единица поля P принадлежит к R_w.

С другой стороны, если $a \in P$, то $w(a) = 0$ тогда и только тогда, если и a, и a^{-1} принадлежат к R_w, т. е. если a является обратимым элементом кольца R_w, так как

$$w(1) = 0. \tag{1}$$

2. *Пусть в поле P заданы логарифмические нормирования w и w' с группами значений G и G', пополненными символом ∞, соответственно. Кольца этих нормирований, рассматриваемые как подкольца поля P, тогда и только тогда совпадают,*

$$R_w = R_{w'}, \tag{2}$$

когда существует такое изоморфное отображение φ упорядоченной группы G на упорядоченную группу G', что для

всех отличных от нуля элементов $a \in P$

$$(w(a))\varphi = w'(a). \tag{3}$$

Действительно, пусть имеет место равенство (2) и пусть $w(a)=0$. Тогда, как отмечено выше, a будет обратимым элементом кольца R_w и, следовательно, кольца $R_{w'}$, т. е. $w'(a)=0$. Верно, конечно, и обратное утверждение.

Таким образом, нормирования w и w' определяют такие гомоморфизмы мультипликативной группы поля P, которые обладают одним и тем же ядром. Поэтому, по III. 2.6, существует изоморфизм φ группы G на группу G', удовлетворяющий условию (3).

Наконец, если $\alpha \in G$ и $\alpha \geqslant 0$, то в R_w существует такой элемент a, что $w(a)=\alpha$. Из (2) следует тогда, что $w'(a)=\alpha\varphi \geqslant 0$ в G'. Изоморфизм φ отображает, таким образом, положительные элементы группы G на положительные элементы G' и, следовательно, удовлетворяет всем требованиям теоремы.

Обратное утверждение теоремы очевидно.

3. Мы видим, что обозрение всех возможных логарифмических нормирований поля P сводится на обозрение всех таких подколец этого поля, которые могут служить для него кольцами нормирования.

Подкольцо R *поля* P *тогда и только тогда может служить для этого поля кольцом нормирования, если для всякого* $a \in P$, $a \neq 0$, *хотя бы один из элементов* a, a^{-1} *принадлежит к* R.

В одну сторону утверждение теоремы почти очевидно: если $a \notin R_w$, т. е. $w(a) < 0$, то из (1) следует $w(a^{-1}) > 0$, а поэтому $a^{-1} \in R_w$.

Пусть теперь подкольцо R удовлетворяет условию теоремы. Оно содержит, следовательно, единицу поля P. Множество S обратимых элементов кольца R будет, очевидно, подгруппой мультипликативной группы P^* поля P. Обозначим через G фактор-группу P^*/S, записанную аддитивно.

Так как кольцо R не содержит делителей нуля, то отличные от нуля элементы из R составляют подполугруппу R^* группы P^*. Ввиду включения $S \subset R^*$ в группе $G=P^*/S$ выделяется подполугруппа $H=R^*/S$. Покажем, что H служит полугруппой положительных элементов при некоторой линейной упорядоченности группы G, т. е. проверим условия 1) — 4) из VI. 1.3.

В самом деле, условие 1) следует из того, что нулем группы G служит подгруппа S, содержащаяся в R^*. Далее, если $\alpha \in H$ и $-\alpha \in H$, то к R^* принадлежат и элементы, составляющие смежный класс α, и элементы, им обратные, а тогда все эти элементы входят в S, т. е. α будет нулем группы G; этим доказано условие 2). Справедливость условия 3) очевидна. Наконец, условие 4) вытекает из предположения, сделанного о подкольце R в формулировке теоремы.

Пополним теперь линейно упорядоченную группу G символом ∞ со свойствами (2) из VI. 4.6. Полагая $w(0) = \infty$, а для каждого $a \in P$, $a \neq 0$, беря в качестве $w(a)$ тот элемент группы G, который, как смежный класс по S, содержит элемент a, мы получим логарифмическое нормирование поля P.

Действительно, выполнение условия 1_0 очевидно. Справедливость условия 2_0 в случае, когда оба элемента a, b отличны от нуля, вытекает из того, что отображение $a \to w(a)$, $a \neq 0$, является гомоморфизмом группы P^* на группу G; если же хотя бы один из эмементов a, b равен нулю, то 2_0 следует из (2) в VI. 4.6.

Проверим, наконец, условие $3_0'$. Так как, по (1) и 2_0,

$$0 = w(1) = w(-1) + w(-1),$$

а группа G не содержит, по VI. 1.4, отличных от нуля элементов конечного порядка, то $w(-1) = 0$ и поэтому, снова по 2_0, для всех $b \in P$

$$w(-b) = w(b).$$

Условие $3_0'$ равносильно, следовательно, в нашем случае условию

$$w(a+b) \geqslant \min(w(a),\ w(b)),$$

которое и будет доказываться.

Оно выполняется, очевидно, если хотя бы один из элементов a, b равен нулю. Если же они оба отличны от нуля, то пусть, например, $w(b) \leqslant w(a)$, т. е. $\frac{a}{b} \in R$. Поэтому, так как единица поля P содержится в R, и $1 + \frac{a}{b} \in R$, т. е., ввиду 2_0 и (1),

$$0 \leqslant w\left(1 + \frac{a}{b}\right) = w[(a+b)b^{-1}] = w(a+b) + w(b^{-1}) =$$

$$= w(a+b) - w(b).$$

Отсюда

$$w(a+b) \geqslant w(b) = \min(w(a),\ w(b)).$$

Теорема доказана.

4. Если в поле P задано логарифмическое нормирование w с кольцом нормирования R_w, то те элементы $a \in P$, для которых $w(a) > 0$, составляют в R_w идеал I_w (см. II. 7.8), называемый *идеалом нормирования* w. Действительно, если $a,\ b \in I_w$, то из $3_0'$ следует, что $a - b \in I_w$; если $a \in I_w$, $x \in R_w$, т. е. $w(a) > 0$, $w(x) \geqslant 0$, то, по 2_0,

$$w(ax) = w(a) + w(x) > 0,$$

т. е. $ax \in I_w$.

Так как, по VI. 5.1, всякий элемент $a \in R_w$, $a \notin J_w$, обратим в R_w, то фактор-кольцо R_w/I_w будет полем; оно называется *полем вычетов* нормирования w.

5. В качестве важного примера найдем все нетривиальные логарифмические нормирования поля рациональных чисел. Пусть w — такое нормирование, R_w и I_w — соответственно кольцо и идеал этого нормирования. Так как $1 \in R_w$, $1 \notin I_w$, то в R_w содержится все кольцо целых чисел C, а пересечение $I_w \cap C$ будет истинным идеалом в C. Это пересечение отлично от нуля, так как иначе все ненулевые целые числа были бы обратимыми в кольце R_w, т. е. это кольцо совпадало бы со всем полем рациональных чисел, что для нетривиального нормирования невозможно. Поэтому, по II. 7.8 и II. 4.2, идеал $I_w \cap C$ является совокупностью (p) целых чисел, кратных некоторому натуральному числу p, $p > 1$.

Так как фактор-кольцо R_w/I_w будет полем, то произведение двух целых чисел, лежащих вне (p), не может попасть в (p). Это равносильно, очевидно, утверждению, что *число p должно быть простым.*

Всякое целое число n, взаимно простое с p, лежит вне идеала I_w и поэтому, по VI. 5.1, обратимо в кольце R_w, т. е. $n^{-1} \in R_w$. Этим доказано, что *в кольце R_w содержится все кольцо R_p тех рациональных чисел, знаменатели которых взаимно просты с p.*

На самом деле даже

$$R_w = R_p.$$

Действительно, если кольцо R_w содержит такое рациональное число $\frac{m}{n}$, что $(m, p) = 1$, а $n \in (p)$, то $m \notin I_w$, т. е. $m^{-1} \in R_w$, а тогда

$$n^{-1} = \frac{m}{n} \cdot m^{-1} \in R_w,$$

т. е. число n оказывается обратимым в кольце R_w в противоречие с тем, что $n \in I_w$.

Обратно, подкольцо R_p поля рациональных чисел при любом простом p удовлетворяет условию теоремы VI. 5.3. Таким образом, *кольца нормирований поля рациональных чисел исчерпываются кольцами R_p, где p пробегает все простые числа.*

6. Найдем то логарифмическое нормирование поля рациональных чисел, для которого кольцом нормирования служит R_p.

Всякое рациональное число a, $a \neq 0$, однозначно записывается в виде

$$a = \frac{m}{n} p^k, \tag{4}$$

где числа m и n взаимно просты между собою и с p, а целое число k больше, равно или меньше нуля. Положим

$$w(a) = k, \quad a \neq 0; \tag{5}$$

кроме того, пусть

$$w(0) = \infty.$$

Мы получаем логарифмическое нормирование поля рациональных чисел со значениями в упорядоченной аддитивной группе целых чисел, пополненной символом ∞, — проверка условий 1_0, 2_0 и 3_0 не представляет никаких затруднений. Это нормирование называется *p-адическим нормированием* поля рациональных чисел.

Из (4) и (5) следует, что *кольцом и идеалом p-адического нормирования служат соответственно кольцо R_p и его идеал R'_p, составленный из тех рациональных чисел, числители несократимых записей которых делятся на p.* Отметим, что

$$R_p = \{R'_p, C\}, \tag{6}$$

где C — кольцо целых чисел. Действительно, если $\frac{m}{n} \in R_p$, то

из $(n, p)=1$ следует, что числа sn, $s=0, 1, 2, \ldots, p-1$, лежат в различных смежных классах кольца C по идеалу (p). Это верно тогда и для чисел $m+sn$, $s=0, 1, 2, \ldots, p-1$, а поэтому одно из этих чисел, например $m+tn$, делится на p. Тогда

$$\frac{m+tn}{n} \in R'_p,$$

но

$$\frac{m}{n} = \frac{m+tn}{n} - t.$$

Используя (6), а также равенство $R'_p \cap C=(p)$ и то, что R'_p является идеалом в R_p, мы на основании теоремы об изоморфизме (см. III. 4.2) получаем, что

$$R_p/R'_p \simeq C/(p).$$

Поле вычетов p-адического нормирования изоморфно, следовательно, простому полю C_p характеристики p (см. III. 2.8 и III. 2.11).

7. Понятно, что p-адическое нормирование поля рациональных чисел можно рассматривать также не как логарифмическое нормирование, а как неархимедово нормирование в смысле VI. 4.3. Для того чтобы совершить переход, обратный к описанному в VI. 4.6, достаточно взять любое действительное число r, $r>1$, и для рационального числа a, записанного в виде (4), положить

$$w(a)=r^{-k},$$

приняв, кроме того, $w(0)=0$.

*Для всякого архимедова нормирования w поля рациональных чисел можно указать такое действительное число α, $0<\alpha\leqslant 1$, что для всех рациональных чисел a

$$w(a)=|a|^{\alpha},$$

где $|a|$ — абсолютная величина числа a [Островский, Acta Math. **41** (1918), 271 — 284].*

8. Пусть в поле P задана действительная норма w в смысле VI. 4.1. Последовательность элементов

$$a_1, a_2, \ldots, a_n, \ldots \tag{7}$$

из P называется *фундаментальной последовательностью*, если для любого действительного числа $\varepsilon>0$ существует

такое натуральное число $N = N(\varepsilon)$, что

$$w(a_n - a_m) < \varepsilon \text{ при } n, m > N.$$

Фундаментальная последовательность (7) называется *сходящейся*, если в поле P можно найти такой элемент a — *предел* этой последовательности, — что для всякого $\varepsilon > 0$ существует натуральное число $N = N(\varepsilon)$, удовлетворяющее условию

$$w(a_n - a) < \varepsilon \text{ при } n > N.$$

Сходящаяся последовательность, имеющая пределом 0, называется *нулевой последовательностью*.

Поле P называется *полным* по норме w, если всякая его фундаментальная последовательность является сходящейся.

*Для всякого поля P с действительной нормой w существует *пополнение*, т. е. такое поле $\bar{P}$ с действительной нормой $\bar{w}$, полное по этой норме, что $P \subseteq \bar{P}$, норма $\bar{w}$ является продолжением нормы w и всякий элемент поля $\bar{P}$ служит пределом некоторой фундаментальной последовательности из поля P.

Если поле рациональных чисел нормировано при помощи абсолютной величины, то его пополнением служит поле действительных чисел, также с абсолютной величиной в качестве нормы. Если же поле рациональных чисел рассматривается с p-адической нормой, то пополнением служит поле p-адических чисел (см. III. 3.12). При этом логарифмической нормой отличного от нуля p-адического числа, записанного в виде (17) из III.3.12, считается целое число k.*

9. Нормированные поля P и P' с действительными нормами называются *изоморфными*, если между ними существует такой изоморфизм, при котором нулевые последовательности одного из этих полей переходят в нулевые последовательности другого поля и обратно.

*Всякое поле с архимедовой действительной нормой изоморфно подполю поля комплексных чисел, нормированному при помощи модулей комплексных чисел [Островский, Acta Math. **41** (1918), 271 — 284].*

§ 6. Теорема Алберта о нормированных алгебрах

1. Пусть в поле P задана действительная норма, которую будем обозначать теперь через $|\alpha|$, $\alpha \in P$. Пусть, далее, R — алгебра над полем P и пусть в R, как в кольце, задана действительная норма w со свойствами 1 — 3 из VI. 4.1.

Будем называть R *нормированной алгеброй*, если для любых $a \in R$, $\alpha \in P$ выполняется равенство

$$w(\alpha a) = |\alpha| w(a). \tag{1}$$

Справедливость этого же равенства будет предполагаться и в том случае, когда мы будем говорить о *псевдонормированной алгебре* (см. VI. 4.7).

2. *Всякая действительная конечномерная алгебра R может быть псевдонормирована* [Альберт, Ann. of Math. **48** (1947), 495 — 501].

Пусть, в самом деле, в алгебре R выбрана база x_i, $i = 1, 2, \ldots, n$, с таблицей умножения

$$x_i x_j = \sum_{k=1}^{n} \varepsilon_{ij}^k x_k.$$

Если μ — отличное от нуля действительное число, то базу алгебры R будут составлять также элементы $y_i = \mu x_i$, $i = 1, 2, \ldots, n$, причем

$$y_i y_j = \sum_{k=1}^{n} \delta_{ij}^k y_k,$$

где

$$\delta_{ij}^k = \mu \varepsilon_{ij}^k.$$

Подберем, что легко сделать, число μ так, чтобы для всех $i, j, k = 1, 2, \ldots, n$ было

$$|\delta_{ij}^k| \leqslant \frac{1}{n}, \tag{2}$$

где $|\delta|$ — абсолютная величина числа δ. Тогда, определяя $w(a)$ для любого элемента $a \in R$, записываемого в виде $a = \sum_{i=1}^{n} \alpha_i y_i$, равенством

$$w(a) = \sum_{i=1}^{n} |\alpha_i|,$$

мы введем в алгебру R псевдонорму.

Действительно, если

$$a = \sum_{i=1}^{n} \alpha_i y_i, \quad b = \sum_{j=1}^{n} \beta_j y_j,$$

то

$$ab = \sum_{k=1}^{n} \left(\sum_{i,\ j=1}^{n} \delta_{ij}^{k} \alpha_i \beta_j \right) y_k,$$

а поэтому, ввиду (2),

$$w(ab) = \sum_{k=1}^{n} \left| \sum_{i,\ j=1}^{n} \delta_{ij}^{k} \alpha_i \beta_j \right| \leqslant \sum_{i,\ j,\ k=1}^{n} |\delta_{ij}^{k}|\,|\alpha_i|\,|\beta_j| \leqslant$$

$$\leqslant \sum_{i,\ j=1}^{n} |\alpha_i|\,|\beta_j| = w(a)\, w(b).$$

Этим доказана справедливость условия 2′ из VI.4.7, выполнение же всех других условий, входящих в определение псевдонормированной алгебры, очевидно.

3. Справедлива, с другой стороны, следующая теорема Алберта [Ann. of Math. **48** (1947), 495—501]:

Поля действительных и комплексных чисел, тело кватернионов и алгебра Кэли являются единственными конечномерными действительными нормированными алгебрами с единицей.

Заметим, что указанные четыре алгебры на самом деле удовлетворяют всем условиям теоремы (см. VI.4.1). С другой стороны, *если в кольце R задана действительная норма w, то в R нет делителей нуля*: если $a, b \in R$, $a \neq 0$, $b \neq 0$, $ab = 0$, то $w(a) \neq 0$, $w(b) \neq 0$, но $w(a)w(b) = w(ab) = 0$, что невозможно. Поэтому, ввиду обобщенной теоремы Фробениуса (см. V.8.1), требует доказательства лишь следующее утверждение:

Всякая конечномерная действительная нормированная алгебра K, обладающая единицей, альтернативна.

4. Начнем доказательство с некоторых замечаний. Прежде всего условимся обозначать норму в алгебре K через $|a|$, где $a \in K$.

Далее, как отмечено выше, в алгебре K нет делителей нуля, а поэтому, ввиду V.8.2, K будет алгеброй с однозначным

делением. Отсюда следует, что при $a \neq 0$, $a \in K$, правое умножение на элемент a (см. V.1.6), являющееся линейным преобразованием аддитивного векторного пространства алгебры K, будет невырожденным. Условимся обозначать это правое умножение через R_a; тождественное линейное преобразование будем обозначать через E.

Наконец, так как алгебра K обладает единицей 1, то, по V.6.2, в ее центре содержится подполе D, изоморфное полю действительных чисел; это будет совокупность элементов вида $\alpha \cdot 1 = \alpha$, где α — действительное число.

Лемма 1. *Если $a \notin D$, то линейное преобразование R_a не имеет действительных характеристических корней.*

В самом деле, если α — такой корень, то линейное преобразование $R_a - \alpha E = R_{a-\alpha}$ будет вырожденным, т. е., как отмечено выше, $a - \alpha = 0$, откуда $a = \alpha \in D$.

5. Лемма 2. *Если $a \notin D$ и $|a| = \alpha$, то модуль любого характеристического корня λ_0 линейного преобразования R_a равен α.*

В самом деле, пусть

$$\lambda_0 = \rho(\cos\varphi + i\sin\varphi). \tag{3}$$

Линейное преобразование $R_a - \lambda_0 E$ комплексного векторного пространства, являющегося расширением действительного аддитивного векторного пространства алгебры K, должно быть вырожденным. Поэтому в K существуют такие элементы b и c, что

$$b + ci \neq 0,$$

откуда

$$\delta = |b| + |c| > 0 \tag{4}$$

и

$$(b + ci)(R_a - \lambda_0 E) = 0.$$

Отсюда

$$(b + ci) R_a = \lambda_0 (b + ci),$$

и поэтому

$$(b + ci) R_a^m = \lambda_0^m (b + ci) \tag{5}$$

для всех натуральных m. Так как R_a является линейным преобразованием действительного векторного пространства K,

то из (5) и (3) вытекают равенства

$$\begin{aligned} bR_a^m &= \rho^m (b\cos m\varphi - c\sin m\varphi), \\ cR_a^m &= \rho^m (b\sin m\varphi + c\cos m\varphi). \end{aligned} \tag{6}$$

Используя определение нормированной алгебры, в частности (1), а также (4) и неравенства $|\cos m\varphi| \leqslant 1$, $|\sin m\varphi| \leqslant 1$, мы из (6) получаем

$$|b|\alpha^m = |bR_a^m| \leqslant \rho^m\delta,$$
$$|c|\alpha^m = |cR_a^m| \leqslant \rho^m\delta.$$

Отсюда, ввиду (4), $\delta\alpha^m \leqslant 2\rho^m\delta$, т. е. $(\alpha\rho^{-1})^m \leqslant 2$, а так как число m произвольно, то $\alpha \leqslant \rho$.

С другой стороны, из (6) вытекают равенства

$$(b\cos m\varphi + c\sin m\varphi) R_a^m = \rho^m b,$$
$$(c\cos m\varphi - b\sin m\varphi) R_a^m = \rho^m c,$$

которые приводят к неравенствам

$$\rho^m |b| \leqslant \delta\alpha^m, \quad \rho^m |c| \leqslant \delta\alpha^m.$$

Отсюда $\rho^m\delta \leqslant 2\delta\alpha^m$, т. е. $(\rho\alpha^{-1})^m \leqslant 2$, а поэтому $\rho \leqslant \alpha$. В результате мы получаем $\rho = \alpha$, что и требовалось доказать.

6. Лемма 3. *Если $a \notin D$, то характеристический многочлен линейного преобразования R_a является степенью неприводимого квадратного трехчлена.*

В самом деле, если λ_0 — характеристический корень для R_a и $b = a + 1$, то $R_b = R_a + E$, и поэтому число $\lambda_0 + 1$ будет характеристическим корнем для R_b. Пусть $\alpha + \beta i$, $\gamma + \delta i$ — два характеристических корня преобразования R_a. Из леммы 2 следует, что эти корни имеют равные модули, т. е.

$$\alpha^2 + \beta^2 = \gamma^2 + \delta^2.$$

Применяя это же к характеристическим корням преобразования R_b — ясно, что $b \notin D$, — мы получим

$$(\alpha + 1)^2 + \beta^2 = (\gamma + 1)^2 + \delta^2.$$

Отсюда $2\alpha = 2\gamma$, т. е. $\alpha = \gamma$, а поэтому $\beta^2 = \delta^2$, т. е. $\beta = \pm\delta$. Эти результаты вместе с леммой 1 заканчивают доказательство леммы.

