П.Кон

УНИВЕРСАЛЬНАЯ АЛГЕБРА

ИЗДАТЕЛЬСТВО «МИР» Москва 1968

Книга известного английского математика профессора Лондонского университета П. Кона — первая в мировой литературе монография, специально посвященная теории универсальных алгебр. Это новое направление общей алгебры развивается сейчас очень бурно и оказывает существенное влияние на другие ее разделы.

Блестяще написанная книга, несомненно, заинтересует не только всех алгебраистов, но и представителей других областей математики. Она будет полезна преподавателям, аспирантам и студентам университетов и педвузов.

ОГЛАВЛЕНИЕ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Началом теории универсальных алгебр, если не говорить об ее предыстории, следует считать работы Г. Биркгофа, опубликованные в первой половине тридцатых годов. Эти работы были замечены алгебраистами, но некоторое время не вызывали откликов и продолжений — общая алгебра в те годы еще далеко не достигла той широты, которая характерна для нее в настоящее время, и задача унифицированного изложения основ различных ветвей общей алгебры еще не представлялась очень актуальной. С другой стороны, само понятие универсальной алгебры, т. е. множества, в котором задана произвольная система алгебраических операций, каждая от произвольного конечного числа аргументов, казалось слишком широким и потому слишком бедным содержанием для того, чтобы стать объектом самостоятельной теории.

Оживление в этой области началось во второй половине сороковых годов — назовем работы Тарского и Шода, причем последний опубликовал на японском языке книгу, посвященную теории универсальных алгебр с бинарными операциями. В первой половине пятидесятых годов начал свои исследования по универсальным алгебрам А. И. Мальцев. К настоящему времени уже накопилась столь большая литература, посвященная универсальным алгебрам, что теперь с полным правом можно говорить о появлении нового раздела общей алгебры.

Задачи этого раздела не исчерпываются объединением основ различных «классических» ветвей алгебры, как это можно было бы заключить из первого абзаца предисловия автора к настоящей книге. Теория универсальных алгебр — это самостоятельная наука со своей собственной проблематикой и своими методами, так что понятие универсальной алгебры при всей его широте оказалось и пригодным для разностороннего изучения, и заслуживающим такого изучения. Вместе с тем теория универсальных алгебр все чаще оказывает существенное влияние на развитие других разделов алгебры.

Конечно, появление этой новой алгебраической науки не означает ликвидации или принижения тех разделов алгебры, которые посвящены изучению отдельных специальных типов универсальных алгебр, таких, как группы, кольца, структуры, полугруппы и т. д. Для сравнения заметим, например, что появление теории полугрупп не означало ликвидации или обеднения теории групп, хотя группа является частным случаем полугруппы, а появление теории колец не означало отмены теории полей, хотя поле есть частный случай кольца.

Книги, посвященные современной теории универсальных алгебр во всей ее широте, в печати пока не появились, хотя это, несомненно, не за горами. Основы теории изложены в одной из глав книги автора этих строк «Лекции по общей алгебре» (1962 г.). Им же посвящена книга известного алгебраиста, профессора Лондонского университета П. М. Кона, перевод которой предлагается сейчас вниманию читателя.

Эта книга представляет собой весьма яркое явление в современной алгебраической литературе. Основы теории универсальных алгебр излагаются в ней с большой широтой и на весьма высоком научном уровне. Отметим хотя бы, что автор систематически рассматривает категории универсальных алгебр — тесная связь теории универсальных алгебр с теорией неабелевых категорий является реальностью современной алгебраической науки. Автор включил также в книгу две главы, относящиеся к теории моделей — это молодая наука, пограничная между общей алгеброй и математической логикой и изучающая множества, в которых заданы некоторые системы конечноместных отношений (а не только операций, как в универсальных алгебрах). Что же касается последней, седьмой главы «Приложения», то отбор материала в ней полностью отражает личные научные интересы автора — она почти целиком относится к теории колец, хотя ясно, что в других разделах общей алгебры можно было бы найти не меньше различных приложений.

Несомненно, что появление этой книги будет весьма содействовать общему повышению уровня алгебраической культуры. Ее с пользой для себя прочтет каждый алгебраист, в каком бы специальном разделе общей алгебры он ни работал. Думаю, что эту книгу следует включать в планы аспирантских экзаменов для любого аспиранта по общей алгебре, какова бы ни была его узкая специальность.

Написана книга в общем прозрачно. Лишь немногие места покажутся читателю более трудными, в том числе, к сожалению, § III.1 об универсальных функторах, играющий в книге фундаментальную роль. Автор требует от читателя некоторой алгебраической подготовки. Для необходимых справок читатель может воспользоваться хотя бы упомянутыми выше «Лекциями по общей алгебре», в настоящей книге неоднократно цитируемыми.

Немногочисленные примечания редактора перевода ни в коей мере не имеют целью дать читателю полное представление о сегодняшнем состоянии теории универсальных алгебр и о разнообразии путей, по которым ведутся в ней исследования, — этой цели не ставил перед собой и автор книги, и она не могла бы быть достигнута при помощи примечаний. По этой же причине в библиографию при переводе не внесено никаких добавлений. При подготовке примечаний я существенно использовал советы как переводчицы Т. М. Баранович, так и других математиков. Приношу им всем мою искреннюю благодарность.

Автор книги по моей просьбе любезно прислал два списка опечаток, исправлений и добавлений. Все замечания автора учтены при работе над переводом.

Москва, октябрь 1967 г. *А. Г. Курош*

ПРЕДИСЛОВИЕ

Универсальная алгебра занимается изучением черт, общих для привычных алгебраических систем, таких, как группы, кольца, структуры и т. д.; при этом определяется настоящее место алгебраических понятий и часто обнаруживаются связи между на первый взгляд различными понятиями, что помогает систематизации результатов. Идеи, содержащиеся здесь, на самом деле очень просты и возникают при естественном обобщении нескольких частных случаев. Однако нужно помнить, что этот подход обычно не дает решения всей проблемы, а только избавляет от тривиальных деталей, давая возможность сконцентрировать силы на сути данной проблемы.

Цель этой книги состоит в том, чтобы дать простое изложение основных результатов универсальной алгебры. Книга не претендует на исчерпывающую полноту и даже на максимум общности там, где это привело бы к потере прозрачности изложения. Включенного в нее подготовительного материала достаточно для того, чтобы сделать текст доступным студентам старших курсов университетов, владеющим основами теории групп и колец и основными понятиями топологии (для чтения главы V). Только заключительный параграф книги (§ VII.7) требует несколько большего знакомства с теорией представлений.

Изложение концентрируется вокруг понятия алгебраической структуры, которое, грубо говоря, определяется как множество с конечноместными операциями. Тот факт, что операции конечноместны, можно считать характерной чертой алгебры, и его следствия можно обнаружить в главе II. Те, даже более фундаментальные, следствия из наличия операций, которые не зависят от их конечноместности, рассматриваются отдельно в главе I. Эта глава содержит также необходимые сведения из теории множеств, которые излагаются с точки зрения алгебраиста.

Одним из основных средств при изучении произвольных алгебр является понятие *свободной алгебры*. Оно особенно важно для таких классов, как группы и кольца, которые полностью определяются тождествами, — т. е. *для многообразий* алгебр, — и это, возможно, затемняет тот факт, что свободные алгебры существуют во многих классах алгебр, не являющихся многообразиями. Чтобы подчеркнуть это обстоятельство, в главе III свободные алгебры исследуются, насколько возможно, вне связи с многообразиями, тогда как свойства, присущие исключительно многообразиям, рассматриваются отдельно в главе IV.

Две упомянутые главы представляют собой единственные точки соприкосновения книги с гомологической алгеброй, и, вероятно, нужно сказать несколько слов об этой связи. Центральной частью гомологической алгебры является теория абелевых категорий; эта теория глубоко развита, но она слишком узка для наших целей. Общая теория категорий, хотя и находится на более ранней стадии развития, имеет в своем распоряжении достаточно средств для получения основных теорем о существовании свободных алгебр, но в исследованиях, посвященных исключительно алгебре, эти результаты гораздо проще доказываются непосредственно. В частности, предположения, при которых здесь получаются эти теоремы, легче проверяются (в случае алгебр), чем соответствующие предположения, найденные в общей теории категорий. Поэтому из теории категорий мы мало заимствовали сверх определений категории и функтора. Эти определения, безусловно, необходимы в любом удовлетворительном изложении теории свободных алгебр, и они дают возможность кратко формулировать результаты, не уводя слишком далеко от главной темы.

Понятие алгебраической структуры в той форме, как оно определено в главе II, слишком узко даже для многих алгебраических рассмотрений, и его нужно заменить понятием *структуры с отношениями* (т. е. множества с набором определенных на нем конечноместных отношений). Кроме самих алгебраических структур, это понятие включает структуры с многозначными или не всюду определенными операциями. В настоящее время структуры с отношениями, удовлетворяющие данной системе аксиом, — или *модели* — являются предметом интенсивного изучения, и здесь получены результаты удивительной силы и красоты. Развитый в книге аппарат универсальной алгебры предоставил нам прекрасную возможность дать хотя бы короткое введение в теорию моделей, что и сделано в главах V и VI.

Материал для заключительной главы о приложениях отобран без какой бы то ни было системы. Сюда включены результаты, которые можно получить на основе предыдущих глав и которые иллюстрируют общую теорию, а также важны для других областей (таких, как построение натуральных чисел в § VII.1 или теория представлений лиевых и йордановых алгебр в §§ VII.5—7) или интересны сами по себе (например, теорема Мальцева о вложимости полугрупп, § VII.3).

Хотя возникновение предмета этой книги можно отнести к прошлому веку (трактат А. Н. Уайтхеда с тем же самым названием появился в 1898 г.), универсальная алгебра, как ее понимают теперь, начинает развиваться только с 30-х годов. Она появилась как естественное развитие абстрактного подхода к алгебре, идущего от Эмми Нётер. По универсальной алгебре (как и другим областям математики) публикуется большое и притом из года в год растущее число статей, но удивительно, что большая часть этой теории все еще остается фольклором. Автору посчастливилось познакомиться с этим фольклором на чрезвычайно ярких и стимулирующих лекциях профессора Филиппа Холла в Кэмбридже в 1947—1951 гг. Они оказали на книгу много большее влияние, чем можно судить по этому упоминанию. С другой стороны, при ссылках автор часто отдает предпочтение более доступным работам, а не первоисточникам и при этом не предпринимает никаких попыток включить замечания исторического характера. Хотя такая попытка была бы, конечно, очень ценной для данной книги, она задержала бы ее опубликование. По этой же причине библиография содержит помимо статей, непосредственно связанных с текстом, только небольшой подбор работ по универсальной алгебре. Автор позволил себе это, поскольку очень полную библиографию можно найти в Mathematical Reviews; кроме того, большая библиография по универсальной алгебре подготовлена Гретцером.

Книга основана на курсе лекций, прочитанных мною в Йельском университете в 1961/62 учебном году. Я благодарен аудитории, состоявшей из таких хороших слушателей, а также многим друзьям, оказывавшим мне услуги при создании книги. В частности, Д. Коэн и Хиггинс прочли некоторые части рукописи и сделали много полезных предложений; Макдональд помогал при чтении корректур; Баутел и Линтон проверили весь текст и обратили мое внимание на ряд неточностей. Всем им я хотел бы выразить мою горячую благодарность. Я благодарен также издательству Харпер и Роу, которое охотно шло навстречу моим пожеланиям, и редактору, мистеру Кронквисту, за его помощь при подготовке рукописи к печати.

Лондон, январь 1965 *П. М. Кон*

ЗАМЕЧАНИЯ

Центральной частью книги является глава II, и ее можно читать сразу после § 1.3, возвращаясь, если нужно, к другим частям главы I. Бóльшую часть глав V и VI можно читать после главы II, и бóльшую часть главы VII можно читать после главы IV. Все исключения из этих правил обычно указываются ссылками на соответствующую главу и параграф.

Теоремы, предложения и леммы снабжены сквозной нумерацией; так, «теорема IV.3.5» означает результат номер 5 из § 3 главы IV. В ссылках внутри одной главы римские цифры опускаются. Конец доказательства отмечается символом ▮.

В библиографию включено помимо работ, на которые есть ссылки в тексте, несколько представляющих интерес статей относительно универсальной алгебры, однако библиография никоим образом не претендует на полноту. Практически все статьи, внесенные в список, появились после 1900 г., и при ссылках на них мы указываем фамилию автора, а в квадратных скобках помещаем две последние цифры года публикации статьи; статьи, опубликованные в один и тот же год, снабжаются штрихами.

ГЛАВА I

МНОЖЕСТВА И ОТОБРАЖЕНИЯ

1. АКСИОМЫ ТЕОРИИ МНОЖЕСТВ

Характерной чертой всякой математической теории является то, что она имеет дело с совокупностями или множествами объектов, причем между объектами этих множеств или между самими множествами существуют некоторые соотношения, в то время как природа самих объектов совершенно несущественна. Рассматривая только те объекты, которые сами являются множествами, можно достичь некоторого упрощения. На первый взгляд кажется, что это приводит к порочному кругу, но трудности могут быть преодолены, если начинать с пустого множества. С другой стороны, необходимо описать те множества, которые могут быть членами других множеств, если мы хотим избежать противоречий, возникающих из рассмотрения «множества всех тех множеств, которые не являются членами самих себя» (парадокс Рассела). Введем поэтому термин «класс» для произвольных совокупностей объектов и будем отличать те классы, которые являются членами других классов, называя их *множествами.* Не вдаваясь в детали аксиоматики (отсылаем читателя для более подробного ознакомления к таким работам, как Бурбаки [54], Гёдель [40], Келли [55], Ван Хао и Макнотон [53]), перечислим аксиомы, выражающие главным образом те условия, при которых класс следует рассматривать как множество.

Говоря формально, теория множеств имеет дело с объектами, называемыми *классами*, для которых определено бинарное отношение

$$A \in B \tag{1}$$

(читается так: «A есть член (или элемент) B» или «A принадлежит B»). Определим *множество* как класс, являющийся элементом некоторого класса. Таким образом, A есть множество тогда и только тогда, когда A находится в отношении (1) с некоторым классом B. Для выражения отрицания отношения (1) мы будем писать так: $A \notin B$. Классы мы будем обозначать прописными буквами, но те классы, которые в данном контексте появляются как элементы других классов, часто будем обозначать строчными буквами.

Обычно два объекта считаются равными, если они имеют одни и те же свойства, т. е. если одни и те же утверждения справедливы для них обоих. В теории множеств удобнее сузить определение равенства и добавить аксиому, ограничивающую на самом деле те утверждения, которые можно получить в этой теории.

Определение. Два класса A и B называются *равными*, $A=B$, если они имеют одни и те же элементы. Отрицание утверждения $A=B$ записывается в виде $A \neq B$.

Чтобы получить обычную интерпретацию равенства, добавим теперь следующую аксиому:

А. 1. Если $A=B$ и $P(X)$ — некоторое высказывание о классах [1]), то $P(A)$ истинно тогда и только тогда, когда истинно $P(B)$.

Например, если $A=B$, то $A \in C$ в том и только том случае, если $B \in C$. Аксиому А. 1 можно рассматривать как ограничение характера утверждений, которые мы хотим обсуждать. Например, в силу приведенного выше определения равенства класс двуногих, не имеющих оперения, равен классу людей (Рассел), но всякое рассуждение о том, является ли двуногий, не имеющий оперения, более способным развить оперение, чем человек, находится вне сферы теории множеств, так как по аксиоме А. 1 нам не разрешается различать эти два описания.

Чтобы иметь согласующуюся с нашими интуитивными представлениями теорию для каждого утверждения, имеющего смысл в этой теории и содержащего переменное X, нам необходим класс, членами которого являются те и только те множества X, для которых это утверждение справедливо, т. е. имеет место аксиома:

А. 2. Если $P(X)$ — некоторое высказывание о классах [1]), то существует класс, членами которого являются те и только те множества X, для которых $P(X)$ истинно.

Класс, определенный в А. 2, обозначается $\{X \mid P(X)\}$, так что для каждого множества A

$$A \in \{X \mid P(X)\} \text{ тогда и только тогда, когда } P(A) \text{ истинно.}$$

Заметим, что аксиому А. 2 можно сделать более определенной, заменив ее небольшим числом аксиом, которые являются ее частными случаями и из которых эту аксиому можно вывести (см. Гёдель [40]). Класс $\{X \mid P(X)\}$, вообще говоря, не является множеством. В том случае, когда он оказывается множеством, высказывание $P(X)$ назы-

[1]) Чтобы уточнить смысл сказанного, нужно описать, какие высказывания допускаются. На самом деле $P(X)$ может быть любым высказыванием, включающим в себя переменные множества, переменные классы, логические символы и кванторы, действующие на переменные множества (см. гл. V).

вается *коллективизируемым* в X. Так, например, если A — заданное множество, то высказывание «$X \in A$» коллективизируемо в X, поскольку класс всех таких X, для которых $X \in A$, есть как раз само множество A. С другой стороны, высказывание «$X \notin X$» не может быть коллективизируемым, если мы хотим избежать упомянутого выше парадокса Рассела. В силу А. 2 класс всех таких множеств X, для которых $X \notin X$, вполне определен, и рассуждение, приводящее к парадоксу Рассела, просто показывает, что существуют классы, не являющиеся множествами [1]).

С помощью А. 2 можно определить обычные операции над множествами, хотя на данном этапе нельзя утверждать, что получающиеся в результате этих операций классы будут множествами, и потому нужно постулировать для этого специальные аксиомы.

Пустой класс определяется равенством

$$\varnothing = \{X \mid X \neq X\}.$$

Полный класс [2]) определяется как

$$T = \{X \mid X = X\}.$$

Если A и B — некоторые классы, то *одиночка*, состоящая из A, и *пара*, состоящая из A и B, определяются равенствами

$$\{A\} = \{X \mid X = A\}, \quad \{A, B\} = \{X \mid X = A \text{ или } X = B\},$$

когда они являются множествами, и не определяются в противном случае. Позже мы увидим, что они определены всякий раз, как только A и B — множества.

Если A — некоторый класс, то *объединением* класса A называется

$$\bigcup A = \{X \mid X \in Y \text{ и } Y \in A \text{ для некоторого } Y\},$$

а *пересечение* класса A задается равенством

$$\bigcap A = \{X \mid X \in Y \text{ для всех } Y, \text{ таких, что } Y \in A\}.$$

Если A и B — множества, то *упорядоченной парой*, состоящей из A и B (в этом порядке), называется

$$(A, B) = \{\{A\}, \{A, B\}\}.$$

Когда $C = \{A, B\}$, то вместо $\bigcup C$ и $\bigcap C$ будем писать $A \cup B$ и $A \cap B$ соответственно; множество A называется *непересекающимся* с B, если $A \cap B = \varnothing$.

[1]) Можно развивать теорию множеств, не используя классы, если ограничиться коллективизируемыми свойствами (см. Бурбаки [54]).

[2]) Этот класс часто называют *универсальным классом*, но мы не будем пользоваться этим термином, чтобы избежать путаницы с универсальными множествами, которые будут определены позднее (§ I.1; см. также § VI. 2).

Если заданы классы A и B, то класс A называется *подклассом* класса B (в обозначениях $A \subseteq B$), если

$$X \in B \text{ для всех таких } X, \text{ что } X \in A.$$

Подкласс, являющийся в то же время множеством, называется *подмножеством*. Если $A \subseteq B$ и $A \neq B$, то A называется *собственным* подклассом и обозначается так: $A \subset B$. Мы также будем писать $B \supseteq A$ или $B \supset A$ вместо $A \subseteq B$ или $A \subset B$ соответственно; далее, отрицание каждого из этих отношений обозначается тем же, но перечеркнутым, символом.

Если A, B — некоторые классы, то класс

$$A \setminus B = \{X \mid X \in A \text{ и } X \notin B\}$$

называется *дополнением* B в A.

Если A — некоторый класс, то

$$\mathscr{B}(A) = \{X \mid X \subseteq A\}$$

называется *булеаном* класса A (в честь Джорджа Буля, 1815—1864 гг; см. также § V. 2).

Если A и B — классы, то

$$A \times B = \{Z \mid Z = (X, Y), \text{ где } X \in A \text{ и } Y \in B\}$$

называют *декартовым произведением* классов A и B.

Функция из A в B — это такой подкласс F класса $A \times B$, что для каждого $X \in A$ существует единственный $Y \in B$, для которого $(X, Y) \in F$. Класс A называется *областью определения* функции F, а класс *значений* функции F

$$\{Y \mid Y \in B \text{ и } (X, Y) \in F \text{ для некоторого } X \in A\}$$

называется ее *областью значений*. Часто, когда хотят сосредоточить внимание на области значений, используют несколько другое определение. Если A — класс, а I — некоторое множество, то областью значений некоторой функции из I в A называют *семейство*[1]) *элементов из* A, *индексированное множеством* I. Если x_i есть элемент класса A, соответствующий элементу $i \in I$, то это семейство обозначается через $(x_i)_{i \in I}$; при этом x_i называется его *i-й координатой*, элемент i — *индексом*, а множество I — *множеством индексов*. Каждое множество можно снабдить индексами, например элементами этого же множества; это значит, что мы можем представить множество A как функцию из A в себя, скажем, как тождественную функцию, при которой каждый элемент из A соответствует самому себе: $A = (a)_{a \in A}$. Таким образом, не ограничивая общности рассу-

---

[1]) Пользуясь этим определением, читатель должен помнить, что на практике функция часто отождествляется со своей областью значений.

ждений, можно иметь дело только с теми множествами, которые снабжены индексами.

Перейдем теперь к главной группе аксиом. Они по существу утверждают, что пустой класс является множеством и что все разумные операции, примененные к множествам, снова дают множества.

А. 3. $\varnothing$ есть множество.

А. 4. Каждый подкласс множества есть множество.

А. 5. Если A, B — множества, то $\{A, B\}$ также является множеством.

А. 6. Если A — множество, то булеан $\mathscr{P}(A)$ также является множеством.

А. 7. Если A — множество, то его объединение $\bigcup A$ также является множеством.

А. 8. Если F — функция, область определения которой есть множество, то ее область значений также является множеством.

Укажем некоторые непосредственные следствия этих аксиом:

(i) Если A, B — множества, то упорядоченная пара (A, B) также будет множеством, и если (A', B') — другая упорядоченная пара множеств, то $(A, B) = (A', B')$ тогда и только тогда, когда $A = A'$ и $B = B'$.

В самом деле $\{A, B\}$ и $\{A\} = \{A, A\}$ являются множествами в силу А. 5; следовательно, $(A, B) = \{\{A\}, \{A, B\}\}$ — также множество. Если задана пара (A, B), то мы можем восстановить (и различить) A и B, рассматривая сначала элементы множества (A, B), а затем элементы этих элементов.

(ii) Если $P(X)$ — некоторое высказывание о классах[1]) и A — множество, то $\{X \mid X \in A$ и $P(X)\}$ будет подклассом в A, а следовательно, по А. 4 — подмножеством. Это часто записывают так: $\{X \in A \mid P(X)\}$. В частности, дополнение любого класса в множестве A будет подмножеством множества A.

(iii) Если A, B — множества, то их декартово произведение $A \times B$ также будет множеством. Действительно, если $X \in A$ и $Y \in B$, то $\{X\}, \{X, Y\} \subseteq A \cup B$; следовательно, $\{X\}, \{X, Y\} \in \mathscr{P}(A \cup B)$, так что $(X, Y) \in \mathscr{P}\mathscr{P}(A \cup B)$. Поэтому

$$A \times B = \{Z \in \mathscr{P}\mathscr{P}(A \cup B) \mid Z = (X, Y) \text{ для некоторых } X \in A \text{ и } Y \in B\},$$

а это показывает, что $A \times B$ является множеством.

(iv) Каждая функция, область определения которой есть множество, сама является множеством. В самом деле, пусть F — функция, а множество A, например, — область ее определения. По А. 8 областью ее значений будет некоторое множество B, и так как $F \subseteq A \times B$, то из (iii) и А.4 вытекает, что F — множество.

---

[1]) См. сноску 1, стр. 14.

Если I — множество, а A — класс, то любая функция из I в A будет множеством, и мы можем рассмотреть класс, элементами которого являются всевозможные функции из I в A. Этот класс обозначается A^I и называется *декартовой степенью*. Поскольку каждая функция из I в A есть подмножество в $I \times A$, т. е. элемент из $\mathscr{P}(I \times A)$, то $A^I \subseteq \mathscr{P}(I \times A)$. В частности, если I и A — множества, то A^I — также множество.

(v) Если $A \neq \varnothing$, то $\bigcap A$ есть множество. Действительно, если $a \in A$, то $\bigcap A$ будет подклассом в a.

Перечисленные аксиомы позволяют нам построить сколь угодно большие конечные[1]), но не бесконечные множества, существование которых нужно постулировать отдельно. Это обычно делается с помощью *аксиомы бесконечности*, в которой утверждается существование бесконечного множества (если только это понятие определено). Мы примем другую аксиому, предполагающую существование универсальных множеств, которые теперь нам и нужно определить (см. Зоннер [62], Габриэль [62]). Оказывается, эта аксиома значительно сильнее аксиомы бесконечности и в большинстве задач исключает необходимость рассмотрения классов, не являющихся множествами.

Определение. Множество U называется *универсальным*, если оно удовлетворяет следующим условиям:

(i) Если $X \in U$, то $X \subseteq U$.

(ii) Если $X \in U$, то $\mathscr{P}(X) \in U$.

(iii) Если $X, Y \in U$, то $\{X, Y\} \in U$.

(iv) Если $F = (F_i)_{i \in I}$, где $F_i \in U$ и $I \in U$, то $\bigcup F \in U$.

В качестве аксиомы бесконечности мы теперь добавим:

А. 9. Каждое множество есть элемент некоторого универсального множества.

Эта аксиома на самом деле устраняет необходимость рассмотрения классов. Например, вместо класса всех множеств мы можем рассматривать класс всех множеств в данном универсальном множестве U, который снова является множеством. Поэтому в дальнейшем мы сохраним термин «класс» за теми множествами, которые не обязательно являются элементами рассматриваемого универсального множества.

Для иллюстрации аксиомы А.9 определим натуральные числа и покажем, что они образуют множество. Пусть U — такое универсальное множество, что $\varnothing \in U$; назовем временно подмножество V множества U *числовым*, если $\varnothing \in V$ и $X \cup \{X\} \in V$, как только $X \in V$.

[1]) Конечно, существование конечных множеств может быть получено из опыта, и какие бы то ни было аксиомы нужны вообще только для бесконечных множеств.

Например, само множество U является числовым: если $X \in U$, то $\{X\} \in U$; следовательно, $\{X, \{X\}\} \in U$ и, снабдив множество $\{X, \{X\}\}$ индексами, мы получаем, что $X \cup \{X\} \in U$. Пусть N — пересечение всех числовых подмножеств множества U; тогда N само является числовым. Обозначая $x \cup \{x\}$ через x', получаем следующие свойства множества N:

N. 1. $\varnothing \in N$.

N. 2. Если $x \in N$, то $x' \in N$.

N. 3. Каждое подмножество множества N, удовлетворяющее условиям N. 1 — 2, совпадает с N.

Здесь N. 3 вытекает из того факта, что N — пересечение всех подмножеств множества U, удовлетворяющих N. 1 и N. 2. Конечно, свойство N. 3 является просто принципом индукции. Определим теперь *натуральные числа* как элементы множества N, первыми среди которых будут

$$0 = \varnothing, \quad 1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \ \ldots$$

Положительным числом будем считать натуральное число $\neq 0$. Класс называется *конечным*, если он может быть индексирован натуральным числом; в противном случае он называется *бесконечным*. С помощью этого определения можно показать, что множество натуральных чисел бесконечно. Сначала отметим следующие свойства:

(a) Если $n \in N$, то $n' \nsubseteq 0$. Действительно, $n' = n \cup \{n\} \neq \varnothing$, в то время как $0 = \varnothing$.

(b) Если $m, n \in N$ и $m \in n$, то $m \subseteq n$. Ясно, что это выполняется, если $n = 0$, так как в этом случае $m \notin n$ для всех $m \in N$. Пусть теперь M — множество всех таких $n \in N$, что $m \subseteq n$ для всех тех $m \in N$, для которых $m \in n$. Если $n \in M$ и $m \in n'$, то либо $m = n$, либо $m \in n$, откуда $m \subseteq n$ в первом и во втором случаях, но $n \subseteq n'$, так что $m \subseteq n'$. Таким образом, если $n \in M$, то $n' \in M$, а поскольку M содержит также и 0, оно должно совпадать с N.

(c) Если $m' \subseteq n'$, то $m \subseteq n$. В самом деле, если $m \cup \{m\} \subseteq n \cup \{n\}$, то $m \in n \cup \{n\}$; следовательно, либо $m \in n$, откуда $m \subseteq n$ в силу (b), либо $m = n$.

Применяя (c) с переставленными m и n, получаем

(d) Если $m' = n'$, то $m = n$.

Заметим, что (a) и (d) вместе с N. 1 — 3 являются обычными аксиомами Пеано для натуральных чисел (см. гл. VII). Впредь мы также будем писать $n + 1$ вместо n' и будем предполагать известными элементарные свойства натуральных чисел. Ограничимся доказательством следующей теоремы.

***Теорема* 1.1.** *Множество натуральных чисел бесконечно.*

Чтобы доказать эту теорему, нужно показать, что если n — некоторое натуральное число, то не существует функции из n в N с множеством N в качестве области значений. Это, конечно, справедливо для $n=0$, так как любая функция с областью определения $0=\varnothing$ должна иметь пустую область значений, в то время как $N\neq\varnothing$. Пусть теперь M — множество таких чисел n, для которых не существует функции из n в N с областью значений N; тогда, как было показано, M удовлетворяет N. 1. Пусть $n\in M$ и предположим, что $n'\notin M$; это значит, что существует функция f из n' в N с областью значений N. Поскольку каждый элемент $\neq 0$ из N имеет вид x' и поскольку x' определяет x в силу (d) однозначно, для любого $y\in N$, такого, что $y\neq 0$, через $y-1$ можно обозначить единственный элемент x из N, который удовлетворяет условию $x'=y$. Кроме того, обозначим через if тот единственный элемент j, для которого $(i, j)\in f$. С помощью этих обозначений можно определить функцию g из n в N, взаимно однозначную, если взаимно однозначно f, следующим образом:

$$kg=\begin{cases} kf-1, & \text{если} \quad kf\neq 0,\\ nf, & \text{если} \quad kf=0.\end{cases}$$

Поскольку $0\subseteq nf$, то этим в самом деле определена функция из n в N с областью значений N, а это противоречит предположению, что $n\in M$. Поэтому если $n\in M$, то $n'\in M$, т. е. M удовлетворяет N. 2, так же как и N. 1, и в силу N. 3 $M=N$. ∎

При построении множества N U было универсальным множеством, содержащим $\varnothing$; по определению каждое непустое универсальное множество должно содержать $\varnothing$, и потому мы имеем

***Следствие* 1.2.** *Всякое непустое универсальное множество бесконечно.* ∎

Теперь аксиома A. 9 обеспечивает существование универсальных множеств, содержащих бесконечные множества в качестве своих элементов. Будем это предполагать относительно всех универсальных множеств, с которыми нам придется иметь дело в дальнейшем.

Существуют некоторые теоретико-множественные конструкции, которые, хотя и не могут привести к противоречиям, однако порождают патологические ситуации, не имеющие аналога в интуитивном представлении. Например, на основе перечисленных выше аксиом мы не можем решить, может ли множество быть элементом самого себя: $X\in X$, и, таким образом, мы вообще не можем сказать, равны или нет множества X и $\{X\}$. Поскольку ситуация, когда $X\in X$, на практике никогда не возникает, лучше всего исключить ее явным образом. Это делается с помощью *аксиомы основания*:

A. 10. Каждый непустой класс A обладает элементом X, не пересекающимся с A.

С помощью этой аксиомы легко видеть, что $X \notin X$ для всех множеств X. Более того, не существует бесконечных убывающих цепей $X_0, X_1, X_2, \ldots$ таких (не обязательно различных) множеств, что

$$X_{n+1} \in X_n \quad (n \in N). \tag{2}$$

Действительно, если бы мы имели семейство множеств, удовлетворяющих условию (2), то класс, элементами которого являются $X_0, X_1, \ldots$, был бы примером, противоречащим аксиоме А. 10.

Иногда полезно следующее расширение введенных ранее обозначений. Пусть $\mathcal{A}$ — класс некоторым способом индексированных множеств, скажем $\mathcal{A} = (A_i)_{i \in I}$. Тогда вместо $\bigcup \mathcal{A}$, $\bigcap \mathcal{A}$ мы также будем писать $\bigcup A_i$, $\bigcap A_i$. В частности, если $\mathcal{A}$ конечно, например $\mathcal{A} = \{A_0, \ldots, A_n\}$, мы пишем

$$\bigcup \mathcal{A} = \bigcup A_i = A_0 \cup \ldots \cup A_n,$$
$$\bigcap \mathcal{A} = \bigcap A_i = A_0 \cap \ldots \cap A_n.$$

Определим теперь *декартово произведение* семейства множеств $(A_i)_{i \in I}$ следующим образом:

$$\prod A_i = \{x \in (\bigcup A)^I \mid x = (x_i)_{i \in I}, \text{ где } x_i \in A_i \text{ для всех } i \in I\}.$$

Это определение не совпадает в случае двух сомножителей с данным ранее определением декартова произведения, но это различие не имеет для нас никакого значения: мы свободно можем интерпретировать декартово произведение тем или другим способом, если имеем дело с двумя (или любым конечным числом) сомножителей (см. упр. 2).

Ясно, что $\prod A_i$ опять есть множество, но даже когда каждое A_i не пусто, нельзя, вообще говоря, показать, что их произведение не пусто. Однако это будет следовать из аксиомы выбора, которая будет введена ниже в § 1.4.

В отличие от объединения и пересечения, где индексирование $\mathcal{A}$ используется только для удобства, это произведение существенно зависит от индексирования, так же как и от класса координат, поскольку, например, произведение изменяется, если какая-либо координата появляется более одного раза. В крайнем случае, когда $A_i = A$ для всех $i \in I$, $\bigcup A_i = \bigcap A_i = A$, тогда как $\prod A_i = A^I$.

Когда I конечно, скажем $I = n + 1$, будем писать также

$$\prod A_i = A_0 \times A_1 \times \ldots \times A_n.$$

УПРАЖНЕНИЯ

1. Показать, что полный класс T не является множеством.

2. Определить наборы из n элементов $(x_1, \ldots, x_n)$ или как семейства, индексированные множеством $\{1, \ldots, n\}$, или же обобщая определение

упорядоченной пары; для каждого определения показать, что $(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$ для любых множеств $x_1, \ldots, x_n, y_1, \ldots, y_n$ тогда и только тогда, когда $x_i = y_i$ $(i = 1, \ldots, n)$.

3. Показать, что $n \notin n$ для любого натурального числа n, не используя А. 10.

4. Сколько существует различных способов индексирования множества из n элементов (i) самим собой, (ii) другим множеством из m элементов?

2. СООТВЕТСТВИЯ

Пусть A и B — множества; тогда *соответствием из A в B* называется подмножество декартова произведения $A \times B$. Таким образом, соответствие представляет собой некоторое множество пар (x, y), где $x \in A$, $y \in B$. Обычно мы будем обозначать соответствия прописными греческими буквами. Если Φ — соответствие из A в B и $A' \subseteq A$, определим

$$A'\Phi = \{y \in B \mid (x, y) \in \Phi \text{ для некоторого } x \in A'\}.$$

В случае, когда $B = A$, Φ называется соответствием *в* A. Каждое множество обладает соответствием

$$\Delta_A = \{(x, x) \mid x \in A\},$$

которое называется *диагональю* в A.

Чтобы описать различные типы соответствий, введем две операции: взятие обратного и умножение. Каждое соответствие Φ обладает *обратным*

$$\Phi^{-1} = \{(x, y) \mid (y, x) \in \Phi\}.$$

Ясно, что если $\Phi \subseteq A \times B$, то $\Phi^{-1} \subseteq B \times A$. Соответствие Φ в A называется *симметричным*, если $\Phi^{-1} = \Phi$, *антисимметричным*, если $\Phi \cap \Phi^{-1} \subseteq \Delta_A$, и *рефлексивным*, если $\Phi \supseteq \Delta_A$.

Для любых соответствий Φ и Ψ определим *произведение*

$$\Phi \circ \Psi = \{(x, y) \mid (x, z) \in \Phi \text{ и } (z, y) \in \Psi \text{ для некоторого } z\}.$$

На самом деле произведение $\Phi \circ \Psi$ будет множеством, так как если $\Phi \subseteq A \times B$ и $\Psi \subseteq C \times D$, то $\Phi \circ \Psi \subseteq A \times D$; в частности, заметим, что $\Phi \circ \Psi = \varnothing$, если $B \cap C = \varnothing$.

Легко проверить следующие тождества:

$$\Phi \circ (\Psi \circ \Theta) = (\Phi \circ \Psi) \circ \Theta, \tag{1}$$

$$(\Phi \circ \Psi)^{-1} = \Psi^{-1} \circ \Phi^{-1}, \tag{2}$$

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

Эти равенства справедливы для любых соответствий Φ, Ψ, Θ. Далее, если Φ — соответствие из A в B, то

$$\Phi \circ \Delta_B = \Delta_A \circ \Phi = \Phi. \tag{4}$$

С помощью этих операций можно определить несколько важных типов соответствий, которые будут часто встречаться в дальнейшем.

Соответствие Φ в A называется *транзитивным*, если

$$\Phi \circ \Phi \subseteq \Phi.$$

Транзитивное рефлексивное соответствие Φ в A называется *предупорядоченностью* в A. Ясно, что тогда Φ^{-1} также является предупорядоченностью в A, которая называется *противоположной* к Φ. Антисимметричная предупорядоченность в A называется также *упорядоченностью* в A или иногда *частичной упорядоченностью* в A, чтобы отличить ее от *линейной упорядоченности*, которая, кроме того, должна удовлетворять равенству $\Phi \cup \Phi^{-1} = A^2$. Под *упорядоченным множеством* мы будем понимать множество вместе с некоторой определенной на нем упорядоченностью.

Если Φ — некоторое соответствие из A в B, то $\Phi \circ \Phi^{-1}$ — соответствие в A, а $\Phi^{-1} \circ \Phi$ — соответствие в B. Если

$$\Phi \circ \Phi^{-1} \supseteq \Delta_A \tag{5}$$

и

$$\Phi^{-1} \circ \Phi \subseteq \Delta_B, \tag{6}$$

то Φ является функцией из A в B в смысле определения из § I.1. Легко доказать следующий результат:

***Предложение* 2.1.** *Если f и g — функции, то $f \circ g$ также является функцией.* ∎

Заметим, что $f \circ g$ вполне может быть пустым множеством, а именно в том случае, когда область значений f не пересекается с областью определения g. Для функций мы часто будем писать fg вместо $f \circ g$ и для данного x из области определения f через xf будем обозначать тот единственный элемент y, для которого $(x, y) \in f$.

Соответствие Φ из A в B называется *биекцией* или *взаимно однозначным соответствием*, если Φ есть функция из A в B и Φ^{-1} — функция из B в A. Два множества называются *равномощными*, если существует взаимно однозначное соответствие между ними. Тот факт, что A и B равномощны, иногда записывают следующим образом: $A \leftrightarrow B$.

Под *n-арным отношением* или *n-местным отношением* (где n — положительное число) мы понимаем множество A вместе с подмножеством Φ множества A^n; мы часто будем называть Φ отношением в A. Так, например, бинарное отношение ($n=2$) есть просто соответствие в некотором фиксированном множестве, тогда как унарное отношение ($n=1$) есть подмножество некоторого фиксированного множества.

УПРАЖНЕНИЯ

1. Показать, что если A и B — множества, то существует взаимно однозначное соответствие между множеством всех пар (x,y) ($x \in A$, $y \in B$) и множеством функций из множества 2 в $A \cup B$, таких, что $0f \in A$, $1f \in B$.

2. Доказать предложение 2.1, используя (5) и (6).

3. Показать, что конечное множество не равномощно никакому своему собственному подмножеству. (Указание: показать, что если f — взаимно однозначное соответствие между множеством S и его собственным подмножеством T и $a \in S$, $a \notin T$, то все элементы a, af, aff, ... различны, и воспользоваться теоремой 1.1.)

4. Показать, что класс, равномощный множеству, сам является множеством.

5. Пусть X — элемент универсального множества U, а множество Y равномощно X. Следует ли отсюда, что $Y \in U$?

3. ОТОБРАЖЕНИЯ И ФАКТОРМНОЖЕСТВА

Определение. *Отображением* называется тройка (A, B, f), состоящая из множества A, второго множества B и функции f из A в B. Множество A называется *источником*, а B — *целью* отображения.

Для отображения (A, B, f) чаще используется запись $f\colon A \to B$, а иногда $A \xrightarrow{f} B$. Последнее обозначение особенно часто применяется в диаграммах для иллюстрации произведения отображений. В отличие от функций, которые всегда можно перемножать, два отображения $f\colon A \to B$ и $g\colon C \to D$ могут быть перемножены только в том случае, если $B = C$, и тогда их произведение обозначается через $fg\colon A \to D$.

Пусть заданы отображения $f\colon A \to B$, $g\colon B \to C$ и $h\colon A \to C$. Если равенство $fg = h$ выполняется, то говорят, что диаграмма отображений

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "h"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

коммутативна. Вообще под коммутативной диаграммой понимают такую сеть изображающих отображения стрелок между множествами, что любые два пути (идущие в направлении стрелок) из одного множества в другое определяют одно и то же отображение между этими множествами. На практике большинство диаграмм составляется из треугольников, как, например, диаграмма, приведенная выше, или квадратов

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle h} \\ C & \xrightarrow[k]{} & D \end{array}$$

где коммутативность означает, что $fh = gk$.

Если задано отображение $f\colon A \to B$, то для каждого $x \in A$ однозначно определенный элемент xf из B называется *образом* элемента x при отображении f. Множество Af всех образов элементов из A также называется *образом* множества A; множество Af является просто областью значений отображения f, рассматриваемого как функция. Если $Af = B$, т. е. $f^{-1} \circ f = \Delta_B$, то отображение f называется *сюръективным*, или отображением *на* B, или *сюръекцией*. Если $f \circ f^{-1} = \Delta_A$, то отображение f называется *инъективным*, или *взаимно однозначным*, или *инъекцией*. Отображение, одновременно являющееся отображением на и взаимно однозначным, называется *биективным*; это просто *взаимно однозначное соответствие* между двумя данными множествами, как было определено в § I.2. Отметим, что соответствие Φ из A в B будет взаимно однозначным в том и только в том случае, если

$$\Phi \circ \Phi^{-1} = \Delta_A, \quad \Phi^{-1} \circ \Phi = \Delta_B.$$

Взаимно однозначное соответствие множества A с самим собой называется также *подстановкой* множества A.

Рассмотрим следующие важные примеры отображений, которые часто будут встречаться в последующем.

(i) В каждом множестве A его диагональ определяет отображение $\Delta_A\colon A \to A$, которое называется *тождественным отображением* и обозначается через 1 или 1_A.

(ii) Если A — некоторое множество и B — множество, содержащее A в качестве подмножества, то диагональ в A определяет отображение $\Delta_A\colon A \to B$, которое называется *вложением* A в B.

(iii) Если дано декартово произведение $P = \prod A_i$, то для каждого фиксированного элемента $i \in I$ функция, сопоставляющая каждому $x \in P$ его i-ю координату, определяет отображение $\varepsilon_i\colon P \to A_i$, которое называется *проекцией* декартова произведения P на сомножитель A_i.

(iv) Пусть дано отображение f: $A \to B$ и подмножество A' множества A. Через i обозначим вложение $A' \to A$. Тогда отображение if: $A' \to B$, называется *ограничением* отображения f на A' и обозначается через $f|A'$. Аналогично, если B' — подмножество в B и $Af \subseteq B'$, то f может быть *срезано* до отображения f': $A \to B'$ ограничением цели. Мы не будем вводить никакого специального обозначения для этого отображения.

(v) Пусть даны два отображения f: $A \to B$ и f': $A' \to B$, где A' — подмножество множества A. Если $f' = f|A'$, то f называется *расширением* отображения f'. Так, например, если f: $A \to B$ — некоторое отображение и $A' \subseteq A$, то f является расширением отображения $f|A'$, но, конечно, в общем случае отображение f не определяется однозначно по $f|A'$.

(vi) Пусть дано множество A и натуральное число n. Любое отображение α: $A^n \to A$ называется *n-арной операцией* на A. При $n = 0$ получается 0-арная операция, по существу элемент из A, тогда как при $n = 1$ получаются в точности отображения A в себя. Используя естественное взаимно однозначное соответствие между $A^n \times A$ и A^{n+1}, задаваемое правилом

$$((x_1, \ldots, x_n), y) \leftrightarrow (x_1, \ldots, x_n, y),$$

мы видим, что n-арную операцию можно рассматривать как частный случай $(n+1)$-арного отношения. Отображения из A^n в A для произвольного конечного n иногда называются *конечноместными* операциями, чтобы отличить их от бесконечноместных операций, т. е. отображений $A^I \to A$, где I бесконечно.

Пусть α есть n-арная операция в A и B — подмножество в A. Тогда B^n также является подмножеством в A^n, и поэтому α определяет отображение множества B^n в A, а именно ограничение α на B^n. Если образ множества B^n при этом отображении содержится в B, мы говорим, что B *замкнуто относительно* α или что B *допускает операцию* α. В таком случае это ограничение может быть срезано до отображения B^n в B, т. е. до n-арной операции на B. Эта операция будет обозначаться через $\alpha|B$ и называться *ограничением* α на B.

(vii) Пусть f: $I \to A$ — отображение. Будем писать a_i вместо if $(i \in I)$. Тогда $(a_i)_{i \in I}$ будет в точности семейством элементов из A, как было определено ранее. Рассматривать отображения с этой точки зрения удобно тогда, когда мы хотим обратить особое внимание на множество образов.

(viii) Если дано множество A, то каждое подмножество B множества A определяет отображение χ_B: $A \to 2$, задаваемое равенствами

$$x\chi_B = \begin{cases} 0, & \text{если } x \notin B, \\ 1, & \text{если } x \in B. \end{cases}$$

χ_B называется *характеристической функцией* подмножества B. Легко проверить, что отображение

$$B \to \chi_B$$

из $\mathscr{B}(A)$ в 2^A является взаимно однозначным отображением.

(ix) Пусть дано некоторое отображение $f\colon A \to B$. Определим отображение

$$f^*\colon \mathscr{B}(B) \to \mathscr{B}(A)$$

правилом

$$Yf^* = \{x \in A \mid xf \in Y\} \quad \text{для любого } Y \in \mathscr{B}(B).$$

Множество Yf^* называется *полным прообразом* множества Y при отображении f, а отображение f^* — *переходом к полным прообразам.*

Эквивалентностью на множестве A называется рефлексивное, симметричное и транзитивное соответствие Φ в A. Таким образом, имеем

(a) $\Phi \supseteq \Delta_A$,

(b) $\Phi^{-1} = \Phi$,

(c) $\Phi \circ \Phi \subseteq \Phi$.

Будем обозначать эквивалентности строчными готическими буквами. Если $\mathfrak{q}$ — эквивалентность на A, то для каждого $x \in A$ определим подмножество $x^{\mathfrak{q}}$ множества A, *$\mathfrak{q}$-класс* элемента x, равенством[1])

$$x^{\mathfrak{q}} = \{y \in A \mid (x, y) \in \mathfrak{q}\}.$$

Вместо $(x, y) \in \mathfrak{q}$ мы часто будем писать $x \equiv y \pmod{\mathfrak{q}}$. Из свойств эквивалентности $\mathfrak{q}$ легко следует, что $x \in x^{\mathfrak{q}}$ и что на самом деле $x \equiv y \pmod{\mathfrak{q}}$ тогда и только тогда, когда $x^{\mathfrak{q}} = y^{\mathfrak{q}}$. В частности, $\mathfrak{q}$-классы образуют *разбиение* множества A, т. е. разложение A на попарно непересекающиеся непустые множества, *классы* этого разбиения. Сами $\mathfrak{q}$-классы являются элементами булеана $\mathscr{B}(A)$; подмножество множества $\mathscr{B}(A)$, состоящее из всех $\mathfrak{q}$-классов, будем обозначать через $A/\mathfrak{q}$ и называть *фактормножеством* множества A по эквивалентности $\mathfrak{q}$. Если каждому $x \in A$ сопоставить $x^{\mathfrak{q}}$, то мы получим отображение из A в $A/\mathfrak{q}$, которое называется *естественным отображением* или *отождествлением*, связанным с $\mathfrak{q}$, и обозначается через $\operatorname{nat}\mathfrak{q}$. Из определения ясно, что $\operatorname{nat}\mathfrak{q}$ будет отображением на $A/\mathfrak{q}$.

Теперь мы можем сформулировать основную теорему о разложении отображений.

---

[1]) Это обозначение не следует путать с обозначением декартовой степени.

Теорема 3.1. *Пусть f: $A \to B$ — произвольное отображение и положим $\mathfrak{q} = f \circ f^{-1}$. Тогда $\mathfrak{q}$ является эквивалентностью на A, множество Af есть подмножество множества B, и для отображения f существует разложение*

$$f = \varepsilon f' \mu, \tag{1}$$

где $\varepsilon = \operatorname{nat} \mathfrak{q}$ — отображение A на $A/\mathfrak{q}$, f' — взаимно однозначное соответствие между $A/\mathfrak{q}$ и Af и μ — вложение, т. е. взаимно однозначное отображение Af в B.

Эту ситуацию можно пояснить следующей коммутативной диаграммой:

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "\varepsilon"'] & B \\
A/\mathfrak{q} \arrow[r, "f'"'] & Af \arrow[u, "\mu"']
\end{tikzcd}$$

Доказательство. По определению $f \circ f^{-1} \supseteq \Delta_A$; далее

$$(f \circ f^{-1})^{-1} = (f^{-1})^{-1} \circ f^{-1} = f \circ f^{-1},$$

и, поскольку $f^{-1} \circ f \subseteq \Delta_B$, имеем

$$f \circ f^{-1} \circ f \circ f^{-1} \subseteq f \circ \Delta_B \circ f^{-1} = f \circ f^{-1};$$

это показывает, что $\mathfrak{q} = f \circ f^{-1}$ является эквивалентностью на A. Ясно, что Af есть подмножество в B, а из определения $\mathfrak{q}$ следует, что $(x, y) \in \mathfrak{q}$ тогда и только тогда, когда $(x, z) \in f$ и $(y, z) \in f$ для некоторого $z \in B$, т. е. тогда и только тогда, когда $xf = yf$; поэтому отображение f': $A/\mathfrak{q} \to Af$, определенное равенством $x^{\mathfrak{q}} f' = xf$, является отображением на. Теперь отсюда вытекает (1), если в качестве ε взять $\operatorname{nat} \mathfrak{q}$, а в качестве μ — вложение $Af \to B$. ∎

Эквивалентность $\mathfrak{q} = f \circ f^{-1}$ называется *ядром* отображения f и обозначается через $\ker f$.

Следствие 3.2. *Пусть $A = \bigcup A_i$ — разбиение множества A; тогда существует одна и только одна эквивалентность, которая определяет это разбиение.*

Чтобы это показать, определим отображение f: $A \to I$, сопоставив каждому $x \in A$ тот единственный индекс $i \in I$, при котором $x \in A_i$. Классы эквивалентных элементов из ядра отображения f являются как раз подмножествами A_i; ясно, что $\ker f$ будет единственной такой эквивалентностью. ∎

Применяя еще раз теорему 3.1, получаем теорему о фактор-множествах:

Теорема 3.3. *Пусть заданы отображение $f\colon A \to B$ и эквивалентность $\mathfrak{q}$ на A. Если $\mathfrak{q} \subseteq \ker f$, то существует единственное отображение $\bar{f}\colon A/\mathfrak{q} \to B$, такое, что диаграмма*

$$\begin{tikzcd} A \arrow[rr, "\operatorname{nat}\mathfrak{q}"] \arrow[dr, "f"'] & & A/\mathfrak{q} \arrow[dl, "\bar{f}"] \\ & B & \end{tikzcd}$$

коммутативна.

Это означает, что $f = (\operatorname{nat}\mathfrak{q})\bar{f}$, где $\operatorname{nat}\mathfrak{q}$ — естественное отображение $A \to A/\mathfrak{q}$. Иначе говоря, это означает, что $\operatorname{nat}\mathfrak{q}$ может быть (единственным образом) выделен сомножителем в f. Иногда теорему коротко (хотя и неточно) формулируют, говоря, что любое отображение можно профакторизовать по эквивалентности, содержащейся в его ядре.

Для доказательства теоремы заметим, что если отображение $\bar{f}$, удовлетворяющее условиям теоремы, существует, то для каждого $x \in A$ должно выполняться равенство

$$(x^{\mathfrak{q}})\bar{f} = xf. \tag{2}$$

Таким образом, может существовать не больше одного отображения $\bar{f}$; с другой стороны, полагая $\mathfrak{f} = \ker f$, имеем $\mathfrak{q} \subseteq \mathfrak{f}$ по предположению, и, следовательно, $x^{\mathfrak{q}} = y^{\mathfrak{q}}$ влечет $x^{\mathfrak{f}} = y^{\mathfrak{f}}$, т. е. $x^{\mathfrak{q}} = y^{\mathfrak{q}}$ влечет $xf = yf$. Поэтому xf зависит только от $x^{\mathfrak{q}}$, а не от самого x. Но это означает, что $\bar{f}$, определенное по формуле (2), однозначно и потому является искомым отображением. ∎

Фактормножества данного множества A до некоторой степени двойственны подмножествам множества A, но эта двойственность не полная. Так, например, отношение «*B есть подмножество множества B*» транзитивно, тогда как отношение «*B есть фактормножество множества A*» не транзитивно. Действительно, множество $\mathscr{P}(A)$ подмножеств множества A упорядочено относительно отношения $\subseteq$. Если через $\mathfrak{Q}(A)$ обозначено множество фактормножеств множества A, то $\mathfrak{Q}(A)$ можно упорядочить, полагая $X \succ Y$, где $X, Y \in \mathfrak{Q}(A)$, если ядро естественного отображения $A \to X$ содержится в ядре естественного отображения $A \to Y$. Применяя теорему о фактормножествах (при $A/\mathfrak{q} = X$, $B = Y$), видим, что в этом случае существует отображение X на Y, которое имеет некоторое право называться «естественным». На этом пути получается замена отсутствующей транзитивности. Чтобы выразить это формально, проще вместо $\mathfrak{Q}(A)$ рассмотреть множество $\mathscr{C}(A)$ всех эквивалентностей на A. В силу следствия 3.2 существует взаимно однозначное соответствие между

$\mathscr{C}(A)$ и $\mathscr{Q}(A)$; кроме того, ясно, что упорядоченность $\succ$, только что определенная на $\mathscr{Q}(A)$, соответствует при этом упорядоченности по включению на $\mathscr{C}(A)$. Отсюда вытекает

Теорема 3.4. *Пусть $\mathfrak{q}$, $\mathfrak{r}$ — такие эквивалентности на множестве A, что $\mathfrak{q} \subseteq \mathfrak{r}$. Тогда существует единственное отображение $\theta\colon A/\mathfrak{q} \to A/\mathfrak{r}$, при котором $(\mathrm{nat}\,\mathfrak{q})\,\theta = \mathrm{nat}\,\mathfrak{r}$. Если $\ker\theta$ обозначить через $\mathfrak{r}/\mathfrak{q}$, то $\mathfrak{r}/\mathfrak{q}$ будет эквивалентностью на $A/\mathfrak{q}$, а θ индуцирует взаимно однозначное соответствие*

$$\theta'\colon (A/\mathfrak{q})/(\mathfrak{r}/\mathfrak{q}) \to A/\mathfrak{r},$$

так что диаграмма

$$\begin{tikzcd}
A \arrow[r, "\mathrm{nat}\,\mathfrak{q}"] \arrow[dr, "\mathrm{nat}\,\mathfrak{r}"'] & A/\mathfrak{q} \arrow[r, "\mathrm{nat}\,(\mathfrak{r}/\mathfrak{q})"] \arrow[d, "\theta"] & (A/\mathfrak{q})/(\mathfrak{r}/\mathfrak{q}) \arrow[dl, "\theta'"] \\
 & A/\mathfrak{r} &
\end{tikzcd}$$

коммутативна.

Чтобы получить θ, применим теорему 3.3 при $B = A/\mathfrak{r}$, $f = \mathrm{nat}\,\mathfrak{r}$; поскольку $\mathrm{nat}\,\mathfrak{q}$ и $\mathrm{nat}\,\mathfrak{r}$ являются отображениями на, то отсюда следует, что θ — отображение на, и если мы теперь воспользуемся теоремой о разложении 3.1, то получим последнее утверждение теоремы. ∎

УПРАЖНЕНИЯ

1. Пусть Φ_i $(i \in I)$ и Ψ — произвольные соответствия. Показать, что

$$\left(\bigcup \Phi_i\right) \circ \Psi = \bigcup \left(\Phi_i \circ \Psi\right),$$

но в общем случае

$$\left(\bigcap \Phi_i\right) \circ \Psi \neq \bigcap \left(\Phi_i \circ \Psi\right).$$

2. Если $\mathfrak{q}_i$ $(i \in I)$ — произвольное семейство эквивалентностей на A, то $\bigcap \mathfrak{q}_i$ снова будет эквивалентностью.

3 Пусть p_n — число эквивалентностей на множестве из n элементов. Получить для p_n следующую рекуррентную формулу:

$$p_{n+1} = \sum \binom{n}{i} p_i \quad (p_0 = 1),$$

где $\binom{n}{i} = \dfrac{n!}{i!\,(n-i)!}$. Доказать также формулу

$$\sum \frac{p_n x^n}{n!} = \exp\left[(\exp x) - 1\right].$$

4. Показать, что каждое взаимно однозначное отображение конечного множества в себя будет отображением на все это множество. (Использовать упр. 2.3.)

5. Пусть в теореме 3.1 $f = \varepsilon_1 f'_1 \mu_1$ — второе разложение, где ε_1, f'_1, μ_1 — такие же, как ε, f', μ соответственно. Показать, что существуют такие взаимно однозначные соответствия α, β, что $\varepsilon_1 = \varepsilon\alpha$, $\mu_1 = \beta\mu$ и $f' = \alpha f'_1 \beta$.

6. Пусть Φ — предупорядоченность в A и $\mathfrak{q} = \Phi \cap \Phi^{-1}$. Проверить, что $\mathfrak{q}$ — эквивалентность, и показать, что $A/\mathfrak{q}$ можно упорядочить естественным образом относительно заданной предупорядоченности на A.

7. Пусть $\Phi \subseteq A \times B$ и пусть $A' = B\Phi^{-1}$, $B' = A\Phi$, $\mathfrak{a}_1 = \Phi \circ \Phi^{-1}$, $\mathfrak{b}_1 = \Phi^{-1} \circ \Phi$, $\mathfrak{a}_n = \mathfrak{a}_{n-1} \circ \mathfrak{a}_1$, $\mathfrak{b}_n = \mathfrak{b}_{n-1} \circ \mathfrak{b}_1$ и $\mathfrak{a} = \bigcup \mathfrak{a}_n$, $\mathfrak{b} = \bigcup \mathfrak{b}_n$. Показать, что $\mathfrak{a}$, $\mathfrak{b}$ — эквивалентности на A', B' соответственно и что Φ естественным образом индуцирует взаимно однозначное соответствие $A'/\mathfrak{a} \to B'/\mathfrak{b}$. (Это утверждение можно считать аналогом теоремы 3.1 для соответствий, и оно доказывается тем же способом.)

8. Пусть A, X, Y — некоторые множества. Показать, что отображение $f\colon X \to Y$ индуцирует отображение $f^\circ\colon A^Y \to A^X$ и отображение $f_\circ\colon X^A \to Y^A$. Выразить проектирующие операторы декартовой степени A^X как f° для подходящего f.

9. Пусть $f\colon A \to B$. Определим $f_*\colon \mathscr{B}(A) \to \mathscr{B}(B)$ по правилу

$$Xf_* = \{xf \mid x \in X\}$$

и f^*, как в примере (ix) (переход к полным прообразам). При каких условиях $f^* f_* = 1$ или $f_* f^* = 1$?

4. УПОРЯДОЧЕННЫЕ МНОЖЕСТВА

Пусть A — упорядоченное множество, т. е. множество вместе с упорядоченностью, определенной на нем. Примем теперь для упорядоченности обычное обозначение $\leqslant$, так что аксиомы, определяющие упорядоченность, читаются следующим образом:

О. 1. Если $x \leqslant y$ и $y \leqslant z$, то $x \leqslant z$.
О. 2. $x \leqslant x$.
О. 3. Если $x \leqslant y$ и $y \leqslant x$, то $x = y$.

Как обычно, будем писать $x < y$, если $x \leqslant y$ и $y \nleqslant x$; будем писать также $x \geqslant y$ вместо $y \leqslant x$ и $x > y$ вместо $y < x$. Упорядоченность называется *линейной*, если, кроме того, любые два элемента *сравнимы*, т. е.

О. 4. $x \leqslant y$ или $y \leqslant x$ для всех $x, y \in A$.

В другом крайнем случае абстрактное множество можно считать *вполне неупорядоченным* множеством, в котором $x \leqslant y$ истинно лишь при $x = y$; таким образом, никакие два различных элемента не сравнимы.

Если B — подмножество в A, то упорядоченность в A, ограниченная множеством B, будет упорядоченностью в B. В этом смысле каждое подмножество упорядоченного множества считается упорядоченным множеством. Если упорядоченность на B, определенная таким способом, оказывается линейной, то B называется *цепью* в A.

Пусть B — некоторое подмножество упорядоченного (или, в более общем случае, предупорядоченного) множества A. Элемент $a \in A$, обладающий тем свойством, что

$$x \leqslant a \quad \text{для всех} \quad x \in B,$$

называется *верхней гранью* множества B в A. Если такие элементы существуют, то говорят, что *B ограничено сверху в A*. Аналогично определяются нижние грани множества B. Упорядоченное множество, в котором каждое конечное подмножество имеет верхнюю грань, называется *направленным* (вверх). Индукцией по числу элементов легко показать, что достаточно потребовать, чтобы любая пара элементов в этом множестве имела верхнюю грань. Аналогично определяется множество, направленное вниз; если не оговорено противное, то «направленное» всегда будет означать «направленное вверх».

Если упорядоченное множество A само обладает верхней гранью a, то ясно, что a будет единственной верхней гранью; этот элемент a называется *наибольшим элементом* множества A. Если элемент $a \in A$ таков, что ни одна из верхних граней одиночки $\{a\}$ в A не превосходит a, то элемент a называется *максимальным* в A. Таким образом, a будет максимальным в A, если только

$$a \nless x \quad \text{для всех} \quad x \in A.$$

Конечно, A может иметь более одного или вообще ни одного максимального элемента. Если множество A обладает наибольшим элементом, то он будет также единственным максимальным элементом. Обратное утверждение, вообще говоря, не верно, однако оно имеет место в цепях, или, в более общем случае, в направленных множествах: максимальный элемент в направленном множестве является также его наибольшим элементом. *Минимальные* элементы множества A и *наименьший* элемент множества A определяются аналогично. Если подмножество B имеет наименьшую верхнюю грань, то она называется *точной верхней гранью* множества B и обозначается $\sup B$. Аналогично наибольшая нижняя грань, если она существует, называется *точной нижней гранью* и обозначается $\inf B$. Все эти определения полностью применимы, когда множество A всего лишь предупорядочено.

Теперь мы можем сформулировать нашу последнюю аксиому.

А. 11. (Лемма Цорна.) Непустое упорядоченное множество, в котором каждая цепь обладает верхней гранью, имеет максимальный элемент.

Вместо А.11 часто постулируется

Аксиома выбора. Для любого множества A существует такая функция f из $\mathscr{B}'(A) = \mathscr{B}(A) \setminus \{\varnothing\}$ в A, что $Bf \in B$, если только $B \in \mathscr{B}'(A)$.

Обычно аксиому А. 11 доказывают с помощью аксиомы выбора (см., например, Халмош [61] или Келли [55]); но поскольку аксиому выбора можно в свою очередь вывести из аксиомы А. 11 (см. § I.5), то несущественно, предполагается ли выполненной А. 11 или аксиома выбора.

Говорят, что упорядоченное множество удовлетворяет *условию минимальности*, если каждое его непустое подмножество обладает минимальным элементом. Если выполняется это условие и, кроме того, число минимальных элементов любого подмножества конечно, то A называется *частично вполне упорядоченным*; а если каждое непустое подмножество обладает единственным минимальным элементом, то A называется *вполне упорядоченным*. Легко видеть, что частично вполне упорядоченное множество будет вполне упорядоченным тогда и только тогда, когда оно линейно упорядочено. Для множеств с условием минимальности имеет место

***Обобщенный принцип индукции.* (*Нётерова индукция.*)** *Пусть A — упорядоченное множество с условием минимальности и B — подмножество множества A, содержащее элемент $a \in A$, как только оно содержит все элементы $x \in A$, такие, что $x < a$*[1]*. Тогда $B = A$.*

Действительно, дополнение B в A не имеет минимального элемента и поэтому должно быть пустым. ∎

Частный случай этого принципа, когда A вполне упорядочено, известен как *принцип трансфинитной индукции*. Последний сам является обобщением принципа индукции для натуральных чисел (см. § I.1), так как натуральные числа N образуют вполне упорядоченное множество относительно отношения $\subseteq$. В § I.5 мы увидим, что каждое множество может быть вполне упорядочено.

Аналогично приведенному выше принципу доказательства по индукции существует принцип определения по индукции, который также применяется к произвольным упорядоченным множествам с условием минимальности (см. Курош [62] или, в случае натуральных чисел, также § VII.1 ниже).

Упорядоченное множество, в котором каждая пара элементов a, b имеет точную верхнюю грань $a \vee b$ и точную нижнюю грань $a \wedge b$, называется *структурой*. По индукции получаем, что в структуре каждое непустое конечное подмножество имеет точную верхнюю и

[1] Отсюда следует, в частности, что все минимальные элементы множества A, если такие существуют, принадлежат B. — *Прим. ред.*

нижнюю грани; если это верно для *любого* подмножества, то структура называется *полной*. В частности, полная структура L всегда обладает наибольшим элементом ($= \inf \varnothing = \sup L$) и наименьшим элементом ($= \sup \varnothing = \inf L$).

Ясно, что всякая структура направлена; кроме того, каждое линейно упорядоченное множество будет структурой (хотя и не обязательно полной). С другой стороны, конечная структура всегда полна. Примером полной структуры является $\mathscr{B}(A)$, где A — произвольное множество. Вообще, пусть A — упорядоченное множество; подмножество X множества A называется *левым отрезком* множества A, если для каждого $x \in X$ из $y \leqslant x$ следует $y \in X$. Аналогично X называется *правым отрезком* множества A, если $y \in X$, как только $y \geqslant x$ для некоторого $x \in X$. Легко проверить, что множество $\mathscr{S}(A)$ всех левых отрезков множества A, упорядоченное по включению, будет полной структурой. Отметим, что любое абстрактное множество A можно считать вполне неупорядоченным; в этом случае $\mathscr{S}(A)$ совпадает с $\mathscr{B}(A)$. При проверке того, что данное упорядоченное множество является полной структурой, полезен следующий критерий:

***Предложение* 4.1.** *Если A — такое упорядоченное множество, в котором каждое подмножество обладает точной нижней гранью*[1]*, то A является полной структурой.*

Действительно, рассмотрим $X \subseteq A$, Y — множество всех верхних граней множества X в A и положим $y = \inf Y$. Тогда любой элемент из X будет нижней гранью множества Y и, следовательно, $x \leqslant y$ для любого $x \in X$; если также $x \leqslant z$ для любого $x \in X$, то $z \in Y$ и, следовательно, $y \leqslant z$. Поэтому $y = \sup X$. ∎

Это предложение нужно применять с некоторой осторожностью, так как если, например, A — подмножество полной структуры L и каждое подмножество множества A имеет точную нижнюю грань в A, то A снова будет полной структурой, но точные верхние грани подмножеств из A будут, вообще говоря, различными в зависимости от того, берутся ли они в A или в L; точнее, для $X \subseteq A$ имеем

$$\sup_L X \leqslant \sup_A X,$$

и равенство выполняется не обязательно.

Подструктурой структуры L называется подмножество A структуры L, которое вместе с каждой парой a, b элементов из A содержит также $a \vee b$ и $a \wedge b$. Таким образом, подструктура вместе с каждым конечным (непустым) подмножеством X содержит также его точные верхнюю и нижнюю грани, взятые в L. В полной струк-

[1]) Обращаем внимание читателя на то, что точной нижней гранью обладает, следовательно, и пустое подмножество, т. е. в A существует наибольший элемент. — *Прим. ред.*

туре от подструктуры требуется, чтобы она содержала точные верхнюю и нижнюю грани любого из своих подмножеств.

Пусть A и B — произвольные упорядоченные множества. Отображение $f\colon A \to B$ называется *монотонным гомоморфизмом*, если

$$x \leqslant y \quad \text{влечет} \quad xf \leqslant yf \quad \text{для всех} \quad x, y \in A.$$

Если $f\colon A \to B$ — монотонный гомоморфизм, а f^{-1} также является отображением, и, более того, монотонным гомоморфизмом (из B в A), то f называется *монотонным изоморфизмом* между A и B, и мы говорим, что A и B монотонно изоморфны. Легко видеть, что если A направлено или линейно упорядочено, то его образ при монотонном гомоморфизме обладает тем же свойством. Однако если f — монотонный гомоморфизм между структурами, то точные верхние и нижние грани могут не сохраняться, т. е., вообще говоря, равенства

$$(x \vee y) f = xf \vee yf, \quad (x \wedge y) f = xf \wedge yf \quad \text{для всех} \ x, \ y \in A$$

не справедливы. Если же это условие выполняется, f называется *структурным гомоморфизмом*. Соответственно *структурным изоморфизмом* называется такое взаимно однозначное соответствие f, что оба отображения f и f^{-1} являются структурными гомоморфизмами. Каждый монотонный изоморфизм между структурами на самом деле является структурным изоморфизмом, хотя соответствующее утверждение для гомоморфизмов не верно.

Для сравнения упорядоченных множеств мы будем пользоваться следующим свойством полных структур, которое на самом деле может быть использовано для их характеризации (см. Девис [55], Тарский [55]).

***Предложение* 4.2.** *Каждый монотонный гомоморфизм полной структуры в себя имеет неподвижную точку.*

Доказательство. Пусть L — структура, $f\colon L \to L$ — монотонный гомоморфизм. Положим $I = \{x \in L \mid x \leqslant xf\}$, $a = \sup I$. Для любого $x \in I$, $x \leqslant xf$ и $x \leqslant a$; поэтому $xf \leqslant af$, откуда $x \leqslant af$ для всех $x \in I$. Таким образом, af — верхняя грань множества I; по определению элемента a это означает, что

$$a \leqslant af, \tag{1}$$

откуда следует, что $a \in I$. В силу (1) $af \leqslant af^2$, т. е. $af \in I$. Поэтому $af \leqslant a$, и вместе с (1) это дает $af = a$. ∎

***Теорема* 4.3.** *Пусть A и B — такие упорядоченные множества, что A монотонно изоморфно левому отрезку множества B, а B монотонно изоморфно правому отрезку множества A. Тогда* *существует взаимно однозначное соответствие* $f\colon A \to B$, *сохраняющее упорядоченность в следующем ослабленном смысле*:

$$x < y \quad \textit{влечет} \quad xf \not> yf \quad \textit{для всех} \quad x,\ y \in A. \tag{2}$$

Доказательство. Пусть $g\colon A \to B_0$ и $h\colon B \to A_0$ — данные монотонные изоморфизмы между множеством A и левым отрезком B_0 множества B и между множеством B и правым отрезком A_0 множества A. Для любого подмножества X множества A обозначим через X' его дополнение в A и подобные обозначения введем для подмножеств множества B. Ясно, что дополнение левого (правого) отрезка является правым (левым) отрезком, и в самом деле $X \to X'$ (для $X \in \mathscr{S}(A)$) будет отображением множества левых отрезков множества A на множество правых отрезков множества A, изменяющим упорядоченность на обратную. Определим отображение θ множества $\mathscr{S}(A)$ в себя правилом

$$X\theta = ((Xg)'\,h)'.$$

Так как g и h сохраняют упорядоченность, а переход к дополнению меняет ее на обратную, то θ сохраняет упорядоченность, т. е. является монотонным гомоморфизмом, а поскольку структура $\mathscr{S}(A)$ полна, то θ имеет неподвижную точку (предложение 4.2), т. е. существует такой левый отрезок A_1 множества A, что $((A_1g)'\,h)' = A_1$. Таким образом, если $B_1 = A_1g$, то $B_1'h = A_1'$. Определим теперь $f\colon A \to B$ следующим образом:

$$xf = \begin{cases} xg, & \text{если} \quad x \in A_1, \\ xh^{-1}, & \text{если} \quad x \in A_1'. \end{cases}$$

Поскольку оба отображения g, h взаимно однозначны, то f также взаимно однозначно, и, кроме того, если $x < y$, то $xf \neq yf$. Поэтому, чтобы проверить (2), нужно только показать, что $x < y$ влечет $xf \not> yf$. Если это не верно, то для некоторых $x,\ y \in A$ имеем

$$x < y \quad \text{и} \quad xf > yf. \tag{3}$$

Если $y \in A_1$, то $x \in A_1$ и $xf = xg < yg = yf$, что противоречит (3). Если $x \in A_1'$, то $y \in A_1'$ и $x = xfh > yfh = y$, что снова противоречит (3). Остается единственная возможность, когда $x \in A_1$ и $y \in A_1'$. Это значит, что $xf \in B_1$, а $yf \in B_1'$, но B_1' — правый отрезок множества B; следовательно, в силу (3) $xf \in B_1'$, и мы снова получаем противоречие. Итак, (3) не может выполняться. ∎

Если применить эту теорему к вполне неупорядоченным (т. е. абстрактным) множествам, то мы получим

***Следствие* 4.4. (*Теорема Шрёдера — Бернштейна.*)** *Если A и B — произвольные множества, $g\colon A \to B$ и $h\colon B \to A$ — некоторые взаимно однозначные отображения (инъекции), то существует взаимно однозначное соответствие между A и B.* ∎

Для линейно упорядоченных множеств из (2) вытекает, что f — монотонный изоморфизм, и мы получаем в этом случае

***Следствие* 4.5.** *Пусть A и B — такие упорядоченные множества, что A монотонно изоморфно левому отрезку множества B, а B монотонно изоморфно правому отрезку множества A. Если хотя бы одно из множеств A или B линейно упорядочено, то A монотонно изоморфно B.*

Действительно, в силу симметрии можно считать, что B линейно упорядочено; применяя теорему, получаем взаимно однозначное соответствие, удовлетворяющее (2), т. е. монотонный гомоморфизм. Так как на самом деле A также линейно упорядочено (поскольку A монотонно изоморфно отрезку множества B), это взаимно однозначное соответствие действительно является монотонным изоморфизмом. ∎

Как можно показать на примерах (см. упр. 7), следствие 4.5 не справедливо для произвольных упорядоченных множеств.

Каждому элементу a упорядоченного множества A можно сопоставить левый отрезок $S_a = \{x \in A \mid x \leqslant a\}$, и нетрудно проверить, что отображение $a \to S_a$ будет монотонным гомоморфизмом множества A в $\mathcal{S}(A)$. Так как это отображение, очевидно, взаимно однозначно, то отсюда вытекает, что A всегда монотонно изоморфно подмножеству множества $\mathcal{S}(A)$. Следующий результат, принадлежащий Дилуорсу и Глисону [62], показывает, что A никогда не может быть изоморфно множеству $\mathcal{S}(A)$.