7. Лемма 4. *Если $a \notin D$, то минимальный многочлен линейного преобразования R_a является неприводимым квадратным трехчленом.*

В силу леммы 3 характеристический многочлен преобразования R_a имеет вид

$$\chi(\lambda) = (\lambda^2 - \alpha\lambda - \beta)^h,$$

где

$$\gamma = -\frac{\alpha^2}{4} - \beta > 0.$$

Поэтому минимальным многочленом будет

$$\varphi(\lambda) = (\lambda^2 - \alpha\lambda - \beta)^k, \quad k \leqslant h,$$

т. е.

$$(R_a^2 - \alpha R_a - \beta E)^k = 0. \tag{7}$$

Пусть $k > 1$. Если

$$b = \gamma^{-\frac{1}{2}}\left(a - \frac{\alpha}{2}\right),$$

так что $b \notin D$, то равенства

$$(R_a^2 - \alpha R_a - \beta E)^l = 0 \quad \text{и} \quad (R_b^2 + E)^l = 0$$

будут равносильными. Таким образом,

$$(R_b^2 + E)^k = 0, \quad (R_b^2 + E)^{k-1} \neq 0. \tag{8}$$

Так как число i служит для линейного преобразования R_b характеристическим корнем, то, по лемме 2, $|b| = 1$. Поэтому, полагая $S = R_b^2$, мы для любого $c \in K$ получаем

$$|cS| = |(cb)b| = |c|.$$

Отсюда

$$|cS^m| = |c| \tag{9}$$

для всех $c \in K$ и всех натуральных m.

Если $T = (S+E)^{k-2}$ — здесь используется, что $k \geqslant 2$, — то, по (8),

$$T \neq 0, \quad T(S+E) \neq 0, \quad T(S+E)^2 = 0.$$

Существует, следовательно, такой элемент c', что

$$c'(S+E)^{k-1} \neq 0,$$

т. е.

$$c = c'T \neq 0, \quad c(S+E) \neq 0, \quad c(S+E)^2 = 0. \tag{10}$$

Из последнего равенства вытекает, что $cS^2 = -c(2S+E)$, т. е. при $m=2$ выполняется равенство

$$cS^m = (-1)^{m-1} c\,[mS+(m-1)E]. \tag{11}$$

Если равенство (11) уже доказано для данного m, то

$$cS^{m+1} = (-1)^{m-1} c\,[mS^2+(m-1)S] =$$
$$= (-1)^m c\,[2mS+mE-(m-1)S] = (-1)^m c[(m+1)S+mE],$$

т. е. (11) справедливо для всех m. Несколько меняя запись этого равенства и беря нормы от обеих его частей, мы получим, ввиду (9), что

$$|c| = |mc(S+E)-c|. \tag{12}$$

Если

$$|c(S+E)| = \delta,$$

то, ввиду (10), $\delta > 0$. Однако

$$|mc(S+E)-c| \geqslant m\delta - |c|,$$

т. е., по (12), при всех m справедливо неравенство

$$2|c| \geqslant m\delta,$$

что невозможно. Этим доказано, что $k=1$, т. е. доказана лемма 4.

8. Отсюда, ввиду (7), следует равенство

$$R_a^2 = \alpha R_a + \beta E,$$

т. е., ввиду существования в алгебре K единицы,

$$a^2 = \alpha a + \beta.$$

Поэтому для любого $b \in K$

$$(ba)\,a = bR_a^2 = b(\alpha R_a + \beta E) = \alpha ba + \beta b = b(\alpha a + \beta) = ba^2.$$

Таким образом, равенство $(ba)\,a = b(aa)$ доказано для $a \notin D$; оно справедливо, однако, и при $a \in D$, так как D содержится в центре алгебры K. Равенство $a(ab) = (aa)\,b$ проверяется аналогичным путем. Этим, в силу теоремы Артина (см. V.7.3), доказана альтернативность алгебры K, т. е. доказана теорема Алберта.

*Поля действительных и комплексных чисел, тело кватернионов и алгебра Кэли являются единственными действительными нормированными алгебрами с делением, обладающими

единицей; конечномерность этих алгебр заранее не предполагается [Альберт, Bull. Amer. Math. Soc. **55** (1949), 763—768; Райт, Proc. Nat. Acad. USA **39** (1953), 330—332].

Поля действительных и комплексных чисел и тело кватернионов являются единственными псевдонормированными действительными ассоциативными алгебрами, не содержащими отличного от нуля элемента x, для которого существует такая последовательность y_n, не являющаяся нулевой последовательностью (см. VI.5.8), что хотя бы одна из последовательностей xy_n или y_nx будет нулевой [Капланский, Duke Math. J. **16** (1949), 399—418].

Само поле комплексных чисел является единственной псевдонормированной комплексной ассоциативной алгеброй с деланием [Мазур, C. R. Paris **207** (1938), 1025—1027; И. М. Гельфанд, Мат. сб. **9** (1941), 3—24].*

§ 7. Замыкания. Топологические пространства

1. Будем говорить, что в частично упорядоченном множестве M задано *отношение замыкания*, если всякому элементу $a \in M$ сопоставлен однозначно определенный элемент $\bar{a} \in M$, называемый *замыканием* элемента a, причем для всех a, $b \in M$ выполняются следующие требования:

1_0) $a \leqslant \bar{a}$;

2_0) если $a \leqslant b$, то $\bar{a} \leqslant \bar{b}$;

3_0) $\bar{\bar{a}} = \bar{a}$, т. е. замыкание любого элемента совпадает со своим замыканием.

Элемент a назовем *замкнутым*, если он совпадает со своим замыканием. Ввиду 3_0) замкнутыми будут замыкания всех элементов и, очевидно, только они. С другой стороны, из 2_0) следует, что $\bar{a}$ содержится во всяком замкнутом элементе, содержащем a, т. е. *отношение замыкания однозначно определяется заданием системы замкнутых элементов.*

Во всяком частично упорядоченном множестве можно задать *тривиальное замыкание*, полагая $\bar{a} = a$ для всех a.

2. Отношение замыкания можно ввести, в частности, в систему $\tilde{M}$ всех подмножеств произвольного множества M, частично упорядоченную по теоретико-множественному включению. В дальнейшем именно в этом смысле мы будем гово-

рить об *отношении замыкания, заданном в произвольном множестве M*. Вполне определен, ясно, смысл таких понятий, как *замыкание подмножества* из M и *замкнутое подмножество*; по существу сохраняются и формулировки условий $1_0)-3_0)$ из VI.7.1.

Заметим, что если в множестве M задано отношение замыкания, то *само множество M замкнуто*, как замыкание самого себя. С другой стороны, *пересечение любой системы замкнутых в M подмножеств само замкнуто.*

В самом деле, пусть в M задана система замкнутых подмножеств A_α (α пробегает некоторое множество индексов) и пусть

$$B=\bigcap_\alpha A_\alpha.$$

Тогда, по условию $2_0)$ из VI.7.1, из $B\subseteq A_\alpha$ следует $\bar{B}\subseteq\bar{A}_\alpha = A_\alpha$, т. е.

$$\bar{B}\subseteq\bigcap_\alpha A_\alpha = B.$$

Так как, с другой стороны, $B\subseteq\bar{B}$ по условию $1_0)$ из VI.7.1, то $\bar{B}=B$, что и требовалось доказать.

Справедлива следующая обратная теорема:

Во всяком множестве M можно задать замыкание, беря в качестве системы замкнутых подмножеств любую систему подмножеств Σ, содержащую как само M, так и пересечение любой своей подсистемы.

В самом деле, если в качестве замыкания $\bar{A}$ для любого подмножества A из M будет взято пересечение всех подмножеств, входящих в Σ и содержащих A — такие существуют, например само M, — то условия $1_0)-3_0)$ будут удовлетворены, а замкнутыми окажутся подмножества из Σ и только они.

3. Два частично упорядоченных множества с замыканиями естественно называть *изоморфными*, если между ними существует такое изоморфное соответствие в смысле I.4.3, при котором образы и прообразы замкнутых элементов замкнуты. В этом же смысле можно говорить об *изоморфном вложении* одного частично упорядоченного множества с замыканиями в другое.

* Если M — частично упорядоченное множество с замыканиями, то в частично упорядоченной системе $\tilde{M}$ всех

подмножеств множества M можно так задать отношение замыкания, что M будет изоморфно вкладываться в $\tilde{M}$. ⁎

4. Понятие множества с отношением замыкания для подмножеств, введенное в VI.7.2, является слишком широким. Накладывая на отношение замыкания некоторые дополнительные ограничения, мы придем к понятию топологического пространства, одному из важнейших общематематических понятий, во многих случаях играющему роль, параллельную роли частично упорядоченных множеств.

Говорят, что в множестве M задана *топология* или что M является *топологическим пространством*, если в нем задано замыкание, удовлетворяющее помимо условий $1_0)-3_0)$ (или равносильных им условий, указанных в формулировке теоремы VI.7.2) также следующим дополнительным условиям:

$4_0)$ замыкание объединения двух (а поэтому и любого конечного числа) подмножеств из M равно объединению замыканий этих подмножеств,

$$\overline{A \cup B} = \bar{A} \cup \bar{B};$$

$5_0)$ всякое подмножество, состоящее из одного элемента, замкнуто.

В действительности *условия* $1_0)$ *и* $2_0)$ *могут быть выведены из условий* $4_0)$ *и* $5_0)$. Так, пусть A — любое подмножество из M и $a \in A$. Тогда, ввиду условий $4_0)$ и $5_0)$,

$$\bar{A} = \overline{A \cup a} = \bar{A} \cup \bar{a} = \bar{A} \cup a,$$

т. е. $a \in \bar{A}$, откуда следует включение $A \subseteq \bar{A}$, доказывающее условие $1_0)$. С другой стороны, если подмножества A и B таковы, что $A \subseteq B$, то, ввиду условия $4_0)$,

$$\bar{B} = \overline{A \cup B} = \bar{A} \cup \bar{B},$$

т. е. $\bar{A} \subseteq \bar{B}$, чем и доказано условие $2_0)$.

Если топологическое пространство M *содержит более одного элемента* — лишь такие пространства могут представлять интерес, — *то его пустое подмножество замкнуто.* Действительно, оно будет замкнутым как пересечение любых двух различных элементов из M, являющихся, по условию $5_0)$, замкнутыми подмножествами.

Заметим, наконец, что, как следует из условия $4_0)$, *объединение любого конечного числа замкнутых подмножеств топологического пространства замкнуто.*

5. Система всех замкнутых подмножеств топологического пространства M частично упорядочена по включению. Частично упорядочена по включению и система всех дополнений в M к замкнутым подмножествам, т. е. система *открытых подмножеств*. Мы получим инверсно изоморфное соответствие (см. I.4.6) между этими двумя частично упорядоченными системами, если всякому замкнутому подмножеству A поставим в соответствие открытое подмножество $M \setminus A$. Это позволяет путем дуализации вывести из известных нам результатов, относящихся к замкнутым множествам, результаты, относящиеся к открытым множествам.

Так, учитывая, что дополнением для пересечения (или объединения) заданной системы подмножеств любого множества всегда служит объединение (соответственно пересечение) дополнений ко всем этим подмножествам, мы получаем, что *объединение любой системы открытых подмножеств и пересечение любого конечного числа открытых подмножеств сами открыты. С другой стороны, и само пространство M, и пустое подмножество являются открытыми*, так как они служат дополнениями друг для друга.

6. Всякое отношение замыкания в множестве M, а поэтому и всякая топология вполне определяются, как мы знаем, заданием системы всех замкнутых подмножеств. Топологию в M можно определить, следовательно, и заданием системы всех открытых подмножеств. Учитывая, что объединение любой системы открытых множеств открыто, можно ограничиться заданием лишь такой системы открытых подмножеств Σ, что всякое (непустое) открытое подмножество пространства M является объединением подмножеств из Σ. Такая система Σ, называемая *полной системой окрестностей* пространства M, определяется, понятно, неоднозначно.

Подмножества, составляющие данную полную систему окрестностей Σ, будут называться *окрестностями*; все те окрестности из Σ, которые содержат данный элемент $a \in M$, составляют *полную систему окрестностей этого элемента*.

Пусть топология в M задана полной системой окрестностей Σ. Тогда *подмножество A из M открыто тогда и только тогда, если для всякого элемента $a \in A$ можно указать такую окрестность U из Σ, что $a \in U$ и $U \subseteq A$* — это следует из того, что A открыто тогда и только тогда, если оно является объединением окрестностей из Σ.

С другой стороны, *если A — произвольное подмножество пространства M, то его замыкание $\bar{A}$ состоит из тех и только тех элементов, любая окрестность которых содержит хотя бы один элемент из A.*

В самом деле, если элемент $x \notin \bar{A}$, то x содержится в открытом множестве $M \setminus \bar{A}$, а поэтому существует окрестность элемента x, содержащаяся в $M \setminus \bar{A}$, т. е. имеющая с A пустое пересечение. С другой стороны, если некоторый элемент x обладает окрестностью U, не содержащей элементов из A, то A содержится в замкнутом множестве $M \setminus U$, а поэтому, ввиду свойства 2_0) из VI.7.1,

$$\bar{A} \subseteq \overline{M \setminus U} = M \setminus U,$$

т. е. $x \notin \bar{A}$.

Отсюда следует, что *подмножество A топологического пространства M замкнуто тогда и только тогда, если всякий элемент x, каждая окрестность которого содержит хотя бы один элемент из A, сам принадлежит к A.*

7. *Некоторая система Σ подмножеств множества M тогда и только тогда является полной системой окрестностей при некоторой топологии, заданной в M, если*

α) для любой упорядоченной пары различных элементов a, b из M можно указать такое подмножество U, принадлежащее к Σ, что $a \in U$, $b \notin U$;

β) для любых двух подмножеств U, V, входящих в Σ и содержащих некоторый элемент a, всегда можно указать в Σ такое подмножество W, что $a \in M$ и $W \subseteq U \cap V$.

Доказательство. Пусть Σ — полная система окрестностей топологического пространства M. Если a и b — различные элементы из M, то, ввиду замкнутости b, подмножество $M \setminus b$ открыто и поэтому является объединением окрестностей из Σ. Так как $a \in M \setminus b$, то, по VI.7.6, в Σ можно найти такую окрестность U, что $a \in U$ и $U \subseteq M \setminus b$, а поэтому $b \notin U$. Этим доказано α). С другой стороны, если заданы окрестности U и V элемента a, то, по VI.7.5, их пересечение $U \cap V$ открыто, а так как a содержится в этом пересечении, то, снова по VI.7.6, существует окрестность W элемента a, содержащаяся в $U \cap V$.

Пусть теперь в множестве M задана произвольная система подмножеств Σ, обладающая свойствами α) и β). Для всякого подмножества $A \subseteq M$ обозначим через $\bar{A}$ совокуп-

ность таких элементов $x \in M$, что всякое подмножество из Σ, содержащее x, содержит хотя бы один элемент из A, и покажем, что этим в M введена топология. Достаточно показать, ввиду VI. 7.4, что выполняются условия 3_0), 4_0) и 5_0).

Если $x \in \bar{\bar{A}}$, то любое подмножество U из Σ, содержащее x, содержит хотя бы один элемент $y \in \bar{A}$, а поэтому, снова по определению $\bar{A}$, подмножество U содержит хотя бы один элемент из A. Отсюда следует, что $x \in \bar{A}$, т. е. $\bar{\bar{A}} \subseteq \bar{A}$. Так как очевидно, с другой стороны, что всегда $A \subseteq \bar{A}$, то $\bar{A} \subseteq \bar{\bar{A}}$ и поэтому $\bar{\bar{A}} = \bar{A}$, т. е. условие 3_0) доказано.

Далее, если A и B — произвольные подмножества из M, а x — любой элемент из объединения $\bar{A} \cup \bar{B}$, то всякое подмножество из Σ, содержащее x, содержит хотя бы один элемент или из A, или из B, т. е. хотя бы один элемент из $A \cup B$, а поэтому $x \in \overline{A \cup B}$. Этим доказано, что $\bar{A} \cup \bar{B} \subseteq \overline{A \cup B}$. С другой стороны, если элемент $y \in \overline{A \cup B}$, то любое подмножество из Σ, содержащее y, содержит хотя бы один элемент из $A \cup B$. Пусть в Σ существуют такие два подмножества U и V, содержащие y, что U не содержит элементов из A, а V — элементов из B. Тогда, по условию β), мы найдем в Σ подмножество W, содержащее y и лежащее в пересечении $U \cap V$, т. е. не содержащее элементов ни из A, ни из B, что невозможно. Таким образом, или все подмножества из Σ, содержащие y, содержат элементы из A, а тогда $y \in \bar{A}$, или же все они содержат элементы из B, а тогда $y \in \bar{B}$. Отсюда следует, что $\overline{A \cup B} \subseteq \bar{A} \cup \bar{B}$. Справедливость условия 4_0) также доказана.

Наконец, справедливость условия 5_0) вытекает из того, что для любого элемента $b \in M$ его замыкание $\bar{b}$ состоит лишь из b, так как, по условию α), для любого другого элемента a можно указать такое подмножество из Σ, которое содержит a, но не содержит b.

Для завершения доказательства теоремы остается показать, что система Σ служит полной системой окрестностей для топологии, построенной нами в множестве M. Если U — подмножество из Σ, то его дополнение $M \setminus U$ будет замкнутым, так как любой элемент из M, лежащий вне $M \setminus U$, содержится в U, т. е. лежит в подмножестве из Σ, не содержащем ни одного элемента из $M \setminus U$. Этим доказано, что U открыто. С другой стороны, пусть A — любое открытое

подмножество, a — элемент из A. Тогда $M \setminus A$ замкнуто, $a \notin M \setminus A$, а поэтому существует такое подмножество U из Σ, содержащее a, пересечение которого с $M \setminus A$ пусто, т. е. $U \subseteq A$. Подмножество A может быть представлено, следовательно, как объединение некоторой системы подмножеств из Σ. Теорема доказана.

8. Два множества с замыканиями, M и M', называются *изоморфными*, если между ними существует такое взаимно однозначное соответствие χ, которое сохраняет отношение замыкания, т. е. для всех $A \subseteq M$

$$\bar{A}\chi = \overline{A\chi}.$$

Отображение χ называется при этом *изоморфным отображением* или *изоморфизмом*. Обратное отображение χ^{-1} будет, очевидно, также изоморфным.

Очевидна связь этого понятия с введенным в VI. 7.3 понятием изоморфизма для частично упорядоченных множеств с замыканиями. В частном случае топологических пространств термин «изоморфизм» заменяется обычно термином «гомеоморфизм»; мы не будем, однако, употреблять этого специального термина.

При изоморфном соответствии между множествами с замыканиями замкнутые подмножества переходят в замкнутые и обратно, причем, ввиду VI. 7.1, *это свойство можно было бы принять в качестве определения изоморфизма.* Отсюда следует, что *в случае топологических пространств изоморфизм может быть определен также как такое взаимно однозначное соответствие между этими пространствами, при котором открытые подмножества переходят в открытые и обратно.*

Если в топологических пространствах M и M' топологии заданы соответственно при помощи полных систем окрестностей Σ и Σ', то взаимно однозначное отображение χ пространства M на пространство M' тогда и только тогда будет изоморфным, если для всякого элемента $a' \in M'$ и любой его окрестности U' существует такая окрестность U элемента $a'\chi^{-1} \in M$, что $U\chi \subseteq U'$, и если для всякого элемента $a \in M$ и любой его окрестности V существует такая окрестность V' элемента $a\chi$, что $V'\chi^{-1} \subseteq V$.

Действительно, пусть χ — изоморфизм и пусть, например, заданы элемент $a' \in M'$ и его окрестность U'. Тогда множество $U'\chi^{-1} \subseteq M$ будет открытым, т. е. содержит окрестность U элемента $a'\chi^{-1}$. Ясно, что $U\chi \subseteq U'$.

Обратно, пусть отображение χ удовлетворяет условиям, указанным в формулировке теоремы, и пусть, например, дано открытое подмножество A пространства M. Если $a\chi$ — произвольный элемент из $A\chi$, то $a \in A$ и в A содержится некоторая окрестность V элемента a. Тогда, по условию теоремы, существует такая окрестность V' элемента $a\chi$, что $V'\chi^{-1} \subseteq V$. Отсюда

$$V' = V'\chi^{-1}\chi \subseteq V\chi \subseteq A\chi.$$

Этим доказано, что $A\chi$ будет открытым подмножеством пространства M'. Теорема доказана.

Применяя эту теорему к случаю, когда M и M' совпадают, а χ является тождественным отображением пространства M на себя, т. е. $a\chi = a$ для всех $a \in M$, мы придем к условию *эквивалентности* двух заданных в M полных систем окрестностей Σ и Σ', т. е. к условию для того, чтобы эти две полные системы окрестностей определяли в M одну и ту же топологию: *это будет тогда и только тогда, когда всякая окрестность любого элемента $a \in M$, взятая в одной из систем Σ, Σ', содержит некоторую окрестность элемента a из другой системы.*

9. Топология, заданная в множестве M, *индуцирует* топологию во всяком подмножестве $A \subseteq M$. Именно, если топология в M задается полной системой окрестностей Σ, то обозначим через Σ_A совокупность всевозможных пересечений $U \cap A$, где $U \in \Sigma$. Из справедливости для системы Σ условий α) и β) теоремы VI. 7.7 немедленно следует справедливость аналогичных условий для системы Σ_A, т. е. эта система служит полной системой окрестностей для некоторой топологии, заданной в A.

Если в пространстве M задана другая полная система окрестностей Σ', эквивалентная с Σ, то эквивалентность в A полных систем окрестностей Σ_A и Σ'_A проверяется на основании VI. 7.8 без всяких затруднений. Таким образом, топология в M однозначно определяет топологию в подмножестве A. Полученное этим путем топологическое пространство A называется *подпространством* пространства M.

Из определения подпространства немедленно следует, что *открытыми и замкнутыми подмножествами подпространства A пространства M будут пересечения с A открытых и соответственно замкнутых подмножеств из M и только они.*

10. Тривиальное замыкание (см. VI. 7.1), введенное в систему всех подмножеств произвольного множества M, удовлетворяет, очевидно, условиям 4_0) и 5_0) из VI. 7.4, т. е. является топологией. Эта топология называется *дискретной*; все подмножества множества M будут в этой топологии и замкнутыми, и открытыми. Всякое множество может рассматриваться, следовательно, как дискретное топологическое пространство, причем в конечных множествах, где всякое подмножество является объединением конечного числа элементов, возможна лишь дискретная топология.

Первым примером недискретного топологического пространства служит *прямая линия*. Рассматривая ее как числовую прямую и определяя для каждого подмножества A замыкание $\bar{A}$ как совокупность чисел, являющихся пределами сходящихся последовательностей чисел из A, мы получим топологию — условия 3_0), 4_0) и 5_0) проверяются без затруднений. Одной из полных систем окрестностей для этой естественной топологии прямой служит система всех (открытых) интервалов. В дальнейшем, говоря о числовой прямой как о топологическом пространстве, мы будем всегда подразумевать ее естественную топологию.

Плоскость и вообще всякое n-мерное действительное евклидово пространство также рассматриваются обычно как топологические пространства. Топология вводится в них так же, как выше в случае прямой, причем используется покоординатная сходимость. В случае плоскости полной системой окрестностей служит система всех (открытых) кругов; эквивалентной полной системой окрестностей будет система всех (открытых) квадратов.

§ 8. Частные типы топологических пространств

1. Как мы знаем (см., например, VI.7.7), для любых двух различных элементов a, b топологического пространства можно указать открытое подмножество U, содержащее элемент a, но не содержащее элемента b. Ограничения более

сильные, чем это свойство, позволяют выделить некоторые специальные важные типы топологических пространств.

Так, топологическое пространство называется *хаусдорфовым*, если для любых двух различных его элементов a, b можно указать такие открытые подмножества U, V, что $a \in U$, $b \in V$ и пересечение $U \cap V$ пусто.

Если топология в M задана полной системой окрестностей Σ, то пространство M тогда и только тогда будет хаусдорфовым, когда пересечение замыканий всех окрестностей любого элемента a содержит лишь сам этот элемент.

В самом деле, если пространство M хаусдорфово, а элемент b отличен от a, то, беря для a и b такие окрестности, соответственно U и V, что $U \cap V$ пусто, мы получим, что $\overline{U} \not\ni b$. С другой стороны, если пространство M удовлетворяет условию, указанному в формулировке теоремы, и если в нем даны два различных элемента a и b, то существует такая окрестность U элемента a, что $b \notin \overline{U}$. Тогда элемент b содержится в открытом подмножестве $V = M \setminus \overline{U}$, причем $U \cap V$ пусто.

2. Топологическое пространство называется *регулярным*, если для любого элемента a и любого замкнутого подмножества B, не содержащего a, можно указать такие непересекающиеся открытые подмножества U, V, что $a \in U$, $B \subseteq V$.

Ясно, что всякое регулярное пространство будет хаусдорфовым. Все пространства, указанные в VI. 7.10, регулярны.

Если топология в M задана полной системой окрестностей Σ, то пространство M тогда и только тогда регулярно, когда для всякой окрестности U любого элемента a можно указать такую окрестность V этого элемента, замыкание которой $\overline{V}$ содержится в U.

Действительно, если пространство M регулярно и в нем взята окрестность U некоторого элемента a, то для a и замкнутого подмножества $M \setminus U$ можно указать такие непересекающиеся открытые подмножества V и W, что $a \in V$, $(M \setminus U) \subseteq W$. Тогда в V содержится некоторая окрестность V_0 элемента a, причем

$$\overline{V_0} \subseteq \overline{V} \subseteq M \setminus W \subseteq M \setminus (M \setminus U) = U.$$

Обратно, пусть пространство M обладает свойством, указанным в формулировке теоремы, и пусть в нем заданы элемент a и замкнутое подмножество B, причем $a \notin B$. Тогда, по условию, существует такая окрестность U элемента a, замыкание которой $\bar{U}$ содержится в открытом подмножестве $M \setminus B$. Пересечение открытых подмножеств U и $M \setminus \bar{U}$ пусто, а так как

$$M \setminus \bar{U} \supseteq M \setminus (M \setminus B) = B,$$

то регулярность пространства M доказана.

Легко проверяется, что *свойство топологического пространства быть хаусдорфовым или регулярным переносится на подпространства этого пространства.*

Более специальным, чем понятие регулярного пространства, является понятие *нормального* пространства: это такое топологическое пространство, что для любых его непересекающихся замкнутых множеств A и B существуют такие непересекающиеся открытые множества U и V, что $A \subseteq U$, $B \subseteq V$.

* Промежуточный класс между регулярными и нормальными пространствами составляют *вполне регулярные* топологические пространства, т. е. пространства со следующим свойством: для любого элемента a и любого замкнутого множества B, не содержащего этого элемента, можно определить на этом пространстве такую непрерывную (в смысле топологии этого пространства) действительную функцию f, что $f(a) = 0$, $f(b) = 1$ для всех $b \in B$ и $0 \leqslant f(x) \leqslant 1$ для всех x. *

3. Очень важный класс топологических пространств составляют бикомпактные пространства. Именно, пространство M называется *бикомпактным*, если оно удовлетворяет любому из следующих условий, эквивалентность которых немедленно следует из сказанного в VI.7.5:

I. Из всякой системы открытых подмножеств, объединение которых совпадает с M, можно выбрать такую конечную подсистему, что уже объединение составляющих ее подмножеств совпадает с M.

II. Из всякой системы замкнутых подмножеств, пересечение которых пусто, можно выбрать такую конечную подсистему, что уже пересечение составляющих ее подмножеств пусто.

Как вытекает из доказываемой в курсах математического анализа теоремы Гейне — Бореля, любой конечный замкнутый отрезок числовой прямой является бикомпактным пространством.

* Каждое из следующих двух условий эквивалентно условиям I и II, и поэтому может быть использовано для определения бикомпактного пространства:

III. Объединение всякой цепи (см. I.4.1), составленной из отличных от M открытых подмножеств, само отлично от M.

IV. Пересечение всякой цепи, составленной из непустых замкнутых подмножеств, само не пусто. *

4. Топологическое пространство называется *локально бикомпактным*, если всякий элемент этого пространства содержится в открытом подмножестве, замыкание которого бикомпактно.

Всякое бикомпактное пространство локально бикомпактно. Примером локально бикомпактного, но не бикомпактного пространства служит числовая прямая. Действительно, всякая точка прямой обладает окрестностью, являющейся конечным открытым интервалом. Замыкание такой окрестности будет замкнутым отрезком, т. е., как отмечено выше, бикомпактно. С другой стороны, сама прямая не бикомпактна: она является объединением всех своих интервалов конечной длины, но не может быть представлена как объединение конечного числа таких интервалов.

В качестве другого примера локально бикомпактного, но не бикомпактного пространства можно назвать любое бесконечное дискретное пространство.

5. *Всякое замкнутое подмножество бикомпактного пространства бикомпактно, а локально бикомпактного пространства — локально бикомпактно.*

Заметим сперва, что если A — замкнутое подмножество любого топологического пространства M, то всякое подмножество B из A, замкнутое в подпространстве A, будет замкнутым и в M. В самом деле, если $\bar{B}$ — замыкание B в M, то, как следует из VI.7.9, $\bar{B} \cap A$ будет замыканием B в A, т. е., ввиду замкнутости B в A,

$$\bar{B} \cap A = B. \tag{1}$$

Так как, однако, само A замкнуто в M, то из $B \subseteq A$ следует $\bar{B} \subseteq A$, а поэтому, ввиду (1), $\bar{B} = B$.

Теперь ясно, что из справедливости в бикомпактном пространстве M условия II из VI.8.3 следует справедливость этого условия во всяком замкнутом подпространстве пространства M. Если же пространство M локально бикомпактно и A — его замкнутое подпространство, то для всякого $a \in A$ существует в M такая окрестность U, замыкание которой $\bar{U}$ бикомпактно. Тогда пересечение $U \cap A$ служит окрестностью для a в A, причем ее замыканием в A является $\bar{U} \cap A$. Это последнее пересечение будет, однако, бикомпактным, так как оно замкнуто в M (как пересечение замкнутых подмножеств) и содержится в бикомпактном пространстве $\bar{U}$.

* Всякое открытое подмножество локально бикомпактного (в частности, бикомпактного) пространства локально бикомпактно.

Всякое локально бикомпактное пространство изоморфно открытому подпространству некоторого бикомпактного пространства [П. С. Александров, Math. Ann. **92** (1924), 294—301]. *

6. Топологическое пространство M называется *несвязным*, если оно распадается на два непустые непересекающиеся замкнутые подмножества (каждое из которых будет, очевидно, и открытым), и *связным* в противоположном случае.

Топологическое пространство M называется *вполне несвязным*, если для любых двух различных элементов $a, b \in M$ существует такое разбиение M на два непересекающиеся замкнутые подмножества A, B, что $a \in A$, $b \in B$.

Всякое дискретное пространство будет, конечно, вполне несвязным. Примером недискретного вполне несвязного пространства служит *рациональная прямая*, т. е. подпространство числовой прямой, составленное из рациональных чисел. Оно не дискретно, так как всякая окрестность на числовой прямой содержит бесконечно много рациональных чисел. С другой стороны, если a и b — два различные рациональные числа, $a < b$, то существует иррациональное число α, расположенное между ними, и мы получим искомое разбиение, беря в качестве A совокупность рациональных чисел,

меньших α, а в качестве B — совокупность рациональных чисел, больших α.

Отметим, что всякое подпространство вполне несвязного топологического пространства само вполне несвязно.

§ 9. Топологические группы

1. Рассмотрение многочисленных примеров алгебраических образований, являющихся в то же время топологическими пространствами (см. VI.7.4), приводит к следующим определениям.

Группоид G, одновременно являющийся топологическим пространством, называется *топологическим группоидом*, если умножение в группоиде G *непрерывно* в заданной топологии, т. е. для любых элементов a, $b \in G$ и любой окрестности W элемента ab (см. VI.7.6) можно указать такие окрестности U и V элементов a и b соответственно, что $UV \subseteq W$ (где UV есть множество элементов из G, представимых хотя бы одним способом в виде произведения uv, $u \in U$, $v \in V$).

Частным случаем топологического группоида будет *топологическая полугруппа.*

Группа G называется *топологической группой*, если она является топологической полугруппой и если, сверх того, операция взятия обратного элемента *непрерывна* в заданной топологии, т. е. для любого элемента $a \in G$ и любой окрестности V элемента a^{-1} существует такая окрестность U элемента a, что $U^{-1} \subseteq V$ (где U^{-1} есть множество элементов вида u^{-1} для всех $u \in U$).

Легко проверить, применяя условия эквивалентности полных систем окрестностей топологического пространства (см. VI.7.8), что свойство операции умножения (или операции перехода к обратному элементу) быть непрерывной не зависит от выбора в G полной системы окрестностей. Интуитивный смысл непрерывности операций состоит в том, что малым изменениям сомножителей (или элемента) соответствуют малые изменения произведения (или обратного элемента).

Задание в группе G такой топологии, по которой эта группа будет топологической группой, называется ее *топологизацией.*

* Существуют группы, являющиеся топологическими полугруппами, но не топологическими группами.

Всякая хаусдорфова бикомпактная топологическая полугруппа (см. VI.8.1 и VI.8.3), в которой выполняется закон сокращения (см. II.5.1), будет группой и даже топологической группой [см. Аренс, Bull. Amer. Math. Soc. **53** (1947), 623—630]. *

2. Всякая группа может рассматриваться как топологическая группа с дискретной топологией (см. VI.7.10). Конечная группа допускает, понятно, лишь дискретную топологизацию. Вопрос о возможности недискретной топологизации любой бесконечной группы пока открыт.

* Всякая бесконечная абелева группа может быть сделана топологической группой с недискретной топологией [Кертес и Селе, Publ. Math. **3** (1953), 187—189]. *

3. *Если A — открытое подмножество топологической группы G и g — элемент из G, то множества Ag, gA, A^{-1} также будут открытыми.*

Докажем лишь первое из этих утверждений. Если $b = ag$, $a \in A$, то $a = bg^{-1}$. Из непрерывности умножения вытекает существование такой окрестности U элемента b, что $Ug^{-1} \subseteq A$ (напомним, что A — открытое множество). Отсюда $U \subseteq Ag$, т. е. множество Ag вместе со всяким своим элементом b содержит и некоторую его окрестность, что и требовалось доказать.

Если g — элемент топологической группы G, то отображения (для всех $x \in G$)

$$x \to xg, \quad x \to gx, \quad x \to x^{-1}$$

являются изоморфными отображениями (см. VI. 7.8) *G, как топологического пространства, на себя.*

Взаимная однозначность указанных отображений очевидна и поэтому можно сослаться на предшествующую теорему, учитывая, что обратным отображением для правой *трансляции* $x \to xg$ будет правая же трансляция $x \to xg^{-1}$, а отображение $x \to x^{-1}$ обратно самому себе.

Отсюда, ввиду VI. 7.8, следует, что *если A — замкнутое подмножество топологической группы G и g — элемент из G, то множества Ag, gA, A^{-1} также будут замкнутыми.*

4. Если a и b — элементы топологической группы G, то трансляция $x \to xa^{-1}b$, $x \in G$, переводит a в b. Отсюда

и из установленного выше следует, что при доказательстве свойств пространства топологической группы, относящихся к отдельным элементам, достаточно рассмотреть лишь один фиксированный элемент, например единицу. Отсюда же следует, что при задании топологии в группе нет необходимости задавать всю полную систему окрестностей и можно ограничиться заданием *полной системы окрестностей единицы* (см. VI. 7.6).

*Система Σ подмножеств группы G тогда и только тогда может служить полной системой окрестностей единицы при некоторой топологизации этой группы, если выполняются следующие условия:

1) пересечение всех множеств, входящих в Σ, содержит лишь единицу группы G;

2) пересечение любых двух множеств из Σ содержит некоторое третье множество, принадлежащее к Σ;

3) для всякого множества U из Σ можно найти в Σ такое множество V, что $VV^{-1} \subseteq U$;

4) для всякого множества U из Σ и всякого элемента $a \in U$ в Σ можно найти такое множество V, что $Va \subseteq U$;

5) для всякого множества U из Σ и любого элемента a группы G можно найти в Σ такое множество V, что $a^{-1}Va \subseteq U$. *

5. *Пространство всякой топологической группы G регулярно и, следовательно, хаусдорфово* (см. VI. 8.1 и VI. 8.2).

Используя критерий регулярности из VI.8.2 и учитывая сказанное в предшествующем пункте, возьмем любую окрестность U единицы группы G. Так как $1 \cdot 1^{-1} = 1$, то существуют такие окрестности V_1 и V_2 элементов 1 и 1^{-1} ($= 1$, понятно), что $V_1V_2 \subseteq U$. Существует, далее, такая окрестность единицы V_3, что $V_3^{-1} \subseteq V_2$. Существует, наконец, окрестность единицы V, лежащая в пересечении $V_1 \cap V_3$ (см. VI.7.7). Ясно, что

$$VV^{-1} \subseteq U. \tag{1}$$

Пусть $a \in \overline{V}$. Так как множество aV открытое, по VI.9.3, и содержит элемент $a = a \cdot 1$ из замыкания множества V, то, по VI.7.6, в aV можно найти элемент b из V. Пусть

$b = ac$, $c \in V$. Отсюда, ввиду (1),

$$a = bc^{-1} \in VV^{-1} \subseteq U,$$

т. е. $V \subseteq U$, что и требовалось доказать.

* Пространство всякой топологической группы вполне регулярно (см. VI.8.2).

Существуют топологические группы, пространства которых не являются нормальными [А. А. Марков, Изв. АН СССР, сер. матем. **9** (1945), 3 — 64]. *

6. Всякая подгруппа A топологической группы G сама будет, очевидно, топологической группой по топологии, индуцируемой в ней (см. VI.7.9) топологией группы G.

Замыкание $\bar{A}$ подгруппы A топологической группы G само будет подгруппой. Если A — нормальный делитель в G, то и $\bar{A}$ будет нормальным делителем. Если A — абелева подгруппа, то и $\bar{A}$ будет абелевой подгруппой.

В самом деле, если $x, y \in \bar{A}$ и U — любая окрестность элемента xy, то существуют такие окрестности V элемента x и W элемента y, что $VW \subseteq U$. Существуют, далее, такие элементы $x', y' \in A$, что $x' \in V$, $y' \in W$. Принадлежащий к подгруппе A элемент $x'y'$ содержится, следовательно, в U. Этим доказано, что $xy \in \bar{A}$.

С другой стороны, если $x \in A$ и U — любая окрестность элемента x^{-1}, то существует такая окрестность V элемента x, что $V^{-1} \subseteq U$. Существует далее, такой элемент $x' \in A$, что $x' \in V$, а поэтому принадлежащий к подгруппе A элемент x'^{-1} содержится в U. Этим доказано, что $x^{-1} \in A$. Таким образом, $\bar{A}$ оказалась подгруппой группы G.

Пусть, далее, A — нормальный делитель группы G. Если $x \in \bar{A}$, $g \in G$ и U — любая окрестность элемента $g^{-1}xg$, то существует такая окрестность V элемента x, что $g^{-1}Vg \subseteq U$. В V можно найти элемент $x' \in A$, поэтому в U содержится элемент $g^{-1}x'g \in g^{-1}Ag = A$. Этим доказано, что $g^{-1}xg \in \bar{A}$, т. е. $\bar{A}$ — нормальный делитель.

Пусть, наконец, подгруппа A абелева. Если $x, y \in \bar{A}$ и U — произвольная окрестность элемента $x^{-1}y^{-1}xy$ — *коммутатора* элементов x и y, — то из непрерывности операций в группе G легко следует существование таких окрестно-

стей V элемента x и W элемента y, что $V^{-1}W^{-1}VW \subseteq U$. Существуют, далее, такие элементы x', $y' \in A$, что $x' \in V$, $y' \in W$. Отсюда

$$1 = x'^{-1}y'^{-1}x'y' \in U,$$

т. е. всякая окрестность элемента $x^{-1}y^{-1}xy$ содержит единицу, а поэтому $x^{-1}y^{-1}xy = 1$, т. е. $xy = yx$. Теорема доказана.

Всякая открытая подгруппа A топологической группы G замкнута.

Действительно, пусть $x \in \bar{A}$. Смежный класс Ax содержит x и, ввиду VI.9.3, открыт, а поэтому в нем содержится элемент из подгруппы A. Это возможно, однако, лишь при $Ax = A$, откуда $x \in A$, т. е. $\bar{A} = A$.

7. Гомоморфизм φ топологической группы G на топологическую группу G' называется *непрерывным*, если он удовлетворяет любому из следующих условий, эквивалентность которых проверяется без всяких затруднений:

1) для всякого подмножества A из G

$$\bar{A}\varphi \subseteq \overline{A\varphi};$$

2) для всякого замкнутого подмножества A' из G' его полный прообраз $A'\varphi^{-1}$ замкнут в G;

3) для всякого открытого подмножества A' из G' его полный прообраз $A'\varphi^{-1}$ открыт в G;

4) для всякой окрестности U' единицы группы G' ее полный прообраз $U'\varphi^{-1}$ открыт в G.

Непрерывный гомоморфизм φ топологической группы G на топологическую группу G' называется *открытым*, если он удовлетворяет любому из следующих эквивалентных между собою условий:

1′) для всякого открытого подмножества A из G его образ $A\varphi$ открыт в G';

2′) для всякой окрестности U единицы группы G ее образ $U\varphi$ содержит некоторую окрестность U' единицы группы G'.

Наконец, топологические группы G и G' называются *изоморфными*, если между ними существует взаимно однозначное соответствие, являющееся изоморфизмом для G и G' как для групп (см. II.4.1) и как для топологических пространств (см. VI.7.8).

8. Пусть A—замкнутая подгруппа топологической группы G, M — множество правых смежных классов группы G по подгруппе A, φ — отображение G на M, переводящее каждый элемент $x \in G$ в смежный класс Ax, Σ — полная система окрестностей пространства G, $\Sigma\varphi$ — система образов окрестностей, входящих в Σ, при отображении φ.

Множество M можно считать топологическим пространством с $\Sigma\varphi$ в качестве полной системы окрестностей.

Для доказательства достаточно применить критерий из VI.7.7. Если $Ax \neq Ay$, то, ввиду замкнутости Ay (см. VI.9.3), в Σ существует такая окрестность U, что $x \in U$ и $U \cap Ay$ пусто. Тогда $U\varphi$ содержит смежный класс Ax, но не содержит смежного класса Ay, т. е. условие α) выполнено.

Пусть, с другой стороны, окрестности U и V из Σ таковы, что $U\varphi \cap V\varphi$ содержит смежный класс Ax. Так как, по VI.9.3, множество aU открыто при всяком $a \in A$, то и произведение AU будет открытым; это же справедливо для AV. Элемент x содержится в $AU \cap AV$ и, следовательно, в этом пересечении содержится окрестность W из Σ, содержащая x. Так как $(AU)\varphi = U\varphi$, $(AV)\varphi = V\varphi$, то $W\varphi \subseteq (U\varphi \cap V\varphi)$, причем $Ax \in W\varphi$. Этим доказано, что условие β) также выполняется, т. е. закончено доказательство теоремы.

Именно в смысле указанной топологии мы будем говорить о *пространстве правых* (или, аналогично, *левых*) *смежных классов* топологической группы по замкнутой подгруппе и, в частности, о *топологии в фактор-группе топологической группы* по замкнутому нормальному делителю.