***Теорема* 4.6.** *Пусть A — упорядоченное множество и $f\colon A_0 \to \mathcal{S}(A)$ — монотонный гомоморфизм подмножества A_0 множества A в $\mathcal{S}(A)$. Тогда f не является отображением на $\mathcal{S}(A)$.*

Действительно, предположим, что f — отображение на $\mathcal{S}(A)$; положим $B = \{x \in A_0 \mid x \notin xf\}$, и пусть $\overline{B}$ — левый отрезок, порожденный подмножеством B, т. е. множество всех таких $y \in A$, что $y \leqslant x$ для некоторого $x \in B$. По предположению $\overline{B} = bf$ для некоторого $b \in A_0$. Если $b \notin \overline{B}$, то получаем противоречие, так как $b \in B \subseteq \overline{B}$ по определению B. Следовательно, $b \in \overline{B}$, т. е. $b \leqslant x$ для некоторого $x \in B$, и поэтому $\overline{B} = bf \subseteq xf$. Но $x \in B \subseteq \overline{B} \subseteq xf$, а в силу определения B это значит, что $x \notin B$, т. е. снова получаем противоречие. ∎

Это доказательство обобщает хорошо известный диагональный процесс Кантора, с помощью которого обычно показывают, что A и

$\mathscr{B}(A)$ не равномощны. Чтобы получить этот результат, будем считать A вполне неупорядоченным множеством; тогда любое отображение множества A (или произвольного подмножества множества A) в $\mathscr{S}(A)$ будет гомоморфизмом, и мы получаем

Следствие 4.7. *Ни для какого множества A не существует взаимно однозначного соответствия между A и $\mathscr{B}(A)$.* ∎

В общем случае для упорядоченных множеств получаем

Следствие 4.8. *Ни для какого упорядоченного множества A не существует монотонного изоморфизма A на $\mathscr{S}(A)$.* ∎

Для некоторых типов упорядоченных множеств полезно представление с помощью графов, которое мы сейчас введем. Под *графом* понимают фигуру, состоящую из точек, *вершин*, вместе с отрезками, *ребрами*, соединяющими некоторые пары вершин. Нас будут интересовать только *ориентированные графы*, в которых каждое ребро имеет определенную ориентацию, соответствующую упорядоченности его концевых точек. Эту ориентацию можно изобразить стрелкой вдоль ребра. Таким образом, коммутативные диаграммы отображений в § I. 3 являются примерами ориентированного графа. Если Γ — произвольный ориентированный граф, то множество $V(\Gamma)$ его вершин можно сделать предупорядоченным, полагая $a \leqslant b$ для любых a, $b \in V(\Gamma)$ тогда и только тогда, когда можно пройти от a до b вдоль ребер этого графа (учитывая их ориентации). Обратно, чтобы изобразить данное предупорядоченное множество A, будем считать его элементы вершинами графа со стрелками от a к b, если только $a \leqslant b$. Полученный ориентированный граф обозначается через $\Gamma(A)$ и называется *графом множества* A. Конечно, для многих упорядоченных множеств эта иллюстрация не очень полезна (например, для упорядоченного по включению множества всех функций из множества N в себя), и большинство приводимых в тексте диаграмм будет относиться к конечным графам, где для ясности наносятся только стрелки, связывающие такие элементы a, b, что *b покрывает a*, т. е. b является минимальным элементом из тех, для которых $b > a$.

Граф называется *связным*, если любые две его вершины могут быть связаны, т. е. существует такая конечная последовательность вершин $a_0 = a$, a_1, ..., $a_n = b$, что a_{i-1} и a_i соединены ребром (независимо от его ориентации). Вообще говоря, граф упорядоченного множества не обязательно связен; например, вполне неупорядоченное множество имеет «вполне несвязный» граф, в котором никакие две различные вершины не связаны. В произвольном графе Γ отношение «*a связано с b*» будет, очевидно, эквивалентностью в $V(\Gamma)$; классы этой эквивалентности называются *связными компонентами* графа Γ.

Следующая теорема редукции (Ньюмен [42]) будет использована позднее (в § III. 9) при рассмотрении нормальной формы элементов в данном представлении.

***Теорема* 4.9.** *Пусть A — предупорядоченное множество и предположим, что*

(i) *для каждого $a \in A$ существует такое положительное число $k = k(a)$, что любая убывающая цепь, начинающаяся с a,*

$$a = a_0 \geqslant a_1 \geqslant \ldots,$$

где $a_{i-1} \neq a_i$, имеет не более k членов, и

(ii) *если a покрывает b_1 и b_2, то множество $\{b_1, b_2\}$ ограничено снизу в A.*

Тогда существует взаимно однозначное соответствие между связными компонентами графа множества A и минимальными элементами этого множества:

$$\Gamma_i \longleftrightarrow a_i \qquad (i \in I).$$

Если A_i — множество вершин из Γ_i, то $a_i \in A_i$ и на самом деле a_i является наименьшим элементом множества A_i.

Доказательство. Пусть Γ_i $(i \in I)$ — связные компоненты графа множества A, и A_i — соответствующие подмножества множества A. Из (i) следует прежде всего, что на самом деле A упорядочено (а не только предупорядочено) и что каждое A_i содержит минимальный элемент; далее, каждый минимальный элемент множества A_i будет, очевидно, минимальным в A. Если мы сможем показать, что A_i содержит только один минимальный элемент, то, так как в силу (i) каждый элемент больше или равен некоторому минимальному элементу, отсюда будет следовать, что единственный минимальный элемент множества A_i должен быть в то же время наименьшим элементом множества A_i.

Пусть поэтому a и b — минимальные элементы множества A_i. По определению множества A_i существует такая последовательность $a_0 = a$, $a_1, \ldots, a_n = b$, что $a_i \leqslant a_{i-1}$ или $a_i \geqslant a_{i-1}$ для любого $i = 1, \ldots, n$. Если $a \neq b$, то, опуская повторения, можно предполагать, что $a_i \neq a_{i-1}$, а, вставив, если нужно, дополнительные члены, можно считать (в силу (i)), что один из элементов a_i, a_{i-1} покрывает другой. Теперь для любого $x \in A$ обозначим через $h(x)$ максимум длин произвольных убывающих цепей, начинающихся с x; эта длина конечна в силу (i), и ясно, что если $x < y$, то $h(x) < h(y)$. Теперь воспользуемся двойной индукцией: (a) по $\max h(a_i)$ и (b) по числу элементов a_i, на которых этот максимум достигается. Если $\max h(a_i) = 0$, то все элементы a_i минимальны, и поэтому все равны; следовательно, $a = b$. Пусть теперь $\max h(a_i) > 0$ и предположим, что этот максимум достигается при $i=j$. Тогда a_j покрывает a_{j-1} и a_{j+1}; следовательно, в силу (ii) существует такое $c \in A$, что $c \leqslant a_{j-1}$, $c \leqslant a_{j+1}$. Поставив c вместо a_j и вставив дополнительные члены, как и раньше, получим последовательность (a'_k) от a до b, быть может, более длинную, чем прежняя, но в которой или $\max h(a'_k)$ имеет меньшее значение, чем $\max h(a_i)$, или оба максимума совпадают, но достигаются на меньшем числе элементов a'_k, чем элементов a_i. Это противоречит предположению индукции, и поэтому $a=b$. ∎

Заметим, что условие (i) значительно сильнее условия минимальности для A. В действительности этот результат все еще остается справедливым, если (i) заменить условием минимальности (см. Ньюмен [42]), но рассмотренный выше случай отвечает нашим целям.

УПРАЖНЕНИЯ

1. Показать, что любое пересечение упорядоченностей на произвольном множестве будет упорядоченностью.

2. (Хаусдорф.). Показать, что следующее предположение эквивалентно лемме Цорна: каждое упорядоченное множество содержит максимальную цепь (т. е. каждое упорядоченное множество A содержит цепь, максимальную в множестве всех цепей множества A, упорядоченном по включению).

3. Если направленное множество имеет максимальный элемент, то он будет и его наибольшим элементом. Вывести отсюда, что структура имеет не больше одного максимального элемента и не больше одного минимального элемента.

4. Привести пример монотонного гомоморфизма между структурами, не являющегося структурным гомоморфизмом.

5. Показать что упорядоченное множество частично вполне упорядочено тогда и только тогда, когда в нем нет бесконечных убывающих цепей и бесконечных вполне неупорядоченных подмножеств (см. § III. 2).

6. Пусть A — упорядоченное множество, в котором каждая цепь имеет не больше m элементов, а любое подмножество попарно несравнимых элементов состоит не более чем из n элементов. Показать, что A имеет не более mn элементов.

7. Пусть A — множество таких пар (m, n) натуральных чисел, что $m \leqslant n$. Упорядочим это множество по правилу: $(m, n) \leqslant (m', n')$ тогда и только тогда, когда $m \leqslant m'$ и $n = n'$, и обозначим через B дополнение множества $\{(0, 0)\}$ в A. Проверить, что A монотонно изоморфно левому отрезку множества B, а B монотонно изоморфно правому отрезку множества A, но A не изоморфно B.

8. Пусть L — полная структура и f — монотонный гомоморфизм структуры L в себя. Показать, что неподвижные точки гомоморфизма f снова образуют полную структуру по отношению к упорядоченности, индуцированной упорядоченностью в L. (Указание: пусть F — множество неподвижных точек; показать, что если $X \subseteq F$, то $\sup I$ совпадает с точной нижней гранью множества X в F, где

$$I = \{y \in L \mid y \leqslant yf \text{ и } y \leqslant x \text{ для всех } x \in X\},$$

и воспользоваться предложением 4.1.) Всегда ли эта структура будет подструктурой структуры L?

9. Проверить, что для любого упорядоченного множества A множество $\mathscr{S}(A)$ левых отрезков из A, упорядоченное по включению, будет полной структурой.

10. Пусть A — упорядоченное множество и для каждого $a \in A$ введем обозначение

$$S_a = \{x \in A \mid x \leqslant a\}.$$

Показать, что $a \to S_a$ определяет мономорфизм $A \to \mathscr{S}(A)$, сохраняющий упорядоченность. Вывести отсюда, что любое упорядоченное множество можно вложить в полную структуру так, чтобы сохранились точные верхние или точные нижние грани, которые существуют в A.

11. Показать, что предупорядоченность, определенная на множестве вершин графа Γ, будет упорядоченностью тогда и только тогда, когда Γ не содержит замкнутых путей, проходящих больше чем через одну вершину.

5. КАРДИНАЛЬНЫЕ И ПОРЯДКОВЫЕ ЧИСЛА

В этом параграфе мы сделаем короткий обзор тех фактов о кардинальных и порядковых числах, которые нам понадобятся, отсылая читателя за подробностями к работам Хаусдорфа [14], Келли [55] или Серпинского [58]. Если не оговорено противное, все множества мы будем считать элементами фиксированного, но произвольного универсального множества U.

Каждому упорядоченному множеству A сопоставим некоторый объект, называемый его *порядковым типом* и обозначаемый через $o(A)$, так, что

$o(A) = o(B)$ тогда и только тогда, когда A и B изоморфны как упорядоченные множества.

Подробнее это означает, что мы разбиваем класс всех упорядоченных множеств (в данном универсальном множестве U) на классы попарно изоморфных множеств и каждому классу сопоставляем элемент данного универсального множества U [1]).

Особенно важны следующие два случая:

(i) A — абстрактное множество, которое считается вполне неупорядоченным. В этом случае мы будем писать $|A|$ вместо $o(A)$ и называть $|A|$ *мощностью* или *кардинальным числом* множества A.

(ii) A — вполне упорядоченное множество. Тогда $o(A)$ называется *порядковым числом* множества A.

Вообще под *кардинальным числом* или *порядковым числом* понимают порядковый тип некоторого вполне неупорядоченного

---

[1]) Сам такой класс, вообще говоря, не будет элементом множества U и поэтому им нельзя воспользоваться.

множества или некоторого вполне упорядоченного множества соответственно. Определим теперь между порядковыми типами бинарное отношение, полагая

$o(A) \leqslant o(B)$ тогда и только тогда, когда A изоморфно левому отрезку множества B.

Легко проверить, что это отношение является предупорядоченностью (на классе порядковых типов, принадлежащих множеству U). В общем случае это отношение не будет упорядоченностью, что можно показать на примере множеств из упр. 4.7. Однако если ограничиться кардинальными числами или порядковыми числами, то мы получим упорядоченность, на самом деле даже линейную упорядоченность. Заметим сначала, что справедлива

Лемма 5.1. *Если A — упорядоченное множество с условием минимальности и $f\colon A \to A$ — монотонный взаимно однозначный гомоморфизм, то $xf \nless x$ для всех $x \in A$.*

Действительно, пусть существует такое $x \in A$, что $xf < x$, и пусть $a \in A$ — минимальный элемент с этим свойством. Так как $af < a$, то $af^2 < af$ и, следовательно, af также обладает этим свойством; но $af < a$, что противоречит определению a. ∎

В случае когда A вполне упорядочено, утверждение леммы состоит в том, что $xf \geqslant x$ для всех $x \in A$.

Теорема 5.2. *Если α и β — два кардинальных числа или два порядковых числа, причем $\alpha \leqslant \beta$ и $\beta \leqslant \alpha$, то $\alpha = \beta$.*

Для кардинальных чисел это вытекает из следствия 4.4. Если α, β — порядковые числа, скажем $\alpha = o(A)$, $\beta = o(B)$, то A монотонно изоморфно левому отрезку множества B, а B монотонно изоморфно левому отрезку множества A. Объединяя эти отображения, получаем монотонный изоморфизм $f\colon A \to A_0$ между множеством A и его левым отрезком, поэтому теорема будет доказана, если мы покажем, что $A_0 = A$. Предположим, что $A_0 \neq A$, и пусть $a \in A$, $a \notin A_0$; тогда $af < a$, так как из $af \geqslant a$ следовало бы, что $a \in A_0$ (поскольку $af \in A_0$). Но это противоречит лемме 5.1; следовательно, $A_0 = A$, и потому B изоморфно A, откуда $\beta = \alpha$. ∎

Покажем теперь, что упорядоченность порядковых чисел линейная.

Теорема 5.3. *Порядковые числа линейно упорядочены отношением $\leqslant$.*

Доказательство. Пусть A и B — вполне упорядоченные множества; для доказательства теоремы нужно только показать, что одно из множеств A или B монотонно изоморфно левому отрезку другого. Пусть R — множество всех функций, каждая из которых определяет монотонный изоморфизм некоторого левого отрезка множества A с некоторым левым отрезком множества B. Тогда R упорядочено по включению, и так как произвольное объединение левых отрезков множества A снова будет левым отрезком в A и аналогичное утверждение верно для B, то отсюда следует, что любая цепь в R имеет верхнюю грань (в самом деле, объединение такой цепи опять будет принадлежать R). По лемме Цорна, R обладает максимальным элементом f, который является функцией, определяющей монотонный изоморфизм между левым отрезком A_0 множества A и левым отрезком B_0 множества B. Конечно, на данном этапе не исключено, что $A_0 = B_0 = f = \varnothing$. Пусть одновременно $A_0 \neq A$ и $B_0 \neq B$, и пусть a — наименьший элемент множества A, не принадлежащий отрезку A_0, а b — наименьший элемент множества B, не принадлежащий отрезку B_0; тогда можно заменить f функцией $f \cup \{(a, b)\}$ и таким образом получить собственное расширение функции f, что противоречит ее максимальности. Следовательно, или $A_0 = A$, или $B_0 = B$ (или и то, и другое) и, соответственно этому, $o(A) \leqslant o(B)$ или $o(B) \leqslant o(A)$. ∎

Чтобы доказать соответствующее свойство для кардинальных чисел, нам потребуется

***Теорема* 5.4.** *Всякое множество можно вполне упорядочить.*

Доказательство. Пусть A — произвольное множество и W — совокупность всех его вполне упорядоченных подмножеств; таким образом, каждый элемент из W является подмножеством X множества A вместе с некоторой упорядоченностью множества X, которая превращает X во вполне упорядоченное множество. Для $X, Y \in W$ положим $X \leqslant Y$, если X является подмножеством множества Y, а вложение $X \to Y$ — монотонным изоморфизмом между множеством X и левым отрезком множества Y. В частности, это означает, что если $X \leqslant Y$, то упорядоченность на X совпадает с той, которую индуцирует упорядоченность на Y. Легко проверить, что так определенное отношение $\leqslant$ будет упорядоченностью на W. Далее, если $(C_i)_{i \in I}$ — некоторая цепь в W, то на множестве $D = \bigcup C_i$ существует упорядоченность, которая однозначно определяется тем, что она индуцирует на каждом C_i заданную упорядоченность. Более того, эта упорядоченность превращает D во вполне упорядоченное множество. Действительно, пусть $X \subseteq D$, $X \neq \varnothing$ и $x \in X$. Тогда $x \in C_i$ для некоторого $i \in I$; следовательно, $X \cap C_i \neq \varnothing$. Пусть a — наименьший элемент в $X \cap C_i$ (относительно упорядоченности, заданной на C_i); тогда a будет наименьшим элементом в $X \cap C_i$ также и относительно упорядоченности, определенной в D, и, следовательно, наименьшим элементом подмножества X в D, так как каждый элемент $y \in X$ должен лежать в C_i, если $y \leqslant a$. Таким образом, $D \in W$ и является верхней гранью цепи $(C_i)_{i \in I}$. По лемме Цорна в W существует максимальный элемент B. Пусть $B \neq A$ и пусть $c \in A$,

$c \notin B$; рассмотрим множество $B^* = B \cup \{c\}$ вместе с упорядоченностью, которая продолжает упорядоченность, заданную на B, и при которой $x < c$ для всех $x \in B$. Относительно этой упорядоченности B^* является вполне упорядоченным множеством, причем $B < B^*$, что противоречит максимальности B. Следовательно, $B = A$, т. е. A можно вполне упорядочить. ∎

***Следствие* 5.5.** *Кардинальные числа линейно упорядочены отношением* $\leqslant$.

Действительно, если A и B — некоторые множества, то по теореме 5.4 их можно вполне упорядочить, а применяя теорему 5.3, получим, что $o(A) \leqslant o(B)$ или $o(B) \leqslant o(A)$; таким образом, имеем $|A| \leqslant |B|$ или $|B| \leqslant |A|$. ∎

Из теоремы 5.3 и следствия 5.5 нетрудно вывести, что порядковые числа (так же как и кардинальные) вполне упорядочены отношением $\leqslant$. Это замечание приводит к другому определению порядковых чисел. Напомним, что порядковые числа были определены как порядковые типы вполне упорядоченных множеств. Мы получили бы более явный способ их определения, если бы для каждого порядкового типа выбрали определенное вполне упорядоченное множество и считали его представителем класса изоморфных вполне упорядоченных множеств. По существу, это делается так же, как при определении натуральных чисел в § I.1; тот же самый метод можно применить и здесь. Таким образом, мы получим все различные типы вполне упорядоченных множеств, если начнем с пустого множества, будем присоединять каждый раз по одному элементу и брать объединения возрастающих цепей. В частности, конечные порядковые числа совпадают с натуральными числами, а первым бесконечным порядковым числом будет множество

$$\{0,\ 1,\ 2,\ \ldots\},$$

обозначаемое обычно через ω. Мы не будем вдаваться в детали этой конструкции (см., например, Келли [55]), а заметим только, что если α — данное порядковое число, то порядковые числа, меньшие α, соответствуют, по определению, собственным левым отрезкам вполне упорядоченного множества типа α и сами они составляют вполне упорядоченное множество типа α. Каждому порядковому числу можно сопоставить кардинальное число $|\alpha|$, а именно кардинальное число вполне упорядоченного множества типа α. Это кардинальное число часто отождествляют с наименьшим порядковым числом, которому оно соответствует; однако кардинальное число множества N обычно обозначают через $\aleph_0$ (читается алеф-нуль). Множество мощности $\aleph_0$ называется также *счетным*. Существование несчетных множеств вытекает из следующей теоремы.

Теорема 5.6. *Для любого упорядоченного множества A, $o(A) \neq o(\mathscr{S}(A))$. Более того, если A вполне упорядочено, то*

$$o(A) < o(\mathscr{S}(A)),$$

а если A вполне неупорядочено, то

$$|A| < |\mathscr{B}(A)|.$$

Доказательство. Первое утверждение вытекает из теоремы 4.6, и чтобы закончить доказательство, нам нужно только показать, в силу следствий 4.7 и 4.8, что $o(A) \leqslant o(\mathscr{S}(A))$ и $|A| \leqslant |\mathscr{B}(A)|$. Таким образом, мы должны определить монотонный изоморфизм $f\colon A \to S_0$, где S_0 — левый отрезок множества $\mathscr{S}(A)$. Легко проверить, что для вполне упорядоченного множества A отображение f, определяемое равенством $af = \{x \in A \mid x < a\}$, будет таким монотонным изоморфизмом. Если A вполне неупорядочено, то положим $af = \{a\}$ и заметим, что это отображение определяет взаимно однозначное отображение множества A в $\mathscr{B}(A)$ и, следовательно, монотонный изоморфизм множества A с левым отрезком множества $\mathscr{B}'(A)$, где $\mathscr{B}'(A)$ — множество всех непустых подмножеств множества A. Таким образом, $o(A) \leqslant o(\mathscr{B}'(A))$ и поэтому $|A| \leqslant |\mathscr{B}'(A)| \leqslant |\mathscr{B}(A)|$. ∎

Следствие 5.7. *Среди порядковых чисел данного универсального множества (так же как и среди кардинальных чисел) нет наибольшего.* ∎

Иначе говоря, это следствие утверждает, что класс всех порядковых чисел (или класс всех кардинальных чисел) не является элементом данного универсального множества.

Если A и B — два произвольных множества мощностей α и β соответственно, то, как легко видеть, $|A \times B|$ зависит только от α и β, а не от самих A, B. Будем писать $|A \times B| = \alpha\beta$ и называть $\alpha\beta$ *произведением* кардинальных чисел α и β. Аналогично можно определить сумму $\alpha + \beta$ как $|A \cup B|$, где A, B — непересекающиеся множества мощностей α, β соответственно. Из свойств объединения и декартова произведения легко следует, что и для суммы, и для произведения справедливы законы коммутативности и ассоциативности. На основе этих определений можно развивать арифметику кардинальных чисел (см., например, Серпинский [58]); мы этого делать не будем, а только заметим, что для любых двух ненулевых кардинальных чисел, из которых по крайней мере одно бесконечно, справедливы равенства

$$\alpha + \beta = \alpha\beta = \max(\alpha, \beta),$$

(см. упр. 7 и 8). Здесь мы докажем второе равенство в частном случае, когда $\alpha = \aleph_0$, а β бесконечно.

***Предложение* 5.8.** *Для любого бесконечного кардинального числа* α

$$\aleph_0\alpha = \alpha. \qquad (1)$$

Доказательство. В случае, когда $\alpha = \aleph_0$, равенство (1) означает, что $N \times N$ равномощно N; это следует, например, из того, что можно перенумеровать пары (m, n) согласно значению $m+n$, а пары с одним и тем же значением $m+n$ перенумеровать согласно m. Далее, если α имеет вид $\aleph_0\gamma$, то по доказанному

$$\aleph_0\alpha = \aleph_0(\aleph_0\gamma) = \aleph_0^2\gamma = \aleph_0\gamma = \alpha,$$

откуда следует (1) для этого случая. Теперь доказательство будет завершено, если мы покажем, что каждое бесконечное кардинальное число можно представить в виде $\aleph_0\gamma$. Следовательно, нужно показать, что каждое бесконечное множество A равномощно произведению $N \times C$, где C — множество, выбранное подходящим образом. Пусть A бесконечно; тогда, по теореме 5.4, A может быть вполне упорядочено. Вполне упорядоченное множество можно считать линейно упорядоченным (на самом деле — вполне упорядоченным) множеством счетных последовательностей, за которым следует конечная (возможно, пустая) последовательность. Так как A бесконечно, то существует по крайней мере одна бесконечная последовательность, и мы можем перерасположить A, переставив конечную последовательность из конца в начало первой последовательности. Множество A теперь состоит только из счетных последовательностей, т. е. из вполне упорядоченных множеств, изоморфных множеству N; если эти множества заиндексированы множеством C, то отсюда следует, что A и $N \times C$ равномощны. ∎

В заключение этого параграфа сделаем замечание по поводу леммы Цорна, которое понадобится нам в дальнейшем. Предположение леммы Цорна относится к упорядоченному множеству A, в котором каждая цепь имеет верхнюю грань. Это предположение выполняется, в частности, если каждая цепь в A имеет точную верхнюю грань в A. Последнее условие можно сформулировать как в более слабой, так и в более сильной форме.

***Предложение* 5.9.** *Пусть A — упорядоченное множество; тогда следующие три условия эквивалентны:*

(i) *Каждое непустое направленное подмножество множества A имеет точную верхнюю грань.*

(ii) *Каждая непустая цепь множества A имеет точную верхнюю грань.*

(iii) *Каждая непустая вполне упорядоченная цепь множества A имеет точную верхнюю грань.*

В условии (iii) цепь считается вполне упорядоченной относительно упорядоченности, индуцированной из A. Заметим, что условие (iii) нужно только для упрощения доказательства эквивалентности условий (i) и (ii) и больше использоваться не будет.

Доказательство. Каждая вполне упорядоченная цепь является цепью, и каждая цепь направлена, следовательно, (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii); чтобы закончить доказательство, покажем, что (iii) $\Rightarrow$ (i). Таким образом, нужно показать, что если (iii) выполняется и D — непустое направленное подмножество множества A, то существует $\sup D$. Идея доказательства состоит в том, чтобы попытаться достичь $\sup D$ с помощью вполне упорядоченных цепей в D. Для этой цели нужно расширить D; этот шаг мы выделили в виде леммы.

Лемма. *Пусть A — упорядоченное множество, удовлетворяющее условию* (iii) *предложения* 5.9. *Пусть, далее, D — непустое направленное множество в A; тогда существует направленное множество E в A, обладающее следующими свойствами*:

(a) $E \supseteq D$.

(b) *Любая верхняя грань множества D является верхней гранью множества E.*

(c) *Каждая вполне упорядоченная цепь в E имеет точную верхнюю грань, снова принадлежащую множеству E.*

Для доказательства леммы рассмотрим множество направленных подмножеств из A, удовлетворяющих условиям (a) и (b). Такие подмножества существуют, например само D. Ясно, что объединение любой цепи направленных множеств, удовлетворяющих условиям (a) и (b), снова будет множеством того же вида; следовательно, по лемме Цорна существует максимальное направленное подмножество E в A, удовлетворяющее условиям (a) и (b). Мы утверждаем, что E удовлетворяет также и условию (c); если это не так, то пусть λ — такое наименьшее порядковое число, что точная верхняя грань некоторой вполне упорядоченной цепи в E длины λ не принадлежит E. Пусть E' — множество всех элементов вида $\sup(a_\mu)$, где $(a_\mu)_{\mu<\lambda}$ — произвольная вполне упорядоченная цепь длины λ в E. Тогда E' — направленное подмножество множества A, удовлетворяющее условиям (a) и (b).

Чтобы установить этот факт, возьмем произвольные a, $b \in E'$, скажем $a = \sup(a_\mu)$, $b = \sup(b_\mu)$ (a_μ, $b_\mu \in E$), и определим индуктивно такое семейство $(c_\mu)_{\mu<\lambda}$, что

$$c_{\mu'} \leqslant c_\mu \quad (\mu' < \mu), \quad a_\mu \leqslant c_\mu, \quad b_\mu \leqslant c_\mu, \quad c_\mu \in E \quad (\mu < \lambda). \tag{2}$$

В качестве c_0 возьмем произвольный элемент множества E, лишь бы $a_0 \leqslant c_0$, $b_0 \leqslant c_0$. Если α удовлетворяет неравенствам $0 < \alpha < \lambda$ и c_μ

определены для $\mu < \alpha$ так, что выполняются условия (2), то по предположению $c'_\alpha = \sup(c_\mu) \in E$, и так как E направлено, то существует такой элемент $c_\alpha \in E$, что

$$a_\alpha \leqslant c_\alpha, \quad b_\alpha \leqslant c_\alpha, \quad c'_\alpha \leqslant c_\alpha.$$

Это значит, что (2) выполняется для $\mu = \alpha$. По трансфинитной индукции получаем вполне упорядоченную цепь $(c_\mu)_{\mu < \lambda}$, удовлетворяющую (2) для каждого $\mu < \lambda$. Если $c = \sup(c_\mu)$, то $c \in E'$ и $c \geqslant a_\mu$, $c \geqslant b_\mu$ для всех $\mu < \lambda$; следовательно, $c \geqslant a$, $c \geqslant b$, откуда следует, что E' направлено. Кроме того, любой элемент $a \in E$ можно представить в виде $\sup(a_\mu)$, где $a_\mu = a$ для всех $\mu < \lambda$; отсюда

$$E \subseteq E'. \tag{3}$$

Далее, так как каждый элемент *множества* E' *является точной* верхней гранью семейства элементов в E, то каждая верхняя грань множества E является верхней гранью множества E', и потому в силу (b) каждая верхняя грань множества D будет верхней гранью множества E'. Таким образом, E' удовлетворяет (a) и (b); в силу *максимальности множества* E заключаем, что $E' = E$. Это означает, что каждая вполне упорядоченная цепь длины λ имеет точную верхнюю грань в E, что противоречит нашему предположению. Следовательно, E должно удовлетворять также условию (c), и лемма доказана.

Чтобы закончить доказательство теоремы, возьмем E, удовлетворяющее условиям леммы, и пусть (a_λ) — максимальная вполне упорядоченная цепь в E. Такие цепи существуют по лемме Цорна. Полагая $a = \sup(a_\lambda)$, имеем $a \in E$. Мы утверждаем, что $\sup D = a$; этим доказательство будет завершено. Прежде всего заметим, что a максимален в E, так как в противном случае мы могли бы расширить вполне упорядоченную цепь (a_λ), что противоречило бы ее максимальности. Так как E направлено, то на самом деле a будет *наибольшим элементом множества* E. Таким образом, a является верхней гранью для E и, следовательно, для D (потому что $D \subseteq E$). Если b — верхняя грань для D, то по построению b будет *также верхней* гранью для E, и потому $b \geqslant a$. Следовательно, a — наименьшая верхняя грань для D, т. е. $\sup D = a$. ∎

УПРАЖНЕНИЯ

1. Показать, что два конечных линейно упорядоченных множества монотонно изоморфны тогда и только тогда, когда они одной и той же мощности.

2. Показать, что линейно упорядоченное множество конечно тогда и только тогда, когда оно вполне упорядочено и относительно заданной упорядоченности, и относительно противоположной упорядоченности.

3. Пусть Ω — множество всех порядковых чисел в заданном универсальном множестве, вполне упорядоченное так, как было определено выше. По-

казать, что для любого $\alpha \in \Omega$ имеет место одно и только одно из следующих утверждений: (i) $\alpha = 0$; (ii) множество таких порядковых чисел β, что $\beta < \alpha$, имеет максимальный элемент (этот элемент называется *непосредственно предшествующим* элементу α); (iii) $\alpha \neq 0$ и $\alpha = \{\sup \beta \in \Omega \mid \beta < \alpha\}$ (в этом случае α называется *предельным порядковым числом*).

4. Если A, B — два непересекающихся упорядоченных множества, то определим их упорядоченную сумму $A + B$ как множество $A \cup B$, упорядоченное так, что $x \leqslant y$ для каждой пары (x, y) из $A \times B$, ни для какой пары из $B \times A$ и для пар из A^2 (или из B^2) тогда и только тогда, когда $x \leqslant y$ в A^2 (или в B^2). Теперь для любых порядковых типов α, β определим $\alpha + \beta$ как порядковый тип упорядоченной суммы $A + B$, где A, B — произвольные непересекающиеся упорядоченные множества типов α, β соответственно. Проверить, что $\alpha + \beta$ зависит только от α, β, а не от A, B и что в случае кардинальных чисел это определение превращается в определение, данное выше. Справедливы ли для этой операции законы коммутативности и ассоциативности?

5. Показать, что каждое порядковое число можно однозначно представить в виде $\lambda + n$, где λ — предельное порядковое число (упр. 3) или 0, а n — натуральное число.

6. Для произвольных упорядоченных множеств A и B определим их *лексикографическое произведение* как множество $A \times B$, упорядоченное по правилу: $(a, b) \leqslant (a', b')$ тогда и только тогда, когда или $a \leqslant a'$, или $a = a'$ и $b \leqslant b'$. Показать, что если A, B вполне упорядочены, то их лексикографическое произведение также вполне упорядочено. Для произвольных порядковых типов α, β определим $\alpha\beta$ как порядковый тип лексикографического произведения упорядоченных множеств A и B типов α и β соответственно. Проверить, что $\alpha\beta$ зависит только от α, β, а не от A, B и что для кардинальных чисел это определение превращается в определение, данное выше. Справедливы ли для этой операции законы коммутативности и ассоциативности?

7. Показать, что как сложение кардинальных чисел, так и умножение кардинальных чисел удовлетворяют законам коммутативности и ассоциативности. Показать также, что если $\alpha \leqslant \alpha'$, $\beta \leqslant \beta'$, то $\alpha + \beta \leqslant \alpha' + \beta'$ и $\alpha\beta \leqslant \alpha'\beta'$.

8. Показать, что если α, β — кардинальные числа, из которых по крайней мере одно бесконечно, то $\alpha + \beta = \max(\alpha, \beta)$. Предполагая, что для бесконечных кардинальных чисел справедливо равенство $\gamma^2 = \gamma$ (см. § VI.6), показать, что, кроме того, $\alpha\beta = \max(\alpha, \beta)$, если α, $\beta \neq 0$.

9. Множество A называется *плотно упорядоченным*, если оно линейно упорядочено и для любых a, $b \in A$, $a < b$, существует такое $c \in A$, что $a < c < b$. Показать, что существуют только четыре различных типа счетных плотно упорядоченных множеств. (Указание: показать, что любое счетное плотно упорядоченное множество монотонно изоморфно замкнутому, открытому или полуоткрытому интервалу рациональных чисел.)

10. Доказать теорему 5.3, не используя лемму Цорна. (Указание: применить трансфинитную индукцию.)

6. КАТЕГОРИИ И ФУНКТОРЫ

В алгебре, как и в топологии, часто приходится рассматривать множества с некоторым строением и с некоторыми отображениями между ними, сохраняющими данное строение. Существует ряд основных понятий, общих для всех таких ситуаций, и уместно определить их и в более общем случае.

Категорией $\mathscr{K}$ называется класс $\mathscr{K}$*-объектов* вместе с классом $\mathscr{K}$*-морфизмов*, которые связаны между собой следующим образом:

С.1. Каждой упорядоченной паре объектов a, b сопоставлено множество $\mathscr{K}$-морфизмов $\mathrm{Hom}(a, b)$, так что каждый $\mathscr{K}$-морфизм принадлежит $\mathrm{Hom}(a, b)$ только для одной пары объектов a, b.

С.2. Если $\alpha \in \mathrm{Hom}(a, b)$ и $\beta \in \mathrm{Hom}(b, c)$, то существует единственный элемент множества $\mathrm{Hom}(a, c)$, называемый *композицией* или *произведением* $\mathscr{K}$-морфизмов α и β и обозначаемый через $\alpha\beta$.

С.3. Если заданы $\alpha \in \mathrm{Hom}(a, b)$, $\beta \in \mathrm{Hom}(b, c)$, $\gamma \in \mathrm{Hom}(c, d)$, так что $(\alpha\beta)\gamma$ и $\alpha(\beta\gamma)$ определены, то

$$(\alpha\beta)\gamma = \alpha(\beta\gamma). \tag{1}$$

С.4. Каждому $\mathscr{K}$-объекту a сопоставлен такой $\mathscr{K}$-морфизм $\varepsilon_a \in \mathrm{Hom}(a, a)$, называемый *тождественным морфизмом*, что для любых $\alpha \in \mathrm{Hom}(b, a)$ и $\beta \in \mathrm{Hom}(a, c)$

$$\alpha\varepsilon_a = \alpha, \qquad \varepsilon_a\beta = \beta. \tag{2}$$

Классы всех $\mathscr{K}$-объектов и $\mathscr{K}$-морфизмов обозначаются также через $\mathrm{Ob}\,\mathscr{K}$ и $\mathrm{Hom}\,\mathscr{K}$ соответственно. Вместо $\alpha \in \mathrm{Hom}(a, b)$ пишут также α: $a \to b$ и говорят «α направлен из a в b»; далее для иллюстрации произведения морфизмов мы будем пользоваться коммутативными диаграммами так же, как для отображений между множествами. В связи с этим отметим, что для некоторых $\mathscr{K}$-морфизмов α: $a \to b$ и β: $c \to d$ произведение $\alpha\beta$ определено тогда и только тогда, когда $b = c$.

Легко проверить, что тождественный морфизм ε_a: $a \to a$ однозначно определен свойствами (2). Таким образом, отображение

$$a \to \varepsilon_a$$

устанавливает взаимно однозначное соответствие между $\mathrm{Ob}\,\mathscr{K}$ и классом тождественных морфизмов, так что категория $\mathscr{K}$ полностью определяется своими морфизмами. Нетрудно дать определение категории только в терминах морфизмов (см. упр. 1); мы не примем этой точки зрения, но отметим возможность такого подхода, так как им можно воспользоваться для сокращения некоторых определений.

Говорят, что категория $\mathscr{K}$ обладает *нулем*, если

С.5. Существует такой $\mathscr{K}$-объект 0, называемый *нулевым объектом*, что для любого $a \in \mathrm{Ob}\,\mathscr{K}$ каждое из множеств $\mathrm{Hom}(a, 0)$ и $\mathrm{Hom}(0, a)$ состоит из одного единственного элемента.

В категории с нулем через ω_{0a} обозначим единственный морфизм в $\mathrm{Hom}(0, a)$, через ω_{a0} — единственный морфизм в $\mathrm{Hom}(a, 0)$ и вообще определим *нулевой морфизм* из a в b равенством

$$\omega_{ab} = \omega_{a0}\omega_{0b}; \tag{3}$$

тогда для любых морфизмов α: $c \to a$, β: $b \to d$ имеем $\alpha\omega_{a0} = \omega_{c0}$, $\omega_{0b}\beta = \omega_{0d}$ и, следовательно,

$$\alpha\omega_{ab} = \omega_{cb}, \qquad \omega_{ab}\beta = \omega_{ad}. \tag{4}$$

Хотя категория может иметь больше одного нулевого объекта, нулевой морфизм однозначно определен равенствами (4). Действительно, если ω'_{ab}: $a \to b$ — другой нулевой морфизм, определенный по отношению к другому нулевому объекту $0'$, то в силу (4) $\omega_{cb} = \omega_{ca}\omega'_{ab} = \omega'_{cb}$.

ПРИМЕРЫ КАТЕГОРИЙ

(i) Все непустые множества в данном универсальном множестве и все отображения между ними образуют категорию, обозначаемую через St*.

(ii) Все множества в данном универсальном множестве и все отображения между ними, включая для каждого множества B отображение $\varnothing \to B$, определяемое пустой функцией $\varnothing$. Эта категория обозначается через St.

(iii) Категория всех групп и гомоморфизмов.

(iv) Категория всех топологических пространств и непрерывных отображений.

(v) Категория всех упорядоченных множеств и монотонных гомоморфизмов.

(vi) Категория всех структур и всех структурных гомоморфизмов.

Изоморфизмом между категориями $\mathscr{K}$ и $\mathscr{K}'$ называется такое взаимно однозначное соответствие $\alpha \to \alpha'$ между $\mathrm{Hom}\,\mathscr{K}$ и $\mathrm{Hom}\,\mathscr{K}'$, что $\alpha\beta$ определено тогда и только тогда, когда определено $\alpha'\beta'$, и в этом случае

$$(\alpha\beta)' = \alpha'\beta'. \tag{5}$$

Отсюда следует, что тождественные морфизмы соответствуют друг другу и, следовательно, $\mathscr{K}$-объекты соответствуют $\mathscr{K}'$-объектам. Точнее, если $a \in \mathrm{Ob}\,\mathscr{K}$, то ε'_a — тождественный морфизм. Действительно, в силу (2) и (5) $\varepsilon_a^2 = \varepsilon_a$, откуда $\varepsilon'^2_a = \varepsilon'_a$, так что если ε'_a: $u \to v$, то $v = u$, а если η_u — тождественный морфизм объекта u, а $\lambda \in \mathrm{Hom}\,\mathscr{K}$ — такой морфизм, что $\lambda' = \eta_u$, то $\varepsilon_a\lambda = \lambda$; следовательно,

$$\eta_u = \varepsilon'_a\eta_u = \varepsilon'_a.$$

Полагая $u=a'$, получаем такое взаимно однозначное соответствие $a\to a'$ между Ob $\mathscr{K}$ и Ob $\mathscr{K}'$, что α: $a\to b$ тогда и только тогда, когда α': $a'\to b'$.

Антиизоморфизмом из $\mathscr{K}$ в $\mathscr{K}'$ называется такое взаимно однозначное соответствие между Hom $\mathscr{K}$ и Hom $\mathscr{K}'$: $\alpha\to\alpha'$, что $\alpha\beta$ определено тогда и только тогда, когда определено $\beta'\alpha'$ и

$$(\alpha\beta)'=\beta'\alpha'. \tag{6}$$

И снова этим установлено взаимно однозначное соответствие между Ob $\mathscr{K}$ и Ob $\mathscr{K}'$, скажем $a\to a'$, притом такое, что α: $a\to b$ тогда и только тогда, когда α': $b'\to a'$.

С каждой категорией $\mathscr{K}$ можно связать категорию $\mathscr{K}^\circ$, *двойственную* к $\mathscr{K}$, морфизмами которой являются те же $\mathscr{K}$-морфизмы, но с умножением

$$\alpha*\beta=\beta\alpha,$$

определенным всякий раз, как определена правая часть равенства. Отсюда следует, что $\mathscr{K}^\circ$ антиизоморфна $\mathscr{K}$. Вообще категория $\mathscr{L}$ антиизоморфна $\mathscr{K}$ тогда и только тогда, когда $\mathscr{L}$ изоморфна $\mathscr{K}^\circ$.

Понятие изоморфизма между категориями является частным случаем понятия функтора. Под *функтором* из категории $\mathscr{K}$ в категорию $\mathscr{L}$ понимают такую пару отображений Ob $\mathscr{K}$ в Ob $\mathscr{L}$ и Hom $\mathscr{K}$ в Hom $\mathscr{L}$, обозначаемых для простоты одной и той же буквой, скажем F, что

(i) $(\varepsilon_a)F=\varepsilon_{aF}$.

(ii) Если $\alpha\beta$ определено в $\mathscr{K}$, то $(\alpha F)(\beta F)$ определено в $\mathscr{L}$ и

$$(\alpha\beta)F=(\alpha F)(\beta F).$$

Точнее, так определенный функтор называется *ковариантным*; под *контравариантным* функтором из $\mathscr{K}$ в $\mathscr{L}$ понимают ковариантный функтор из $\mathscr{K}$ в $\mathscr{L}^\circ$, или, что эквивалентно, из $\mathscr{K}^\circ$ в $\mathscr{L}$.

Подкатегория $\mathscr{L}$ категории $\mathscr{K}$ состоит из такого подкласса класса Ob $\mathscr{K}$ и такого подкласса класса Hom $\mathscr{K}$, обозначаемых через Ob $\mathscr{L}$ и Hom $\mathscr{L}$ соответственно, что

(i) Если $a\in$ Ob $\mathscr{L}$, то $\varepsilon_a\in$ Hom $\mathscr{L}$.

(ii) Если α, $\beta\in$ Hom $\mathscr{L}$ и $\alpha\beta$ определено в $\mathscr{K}$, то $\alpha\beta\in$ Hom $\mathscr{L}$.

(iii) Если $\alpha\in$ Hom $\mathscr{L}$ и α: $a\to b$, то a, $b\in$ Ob $\mathscr{L}$.

Если a, $b\in$ Ob $\mathscr{L}$, то часто пишут $\mathrm{Hom}_{\mathscr{L}}(a, b)$ вместо $\mathrm{Hom}_{\mathscr{K}}(a, b)\cap$ Hom $\mathscr{L}$. Подкатегория $\mathscr{L}$ категории $\mathscr{K}$ называется *полной*, если $\mathrm{Hom}_{\mathscr{L}}(a, b)=\mathrm{Hom}_{\mathscr{K}}(a, b)$ для любых a, $b\in$ Ob $\mathscr{L}$. Таким образом, полная подкатегория категории $\mathscr{K}$ полностью определена, как только задан класс ее объектов; например, абелевы группы и гомоморфизмы образуют полную подкатегорию категории групп и гомоморфизмов. Структуры и структурные гомоморфизмы образуют подкатегорию категории упорядоченных множеств и гомоморфизмов между ними, которая, однако, не полна, как мы видели в § I.4.

Пусть $\mathcal{K}$ — произвольная категория; тогда $\mathcal{K}$-морфизм α: $a \to b$ называется *обратимым* или *эквивалентностью*, если существует такой $\mathcal{K}$-морфизм β: $b \to a$, что $\alpha\beta = \varepsilon_a$, $\beta\alpha = \varepsilon_b$. Легко видеть, что если такой морфизм β существует, то он определяется однозначно морфизмом α. Этот морфизм обозначается через α^{-1} и называется *обратным* к α. Два $\mathcal{K}$-объекта a и b называются *эквивалентными*: $a \sim b$, если существует эквивалентность α: $a \to b$. Так, например, два произвольных нулевых объекта категории с нулем эквивалентны.

Пусть заданы две категории $\mathcal{K}$, $\mathcal{L}$ и два функтора F, G из $\mathcal{K}$ в $\mathcal{L}$. Тогда *естественным преобразованием* функторов τ: $F \to G$ называется функция, сопоставляющая каждому $a \in \mathrm{Ob}\,\mathcal{K}$ такой $\mathcal{L}$-морфизм $\tau(a)$: $aF \to aG$, что для произвольного α: $a \to b$ следующая диаграмма коммутативна:

$$\begin{tikzcd} aF \arrow[r, "\alpha F"] \arrow[d, "\tau(a)"'] & bF \arrow[d, "\tau(b)"] \\ aG \arrow[r, "\alpha G"'] & bG \end{tikzcd}$$

Если $\tau(a)$ является $\mathcal{L}$-эквивалентностью для каждого $a \in \mathrm{Ob}\,\mathcal{K}$, то τ называется *естественной эквивалентностью*. В частности, если $\mathcal{L} = \mathcal{K}$ и F — тождественный функтор, то естественным преобразованием будет такой $\mathcal{K}$-морфизм $\tau(a)$, для которого приведенная выше диаграмма коммутативна. Этот случай будет наиболее часто встречаться в дальнейшем. В качестве простой иллюстрации рассмотрим обычную конструкцию поля частных области целостности как функтор из категории областей целостности и мономорфизмов в категорию полей и гомоморфизмов. Можно проверить, что вложение области целостности в его поле частных будет естественным преобразованием. Это не будет выполняться, если взять в качестве наших категорий области целостности со всеми гомоморфизмами между ними и поля с их гомоморфизмами соответственно; в этом случае, чтобы получить функтор, нужно расширить последнюю категорию до категории всех полей и «точек» (см. Ленг [58]).

УПРАЖНЕНИЯ

1. Показать, что $\mathrm{Hom}\,\mathcal{K}$ для произвольной категории $\mathcal{K}$ удовлетворяет следующим условиям:

(i) Для некоторых упорядоченных пар α, $\beta \in \mathrm{Hom}\,\mathcal{K}$ определен элемент $\alpha\beta \in \mathrm{Hom}\,\mathcal{K}$.

(ii) Если $\alpha\beta$ и $\beta\gamma$ определены, то $(\alpha\beta)\gamma$ и $\alpha(\beta\gamma)$ определены и равны. Более того, $\beta\gamma$ определено всякий раз, как определено $(\alpha\beta)\gamma$ для некоторого α или определено $\beta(\gamma\delta)$ для некоторого δ.

(iii) Каждый элемент класса $\operatorname{Hom}\mathcal{K}$ имеет левую единицу и правую единицу. (Элемент $\varepsilon \in \operatorname{Hom}\mathcal{K}$ называется *левой* (*правой*) *единицей* для α, если $\varepsilon\alpha$ $(\alpha\varepsilon)$ определено, и $\varepsilon\beta = \beta$, $\gamma\varepsilon = \gamma$ всякий раз, когда левые стороны определены.)

Показать, что и обратно, любой класс, удовлетворяющий этим условиям, образует класс морфизмов некоторой категории.

2. Пусть $\mathcal{S}_U$ — категория всех множеств и отображений в данном универсальном множестве U. Показать, что подкатегории категории $\mathcal{S}_U$ с функторами в качестве морфизмов образуют категорию.

3. Категория называется *двойственной самой себе*, если она изоморфна своей двойственной категории. Показать, что категория всех множеств и соответствий между ними (в данном универсальном множестве) двойственна самой себе.

4. (a) Показать, что в категории всех множеств и отображений отображение α взаимно однозначно тогда и только тогда, когда оно обладает правым обратным (т. е. если α: $a \to b$, то существует такое β: $b \to a$, что $\alpha\beta = \varepsilon_a$), и будет отображением на тогда и только тогда, когда оно обладает левым обратным (т. е. существует такое γ: $b \to a$, что $\gamma\alpha = \varepsilon_b$).

(b) Показать, что для любого отображения α следующие условия эквивалентны: (i) α обратимо, (ii) α обладает единственным правым обратным, (iii) α обладает единственным левым обратным, (iv) α обладает правым обратным и левым обратным.

5. Показать, что в полугруппе S_P отображений бесконечного множества P в себя справедливы следующие утверждения:

(a) Если отображение имеет больше одного правого обратного, то оно имеет бесконечно много правых обратных.

(b) Существует отображение, имеющее только два различных левых обратных.

Вывести отсюда, что S_P как категория не является двойственной самой себе. Будет ли S_P двойственной себе, если P конечно?

6. Пусть $\mathcal{K}$ — произвольная категория; $\mathcal{K}$-морфизм μ называется *мономорфизмом*, если $\alpha\mu = \beta\mu$ влечет $\alpha = \beta$. Если μ: $b \to a$ есть $\mathcal{K}$-мономорфизм, то b называется *подобъектом* объекта a с $\mathcal{K}$-морфизмом μ. Показать, что подобъекты объекта a предупорядочены по правилу: $c \leqslant b$, если ν: $c \to a$ и μ: $b \to a$ — данные мономорфизмы и $\nu = \alpha\mu$ для некоторого α. Показать также, что $c \leqslant b$ и $b \leqslant c$ тогда и только тогда, когда $b \sim c$. Двойственным образом определить *факторобъекты* объекта a в терминах эпиморфизмов и доказать для них соответствующие утверждения.

7. Пусть $\mathcal{K}$ — произвольная категория. Для a, $b \in \operatorname{Ob}\mathcal{K}$ будем писать $a \leqslant b$ тогда и только тогда, когда $\operatorname{Hom}(a, b) \neq \varnothing$. Показать, что так определенное отношение будет предупорядоченностью на $\operatorname{Ob}\mathcal{K}$.

ГЛАВА II

АЛГЕБРЫ

Алгеброй на множестве A по существу является совокупность конечноместных операций на A. Большинство понятий, введенных для множеств, такие, как подмножество, отображение, эквивалентность, имеют аналоги для алгебр, а именно подалгебра, гомоморфизм, конгруэнция. Теоремам об отображениях из § I.3 соответствуют теперь теоремы об изоморфизмах, которые, вероятно, лучше всего известны в случае групп. Аналогия оказывается менее полной для теорем Жордана — Гёльдера и Крулля — Шмидта, которые поэтому рассматриваются сначала в их абстрактном виде в теории структур, а затем для алгебр.

Кроме того, важную роль играет множество подалгебр данной алгебры и в меньшей степени множество всех конгруэнций; они образуют полные структуры с некоторыми характерными свойствами, от которых зависит применимость леммы Цорна. Мы начнем поэтому с абстрактного изучения этих свойств.

1. СИСТЕМЫ ЗАМЫКАНИЙ

Пусть A — произвольное множество и $\mathscr{B}(A)$ — его булеан, т. е. множество всех его подмножеств. Мы хотим рассматривать некоторые подмножества булеана $\mathscr{B}(A)$, или, как мы будем говорить, *системы* подмножеств множества A. Система $\mathscr{C}$ подмножеств множества A называется *системой замыканий*, если система $\mathscr{C}$ замкнута относительно пересечений, т. е.

$$\bigcap \mathscr{D} \in \mathscr{C} \text{ для любой подсистемы } \mathscr{D} \subseteq \mathscr{C}.$$

В частности, взяв $\mathscr{D} = \varnothing$, видим, что A всегда принадлежит $\mathscr{C}$. Так как система замыканий замкнута относительно произвольных пересечений, то из предложения I. 4.1 следует, что система замыканий является полной структурой (относительно упорядоченности по включению). Однако это не обязательно подструктура в $\mathscr{B}(A)$, так как операция объединения в $\mathscr{C}$, вообще говоря, отлична от этой операции в $\mathscr{B}(A)$ (см. примеры ниже).

Наиболее важными примерами систем замыканий являются следующие:

(i) Система всех подгрупп группы G является системой замыканий. Этот случай позднее будет обобщен.

(ii) Пусть X — топологическое пространство и $\mathscr{T}$ — система его замкнутых подмножеств. Тогда $\mathscr{T}$ будет системой замыканий со следующим дополнительным свойством:

$$A \cup B \in \mathscr{T} \text{ для любых } A,\ B \in \mathscr{T}. \tag{1}$$

Таким образом, $\mathscr{T}$ — подструктура в $\mathscr{B}(X)$, хотя в общем случае и не полная. Прозвольная система замыканий, удовлетворяющая условию (1), называется *топологической*. Если задана топологическая система замыканий $\mathscr{T}$ на множестве X, которая, кроме того, содержит $\varnothing$, то можно определить на X топологию, объявив элементы системы $\mathscr{T}$ замкнутыми множествами. Конечно, полученная топология, вообще говоря, не будет отделимой.

Вторым понятием, которое нам нужно и которое, как будет выяснено, эквивалентно понятию системы замыканий, является понятие оператора замыкания на множестве. *Оператором замыкания* на множестве A называется отображение J множества $\mathscr{B}(A)$ в себя, обладающее следующими свойствами:

J. 1. Если $X \subseteq Y$, то $J(X) \subseteq J(Y)$,
J. 2. $X \subseteq J(X)$,
J. 3. $JJ(X) = J(X)$

для всех $X,\ Y \in \mathscr{B}(A)$. Для каждой системы замыканий $\mathscr{C}$ можно определить оператор замыкания J равенством

$$J(X) = \bigcap \{Y \in \mathscr{C} \mid Y \supseteq X\}. \tag{2}$$

Этот оператор удовлетворяет условиям J. 1—2 по определению. Далее имеем

$$J(X) = X \textit{ тогда и только тогда, когда } X \in \mathscr{C}, \tag{3}$$

поскольку $\mathscr{C}$ — система замыканий; так как $J(X) \in \mathscr{C}$, то этим доказано J. 3.

Обратно, если задан оператор замыкания J (удовлетворяющий J. 1—3), то положим

$$\mathscr{C} = \{X \subseteq A \mid J(X) = X\}. \tag{4}$$

Если $(X_i)_{i \in I}$ — произвольное семейство в $\mathscr{C}$ и $\bigcap X_i = X$, то $X \subseteq X_i$; следовательно, по J. 1, $J(X) \subseteq J(X_i) = X_i$ для всех i, и поэтому

$$J(X) \subseteq \bigcap X_i = X.$$

Вместе с условием J. 2 это показывает, что $J(X)=X$, т. е. $X\in\mathscr{C}$. Таким образом, с помощью J мы построили систему замыканий $\mathscr{C}$, причем сделали это, не использовав условие J. 3. Воспользуемся теперь этим условием и покажем, что соответствие $\mathscr{C}\to J$ взаимно однозначно.

Во-первых, пусть $\mathscr{C}$ — произвольная система замыканий, J — оператор, определенный равенством (2), и $\mathscr{C}'$ — система замыканий, определенная оператором J по формуле (4). Тогда $\mathscr{C}'=\mathscr{C}$ в силу (3). Возьмем затем произвольный оператор замыкания J, и пусть $\mathscr{C}$ — система замыканий, определенная оператором J по формуле (4), а J' — оператор, определенный системой $\mathscr{C}$ по формуле (2). Как только что было показано, $\mathscr{C}$ тогда также определяется оператором J', и, следовательно,

$$J(X)=X \text{ тогда и только тогда, когда } J'(X)=X. \tag{5}$$

В силу J. 3, $JJ(X)=J(X)$; поэтому из (5) вытекает, что $J'J(X)=J(X)$. Но $X\subseteq J(X)$ и, применяя J', получаем $J'(X)\subseteq \subseteq J'J(X)=J(X)$, а обратное включение следует из соображений симметрии. Таким образом, доказана

Теорема 1.1. *Каждая система замыканий $\mathscr{C}$ на множестве A определяет оператор замыкания J на A по правилу*

$$J(X)=\bigcap\{Y\in\mathscr{C}\mid Y\supseteq X\}.$$

Обратно, каждый оператор замыкания J на A определяет систему замыканий

$$\mathscr{C}=\{X\subseteq A\mid J(X)=X\},$$

и так определенное соответствие $\mathscr{C}\longleftrightarrow J$ между системами замыканий и операторами замыкания взаимно однозначно. ∎

Отметим, что системы замыканий и операторы замыкания могут быть определены на любой полной структуре L и соотношения между ними, установленные в теореме 1.1, сохраняются; в действительности теорема 1.1 является просто частным случаем соответствующей теоремы при $L=\mathscr{B}(A)$ для произвольной полной структуры L.

Элементы системы $\mathscr{C}$ называются *$\mathscr{C}$-множествами* или *замкнутыми множествами* множества A, а $J(X)$ называется *замыканием* множества X в A ($J(X)$ на самом деле замкнуто в силу J. 3). Как было отмечено, $\mathscr{C}$ является полной структурой относительно $\subseteq$. Точнее, если задано некоторое семейство $(X_i)_{i\in I}$ в $\mathscr{C}$, то множество $\bigcap X_i$ будет наибольшим замкнутым множеством, содержащимся во всех множествах X_i, а $\bigcap\{Y\in\mathscr{C}\mid Y\supseteq X_i$ для всех $i\in I\}$ — наименьшим замкнутым множеством, содержащим все множества X_i.

Дадим теперь третий пример системы замыканий, который будет важен в дальнейшем.

Пусть A и B — некоторые множества и Φ — соответствие из A в B, т. е. подмножество произведения $A \times B$. Для любого подмножества X множества A определим подмножество X^* множества B равенством

$$X^* = \{y \in B \mid (x, y) \in \Phi \quad \text{для всех} \quad x \in X\}$$

и аналогично для любого подмножества Y множества B определим подмножество Y^* множества A равенством

$$Y^* = \{x \in A \mid (x, y) \in \Phi \quad \text{для всех} \quad y \in Y\}.$$

Таким образом, имеем отображения

$$X \to X^*, \qquad Y \to Y^* \tag{6}$$

множеств $\mathscr{B}(A)$, $\mathscr{B}(B)$ друг в друга, обладающие следующими свойствами:

$$\left.\begin{array}{lll} \text{если} & X_1 \subseteq X_2, & \text{то} \quad X_1^* \supseteq X_2^*, \\ \text{если} & Y_1 \subseteq Y_2, & \text{то} \quad Y_1^* \supseteq Y_2^*, \end{array}\right\} \tag{7}$$

$$X \subseteq X^{**}, \quad Y \subseteq Y^{**}, \tag{8}$$

$$X^{***} = X^*, \quad Y^{***} = Y^*. \tag{9}$$

Условия (7) и (8) вытекают непосредственно из определений; если (7) применить к (8), получаем $X^* \supseteq X^{***}$, в то время как (8), примененное к X^*, дает обратное неравенство. Таким образом, любые отображения (6), удовлетворяющие (7) и (8), удовлетворяют также (9).

Пара отображений (6) между $\mathscr{B}(A)$ и $\mathscr{B}(B)$, или в более общем случае между любыми упорядоченными множествами, называется *соответствием Галуа*, если выполняются условия (7), (8) (и, следовательно, (9)). Большинство встречающихся в практике соответствий Галуа возникает из соответствий между множествами описанным выше способом (см. также работу Оре [44]).

ПРИМЕРЫ СООТВЕТСТВИЙ ГАЛУА

(i) Пусть F — (коммутативное) поле и G — группа всех автоморфизмов поля F. Тогда пары $(x, \alpha) \in F \times G$, для которых $x^\alpha = x$, образуют соответствие, устанавливающее соответствие Галуа между некоторыми подполями поля F и некоторыми подгруппами группы G. Если G — группа не всех автоморфизмов поля F, а только конечная группа автоморфизмов поля F и E — подполе поля F, состоящее из элементов, остающихся неподвижными при G, то это соответствие будет соответствием между всеми подгруппами группы G и всеми подполями поля F, содержащими подполе E. (Этот случай рассматривается в теории Галуа, откуда и получили свое название соответствия Галуа.)

(ii) Пусть A — простая (конечномерная линейная ассоциативная) алгебра. Рассмотрим соответствие из A в себя, определенное соотношением $xy = yx$. Это соответствие устанавливает соответствие Галуа множества подалгебр алгебры A с самим собой (см. Артин, Несбит и Тролл [44]).

(iii) Пусть R — коммутативное кольцо с единицей. Определим соответствие в R правилом $x \neq y$. Это соответствие устанавливает, в частности, соответствие Галуа между простыми идеалами кольца R и некоторыми мультипликативно замкнутыми подмножествами кольца R (см. Зарисский и Самюэль [58]).

Чтобы установить связь соответствий Галуа с системами замыканий, заметим, что при любом соответствии Галуа отображение $X \to X^{**}$ будет оператором замыкания в A, а $Y \to Y^{**}$ будет оператором замыкания в B (в силу (7) — (9)). Более того, отображения (6) определяют взаимно однозначное соответствие между этими двумя системами замыканий.

Оператор замыкания J на множестве A называется *алгебраическим*, если для любых $X \subseteq A$ и $a \in A$

$a \in J(X)$ влечет $a \in J(X_f)$ для некоторого конечного подмножества X_f множества X.

Теперь система замыканий называется *алгебраической*, если только соответствующий оператор замыкания является алгебраическим. Чтобы иметь более непосредственное описание алгебраических систем замыканий, нам необходимо еще одно определение. Непустая система $\mathscr{C}$ подмножеств множества A называется *индуктивной*, если каждая цепь в $\mathscr{C}$ обладает точной верхней гранью в $\mathscr{C}$. В силу предложения I.5.9 (примененного к $\mathscr{B}(A)$) слово «цепь» здесь можно заменить словами «направленное множество». Теперь мы имеем следующую характеризацию алгебраических систем замыканий, принадлежащую Ю. Шмидту [52]:

***Теорема* 1.2.** *Система замыканий является алгебраической тогда и только тогда, когда она индуктивна.*

Доказательство. Пусть $\mathscr{C}$ — алгебраическая система замыканий на некотором множестве, $\mathscr{K}$ — цепь в $\mathscr{C}$ и $K = \sup \mathscr{K}$. Для доказательства включения $K \in \mathscr{C}$ нужно только проверить, что $J(K_f) \subseteq K$ для каждого конечного подмножества K_f множества K. Пусть $K_f = \{x_1, \ldots, x_n\}$; тогда каждое x_i принадлежит некоторому члену цепи $\mathscr{K}$, а так как $\mathscr{K}$ — цепь, то можно найти член $L \in \mathscr{K}$, содержащий все x_i. Тогда $K_f \subseteq L \subseteq K$ и $L \in \mathscr{C}$; следовательно, $J(K_f) \subseteq J(L) = L \subseteq K$, т. е. $J(K_f) \subseteq K$, что мы и хотели показать.

Обратно, пусть $\mathscr{C}$ — индуктивная система замыканий на A и J — соответствующий оператор замыкания. Нужно показать, что для любого $X \subseteq A$

$$J(X) = \sup \{J(X_f) \mid X_f \subseteq X,\ X_f \text{ конечно}\}.$$

Пусть $\mathscr{K} = \{J(X_f) \mid X_f \subseteq X,\ X_f \text{ конечно}\}$ для фиксированного $X \subseteq A$; тогда нужно показать, что $\sup \mathscr{K} \in \mathscr{C}$. Отсюда будет следовать, что $\sup \mathscr{K} = J(X)$, поскольку $\sup \mathscr{K}$ является наименьшим замкнутым множеством, содержащим все элементы множества X. Теперь для любых $Y,\ Z \subseteq A$ имеем

$$J(Y) \cup J(Z) \subseteq J(Y \cup Z),$$

и если $Y,\ Z$ — конечные подмножества множества X, то $Y \cup Z$ также конечно. Это показывает, что $\mathscr{K}$ направлено, и, следовательно, $\sup \mathscr{K} \in \mathscr{C}$, что и утверждалось. ∎

Используя предложение I.5.9, получаем

***Следствие* 1.3.** *Если $\mathscr{C}$ — алгебраическая система замыканий на A и $\mathscr{K}$ — направленная подсистема системы $\mathscr{C}$, то $\sup \mathscr{K} \in \mathscr{C}$.* ∎

Из леммы Цорна вытекает, что каждая непустая индуктивная система подмножеств множества A содержит максимальное подмножество. Это приводит к следствию из теоремы 1.2, в котором содержатся наиболее важные применения леммы Цорна к алгебре.

***Теорема* 1.4.** *Пусть $\mathscr{C}$ — алгебраическая система замыканий в A, и пусть $A_0,\ A_1,\ B$ — такие подмножества множества A, что $B \in \mathscr{C}$ и $B \cap A_1 = A_0$. Тогда $\mathscr{C}$ содержит элемент C, который является максимальным в $\mathscr{C}$ относительно свойств $C \supseteq B$, $C \cap A_1 = A_0$.*

Для доказательства этого утверждения возьмем систему $\mathscr{C}'$ всех таких множеств $X \in \mathscr{C}$, что $X \supseteq B$ и $X \cap A_1 = A_0$, и покажем, что $\mathscr{C}'$ обладает максимальным элементом. Во-первых, $\mathscr{C}' \neq \varnothing$, так как $B \in \mathscr{C}'$. Пусть теперь (X_i) — некоторая цепь в $\mathscr{C}'$ и положим $X = \sup X_i$. Тогда $X \in \mathscr{C}$, так как система $\mathscr{C}$ индуктивна. Далее, $X \supseteq B$ и $X \cap A_1 = A_0$; поэтому $X \in \mathscr{C}'$. Таким образом, система $\mathscr{C}'$ индуктивна, и по лемме Цорна $\mathscr{C}'$ обладает максимальным элементом. ∎

УПРАЖНЕНИЯ

1. Пусть $X \to H(X)$ — произвольное отображение множества $\mathscr{B}(A)$ в себя. Показать, что $J(X) = H(X) \cup X$ определяет оператор замыкания тогда и только тогда, когда $X \subseteq J(Y)$ влечет $J(X) \subseteq J(Y)$.

2. Пусть J_0 — некоторое отображение множества $\mathscr{B}(A)$ в себя, удовлетворяющее условию J. 1; определим $J_1(X) = J_0(X) \cup X$. Проверить, что J_1 удовлетворяет J. 1 и J. 2, и если $\mathscr{C}$ — система замыканий, соответствующая J_1, то описать оператор замыкания J, соответствующий $\mathscr{C}$.

3. Показать, что совокупность всех алгебраических систем замыканий на данном множестве A является системой замыканий на $\mathscr{B}(A)$. Всегда ли эта система замыканий будет алгебраической?.

4. Пусть $\mathscr{C}$ — алгебраическая система замыканий на A. Тогда каждая непустая подсистема системы $\mathscr{C}$ имеет максимальный элемент тогда и только тогда, когда каждое множество $X \in \mathscr{C}$ является замыканием конечного подмножества.

5. (Хигмэн.) Пусть Γ — множество всех систем замыканий на A. Определим операцию $\mathscr{C} \to \mathscr{C}^*$ на Γ равенством

$$J_{\mathscr{C}^*}(X) = \bigcup \{J_{\mathscr{C}}(X_f) \mid X_f \subseteq X,\ X_f \text{ — конечно}\}.$$

Показать, что этим определен оператор замыкания на Γ и что на самом деле $\mathscr{C}^*$ является наименьшей алгебраической системой замыканий, содержащей $\mathscr{C}$.

6. (Хиггинс.) Показать, что индуктивная система $\mathscr{C}$ подмножеств множества A, содержащая все конечные подмножества, должна совпадать с $\mathscr{B}(A)$. (Указание: для любого $X \subseteq A$ построить такое максимальное подмножество Y множества X, что $Y \cup A_f \in \mathscr{C}$ для всех конечных подмножеств A_f, и показать, что $Y = X$.) Вывести отсюда теорему 1.2, не используя предложение I.5.9. (Указание: показать, что если $\mathscr{C}$ индуктивна, то система всех таких $X \subseteq A$, что $J_{\mathscr{C}}(X) = J_{\mathscr{C}^*}(X)$ [в обозначениях упр. 5], индуктивна и содержит все конечные подмножества.)

7. Установить, что при соответствии Галуа $X \to X^*$, $Y \to Y^*$ выполняются тождества

$$\left(\bigcup X_i\right)^* = \bigcap X_i^*,$$
$$\left(\bigcap X_i^{**}\right)^* = \left(\bigcup X_i^*\right)^{**}$$

для произвольных семейств подмножеств $(X_i)_{i \in I}$.

8. Показать, что отношение $x \leqslant y$ в упорядоченном множестве A определяет соответствие Галуа между левыми отрезками и правыми отрезками множества A и что отображение $x \to \{x\}^{**}$ множества A в $\mathscr{S}(A)$ будет вложением множества A в полную структуру (заметим, что если в качестве A взять множество всех рациональных чисел, то мы получим построение действительных чисел с помощью дедекиндовых сечений).

9. Система $\mathscr{C}$ подмножеств множества A называется системой *конечного характера* (*характера* n), если существует такая система $\mathscr{F}$ конечных подмножеств (подмножеств, состоящих не более чем из n элементов) множества A, что каждое $X \in \mathscr{C}$ однозначно определяется своими пересечениями $F \cap X$ для всех $F \in \mathscr{F}$. Показать, что система замыканий будет алгебраической тогда и только тогда, когда она является системой конечного характера. Привести пример системы конечного характера, которая не является системой характера n ни для какого n.

10. Показать, что множество всех предупорядоченностей на множестве является алгебраической системой замыканий. Верно ли это для множества всех упорядоченностей?

2. Ω-АЛГЕБРЫ

Как уже было указано, под алгеброй понимается множество с некоторыми определенными на нем операциями. Если мы хотим сравнивать различные алгебры, то, прежде всего, нужно установить соответствие между их операциями. Наиболее удобно для этого операции каждой алгебры снабдить индексами из множества индексов, которое остается постоянным в каждой рассматриваемой задаче. Это удобно еще и потому, что не возникает трудностей в обозначениях, когда, как вполне может случиться, соответствие между операциями двух этих алгебр многозначно. Единственное ограничение, которое при этом налагается, состоит в том, чтобы n-арным операциям соответствовали n-арные. Таким образом, имеем

Определение 1. *Областью операторов* называется множество Ω вместе с отображением $a\colon \Omega \to N$; элементы множества Ω называются *операторами*, и если $\omega \in \Omega$, то $a(\omega)$ называется *арностью* оператора ω. Если $a(\omega) = n$, то говорят, что оператор ω является *n-арным*, и пишут

$$\Omega(n) = \{\omega \in \Omega \mid a(\omega) = n\}.$$

Определение 2. Пусть A — множество, а Ω — область операторов; тогда *структурой Ω-алгебры* на A называется семейство отображений

$$\Omega(n) \to A^{A^n} \qquad (n \in N).$$

Таким образом, каждому $\omega \in \Omega(n)$ сопоставляется n-арная операция на A. Множество A с этой структурой называется также *Ω-алгеброй* и иногда обозначается через A_Ω, чтобы подчеркнуть ее зависимость от Ω.

Основное множество A называется также *носителем* Ω-алгебры A_Ω.

Если задана Ω-алгебра A и $\omega \in \Omega(n)$, то оператор ω, примененный к набору из n элементов $(a_1, \ldots, a_n)$ множества A, дает элемент множества A, который записывается в виде $a_1 a_2 \ldots a_n \omega$.

В случае $n = 0$ это просто означает, что ω является элементом множества A; таким образом, 0-арный оператор выбирает в данной алгебре некоторый отмеченный элемент. По этой причине 0-арный оператор иногда называется *постоянным оператором*. Например, при определении групп можно использовать 0-арный оператор, значением которого является единица (см. ниже). Этот оператор можно обозначить через 1, и этим оправдывается обозначение единицы во всех группах одним и тем же символом.

Рассмотрим теперь Ω-алгебры с фиксированной областью Ω и введем некоторые стандартные понятия.

Если заданы Ω-алгебры A_Ω и B_Ω, то говорят, что B есть *подалгебра* Ω-алгебры A, если носитель Ω-алгебры B является подмножеством носителя Ω-алгебры A, а $\omega \in \Omega$ определяет такие операции ω_A, ω_B на A и B соответственно, что B замкнуто относительно ω_A и

$$\omega_A \mid B = \omega_B \text{ для каждого } \omega \in \Omega.$$

Таким образом, всякое подмножество носителя Ω-алгебры A, которое замкнуто относительно каждого $\omega \in \Omega$, можно считать Ω-подалгеброй Ω-алгебры A, определяемой однозначно. Множество всех подалгебр Ω-алгебры A обозначается через $\mathscr{B}_\Omega(A)$. Это множество всегда содержит A, в то время как $\varnothing$ будет его элементом тогда и только тогда, когда Ω не содержит постоянных операторов. Подалгебра алгебры A называется *собственной*, если она отлична от самой алгебры A.

Пусть заданы Ω-алгебры A и B, отображение $f\colon A \to B$ и $\omega \in \Omega(n)$; говорят, что f *согласовано* с ω, если для всех $a_1, \ldots, a_n \in A$

$$(a_1 f) \ldots (a_n f)\,\omega = (a_1 \ldots a_n \omega)\, f. \qquad (1)$$

Если f согласовано с каждым $\omega \in \Omega$, то f называется *гомоморфизмом* или *гомоморфным отображением* A в B. Гомоморфизм $f\colon A \to B$ называется *изоморфизмом* между A и B, если обратное к нему соответствие $f^{-1}\colon B \to A$ также является гомоморфизмом. Если существует изоморфизм между A и B, то говорят, что A и B *изоморфны*, и пишут $A \cong B$. Другие частные случаи гомоморфизмов называются следующим образом: взаимно однозначный гомоморфизм называется *мономорфизмом*; гомоморфизм на называется *эпиморфизмом*; гомоморфизм, источником и целью которого является одна и та же алгебра, называется *эндоморфизмом*; эндоморфизм, являющийся в то же время изоморфизмом, называется *автоморфизмом*. Пусть заданы Ω-алгебры A и B; если существует мономорфизм A в B, то говорят, что A *может быть вложена* или *вложима* в B; если существует эпиморфизм A на B, то B называется *гомоморфным образом* алгебры A.

Каждому семейству $(A_\lambda)_{\lambda \in \Lambda}$ Ω-алгебр сопоставляется прямое произведение, которое определяется следующим образом. Пусть P — декартово произведение множеств A_λ с проекциями $\varepsilon_\lambda\colon P \to A_\lambda$. Тогда любой элемент $a \in P$ полностью определяется своими компонентами $a\varepsilon_\lambda$, и произвольный набор элементов $a(\lambda) \in A_\lambda$ определяет единственный элемент $a \in P$, для которого $a\varepsilon_\lambda = a(\lambda)$ $(\lambda \in \Lambda)$. Поэтому, если $a_1, \ldots, a_n \in P$ и $\omega \in \Omega(n)$, то можно определить $a_1 \ldots a_n\omega$ равенством

$$(a_1 \ldots a_n \omega)\,\varepsilon_\lambda = (a_1\varepsilon_\lambda) \ldots (a_n\varepsilon_\lambda)\,\omega. \qquad (2)$$

Этим способом на P определяется структура Ω-алгебры, а вид равенства (2) показывает, что проекции будут гомоморфизмами. Так определенная алгебра называется *прямым произведением* алгебр A_λ и обозначается через $\prod A_\lambda$. Заметим, что эти алгебры A_λ не обязательно различны. Например, если $A_\lambda = A$ для всех $\lambda \in \Lambda$, получаем *прямую степень* алгебры A, носителем которой является A^Λ и которая сама обозначается через A^Λ. Если элементы алгебры A^Λ рассматриваются как функции из Λ в A, то операции в A^Λ выполняются покомпонентно; например, если в A определено сложение, то в A^Λ имеем

$$(f+g)(\lambda)=f(\lambda)+g(\lambda) \qquad (\lambda \in \Lambda).$$

На данном множестве A, вообще говоря, можно определить различные структуры Ω-алгебр, дающих Ω-алгебры, которые могут быть, а могут и не быть изоморфными, но если A имеет только один элемент, то структуру Ω-алгебры можно определить только одним способом, так как для любого натурального числа n существует единственное отображение A^n в A. Ω-алгебра, содержащая единственный элемент, называется *тривиальной*; из того, что было сказано, следует, что все тривиальные Ω-алгебры изоморфны.