* Фактор-группа G/A топологической группы G по замкнутому нормальному делителю является топологической группой, а естественный гомоморфизм G на G/A — открытым гомоморфизмом.

Если φ—открытый гомоморфизм топологической группы G на топологическую группу G', то ядро A этого гомоморфизма является замкнутым нормальным делителем и существует такое изоморфное отображение ψ топологической группы G' на топологическую группу G/A, что произведение $\varphi\psi$ совпадает с естественным гомоморфизмом G на G/A.

Фактор-группа G/A топологической группы G тогда и только тогда дискретна, если нормальный делитель A открыт. *

9. Топологизация группы G называется *линейной* (соответственно *вполне линейной*), если она может быть задана полной системой окрестностей единицы, состоящей из подгрупп (из нормальных делителей) этой группы.

Дискретная топологизация всякой группы будет, очевидно, вполне линейной.

Система Σ нормальных делителей группы G тогда и только тогда служит полной системой окрестностей единицы при некоторой (вполне линейной) топологизации этой группы, если

1′) *пересечение всех нормальных делителей, входящих в Σ, содержит лишь единицу группы G;*

2′) *пересечение любых двух нормальных делителей из Σ содержит некоторый третий нормальный делитель, принадлежащий к Σ.*

Необходимость условий 1′) и 2′) очевидна. С другой стороны, если система нормальных делителей Σ удовлетворяет этим условиям, то система Σ_0 всех смежных классов по всем нормальным делителям из Σ удовлетворяет условиям α) и β) из VI.7.7, т. е. служит полной системой окрестностей для некоторой топологии в множестве G. Действительно, если $a, b \in G$, $a \neq b$, то, по 1′), в Σ найдется такой нормальный делитель A, что $a^{-1}b \notin A$, а тогда a и b лежат в разных смежных классах по A. Если же $a \in G$, $A, B \in \Sigma$, то, по 2′), в Σ содержится такой нормальный делитель C, что $C \subseteq A \cap B$, а тогда $aC \subseteq (aA \cap aB)$.

Остается показать, что операции группы G непрерывны в этой топологии (см. VI.9.1). Если $a, b \in G$, $A \in \Sigma$, то $aA \cdot bA = (ab)A$, что доказывает непрерывность умножения; если же $a \in G$, $A \in \Sigma$, то $(aA)^{-1} = a^{-1}A$, откуда вытекает непрерывность операции взятия обратного элемента. Теорема доказана.

Из этой теоремы следует, в частности, что *всякая убывающая последовательность нормальных делителей группы G, пересечение которой равно E, определяет вполне линейную топологизацию этой группы.*

10. *Всякая линейно топологическая группа G вполне несвязна* (см. VI.8.6).

В самом деле, пусть система подгрупп Σ служит полной системой окрестностей единицы группы G. Если $a, b \in G$, $a \neq b$, то в Σ содержится такая подгруппа A, что $a^{-1}b \notin A$,

т. е. $aA \neq bA$. Ввиду VI.9.3 всякий смежный класс xA, в том числе и aA, является открытым множеством. Открытым будет и множество $G \setminus aA$ как объединение всех отличных от aA левых смежных классов группы G по подгруппе A. Мы получили разбиение группы G на два непересекающиеся открытые (замкнутые) подмножества, причем $a \in aA$, $b \in G \setminus aA$.

* Всякая локально бикомпактная (см. VI.8.4) вполне несвязная топологизация произвольной группы линейна.

Всякая бикомпактная (см. VI.8.3) вполне несвязная топологизация произвольной группы вполне линейна. *

§ 10. Связь топологии и нормирования в кольцах и телах

1. Кольцо R называется *топологическим кольцом*, если в множестве R задана топология, относительно которой аддитивная группа кольца R является топологической группой, а мультипликативный группоид этого кольца — топологическим группоидом (см. VI.9.1).

Ассоциативное тело K называется *топологическим телом*, если в K задана топология, относительно которой оно является топологическим кольцом, и если, сверх того, операция взятия обратного элемента непрерывна в смысле VI.9.1. Мультипликативная группа топологического тела будет, следовательно, топологической группой. Определение топологического тела легко преобразуется к такому виду, когда его можно применить и к неассоциативным телам или кольцам с делением.

Читатель без труда сформулирует определение изоморфизма топологических колец. Вообще, многие вопросы, рассмотренные в предшествующем параграфе для топологических групп, могут быть поставлены и для топологических колец и тел. Мы не будем, однако, этим сейчас заниматься.

2. *Всякое псевдонормированное кольцо* R (см. VI.4.7) *с действительными значениями псевдонормы* w *является топологическим кольцом, причем его полную систему окрестностей нуля составляют множества* U_α (*где* α — *любое положительное действительное число*) *тех элементов* a *из* R, *для которых* $w(a) < \alpha$.

Доказательство. Мы знаем из VI.9.3, что если бы аддитивная группа кольца R уже была топологической группой, то в ней вместе с U_α открытыми были бы и все множества вида $a+U_\alpha$. Покажем, что система всех таких множеств (при любых $a\in R$ и любых положительных действительных α) на самом деле служит полной системой окрестностей для некоторой топологии в множестве R (см. VI.7.7).

Пусть $a,\ b\in R,\ a\neq b$. Если $w(b-a)=\gamma$, то $\gamma>0$. Множество $a+U_\gamma$ содержит элемент a, так как $0\in U_\gamma$, но не содержит элемента b, так как $b-a\notin U_\gamma$.

Пусть, с другой стороны,

$$a\in(b+U_\beta)\cap(c+U_\gamma).$$

Тогда $w(a-b)=\delta_1<\beta$, $w(a-c)=\delta_2<\gamma$. Положим

$$\alpha=\min(\beta-\delta_1,\ \gamma-\delta_2).$$

Если $x\in R$, $w(x)<\alpha$, то

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

причем

$$w[(a-b)+x]<\delta_1+\alpha\leqslant\delta_1+(\beta-\delta_1)=\beta.$$

Этим доказано, что $a+U_\alpha\subseteq b+U_\beta$. Аналогично и $a+U_\alpha\subseteq$ $\subseteq c+U_\gamma$.

Мы получили топологию в множестве R, причем видим, что во всякой окрестности элемента $a\in R$ содержится окрестность вида $a+U_\alpha$. Докажем непрерывность операций кольца R в этой топологии.

Пусть $a,\ b\in R$ и $a+b+U_\gamma$ — данная окрестность элемента $a+b$. Если $\delta=\frac{1}{2}\gamma$ и $x,\ y\in U_\delta$, то

$$w(x+y)\leqslant w(x)+w(y)<2\delta=\gamma.$$

Этим доказано, что

$$(a+U_\delta)+(b+U_\delta)\subseteq a+b+U_\gamma,$$

т. е. доказана непрерывность сложения.

Пусть, далее, $a\in R$ и $-a+U_\alpha$ — данная окрестность элемента $-a$. Если $x\in U_\alpha$, то, так как $w(-x)=w(x)$ и $-x\in U_\alpha$, будет

$$-(a+U_\alpha)\subseteq -a+U_\alpha.$$

Этим доказана непрерывность операции взятия противоположного элемента.

Если, наконец, $a,\ b \in R$, $w(a)=\alpha$, $w(b)=\beta$ и $ab+U_\gamma$ — данная окрестность элемента ab, то в качестве δ возьмем такое положительное действительное число, что

$$\alpha\delta+\delta\beta+\delta^2<\gamma.$$

Если $x,\ y \in U_\delta$, то

$$w(ay+xb+xy) \leqslant w(a)\,w(y)+w(x)\,w(b)+w(x)\,w(y)<\gamma,$$

т. е.

$$(a+U_\delta)(b+U_\delta) \subseteq ab+U_\gamma,$$

чем доказана непрерывность произведения. Теорема доказана.

3. *Если в ассоциативном теле K задана действительная норма $w(a)$* (см. VI. 4.1), *то в топологии, определенной в* VI. 10.2, *K будет топологическим телом.*

Мы уже знаем, что K будет топологическим кольцом, и поэтому остается доказать лишь непрерывность операции взятия обратного элемента.

Заметим сперва, что из

$$w(a)=w(a\cdot 1)=w(a)\cdot w(1), \qquad a \in K,$$

следует $w(1)=1$. Поэтому для $a \neq 0$, ввиду

$$w(a)\cdot w(a^{-1})=w(aa^{-1})=w(1)=1,$$

будет

$$w(a^{-1})=[w(a)]^{-1}.$$

Пусть теперь $a \in K$, $a \neq 0$, $w(a)=\alpha$ и пусть $a^{-1}+U_\gamma$ — данная окрестность элемента a^{-1}. Положим

$$\delta=\frac{a\gamma}{a^{-1}+\gamma}; \tag{1}$$

ясно, что $0<\delta<\alpha$. Пусть $w(x)<\delta$. Тогда $a+x \neq 0$ и существует такое $y \in K$, что

$$(a+x)^{-1}=a^{-1}+y.$$

Отсюда

$$y=(a+x)^{-1}-a^{-1}=a^{-1}[a-(a+x)](a+x)^{-1}=$$
$$=a^{-1}(-x)(a+x)^{-1}.$$

Однако $w(a^{-1}) = \alpha^{-1}$, $w(-x) = w(x) < \delta$. Далее,

$$w(a) = w[(a+x)-x] \leqslant w(a+x) + w(x),$$

откуда

$$w(a+x) \geqslant w(a) - w(x) > \alpha - \delta > 0,$$

а поэтому

$$w[(a+x)^{-1}] = [w(a+x)]^{-1} < (\alpha - \delta)^{-1}.$$

Таким образом,

$$w(y) < \alpha^{-1}\delta\,(\alpha - \delta)^{-1},$$

что после замены δ его выражением (1) приводит к

$$w(y) < \gamma.$$

Этим доказано, что $(a + U_\delta)^{-1} \subseteq a^{-1} + U_\gamma$. Теорема доказана.

4. Обычное нормирование поля действительных чисел и поля комплексных чисел при помощи абсолютной величины (модуля) *индуцирует* (в смысле доказанных выше теорем) обычную топологизацию этих полей. Обычное нормирование тела кватернионов (см. VI.4.1) индуцирует топологизацию этого тела, совпадающую на его аддитивной группе с обычной топологизацией четырехмерного евклидова пространства (см. VI.7.10). Именно эти топологизации указанных трех тел мы будем иметь в виду, когда будем говорить об этих телах как о топологических телах.

В поле рациональных чисел и в поле p-адических чисел (см. III.3.12) их p-адическое нормирование (см. VI.5.6 и VI.5.8) также индуцирует топологизацию. Эта топологизация (равно как и порождаемые ею топологизации кольца целых p-адических чисел и аддитивных групп указанных полей и кольца) называется их *p-адической топологизацией*. Ввиду целочисленности и логарифмичности p-адической нормы систему окрестностей нуля в этой топологии составляют множества U_k (где k — любое целое число) таких чисел a (рациональных или p-адических), p-адическая норма которых строго *больше* k.

5. Пусть K — ассоциативное топологическое тело. Элемент $a \in K$ называется *топологически нильпотентным*, если последовательность его степеней a^n, $n = 1, 2, \ldots$, сходится к нулю, т. е. любая окрестность нуля U содержит все

эти степени, кроме, может быть, конечного числа их. Элемент $a \in K$, $a \neq 0$, называется *нейтральным*, если ни a, ни a^{-1} не являются топологически нильпотентными. Наконец, множество A, $A \subset K$, называется *ограниченным справа*, если для любой окрестности нуля U можно указать такую окрестность нуля V, что $AV \subseteq U$.

Докажем следующую теорему [Капланский, Duke Math. J. **14** (1947), 527—541; для топологических полей, в несколько иной формулировке — И. Р. Шафаревич, ДАН СССР **40** (1943), 149—151]:

Пусть K — ассоциативное топологическое тело. Топология этого тела тогда и только тогда индуцируется действительной нормой, если выполняются условия:

1) *множество N всех топологически нильпотентных элементов тела K открыто и ограничено справа;*

2) *если элемент a — топологически нильпотентный, а элемент b — топологически нильпотентный или нейтральный, то произведение ba топологически нильпотентно.*

6. Необходимость этих условий проверяется без затруднений. Если топология тела K индуцируется действительной нормой $w(a)$, то топологическая нильпотентность элемента a равносильна тому, что $w(a) < 1$, а нейтральность элемента a — тому, что $w(a) = 1$. Отсюда сразу вытекает условие 2). Ограниченность справа множества N следует из включения $NU_\gamma \subseteq U_\gamma$. Наконец, множество N будет и открытым, так как $N = U_1$.

7. Перейдем к доказательству достаточности этих условий. Покажем сперва, что если $a \in N$ и $a \neq 0$, то $a^{-1} \notin N$. Пусть это не так и пусть U — произвольная окрестность нуля. Тогда, ввиду равенства $0 \cdot 0 = 0$ и непрерывности умножения, существуют такие окрестности нуля V и W, что $V \cdot W \subseteq U$. Так как при достаточно больших натуральных n $a^n \in V$, $a^{-n} \in W$, то $1 \in U$, что невозможно, так как U была произвольная окрестность нуля.

Обозначим через M множество всех нейтральных элементов. Условие 2) из формулировки теоремы можно записать теперь в виде

$$(N \cup M) N \subseteq N. \tag{2}$$

Ясно, что $1 \in M$. Из определения нейтрального элемента следует, что если $a \in M$, то и $a^{-1} \in M$. Пусть, далее, $a, b \in M$. Если $ab \in N$, то, по (2), $a^{-1}(ab) = b \in N$; если же $(ab)^{-1} \in N$, то $b(ab)^{-1} = a^{-1} \in N$. Таким образом, $ab \in M$, т. е.

$$MM \subseteq M. \tag{3}$$

Пусть теперь $a \in N$, $b \in M$. Если $ab \in M$, то, ввиду (3) и $b^{-1} \in M$, $(ab)b^{-1} = a \in M$. Если же $(ab)^{-1} \in N$, то $b(ab)^{-1} = a^{-1} \in N$. Таким образом, $ab \in N$, т. е.

$$NM \subseteq N. \tag{4}$$

Из (2) — (4) следует

$$(N \cup M)(N \cup M) \subseteq (N \cup M). \tag{5}$$

Пусть, далее, $a \in N$, а x — произвольный элемент тела K, отличный от нуля. Если U — заданная окрестность нуля, то из $x^{-1} \cdot 0 \cdot x = 0$ и непрерывности умножения следует существование такой окрестности нуля V, что $x^{-1}Vx \subseteq U$. Так как $a^n \in V$ при достаточно больших натуральных n, то $x^{-1}a^n x = (x^{-1}ax)^n \in U$; отсюда $x^{-1}ax \in N$, т. е.

$$x^{-1}Nx \subseteq N. \tag{6}$$

Если же $a \in M$, $x \neq 0$, то $x^{-1}ax \in M$, так как из $b = x^{-1}ax \in N$ следовало бы, ввиду (6), $xbx^{-1} = a \in N$, а из $b^{-1} \in N$ следовало бы $a^{-1} \in N$. Таким образом,

$$x^{-1}Mx \subseteq M. \tag{7}$$

8. Из полученных результатов, в частности из (3) и (7), вытекает, что M *будет нормальным делителем в мультипликативной группе* K^* *отличных от нуля элементов тела* K. Можно рассмотреть, следовательно, фактор-группу K^*/M. Отметим, что эта фактор-группа будет единичной тогда и только тогда, если N состоит лишь из одного нуля, т. е., ввиду условия 1), если топология тела K дискретна, — следует учесть, что тело K не может содержать *нильпотентных* элементов, т. е. таких элементов a, что $a \neq 0$, но $a^n = 0$ при некотором натуральном n.

Ввиду (5) множество $N \cup M$ (без нуля) распадается на полные смежные классы по M и эти смежные классы составляют в фактор-группе K^*/M подполугруппу. Легко проверяются, ввиду (6) и (7), условия 1) — 4) из VI.1.3, т. е.

эта подполугруппа будет полугруппой положительных элементов при некоторой линейной упорядоченности группы K^*/M.

Полученная упорядоченность оказывается архимедовой (см. VI. 3.3). В самом деле, если a, $b \in K^*$ и смежные классы aM и bM строго положительны, то $a \in N$, $b \in N$. Пусть U — данная окрестность нуля; можно считать, что $U \subseteq N$, так как N открыто. Ввиду $0 \cdot b^{-1} = 0$ существует такая окрестность нуля V, что $Vb^{-1} \subseteq U$, а так как из $a \in N$ вытекает существование такого натурального числа k, что $a^k \in V$, то $a^k b^{-1} \in U$ и поэтому $a^k b^{-1} \in N$. Отсюда следует, что в упорядоченной группе K^*/M будет $(aM)^k > bM$, т. е. архимедовость этой группы доказана.

9. Ввиду теоремы Гельдера (VI. 3.4) группа K^*/M изоморфна подгруппе аддитивной группы действительных чисел с ее естественной упорядоченностью. Это определяет гомоморфное отображение φ группы K^* в аддитивную группу действительных чисел, причем в нуль отображаются элементы из M и только они, а образы отличных от нуля элементов из N (и только этих элементов) строго положительны. Пусть λ — пока произвольное положительное действительное число. Положим для $a \in K$

$$\left.\begin{aligned} &w(a) = 2^{-\lambda \cdot a\varphi}, \qquad a \neq 0, \\ &w(0) = 0. \end{aligned}\right\} \tag{8}$$

Ясно, что условия 1 и 2 из VI. 4.1 выполняются. Позже мы покажем, что возможен такой выбор λ, при котором будет выполняться и условие 3.

Из (8) легко следует, что $w(a) = 1$ тогда и только тогда, когда $a \in M$, а $w(a) < 1$ тогда и только тогда, когда $a \in N$. Как в VI. 10.2, обозначим через U_α (где α — положительное действительное число) множество тех элементов $a \in K$, для которых $w(a) < \alpha$. Если топология тела K дискретна, то при $\alpha < 1$ будет $U_\alpha = 0$.

Пусть топология тела K не дискретна. Рассмотрим произвольное U_α. В K существует такой элемент b, что $w(b) > \alpha^{-1}$. Так как множество N открытое, то найдется такая окрестность нуля U, что $bU \subseteq N = U_1$. Поэтому $U \subseteq U_\alpha$.

Обратно, пусть U — произвольная окрестность нуля тела K. Ввиду ограниченности справа множества N и предположенной нами недискретности тела K существует такое

$c \neq 0$, что $Nc \subseteq U$. Отсюда следует, что если $\alpha = w(c)$, то $U_\alpha \subseteq U$, так как $U_\alpha = U_1 c = Nc$.

Таким образом, *если* λ *будет подобрано так, что* $w(a)$ *окажется нормой, то топология, индуцируемая этой нормой в смысле* VI. 10.2, *будет совпадать с исходной топологией тела* K (см. определение эквивалентности систем окрестностей в VI. 7.8).

10. Продолжая считать λ выбранным произвольно, докажем существование такого числа l, что для всех $a \in K$, имеет место неравенство

$$w(1+a) \leqslant l(1+w(a)). \tag{9}$$

В самом деле, если бы такого числа l не существовало, то мы нашли бы такую последовательность элементов $a_n \in K$, $a_n \neq -1$, $n = 1, 2, \ldots$, что при $n \to \infty$

$$\frac{1+w(a_n)}{w(1+a_n)} = \frac{1}{w(1+a_n)} + \frac{w(a_n)}{w(1+a_n)} \to 0,$$

т. е.

$$\frac{1}{w(1+a_n)} = w((1+a_n)^{-1}) \to 0,$$

$$\frac{w(a_n)}{w(1+a_n)} = w(a_n(1+a_n)^{-1}) \to 0.$$

Отсюда следовало бы, однако, ввиду доказанного в предшествующем пункте, что последовательности

$$(1+a_n)^{-1} \quad \text{и} \quad a_n(1+a_n)^{-1}, \quad n = 1, 2, \ldots, \tag{10}$$

сходились бы к нулю в топологии тела K, что невозможно, так как сложение в теле K непрерывно, а сумма n-х членов последовательностей (10) равна 1.

Из (9) следует, что если хотя бы один из элементов a, $b \in K$ отличен от нуля, то

$$w(a+b) \leqslant l(w(a)+w(b)). \tag{11}$$

Действительно, если $a \neq 0$, то

$$w(a+b) = w[a(1+a^{-1}b)] \leqslant$$
$$\leqslant lw(a)[1+w^{-1}(a)w(b)] = l(w(a)+w(b)).$$

Ясно, что (11) справедливо и при $a = b = 0$. Из (11) следует

$$w(a+b) \leqslant 2l \max(w(a), w(b)). \tag{12}$$

11. Существует столь малое положительное действительное число ν, что $(2l)^{\nu} \leqslant 2$. Заменим в определении (8) число λ числом $\lambda\nu$. Так как при этом число $w(a)$ возводится в степень ν, то, относя с этого момента символ w к новому выбору числа λ, мы из (12) получим

$$w(a+b) \leqslant 2 \max (w(a), w(b)). \tag{13}$$

Отсюда легко следует для $k = 1, 2, \ldots$

$$w(a_1 + a_2 + \ldots + a_{2^k}) \leqslant 2^k \max_{1 \leqslant i \leqslant 2^k} w(a_i). \tag{14}$$

Условимся обозначать через n n-кратное единицы тела K; этот элемент будет встречаться лишь под знаком w, и поэтому нет опасности смешать его с натуральным числом n. Отметим также, что K не предполагается телом без характеристики. Из (14) следует

$$w(2^k) \leqslant 2^k, \qquad k = 1, 2, \ldots \tag{15}$$

Покажем, что для любого натурального n

$$w(n) \leqslant 2n. \tag{16}$$

В самом деле, пусть $2^k \leqslant n < 2^{k+1}$. Будем доказывать (16) индукцией по k, так как при $k = 0$ это утверждение справедливо. Так как $n = (n - 2^k) + 2^k$, то при $w(n - 2^k) \leqslant w(2^k)$ из (13) и (15) вытекает

$$w(n) \leqslant 2w(2^k) \leqslant 2 \cdot 2^k \leqslant 2n.$$

Если же $w(n - 2^k) \geqslant w(2^k)$, то, применяя, ввиду $n - 2^k < 2^k$, индуктивное предположение, получаем, что

$$w(n) \leqslant 2w(n - 2^k) \leqslant 2 \cdot 2(n - 2^k) = 4n - 2^{k+2} < 2n.$$

12. Возьмем теперь произвольный элемент $a \in K$ и применим (14) к разложению элемента $(1+a)^{n-1}$ по формуле бинома, полагая n равным некоторой степени числа 2. Формула бинома в рассматриваемом случае применима, так как элементы a и 1 перестановочны. Так как, ввиду (16),

$$w(C_{n-1}^k) \leqslant 2C_{n-1}^k,$$

где C_{n-1}^k — биномиальный коэффициент, то

$$w((1+a)^{n-1}) \leqslant n \max w(C_{n-1}^k a^k) = n \max [w(C_{n-1}^k) w(a^k)] \leqslant$$
$$\leqslant 2n \max (C_{n-1}^k w^k(a)) \leqslant 2n(1 + w(a))^{n-1}.$$

Отсюда следует

$$[w(1+a)]^{n-1} \leqslant 2n\,(1+w(a))^{n-1},$$

а так как n может быть сколь угодно большой степенью числа 2, то

$$w(1+a) \leqslant 1+w(a).$$

Неравенство 3_2 из VI. 4.1, равносильное в рассматриваемом нами случае действительной нормы условию 3 из определения нормы — именно, в этом случае $w(-1)=1$ и поэтому выполняется равенство 3_1 из VI. 4.1, — выводится теперь так же, как (11) было выведено из (9). Теорема VI. 10.5 доказана.

* Если ассоциативное топологическое тело локально бикомпактно (см. VI. 8.4), то его топология индуцируется действительной нормой [Капланский, Duke Math. J. **14** (1947), 527—541].

Поле действительных чисел, поле комплексных чисел и тело кватернионов, рассматриваемые с их естественной топологией (см. VI. 10.4), являются единственными связными (см. VI. 8.6) локально бикомпактными ассоциативными топологическими телами [Л. С. Понтрягин, Ann. of Math. **33** (1932), 163—174].

Пусть F — топологическое поле. Топология поля F тогда и только тогда индуцируется неархимедовой нормой (см. VI. 4.3) со значениями в некоторой линейно упорядоченной группе, пополненной нулем, если: 1) в F существует окрестность нуля, порождающая ограниченную аддитивную подгруппу; 2) если подмножество $A \subset F$ не пересекается с некоторой окрестностью нуля, то A^{-1} ограничено [Зелинский, Bull. Amer. Math. Soc. **54** (1948), 1145—1150]. *

§ 11. Соответствия Галуа. Основная теорема теории Галуа

1. Говорят, что между частично упорядоченными множествами M и M' установлено *соответствие Галуа*, если указаны отображения φ: $M \to M'$ и ψ: $M' \to M$, удовлетворяющие (для любых a, $b \in M$, $a', b' \in M'$) следующим требованиям:

α) если $a \leqslant b$, то $a\varphi \geqslant b\varphi$;
если $a' \leqslant b'$, то $a'\psi \geqslant b'\psi$;

β) $a\varphi\psi \geqslant a$, $a'\psi\varphi \geqslant a'$.

Это понятие тесно связано с понятием замыкания в частично упорядоченном множестве (см. VI. 7.1):

Если между частично упорядоченными множествами M и M' установлено соответствие Галуа, то равенства

$$\begin{aligned} \bar{a} &= a\varphi\psi, \quad a\in M, \\ \overline{a'} &= a'\psi\varphi, \quad a'\in M', \end{aligned} \tag{1}$$

определяют соответственно в M и в M' отношения замыкания. Если M_0 и M'_0 — системы всех элементов из M и M' соответственно, замкнутых при этих замыканиях, то φ отображает инверсно изоморфно M_0 на M'_0, а ψ отображает инверсно изоморфно M'_0 на M_0, причем на этих множествах отображения φ и ψ обратны друг другу.

Покажем, что равенства (1) вводят в множествах M и M' отношения замыкания. Ясно, что β) непосредственно приводит к условию 1_0) из VI. 7.1, а из α) следует условие 2_0). С другой стороны, из β) следует, ввиду $a\varphi\in M'$, неравенство

$$a\varphi\psi\varphi \geqslant a\varphi,$$

а так как, по α), из $a\varphi\psi \geqslant a$ вытекает

$$a\varphi\psi\varphi \leqslant a\varphi,$$

то на самом деле

$$a\varphi\psi\varphi = a\varphi, \tag{2}$$

и поэтому

$$a\varphi\psi\varphi\psi = a\varphi\psi, \quad a\in M. \tag{3}$$

Этим доказано, что выполняется и условие 3_0) из VI. 7.1.

Системы M_0 и M'_0 элементов, замкнутых в M и M' относительно построенных нами замыканий, состоят соответственно из элементов $a\varphi\psi$, где $a\in M$, и $a'\psi\varphi$, где $a'\in M'$. Равенство (2), записанное в виде

$$(a\varphi)\,\psi\varphi = a\varphi,$$

показывает, что образ при φ любого элемента a из M замкнут в M'. Отсюда следует, что φ отображает систему M_0 в систему M'_0. Аналогично отображение ψ переводит M'_0 в M_0.

Из справедливости равенства (3) и аналогичного ему равенства

$$a'\psi\varphi\psi\varphi = a'\psi\varphi, \quad a'\in M',$$

вытекает, однако, что в действительности φ и ψ, рассматриваемые лишь на M_0 и M_0', будут обратными друг другу взаимно однозначными отображениями. Они являются даже инверсными изоморфизмами, как следует из α). Теорема доказана.

2. Приведем лишь одно из многочисленных применений соответствий Галуа в алгебре. Рассмотрим поле K с отмеченным в нем подполем P и обозначим через $G(K, P)$ множество всех автоморфизмов поля K, оставляющих на месте каждый элемент из P. Это множество будет, очевидно, группой относительно умножения автоморфизмов. Группа $G(K, P)$ называется *группой Галуа* поля K над подполем P.

Обозначим через M множество всех подмножеств A поля K, содержащих в себе подполе P,

$$P \subseteq A \subseteq K,$$

а через M' — множество всех подмножеств A' группы $G(K, P)$, причем оба эти множества рассматриваются с их теоретико-множественной частичной упорядоченностью. Для всякого $A \in M$ обозначим через $A\varphi$ совокупность тех автоморфизмов из $G(K, P)$, которые оставляют множество A поэлементно неподвижным. С другой стороны, для всякого $A' \in M'$ обозначим через $A'\psi$ множество всех элементов поля K, оставляемых на месте всеми автоморфизмами из A'.

Ясно, что $A\varphi$ *будет подгруппой группы Галуа* $G(K, P)$ *и* $A'\psi$ *— подполем поля* K, *содержащим* P. Немедленно проверяется также, что отображения φ и ψ удовлетворяют условиям α) и β) из VI. 11.1. Нами установлено, следовательно, соответствие Галуа между множествами M и M', что определяет замыкания в каждом из этих двух множеств. Наконец, *отображения* φ *и* ψ *являются обратными друг другу инверсно изоморфными соответствиями* между системами $M_0 \subset M$ и $M_0' \subset M'$ замкнутых элементов, т. е. *между некоторой системой подполей поля* K, *содержащих подполе* P, *и некоторой системой подгрупп группы Галуа* $G(K, P)$.

3. Особенно интересны те случаи, когда оказываются замкнутыми как все подполя, промежуточные между P и K, так и все подгруппы группы Галуа, т. е. когда обозрение в с е х подполей поля K, содержащих поле P, сводится на

обозрение всех подгрупп группы $G(K, P)$. Рассмотрим один такой случай.

Будем предполагать, что рассматриваются лишь поля без характеристики (см. III. 2.11). Будем считать также, что читатель уже знаком из курса высшей алгебры с основами алгебры многочленов над полями [см., например, А. Г. Курош, Курс высшей алгебры, изд. 10, 1971, §§ 47 — 49; дальше цитируется как «Курс»].

Пусть, как и выше, $P \subset K$. Элемент $\alpha \in K$ называется *алгебраическим* над полем P, если он является корнем некоторого многочлена из кольца $P[x]$ и, следовательно, корнем однозначно определенного неприводимого многочлена $\varphi(x)$, старший коэффициент которого равен единице. Степень этого многочлена называется *степенью* элемента α, а его корни, лежащие в поле K или в некотором расширении этого поля, — элементами, *сопряженными* с α.

Поле K называется *алгебраическим расширением* поля P, если всякий элемент из K алгебраичен над P. Поле K есть *конечное расширение* поля P, а именно *расширение степени* n, если K является конечномерной линейной алгеброй над P (см. V. 6.6), причем имеет размерность n. Степень K над P будет обозначаться символом $(K:P)$.

Всякое конечное расширение является алгебраическим расширением.

Действительно, если $(K:P)=n$, то всякие $n+1$ элементы из K линейно зависимы над P. В частности, если $\alpha \in K$, то элементы $1, \alpha, \alpha^2, \ldots, \alpha^n$ линейно зависимы над P, а это означает, что α является корнем многочлена степени n из кольца $P[x]$.

4. Теорема о примитивном элементе. *Если поле K без характеристики является алгебраическим расширением поля P и порождается присоединением к P конечного числа элементов, то K порождается присоединением к P одного элемента.*

Достаточно рассмотреть случай присоединения двух элементов. Пусть

$$K = P(\alpha, \beta).$$

Если $\varphi(x)$ и $\psi(x)$ — неприводимые над P многочлены, имеющие своими корнями соответственно α и β, то существует такое расширение L поля K (например, поле разложения про-

изведения $\varphi(x)\psi(x)$, см. «Курс», § 49), в котором оба эти многочлена имеют все свои корни.

Пусть

$$\alpha_1 = \alpha,\ \alpha_2,\ \ldots,\ \alpha_k$$

будут все лежащие в L корни многочлена $\varphi(x)$; они различны, так как $\varphi(x)$ не имеет кратных корней. Аналогично

$$\beta_1 = \beta,\ \beta_2,\ \ldots,\ \beta_l$$

будут все лежащие в L корни многочлена $\psi(x)$. Так как P, как поле без характеристики, бесконечно, то найдется такой элемент $c \in P$, что

$$\alpha_i + c\,\beta_j \neq \alpha + c\,\beta, \tag{4}$$

если хотя бы один из индексов i, j отличен от 1.

Положим

$$\gamma = \alpha + c\beta. \tag{5}$$

Ясно, что $P(\gamma) \subseteq K$. Рассмотрим теперь многочлен

$$\overline{\varphi}(x) = \varphi(\gamma - cx)$$

с коэффициентами из поля $P(\gamma)$. Так как, по (5),

$$\overline{\varphi}(\beta) = \varphi(\gamma - c\beta) = \varphi(\alpha) = 0$$

и, как мы знаем, $\psi(\beta) = 0$, то многочлены $\overline{\varphi}(x)$ и $\psi(x)$ имеют общий корень β. Это единственный их общий корень: если $\overline{\varphi}(\beta_j) = 0$, $j \neq 1$, то

$$\varphi(\gamma - c\beta_j) = 0,$$

т. е. $\gamma - c\beta_j$ равно некоторому α_i в противоречие с условием (4).

Отсюда следует, что $x - \beta$ будет наибольшим общим делителем многочленов $\overline{\varphi}(x)$ и $\psi(x)$. Коэффициенты этих многочленов, а поэтому и их наибольшего общего делителя, лежат в поле $P(\gamma)$, т. е. $\beta \in P(\gamma)$. Отсюда, по (5), и $\alpha \in P(\gamma)$. Таким образом,

$$K = P(\alpha, \beta) = P(\gamma),$$

что и требовалось доказать.

5. Алгебраическое расширение K поля P называется *нормальным расширением*, если всякий неприводимый многочлен из кольца $P[x]$, имеющий в поле K хотя бы один корень, имеет в K все свои корни, т. е. разлагается над K на линейные множители.

* Поле K тогда и только тогда будет нормальным расширением своего подполя P, если K порождается присоединением к P всех корней некоторого множества многочленов из кольца $P[x]$. *

6. *Если поле K без характеристики является конечным степени n и нормальным расширением своего подполя P, то группа Галуа $G(K, P)$ конечна и имеет порядок n.*

В самом деле, K алгебраично над P, по VI.11.3, и, по VI.11.4, обладает примитивным элементом,

$$K = P(\alpha).$$

Так как $(K:P) = n$, то всякий элемент $\beta \in K$ обладает однозначной записью вида

$$\beta = b_0 + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1},$$
$$b_0, b_1, b_2, \ldots, b_{n-1} \in P, \tag{6}$$

а поэтому α имеет степень n над полем P. Ввиду нормальности K над P в поле K содержаться n различных (так как поле без характеристики) элементов, сопряженных с α:

$$\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n. \tag{7}$$

Ясно, что

$$K = P(\alpha_i), \qquad i = 1, 2, \ldots, n.$$

Как известно (см. «Курс», § 49), существует однозначно определенный автоморфизм поля K, оставляющий элементы поля P на месте и переводящий α в α_i, $i = 1, 2, \ldots, n$, а именно автоморфизм φ_i, отображающий элемент β из (6) в элемент

$$\beta_i = b_0 + b_1\alpha_i + b_2\alpha_i^2 + \ldots + b_{n-1}\alpha_i^{n-1}.$$

Это дает n элементов группы Галуа $G(K, P)$. С другой стороны, пусть φ будет произвольный автоморфизм поля K, принадлежащий к $G(K, P)$, и пусть $\alpha\varphi = \alpha'$. Если

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n$$

— тот неприводимый многочлен из кольца $P[x]$, корнем которого является α, то, так как $a\varphi = a$ для всех $a \in P$,

$$f(\alpha') = \alpha'^n + a_1\alpha'^{n-1} + \ldots + a_n =$$
$$= (\alpha^n + a_1\alpha^{n-1} + \ldots + a_n)\varphi = [f(\alpha)]\varphi = 0\varphi = 0.$$

Элемент α' совпадает, следовательно, с одним из элементов α_i из (7), а поэтому автоморфизм φ совпадает с соответствующим автоморфизмом φ_i. Теорема доказана.

7. Ясно, что поля Q, промежуточные между P и K,

$$P \subseteq Q \subseteq K, \tag{8}$$

составляют структуру по теоретико-множественному включению. Ясно также, что из $K = P(\alpha)$ следует $K = Q(\alpha)$ для всякого Q, удовлетворяющего включениям (8).

Если поле K конечно над полем P, то промежуточное поле Q конечно над P, K конечно над Q и

$$(K:P) = (K:Q)(Q:P).$$

В самом деле, конечность Q над P следует из того, что Q является подпространством векторного пространства K над полем P. Конечность K над Q вытекает из того, что мы получим базу K над Q, если возьмем в базе K над P максимальную подсистему, линейно независимую над Q. Пусть, наконец, $\alpha_1, \alpha_2, \ldots, \alpha_k$ будет база K над Q, а $\beta_1, \beta_2, \ldots, \beta_l$ — база Q над P. Тогда для любого $\gamma \in K$ будет

$$\gamma = \sum_{i=1}^{k} b_i \alpha_i, \qquad b_i \in Q, \qquad i = 1, 2, \ldots, k, \tag{9}$$

а так как

$$b_i = \sum_{j=1}^{l} a_{ij} \beta_j, \qquad a_{ij} \in P, \tag{10}$$

то

$$\gamma = \sum_{i=1}^{k} \sum_{j=1}^{l} a_{ij} (\alpha_i \beta_j). \tag{11}$$

Линейная независимость над P системы kl элементов $\alpha_i \beta_j$ вытекает из того, что из равенства нулю правой части равенства (11) следовало бы, ввиду линейной независимости системы $\alpha_1, \alpha_2, \ldots, \alpha_k$ над Q, равенство нулю коэффициентов b_i в (9), где b_i имеют вид (10), а тогда, ввиду линейной независимости системы $\beta_1, \beta_2, \ldots, \beta_l$ над P, равны нулю все коэффициенты a_{ij}.

Если поле K нормально над полем P, то оно нормально и над всяким промежуточным полем Q.

Пусть, в самом деле, неприводимый над Q многочлен $g(x)$ обладает в K корнем α. Неприводимый над P многочлен $f(x)$, корнем которого является α, имеет в поле K все свои корни, а так как $g(x)$ служит делителем для $f(x)$ в кольце $Q[x]$ (см. «Курс», § 48), то и $g(x)$ разлагается над полем K на линейные множители.

8. Основная теорема теории Галуа. *Если поле K без характеристики является конечным и нормальным расширением поля P, то соответствие, сопоставляющее всякому промежуточному полю Q* (см. (8)) *группу Галуа $G(K, Q)$ поля K над этим полем Q, является инверсным изоморфизмом между структурой всех промежуточных полей и структурой всех подгрупп группы Галуа $G(K, P)$.*

Действительно, отображение φ из соответствия Галуа, рассмотренного в VI. 11.2, сопоставляет всякому промежуточному полю Q подгруппу группы $G(K, P)$, являющуюся группой Галуа K над Q,

$$Q\varphi = G(K, Q).$$

Основная теорема будет, следовательно, доказана, если мы покажем, что при замыканиях, определяемых указанным соответствием Галуа, будут замкнутыми как все промежуточные поля, так и все подгруппы группы Галуа.

Если Q — произвольное промежуточное поле, то

$$Q\varphi = G(K, Q) = U \subseteq G(K, P),$$

$$U\psi = Q' = Q\varphi\psi,$$

$$Q'\varphi = G(K, Q') = U' = U\psi\varphi \subseteq G(K, P).$$

Поэтому $Q \subseteq Q'$, $U \subseteq U'$. Обозначим через s и s' соответственно порядки подгрупп U и U'. Тогда

$$s \leqslant s'$$

и, по VI. 11.7,

$$(K : Q) \geqslant (K : Q'). \tag{12}$$

Однако, по VI. 11.6,

$$(K : Q) = s, \quad (K : Q') = s'.$$

Поэтому в (12) имеет место равенство, откуда

$$Q' = Q.$$

Пусть теперь U — произвольная подгруппа группы $G(K, P)$. Положим

$$\begin{aligned} U\psi &= Q, \\ Q\varphi &= U\psi\varphi = U' \subseteq G(K, P). \end{aligned} \tag{13}$$

Тогда $U \subseteq U'$, т. е., как и выше, $s \leqslant s'$. Пусть, однако, $K = Q(\alpha)$. Если

$$\varepsilon = \sigma_1, \ \sigma_2, \ \ldots, \ \sigma_s \tag{14}$$

— все автоморфизмы, включая тождественный автоморфизм ε, составляющие подгруппу U, то α будет корнем многочлена степени s

$$f(x) = (x - \alpha\sigma_1)(x - \alpha\sigma_2) \ldots (x - \alpha\sigma_s).$$

Коэффициенты этого многочлена, написанные по формулам Вьета, не меняются при любом из автоморфизмов (14) — умножение всех элементов группы U справа на один из ее элементов лишь переставляет эти элементы. Поэтому, в силу определения отображения ψ и (13),

$$f(x) \in Q[x],$$

т. е. степень α над Q не больше s, откуда

$$s' = (K : Q) \leqslant s.$$

Таким образом, $s' = s$, т. е. $U' = U$. Теорема доказана.

Из этой теоремы следует, в частности, что *в рассматриваемых условиях число полей, промежуточных между P и K, будет конечным.*

* В условиях основной теоремы промежуточное поле Q тогда и только тогда нормально над полем P, если соответствующая подгруппа $U = G(K, Q)$ является нормальным делителем группы $G(K, P)$. Группа $G(Q, P)$ изоморфна при этом фактор-группе

$$G(K, P)/U.$$

В случае полей без характеристики конечность и нормальность K над P не только достаточны, но и необходимы для справедливости утверждения основной теоремы.

Если поле K без характеристики является алгебраическим и нормальным (но не обязательно конечным) расширением поля P, то соответствие

$$Q \to G(K, Q)$$

является инверсным изоморфизмом между структурой всех подполей, промежуточных между P и K, и структурой всех подгрупп группы $G(K, P)$, замкнутых в линейной топологии этой группы (см. VI.9.9), определяемой следующим образом: полную систему окрестностей единицы составляют подгруппы $G(K, Q_0)$, где Q_0 пробегает все подполя поля K, являющиеся конечными нормальными расширениями поля P [Крулль, Math. Ann. **100** (1928), 687 — 698]. *

УКАЗАТЕЛЬ ЛИТЕРАТУРЫ [1])

1 Адамсон И. Т. (Adamson I. T.), Rings, moduls and algebras, Edinburgh, 1971.

2*. Азумая Г. (Azumaya G.), Алгебраическая теория простых колец (на японском языке), Токио, 1951.

3*. Алберт А. А. (Albert A. A.), Modern higher algebra, Chicago, 1937.

4*. Алберт А. А. (Albert A. A.), Structure of algebras, N. Y., 1939.

5* Алберт А. А. (Albert A. A.), Fundamental concepts of higher algebra, Chicago — London, 1956; перепечатки, 1959, 1961.

6*. Александров П. С., Введение в теорию групп, М., 1938; 2-е изд., М., 1951; румынский перевод, Бухарест, 1954; немецкий перевод, Берлин, 1954, 1960, 1971; украинский перевод, Киев, 1955; польский перевод, Варшава, 1956; английский перевод, Лондон, 1959.