Пусть U — произвольное непустое универсальное множество; тогда Ω-алгебры с носителями в множестве U вместе со всеми гомоморфизмами между ними образуют категорию, которую мы будем обозначать через $(\Omega)_U$ или просто через (Ω), поскольку в дальнейшем U будет обычно фиксированным. При этом две Ω-алгебры считаются совпадающими тогда и только тогда, когда они имеют один и тот же носитель и тождественное отображение определяет изоморфизм между ними; из этого определения следует, что на данном множестве может существовать, вообще говоря, больше, чем одна структура Ω-алгебры, так что (Ω) не будет подкатегорией категории St всех множеств и отображений (в U).

В заключение этого параграфа приведем некоторые примеры алгебр.

(i) *Группоиды*. Группоидом называется множество с единственной бинарной операцией. Здесь Ω состоит из единственного элемента μ арности два. Группоид A, удовлетворяющий закону ассоциативности

$$xy\mu z\mu = xyz\mu\mu \text{ для всех } x,\ y,\ z \in A, \tag{3}$$

называется *полугруппой*. Полугруппы и их гомоморфизмы образуют полную подкатегорию категории группоидов. *Нейтральным элементом* в группоиде называется такой элемент e, что

$$xe\mu = ex\mu = x \text{ для всех } x \in A. \tag{4}$$

Легко проверить, что группоид может иметь не больше одного нейтрального элемента.

(ii) *Группоиды с* 1. Группоидом с 1 называется множество A с двумя операциями: бинарной μ и 0-арной 1, причем

$$x1\mu = 1x\mu = x \text{ для всех } x \in A. \tag{5}$$

Хотя различие между «группоидом с нейтральным элементом» и «группоидом с 1» только формальное, настоящее различие появляется, когда мы переходим к рассмотрению подгруппоидов и гомоморфизмов. Действительно, если A — группоид с нейтральным элементом e, то подгруппоид группоида A не обязан содержать e и гомоморфизм между такими группоидами не обязан отображать нейтральный элемент одного группоида в нейтральный элемент другого. Но если считать A «группоидом с 1», а e — значением постоянного оператора 1, то допустимы только подгруппоиды, содержащие e, и только гомоморфизмы, сохраняющие нейтральные элементы. В частности, группоиды с 1 и их гомоморфизмы образуют подкатегорию в категории всех группоидов (и гомоморфизмов), которая, однако, не полна.

(iii) *Группы.* Группой называется непустая полугруппа, в которой уравнения $ax\mu = b$, $ya\mu = b$ имеют решения x, y при произвольном выборе элементов a и b. Как хорошо известно, эти уравнения имеют единственные решения (см., например, Курош [62], гл. 2). Другое определение группы относительно бинарного оператора μ, унарного оператора θ и 0-арного оператора 1 можно дать следующим образом. Группой называется $(\mu, \theta, 1)$-алгебра, удовлетворяющая приведенным выше условиям (3) и (5) и, кроме того, условию

$$xx\theta\mu = x\theta x\mu = 1 \tag{6}$$

для всех $x \in A$. Доказательство эквивалентности этих определений также хорошо известно и может быть предоставлено читателю (см. Курош [62], гл. 2). Конечно, привычнее писать xy вместо $xy\mu$, x^{-1} вместо $x\theta$ и называть 1 *единицей*; в частных примерах мы также будем пользоваться этим обозначением, так что (3), (5) и (6) могут быть переписаны в виде

$$(xy)z = x(yz), \tag{3$'$}$$

$$x1 = 1x = x, \tag{5$'$}$$

$$xx^{-1} = x^{-1}x = 1. \tag{6$'$}$$

Заметим, что хотя смысл равенства (3) однозначно определен его записью, в равенстве (3′) мы вынуждены поставить скобки, чтобы различать выражения слева и справа, и это было бы по-прежнему необходимо, даже если бы мы обозначили операцию некоторым символом, таким, как точка, записанным *между* элементами, к которым она применяется. Вообще в § III. 2 будет доказано, что скобки не нужны, если все операторы записываются *справа* от аргументов (или слева). Категория всех групп и гомоморфизмов будет обозначаться через Gp.

Часто для групп пользуются аддитивной записью, которая заключается в том, что пишут $x+y$ вместо $xy\mu$, $-x$ вместо $x\theta$ и 0 вместо 1. Тождества (3), (5), (6) читаются тогда следующим образом:

$$(x+y)+z = x+(y+z), \tag{3$''$}$$

$$x+0 = 0+x = x, \tag{5$''$}$$

$$x+(-x) = (-x)+x = 0. \tag{6$''$}$$

Аддитивной записью пользуются особенно часто (но не исключительно) для *абелевых* групп, т. е. групп, удовлетворяющих закону коммутативности:

$$x + y = y + x. \tag{7}$$

(iv) *Группы с операторами.* Пусть G — группа с множеством Ω таких унарных операторов, что

$$(xy)\,\omega = (x\omega)(y\omega) \qquad (x,\ y \in G,\ \omega \in \Omega). \tag{8}$$

Тогда G называется *группой с операторами*. Вообще *группой с мультиоператорами* (Хиггинс [56]) называется группа с множеством таких не обязательно унарных операторов ω, что

$$11\ \dots\ 1\omega = 1 \qquad (\omega \in \Omega).$$

Таким образом, произвольную Ω-алгебру, которая является в то же время группой и содержит 1 в качестве Ω-подалгебры, можно считать группой с мультиоператорами. Оказывается, что многие из общих структурных теорем для групп с небольшими изменениями переносятся на группы с мультиоператорами (см. Хиггинс [56]).

(v) *Квазигруппы.* Квазигруппой называется группоид, в котором каждое из уравнений $xa = b$, $ay = b$ имеет единственное решение для каждой пары элементов a, b. Квазигруппа с нейтральным элементом называется *лупой*.

(vi) *Кольца.* Кольцом называется абелева группа (записываемая аддитивно), которая в то же время является полугруппой [1]) относительно бинарного оператора, называемого *умножением* и обозначаемого обычным образом, причем эти операторы связаны законами дистрибутивности:

$$x(y + z) = xy + xz,$$
$$(x + y)\,z = xz + yz.$$

Если, кроме того, существует 0-арный оператор 1, который ведет себя как нейтральный элемент относительно умножения, $1x = x1 = x$, то говорят о кольце с единицей 1. Если через Rg обозначить категорию колец и их гомоморфизмов, а через Rg* обозначить категорию колец с 1 и их гомоморфизмов, то Rg* будет подкатегорией категории Rg, но не полной: Rg-морфизм между Rg*-объектами R и S будет Rg*-морфизмом тогда и только тогда, когда он отображает 1 кольца R в 1 кольца S.

(vii) *Модули над кольцами.* Модулем над кольцом R, или *R-модулем*, называется абелева группа M с такими унарными операторами ω_a для каждого $a \in R$, что операция, определенная оператором ω_a, является эндоморфизмом группы M и

$$\omega_{ab} = \omega_a\omega_b, \quad \omega_{a+b} = \omega_a + \omega_b \qquad (a,\ b \in R). \tag{9}$$

---

[1]) Или, в более общем случае, группоидом. — *Прим. ред.*

Заметим, что различные операторы могут определять одну и ту же операцию. В случае когда R — кольцо с 1, обычно требуют, чтобы модуль был *унитарным*; это означает, что эндоморфизм ω_1, определяемый единицей, тождествен на M. Если вместо первого равенства (9) имеем $\omega_{ab}=\omega_b\omega_a$, то говорят о *левом* R-модуле. Взяв в качестве M аддитивную группу кольца R с правым или левым умножением

$$\rho_a\colon x\to xa,\quad \lambda_a\colon x\to ax,$$

получаем примеры R-модуля и левого R-модуля соответственно. Если R — кольцо с 1, то полученные модули унитарны.

Иногда определяют модуль над группой G, или G-модуль, как множество P с такими унарными операторами ω_x для каждого $x\in G$, что

$$\omega_{xy}=\omega_x\omega_y,\quad \omega_1=1\quad (x,\ y\in G).$$

(viii) *Линейные алгебры.* Пусть K — коммутативное кольцо с 1; тогда *K-линейной алгеброй* A называется унитарный K-модуль, являющийся в то же время кольцом, притом таким, что

$$(ab)\alpha=(a\alpha)b=a(b\alpha)\qquad (a,\ b\in A,\ \alpha\in K).$$

Если A также имеет нейтральный элемент, обозначаемый, скажем, через e, то отображение $\alpha\to e\alpha$ ($\alpha\in K$) будет гомоморфизмом $K\to A$, который полностью определяет структуру K-модуля на A.

(ix) *Множества.* Множество можно считать $\varnothing$-алгеброй. В этом смысле все, что говорится об Ω-алгебрах, применимо к частному случаю множеств.

(x) *Натуральные числа.* Пусть Ω состоит из 0-арного оператора, обозначаемого через 0, и унарного оператора, обозначаемого через $'$. Натуральные числа представляют собой частный случай такой алгебры (см. § I. 1 и § VII. 1).

(xi) *Структуры.* Структуру можно считать алгеброй с двумя бинарными операторами (см. § II. 4), но полная структура *не* является алгеброй в том смысле, как здесь определено, поскольку в ее определении участвуют, вообще говоря, бесконечноместные операции.

(xii) *Упорядоченные множества.* Упорядоченное множество не является алгеброй, так как оно определяется с помощью отношения ($x\leqslant y$), а не с помощью операций. Но мы можем, хотя и несколько искусственно, описать упорядоченное множество с помощью операций. Например, для каждой пары таких элементов $(a,\ b)$, что $a\leqslant b$, можно ввести унарный оператор $\lambda=\lambda(a,\ b)$, определяемый равенствами

$$x\lambda=\begin{cases} b, & \text{если } x=a,\\ x & \text{во всех остальных случаях.}\end{cases}$$

Заметим, что здесь операторы (а не только операции, ими определяемые) зависят от носителя. В гл. V будет описан более естественный способ рассмотрения отношений в некоторой алгебре.

(xiii) *Поля.* Поле не является алгеброй, поскольку операции, которые обычно используются, определены не всюду: x^{-1} определен только для $x \neq 0$. Можно обойти эту трудность, полагая

$$x\theta = \begin{cases} x^{-1}, & \text{если } x \neq 0, \\ 0, & \text{если } x = 0, \end{cases}$$

и таким образом из нашего поля формально сделать алгебру; но это определение имеет другие недостатки: например, равенство $x \cdot x\theta = 1$ выполняется только тогда, когда $x \neq 0$, в то время как $x \cdot x^{-1} = 1$ выполняется всякий раз, как определены обе части равенства. Позже, в гл. IV, мы увидим, что нельзя дать определение полей (аналогичное данным выше определениям групп и колец) как алгебр, удовлетворяющих некоторым тождествам.

Если Ω — область операторов, то, сопоставляя каждому $\omega \in \Omega(n)$ отображение подмножества множества A^n в A, получаем структуру, называемую *частичной Ω-алгеброй.* Как и в случае полей, частичную алгебру можно всегда считать алгеброй, если взять фиксированный элемент $c \in A$ и для любого $a \in A^n$, для которого $a\omega$ не определено, положить $a\omega = c$. Таким образом, произвольную частичную алгебру с непустым носителем можно считать алгеброй в определенном выше смысле.

(xiv) *Расширения. Пусть C — фиксированная* Ω-алгебра; тогда *Ω-алгеброй над C* называется Ω-алгебра A с гомоморфизмом

$$\lambda\colon C \to A.$$

Если λ взаимно однозначен, то C можно отождествить с подалгеброй алгебры A, и тогда A называется *расширением* алгебры C; это часто записывается так: A/C. Эквивалентно Ω-алгебру над C можно определить как алгебру с операторами Ω и с таким постоянным оператором $\gamma(a)$ для каждого $a \in C$, что

$$\gamma(a_1) \ldots \gamma(a_n)\omega = \gamma(a_1 \ldots a_n\omega) \quad (\omega \in \Omega(n)).$$

(xv) *Проективные плоскости.* Проективной плоскостью называется множество, состоящее из элементов двух видов («прямых» и «точек»), вместе с бинарной операцией, подчиненной некоторым правилам (см., например, М. Холл [59]), которая определена только на парах элементов одного вида и принимает значения другого вида, чем аргументы; таким образом, произведением двух (различных) точек будет прямая, произведением двух (различных) прямых будет точка, а другие произведения не определены. Это снова частичная алгебра.

(xvi) *Топологические пространства.* Топологическое пространство можно определить как множество с некоторыми бесконечноместными операциями: для каждого подмножества A и каждой точки x из $\bar{A}$, замыкания множества A, введем оператор $\tau(A, x)$, который сопоставляет x множеству A. Таким образом, топологическое пространство не удается сделать алгеброй, потому что оператор $\tau(A, x)$ будет бесконечноместным, как только A бесконечно. На самом же деле это определение позволяет считать топологическое пространство алгеброй всякий раз, когда система всех замкнутых подмножеств оказывается алгебраической системой замыканий. Это утверждение является частным случаем теоремы 5.2, приведенной ниже.

Эти примеры алгебр и неалгебр служат для иллюстрации определения алгебры и налагаемых им ограничений. Итак, мы ограничили себя однозначными и всюду определенными отношениями, т. е. *операциями*; как мы увидим в главах V и VI, отношения требуют существенно отличных подходов. Приходится ограничиться финитарными операциями, если мы хотим, чтобы подалгебры образовывали алгебраическую систему замыканий (см. § II. 5), и на самом деле изучение бесконечноместных операций до настоящего времени привлекало мало внимания (см. Сломинский [59]). Наконец, следует заметить, что за несколькими исключениями операторы в приведенных примерах самое большее бинарны. И это неслучайно, так как в некотором смысле все финитарные операторы могут быть построены из бинарных (§ III. 7). Однако, вероятно, не может быть никакого естественного способа для осуществления этого в каждом данном случае, и, кроме того, достигаемое при этом упрощение было бы не очень значительно. Поэтому мы будем рассматривать n-арные операторы для произвольного конечного n.

УПРАЖНЕНИЯ

1. Показать, что категория является частичной полугруппой.

2. Проверить, что подстановки множества P образуют группу $\Sigma(P)$, *симметрическую группу* на множестве P, и что структура G-модуля на множестве P полностью определяется гомоморфизмом $G \to \Sigma(P)$.

3. Пусть P есть G-модуль, где G — группа, и для каждого $p \in P$ определим *стабилизатор* $G_p = \{x \in G \mid px = p\}$ элемента p. Показать, что стабилизатор произвольного $p \in P$ будет подгруппой группы G. Что будут представлять собой стабилизаторы элементов группы G, если G считать G-модулем с правым умножением?

4. Определить S-модуль, где S — полугруппа с 1, и показать, что саму полугруппу S можно считать S-модулем при правом умножении. Показать, что эндоморфизмами полугруппы S как S-модуля будут только левые умножения $\lambda_a: x \to ax$. (Указание: эндоморфизмом полугруппы S как S-модуля является такое отображение θ: $S \to S$, что $(ab)\theta = (a\theta)b$ для всех $a, b \in S$.)

5. Показать, что любая группа является группой всех автоморфизмов некоторой алгебры. (Указание: использовать упр. 4; см. *также* Биркгоф [35].)

6. Показать, что алгебра с конечным носителем, состоящим из n элементов, имеет не больше $n!$ автоморфизмов и не больше n^n эндоморфизмов.

7. Для произвольной группы G определить левый G-модуль как множество P с операторами ω_a, удовлетворяющими равенствам $\omega_{ab} = \omega_b\omega_a$, $\omega_1 = 1$. Показать, что каждый левый G-модуль можно считать G-модулем.

8. (Биркгоф.) Показать, что множество $\mathscr{C}(A)$ всех эквивалентностей на множестве A образует полную структуру относительно упорядоченности по включению. Показать, что если A конечно, то группа автоморфизмов структуры $\mathscr{C}(A)$ изоморфна симметрической группе на множестве A. (Указание: заметить, что *особая* эквивалентность, т. е. эквивалентность, классами которой являются одноэлементное множество и дополнение к нему, отображается в особую при произвольном автоморфизме структуры $\mathscr{C}(A)$, и показать, что каждую эквивалентность на множестве A можно выразить через особые.)

9. Определим *центр* кольца R как

$$Z(R) = \{a \in R \mid ax = xa \text{ для всех } x \in R\}.$$

Показать, что центр K-линейной алгебры A будет подалгеброй алгебры A. Более того, если A имеет единицу e, то отображение $\alpha \to e\alpha$ будет гомоморфизмом кольца K в $Z(A)$; и, обратно, если задано кольцо R, то любой гомоморфизм $K \to Z(R)$ определяет структуру K-линейной алгебры на R.

10. Пусть (A_λ) — произвольное семейство Ω-алгебр. Показать, что структура Ω-алгебры на прямом произведении ΠA_λ определяется однозначно, если потребовать, чтобы проекции были гомоморфизмами.

11. Пусть A — группоид, операция которого обозначена через xy и на котором, быть может, определены другие операции. Алгебра A называется *внутренним прямым произведением* своих подалгебр B и C, если B и C таковы, что отображение $(b, c) \to bc$ является изоморфизмом между $B \times C$ и A. Записать необходимые и достаточные условия, при которых алгебру A можно представить в виде внутреннего прямого произведения подалгебр B и C. (См. Йонсон и Тарский [47].)

12. Пусть a и b — две прямые на плоскости, A_i и B_i $(i = 1, 2, 3)$ — произвольные тройки точек на a и b соответственно и C_i — точка пересечения прямых A_jB_k и A_kB_j (для любой перестановки ijk чисел 1, 2, 3). По теореме Паппа точки C_i коллинеарны некоторой прямой, скажем прямой c; конфигурация, состоящая из девяти точек A_i, B_i, C_i и девяти прямых a, b, c и A_jB_k, A_kB_j, называется *конфигурацией Паппа*. Показать, что если P и Q — две произвольные различные точки конфигурации Паппа, то существует и притом только одна точка R этой конфигурации (отличная от P и Q), для которой: (i) либо PQR является прямой этой конфигурации, (ii) либо PRS не является прямой этой конфигурации ни для какой точки $S \neq Q$.

Пусть Γ — множество, состоящее из девяти точек конфигурации Паппа, и E — десятая точка. Определим для произвольных $P, Q \in \Gamma$

$$P \cdot Q = \begin{cases} P, & \text{если } Q = E, \\ Q, & \text{если } P = E, \\ E, & \text{если } P = Q, \\ R & \text{во всех остальных случаях,} \end{cases}$$

где R — определенная выше точка. Показать, что так определенная алгебраическая структура на Γ будет коммутативной лупой, но не будет группой. Показать также, что подлупа, порожденная любыми двумя элементами, будет группой.

3. ТЕОРЕМЫ ОБ ИЗОМОРФИЗМАХ

Существует другой способ определения гомоморфизмов, который полезен в некоторых приложениях. Напомним, что отображение из A в B определяется с помощью функции из A в B, т. е. определенного вида подмножества множества $A \times B$. Теперь мы можем сказать, что гомоморфизмом $f\colon A \to B$ является отображение, функция которого служит также подалгеброй алгебры $A \times B$. Действительно, утверждение «f замкнуто относительно $\omega \in \Omega(n)$» означает, что если заданы $(a_i, b_i) \in f$, $i = 1, \ldots, n$, то

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

откуда следует, что

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

Но это как раз и есть условие согласованности для ω. Чтобы воспользоваться новым определением, нам потребуется одна лемма:

Лемма **3.1.** *Пусть A, B, C суть Ω-алгебры, A' — подалгебра алгебры A и Φ, Ψ — подалгебры алгебр $A \times B$ и $B \times C$ соответственно. Тогда $A'\Phi$, Φ^{-1} и $\Phi \circ \Psi$ снова замкнуты относительно Ω (т. е. являются подалгебрами алгебр B, $B \times A$ и $A \times C$ соответственно).*

Для доказательства первого утверждения возьмем $b_i \in A'\Phi$ ($i = 1, \ldots, n$); тогда существуют такие $a_i \in A'$, что $(a_i, b_i) \in \Phi$ ($i = 1, \ldots, n$), а так как A' и Φ замкнуты относительно Ω, то для произвольного $\omega \in \Omega(n)$ имеем

$$a_1 \ldots a_n\omega \in A' \quad \text{и} \quad (a_1 \ldots a_n\omega,\ b_1 \ldots b_n\omega) \in \Phi,$$

откуда $b_1 \ldots b_n\omega \in A'\Phi$. Остальные утверждения доказываются аналогично. ∎

Из этой леммы вытекают следующие утверждения:

Предложение **3.2.** *Произведение гомоморфизмов снова является гомоморфизмом; аналогичные утверждения имеют место для изоморфизмов, эндоморфизмов или автоморфизмов.* ∎

Предложение **3.3.** *Образ при гомоморфизме является подалгеброй цели.* ∎

Определение. Эквивалентность на Ω-алгебре A, являющаяся в то же время подалгеброй алгебры A^2, называется *конгруэнцией* на A. Множество всех конгруэнций на A обозначается через $\mathscr{C}_\Omega(A)$.

При помощи этого определения получаем

***Предложение* 3.4.** *Ядро гомоморфизма является конгруэнцией.*

Действительно, ядром отображения f называется $f \circ f^{-1}$. По лемме 3.1 ядро будет подалгеброй, а по теореме I. 3.1 — эквивалентностью; следовательно, ядро является конгруэнцией. ∎

Коротко об интерпретации конгруэнций в частном случае групп. Пусть G — группа с единицей e и $\mathfrak{q}$ — конгруэнция на G в определенном выше смысле. Тогда $N = e^{\mathfrak{q}}$ будет нормальным делителем группы G, а $\mathfrak{q}$-классы будут смежными классами группы G по N. В самом деле, $a^{\mathfrak{q}} = Na$ для любого $a \in G$, так что $\mathfrak{q}$ полностью определяется нормальным делителем N. Если теперь f — гомоморфизм группы G (в некоторую группу), то его ядром, в смысле теории групп, будет нормальный делитель группы G, а именно класс конгруэнции $f \circ f^{-1}$, содержащий e. Этим и оправдывается то обстоятельство, что этот класс $\left(\text{а не } f \circ f^{-1}\right)$ называется ядром гомоморфизма f в этом случае.

Кольца можно считать частным случаем групп; 0-класс конгруэнции на кольце R является такой подгруппой $\mathfrak{a}$ аддитивной группы кольца R, что

$$xa \in \mathfrak{a} \quad \text{для всех} \quad x \in R \quad \text{и} \quad a \in \mathfrak{a} \tag{1}$$

и

$$ax \in \mathfrak{a} \quad \text{для всех} \quad x \in R \quad \text{и} \quad a \in \mathfrak{a}. \tag{2}$$

Аддитивная подгруппа $\mathfrak{a}$, удовлетворяющая условиям (1) и (2), называется *идеалом* кольца R. Если выполняется только (1) (или только (2)), то имеем левый (или правый) идеал кольца R. Такой идеал получается как 0-класс конгруэнции на R, если R считается левым (правым) R-модулем.

Каждому нормальному делителю N группы G соответствует гомоморфизм с ядром N; нужно только взять естественный гомоморфизм на факторгруппу G/N. Тем же способом для каждой Ω-алгебры A и каждой конгруэнции $\mathfrak{q}$ на A можно определить факторалгебру $A/\mathfrak{q}$ и естественный гомоморфизм $A \to A/\mathfrak{q}$ с ядром $\mathfrak{q}$. Это и составляет содержание следующей теоремы.

***Теорема* 3.5.** *Пусть A есть Ω-алгебра и $\mathfrak{q}$ — конгруэнция на A. Тогда существует такая единственная структура Ω-алгебры на фактормножестве $A/\mathfrak{q}$, что естественное отображение $A \to A/\mathfrak{q}$ является гомоморфизмом.*

Обозначим полученную алгебру также через $A/\mathfrak{q}$ и назовем ее *факторалгеброй* алгебры A по конгруэнции $\mathfrak{q}$ с *естественным гомоморфизмом* $A \to A/\mathfrak{q}$. Факторалгебра любой подалгебры алгебры A называется также *фактором* алгебры A.

Доказательство. Пусть $\theta = \mathrm{nat}\,\mathfrak{q}$ — естественное отображение $A \to A/\mathfrak{q}$. Очевидным образом оно индуцирует отображение $\theta_n\colon A^n \to (A/\mathfrak{q})^n$, и для доказательства теоремы нужно только показать, что диаграмму

$$\begin{tikzcd} A^n \arrow[r, "\omega"] \arrow[d, "\theta_n"'] & A \arrow[d, "\theta"] \\ (A/\mathfrak{q})^n & A/\mathfrak{q} \end{tikzcd}$$

можно дополнить до коммутативной единственным способом. Если отображение $\bar{\omega}\colon (A/\mathfrak{q})^n \to A/\mathfrak{q}$, обладающее этим свойством, существует, то оно должно удовлетворять равенству

$$a_1^{\mathfrak{q}} \ldots a_n^{\mathfrak{q}}\bar{\omega} = (a_1 \ldots a_n\omega)^{\mathfrak{q}}, \tag{3}$$

а это равенство определяет $\bar{\omega}$, очевидно, единственным образом, если мы сможем показать, что правая часть равенства не зависит от выбора элементов a_i в их $\mathfrak{q}$-классах. Таким образом, пусть $(a_i, a_i') \in \mathfrak{q}$; тогда, так как $\mathfrak{q}$ — подалгебра, то

$$(a_1 \ldots a_n\omega,\ a_1' \ldots a_n'\omega) \in \mathfrak{q},$$

т. е.

$$(a_1 \ldots a_n\omega)^{\mathfrak{q}} = (a_1' \ldots a_n'\omega)^{\mathfrak{q}},$$

что и утверждалось. ∎

В качестве примера отметим, что каждая Ω-алгебра A имеет конгруэнции Δ и A^2. В первом случае мы получаем изоморфизм

$$A/\Delta \cong A,$$

тогда как A/A^2 — тривиальная алгебра. Любая конгруэнция на A, не совпадающая с A^2, называется *собственной*, а конгруэнция, отличная от Δ, называется *нетривиальной*.

Пусть $\mathfrak{q}$ — конгруэнция на алгебре A. Если S — такое подмножество алгебры A, пересечение которого с каждым $\mathfrak{q}$-классом состоит не более чем из одного элемента, т. е.

$$\mathfrak{q} \cap S^2 = \Delta_S, \tag{4}$$

то говорят, что $\mathfrak{q}$ *разделяет* S; если пересечение каждого $\mathfrak{q}$-класса с множеством S состоит точно из одного элемента, т. е. выполняется (4) и объединение всех $\mathfrak{q}$-классов, пересекающихся с S, совпадает с A:

$$S^{\mathfrak{q}} = A, \tag{5}$$

то говорят, что S является *трансверсалом* для $A/\mathfrak{q}$ в A.

Теперь мы можем сформулировать три знаменитых теоремы об изоморфизмах. Эти теоремы, впервые в явном виде сформулированные Э. Нётер (см. Ван дер Варден [37]), вытекают из теорем I.3.1, I.3.3 и I.3.4 о множествах и отображениях и применимы при очень общих условиях к множествам с определенными на них структурами и отображениям между множествами, сохраняющим эти структуры. Таким образом, эти теоремы естественнее всего отнести к теории категорий, где они фигурируют в качестве аксиом (см. аксиомы абелевых категорий, Маклейн [63]). Мы не будем стремиться к такой общности, а ограничимся алгебраическими структурами. Здесь можно сказать несколько больше, чем в общем случае; в самом деле, справедлива следующая очевидная лемма, не имеющая аналога для более общих структур, как, например, для топологических групп (см. Бурбаки [51]):

***Лемма* 3.6.** *Взаимно однозначный эпиморфизм является изоморфизмом.*

Доказательство. Пусть $f\colon A \to B$ — взаимно однозначный эпиморфизм; тогда $f^{-1}\colon B \to A$ также будет отображением, а по лемме 3.1 f^{-1} будет гомоморфизмом; следовательно, f — изоморфизм. ∎

Теорема* 3.7. *(Первая теорема об изоморфизмах.) *Пусть $f\colon A \to B$ — произвольный гомоморфизм Ω-алгебр с ядром $\mathfrak{q}$. Тогда имеет место разложение*

$$f = \varepsilon f' \mu,$$

где $\varepsilon = \operatorname{nat} \mathfrak{q}$ — естественный гомоморфизм $A \to A/\mathfrak{q}$, μ — вложение $Af \to B$ и

$$f'\colon A/\mathfrak{q} \to Af$$

— изоморфизм.

Эта теорема сразу же вытекает из теоремы I.3.1, нужно только проверить, что определенное там отображение f' будет гомоморфизмом, и затем применить лемму 3.6. ∎

Часто оказывается полезным следствие, вытекающее из теоремы о фактормножествах (теорема I.3.3).

***Следствие* 3.8.** *Пусть $f\colon A \to B$ — произвольный гомоморфизм Ω-алгебр и $\mathfrak{q}$ — конгруэнция на A, содержащаяся в ядре гомо-*

морфизма f. Тогда существует такой единственный гомоморфизм $\bar{f}$: $A/\mathfrak{q} \to B$, что диаграмма

$$\begin{tikzcd} A \arrow[rr, "\mathrm{nat}\,\mathfrak{q}"] \arrow[dr, "f"'] & & A/\mathfrak{q} \arrow[dl, "\bar{f}"] \\ & B & \end{tikzcd}$$

коммутативна.

Это утверждение вытекает непосредственно из теоремы I.3.3. ∎

В силу теоремы 3.5 гомоморфными образами каждой Ω-алгебры A являются она сама и тривиальная алгебра. Если алгебра не имеет других гомоморфных образов и не тривиальна, то она называется *простой*. По теореме 3.7 *Ω-алгебра A проста тогда и только тогда*, когда она имеет точно две конгруэнции, а именно A^2 и Δ.

Теорема 3.9. **(Вторая теорема об изоморфизмах.)** *Пусть A есть Ω-алгебра, A_1 — подалгебра алгебры A и $\mathfrak{q}$ — конгруэнция на A. Тогда $A_1^{\mathfrak{q}}$ является подалгеброй алгебры A, $\mathfrak{q}_1 = \mathfrak{q} \cap A_1^2$ — конгруэнцией на A_1* и

$$A_1/\mathfrak{q}_1 \cong A_1^{\mathfrak{q}}/\mathfrak{q}. \tag{6}$$

Доказательство. Пусть $\theta = \mathrm{nat}\,\mathfrak{q}$ — естественное отображение и $\theta_1 = \theta \mid A_1$ — его ограничение на A_1. Тогда θ_1 будет гомоморфизмом алгебры A_1 в $A/\mathfrak{q}$, образом $A_1\theta_1$ подалгебры A_1 при этом гомоморфизме будет множество $\mathfrak{q}$-классов, пересекающихся с A_1 (т. е. $A_1^{\mathfrak{q}}/\mathfrak{q}$), а ядром этого гомоморфизма служит $\mathfrak{q} \cap A_1^2 = \mathfrak{q}_1$. Отсюда в силу теоремы 3.7 получаем (6), а остальное проверяется непосредственно. ∎

Частный случай этой теоремы при $\mathfrak{q}_1 = \Delta_{A_1}$ имеет смысл сформулировать отдельно:

Следствие 3.10. *Если A есть Ω-алгебра, A_1 — подалгебра и $\mathfrak{q}$ — конгруэнция, разделяющая A_1, то*

$$A_1 \cong A_1^{\mathfrak{q}}/\mathfrak{q}. \ ∎$$

Теорема 3.9 в действительности утверждает, что произвольная подалгебра факторалгебры A изоморфна фактору алгебры A. Обратное, конечно, не верно, как показывает существование простых неабелевых групп.

Переводя на язык алгебр теорему I.3.4, получаем следующую теорему:

Теорема 3.11. (**Третья теорема об изоморфизмах.**) *Пусть A есть Ω-алгебра и $\mathfrak{q}$, $\mathfrak{r}$ — такие конгруэнции на A, что*

$\mathfrak{q} \subseteq \mathfrak{r}$. *Тогда существует такой единственный гомоморфизм* θ: $A/\mathfrak{q} \to A/\mathfrak{r}$, *что* $(\operatorname{nat} \mathfrak{q})\,\theta = \operatorname{nat} \mathfrak{r}$. *Если* $\ker \theta = \mathfrak{r}/\mathfrak{q}$, *то* $\mathfrak{r}/\mathfrak{q}$ *является конгруэнцией на* $A/\mathfrak{q}$ *и* θ *индуцирует такой изоморфизм*

$$\theta'\colon (A/\mathfrak{q})/(\mathfrak{r}/\mathfrak{q}) \to A/\mathfrak{r},$$

что $\theta = (\operatorname{nat} \mathfrak{r}/\mathfrak{q})\,\theta'$. ∎

Фиксируя $\mathfrak{q}$ и изменяя $\mathfrak{r}$, получаем

Следствие 3.12. *Пусть* A *есть* Ω*-алгебра и* $\mathfrak{q}$ *— конгруэнция на* A. *Если рассматривать* $\operatorname{nat} \mathfrak{q}$ *как отображение* $A^2 \to (A/\mathfrak{q})^2$, *то переход к полным прообразам при отображении* $\operatorname{nat} \mathfrak{q}$ *индуцирует отображение*

$$\mathfrak{r} \to \mathfrak{r}/\mathfrak{q}, \tag{7}$$

которое устанавливает взаимно однозначное соответствие между множеством конгруэнций на A, *содержащих* $\mathfrak{q}$, *и множеством конгруэнций на* $A/\mathfrak{q}$; *кроме того,*

$$A/\mathfrak{r} \cong (A/\mathfrak{q})/(\mathfrak{r}/\mathfrak{q}). \ ∎$$

Теперь замечание, приведенное после следствия 3.8, можно переформулировать так:

Следствие 3.13. *Пусть* A *есть* Ω*-алгебра и* $\mathfrak{q}$ *— конгруэнция на* A; *тогда* $\mathfrak{q}$ *будет максимальной собственной конгруэнцией в том и только в том случае, когда алгебра* $A/\mathfrak{q}$ *простая.* ∎

Во многих задачах заданные алгебры определены только с точностью до изоморфизма и требуется получить ответ также только с точностью до изоморфизма. При этих обстоятельствах часто полезен следующий результат:

Предложение 3.14. *Пусть* A *есть* Ω*-алгебра и* B *— подалгебра алгебры* A. *Если* B' *есть* Ω*-алгебра, изоморфная алгебре* B, *то существует* Ω*-алгебра* A', *изоморфная* A *и содержащая* B' *в качестве подалгебры. Точнее, если* θ: $B' \to B$ *— изоморфизм, то существует такая* Ω*-алгебра* A', *содержащая* B' *в качестве подалгебры, и такой изоморфизм* $\bar{\theta}$: $A' \to A$, *что* $\bar{\theta} \mid B' = \theta$.

Доказательство. Можно предполагать, что $A \cap B' = \varnothing$, заменяя, если нужно, A ее изоморфным образом (например, при подходящем выборе элемента u алгебра $A \times \{u\}$ не пересекается с B' и изоморфна алгебре A). Определим теперь $A' = B' \cup (A \setminus B)$ и расширим θ до отображения $\bar{\theta}$: $A' \to A$, считая его тождественным на $A \setminus B$. Теперь существует единственная алгебра на A', при которой $\overline{\theta}$ является изоморфизмом, и легко видеть, что B будет подалгеброй так определенной алгебры A'. ∎

УПРАЖНЕНИЯ

1. Сформулировать и доказать теоремы, аналогичные теоремам об изоморфизмах, для категории Ω-алгебр и всех соответствий, допускающих Ω (говорят, что соответствие из A в B допускает Ω, если оно является подалгеброй алгебры $A \times B$). (См. упр. I.3.7.)

2. Сформулировать и доказать теоремы, аналогичные теоремам об изоморфизмах, для категории топологических пространств и непрерывных отображений.

3. Дать описание конгруэнций на группе с мультиоператорами.

4. Дать описание конгруэнций на полугруппе.

5. Показать, что если G — некоторая группа и P есть G-модуль, то отношение на P, определенное по правилу:

$$p \sim q \text{ тогда и только тогда, когда } p = qx \text{ для некоторого } x \in G,$$

будет *эквивалентностью на P и что классом этой эквивалентности*, содержащим p, будет множество $pG = \{px \in P \mid x \in G\}$. (Это множество называется *траекторией* элемента p при действии группы G.)

6. Если G — группа и H — подгруппа, то G можно считать (левым) H-модулем при левом умножении на элементы группы H. Показать, что если обозначить этот модуль через ${}_HG$, то множество траекторий элементов модуля ${}_HG$ будет G-модулем при правом умножении на элементы группы G. Показать, что если этот G-модуль обозначить через G/H, то G/H состоит из единственной траектории, и что каждая траектория произвольного G-модуля изоморфна модулю вида G/H для некоторой подгруппы H группы G. Точнее, показать, что траектория элемента p изоморфна модулю G/G_p, где G_p — стабилизатор элемента p; вывести соотношение

$$|pG| \cdot |G_p| = |G|.$$

4. СТРУКТУРЫ

При изучении общих алгебр часто встречаются структуры, и, может быть, целесообразно здесь установить их свойства для дальнейших ссылок и, в частности, потому, что сами структуры могут считаться алгебрами. В § I.4 структура была определена как упорядоченное множество, в котором каждая пара элементов имеет точную верхнюю (sup) и точную нижнюю (inf) грани. Так как sup и inf однозначно определены, то на самом деле они представляют собой два бинарных оператора и структуру можно считать алгеброй относительно этих операторов:

***Предложение* 4.1.** *Пусть L — произвольная структура; тогда для любых $a, b, c \in L$*

$$\left.\begin{aligned} a\vee(b\vee c)&=(a\vee b)\vee c,\\ a\wedge(b\wedge c)&=(a\wedge b)\wedge c,\end{aligned}\right\} \quad \text{(закон ассоциативности)} \tag{1}$$

$$\left.\begin{aligned} a\vee b&=b\vee a,\\ a\wedge b&=b\wedge a,\end{aligned}\right\} \quad \text{(закон коммутативности)} \tag{2}$$

$$\left.\begin{aligned} a\wedge(a\vee b)&=a,\\ a\vee(a\wedge b)&=a.\end{aligned}\right\} \quad \text{(закон поглощения)} \tag{3}$$

Обратно, если L — алгебра с двумя бинарными операторами $\vee$ и $\wedge$, удовлетворяющими (1) — (3), *то на L можно определить упорядоченность по следующему правилу:*

$$a \leqslant b \text{ тогда и только тогда, когда } a \vee b = b, \tag{4}$$

и относительно этой упорядоченности L будет структурой, причем $\sup(a, b) = a \vee b$, $\inf(a, b) = a \wedge b$.

Доказательство. Из определения оператора $a \vee b$ как точной верхней грани следует, что единственную точную верхнюю грань элементов a и b можно записать или в виде $a\vee b$ или в виде $b\vee a$, а $\sup(a, b, c)$ можно записать в виде $a \vee (b \vee c)$ или $(a \vee b) \vee c$; аналогичное замечание применимо к $a \wedge b$, и это показывает, что (1) и (2) выполняются. Далее, имеет место (3), так как $a \leqslant a \vee b$.

Пусть теперь L — алгебра с двумя операторами $\vee$, $\wedge$, удовлетворяющими (1) — (3). Тогда

$$a \vee b = b \text{ тогда и только тогда, когда } a \wedge b = a. \tag{5}$$

Действительно, если $a \vee b = b$, то в силу (3) $a = a \wedge (a \vee b) = a \wedge b$, а обратное вытекает из соображений симметрии. Если определить отношение $\leqslant$, как в (4), то это отношение будет упорядоченностью: если заданы $a \leqslant b$, $b \leqslant c$, то имеем $a \vee b = b$, $b \vee c = c$, и, следовательно, в силу (1), $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$, т. е. $a \leqslant c$. Далее, в силу (3) имеем $a \wedge (a \vee a) = a$; поэтому $a \vee a = a \vee (a \wedge (a \vee a)) = a$ и, таким образом, $a \leqslant a$. Далее, если $a \leqslant b$, $b \leqslant a$, то в силу (2) $b = a \vee b = b \vee a = a$, и это показывает, что отношение $\leqslant$ является упорядоченностью. По определению оператора $a \vee b$ и в силу (2) $a \vee b$ будет верхней гранью для $\{a, b\}$; если c — также верхняя грань для $\{a, b\}$, то $a \leqslant c$, $b \leqslant c$, откуда $c = a \vee c = b \vee c$ и, таким образом, $c = a \vee (b \vee c) = (a \vee b) \vee c$; этим установлено, что $a \vee b \leqslant c$, т. е. $a \vee b$ является наименьшей верхней гранью элементов a и b.

Так как в силу (5) определение отношения $\leqslant$ симметрично относительно $\vee$ и $\wedge$, то отсюда также следует, что $\inf(a, b) = a \wedge b$. ∎

В силу этого результата структуры можно считать алгебрами, и определения подструктуры и структурного гомоморфизма из § I.4 оказываются частными случаями общих определений из § II.3.

Симметрия, на которую мы сослались при доказательстве предложения 4.1, основана на том наблюдении, что аксиомы структуры преобразуются сами в себя, если переставить $\vee$ и $\wedge$, а также если переставить $\leqslant$ и $\geqslant$. Поэтому, если сделать эти же изменения в некоторой теореме, то мы снова получим теорему, называемую двойственной к первой. Этот принцип, который сокращает работу при доказательстве теорем в теории структур почти вдвое, называется *принципом двойственности* по аналогии с проективной геометрией (которая, по существу, изучает структуру подпространств векторного пространства). Однако этот принцип сокращает работу не совсем вдвое потому, что для некоторых предложений он может и не дать ничего нового (а именно для тех, которые двойственны сами себе).

Пусть в произвольной структуре L заданы такие $a, b \in L$, что $a \leqslant b$; подмножество

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

называется *интервалом*, определенным элементами a и b. Такой интервал не обязан быть цепью, но всегда будет подструктурой структуры L с наибольшим элементом b и наименьшим элементом a. Каждому интервалу $I = [a, b]$ сопоставим два отображения L в I, а именно *операторы проектирования* λ и ρ, определяемые следующим образом:

$$\lambda\colon x \to (x \wedge b) \vee a, \quad \rho\colon x \to (x \vee a) \wedge b.$$

Легко проверить, что утверждения (i) $x \in I$, (ii) $x\lambda = x$ и (iii) $x\rho = x$ эквивалентны; поэтому

$$\lambda\rho = \lambda^2 = \lambda, \qquad \rho\lambda = \rho^2 = \rho.$$

Кроме того, так как $x \wedge b \leqslant x\rho$ и $a \leqslant x\rho$, то отсюда следует, что $x\lambda \leqslant x\rho$, т. е.

$$(x \wedge b) \vee a \leqslant (x \vee a) \wedge b \quad \text{для всех} \quad x \in L. \tag{6}$$

Если в (6) выполняется равенство для всех $x \in L$, то интервал I называется *модулярным*. Особенно важны те структуры, в которых все интервалы модулярны; они называются *модулярными* структурами или *дедекиндовыми* структурами (Дедекинд [00]). Таким образом, структура L модулярна тогда и только тогда, когда

$$(c \vee a) \wedge b \leqslant (c \wedge b) \vee a \text{ для всех таких } a, b, c \in L, \text{ что } a \leqslant b. \tag{7}$$

В силу (6) условие (7) эквивалентно условию

$(c \vee a) \wedge b = (c \wedge b) \vee a$ для всех таких $a, b, c \in L$, что $a \leqslant b$. (8)

Условие (8) иногда называется *законом модулярности*; строго говоря, закон модулярности не является тождеством в обычном смысле (см. § IV. 1 ниже), но эквивалентен некоторому тождеству (см. упр. 1).

Наиболее важным примером модулярной структуры является, вероятно, множество нормальных делителей группы. Множество $\mathcal{N}(G)$ всех нормальных делителей группы G упорядочено по включению и, как легко видеть, будет структурой, в которой

$$A \wedge B = A \cap B,$$
$$A \vee B = AB = \{ab \in G \mid a \in A, \ b \in B\}.$$

Высказывание «структура $\mathcal{N}(G)$ модулярна» равносильно утверждению, что

$$CA \cap B \subseteq (C \cap B)A, \quad \text{если только} \quad A \subseteq B. \tag{9}$$

Для проверки этого возьмем $b \in CA \cap B$, скажем $b = ca$ $(c \in C, a \in A)$; тогда, так как $a^{-1} \in A \subseteq B$, то $c = ba^{-1} \in B$, и потому $c \in C \cap B$, откуда $b \in (C \cap B)A$. Это остается справедливым и для групп с (унарными) операторами; в частности, структура всех подмодулей R-модуля (где R — произвольное кольцо) модулярна.

Выведем теперь критерий модулярности данной структуры. Сначала несколько общих определений. В произвольной структуре L с наименьшим элементом 0 и наибольшим элементом 1 два элемента x и y называются *дополнительными*, если

$$x \wedge y = 0, \quad x \vee y = 1.$$

Элемент, дополнительный к x, называется также *дополнением* элемента x в L. Два элемента, обладающие общим дополнением x в L, называются *x-связанными* или просто *связанными* в L. Это отношение симметрично, но вообще не транзитивно и даже не рефлексивно.

***Предложение* 4.2.** *Структура L модулярна тогда и только тогда, когда в каждом интервале I структуры L любые два сравнимых и связанных в I элемента равны.*

Доказательство. Как мы видели, L не модулярна в том и только в том случае, если выполняется строгое неравенство

$$(c \wedge b) \vee a < (c \vee a) \wedge b \tag{10}$$

по крайней мере для одной тройки таких элементов $a, b, c \in L$, что $a \leqslant b$. Если $a = b$, то обе части неравенства (10) равны в силу закона поглощения, так что можно считать $a < b$. Предположим сначала, что выполняется строгое неравенство (10): положим $a_1 = (c \wedge b) \vee a$,

$b_1=(c\vee a)\wedge b$; тогда $a\leqslant a_1<b_1\leqslant b$; отсюда $c\wedge b_1\leqslant(c\wedge b)\vee a=a_1$, $c\vee a_1\geqslant(c\vee a)\wedge b=b_1$; поэтому $c\wedge b_1=c\wedge a_1=a_2$, $c\vee a_1=$ $=c\vee b_1=b_2$ и, таким образом, a_1 и b_1 сравнимы и связаны в $[a_2, b_2]$, хотя и не равны. Обратно, если a', b' — различные элементы, сравнимые и связанные в $[a, b]$, скажем $a'\wedge c=b'\wedge c=a$, $a'\vee c=b'\vee c=b$ и $a\leqslant a<b'\leqslant b$, то $(c\wedge b')\vee a'=a'<b'=$ $=(c\vee a')\wedge b'$; поэтому L не модулярна. ∎

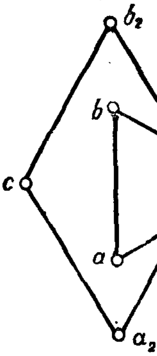

Рис. 1.

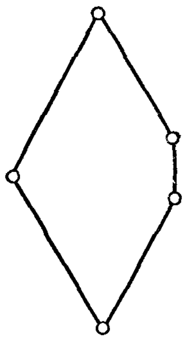
Рис. 2.

Свойство, сформулированное в этом предложении, использует только пять элементов, а именно концевые точки интервала, данный элемент и два его дополнения. Рассматривая подструктуру, образованную этими элементами, получаем

***Следствие* 4.3.** *Структура модулярна тогда и только тогда, когда она не содержит подструктуры, изоморфной пятиэлементной структуре, представленной на рис.* 2. ∎

Второй важный класс структур образуют дистрибутивные структуры. Структура L называется *дистрибутивной*, если она удовлетворяет следующим тождествам:

$$(a\vee b)\wedge c=(a\wedge c)\vee(b\wedge c)\quad \text{для всех}\quad a, b, c\in L, \tag{11}$$

$$(a\wedge b)\vee c=(a\vee c)\wedge(b\vee c)\quad \text{для всех}\quad a, b, c\in L. \tag{12}$$

На самом деле достаточно предполагать, что выполняется одно из тождеств (11), (12), поскольку тогда будет выполняться и другое; это вытекает из следующего предложения, которое показывает также, что каждая дистрибутивная структура модулярна.

***Предложение* 4.4.** *Для любой структуры L следующие три условия эквивалентны:* (i) *условие* (11), (ii) *условие* (12) *и*

(iii) $\quad (c\vee a)\wedge b\leqslant(c\wedge b)\vee a$ *для всех* $a, b, c\in L$.

В частности, каждая дистрибутивная структура L удовлетворяет условию (iii) *и потому модулярна.*

Доказательство. Если выполняется (i), то

$$(c \vee a) \wedge b = (c \wedge b) \vee (a \wedge b) \leqslant (c \wedge b) \vee a.$$

Обратно, предположим, что выполняется (iii), тогда

$$(a \vee b) \wedge c \leqslant (b \wedge c) \vee a;$$

применяя к обеим частям $\wedge c$, получаем

$$(a \vee b) \wedge c \leqslant [(b \wedge c) \vee a] \wedge c \leqslant (a \wedge c) \vee (b \wedge c). \qquad (13)$$

Так как $a \vee b \geqslant (a \wedge c) \vee (b \wedge c)$ и $c \geqslant (a \wedge c) \vee (b \wedge c)$, имеем $(a \vee b) \wedge c \geqslant (a \wedge c) \vee (b \wedge c)$, что вместе с (13) дает (i). Итак, (i)$\Leftrightarrow$(iii), и в силу двойственности (ii)$\Leftrightarrow$(iii), откуда следует, что (i), (ii), (iii) эквивалентны. Кроме того, любая структура, удовлетворяющая (iii), удовлетворяет также (7) и поэтому модулярна. ∎

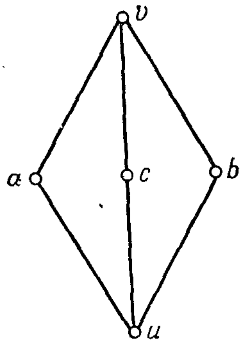

Рис. 3.

Существует критерий дистрибутивности структуры, аналогичный предложению 4.2.

***Предложение* 4.5.** *Структура L дистрибутивна тогда и только тогда, когда в каждом интервале I структуры L любые два связанных в I элемента равны.*

Доказательство. Пусть L дистрибутивна и предположим, что a, b являются c-связанными в $[u, v]$. Тогда

$$a = a \wedge (b \vee c) = (a \wedge b) \vee u = a \wedge b;$$

следовательно, $a \leqslant b$ и так как L модулярна (предложение 4.4), то отсюда вытекает, в силу предложения 4.2, что $a = b$.

Обратно, предположим, что L удовлетворяет данным условиям; тогда по предложению 4.2 L модулярна. Возьмем произвольные три элемента $c_1, c_2, c_3 \in L$; запишем $a_1 = c_2 \wedge c_3$, $b_1 = c_2 \vee c_3$ и, переставляя циклически 1, 2, 3, *определим* a_2, a_3, b_2, b_3. *Так как* $a_i \leqslant b_i$, то в силу закона модулярности имеем

$$(c_i \vee a_i) \wedge b_i = (c_i \wedge b_i) \vee a_i = d_i;$$

положим также $u = a_1 \vee a_2 \vee a_3$ и $v = b_1 \wedge b_2 \wedge b_3$. Тогда, так как $c_2 \wedge b_2 \leqslant b_1$ и $c_1 \leqslant b_2$, имеем (дважды применяя закон модулярности)

$$\begin{aligned}(c_1 \wedge b_1) \vee (c_2 \wedge b_2) &= [c_1 \vee (c_2 \wedge b_2)] \wedge b_1 = \\ &= [(c_2 \vee c_1) \wedge b_2] \wedge b_1 = \\ &= b_3 \wedge b_2 \wedge b_1 = \\ &= v.\end{aligned}$$

Поэтому

$$d_1 \vee d_2 = (c_1 \wedge b_1) \vee a_1 \vee (c_2 \wedge b_2) \vee a_2 = \\ = v \vee a_1 \vee a_2 = v.$$

Циклически переставляя 1, 2 и 3, находим, что

$$d_1 \vee d_2 = d_2 \vee d_3 = d_3 \vee d_1 = v, \tag{14}$$

и в силу двойственности

$$d_1 \wedge d_2 = d_2 \wedge d_3 = d_3 \wedge d_1 = u. \tag{15}$$

Это показывает, что d_i и d_j связаны в $[u, v]$ для $i, j = 1, 2, 3$, $i \neq j$, и, следовательно, $d_1 = d_2 = d_3$. В силу (14) и (15) $u = d_1 = v$ и, таким образом,

$$c_1 \vee a_1 \geqslant u = v \geqslant c_2 \wedge b_2.$$

Подставляя сюда выражения для a_1 и b_2, находим, что

$$c_1 \vee (c_2 \wedge c_3) \geqslant c_2 \wedge (c_1 \vee c_3).$$

Так как c_1, c_2, c_3 — произвольные элементы структуры L, то в силу предложения 4.4 дистрибутивность этим доказана. ▮

Как и раньше, условие этого предложения можно выразить в терминах некоторой пятиэлементной структуры.

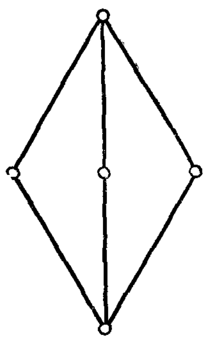

Рис. 4.

***Следствие* 4.6.** *Структура дистрибутивна тогда и только тогда, когда она модулярна и не содержит подструктуры, изоморфной пятиэлементной структуре, представленной на рис. 4.* ▮

Пусть L — модулярная структура и a, b — два произвольных элемента в L; тогда между интервалами $I = [a \wedge b, a]$ и $J = [b, a \vee b]$, как между структурами, существует изоморфизм, который можно установить следующим образом. Для любого $x \in I$ имеем $x \vee b \in J$, и так как $a \wedge b \leqslant x \leqslant a$, то отсюда следует, что $(x \vee b) \wedge a = x \vee (b \wedge a) = x$. Двойственным образом, если $y \in J$, то $y \wedge a \in I$ и $(y \wedge a) \vee b = y$. Таким образом, отображения

$$x \to x \vee b \quad (x \in I), \qquad y \to y \wedge a \quad (y \in J) \tag{16}$$

обратны друг другу. Так как каждое из этих отображений сохраняет упорядоченность, то они устанавливают структурный изоморфизм между I и J. Два произвольных интервала, связанные указанным способом, называются *перспективными* при перспективе (16). В более общем случае два интервала I и J называются *проективными*, если существует цепь от I до J, т. е. цепь $I_0 = I$, I_1, ..., $I_n = J$, таких интервалов, что I_{i-1} и I_i перспективны. Например, если a и b —

произвольные связанные элементы в модулярной структуре с 0 и 1, то интервалы $[0, a]$ и $[0, b]$ проективны.

Так как любые два перспективных интервала изоморфны, то отсюда вытекает, что любые два проективных интервала изоморфны. Эти утверждения можно считать аналогами второй теоремы об изоморфизме, и, как и в теории групп, ими можно воспользоваться для получения теоремы об уплотнении цепей. Две цепи в структуре L

$$e = a_0 \leqslant a_1 \leqslant \ldots \leqslant a_m = a, \tag{17}$$

$$e = b_0 \leqslant b_1 \leqslant \ldots \leqslant b_n = a, \tag{18}$$

между одними и теми же элементами e и a называются *изоморфными*, если $m = n$ и существует такая перестановка π чисел $1, \ldots, n$, что интервал $[a_{i-1}, a_i]$ изоморфен интервалу $[b_{i\pi-1}, b_{i\pi}]$. Если в цепь (17) вставить дополнительные члены, то полученная цепь называется *уплотнением* цепи (17). Теперь может быть сформулирована

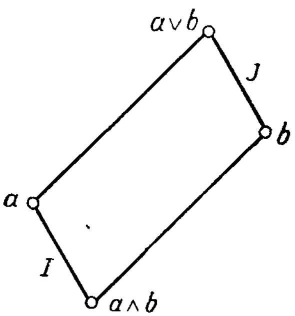

Рис. 5.

***Теорема 4.7.* (*Теорема об уплотнениях цепей.*)** *В модулярной структуре любые две цепи между одними и теми же двумя точками обладают изоморфными уплотнениями.*

Вообще говоря, этот результат остается справедливым и в произвольной структуре для таких двух цепей, все интервалы которых модулярны.

Доказательство. Для произвольных $i = 1, \ldots, m$, $j = 1, \ldots, n$ запишем

$$a_{ij} = (a_i \wedge b_j) \vee b_{j-1}, \quad b_{ji} = (b_j \wedge a_i) \vee a_{i-1},$$

где a_i, b_j — члены цепей (17) и (18) соответственно; аналогично определяются элементы a_{0j} и b_{0i}. Тогда

$$a_{i-1j} \wedge a_i \wedge b_j = (a_{i-1} \vee b_{j-1}) \wedge b_j \wedge a_i$$

и

$$a_{i-1j} \vee (a_i \wedge b_j) = [(a_{i-1} \wedge b_j) \vee b_{j-1}] \vee (a_i \wedge b_j) =$$
$$= (a_i \wedge b_j) \vee b_{j-1} = a_{ij}.$$

Следовательно, интервал $[(a_{i-1} \vee b_{j-1}) \wedge a_i \wedge b_j, a_i \wedge b_j]$ находится в перспективе с $[a_{i-1\,j}, a_{ij}]$, а в силу симметрии также и с $[b_{j-1\,i}, b_{ji}]$.

Таким образом, интервалы $[b_{j-1\,i}, b_{ji}]$ и $[a_{i-1\,j}, a_{ij}]$ изоморфны для $i=1, \ldots, m$, $j=1, \ldots, n$. Теперь цепи

$$e=a_{01}\leqslant a_{11}\leqslant \ldots \leqslant a_{m1}\leqslant a_{12}\leqslant \ldots \leqslant a_{m2}\leqslant a_{13}\leqslant \ldots \leqslant a_{mn}=a,$$

$$e=b_{01}\leqslant b_{11}\leqslant \ldots \leqslant b_{n1}\leqslant b_{12}\leqslant \ldots \leqslant b_{n2}\leqslant b_{13}\leqslant \ldots \leqslant b_{nm}=a$$

являются уплотнениями цепей (17) и (18) соответственно, и, как было показано, эти уплотнения изоморфны. ∎

Определим *длину* произвольной структуры L как точную верхнюю грань числа нетривиальных интервалов (т. е. интервалов с различными концами) в произвольной цепи. В частности, структура будет конечной длины, если существует конечная верхняя грань длин ее цепей; такая структура обязательно имеет наибольший и наименьший элементы. Из теоремы 4.7 мы получим теперь следующий аналог теоремы Жордана — Гёльдера для групп:

***Следствие* 4.8.** *В модулярной структуре конечной длины любую цепь можно уплотнить до максимальной цепи и любые две максимальные цепи между двумя данными концевыми точками имеют одну и ту же длину.*

Действительно, если уплотнить максимальную цепь, то ее длина не изменится, и ясно, что изоморфные максимальные цепи имеют одну и ту же длину. ∎

Если L — модулярная структура конечной длины, то любая ее подструктура снова будет конечной длины; в частности, для каждого $a\in L$ длина интервала $[0, a]$ обозначается через $l(a)$ и называется также *длиной* элемента a. Таким образом, длина самой структуры L равна $l(1)$; ясно, что для любого $a\in L$

$$l(a)\leqslant l(1),$$

и равенство выполняется тогда и только тогда, когда $a=1$. Кроме того, для любых $a, b\in L$, сравнивая длины изоморфных интервалов $[a\wedge b, a]$ и $[b, a\vee b]$, получаем

$$l(a)+l(b)=l(a\wedge b)+l(a\vee b). \tag{19}$$

Интервал называется *простым*, если он нетривиален и не содержит никаких элементов, кроме своих концевых точек. Ясно, что два простых интервала изоморфны; поэтому утверждение, что две максимальные цепи между одними и теми же концевыми точками (в модулярной структуре) изоморфны, просто равносильно высказыванию, что они имеют одну и ту же длину. Этот факт показывает, что следствие 4.8 намного слабее теоремы Жордана — Гёльдера для групп. В действительности это следствие можно усилить, если воспользоваться тем фактом (установленным в процессе доказательства теоремы 4.7), что соответствующие интервалы проективны, а не просто изоморфны.

Однако этого не стоит делать, так как даже и тогда мы не смогли бы получить теорему Жордана — Гёльдера для групп как частный случай, потому что эта теорема относится к цепям подгрупп, каждая из которых нормальна в предшествующей, а не обязательно во всей группе; таким образом, мы не можем ограничиться модулярными структурами. Например, структура всех подгрупп конечной p-группы не обязательно модулярна, хотя любая подгруппа является членом некоторой цепи подгрупп, каждая из которых нормальна в следующей (см. Судзуки [56]).

В противоположность теореме Жордана — Гёльдера, относящейся к максимальным цепям, теорему Крулля — Шмидта, относящуюся к максимальным прямым разложениям, можно сформулировать целиком в пределах структуры нормальных делителей всей группы, а поэтому легче дать теоретико-структурную формулировку теоремы Крулля — Шмидта, чем теоремы Жордана — Гёльдера (хотя последнюю легче доказать). Поэтому сформулируем ее как результат теории структур, а позже (см. § II. 6) применим к общим алгебрам.

Пусть L — модулярная структура с наименьшим элементом 0. Тогда конечное подмножество $\{a_1, a_2, \ldots, a_n\}$ структуры L называется *независимым*, если

$$a_i \wedge (a_1 \vee \ldots \vee a_{i-1} \vee a_{i+1} \vee \ldots \vee a_n) = 0 \quad (i = 1, \ldots, n). \tag{20}$$

Если элемент a представлен в виде объединения независимого множества,

$$a = a_1 \vee \ldots \vee a_n \qquad (a_1, \ldots, a_n \text{ независимы}),$$

то a называется *прямым объединением* элементов $a_1, \ldots, a_n$, и мы пишем

$$a = a_1 \times \ldots \times a_n.$$

Например, если L_i — структура с наименьшим элементом 0_i и наибольшим элементом 1_i $(i = 1,2)$, то в прямом произведении структур L_1 и L_2 имеем

$$(1_1, 1_2) = (1_1, 0_2) \times (0_1, 1_2).$$

Вообще в произвольной структуре L с 0 и 1 любая пара дополнительных элементов a и b определяет представление наибольшего элемента 1 в виде прямого объединения:

$$1 = a \times b.$$

Конечно, это не означает, что L обязательно разлагается в прямое произведение (см., например, рис. 4).

Отметим, что для независимости множества $\{a_1, \ldots a_n\}$ достаточно, чтобы

$$(a_1 \vee \ldots \vee a_{i-1}) \wedge a_i = 0 \quad (i = 2, \ldots, n). \tag{21}$$

Это можно доказать индукцией по n (во всякой модулярной структуре). Мы не будем приводить отдельного доказательства этого результата (читатель легко может восполнить этот пробел), потому что нам нужен этот результат только для модулярных структур конечной длины; в этом случае он непосредственно вытекает из следующего предложения:

***Предложение* 4.9.** *В модулярной структуре конечной длины всякое подмножество* $\{a_1, \ldots, a_n\}$ *удовлетворяет неравенству*

$$l(a_1 \vee \ldots \vee a_n) \leqslant \sum l(a_i), \tag{22}$$

причем равенство имеет место тогда и только тогда, когда элементы $a_1, \ldots, a_n$ *независимы.*

Доказательство. Для $n=1$ утверждение очевидно; поэтому будем доказывать его индукцией по n. Итак, пусть $n>1$; тогда в силу (19)

$$\begin{aligned} l(a_1 \vee \ldots \vee a_n) + l((a_1 \vee \ldots \vee a_{n-1}) \wedge a_n) = \\ = l(a_1 \vee \ldots \vee a_{n-1}) + l(a_n). \end{aligned} \tag{23}$$

Замечая, что $l((a_1 \vee \ldots \vee a_{n-1}) \wedge a_n) \geqslant 0$, и применяя к правой части равенства предположение индукции, получаем, что (22) выполняется всегда. Если в (22) имеем равенство, то отсюда вытекает, в частности, что $l((a_1 \vee \ldots \vee a_{n-1}) \wedge a_n) = 0$, откуда

$$(a_1 \vee \ldots \vee a_{n-1}) \wedge a_n = 0; \tag{24}$$

так как предположение индукции симметрично относительно $a_1, \ldots, a_n$, то имеет место (20); поэтому элементы $a_1, \ldots, a_n$ независимы. Обратно, если $a_1, \ldots, a_n$ независимы, то $a_1, \ldots, a_{n-1}$ независимы; поэтому по предположению индукции

$$l(a_1 \vee \ldots \vee a_{n-1}) = l(a_1) + \ldots + l(a_{n-1});$$

в то же время имеем (24) и, подставляя его в (23), видим, что в (22) имеет место равенство. ∎

Часто приходится применять утверждение о том, что если a является сомножителем в прямом разложении элемента b, то любой элемент интервала $[a, b]$ можно представить в виде прямого объединения, содержащего a в качестве сомножителя. Сформулируем это в виде леммы:

***Лемма* 4.10.** *Если в модулярной структуре с* 0 *и* 1

$$1 = a \times a' \quad \text{и} \quad a \leqslant b,$$

то $b = a \times (b \wedge a')$.

Действительно, $a \wedge (b \wedge a') = a \wedge a' = 0$ и, так как $a \leqslant b$, имеем $a \vee (b \wedge a') = b \wedge (a \vee a') = b$. ∎

Элемент a называется *неразложимым*, если $a \neq 0$ и не существует никакого прямого разложения вида $a = b \times c$, в котором $b \neq a$ и $c \neq a$. Если a представлен в виде прямого объединения неразложимых элементов, то говорят о *полном разложении* для a.

Теорема* 4.11. *(Теорема Крулля — Шмидта для структур.) *Если в модулярной структуре L конечной длины даны два полных разложения наибольшего элемента* 1:

$$1 = a_1 \times \ldots \times a_m \tag{25}$$

и

$$1 = b_1 \times \ldots \times b_n, \tag{26}$$

то каждое a_i связано с некоторым b_j.

Доказательство. Запишем $a'_i = a_1 \times \ldots \times a_{i-1} \times a_{i+1} \times \ldots \ldots \times a_m$ и аналогично определим b'_j относительно $b_1, \ldots, b_n$. Индукцией по длине структуры L докажем, что каждое a_i a'_i-связано с некоторым b_j. Сначала заметим, что для всякого элемента $c \in L$

$$c \leqslant \bigvee_i \left((c \vee a'_i) \wedge a_i\right). \tag{27}$$

Действительно, если для краткости записать $c_i = c \vee a'_i$, то $c_i \geqslant a'_i \geqslant a_k$ для $i \neq k$, откуда

$$\begin{aligned}\bigvee_i (c_i \wedge a_i) &= (c_1 \wedge a_1) \vee (c_2 \wedge a_2) \vee \ldots \vee (c_m \wedge a_m) = \\ &= c_1 \wedge [a_1 \vee (c_2 \wedge a_2) \vee \ldots \vee (c_m \wedge a_m)] = \\ &= c_1 \wedge c_2 \wedge [a_1 \vee a_2 \vee (c_3 \wedge a_3) \vee \ldots \vee (c_m \wedge a_m)] = \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &= c_1 \wedge c_2 \wedge \ldots \wedge c_m \wedge (a_1 \vee a_2 \vee \ldots \vee a_m) \geqslant c,\end{aligned}$$

что и доказывает неравенство (27).

Теперь рассмотрим два случая.

(i) $a_1 \vee b'_j < 1$ *для некоторого* j.

Запишем $c_j = (a_1 \vee b'_j) \wedge b_j$, $c = c_1 \vee \ldots \vee c_n$; тогда, так как $c_j \leqslant b_j$, то элементы $c_1, \ldots, c_n$ снова независимы; поэтому

$$c = c_1 \times \cdots \times c_n. \tag{28}$$

Если бы мы имели $c_j = b_j$ для всех j, то $a_1 \vee b'_j \geqslant b_j$ для всех j и, следовательно, $a_1 \vee b'_j \geqslant b_j \vee b'_j = 1$, что противоречит нашему предположению; поэтому $c_j < b_j$ для некоторого j, откуда следует, что $l(c) < l(1)$, и поэтому можно применить индуктивное предположение к интервалу $[0, c]$. Теперь в силу (27) $c \geqslant a_1$; следовательно, (лемма 4.10),

$$c = a_1 \times (c \wedge a_1'). \tag{29}$$

Если в (28) мы разложим каждое c_j так, чтобы получить полное разложение элемента c, и сравним полученное разложение с (29), то увидим, что неразложимый множитель a_1 $(c \wedge a_1')$-связан с некоторым неразложимым множителем некоторого c_j из (28); скажем, для $j=1$ имеем $c_1 = d \times e$, где d неразложим, и к тому же

$$c = d \times (c \wedge a_1'). \tag{30}$$

Теперь

$$d \vee a_1' = d \vee (c \wedge a_1') \vee a_1' = \\ = a_1 \vee (c \wedge a_1') \vee a_1' = 1.$$

Поскольку a_1 и d связаны, то они имеют одну и ту же длину, и, так как $d \vee a_1' = a_1 \vee a_1' = 1$, то в силу (19) отсюда вытекает, что $d \wedge a_1' = a_1 \wedge a_1' = 0$; таким образом,

$$1 = d \times a_1'. \tag{31}$$

Далее, $d \leqslant c_1 \leqslant b_1$; следовательно, $b_1 = d \times (b \wedge a_1')$ (по лемме 4.10), и так как b_1 неразложим, то отсюда вытекает, что $b_1 = d$; итак, a_1 a_1'-связан с b_1. Заметим, что поскольку $b_1 = d = c_1 = (a_1 \vee b_1') \wedge b_1$, то мы также имеем

$$a_1 \vee b_1' = 1. \tag{32}$$

(ii) $a_1 \vee b'_j = 1$ *для всех* j.

Если $b_j \vee a_1' < 1$ для всех j, то, применяя (i) и поменяв предварительно ролями элементы $a_1, \ldots, a_m$ и $b_1, \ldots, b_n$, видим, что каждый b_j связан с некоторым $a_{j'}$. Таким образом, в (26) можно заменить b_1 на $a_{1'}$, затем b_2 на $a_{2'}$ и так далее до тех пор, пока мы не достигнем такого j, для которого $j' = 1$. Такой индекс j должен существовать, так как в противном случае, перебрав все элементы $b_1, \ldots, b_n$, мы получили бы полное разложение наибольшего элемента 1 на некоторые из элементов a_i, среди которых отсутствовало бы a_1, что противоречит (25). Но если $j' = 1$, то в силу (32) имеем $b_j \vee a_1' = 1$, что противоречит нашему предположению. Следовательно, для некоторого j, скажем для $j = 1$, должно иметь место равенство

$b_j \vee a_1' = 1$. Используя это равенство и тот факт, что $a_1 \vee a_1' = 1$, в силу (19) получаем

$$l(b_1) + l(a_1') = l(1) + l(b_1 \wedge a_1') = l(a_1) + l(a_1') + l(b_1 \wedge a_1'),$$

т. е.

$$l(b_1) - l(a_1) = l(b_1 \wedge a_1') \geqslant 0. \tag{33}$$

Но по предположению имеем также $a_1 \vee b_1' = 1$; отсюда, переставив a_1 и b_1, получаем

$$l(a_1) - l(b_1) = l(a_1 \wedge b_1') \geqslant 0. \tag{34}$$

Сравнение неравенств (33) и (34) показывает, что $l(a_1) = l(b_1)$, и, подставляя это в (33), находим, что $l(b_1 \wedge a_1') = 0$; следовательно, $b_1 \wedge a_1' = 0$ и поэтому $1 = b_1 \times a_1'$, т. е. a_1 a_1'-связан с b_1. ∎

Если в этой теореме взять разложение (25) и заменить элемент a_1 на некоторый связанный с ним элемент b_j, скажем на b_1, а затем заменить a_2 на некоторый b_j (второй раз применяя теорему), то ясно, что этот b_j будет отличен от b_1 и после изменения нумерации можно считать его равным b_2. По индукции получаем разложение

$$1 = b_1 \times b_2 \times \ldots \times b_{i-1} \times a_i \times \ldots \times a_m$$

для $i = 1, 2, \ldots, m$. В частности, взяв $i = m$, видим, что $n \geqslant m$, а в силу симметрии $m \geqslant n$. Таким образом, имеем

Следствие 4.12. *Если даны два полных разложения* (25) *и* (26) *наибольшего элемента* 1 *в модулярной структуре конечной длины, то $m = n$ и для некоторой перестановки π чисел $1, \ldots, n$ интервал $[0, a_i]$ проективен интервалу $[0, b_{i\pi}]$.* ∎

В дистрибутивной структуре связанные элементы равны, и потому имеет место

Следствие 4.13. *В дистрибутивной структуре конечной длины сомножители в полном разложении наибольшего элемента* 1 *определены однозначно, с точностью до их порядка.* ∎

В некоторых случаях представляют интерес разложения вида

$$1 = a_1 \vee \ldots \vee a_m, \tag{35}$$

где $a_1, \ldots, a_m$ не обязательно независимы, но вместо этого каждый элемент a_i предполагается *неприводимым*, т. е. a_i не может быть представлен в виде объединения двух элементов, каждый из которых отличен от a_i. При этом естественно ограничиться *несократимыми* разложениями, т. е. разложениями вида (35), в которых ни один из a_i не может быть отброшен. Такое разложение определяет каждое a_i не так точно, как прямое разложение, и потому нельзя ожидать столь же сильного утверждения о единственности, как в теореме Крулля — Шмидта; однако мы снова получаем свойство замещения, которое сформулировано в следующей теореме:

Теорема 4.14. ***(Теорема Куроша — Оре.)*** *Пусть в модулярной структуре L даны два представления наибольшего элемента 1 в виде несократимого объединения неприводимых элементов:*

$$1 = p_1 \vee \ldots \vee p_r, \tag{36}$$

$$1 = q_1 \vee \ldots \vee q_s. \tag{37}$$

Тогда $r = s$ и каждый элемент p_i может быть замещен на некоторый элемент q_j, т. е. после подходящего изменения нумерации элементов $q_1, \ldots, q_s$ получаем

$$1 = q_1 \vee \ldots \vee q_i \vee p_{i+1} \vee \ldots \vee p_r \quad (i = 1, \ldots, r). \tag{38}$$

Доказательство. Пусть $p_1' = p_2 \vee \ldots \vee p_r$; тогда, в силу несократимости данного разложения, $p_1' < 1$ и $p_1' \vee p_1 = 1$. Положим $a_j = p_1' \vee q_j$; тогда $1 \geqslant a_j \geqslant p_1'$; следовательно, $p_1 \geqslant p_1 \wedge a_j \geqslant \geqslant p_1 \wedge p_1'$. Теперь p_1 неприводим в $[p_1 \wedge p_1', p_1]$, отсюда элемент 1 неприводим в $[p_1', 1]$, и так как $a_1 \vee \ldots \vee a_s = 1$, то $a_j = 1$ для некоторого j, скажем для $j = 1$. Но это означает, что

$$1 = q_1 \vee p_2 \vee \ldots \vee p_r.$$

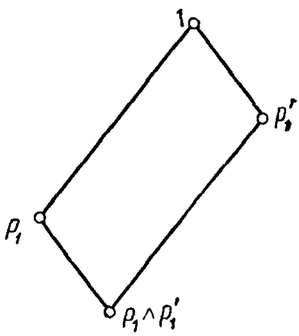

Рис. 6.

Это представление снова несократимо, потому что q_1 не может быть отброшен, а если бы можно было отбросить какой-нибудь p_i, то, заменяя q_1 на некоторое p_j из (36), мы получили бы более короткое разложение наибольшего элемента 1 относительно одних только элементов $p_1, \ldots, p_r$. Поэтому, повторяя этот процесс и заменяя p_2 на некоторый q_j, мы должны получить $j \neq 1$ и после изменения нумерации элементов $q_1, \ldots, q_s$ можем считать, что $j = 2$. Продолжая таким образом, получаем (38); при $i = r$ это показывает, что $r \geqslant s$, а в силу симметрии заключаем, что $r = s$. ∎

Эта теорема, быть может, лучше известна в двойственной форме, в которой она впервые была доказана Э. Нётер [21] для идеалов в нётеровых кольцах (единственность примарных разложений). В абстрактной форме эта теорема была доказана в работах Куроша [35] и Оре [36]. В этой же работе Оре доказал и теорему Крулля — Шмидта в структурной форме. По обеим этим теоремам существует большая литература (см., например, Биркгоф [48]).

Для дистрибутивных структур мы снова получаем сильную единственность:

***Предложение* 4.15.** *В дистрибутивной структуре каждое несократимое представление наибольшего элемента* 1 *в виде объединения неприводимых элементов,*

$$1 = p_1 \vee \ldots \vee p_r,$$

единственно с точностью до порядка членов.