7. Александров П. С., Комбинаторная топология, М. — Л., 1947.

8. Александров П. С., Введение в общую теорию множеств и функций, М. — Л., 1948.

9. Александров П. С. и Хопф Х. (Alexandroff P. und Hopf H.), Topologie I, Berlin, 1935.

10*. Альмейда Коста А. (Almeida Costa A.), Abelian groups, noncommutative rings and ideals, hypercomplex systems and representation, Lisboa, в 2-х тт., 1942, 1948.

11*. Альмейда Коста А. (Almeida Costa A.), Anéis associativos não comutativos, Lisboa, 1955.

12. Альмейда Коста А. (Almeida Costa A.), Cours d'algèbre générale, в 2-х тт., Lisboa, 1968.

13. Андрунакиевич В. А., Арнаутов В. И. и Рябухин Ю. М., Кольца, в сб. «Алгебра. Топология. Геометрия. 1965 (Итоги науки, ВИНИТИ АН СССР)», М., 1967, 133—180.

14*. Артин Э. (Artin E.), Galois theory, Notre Dame, 1942; 2-е изд., 1946, 1948; китайский перевод, Шанхай, 1958; немецкий перевод, Лейпциг, 1960.

15*. Артин Э. (Artin E.), Geometric algebra, N. Y. — London, 1957; русский перевод, «Геометрическая алгебра», М., 1969.

16. Артин Э. (Artin E.), Algebraic numbers and algebraic functions, London, 1968.

---

[1]) Звездочкой отмечена литература, вошедшая в 1-е издание книги.

17*. Артин Э., Несбитт Ц. и Трэлл Р. (Artin E., Nesbitt C. J. and Thrall R. M.), Rings with minimum condition, Ann. Arbor, 1944.
18. Атья М. и Макдональд И. (Atiyah M. F. and Macdonald I. G.), Introduction to commutative algebra, Reading (Mass.), 1969; русский перевод, «Введение в коммутативную алгебру», М., 1972.
19. Бальцежик С. (Balcerzyk S.), Wstęp do algebry homologiczej, Warszawa, 1970.
20. Баранович Т. М., Универсальные алгебры, в сб. «Алгебра. Топология. Геометрия. 1966 (Итоги науки, ВИНИТИ АН СССР)», М., 1968, 109—136.
21*. Барбильян Д. (Barbilian D.), Teoria aritmetica a idealelor (in inele necomutative), Bucureşti, 1956.
22. Баршай Я. (Barshay J.), Topics in rings theory, N. Y., 1969.
23*. Баумгартнер Л. (Baumgartner L.), Gruppentheorie, Berlin — Leipzig, 1921; 3-е изд., 1958; русский перевод «Теория групп», М. — Л., 1934.
24. Белоусов В. Д., Неассоциативные бинарные системы, в сб. «Алгебра. Топология. Геометрия. 1965 (Итоги науки, ВИНИТИ АН СССР)», М., 1967, 63—81.
25. Белоусов В. Д., Основы теории квазигрупп и луп, М., 1967.
26. Белоусов В. Д., Алгебраические сети и квазигруппы, Кишинев, 1971.
27. Берж К. (Berge Cl.), Théorie des graphes et ses applications, Paris, 1958.
28. Берлекэмп Э. (Berlekamp E. R.), Algebraic coding theory, N. Y. — St. Louis — San Francisco — Toronto — London — Sydney, 1968; русский перевод, «Алгебраическая теория кодирования», М., 1971.
29. Берман С. Д., Представления конечных групп, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», М., 1966, 83—122.
30*. Бёрнер Х. (Boerner H.), Darstellungen von Gruppen mit Berücksichtigung der Bedürfnisse der modernen Physik, Berlin — Göttingen — Heidelberg, 1955.
31*. Бернсайд В. (Burnside W.), Theory of groups of finite order, Cambridge, 1897; 2-е изд., Cambridge, 1911; перепечатки, N. Y., 1955, 1958.
32*. Биркгоф Г. (Birkhoff G.), Lattice theory, N. Y., 1940; 2-е, переработанное изд., N. Y., 1948; 3-е изд., Providence, 1967; русский перевод, «Теория структур», М., 1952.
33. Биркгоф Г. (Birkhoff G.), The role of modern algebra in computing, «Comput. Algebra and number theory (SIAM — AMS Proc. 4)», Providence, 1971, 1—47.
34. Биркгоф Г. и Барти Т. (Birkhoff G. and Bartee T.), Modern applied algebra, N. Y., 1970.
35*. Биркгоф Г. и Маклейн С. (Birkhoff G. and MacLane S.), A survey of modern algebra, N. Y., 1941; перепечатка, 1944; 2-е, переработанное изд., 1953; 3-е изд., 1965.
36. Вокуть Л. А., Жевлаков К. А. и Кузьмин Е. Н., Теория колец, в сб. «Алгебра. Топология. Геометрия. 1968 (Итоги науки, ВИНИТИ АН СССР)», М., 1970, 9—56.

37*. Боревич З. И. и Фаддеев Д. К., Теория гомологий в группах, I, Вестник Ленингр. ун-та, 1956, № 7, 3—39; II, там же, 1959, № 7, 72—87.
38. Боревич З. И. и Шафаревич И. Р., Теория чисел, М., 1964; 2-е изд., 1972.
39. Борель А. (Borel A.), Linear algebraic groups, N. Y. — Amsterdam, 1969; русский перевод, «Линейные алгебраические группы», М., 1972.
40*. Борувка О. (Borůvka O.), Ůvod do theorie grup, Praha, 1944; 2-е изд., 1952.
41. Борувка О. (Borůvka O.), Grundlagen der Gruppoid- und Gruppentheorie, Berlin, 1960.
42*. Брак Р. (Bruck R. H.), A survey of binary systems, Berlin — Göttingen — Heidelberg, 1958; 2-е изд., 1966; 3-е изд., 1971.
43. Браун Х. и Кёхер М. (Braun H. and Koecher M.), Jordan-Algebren, Berlin — Heidelberg — N. Y., 1966.
44. Бринкман Г.-Б. и Пуппе Д. (Brinkmann H.-B. und Puppe D.), Kategorien und Functoren, «Lecture Notes in Math.», № 18, Berlin — Heidelberg — N. Y., 1966.
45. Бринкман Г.-Б. и Пуппе Д. (Brinkmann H.-B. und Puppe D.), Abelsche und exakte Kategorien, Korrespondenzen, Berlin — Heidelberg — N. Y., 1969.
46. Буксбаум Д. (Buchsbaum D. A.), Exact categories and duality, Trans. Amer. Math. Soc. 80, № 1 (1955), 1—34; русский перевод, «Точные категории и двойственность» (в книге: Картан А. и Эйленберг С., Гомологическая алгебра, М., 1960, стр. 451—496).
47. Букур И. и Деляну А. (Bukur I. and Deleany A.), Introduction to the theory of categories and functors, London — N. Y. — Sydney, 1969; русский перевод, «Введение в теорию категорий и функторов», М., 1972.
48. Бурбаки Н. (Bourbaki N.), Éléments de mathématique; partie I, livre I, Théorie des ensembles, Paris, 1957—1963; русский перевод, «Начала математики», часть 1, книга 1, «Теория множеств», М., 1965.
49. Бурбаки Н. (Bourbaki N.), Éléments de mathématique; partie I, livre II, Algèbre, Paris, 1958—1964; существенно переработанное изд., Paris, 1970; русский перевод, «Элементы математики», книга 2, «Алгебра», в 3-х тт. (I. Алгебраические структуры. Линейная и полилинейная алгебра; II. Многочлены и поля. Упорядоченные группы; III. Модули. Кольца. Формы), М., 1962—1966.
50. Бурбаки Н. (Bourbaki N.), Éléments de mathématique; partie I, livre III, Topologie générale, Paris, 1940—1947; существенно переработанное издание, Paris, 1960—1967; русские переводы, «Элементы математики», книга 3, «Общая топология», в 2-х книгах (I. Основные структуры; II. Числа и связанные с ними группы и пространства), М., 1958—1959; с переработанного французского изд. (I. Основные структуры; II. Топологические группы Числа и связанные с ними группы и пространства), М., 1968—1969.

51. Бурбаки Н. (Bourbaki N.), Éléments de mathématique; partie II, Algèbre commutative, Paris, 1960—1965; русский перевод, «Элементы математики. Коммутативная алгебра», М., 1971.
52. Бурбаки Н. (Bourbaki N.), Éléments de mathématique; partie II, Groupes et algèbres de Lie, Paris, 1968; русский перевод, «Элементы математики. Группы и алгебры Ли (гл. IV. Группы Кокстера и системы Титса; гл. V. Группы, порожденные отражениями; гл. VI. Системы корней)», М., 1972.
53. Бурбаки Н. (Bourbaki N.), Éléments de mathématique; fasc. XXXII, Théories spectrales, Paris, 1967; русский перевод, «Элементы математики. Спектральная теория», М., 1972.
54. Бурроу М. (Burrow M.), Representation theory of finite groups, N. Y. — London, 1965.
55. Бусаркин В. М. и Горчаков Ю. М., Конечные расщепляемые группы, М., 1968.
56. Бэр Р. (Baer R.), Automorphismen von Erweiterungsgruppen, Paris, 1935.
57*. Бэр Р. (Baer R.), Linear algebra and projective geometry, N. Y., 1952; русский перевод, «Линейная алгебра и проективная геометрия», М., 1955.
58. Бэренс Э.-А. (Behrens E.-A.), Ring theory, N. Y. — London, 1971.
59*. Ван-дер-Варден Б. Л. (van der Waerden B. L.), Moderne Algebra, в 2-х тт., Berlin, 1930, 1931; 2-е изд., 1937, 1940; 3-е изд., 1950; 4-е изд., «Algebra», Berlin — Göttingen — Heidelberg, 1955; перепечатка, 1959; 5-е изд., 1960; 6-е изд., 1964; русский перевод, «Современная алгебра», М. — Л., 1934, 1937; 2-й русский перевод, М. — Л., 1947; английский перевод, Нью-Йорк, 1949; венгерский перевод, Будапешт, 1953; португальский перевод, Лиссабон, 1954; китайский перевод, Ухань, 1943.
60. Ван-дер-Варден Б. Л. (van der Waerden B. L.), Die Gruppentheoretische Methode in der Quantenmechanik, Berlin, 1932.
61*. Ван-дер-Варден Б. Л. (van der Waerden B. L.), Gruppen von linearen Transformationen, Berlin, 1935; перепечатка, N. Y., 1948.
62. Ван-дер-Варден Б. Л. (van der Waerden B. L.), Einführung in die algebraische Geometrie, Berlin, 1939.
63. Варнер С. (Warner S.), Classical modern algebra, N. Y., 1971.
64. Варусфель А. (Warusfel A.), Structures algébriques finies, groupes, anneaux, corps, Paris, 1971.
65*. Василаке С. (Vasilache S.), Elemente de teoria multimilor şi a structurilor algebrice, Bucureşti, 1956.
66. Вебер Г. М. (Weber H. M.), Lehrbuch der Algebra, в 2-х тт., Braunschweig, 1895, 1896; 2-е изд., в 3-х тт., Brauschweig, 1898, 1899, 1908; 3-е изд., в 3-х тт., N. Y., 1962.
67*. Вейль А. (Weil A.), L'intégration dans les groupes topologiques et ses applications, Paris, 1940; русский перевод, «Интегрирование в топологических группах и его применения», М., 1950.
68. Вейль А. (Weil A.), Foundations of algebraic geometry, N. Y., 1946.

69. Вейль А. (Weil A.), Basic number theory, Berlin — Heidelberg — N. Y., 1967; русский перевод, «Основы теории чисел», М., 1972.
70. Вейль Г. (Weyl H.), Gruppentheorie und Quantenmechanik, Leipzig, 1931.
71*. Вейль Г. (Weyl H.), The classical groups, their invariants and representations, Princeton, 1939; 2-е изд., 1946; русский перевод, «Классические группы, их инварианты и представления», М., 1947.
72. Вейль Г. (Weyl H.), Algebraic theory of numbers, 1940; русский перевод, «Алгебраическая теория чисел», М., 1947.
73. Вейль Г. (Weyl H.), Symmetry, London, 1952; немецкий перевод, Basel — Stuttgart, 1955; русский перевод «Симметрия», М., 1968.
74. Вейс Э. (Weiss E.), Cohomology of groups, N. Y. — London, 1969.
75. Венков Б. Б., Гомологическая алгебра, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», М., 1966, 203—235.
76. Виландт Г. (Wielandt H. W.), Unendliche Permutationsgruppen, Tübingen, 1960.
77. Виландт Г. (Wielandt H. W.), Finite permutation groups, N. Y. — London, 1964; 2-е изд., 1968.
78*. Виленкин Н. Я., Теория топологических групп, II, Успехи матем. наук 5, № 4 (1950), 19—74.
79. Винберг Э. Б., Группы Ли и однородные пространства, в сб. «Алгебра. Топология, 1962 (Итоги науки, ВИНИТИ АН СССР)», М., 1963, 5—32.
80. Виноградов А. А., Упорядоченные алгебраические системы, в сб. «Алгебра. Топология. Геометрия. 1965 (Итоги науки, ВИНИТИ АН СССР)», М., 1967, 83—131.
81. Виноградов А. А., Упорядоченные алгебраические системы, в сб. «Алгебра. Топология. Геометрия. 1966 (Итоги науки, ВИНИТИ АН СССР)», М., 1968, 91—108.
82. Владимиров Д. А., Булевы алгебры, М., 1969.
83. Вольвачев Р. Т. и Супруненко Д. А., Линейные группы, в сб. «Алгебра. Топология. Геометрия, 1965 (Итоги науки, ВИНИТИ АН СССР)», М., 1967, 45—61.
84*. Вольф П. (Wolf P.), Algebraische Theorie der Galoisschen Algebren, Berlin, 1956.
85. Габриэль П. (Gabriel P.), Des catégories abéliennes, Bull. Soc. math. France **90**, № 3 (1962), 323—448.
86. Габриель П. и Цисман М. (Gabriel P. and Zisman M.), Calculus of fractions and homotopy theory, Berlin — Heidelberg — N. Y., 1967; русский перевод, «Категории частных и теория гомотопий», М., 1971.
87. Галуа Э. (Galois É.), Oeuvres mathématiques, Paris, 1897; 2-е изд., 1951; русский перевод, «Сочинения», М. — Л., 1936.
88. Гельфанд И. М., Райков Д. А. и Шилов Г. Е., Коммутативные нормированные кольца, М., 1960.
89. Герике Х. (Gericke H.), Theorie der Verbände, Mannheim, 1963.
90. Гечег Ф. и Пеак И. (Gécseg F. and Peák I.), Algebraic theory of automata, Budapest, 1972.

91. Гинзбург А. (Ginzburg A.), Algebraic theory of automata, N. Y. — London, 1968.
92. Гиро Ж. (Giraud Jean), Cohomologie non abélienne, Berlin — Heidelberg — N. Y., 1971.
93. Глейхгевихт Б. (Gleichgewicht B.), Elementy algebry abstrakcyjnej, в 2-х тт., Warszawa, 1966, 1970.
94*. Гливенко В. И., Théorie générale des structures, Paris, 1938.
95. Глускин Л. М., Полугруппы, в сб. «Алгебра. Топология. 1962 (Итоги науки, ВИНИТИ АН СССР)», М., 1963, 33—58.
96. Глускин Л. М., Полугруппы, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», М., 1966, 161—202.
97. Глускин Л. М., Шайн Б. М. и Шеврин Л. Н., Полугруппы, в сб. «Алгебра. Топология. Геометрия. 1966 (Итоги науки, ВИНИТИ АН СССР)», М., 1968, 9—56.
98. Глухов М. М., Стеллецкий И. В. и Фофанова Т. С., Теория структур, в сб. «Алгебра. Топология. Геометрия. 1968 (Итоги науки, ВИНИТИ АН СССР)», М., 1970, 101—154.
99*. Глушков В. М., Строение локально бикомпактных групп и пятая проблема Гильберта, УМН **12**, № 2 (1957), 3—41.
100. Глушков В. М., Абстрактная теория автоматов, УМН **16**, № 5 (1961), 3—62; поправка, там же **17**, № 2 (1962), 270.
101. Глушков В. М., Теория алгоритмов, Киев, 1961.
102. Годеман Р. (Godement R.), Topologie algébrique et théorie des faisceaux, Paris, 1958.
103. Годеман Р. (Godement R.), Cours d'algèbre, Paris, 1963.
104. Горенштейн Д. (Gorenstein D.), Finite groups, N. Y. — Evansten — London, 1968.
105. Граве Д. А., Теория конечных групп, Киев, 1908.
106*. Граев М. И., Теория топологических групп, I, УМН **5**, № 2 (1950), 3—56.
107. Грёбнер В. (Gröbner W.), Moderne algebraische Geometrie. Die idealtheoretischen Grundlagen, Wien — Innsbruck, 1949.
108. Грей М. (Gray M.), A radical approach to algebra, Reading (Mass.), 1970.
109. Гретцер Г. (Grätzer G.), Universal algebra, Princeton (N. J.), 1968.
110. Гретцер Г. (Grätzer G.), Lattice theory. First concepts and distributive lattice, San Francisco, 1971.
111. Гросман И. и Магнус В. (Grossman I. and Magnus W.), Groups and their graphs, N. Y., 1964; русский перевод, «Группы и их графы», М., 1971.
112. Гротендик А. (Grothendieck A.), Sur quelques points d'algèbre homologique, Tôhoku Math. J., second series, **9**, № 2—3 (1957), 119—221; русский перевод, «О некоторых вопросах гомологической алгебры», М., 1961.
113. Гротендик А. и Дьёдонне Ж. (Grothendieck A. et Diendonné J. A.), Eléments de géométrie algébrique I, Berlin — Heidelberg — N. Y., 1971.
114. Гудстейн Р. (Goodstein R.), Boolean algebra, Oxford — London — Paris — Frankfurt — N. Y., 1963.

115. Двингер Ф. (Dwinger Ph.), Introduction to Boolean algebras, Würzburg, 1961; 2-е, дополненное изд., 1971.
116*. Дёйринг М. (Deuring M.), Algebren, Berlin, 1935; N. Y., 1948.
117. Дейсен П. (Deussen P.), Halbgruppen und Automaten, Berlin — Heidelberg — N. Y., 1971.
118. Демазюр М. и Габриэль П. (Demazure M. et Gabriel P.), Groupes algébriques. I. Géométrie algébrique — généralités, groupes commutatifs, Paris — Amsterdam, 1970.
119. Дёмушкин С. П., Теория полей классов. Расширения полей, в сб. «Алгебра. Топология. Геометрия. 1967 (Итоги науки, ВИНИТИ АН СССР)», М., 1969, 59—69.
120. Джанс И. П. (Jans J. P.), Rings and homology, N. Y., 1964.
121. Джейтеджейнкар А. (Jategaonkar A. V.), Left principal ideals rings, Berlin — Heidelberg — N. Y., 1970.
122*. Джекобсон Н. (Jacobson N.), The theory of rings, N. Y., 1943; русский перевод, «Теория колец», М., 1947.
123*. Джекобсон Н. (Jacobson N.), Lectures in abstract algebra, Princeton (N. J.) — Toronto — N. Y. — London, vol. I, 1951; vol. II, 1953; vol. III, 1964; китайский перевод, Пекин, 1960.
124*. Джекобсон Н. (Jacobson N.), Structure of rings, Providence, R. I., 1956; 2-е изд., 1964; русский перевод, «Строение колец», М., 1961.
125. Джекобсон Н. (Jacobson N.), Lie algebras, N. Y. — London, 1962; русский перевод, «Алгебры Ли», М., 1964.
126. Джонсон Б. (Jónsson B.), Topics in universal algebra, «Lect. Notes Math.», 1972.
127*. Джонсон Р. (Johnson R. E.), First cours of abstract algebra, N. Y., 1953.
128. Дивинский Н. (Divinsky N. J.), Rings and radical, London, 1965.
129. Диксон Дж. Д. (Dixon John D.), The structure of linear groups, London, 1971.
130*. Диксон Л. (Dickson L. E.), Linear groups with an exposition of the Galois field theory, Leipzig, 1901; перепечатка, N. Y., 1958.
131. Диксон Л. (Dickson L. E.), Linear algebras, Cambridge, 1914; русский перевод, «Линейные алгебры», Харьков, 1935.
132. Диксон Л. (Dickson L. E.), Algebras and their arithmetics, Chicago, 1923; перепечатка, N. Y., 1938; N. Y., 1960.
133. Диксон Л. (Dickson L. E.), Modern algebraic theories, Chicago, 1926; перепечатка, N. Y. — London, 1959.
134. Дин Р. (Dean R. A.), Elements of abstract algebra, N. Y., 1966.
135. Доннелен Т. (Donnellan Th.), Lattice theory, Oxford — London, 1968.
136. Дынкин Е. Б., Структура полупростых алгебр Ли, УМН 2, № 4 (1947), 59—127.
137. Дьёдонне Ж. (Diendonné J.), Sur les groupes classiques, Paris, 1948; перепечатка, Paris, 1958.
138. Дьёдонне Ж. (Diendonné J.), La géométrie des groupes classiques, Berlin — Göttingen — Heidelberg, 1955; 2-е изд., Berlin — Göttingen — Heidelberg, 1963; 3-е изд., Berlin, 1971.