Доказательство. Предположим, что существует второе такое разложение $1 = q_1 \vee \ldots \vee q_s$; тогда $p_1 \leqslant 1 = q_1 \vee \ldots \vee q_s$, откуда

$$p_1 = p_1 \wedge (q_1 \vee \ldots \vee q_s) = \\ = (p_1 \wedge q_1) \vee (p_1 \wedge q_2) \vee \ldots \vee (p_1 \wedge q_s).$$

Так как p_1 неприводим, то $p_1 = p_1 \wedge q_j$ для некоторого j, т. е.

$$p_1 \leqslant q_j.$$

С помощью точно таких же рассуждений получаем $q_j \leqslant p_i$ для некоторого i, и, таким образом, $p_1 \leqslant p_i$, что возможно только при $i = 1$. Отсюда $p_1 = q_j$; теперь по индукции получаем нужный результат. ∎

УПРАЖНЕНИЯ

1. Показать, что структура L модулярна тогда и только тогда, когда для любых $a, b, c \in L$

$$(c \wedge (a \vee b)) \vee b = (c \vee b) \wedge (a \vee b).$$

2. Показать, что структура L дистрибутивна тогда и только тогда, когда $a \wedge b \leqslant c$ и $a \leqslant b \vee c$ влечет $a \leqslant c$ для любых $a, b, c \in L$.

3. Показать, что структура подгрупп прямого произведения двух циклических групп второго порядка модулярна, но не дистрибутивна.

4. Показать, что структура подгрупп знакопеременной группы четвертой степени не модулярна.

5. В структуре L с наименьшим элементом 0 элемент a называется *атомом*, если интервал $[0, a]$ простой. Показать, что если L — модулярная структура, в которой 1 является прямым объединением двух атомов, скажем a и b, то L разлагается в прямое произведение интервалов $[0, a]$ и $[0, b]$ тогда и только тогда, когда L дистрибутивна.

6. Пусть L — модулярная структура с наименьшим элементом 0. Пусть даны три таких элемента $c_1, c_2, c_3 \in L$, что $c_1 \wedge c_2 = 0$ и $c_1 \wedge (c_2 \vee c_3) \neq 0$. Показать, что $(c_1 \vee c_2) \wedge c_3 \neq 0$. (Это свойство известно как *свойство замещения;* см. § VII. 2.)

7. Структура называется *структурой с дополнениями*, если в ней имеются 0 и 1 и каждый элемент обладает дополнением. Показать, что модулярная структура конечной длины будет структурой с дополнениями тогда и только тогда, когда 1 является объединением атомов. [В структуре всех подмодулей унитарного модуля оба эти условия эквивалентны и без пред-

положения конечной длины (см., например, Картан и Эйленберг [56], гл. I), но в общем случае ни одно из них не вытекает из другого (см. следующее упр. и упр. V.2.5).]

8. Положительные числа образуют структуру с наименьшим элементом 1 относительно упорядоченности по делимости. Показать, что если присоединить наибольший элемент U, определенный как точная верхняя грань всех элементов этой структуры, то U можно представить в виде (бесконечного) объединения атомов, но полученная структура не будет структурой с дополнениями.

9. Коммутативная область целостности называется *кольцом Безу*, если ее главные идеалы образуют подструктуру в структуре всех идеалов. Показать, что в кольце Безу структура главных идеалов дистрибутивна. (Указание: заметить, что эта структура модулярна, и воспользоваться предложением 4.5. В книге Зарисского и Самюэля [58] (гл. V) показано, что дистрибутивность структуры идеалов кольца эквивалентна китайской теореме об остатках.)

10. Пусть L — множество главных идеалов в коммутативной области целостности, упорядоченное по включению. Показать, что если $a, b \in L$ имеют точную нижнюю грань, то они имеют и точную верхнюю грань, но что обратное, вообще говоря, не верно. (Здесь упорядоченность противоположна упорядоченности, определенной в упр. 8. Указание: рассмотреть кольцо полиномов от x с целыми коэффициентами и четным коэффициентом при x.) Показать, что если каждая пара элементов имеет точную верхнюю грань, то L будет структурой.

11. Показать, что в любой структуре L подструктура, порожденная двумя цепями с модулярными интервалами, дистрибутивна.

12. Дать прямое доказательство следствия 4.13 (не используя теоремы 4.11).

13. Показать, что модулярная структура L дистрибутивна тогда и только тогда, когда для любых $a, b_1, b_2 \in L$ равенство $a \wedge b_1 = a \wedge b_2 = c$ влечет $a \wedge (b_1 \vee b_2) = c$.

14. Определить *централизатор* эквивалентности $\mathfrak{q}$ на множестве S как

$$Z_\mathfrak{q} = \{\mathfrak{r} \in \mathscr{C}(S) \mid \mathfrak{r} \circ \mathfrak{q} = \mathfrak{q} \circ \mathfrak{r}\}.$$

Показать, что $Z_\mathfrak{q}$ будет подструктурой структуры $\mathscr{C}(S)$.

15. Пусть L — модулярная структура с 0 и 1. Показать, что если даны $a \leqslant x \leqslant b$ и если x' — дополнение элемента x в L, то $(x' \vee a) \wedge b$ будет дополнением элемента x в $[a, b]$.

16. Показать, что модулярная структура имеет конечную длину тогда и только тогда, когда она удовлетворяет условиям максимальности и минимальности.

17. Показать, что дистрибутивная структура конечной длины конечна. (Заметить, что дополнением любого атома a будет всякий максимальный элемент $b \not\geqslant a$. Применить теперь предложение 4.5 и воспользоваться индукцией по n.)

5. СТРУКТУРА ПОДАЛГЕБР

Зафиксируем теперь Ω-алгебру A и рассмотрим множество $\mathscr{B}_\Omega(A)$ всех ее подалгебр. Заметим сначала, что $\mathscr{B}_\Omega(A)$ будет системой замыканий на A и, следовательно, полной структурой. Действительно, если $(A_\lambda)_{\lambda \in \Lambda}$ — семейство подалгебр алгебры A, то для каждого $\omega \in \Omega$ каждая подалгебра A_λ замкнута относительно ω, и поэтому то же самое верно для $\bigcap A_\lambda$. Обозначим соответствующий оператор замыкания через J_Ω; таким образом, $J_\Omega(X)$ будет пересечением всех подалгебр, содержащих X. Следующее предложение дает явный способ построения $J_\Omega(X)$.

***Предложение* 5.1.** *Пусть A — некоторая Ω-алгебра и X — подмножество алгебры A. Определим подмножество X_k алгебры A индукцией по k:*

$$X_0 = X,$$

$$X_{k+1} = \{x \in A \mid x \in X_k \text{ или } x = a\omega \text{ для некоторого } a \in X_k^n \text{ и } \omega \in \Omega(n)\};$$

тогда

$$\bigcup_{k=0}^{\infty} X_k = J_\Omega(X).$$

Доказательство. Если положим $U = \bigcup X_k$, то по определению X_k имеем $X_0 \subseteq J_\Omega(X)$, и если $X_k \subseteq J_\Omega(X)$, то $X_{k+1} \subseteq J_\Omega(X)$; по индукции отсюда вытекает, что $X_k \subseteq J_\Omega(X)$ для всех k, и поэтому $U \subseteq J_\Omega(X)$. С другой стороны, U служит подалгеброй алгебры A. Действительно, если $a \in U^n$, скажем $a = (a_1, \ldots, a_n)$, где $a_i \in X_{k_i}$, и если $k = \max\{k_1, \ldots, k_n\}$, то $a \in X_k^n$, откуда $a\omega \in X_{k+1} \subseteq U$. Это показывает, что U — подалгебра; так как она содержит X, то должна содержать $J_\Omega(X)$, и поэтому $U = J_\Omega(X)$. ∎

Назовем $J_\Omega(X)$ *объединением* множества X или *подалгеброй, порожденной множеством* X, а X — *множеством образующих* подалгебры $J_\Omega(X)$. В частности, множеством образующих алгебры A будет такое подмножество X из A, что $J_\Omega(X) = A$. Если A обладает конечным множеством образующих, то говорят, что A — алгебра с *конечным числом образующих*. Каждая Ω-алгебра содержит наименьшую подалгебру, а именно подалгебру $J_\Omega(\varnothing)$, порожденную пустым множеством. Эта подалгебра называется *минимальной подалгеброй*; ясно, что она пуста тогда и только тогда, когда Ω не содержит постоянных операторов[1]).

Из предложения 5.1 можно вывести, что оператор J_Ω будет алгебраическим. Действительно, если $a \in J_\Omega(X)$, то $a \in X_k$ для некоторого k. Возьмем наименьшее число k, для которого в X_k существует элемент a, не принадлежащий $J_\Omega(X')$ ни для какого конечного подмножества X' множества X; тогда $k > 0$ и такой элемент не может принадлежать X_{k-1}. Следовательно, по определению X_k существует

[1]) Это показывает, что тривиальная подалгебра не обязательно минимальна и что, вообще говоря, минимальная подалгебра не является тривиальной.

такое $\omega \in \Omega$ и такие $b_1, \ldots, b_n \in X_{k-1}$, где $a(\omega) = n$, что $a = b_1 \cdots b_n\omega$. По определению числа k имеем $b_i \in J_\Omega(Y_i)$, где Y_i — конечное подмножество множества X. Отсюда $a \in J_\Omega(Y)$, где $Y = \bigcup Y_i$ снова конечно. Это противоречит определению элемента a, и отсюда мы заключаем, что каждый элемент подалгебры $J_\Omega(X)$ принадлежит $J_\Omega(X')$ для некоторого конечного подмножества X' множества X, т. е. оператор J_Ω — алгебраический.

Справедливо также и обратное утверждение:

Если $\mathscr{C}$ — произвольная алгебраическая система замыканий на множестве A, то для подходящего Ω существует такая структура Ω-алгебры на A, что $\mathscr{B}_\Omega(A) = \mathscr{C}$.

Для доказательства обозначим через J оператор замыкания для $\mathscr{C}$. Если заданы элементы $a_1, \ldots, a_n \in A$ и $b \in J(\{a_1, \ldots, a_n\})$, то возьмем символ

$$\omega = \omega(a_1, \ldots, a_n, b) \in \Omega \tag{1}$$

и определим n-арную операцию на A по правилу:

$$x_1 \cdots x_n\omega = \begin{cases} b, & \text{если } x_i = a_i \quad (i = 1, \ldots, n) \text{ или если } n = 0, \\ x_1 & \text{в противном случае.} \end{cases}$$

Это определяет структуру Ω-алгебры на A, где для каждого натурального числа n операторы из $\Omega(n)$ заданы формулой (1). Возможно, что таким образом определено бесконечно много операторов, но каждый из них будет конечноместным. Пусть J_Ω — оператор замыкания, соответствующий системе $\mathscr{B}_\Omega(A)$ подалгебр; мы утверждаем, что $J = J_\Omega$. Пусть $X \subseteq A$ и предположим сначала, что X конечно. Тогда $J(X) = J_\Omega(X)$ по определению системы операторов Ω. Пусть теперь X — произвольное подмножество множества A; тогда, так как оба оператора замыкания J и J_Ω — алгебраические (первый по предположению, а второй в силу доказанного выше), имеем

$$J(X) = \bigcup J(X') = \bigcup J_\Omega(X') = J_\Omega(X),$$

где X' пробегает конечные подмножества множества X. Итак, доказан следующий результат, принадлежащий Ф. Холлу (не опубликован) и Ю. Шмидту [52]:

***Теорема* 5.2.** *Система $\mathscr{B}_\Omega(A)$ подалгебр Ω-алгебры A является алгебраической системой замыканий. Обратно, если дана алгебраическая система замыканий $\mathscr{C}$ на множестве A, то для подходящей области операторов Ω можно определить такую структуру Ω-алгебры на A, что $\mathscr{B}_\Omega(A) = \mathscr{C}$.* ∎

Конечно, в теореме 5.2 можно выбрать структуру Ω-алгебры многими способами так, чтобы получалась данная система замыканий.

В частности, область операторов часто можно выбрать более экономно, чем это было сделано выше.

Теорема 5.2 вместе с теоремой 1.4 дает важное следствие из леммы Цорна (Нейман [37′]):

Теорема 5.3. *Пусть A есть Ω-алгебра, B — подалгебра и S — подмножество алгебры A. Тогда существует подалгебра C алгебры A, максимальная относительно свойств $C \supseteq B$ и $C \cap S = B \cap S$.*

Если вспомнить, что $B_\Omega(A)$ — алгебраическая система замыканий, то этот результат получается простой переформулировкой теоремы 1.4. ∎

Если мы попытаемся применить теорему 5.3 для $S = \varnothing$, то сделаем очевидный вывод, что сама алгебра A удовлетворяет условиям теоремы; ясно, что A—(единственный) наибольший элемент системы $\mathscr{B}_\Omega(A)$, и чтобы это получить, не нужно пользоваться теоремой 5.3. С другой стороны, множество всех *собственных* подалгебр алгебры A, т. е. всех подалгебр, отличных от самой алгебры, может не иметь ни наибольшего, ни даже максимального элемента (см. упр. 3). Однако в некотором частном случае можно утверждать, что максимальные собственные подалгебры существуют (см. Нейман [37′]).

Теорема 5.4. *Пусть A есть Ω-алгебра с конечным числом образующих и B — собственная подалгебра алгебры A; тогда существует максимальная собственная подалгебра, содержащая B.*

Доказательство. По предположению A обладает конечным множеством образующих, скажем $\{x_1, \ldots, x_r\}$. Пусть $\mathscr{S}$ — множество всех собственных подалгебр алгебры A, содержащих B. Тогда $\mathscr{S}$ не пусто, поскольку $B \in \mathscr{S}$, и чтобы доказать сформулированный результат, нужно только показать, что $\mathscr{S}$ индуктивно. Пусть $\mathscr{C}$ — цепь в $\mathscr{S}$ и положим $C = \bigcup \mathscr{C}$; если $C = A$, то $x_i \in C$ для каждого $i = 1, \ldots, r$ и, следовательно, $x_i \in C_i$ для некоторого $C_i \in \mathscr{C}$. Так как $\mathscr{C}$ — цепь, то существует такой индекс j, что $C_i \subseteq C_j$ и, следовательно, $x_i \in C_j$ для $i = 1, \ldots, r$; так как $x_1, \ldots, x_r$ порождают A, то $C_j = A$, а это противоречит тому факту, что C_j — собственная подалгебра. Итак, подалгебра C должна быть собственной, но она содержит B и потому $C \in \mathscr{C}$. Этим показано, что множество $\mathscr{S}$ индуктивно, и по лемме Цорна оно содержит максимальный элемент. ∎

Алгебра с конечным множеством образующих всегда обладает минимальным множеством образующих: если дано некоторое конечное множество образующих X алгебры A, то нужно только взять минимальное множество среди тех множеств образующих Y алгебры A, для которых $Y \subseteq X$, а это всегда возможно. В противоположность этому, если A не обладает конечным множеством образующих, то она может не иметь минимального множества образующих (как, например, аддитивная группа рациональных чисел); однако, когда алгебра обладает минимальным множеством образующих, его мощность полностью определяется данной алгеброй:

***Предложение* 5.5.** *Пусть A есть Ω-алгебра и X — минимальное множество образующих этой алгебры. Если X—бесконечное множество и α — его мощность, то мощность любого множества образующих алгебры A не меньше α. В частности, A не может обладать конечным множеством образующих, и любые два минимальных множества образующих алгебры A равномощны.*

Доказательство. Пусть Y — произвольное множество образующих алгебры A; запишем $|Y|=\beta$. Каждый $y \in Y$ принадлежит алгебре $A = J_\Omega(X)$, и, следовательно, существует такое конечное подмножество X_y множества X, что

$$y \in J_\Omega(X_y). \tag{2}$$

Мы утверждаем, что

$$X = \bigcup X_y. \tag{3}$$

Действительно, ясно, что $\bigcup X_y \subseteq X$, и в силу (2) $J_\Omega(\bigcup X_y) \supseteq \supseteq J_\Omega(Y) = A$; таким образом, $\bigcup X_y$ оказывается подмножеством множества X, которое также порождает алгебру A, и поэтому (3) вытекает из минимальности множества X. Теперь, если Y конечно, то (3) показывает, что X является объединением конечного числа конечных множеств, что противоречит бесконечности множества X. Следовательно, Y бесконечно, и из (3) находим, что

$$\alpha = |X| \leqslant \sum |X_y| \leqslant \aleph_0\beta = \beta.$$

Это показывает, что мощность множества Y не меньше α. Если Y также минимально, то, заменив X на Y, видим, что $\beta \leqslant \alpha$, и, следовательно, $\alpha = \beta$. ∎

Для алгебр с конечными множествами образующих этот результат не сохраняется; например, циклическая группа шестого порядка имеет один образующий элемент, скажем a, и минимальное множество образующих из двух элементов, а именно $\{a^2, a^3\}$. Тем не менее в некоторых случаях аналогичный результат имеет место, а именно для множеств свободных образующих некоторых свободных алгебр (§ III.5).

В заключение докажем некоторое структурное свойство, показывающее, что несколько особую роль играют унарные (и 0-арные) операторы. Напомним, что $\mathscr{B}_\Omega(A)$, как всякая система замыканий, является полной структурой, но, конечно, не обязательно подструктурой структуры $\mathscr{B}(A)$. Высказывание, что $\mathscr{B}_\Omega(A)$ — подструктура структуры $\mathscr{B}(A)$, означало бы, что для любых $B, C \in \mathscr{B}_\Omega(A)$ имеют место включения

$$B \cap C \in \mathscr{B}_\Omega(A), \quad B \cup C \in \mathscr{B}_\Omega(A).$$

Первое из этих условий выполняется всегда, чего нельзя сказать о втором; например, объединение двух подгрупп в общем случае не будет подгруппой. На самом деле второе условие как раз выражает тот факт, что $\mathscr{B}_\Omega(A)$ является топологической системой замыканий. Это условие можно выразить также на языке области операторов следующим образом.

Теорема 5.6. *Пусть $\mathscr{C}$ — алгебраическая система замыканий на множестве A; тогда следующие три условия относительно $\mathscr{C}$ эквивалентны:*

(i) *$\mathscr{C}$ — подструктура структуры $\mathscr{B}(A)$.*
(ii) *$\mathscr{C}$ — топологическая система замыканий.*
(iii) *Существует такая область операторов Ω, арность операторов которой не больше единицы (т. е. все они унарны или 0-арны), и такая структура Ω-алгебры на A, что $\mathscr{B}_\Omega(A) = \mathscr{C}$.*

Доказательство. Эквивалентность (i) и (ii) вытекает из определений. Предположим теперь, что имеет место (iii), и пусть $B, C \in \mathscr{B}_\Omega(A)$. Тогда всякий 0-арный оператор определяет элемент подалгебры $B \cap C$, в то время как унарный оператор, примененный к $b \in B$, дает элемент из B, а примененный к $c \in C$ дает элемент из C. Таким образом, $B \cup C$ замкнуто относительно Ω, т. е. $B \cup C \in \mathscr{B}_\Omega(A)$.

Обратно, если $\mathscr{C}$ — топологическая система замыканий и J — соответствующий оператор замыкания, то для каждого $a \in J(\varnothing)$ возьмем 0-арный оператор $\lambda = \lambda(a)$ и положим $\lambda = a$. Далее, пусть $a \in A$; тогда для каждого $b \in J(\{a\})$ возьмем унарный оператор $\mu = \mu(a, b)$ и положим

$$x\mu = \begin{cases} b, & \text{если } x = a, \\ x & \text{в противном случае.} \end{cases}$$

Пусть Ω — множество всех λ, μ. Для завершения доказательства осталось показать, что $\mathscr{B}_\Omega(A) = \mathscr{C}$ или, что то же самое,

$$J_\Omega(X) = J(X) \tag{4}$$

для всех подмножеств X множества A. Если X пусто или состоит из единственного элемента, то (4) следует из определения множества операторов Ω. Но оба оператора J и J_Ω топологические (первый — по предположению, а второй — в силу первой части доказательства); следовательно, по индукции, (4) имеет место для всех конечных подмножеств множества A. Наконец, оба оператора J и J_Ω алгебраические, и поэтому (4) имеет место в общем случае. ∎

При применении этой теоремы нужно соблюдать некоторую осторожность. Так, если A есть Ω-алгебра, для которой система $\mathscr{B}_\Omega(A)$

топологическая, то отсюда не следует, что Ω состоит только из операторов, арность которых не больше единицы; например, она может иметь бинарный оператор, который на A, быть может, не зависит от второго аргумента. Это не означает также, что $\mathscr{B}_\Omega(A)$ можно определить на языке одних только 0-арных и унарных операторов области Ω; может случиться, что для этого придется строить новую область операторов (состоящую только из 0-арных и унарных операторов) (см. упр. 4).

Тем же способом доказывается следующее обобщение теоремы 5.6, которое понадобится в дальнейшем. Если Ω^* — область операторов, содержащая Ω, то говорят, что структура Ω-алгебры A *расширена* до структуры Ω^*-алгебры, если на A определена такая структура Ω^*-алгебры, что действие любого $\omega \in \Omega$ такое же, как в A.

Теорема 5.7. *Пусть A есть Ω-алгебра и предположим, что на A задана структура Ω^*-алгебры, которая расширяет данную структуру Ω-алгебры на A, где $\Omega^* \supseteq \Omega$. Тогда $\mathscr{B}_{\Omega^*}(A) \subseteq \mathscr{B}_\Omega(A)$ и, кроме того, $\mathscr{B}_{\Omega^*}(A)$ будет подструктурой $\mathscr{B}_\Omega(A)$ тогда и только тогда, когда Ω можно расширить присоединением только 0-арных и унарных операторов до такой области Ω', что на A можно определить структуру Ω'-алгебры, расширяющую данную Ω-структуру так, что*

$$\mathscr{B}_{\Omega'}(A) = \mathscr{B}_{\Omega^*}(A).$$

Доказательство такое же, как в теореме 5.6; с другой стороны, мы получим отсюда теорему 5.6 как частный случай, если заменим Ω^* на Ω, а Ω на $\varnothing$. ∎

УПРАЖНЕНИЯ

1. Если $f: A \to B$, $g: A \to B$ — гомоморфизмы Ω-алгебр, то множество $A_0 = \{x \in A \mid xf = xg\}$ будет подалгеброй алгебры A.

2. Пусть A есть Ω-алгебра; элемент $a \in A$ называется *необразующим* для A, если для любого подмножества X алгебры A равенство $J_\Omega(X \cup \{a\}) = A$ влечет $J_\Omega(X) = A$. Показать, что множество всех необразующих алгебры A будет подалгеброй в A (называемой *подалгеброй Фраттини*), выдерживающей все автоморфизмы алгебры A. Показать также, что подалгебра Фраттини является пересечением всех максимальных собственных подалгебр алгебры A (если максимальных собственных подалгебр в A не существует, то это пересечение равно A как пересечение пустого семейства подалгебр).

3. Показать, что аддитивная группа рациональных чисел не имеет максимальных собственных подгрупп. Показать также, что эта группа не имеет минимального множества образующих, но что кольцо рациональных чисел обладает минимальным множеством образующих.

4. Пусть G — неодноэлементная группа, и ω — бинарный оператор, определенный на G по правилу:

$$ab\omega = \begin{cases} ab^{-1}, & \text{если один из элементов } a, b \text{ является степенью другого,} \\ 1 & \text{в противном случае.} \end{cases}$$

Взяв $\Omega = \{\omega\}$, проверить, что структура подалгебр Ω-алгебры G топологическая, несмотря на то что Ω вовсе не содержит ни унарных, ни 0-арных операторов.

5. Пусть $\mathscr{C}$ — алгебраическая система замыканий на множестве A. Показать, что

(a) $\mathscr{C}$ можно считать структурой всех подалгебр относительно некоторой структуры Ω-алгебры на A (где Ω состоит только из унарных операторов) тогда и только тогда, когда система $\mathscr{C}$ топологическая и $\varnothing \in \mathscr{C}$;

(b) $\mathscr{C}$ можно считать структурой всех подалгебр относительно некоторой структуры Ω-алгебры на A (где Ω состоит только из 0-арных операторов) тогда и только тогда, когда $\mathscr{C}$ состоит из всех подмножеств множества A, содержащих данное фиксированное подмножество A_0 из A.

6. Показать, что в структуре $\mathscr{B}_\Omega(A)$ подалгебр Ω-алгебры A каждый интервал, у которого концевые точки не совпадают, содержит простой интервал. (Указание: использовать тот факт, что $\mathscr{B}_\Omega(A)$ является полной структурой.)

7. Пусть A есть Ω-алгебра и B — ее подалгебра; тогда B обладает конечным числом образующих в том и только том случае, если B нельзя представить в виде $\sup(B_\lambda)$, где $(B_\lambda)_{\lambda \in \Lambda}$ — направленное семейство подалгебр $\neq B$ алгебры A.

8. (Биркгоф и Фринк.) Пусть L — полная структура; элемент $a \in L$ называется *недостижимым*, если его нельзя представить в виде $\sup(a_\lambda)$, где $(a_\lambda)_{\lambda \in \Lambda}$ — направленное семейство в L. Показать, что полная структура L изоморфна структуре $\mathscr{B}_\Omega(A)$ всех подалгебр некоторой Ω-алгебры A (для некоторого Ω) тогда и только тогда, когда каждый элемент структуры L представим в виде объединения недостижимых элементов и, кроме того, L *непрерывна сверху*, т. е. для любого $a \in L$ и направленного семейства $(b_\lambda)_{\lambda \in \Lambda}$ в L

$$a \wedge \Big(\bigvee_{\lambda \in \Lambda} b_\lambda\Big) = \bigvee_{\lambda \in \Lambda} (a \wedge b_\lambda).$$

(Указание: в качестве A взять множество недостижимых элементов структуры L и определить замыкание подмножества $X \subseteq A$ как наименьший левый отрезок структуры L, содержащий подструктуру, порожденную множеством X.) [1])

9. Показать, что алгебра, порожденная пустым множеством $\varnothing$, не имеет собственных подалгебр.

---

[1]) Грецер и Шмидт (*Acta Sci. Math.*, 24 (1963), 34—59) показали, что эта же характеризация сохраняется для полных структур, изоморфных структуре всех конгруэнций некоторой алгебры, а Искандер (*Изв. АН СССР*, серия матем., **29** (1965), 1357—1372) — для полных структур, изоморфных структуре всех соответствий некоторой алгебры (т. е. всех подалгебр ее прямого квадрата); последнее обобщает нетривиальную часть теоремы Биркгофа — Фринка. — *Прим. ред.*

10. Показать, что если A — произвольная алгебра с конечным числом образующих, то всякое множество образующих алгебры A содержит конечное подмножество, которое порождает A.

11. Для любого множества X определить на X^2 множество Ω конечноместных операторов так, чтобы соответствующие Ω-подалгебры были в точности предупорядоченностями множества X. (См. упр. 1.10.)

6. СТРУКТУРА КОНГРУЭНЦИЙ

Пусть A — некоторая Ω-алгебра; вместе с множеством $\mathscr{C}_\Omega(A)$ всех конгруэнций будем рассматривать множество $\mathscr{C}(A)$ эквивалентностей на A (как на множестве). Заметим, что в частном случае, когда $\Omega = \varnothing$, имеем $\mathscr{C}_\Omega(A) = \mathscr{C}(A)$, так что любой результат относительно $\mathscr{C}_\Omega$ применим также к $\mathscr{C}$. В общем случае имеют место включения

$$\mathscr{C}_\Omega(A) \subseteq \mathscr{C}(A) \subseteq \mathscr{B}(A^2). \tag{1}$$

Легко видеть (это также будет следовать из теоремы 6.2), что $\mathscr{C}_\Omega(A)$ всегда является полной структурой. В частности, $\mathscr{C}(A)$ тоже будет полной структурой, и наша цель состоит в том, чтобы установить соотношения между структурами из (1). Оказывается, что хотя $\mathscr{C}(A)$ не обязательно будет подструктурой структуры $\mathscr{B}(A^2)$, $\mathscr{C}_\Omega(A)$ всегда является подструктурой в $\mathscr{C}(A)$.

По определению, конгруэнцией называется эквивалентность, замкнутая относительно операторов ω $(\omega \in \Omega)$. Теперь каждый n-арный оператор ω определяет n-арную операцию на A:

$$(x_1, \ldots, x_n) \to x_1 \ldots x_n\omega. \tag{2}$$

Фиксируя в A значения некоторых из аргументов, получаем r-арные операции для $r \leqslant n$; в частности, если зафиксируем все x_i, кроме одного, то получим для любых $n-1$ элементов $a_1, \ldots, a_{n-1} \in A$ и любого $i = 1, \ldots, n$ унарную операцию

$$x \to a_1 \ldots a_{i-1} x a_i \ldots a_{n-1}\omega. \tag{3}$$

Будем говорить, что операция (3) является *элементарной трансляцией*, полученной из (2) *специализацией* в A. Вообще отображение θ: $A \to A$ называется *трансляцией*, если $\theta = 1$ или θ может быть представлено в виде произведения конечного числа элементарных трансляций. Частным случаем трансляций являются операции на A, определяемые унарными операторами; но отметим, что в общем случае подалгебра алгебры A может быть не замкнута относительно всех трансляций, хотя замкнута относительно всех унарных операторов; например, в группе G единственной подгруппой, замкнутой относительно всех трансляций, будет сама группа G. Для конгруэнций ситуация оказывается несколько иной:

***Предложение* 6.1.** *Эквивалентность $\mathfrak{q}$ на Ω-алгебре A является конгруэнцией тогда и только тогда, когда она замкнута относительно всех трансляций; точнее, всякая конгруэнция замкнута относительно всех трансляций в A, в то время как любая эквивалентность, замкнутая относительно всех элементарных трансляций, будет конгруэнцией.*

Доказательство. Если $\mathfrak{q}$ — конгруэнция, то для любого $\omega \in \Omega(n)$ и любых $a_1, \ldots, a_n, b \in A$, если $a_i \equiv b \pmod{\mathfrak{q}}$, то

$$a_1 \ldots a_n\omega \equiv a_1 \ldots a_{i-1}ba_{i+1} \ldots a_n\omega \pmod{\mathfrak{q}};$$

поэтому $\mathfrak{q}$ замкнута относительно всех элементарных трансляций и, значит, в силу простой индукции $\mathfrak{q}$ замкнута относительно всех трансляций. Обратно, предположим, что $\mathfrak{q}$ замкнута относительно всех элементарных трансляций, и пусть $a_i, a_i' \in A$ и $a_i \equiv a_i' \pmod{\mathfrak{q}}$ $(i = 1, \ldots, n)$; тогда имеем по $\operatorname{mod} \mathfrak{q}$

$$\begin{aligned} a_1 \ldots a_n\omega &\equiv a_1'a_2 \ldots a_n\omega \equiv \\ &\equiv a_1'a_2'a_3 \ldots a_n\omega \equiv \\ &\quad \cdots\cdots \\ &\equiv a_1'a_2' \ldots a_n'\omega. \end{aligned}$$

Таким образом, $\mathfrak{q}$ замкнута относительно ω, и так как это верно для каждого $\omega \in \Omega(n)$ $(n = 0, 1, \ldots)$, то $\mathfrak{q}$ на самом деле будет конгруэнцией. ∎

Чтобы показать, что конгруэнции на A образуют полную структуру, докажем более сильное утверждение, что $\mathscr{C}_\Omega(A)$ является алгебраической системой замыканий на A^2. Проще всего это сделать, задав такую область операторов Γ и такую структуру Γ-алгебры на A^2, что $\mathscr{B}_\Gamma(A^2) = \mathscr{C}_\Omega(A)$. Для этого область Γ должна состоять из операторов, которые действуют на A^2 следующим образом:

(i) Для каждого $a \in A$ существует такой 0-арный оператор $\lambda = \lambda(a)$, что
$$\lambda = (a, a).$$

(ii) Существует один такой унарный оператор ν, что
$$(x, y)\mu = (y, x).$$

(iii) Существует один такой бинарный оператор ν, что
$$(x, y)(z, t)\nu = \begin{cases} (x, t), & \text{если } y = z, \\ (x, y) & \text{в противном случае.} \end{cases}$$

(iv) Для каждого $\omega \in \Omega(n+1)$, где $n=0, 1, \ldots$, для каждого набора $(a_1, \ldots, a_n)$ элементов из A и каждого числа $i=1, 2, \ldots, n+1$ существует такой унарный оператор $\rho=\rho(\omega, a_1, \ldots, a_n, i)$, что

$$(x, y)\rho=(a_1 \ldots a_{i-1}xa_i \ldots a_n\omega,\ a_1 \ldots a_{i-1}ya_i \ldots a_n\omega).$$

Все эти операторы конечноместны, и по определению эквивалентности ясно, что всякая эквивалентность на A — это в точности подмножество из A^2, замкнутое относительно всех λ, μ, ν, в то время как конгруэнция — это подмножество из A^2, замкнутое относительно всех λ, μ, ν и всех ρ. Таким образом доказана

***Теорема* 6.2.** *Множество $\mathscr{C}_\Omega(A)$ конгруэнций на A является алгебраической системой замыканий и, следовательно, полной структурой.* ∎

В частности, рассматривая только операторы λ, μ и ν, получаем

***Следствие* 6.3.** *Множество $\mathscr{C}(A)$ эквивалентностей на множестве A является алгебраической системой замыканий.* ∎

Если применить теорему 5.3, то получим

***Следствие* 6.4.** *Пусть A есть Ω-алгебра, Φ — соответствие в A и $\mathfrak{q}$ — конгруэнция на A. Тогда существует конгруэнция $\bar{\mathfrak{q}}$ в A, максимальная относительно свойств $\bar{\mathfrak{q}} \supseteq \mathfrak{q}$, $\bar{\mathfrak{q}} \cap \Phi=\mathfrak{q} \cap \Phi$.* ∎

Это следствие применяется главным образом в случае, когда $\mathfrak{q}$ является диагональю в A, а Φ состоит из одной пары различных элементов алгебры A. Тогда в нем утверждается, что для любых двух различных элементов a и b алгебры A существует максимальная конгруэнция, разделяющая a и b.

При доказательстве теоремы 6.2 конгруэнции алгебры A были получены как эквивалентности, замкнутые относительно всех унарных операторов ρ. Поэтому из теоремы 5.7 получаем

***Следствие* 6.5.** *Структура конгруэнций $\mathscr{C}_\Omega(A)$ Ω-алгебры A образует подструктуру структуры $\mathscr{C}(A)$ эквивалентностей на A.* ∎

Это означает, что если $\mathfrak{q}$ и $\mathfrak{r}$ — две конгруэнции на A, то для того чтобы получить наименьшую конгруэнцию, содержащую и $\mathfrak{q}$, и $\mathfrak{r}$, нужно только взять $\mathfrak{q} \vee \mathfrak{r}$ в $\mathscr{C}(A)$; иными словами, наименьшая эквивалентность, содержащая $\mathfrak{q}$ и $\mathfrak{r}$, будет уже конгруэнцией. Обозначим эту эквивалентность через $\mathfrak{q} \vee \mathfrak{r}$ и будем называть ее эквивалентностью, *порожденной* конгруэнциями $\mathfrak{q}$ и $\mathfrak{r}$. Это согласуется с принятой терминологией, если считать $\mathfrak{q} \vee \mathfrak{r}$ наименьшей подалгеброй Γ-алгебры A^2, содержащей $\mathfrak{q}$ и $\mathfrak{r}$.

При более подробном изучении структурных операций в $\mathscr{C}_\Omega(A)$ можно ограничиться в силу следствия 6.5 случаем $\Omega = \varnothing$; итак, пусть A — произвольное множество. Тогда структурные операции в $\mathscr{C}(A)$ могут быть описаны следующим образом: $\mathfrak{q} \wedge \mathfrak{r} = \mathfrak{q} \cap \mathfrak{r}$, потому что $\mathscr{C}(A)$ замкнута относительно пересечений; чтобы получить $\mathfrak{q} \vee \mathfrak{r}$, определим $\mathfrak{s}_0 = \Delta_A$ и для $k \geqslant 0$ положим $\mathfrak{s}_{k+1} = \mathfrak{s}_k \circ \mathfrak{r} \circ \mathfrak{q}$; тогда

$$\mathfrak{s}_0 \subseteq \mathfrak{s}_1 \subseteq \ldots \subseteq \bigcup \mathfrak{s}_k = \mathfrak{q} \vee \mathfrak{r}. \tag{4}$$

Легко проверить, что $\mathfrak{s} = \bigcup \mathfrak{s}_k$ будет эквивалентностью, содержащей $\mathfrak{q}$ и $\mathfrak{r}$, и на самом деле наименьшей такой эквивалентностью, откуда и вытекает (4). Наиболее важным является тот частный случай, когда цепь $\mathfrak{s}_k$ обрывается на первом шаге:

***Предложение* 6.6.** *Пусть A — произвольное множество и $\mathfrak{q}, \mathfrak{r} \in \mathscr{C}(A)$. Тогда $\mathfrak{q} \circ \mathfrak{r}$ будет эквивалентностью тогда и только тогда, когда $\mathfrak{q}$ и $\mathfrak{r}$ перестановочны, и в этом случае*

$$\mathfrak{q} \vee \mathfrak{r} = \mathfrak{q} \circ \mathfrak{r}.$$

Доказательство. Ясно, что $\mathfrak{q} \vee \mathfrak{r} \supseteq \mathfrak{q} \circ \mathfrak{r} \supseteq \mathfrak{q} \cup \mathfrak{r}$ для любых эквивалентностей $\mathfrak{q}$ и $\mathfrak{r}$, так что если $\mathfrak{q} \circ \mathfrak{r}$ является эквивалентностью, то она совпадает с $\mathfrak{q} \vee \mathfrak{r}$ и, кроме того,

$$\mathfrak{q} \circ \mathfrak{r} = (\mathfrak{q} \circ \mathfrak{r})^{-1} = \mathfrak{r}^{-1} \circ \mathfrak{q}^{-1} = \mathfrak{r} \circ \mathfrak{q}.$$

Обратно, если $\mathfrak{q} \circ \mathfrak{r} = \mathfrak{r} \circ \mathfrak{q}$, то

$$(\mathfrak{q} \circ \mathfrak{r})^{-1} = \mathfrak{r}^{-1} \circ \mathfrak{q}^{-1} = \mathfrak{r} \circ \mathfrak{q} = \mathfrak{q} \circ \mathfrak{r},$$

следовательно, отношение $\mathfrak{q} \circ \mathfrak{r}$ симметрично. Ясно, что оно рефлексивно и

$$\mathfrak{q} \circ \mathfrak{r} \circ \mathfrak{q} \circ \mathfrak{r} = \mathfrak{q} \circ \mathfrak{q} \circ \mathfrak{r} \circ \mathfrak{r} = \mathfrak{q} \circ \mathfrak{r},$$

откуда вытекает также транзитивность $\mathfrak{q} \circ \mathfrak{r}$, а поэтому $\mathfrak{q} \circ \mathfrak{r}$ — эквивалентность. ∎

***Следствие* 6.7.** *Пусть A есть Ω-алгебра и $\mathfrak{q}, \mathfrak{r}$ — произвольные конгруэнции на A; $\mathfrak{q} \circ \mathfrak{r}$ будет конгруэнцией на A тогда и только тогда, когда $\mathfrak{q}$ и $\mathfrak{r}$ перестановочны и в этом случае*

$$\mathfrak{q} \vee \mathfrak{r} = \mathfrak{q} \circ \mathfrak{r}. \ ∎$$

Если множество A содержит по крайней мере три элемента, то $\mathscr{C}(A)$ не будет подструктурой в $\mathscr{B}(A^2)$, и можно легко найти пару неперестановочных эквивалентностей. Однако если на A задана структура Ω-алгебры, то структура $\mathscr{C}_\Omega(A)$ будет, вообще говоря, меньше чем $\mathscr{C}(A)$, а если область операторов Ω достаточно сложна, то может оказаться, что все конгруэнции на A перестановочны. Достаточное условие перестановочности конгруэнций сформулировано в следующем предложении:

***Предложение* 6.8.** *Пусть A есть Ω-алгебра; тогда конгруэнции на A перестановочны, если для каждой пары a, $b \in A$ существует трансляция алгебры A, переставляющая a и b.*

Доказательство. Пусть A есть Ω-алгебра, удовлетворяющая сформулированному условию, и пусть $\mathfrak{q}$, $\mathfrak{r} \in \mathscr{C}_\Omega(A)$. Если $(a, b) \in \mathfrak{q} \circ \mathfrak{r}$, то это означает, что для некоторого $c \in A$

$$a \equiv c \pmod{\mathfrak{q}} \text{ и } c \equiv b \pmod{\mathfrak{r}}.$$

По предположению существует трансляция τ алгебры A, переставляющая a и b, и так как $\mathfrak{q}$ и $\mathfrak{r}$ замкнуты относительно τ (предложение 6.1), то имеем

$$b \equiv c^\tau \pmod{\mathfrak{q}} \text{ и } c^\tau \equiv a \pmod{\mathfrak{r}};$$

следовательно, $(b, a) \in \mathfrak{q} \circ \mathfrak{r}$, т. е. $(a, b) \in \mathfrak{r} \circ \mathfrak{q}$. Это показывает, что $\mathfrak{q} \circ \mathfrak{r} \subseteq \mathfrak{r} \circ \mathfrak{q}$, а в силу симметрии $\mathfrak{q} \circ \mathfrak{r} \supseteq \mathfrak{r} \circ \mathfrak{q}$, откуда $\mathfrak{q} \circ \mathfrak{r} = \mathfrak{r} \circ \mathfrak{q}$. ∎

Из этого предложения немедленно вытекает, что на группе все конгруэнции перестановочны, поскольку, если a, b — произвольные элементы группы G, то τ: $x \to ax^{-1}b$ будет трансляцией, которая переставляет a и b. Этим доказано даже более общее утверждение, что конгруэнции перестановочны на любой группе с мультиоператорами.

В главе III нам встретятся другие условия перестановочности конгруэнций на Ω-алгебрах. Условия такого рода важны не только с практической точки зрения, так как облегчают нахождение объединений эквивалентностей (ввиду предложения 6.6), но и с теоретической, поскольку обеспечивают модулярность структуры $\mathscr{C}_\Omega(A)$:

***Предложение* 6.9.** *Если на Ω-алгебре A все конгруэнции перестановочны, то структура $\mathscr{C}_\Omega(A)$ конгруэнций на A модулярна.*

Доказательство такое же, как и в частном случае групп: если даны $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r} \in \mathscr{C}_\Omega(A)$, где $\mathfrak{q} \subseteq \mathfrak{r}$, то нужно показать, что

$$(\mathfrak{p} \circ \mathfrak{q}) \cap \mathfrak{r} \subseteq (\mathfrak{p} \cap \mathfrak{r}) \circ \mathfrak{q}.$$

Пусть $(a, b) \in (\mathfrak{p} \circ \mathfrak{q}) \cap \mathfrak{r}$, и пусть $a \equiv c \pmod{\mathfrak{p}}$, $c \equiv b \pmod{\mathfrak{q}}$; тогда

$$a \equiv b \pmod{\mathfrak{r}}$$

и

$$b \equiv c \pmod{\mathfrak{r}},$$

так как $\mathfrak{q} \subseteq \mathfrak{r}$; следовательно, $a \equiv c \pmod{\mathfrak{p} \cap \mathfrak{r}}$ и поэтому $(a, b) \in (\mathfrak{p} \cap \mathfrak{r}) \circ \mathfrak{q}$. ∎

Если воспользоваться перестановочностью конгруэнций, то из теорем об изоморфизмах можно сделать следующие выводы, которые в действительности являются перенесением теорем Жордана — Гёльдера и Шрайера на общие алгебры. Начнем с доказательства теоремы, обобщающей вторую теорему об изоморфизмах.

***Теорема* 6.10. (*Лемма Цассенхауза.*)** *Пусть A есть Ω-алгебра, B и C — подалгебры алгебры A, $\mathfrak{q}$ и $\mathfrak{r}$—конгруэнции на B и C соответственно. Предположим, что все конгруэнции на $B \cap C$ перестановочны; тогда $\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}\in\mathscr{C}_\Omega((B\cap C)^{\mathfrak{q}})$, $\mathfrak{r}\circ\mathfrak{q}\circ\mathfrak{r}\in\mathscr{C}_\Omega((B\cap C)^{\mathfrak{r}})$ и*

$$(B\cap C)^{\mathfrak{q}}/\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}\cong(B\cap C)^{\mathfrak{r}}/\mathfrak{r}\circ\mathfrak{q}\circ\mathfrak{r}.$$

Доказательство. Положим $D=B\cap C$, $\mathfrak{q}'=\mathfrak{q}\cap C^2$, $\mathfrak{r}'=\mathfrak{r}\cap B^2$; тогда $\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}=\mathfrak{q}\circ\mathfrak{r}'\circ\mathfrak{q}$ и

$$\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}\circ\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}=\mathfrak{q}\circ\mathfrak{r}'\circ\mathfrak{q}'\circ\mathfrak{r}'\circ\mathfrak{q}=\mathfrak{q}\circ\mathfrak{r}'\circ\mathfrak{q};$$

следовательно, отношение $\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}$ транзитивно; ясно, что оно также рефлексивно, симметрично и замкнуто относительно Ω; таким образом, $\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}$ — конгруэнция на $D^{\mathfrak{q}}$. Аналогично $\mathfrak{r}\circ\mathfrak{q}\circ\mathfrak{r}$ — конгруэнция на $D^{\mathfrak{r}}$, а $\mathfrak{q}'\circ\mathfrak{r}'$ — конгруэнция на D. Далее,

$$(\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q})\cap D^2=\mathfrak{q}'\circ\mathfrak{r}';$$

отсюда по второй теореме об изоморфизмах (теорема 3.9)

$$D^{\mathfrak{q}}/\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}\cong D/\mathfrak{q}'\circ\mathfrak{r}'.$$

В силу симметрии имеем

$$D^{\mathfrak{r}}/\mathfrak{r}\circ\mathfrak{q}\circ\mathfrak{r}\cong D/\mathfrak{q}'\circ\mathfrak{r}',$$

откуда и вытекает нужный результат. ∎

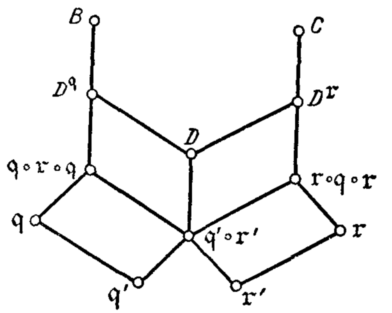

Рис. 7.

Фактороалгебра $D^{\mathfrak{q}}/\mathfrak{q}\circ\mathfrak{r}\circ\mathfrak{q}$ часто называется *проекцией* $C/\mathfrak{r}$ в $B/\mathfrak{q}$. Тогда теорема 6.10 просто утверждает, что при сделанных предположениях, если $\overline{B}$ и $\overline{C}$ — два произвольных фактора алгебры A, то проекция $\overline{B}$ в $\overline{C}$ изоморфна проекции $\overline{C}$ в $\overline{B}$.

Пусть A есть Ω-алгебра с подалгеброй E; тогда под *нормальным рядом* от E до A понимают конечный ряд подалгебр алгебры A

$$E=A_0\subseteq A_1\subseteq\ldots\subseteq A_m=A \tag{5}$$

вместе с такими конгруэнциями $\mathfrak{q}_i$ на A_i ($i\geqslant 1$), что A_{i-1} является в точности $\mathfrak{q}_i$-классом. Так как A_{i-1} — подалгебра, то это означает, что фактороалгебра $A_i/\mathfrak{q}_i$ обладает тривиальной подалгеброй, а именно $A_{i-1}^{\mathfrak{q}_i}$. Имеем $A_{i-1}=A_{i-1}^{\mathfrak{q}_i}=E^{\mathfrak{q}_i}$ (как множества), так что (5) можно также записать в виде

$$E=E^{\mathfrak{q}_1}\subseteq E^{\mathfrak{q}_2}\subseteq\ldots\subseteq E^{\mathfrak{q}_m}=A.$$

Если в (5) каждый интервал $[A_{i-1}, A_i]$ заменить нормальным рядом от A_{i-1} до A_i так, чтобы вновь вставленные подалгебры, так же как и все классы вставленных конгруэнций, были объединениями $\mathfrak{q}_i$-классов, то мы снова получим нормальный ряд от E до A, который называется *уплотнением* ряда (5). Всякое такое уплотнение можно получить, если выбрать некоторый нормальный ряд в каждом $A_i/\mathfrak{q}_i$ и взять *полный прообраз* при $\operatorname{nat}\mathfrak{q}_i$.

Говорят, что ряд (5) и второй нормальный ряд

$$E = B_0 \subseteq B_1 \subseteq \ldots \subseteq B_n = A \tag{6}$$

с конгруэнциями $\mathfrak{r}_j$ *изоморфны*, если $m = n$ и существует такая перестановка π из чисел $1, 2, \ldots, n$, что

$$A_i/\mathfrak{q}_i \cong B_{i\pi}/\mathfrak{r}_{i\pi}.$$

С помощью этих определений можно сформулировать теорему Шрейера для Ω-алгебр с перестановочными конгруэнциями.

***Теорема* 6.11. (*Теорема Шрейера.*)** *Пусть A есть Ω-алгебра с подалгеброй E, причем на любой подалгебре алгебры A все конгруэнции перестановочны. Тогда любые два нормальных ряда от E до A обладают изоморфными уплотнениями.*

Доказательство. Пусть даны ряды (5) и (6) с конгруэнциями $\mathfrak{q}_i$ и $\mathfrak{r}_j$ соответственно. Положим

$$\begin{aligned} F_{ij} &= (A_i \cap B_j)^{\mathfrak{r}_j}/\mathfrak{q}_i \circ \mathfrak{r}_j \circ \mathfrak{q}_i, \\ G_{ji} &= (A_i \cap B_j)^{\mathfrak{q}_i}/\mathfrak{r}_j \circ \mathfrak{q}_i \circ \mathfrak{r}_j; \end{aligned} \qquad (i = 1, \ldots, m;\ j = 1, \ldots, n)$$

тогда по лемме Цассенхауза

$$F_{ij} \cong G_{ji}. \tag{7}$$

Если мы положим $D = A_i \cap B_j$, $\mathfrak{r}' = \mathfrak{r}_j \cap A_i^2$, $\mathfrak{q}' = \mathfrak{q}_i \cap B_j^2$, то, так как $E \subseteq A_i$ для $i = 1, \ldots, m$, имеем

$$E^{\mathfrak{q}_i \circ \mathfrak{r}_j \circ \mathfrak{q}_i} = E^{\mathfrak{q}' \circ \mathfrak{r}' \circ \mathfrak{q}_i} = E^{\mathfrak{r}' \circ \mathfrak{q}_i} = B_{j-1}^{\mathfrak{q}_i} = (A_i \cap B_{j-1})^{\mathfrak{q}_i}.$$

Таким образом, $F_{i1}, \ldots, F_{in}$ являются факторами нормального ряда в $A_i/\mathfrak{q}_i$; поэтому можно уплотнить (5) до нормального ряда с факторами $F_{11}, F_{12}, \ldots, F_{1n}, F_{21}, \ldots, F_{mn}$. По соображениям симметрии можно уплотнить и (6) до нормального ряда с факторами G_{ji}, и в силу (7) эти уплотнения изоморфны. ∎

Фактор называется *тривиальным*, если он является тривиальной алгеброй. Ясно, что если мы имеем два изоморфных ряда и отбросим тривиальные факторы обоих этих рядов, то снова получим два нормальных ряда, изоморфных друг другу, но без повторений. Нормальный ряд без повторений, у которого нет собственных уплотнений (т. е. уплотнений без повторений), называется *композиционным рядом.* Таким образом, нормальный ряд будет композиционным рядом тогда и только тогда, когда все его факторы являются простыми алгебрами.

***Следствие* 6.12. (*Теорема Жордана — Гёльдера.*)** *Если A и E удовлетворяют условиям теоремы* 6.11, *то любые два композиционных ряда от E до A изоморфны.* ∎

***Следствие* 6.13.** *Если A и E удовлетворяют условиям теоремы* 6.11 *и существует композиционный ряд от E до A, то любой нормальный ряд от E до A можно уплотнить до композиционного.* ∎

Мы получим важный частный случай, если в качестве E возьмем тривиальную подалгебру алгебры A. Например, это всегда можно сделать для групп; более того, так как конгруэнции на группе перестановочны, то как частный случай теоремы 6.11 и ее следствий получаем обычные теорему Шрейера и теорему Жордана — Гёльдера для групп. В качестве второго примера рассмотрим Ω-алгебру A с нормальным рядом (5). Если $\mathfrak{q}_i = \mathfrak{q}_i^* \cap A_i^2$, где $\mathfrak{q}_i^*$ — конгруэнция на A, то (5) называется *инвариантным рядом.* Легко видеть, что полученные в теореме 6.11 уплотнения будут инвариантными рядами, если только начинать с инвариантных рядов. Таким образом, мы получаем теорему об уплотнении инвариантных рядов, которую предоставляем сформулировать читателю. Инвариантный ряд без собственных уплотнений и без повторений называется *главным рядом.* Тогда получаем следствие, аналогичное следствиям 6.12 и 6.13:

***Следствие* 6.14.** *Если A есть Ω-алгебра с перестановочными конгруэнциями и E — подалгебра алгебры A, то любые два главных ряда от E до A изоморфны; и если главные ряды существуют, то любой инвариантный ряд от E до A можно уплотнить до главного ряда.* ∎

Теорема Жордана — Гёльдера для общих алгебр была доказана и при ряде других условий; было показано, что для алгебр с условиями максимальности и минимальности для подалгебр следующие условия необходимы и достаточны для того, чтобы было справедливо утверждение следствия 6.12 (Голди [52]): пусть даны две конгруэнции $\mathfrak{q}$ и $\mathfrak{r}$, встречающиеся в различных композиционных рядах, B, C — подалгебры, на которых определены $\mathfrak{q}$ и $\mathfrak{r}$, и пусть $D = B \cap C$, $\mathfrak{q}' = \mathfrak{q} \cap D^2$, $\mathfrak{r}' = \mathfrak{r} \cap D^2$; тогда

$$E^{\mathfrak{q}' \circ \mathfrak{r}'} = E^{\mathfrak{r}' \circ \mathfrak{q}'}.$$

Перейдем теперь к теореме Крулля — Шмидта; чтобы применить структурный вариант этой теоремы, доказанный в § II.4, рассмотрим представление данной алгебры A в виде конечного прямого произведения

$$A \cong A_1 \times \ldots \times A_n.$$

Если проекцию на сомножитель A_i обозначить через ε_i: $A \to A_i$, то ясно, что

(i) для любых $x, y \in A$, если $x\varepsilon_i = y\varepsilon_i$ ($i = 1, \ldots, n$), то $x = y$;

(ii) если дано произвольное семейство (a_i), $a_i \in A_i$ ($i = 1, \ldots, n$), то существует такой $x \in A$, что $x\varepsilon_i = a_i$ (заметим, что x определен однозначно в силу (i)).

Обратно, если дано конечное семейство алгебр и эпиморфизмов ε_i: $A \to A_i$, удовлетворяющих (i) и (ii), то можно показать, что имеет место (8). Действительно, если определить отображение θ: $A \to \prod A_i$ по правилу

$$x\theta = (x\varepsilon_i),$$

то θ будет гомоморфизмом, поскольку каждый ε_i является гомоморфизмом, мономорфизмом в силу (i) и эпиморфизмом в силу (ii); следовательно, θ — изоморфизм. Условия (i) и (ii) можно также выразить на языке ядер эпиморфизмов ε_i следующим образом:

Теорема 6.15. *Если Ω-алгебра A представлена в виде прямого произведения*

$$A \cong A_1 \times \ldots \times A_n \tag{8}$$

с проекциями ε_i: $A \to A_i$ и если $\mathfrak{q}_i = \ker \varepsilon_i$, то конгруэнции $\mathfrak{q}_i$ удовлетворяют равенствам

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n = \Delta, \tag{9}$$

$$(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{i-1}) \circ \mathfrak{q}_i = A^2 \quad (i = 2, \ldots, n). \tag{10}$$

Обратно, любое семейство конгруэнций $(\mathfrak{q}_i)$, удовлетворяющее (9) и (10), определяет представление алгебры A в виде прямого произведения (8), где $A_i \cong A/\mathfrak{q}_i$. Кроме того, конгруэнции $\mathfrak{q}_i$ попарно перестановочны.

Доказательство. Если задано (8), то пусть $\varepsilon^{(i)}$: $A \to A_1 \times \ldots \times A_i$ — проекция; тогда легко видеть, что $\ker \varepsilon^{(i)} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_i$. В частности, так как $\ker \varepsilon^{(n)} = \Delta$, то имеем (9). Далее, для любых элементов $a_i \in A_i$ существует такой $x \in A$, что $x\varepsilon^{(n-1)} = (a_1, \ldots, a_{n-1})$, $x\varepsilon_n = a_n$. Так как a_i был произвольным элементом в A_i, то это означает, что для любых данных $y, z \in A$ существует такой $x \in A$, что

$$x \equiv y \pmod{\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{n-1}},$$
$$x \equiv z \pmod{\mathfrak{q}_n}.$$

Таким образом,

$$(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{n-1}) \circ \mathfrak{q}_n = A^2. \tag{11}$$

В силу симметрии имеем

$$\Big(\bigcap_{j \neq i} \mathfrak{q}_j\Big) \circ \mathfrak{q}_i = A^2, \tag{12}$$

и, следовательно, имеет место (10). Далее, в силу (12)

$$\mathfrak{q}_i \circ \mathfrak{q}_j = A^2 = \mathfrak{q}_j \circ \mathfrak{q}_i \quad (i \neq j),$$

так что все конгруэнции $\mathfrak{q}$ перестановочны.

Обратно, пусть даны $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$, удовлетворяющие (9) и (10); запишем $A_i = A/\mathfrak{q}_i$ и положим $\varepsilon_i = \operatorname{nat} \mathfrak{q}_i$. Если $x\varepsilon_i = y\varepsilon_i$ для $i = 1, \ldots, n$, то в силу (9) $x = y$. Пусть теперь даны $a_i \in A_i$. Если

$$x^{(i)}\varepsilon_j = a_j \quad (j = 1, \ldots, i) \text{ для некоторого } x^{(i)} \in A, \tag{13}$$

то в силу (10) существует такое $x^{(i+1)} \in A$, что

$$x^{(i+1)}\varepsilon_j = a_j \quad \text{для} \quad j = 1, \ldots, i+1.$$

Но (13) имеет место для $i = 1$ и, следовательно, по индукции для всех $i \leqslant n$. В частности, для $i = n$ получаем (ii), и утверждение доказано. ∎

Отметим, что (9) и (10) просто утверждают, что $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ образуют независимое множество в структуре $\mathscr{C}_\Omega(A)$, если считать A^2 наименьшим, а Δ наибольшим элементом. Другими словами, (9) и (10) являются условиями того, чтобы Δ было прямым объединением конгруэнций $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ в структуре, дуальной к $\mathscr{C}_\Omega(A)$.

Напомним также, что если все конгруэнции на A перестановочны, то $\mathscr{C}_\Omega(A)$ модулярна (предложение 6.9). Пусть алгебра A удовлетворяет этому условию, и предположим, кроме того, что структура $\mathscr{C}_\Omega(A)$ конечной длины. Тогда структурная теорема Крулля — Шмидта показывает, что для любых двух полных разложений

$$\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_m = \mathfrak{r}_1 \cap \ldots \cap \mathfrak{r}_n = \Delta$$

$m = n$ и каждая конгруэнция $\mathfrak{q}_i$ связана с некоторой конгруэнцией $\mathfrak{r}_j$. Это означает, что существует такая конгруэнция $\mathfrak{q}' \in \mathscr{C}_\Omega(A)$, что

$$\mathfrak{q}_i \cap \mathfrak{q}' = \mathfrak{r}_j \cap \mathfrak{q}' = \Delta, \quad \mathfrak{q}_i \circ \mathfrak{q}' = \mathfrak{r}_j \circ \mathfrak{q}' = A^2.$$

В действительности в силу доказательства теоремы 4.11 в качестве $\mathfrak{q}'$ можно взять $\bigcap_{k \neq i} \mathfrak{q}_k$. Таким образом, полагая $A_i = A/\mathfrak{q}_i$, $B_j = A/\mathfrak{r}_j$, $A' = A/\mathfrak{q}'$, имеем

$$A \cong A_i \times A' \cong B_j \times A'; \tag{14}$$

этим доказана

Теорема 6.16. (Теорема о замещении для прямых разложений.) *Пусть A есть Ω-алгебра, на которой все конгруэнции пе-*

рестановочны и структура конгруэнций которой конечной длины. Тогда для любых двух прямых разложений

$$A \cong A_1 \times \ldots \times A_m \cong B_1 \times \ldots \times B_n$$

алгебры A с неразложимыми сомножителями $m = n$ и каждый множитель A_i может быть замещен некоторым B_j. ∎

Хорошо было бы иметь возможность утверждать, что A_i и B_j, связанные как в (14), на самом деле изоморфны как Ω-алгебры. В общем случае это не верно (см. упр. 10), но следующая теорема дает простое условие, при котором имеет место изоморфизм. Пусть $\mathfrak{q}$, $\mathfrak{r}$, $\mathfrak{q}'$ — такие конгруэнции на A, что

$$\mathfrak{q} \circ \mathfrak{q}' = \mathfrak{r} \circ \mathfrak{q}' = A^2, \quad \mathfrak{q} \cap \mathfrak{q}' = \mathfrak{r} \cap \mathfrak{q}' = \Delta.$$

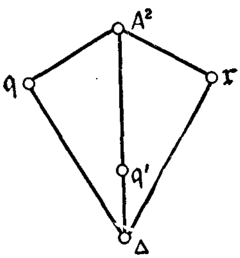

Рис. 8.

Эти условия означают, что каждый $\mathfrak{q}'$-класс является общим трансверсалом для $A/\mathfrak{q}$ и $A/\mathfrak{r}$. Если $A/\mathfrak{q}'$ обладает тривиальной подалгеброй, то соответствующий $\mathfrak{q}'$-класс сам будет подалгеброй, которая тогда должна быть изоморфной и $A/\mathfrak{q}$, и $A/\mathfrak{r}$. Таким образом, получаем следующую теорему:

***Теорема* 6.17. (*Теорема Крулля — Шмидта для алгебр.*)** *Пусть A есть Ω-алгебра с перестановочными конгруэнциями, обладающая главным рядом и тривиальной подалгеброй. Тогда для любых двух полных разложений*

$$A \cong A_1 \times \ldots \times A_m \cong B_1 \times \ldots \times B_n$$

$m = n$ и $A_i \cong B_i$ при соответствующем изменении нумерации множителей $B_1, \ldots, B_n$.

Это вытекает из замечаний, предшествующих формулировке теоремы, если заметить, что любой гомоморфный образ алгебры A снова обладает тривиальной подалгеброй. ∎

Мы видели, что конгруэнции на группе перестановочны; поэтому этот результат можно применить к произвольной группе с главными рядами, или, в более общем случае, к произвольной группе с унарными операторами или с мультиоператорами, обладающей главными рядами. На самом деле в случае групп этот результат может быть немного усилен. Напомним, что *центром* группы G называется множество

$$Z = \{x \in G \mid xy = yx \text{ для всех } y \in G\}.$$

Две подгруппы H, K группы G называются *центрально изоморфными*, если существует такой изоморфизм α: $H \to K$, что $x^{-1} \cdot x\alpha \in Z$ для всех $x \in H$. Тогда имеем

***Следствие* 6.18.** *Если G — произвольная группа, обладающая главными рядами, и*

$$G \cong G_1 \times \ldots \times G_m \cong H_1 \times \ldots \times H_n$$

— два любых полных разложения группы G, то $m = n$ и подгруппа G_i центрально изоморфна подгруппе H_i при подходящем изменении нумерации подгрупп $H_1, \ldots, H_n$. В частности, если G обладает тривиальным центром, то множители G_i определены однозначно.

Действительно, по теореме 6.17 имеем $G = G_1 \times K = H_1 \times K$, где прямые множители группы G отождествлены с ее подгруппами. Любой элемент $x \in G$ имеет вид

$$x = x_1 z = y_1 z',$$

где $x_1 \in G_1$, $y_1 \in H_1$ и z, $z' \in K$. Теперь $x_1^{-1} y_1 = z z'^{-1} = t$, скажем, и K поэлементно перестановочна с G_1 и H_1; поэтому t поэлементно перестановочен с G_1 и H_1; с другой стороны, y_1 перестановочен с K и x_1 перестановочен с K, и поэтому t также перестановочен с K, откуда t перестановочен с любым элементом из G, т. е. $t \in Z$. ∎

Было получено много подобных результатов при различных условиях, налагаемых на Ω-алгебры. Например, Джекобсоном ([56], гл. III) был получен вариант теоремы Крулля — Шмидта для модулей над кольцом, в котором не предполагается в явном виде существования главных рядов; тем не менее, как показывают примеры (Йонсон [57]), некоторые условия конечности должны все-таки быть наложены. Для группоидов с нейтральным элементом аналогичный результат относительно представлений группоидов в виде внутреннего прямого произведения был получен Йонсоном и Тарским [47].

УПРАЖНЕНИЯ

1. Если любые две конгруэнции на Ω-алгебре A перестановочны, то это же справедливо для любой ее факторалгебры. (Указание: воспользоваться следствием 3.12.)

2. Под *упорядоченной полугруппой* понимают полугруппу S, которая вместе с тем является таким упорядоченным множеством, что $a_i \leqslant b_i$ $(i = 1, 2)$ влечет $a_1 a_2 \leqslant b_1 b_2$. Элемент e полугруппы S называется *идемпотентом*, если $e^2 = e$.

(а) Пусть S — упорядоченная полугруппа с наименьшим элементом 1, который является также единицей. Показать, что любой элемент a, удовлетворяющий условию $a^2 \leqslant a$, будет идемпотентом. Если a и b — идемпотенты, то ab будет идемпотентом при условии, что $ba \leqslant ab$.

(b) Показать, что если S удовлетворяет условиям пункта (а) и обладает монотонным антиавтоморфизмом второго порядка, т. е. таким отображением S в себя, $a \to a'$, что (i) $a \leqslant b \Rightarrow a' \leqslant b'$, (ii) $a'' = a$, (iii) $(ab)' = b'a'$, то для любых идемпотентов a и b ab тогда и только тогда будет идемпотентом, когда $ba = ab$. Вывести отсюда предложение 6.6.

3. Если A есть Ω-алгебра и S — произвольное подмножество алгебры A, то будем писать $a \sim b \pmod S$, если $a = b$ или $a, b \in S^{\tau}$, где τ — некоторая трансляция алгебры A. Далее, будем писать $a \approx b \pmod S$, если существует такая конечная последовательность $x_0 = a, x_1, \ldots, x_n = b$, что $x_{i-1} \sim x_i \pmod S$. Показать, что отношение $a \approx b$ будет конгруэнцией на A и что это будет наименьшая конгруэнция, которая обладает классом, содержащим S.

4. Пусть A и S такие, как в упр. 3, и определим

$$\mathfrak{q} = \{(x, y) \in A^2 \mid x^{\tau} \in S \Leftrightarrow y^{\tau} \in S \text{ для любой трансляции } \tau\}.$$

Показать, что $\mathfrak{q}$ будет наибольшей среди конгруэнций на A, для которых S является объединением $\mathfrak{q}$-классов.

5. (Мальцев.) Пусть A и S такие, как в упр. 3; показать, что S будет классом единственной конгруэнции на A тогда и только тогда, когда для всех $x, y \in A$

$$x^{\tau} \in S \Leftrightarrow y^{\tau} \in S \quad \text{для всех трансляций } \tau$$

влечет $x \approx y$ (см. упр. 3, определение).

6. (Мальцев.) Трансляция на Ω-алгебре A называется *обратимой*, если для нее существует обратное отображение, также являющееся трансляцией. Показать, что обратимые трансляции на A образуют группу Γ и если Γ действует на A транзитивно (т. е. если A, как Γ-модуль, состоит из одной траектории), то все конгруэнции на A перестановочны. (Указание: проверить, что если τ_{ab} — обратимая трансляция, отображающая a в b, то отображение $x \to x\sigma$, где $x\sigma = a\tau_{xb}\tau_{bb}^{-1}$, будет трансляцией.)

7. Пусть $\mathfrak{q}$ — конгруэнция на структуре L. Показать, что если $a \equiv b \pmod{\mathfrak{q}}$, то $a \wedge b \equiv a \vee b \pmod{\mathfrak{q}}$.

8. (Фунаяма, Накаяма.) Показать, что структура конгруэнций на произвольной структуре дистрибутивна. (Указание: воспользоваться упр. 7 при проверке того, что $a \equiv b \pmod{\mathfrak{q} \cap (\mathfrak{r} \vee \mathfrak{s})}$ влечет $a \equiv b \pmod{(\mathfrak{q} \cap \mathfrak{r}) \vee (\mathfrak{q} \cap \mathfrak{s})}$.

9. Конгруэнция $\mathfrak{q}$ на Ω-алгебре A называется *совершенной*, если любой трансверсал факторалгебры $A/\mathfrak{q}$ порождает A. Показать, что если X — минимальная система образующих алгебры A и $\mathfrak{q}$ — совершенная конгруэнция на A, то $\mathfrak{q}$ разделяет X.

10. (Йонсон.) Пусть Ω состоит из одного унарного оператора. Построить две такие неизоморфные Ω-алгебры A, B, каждая из которых двухэлементна и $A \times B \cong B \times B$. (Указание: в каждом случае в качестве операции взять некоторую подстановку соответствующего носителя.)

7. ЛОКАЛЬНЫЕ И РЕЗИДУАЛЬНЫЕ СВОЙСТВА

В предыдущем параграфе мы получили описание конечных прямых произведений на языке ядер проекций на множители. Для произведений с произвольным числом множителей это описание принимает более сложный вид. Рассмотрим поэтому Ω-алгебру A с семейством эпиморфизмов

$$\varepsilon_{\lambda}\colon A \to A_{\lambda} \quad (\lambda \in \Lambda), \tag{1}$$

удовлетворяющих только первому из условий § II.6:

(i) для любых x, $y \in A$, если $x\varepsilon_\lambda = y\varepsilon_\lambda$ для всех $\lambda \in \Lambda$, то $x = y$.

Тогда те же самые рассуждения показывают, что A изоморфна подалгебре прямого произведения $\prod A_\lambda$; отождествляя A с этой подалгеброй алгебры $\prod A_\lambda$, видим, что естественные проекции ε_λ, ограниченные на A, все еще остаются эпиморфизмами. Поэтому введем следующее определение:

Определение. Пусть $(A_\lambda)_{\lambda \in \Lambda}$ — некоторое семейство Ω-алгебр. Тогда подалгебра A прямого произведения $\prod A_\lambda$ называется *подпрямым произведением* семейства $(A_\lambda)_{\lambda \in \Lambda}$, если $\varepsilon_\lambda \mid A$ являются эпиморфизмами (для каждого $\lambda \in \Lambda$).

Обычно подпрямые произведения возникают следующим образом:

***Предложение* 7.1.** *Пусть A есть Ω-алгебра и $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$ — семейство конгруэнций на A. Положим $\mathfrak{q} = \bigcap \mathfrak{q}_\lambda$ и $A_\lambda = A/\mathfrak{q}_\lambda$; тогда Ω-алгебра $A/\mathfrak{q}$ изоморфна подпрямому произведению семейства $(A_\lambda)_{\lambda \in \Lambda}$.*

Доказательство. Рассмотрим отображение $\theta\colon A \to \prod A_\lambda$, определенное по правилу:

$$(a\theta)\varepsilon_\lambda = a^{\mathfrak{q}_\lambda} \quad (a \in A,\ \lambda \in \Lambda). \tag{2}$$

По определению θ будет гомоморфизмом с ядром $\mathfrak{q}$; поэтому, факторизуя по $\mathfrak{q}$, получаем мономорфизм $A/\mathfrak{q} \to \prod A_\lambda$. Таким образом, $A/\mathfrak{q}$ можно вложить в $\prod A_\lambda$, и (2) показывает теперь, что $\theta\varepsilon_\lambda$ — эпиморфизм. ∎

***Следствие* 7.2.** *Если A — некоторая Ω-алгебра с таким семейством конгруэнций $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$, что $\bigcap \mathfrak{q}_\lambda = \Delta$, то A изоморфна подпрямому произведению алгебр $A/\mathfrak{q}_\lambda$.*

Это утверждение является частным случаем предложения 7.1 при $\mathfrak{q} = \Delta$ и вытекает из него, если вспомнить, что $A/\Delta \cong A$. ∎

Семейство $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$ конгруэнций на A называется *разделяющим* семейством конгруэнций, если $\bigcap \mathfrak{q}_\lambda = \Delta$ (т. е. $\bigcap \mathfrak{q}_\lambda$ разделяет A). Иначе говоря в следствии 7.2 тогда утверждается, что A можно представить в виде подпрямого произведения алгебр A_λ при условии, что существует разделяющее семейство конгруэнций $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$ с факторалгебрами A_λ. Пусть A есть Ω-алгебра с таким разделяющим семейством конгруэнций $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$, что $\mathfrak{q}_\lambda \neq \Delta$ для всех $\lambda \in \Lambda$; тогда A называется *подпрямо разложимой*; в противном случае A называется *подпрямо неразложимой*. Иначе говоря, A подпрямо неразложима тогда и только тогда, когда в каждом представлении (2) алгебры A в виде подпрямого произведения по крайней мере один из $\theta\varepsilon_\lambda$ будет изоморфизмом.

С помощью этого определения получается полезная теорема о представлении алгебр в виде подпрямого произведения, принадлежащая Биркгофу [44].

Теорема 7.3. *Каждая Ω-алгебра A представима в виде подпрямого произведения подпрямо неразложимых Ω-алгебр.*

Доказательство. Пусть $\mathfrak{q}$ — некоторая конгруэнция на A; будем говорить, что $\mathfrak{q}$ *неразложима в пересечение*, если не существует такого семейства конгруэнций $(\mathfrak{r}_\lambda)_{\lambda\in\Lambda}$, что $\mathfrak{r}_\lambda\supset\mathfrak{q}$ для всех $\lambda\in\Lambda$ и $\bigcap\mathfrak{r}_\lambda=\mathfrak{q}$. Из следствия 3.12 вытекает, что $\mathfrak{q}$ неразложима в пересечение тогда и только тогда, когда $A/\mathfrak{q}$ подпрямо неразложима. Пусть теперь $(\mathfrak{q}_\lambda)_{\lambda\in\Lambda}$ — семейство всех конгруэнций на A, неразложимых в пересечение; если мы сможем показать, что

$$\bigcap\mathfrak{q}_\lambda=\Delta, \tag{3}$$

то отсюда будет вытекать сформулированная теорема, так как тогда в силу следствия 7.2 алгебра A будет представлена в виде подпрямого произведения подпрямо неразложимых алгебр $A/\mathfrak{q}_\lambda$. Докажем равенство (3). Пусть $x,\ y\in A$, $x\neq y$, и пусть $\mathfrak{q}_0$ — такая максимальная конгруэнция на A, что $(x,\ y)\notin\mathfrak{q}_0$ (она существует в силу следствия 6.4). Тогда любая конгруэнция, которая содержит $\mathfrak{q}_0$ в качестве собственного подмножества, содержит также и $(x,\ y)$, и, следовательно, пересечение всех конгруэнций, содержащих $\mathfrak{q}_0$ в качестве собственного подмножества, также содержит $(x,\ y)$. Но $(x,\ y)\notin\mathfrak{q}_0$, и этим показано, что $\mathfrak{q}_0$ неразложима в пересечение; поскольку $x,\ y$ — произвольная пара различных элементов алгебры A, то отсюда вытекает (3). ∎

Несколько неполная двойственность, которая была замечена в теории множеств (в § I.3) и которая, очевидно, распространяется (в еще менее полной степени) на общие алгебры, наводит на мысль рассмотреть следующее понятие, двойственное понятию разделяющего семейства конгруэнций. Пусть A — произвольная Ω-алгебра; тогда под *локальной системой* подалгебр алгебры A понимают систему $\mathcal{S}$ непустых подалгебр алгебры A, которая направлена по включению и для которой $\bigcup\mathcal{S}=A$.

Тривиальными примерами локальных систем являются (i) система всех непустых подалгебр алгебры A и (ii) система, состоящая из одной алгебры A (при условии, что $A\neq\varnothing$). Система всех подалгебр с конечным числом образующих алгебры A представляет собой важный пример локальной системы. Как легко видеть, произвольная локальная система в A, замкнутая относительно подалгебр (т. е. такая система, которая вместе со всякой алгеброй содержит все ее подалгебры), обязательно содержит все подалгебры с конечным числом образующих алгебры A.