139*. Дюбрей П. (Dubreil P.), Algèbre, v. I, Paris, 1946; 2-е изд., Paris, 1954; 3-е изд., 1963.
140. Дюбрей П. и Дюбрей-Жакотэн М. Л. (Dubreil P. et Dubreil-Jacotin M. L.), Leçons d'algèbre moderne, Paris, 1961; 2-е изд., Paris, 1964.
141*. Дюбрей-Жакотэн М. Л., Лезьё Л. и Круазо Р. (Dubreil-Jacotin M. L., Lesieur L. et Croisot R.), Leçons sur la théorie des treillis, des structures algébriques ordonnées et des treillis géométriques, Paris, 1953.
142. Жаффар П. (Jaffard P.), Les systèmes d'idéaux, Paris, 1960.
143. Желобенко Д. П., Компактные группы Ли и их представления, М., 1970.
144*. Жордан К. (Jordan C.), Traité des substitutions et des équations algébriques, Paris, 1870; фоторепродукция, Paris, 1957.
145. Зарисский О. (Zariski O.), An introduction to the theory of algebraic surfaces, Berlin — Heidelberg — N. Y., 1969; 2-е, пополненное изд., «Algebraic surfaces», там же, 1971.
146*. Зарисский О. и Самюэль П. (Zariski O. and Samuel P.), Commutative algebra, v. 1, 1958; v. 2, 1960; Princeton (N. J.) — Toronto — London — N. Y.; русский перевод, «Коммутативная алгебра», в 2-х тт., М., 1963.
147. Зыков А. А., Теория конечных графов, I, Новосибирск, 1969.
148*. Капланский И. (Kaplansky I.), Infinite Abelian groups, Ann. Arbor, 1954; перепечатка, 1956; 2-е изд., 1969.
149*. Капланский И. (Kaplansky I.), An introduction to differential algebra, Paris, 1957; русский перевод, «Введение в дифференциальную алгебру», М., 1959.
150. Капланский И. (Kaplansky I.), Rings of operators, N. Y., 1968.
151. Капланский И. (Kaplansky I.), Fields and rings, Chicago, 1969.
152. Капланский И. (Kaplansky I.), Commutative rings, Boston, 1970.
153. Капп К. М. и Шнейдер Х. (Kapp K. M. and Schneider H.), Completely 0-simple semigroups, N. Y., 1969.
154. Карвалло М. (Carvallo M.), Monographie des treillis et algèbre de Boole, Paris, 1962.
155. Каргаполов М. И. и Мерзляков Ю. И., Бесконечные группы, в сб. «Алгебра. Топология. Геометрия. 1966 (Итоги науки, ВИНИТИ АН СССР)», М., 1968, 57—90.
156. Каргаполов М. И. и Мерзляков Ю. И., Основы теории групп, М., 1972.
157*. Кармайкл Р. (Carmichael R. D.), Introduction to the theory of groups of finite order, Boston, 1937; перепечатка, N. Y., 1956.
158*. Картан А. и Эйленберг С. (Cartan H. and Eilenberg S.), Homological algebra, Princeton (N. J.), 1956; русский перевод, «Гомологическая алгебра», М., 1960.
159. Картан Э. (Cartan E.), Sur la structure des groupes de transformations finis et continus, Thèse, Paris, 1894.

160*. Кейсан М. и Деляше А. (Queysanne M. et Delachet A.), L'algèbre moderne, Paris, 1955; 2-е изд., 1957; 3-е изд., 1960.
161. Кертес А. (Kertész A.), Vorlesungen über Artinsche Ringe, Budapest, 1968; Leipzig, 1968.
162. Клауда Д. (Klauda D.), Allgemeine Mengenlehre, в 2-х тт., 2-е, дополненное изд., Berlin, 1968.
163. Клини С. (Kleene S. C.), Introduction to metamathematics, N. Y. — Toronto, 1952; русский перевод, «Введение в метаматематику», М., 1957.
164. Клиффорд А. и Престон Г. (Clifford A. H. and Preston G. B.), The algebraic theory of semigroups, в 2-х тт., Providence, 1961, 1967; русский перевод, «Алгебраическая теория полугрупп», в 2-х тт., М., 1972.
165. Кнайт Дж. Т. (Knight J. T.), Commutative algebra, «Lect. Notes Math.», London, 1971.
166. Кнатсон Д. (Knutson D.), Algebraic spaces, «Lect. Notes Math.», London, 1971.
167. Кокорин А. И. и Копытов В. М., Линейно упорядоченные группы, М., 1972.
168*. Кокстер Х. С. М. и Мозер В.О.Дж. (Coxeter H. S. M. and Moser W. O. J.), Generators and relations for discrete groups, Berlin — Göttingen — Heidelberg, 1957; 2-е изд., 1965.
169. Кон П. М. (Cohn P. M.), Lie groups, Cambridge, 1957.
170. Кон П. М. (Cohn P. M.), Universal algebra, N. Y. — London, 1965; русский перевод, «Универсальная алгебра», М., 1968.
171. Кон П. М. (Cohn P. M.), Free rings and their relations, N. Y. — London, 1971.
172. Кострикин А. И., Конечные группы, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», М., 1966, 7—46.
173*. Кохендёрфер Р. (Kochendörffer R.), Einführung in die Algebra, Berlin, 1955; 2-е изд., Berlin, 1962.
174. Кохендёрфер Р. (Kochendörffer R.), Lehrbuch der Gruppentheorie unter besonderer Berücksichtigung der endlichen Gruppen, Leipzig, 1966.
175. Коэн П. Дж. (Cohen P. J.), Set theory and the continuum hypothesis, N. Y. — Amsterdam, 1966; русский перевод, «Теория множеств и континуум-гипотеза», М., 1969.
176. Крауч Р. Б. и Бэкмен Д. Н. (Crouch R. B. and Beckman D. N.), The structure of abstract algebra, Glenwiew (Ill.).
177*. Крулль В. (Krull W.), Idealtheorie, Berlin, 1935; перепечатка, N. Y., 1948; 2-е изд., Berlin — Heidelberg — N. Y., 1968.
178. Круз Р. Л. и Прайс Д. Т. (Kruse R. L. and Price D. T.), Nilpotent rings, N. Y. — London — Paris, 1969.
179. Куратовский К. (Kuratowski K.), Topology, в 2-х тт., N. Y. — London — Warszawa, 1966, 1968; русский перевод, «Топология», М., 1966, 1969.
180. Куратовский К. и Мостовский А. (Kuratowski K. and Mostowski A.), Teoria mnogości, Warszawa, 1952; 2-е, переработанное изд., 1966; английское изд., «Set theory», Amsterdam — Warszawa, 1967; русский перевод, «Теория множеств», М., 1970.
181*. Курош А. Г., Пути развития и некоторые очередные проблемы теории бесконечных групп, УМН **3** (1937), 5—15.

182*. Курош А. Г., Теория групп, М. — Л., 1944, 2-е, переработанное изд., М., 1953; 3-е, дополненное (с обзором «Развитие теории бесконечных групп за 1952—1965 гг.») изд., М., 1967. Переводы: с 1-го изд. — на немецкий (с добавлением Б. Неймана), Берлин, 1953; со 2-го изд. — на венгерский (с добавлением Б. Неймана), Будапешт, 1955; на английский (в 2-х тт., с добавлением К. Хирша), Нью-Йорк, 1955, 1956 (повторно — в 1960); на румынский, Бухарест, 1959; на японский (в 2-х тт.), Япония, 1960, 1961; на китайский, КНР (первый из двух томов), 1964; с 3-го изд. — на немецкий в 2-х тт., с пополнением автором библиографии за 1966—1968 гг.), Берлин, 1970, 1972.

183*. Курош А. Г., Современное состояние теории колец и алгебр, УМН **6**, № 2 (1951), 3—15.

184. Курош А. Г., Лекции по общей алгебре, 1-е изд., М., 1962; переводы: на английский (авторизованный перевод К. А. Хирша), Нью-Йорк, 1963; перепечатка, 1965; на немецкий, Лейпциг, 1964; на китайский, КНР, 1964; на польский, Варшава, 1965; на французский, Париж, 1967; на чешский, Прага, 1968; на японский (в 2-х тт.), 1966, 1970.

185. Курош А. Г., Мультиоператорные кольца и алгебры, УМН **24**, № 1 (1969), 3—15.

186. Курош А. Г., Общая алгебра (лекции 1969/70 учебного года), МГУ, М., 1970.

187. Курош А. Г., Лившиц А. Х. и Шульгейфер Е. Г., Основы теории категорий, УМН **15**, № 6 (1960), 3—52; переводы: на румынский, Бухарест, 1961; на английский, США, 1962; на немецкий, Берлин, 1963 [см. 187′].

187′. Курош А. Г., Лившиц А. Х., Шульгейфер Е. Г. и Цаленко М. Ш. (Kurosch A. G., Liwschitz A. Ch., Schulgeifer E. G. und Zalenko M. S.), Zur Theorie der Kategorien, Berlin, 1963 (книга состоит из немецких переводов статей [187] и [374]).

188*. Курош А. Г. и Черников С. Н., Разрешимые и нильпотентные группы, УМН **2**, № 3 (1947), 18—59; английский перевод, Нью-Йорк, 1953.

189. Кэртис Ч. и Райнер И. (Curtis C. W. and Reiner I.), Representation theory of finite groups and associative algebras, N. Y. — London, 1962; русский перевод, «Теория представлений конечных групп и ассоциативных алгебр», М., 1969.

190. Ламбек И. (Lambek J.), Lectures on rings and modules, Waltham — Toronto — London, 1966; русский перевод, «Кольца и модули», М., 1971.

191. Ламбек И. (Lambek J.), Torsion theories, additive semantics and rings of quotients, Berlin — Heidelberg — N. Y., 1971.

192. Леви-Брюль Ж. (Lévy-Bruhl J.), Introduction aux structures algébriques, Paris, 1968.

193*. Ледерман В. (Ledermann W.), Introduction to the theory of finite groups, Edinbourgh — London — N. Y., 1949; 2-е изд., 1953; 3-е изд., 1957; 4-е, дополненное изд., 1961.

194. Лезьё Л. и Круазо Р. (Lesieur L. et Croisot R.), Algèbre Noethérienne non commutative, Paris, 1963.

195. Леман А. (Lehman A.), Postulates for a normed Boolean algebra, Madison (Wisconsin), 1963.

196. Ленг С. (Lang S.), Introduction to algebraic geometry, N. Y. — London, 1958.
197. Ленг С. (Lang S.), Abelian varieties, N. Y. — London, 1959
198. Ленг С. (Lang S.), Diophantine geometry, N. Y., 1962.
199. Ленг С. (Lang S.), Algebraic numbers, Reading (Mass.) — Palo Alto — London, 1964; русский перевод, «Алгебраические числа», М., 1966.
200. Ленг С. (Lang S.), Algebra, Reading (Mass.), 1965; русский перевод, «Алгебра», М., 1968.
201. Ленер И. (Lehner J.), Discontinuous groups and automorphic functions, Providenc, 1964.
202*. Лентин А. и Ривo Ж. (Lentin A. et Rivaud J.), Éléments d'algèbre moderne, Paris, 1956; 2-е изд., 1957; 3-е изд., 1958.
203. Лентин А. и Ривo Ж., (Lentin A. et Rivaud J.), Leçons d'algèbre moderne, Paris, 1961; 2-е изд., «Algebra moderna» (исп.), Madrid, 1967.
204. Лившиц А. Х., Цаленко М. Ш. и Шульгейфер Е. Г., Теория категорий, в сб. «Алгебра. Топология. 1962 (Итоги науки, ВИНИТИ АН СССР)», М., 1963, 90—106.
205. Линдон Р. (Lyndon R. C.), Notes on logic, Toronto — N. Y. — London, 1966; русский перевод, «Заметки по логике», М., 1968.
206*. Литлвуд Д. Е. (Littlewood D. E.), The theory of group characters and matrix representations of groups, 2-е изд., Oxford, 1950.
207. Литлвуд Д. Е. (Littlewood D. E.), The skeleton-key of Mathematics, 3-е изд., London, 1960.
208. Лифшиц В. Н. и Садовский Л. Е., Алгебраические модели вычислительных машин, УМН **27**, № 3 (1972), 79—125.
209. Лоренц Ф. (Lorenz F.), Quadratische Formen über Körpern, Berlin — Heidelberg — N. Y., 1970.
210*. Лоумонт Дж. (Lomont J. S.), Application of finite groups, N. Y. — London, 1959.
211*. Луговский Г. и Вейнерт Г. И. (Lugowski H. und Weinert H. J.), Grundzüge der Algebra, Teil 1, Allgemeine Gruppentheorie, Leipzig, 1957; Teil 2, Allgemeine Ring- und Körpertheorie, Leipzig, 1958, 1959; 3-е изд., 1967; Teil 3, Auflösungstheorie algebraischer Gleichungen, Leipzig, 1960; 2-е изд., 1967.
212. Любарский Г. Я., Теория групп и ее применение к физике, М., 1958.
213*. Ляпин Е. С., Полугруппы, М., 1960.
214. Магнус В. (Magnus W.), Allgemeine Gruppentheorie (In Enzyklopädie der mathematischen Wissenschaften, 2-е изд., Bd. I/1, H. 9, 1939).
215. Магнус В., Каррас А. и Солитэр Д. (Magnus W., Karrass A. and Solitar D.), Combinatorial group theory: presentations of groups in terms of generators and relations, N. Y. — London — Sydney, 1966.
216. Макдаффи Г. (MacDuffee C. C.), An introduction to abstract algebra, N. Y., 1940; Gloucester (Mass.), 1966.
217*. Маккой Н. Х. (McCoy N. H.), Rings and ideals, Baltimore, 1948.

218. Маккой Н. Х. (McCoy N. H.), Interoduction to modern algebra, Boston (Mass.) — London, 1960.
219. Маккой Н. Х. (McCoy N. H.), The theory of rings, N. Y. — London, 1964.
220. Маклейн С. (MacLane S.), Homology, Berlin — Göttingen — Heidelberg, 1963; русский перевод, «Гомология», М., 1966.
221. Маклейн С. (MacLane S.), Kategorien. Begriffssprache und mathematische Theorie, Berlin — Heidelberg — N. Y., 1972.
222. Маклейн С. и Биркгоф Г. (MacLane S. and Birkhoff G.), Algebra, N. Y. — London, 1967.
223. Мальцев А. И., Группы и другие алгебраические системы, в сб. «Математика, ее содержание, методы и значение», т. 3, М., 1956, 248—331.
224. Мальцев А. И., Конструктивные алгебры, I, УМН **16**, № 3 (1961), 3—60.
225. Мальцев А. И., Алгоритмы и рекурсивные функции, М., 1965.
226. Мальцев А. И., Алгебраические системы, М., 1970.
227. Мамфорд Д. (Mumford D.), Lectures on curves on an algebraic surface, Princeton (N. J.), 1966; русский перевод, «Лекции о кривых на алгебраической поверхности», М., 1968.
228. Мамфорд Д. (Mumford D.), Abelian varieties, Bombay, 1968; русский перевод, «Абелевы многообразия», М., 1971.
229. Манин Ю. И., Кубические формы. Алгебра, геометрия, арифметика, М., 1972.
230. Маркус С. (Marcus S.), Algebraic linguistics; Analytical models, N. Y. — London, 1967; русский перевод, «Теоретико-множественные модели языков», М., 1970.
231. Мацумура Х. (Matsumura H.), Commutative algebra, N. Y., 1970.
232. Маэда Ф. и Маэда С. (Maeda F. and Maeda S.), Theory of symmetric lattices, Berlin — Heidelberg — N. Y., 1970.
233. Мендельсон Э. (Mendelson E.), Introduction to mathematical logic, Princeton (N. J.) — Toronto — N. Y. — London, 1963; русский перевод, «Введение в математическую логику», М., 1971.
234. Мерзляков Ю. И., Линейные группы, в сб. «Алгебра. Топология. Геометрия, 1970 (Итоги науки, ВИНИТИ АН СССР)», М., 1971, 75—110.
235*. Миллер Г., Бличфилд Х. и Диксон Л. (Miller G. A. Blichfeldt H. F. and Dickson L. E.), Theory and applications of finite groups, N. Y. — London, 1916; 2-е изд., 1938.
236*. Миллер К. (Miller K. S.), Elements of modern abstract algebra, N. Y., 1958.
237. Митчел Б. (Mitchell B.), Theory of categories, N. Y. — London, 1965.
238. Михалев А. В., Скорняков Л. А., Модули, в сб. «Алгебра. Топология. Геометрия. 1968 (Итоги науки, ВИНИТИ АН СССР)», М., 1970, 57—100.
239. Мишина А. П., Абелевы группы, в сб. «Алгебра. Топология. Геометрия. 1965 (Итоги науки, ВИНИТИ АН СССР)», М., 1967, 9—44.

240. Мишина А. П., Скорняков Л. А., Абелевы группы и модули, М., 1969.
241*. Моисил Г. К. (Moisil Gr. C.), Introducere in algebra, I, Inele şi ideale, т. 1, Bucureşti, 1954.
242*. Монтгомери Д. и Циппин Л. (Montgomery D. and Zippin L.), Topological transformation groups, N.Y. — London, 1955.
243*. Монтейро А. А. (Monteiro A. A.), Filtros e ideals, Rio de Janeiro, 1955.
244*. Моргадо Ж. (Morgado J.), Elementos de álgebra moderna: reticulados, sistemas parcialmente ordenados, т. I, Porto, 1956.
245* Мурнаган Ф. (Murnaghan F. D.), The theory of group representations, 1938; русский перевод, «Теория представлений групп», М., 1950.
246. Нагата М. (Nagata M.), Local rings, N. Y., 1962.
247. Наймарк М. А., Нормированные кольца, М., 1956.
248. Наймарк М. А., Линейные представления группы Лоренца, М., 1958.
249*. Накаяма Т. и Адзумая Г. (Nakayama T. and Azumaya G.), Doisûgaku II. Kanron (Алгебра. II. Теория колец, на японском яз.), Tokyo, 1954.
250. Нейкирх Ю. (Neukirch J.), Klassenkörpertheorie, Mannheim—Wien — Zürich, 1969.
251*. Нейман Дж. (Neumann J., von), Lectures on continuous geometries, в 2-х тт., Princeton, 1936, 1937.
252. Нейман Дж. (Neumann J., von), Continuous geometry, Princeton (N. J.), 1960.
253. Нейман Дж. (Neumann J., von), Collected works, vol. I (Logic theory of sets and quantum mechanics), vol. 2 (Operators, ergodic theory and almost periodic functions in a group), vol. 3 (Rings of operators), vol. 4 (Continuous geometry and other topics), vol. 5 (Design of computers, theory of automata and numerical analysis), vol. 6 (Theory of games, astrophysics, hydrodynamics and meteorology), Oxford — London — N. Y. — Paris, 1961—1963.
254. Нейман Х. (Neumann Hanna), Varieties of groups, Berlin — Heidelberg — N. Y., 1967; русский перевод, «Многообразия групп», М., 1969.
255. Новиков П. С., Алгоритмическая неразрешимость проблемы слов в теории групп, Труды Матем. ин-та им. Стеклова АН СССР **44**, 1955.
256. Новиков П. С., Элементы математической логики, М., 1959; 2-е изд., 1973.
257. Новиков П. С. и Адян С. И., О бесконечных периодических группах, Изв. АН СССР, серия матем., **32** (1968), 212—244, 251—524, 709—731.
258*. Норскотт Д. Г. (Northcott D. G.), Ideal theory, London, Cambridge, 1953.
259. Норскотт Д. Г. (Northcott D. G.), An introduction to homological algebra, London, Cambridge, 1960.
260*. Окунев Л. Я., Основы современной алгебры, М., 1941.
261. Оре О. (Ore O.), Theory of graphs, Providence (Rhode Island), 1962; русский перевод, «Теория графов», М., 1968.

262*. Осима, Теория групп (японск.), Кёрицу — Сюппан, 1954.
263. Парейгис Б. (Pareigis B.), Kategorien und Functoren, Stuttgart, 1969; английский перевод, «Categories and functors», N. Y. — London, 1970.
264. Паршин А. Н., Арифметика алгебраических многообразий, в сб. «Алгебра. Топология. Геометрия. 1970 (Итоги науки, ВИНИТИ, АН СССР)», М., 1971, 111—151.
265. Перрон О. (Perron O.), Die Lehre von den Kattenbrüchen, Leipzig — Berlin, 1913; 2-е, улучшенное изд., Leipzig — Berlin, 1929.
266. Перрон О. (Perron O.), Algebra, в 2-х тт., Berlin — Leipzig, 1927.
267*. Пикерт Г. (Pickert G.), Einführung in die höhere Algebra, Göttingen, 1951.
268*. Пикерт Г. (Pickert G.), Projektive Ebenen, Berlin — Göttingen — Heidelberg, 1955.
269. Пирс Р. (Pierce R. S.), Introduction to the theory of abstract algebras, N. Y., 1968.
270*. Плоткин Б. И., Обобщенные разрешимые и обобщенные нильпотентные группы, УМН **13**, № 4 (1958), 89—172.
271. Плоткин Б. И., Группы автоморфизмов алгебраических систем, М., 1966.
272. Плоткин Б. И., Общая теория групп, в сб. «Алгебра. Топология. Геометрия. 1970 (Итоги науки, ВИНИТИ АН СССР)», М., 1971, 5—73.
273*. Понтрягин Л. С., Непрерывные группы, М. — Л., 1938; 2-е изд., М., 1954; 3-е, исправленное изд., М., 1973; переводы: английский, Принстон, 1939; румынский (в 2-х тт.), Бухарест, 1956; немецкий, Лейпциг (в 2-х тт.), 1957, 1958; польский, Варшава, 1961.
274. Понтрягин Л. С., Основы комбинаторной топологии, М. — Л., 1947.
275. Попеску Н. (Popescu N.), Categorii abeliene, Bucureşti, 1971.
276. Попеску Н. и Раду А. (Popescu N. and Radu A.), Theoria categoriilor şi a fascicúlelor, Bucureşti, 1971.
277*. Постников М. М., Определенные семейства функций и алгебры без делителей нуля над полем действительных чисел, УМН **9**, № 2 (1954), 67—104.
278*. Постников М. М., Основы теории Галуа, М., 1960.
279. Пуанкаре А. (Poincaré H.), Quelques remarques sur les groupes finis et continus, Oeuvres complètes, III, Paris, 1954.
280. Пуату Г. и Жаффар П. (Poitou G. et Jaffard P.), Introduction à la théorie des catégories, Paris, 1965.
281. Пуппе Д. (Puppe D.), Korrespondenzen in Abelschen Kategorien, Math. Ann. **148**, № 1 (1962), 1—30; русский перевод, «Соответствия в абелевых категориях», сб. «Математика» **8**, № 6 (1964), 109—139.
282*. Редеи Л. (Rédei L.), Algebra; v. I, Budapest, 1954; немецкий, переработанный перевод, Leipzig, 1959.
283. Редеи Л. (Rédei L.), Theorie der endlich erzeugbaren kommutativen Halbgruppen, Leipzig, 1963.