Перейдем теперь к рассмотрению *свойств* Ω-алгебр, таких, как, например, свойство быть конечной или свойство содержаться в данной алгебре в качестве подалгебры. Мы будем интересоваться только *абстрактными свойствами*, т. е. такими свойствами P, которыми обладают вместе с алгеброй A все изоморфные ей алгебры. Таким образом, свойство быть конечной является абстрактным свойством, а свойство быть подалгеброй данной алгебры, например, не является абстрактным. Если P — некоторое свойство алгебр, то говорят, что алгебра A *локально* обладает свойством P, если существует локальная система подалгебр алгебры A, каждая из которых обладает свойством P. Если каждая алгебра, которая локально обладает свойством P, в действительности сама обладает этим свойством, то P называется *локальным свойством* алгебр. Так, например, свойство быть абелевой является локальным свойством групп; с другой стороны, свойство быть конечной не является локальным свойством: мультипликативная группа всех комплексных корней из единицы локально конечна, но не конечна.

Аналогично говорят, что Ω-алгебра *резидуально* обладает свойством P, если существует такое разделяющее семейство $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$ конгруэнций на A, что каждая факторалгебра $A/\mathfrak{q}_\lambda$ обладает свойством P. В силу следствия 7.2 A резидуально обладает свойством P тогда и только тогда, когда она может быть представлена в виде подпрямого произведения Ω-алгебр, обладающих свойством P. Далее, свойство P называется *резидуальным свойством*, если всякая Ω-алгебра, резидуально обладающая свойством P, в действительности сама обладает этим свойством. Например, для групп свойство быть абелевой резидуально, так как если группа G резидуально абелева, то она является подпрямым произведением абелевых групп, и, следовательно, сама абелева, но свойство быть конечной не является резидуальным свойством. Мы закончим этот параграф результатом, устанавливающим некоторую связь между локальными и резидуальными свойствами.

***Предложение* 7.4.** *Всякое резидуальное свойство Ω-алгебр, сохраняющееся при переходе к гомоморфным образам, локально.*

Доказательство. Пусть P—свойство, удовлетворяющее условиям этого предложения, и пусть A есть Ω-алгебра с локальной системой $(A_\lambda)_{\lambda \in \Lambda}$ подалгебр, обладающих свойством P. Для удобства предупорядочим множество индексов Λ по правилу:

$$\lambda \leqslant \mu \text{ тогда и только тогда, когда } A_\lambda \subseteq A_\mu.$$

Тогда ясно, что Λ направлено. Теперь возьмем прямое произведение $D=\prod A_\lambda$ с проекциями ε_λ: $D\to A_\lambda$ и рассмотрим подмножество

$$B=\{x\in D \mid \text{существует такое } \lambda_0=\lambda_0(x), \text{ что } x\varepsilon_\lambda=x\varepsilon_{\lambda_0} \text{ для } \lambda\geqslant\lambda_0\}.$$

Таким образом, B — это подмножество элементов алгебры D, координаты которых, начиная с некоторой, постоянны. Это постоянное значение $x\varepsilon_\lambda$ обозначим через $x\varepsilon$. Мы утверждаем, что B — подалгебра алгебры D и, на самом деле, подпрямое произведение алгебр A_λ. Действительно, если $\omega\in\Omega(n)$, $x_1, \ldots, x_n\in B$, то предположим, что $x_i\varepsilon_\lambda=x_i\varepsilon$ для $\lambda\geqslant\lambda_i$; тогда, так как Λ направлено, существует такое $\lambda_0\in\Lambda$, что $\lambda_0\geqslant\lambda_i$ для $i=1, \ldots, n$; следовательно, $x_i\varepsilon_\lambda=x_i\varepsilon$ для $\lambda\geqslant\lambda_0$ и поэтому

$$(x_1\cdots x_n\omega)\varepsilon_\lambda=(x_1\varepsilon_\lambda)\cdots(x_n\varepsilon_\lambda)\omega=(x_1\varepsilon)\cdots(x_n\varepsilon)\omega.$$

Это выполняется для $\lambda\geqslant\lambda_0$, и поэтому $(x_1\cdots x_n\omega)\varepsilon_\lambda$ совпадает с $(x_1\cdots x_n\omega)\varepsilon$ по определению ε. Если заданы произвольное $\lambda\in\Lambda$ и произвольное $a\in A_\lambda$, то $a\in A_\mu$ для всех $\mu\geqslant\lambda$ и, следовательно, элемент x алгебры D, определенный по формуле

$$x\varepsilon_\mu=\begin{cases} a, & \text{если } \mu\geqslant\lambda,\\ \text{произвольный элемент в } A_\mu & \text{в противном случае,}\end{cases}$$

принадлежит подалгебре B и обладает тем свойством, что $x\varepsilon=a$; этим показано, что $\varepsilon_\lambda|B$ будет эпиморфизмом, и, таким образом, B является подпрямым произведением алгебр A_λ.

Так как $x\varepsilon\in A$ для любого $x\in B$, то ε является отображением алгебры B в алгебру A, а проведенные выше рассуждения показывают, что ε — гомоморфизм. Более того, ε — эпиморфизм, так как каждый элемент $a\in A$ содержится в A_λ для некоторого $\lambda\in\Lambda$ и, следовательно, для всех $\mu\geqslant\lambda$. Итак, A является гомоморфным образом подпрямого произведения алгебр A_λ и поэтому обладает свойством P. ∎

УПРАЖНЕНИЯ

1. Показать, что для любого наследственного свойства P свойство локально обладать свойством P является локальным свойством, а свойство резидуально обладать свойством P является резидуальным свойством.

2. Абелева группа называется группой *без кручения*, если не существует элементов конечного порядка, кроме нейтрального элемента. Показать, что свойство быть абелевой группой без кручения является одновременно локальным и резидуальным, но не сохраняется при переходе к гомоморфным образам.

3. Группа G называется p-группой (где p — простое число), если порядок каждого элемента группы G является степенью числа p. Показать, что свойство быть p-группой является локальным свойством, сохраняющимся при переходе к подгруппам, но не является резидуальным. (Указание: каждая абелева группа без кручения резидуально обладает свойством быть p-группой.)

4. Группа G называется *упорядоченной*, если ее носитель можно упорядочить так, что $a \leqslant b$, $a' \leqslant b'$ влечет $aa' \leqslant bb'$. Если G — абстрактная группа, носитель которой может быть упорядочен таким образом, что G превращается в линейно упорядоченную группу, то говорят, что G может быть линейно упорядочена. Показать, что свойство групп «G может быть линейно упорядочена» является резидуальным, но не сохраняется при переходе к гомоморфным образам. (Указание: прямое произведение любого семейства линейно упорядоченных групп можно упорядочить, если некоторым образом вполне упорядочить множество индексов, а затем упорядочить данное произведение лексикографически. Во-вторых, всякая свободная абелева группа может быть линейно упорядочена, но не всякий ее гомоморфный образ может быть так упорядочен.)

5. (Дьёдонне, Лоренцен.) Определить каноническую упорядоченность на прямом произведении упорядоченных групп $\prod G_\lambda$ по правилу: $(x_\lambda) \leqslant (y_\lambda)$ тогда и только тогда, когда $x_\lambda \leqslant y_\lambda$ для всех $\lambda \in \Lambda$. Показать, что упорядоченная абелева группа G (записываемая аддитивно) является подпрямым произведением линейно упорядоченных групп (с канонической упорядоченностью) тогда и только тогда, когда для любого $x \in G$ и любого положительного целого числа n из $nx \geqslant 0$ следует $x \geqslant 0$.

6. Пусть R — коммутативное кольцо с 1. Показать, что если R не имеет нильпотентных элементов $\neq 0$ (т. е. если $x^n = 0$ влечет $x = 0$) и R подпрямо неразложимо, то R — область целостности. Вывести отсюда, что всякое кольцо без нильпотентных элементов $\neq 0$ может быть представлено в виде подпрямого произведения областей целостности.

7. Подпрямое произведение A семейства $(A_\lambda)_{\lambda \in \Lambda}$ алгебр называется *несократимым*, если ограничение на A естественной проекции на собственный сомножитель $\prod A_\mu$ ($\mu \in \Lambda'$, где $\Lambda' \subset \Lambda$) не является мономорфизмом. Показать, что если $\varepsilon_\lambda \colon A \to A_\lambda$ — ограничения естественных проекций, то подпрямое произведение A несократимо тогда и только тогда, когда

$$\ker \varepsilon_\lambda \not\supseteq \bigcap_{\mu \neq \lambda} \ker \varepsilon_\mu$$

для каждого $\lambda \in \Lambda$.

8. Показать, что всякое подпрямое произведение конечного числа сомножителей также может быть представлено в виде несократимого подпрямого произведения некоторых из этих сомножителей. Показать, кроме того, что несократимое подпрямое произведение конечного числа простых колец обязательно будет их прямым произведением.

9. Показать, что всякая дистрибутивная структура, содержащая более двух элементов, подпрямо разложима. (Указание: для любого $a \in L$ рассмотреть левый и правый отрезки, порожденные элементом (a, a) в L^2, и показать, что пересечение конгруэнций, порожденных этими отрезками, будет диагональю в L.)

Проверить, что для любого множества A булеан $\mathscr{B}(A)$ является дистрибутивной структурой и что, кроме того, $\mathscr{B}(A) \cong 2^A$, где $2 = \{0, 1\}$ считается дистрибутивной структурой с упорядоченностью $0 < 1$. Показать, что, обратно, каждую дистрибутивную структуру L можно вложить в структуру вида $\mathscr{B}(A)$ для некоторого множества A, которое можно выбрать конечным, если L конечна.

10. Показать, что свойство группы быть простой является локальным свойством. (Указание: G проста тогда и только тогда, когда для любых $x, y \in G$, $y \neq 1$, существует произведение элементов, сопряженных с элементами y и y^{-1}, равное x.) Используя тот факт, что знакопеременная

группа, степень которой больше четырех, проста, показать, что группа всех четных подстановок с конечными носителями на счетном множестве проста.

11. Показать, что свойство групп быть резидуально конечной является резидуальным, но не является локальным (использовать упр. 1 и 10).

12. Показать, что свойство быть свободной абелевой группой не является локальным свойством.

8. СТРУКТУРА КАТЕГОРИЙ Ω-АЛГЕБР

Мы видели, что для заданной области операторов Ω все Ω-алгебры со всеми Ω-гомоморфизмами между ними образуют категорию, которая была обозначена через (Ω). Всюду в дальнейшем универсальное множество U будет произвольным, но фиксированным, так что мы не будем его явно указывать, но когда речь идет о Ω-алгебрах, нужно помнить, что рассматриваются только алгебры, носители которых принадлежат U.

Подкатегория $\mathcal{K}$ категории (Ω) называется *тривиальной*, если она содержит только одноэлементные алгебры, и *нетривиальной* в противном случае. Если вместе с каждой алгеброй A категория $\mathcal{K}$ содержит все алгебры, ей изоморфные, и вместе с любыми двумя изоморфными алгебрами A, A' содержит все изоморфизмы между A и A', то $\mathcal{K}$ называется *абстрактной*. Категория $\mathcal{K}$ называется *регулярной*, если каждый $\mathcal{K}$-гомоморфизм можно представить в виде $\varepsilon\mu$, где ε есть $\mathcal{K}$-эпиморфизм, а μ есть $\mathcal{K}$-мономорфизм. Ясно, что абстрактная категория $\mathcal{K}$ регулярна тогда и только тогда, когда для каждого $\mathcal{K}$-гомоморфизма α: $A \to B$ образ $A\alpha$ является $\mathcal{K}$-алгеброй, вложение i: $A\alpha \to B$ есть $\mathcal{K}$-гомоморфизм и α можно представить в виде $\alpha = \alpha_0 i$, где α_0: $A \to A\alpha$ является $\mathcal{K}$-эпиморфизмом.

Если $\mathcal{S}$ — некоторое множество Ω-алгебр, то из $\mathcal{S}$ можно образовать категорию, например взяв полную подкатегорию категории (Ω) с $\mathcal{S}$ в качестве класса объектов; в общем случае эта категория не будет ни абстрактной, ни регулярной. Однако заметим, что если $\mathcal{K}$ — подкатегория категории (Ω), то существует однозначно определенная *наименьшая абстрактная подкатегория категории* (Ω), содержащая $\mathcal{K}$; нужно только присоединить все изоморфные образы $\mathcal{K}$-алгебр и всевозможные изоморфизмы между ними. Если дано множество $\mathcal{S}$ Ω-*алгебр, то всегда можно построить регулярную категорию с* $\mathcal{S}$ в качестве класса объектов, например допуская в качестве отображений только изоморфизмы, но часто бывает нужно вложить данную подкатегорию категории (Ω) в регулярную подкатегорию. Для того чтобы это сделать, заметим, что множество $\mathcal{S}$ Ω-алгебр вместе с некоторыми мономорфизмами и эпиморфизмами между ними порождает регулярную подкатегорию категории (Ω) тогда и только тогда, когда для каждого мономорфизма μ и каждого эпиморфизма ε, для которых $\mu\varepsilon$ определено, существуют такие мономорфизм μ_1 и эпиморфизм ε_1 из этого множества, что $\mu\varepsilon = \varepsilon_1\mu_1$.

***Предложение* 8.1.** *Класс абстрактных подкатегорий, а также класс абстрактных регулярных подкатегорий категории* (Ω) *образуют полные структуры.*

Доказательство. Если $(\mathscr{K}_\lambda)_{\lambda\in\Lambda}$ — некоторое семейство абстрактных подкатегорий категории (Ω), то через $\mathscr{K} = \bigcap \mathscr{K}_\lambda$ обозначим категорию, классом объектов которой является $\bigcap \mathrm{Ob}\,\mathscr{K}_\lambda$, а классом морфизмов служит $\bigcap \mathrm{Hom}\,\mathscr{K}_\lambda$. Легко проверить, что это снова абстрактная подкатегория категории (Ω), и, следовательно, по предложению I.4.1 абстрактные подкатегории образуют полную структуру. Предположим теперь, что каждая подкатегория $\mathscr{K}_\lambda$, кроме того, регулярна, и пусть α: $A \to B$ есть $\mathscr{K}_\lambda$-гомоморфизм для каждого $\lambda\in\Lambda$. Тогда $A\alpha$ будет $\mathscr{K}_\lambda$-алгеброй, вложение i: $A\alpha \to B$ будет $\mathscr{K}_\lambda$-гомоморфизмом и $\alpha = \alpha_0 i$ (где α_0: $A \to A\alpha$) будет $\mathscr{K}_\lambda$-эпиморфизмом для каждого $\lambda\in\Lambda$; отсюда i и α_0 являются $\mathscr{K}$-гомоморфизмами. ∎

Обозначим структуру всех абстрактных регулярных подкатегорий категории (Ω) через $\Gamma(\Omega)$ и определим некоторые операторы замыкания на $\Gamma(\Omega)$ в смысле § II.1; это возможно, так как мы имеем дело с полной структурой. Такие операторы замыкания (которые систематически вводились Ф. Холлом для класса групп) будут обозначаться полужирными заглавными буквами; если $\mathbf{A}$ — оператор замыкания, то будем говорить, что категория $\mathscr{K}$ $\mathbf{A}$-*замкнута*, если $\mathbf{A}\mathscr{K} = \mathscr{K}$. Важнейшими примерами операторов замыкания на $\Gamma(\Omega)$ являются следующие:

(i) *Подалгебры.* Для любой категории $\mathscr{K}\in\Gamma(\Omega)$ через $\mathbf{S}\mathscr{K}$ обозначим регулярную категорию, порожденную всеми подалгебрами $\mathscr{K}$-алгебр и всеми ограничениями $\mathscr{K}$-гомоморфизмов, срезанных до подалгебр $\mathscr{K}$-алгебр. Легко проверить, что $\mathbf{S}$ будет оператором замыкания. Если категория $\mathscr{K}$ $\mathbf{S}$-замкнута, то говорят также, что она *замкнута относительно подалгебр* или что она *наследственна.*

(ii) *Факторалгебры.* Если дана категория $\mathscr{K}\in\Gamma(\Omega)$, то через $\mathbf{Q}\mathscr{K}$ обозначим регулярную категорию, порожденную всеми гомоморфными образами $\mathscr{K}$-алгебр вместе со всеми гомоморфизмами, индуцированными $\mathscr{K}$-гомоморфизмами. Тот факт, что $\mathbf{Q}$ — оператор замыкания, вытекает из следствия 3.12. Если категория $\mathbf{Q}$-замкнута, то говорят, что она *замкнута относительно гомоморфных образов.*

(iii) *Прямые произведения.* Если дана категория $\mathscr{K}\in\Gamma(\Omega)$, то через $\mathbf{P}\mathscr{K}$ обозначим регулярную категорию, порожденную всеми прямыми произведениями $P = \prod A_\lambda$ семейств $\mathscr{K}$-алгебр вместе с проекциями ε_λ: $P \to A_\lambda$ и такими гомоморфизмами между произведениями, которые индуцируются $\mathscr{K}$-гомоморфизмами между сомножителями. Если категория **P**-замкнута, то говорят, что она *замкнута относительно прямых произведений*. Если вспомнить, что множество индексов является элементом фиксированного универсального множества U, то снова ясно, что **P** — оператор замыкания.

(iv) *Локальные системы*. Если дана категория $\mathscr{K} \in \Gamma(\Omega)$, то через $\mathbf{L}\mathscr{K}$ обозначим абстрактную категорию, порожденную теми Ω-алгебрами A, которые локально являются $\mathscr{K}$-алгебрами, т. е. обладают локальной системой $(A_\lambda)_{\lambda\in\Lambda}$ $\mathscr{K}$-алгебр с вложениями $i_\lambda\colon A_\lambda \to A$, и гомоморфизмами, индуцированными $\mathscr{K}$-гомоморфизмами между алгебрами соответствующих локальных систем. Если $\mathbf{L}\mathscr{K} = \mathscr{K}$, то категория $\mathscr{K}$ называется *локальной*. Крюз (A. H. Kruse) привел пример, в котором **L** не является оператором замыкания (эта работа будет опубликована в *J. London Math. Soc.*).

(v) *Резидуальные системы*. Пусть $\mathscr{K} \in \Gamma(\Omega)$ и $\mathbf{R}\mathscr{K}$ — регулярная категория всех тех Ω-алгебр A, которые резидуально являются $\mathscr{K}$-алгебрами; это значит, что существует такое разделяющее семейство конгруэнций $(\mathfrak{q}_\lambda)$, что $A/\mathfrak{q}_\lambda$ есть $\mathscr{K}$-алгебра. Кроме того, $\operatorname{nat}\mathfrak{q}_\lambda$ является $\mathbf{R}\mathscr{K}$-гомоморфизмом, и гомоморфизм $\alpha\colon B \to A$ будет $\mathbf{R}\mathscr{K}$-гомоморфизмом в том случае, если $\alpha(\operatorname{nat}\mathfrak{q}_\lambda)$ суть $\mathscr{K}$-гомоморфизмы для всех $\lambda \in \Lambda$. **R**-замкнутая категория называется *резидуальной*. Оператор **R** снова будет оператором замыкания, и, кроме того, всякая резидуальная категория замкнута относительно прямых произведений; вообще для любой категории $\mathscr{K}$ категория $\mathbf{P}\mathscr{K}$ является подкатегорией категории $\mathbf{R}\mathscr{K}$.

Если **A** и **B** — операторы замыкания на $\Gamma(\Omega)$, то будем писать $\mathbf{A} \leqslant \mathbf{B}$ для обозначения того, что категория $\mathbf{A}\mathscr{K}$ является подкатегорией категории $\mathbf{B}\mathscr{K}$ для каждой категории $\mathscr{K} \in \Gamma(\Omega)$. Определим, далее, оператор **AB** равенством

$$(\mathbf{AB})\mathscr{K} = \mathbf{A}(\mathbf{B}\mathscr{K}).$$

В общем случае **AB** не обязан быть оператором замыкания, но нетрудно видеть, что всегда существует наименьший оператор замыкания, содержащий **A** и **B**, который мы будем обозначать через $\mathbf{A} \vee \mathbf{B}$. Это вытекает из того, что совокупность систем замыканий (соответствующих операторам замыкания) сама образует полную структуру. Можно проверить это и непосредственно тем же способом, как в замечаниях, предшествующих предложению 6.6; тогда так же, как и в этом предложении, можно вывести, что **AB** есть оператор замыкания, если $\mathbf{AB} \geqslant \mathbf{BA}$. На самом деле, множество всех операторов (т. е. унарных операций) на $\Gamma(\Omega)$, удовлетворяющих условиям J. 1—2 из § II.1, образует упорядоченную полугруппу с 1 в качестве наименьшего элемента, а операторами замыкания будут те и только те элементы этой полугруппы, которые идемпотентны (см. упр. 6.2).

Между определенными выше операторами существует некоторая связь, важная для дальнейшего изложения.

***Предложение* 8.2.** *Оператор* $\mathbf{U} = \mathbf{SP}$ *является оператором замыкания и*

$$\mathbf{P} \leqslant \mathbf{R} \leqslant \mathbf{SP}. \tag{1}$$

Доказательство. В силу сделанных выше замечаний для того, чтобы показать, что $\mathbf{SP}$ — оператор замыкания, достаточно проверить, что

$$\mathbf{PS} \leqslant \mathbf{SP}. \tag{2}$$

Пусть $A \in \mathbf{PS}\mathcal{K}$; тогда $A = \prod A_\lambda$, где A_λ — подалгебра некоторой $\mathcal{K}$-алгебры B_λ. Теперь $\prod A_\lambda$ можно вложить в $\prod B_\lambda$, откуда A изоморфна подалгебре алгебры $\prod B_\lambda$, т. е. $A \in \mathbf{SP}\mathcal{K}$; аналогично можно показать, что каждый $\mathbf{PS}\mathcal{K}$-гомоморфизм является $\mathbf{SP}\mathcal{K}$-гомоморфизмом, что и доказывает (2). Далее, Ω-алгебра будет резидуально $\mathcal{K}$-алгеброй тогда и только тогда, когда она представима в виде подпрямого произведения $\mathcal{K}$-алгебр. В частности, каждое прямое произведение $\mathcal{K}$-алгебр будет резидуально $\mathcal{K}$-алгеброй, откуда $\mathbf{P} \leqslant \mathbf{R}$, а подпрямое произведение является, очевидно, подалгеброй прямого произведения и, таким образом, $\mathbf{R} \leqslant \mathbf{U}$, что и доказывает (1). ∎

УПРАЖНЕНИЯ

1. Показать, что $\mathbf{P}\mathcal{K}$ и $\mathbf{R}\mathcal{K}$ всегда содержат тривиальные алгебры, и если $\varnothing$ обладает структурой Ω-алгебры (т. е. если $\Omega(0) = \varnothing$), то $\mathbf{L}\mathcal{K}$ всегда содержит $\varnothing$ в качестве алгебры.

2. Показать, что $\mathbf{SQ} \leqslant \mathbf{QS}$, но равенство выполняется не всегда. (Использовать следствие 3.12 при установлении неравенства и проверить, что это неравенство будет строгим в категории групп и гомоморфизмов.)

3. Показать, что в общем случае $\mathbf{SP} \neq \mathbf{PS}$.

4. Показать, что $\mathbf{QL} \leqslant \mathbf{LQ}$.

5. Показать, что $\mathbf{SR} = \mathbf{RS} = \mathbf{U}$.

6. Переформулировать предложение 7.4 в терминах, принятых в этом параграфе.

ГЛАВА III

СВОБОДНЫЕ АЛГЕБРЫ

Многие важные классы алгебр, среди них группы, кольца и структуры, состоят из всех гомоморфных образов некоторых «свободных» в этом классе алгебр, которые по существу определяются мощностью множества свободных образующих. Такие классы называются *многообразиями* алгебр и будут изучаться в главе IV, но свободные алгебры важны также в более общих ситуациях, и поэтому мы посвятим эту главу изучению свойств свободных алгебр, не зависящих от понятия многообразия. Понятие свободной алгебры представляет собой частный случай понятия универсального функтора в теории категорий, и поэтому мы опишем сначала универсальные функторы в общих категориях (см. Самюэль [48], Маклейн [63]).

1. УНИВЕРСАЛЬНЫЕ ФУНКТОРЫ

Пусть $\mathscr{K}$ — некоторая категория и F — произвольный функтор из $\mathscr{K}$ в St. Таким образом, F сопоставляет каждому $a \in \mathrm{Ob}\,\mathscr{K}$ множество $F(a)$ и каждому $\mathscr{K}$-морфизму α: $a \to b$ отображение $F(\alpha)$: $F(a) \to F(b)$. Если задано $\xi \in F(a)$, то будем писать $\xi\alpha$ вместо $\xi F(\alpha)$; тогда тот факт, что F — функтор, выражается равенствами

$$(\xi\alpha)\beta = \xi(\alpha\beta), \quad \xi\varepsilon_a = \xi \qquad (\xi \in F(a), \ \alpha, \ \beta \in \mathrm{Hom}\,\mathscr{K}),$$

если только обе части определены.

Если существует $\mathscr{K}$-объект u и элемент ρ множества $F(u)$, обладающие тем свойством, что каждому $\xi \in F(a)$ соответствует такой единственный $\xi' \in \mathrm{Hom}(u, a)$, что

$$\xi = \rho\xi',$$

то u называется *универсальным $\mathscr{K}$-объектом с универсальным морфизмом* ρ для функтора F. Таким образом, класс $\bigcup F(a)$ порождается элементом ρ при правом умножении на $\mathscr{K}$-морфизмы; это свойство часто называется *универсальным свойством* пары (u, ρ).

Конечно, универсальный объект не обязательно существует, но если существует, то определен по существу однозначно:

***Предложение* 1.1.** *Пусть F — функтор из категории $\mathscr{K}$ в* St, *и предположим, что две пары (u_1, ρ_1) и (u_2, ρ_2) универсальны для этого функтора. Тогда u_1 и u_2 эквивалентны, причем существует такая единственная эквивалентность θ: $u_1 \to u_2$, что $\rho_1\theta = \rho_2$.*

Доказательство. В силу универсального свойства объекта u_1 существует такой единственный морфизм θ: $u_1 \to u_2$, что

$$\rho_1\theta = \rho_2, \tag{1}$$

а в силу универсального свойства объекта u_2 существует такой морфизм φ: $u_2 \to u_1$, что $\rho_2\varphi = \rho_1$. Следовательно, $\rho_1\theta\varphi = \rho_1 = \rho_1\varepsilon_{u_1}$; в силу единственности находим, что

$$\theta\varphi = \varepsilon_{u_1}$$

и аналогично

$$\varphi\theta = \varepsilon_{u_2}.$$

Этим показано, что θ есть $\mathscr{K}$-эквивалентность. Поскольку θ — единственный морфизм, удовлетворяющий условию (1), то это единственная эквивалентность. ∎

Если $\mathscr{K}$ и $\mathscr{L}$ — некоторые категории, то будем говорить, что $\mathscr{L}$ *представлена* в $\mathscr{K}$, если существует ковариантный функтор F из $\mathscr{L}^0 \times \mathscr{K}$ в St. Таким образом, произвольной паре $A \in \mathrm{Ob}\,\mathscr{L}$, $a \in \mathrm{Ob}\,\mathscr{K}$ соответствует множество $F(A, a)$, и это соответствие $(A, a) \to F(A, a)$ контравариантно по A и ковариантно по a. Если заданы произвольные морфизмы φ: $B \to A$ и α: $a \to b$ в $\mathscr{L}$ и $\mathscr{K}$ соответственно, то существует отображение $F(\varphi, \alpha)$: $F(A, a) \to F(B, b)$. Обозначим результат применения этого отображения к $\xi \in F(A, a)$ через $\varphi\xi\alpha$. Тогда функторный характер соответствия F выражается равенствами

$$(\psi\varphi)\xi = \psi(\varphi\xi), \qquad \varepsilon_A\xi = \xi \qquad (\varphi, \psi \in \mathrm{Hom}\,\mathscr{L}),$$
$$\xi(\alpha\beta) = (\xi\alpha)\beta, \qquad \xi\varepsilon_a = \xi \qquad (\alpha, \beta \in \mathrm{Hom}\,\mathscr{K}),$$

которые выполняются, как только обе части определены.

В большинстве приложений объектами категорий $\mathscr{L}$ и $\mathscr{K}$ будут множества с некоторыми структурами и $F(A, a)$ будет состоять из некоторых отображений из A в a (как множеств). По этой причине элементы множества $F(A, a)$ мы будем обычно называть *допустимыми морфизмами* данного представления. Теперь вместо единственного универсального $\mathscr{K}$-объекта мы имеем по одному универсальному $\mathscr{K}$-объекту для каждого $\mathscr{L}$-объекта, что, как скоро будет показано, определяет функтор из $\mathscr{L}$ в $\mathscr{K}$. Например, если $\mathscr{L}$ — подкатегория категории $\mathscr{K}$, то $\mathscr{L}$ представлена в $\mathscr{K}$ и каждый $\mathscr{L}$-объект является своим собственным универсальным объектом при этом представлении. Менее тривиальный пример получается в том случае, когда $\mathscr{K}$ — подкатегория категории $\mathscr{L}$; вообще будем говорить, что категория $\mathscr{K}$ *подчинена* категории $\mathscr{L}$ (в обозначениях $\mathscr{K} \prec \mathscr{L}$), если существует такой функтор ι из $\mathscr{K}$ в $\mathscr{L}$, что для любых $\mathscr{K}$-морфизмов α, α': $a \to b$ (a, $b \in \mathrm{Ob}\,\mathscr{K}$) из $\alpha\iota = \alpha'\iota$ следует $\alpha = \alpha'$. $\mathscr{L}$-объект $a\iota$, соответствующий $\mathscr{K}$-объекту a, будем называть *$\mathscr{L}$-носителем* $\mathscr{K}$-объекта a, а морфизм $\alpha\iota$ будем называть *$\mathscr{L}$-морфизмом*, определяемым $\mathscr{K}$-морфизмом α. В частности, если $\mathscr{K}$ и $\mathscr{L}$ состоят из множеств с некоторой структурой и отображений, сохраняющих эту структуру, то $\mathscr{K} \prec \mathscr{L}$, если $\mathscr{L}$-объекты обладают более слабой структурой, чем $\mathscr{K}$-объекты, и функтор ι действует так, что «игнорирует» или «забывает» эту $\mathscr{K}$-структуру, т. е. является *пренебрегающим функтором* в терминологии Маклейна. Типичным примером такого функтора является функтор из категории групп в категорию множеств, при котором каждой группе сопоставляется ее носитель и гомоморфизмы рассматриваются как отображения между носителями. Это показывает, что категория Gp групп и гомоморфизмов подчинена категории St множеств и отображений; конечно, категория групп не будет подкатегорией категории множеств, поскольку различные группы могут иметь один и тот же носитель.

Если $\mathscr{K} \prec \mathscr{L}$ и ι — соответствующий функтор, то всегда можно представить $\mathscr{L}$ в $\mathscr{K}$, полагая $F(A, a) = \mathrm{Hom}(A, a\iota)$, $F(\varphi, \alpha)$: $\xi \to \varphi\xi(\alpha\iota)$. Отметим, что во всех интересующих нас случаях подчиненные категории получаются с помощью пренебрегающего функтора. Так, например, категория Gp подчинена категории St; соответствующее представление получается, если сопоставить каждому множеству X и каждой группе G все отображения множества X в носитель группы G. Как мы увидим позже, для множества X существует универсальный объект, а именно свободная группа над множеством X. Чтобы получить другой пример, заметим, что категория линейно упорядоченных множеств и монотонных гомоморфизмов подчинена категории St, и поэтому существует представление множеств в линейно упорядоченных множествах, но универсальный объект для этого представления в общем случае не существует. В дальнейшем функтор ι мы обычно будем опускать; это соответствует принятому соглашению не вводить специального обозначения для носителя алгебры или не делать различия между гомоморфизмом алгебр и соответствующим отображением носителей этих алгебр.

Вернемся теперь к общему случаю категорий $\mathscr{K}$ и $\mathscr{L}$, где $\mathscr{L}$ представлена в $\mathscr{K}$, и предположим, что для каждого $\mathscr{L}$-объекта A существует универсальный $\mathscr{K}$-объект $U(A)$ с морфизмом $\rho(A)$: $A \to U(A)$, обладающим универсальным свойством. Тогда пара $(U(A), \rho(A))$, которая в силу предложения 1.1 определена данным представлением однозначно с точностью до $\mathcal{K}$-эквивалентности, называется *универсальным функтором* для данного представления. Это название оправдывается следующей теоремой.

Теорема 1.2. *Пусть даны категории $\mathcal{K}$ и $\mathcal{L}$ и представление $\mathcal{L}$ в $\mathcal{K}$, для которого существует универсальный функтор U. Тогда U на самом деле будет функтором из $\mathcal{L}$ в $\mathcal{K}$; он определен однозначно с точностью до $\mathcal{K}$-эквивалентности.*

Доказательство. Пусть α: $A \to B$ есть $\mathcal{L}$-морфизм; умножая на ρ, получаем морфизм $\alpha\rho$: $A \to U(B)$ и, следовательно, такой единственный $\mathcal{K}$-морфизм $U(\alpha)$: $U(A) \to U(B)$, что диаграмма

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\rho"'] & B \arrow[d, "\rho"] \\ U(A) \arrow[r, "U(\alpha)"] & U(B) \end{tikzcd}$$

коммутативна. Если β: $B \to C$ — другой $\mathcal{L}$-морфизм, получаем коммутативную диаграмму

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\rho"'] & B \arrow[r, "\beta"] \arrow[d, "\rho"'] & C \arrow[d, "\rho"'] \\ U(A) \arrow[r, "U(\alpha)"] & U(B) \arrow[r, "U(\beta)"] & U(C) \end{tikzcd}$$

По определению $\mathcal{K}$-морфизма $U(\alpha\beta)$ имеем $\alpha\beta\rho = \rho U(\alpha\beta)$, а также $\alpha\beta\rho = \rho U(\alpha) U(\beta)$; отсюда в силу единственности заключаем, что

$$U(\alpha\beta) = U(\alpha) U(\beta).$$

Далее, если ε_A: $A \to A$ — тождественный морфизм, то

$$\varepsilon_A \rho = \rho = \rho U(\varepsilon_A),$$

откуда $U(\varepsilon_A) = \varepsilon_{U(A)}$. Этим показано, что U — функтор, а его единственность вытекает из предложения 1.1. ∎

Если $\mathcal{K}$ подчинена $\mathcal{L}$, то мы имеем также представление $\mathcal{K}$ в $\mathcal{L}$, но это представление, очевидно, обладает универсальным функтором, а именно

$$\eta_a: a \to a\iota;$$

переходя к двойственным категориям, получаем представление категории $\mathcal{L}^\circ$ в категории $\mathcal{K}^\circ$, которые может обладать, а может и не обладать универсальным функтором. Вообще если $\mathcal{K}$ представлена в $\mathcal{L}$, то $\mathcal{L}^\circ$ представлена в $\mathcal{K}^\circ$, и если универсальный функтор для этого представления существует, то мы получаем ковариантный функтор из $\mathscr{L}^\circ$ в $\mathscr{K}^\circ$ или, эквивалентно этому, ковариантный функтор из $\mathscr{L}$ в $\mathscr{K}$. Этот функтор называется *коуниверсальным функтором* для представления $\mathscr{K}$ в $\mathscr{L}$. Ясно, что опять коуниверсальный функтор определен однозначно с точностью до $\mathscr{K}$-эквивалентности.

Следующий пример является важным примером представления категорий. Пусть $\mathscr{K}$ — категория и Λ — предупорядоченное множество. Тогда Λ-*системой* в $\mathscr{K}$ называется семейство $(a_\lambda, \alpha_{\lambda\mu})$ $\mathscr{K}$-объектов a_λ, заиндексированных элементами множества Λ, вместе с $\mathscr{K}$-морфизмами $\alpha_{\lambda\mu}$: $a_\lambda \to a_\mu$ для всех таких $\lambda, \mu \in \Lambda$, что $\lambda \leqslant \mu$, причем выполняются условия

$$\alpha_{\lambda\lambda} = 1, \quad \alpha_{\lambda\mu}\alpha_{\mu\nu} = \alpha_{\lambda\nu}, \text{ если только } \lambda \leqslant \mu \leqslant \nu. \tag{2}$$

Через $\mathscr{F}(\mathscr{K})$ обозначим категорию, объекты которой являются Λ-системами в $\mathscr{K}$ для произвольных предупорядоченных множеств Λ, а морфизмы определяются следующим образом: если даны $\mathscr{F}(\mathscr{K})$-объекты $(a_\lambda, \alpha_{\lambda\mu})_{\lambda, \mu \in \Lambda}$ и $(b_\xi, b_{\xi\eta})_{\xi, \eta \in \mathbf{M}}$, то $\mathscr{F}(\mathscr{K})$-морфизмом между этими объектами называется монотонный гомоморфизм $\lambda \to \lambda'$ предупорядоченного множества Λ в предупорядоченное множество $\mathbf{M}$ вместе с семейством таких $\mathscr{K}$-морфизмов

$$\varphi_\lambda: a_\lambda \to b_{\lambda'},$$

что

$$\alpha_{\lambda\mu}\varphi_\mu = \varphi_\lambda\beta_{\lambda'\mu'} \qquad (\lambda, \mu \in \Lambda).$$

Если число 1 считать упорядоченным множеством, состоящим из единственного элемента, то 1-системы в $\mathscr{K}$ и их $\mathscr{F}(\mathscr{K})$-морфизмы образуют полную подкатегорию категории $\mathscr{F}(\mathscr{K})$, изоморфную категории $\mathscr{K}$. Поэтому будем считать, что $\mathscr{K}$ вложена в $\mathscr{F}(\mathscr{K})$ посредством этого изоморфизма, так что в дальнейшем категорию $\mathscr{K}$ можно рассматривать как подкатегорию категории $\mathscr{F}(\mathscr{K})$. Таким образом, мы имеем представление $\mathscr{F}(\mathscr{K})$ в $\mathscr{K}$, и возникает вопрос, существует ли универсальный функтор или коуниверсальный функтор для этого представления. При ответе на этот вопрос целесообразнее рассматривать не всю категорию $\mathscr{F}(\mathscr{K})$, а подкатегорию (содержащую, конечно, $\mathscr{K}$), которая получается, если некоторым образом ограничить класс предупорядоченных множеств. Например, можно рассматривать только линейно упорядоченные множества, или только вполне неупорядоченные множества, или направленные множества. Приведем несколько примеров, которые понадобятся нам в дальнейшем.

(i) *Универсальный функтор для $\mathscr{F}(\mathscr{K})$ над вполне неупорядоченными множествами.* В случае вполне неупорядоченных множеств при построении $\mathscr{F}(\mathscr{K})$-объектов морфизмы не участвуют и (2) пусто. По определению универсальный функтор в данном случае сопоставляет каждому семейству $(a_\lambda)_{\lambda \in \Lambda}$ $\mathscr{K}$-объектов такой $\mathscr{K}$-объект $p = \coprod a_\lambda$, единственный с точностью до $\mathscr{K}$-эквивалентности, и такое семейство $\mathscr{K}$-морфизмов

$$\rho_\lambda\colon a_\lambda \to p, \tag{3}$$

что для каждого семейства $\mathscr{K}$-морфизмов $\varphi_\lambda\colon a_\lambda \to b$ $(b \in \mathrm{Ob}\,\mathscr{K})$ существует единственный $\mathscr{K}$-морфизм $\varphi\colon p \to b$, для которого $\varphi_\lambda = \rho_\lambda\varphi$. $\mathscr{K}$-объект $\coprod a_\lambda$ называется *свободным объединением* семейства (α_λ) с *каноническими морфизмами* (3). Такое свободное объединение существует, в частности, для категории St; при этом произвольному семейству множеств (A_λ) сопоставляется множество $P = \coprod A_\lambda$, являющееся объединением таких попарно непересекающихся множеств A'_λ, что A'_λ равномощно A_λ. В этом случае $\coprod A_\lambda$ называется также *непересекающейся суммой* множеств A_λ. В § III.6 будет показано, что свободное объединение существует в (Ω), и будут рассмотрены другие категории Ω-алгебр с этим свойством.

(ii) *Коуниверсальный функтор для $\mathscr{F}(\mathscr{K})$ над вполне неупорядоченными множествами.* Этот функтор каждому семейству $(a_\lambda)_{\lambda \in \Lambda}$ $\mathscr{K}$-объектов сопоставляет $\mathscr{K}$-объект $c = \prod a_\lambda$, единственный с точностью до $\mathscr{K}$-эквивалентности, и такое семейство $\mathscr{K}$-морфизмов

$$\sigma_\lambda\colon c \to a_\lambda, \tag{4}$$

что для каждого семейства морфизмов $\varphi_\lambda\colon b \to a_\lambda$ $(b \in \mathrm{Ob}\,\mathscr{K})$ существует единственный $\mathscr{K}$-морфизм $\varphi\colon b \to c$, для которого $\varphi_\lambda = \varphi\sigma_\lambda$. $\mathscr{K}$-объект $\prod a_\lambda$ называется *прямым объединением* семейства (a_λ) с *каноническими морфизмами* (4). Например, в случае категории St прямым объединением будет просто декартово произведение; для (Ω) это будет прямым произведением, и мы увидим в § III.6, что прямые объединения существуют также в некоторых подкатегориях категории (Ω), даже если эти категории не замкнуты относительно прямых произведений.

(iii) *Универсальный функтор для $\mathscr{F}(\mathscr{K})$ над направленными множествами.* Каждой Λ-системе $(a_\lambda, \alpha_{\lambda\mu})$ в $\mathscr{K}$ этот универсальный функтор сопоставляет $\mathscr{K}$-объект d и семейство $\rho_\lambda\colon a_\lambda \to d$, удовлетворяющее условию

$$\alpha_{\lambda\mu}\rho_\mu = \rho_\lambda \qquad (\lambda \leqslant \mu),$$

так, что для каждого семейства морфизмов $\varphi_\lambda\colon a_\lambda \to b$, для которого $\alpha_{\lambda\mu}\varphi_\mu = \varphi_\lambda$, существует такой морфизм $\varphi\colon d \to b$, что $\varphi_\lambda = \rho_\lambda\varphi$. Объект d называется *прямым пределом* данной системы и обозначается

$$d = \varinjlim (a_\lambda, \alpha_{\lambda\mu}).$$

Если Λ направлено, то Λ-система в $\mathscr{K}$ называется также *направленной системой.*

(iv) *Коуниверсальный функтор для* $\mathscr{F}(\mathscr{K})$ *над множествами, направленными вниз.* Каждой Λ-системе $(a_\lambda, \alpha_{\lambda\mu})$ этот функтор сопоставляет $\mathscr{K}$-объект c и семейство σ_λ: $c \to a_\lambda$, удовлетворяющее условию

$$\sigma_\lambda \alpha_{\lambda\mu} = \sigma_\mu \qquad (\lambda \leqslant \mu),$$

так, что для каждого семейства морфизмов φ_λ: $b \to a_\lambda$, для которого $\varphi_\lambda \alpha_{\lambda\mu} = \varphi_\mu$, существует такой морфизм φ: $b \to c$, что $\varphi_\lambda = \varphi\sigma_\lambda$. Объект c называется *обратным пределом* данной системы и обозначается так:

$$c = \varprojlim (a_\lambda, \alpha_{\lambda\mu}).$$

Нетрудно доказать, что прямые и обратные пределы существуют для категории (Ω); точнее, прямые пределы существуют в любой локальной категории Ω-алгебр, замкнутой относительно гомоморфных образов, а обратные пределы существуют в любой наследственной резидуальной категории Ω-алгебр. Докажем только первое из этих утверждений, поскольку только оно нам и нужно.

***Предложение* 1.3.** *Любая локальная категория Ω-алгебр, замкнутая относительно гомоморфных образов, замкнута относительно прямых пределов.*

Доказательство аналогично доказательству предложения II. 7.4. Пусть $\mathscr{K}$ — локальная категория Ω-алгебр, замкнутая относительно гомоморфных образов; если дана некоторая Λ-система $(A_\lambda, \alpha_{\lambda\mu})$ $\mathscr{K}$-алгебр и гомоморфизмов, где Λ направлено, то построим $P = \prod A_\lambda$, где произведение берется по всем алгебрам A_λ с непустыми носителями, и рассмотрим множество T *нитей* в P, т. е. таких элементов $x = (x_\lambda)$, что для некоторого $\lambda_0 \in \Lambda$ (зависящего от x) выполняется равенство

$$x_\lambda \alpha_{\lambda\mu} = x_\mu \quad \text{для всех} \quad \mu \geqslant \lambda \geqslant \lambda_0.$$

Две нити x и y называются *эквивалентными*, если существует такое $\lambda_1 \in \Lambda$, что $x_\lambda = y_\lambda$ для всех $\lambda \geqslant \lambda_1$. Ясно, что это отношение рефлексивно и симметрично, а поскольку Λ направлено, то также и транзитивно, так что на множестве T получаем отношение эквивалентности, скажем $\mathfrak{q}$. Так же как при доказательстве предложения II. 7.4, видим, что T — подалгебра алгебры P и что $\mathfrak{q}$ — конгруэнция на T. Полагая $D = T/\mathfrak{q}$, для каждого $\lambda \in \Lambda$ получаем гомоморфизм

$$\rho_\lambda\colon A_\lambda \to D, \tag{5}$$

определяемый следующим образом: для данного $a \in A_\lambda$ рассмотрим нить x, задаваемую равенствами

$$x_\mu = \begin{cases} a\alpha_{\lambda\mu}, & \text{если } \mu \geqslant \lambda, \\ \text{любой элемент алгебры } A_\mu & \text{в противном случае.} \end{cases}$$

Ясно, что $\mathfrak{q}$-класс, содержащий x, зависит только от a и не зависит от выбора координат x_μ для $\mu \not\geqslant \lambda$. Поэтому можно записать $x^{\mathfrak{q}} = a\rho_\lambda$. Заметим, что для любого $\mu \geqslant \lambda$ элемент $a\alpha_{\lambda\mu}$ определяет тот же $\mathfrak{q}$-класс, что и a, т. е.

$$\alpha_{\lambda\mu}\rho_\mu = \rho_\lambda \quad \text{для} \quad \lambda \leqslant \mu.$$

Мы утверждаем, что D — прямой предел с каноническими гомоморфизмами ρ_λ. Чтобы установить универсальное свойство, возьмем семейство гомоморфизмов φ_λ: $A_\lambda \to B$, удовлетворяющих условиям $\alpha_{\lambda\mu}\varphi_\mu = \varphi_\lambda$. На самом деле это означает, что с помощью φ_λ координаты произвольной нити x отображаются в такое семейство (b_λ) элементов алгебры B, что $b_\lambda = b_\mu$ для всех λ, $\mu \geqslant \lambda_0$ (для некоторого $\lambda_0 \in \Lambda$); кроме того, это постоянное значение b_λ будет одним и тем же для всех эквивалентных нитей, и поэтому получаем отображение φ: $D \to B$, которое, как легко видеть, удовлетворяет равенствам

$$\varphi_\lambda = \rho_\lambda\varphi. \tag{6}$$

Теперь образы при канонических отображениях ρ_λ: $A_\lambda \to D$ образуют локальную систему $\mathcal{K}$-алгебр для D; следовательно, D сама является $\mathcal{K}$-алгеброй и ρ_λ являются $\mathcal{K}$-гомоморфизмами. Далее, так как φ_λ суть $\mathcal{K}$-гомоморфизмы, то в силу (6) и регулярности категории $\mathcal{K}$ отсюда вытекает, что φ будет $\mathcal{K}$-гомоморфизмом. ∎

УПРАЖНЕНИЯ

1. Проверить, что вложение категории $\mathcal{K}$ в $\mathcal{F}(\mathcal{K})$ действительно определяет представление категории $\mathcal{F}(\mathcal{K})$ в $\mathcal{K}$, и показать, что в случае $\mathcal{K} = \mathrm{St}$ это представление обладает универсальным функтором и коуниверсальным функтором.

2. Пусть $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$ — такие категории, что $\mathcal{K}$ подчинена $\mathcal{L}$, а $\mathcal{L}$ подчинена $\mathcal{M}$; проверить, что $\mathcal{K}$ подчинена $\mathcal{M}$. Показать далее, что если представления $\mathcal{M}$ в $\mathcal{L}$ и $\mathcal{L}$ в $\mathcal{K}$ обладают универсальными функторами U, V соответственно, то представление $\mathcal{M}$ в $\mathcal{K}$ обладает универсальным функтором $A \to V(U(A))$. Обратно, если $\mathcal{M}$ обладает универсальным функтором в $\mathcal{K}$, то $\mathcal{L}$ также обладает универсальным функтором в $\mathcal{K}$, а $\mathcal{M}$ может и не обладать универсальным функтором в $\mathcal{L}$. (Для последней части взять $\mathcal{M} = \mathcal{F}(\mathcal{K})$ относительно вполне неупорядоченных множеств индексов и $\mathcal{L} = \mathcal{F}_0(\mathcal{K})$ — подкатегорию конечных семейств $\mathcal{K}$-объектов.)

3. Пусть $\mathcal{K}$ подчинена $\mathcal{L}$ и предположим, что представление $\mathcal{L}$ в $\mathcal{K}$ обладает универсальным функтором U. Если, кроме того, $\mathcal{L}$ замкнута относи-

тельно свободных объединений и $a = \bigsqcup a_\lambda$, где (a_λ) — семейство $\mathscr{L}$-объектов, то $U(a)$ будет свободным $\mathscr{K}$-объединением семейства $(U(a_\lambda))$.

4. Доказать, что всякая резидуальная категория Ω-алгебр, замкнутая относительно подалгебр, замкнута относительно обратных пределов.

5. Показать, что если A — прямой предел направленной системы Ω-алгебр, то A может быть определена как такая Ω-алгебра, для которой канонические отображения являются гомоморфизмами. Показать, что если алгебры данной системы принадлежат категории $\mathscr{K}$, замкнутой относительно гомоморфных образов, то A будет локально $\mathscr{K}$-алгеброй.

2. АЛГЕБРЫ Ω-СЛОВ

Применим теперь результаты предыдущего параграфа к категории (Ω). Ясно, что категория (Ω) подчинена категории St с помощью функтора, сопоставляющего каждой алгебре ее носитель. Таким образом, получаем представление категории St в (Ω), и наша цель — показать, что это представление обладает универсальным функтором. Этот функтор каждому множеству X сопоставляет Ω-алгебру, которую мы будем называть *алгеброй Ω-слов над X* и обозначать через $W_\Omega(X)$. Некоторый интерес представляет конструктивное доказательство существования этой алгебры, поэтому начнем с конструкции алгебры $W_\Omega(X)$, а позже проверим универсальное свойство этой алгебры.

Пусть Ω — некоторая область операторов, X — произвольное множество, и определим Ω-алгебру $W(\Omega; X)$, *алгебру Ω-строк над X*, следующим образом: под *Ω-строкой над X* понимают конечную последовательность элементов (т. е. набор из n элементов для $n \geqslant 1$) непересекающейся суммы $\Omega \sqcup X$. На множестве $W(\Omega; X)$ всех Ω-строк над X определим структуру Ω-алгебры с помощью формального приписывания; таким образом, если $\omega \in \Omega(n)$ и $a_i \in W(\Omega; X)$ $(i = 1, \ldots, n)$, скажем

$$a_i = (a_{i1}, \ldots, a_{ik_i}) \quad (a_{ij} \in \Omega \sqcup X),$$

то

$$a_1 \ldots a_n\omega = (a_{11}, \ldots, a_{1k_1}, a_{21}, \ldots, a_{nk_n}, \omega). \tag{1}$$

Если X не пересекается с Ω, то можно заменить непересекающуюся сумму обычным объединением, и если отождествить Ω-строки, состоящие из одного члена, с соответствующим элементом множества $\Omega \cup X$, то можно считать Ω и X подмножествами множества $W(\Omega; X)$; тогда обе части формулы (1) можно обозначить через

$$a_{11} \ldots a_{1k_1} a_{21} \ldots a_{nk_n}\omega. \tag{2}$$

Для простоты обозначений мы часто будем предполагать, что X не пересекается с Ω; скоро станет ясно, что это предположение не ограничивает общности.

Определение. Подалгебра алгебры $W(\Omega; X)$, порожденная множеством X, называется *алгеброй Ω-слов над X* и обозначается через $W_\Omega(X)$. Ее элементы называются *Ω-словами над X*, а X называется *алфавитом*.

В первую очередь нужно заметить, что $W_\Omega(X)$ определяется по существу мощностью множества X.

***Предложение* 2.1.** *Если X и Y — некоторые множества, то алгебры Ω-слов над X и Y изоморфны,*

$$W_\Omega(X) \cong W_\Omega(Y),$$

тогда и только тогда, когда X и Y равномощны.

Доказательство. Если $\theta\colon X \to Y$ — взаимно однозначное соответствие, то мы получим изоморфизм между $W(\Omega; X)$ и $W(\Omega; Y)$, заменяя в каждой Ω-строке над X каждое $x \in X$ на $x\theta$. Ограничивая этот изоморфизм на $W_\Omega(X)$, получим отображение, при котором образом алгебры $W_\Omega(X)$ будет $W_\Omega(Y)$. Ясно, что на самом деле это отображение будет изоморфизмом между $W_\Omega(X)$ и $W_\Omega(Y)$.

Обратно, предположим, что

$$W_\Omega(X) \cong W_\Omega(Y). \tag{3}$$

На любой Ω-алгебре A можно определить конгруэнцию $\mathfrak{q}$, полагая, что $a \equiv b \pmod{\mathfrak{q}}$ тогда и только тогда, когда $a = b$ или $a = x\omega$, $b = y\bar{\omega}$ для некоторого $x \in A^n$, $y \in A^m$, $\omega \in \Omega(n)$, $\bar{\omega} \in \Omega(m)$. Свойства конгруэнции легко проверяются; так определенную факторалгебру $A/\mathfrak{q}$ обозначим через A^0. Тогда для любой алгебры Ω-слов $W = W_\Omega(X)$ алгебра W^0 состоит из одиночек элементов множества X и, кроме того, класса, содержащего все остальные элементы. Таким образом, $|W_\Omega(X)^0| = |X| + 1$. Следовательно, если выполняется (3), то имеем

$$|X| + 1 = |Y| + 1,$$

откуда $|X| = |Y|$. ∎

Заметим, что изоморфизм между $W_\Omega(X)$ и $W_\Omega(Y)$, полученный в первой части доказательства, однозначно определяется соответствием θ. Это вытекает из весьма общей леммы.

***Лемма* 2.2.** *Пусть A есть Ω-алгебра и X — множество образующих алгебры A. Тогда всякий гомоморфизм алгебры A в другую Ω-алгебру полностью определяется его ограничением на X.*

Действительно, если θ_1 и θ_2 — два гомоморфизма из A в B, совпадающие на X, т. е.

$$x\theta_1 = x\theta_2 \tag{4}$$

для всех $x \in X$, то пусть A' — подмножество всех элементов $x \in A$, для которых имеет место (4); тогда A' будет подалгеброй алгебры A, поскольку если $a_i\theta_1 = a_i\theta_2$ $(i = 1, \ldots, n)$ и $\omega \in \Omega(n)$, то

$$(a_1 \ldots a_n\omega)\theta_1 = (a_1\theta_1) \ldots (a_n\theta_1)\omega = \\ = (a_1\theta_2) \ldots (a_n\theta_2)\omega = (a_1 \ldots a_n\omega)\theta_2.$$

Так как по предположению A' содержит множество образующих X, то отсюда следует, что $A' = A$, т. е. (4) имеет место для всех элементов алгебры A. ▮

Чтобы получить более явное описание Ω-слов, введем понятие длины и валентности. Если дана Ω-строка над X,

$$w = c_1 \ldots c_N \quad (c_i \in \Omega \sqcup X),$$

то число N будем называть *длиной строки* w и обозначать через $l(w)$. *Валентностью* строки w, обозначаемой через $v(w)$, называется

$$v(w) = \sum v(c_i),$$

где

$$v(c) = \begin{cases} 1, & \text{если} \quad c \in X, \\ -n+1, & \text{если} \quad c \in \Omega(n). \end{cases}$$

Таким образом, элементы множества X имеют ту же самую валентность, что и постоянные операторы. С помощью этих определений мы получим следующий критерий *для того, чтобы Ω-строка была* Ω-словом (см. Ф. Холл [58]; об истории этой теоремы см. также Розенблюм [50]).

***Теорема* 2.3.** *Ω-строка $w = c_1 \ldots c_N$ над X является Ω-словом в том и только том случае, если для каждого левого отрезка $w_i = c_1 \ldots c_i$ строки w*

$$v(w_i) > 0 \quad (i = 1, \ldots, N) \tag{5}$$

и, кроме того,

$$v(w) = 1. \tag{6}$$

Заметим, что интуитивно это очевидно, так как $v(c)$ по существу символизирует «равновесие элементов» для $c \in \Omega \sqcup X$. Так, если $c \in \Omega(n)$, то для c нужно «сырье» в количестве n элементов, а получается «продукция» из одного элемента, так что

$$v(c) = \text{«продукция»} - \text{«сырье»}.$$

Теперь (5) обеспечивает на каждом данном шаге существование достаточного числа элементов, с которыми можно оперировать, а (6) утверждает, что конечным результатом будет один элемент.

Для доказательства теоремы покажем индукцией по длине $l(w)$, что вообще w будет последовательностью из r Ω-слов тогда и только тогда, когда имеет место (5) и

$$v(w) = r. \tag{6'}$$

Это утверждение превращается в утверждение теоремы при $r=1$. Ясно, что результат справедлив для слов длины 1. Пусть теперь w — некоторое Ω-слово, скажем

$$w = a_1 \ldots a_n\omega \quad (a_i \in W_\Omega(X),\ \omega \in \Omega(n)).$$

По предположению индукции имеем $v(a_i)=1$ и $v(\omega)=1-n$; отсюда

$$v(w)=n+1-n=1.$$

Кроме того, каждый левый отрезок каждого a_i обладает положительной валентностью, и потому то же самое справедливо для w. Если теперь w — последовательность из r Ω-слов, то снова имеет место (5), а (6′) получается, если сложить валентности каждого из слов.

Обратно, пусть w — некоторая Ω-строка, удовлетворяющая (5) и (6′). Если $l(w)=1$, то $v(w)=1$ и $w \in X \sqcup \Omega(0)$, так что w будет тогда Ω-словом. Если $l(w)>1$, то предположим, что $w=w'c$, где $c \in \Omega \sqcup X$ и $v(w')=r'>0$ в силу (5). По предположению индукции w' будет тогда последовательностью из r' Ω-слов. Далее, имеем

$$v(c)=v(w)-v(w')=r-r'.$$

Теперь либо $r-r'=1$ (тогда c должно быть Ω-словом и, следовательно, w — последовательностью из $r'+1=r$ слов), либо $r-r'= 1-s \leqslant 0$, и в этом случае c есть s-арный оператор. Далее,

$$s=r'-(r-1) \leqslant r',$$

поэтому из c и из s предшествующих слов можно построить только одно новое Ω-слово и получить последовательность из $r'-s+1=r$ Ω-слов, как и утверждалось. ∎

При доказательстве этой теоремы мы получили

***Следствие* 2.4.** *Ω-строка, удовлетворяющая условиям* (5) *и* (6′), *может быть записана в виде последовательности из r Ω-слов*

$$w=w_1w_2 \ldots w_r$$

единственным образом. ∎

***Следствие* 2.5.** *Если $w=c_1 \ldots c_N$ — произвольное Ω-слово вида*

$$w=a_1 \ldots a_n\omega \quad (a_i \in W_\Omega(X)), \tag{7}$$

то любая собственная последовательность $w'=c_ic_{i+1} \ldots c_j$ $(j-i<N-1)$, которая сама является Ω-словом, находится внутри единственного слова a_k выражения (7).

Действительно, в противном случае $w'=uv$, где u — некоторый правый отрезок слова a_h. По условию, наложенному на валентность слова w', $v(u)>0$, в то время как аналогичное условие для a_h показывает, что $v(u) \leqslant 0$, если только $u \neq a_h$. Таким образом, w' имеет вид $w' = a_h a_{h+1} \ldots a_k w''$, где $v(w'') = -(k-h) \leqslant 0$. Это невозможно, если w'' является левым отрезком слова a_{k+1}; следовательно, $k = n$ и $w'' = \omega$; но это возможно только в том случае, если $h = 1$ и $w' = w$, что противоречит предположению. ∎

Пусть A есть Ω-алгебра; легко видеть, что если в Ω-слове w над X заменить каждый элемент множества X на элемент алгебры A, то в силу следствия 2.4 получим однозначно определенный элемент алгебры A. Это ясно, если $l(w) = 1$, поэтому предположим, что $l(w) > 1$, и воспользуемся индукцией. Имеем

$$w = w_1 \ldots w_n \omega,$$

где $\omega \in \Omega(n)$, и в силу следствия 2.4 w_i однозначно определены и являются Ω-словами меньшей длины, чем w. Если заменить элементы множества X на элементы алгебры A, то по предположению индукции каждое w_i превратится в элемент алгебры, и, следовательно, то же будет с w. Кроме того, полученный таким образом элемент алгебры A будет единственным. Воспользуемся теперь этим замечанием, чтобы установить универсальное свойство алгебры Ω-слов.

***Теорема* 2.6.** *Пусть A есть Ω-алгебра и X — произвольное множество. Тогда любое отображение θ: $X \to A$ можно продолжить единственным образом до гомоморфизма $\bar{\theta}$: $W_\Omega(X) \to A$.*

Доказательство. Чтобы продолжить θ, определим отображение $\bar{\theta}$: $W_\Omega(X) \to A$ следующим образом. Каждое Ω-слово w однозначно представимо в виде

$$w = c_1 \cdots c_N \quad (c_i \in \Omega \sqcup X);$$

положим

$$w\bar{\theta} = c_1' \cdots c_N',$$

где

$$c' = \begin{cases} c, & \text{если} \quad c \in \Omega, \\ c\theta, & \text{если} \quad c \in X. \end{cases}$$

Таким образом, $w\bar{\theta}$ является как раз тем единственным элементом алгебры A, который получен заменой $x \in X$ на $x\theta$. Легко проверить, что $\bar{\theta}$ будет гомоморфизмом, единственным в силу леммы 2.2, и теорема доказана. ∎

Если w — некоторое Ω-слово над X и $x_1, \ldots, x_n$ — те элементы множества X, которые на самом деле участвуют в записи слова w, то w можно считать функцией от $x_1, \ldots, x_n$, и мы будем часто указывать на эту зависимость от $x_1, \ldots, x_n$, записывая w в виде

$$w = w(x_1, \ldots, x_n).$$

Если θ: $X \to A$ — произвольное отображение в Ω-алгебру A и $x_i\theta = a_i$, то образ слова w при индуцированном гомоморфизме $\bar{\theta}$ естественно обозначить через

$$w\bar{\theta} = w(a_1, \ldots, a_n).$$

Утверждение теоремы 2.6 о том, что $w(a_1, \ldots, a_n)$ однозначно определяется по $w(x_1, \ldots, x_n)$ и отображению θ: $x_i \to a_i$, существенно зависело от того факта, что операторы всегда записываются с одной стороны от той строки элементов, к которой они применяются. Так, например, если $+$ есть бинарный оператор и результат применения его к (a, b) обозначается через $a+b$, то необходимо различать

$$a+(b+c) \quad \text{и} \quad (a+b)+c \tag{8}$$

с помощью скобок (как мы это сделали) или с помощью каких-нибудь других средств. Однако если согласно обозначениям, принятым в главе II, результат применения оператора $+$ обозначить через $ab+$, то выражения (8) превратятся в

$$abc++ \quad \text{и} \quad ab+c+$$

Теперь скобки больше не нужны (это замечание принадлежит Лукашевичу). В частных случаях мы обычно будем придерживаться принятых обозначений для операторов.

Важным следствием теоремы 2.6 является приведенный ниже результат, утверждающий существование представлений Ω-алгебр (см. § III.8 ниже).

Теорема 2.7. *Всякая Ω-алгебра A может быть представлена в виде гомоморфного образа алгебры Ω-слов $W_\Omega(X)$ для подходящего множества X.*

Действительно, если X — некоторое множество образующих алгебры A, то тождественное отображение множества X на себя можно продолжить до гомоморфизма φ: $W_\Omega(X) \to A$. Образ алгебры $W_\Omega(X)$ при этом гомоморфизме будет подалгеброй алгебры A, содержащей X, и, следовательно, должен совпадать с самой алгеброй A. Таким образом, A является гомоморфным образом алгебры $W_\Omega(X)$. ∎

Очевидно, эту теорему можно применить для установления того факта, что если A есть Ω-алгебра, порожденная множеством X, то любой элемент $a \in A$ можно представить как Ω-слово над X, быть может, различными способами. Минимум длин Ω-слов, представляющих элемент a, будет называться *длиной* элемента a относительно X и обозначаться через $l_X(a)$ или короче через $l(a)$. Ясно, что $l(a) = 1$ в том и только том случае, когда $a \in X \cup \Omega(0)$; если $l(a) > 1$, то, взяв Ω-слово длины $l(a)$, представляющее элемент a, получаем представление

$$a = b_1 \ldots b_n\omega, \quad \text{где} \quad \omega \in \Omega \quad \text{и} \quad l(a) = \sum l(b_i) + 1. \tag{9}$$

Каждый элемент алгебры A имеет конечную длину относительно данного множества образующих алгебры A, и это дает возможность доказывать результаты относительно алгебры A индукцией по длине элементов. Например, докажем здесь принадлежащую Хигмэну [52] теорему об упорядоченных алгебрах, которая будет нужна позже (в гл. VII). Точнее, этот результат относится к предупорядоченным алгебрам, и мы начнем с обобщения понятия частичной вполне упорядоченности (§ I.4) для предупорядоченных множеств.

Предупорядоченное множество A называется *частично вполне упорядоченным*, если каждая строго убывающая последовательность [1]

$$a_1 > a_2 > \dots$$

обрывается и каждое подмножество попарно несравнимых элементов в A конечно. Для упорядоченных множеств это определение сводится к прежнему; вообще если A предупорядочено и $A/\mathfrak{q}$ — соответствующее упорядоченное множество (см. упр. I.3.6), то A частично вполне упорядочено тогда и только тогда, когда $A/\mathfrak{q}$ частично вполне упорядочено. Эквивалентные формулировки этого условия содержатся в следующей лемме.

Лемма **2.8.** *Для любого предупорядоченного множества A следующие три условия эквивалентны:*

(i) *Каждая бесконечная последовательность в A содержит возрастающую подпоследовательность, т. е. если дана последовательность (a_i) в A, то существует такая бесконечная последовательность (n') натуральных чисел, что $m' < n'$ влечет $a_{m'} \leqslant a_{n'}$.*

(ii) *Для каждой бесконечной последовательности (a_i) в A существует такая пара чисел m и n, что $m < n$ и $a_m \leqslant a_n$.*

(iii) *A частично вполне упорядочено.*

Доказательство. Очевидно, (i) влечет (ii) и, в силу определения частично вполне упорядоченного множества, (ii) влечет (iii); поэтому остается показать, что (iii) влечет (i). Итак, предположим, что A частично вполне упорядочено, и возьмем бесконечную последовательность (a_i) в A. Временно будем называть элемент a_i *строго минимальным*, если $a_n \nless a_i$ ни для какого n. Тогда число строго минимальных элементов в данной последовательности должно быть конечным, и поэтому можно выбрать *один такой* элемент, *скажем* $a_{1'}$, что

$$a_{1'} \leqslant a_n \quad \text{для бесконечного множества номеров } n. \qquad (10)$$

Отбрасывая все члены a_n, которые не удовлетворяют (10), получим такую бесконечную последовательность, скажем (b_j), что

[1]) Напомним, что $a > b$ означает $a \geqslant b$, но не $b \geqslant a$.

$b_1 = a_{1'} \leqslant b_n$ для всех n. Повторяя те же рассуждения для последовательности (b_j) $(j \geqslant 2)$, индукцией по n получим бесконечную возрастающую подпоследовательность подпоследовательности (a_i); это показывает, что имеет место (i). ∎

Если A и B — произвольные предупорядоченные множества, то их декартово произведение предупорядочено по правилу:

$$(a, b) \leqslant (a', b') \text{ в том и только том случае, если } a \leqslant a' \text{ и } b \leqslant b'.$$

Декартово произведение двух частично вполне упорядоченных множеств снова частично вполне упорядочено. Действительно, любая бесконечная последовательность элементов такого произведения содержит бесконечную подпоследовательность, первые компоненты членов которой расположены в возрастающем порядке, а эта подпоследовательность содержит бесконечную подпоследовательность, вторые компоненты членов которой расположены в возрастающем порядке. Аналогичные определение и доказательство показывают, что произведение любого конечного числа частично вполне упорядоченных множеств снова частично вполне упорядочено.

Перейдем теперь к Ω-алгебрам; Ω-алгебра A *предупорядочена по делимости*, если ее носитель предупорядочен таким образом, что для любого $\omega \in \Omega$

(a) если $a_i \leqslant b_i$ $(i = 1, \ldots, n)$, то $a_1 \cdots a_n\omega \leqslant b_1 \ldots b_n\omega$,

(b) если $a \leqslant b_i$ для некоторого i, то $a \leqslant b_1 \cdots b_n\omega$.

Теперь теорему Хигмэна можно сформулировать следующим образом:

***Теорема* 2.9.** *Пусть A есть Ω-алгебра с предупорядоченностью по делимости, причем Ω конечно. Если A порождается частично вполне упорядоченным множеством X, то алгебра A сама частично вполне упорядочена.*

Доказательство. Если алгебра A не является частично вполне упорядоченной, то существует такая последовательность (a_i) в A, что

$$a_i \nleqslant a_j \quad \text{для всех таких } i, j, \text{ что } i < j. \tag{11}$$

Назовем последовательность (a_i) *невозрастающей*, если она удовлетворяет (11). Среди всех невозрастающих последовательностей (a_i) в A выберем одну, у которой a_1 имеет минимальную длину. Среди невозрастающих последовательностей, начинающихся с этого a_1, выберем одну, у которой a_2 имеет минимальную длину, и т. д. Тогда так построенная бесконечная последовательность $a_1, a_2, \ldots$

сама будет невозрастающей. Теперь для каждого $i = 1, 2, \ldots$ либо $l(a_i) = 1$, либо

$$a_i = b_{i1} \cdots b_{in_i}\omega_i, \quad b_{ik} \in A, \quad \sum l(b_{ik}) + 1 = l(a_i). \tag{12}$$

Заметим, что если $l(a_i) = 1$, то $a_i \in X \cup \Omega(0)$, и так как $\Omega(0)$ конечно, то множество $X \cup \Omega(0)$ частично вполне упорядочено. Отсюда следует, что может существовать лишь конечное число элементов a_i длины 1, так как в силу (11) они образуют невозрастающую последовательность. Таким образом, элементы a_i вида (12) все еще образуют бесконечную последовательность.

Мы утверждаем, что множество B всех элементов b_{ik}, встречающихся в (12), частично вполне упорядочено. Действительно, в противном случае можно было бы найти в B бесконечную невозрастающую последовательность $(b_{i'i^*})$ $(i = 1, 2, \ldots)$, т. е.

$$b_{i'i^*} \not\leqslant b_{j'j^*} \quad \text{для всех таких} \quad i, j, \text{ что } i < j. \tag{13}$$

Пусть i_0 — наименьшее значение номеров i', встречающихся в этой последовательности; тогда, отбрасывая конечное число членов этой последовательности, можно предполагать, что $i_0 = 1'$. Рассмотрим теперь последовательность

$$a_1, \ldots, a_{1'-1}, b_{1'1^*}, b_{2'2^*}, \ldots. \tag{14}$$

Если $a_h \leqslant b_{i'i^*}$ для некоторого $h < 1'$ и некоторого i, то $a_h \leqslant a_{i'}$, а это противоречит (11). Итак, $a_h \not\leqslant b_{i'i^*}$ и вместе с (11) и (13) это показывает, что последовательность (14) невозрастающая. Но в силу (12) $l(b_{1'1^*}) < l(a_{1'})$, что противоречит выбору $a_{1'}$. Таким образом, B не содержит невозрастающих последовательностей, т. е. B частично вполне упорядочено. Так как Ω конечно, то некоторое $\omega \in \Omega$ встречается в (12) бесконечное число раз; следовательно, переходя к подпоследовательности последовательности (a_i), можно предполагать, что $\omega = \omega_i$ для всех i. Пусть $a(\omega) = n$, тогда декартова степень B^n снова частично вполне упорядочена; значит, последовательность $a_i = b_{i1} \cdots b_{in}\omega$ содержит возрастающую подпоследовательность; но это противоречит (11), и теорема доказана. ∎

Эту теорему можно сформулировать также на языке графов, и на самом деле приведенное выше доказательство основано на доказательстве более общего результата теории графов, принадлежащего Нэш-Вильямсу [63]; см. также Краскэл [60] и упр. 10 ниже.

УПРАЖНЕНИЯ

1. Нужны ли скобки, если каждый оператор записывается с одной стороны от строки элементов, к которой он применяется, и для каждого n все n-арные операторы записываются с одной и той же стороны (т. е. или справа, или слева, но, быть может, с разных сторон для различных n)?

2. (Ф. Холл.) Показать, что число Ω-слов длины k, в запись которых n-арные операторы входят k_n раз (считая элементы множества X 0-арными операторами), равно

$$\frac{(k-1)!}{k_0!\,k_1!\,\ldots}.$$

3. Показать, что Ω-алгебра A будет алгеброй Ω-слов, если в ней существует такое множество образующих X, что для любых ω, $\bar{\omega}\in\Omega$ и любых a_i, $b_j\in A$ (i) $a_1\cdots a_n\omega\notin X$ и (ii) $a_1\cdots a_n\omega=b_1\cdots b_m\bar{\omega}$ влечет $m=n$, $\omega=\bar{\omega}$ и $a_i=b_i$ $(i=1, \ldots, n)$.

4. Показать, что A будет локально алгеброй Ω-слов тогда и только тогда, когда выполняется условие (ii) упр. 3. Привести пример Ω-алгебры, которая локально является алгеброй Ω-слов, но не является алгеброй Ω-слов. (Взять Ω, состоящее из одного унарного оператора.)

5. Показать, что всякая подалгебра алгебры $W_\Omega(X)$ имеет вид $W_\Omega(Y)$ для некоторого Y. (В качестве Y взять минимальное множество образующих этой подалгебры и применить упр. 3.)

6. Показать, что группа автоморфизмов алгебры Ω-слов над X изоморфна симметрической группе над X.

7. Пусть A и B суть Ω-алгебры с одним и тем же множеством образующих X, и обозначим через H подалгебру алгебры $A\times B$, порожденную элементами (x, x) $(x\in X)$. Показать, что если ε — проекция $A\times B\to A$, ограниченная на H, то ε всегда будет эпиморфизмом, и что ε будет изоморфизмом при любом выборе алгебры B (порожденной множеством X) тогда и только тогда, когда A — алгебра Ω-слов над X.

8. (Эрдёш.) Показать, что если множество X натуральных чисел таково, что всякое его бесконечное подмножество содержит два числа, одно из которых делит другое, то то же самое справедливо для множества всевозможных произведений элементов из X.

9. Показать, что если X — предупорядоченное множество, то на алгебре Ω-слов $W_\Omega(X)$ можно определить предупорядоченность по делимости, которая индуцирует на X данную предупорядоченность.

10. Пусть Ω — частично вполне упорядоченная область операторов; тогда говорят, что Ω-алгебра A *предупорядочена по делимости*, если она предупорядочена таким образом, что для любых ω, $\bar{\omega}\in\Omega$

(a′) если $a_i\leqslant b_{i'}$ для некоторых индексов $1'<2'<\cdots<r'$ из набора $1, \ldots, s$ и $\omega\leqslant\bar{\omega}$, то $a_1\cdots a_r\omega\leqslant b_1\cdots b_s\bar{\omega}$,

(b) если $a\leqslant b_i$ для некоторого i, то $a\leqslant b_1\cdots b_r\omega$.

Проверить, что это определение превращается в определение, данное выше, если взять Ω конечным и вполне неупорядоченным. Показать, что при таком новом определении теорема 2.9 имеет место для всякой частично вполне упорядоченной области операторов. (Показать сначала, что конечные последовательности элементов множества B, определяемого так же, как при доказательстве теоремы 2.9, частично вполне упорядочены, если считать эти последовательности элементами свободной полугруппы над B и применить теорему 2.9; в последней части доказательства использовать эту полугруппу вместо B^n.)