284. Резерфорд Д. (Rutherford D.), Introduction to lattice theory, Edinburg — London, 1965.
285*. Рейдемейстер К. (Reidemeister K.), Einführung in die kombinatorische Topologie, Braunschweig, 1932.
286. Рибенбойм П. (Ribenboim P.), Théorie des groupes ordonnés, Bahia Blanca, 1963.
287. Рибенбойм П. (Ribenboim P.), Rings and modules, N. Y. — London — Sydney — Toronto, 1969.
288. Ригер Л. (Rieger L.), Algebraic methods of mathematical logic (перевод с чешского), N. Y. — London, 1967.
289. Рикарт Ч. (Rickart Ch. E.), General theory of Banach algebras, Princeton (N. J.) — Toronto — N. Y. — London, 1960.
290*. Ритт Дж. Ф. (Ritt J. F.), Differential equations from the algebraic standpoint, N. Y., 1932; 2-е изд., 1947.
291*. Ритт Дж. Ф. (Ritt J. F.), Differential algebra, N. Y., 1950.
292. Робертсон А. П. и Робертсон В. Дж. (Robertson A. P. and Robertson W. J.), Topological vector spaces, Cambridge, 1964; русский перевод, «Топологические векторные пространства», М., 1967.
293. Робинсон А. (Robinson A.), On the metamathematics of algebra, Amsterdam, 1951.
294. Робинсон А. (Robinson A.), Introduction to model theory and to the metamathematics of algebra, Amsterdam, 1963; русский перевод, «Введение в теорию моделей и метаматематику алгебры», М., 1967.
295. Робинсон Г. (Robinson G. de B.), Representation theory of the symmetric group, Toronto, 1961.
296. Ротман Дж. Дж. (Rotman J. J.), The theory of groups; an introduction, Boston, 1965.
297. Са Чин-хан (San Chin-han), Abstract algebra, N. Y., 1967.
298. Садовский Л. Е., Некоторые теоретико-структурные вопросы теории групп, УМН **23**, № 3 (1968), 123—157.
299*. Самуэль П. (Samuel P.), Algèbre locale, Paris, 1953.
300. Самуэль П. (Samuel P.), Méthodes d'algèbre abstraite en géométrie algébrique, Berlin — Göttingen — Heidelberg, 1955.
301. Сас Г. (Szász G.), Bevezetés a hálóelméletbe, Budapest, 1959; немецкий перевод, «Einführung in die Verbandstheorie», Budapest, 1962; французский, пополненный перевод, «Théorie des treillis», Budapest, 1971.
302*. Сато С., Теория групп (на японском); китайский перевод, Шанхай, 1934.
303. Сегье Ж. А., де (Séguier J. A., de), Théorie des groupes finis, v. 1, Éléments de la théorie des groupes abstraits, Paris, 1904.
304. Сегье Ж. А., де (Séguier J. A., de), Éléments de la théorie des groupes de substitutions, Paris, 1912.
305. Сегье Ж. А., де, и Потрон М. (Séguier J. A., de, et Potron M.), Théorie de groupes abstraits, Paris, 1938.
306. Семадени З. и Вивегер А. (Semadeni Z., Wiweger A.), Wstęp do teorii kategorii i functorow, Warszawa, 1972.
307. Семинар «Софус Ли» (Séminaire «Sophus Lie»), Théorie des algèbres de Lie. — Topologie des groupes de Lie, Paris, 1955; русский перевод, «Теория алгебр Ли. — Топология групп Ли», М., 1962.

308. Серр Ж.-П. (Serre J.-P.), Corps locaux, Paris, 1962; 2-е, исправленное изд, Paris, 1968.
309. Серр Ж.-П. (Serre J.-P.), Lie algebras and Lie groups; N. Y. — Amsterdam, 1965; русский перевод, «Алгебры Ли и группы Ли», М., 1969.
310. Серр Ж.-П. (Serre J.-P.), Algebres de Lie semi-simples complexes, N. Y. — Amsterdam, 1966; русский перевод, «Комплексные полупростые алгебры Ли» (помещен в качестве 3-й части в переводе книги [309]).
311. Серр Ж.-П. (Serre J.-P.), Représentations linéaires des groupes finis, Paris, 1967; 2-е, переработанное изд., 1971; русский перевод, «Линейные представления конечных групп», М., 1970.
312. Серр Ж.-П. (Serre J.-P.), Abelian l-adic representations and elliptic curves, N. Y., 1968.
313. Серр Ж.-П. (Serre J.-P.), Cours d'arithmétique, Paris, 1970; русский перевод, «Курс арифметики», М., 1972.
314. Сикорский Р. (Sikorski R.), Boolean algebras, Berlin — Göttingen — Heidelberg — N. Y., 1960; 2-е изд., 1964; русский перевод, «Булевы алгебры», М., 1969.
315. Сколем Т. (Skolem T.), Zur Theorie der associativen Zahlensysteme, Oslo, 1927.
316*. Скорняков Л. А., Проективные плоскости, УМН **6**, № 6 (1951), 112—154; английский перевод, 1953.
317. Скорняков Л. А., Дедекиндовы структуры с дополнениями и регулярные кольца, М., 1961.
318. Скорняков Л. А., Кольца, в сб. «Алгебра. Топология. 1962 (Итоги науки, ВИНИТИ АН СССР)», М., 1963, 59—79.
319. Скорняков Л. А., Модули, в сб. «Алгебра. Топология. 1962 (Итоги науки, ВИНИТИ АН СССР)», М., 1963, 80—89.
320. Скорняков Л. А., Теория структур, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», 1966, 237—274.
321. Скорняков Л. А., Модули, в сб. «Алгебра. Топология. Геометрия. 1965 (Итоги науки, ВИНИТИ АН СССР)», М., 1967.
322. Скорняков Л. А., Элементы теории структур, М., 1970.
323. Скорца Г. (Scorza G.), Corpi numericie algebre, Messina, 1921.
324*. Скорца Г. (Scorza G.), Gruppi astratti, Roma, 1942.
325. Скотт В. Р. (Scott W. R.), Group theory, Englewood Cliffs (N. Y.), 1964.
326. Спеньер Э. (Spanier E.), Algebraic topology, N. Y. — London, 1966; русский перевод, «Алгебраическая топология», М., 1971.
327. Стинрод Н. и Эйленберг С. (Eilenberg S. and Steenrod N.), Foundations of algebraic topology, Princeton (N. J.) 1952; русский перевод, «Основания алгебраической топологии», М., 1958.
328*. Судзуки М. (Suzuki M.), Structure of a group and the structure of its lattice of subgroups, Berlin — Göttingen — Heidelberg, 1956; русский перевод, «Строение группы и строение структуры ее подгрупп», М., 1960.
329. Супруненко Д. А., Разрешимые и нильпотентные линейные группы, Минск, 1958.
330. Супруненко Д. А., Группы матриц, М., 1972.

331. Супруненко Д. А. и Тышкевич Р. И., Перестановочные матрицы, Минск, 1966.
332*. Сушкевич А. К., Теория обобщенных групп, Харьков — Киев, 1937.
333*. Таннака Т., Принцип двойственности (на японском), Токио, 1951.
334 Уайтхед А. Н. (Whitehead A. N.), A treatise on universal algebra, with application, I, Cambridge, 1898; перепечатка, N. Y., 1960.
335. Уокер Р. (Walker R. J.), Algebraic curves, Princeton (N. J.), 1950; русский перевод, «Алгебраические кривые», М., 1952.
336. Фейт В. (Feit W.), Characters of finite groups, N. Y. — Amsterdam, 1967.
337. Фейт В. и Томпсон Дж. (Feit W. and Thompson J. G.), Solvability of groups of odd order, Pacif. J. Math. **13**, № 3 (1963), 775—1029.
338. Феферман С. (Feferman S.), The number systems. Foundations of algebra and analysis, Palo Alto — London, 1963; русский перевод, «Числовые системы. Основания алгебры и анализа», М., 1971.
339. Фиреге Х. (Viereggе H.), Einführung in die Klassische Algebra, Berlin, 1972.
340. Форэ Р. и Хёргон Е. (Faure R. and Heurgon E.), Structures ordonées et algèbres de Boole, Paris, 1971.
341. Фрейд П. (Freyd P.), Abelian categories: An introduction to the theory of functors, N. Y., 1964.
342. Френкель А. (Fraenkel A. A.), Mengenlehre und Logic, Berlin, 1959.
343. Френкель А. и Бар-Хиллел И. (Fraenkel A. A. and Bar-Hillel Y.), Foundations of set theory, Amsterdam, 1958; русский перевод, «Основания теории множеств», М., 1966.
344. Фробениус Ф. Г. (Frobenius F. G.), Теория характеров и представлений групп (сборник переводов с немецкого 9 работ Фробениуса), Харьков, 1937.
345. Фробениус Ф. Г. (Frobenius F. G.), Gesammelte Abhandlungen, herausgegeben von J.-P. Serre, в 3-х тт., Berlin — Heidelberg — N. Y., 1968.
346*. Фукс Л. (Fuchs L.), Abelian groups, Budapest, 1958; перепечатка, Oxford — London — N. Y. — Paris, 1960.
347. Фукс Л. (Fuchs L.), Partially ordered algebraic systems, Oxford — London — N. Y. — Paris, 1963; русский перевод, «Частично упорядоченные алгебраические системы», М., 1965.
348. Фукс Л. (Fuchs L.), Infinite Abelian groups, v. 1, N. Y. — London, 1970; русский перевод, «Бесконечные абелевы группы», М., 1973.
349. Халмош П. Р. (Halmos P. R.), Algebraic logic, N. Y., 1962.
350. Халмош П. Р. (Halmos P. R.), Lectures on Boolean algebras, Toronto — N. Y. — London, 1963.
351. Хассе М. и Михлер Л. (Hasse M. und Michler L.), Theorie der Kategorien, Berlin, 1966.
352. Хассе Х. (Hasse Helmut), Höhere Algebra, vv. 1, 2, Berlin — Leipzig, 1926, 1927.

353*. Хаупт О. (Haupt O.), Einführung in die Algebra, в 2-х тт. Leipzig, 1929; 2-е изд., Leipzig, 1952; 3-е изд., Leipzig, 1956.
354. Хаусдорф Ф. (Hausdorff F.), Grundzüge der Mengenlehre, Leipzig, 1914; 2-е, переработанное изд., «Mengenlehre», Berlin — Leipzig, 1927; русский перевод, «Теория множеств», М. — Л., 1937.
355. Хаусснер М. и Шварц Дж. Т. (Hausner M. and Schwartz J. T.), Lie groups; Lie algebras, N. Y., 1968.
356. Хейне В. (Heine V.), Group theory in quantum mechanics, London — Oxford — N. Y. — Paris, 1960; русский перевод, «Теория групп в квантовой механике», М., 1963.
357*. Хермес Х. (Hermes H.), Einführung in die Verbandstheorie, Berlin — Göttingen — Heidelberg, 1955; 2-е изд., Berlin — Heidelberg — N. Y., 1967.
358. Херстейн И. Н. (Herstein I. N.), Topics in algebra, N. Y. — Toronto — London, 1964.
359. Херстейн И. Н. (Herstein I. N.), Noncommutative rings, N. Y., 1968.
360. Хилл Э. (Hill E.), Functional analysis and semi-groups, N. Y., 1948; русский перевод, «Функциональный анализ и полугруппы», М., 1951.
361. Хилл Э. и Филлипс Р. (Hille E. and Phillips R.), Functional analysis and semi-groups, Providence, 1957.
362. Хилтон П. и Уайли С. (Hilton P. J. and Wylie S.), Homology theory: an introduction to algebraic topology, Cambridge, London, 1960; русский перевод, «Теория гомологий: введение в алгебраическую топологию», М., 1966.
363. Хилтон П. и Штэмбах У. (Hilton P. J. and Stammbach U.), A course in homological algebra, N. Y. — Berlin — Heidelberg, 1971.
364. Хилтон Х. (Hilton H.), An introduction to the theory of groups of finite order, Oxford, 1908.
365. Ходж В. и Пидо Д. (Hodge W.V.D. and Pedoe D.), Methods of algebraic geometry, в 3-х тт., Cambridge, 1947, 1952, 1954; русский перевод, «Методы алгебраической геометрии», в 3-х тт., М., 1954—1955.
366*. Холл М. (Hall M.), Projective planes and related topics, Calif. Inst. of technol., 1954.
367. Холл М. (Hall M.), The theory of groups, N. Y., 1959; русский перевод, «Теория групп», М., 1962.
368. Холл М. (Hall M.), Combinatorial theory, Waltham (Mass.) — Toronto — London, 1967; русский перевод, «Комбинаторика», М., 1970.
369. Холл М. и Сеньор Дж. К. (Hall M. and Senior J. K.), The groups of order 2^n ($n \leqslant 6$), N. Y. — London, 1964.
370. Холл Ф. М. (Hall F. M.), An introduction to abstract algebras, в 2-х тт. Cambridge (London), 1966, 1969; 2-е изд., 1972.
371. Хольцер Л. (Holzer L.), Klassenkörpertheorie, Leipzig, 1966.
372. Ху С. Т. (Hu S. T.), Introduction to homological algebra, San Francisco, 1968.
373. Хупперт Б. (Huppert B.), Endliche Gruppen, I, Berlin — Heidelberg — N. Y., 1967.

374. Цаленко М. Ш., К основам теории категорий, УМН **15**, № 6 (1960), 53—58; немецкий перевод — в книге [187′].
375. Цаленко М. Ш. и Шульгейфер Е. Г., Категории, в сб. «Алгебра. Топология. Геометрия. 1967 (Итоги науки, ВИНИТИ АН СССР)» М., 1969, 9—57.
376. Цаленко М. Ш. и Шульгейфер Е. Г., Лекции по теории категорий, МГУ, М., 1970.
377*. Цаппа Г. (Zappa G.), Gruppi, corpi, equazioni; 2-е изд., Napoli, 1954.
378. Цаппа Г. (Zappa G.), Fondamenti di teoria dei gruppi, в 2-х тт., Roma, 1965, 1970.
379*. Цассенхауз Г. (Zassenhaus H.), Lehrbuch der Gruppentheorie, Bd. I, Leipzig — Berlin, 1937; 2-е изд., «The theory of groups», Göttingen, 1956; перепечатка, N. Y., 1958.
380. Чарин В. С., Топологические группы, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», М., 1966, 123—160.
381*. Чеботарев Н. Г., Основы теории Галуа, в 2-х тт., Л. — М., 1934—1937; немецкий перевод, Гронинген, 1950.
382*. Чеботарев Н. Г., Теория Галуа, М. — Л., 1936.
383. Чеботарев Н. Г., Теория групп Ли, М. — Л., 1940.
384. Чеботарев Н. Г., Теория алгебраических функций, М. — Л., 1948.
385*. Чеботарев Н. Г., Введение в теорию алгебр, М. — Л., 1949; китайский перевод, Пекин, 1954.
386. Чеботарев Н. Г., Собрание сочинений, в 3-х тт., М. — Л., 1949—1950.
387. Чейз С. и Свидлер М. (Chase S. U. and Sweedler M. E.), Hopf algebras and Galois theory, Berlin, 1969.
388*. Черников С. Н., Условия конечности в общей теории групп, УМН **14**, № 5 (1959), 45—96.
389. Черников С. Н., Линейные неравенства, М., 1968.
390. Черников С. Н., Линейные неравенства, в сб. «Алгебра. Топология. Геометрия. 1966 (Итоги науки, ВИНИТИ АН СССР)», М., 1968, 137—187.
391. Черников С. Н., О группах с ограничениями для подгрупп, в сб. «Группы с ограничениями для подгрупп», Киев, 1971.
392. Чёрч А. (Church A.), Introduction to mathematical logic, I., Princeton (N. J.), 1956; русский перевод, «Введение в математическую логику, I», М., 1960.
393*. Чжан Хо-жуй, Основы современной алгебры (на китайском), Шанхай, 1952.
394. Чунихин С. А., Подгруппы конечных групп, Минск, 1964.
395. Чунихин С. А. и Шеметков Л. А., Конечные группы, в сб. «Алгебра. Топология. Геометрия, 1969 (Итоги науки, ВИНИТИ АН СССР)», М., 1971, 7—70.
396. Шатле А. (Chatelet A.), Les groupes abéliens finis et les modules de points entière, Paris — Lille, 1925.
397*. Шатле А. (Chatelet A.), Arithmétique et algèbre modernes, vol. 1 (Notions fondamentales, groupes), Paris, 1954; vol. 2 (Anneaux et corps, calcul algébrique, idéaux et divisibilité), Paris, 1956.
398. Шафаревич И. Р., Основы алгебраической геометрии, М., 1972.

399. Шафер Р. (Schafer R. D.), An introduction to nonassociative algebras, N. Y. — London, 1966.
400. Шевалле К. (Chevalley C.), Theory of Lie groups, vol. 1, Princeton, 1946; русский перевод, «Теория групп Ли», М., 1948.
401. Шевалле К. (Chevalley C.), Introduction to the theory of algebraic functions of one variable, N. Y., 1951; русский перевод, «Введение в теорию алгебраических функций от одной переменной», М., 1959.
402. Шевалле К. (Chevalley C.), Théorie des groupes de Lie, vol. 2, Groupes algébriques, Paris, 1951; русский перевод, «Теория групп Ли, т. 2, Алгебраические группы», М., 1958.
403*. Шевалле К. (Chevalley C.), Théorie des groupes de Lie, vol. 3, Théorèmes généraux sur les algèbres de Lie, Paris, 1955; русский перевод, «Теория групп Ли, т. 3, Общая теория алгебр Ли», М., 1958.
404*. Шевалле К. (Chevalley C.), Fundamental concepts of algebra, N. Y., 1956; допечатка, N. Y., 1965.
405. Шенкман Е. (Schenkman E.), Group theory, Toronto — N. Y. — London, 1965.
406*. Шиллинг О. (Schilling O. F. G.), The theory of valuations, N. Y., 1950.
407*. Ширшов А. И., Некоторые вопросы теории колец, близких к ассоциативным, УМН **13**, № 6 (1958), 3—20.
408. Шмелькин А. Л., Абстрактная теория бесконечных групп, в сб. «Алгебра. 1964 (Итоги науки, ВИНИТИ АН СССР)», М., 1966, 47—82.
409*. Шмидт О. Ю., Абстрактная теория групп, Киев, 1916; 2-е изд., М. — Л., 1933 (см. также в [410]).
410. Шмидт О. Ю., Избранные труды. Математика, М., 1959.
411. Шмидт Э. Т. (Schmidt E. T.), Kongruenzrelationen algebraischer Structuren, Berlin, 1969.
412*. Шода К., Общая алгебра (на японском), Токио, 1947.
413. Шпайзер А. (Speiser A.), Die Theorie der Gruppen von endlicher Ordnung, Berlin, 1923; 2-е изд., Berlin, 1927; 3-е изд., Berlin, 1937; 4-е, дополненное и исправленное изд., Basel — Stuttgart, 1956; английский перевод, 1945.
414*. Шпехт В. (Specht W.), Gruppentheorie, Berlin — Göttingen — Heidelberg, 1956.
415. Штейнштрём Б. (Stenström B.), Rings and modules of quotients, Berlin — Heidelberg — N. Y., 1971.
416. Шуберт Х. (Schubert H.), Kategorien, в 2-х тт., Berlin — Heidelberg — N. Y., 1970.
417. Энглефилд М. (Englefield M. J.), Group theory and the Coulomb problem, N. Y., 1972.
418*. Эндрю Р. В. (Andree R. V.), Selections from modern abstract algebra, N. Y., 1958.
419. Эресман Ш. (Ehresmann Ch.), Catégories et structures, Paris, 1965.
420. Эресман Ш. (Ehresmann Ch.), Algèbre, part 1, Paris, 1968.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Александр Геннадиевич Курош

ЛЕКЦИИ ПО ОБЩЕЙ АЛГЕБРЕ

М., 1973 г., 400 стр. с илл.

Редакторы *О. Н. Головин, Ф. И. Кизнер*

Техн. редактор *Е. Н. Земская*

Корректоры *З. В. Автонеева, А. Л. Ипатова*

Сдано в набор 23/III 1973 г. Подписано к печати 26/VII 1973 г. Бумага 84×108$^{1}/_{32}$, тип. № 1. Физ. печ. л. 12,5. Условн. печ. л. 21. Уч.-изд. л. 20,93. Тираж 30 000 экз. Т-11158. Цена книги 1 р. 62 к. Заказ № 778.

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

Ордена Трудового Красного Знамени Ленинградская типография № 1 «Печатный Двор» имени А. М. Горького Союзполиграфпрома при Государственном комитете Совета Министров СССР по делам издательств, полиграфии и книжной торговли. Ленинград, Гатчинская ул., 26.