3. КЛОНЫ ОПЕРАЦИЙ

Пусть A — непустое множество; через $\mathfrak{O}(A)$ обозначим множество всех конечноместных операций на A. Как мы видели, структура Ω-алгебры на A определяется некоторым подмножеством множества $\mathfrak{O}(A)$; из операций этого подмножества можно составить путем композиции другие операции, и решающую роль играет не множество операций на A, определяемых областью Ω, а множество всех операций, которые могут быть составлены таким способом из этих операций. Способ, с помощью которого составляются эти операции на A, можно рассматривать как результат применения некоторых операторов, действующих на $\mathfrak{O}(A)$, и эти операторы определяют на $\mathfrak{O}(A)$ некоторую алгебраическую структуру, которую мы теперь опишем более подробно.

Заметим, что $\mathfrak{O}(A)$ можно представить в виде непересекающейся суммы

$$\mathfrak{O}(A)=\bigsqcup \mathfrak{O}_n(A),$$

где $\mathfrak{O}_n(A)$ — множество всех n-арных операций на A. Если заданы произвольные m элементов $\alpha_1, \ldots, \alpha_m \in \mathfrak{O}_n$ и $\beta \in \mathfrak{O}_m$, то существует единственная n-арная операция γ, определяемая равенством

$$c\gamma=(c\alpha_1) \cdots (c\alpha_m)\beta \quad \text{для всех} \quad c \in A^n. \tag{1}$$

Эта операция γ будет обозначаться через $\alpha_1 \cdots \alpha_m\beta$ и называться *композицией* $\alpha_1, \ldots, \alpha_m$ *с* β, так что имеем

$$c(\alpha_1 \cdots \alpha_m\beta)=(c\alpha_1) \cdots (c\alpha_m)\beta. \tag{2}$$

Далее, для каждого $n>0$ существует n элементов $\delta_n^{(i)} \in \mathfrak{O}_n$, определяемых равенствами

$$c\delta_n^{(i)}=c_i, \quad \text{где} \quad c=(c_1, \ldots, c_n) \in A^n. \tag{3}$$

Таким образом, оператор $\delta_n^{(i)}$ выбирает i-ю координату; $\delta_n^{(i)}$ называется *единичным оператором*. Теперь $\mathfrak{O}(A)$ можно считать частичной алгеброй с композицией в качестве $(m+1)$-арной операции (по крайней мере в случае (1)) и единичными операторами в качестве 0-арных операций, значениями которых (в случае (3)) являются n-арные операции на A. Для композиции произвольного типа нужно точно установить ее область определения; в самом деле, будет ли определена композиция $\alpha_1, \ldots, \alpha_m$ с β, зависит только от арности операций $\alpha_1, \ldots, \alpha_m$, β. Любое множество операций на A, замкнутое относительно операций (1) и (3), т. е. замкнутое относительно композиции и содержащее единичные операторы, называется *замкнутым множеством операций на* A, или короче, *клоном* на A (Ф. Холл). В частности, $\mathfrak{O}(A)$ является клоном, и любой клон на A считается в то же время *подклоном* клона $\mathfrak{O}(A)$. Если $\mathcal{F}$, $\mathcal{G}$ — произвольные клоны, то *гомоморфизмом клонов* $\mathcal{F} \to \mathcal{G}$ называется отображение, сохраняющее арность каждого элемента и согласованное с операциями клонов. Таким образом, клоны являются примером градуированных алгебр в смысле Хиггинса [63].

Пусть A есть Ω-алгебра; тогда действие операторов из Ω на A определяет некоторые операции на A; клон, порожденный этими операциями, называется *клоном действия* Ω на A. Обозначая этот клон через $\mathcal{F}$, видим, что элементами клона $\mathcal{F}$ будут те и только те операции на A, которые могут быть получены повторной композицией из Ω и единичных операторов. Отсюда следует, что Ω-подалгебрами алгебры A будут те и только те подмножества алгебры A, которые замкнуты относительно операций клона $\mathcal{F}$. Вообще если X — произвольное подмножество алгебры A, то множество $X\mathcal{F}$, состоящее из всех значений операций из $\mathcal{F}$, когда аргументы принимают любые значения из X, будет подмножеством, замкнутым относительно $\mathcal{F}$, и, следовательно, подалгеброй алгебры A. Как легко видеть, на самом деле это подалгебра, порожденная множеством X. Точнее, имеет место

***Предложение* 3.1.** *Пусть A есть Ω-алгебра и $\mathcal{F}$ — клон действия Ω на A. Если $c=(c_1, \ldots, c_n) \in A^n$, то $c\mathcal{F}$ является Ω-подалгеброй алгебры A, порожденной элементами $c_1, \ldots, c_n$.*

Доказательство непосредственно вытекает из определения клона $\mathcal{F}$. ∎

Чтобы подробнее изучить клон действия Ω, нам потребуется понятие централизатора в $\mathfrak{O}(A)$. Пусть α, $\beta \in \mathfrak{O}(A)$, где A — произвольное множество; обозначим арности операций α, β через m, n соответственно. Если C — некоторая матрица типа $m \times n$ из элементов множества A, то к каждой строке матрицы C можно применить β и, таким образом, получить столбец из m элементов множества A, который можно обозначить через $C\beta$. Для любого столбца b из m элементов множества A обозначим через αb результат применения α к b. Тогда, применяя α к n столбцам матрицы C, получим строку из n элементов множества A, которую обозначим через αC. При таком соглашении $(\alpha C)\beta$ и $\alpha(C\beta)$ определены как элементы множества A. Если

$$(\alpha C)\beta = \alpha(C\beta) \quad \text{для всех матриц типа } m \times n \text{ над } A, \tag{4}$$

то говорят, что α и β *перестановочны*. Так, например, в случае Ω-алгебры Ω-эндоморфизмы будут унарными операциями, перестановочными со всеми операциями, определяемыми элементами области Ω.

Пусть A — некоторое множество и U — произвольное подмножество из $\mathfrak{O}(A)$; говорят, что элемент α из $\mathfrak{O}(A)$ *централизует* U, если α перестановочен с каждым элементом из U. Множество всех элементов, централизующих U, называется *централизатором* U

в $\mathfrak{S}(A)$ и обозначается через U^*, причем централизатор всего множества $\mathfrak{S}(A)$ называется *центром* клона $\mathfrak{S}(A)$. Для простоты обозначений удобно писать элементы из U^* с противоположной стороны относительно элементов из U; так, если U действует справа, то U^* действует слева, и тогда закон коммутативности принимает вид закона ассоциативности (4).

***Предложение* 3.2.** *Пусть A — произвольное множество; тогда централизатор любого подмножества клона $\mathfrak{S}(A)$ будет подклоном в $\mathfrak{S}(A)$. В частности, центром клона $\mathfrak{S}(A)$ будет клон, состоящий из всех единичных операторов, если только A содержит больше одного элемента.*

Доказательство. Ясно, что всякий единичный оператор перестановочен с каждой операцией. Пусть теперь U — некоторое подмножество из $\mathfrak{S}(A)$; выберем $\alpha_1, \ldots, \alpha_m, \beta \in U^*$, где α_i n-арны и β m-арна, и пусть η — произвольная k-арная операция в U. Тогда для любой матрицы C типа $k \times n$ над A

$$\begin{aligned}(\eta C)(\alpha_1 \cdots \alpha_m\beta) &= [(\eta C)\alpha_1] \cdots [(\eta C)\alpha_m]\beta = \\ &= [\eta(C\alpha_1)] \cdots [\eta(C\alpha_m)]\beta = \\ &= \{\eta[(C\alpha_1) \cdots (C\alpha_m)]\}\beta = \\ &= \eta\{[(C\alpha_1) \cdots (C\alpha_m)]\beta\} = \\ &= \eta[C(\alpha_1 \cdots \alpha_m\beta)];\end{aligned}$$

это показывает, что U^* замкнуто относительно композиции и поэтому является клоном.

Предположим, что A содержит больше одного элемента и α принадлежит центру клона $\mathfrak{S}(A)$. Если α есть 0-арный оператор, то его значение должно быть неподвижным элементом при любой подстановке множества A, что неверно, поскольку A содержит больше одного элемента. Поэтому $a(\alpha) = n \geqslant 1$; предположим теперь, что $\alpha \neq \delta_n^{(i)}$ $(i = 1, \ldots, n)$; тогда значение $c\alpha$, когда $c = (c_1, \ldots, c_n)$ пробегает A^n, отлично от c_i. Таким образом, можно найти такую матрицу C типа $n \times n$ над A, что столбец $C\alpha$ отличен от всех столбцов матрицы C. Определим операцию $\beta \in (\mathfrak{S}_n(A))^n$ (действующую слева) следующим образом: $\beta x = x$ для всех таких столбцов x, что $x \neq C\alpha$, а $\beta(C\alpha)$ положим равным первому столбцу матрицы C. Тогда

$$(\beta C)\alpha = C\alpha \neq \beta(C\alpha),$$

что противоречит предположению; следовательно, α должен быть единичным оператором. ∎

Пусть A — некоторая Ω-алгебра; через U обозначим множество операций, определяемых действием Ω, и через $\mathcal{F}$ — клон действия Ω. Таким образом, $\mathcal{F}$ — это клон, порожденный множеством U, и в силу предложения 3.2 ясно, что централизатор U^* множества U содержится в централизаторе клона $\mathcal{F}$. Отсюда следует, что $\mathcal{F} \subseteq U^{**}$, но равенство здесь не обязательно выполняется. Назовем U^{**} *бицентрализатором* области операторов Ω; если, кроме того,

$$\mathcal{F} = U^{**}, \tag{5}$$

то будем говорить, что Ω действует *бицентрально*. Требование (5) очень сильное, и на практике полезнее иметь более слабые условия. Будем говорить, что Ω действует *полно* на A, если для каждого $\varphi \in U^{**}$ и каждого $c \in A^n$, где $n = a(\varphi)$, существует такое $\varphi' \in \mathcal{F}$, что

$$c\varphi = c\varphi'. \tag{6}$$

Если для каждого конечного множества элементов $c_1, \ldots, c_r \in A^n$ существует такое $\varphi' \in \mathcal{F}$, что

$$c_i\varphi = c_i\varphi' \quad (i = 1, \ldots, r), \tag{7}$$

то говорят, что Ω действует *плотно* на A. Ясно, что если множество операций действует бицентрально, то оно действует плотно, и если Ω действует плотно, то оно действует полно. Если рассматривать A как дискретное топологическое пространство, то $\mathfrak{S}_n(A) = A^{A^n}$ будет топологическим пространством в топологии декартова произведения, и, следовательно, $\mathfrak{S}(A) = \bigsqcup \mathfrak{S}_n(A)$ превращается в топологическое пространство. Полученная топология называется *топологией произведения*, и утверждение, что Ω действует на A плотно, равносильно утверждению, что множество $\mathcal{F}$, клон действия Ω, плотно в бицентрализаторе области Ω. Когда A конечно, это равносильно тому, что Ω действует бицентрально. Вообще имеет место

***Предложение* 3.3.** *Пусть A — некоторая Ω-алгебра и через Θ обозначим централизатор области Ω. Если A, как Θ-алгебра, порождается конечным множеством элементов, то Ω действует плотно тогда и только тогда, когда Ω действует бицентрально.*

Доказательство. Предположим сначала, что Ω действует плотно. Пусть $X = \{x_1, \ldots, x_k\}$ — конечное множество образующих Θ-алгебры A, и пусть φ — некоторый элемент в бицентрализаторе области операторов Ω. Если $a(\varphi) = n$, то X^n снова конечно (состоит из k^n элементов), и так как Ω действует плотно, то клон действия Ω содержит такое φ', что

$$y\varphi = y\varphi' \quad \text{для всех } y \in X^n.$$

Алгебра A порождается множеством X; следовательно, любой элемент $c \in A^n$ имеет вид θY, где $\theta \in \Theta$ и Y — матрица типа $m \times n$ над X. Отсюда

$$c\varphi = (\theta Y)\varphi = \theta(Y\varphi) = \theta(Y\varphi') = (\theta Y)\varphi' = c\varphi'.$$

Таким образом, равенство (6) имеет место для всех $c \in A^n$, а это и означает, что Ω действует бицентрально. Обратно, всякая область операторов Ω, действующая бицентрально, действует плотно. ∎

Перейдем теперь к вопросу о том, при каких условиях Ω действует плотно. Нашей главной целью является теорема плотности, которая утверждает, что Ω действует плотно на A тогда и только тогда, когда Ω действует полно на A^r для всех r. Сначала нам потребуется лемма о бицентрализаторах.

Лемма 3.4. *Пусть A есть Ω-алгебра с бицентрализатором Φ. Тогда для любого $r \geqslant 1$ Φ будет также бицентрализатором области операторов Ω, действующей на A^r.*

Доказательство. Пусть Θ — централизатор области Ω, действующей на A, и Θ' — централизатор области Ω, действующей на A^r. Если задан n-арный оператор $\omega \in \Omega$, то m-арная операция θ на A^r перестановочна с ω при условии, что для любой матрицы C типа $m \times n$ над A^r

$$(\theta C)\,\omega = \theta\,(C\omega). \tag{8}$$

Так как значениями операции θ будут элементы из A^r, θ можно считать строкой из r (mr)-арных операций на A, скажем $\theta_1, \ldots, \theta_r$, и (8) просто означает, что каждая операция θ_i перестановочна с ω, как оператором на A. Таким образом, $\theta \in \Theta'$ в том и только том случае, если $\theta_i \in \Theta$ $(i = 1, \ldots, r)$. Пусть теперь Φ и Φ' — централизаторы множеств Θ и Θ' соответственно; нужно показать, что $\Phi' = \Phi$. Если задана операция $\varphi \in \Phi'$, где φ, скажем, n-арна, то

$$\varphi = (\varphi_1, \ldots, \varphi_r)$$

состоит из r таких (nr)-арных операций на A, что

$$(\theta C)\,\varphi = \theta\,(C\varphi) \quad \text{для любого } \theta \in \Theta' \text{ и } C \in A^{m \times n \times r}. \tag{9}$$

Здесь $C \in A^{m \times n \times r}$ означает, что C — параллелепипед из $m \times n \times r$ элементов алгебры A. Каждая операция θ_i применяется к сечению

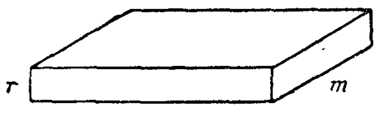

Рис. 9.

параллелепипеда C из $m \times r$ элементов; выберем θ так, чтобы θ_i сопоставляли каждому сечению типа $m \times r$ элемент с индексом (1.1). Такая операция состоит из единичных операторов и поэтому принадлежит Θ'. Теперь при таком выборе операции θ (9) показывает, что операция φ_1, применяемая к сечению типа $n \times r$, не зависит от элементов этого сечения с индексами (h, j) для всех j, за исключением $j = 1$. Другими словами, операцию φ_1 и аналогично каждую операцию φ_i можно считать n-арной. Далее, при том же самом выборе операции θ получаем, что $\varphi_1 = \ldots = \varphi_r$. Таким образом, φ определяет n-арную операцию на A. Так как эта операция централизует Θ, то она должна принадлежать Φ, откуда $\Phi' \subseteq \Phi$. Обратно, если $\varphi \in \Phi$, то φ принадлежит централизатору множества Θ', поскольку Ω и Φ, действующие на A^r, имеют один и тот же централизатор, и поэтому $\varphi \in \Phi'$. Итак, $\Phi' = \Phi$. ∎

Рассмотрим теперь Ω-алгебру A; через $\mathcal{F}$ обозначим клон действия и через Φ — бицентрализатор области Ω на A. Утверждение, что Ω действует на A полно, означает следующее: для каждого $c \in A^n$ и каждой n-арной операции $\varphi \in \Phi$ существует такая операция $\varphi' \in \mathcal{F}$, что $c\varphi = c\varphi'$. Если $c = (c_1, \ldots, c_n)$, то $c\varphi'$ будет элементом Ω-подалгебры, порожденной элементами $c_1, \ldots, c_n$, и, обратно, каждый элемент этой подалгебры имеет вид $c\varphi'$ $(\varphi' \in \mathcal{F})$. Таким образом, Ω действует полно в том и только том случае, если для каждого $\varphi \in \Phi$ и каждого $c \in A^n$, где $a(\varphi) = n$, $c\varphi \in c\mathcal{F}$. Аналогично Ω действует плотно тогда и только тогда, когда для каждой операции $\varphi \in \Phi$ и каждой матрицы C типа $r \times n$ над A $C\varphi$ принадлежит подалгебре алгебры A^r, порожденной n столбцами матрицы C. Так как Φ является в то же время бицентрализатором области операторов Ω, действующей на A^r, то это просто показывает, что Ω действует полно на A^r, и мы получаем следующую теорему:

***Теорема* 3.5. (*Теорема плотности.*)** *Пусть A — некоторая Ω-алгебра. Тогда Ω действует плотно на A в том и только том случае, если Ω действует полно на A^r для $r = 1, 2, \ldots$.* ∎

Чтобы получить удобные достаточные условия, при которых имеет место теорема плотности, нужно наложить какие-то условия на алгебры. Рассмотрим только одно условие, которое, в частности, может быть применено в случае модулей над кольцом для получения обычной теоремы плотности. Ω-алгебра A называется *вполне сжимаемой*, если для каждого натурального $n = 1, 2, \ldots$ и каждой подалгебры B алгебры A^n существует Ω-эндоморфизм алгебры A^n, отображающий A^n на B. Тогда имеет место

***Предложение* 3.6.** *Во всякой вполне сжимаемой Ω-алгебре A Ω действует плотно.*

Доказательство. Фиксируем r и пусть Φ — бицентрализатор области операторов Ω, действующей на A^r. Если задана некоторая n-арная операция $\varphi \in \Phi$ и некоторые $c_1, \ldots, c_r \in A^n$, то через B обозначим подалгебру алгебры A^r, порожденную n столбцами матрицы $C = \begin{pmatrix} c_1 \\ \vdots \\ c_r \end{pmatrix}$. Если π — эндоморфизм алгебры A^n, отображающий A^n на B, то $C = \pi X$, где X — матрица типа $r \times n$ с элементами из A. Отсюда

$$C\varphi = (\pi X)\varphi = \pi(X\varphi) \in B.$$

Это показывает, что $C\varphi = C\varphi'$ для некоторого $\varphi' \in \mathcal{F}$, поскольку B порождается столбцами матрицы C; иными словами, Ω действует полно на A^r и, следовательно, в силу теоремы плотности действует плотно на A. ∎

Если в качестве Ω-алгебр мы возьмем R-модули, где R — данное кольцо, то всякий вполне приводимый модуль (т. е. всякий модуль, который может быть представлен в виде суммы неприводимых модулей) будет вполне сжимаемым в смысле данного выше определения, поскольку если M вполне приводим, то M^r также вполне приводим, и тогда всякий его подмодуль выделяется прямым слагаемым. На этом пути получаем теорему плотности Шевалле — Джекобсона для модулей (Джекобсон [56], гл. VI): если M — вполне приводимый унитарный R-модуль, где R — кольцо с единицей, то R действует плотно на M.

УПРАЖНЕНИЯ

1. Показать, что когда A состоит из одного элемента, $\mathfrak{S}(A)$ совпадает со своим центром.

2. Для произвольного множества A найти централизатор множества $\mathfrak{S}_1(A)$ и вообще множества $\mathfrak{S}_n(A)$.

3. (Ф. Холл.) *Абстрактным клоном* называется частичная алгебра A, определяемая следующим образом: каждому $c \in A$ сопоставлено неотрицательное целое число $\alpha(c)$; A обладает такими постоянными операторами $d_n^{(i)}$ ($i = 1, \ldots, n$; $n = 1, 2, \ldots$), что $\alpha\left(d_n^{(i)}\right) = n$, и для каждого натурального числа r существует $(r+1)$-арная операция

$$(a_1, \ldots, a_r, b) \to a_1 \cdots a_r b\mu,$$

которая определена только тогда, когда $\alpha(a_1) = \ldots = \alpha(a_r)$, $\alpha(b) = r$; кроме того, в этом случае $\alpha(a_1 \ldots a_r b\mu) = \alpha(a_1)$. Эти операции подчинены следующим правилам:

(i) $$(ab_1\mu) \ldots (ab_s\mu)\, c\mu = abc\mu\mu,$$

где $a = (a_1, \ldots, a_r)$, $b = (b_1, \ldots, b_s)$ и $\alpha(a_i) = n$, $\alpha(b_j) = r$, $\alpha(c) = s$;

(ii) $$a\, d_r^{(i)}\mu = a_i,$$

где a означает то же самое, что в (i).

Показать, что всякий клон операций является абстрактным клоном [1]).

---

[1]) О представлении абстрактных клонов в клонах операций см. работу Я. В. Хиона (*Сиб. матем. журн.*, 8 (1967), 174—194).— *Прим. ред.*

4. Определить $W_\Omega(X)$ как абстрактный клон и показать, что для всякой Ω-алгебры A существует естественный гомоморфизм клонов $W_\Omega(X) \to \mathfrak{G}(A)$. Показать, что и обратно, если A — произвольное множество, то всякий гомоморфизм клонов $W_\Omega(X) \to \mathfrak{G}(A)$ определяет структуру Ω-алгебры на A.

5. Пусть R—кольцо, не обязательно с единицей. Будем считать R-модуль M вполне приводимым, если всякий его подмодуль выделяется прямым слагаемым и для $x \in M$ равенство $xR = 0$ влечет $x = 0$. Показать, что $x \in xR$ для всякого $x \in M$, и вывести отсюда, что теорема плотности остается справедливой и в этом случае.

4. ПРЕДСТАВЛЕНИЯ КАТЕГОРИЙ Ω-АЛГЕБР

Мы видели, что алгебры Ω-слов могут быть определены как универсальный функтор представления категории St в (Ω). Эту ситуацию можно обобщить, заменяя St категорией $\mathcal{L}$, подчиненной категории St, и заменяя (Ω) категорией $\mathcal{K}$ Ω-алгебр, подчиненной категории $\mathcal{L}$. Это приводит к представлению категории $\mathcal{L}$ в $\mathcal{K}$ (называемому естественным представлением), и наша цель состоит в том, чтобы найти условия, при которых это представление обладает универсальным функтором.

В дальнейшем каждая подкатегория $\mathcal{K}$ категории (Ω) предполагается абстрактной и регулярной, если не оговорено противное. Для таких категорий $\mathcal{K}$ понятие представления будет ограничено следующим образом. Если $\mathcal{L} \prec \mathrm{St}$, то будем говорить, что $\mathcal{L}$ *представлена* в $\mathcal{K}$, если существует такое представление категории $\mathcal{L}$ в $\mathcal{K}$ в смысле § III. 1, что (i) всякий допустимый морфизм $\rho\colon X \to A$ $(X \in \mathrm{Ob}\,\mathcal{L},\ A \in \mathrm{Ob}\,\mathcal{K})$ определяет отображение (снова обозначаемое через ρ) носителя $\mathcal{L}$-объекта X в носитель $\mathcal{K}$-объекта A; (ii) подалгебра A_0 алгебры A, порожденная образом носителя X при отображении ρ, является $\mathcal{K}$-алгеброй; (iii) вложение $i\colon A_0 \to A$ является $\mathcal{K}$-гомоморфизмом; (iv) если ρ срезано до отображения ρ_0 в A_0, так что $\rho = \rho_0 i$, то ρ_0 допустимо. Так, например, если $\mathcal{K}$ — наследственная подкатегория категории (Ω), то эти дополнительные условия просто означают, что каждый допустимый морфизм $\rho\colon X \to A$ может быть срезан до отображения на подалгебру, порожденную образом носителя X при отображении ρ. Вообще если $\mathcal{K} \prec \mathcal{L} \prec \mathrm{St}$, где $\mathcal{K} \subseteq (\Omega)$, то под *естественным представлением* $\mathcal{L}$ в $\mathcal{K}$ мы понимаем представление, допустимыми морфизмами которого являются все такие $\mathcal{L}$-морфизмы

$$\rho\colon X \to A$$

$\mathcal{L}$-объекта X в $\mathcal{L}$-носитель $\mathcal{K}$-алгебры A, что подалгебра A_0, порожденная образом носителя $\mathcal{L}$-объекта X при отображении множеств, соответствующем морфизму ρ, будет $\mathcal{K}$-алгеброй и вложение i: $A_0 \to A$ будет $\mathscr{K}$-гомоморфизмом. Легко проверить, что на самом деле это будет представлением.

Если α: $X \to Y$ — некоторое отображение множеств, то будем писать также $\operatorname{im}\alpha$ вместо $X\alpha$. Заметим, что из определений вытекает

***Предложение* 4.1.** *Если категория $\mathscr{L}$, подчиненная категории* St, *представлена в абстрактной регулярной категории $\mathscr{K}$ Ω-алгебр и для этого представления существует универсальный функтор (U, u), то $\operatorname{im} u$ порождает $U(X)$.*

Доказательство. По определению универсальное отображение

$$u\colon X \to U(X)$$

будет допустимым морфизмом. Пусть U_0 — подалгебра алгебры $U(X)$, порожденная $\operatorname{im} u$; тогда $u = u_0 i$, где u_0: $X \to U_0$ — допустимый морфизм и i: $U_0 \to U$ — вложение. Следовательно, существует такой единственный $\mathscr{K}$-гомоморфизм α: $U \to U_0$, что $u_0 = u\alpha$. Отсюда вытекает, что

$$u = u_0 i = u\alpha i.$$

Здесь оба отображения 1: $U \to U$ и αi: $U \to U$ являются $\mathscr{K}$-гомоморфизмами; следовательно, в силу единственности $1 = \alpha i$ и этим показано, что i — эпиморфизм, т. е. $U_0 = U$. ∎

Рассмотрим теперь представление категории $\mathscr{L}$ в резидуальной категории $\mathscr{K}$ Ω-алгебр. Это представление называется *резидуальным*, если выполнено следующее условие: если A есть $\mathscr{K}$-алгебра, представленная в виде подпрямого произведения семейства $(A_\lambda)_{\lambda \in \Lambda}$ $\mathscr{K}$-алгебр с проекциями ε_λ: $A \to A_\lambda$, то для всякого отображения ρ носителя $\mathscr{L}$-объекта X в носитель алгебры A, для которого отображение $\rho\varepsilon_\lambda$ соответствует допустимому морфизму $X \to A_\lambda$, отображение ρ само соответствует допустимому морфизму $X \to A$. С помощью этих определений можно сформулировать основной результат о существовании универсального функтора:

***Теорема* 4.2.** *Пусть $\mathscr{K}$ — резидуальная категория Ω-алгебр, и пусть $\mathscr{L}$ — некоторая категория, подчиненная категории* St *и обладающая резидуальным представлением в $\mathscr{K}$. Тогда это представление обладает универсальным функтором.*

Доказательство. Пусть X есть $\mathscr{L}$-объект и $W_\Omega(X)$ есть алгебра Ω-слов над X, рассматриваемом как множество, с каноническим вложением

$$\rho\colon X \to W. \tag{1}$$

Через $(\mathfrak{q}_\lambda)_{\lambda \in \Lambda}$ обозначим семейство всех таких конгруэнций на W, что $W/\mathfrak{q}_\lambda \in \mathrm{Ob}\,\mathscr{K}$ и отображение

$$\rho(\mathrm{nat}\,\mathfrak{q}_\lambda)\colon\ X \to W/\mathfrak{q}_\lambda \tag{2}$$

допустимо. Полагая $\rho_\lambda = \rho(\mathrm{nat}\,\mathfrak{q}_\lambda)$ и $A_\lambda = W/\mathfrak{q}_\lambda$, получаем семейство допустимых отображений $\rho_\lambda\colon X \to A_\lambda$, которое естественным образом определяет отображение

$$\sigma\colon\ X \to \prod A_\lambda. \tag{3}$$

Пусть $\mathrm{im}\,\sigma$ порождает подалгебру $U(X)$ алгебры $A = \prod A_\lambda$; срезая отображение σ до $U(X)$, из (3) получаем такое отображение

$$u\colon\ X \to U(X),$$

что $ui = \sigma$, где $i\colon U(X) \to A$ — вложение. Мы утверждаем, что (U, u) — требуемый функтор. Во-первых, если проекцию $\prod A_\mu$ на A_λ обозначить через ε_λ, то для всякого $\lambda \in \Lambda$

$$\sigma\varepsilon_\lambda = \rho_\lambda.$$

Таким образом, $\sigma\varepsilon_\lambda$ допустимо для всех $\lambda \in \Lambda$, и, следовательно, σ также допустимо. Так как $\sigma = ui$, то отсюда вытекает, что $U(X)$ есть $\mathscr{K}$-алгебра, i есть $\mathscr{K}$-гомоморфизм и u допустимо. Заметим, кстати, что так как $\mathrm{im}\,\rho$ порождает W, то $\mathrm{im}\,\rho_\lambda$ порождает A_λ и $\mathrm{im}\,i\varepsilon_\lambda$ также порождает A_λ; но $i\varepsilon_\lambda$ — гомоморфизм, откуда $\mathrm{im}\,i\varepsilon_\lambda = A_\lambda$, т. е. $i\varepsilon_\lambda$ — эпиморфизм. Поэтому $U(X)$ является подпрямым произведением алгебр A_λ.

Пусть теперь B есть $\mathscr{K}$-алгебра и

$$\alpha\colon\ X \to B$$

— допустимое отображение. Срезая α до подалгебры, порожденной $\mathrm{im}\,\alpha$, можем предположить, что $\mathrm{im}\,\alpha$ порождает B. Отображение α можно продолжить до эпиморфизма

$$\beta\colon\ W \to B;$$

если $\ker\beta = \mathfrak{q}$, то $\beta = (\mathrm{nat}\,\mathfrak{q})\beta^*$, где

$$\beta^*\colon\ W/\mathfrak{q} \to B$$

является изоморфизмом. Теперь α допустимо, и по построению

$$\alpha = \rho\beta = \rho(\mathrm{nat}\,\mathfrak{q})\beta^*;$$

так как β^* — изоморфизм, то отсюда вытекает, что $\alpha\beta^{*-1} = \rho(\operatorname{nat}\mathfrak{q})$ допустимо. Следовательно, $\mathfrak{q} = \mathfrak{q}_\lambda$ для некоторого $\lambda \in \Lambda$, и мы получаем следующую диаграмму:

$$\begin{tikzcd}
X \arrow[rr, "u"] \arrow[dd, "\rho"'] \arrow[dr, "\alpha"] & & U(X) \arrow[dd, "i\varepsilon_\lambda"] \arrow[dl, "\alpha'"'] \\
& B & \\
W \arrow[rr, "\operatorname{nat}\mathfrak{q}"'] \arrow[ur, "\beta"] & & W/\mathfrak{q}_\lambda \arrow[ul, "\beta^*"']
\end{tikzcd}$$

где $\alpha' = i\varepsilon_\lambda\beta^*$, а квадрат и все треугольники, быть может за исключением самого верхнего, коммутативны. Пользуясь коммутативностью остальных треугольников и квадрата, находим

$$\alpha = \rho\beta = \rho(\operatorname{nat}\mathfrak{q})\beta^* = ui\varepsilon_\lambda\beta^* = u\alpha',$$

так что верхний треугольник будет также коммутативным и α' — нужное отображение. Ясно, что это отображение будет $\mathscr{K}$-гомоморфизмом (так как $i\varepsilon_\lambda$ и β^* суть $\mathscr{K}$-гомоморфизмы), причем единственным, поскольку если $\alpha = u\alpha_1 = u\alpha_2$, то α_1 и α_2 совпадают на $\operatorname{im} u$ и, следовательно (по лемме 2.2), на $U(X)$, т. е. $\alpha_1 = \alpha_2$. ∎

В частности, если $\mathscr{K} < \mathscr{S}$, то естественное представление $\mathscr{S}$ в $\mathscr{K}$ резидуально, и мы получаем

Следствие 4.3. *Если $\mathscr{K}$ — резидуальная подкатегория категории (Ω) и $\mathscr{K} < \mathscr{S} < \mathrm{St}$, то естественное представление $\mathscr{S}$ в $\mathscr{K}$ обладает универсальным функтором.* ∎

Следствие 4.4. *Если $\mathscr{K}$ — наследственная подкатегория категории (Ω), замкнутая относительно прямых произведений, и $\mathscr{K} < \mathscr{S} < \mathrm{St}$, то естественное представление $\mathscr{S}$ в $\mathscr{K}$ обладает универсальным функтором.* ∎

Пусть $\mathscr{S} < \mathrm{St}$ представлена в категории $\mathscr{K}$ Ω-алгебр и предположим, что для этого представления существует универсальный функтор U. Если для каждого $\mathscr{S}$-объекта X универсальное отображение

$$u\colon X \to U(X)$$

взаимно однозначно, то функтор U называется *инъективным*. Легко видеть, что универсальный функтор U инъективен в том и только том случае, если для каждого $\mathscr{S}$-объекта X существует взаимно однозначное отображение этого объекта в некоторую $\mathscr{K}$-алгебру. Действительно, если $\rho\colon X \to A$ — допустимое взаимно однозначное отображение, то существует такой гомоморфизм ρ': $U(X) \to A$, что $\rho = u\rho'$, и так как ρ взаимно однозначно, то отсюда вытекает, что u должно быть взаимно однозначным. Обратно, если u взаимно однозначно, то можно взять $A = U(X)$, чтобы получить взаимно однозначное представление $\mathscr{L}$-объекта X.

Универсальный функтор часто существует для других, неалгебраических представлений. Например, категория компактных хаусдорфовых пространств и непрерывных отображений подчинена категории всех хаусдорфовых пространств и непрерывных отображений (в действительности является ее подкатегорией). Соответствующее естественное представление обладает универсальным функтором, который сопоставляет каждому хаусдорфову пространству X компактное хаусдорфово пространство $U(X)$, называемое *компактным замыканием Стоуна — Чеха* пространства X (см. Самюэль [48] или Келли [55]). Этот функтор инъективен на подкатегории вполне регулярных хаусдорфовых пространств (пространство X *вполне регулярно*, если для каждой точки $p \in X$ и каждой окрестности N этой точки существует такая действительная непрерывная функция f на X, что $f(p) = 1$, $f(x) = 0$ для $x \notin N$).

УПРАЖНЕНИЯ

1. Показать, что если $\mathscr{K}$ и $\mathscr{L}$ — абстрактные регулярные категории Ω-алгебр, то всякая абстрактная регулярная категория, содержащая обе категории $\mathscr{K}$ и $\mathscr{L}$ в качестве подкатегорий, определяет представление $\mathscr{L}$ в $\mathscr{K}$.

2. Проверить, что если $\mathscr{K} \subseteq (\Omega)$, $\mathscr{K} < \mathscr{L} < \mathrm{St}$ и $\mathscr{K}$ регулярна и резидуальна, то естественное представление $\mathscr{L}$ в $\mathscr{K}$ резидуально.

5. СВОБОДНЫЕ АЛГЕБРЫ В КАТЕГОРИЯХ Ω-АЛГЕБР

Применим теперь результаты предыдущего параграфа к случаю $\mathscr{L} = \mathrm{St}$. Если существует универсальный функтор для естественного представления категории St в категории $\mathscr{K}$ Ω-алгебр, то для любого множества X алгебра $U(X)$ называется *универсальной $\mathscr{K}$-алгеброй над X*. Если этот универсальный функтор инъективен, то X можно отождествить с его образом в $U(X)$; в этом случае $U(X)$ называется *свободной $\mathscr{K}$-алгеброй над X*, в то время как X называется множеством *$\mathscr{K}$-свободных* образующих алгебры $U(X)$; говорят также, что *$\mathscr{K}$ — категория со свободными алгебрами*. В силу свойств функторов свободная $\mathscr{K}$-алгебра над X, если она существует, определена однозначно с точностью до изоморфизма над X. Так, например, по теореме 2.6 (Ω) является категорией со свободными алгебрами.

Ясно, что тривиальная категория не может обладать свободными алгебрами ни для какого множества, содержащего больше одного элемента; во всех остальных случаях существование свободных алгебр вытекает из существования универсального функтора:

***Предложение* 5.1.** *Если $\mathscr{K}$ — нетривиальная категория Ω-алгебр и для естественного представления* St *в $\mathscr{K}$ существует универсальный функтор, то найдется такая мощность α, что для каждого множества X мощности, не меньшей α, свободная $\mathscr{K}$-алгебра над X существует. Кроме того, каждая $\mathscr{K}$-алгебра является гомоморфным образом некоторой свободной $\mathscr{K}$-алгебры.*

Доказательство. По предположению в $\mathscr{K}$ существует алгебра A, содержащая больше одного элемента. Пусть X_0 — множество образующих алгебры A, содержащее больше одного элемента; тогда вложение $X_0 \to A$ допустимо (при естественном представлении); следовательно, универсальное отображение

$$u_0\colon X_0 \to U(X_0)$$

взаимно однозначно. Положим $\alpha = |X_0|$; тогда для любого множества X мощности, не меньшей α, существует отображение ρ множества X на множество X_0 и для любого такого ρ отображение $\rho u_0\colon X \to U(X_0)$ допустимо. Более того, если даны $x,\ y \in X,\ x \neq y$, то ρ можно выбрать таким, чтобы $x\rho \neq y\rho$; поэтому $x\rho u_0 \neq y\rho u_0$ и, таким образом, $xu \neq yu$, где $u\colon X \to U(X)$ — универсальное отображение. Так как это верно для любой пары элементов x, y множества X, то u взаимно однозначно.

В процессе доказательства алгебра A была представлена как гомоморфный образ свободной $\mathscr{K}$-алгебры $U(X_0)$; это применимо к любой $\mathscr{K}$-алгебре A, поэтому последнее утверждение доказано. ∎

В предположениях предложения 5.1 $\mathscr{K}$ не обязательно обладает свободными алгебрами для всех множеств X; например, категория, состоящая из всех несчетных групп и тривиальной группы (и всех гомоморфизмов между ними) обладает универсальным функтором: $U(X)$ — свободная группа над X, если X несчетно, и тривиальная группа в противном случае. Таким образом, для конечных непустых множеств X $U(X)$ не будет свободной группой над X. Однако, если $\mathscr{K}$ наследственна, то при доказательстве предложения 5.1 можно взять алгебру A, порожденную двухэлементным множеством X_0. Таким образом, получаем

***Следствие* 5.2.** *Если $\mathscr{K}$ — нетривиальная наследственная категория Ω-алгебр и для естественного представления* St *в $\mathscr{K}$ существует универсальный функтор, то $\mathscr{K}$ — категория со свободными алгебрами.* ∎

Чтобы найти условия, при которых универсальный функтор существует, воспользуемся следствием 4.3. Объединяя его с предложением 5.1, получаем такую теорему:

Теорема 5.3. *Пусть $\mathcal{K}$ — нетривиальная и резидуальная подкатегория категории* (Ω). *Тогда найдется такая мощность* α, *что для каждого множества* X *мощности, не меньшей* α, *свободная* $\mathcal{K}$*-алгебра над* X *существует и каждая* $\mathcal{K}$*-алгебра является гомоморфным образом свободной* $\mathcal{K}$*-алгебры.* ∎

В частности, условия этой теоремы выполняются для нетривиальной наследственной подкатегории $\mathcal{K}$ категории (Ω), замкнутой относительно прямых произведений.

Рассмотрим теперь категорию $\mathcal{K}$ Ω-алгебр со свободными алгебрами. В этом случае вместо $U(X)$ будем писать $F(X)$ или $F(X; \mathcal{K})$. Из единственности свободных алгебр вытекает ряд полезных следствий.

Предложение 5.4. *Пусть $\mathcal{K}$ — подкатегория категории* (Ω) *со свободными алгебрами,* X *— некоторое множество и* Y *— подмножество в* X. *Если* i: $Y \to X$ *— вложение, то индуцируемый им гомоморфизм* $F(i)$: $F(Y) \to F(X)$ *взаимно однозначен.*

Действительно, вложение i: $Y \to X$ обладает таким правым обратным τ: $X \to Y$, что $i\tau = 1_Y$; следовательно, $F(i)$ обладает правым обратным и поэтому взаимно однозначен. ∎

Это предложение позволяет отождествить $F(Y)$ с подалгеброй алгебры $F(X)$; ясно, что эта подалгебра будет собственной, если только Y — собственное подмножество множества X; следовательно, X — минимальное множество образующих алгебры $F(X)$.

Предложение 5.5. *Пусть $\mathcal{K}$ — подкатегория категории* (Ω) *со свободными алгебрами,* X *— некоторое множество и* $\mathfrak{q}$ *— эквивалентность на* X. *Отождествим* X *с подмножеством алгебры* $F(X)$ *(посредством универсального отображения), и пусть* $\bar{\mathfrak{q}}$ *— конгруэнция на* $F(X)$, *порожденная эквивалентностью* $\mathfrak{q}$. *Тогда*

$$\bar{\mathfrak{q}} \cap X^2 = \mathfrak{q} \tag{1}$$

и

$$F(X)/\bar{\mathfrak{q}} \cong F(X/\mathfrak{q}).$$

Доказательство. Положим $X' = X/\mathfrak{q}$ и для краткости запишем $F = F(X)$ и $F' = F(X')$. Естественное отображение θ: $X \to X'$ индуцирует гомоморфизм $F(\theta)$: $F \to F'$, ядро которого $\mathfrak{k}$ содержит $\mathfrak{q}$, а поэтому и $\bar{\mathfrak{q}}$. Мы утверждаем, что

$$\mathfrak{k} \cap X^2 = \mathfrak{q}. \tag{2}$$

Действительно, если $(x, y) \in \mathfrak{k} \cap X^2$, то $xF(\theta) = yF(\theta)$, и, следовательно, $(x, y) \in \mathfrak{q}$; таким образом, $\mathfrak{k} \cap X^2 \subseteq \mathfrak{q}$, а обратное включение очевидно. Так как $\mathfrak{k} \supseteq \bar{\mathfrak{q}}$, то $F(\theta)$: $F \to F'$ можно представить в виде произведения $\operatorname{nat} \bar{\mathfrak{q}}$ и некоторого гомоморфизма

$$\varphi: F/\bar{\mathfrak{q}} \to F'. \tag{3}$$

Ясно, что этот гомоморфизм индуцирует тождественное отображение на $X' = X/\mathfrak{q}$. Поэтому $\varphi | X'$ обладает обратным; это обратное отображение продолжается до гомоморфизма $F' \to F/\bar{\mathfrak{q}}$, так как алгебра F' свободна, и поэтому сам гомоморфизм φ обладает обратным, т. е. (3) — *изоморфизм*. Это означает, что $\mathfrak{f} = \bar{\mathfrak{q}}$, и теперь (1) вытекает из (2). ∎

В качестве иллюстрации (которая пригодится в дальнейшем) рассмотрим свободную $\mathscr{K}$-алгебру A над a, b, c. Если добавить соотношение $b = c$, то мы получим свободную $\mathscr{K}$-алгебру над a и b.

Так как два множества эквивалентны (в категории St) тогда и только тогда, когда они имеют одну и ту же мощность, то отсюда следует, что в категории $\mathscr{K}$ со свободными алгебрами существует единственная с точностью до изоморфизма свободная $\mathscr{K}$-алгебра F_α для каждой мощности α. Эта алгебра называется свободной $\mathscr{K}$-алгеброй *ранга* α. Теперь возникает вопрос, могут ли свободные $\mathscr{K}$-алгебры различных рангов быть изоморфными. Из замечания, сделанного после предложения 5.4, вытекает, что множество X является минимальным множеством образующих свободной $\mathscr{K}$-алгебры $F(X)$; поэтому в силу предложения II. 5.5 две свободные $\mathscr{K}$-алгебры различных рангов не изоморфны, если по крайней мере один из рангов бесконечен. Это не всегда справедливо, если оба ранга конечны, но имеет место следующее достаточное условие, принадлежащее Йонсону и Тарскому [61]:

Теорема 5.6. *Пусть $\mathscr{K}$ — подкатегория категории (Ω) со свободными алгебрами, и пусть $\mathscr{K}$ обладает по крайней мере одной конечной алгеброй, содержащей более одного элемента. Тогда свободные $\mathscr{K}$-алгебры различных рангов не изоморфны.*

Доказательство. В силу замечаний, предшествующих этой теореме, нужно рассмотреть только тот случай, когда оба ранга конечны. Докажем более сильное утверждение, что для конечного n каждое множество образующих алгебры F_n содержит по меньшей мере n элементов. Таким образом, n будет охарактеризовано классом алгебр, изоморфных алгебре F_n, как наименьшая мощность множества образующих алгебры F_n, откуда и вытекает теорема.

Пусть X — множество свободных образующих алгебры F_n, состоящее из n элементов, Y — некоторое другое множество образующих и B — конечная $\mathscr{K}$-алгебра, содержащая более одного элемента. По определению алгебры F_n каждое отображение $X \to B$ можно продолжить до единственного $\mathscr{K}$-гомоморфизма $F_n \to B$; поэтому множество H всех $\mathscr{K}$-гомоморфизмов $F_n \to B$ равномощно множеству B^X. Пусть $\theta \in H$; тогда ограничение $\theta | Y$ определяет отображение $Y \to B$, т. е. элемент множества B^Y, и различные гомоморфизмы определяют различные отображения (по лемме 2.2). Таким образом, имеем взаимно однозначное отображение $B^X \to B^Y$. Отсюда следует, что $|B^X| \leqslant |B^Y|$, и так как B и X оба конечны, то $n = |X| \leqslant |Y|$. ∎

Следующее предложение устанавливает еще одно свойство свободных алгебр, характеризующее в некоторых категориях свободные алгебры способом, не зависящим от выбора множества образующих.

Предложение 5.7. *Пусть $\mathcal{K}$ — категория Ω-алгебр со свободными алгебрами, и пусть F — свободная $\mathcal{K}$-алгебра над множеством X. Если A, B — произвольные $\mathcal{K}$-алгебры, β: $F \to B$ есть $\mathcal{K}$-гомоморфизм и α: $A \to B$ есть $\mathcal{K}$-эпиморфизм, то существует такой $\mathcal{K}$-гомоморфизм γ: $F \to A$, что $\gamma\alpha = \beta$ (конечно, γ может быть не единственным).*

Доказательство.

$$\begin{tikzcd} F \arrow[r, dotted, "\gamma"] \arrow[dr, "\beta"'] & A \arrow[d, "\alpha"] \\ & B \end{tikzcd}$$

Определим γ на X следующим образом: пусть $x \in X$, тогда $x\beta \in B$ и поэтому $x\beta = a\alpha$ для некоторого $a \in A$. Выберем таким способом по одному a для каждого $x \in X$ и положим $x\gamma = a$; тогда по определению

$$x\gamma\alpha = x\beta \qquad (x \in X).$$

Теперь γ можно продолжить до гомоморфизма γ: $F \to A$; тогда $\gamma\alpha$ и β будут гомоморфизмами, совпадающими на X и, следовательно, равными. ∎

$\mathcal{K}$-алгебра F, обладающая свойством, установленным в предложении 5.7, называется *$\mathcal{K}$-проективной*. Это предложение утверждает, следовательно, что всякая свободная $\mathcal{K}$-алгебра $\mathcal{K}$-проективна. Для категории групп и гомоморфизмов верно и обратное: всякая проективная группа свободна. Аналогичный результат имеет место для абелевых групп, но соответствующее утверждение для R-модулей неверно, если R — полупростое кольцо с условием минимальности, не являющееся телом (см., например, Маклейн [63]).

УПРАЖНЕНИЯ

1. Показать, что категория, состоящая из всех неабелевых групп и тривиальной группы (со всеми гомоморфизмами) обладает универсальным функтором, но не обладает свободными группами над множествами, состоящими из одного элемента.

2. Проверить, что для любой категории $\mathcal{K}$ со свободными алгебрами всякое множество X является минимальным множеством образующих свободной $\mathcal{K}$-алгебры над X.

3. Обобщить упр. 2.7 на категории со свободными алгебрами.

4. (Йонсон и Тарский.) Пусть $\mathcal{K}$ — категория со свободными алгебрами, и обозначим через F_n свободную $\mathcal{K}$-алгебру ранга n. Показать, что если каждое множество образующих алгебры F_n, состоящее из n элементов, является множеством свободных образующих (для всех конечных n), то каждое множество образующих алгебры F_n содержит по крайней мере n элементов; вывести отсюда, что утверждение теоремы 5.6 имеет место в этом случае.

5. (Йонсон и Тарский.) Пусть Ω состоит из бинарного и двух унарных операторов, результат применения которых записывается через $x \cdot y$, $x\lambda$, $x\rho$ соответственно. Обозначим через $\mathcal{K}$ категорию всех таких Ω-алгебр, что $x\lambda \cdot x\rho = x$, $(x \cdot y)\lambda = x$, $(x \cdot y)\rho = y$. Если дано, что $\mathcal{K}$ — категория со свободными алгебрами (из следствия IV. 3.3 ниже вытекает, что $\mathcal{K}$ действительно является категорией со свободными алгебрами), то показать, что все свободные $\mathcal{K}$-алгебры ненулевого конечного ранга изоморфны. (Показать, что если A свободна над $X \cup \{a, b\}$ и $X \cap \{a, b\} = \varnothing$, то A свободна также над X.) [1]

6. (Мальцев.) Пусть $\mathcal{K}$ — категория со свободными алгебрами и F_n — свободная $\mathcal{K}$-алгебра ранга n. Если никакая собственная факторалгебра алгебры F_n не изоморфна алгебре F_n, то всякое множество образующих алгебры F_n, состоящее из n элементов, свободно.

7. Показать, что всякий унитарный модуль над телом свободен и вывести отсюда, что структура подмодулей такого модуля будет структурой с дополнениями. (Воспользоваться предложением 5.7.)

8. (Пирс.) Показать, что если $\mathcal{K}$ — абстрактная наследственная категория со свободными алгебрами и $Q\mathcal{K}$ — категория гомоморфных образов (§ II. 8), то алгебра A $Q\mathcal{K}$-свободна в том и только том случае, если она $\mathcal{K}$-свободна.

6. СВОБОДНЫЕ И ПРЯМЫЕ ОБЪЕДИНЕНИЯ Ω-АЛГЕБР

Два универсальных функтора, а именно свободные и прямые объединения, введенные в § III. 1, существуют для многих категорий Ω-алгебр. Если $\mathcal{K}$ — регулярная категория Ω-алгебр, то $\mathcal{K}$ подчинена категории $\mathcal{F}(\mathcal{K})$ семейств $\mathcal{K}$-алгебр (над вполне неупорядоченными множествами), и поэтому можно применить следствие 4.3:

***Теорема* 6.1.** *Пусть $\mathcal{K}$ — произвольная регулярная резидуальная категория Ω-алгебр. Тогда свободное $\mathcal{K}$-объединение любого семейства $\mathcal{K}$-алгебр существует.* ∎

В категории $\mathcal{K}$ со свободными объединениями $\mathcal{K}$-алгебра A называется *свободным произведением* $\mathcal{K}$-алгебр A_λ ($\lambda \in \Lambda$), если A_λ являются подалгебрами алгебры A, причем

[1] В работе Сверчковского (*Fund. Math.*, **50** (1961), 35—44) полностью рассмотрен следующий вопрос: если в многообразии (см. § IV. 1) существуют изоморфные свободные алгебры различных конечных рангов, то для каких именно рангов это может иметь место. — *Прим. ред.*

(i) для свободного объединения $P=\coprod A_\lambda$ существует изоморфизм $\theta\colon A\to P$, ограничение которого на A_λ является каноническим отображением;

(ii) $A_\lambda \cap A_\mu$ — минимальная подалгебра алгебры A для $\lambda\neq\mu$.

Если дано семейство (A_λ) $\mathscr{K}$-алгебр, то может не существовать $\mathscr{K}$-алгебры A, которая была бы их свободным произведением (например, необходимо, чтобы минимальные подалгебры всех A_λ были изоморфны), но если такое свободное произведение существует, то по определению оно однозначно определяется (с точностью до изоморфизма) свободным объединением алгебр A_λ. Будем говорить, что $\mathscr{K}$-алгебра A *сжимаема*, если существует такой $\mathscr{K}$-гомоморфизм

$$\theta\colon A\to C$$

алгебры A на ее минимальную подалгебру C, что $\theta\,|\,C=1$. Тогда можно сформулировать следующее условие для существования свободных произведений:

Предложение 6.2. *Пусть задана категория $\mathscr{K}$ Ω-алгебр, и пусть (A_λ) — семейство $\mathscr{K}$-алгебр, для которого существует свободное объединение P. Если каждая алгебра A_λ сжимаема и для любых $\lambda, \mu\in\Lambda$ минимальные подалгебры алгебр A_λ и A_μ изоморфны, то P является свободным произведением алгебр A_λ.*

Доказательство. Очевидно, это утверждение имеет место, если Λ состоит из одного элемента, поэтому можно предполагать, что Λ содержит больше одного элемента.

Нужно показать, что канонические отображения

$$\rho_\lambda\colon A_\lambda\to P \tag{1}$$

взаимно однозначны, а затем доказать, что если отождествить алгебру A_λ с ее образом в P, то алгебры A_λ пересекаются в P по минимальной подалгебре. Пусть C_λ — минимальная подалгебра алгебры A_λ; по предположению существует сжатие

$$\varepsilon_\lambda\colon A_\lambda\to C_\lambda, \tag{2}$$

и так как все C_λ изоморфны, то можно взять изоморфизм

$$\theta_\lambda\colon C_\lambda\to C \tag{3}$$

с фиксированной алгеброй C. Рассмотрим теперь произвольную пару различных индексов из Λ, скажем $\lambda=1, 2$. Определим семейство отображений $A_\lambda\to A_1$ по формулам

$$\varphi_\lambda=\begin{cases} 1, & \lambda=1,\\ \varepsilon_\lambda\theta_\lambda\theta_1^{-1}, & \lambda\neq 1.\end{cases}$$

В силу универсального свойства существует такой гомоморфизм φ: $P \to A_1$, что $\varphi_\lambda = \rho_\lambda \varphi$. Взяв $\lambda = 1$, находим, что $\rho_1 \varphi = 1$, откуда ρ_1 взаимно однозначно; кроме того, если $c \in A_1\rho_1 \cap A_2\rho_2$, скажем $c = a\rho_1 = b\rho_2$, то $c\varphi = a\varphi_1 = a$ и $c\varphi = b\varphi_2 = b\varepsilon_2\theta_2\theta_1^{-1} \in C_1$, откуда $a \in C_1$, $c = a\rho_1 \in C_1\rho_1$. Таким образом, $A_1\rho_1 \cap A_2\rho_2$ содержится в $C_1\rho_1$ и, следовательно, *является минимальной подалгеброй алгебры* P. Так как 1, 2 были произвольными элементами из Λ, то этим показано, что P — свободное произведение. ∎

Если каждая минимальная $\mathcal{K}$-подалгебра тривиальна, то все минимальные подалгебры изоморфны и каждая $\mathcal{K}$-алгебра сжимаема; это остается справедливым и в более общем случае, если только известно, что каждая $\mathcal{K}$-алгебра обладает тривиальной подалгеброй. Нужно только ввести 0-арный оператор, который выбирает определенную тривиальную подалгебру в каждой $\mathcal{K}$-алгебре. Таким образом, в качестве следствия из предложения 6.2 получаем следующий результат, принадлежащий Сикорскому [53]:

***Следствие* 6.3.** *Если каждая $\mathcal{K}$-алгебра обладает тривиальной подалгеброй и в категории $\mathcal{K}$ существуют свободные объединения, то свободное произведение любого семейства $\mathcal{K}$-алгебр существует.* ∎

В гл. IV будет показано, что в категории Gp всех групп свободные объединения существуют (это нетрудно также проверить с помощью теоремы 6.1). Поэтому в силу следствия 6.3 в Gp существуют свободные произведения. Аналогичный результат справедлив для полугрупп и колец, но не для колец с единицей (см. Кон [59]).

В заключение отметим простое достаточное условие для существования прямых объединений.

***Теорема* 6.4.** *Пусть $\mathcal{K}$ — произвольная категория Ω-алгебр, замкнутая относительно прямых произведений. Тогда прямое $\mathcal{K}$-объединение произвольного семейства $\mathcal{K}$-алгебр существует и совпадает с прямым произведением.*

Чтобы доказать этот результат, достаточно показать, что прямое произведение $P = \prod A_\lambda$ с проекциями ε_λ в качестве канонических гомоморфизмов обладает универсальным свойством. Таким образом, если дано семейство гомоморфизмов φ_λ: $B \to A_\lambda$, то необходимо построить такой гомоморфизм φ: $B \to P$, что $\varphi_\lambda = \varphi\varepsilon_\lambda$, т. е. для любого $b \in B$

$$b\varphi\varepsilon_\lambda = b\varphi_\lambda. \tag{4}$$

Такое отображение φ получается объединением отображений φ_λ, т. е. нужно положить $b\varphi = (b\varphi_\lambda)$; это отображение однозначно определено в силу (4) и является $\mathcal{K}$-гомоморфизмом, так как φ_λ суть $\mathcal{K}$-гомоморфизмы. ∎

В упражнениях будут приведены примеры, показывающие, что это условие не является необходимым.

УПРАЖНЕНИЯ

1. Показать, что во всякой категории $\mathcal{K}$ со свободными алгебрами, которая замкнута относительно гомоморфных образов, свободное объединение произвольного семейства $\mathcal{K}$-алгебр существует.

2. Показать, что категория конечных абелевых групп и гомоморфизмов замкнута относительно гомоморфных образов, но не имеет свободных алгебр. Показать далее, что семейство $(C_n)_{n \geqslant 1}$, где C_n — циклическая группа порядка n, не имеет свободного объединения в этом классе. Во второй части использовать упр. 1.

3. Показать, что категория коммутативных колец без делителей нуля обладает свободными алгебрами, но не замкнута относительно гомоморфных образов. Привести пример, показывающий, что свободные объединения, вообще говоря, не существуют.

4. Показать, что категория всех конечных абелевых групп (и гомоморфизмов) не замкнута относительно свободных объединений.

5. (Рейд.) Пусть $\mathcal{K}$ — категория Ω-алгебр, замкнутая относительно свободных объединений, и пусть (A_λ) — семейство $\mathcal{K}$-алгебр, имеющих представление в A_1 $(1 \in \Lambda)$. Показать, что каноническое отображение $\rho_1\colon A_1 \to \coprod A_\lambda$ взаимно однозначно. Вывести отсюда следствие 6.3.

6. Показать, что категория абелевых периодических групп не замкнута относительно прямых произведений, но обладает прямыми объединениями. Доказать то же самое для произвольных периодических групп.

7. ПРОИЗВОДНЫЕ ОПЕРАТОРЫ

Пусть Ω — область операторов; мы видели, что на каждой Ω-алгебре A данный элемент $\omega \in \Omega$ определяет некоторую операцию. Кроме этих операций, заданных явно, существуют операции, которые получаются с помощью композиции операторов из Ω и образуют клон действия Ω на A. Эти операции могут быть также выражены на языке структуры клона на $W_\Omega(X)$, как указано в упр. 3.4, но мы не будем этого делать, поскольку нас не интересует сам процесс композиции. Чтобы получить операцию, определенную произвольным Ω-словом $w = w(x_1, \ldots, x_n)$ относительно $x_1, \ldots, x_n$, обозначим через a образ этого слова в A при гомоморфизме, продолжающем отображение $x_i \to a_i$, так что

$$a = w(a_1, \ldots, a_n).$$

Таким образом, можно считать, что слово w определяет n-арный оператор $\overline{w}$ по правилу:

$$a_1 \cdots a_n\overline{w} = w(a_1, \ldots, a_n).$$

Оператор $\overline{w}$ называется *производным* от Ω. В этом смысле каждое Ω-слово определяет производный оператор; для достаточно большого алфавита X эти операторы включают, в частности, операторы из самой области Ω; на самом деле это верно для любого бесконечного алфавита X. Действительно, если $\omega \in \Omega(n)$ и $x_1, \ldots, x_n$ — произвольные различные элементы алфавита X, то ω получается из $x_1x_2 \ldots x_n\omega$ или также из $x_n \ldots x_2x_1\omega$, но не из $x_1x_1 \ldots x_1\omega$, если только $n \neq 1$. Заметим, что из каждого n-арного производного оператора мы получим k-арную операцию на A, заменяя $n-k$ его аргументов на элементы алгебры A. Унарные производные операторы и унарные операции, полученные таким образом из производных операторов, снова называют *трансляциями* или, точнее, *производными трансляциями*, чтобы подчеркнуть тот факт, что их не всегда можно получить описанным способом из операций только области Ω; так, например, в группе G операцию $x \to x^2$ не всегда можно выразить через операции axb и $ax^{-1}b$.

Множество всех производных операторов области Ω обозначается через $\bar{\Omega}$. Ясно, что всякая Ω-алгебра A замкнута относительно $\bar{\Omega}$; вообще Ω-подалгебры и $\bar{\Omega}$-подалгебры алгебры A одни и те же. Пусть теперь Ω' — подмножество множества $\bar{\Omega}$; тогда Ω' называется *ограничением* Ω. Каждая Ω-алгебра A имеет структуру Ω'-алгебры, индуцированную ограничением, и всякая подалгебра Ω-алгебры A замкнута относительно Ω', но обратное, вообще говоря, неверно. Аналогично каждый Ω-гомоморфизм является также Ω'-гомоморфизмом, но обратное, вообще говоря, неверно. Действительно, категория (Ω) подчинена категории (Ω') посредством пренебрегающего функтора, который «забывает» ту часть $\bar{\Omega}$, которая не принадлежит Ω'.

В качестве примера возьмем категорию Gp групп и рассмотрим коммутатор как производный оператор:

$$[x, y] = x^{-1}y^{-1}xy. \tag{1}$$

Ограничиваясь этим оператором, можно считать, что Gp подчинена категории группоидов, скажем Γ. Тогда Γ-подалгеброй группы будет подмножество этой группы, замкнутое относительно коммутирования. Такое подмножество не всегда замкнуто относительно взятия обратного $x \to x^{-1}$ (например, в абелевых группах с элементами бесконечного порядка). Множество образов при отображении $(x, y) \to [x, y]$ всегда замкнуто относительно взятия обратного, и если оно не пусто, то замкнуто также относительно постоянного оператора e, но, может быть, не замкнуто относительно умножения и потому не всегда является подгруппой (Кармайкл [37], стр. 39).

Эта конструкция приводит к представлению группоидов в группах; так как Gp резидуальна и регулярна, то по теореме 4.2 для этого представления существует универсальный функтор. Другие примеры будут рассмотрены в гл. VII.

Если Ω — область операторов, содержащая только унарные и 0-арные операторы, то арность каждого производного оператора не больше единицы. Интуитивно это очевидно, а также может быть выведено из теоремы II. 5.6, в которой на языке структуры подалгебр дан критерий того, чтобы операторы были самое большее унарными. Аналогично на языке структуры подалгебр можно сформулировать условие, при котором область Ω содержит только 0-арные операторы или только унарные операторы (упражнение II. 5.5). Если же допускаются бинарные операторы, то этого уже сделать нельзя; наоборот, в большинстве случаев все операторы могут быть выражены через бинарные.

Теорема 7.1. *Пусть Ω — произвольная область операторов; тогда существует область операторов Ω^*, арность которых не больше двух, такая, что Ω может быть вложена в область производных операторов области Ω^* и каждая Ω-алгебра A может быть вложена в Ω^*-алгебру A^*. Более того, если A бесконечна, то можно взять A^* с тем же носителем, что и A, тогда как если A конечна, то можно взять A^* счетной.*

При доказательстве нам придется использовать тот факт, что бесконечное множество равномощно своему квадрату. Чтобы не прерывать изложения, будем пока предполагать это известным; так как позже нам нужно будет более общее утверждение, то за доказательством мы отсылаем читателя к лемме VI. 6.1.

Возьмем область Ω^*, содержащую по одному унарному оператору ω' для каждого оператора $\omega \in \Omega$ и, кроме того, бинарный оператор μ. Предположим сначала, что A бесконечно; тогда A имеет такую же мощность, что и A^2, и поэтому существует взаимно однозначное соответствие

$$\nu\colon A \to A^2.$$

Вообще определим результат применения отображения ν к упорядоченному набору из n элементов множества A по правилу:

$$(x_1, \ldots, x_n)\nu = (x_1, \ldots, x_n\nu).$$

Ясно, что этим определено взаимно однозначное соответствие между A^n и A^{n+1}. Отсюда следует, что ν^k будет взаимно однозначным соответствием между A и A^{1+k}. Теперь для всякого $\omega \in \Omega(n)$ определим действие соответствующего унарного оператора $\omega' \in \Omega^*$ по правилу:

$$x\omega' = x\nu^{n-1}\omega \qquad (n \geqslant 1); \tag{2}$$

если $n = 0$, то положим $x\omega' = \omega$. Через μ обозначим ν^{-1}; тогда μ — бинарный оператор на A, и в силу (2), когда $n \geqslant 2$,

$$x_1 \ldots x_n\omega = x_1 \ldots x_n\mu^{n-1}\omega'.$$

Следовательно, ω является производным Ω^*-оператором. Если A конечно, то можно вложить A в счетное множество A^* и определить операторы из Ω на $A^* \setminus A$ произвольно; теперь, чтобы на A^* определить Ω^*-алгебру, можно использовать первую часть доказательства. ∎

Конечно, конструкция, приведенная в этом доказательстве, не имеет практического значения, так как существенно зависит от выбора взаимно однозначного соответствия ν: $A \to A^2$. В гл. IV дан другой практически более удобный метод сведения операторов к бинарным.

Уже из простого подсчета ясно, что на конечном множестве не всякую операцию можно выразить через бинарные операции. Так, на множестве из k элементов существует k^{k^n} n-арных операций, а число тернарных операций равно k^{k^3}. Комбинируя две бинарные операции α, β, можно получить четыре тернарных операции, а именно $xy\alpha z\beta$, $xy\beta z\alpha$, $xyz\alpha\beta$ и $xyz\beta\alpha$; поэтому число этих операций не больше, чем k^{4k^2}, а это меньше, чем k^{k^3} для $k \geqslant 5$. Заметим, что для $k = 3$ число унарных операций равно 27, число бинарных — 19683, а число тернарных — почти 10^{13} [1]).

Пусть $\mathscr{K}$ — произвольная категория Ω-алгебр и Ω' — ограничение Ω. Если объекты категории $\mathscr{K}$ считать Ω'-алгебрами, то вместе с $\mathscr{K}$-гомоморфизмами, рассматриваемыми как Ω'-гомоморфизмы, они образуют подкатегорию $\mathscr{L}$ категории (Ω'). Категорию $\mathbf{S}\mathscr{L}$ будем обозначать через $\mathscr{K}'$ и называть *категорией, полученной из* $\mathscr{K}$ *ограничением* Ω *до* Ω'. Для простоты будем предполагать, что $\mathscr{K}$ наследственна; тогда, применяя следствие 4.4, получаем следующую теорему:

Теорема 7.2. *Пусть $\mathscr{K}$ — наследственная категория Ω-алгебр, замкнутая относительно прямых произведений, и пусть $\mathscr{K}'$ — категория, полученная из $\mathscr{K}$ ограничением Ω до Ω'. Тогда для естественного представления $\mathscr{K}'$ в $\mathscr{K}$ существует универсальный функтор.*

Для доказательства теоремы необходимо показать, что $\mathscr{K}$ подчинена $\mathscr{K}'$, а последнее вытекает непосредственно из определений. ∎

В главе IV будет дана явная конструкция этого универсального функтора для широкого класса категорий, а также критерий инъективности этого функтора.

Мы закончим этот параграф критерием перестановочности конгруэнций, сформулированным на языке производных операторов (см. Мальцев [54]) [2]).

---

[1]) См. также работу Харрисона (*Proc. Amer. Math. Soc.*, **17** (1966), 731—737). — *Прим. ред.*

[2]) См. в этой связи также работу Ламбека (*Canad. J. Math.*, **10** (1958), 45—56). — *Прим. ред.*

Теорема 7.3. *Пусть $\mathscr{K}$ — категория Ω-алгебр со свободными алгебрами. Тогда конгруэнции на каждой $\mathscr{K}$-алгебре перестановочны в том и только том случае, если существует такой производный тернарный оператор* ω, *что*

$$xxz\omega = z, \qquad xzz\omega = x. \tag{3}$$

Доказательство. Если существует оператор ω, удовлетворяющий (3), то трансляция $axb\omega$ переводит элементы a и b друг в друга; следовательно, по предложению II. 6.8 конгруэнции на любой $\mathscr{K}$-алгебре A перестановочны. Для доказательства обратного утверждения возьмем свободную $\mathscr{K}$-алгебру F над a, b, c и через $\mathfrak{q}$ обозначим конгруэнцию, порожденную парой (a, b), а через $\mathfrak{r}$ — конгруэнцию, порожденную парой (b, c). Тогда $(a, c) \in \mathfrak{q} \circ \mathfrak{r}$, а по предположению $\mathfrak{q} \circ \mathfrak{r} = \mathfrak{r} \circ \mathfrak{q}$; отсюда $(a, c) \in \mathfrak{r} \circ \mathfrak{q}$, т. е. существует такой $d \in F$, что $(a, d) \in \mathfrak{r}$ и $(d, c) \in \mathfrak{q}$. Так как $d \in F$, то d можно представить в виде Ω-слова относительно a, b, c, скажем

$$d = abc\omega,$$

где ω — тернарный производный оператор. Теперь, в силу предложения 5.5, $F/\mathfrak{q}$ — свободная $\mathscr{K}$-алгебра над a, c и $F/\mathfrak{r}$ — свободная $\mathscr{K}$-алгебра над a, c. Но $d = c$ в $F/\mathfrak{q}$, откуда

$$aac\omega = c, \tag{4}$$

тогда как $d = a$ в $F/\mathfrak{r}$ и поэтому

$$acc\omega = a. \tag{5}$$

Оба равенства (4) и (5) являются равенствами, связывающими элементы свободной $\mathscr{K}$-алгебры над a, c, и поэтому они выполняются тождественно в каждой $\mathscr{K}$-алгебре. ∎

УПРАЖНЕНИЯ

1. Пусть Ω состоит из тернарного оператора ω, а Ω' — из σ, τ, где $xy\sigma = xxy\omega$, $xy\tau = xyy\omega$. Показать, что если W, W' — соответственно алгебры Ω-слов и Ω'-слов над множеством X, то канонический гомоморфизм $W' \to W$ (полученный продолжением тождественного отображения $1: X \to X$) не будет взаимно однозначным.

2. Показать, что на структурах не существует производного тернарного оператора, удовлетворяющего условиям теоремы 7.3. (Взять линейно упорядоченное множество.)

3. Показать, что на структуре с относительными дополнениями все конгруэнции перестановочны. (В качестве $xyz\omega$ взять дополнение элемента y в $[x \wedge z, x \vee z]$ и применить теорему 7.3.)

4. Показать, что на свободном группоиде по меньшей мере с тремя свободными образующими не все конгруэнции перестановочны.

5. (Мальцев.) Квазигруппу можно определить как алгебру с тремя бинарными операторами, удовлетворяющими некоторым тождествам. Этими операторами являются произведение $ab\mu$ и решения уравнений $xb\mu = c$, $ay\mu = c$, обозначаемые $cb\rho$, $ca\lambda$ соответственно (см. § IV.2). Показать, что на непустой квазигруппе, как алгебре относительно μ, λ и ρ, все конгруэнции перестановочны. (Взять $xyz\omega = xay\lambda\mu az\lambda\rho$, где a — некоторый фиксированный элемент.)

6. Пусть Ω — некоторая область операторов, и предположим, что каждому $\omega \in \Omega(n)$ сопоставлен производный n-арный оператор w_ω. Показать, что если A — произвольная Ω-алгебра и $W = W_\Omega(X)$, то всякое отображение θ: $X \to A$ можно продолжить единственным образом до такого отображения $\overline{\theta}$: $W \to A$, что для любых $\omega \in \Omega(n)$ и $a \in W^n$

$$(a\omega)\overline{\theta} = (a\overline{\theta})\, w_\omega.$$

Будет ли это выполняться, если заменить W на свободную алгебру над X в некоторой категории $\mathcal{K}$ со свободными алгебрами, а A заменить на произвольную $\mathcal{K}$-алгебру? (Рассмотреть категорию алгебр с унарным оператором $x \to x'$, удовлетворяющих тождеству $x'' = x$.)

8. ПРЕДСТАВЛЕНИЯ Ω-АЛГЕБР

На практике алгебры часто возникают естественным образом как множества гомоморфизмов некоторого данного вида. Например, группы возникают как множества автоморфизмов, полугруппы — как множества эндоморфизмов, кольца — как множества эндоморфизмов абелевых групп. Но может также случиться, что Ω-алгебра определена абстрактно своим носителем вместе с определенными на нем операциями — в виде «таблиц умножения», дающих результат применения каждого n-арного оператора к каждому набору из n элементов. Это описание часто можно представить и в более экономном виде. Предположим для определенности, что мы имеем дело с алгеброй A в данной категории $\mathcal{K}$ Ω-алгебр. Вместо описания всего носителя достаточно задать множество образующих X алгебры A и вместо полной таблицы умножения нужно только задать достаточное число соотношений, по которым остальные полностью определяются. Каждое вхождение операции $\omega \in \Omega(n)$ в таблицу умножения имеет вид

$$a_1 \cdots a_n\omega = b \quad (a_1, \ldots, a_n,\ b \in A).$$

Если выразить $a_1, \ldots, a_n$, b через элементы множества образующих X, то получим соотношение

$$f(x) = g(x),$$

где f, g — некоторые Ω-слова относительно $x_1, \ldots, x_r \in X$. Всякое множество соотношений, которое достаточно для определения действия всех операторов в A, называется *множеством определяющих соотношений* для A относительно множества образующих X.

Если Φ — такое множество определяющих соотношений, то определение алгебры A в терминах X и Φ называется *заданием* алгебры A и обозначается так:

$$A = \mathscr{K}\{X \mid \Phi\}. \tag{1}$$

Для данной алгебры A существует, конечно, много заданий, поскольку обычно можно многими способами выбрать множество образующих X и в зависимости от этого выбора и от $\mathscr{K}$ можно многими способами выбрать множество определяющих соотношений. На практике стараются взять категорию $\mathscr{K}$ как можно меньшей, чтобы упростить определяющие соотношения. Так, например, задание данной группы, которая случайно оказалась абелевой, можно обычно упростить, если ограничиться категорией абелевых групп, поскольку тогда можно отбросить все соотношения, выражающие коммутативность.

Будет удобно расширить введенное выше понятие задания следующим образом: вместо того, чтобы в качестве X брать множество образующих алгебры A, разрешим множеству X быть некоторым множеством символов, каждый из которых отождествлен с некоторым элементом алгебры A таким образом, что полученные элементы алгебры A образуют множество образующих. Этим достигается некоторое обобщение, поскольку различные элементы множества X могут представлять один и тот же элемент алгебры A. В то же время это больше соответствует практической цели, которой служат задания, так как если категория $\mathscr{K}$ должным образом ограничена, то любое множество X с любым множеством определяющих соотношений будет определять $\mathscr{K}$-алгебру (см. теорему 8.2 ниже), но решение вопроса, представляют ли два данных элемента множества X один и тот же элемент алгебры A, обычно является нетривиальной задачей (на самом деле это частный случай проблемы тождества, см. § III.9).

Итак, заданием $\mathscr{K}$-алгебры A является некоторое множество X вместе с некоторым множеством Φ соотношений между Ω-словами над X. Заметим, что если категория $\mathscr{K}$ Ω-алгебр произвольна, то задание $\mathscr{K}\{X \mid \Phi\}$ может вовсе не определять никакой алгебры в $\mathscr{K}$. Например, пусть $\mathscr{K}$ — категория бесконечных групп и $\{X \mid \Phi\}$ — задание конечной группы, скажем $\mathscr{K}\{x \mid x^2 = 1\}$; ясно, что не существует бесконечной группы с таким заданием. Чтобы получить удобное для приложений достаточное условие, нам нужна лемма, которая будет использована и в дальнейшем.

***Лемма* 8.1.** *Пусть A и B — некоторые Ω-алгебры, и пусть дано множество X и такие отображения α: $X \to A$, β: $X \to B$, что* (i) $\operatorname{im}\alpha$ *порождает* A; (ii) *всякое соотношение в A между элементами $x\alpha$ $(x \in X)$ выполняется также между соответствующими элементами $x\beta$ в B. Тогда существует такой единственный гомоморфизм φ: $A \to B$, что $\alpha\varphi = \beta$.*

Доказательство. Пусть $W = W_\Omega(X)$—алгебра Ω-слов над X; тогда отображения α, β можно продолжить до гомоморфизмов $\bar{\alpha}$: $W \to A$, $\bar{\beta}$: $W \to B$ соответственно. Так как $\operatorname{im}\bar{\alpha}$ является подалгеброй в A, содержащей $\operatorname{im}\alpha$, то в силу (i) отсюда следует, что $\operatorname{im}\bar{\alpha} = A$, т. е. $\bar{\alpha}$ — эпиморфизм. Пусть $\mathfrak{q} = \ker\bar{\alpha}$; тогда существует такой изоморфизм

$$\alpha^*\colon\ W/\mathfrak{q} \to A,$$

что $(\operatorname{nat}\mathfrak{q})\alpha^* = \bar{\alpha}$. Теперь в силу (ii) $\mathfrak{q} \subseteq \ker\bar{\beta}$; следовательно, существует такой гомоморфизм β^*: $W/\mathfrak{q} \to B$, что $(\operatorname{nat}\mathfrak{q})\beta^* = \bar{\beta}$. Если мы положим $\varphi = (\alpha^*)^{-1}\beta^*$, то

$$\alpha\varphi = i\bar{\alpha}\varphi = i(\operatorname{nat}\mathfrak{q})\alpha^*\varphi = i(\operatorname{nat}\mathfrak{q})\beta^* = i\bar{\beta} = \beta,$$

где i: $X \to W$ — вложение. Итак, φ — искомое отображение, и оно будет единственным, поскольку любые два гомоморфизма, удовлетворяющие условиям леммы, должны совпадать на $\operatorname{im}\alpha$ и, следовательно, на A. ∎

***Теорема* 8.2.** *Пусть $\mathscr{K}$ — резидуальная категория Ω-алгебр. Тогда каждое задание*

$$\mathscr{K}\{X \mid \Phi\} \tag{2}$$

определяет $\mathscr{K}$-алгебру, единственную с точностью до изоморфизма.

Доказательство. Пусть $W = W_\Omega(X)$, и пусть $(\varphi_\lambda)_{\lambda\in\Lambda}$ — семейство всех таких эпиморфизмов алгебры W на некоторую $\mathscr{K}$-алгебру A_λ, что

$$f(x\varphi_\lambda) = g(x\varphi_\lambda) \text{ для всех соотношений } (f,\ g) \text{ из } \Phi.$$

Если положить $\mathfrak{q}_\lambda = \ker\varphi_\lambda$, то $W/\mathfrak{q}_\lambda \cong A_\lambda$, и потому если $\mathfrak{q} = \bigcap \mathfrak{q}_\lambda$, то $W/\mathfrak{q}$ является подпрямым произведением алгебр A_λ и, значит, $\mathscr{K}$-алгеброй. Мы утверждаем, что

$$W/\mathfrak{q} \cong \mathscr{K}\{X \mid \Phi\}. \tag{3}$$

Во-первых, если $\varphi = \operatorname{nat}\mathfrak{q}$, то $X\varphi$ порождает $W/\mathfrak{q}$ и, очевидно, все соотношения Φ выполняются в $W/\mathfrak{q}$; итак, мы получим (3), если сможем показать, что Φ — множество определяющих соотношений для $W/\mathfrak{q}$ как $\mathscr{K}$-алгебры. Для этого достаточно показать, что каждая $\mathscr{K}$-алгебра, порожденная множеством X с соотношениями Φ, будет гомоморфным образом алгебры $W/\mathfrak{q}$. Пусть B есть $\mathscr{K}$-алгебра, порожденная множеством X, в которой выполняются соотношения Φ; тогда по лемме существует гомоморфизм θ: $W/\mathfrak{q} \to B$, который индуцирует тождественное отображение на X, что и требовалось показать. Отсюда также ясно, что алгебра, определяемая заданием (2), единственна с точностью до изоморфизма. ∎

Позже нам встретятся важные классы категорий, в которых условие теоремы 8.2 всегда имеет место. Мы уже видели, что категория бесконечных групп не удовлетворяет этому условию; она не резидуальна, так как не содержит тривиальной группы. В качестве другого следствия леммы получаем теорему, впервые доказанную Диком [1882] в случае групп.

***Теорема* 8.3.** *Пусть $\mathscr{K}$ — произвольная категория Ω-алгебр и A есть $\mathscr{K}$-алгебра, заданная в виде*

$$A = \mathscr{K}\{X \mid \Phi\}. \tag{1}$$

Если B есть $\mathscr{K}$-алгебра с множеством образующих X, причем все соотношения Φ выполняются в B, то B является гомоморфным образом алгебры A. ∎

Эта теорема выражает следующий результат (который для резидуальных категорий вытекает также из теоремы 8.2): алгебра A с заданием (1) универсальна для таких представлений множества X в $\mathscr{K}$-алгебрах с помощью отображений, что соотношения Φ выполняются для образов элементов множества X.

Задание (1) алгебры A называется *конечным*, если оба множества X и Φ конечны. Для алгебры A, конечнозаданной в этом смысле, существует простой метод, принадлежащий (для групп) Тице (см. Шода [49]), при помощи которого можно получить все конечные задания этой алгебры из данного.

***Теорема* 8.4.** *Пусть $\mathscr{K}$ — резидуальная категория Ω-алгебр, и пусть A есть $\mathscr{K}$-алгебра с конечным заданием*

$$A = \mathscr{K}\{X \mid \Phi\}. \tag{1}$$

Тогда всякое другое конечное задание алгебры A получается из (1) *посредством следующих операций или обратных к ним:*

(i) *Замена Φ на $\Phi \cup \{(u, v)\}$, где (u, v) — следствие соотношений Φ.*

(ii) *Замена X на $X \cup \{y\}$ и Φ — на $\Phi \cup \{(y, u)\}$, где u — произвольное слово над X, а y — буква, не встречающаяся в X.*

Доказательство. Ясно, что (i) и (ii), примененные к любому конечному заданию алгебры A, дают другое конечное задание. Пусть теперь A конечно задана в виде (1), и пусть

$$A = \mathscr{K}\{Y \mid \Psi\} \tag{4}$$

— другое ее конечное задание. Так как (4) определяет A только с точностью до изоморфизма, то можно предположить, что $X \cap Y = \varnothing$. Теперь в силу (1) каждое $y \in Y$ можно выразить через элементы множества X, скажем $y = f_y(x)$, и, таким образом, из задания (1) с помощью операций вида (ii) мы получаем задание

$$A = \mathscr{K}\{X \cup Y \mid \Phi \cup \Phi'\}, \quad \Phi' = \{(y, f_y(x)) \mid y \in Y\}. \tag{5}$$

Но каждый элемент множества Ψ является следствием соотношений $\Phi \cup \Phi'$, поэтому, применяя (i), получаем

$$A = \mathscr{K}\{X \cup Y \mid \Phi \cup \Phi' \cup \Psi\}. \tag{6}$$

Наконец, каждое $x \in X$ имеет вид $x = g_x(y)$, и если

$$\Psi' = \{(x, g_x(y)) \mid x \in X\},$$

то, применяя еще раз (ii), имеем

$$A = \mathscr{K}\{X \cup Y \mid \Phi \cup \Phi' \cup \Psi \cup \Psi'\}. \tag{7}$$

Ясно, что (7) симметрично относительно заданий (1) и (4); поэтому, проводя те же рассуждения в обратном порядке, поменяв ролями (1) и (4), получаем (4). ∎

Этот результат применяется главным образом в следующей ситуации: алгебра A конечно задана в виде (1), и Y — другое множество образующих. Тогда $y = f_y(x)$ для каждого $y \in Y$, и, как и в приведенном доказательстве, получаем задание (5). Его можно теперь упростить, исключая с помощью операций, обратных к (i) и (ii), как можно больше элементов старого множества образующих X. При применении теоремы 8.4 важно помнить, что нам даны задания (1) и (4) одной и той же алгебры. Если же нам просто даны два конечных задания, то в общем случае не существует метода, с помощью которого можно решить, когда соответствующие алгебры изоморфны (из существования такого метода в общем случае вытекало бы положительное решение проблемы тождества, см. § III.9).

УПРАЖНЕНИЯ

1. Пусть G — группа с заданием $G = \mathrm{Gp}\{x, y \mid x^3 = y^2 = 1\}$; показать, что если $z = xy^{-1}$, то относительно y и z G имеет задание $G = \mathrm{Gp}\{y, z \mid y^2 = (yz)^3 = 1\}$.

2. Доказать теоремы 8.2 и 8.3 при помощи теоремы 4.2. (См. замечание, следующее за теоремой 8.3.)

9. ПРОБЛЕМА ТОЖДЕСТВА

Пусть $\mathscr{K}$ — резидуальная категория Ω-алгебр и A есть $\mathscr{K}$-алгебра, заданная в виде

$$A = \mathscr{K}\{X \mid \Phi\}. \tag{1}$$

Элементы алгебры A представлены Ω-словами над X, причем два слова f, g представляют один и тот же элемент алгебры A тогда и только тогда, когда одно может быть получено из другого применением соотношений Φ и правил в $\mathscr{K}$. Здесь роль категории $\mathscr{K}$ просто состоит в том, что существуют некоторые тождественные соотношения или законы (см. § IV.1), которые должны выполняться в $\mathscr{K}$. Итак, для того чтобы определение алгебры A посредством задания (1) имело какое-нибудь практическое значение, нам нужен алгоритм, т. е. правило для установления в конечное число шагов, когда два Ω-слова над X представляют один и тот же элемент алгебры A. Проблема нахождения такого алгоритма называется *проблемой тождества* для A (в задании (1)). Для некоторых классов алгебр проблема тождества была полностью решена; так, например, из основной теоремы для конечнопорожденных абелевых групп вытекает, что всякая конечнопорожденная абелева группа обладает заданием, для которого проблема тождества разрешима непосредственно. Проблема тождества была решена также для некоторых классов неабелевых групп, но показано, что для групп в общем случае она не разрешима. Точнее, существуют группы с таким заданием, для которого проблема тождества не разрешима (Новиков [55], Бун [57], Бриттон [58]). Даже если проблема тождества в группе G не разрешима в описанном выше смысле, может существовать алгоритм для перечисления всех пар слов, представляющих равные элементы в G (хотя для данной пары не существует способа для определения в конечное число шагов, равны они или нет). Тогда говорят, что в такой группе проблема тождества *рекурсивно разрешима*. Такой группой является, например, всякая конечнозаданная группа или вообще всякая конечнопорожденная подгруппа конечнозаданной группы. Хигмэн [61] доказал, что и обратно каждая конечнопорожденная группа с рекурсивно разрешимой проблемой тождества может быть вложена в конечнозаданную группу. Так как не каждую конечнопорожденную группу можно так вложить, то этим доказано существование групп, в которых проблема тождества рекурсивно не разрешима.

Чтобы доказывать неразрешимость, нужно, конечно, определить понятие алгоритма гораздо точнее. С другой стороны, чтобы доказать разрешимость проблемы тождества (а это мы только и будем делать), достаточно приведенных выше грубых формулировок. Мы обсудим один общий метод решения проблемы тождества, который часто применяется на практике. Для простоты в качестве $\mathscr{K}$ возьмем категорию (Ω) всех Ω-алгебр и гомоморфизмов и предположим, что Ω-алгебра A имеет задание

$$A = \Omega\{X \mid \Phi\}, \tag{2}$$

где Φ состоит из соотношений

$$u_\lambda(x) = v_\lambda(x) \quad (\lambda \in \Lambda). \tag{3}$$

Итак, A состоит из классов эквивалентных Ω-слов над X, где два Ω-слова f, g эквивалентны тогда и только тогда, когда существуют такие слова $w_0, w_1, \ldots, w_n$, что $w_0 = f$, $w_n = g$ и в каждой паре соседних слов w_{k-1}, w_k одно получено из другого заменой входящего в него подслова $u_\lambda(x)$ на $v_\lambda(x)$ (или наоборот). Эти классы эквивалентных Ω-слов являются в точности $\mathfrak{q}$-классами алгебры Ω-слов $W = W_\Omega(X)$, где $\mathfrak{q}$ — конгруэнция на W, порожденная парами (u_λ, v_λ), и $W/\mathfrak{q} \cong A$. Пусть

$$\theta\colon W \to A \tag{4}$$

— эпиморфизм с ядром $\mathfrak{q}$; напомним, что трансверсалом алгебры A в W называется подмножество T алгебры W, пересекающееся с каждым $\mathfrak{q}$-классом в точности по одному элементу. T можно также охарактеризовать тем свойством, что ограничение $\theta' = \theta \mid T$ должно быть взаимно однозначным соответствием. В общем случае θ' не будет гомоморфизмом, так как T не обязательно будет подалгеброй алгебры W. Однако можно использовать θ для определения T как Ω-алгебры, изоморфной A. Пусть $\tau\colon W \to W$ — отображение, которое ставит в соответствие каждому $w \in W$ единственный представитель класса $w^{\mathfrak{q}}$, принадлежащий T; это отображение τ называется *сжатием*[1]), соответствующим T. Тогда каждое $\omega \in \Omega(n)$ определяет n-арную операцию ω_T на T по правилу:

$$a_1 \cdots a_n \omega_T = (a_1 \cdots a_n \omega)\tau.$$

Это определяет A (с точностью до изоморфизма), как только нам известен трансверсал T и соответствующее сжатие τ. Таким образом, проблема тождества для A сводится к определению трансверсала для A в W.

Если алгебра A определена заданием (2), то имеем гомоморфизм (4), например взяв $A = W/\mathfrak{q}$ и $\theta = \operatorname{nat} \mathfrak{q}$. Теперь, если S — произвольное подмножество алгебры W, то обычно легко определить, будет ли ограничение $\theta \mid S$ отображением на всю алгебру A. Если оно в то же время взаимно однозначно, то отсюда будет следовать, что S — трансверсал, но часто взаимную однозначность трудно проверить непосредственно. Вместо этого можно поступить следующим образом. Пусть S — такое подмножество алгебры W, что $S^{\mathfrak{q}} = W$ (т. е. $\theta \mid S$ — отображение на), и для каждого $w \in W$ выберем элемент $w\sigma \in S \cap w^{\mathfrak{q}}$ так, чтобы $w\sigma = w$, если только $w \in S$. Полученное отображение $\sigma\colon W \to S$ определяется множеством S неоднозначно (если только S не трансверсал); назовем его *идемпотентным отображением, согласованным с* $\mathfrak{q}$. Определим теперь структуру Ω-алгебры на S по правилу:

$$a_1 \cdots a_n \omega_S = (a_1 \cdots a_n \omega)\sigma \quad (\omega \in \Omega(n),\ a_i \in S). \tag{5}$$

---

[1]) В частном случае, когда τ — гомоморфизм, это определение согласуется с определением, данным в § III. 6.

Предположим, что в S выполняются соотношения (3), т. е.

$$u_\lambda(x\sigma) = v_\lambda(x\sigma). \tag{6}$$

Тогда мы утверждаем, что S — трансверсал для A. Действительно, так как определяющие соотношения для A выполняются в алгебре S, то отсюда вытекает, что S — гомоморфный образ алгебры A при отображении, которое переводит $x\theta$ в $x\sigma$ $(x \in X)$. Следовательно, для любых $s, t \in S$, если $s \equiv t \pmod{\mathfrak{q}}$, то $s = s\sigma = t\sigma = t$. Поэтому каждый класс $s^{\mathfrak{q}}$ пересекает S по единственному элементу, и потому S — трансверсал.

Те же самые рассуждения применимы для любой резидуальной категории $\mathscr{K}$ со свободными алгебрами, если вместо W взять F, свободную $\mathscr{K}$-алгебру над X, хотя это имеет практический интерес только если проблема тождества может быть решена для F[1]. Итак, доказана

***Теорема* 9.1.** *Пусть $\mathscr{K}$ — резидуальная категория со свободными алгебрами и A есть $\mathscr{K}$-алгебра, заданная в виде*

$$A = \mathscr{K}\{X \mid \Phi\}, \tag{1}$$

где Φ состоит из соотношений

$$u_\lambda(x) = v_\lambda(x) \quad (\lambda \in \Lambda).$$

Пусть, далее, F — свободная $\mathscr{K}$-алгебра над X и $\mathfrak{q}$ — конгруэнция, порожденная всеми парами (u_λ, v_λ) $(\lambda \in \Lambda)$. Тогда

$$A \cong F/\mathfrak{q}.$$

Если, кроме того, S — такое подмножество алгебры F, что $S^{\mathfrak{q}} = F$ и σ — идемпотентное отображение F в S, согласованное с $\mathfrak{q}$, то S можно считать Ω-алгеброй, определив

$$a_1 \ldots a_n\omega_S = (a_1 \ldots a_n\omega)\sigma \quad (\omega \in \Omega(n),\ a_i \in S).$$

Если полученная Ω-алгебра будет $\mathscr{K}$-алгеброй, в которой выполняются соотношения

$$u_\lambda(x\sigma) = v_\lambda(x\sigma),$$

то S является трансверсалом для A и алгебра S изоморфна A. ∎

В качестве примера использования этого метода рассмотрим определение симметрической группы третьей степени образующими и определяющими соотношениями. Имеем задание

$$G = \mathrm{Gp}\{x, y \mid x^2 = y^3 = 1,\ x^{-1}yx = y^2\}. \tag{7}$$

[1]) Проблема тождества может быть решена для свободных алгебр во многих категориях $\mathscr{K}$; для самой категории (Ω) проблема тождества для свободной алгебры имеет, конечно, тривиальное решение, так как два слова равны тогда и только тогда, когда они графически совпадают.

Применяя данные соотношения, каждое групповое слово относительно x и y можно привести к виду

$$x^r y^s \quad (r=0,\ 1;\ s=0,\ 1,\ 2). \tag{8}$$

Таким образом, существует не больше шести $\mathfrak{q}$-классов, т. е. порядок группы G не больше шести. Чтобы доказать, что он равен шести, нужно показать, что шесть элементов (8) представляют различные элементы группы G. Это можно сделать, взяв конкретную реализацию группы G, т. е. группу с двумя образующими x и y и определяющими соотношениями группы G. Так как симметрическая группа третьей степени является такой группой, то этим доказано, что G имеет шесть элементов. Но этот результат можно также установить, применяя теорему 9.1 и не обращаясь к реализации группы G. Итак, возьмем шесть элементов (8) в F, составим их произведения в F и приведем их к виду одного из элементов (8). Это дает следующую таблицу умножения:

	1	x	y	xy	y^2	xy^2
1	1	x	y	xy	y^2	xy^2
x	x	1	xy	y	xy^2	y^2
y	y	xy^2	y^2	x	1	xy
xy	xy	y^2	xy^2	1	x	y
y^2	y^2	xy	1	xy^2	y	x
xy^2	xy^2	y	x	y^2	xy	1

Пользуясь случаем, заметим, что отображение σ не обязательно определять на всей группе F, достаточно сделать это только для произведений образующих. Для завершения конструкции нужно теперь только показать, что приведенная таблица определяет группу, в которой выполняются данные соотношения между x и y. Из рассмотрения таблицы непосредственно следует, что эти соотношения выполняются, а что касается тождеств, определяющих группы, то не сразу очевиден только закон ассоциативности, но процесс его проверки чисто механический, хотя и длинный. Заметим, что если только показано, что число возможных $\mathfrak{q}$-классов должно быть конечным, как в этом примере, то оставшаяся часть задачи всегда может быть доведена до конца в конечное число шагов. Поэтому получаем следующий результат, вытекающий из теоремы 9.1:

***Следствие* 9.2.** *Если F и $\mathfrak{q}$ такие же, как в теореме* 9.1, *S — такое конечное подмножество алгебры F, что $S^{\mathfrak{q}}=F$, и если существует алгоритм, сопоставляющий каждому элементу a из F элемент из $S \cap a^{\mathfrak{q}}$, то проблема тождества для $A=F/\mathfrak{q}$ разрешима.* ∎

Как видно из приведенного выше примера, основная трудность в случае групп состоит в проверке закона ассоциативности. Эту работу можно сократить, если в качестве нашей категории взять не категорию всех групп, а категорию групп подстановок на множестве S.

Процесс, описанный в теореме 9.1, можно истолковать графически, что иногда оказывается полезным. Представим элементы алгебры F вершинами графа; пусть $w \in F$ — произвольный элемент, в котором встречается u_λ для некоторого $\lambda \in \Lambda$, скажем

$$w = f(x, u_\lambda),$$

где f есть Ω-слово относительно x-ов и одного из вхождений u_λ. Если слово w' определено равенством

$$w' = f(x, v_\lambda),$$

то соединим в нашем графе w с w' отрезком и будем говорить, что w' может быть получено из w *прямым переходом*, а w может быть получено из w' *обратным переходом*. Таким образом, получаем ориентированный граф Γ с элементами алгебры F в качестве вершин. Ясно, что различные $\mathfrak{q}$-классы являются в точности связными компонентами графа Γ. Применим теперь теорему I.4.9; назовем элемент алгебры F *приведенным*, если к нему нельзя применить прямого перехода (т. е. если это минимальный элемент относительно предупорядоченности на Γ); тогда имеет место следующая теорема:

***Теорема* 9.3.** *Пусть $\mathcal{K}$ — резидуальная категория со свободными алгебрами, и пусть A есть $\mathcal{K}$-алгебра, заданная в виде*

$$A = \mathcal{K}\{X \mid \Phi\}.$$

Предположим, далее, что

(i) *для каждого $w \in F$ существует такое целое число k, что число последовательных прямых переходов, которые можно применить к w, не может превосходить k;*

(ii) *если w_1 и w_2 получены из одного и того же элемента $u \in F$ прямым переходом, то существует элемент $v \in F$, который может быть получен из w_1 и w_2 прямыми переходами.*

Тогда с помощью конечного числа прямых переходов каждый элемент $w \in F$ можно преобразовать в приведенное слово $\bar{w} \in F$, которое зависит только от w и не зависит от выбора переходов. Более того, приведенные слова образуют трансверсал алгебры A в F.

Действительно, элементы алгебры A соответствуют $\mathfrak{q}$-классам, т. е. связным компонентам графа, определенного данным заданием. Поэтому по теореме I.4.9 минимальные элементы образуют трансверсал алгебры A в F, и сформулированный результат вытекает из теоремы 9.1. ∎

Приведенное слово $\bar{w}$ часто называется *нормальной формой* слова w. Эта теорема снова дает решение проблемы тождества для A, заданной в виде (1): чтобы выяснить, представляют ли w_1 и w_2 один и тот же элемент алгебры A, нужно только перейти к соответствующим приведенным словам $\bar{w}_1$ и $\bar{w}_2$ и посмотреть, совпадают они или нет.

Отметим, что если $\mathscr{K} = (\Omega)$, то условие (i) теоремы всегда выполняется, когда $l(u_\lambda) > l(v_\lambda)$ для всех $\lambda \in \Lambda$, так как тогда каждый переход уменьшает длину слова w и поэтому можно применить последовательно не больше чем $l(w)$ переходов.

УПРАЖНЕНИЕ

1. Пусть $\mathscr{K}$—резидуальная категория Ω-алгебр, обладающая свободными алгебрами. Показать, что если существует алгоритм для решения вопроса, когда два представления определяют изоморфные $\mathscr{K}$-алгебры, то проблема тождества для представлений $\mathscr{K}$-алгебр разрешима.

ГЛАВА IV

МНОГООБРАЗИЯ

Многие важные классы алгебр, встречающиеся на практике, такие, как группы, кольца, структуры и др., могут быть полностью описаны тождественными соотношениями. Эти примитивные классы или многообразия имеют много полезных свойств; в частности, они всегда обладают свободными алгебрами, и элементы данного многообразия можно охарактеризовать как гомоморфные образы свободных алгебр. Всякое многообразие $\mathscr{V}$ Ω-алгебр определяет некоторую подкатегорию категории (Ω), а именно ту полную подкатегорию, объектами которой являются все элементы многообразия $\mathscr{V}$. Получающаяся категория всегда локальна, резидуальна, наследственна и замкнута относительно гомоморфных образов и прямых произведений. Наоборот, алгебры всякой резидуальной категории, замкнутой относительно гомоморфных образов, образуют многообразие. Таким образом, большинство результатов главы III применимо к многообразиям; кроме того, существует ряд черт, специфических для многообразий, которые также будут нами рассмотрены.

1. ОПРЕДЕЛЕНИЕ И ОСНОВНЫЕ СВОЙСТВА

Пусть даны область операторов Ω и множество X; как и раньше, алгебру Ω-слов над X будем обозначать через $W = W_\Omega(X)$. Если A — некоторая Ω-алгебра и α: $W \to A$ — гомоморфизм, то α отображает всякое Ω-слово w в элемент $w\alpha$ алгебры A, который называется значением w в A. Если считать w производным оператором, то его значения в A составляют в точности образ в A при той операции, которая определяется оператором w.

Определение. *Законом* или *тождеством* над Ω в алфавите X называется пара $(w_1, w_2) \in W^2$ или иногда равенство

$$w_1 = w_2, \tag{1}$$

образованное из этой пары. Будем говорить, что тождество (1) *выполняется* в A или что A *удовлетворяет* (1), если при любом гомоморфизме $W \to A$ значения w_1 и w_2 совпадают. Другими словами, производные операторы w_1 и w_2 определяют одну и ту же операцию на A.

Эта связь между тождествами и алгебрами устанавливает соответствие Галуа между классом всех Ω-алгебр (в данном универсальном множестве U) и множеством всех тождеств в данном алфавите X. Если Σ — некоторое множество тождеств, то *многообразием* $\mathscr{V}_\Omega(\Sigma)$, определяемым тождествами Σ, называется класс всех Ω-алгебр, удовлетворяющих всем тождествам из Σ. Итак, под многообразием Ω-алгебр мы понимаем класс всех Ω-алгебр, удовлетворяющих некоторому данному множеству тождеств. Вместо термина «многообразие» иногда употребляются термины «эквационально определимый класс» (Тарский) и «примитивный класс» (Мальцев).

Конечно, приведенное выше определение многообразий зависит от алфавита X, но теперь мы покажем, что все многообразия могут быть получены с помощью некоторого фиксированного алфавита, бесконечного, но в остальном произвольного. Обычно в качестве стандартного алфавита мы будем брать счетное множество

$$X_0 = \{x_1, x_2, \ldots\},$$

которое перенумеровано целыми положительными числами.

Теорема 1.1. *Пусть Σ — некоторое множество тождеств над Ω в алфавите X. Тогда многообразие, определяемое множеством Σ, может быть также определено множеством Σ_0 тождеств в стандартном алфавите X_0 (или вообще в произвольном бесконечном алфавите).*

Доказательство. Будем говорить, что два тождества (не обязательно в одном и том же алфавите) *эквивалентны*, если в каждой Ω-алгебре либо оба эти тождества выполняются, либо ни одно из них не выполняется. Например, переименовывая переменные, мы переходим от любого тождества к эквивалентному тождеству. Так как всякое тождество в X зависит только от конечного числа элементов алфавита X, то его всегда можно заменить эквивалентным тождеством в X_0, и таким образом мы получаем множество Σ_0 тождеств в X_0, эквивалентное множеству Σ. ∎

В дальнейшем будем предполагать, что каждое многообразие определено множеством тождеств в стандартном алфавите. Рассмотрим более подробно соответствие Галуа между классом всех Ω-алгебр и W_0^2, где $W_0 = W_\Omega(X_0)$. Это соответствие Галуа определяет две мультипликативно *замкнутые системы* (см. § II.1): замкнутое множество Ω-алгебр будет просто многообразием; чтобы выяснить, что́ такое замкнутое множество тождеств, необходимо еще одно определение. Будем говорить, что конгруэнция $\mathfrak{q}$ на Ω-алгебре A *вполне инвариантна*, если она выдерживает любой эндоморфизм алгебры A.

***Теорема* 1.2.** *Пусть $W_0 = W_\Omega(X_0)$ — алгебра Ω-слов над стандартным алфавитом. Тогда соответствие Галуа между Ω-алгебрами и тождествами устанавливает естественное взаимно однозначное соответствие между многообразиями Ω-алгебр и вполне инвариантными конгруэнциями на W_0.*

Доказательство. Если $\mathscr{C}$ — некоторый класс Ω-алгебр, то пусть $\mathscr{C}'$ — множество тождеств, выполняющихся во всех $\mathscr{C}$-алгебрах, и если Σ — некоторое множество тождеств, то пусть $\Sigma' = \mathscr{V}_\Omega(\Sigma)$ — многообразие, определяемое множеством Σ. Заметим сначала, что $\mathscr{C}'$ — вполне инвариантная конгруэнция на W_0. Свойства конгруэнции очевидны: в каждой $\mathscr{C}$-алгебре имеем $w = w$ для любого $w \in W_0$; если выполняется тождество $w_1 = w_2$, то выполняется также тождество $w_2 = w_1$, и если выполняются тождества $w_1 = w_2$, $w_2 = w_3$, то выполняется также $w_1 = w_3$. Далее, если $u_i = v_i$ $(i = 1, \ldots, n)$ — тождества, выполняющиеся в A, и $\omega \in \Omega(n)$, то

$$u_1 \ldots u_n\omega = v_1 \ldots v_n\omega$$

выполняется в A. Пусть теперь $(w_1, w_2) \in \mathscr{C}'$, и пусть θ — произвольный эндоморфизм алгебры W_0. Если $\alpha\colon W_0 \to A$, где $A \in \mathscr{C}$ — некоторый гомоморфизм, то $\theta\alpha$ — также гомоморфизм, откуда $w_1\theta\alpha = w_2\theta\alpha$. Этим показано, что тождество $w_1\theta = w_2\theta$ выполняется в A и поэтому $(w_1\theta, w_2\theta) \in \mathscr{C}'$; итак, конгруэнция $\mathscr{C}'$ вполне инвариантна.

Для завершения доказательства покажем, что

$$\mathscr{V}'' = \mathscr{V} \tag{2}$$

для любого многообразия $\mathscr{V}$ и

$$\mathfrak{q}'' = \mathfrak{q} \tag{3}$$

для любой вполне инвариантной конгруэнции $\mathfrak{q}$ на W_0.

По определению многообразия для некоторого $\Sigma \subseteq W_0^2$ имеет место $\mathscr{V} = \Sigma'$; следовательно, $\mathscr{V}'' = \Sigma''' = \Sigma' = \mathscr{V}$, т. е. (2) доказано. Далее, пусть $\mathfrak{q}$ — вполне инвариантная конгруэнция на W_0. Мы утверждаем, что

$$W_0/\mathfrak{q} \in \mathfrak{q}'. \tag{4}$$

Для доказательства этого достаточно показать, что тождества, соответствующие элементам конгруэнции $\mathfrak{q}$, выполняются в $W_0/\mathfrak{q}$. Итак, пусть $(w_1, w_2) \in \mathfrak{q}$ и пусть $\alpha\colon W_0 \to W_0/\mathfrak{q}$ — некоторый гомоморфизм. В силу предложения III.5.7 существует такой эндоморфизм $\alpha'\colon W_0 \to W_0$, что диаграмма

$$\begin{tikzcd}
W_0 \arrow[rr, "\alpha'"] \arrow[dr, "\alpha"'] & & W_0 \arrow[dl, "\mathrm{nat}\,\mathfrak{q}"] \\
& W_0/\mathfrak{q} &
\end{tikzcd}$$

коммутативна. Но $\mathfrak{q}$—вполне инвариантна; следовательно, $(w_1\alpha', w_2\alpha') \in \mathfrak{q}$ и поэтому $w_1\alpha = w_1\alpha' (\operatorname{nat} \mathfrak{q}) = w_2\alpha' (\operatorname{nat} \mathfrak{q}) = w_2\alpha$, что мы и хотели показать. Итак, (4) выполняется. Возвращаясь к (3), заметим, что во всяком случае $\mathfrak{q}'' \supseteq \mathfrak{q}$. Если теперь $(w_1, w_2) \notin \mathfrak{q}$, то $w_1 = w_2$ не выполняется тождественно в $W_0/\mathfrak{q}$, так как $w_1 \not\equiv w_2 (\operatorname{mod} \mathfrak{q})$, но $W_0/\mathfrak{q} \in \mathfrak{q}'$ в силу (4) и потому $(w_1, w_2) \notin \mathfrak{q}''$; следовательно, $\mathfrak{q}'' \subseteq \mathfrak{q}$, откуда и вытекает (3). ▮

Из определений § II.2 вытекает, что следующие классы алгебр являются многообразиями: группоиды, полугруппы (с нейтральным элементом), группы (с операторами), абелевы группы, кольца (с единицей), R-модули (над данным кольцом R) и структуры. Иногда можно определить как многообразия другие классы алгебр, хотя на первый взгляд кажется, что они не являются многообразиями. В § II.2 это уже было сделано для групп. Аналогично квазигруппы также можно определить как многообразие алгебр с тремя бинарными операторами μ, ρ, λ, записывая умножение как $ab\mu$ и полагая $a = cb\rho$, $b = ca\lambda$, если

$$ab\mu = c. \tag{5}$$

В любой квазигруппе эти операторы удовлетворяют тождествам

$$xy\mu y\rho = x, \quad xy\mu x\lambda = y, \quad zy\rho y\mu = z, \quad xzx\lambda\mu = z. \tag{6}$$

Обратно, как легко проверить, всякая (μ, ρ, λ)-алгебра, удовлетворяющая (6), будет квазигруппой. Конечно, это определение не полностью эквивалентно предыдущему, так как подалгебры при этих двух определениях будут разными. По этой причине алгебры многообразия, определяемого тождествами (6), называются иногда *эквазигруппами*. Тем же способом лупы (или точнее элупы) могут быть определены как некоторое многообразие алгебр с тремя бинарными операторами и одним 0-арным оператором.

Если C — некоторая фиксированная Ω-алгебра, то Ω-алгебры над C образуют многообразие; действительно, как было показано в § II.2, всякую Ω-алгебру над C можно определить как алгебру с операторами Ω и некоторыми 0-арными операторами (соответствующими элементам алгебры C), которые удовлетворяют некоторым тождествам.

УПРАЖНЕНИЯ

1. Показать, что если алгебра $W_0/\mathfrak{q}$ в (4) не тривиальна, то она будет свободной $\mathfrak{q}'$-алгеброй над X_0.

2. Показать, что модулярные структуры образуют многообразие.

3. Показать, что многообразие групп, определяемое конечным множеством тождеств, может быть определено одним тождеством.

4. (Мальцев [54].) Пусть Q — непустая квазигруппа и $u \in Q$. Показать, что относительно производных операций $xy\mu' = xuu\lambda\mu uy\lambda\rho$, $xy\rho' = xuy\lambda\mu uu\lambda\rho$, $xy\lambda' = uyuu\lambda\mu x\lambda\rho$ Q будет лупой с нейтральным элементом u.

5. Показать, что относительно правого деления как бинарной операции группы могут быть определены как алгебры, удовлетворяющие тождествам $xz\rho yz\rho\rho = xy\rho$, $xx\rho yy\rho y\rho\rho = y$. Аналогично абелевы группы могут быть определены тождествами $xxy\rho\rho = y$, $xy\rho z\rho = xz\rho y\rho$.

6. (Хигмэн, Нейман [52].) Показать, что группы могут быть определены одним тождеством $xxx\rho y\rho z\rho xx\rho x\rho z\rho\rho\rho = y$, а абелевы группы могут быть определены одним тождеством $xyz\rho yx\rho\rho\rho = z$ [1]).

2. СВОБОДНЫЕ ГРУППЫ И СВОБОДНЫЕ КОЛЬЦА

Нетривиальное многообразие всегда обладает свободными алгебрами. Это будет вытекать из характеризации многообразий, данной в следующем параграфе, но может быть показано также непосредственно: если взять Ω-алгебру

$$A = \Omega\{X \mid \Phi\}, \tag{1}$$

где Φ состоит из всех соотношений, полученных подстановкой в любое тождество многообразия $\mathscr{V}$ произвольных слов над множеством X, то мы получим свободную $\mathscr{V}$-алгебру над X. В частности, это обеспечивает существование свободных алгебр в категориях, упомянутых в § IV.1. Однако, чтобы свободные алгебры были действительно полезны, для их элементов должна существовать простая нормальная форма, т. е. проблема тождества должна иметь простое решение. Так обстоит дело в случае групп и ассоциативных колец, и здесь мы опишем эту нормальную форму отчасти для того, чтобы применить технику §§ III.8—9, а отчасти для того, чтобы пролить бóльший свет на концепцию свободной алгебры.

Лучше всего начать с рассмотрения полугрупп. Нормальная форма для элементов свободной полугруппы может быть получена чрезвычайно просто, и она будет использована при рассмотрении групп и даже общих алгебр (см. § IV.4).

---

[1]) Соответствующий результат для колец см. в работе Ю. И. Соркина (*УМН*, 12 : 4 (1957), 357—362). Объединение этих двух результатов в рамках теории мультиоператорных групп см. в работе Т. В. Соколовской (*Сиб. матем. журн.*, 8 (1967), 853—858).

Заметим, что многообразия алгебр можно рассматривать с точностью до эквивалентности, считая два многообразия эквивалентными, если, грубо говоря, каждое из них получается из другого переходом к некоторой системе производных операций. Отметим в этой связи работу А. А. Терехова (*Уч. зап. Ивановск. пед. ин-та*, 18 (1958), 61—66), посвященную изучению многообразий алгебр с совпадающими прямыми и свободными произведениями. В работах Чаканя (*Acta Sci. Math.*, 23 (1962), 46—57; 24 (1963), 157—164) указано несколько характеризаций многообразий, эквивалентных многообразию всех правых унитарных модулей над некоторым ассоциативным кольцом с единицей. — *Прим. ред.*

Пусть Sg — категория полугрупп. Для построения свободной полугруппы над множеством X рассмотрим группоид Φ_X, элементами которого являются всевозможные непустые строки элементов множества X с последовательным приписыванием в качестве умножения. Легко видеть, что Φ_X ассоциативен, т. е. является полугруппой, и так как он порождается множеством X, то должен быть гомоморфным образом свободного группоида Γ_X над X, т. е. алгебры слов над X. Но любые два элемента группоида Γ_X, которые отображаются в один элемент при этом гомоморфизме, могут отличаться друг от друга только расположением скобок (т. е. порядком, в котором выполнено умножение), и поэтому они отображаются в один элемент при всяком гомоморфизме в любую полугруппу. Это показывает, что Φ_X на самом деле будет свободной полугруппой над X; отметим, что в действительности мы воспользовались заданием (1), что избавило нас от проверки универсального свойства.

Если вместо Sg рассмотреть категорию Sg^* полугрупп с нейтральным элементом 1, то свободная полугруппа с 1 получается присоединением к Φ_X нейтрального элемента, т. е. нужно взять $\Phi_X^1 = \Phi_X \sqcup \{1\}$ и определить

$$a1 = 1a = a \qquad (a \in \Phi_X^1).$$

Представляя 1 пустой строкой, можно считать Φ_X^1 множеством всех строк над X (включая пустую строку) с последовательным приписыванием в качестве умножения. Иногда удобнее считать X индексированным, скажем $X = (x_i)$; тогда элементами полугруппы Φ_X^1 будут *одночлены*

$$x_I = x_{i_1} \cdots x_{i_n},$$

соответствующие различным строкам $I = (i_1, \ldots, i_n)$, получаемым из множества индексов.

Переходя теперь к группам, возьмем в качестве области операторов множество, состоящее из бинарного оператора (умножения), унарного оператора (взятия обратного) и 0-арного оператора 1 (нейтрального элемента), и запишем свободную группу над X посредством задания (1). Это задание можно еще больше упростить на основании следующей почти тривиальной леммы.

***Лемма* 2.1.** *Если группа G порождается множеством Y, замкнутым относительно взятия обратного, то полугруппа с 1, порожденная множеством Y, совпадает с G.*

Нужно только проверить, что элемент, обратный к любому произведению элементов из Y, сам будет произведением элементов из Y, а это вытекает из формулы

$$(y_1 \cdots y_n)^{-1} = y_n^{-1} \cdots y_1^{-1}, \tag{2}$$

так как Y замкнуто относительно взятия обратного. ∎

Пусть теперь F_X — свободная группа над X; положим $X^{-1} = \{x^{-1} \mid x \in X\}$; тогда множество $Y = X \cup X^{-1}$ замкнуто относительно взятия обратного и порождает F_X как группу. С другой стороны, рассмотрим полугруппу с 1, определенную заданием

$$E_X = \mathrm{Sg}^* \{X \cup X^{-1} \mid xx^{-1} = x^{-1}x = 1 \quad (x \in X)\}. \tag{3}$$

Так как все соотношения полугруппы E_X выполняются в F_X, то отсюда вытекает, что F_X является гомоморфным образом полугруппы E_X, и если с помощью (2) определить обратные элементы вообще для всех элементов в E_X, то на самом деле E_X будет группой и поэтому будет изоморфна группе F_X. Таким образом, получаем задание свободной группы над X как полугруппы над $Y = X \cup X^{-1}$, т. е. как гомоморфного образа полугруппы Φ_Y^1. Чтобы получить нормальную форму для элементов группы F_X, рассмотрим граф на Φ_Y^1, отрезки которого определяются прямыми переходами

$$uxx^{-1}v \to uv, \quad ux^{-1}xv \to uv \quad (u, v \in \Phi_Y^1, \ x \in X)$$

и обратными к ним. Так как прямой переход уменьшает длину каждого слова (элемента полугруппы Φ_Y^1), к которому он применяется, то число прямых переходов, которые можно применить к любому слову w, ограничено длиной слова w. Более того, если каждое из слов w_1, w_2 получено прямым переходом из одного и того же элемента u, то: *либо* (i) эти переходы действуют на непересекающихся частях слова u и потому могут быть произведены независимо для получения из каждого элемента w_1 или w_2 элемента v прямым переходом: $u = u_1yy^{-1}u_2zz^{-1}u_3$, $w_1 = u_1u_2zz^{-1}u_3$, $w_2 = u_1yy^{-1}u_2u_3$ и $v = u_1u_2u_3$, где y, $z \in Y$; *либо* (ii) может случиться, что эти переходы действуют на пересекающихся частях, скажем $u = u_1yy^{-1}yu_2$ $(y \in Y)$, и w_1, w_2 получаются применением прямых переходов $yy^{-1} \to 1$, $y^{-1}y \to 1$ к выделенной части слова u. В обоих случаях получаем u_1yu_2 и поэтому $w_1 = w_2$. Итак, условия теоремы III.9.3 выполняются, и поэтому мы получили нормальную форму приведенных слов:

Теорема 2.2. *Если F_X — свободная группа над X, то каждый элемент группы F_X можно представить единственным образом в виде*

$$y_1y_2 \ldots y_n \quad (y_i \in X \cup X^{-1}, \ y_{i-1} \neq y_i^{-1}). \ \blacksquare \tag{4}$$

Эту теорему можно доказать многими другими способами; некоторые из них, использующие специфические черты групп, являются, возможно, более прямыми, чем приведенное доказательство, но ни одно из них не делает утверждение столь тривиальным, каким оно кажется на первый взгляд. Трудность любого доказательства состоит в установлении того факта, что все элементы вида (4) представляют различные элементы группы F_X. Если делать это непосредственно, то нужно взять сами выражения (4) в качестве элементов группы и так определить умножение между ними, чтобы получить F_X, но тогда требует проверки закон ассоциативности (эту проверку можно осуществить, применяя теорему III.9.1). Несколько более короткий способ состоит в том, чтобы представить группу F_X как группу подстановок на элементах вида (4); здесь нужно только проверять условия для представления.

В качестве второго примера рассмотрим случай ассоциативных колец с единицей 1. Так как всякое такое кольцо можно считать линейной алгеброй над кольцом целых чисел, то вообще будем рассматривать линейные K-алгебры, где K — коммутативное и ассоциативное кольцо с 1. Тогда линейной K-алгеброй A с 1 будет по существу кольцо A с каноническим гомоморфизмом $K \to Z(A)$, где $Z(A) = \{z \in A \mid zx = xz$ для всех $x \in A\}$ — центр кольца A. Категория As_K ассоциативных линейных K-алгебр с 1 подчинена категории Sg^*, и поэтому можно представить Sg^* в As_K. Универсальный функтор $U(S)$ для этого представления называется *полугрупповой алгеброй полугруппы S над кольцом K*. В терминах задания $S = \mathrm{Sg}^*\{X \mid \Phi\}$ полугруппы S имеем

$$U(S) = \mathrm{As}_K\{X \mid \Phi\}.$$

Это задание становится особенно простым, если взять $X = S$ и в качестве Φ — множество равенств, составляющих таблицу умножения полугруппы S. Тогда элементы алгебры $U(S)$ однозначно представляются в виде $\Sigma s\alpha_s$, где $\alpha_s \in K$, $s \in S$ и $\alpha_s = 0$ для всех s, за исключением конечного числа. Сложение и умножение определяются равенствами

$$\Sigma s\alpha_s + \Sigma t\beta_t = \Sigma s(\alpha_s + \beta_s), \qquad (\Sigma s\alpha_s)(\Sigma t\beta_t) = \Sigma st\alpha_s\beta_t,$$

где st — произведение элементов s и t в S. Итак, $U(S)$ можно считать свободным K-модулем с базисом S, умножение в котором индуцируется умножением в S (т. е. базисные элементы перемножаются, как в S, а остальные — в силу линейности). Заметим кстати, что это описание совсем не зависит от закона ассоциативности, поэтому тем же способом можно представить группоиды в (неассоциативных) линейных K-алгебрах; для всякого группоида Γ *алгеброй группоида Γ над K* называется свободный K-модуль с базисом Γ, умножение в котором индуцируется умножением в Γ.

Чтобы получить свободную K-алгебру над X, построим свободную полугруппу с 1 над X и возьмем ее полугрупповую алгебру над K.

Взяв X для удобства индексированным, можно сформулировать полученный результат следующим образом:

Теорема 2.3. *Пусть K — некоторое коммутативное и ассоциативное кольцо с 1. Тогда для всякого множества $X=(x_i)$ свободной ассоциативной K-алгеброй с 1 над X будет свободный K-модуль с базисом, состоящим из одночленов x_I.* ∎

Аналогично получается свободная коммутативная ассоциативная K-алгебра над X (скажем $\overline{A}_X$) как полугрупповая алгебра над K свободной коммутативной полугруппы $\overline{\Phi}_X$ над X. Взяв $X=(x_i)$ снова индексированным с помощью линейно упорядоченного множества индексов, видим, что в силу закона коммутативности элементы полугруппы $\overline{\Phi}_X$ можно однозначно представить в виде *возрастающих* одночленов

$$x_I = x_{i_1} \cdots x_{i_n}, \quad \text{где } i_1 \leqslant \ldots \leqslant i_n.$$

Отсюда получаем следующую теорему:

Теорема 2.4. *Если K выбрано таким же, как в теореме 2.3, и $X=(x_i)$ — некоторое множество с линейно упорядоченным множеством индексов, то свободной коммутативной и ассоциативной K-алгеброй с 1 над X будет свободный K-модуль с базисом, состоящим из возрастающих одночленов над X.* ∎

УПРАЖНЕНИЯ

1. (Моримото.) Показать, что если $f(x, y)$ — такой производный оператор в группе, для которого $f(x, f(y, z)) = f(f(x, y), z)$, то f совпадает с одним из операторов xy, yx, x, y, 1.

2. Показать, что если $f(x, y)$ — производный оператор в линейной K-алгебре с 1, для которого $f(x, f(y, z)) = f(f(x, y), z)$, то f совпадает с одним из операторов x, y, $\alpha+\beta(x+y)+\gamma xy$ или $\alpha+\beta(x+y)+\gamma yx$, где $\alpha\gamma+\beta-\beta^2=0$.

3. Показать, что число элементов длины k в свободной полугруппе с q свободными образующими равно q^k, а в свободной группе с q свободными образующими это число равно $2q(2q-1)^{k-1}$. Чему равны соответствующие числа для свободной коммутативной полугруппы и для свободной абелевой группы?

3. ПОРОЖДЕНИЕ МНОГООБРАЗИЙ

Пользуясь определением многообразия, не легко ответить на вопрос, будет ли данный класс алгебр многообразием или нет. Дадим теперь необходимые и достаточные условия (принадлежащие Биркгофу [35]), при которых класс алгебр является многообразием.

***Теорема* 3.1.** *Полная подкатегория $\mathscr{K}$ категории (Ω) всех Ω-алгебр является многообразием тогда и только тогда, когда выполняются следующие четыре условия:*

(i) *$\mathscr{K}$ содержит алгебру с непустым носителем.*
(ii) *$\mathscr{K}$ наследственна.*
(iii) *$\mathscr{K}$ замкнута относительно гомоморфных образов.*
(iv) *$\mathscr{K}$ замкнута относительно прямых произведений.*

Заметим, что всякая категория, удовлетворяющая (iii), абстрактна [1].

Доказательство. Необходимость этих условий очевидна, и проверка может быть предоставлена читателю. При доказательстве достаточности будем предполагать, что категория $\mathscr{K}$ нетривиальна, так как тривиальная абстрактная категория, удовлетворяющая (i), очевидно, является многообразием.

Если через $\mathscr{V}$ обозначен класс всех $\mathscr{K}$-алгебр, то ясно, что

$$\mathscr{V}'' \supseteq \mathscr{V},$$

и нужно доказать равенство. Пусть $A \in \mathscr{V}''$; представим A как гомоморфный образ алгебры Ω-слов W над достаточно большим множеством X (по теореме III. 2.7):

$$\theta\colon W \to A. \tag{1}$$

В силу теоремы III. 5.3 и следующего за ней замечания $\mathscr{K}$ обладает свободными алгебрами произвольного ранга; пусть F — свободная $\mathscr{K}$-алгебра над X; тогда тождественное отображение множества X можно продолжить до эпиморфизма α: $W \to F$, скажем с ядром $\mathfrak{q}$. Если $(u, v) \in \mathfrak{q}$, то Ω-слова u и v имеют одно и то же значение в F и, следовательно, во всякой $\mathscr{K}$-алгебре, т. е. $u = v$ есть тождество в $\mathscr{K}$, и поэтому это тождество выполняется на A. Итак, $u\theta = v\theta$; отсюда $\mathfrak{q} \subseteq \ker\theta$ и $\theta = (\mathrm{nat}\,\mathfrak{q})\,\theta^*$, где

$$\theta^*\colon F \to A$$

— эпиморфизм. Так как $F \in \mathscr{V}$, то из (iii) вытекает, что $A \in \mathscr{V}$. ∎

Проследив последнюю часть доказательства, получаем

***Следствие* 3.2.** *Пусть F — свободная алгебра категории $\mathscr{K}$; тогда каждое соотношение в F является тождеством в $\mathscr{K}$, и, обратно, всякое тождество в $\mathscr{K}$ является соотношением в F.* ∎

---

[1] С. Р. Когаловский (*Сиб. матем. журн.*, 4 (1963), 97—119; *УМН*, 20 : 5 (1965), 206—207) показал, что в этой теореме условия (ii) и (iv) можно исключить, заменив их следующим условием: $\mathscr{K}$ замкнута относительно подпрямых произведений. См. также Б. М. Шайн (*УМН*, 20 : 6 (1965), 173—174) и следствие 3.6 ниже. — *Прим. ред.*

Из теоремы 3.1 вытекают также следующие утверждения:

***Следствие* 3.3.** *Каждое нетривиальное многообразие*[1]) *обладает свободными алгебрами.* ∎

***Следствие* 3.4.** *Каждое многообразие локально, резидуально и замкнуто относительно свободных и прямых объединений.*

Это вытекает из предложения II.7.4, теоремы III.6.1 и теоремы III.6.4. ∎

Пусть $\mathscr{K}$ — некоторая категория Ω-алгебр и $\mathscr{K}'$ — множество всех тождеств, выполняющихся в каждой $\mathscr{K}$-алгебре. Тогда $\mathscr{K}''$ — многообразие, определяемое множеством тождеств $\mathscr{K}'$, и поэтому является наименьшим многообразием, содержащим каждую $\mathscr{K}$-алгебру. Будем также говорить, что $\mathscr{K}''$ — многообразие, *порожденное* категорией $\mathscr{K}$, и писать

$$\mathscr{K}'' = \mathbf{V}\mathscr{K}.$$

Из определения $\mathscr{K}''$ через соответствие Галуа вытекает, что $\mathbf{V}$ — оператор замыкания на категориях; в частности, категория $\mathscr{K}$ $\mathbf{V}$-замкнута тогда и только тогда, когда $\mathscr{K}$ сама является многообразием. Явное выражение для $\mathbf{V}$, принадлежащее Ф. Холлу, дано в следующей теореме:

***Теорема* 3.5.** *Если $\mathscr{K}$ — некоторая категория Ω-алгебр, то многообразие, порожденное категорией $\mathscr{K}$, состоит из всех гомоморфных образов подпрямых произведений $\mathscr{K}$-алгебр, т. е.*

$$\mathbf{V} = \mathbf{QR}. \tag{2}$$

Доказательство. Обе части равенства (2), примененные к тривиальной категории, очевидно, дают один и тот же результат; поэтому пусть $\mathscr{K}$ — нетривиальная категория. По теореме 3.1, $\mathbf{R}\mathscr{K} \subseteq \mathbf{V}\mathscr{K}$ и $\mathbf{QR}\mathscr{K} \subseteq \mathbf{V}\mathscr{K}$; поэтому остается доказать обратное включение. По теореме III.5.3 $\mathbf{R}\mathscr{K}$ будет категорией, обладающей свободными алгебрами всех рангов, превышающих некоторое кардинальное число α, и каждая $\mathbf{R}\mathscr{K}$-алгебра является гомоморфным образом одной из этих свободных алгебр. Рассмотрим теперь категорию $\mathbf{QR}\mathscr{K}$; она состоит из всех гомоморфных образов всех свободных $\mathbf{R}\mathscr{K}$-алгебр. Итак, $\mathbf{QR}\mathscr{K}$ обладает свободными алгебрами ранга $> \alpha$, и поэтому $\mathbf{SQR}\mathscr{K}$ обладает свободными алгебрами произвольного ранга[2]). Если этот ранг положительный, то в силу предложения III.5.5

[1]) Многообразие нетривиально, если оно нетривиально как категория, т. е. если оно содержит алгебру, состоящую более чем из одного элемента.

[2]) Стэнли (*Mich. Math. J.*, **13** (1966), 127—128) указал на пробел в этом месте доказательства (случай свободных алгебр ранга 0) и восполнил его. — *Прим. ред.*

эти свободные алгебры уже лежат в $\mathbf{QR}\mathcal{K}$, так что $\mathbf{QR}\mathcal{K}$ обладает свободными алгебрами всех положительных рангов. Пусть теперь $A \in \mathbf{V}\mathcal{K}$, $A \neq \varnothing$; возьмем произвольное множество образующих $X \neq \varnothing$ алгебры A, и пусть F — свободная $\mathbf{QR}\mathcal{K}$-алгебра над X. Тогда всякое соотношение в F будет тождеством в $\mathcal{K}$ (в силу следствия 3.2) и потому выполняется в A; по теореме Дика (теорема III. 8.3) тождественное отображение множества X на себя продолжается до эпиморфизма $F \twoheadrightarrow A$, и поэтому $A \in \mathbf{QR}\mathcal{K}$. В исключенном случае ($A = \varnothing$) формально можно представить A в виде прямого произведения пустого семейства. ∎

Из этой теоремы получаем следующее усиление критерия Биркгофа (теорема 3.1):

***Следствие* 3.6.** *Если $\mathcal{K}$ — некоторая резидуальная категория, замкнутая относительно гомоморфных образов, то $\mathcal{K}$-алгебры образуют многообразие.*

Действительно, тогда $\mathbf{V}\mathcal{K} = \mathbf{QR}\mathcal{K} = \mathbf{Q}\mathcal{K} = \mathcal{K}$. ∎

Заметим, что ни теорема 3.5, ни следствие 3.6 не содержат никакого утверждения о $\mathcal{K}$-гомоморфизмах; Стэнли показал, что всякая резидуальная категория, замкнутая относительно гомоморфных образов, будет полной подкатегорией категории (Ω) (работа будет опубликована в *Michigan Math. Journal*).

Доказательство теоремы 3.5 показывает, что если $\mathcal{K}$ — некоторая категория со свободными алгебрами, то класс всех гомоморфных образов всех свободных $\mathcal{K}$-алгебр образует многообразие, которое не может быть ничем иным как $\mathbf{V}\mathcal{K}$. Отсюда вытекает, что свободная $\mathcal{K}$-алгебра над X изоморфна свободной $\mathbf{V}\mathcal{K}$-алгебре над X или, другими словами, так как свободные алгебры определены только с точностью до изоморфизма и категории абстрактны, то каждая свободная $\mathbf{V}\mathcal{K}$-алгебра принадлежит $\mathcal{K}$. Обратно, если свободная $\mathbf{V}\mathcal{K}$-алгебра принадлежит $\mathcal{K}$, то она будет свободной $\mathcal{K}$-алгеброй. Итак, получен следующий критерий того, что категория обладает свободными алгебрами:

***Предложение* 3.7.** *Категория $\mathcal{K}$ Ω-алгебр обладает свободными $\mathcal{K}$-алгебрами тогда и только тогда, когда каждая свободная $\mathbf{V}\mathcal{K}$-алгебра является $\mathcal{K}$-алгеброй.* ∎

Это предложение применимо не только к подкатегориям категории (Ω), но и к любому классу $\mathscr{C}$ Ω-алгебр. Формально это можно получить из проведенных рассуждений, если рассмотреть категорию $[\mathscr{C}]$, состоящую из всех алгебр, изоморфных алгебрам класса $\mathscr{C}$, со всеми гомоморфизмами между ними. Применяя операторы замыкания $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{V}$, мы часто будем опускать скобки и писать $\mathbf{V}\mathscr{C}$ вместо $\mathbf{V}[\mathscr{C}]$ и т. д.

Особый интерес представляет случай, когда $\mathscr{C}$ состоит из одной алгебры A. Тогда $\mathbf{V}\mathscr{C}$ будет наименьшим многообразием, содержащим A; будем также говорить, что A — *порождающая алгебра* в $\mathbf{V}\mathscr{C}$, и писать $\hat{A}$ вместо $\mathbf{V}\{A\}$. Иначе говоря, если $\mathscr{V}$ — многообразие, то порождающей алгеброй для $\mathscr{V}$ будет такая $\mathscr{V}$-алгебра A, что каждое тождество алгебры A выполняется в $\mathscr{V}$.

***Предложение* 3.8.** *Каждое многообразие обладает порождающими алгебрами; в частности, если $\mathscr{V}$ — нетривиальное многообразие, то всякая свободная $\mathscr{V}$-алгебра над бесконечным алфавитом является порождающей для $\mathscr{V}$.*

Доказательство. Ясно, что тривиальная алгебра будет порождающей для тривиального многообразия; поэтому пусть $\mathscr{V}$ — нетривиальное многообразие и F — свободная $\mathscr{V}$-алгебра над бесконечным алфавитом; тогда $\hat{F} \subseteq \mathscr{V}$. Пусть теперь $A \in \mathscr{V}$; тогда каждая конечнопорожденная подалгебра алгебры A будет $\mathscr{V}$-алгеброй и, следовательно, гомоморфным образом алгебры F. Поэтому A — локально $\hat{F}$-алгебра, но $\hat{F}$ — локальная категория (по следствию 3.4), и поэтому $A \in \hat{F}$. ∎

Мы видели, что многообразие $\mathscr{V}$ может быть определено либо (i) множеством всех своих тождеств над некоторым бесконечным алфавитом (теорема 1.1), либо (ii) свободной $\mathscr{V}$-алгеброй над некоторым бесконечным алфавитом (предложение 3.8). Если алфавит конечный, то эти два описания могут оказаться неэквивалентными. Для выяснения соотношений между ними нам сначала нужны некоторые определения.

Пусть $\mathscr{V}$ — некоторое многообразие, и через $F_n(\mathscr{V})$ обозначена свободная $\mathscr{V}$-алгебра ранга n. Для каждого кардинального числа n сопоставим многообразию $\mathscr{V}$ два многообразия $\mathscr{V}^n$ и $\mathscr{V}_n$, одно из которых содержит $\mathscr{V}$, а другое содержится в нем. А именно, $\mathscr{V}^n$ — класс всех Ω-алгебр, удовлетворяющих всем тождествам многообразия $\mathscr{V}$, зависящим не более чем от n букв, и $\mathscr{V}_n$ — класс всех Ω-алгебр, удовлетворяющих всем тождествам, выполняющимся в $F_n(\mathscr{V})$. Из этого определения ясно, что $\mathscr{V}^n$ и $\mathscr{V}_n$ — многообразия и, как показано выше, $\mathscr{V}^n = \mathscr{V}_n = \mathscr{V}$ для всех бесконечных n. Далее, легко проверить, что

$$\mathscr{V}_1 \subseteq \mathscr{V}_2 \subseteq \ldots \subseteq \mathscr{V} \subseteq \ldots \subseteq \mathscr{V}^2 \subseteq \mathscr{V}^1;$$
$$\bigcup \mathscr{V}_n = \bigcap \mathscr{V}^n = \mathscr{V}.$$

Наименьшее значение n, при котором $\mathscr{V}^n = \mathscr{V}$, называется *аксиоматическим рангом* многообразия $\mathscr{V}$ и обозначается через $r_a(\mathscr{V})$; наименьшее n, при котором $\mathscr{V}_n = \mathscr{V}$, называется *базисным рангом* многообразия $\mathscr{V}$ и обозначается через $r_b(\mathscr{V})$. Из этого определения видно, что r_a — такое наименьшее число, что $\mathscr{V}$ может быть определено тождествами от r_a букв (или $\aleph_0$, если такого числа не существует), а r_b — такое наименьшее число, что каждая $\mathfrak{V}$-алгебра удовлетворяет всем тождествам, выполняющимся в свободной $\mathfrak{V}$-алгебре ранга r_b, т. е. такое число, что $F_{r_b}(\mathfrak{V})$ — порождающая алгебра для $\mathfrak{V}$ (или $\aleph_0$, если такого числа не существует). В общем случае ни r_a, ни r_b не обязаны быть конечными; пример многообразия групп, для которого r_b бесконечен, содержится в работе Хигмэна [59], пример многообразия алгебр, для которого r_a бесконечен, — в работе Линдона [54]. Не известно, будет ли r_a конечен для любого многообразия групп, но для многих хорошо изученных многообразий алгебр оба ранга r_a и r_b конечны. Для упрощения вычисления $r_a(\mathfrak{V})$ может быть полезно

***Предложение* 3.9.** *Пусть $\mathfrak{V}$ — некоторое многообразие Ω-алгебр. Алгебра A принадлежит многообразию $\mathfrak{V}^n$ тогда и только тогда, когда все ее подалгебры с n образующими принадлежат $\mathfrak{V}$.*

Доказательство. Положим $F_n = F_n(\mathfrak{V})$, и пусть X_n — множество свободных образующих алгебры F_n. В силу следствия 3.2 всякое соотношение в F_n будет тождеством многообразия $\mathfrak{V}$ и, очевидно, зависит не более чем от n букв. Предположим теперь, что $A \in \mathfrak{V}^n$, и пусть

$$\theta\colon X_n \to A \tag{3}$$

— произвольное отображение; тогда всякое соотношение в F_n будет тождеством многообразия $\mathfrak{V}$, зависящим не более чем от n букв, и поэтому выполняется в A; следовательно, θ продолжается до гомоморфизма. Это справедливо для любого отображения θ; поэтому все подалгебры алгебры A с n образующими принадлежат $\mathfrak{V}$. Обратно, если это условие выполняется, то всякое отображение (3) продолжается до гомоморфизма; следовательно, любое тождество, зависящее не более чем от n букв, выполняется в A, так как выполняется в F_n, и потому $A \in \mathfrak{V}^n$. ∎

Чтобы показать, как применяется это предложение, определим аксиоматический и базисный ранги для многообразия Gp всех групп. Так как группы могут быть определены тождествами, зависящими от трех букв, то имеем $r_a(\mathrm{Gp}) \leqslant 3$. Мы утверждаем, что выполняется равенство. Чтобы это установить, достаточно показать, что $\mathrm{Gp}^2 \supset \mathrm{Gp}$, а это будет доказано, если мы построим лупу, все подлупы которой с двумя образующими являются группами. Такая лупа получается, если взять элементы $\pm e_i$, где e_i $(i = 1, \ldots, 8)$ пробегает базис алгебры Кэли — Диксона в обычной форме (см., например, Курош [62], гл. V). Рассмотрим теперь базисный ранг: так как свободная группа ранга 2 содержит свободную группу бесконечного ранга в качестве подгруппы, то имеем $r_b(\mathrm{Gp}) \leqslant 2$; и здесь имеет место равенство, так как свободная группа ранга 1 абелева и поэтому, конечно, не может быть порождающей для Gp. Итак, имеем $r_a(\mathrm{Gp})=3$, $r_b(\mathrm{Gp})=2$.

Рассмотрим теперь некоторое множество Σ тождеств от n букв $x_1, \ldots, x_n$. Можно считать Σ подмножеством в W_n^2, где W_n—алгебра Ω-слов над $x_1, \ldots, x_n$; поэтому можно заменить Σ вполне инвариантной конгруэнцией на W_n, которую Σ порождает. Если эту конгруэнцию обозначить через $\mathfrak{q}$, то $F_n = W_n/\mathfrak{q}$ будет свободной алгеброй ранга n для многообразия Σ'. С помощью этих обозначений (поскольку $\mathfrak{q}$ может быть любой вполне инвариантной конгруэнцией на W_n) получаем

***Предложение* 3.10.** *Пусть $\mathfrak{q}$ — некоторая вполне инвариантная конгруэнция на W_n и положим $F_n = W_n/\mathfrak{q}$. Если дано некоторое многообразие $\mathcal{V}$, то пусть $\mathfrak{r}_n$—множество всех его тождеств от $x_1, \ldots, x_n$. Тогда*

(i) $\mathfrak{r}_n \subseteq \mathfrak{q}$ *в том и только том случае, если* $F_n \in \mathcal{V}^n$;

(ii) $\mathfrak{r}_n \supseteq \mathfrak{q}$ *в том и только том случае, если* $\mathcal{V}_n \subseteq \mathfrak{q}'$.

В частности, $\mathfrak{r}_n = \mathfrak{q}$ *в том и только том случае, если* $\mathcal{V}^n = \mathfrak{q}'$, $\mathcal{V}_n = \hat{F}_n$, *а это выполняется при условии, что*

$$\hat{F}_n \subseteq \mathcal{V} \subseteq \mathfrak{q}'. \tag{4}$$

Доказательство. По определению $\mathcal{V}^n = \mathfrak{r}_n'$, откуда в силу теоремы 1.2 вытекает (i), так как обе конгруэнции $\mathfrak{q}$ и $\mathfrak{r}_n$ вполне инвариантны. Положим, далее, $G_n = W_n/\mathfrak{r}_n$; тогда G_n — свободная $\mathcal{V}$-алгебра над $x_1, \ldots, x_n$ и поэтому $\mathcal{V}_n = \hat{G}_n$, откуда вытекает (ii). Теперь последнее утверждение очевидно, если заметить, что (4) влечет $\mathcal{V}_n = \hat{F}_n$, $\mathcal{V}^n = \mathfrak{q}'$. ∎

Для более детального изучения многообразий $\mathcal{V}^n$ и $\mathcal{V}_n$, когда $\mathcal{V}$ — некоторое многообразие групп, мы отсылаем читателя к работе X. Нейман [56].

Свободные алгебры многообразия, порожденного классом алгебр $\mathscr{C}$, можно охарактеризовать следующим образом:

***Теорема* 3.11.** *Пусть $\mathscr{C}$ — класс Ω-алгебр и $\mathcal{V}$ — многообразие, порожденное классом $\mathscr{C}$. Тогда $\mathcal{V}$-алгебра F свободна над подмножеством X тогда и только тогда, когда каждое отображение*

$$\varphi\colon X \to A \qquad (A \in \mathscr{C})$$

множества X в алгебру A класса $\mathscr{C}$ можно продолжить до гомоморфизма $\varphi^*\colon F \to A$.

Доказательство. Необходимость условия теоремы очевидна. Обратно, предположим, что это условие выполняется, и пусть $B \in \mathcal{V}$.

Тогда каждое отображение $\theta\colon X \to B$ можно продолжить до гомоморфизма

$$\bar{\theta}\colon W \to B, \tag{5}$$

где $W = W_\Omega(X)$ — алгебра Ω-слов над X. Далее, вложение $X \to F$ продолжается до эпиморфизма $W \to F$, так что, производя очевидное отождествление, можно предполагать, что $F = W/\mathfrak{q}$. Для завершения доказательства покажем, что $\bar{\theta}$ можно представить в виде $\bar{\theta} = (\mathrm{nat}\,\mathfrak{q})\,\theta^*$, где $\theta^*\colon F \to B$ продолжает θ. Это будет доказано, если мы сможем показать, что

$$\mathfrak{q} \subseteq \ker \bar{\theta}. \tag{6}$$

Пусть $(u, v) \in \mathfrak{q}$; чтобы получить (6), нужно показать, что $u\bar{\theta} = v\bar{\theta}$. Для этого, конечно, достаточно установить, что

$$u = v \tag{7}$$

будет тождеством в $\mathscr{C}$, так как тогда оно должно быть также тождеством в B. Пусть теперь $\varphi\colon X \to A$ — произвольное отображение, где $A \in \mathscr{C}$; продолжим его до гомоморфизма $\varphi^*\colon F \to A$; тогда $u^{\mathfrak{q}}\varphi^* = v^{\mathfrak{q}}\varphi^*$, так как $u^{\mathfrak{q}} = v^{\mathfrak{q}}$. Это показывает, что (7) — тождество в A, как и утверждалось; поэтому F $\mathscr{V}$-свободна над X. ∎

Этот результат дает возможность простым способом охарактеризовать Ω-алгебры, свободные в *некотором* многообразии $\mathscr{V}$.

***Следствие* 3.12.** *Пусть A есть Ω-алгебра с множеством образующих X. Тогда A свободна над X (в некотором классе Ω-алгебр) в том и только том случае, если каждое отображение $X \to A$ продолжается до эндоморфизма алгебры A.*

Действительно, очевидно, что это условие необходимо, а достаточность вытекает из теоремы 3.11. ∎

Ω-алгебра, удовлетворяющая условию этого следствия, часто называется *относительно свободной*; итак, A относительно свободна над X тогда и только тогда, когда она $\hat{A}$-свободна над X. Относительно свободными алгебрами являются, например, свободные алгебры данного многообразия; пример алгебры, которая не будет относительно свободной ни для какого своего подмножества, приведен в упр. 2.

Если A — порождающая алгебра многообразия $\mathscr{V}$, то по теореме 3.5 все $\mathscr{V}$-алгебры могут быть получены как гомоморфные образы подпрямых степеней алгебры A. В этом случае интересно получить более явное описание свободных $\mathscr{V}$-алгебр:

***Теорема* 3.13.** *Пусть A — некоторая Ω-алгебра; тогда свободная $\hat{A}$-алгебра ранга α получается следующим образом: пусть*

I — множество мощности α и для каждого $i \in I$ определено отображение δ_i: $A^I \to A$ равенством

$$\left((a_j)_{j \in I}\right)\delta_i = a_i. \tag{8}$$

Тогда подалгебра алгебры A^{A^I}, порожденная элементами δ_i ($i \in I$), будет свободной $\hat{A}$-алгеброй над этими элементами.

Доказательство. Пусть F — подалгебра, порожденная элементами δ_i ($i \in I$); если задано некоторое $a \in A^I$, скажем $a = (a_i)$, то обозначим через ε_α проекцию A^{A^I} на соответствующий сомножитель. Ограничение проекции ε_α на F определяет гомоморфизм

$$\varepsilon'_\alpha: F \to A,$$

который в силу (8) отображает δ_i в a_i. Итак, каждое отображение $(\delta_i) \to A$ продолжается до гомоморфизма $F \to A$, и в силу теоремы 3.11 это означает, что F является $\hat{A}$-свободной над элементами δ_i. ∎

Когда α конечно, скажем $\alpha = n$, отображения δ_i будут просто единичными операторами в клоне $\mathfrak{S}(A)$ (см. § III. 3); итак, свободная $\hat{A}$-алгебра ранга n является подалгеброй алгебры A^{A^n}, порожденной n-арными единичными операторами. Она обязательно конечна, когда n и A конечны, и, таким образом, мы получим следующий результат, принадлежащий Б. Нейману [37] в случае групп:

Следствие 3.14. *Если A — конечная Ω-алгебра, то каждая свободная $\hat{A}$-алгебра конечного ранга конечна и, следовательно, каждая $\hat{A}$-алгебра с конечным числом образующих конечна.* ∎

Многообразия Ω-алгебр образуют полную структуру с наибольшим элементом (Ω) и наименьшим элементом — тривиальным многообразием. В случае групп на множестве подмногообразий многообразия Gp можно определить умножение, и довольно неожиданным оказывается, что получающийся группоид будет свободной полугруппой (Б., Х. и П. Нейманы [62])[1]). В общем случае для произвольного Ω умножения не существует, но тем не менее мы имеем структуру. Атомы этой структуры (т. е. минимальные нетривиальные многообразия) мы будем называть *минимальными многообразиями*. Их также называют *эквационально полными* классами, поскольку они определяются максимальными собственными вполне инвариантными конгруэнциями алгебры Ω-слов (соответствующими максимальным непротиворечивым множе-

[1]) Независимо этот результат получил также А. Л. Шмелькин (*ДАН СССР*, **149** (1963), 543—545). Обобщение умножения многообразий групп на случай произвольного класса алгебраических систем рассматривается в работе А. И. Мальцева (*Сиб. матем. журн.*, **8** (1967), 346—365).— *Прим. ред.*

ствам тождеств). Если W — алгебра Ω-слов над множеством X, содержащим больше одного элемента, то вполне инвариантная конгруэнция η на W будет собственной тогда и только тогда, когда она не содержит элементов вида (x, y), где x и y — некоторые различные элементы алгебры W. Отсюда вытекает, что всякая вполне инвариантная конгруэнция может быть вложена в максимальную собственную вполне инвариантную конгруэнцию на W. Этим доказано

***Предложение* 3.15.** *Каждое нетривиальное многообразие содержит минимальные многообразия.* ∎

В минимальном многообразии всякая алгебра, содержащая больше одного элемента, будет порождающей; будем называть порождающие алгебры минимальных многообразий *элементарными*; итак, алгебра A элементарна тогда и только тогда, когда многообразие $\hat{A}$ минимально.

Пусть $\mathscr{V}$ — некоторое нетривиальное многообразие и $\mathscr{M}$ — минимальное многообразие, содержащееся в $\mathscr{V}$. Ясно, что алгебра $F_2(\mathscr{M})$ будет гомоморфным образом алгебры $F_2(\mathscr{V})$, и так как $F_2(\mathscr{M})$ является порождающей для $\mathscr{M}$, то отсюда следует, что минимальные подмногообразия многообразия $\mathscr{V}$ полностью определяются относительно свободными гомоморфными образами алгебры $F_2(\mathscr{V})$. В частности, если $F_2(\mathscr{V})$ конечна, то для нее существует лишь конечное число гомоморфных образов, и мы получаем следующий результат, принадлежащий Скотту [56]:

***Теорема* 3.16.** *Пусть $\mathscr{V}$ — такое нетривиальное многообразие, что $F_2(\mathscr{V})$ конечна. Тогда $\mathscr{V}$ содержит лишь конечное число минимальных подмногообразий. В частности, если A — конечная Ω-алгебра, содержащая больше одного элемента, то $\hat{A}$ обладает лишь конечным числом минимальных подмногообразий.*

Последнее утверждение справедливо, так как в силу следствия 3.14 $F_2(\hat{A})$ конечна. ∎

Алгебру A будем называть *F_n-простой*, если A нетривиальна и для каждого нетривиального гомоморфного образа B алгебры $F_n(\hat{A})$

$$F_n(\hat{A}) \cong F_n(\hat{B}).$$

Определение элементарных алгебр упрощается благодаря следующему критерию, также принадлежащему Скотту [56]:

***Теорема* 3.17.** *Ω-алгебра A элементарна тогда и только тогда, когда A F_n-проста и принадлежит $(\hat{A})_n$ для некоторого $n > 1$.*

Доказательство. Условия, наложенные на A, показывают, что (i) если B — произвольная $\hat{A}$-алгебра с n образующими, то

$(\widehat{B})_n \supseteq (\widehat{A})_n$ и (ii) $(\widehat{A})_n \supseteq (\widehat{A})$. Так как во всяком случае $(\widehat{B})_n \subseteq (\widehat{A})_n \subseteq \widehat{A}$, то из этих условий вытекает, что $\widehat{B} \supseteq \widehat{A}$, откуда

$$\widehat{B} = \widehat{A}. \tag{9}$$

Взяв в качестве B любую нетривиальную алгебру некоторого минимального подмногообразия многообразия $\widehat{A}$, из (9) получаем, что $\widehat{A}$ должно быть минимальным, и, следовательно, A элементарна. Обратно, если A элементарна, то (9) имеет место для каждой нетривиальной $\widehat{A}$-алгебры, и, следовательно, (i) и (ii) выполняются для всех $n > 1$. ∎

Если A конечна, то эти условия дают возможность решить в конечное число шагов, будет ли A элементарной. В качестве иллюстрации опишем элементарные группы. Если G — элементарная группа, то G нетривиальна и поэтому содержит нетривиальную циклическую подгруппу; выбирая подходящий фактор группы G, получаем циклическую группу Z_p простого порядка p в $\widehat{G}$. Так как Z_p порождающая для $\widehat{G}$, то каждая $\widehat{G}$-группа, и в частности сама группа G, абелева и удовлетворяет тождеству $x^p = 1$, т. е. G — элементарная абелева. Обратно, с помощью теоремы 3.17 легко видеть, что элементарная абелева группа будет элементарной.

УПРАЖНЕНИЯ

1. Показать, что условия теоремы 3.1 независимы. Для этого проверить, что класс, приведенный ниже под номером (n), удовлетворяет всем условиям теоремы 3.1, за исключением условия (n) (n = i, ..., iv):

(i) $\varnothing$; (ii) класс делимых абелевых групп (G *делима*, если $x^n = a$ обладает решением x в G для каждого a из G и каждого положительного целого n); (iii) класс абелевых групп без кручения; (iv) класс конечных абелевых групп.

2. Показать, что конечная абелева p-группа относительно свободна тогда и только тогда, когда она элементарная абелева [1]).

3. Пусть $\mathcal{K}$ — категория всех таких групп, в которых каждая максимальная подгруппа имеет бесконечный индекс, со всеми гомоморфизмами между ними. Показать, что $\mathcal{K}$ не резидуальна. (Воспользоваться теоремой 3.5.)

4. Пусть $A = W/\mathfrak{q}$ — произвольная Ω-алгебра в данном задании, где W — алгебра Ω-слов над стандартным алфавитом; через $\mathfrak{r}$ обозначим наибольшую вполне инвариантную конгруэнцию, содержащуюся в $\mathfrak{q}$. Тогда $W/\mathfrak{r}$ будет свободной $\widehat{A}$-алгеброй счетного ранга.

5. (Тарский.) Показать, что категория алгебр будет многообразием тогда и только тогда, когда она локальна и замкнута относительно гомоморфных образов и конечных прямых произведений.

---

[1]) На самом деле тогда и только тогда, когда она является прямой суммой циклических групп одного и того же порядка p^n, $n \geqslant 1$. — *Прим. ред.*

6. Показать, что если $\mathscr{V}$ — некоторое многообразие алгебр, то все свободные алгебры ранга m многообразий $\mathscr{V}^{n+1}$, $\mathscr{V}$, $\mathscr{V}_n$ изоморфны при условии, что $n \geqslant m$. Привести пример, когда все эти три многообразия различны. (Взять $n=1$, а в качестве $\mathscr{V}$ — ассоциативные кольца.)

7. Пусть A — относительно свободна над X. Тогда, если X бесконечно, то $\hat{A}$ — единственное многообразие, для которого A будет свободной алгеброй над X. Если X конечно и содержит n элементов, то показать, что для некоторого многообразия $\mathscr{V}$ свободная $\mathscr{V}$-алгебра ранга n изоморфна алгебре A тогда и только тогда, когда

$$\hat{A} \subseteq \mathscr{V} \subseteq (\hat{A})^n.$$

8. Показать, что для многообразия $\mathscr{V}$, если $\mathscr{V}^n \neq \mathscr{V}$ и $r_a(\mathscr{V}^n) \leqslant n$, то $r_b(\mathscr{V}^n) > n$.

9. Показать, что для многообразия абелевых групп $r_a = 3$, $r_b = 1$. (Рассмотреть лупу, соответствующую конфигурации Паппа, упр. II. 2.12.)

10. Показать, что для многообразия ассоциативных колец $r_a = 3$, $r_b = 2$.

11. Если через As обозначено многообразие ассоциативных колец, то As^2 будет многообразием альтернативных колец и As^1 — многообразием колец с ассоциативными степенями; показать, что $r_a = 2$, $r_b \geqslant 3$ для As^2 и $r_a = 1$, $r_b \geqslant 2$ для As^1.

12. Ω-алгебра A называется *n-примальной*, если клон действия области Ω на A содержит все n-арные операции на A (см. § III. 3). Показать, что A n-примальна тогда и только тогда, когда A^{A^n} порождается как Ω-алгебра единичными операторами.

13. (Фостер.) Показать, что если Ω счетно, то всякая Ω-алгебра, n-примальная для некоторого конечного n, должна быть конечной. (Заметить, что бесконечное множество обладает несчетным множеством n-арных операций.)

14. (Фостер.) Пусть A — нетривиальная Ω-алгебра, n-примальная для всех n, и предположим, что Ω не более чем счетно. Показать, что расширения алгебры A в многообразии $\hat{A}$ являются подпрямыми степенями алгебры A, содержащими постоянные функции.

15. (Тарский.) Показать, что ассоциативное кольцо R элементарно тогда и только тогда, когда оно коммутативно и, для некоторого простого p, $px = 0$ для всех $x \in R$, и либо $xy = 0$ для всех $x, y \in R$, либо $x^p = x$ для всех $x \in R$.

16. (Калицкий и Скотт.) Описать все элементарные полугруппы с двумя элементами.

17. (Шютценбергер.) Показать, что структура элементарна тогда и только тогда, когда она дистрибутивна. (Воспользоваться упр. II. 7.9.)

4. ПРЕДСТАВЛЕНИЯ В МНОГООБРАЗИЯХ АЛГЕБР

Применим теперь теорию представлений, развитую в § III. 4, к многообразиям. Так как каждое многообразие резидуально, то по теореме III. 4.2 резидуальное представление категории $\mathscr{S}$ в многообразии $\mathscr{V}$ Ω-алгебр обладает универсальным функтором. Далее, так как многообразие является частным случаем резидуальной категории, то существует специальный вид резидуальных представлений, которые могут быть определены с помощью тождеств в случае, когда $\mathscr{L}$ — категория алгебр (не обязательно с той же областью операторов, что и $\mathscr{V}$).

Итак, возьмем теперь две области операторов Ω, Θ, многообразие $\mathscr{V}$ Ω-алгебр и категорию $\mathscr{L}$ Θ-алгебр со свободными алгебрами. Рассмотрим произвольное отображение

$$\rho\colon B \to A \tag{1}$$

$\mathscr{L}$-алгебры B в $\mathscr{V}$-алгебру A; если дано множество $w_1, \ldots, w_s$ Θ-слов над $x_1, \ldots, x_r$ и два Ω-слова f, g над $y_1, \ldots, y_s$, то будем говорить, что отображение (1) удовлетворяет тождеству

$$f(w_1\rho, \ldots, w_s\rho) = g(w_1\rho, \ldots, w_s\rho), \tag{2}$$

если обе части равенства (2) оказываются равными при замене $x_1, \ldots, x_r$ произвольными элементами алгебры B. Из определения ясно, что для каждого множества Σ тождеств вида (2) множество всех отображений $\mathscr{L}$-алгебр в $\mathscr{V}$-алгебры, удовлетворяющих тождествам Σ, определяет представление $\mathscr{L}$ в $\mathscr{V}$. Эти представления, определяемые тождествами, можно охарактеризовать следующим образом:

Теорема 4.1. *Если $\mathscr{V}$ — многообразие алгебр и $\mathscr{L}$ — категория алгебр (не обязательно с той же областью операторов) со свободными алгебрами, то данное представление $\mathscr{L}$ в $\mathscr{V}$ можно определить тождествами тогда и только тогда, когда оно резидуально и удовлетворяет следующему условию:*

если $\rho\colon B \to A$ — такое отображение $\mathscr{L}$-алгебры B в $\mathscr{V}$-алгебру A, что для некоторого $\mathscr{L}$-эпиморфизма $\beta\colon B_1 \to B$ отображение $\beta\rho\colon B_1 \to A$ допустимо, то само ρ допустимо.

Говорят, что представление $\mathscr{L}$ в $\mathscr{V}$, удовлетворяющее этому последнему условию, *замкнуто относительно гомоморфизмов.*

Доказательство. Необходимость условий теоремы очевидна, и проверка этого может быть предоставлена читателю. Предположим теперь, что условия теоремы выполняются; тогда по теореме III. 4.2 существует универсальный функтор (U, u) для представления $\mathscr{L}$ в $\mathscr{V}$, и отображение

$$u\colon B \to U(B) \tag{3}$$

допустимо. Кроме того, в силу предложения III. 4.1 $\operatorname{im} u$ порождает $U(B)$. Пусть G — свободная $\mathscr{L}$-алгебра над множеством X; рассмотрим произвольное соотношение

$$f(x_i u) = g(x_i u) \quad (x_i \in X) \tag{4}$$

в $U(G)$. Мы утверждаем, что при данном представлении соотношение (4) выполняется тождественно. Если $\beta\colon G \to B$ — некоторый $\mathscr{L}$-го-морфизм и β': $U(G) \to U(B)$ — индуцируемый им $\mathscr{V}$-гомоморфизм, то, полагая $x_i\beta = b_i$, имеем

$$f(b_iu) = f(x_i\beta u) = f(x_iu)\beta' = g(x_iu)\beta' = g(x_i\beta u) = g(b_iu). \quad (5)$$

Взяв теперь любое допустимое отображение ρ: $B \to A$ $(A \in \mathscr{V})$, имеем $\rho = u\rho^*$, где ρ^*: $U(B) \to A$, и в силу (4) и (5)

$$f(b_i\rho) = f(b_iu)\rho^* = g(b_iu)\rho^* = g(b_i\rho).$$

Этим показано, что (4) выполняется тождественно. Пусть теперь Σ — множество всех тождеств, выполняющихся при данном представлении, и рассмотрим отображение

$$\rho\colon B \to A \quad (B \in \operatorname{Ob}\mathscr{L},\ A \in \mathscr{V}), \quad (6)$$

при котором выполняются все тождества из Σ. Возьмем свободную $\mathscr{L}$-алгебру G над множеством X с $\mathscr{L}$-эпиморфизмом β: $G \to B$; тогда $\operatorname{im} u$ порождает $U(G)$, и всякое соотношение в $U(G)$ между элементами xu $(x \in G)$ является тождеством из Σ и поэтому по определению отображения ρ выполняется также для элементов $x\beta\rho$. По лемме III. 8.1 существует $\mathscr{V}$-гомоморфизм β^*: $U(G) \to A$, при котором диаграмма

$$\begin{tikzcd} G \arrow[r, "u"] \arrow[d, "\beta"'] & U(G) \arrow[d, "\beta^*"] \\ B \arrow[r, "\rho"] & A \end{tikzcd}$$

коммутативна. Таким образом, $\beta\rho$ допустимо, а так как β есть $\mathscr{L}$-эпиморфизм, то ρ допустимо. ∎

Поскольку эти условия необходимы, получаем

***Следствие* 4.2.** *Если $\mathscr{V}$ и $\mathscr{W}$ — некоторые многообразия алгебр, то универсальный функтор существует для любого представления $\mathscr{W}$ в $\mathscr{V}$, которое определяется тождествами.* ∎

Мы получим важный частный случай, если возьмем $\mathscr{V} < \mathscr{L}$ и рассмотрим естественное представление $\mathscr{L}$ в $\mathscr{V}$. Допустимыми отображениями будут по определению такие отображения ρ: $B \to A$ $\mathscr{L}$-алгебры B в $\mathscr{V}$-алгебру A, при которых для любого n-арного оператора ω, действующего в $\mathscr{L}$, и любых $b_1, \ldots, b_n \in B$ имеем

$$(b_1\rho \ldots b_n\rho)\omega = (b_1 \ldots b_n\omega)\rho. \quad (7)$$

Итак, естественное представление $\mathscr{L}$ в $\mathscr{V}$, т. е. представление $\mathscr{L}$ в $\mathscr{V}$ посредством $\mathscr{L}$-гомоморфизмов, определяется тождествами (7), и нами доказано

***Следствие* 4.3.** *Пусть $\mathscr{V}$ — многообразие алгебр, подчиненное категории $\mathscr{L}$ алгебр (не обязательно с той же областью операторов, что и $\mathscr{V}$) со свободными алгебрами. Тогда естественное представление определяется тождествами и обладает универсальным функтором.* ∎

Пусть дано многообразие $\mathscr{V}$ Ω-алгебр, и пусть $\mathscr{V}'$ — категория, полученная ограничением Ω до Ω'. Тогда $\mathscr{V}'$-алгебрами (с точностью до изоморфизма) будут Ω'-подалгебры $\mathscr{V}$-алгебр; следовательно, $\mathscr{V}'$ наследственна. Кроме того, если $(B_\lambda)_{\lambda \in \Lambda}$ — некоторое семейство $\mathscr{V}'$-алгебр, то можно считать B_λ Ω'-подалгеброй некоторой $\mathscr{V}$-алгебры A_λ. Следовательно, прямое произведение $\prod B_\lambda$ будет Ω'-подалгеброй алгебры $\prod A_\lambda$, и это показывает, что $\mathscr{V}'$ замкнута относительно прямых произведений. В силу следствия III.5.2 $\mathscr{V}'$ будет категорией со свободными алгебрами, и этим доказана первая часть следующей теоремы:

***Теорема* 4.4.** *Пусть $\mathscr{V}$ — нетривиальное многообразие Ω-алгебр и $\mathscr{V}'$ — категория Ω'-алгебр, полученная ограничением Ω до Ω'; тогда $\mathscr{V}'$ замкнута относительно подалгебр и прямых произведений. Кроме того, если F — свободная $\mathscr{V}$-алгебра над множеством X, то Ω'-подалгебра Ω-алгебры F, порожденная множеством X, будет свободной $\mathscr{V}'$-алгеброй над X.*

Для доказательства последнего утверждения теоремы через F' обозначим Ω'-подалгебру Ω-алгебры F, порожденную множеством X; тогда по определению $F' \in \mathscr{V}'$. Теперь всякая $\mathscr{V}'$-алгебра B изоморфна Ω'-подалгебре некоторой $\mathscr{V}$-алгебры A и, не ограничивая общности рассуждений, можно считать B вложенной в A. Всякое отображение $\varphi\colon X \to B$ индуцирует отображение $\varphi i\colon X \to A$, где $i\colon B \to A$ — вложение, и поэтому φi можно продолжить до Ω-гомоморфизма $\bar{\varphi}\colon F \to A$. Ограничение $\varphi' = \bar{\varphi} | F'$ будет Ω'-гомоморфизмом, продолжающим φ, и притом единственным, поскольку φ' однозначно определяется своими значениями на X. Этим показано, что F' — свободная $\mathscr{V}'$-алгебра над X. ∎

Заметим, что $\mathscr{V}'$ не обязательно будет многообразием. Например, если $\mathscr{V}$ — многообразие ассоциативных алгебр и $\mathscr{V}'$ — категория, состоящая из специальных йордановых алгебр (см. § VII. 7), то $\mathscr{V}'$ не замкнута относительно гомоморфных образов и поэтому не является многообразием, хотя по теореме 4.4 можно говорить о «свободной специальной йордановой алгебре» над любым множеством.

В следствии 4.3 было показано, что естественное представление категории, полученной ограничением области операторов, всегда обладает универсальным функтором. Существует простой критерий инъективности этого функтора, который часто оказывается полезным.

***Теорема* 4.5.** *Пусть $\mathscr{V}$ — многообразие Ω-алгебр и $\mathscr{V}'$ — категория, полученная ограничением Ω до Ω'. Если B — гомоморфный образ свободной $\mathscr{V}'$-алгебры, скажем*

$$B = F'/\mathfrak{q},$$

где F' есть $\mathscr{V}'$-подалгебра, порожденная множеством X в свободной $\mathscr{V}$-алгебре F над X, и если $\bar{\mathfrak{q}}$ есть Ω-конгруэнция на F, порожденная Ω'-конгруэнцией $\mathfrak{q}$, то универсальной $\mathscr{V}$-алгеброй для B будет

$$U(B) \cong F/\bar{\mathfrak{q}}, \tag{8}$$

и каноническое отображение u: $B \to U(B)$ взаимно однозначно тогда и только тогда, когда

$$\bar{\mathfrak{q}} \cap F'^2 = \mathfrak{q}. \tag{9}$$

Доказательство. Канонический гомоморфизм θ: $F' \to B$, ограниченный на X, вместе с отображением u: $B \to U(B)$ определяют отображение X в $U(B)$, которое продолжается до Ω-гомоморфизма $\bar{\theta}$: $F \to U(B)$. Так как $\ker\theta = \mathfrak{q}$, то отсюда вытекает, что $\ker\bar{\theta} \supseteq \mathfrak{q}$, и поэтому $\ker\bar{\theta} \supseteq \bar{\mathfrak{q}}$, так как $\bar{\mathfrak{q}}$ — наименьшая Ω-конгруэнция, содержащая $\mathfrak{q}$. Отсюда находим

$$\theta^*\colon\ F/\bar{\mathfrak{q}} \to U(B), \tag{10}$$

где $\bar{\theta} = (\operatorname{nat}\bar{\mathfrak{q}})\,\theta^*$. Теперь во всяком случае $\mathfrak{q} \subseteq \bar{\mathfrak{q}} \cap F'^2$; следовательно, существует эпиморфизм

$$F'/\mathfrak{q} \to F'/\bar{\mathfrak{q}} \cap F'^2 \cong F'^{\bar{\mathfrak{q}}}/\bar{\mathfrak{q}}$$

(по второй теореме об изоморфизме), но в то же время

$$F'^{\bar{\mathfrak{q}}}/\bar{\mathfrak{q}} \subseteq F/\bar{\mathfrak{q}},$$

поэтому в итоге получаем гомоморфизм

$$\varphi\colon\ B = F'/\mathfrak{q} \to F/\bar{\mathfrak{q}}; \tag{11}$$

из определения θ^* вытекает, что

$$u = \varphi\theta^*. \tag{12}$$

Теперь всякое допустимое отображение α: $B \to A$ $(A \in \mathscr{V})$ можно представить в виде $\alpha = u\alpha'$; отсюда в силу (12) $\alpha = \varphi\theta^*\alpha'$. Если бы в то же время мы имели $\alpha = \varphi\beta$, то β и $\theta^*\alpha'$ совпадали бы на $\operatorname{im}\varphi$ и, следовательно, на $F/\bar{\mathfrak{q}}$, что и доказывает единственность $\theta^*\alpha'$. Итак, $F/\bar{\mathfrak{q}}$ с отображением (11) обладает универсальным свойством и поэтому может быть отождествлена с $U(B)$. Теперь $\ker\varphi = (\bar{\mathfrak{q}} \cap F'^2)/\mathfrak{q}$ и $\ker\varphi$ будет диагональю тогда и только тогда, когда выполняется (9). ∎

В главе VII эти результаты будут применены к линейным алгебрам; ниже с помощью этих же результатов дается метод вложения произвольных Ω-алгебр в полугруппы. Этот метод основан на конструкции алгебры Ω-слов из § III. 2 и по существу принадлежит Мальцеву [52], который использует его для представления линейных алгебр в ассоциативных алгебрах.

Пусть Ω — некоторая область операторов и через $\mathrm{Sg}(\Omega)$ обозначим класс всех полугрупп над Ω, т. е. полугрупп с элементами из Ω в качестве констант. *Ясно, что* $\mathrm{Sg}(\Omega)$ *будет многообразием;* чтобы избежать недоразумений, будем обозначать полугрупповое умножение через $\circ$. Всякую полугруппу из $\mathrm{Sg}(\Omega)$ можно считать Ω-алгеброй, определив

$$a_1a_2 \cdots a_n\omega = a_1 \circ a_2 \circ \cdots \circ a_n \circ \omega \quad (\omega \in \Omega(n)). \tag{13}$$

Итак, $\mathrm{Sg}(\Omega) \prec (\Omega)$, и поэтому (Ω) может быть представлена в $\mathrm{Sg}(\Omega)$ с помощью естественного представления. В силу следствия 4.3 это представление обладает универсальным функтором; таким образом, каждой Ω-алгебре A поставлена в соответствие полугруппа $U(A)$ над Ω вместе с отображением

$$u\colon\ A \to U(A), \tag{14}$$

которое является Ω-гомоморфизмом (если считать $U(A)$ в силу (13) Ω-алгеброй) и универсальным отображением для гомоморфизмов алгебры A в полугруппы над Ω. Мы утверждаем, что (14) взаимно однозначно; для доказательства этого нужно только показать, что A может быть точно представлена в некоторой полугруппе над Ω. Такую полугруппу можно построить следующим образом. Пусть Σ—множество всех таких конечных строк из элементов непересекающейся суммы $A \sqcup \Omega$ (включая пустую строку), что ни за каким блоком из n последовательно расположенных элементов алгебры A не следует элемент из $\Omega(n)$. Представим A отображениями множества Σ в себя, сопоставляя элементу $a \in A$ операцию ρ_a, определяемую равенством

$$(x_1, \ldots, x_r)\rho_a = (x_1, \ldots, x_r, a) \quad (x_i \in A \sqcup \Omega).$$

Ясно, что $(x_1, \ldots, x_r, a)$ снова принадлежит Σ. Далее, представим Ω, сопоставляя $\omega \in \Omega(n)$ операцию σ_ω, определяемую равенствами

$$(x_1, \ldots, x_r)\sigma_\omega = \begin{cases} (x_1, \ldots, x_m, x_{m+1} \cdots x_r\omega), & \text{если } r = m + n \geqslant n \\ & \text{и } x_i \in A \quad \text{для} \quad i > m, \\ (x_1, \ldots, x_r, \omega) & \text{в противном случае.} \end{cases}$$

Теперь легко проверить, что

$$\rho_{a_1}\rho_{a_2} \cdots \rho_{a_n}\sigma_\omega = \rho_{a_1a_2 \cdots a_n\omega}.$$

Следовательно, мы имеем Ω-гомоморфизм Ω-алгебры A в полугруппу унарных операций на Σ. Кроме того, если ( ) — пустая строка, то

$$(\ )\rho_a = (a) \quad (a \in A),$$

поэтому $\rho_a = \rho_b$ в том и только том случае, если $a = b$. Полученный результат можно сформулировать в виде следующего предложения:

***Предложение* 4.6.** *Всякую Ω-алгебру A можно вложить в полугруппу над Ω, и для всех таких вложений существует универсальная полугруппа над Ω*[1]. ∎

Конечно, в частном случае, когда $A = W_\Omega(X)$, это вложение будет в точности вложением в полугруппу всех Ω-строк над X.

В многообразиях свободные произведения не обязательно существуют (в отличие от свободных объединений), и чтобы доказать существование, нужно по существу показать, что некоторый универсальный функтор инъективен. Другая форма определения свободных произведений в многообразиях дана в следующей теореме:

***Теорема* 4.7.** *Пусть $\mathscr{V}$ — многообразие; тогда $\mathscr{V}$-алгебра A является свободным произведением семейства $(A_\lambda)_{\lambda \in \Lambda}$ своих подалгебр, если для каждого $\lambda \in \Lambda$ существует такое задание*

$$A_\lambda = \mathscr{V}\{X_\lambda | \Phi_\lambda\}, \tag{15}$$

что $\mathscr{V}\{X|\Phi\}$ является заданием $\mathscr{V}$-алгебры A, где $X = \bigsqcup X_\lambda$, $\Phi = \bigsqcup \Phi_\lambda$ и для любой пары $\lambda \neq \mu$ $A_\lambda \cap A_\mu$ — минимальная подалгебра $\mathscr{V}$-алгебры A.

Доказательство. Покажем сначала, что A — свободное объединение $\mathscr{V}$-алгебр A_λ. Так как в силу (15) A_λ определены только с точностью до изоморфизма, то можно взять X_λ попарно непересекающимися и положить тогда $X = \bigcup X_\lambda$. Пусть $\varphi_\lambda\colon A_\lambda \to B$ — некоторое семейство гомоморфизмов; рассмотрим такое отображение $\varphi\colon X \to B$, что $\varphi | X_\lambda = \varphi_\lambda | X_\lambda$. Всякое соотношение между элементами множества X в A является следствием соотношений Φ_λ и поэтому выполняется также для их образов в B. Следовательно (по лемме III.8.1), φ можно продолжить до гомоморфизма $\bar\varphi\colon A \to B$, который совпадает с φ_λ на X_λ и, значит, совпадает также с φ_λ на A_λ. Кроме того, $\bar\varphi$ будет единственным таким гомоморфизмом, так как задано его действие на множестве образующих X алгебры A. Это показывает,

[1] Этот результат независимо получил также Ю. К. Ребане, а в его работе (*Сиб. матем. ж.*, 7 (1966), 878—885) начата реализация следующей программы: охарактеризовать Ω-алгебры, которые могут быть изоморфно вложены (при этом рассматриваются «полилинейные» вложения) в полугруппу с некоторыми заданными хорошими свойствами — коммутативность и т. д.— *Прим. ред.*

что A — свободное объединение с вложениями $A_\lambda \to A$ в качестве канонических гомоморфизмов. По предположению различные сомножители пересекаются по минимальной подалгебре алгебры A, а это показывает, что A — свободное произведение. ∎

Из следствия III.6.3 получаем

Следствие 4.8. *Пусть $\mathscr{V}$ — многообразие, в котором каждая минимальная подалгебра тривиальна; тогда свободное произведение любого семейства $\mathscr{V}$-алгебр существует.* ∎

Это следствие показывает, что существует свободное произведение групп, полугрупп с 1, колец и т. д. Конечно, нужно точно определить многообразие, в котором мы действуем; так, свободное произведение абелевых групп будет различным в зависимости от того, находимся ли мы в многообразии всех групп или в многообразии всех абелевых групп[1]).

УПРАЖНЕНИЯ

1. Показать, что свободное произведение семейства $\mathscr{V}$-алгебр существует тогда и только тогда, когда существует свободное произведение для каждого конечного подсемейства; вывести отсюда, что свойство существования свободных произведений локально. (Воспользоваться теоремой 4.7.)

2. Пусть $\mathscr{V}$ — многообразие алгебр и $\mathscr{L}$ — категория алгебр со свободными алгебрами, которая обладает двумя такими представлениями R_1 и R_2 в $\mathscr{V}$, что каждое R_2-допустимое отображение является также R_1-допустимым. Показать, что если для каждого представления R_i существует универсальный функтор (U_i, u_i), то существует канонический эпиморфизм

$$v\colon U_1(B) \to U_2(B) \quad (B \in \mathrm{Ob}\mathscr{L}). \tag{16}$$

Показать, что если R_2 замкнуто относительно гомоморфных образов и если для некоторой $\mathscr{L}$-алгебры B (16) является изоморфизмом, то v будет изоморфизмом для всякого гомоморфного образа $\mathscr{L}$-алгебры B.

---

[1]) Для большинства важных конкретных многообразий алгебр рассматривался вопрос о строении подалгебр свободных алгебр этих многообразий. При этом иногда оказывается, что подалгебра свободной алгебры сама свободна (см. § VII.2, п. (iv)); иногда же это не так. Рассматривался также более общий вопрос о строении подалгебр свободного (в этом многообразии) произведения и связанный с ним вопрос о существовании изоморфных продолжений для двух любых свободных разложений данной алгебры. В некоторых случаях эти вопросы получают исчерпывающее решение — группы, лупы, неассоциативные алгебры над полем, мультиоператорные группы, мультиоператорные алгебры над полем и др.; в других случаях аналогичные теории заведомо не могут быть построены — кольца, ассоциативные алгебры над полем, полугруппы и др. Возникает весьма далекая от завершения программа рассмотрения этих вопросов в рамках общей теории универсальных алгебр. В этом направлении идут работы Т. М. Баранович (*Матем. сб.*, **67** (1965), 135—153; *Сиб. матем. ж.*, **7** (1966), 1230—1249). — *Прим. ред.*

3. Пусть $\mathscr{V}$ — некоторое многообразие алгебр и $\mathscr{K} = \mathscr{F}(\mathscr{V})$ — категория семейств $\mathscr{V}$-алгебр (над вполне неупорядоченным множеством индексов). Показать, что универсальный функтор существует для представления категории $\mathscr{F}(\mathscr{V})$ в $\mathscr{V}$ с помощью функций, гомоморфных по каждому аргументу. (Если $\mathscr{V}$ — многообразие абелевых групп, то этот функтор будет тензорным произведением.)

4. Для любого положительного целого числа n обозначим через Z_n кольцо целых чисел по $\operatorname{mod} n$. Получить необходимые и достаточные условия для существования свободного произведения колец Z_m и Z_n в категории: (i) коммутативных (и ассоциативных) колец, (ii) коммутативных колец без делителей нуля, (iii) коммутативных колец с 1. (В каждом из этих случаев условия должны обеспечивать принадлежность Z_n, Z_m данной категории.)

5. Показать, что если H — фиксированная группа, то категория расширений группы H замкнута относительно свободных произведений (свободное произведение в этой категории называется также *свободным произведением с объединенной подгруппой* H).

6. Во всякой категории морфизм μ называется *регулярным слева* (*справа*), если $\mu\alpha = \mu\beta$ ($\alpha\mu = \beta\mu$) влечет $\alpha = \beta$. Показать, что в категории Gp регулярные слева морфизмы являются эпиморфизмами, а регулярные справа морфизмы — мономорфизмами. (Воспользоваться упражнением 5.)

7. Показать, что всякое упорядоченное множество A можно вложить в свободную структуру L таким образом, что упорядоченность в A индуцируется упорядоченностью структуры L.

8. Если дано некоторое многообразие $\mathscr{V}$ Ω-алгебр, то пусть F_X — свободная $\mathscr{V}$-алгебра над множеством X и для всякого $A \in \mathscr{V}$ обозначим через $A(X)$ свободное объединение (в $\mathscr{V}$) алгебр A и F_X. Показать, что каноническое отображение $A \to A(X)$ взаимно однозначно (алгебра $A(X)$ называется *расширением алгебры A, полученным присоединением неизвестных* $x \in X$).

ГЛАВА V

СТРУКТУРЫ С ОТНОШЕНИЯМИ И МОДЕЛИ

Понятие алгебры, развитое в главах II—IV, охватывает большинство алгебраических структур, встречающихся на практике, но существует несколько важных исключений. Так, хотя группы, кольца и векторные пространства относятся к алгебрам, ни упорядоченные группы, ни поля не удовлетворяют определению алгебры. Заметим, что упорядоченная группа является структурой с некоторыми операциями и, кроме того, одним отношением. Поле является структурой с «операциями», не всюду определенными. Как мы видели в § II.2, и упорядоченные группы, и поля формально можно было бы определить как алгебры, но лишь ценой некоторой искусственности. Для естественного обобщения наряду с операциями нужно иметь отношения, или, по крайней мере, одни отношения, поскольку оказывается, что операции могут быть получены как частный случай отношений. Кроме того, при записи определений некоторых структур могут понадобиться как неравенства, так и равенства. Их можно записать, если ввести логические символы, что приводит к рассмотрению классов алгебр, отличных от многообразий.

1. СТРУКТУРЫ С ОТНОШЕНИЯМИ НАД ОБЛАСТЬЮ ПРЕДИКАТОВ

Как и в главе II, возьмем сначала множество Ω таких символов, что каждому $\omega \in \Omega$ сопоставлено неотрицательное число $a = a(\omega)$. Однако вместо того, чтобы использовать ω для определения n-арной операции, мы хотим теперь дать более общее определение $(n+1)$-арного отношения. По этой причине в дальнейшем мы будем говорить об элементах из Ω как о *предикатах*, а не операторах, и называть Ω *областью предикатов*. Если $a(\omega) = m - 1$, то ω называется m-арным предикатом и говорят, что *арность* ω как предиката равна m. Как и раньше, положим $\Omega(n) = \{\omega \in \Omega \mid a(\omega) = n\}$.

Определение. *Структурой с отношениями* над областью предикатов Ω или короче Ω-*структурой* называется непустое множество M вместе с некоторым правилом, по которому каждому n-арному предикату $\omega \in \Omega$ сопоставляется n-арное отношение в M. Как и в алгебрах, множество M называется *носителем* Ω-структуры, и мы не будем вводить специального обозначения, чтобы различать структуру и ее носитель, так как предполагаемый смысл всегда будет ясен из контекста.

Поскольку n-арная операция является частным случаем $(n+1)$-арного отношения, то очевидно, что алгебры можно считать частным случаем структур с отношениями. Соответственно Ω-структура M называется *алгеброй относительно подобласти* Ω' области Ω, если для каждого $\omega \in \Omega'$ отношение в M, определенное предикатом ω, является операцией. В общем случае если ω_M — отношение в M, определенное предикатом $\omega \in \Omega(m-1)$, и $a \in M^m$, мы будем часто писать

$$M \models \omega(a)$$

и говорить, что $\omega(a)$ *выполняется* в M, если нужно указать, что $a \in \omega_M$. Если $\omega(a)$ выполняется для всех $a \in M^m$, мы будем говорить, что ω *истинно* в M, и писать

$$M \vdash \omega.$$

Чтобы указать, что $\omega(a)$ не выполняется в M, мы будем писать $M \sim\models \omega(a)$, и если ω не является истинным в M, то будем писать $M \sim\vdash \omega$; здесь нужно помнить, что $M \sim\vdash \omega$ не означает, что $M \sim\models \omega(a)$ для всех $a \in M^m$ (эта запись означает только, что $M \sim\models \omega(a)$ имеет место для некоторого a). Ω-структура M, в которой каждый предикат является истинным, называется *полной*; ясно, что такая структура полностью определяется своим носителем. Под *тривиальной* Ω-структурой будем понимать полную Ω-структуру, состоящую из одного элемента.

Рассмотрим две Ω-структуры M и N. Для любого $\omega \in \Omega$ отношения, определенные в M и в N предикатом ω, обозначим через ω_M и ω_N соответственно; далее, будем писать $m = a(\omega) + 1$. Будем говорить, что N — *подструктура* структуры M, если носитель структуры N является подмножеством носителя структуры M и

$$\omega_N = \omega_M \cap N^m \qquad (\omega \in \Omega(m-1);\ m = 1, 2, \ldots). \tag{1}$$

Пусть задана Ω-структура M. Если взять некоторое непустое подмножество N множества M и определить ω_N равенством (1), то мы, очевидно, получим Ω-структуру на N; итак, каждое подмножество $N\,(\neq \varnothing)$ Ω-структуры M можно однозначно определить как подструктуру в M, и если не оговорено противное, то под Ω-структурой на N мы всегда будем подразумевать эту Ω-структуру.

Отображение φ одной Ω-структуры M в другую N называется *гомоморфизмом* при условии, что для любых $\omega \in \Omega(m-1)$ и $a \in M^m$,

$$\text{если } M \models \omega(a), \text{ то } N \models \omega(a\varphi),$$

где $a\varphi = (a_1\varphi, \ldots, a_m\varphi)$, когда $a = (a_1, \ldots, a_m)$. Если отображение φ обладает обратным, которое также является гомоморфизмом, то будем называть φ *изоморфизмом* структур M и N; в этом случае будем также говорить, что M и N *изоморфны*, и писать $M \cong N$. Если M изоморфна подструктуре структуры N, то будем говорить, что M *вложима* в N. Термины «мономорфизм», «эпиморфизм», «эндоморфизм» и «автоморфизм» определяются аналогично случаю алгебр. Однако нужно отметить, что взаимно однозначный эпиморфизм не обязательно будет изоморфизмом, т. е. аналог леммы II. 3.6 не справедлив.

Если даны две Ω-структуры M и N, то будем говорить, что N есть *факторструктура* структуры N, если существует такой эпиморфизм θ: $M \to N$, что для любых $\omega \in \Omega(m-1)$ и $b \in N^m$

$$N \models \omega(b) \text{ тогда и только тогда, когда}$$

$$\text{существует такое } a \in M^m, \text{ что } a\theta = b \text{ и } M \models \omega(a).$$

Эти условия относительно θ вместе с Ω-структурой на M служат для однозначного определения Ω-структуры на N. Поэтому если M — некоторая Ω-структура и $\mathfrak{q}$ — эквивалентность на M, то фактормножество $M/\mathfrak{q}$ вместе с отображением $\mathrm{nat}\,\mathfrak{q}$ определяет единственную факторструктуру на $M/\mathfrak{q}$, и говоря о $M/\mathfrak{q}$ как о Ω-структуре, мы всегда будем подразумевать эту факторструктуру, если не оговорено противное.

Заметим, что любое произведение гомоморфизмов, если оно определено, снова будет гомоморфизмом; любое отображение в полную Ω-структуру является гомоморфизмом; и отображение полной Ω-структуры будет гомоморфизмом в том и только том случае, если образ будет полной Ω-структурой.

***Предложение* 1.1.** (i) *Пусть φ: $M \to N$ — гомоморфизм Ω-структур. Тогда N будет факторструктурой структуры M лишь в том случае, если φ — эпиморфизм, и Ω-структура на N является наименьшей Ω-структурой, при которой φ является гомоморфизмом.* (ii) *Факторструктура факторструктуры структуры M снова является факторструктурой структуры M (с точностью до изоморфизма).*

Доказательство утверждения (i) ясно из определений. Докажем (ii). Пусть N — факторструктура структуры M и P — факторструктура структуры N с эпиморфизмами α: $M \to N$, β: $N \to P$. Обозначим через P' наименьшую структуру с тем же носителем, что и P, при которой $\alpha\beta$ — гомоморфизм. Так как α, β — гомоморфизмы, то структура P' содержится в структуре P (как множество отношений), т. е. тождественное отображение носителя индуцирует гомоморфизм $P' \to P$. Пусть теперь $\omega \in \Omega(m-1)$ и $c \in P^m$ таковы, что $P \models \omega(c)$. Тогда по определению существует такое $b \in N^m$, что $b\beta = c$ и $N \models \omega(b)$, и, следовательно, существует такое $a \in M^m$, что $a\alpha = b$ и $M \models \omega(a)$. Теперь $a\alpha\beta = c$, поэтому $P' \models \omega(c)$, и это показывает, что гомоморфизм $P' \to P$, индуцируемый тождественным отображением, является изоморфизмом, т. е. P' и P равны. ∎

Пусть $(M_\lambda)_{\lambda \in \Lambda}$ — семейство Ω-структур; тогда декартово произведение $M = \prod M_\lambda$ с проекциями ε_λ: $M \to M_\lambda$ может быть превращено в Ω-структуру по следующему правилу:

$$M \models \omega(a) \text{ тогда и только тогда,} \\ \text{когда } M \models \omega(a\varepsilon_\lambda) \text{ для всех } \lambda \in \Lambda, \tag{2}$$

где $a \in M^m$, $\omega \in \Omega(m-1)$ $(m = 1, 2, \ldots)$. Иными словами, M несет наибольшую Ω-структуру, при которой все проекции являются гомоморфизмами.

2. БУЛЕВЫ АЛГЕБРЫ

Для дальнейшего изучения Ω-структур было бы полезно иметь аналог алгебры Ω-слов. Но можно считать, что алгебра Ω-слов над множеством X состоит из всех производных операторов, примененных к X. Аналогично в случае Ω-структур вводятся *производные предикаты*; однако множество этих предикатов будет не Ω-структурой, а алгеброй с операторами, совершенно не зависящими от Ω. Поэтому сначала будем изучать эти алгебры абстрактно; они названы в честь Дж. Буля, который впервые использовал их при систематическом изучении исчисления высказываний.

Сначала напомним, что структура L дистрибутивна тогда и только тогда, когда относительные дополнения в L (если они существуют) единственны (предложение II. 4.5). В частности, если L имеет 0 и 1 и каждый элемент x обладает дополнением x', то можно считать $x \to x'$ унарным оператором. Такая структура будет структурой с дополнениями в смысле следующего определения:

Определение. Структура L называется *структурой с дополнениями*, если она обладает наименьшим элементом 0 и таким унарным оператором $x \to x'$, что

$$x'' = x, \tag{1}$$

$$(x \vee y)' = x' \wedge y', \tag{2}$$

$$x \wedge x' = 0. \tag{3}$$

Ясно, что структуры с дополнениями образуют многообразие с операторами $\vee$, $\wedge$, $'$, 0, тождествами (1) — (3) вместе с тождествами структуры и тождеством

$$0 \vee x = x, \tag{4}$$

характеризующим 0 как наименьший элемент структуры L. Кроме того, в силу (1) и (2) один из операторов $\vee$, $\wedge$ может быть выражен через другой, так что структуры с дополнениями могут быть определены через одни только $\vee$, $'$, 0. Мы не будем этого выводить и отметим только некоторые следствия из (1) — (4).

В силу (4), $0 \leqslant x$ для всех $x \in L$, т. е.

$$0 \wedge x = 0. \tag{5}$$

Если мы положим $1 = 0'$, а (5) и (4) подставим в (2), то получим

$$1 \wedge x = x, \qquad 1 \vee x = 1. \tag{6}$$

Поэтому 1 оказывается наибольшим элементом структуры L. Далее, из (3) и (1) получаем

$$x \vee x' = 1. \tag{7}$$

Дадим теперь следующее

Определение. *Булевой алгеброй* называется дистрибутивная структура с дополнениями.

Из определения ясно, что булевы алгебры образуют многообразие. Кроме того, всякий монотонный изоморфизм между булевыми алгебрами является структурным изоморфизмом, и так как он переводит дополнительные пары в дополнительные пары, то имеет место

***Предложение* 2.1.** *Всякий монотонный изоморфизм между булевыми алгебрами является изоморфизмом булевых алгебр.* ∎

ПРИМЕРЫ БУЛЕВЫХ АЛГЕБР

(i) Множество $\mathscr{B}(A)$ всех подмножеств данного множества A будет булевой алгеброй, если взять $0 = \varnothing$ и, для $X \subseteq A$, $X' = A \setminus X$. Вообще всякая система подмножеств множества A, содержащая $\varnothing$ и замкнутая относительно дополнений и конечных объединений, будет булевой алгеброй; это просто подалгебра алгебры $\mathscr{B}(A)$, которая только что была определена (такая подалгебра называется *полем множеств* на A).

(ii) Во всяком интервале $I = [a, b]$ дистрибутивной структуры L множество элементов интервала I, обладающих дополнениями в I, образует булеву алгебру.

(iii) Двухэлементная структура является булевой алгеброй. Пусть a и b — элементы этой структуры и, скажем, $a \vee b = b$, тогда $a \leqslant b$, и эта структура превращается в булеву алгебру, если положить $a' = b$, $b' = a$. Эта структура будет обозначаться через 2.

(iv) Логика высказываний анализирует форму утверждений, которые могут быть сделаны в данном контексте. Если «P» и «Q» — некоторые высказывания, обозначенные символами p и q соответственно, то можно образовать высказывания «P и Q», «P или Q», «не P»; их можно обозначить через $p \wedge q$, $p \vee q$ и p' соответственно. С помощью этих определений множество высказываний становится булевой алгеброй при условии, что два высказывания считаются равными, если они имеют одно и то же значение истинности при любых обстоятельствах. Здесь в качестве наименьшего элемента 0 можно взять «никто не читает эту книгу в данный момент» или некоторое другое высказывание, про которое известно, что оно ложно.

Следующий пример является важным примером булевой алгебры. Пусть R — кольцо, в котором каждый элемент идемпотентен:

$$x^2 = x \quad \text{для всех} \quad x \in R. \tag{8}$$

Тогда $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$, откуда $xy + yx = 0$. Полагая $y = x$, находим $2x = 0$, т. е. $x = -x$, и поэтому

$$xy = yx.$$

Другими словами, каждое кольцо, удовлетворяющее условию (8), коммутативно и является кольцом характеристики 2. Предположим теперь, что, кроме того, R обладает единицей 1 и ассоциативно; если определить в R операции

$$x \wedge y = xy, \quad x' = 1 - x,$$

то R будет булевой алгеброй относительно этих операций с нулем кольца R в качестве наименьшего элемента. Проверка этого может быть предоставлена читателю. Обратно, во всякой булевой алгебре можно определить кольцевые операции, полагая

$$xy = x \wedge y, \quad x + y = (x \wedge y') \vee (x' \wedge y);$$

тогда полученная алгебра будет ассоциативным кольцом с 1, удовлетворяющим тождеству идемпотентности (8). Такое кольцо называется *булевым*; из этих определений видно, что булевы кольца полностью эквивалентны булевым алгебрам. Хотя мы будем пользоваться главным образом структурными операциями, полезно помнить о кольцевых операциях. Например, в кольце, порожденном множеством X, закон дистрибутивности позволяет нам представить каждый элемент в виде линейной комбинации произведений элементов множества X. Аналогично в булевой алгебре, порожденной множеством X, каждый элемент можно представить в виде точной верхней грани точных нижних граней элементов x и x' $(x \in X)$; в силу двойственности то же самое будет иметь место, если $\vee$ и $\wedge$ поменять местами.

Сформулируем это в виде следующего предложения.

***Предложение* 2.2. (*Конъюнктивная нормальная форма.*)** *Пусть B — булева алгебра, порожденная элементами $x_1, \ldots, x_n$; тогда каждый элемент алгебры B может быть представлен в виде $w_1 \wedge \ldots \wedge w_r$, где*

$$w_k = y_{k1} \vee \ldots \vee y_{kh_k}, \quad y_{kl} = x_i \quad \text{или} \quad x_i'. \ \blacksquare$$

Булева алгебра, полная как структура, называется *полной* булевой алгеброй. Например, $\mathscr{B}(A)$ полна для любого множества A; с другой стороны, подалгебра алгебры $\mathscr{B}(A)$, порожденная одиночками, не будет полной, если только множество A не будет конечным. Во всякой булевой алгебре, полной или неполной, имеют место следующие тождества, известные как *тождества де Моргана*:

***Предложение* 2.3.** *Пусть (a_i) — некоторое семейство элементов булевой алгебры B. Если в каждом из равенств*

$$(\bigvee a_i)' = \bigwedge a_i', \tag{9}$$

$$(\bigwedge a_i)' = \bigvee a_i' \tag{10}$$

одна из частей существует, то существует и вторая и обе части равны.

Доказательство. Предположим, что $a = \bigvee a_i$; тогда $a_i \leqslant a$ для всех $i \in I$ и, следовательно,

$$a' \leqslant a_i' \quad \text{для всех} \quad i \in I.$$

Если в то же время $b \leqslant a_i'$ для всех $i \in I$, то $b' \geqslant a_i$, откуда $b' \geqslant a$, и поэтому $b \leqslant a'$. Это показывает, что $a' = \bigwedge a_i'$, т. е. выполняется (9). Итак, (9) имеет место при условии, что левая часть равенства (9) существует; в силу двойственности (10) имеет место при условии, что левая часть равенства (10) существует. Предположим теперь, что существует правая часть равенства (9); тогда в силу доказанного относительно равенства (10) $\bigvee a_i'' = \bigvee a_i$ существует и (9) снова имеет место; (10) теперь получается аналогично. $\blacksquare$

Всякая булева алгебра удовлетворяет следующему бесконечному закону дистрибутивности:

$$\bigvee (a_i \wedge b) = (\bigwedge a_i) \wedge b \tag{11}$$

при условии, что обе части равенства существуют. Однако можно рассматривать более общий закон дистрибутивности, который не всегда имеет место. Будем говорить, что булева алгебра B *вполне дистрибутивна*, если для любого семейства элементов $(a_{ij})_{i \in I,\, j \in J}$

алгебры B как только одна из частей равенства

$$\bigwedge_I \left(\bigvee_J a_{ij}\right) = \bigvee_{\alpha \in J^I} \left(\bigwedge_I a_{i\alpha(i)}\right) \qquad (12)$$

существует, то существует и другая и обе части равны. Например, алгебра $\mathscr{B}(A)$ полна и вполне дистрибутивна для любого множества A. Следующий результат Тарского показывает, что это по существу единственный случай:

***Теорема* 2.4.** *Полная и вполне дистрибутивная булева алгебра изоморфна алгебре $\mathscr{B}(A)$ для некоторого множества A.*

Доказательство. Пусть B — данная алгебра. Запишем

$$1 = \bigwedge_{a \in B} (a \vee a').$$

Преобразуя правую часть в силу закона дистрибутивности, получаем

$$1 = \bigvee_{C \subseteq B} f(C), \qquad (13)$$

где для всякого $C \subseteq B$

$$f(C) = \left(\bigwedge_{a \in C} a\right) \wedge \left(\bigwedge_{b \notin C} b'\right).$$

Мы утверждаем, что каждое $f(C)$ есть либо 0, либо *атом*, т. е. минимальный элемент, отличный от 0. Действительно, если $f(C) \neq 0$ и $0 \neq c \leqslant f(C)$, то либо $c \in C$ и тогда $f(C) \leqslant c$, откуда $f(C) = c$, либо $c \notin C$ и тогда $f(C) \leqslant c'$, откуда $c \leqslant c'$, а это означает, что $c = c \wedge c' = 0$. Таким образом, в любом случае $f(C) = c$, так что и в самом деле $f(C)$ — атом.

Пусть A — множество всех $f(C) \neq 0$; покажем, что $B \cong \mathscr{B}(A)$. Каждому подмножеству множества A поставим в соответствие элемент алгебры B, а именно его точную верхнюю грань в B (которая существует, так как B полна); обратно, если $c \in B$, то $c = c \wedge (\bigvee f(C))$ в силу (13), откуда

$$c = \bigvee \{f(C) \mid f(C) \leqslant c\}.$$

Итак, имеем взаимно однозначное соответствие между B и $\mathscr{B}(A)$; ясно, что это соответствие сохраняет упорядоченность и поэтому является изоморфизмом. ∎

Заметим, что A — множество всех атомов алгебры B. В частности, если B конечна, то она, очевидно, полна и вполне дистрибутивна, и мы получаем

***Следствие* 2.5.** *Всякая конечная булева алгебра изоморфна $\mathscr{B}(A)$ для некоторого конечного множества A.* ∎

Рассмотрим теперь гомоморфизм булевых алгебр. Так как операции булевой алгебры могут быть выражены через операции булева кольца и наоборот, то отсюда вытекает, что гомоморфизмы булевых алгебр будут теми же самыми, что и гомоморфизмы булевых колец. В частности, ядро такого гомоморфизма

$$\varphi\colon A \to B$$

полностью определяется полным прообразом, скажем N, нуля. Поэтому будем называть N *идеалом* (как в теории колец), даже если мы рассматриваем A и B как булевы алгебры. Относительно структурных операций идеал определяется следующими свойствами:

(i) если $a, b \in N$, то $a \vee b \in N$,
(ii) если $a \in N$ и $b \leqslant a$, то $b \in N$.

Идеал называется *собственным*, если
(iii) $1 \notin N$.

Это последнее условие равносильно тому, что $N \neq A$. Полный прообраз единицы 1 при гомоморфизме называется *дуальным идеалом*; если этот идеал собственный, т. е. соответствует нетривиальному гомоморфизму, то он называется *фильтром* булевой алгебры A. Таким образом, фильтр определяется свойствами, двойственными вышеперечисленным свойствам (i) — (iii):

(i′) если $a, b \in F$, то $a \wedge b \in F$,
(ii′) если $a \in F$ и $b \geqslant a$, то $b \in F$,
(iii′) $0 \notin F$.

Пусть R — кольцо (не обязательно булево); тогда под *максимальным идеалом* понимают идеал кольца R, максимальный в множестве всех собственных идеалов кольца R. Если R обладает единицей 1, то собственными идеалами будут те и только те идеалы, которые не содержат 1. Таким образом, применяя следствие II.6.4, получаем следующую теорему:

Теорема 2.6. (**Крулль.**) *Каждый собственный идеал кольца с 1 содержится в максимальном идеале.* ∎

В частности, этот результат можно применить к булевым алгебрам. Максимальный фильтр в булевых алгебрах обычно называется *ультрафильтром*; таким образом, переходя в теореме 2.6 к двойственным понятиям, получаем следующую теорему:

Теорема 2.7. *Каждый фильтр булевой алгебры содержится в ультрафильтре.* ∎

Максимальные идеалы в булевых алгебрах можно охарактеризовать другим способом, который имеет большое значение. Этот способ основывается на том факте, что простые булевы алгебры могут быть очень просто описаны явным образом.

Предложение **2.8.** *Булева алгебра проста тогда и только тогда, когда она изоморфна булевой алгебре* 2.

В самом деле, ясно, что 2 проста; обратно, если A проста, то $A \neq 0$ и A не имеет собственных гомоморфных образов, т. е. не имеет никаких идеалов, кроме 0 и A. Пусть $a \in A$, $a \neq 0$; тогда идеал, порожденный a, должен быть ненулевым, и поэтому он совпадает с A, откуда $ab = 1$ для некоторого $b \in A$. Следовательно, $a = a(ab) = a^2b = ab = 1$. Этим показано, что $A = \{0, 1\} = 2$, как и утверждалось. ▌

Итак, мы получили важное

Следствие **2.9.** (*Тарский.*) *Пусть I—идеал булевой алгебры A; I является максимальным тогда и только тогда, когда $A/I \cong 2$.* ▌

На языке самой алгебры A это означает, что идеал I максимален в A тогда и только тогда, когда для каждого $a \in A$ либо $a \in I$, либо $a' \in I$. Переходя к двойственному утверждению, видим, что ультрафильтры булевой алгебры A характеризуются тем же свойством.

В дальнейшем мы будем иметь дело главным образом с фильтрами алгебр вида $\mathscr{B}(A)$. Если I — некоторое множество, то под фильтром $\mathscr{F}$ на I будем понимать систему подмножеств множества I, являющуюся фильтром булевой алгебры $\mathscr{B}(I)$. Члены фильтра $\mathscr{F}$ будут называться также $\mathscr{F}$-множествами. Подсистема $\mathscr{S}$ фильтра $\mathscr{F}$, которая порождает $\mathscr{F}$ (как фильтр), называется *базой* фильтра $\mathscr{F}$. Чтобы получить дуальный идеал, порожденный системой $\mathscr{S}$, образуем систему $\mathscr{S}^*$, состоящую из пересечений всевозможных конечных подсистем системы $\mathscr{S}$, и возьмем все множества, содержащие некоторое $\mathscr{S}^*$-множество. Полученный дуальный идеал будет фильтром в том и только том случае, если $\varnothing \notin \mathscr{S}^*$. Если это условие выполняется, то говорят, что $\mathscr{S}$ обладает *свойством конечных пересечений*. Таким образом, $\mathscr{S}$ является базой фильтра тогда и только тогда, когда $\mathscr{S}$ обладает свойством конечных пересечений.

Пусть I — бесконечное множество мощности α, и через Φ обозначим систему всех подмножеств множества I, дополнение которых в I имеет мощность, меньшую чем α. Ясно, что Φ — фильтр на I, называемый *минимальным фильтром Фреше*. Под *фильтром Фреше* на I мы понимаем всякий фильтр, содержащий Φ. Иногда нам нужно будет знать, когда данная база некоторого фильтра содержится в фильтре Фреше. На этот вопрос дает ответ

Предложение **2.10.** *Система $\mathscr{S}$ подмножеств множества I содержится в некотором фильтре Фреше тогда и только тогда, когда каждое пересечение конечного числа множеств системы $\mathscr{S}$ имеет мощность, равную $|I|$.*

Действительно, ясно, что $\mathcal{S}$ содержится в некотором фильтре Фреше тогда и только тогда, когда $\mathcal{S} \cup \Phi$ — база фильтра, т. е. тогда и только тогда, когда каждое $\mathcal{S}^*$-множество пересекается с каждым Ф-множеством, где через $\mathcal{S}^*$ снова обозначена система всех пересечений конечного числа множеств системы $\mathcal{S}$. Однако подмножество J множества I пересекается с каждым Ф-множеством тогда и только тогда, когда дополнение произвольного Ф-множества не содержит J, т. е. тогда и только тогда, когда $|J| = |I|$. ∎

Фильтр $\mathcal{F}$ на I называется *главным*, если он порождается одним элементом, скажем J. Ясно, что такой фильтр будет ультрафильтром в том и только том случае, если J состоит из одного элемента, и на конечном множестве I эти фильтры будут единственными ультрафильтрами. Бесконечное множество всегда обладает неглавными ультрафильтрами, поскольку, например, минимальный фильтр Фреше содержится в ультрафильтре, который будет неглавным. Однако это доказательство существования неглавных ультрафильтров существенно зависит от леммы Цорна, и неизвестно никаких явных конструкций неглавных ультрафильтров.

Этого краткого обзора теории булевых алгебр будет достаточно для тех приложений, которые мы имеем в виду; конечно, наш обзор не претендует на полноту в каком-либо смысле или хотя бы на систематичность отбора результатов. Мы отсылаем читателя, желающего прочитать более подробное введение, к книге Двингера [61] или для более детального ознакомления к книге Сикорского [60]; работы Халмоша [62] посвящены вопросам, особенно важным для приложений к логике, включая иное изложение содержания этого параграфа.

УПРАЖНЕНИЯ

1. Записать систему тождеств булевых алгебр относительно $(\vee, ', 0)$.

2. Пусть R — коммутативное кольцо с 1. Через I обозначим множество идемпотентов кольца R. Показать, что I будет булевой алгеброй относительно операций $x \wedge y = xy$, $x' = 1 - x$. Операции I, как в булевом кольце, выразить через кольцевые операции на R. При каких условиях I, как булево кольцо, будет подкольцом кольца R?

3. Доказать (11) в полной булевой алгебре; вообще доказать тождество $(\bigwedge a_i) \vee (\bigwedge b_j) = \bigwedge (a_i \vee b_j)$.

4. Описать все полные подалгебры булевой алгебры $\mathcal{B}(I)$ для любого множества I.

5. Проверить, что если I — бесконечное множество и $\mathcal{F}$ — система всех конечных подмножеств множества I, то $\mathcal{F}$ — идеал в $\mathcal{B}(I)$. Проверить, что алгебра $\mathcal{B}(I)/\mathcal{F}$ не имеет атомов; показать, что $\mathcal{B}(I)/\mathcal{F}$ полна, но не вполне дистрибутивна.

6. (Стоун.) Показать, что пересечение всех максимальных идеалов булевой алгебры равно 0. Вывести отсюда, что всякая булева алгебра B изоморфна подалгебре алгебры $\mathcal{B}(M)$, где в качестве M можно взять множество всех максимальных идеалов алгебры B. (Заметить, что если $a \neq 0$, то

любой максимальный идеал, содержащий a', не содержит a; применить теперь предложение II. 7.1.)

7. Показать, что базисный ранг для булевых алгебр равен нулю, т. е. что 2 порождает многообразие булевых алгебр. (Использовать упражнение 6.)

8. Показать, что каждая конечнопорожденная булева алгебра конечна. (Воспользоваться следствием IV. 3.14.)

9. Показать, что любые две конечные булевы алгебры с одним и тем же числом элементов изоморфны. (Воспользоваться следствием 2.5 и предшествующим ему замечанием.)

10. Показать, что любые две счетно бесконечные булевы алгебры без атомов изоморфны.

11. Показать, что свободная булева алгебра с k свободными образующими имеет 2^{2^k} элементов. (Взять множество I из k элементов и показать, что любое отображение $\mathscr{B}(I) \to 2$ можно построить при помощи булевых операций из характеристических функций на одиночках; затем применить теорему IV. 3.13.)

12. (Фостер.) Показать, что конечная булева алгебра n-примальна для каждого n. (Воспользоваться упражнением 11 и теоремой IV. 3.13.)

13. Привести пример недистрибутивной структуры с дополнениями и показать, что предложение 2.1 не всегда выполняется для таких структур. (Рассмотреть конечную модулярную структуру длины 2.)

14. Показать, что за единственным исключением конечные структуры с дополнениями имеют четное число элементов.

15. В булевой алгебре B отображение $x \to x'$ является изоморфизмом алгебры B с двойственной к ней алгеброй. Переформулировать этот факт для булевых колец.

16. Показать, что всякий неглавный ультрафильтр на бесконечном множестве содержит все подмножества с конечными дополнениями. Вывести отсюда, что на счетном множестве каждый неглавный ультрафильтр будет фильтром Фреше.

17. Показать, что если A — направленное множество, то правые отрезки множества A обладают свойством конечных пересечений.

18. Показать, что если G — группа с тривиальным центром, то прямые множители группы G образуют булеву алгебру.

19. Показать, что если C — некоторая подалгебра булевой алгебры B, то всякий гомоморфизм $\varphi: C \to 2$ продолжается до гомоморфизма $\bar{\varphi}: B \to 2$. (Вложить $\ker \varphi$ в максимальный идеал алгебры B и воспользоваться следствием 2.9.)

20. (Двингер и Якуб [63].) Показать, что существует свободное произведение любого семейства булевых алгебр, являющихся расширениями фиксированной булевой алгебры C. (Воспользоваться упражнением 19, чтобы доказать, что если $C = 2$, то всякая булева алгебра сжимаема, и применить предложение III. 6.2; для общего случая воспользоваться первой частью упражнения 6.)

3. ПРОИЗВОДНЫЕ ПРЕДИКАТЫ

Ω-структуры обладают значительно более слабой «структурой», чем Ω-алгебры; это можно увидеть уже из того факта, что каждое подмножество и каждое фактормножество Ω-структуры снова являются носителями Ω-структуры. Поэтому необходимо ограничить понятие Ω-структуры, налагая дополнительные условия. Простейшая форма, которую может принять такое условие, состоит в утверждении, что данный предикат истинен в данной структуре. В более общем случае мы можем построить из данных предикатов другие производные предикаты, и наши условия могут тогда принять форму утверждения истинности некоторых производных предикатов.

Множество производных предикатов будет определено как некоторая булева алгебра следующим образом. Пусть I — бесконечное множество символов, называемых *переменными*, и рассмотрим выражения

$$\varepsilon(i, j) \quad (i, j \in I), \tag{1}$$

$$\omega(i_1, \ldots, i_m) \quad (i_k \in I, \ \omega \in \Omega(m-1)). \tag{2}$$

Теперь производным Ω-предикатом будет по существу элемент свободной булевой алгебры над выражениями (1), (2) в качестве свободных образующих. Это утверждение требует некоторого видоизменения для того, чтобы принять в расчет кванторы. Прежде чем вводить их, дадим несколько определений, которые, хотя и не являются необходимыми, но полезны, так как предвосхищают те понятия, которые будут определены позже.

Производный предикат называется также *формулой*; формула вида (1) или (2) называется *атомной*. Если P и Q — некоторые формулы, то $P \vee Q$ называется *дизъюнкцией* формул P и Q, $P \wedge Q$ называется их *конъюнкцией* и P' — *отрицанием* формулы P; отрицание обозначается также через $\sim P$. Всякая формула, построенная из атомных формул с помощью одних только $\vee$ и $\wedge$ (без $\sim$), называется *положительной*. Далее, $P' \vee Q$ обозначается также через $P \Rightarrow Q$ и называется *импликацией*, а $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$ обозначается через $P \Leftrightarrow Q$ и называется *эквивалентностью*. Вместо 1 и 0 будем писать t и f соответственно («правда» и «ложь»).

Прежде чем мы сможем описать отношения, соответствующие этим предикатам, нужно определить арность каждого предиката. Каждой формуле P сопоставим конечное множество I_P переменных, называемых *свободными переменными* формулы P; тогда арность формулы P определяется как число ее свободных переменных. Множество I_P свободных переменных формулы P определяется индуктивно по ее длине (как слова в булевой алгебре формул). Для атомной формулы (1) свободными переменными будут i, j, а для (2) — $i_1, \ldots, i_m$. Поэтому, в частности, арность формулы (2) равна m тогда и только тогда, когда переменные, встречающиеся в ω, различны; это показывает, что при употреблении этого термина не будет никакой двусмысленности. Вообще если P и Q — некоторые формулы и I_P, I_Q — множества их свободных переменных, то для $P \vee Q$ и $P \wedge Q$ множеством свободных переменных будет $I_P \cup I_Q$, а для $\sim P$ множеством свободных переменных будет I_P.

Введем теперь еще два оператора на множестве формул; это будут унарные операторы $\bigvee\limits_i$, $\bigwedge\limits_i$, называемые *квантором существования* и *квантором общности* относительно i. Итак, для каждого $i \in I$ определен один квантор существования $\bigvee\limits_i$ и один квантор общности $\bigwedge\limits_i$. Они связаны равенством

$$\bigwedge_i P = \sim\Big(\bigvee_i \sim P\Big), \tag{3}$$

которое показывает, что каждый из них определяется другим. Потребуем также выполнения тождеств

$$\begin{gathered}\bigvee_i \bigvee_i P = \bigvee_i P, \quad \bigvee_i \bigvee_j P = \bigvee_j \bigvee_i P, \\ \Big(\bigvee_i P\Big) \vee \Big(\bigvee_i Q\Big) = \bigvee_i (P \vee Q)\end{gathered} \tag{4}$$

и двойственных тождеств, полученных из (4) применением (3). Таким образом, наше множество производных предикатов расширяется путем присоединения формул с кванторами. Будем пользоваться тем же термином «формула» для обозначения любого производного предиката в новом смысле, тогда как предикат в прежнем смысле, т. е. без кванторов, будем теперь называть *открытой формулой*. Если I_P — множество свободных переменных формулы P, то множеством свободных переменных формулы $\bigvee\limits_i P$ $\Big($или $\bigwedge\limits_i P\Big)$ будет $I_P \setminus \{i\}$. Всякое переменное, участвующее в формуле не так, как свободное переменное, называется *связанным*; например i связано в $\bigvee\limits_i P$. Конечно, переменное может быть одновременно и свободным, и связанным: если i свободно в P и Q, то i связано в $\bigvee\limits_i P$ и, следовательно, одновременно свободно и связано в $\Big(\bigvee\limits_i P\Big) \wedge Q$. В таких случаях, чтобы избежать недоразумений, всегда можно переименовать i, входящее как связанное переменное, т. е. вместо

$$\Big(\bigvee_i P(i)\Big) \wedge Q(i) \tag{5}$$

можно рассматривать

$$\Big(\bigvee_j P(j)\Big) \wedge Q(i), \tag{6}$$

где $j \in I$ не участвует ни в P, ни в Q. Когда мы перейдем к определению отношений, соответствующих (5) и (6), то увидим, что между ними нет никакого различия (точно так же, как тождества от различных переменных могут быть эквивалентными, см. § IV.1).

Наконец, формула без свободных переменных называется *элементарным предложением* или просто *предложением*. Примерами предложений являются t, f и формулы, полученные связыванием свободных переменных, т. е. применением каких-либо кванторов ко всем свободным переменным в некоторой формуле.

Пусть P—формула со свободными переменными $I_P = \{i_1, \ldots, i_n\}$; запишем это в виде $P(i_1, \ldots, i_n)$ или $P(I_P)$ и в каждой Ω-структуре M определим n-арное отношение, соответствующее формуле P. Если P атомна, то P имеет вид (1) или (2). В первом случае для любых a, $b \in M$ положим

$$M \models \varepsilon(a, b) \text{ тогда и только тогда, когда } a = b.$$

По этой причине обычно будем писать $i = j$ вместо $\varepsilon(i, j)$. Когда P имеет вид (2), значение формулы $P(a_1, \ldots, a_n)$ $(a_k \in M)$ задано определенной на M Ω-структурой. Пусть теперь P и Q—некоторые формулы с множествами свободных переменных I_P, I_Q, для которых отношения в M уже определены, и пусть θ: $I_P \cup I_Q \to M$ — произвольное отображение; тогда положим

$$M \models P(I_P\theta) \vee Q(I_Q\theta) \text{ тогда и только тогда,}$$
$$\text{когда } M \models P(I_P\theta) \text{ или } M \models Q(I_Q\theta),$$

и

$$M \models \sim P(I_P\theta) \text{ тогда и только тогда,}$$
$$\text{когда } M \sim\models P(I_P\theta).$$

В частности, $M \models \sim\varepsilon(a, b)$ тогда и только тогда, когда $a \neq b$; по этой причине обычно будем писать $i \neq j$ вместо $\sim\varepsilon(i, j)$. Наконец, положим

$$M \models \bigvee_i P(I_P\theta) \text{ тогда и только тогда,}$$
$$\text{когда } M \models P(I_P\theta') \text{ для некоторого отображения}$$
$$\theta'\colon I_P \to M, \text{ при котором } j\theta = j\theta' \text{ для } j \neq i.$$

Итак, если $I_P = \{i_1, \ldots, i_n\}$ и $i = i_1$, то $M \models \bigvee_i P(i, a_2, \ldots, a_n)$ тогда и только тогда, когда $M \models P(b, a_2, \ldots, a_n)$ для некоторого $b \in M$. Положим также

$$M \models t.$$

Теперь для любой формулы с n различными свободными переменными индукцией по длине слов определяется n-арное отношение в M. Таким образом, в частности, определено действие операторов $\wedge$, $\Rightarrow$, $\Leftrightarrow$ и $\bigwedge$. Часто бывает удобно в качестве θ брать отображение всего I в M и писать $P\theta$ вместо $P(I_P\theta)$; легко проверить, что в этих обозначениях

$M \models P\theta \wedge Q\theta$ тогда и только тогда, когда $M \models P\theta$ и $M \models Q\theta$;

$M \models P\theta \Rightarrow Q\theta$ тогда и только тогда, когда $M \models Q\theta$, как только $M \models P\theta$;

$M \models P\theta \Leftrightarrow Q\theta$ тогда и только тогда, когда либо в M выполняются и $P\theta$ и $Q\theta$, либо не выполняются ни $P\theta$, ни $Q\theta$;

$M \models \bigwedge_i P\theta$ тогда и только тогда, когда $M \models P\theta'$ для любого отображения $\theta'\colon I \to M$, при котором $j\theta' = j\theta$ для всех $j \neq i$.

Отметим также, что f никогда не выполняется в M и что предложение P истинно в M тогда и только тогда, когда $M \models P \Leftrightarrow t$. Кроме того, если предложение выполняется в M, то оно истинно в M. Итак, для любого предложения P

$$\text{либо } M \vdash P, \text{ либо } M \vdash \sim P.$$

Из любой формулы мы получим предложение, если применим квантор общности ко всем свободным переменным. Будем обозначать это, приписывая впереди $\bigwedge$. Тогда для любой формулы P

$$M \vdash P \text{ тогда и только тогда, когда } M \models \bigwedge P.$$

Два предложения P, Q эквивалентны в M (в обозначениях $M \vdash P \Leftrightarrow Q$) в том и только том случае, если

$$M \vdash P \text{ тогда и только тогда, когда } M \vdash Q.$$

Это означает, что если речь идет об M, то всякое предложение P может быть заменено эквивалентным предложением Q. Например, предложения, полученные применением кванторов общности к (5) и (6), эквивалентны в любой Ω-структуре. Те пары предложений, которые эквивалентны в любой Ω-структуре, обычно отождествляются. Это приводит к рассмотрению не булевой алгебры производных предикатов, а некоторого ее гомоморфного образа. Определяющие соотношения этой алгебры обычно имеют форму тождеств, так что в действительности мы имеем дело с относительно свободной булевой алгеброй. Определяющие тождества этого многообразия называются *тавтологиями*; нетрудно видеть, что всякая тавтология является следствием тавтологий вида

$$P = t,$$

и всякое предложение P, встречающееся в каком-либо тождестве этого вида, также называется тавтологией. Подробное изучение множеств определяющих тождеств для тавтологий относится к исчислению предикатов (см. Клини [51], Чёрч [56]). Не вдаваясь в подробности, отметим только, что каждое из тождеств определенной выше булевой алгебры в действительности соответствует тавтологии, что и нужно проверить; эту задачу можно предоставить читателю. *В дальнейшем мы ограничимся рассмотрением булевой алгебры производных предикатов и ее действием на Ω-структурах.* Иными словами, нас будет интересовать семантическая сторона исчисления предикатов, а именно конкретная интерпретация формул, определенная выше, а не синтаксическая сторона этого исчисления, в которой делаются выводы об истинности формул по их внутренней структуре.

Мимоходом отметим, что из определения гомоморфизма как отображения, сохраняющего Ω-предикаты, вытекает, что гомоморфизм не всегда сохраняет производные предикаты. Этим объясняется тот факт, что в структурах с отношениями гомоморфизмы играют подчиненную роль; мы вернемся к этому в § VI. 5.

Предложение вида

$$(i_1) \ldots (i_n) P(i_1, \ldots, i_n),$$

где $P(i_1, \ldots, i_n)$ — открытая формула со свободными переменными $i_1, \ldots, i_n$ и (i_r) — некоторый квантор, поставленный вместо $\bigwedge$ или $\bigvee$, называется *пренексным предложением* или предложением в *пренексной нормальной форме*. Можно показать, что каждое предложение эквивалентно некоторому предложению в пренексной нормальной форме. *Это не очень трудно, но мы ограничимся примером.* Так, предложение

$$\bigwedge_i \bigwedge_j [R(i, j) \vee R(j, i)] \wedge \left[\bigvee_i \sim R(i, i)\right] \tag{7}$$

в том виде, как оно записано, не является предложением в пренексной нормальной форме, но оно эквивалентно пренексному предложению

$$\bigwedge_i \bigwedge_j \bigvee_k [R(i, j) \vee R(j, i)] \wedge [\sim R(k, k)]. \tag{8}$$

Из определений видно, что любой квантор существования можно выразить через квантор общности и наоборот, но при этом свойство быть пренексным обычно теряется. Поэтому тип квантора в пренексном предложении, вообще говоря, нельзя варьировать по желанию. Пренексное предложение называется *универсальным*, если все его кванторы являются кванторами общности, и *экзистенциальным*, если все его кванторы являются кванторами существования. В частности, пренексное предложение, полученное из открытой формулы применением $\bigwedge$ ($\bigvee$), называется его *универсальным* (*экзистенциальным*) *замыканием*.

УПРАЖНЕНИЯ

1. Показать, что отношение $P \Rightarrow Q$ между производными предикатами является предупорядоченностью, а $P \Leftrightarrow Q$ — соответствующей эквивалентностью.

2. Проверить, что определяющие тождества булевых алгебр и (4) являются тавтологиями, т. е. что обе стороны соответствующих равенств определяют одни и те же отношения в любом случае. Показать также, что

$$\left(\bigvee_i P\right) \wedge \left(\bigvee_i Q\right) = \bigvee_i (P \wedge Q)$$

в общем случае не является тавтологией.

3. Показать, что предложения образуют подалгебру S алгебры всех производных предикатов и что для всякой Ω-структуры M предложения, которые не выполняются в M, образуют максимальный идеал $\mathfrak{q}$ в S. (Проверить, что $S/\mathfrak{q} \cong 2$.)

4. ЗАМКНУТЫЕ КЛАССЫ ПРЕДЛОЖЕНИЙ И АКСИОМАТИЗИРУЕМЫЕ КЛАССЫ МОДЕЛЕЙ

Впредь будем считать Ω фиксированной областью предикатов; при этом подразумевается, что носители всех встречающихся Ω-структур принадлежат универсальному множеству U, фиксированному раз и навсегда. Если M — некоторая Ω-структура и P — формула в стандартном алфавите I над Ω, то было определено отношение

$$M \models P. \qquad (1)$$

Таким путем мы получаем соответствие Галуа между классом $[\Omega]$ всех Ω-структур и множеством $\overline{\Omega}_I$ всех производных предикатов (в I). В силу этого соответствия

(i) любому классу $\mathscr{C}$ Ω-структур соответствует множество $\mathscr{C}^*$ всех формул, истинных в каждой Ω-структуре $M \in \mathscr{C}$;

(ii) любому множеству Σ формул соответствует класс Σ^* всех тех Ω-структур, в которых все формулы из Σ истинны.

Всякая Ω-структура из Σ^* называется *моделью* для Σ или Σ-*моделью*; всякое предложение из $\mathscr{C}^*$ называется *теоремой* в $\mathscr{C}$ или $\mathscr{C}$-*теоремой*. Отметим, что не все формулы из $\mathscr{C}^*$ являются $\mathscr{C}$-теоремами, а только те, которые не имеют свободных переменных. С другой стороны, $\mathscr{C}^*$ полностью определяется своими теоремами, поскольку формула P принадлежит $\mathscr{C}^*$ тогда и только тогда, когда ее универсальное замыкание является $\mathscr{C}$-теоремой.

Класс Ω-структур вида Σ^* для некоторого множества Σ предложений называется *аксиоматизируемым классом*, а Σ называется множеством *аксиом*. Если Σ конечно, то класс Σ^* называется *элементарным*; заменяя конечное множество Σ конъюнкцией его элементов, видим, что элементарный класс всегда может быть определен одной аксиомой. Множество формул вида $\mathscr{C}^*$, где $\mathscr{C}$ — некоторый класс Ω-структур, называется *модельно-замкнутым*; если $\mathscr{C} \neq \varnothing$, то множество $\mathscr{C}^*$ называется *теорией*. Соответствие Галуа, определенное отношением (1), можно теперь описать в теореме:

Теорема 4.1. *Модельно-замкнутые множества формул над Ω образуют систему замыканий множеств, которым посредством естественного взаимно однозначного соответствия*

$$\Sigma \to \Sigma^*, \quad \mathscr{C} \to \mathscr{C}^*$$

сопоставлены аксиоматизируемые классы Ω-структур. ∎

Заметим, что модельно-замкнутое множество будет теорией тогда и только тогда, когда оно является собственным подмножеством множества $\overline{\Omega}_I$. Действительно, теория Σ истинна для некоторой модели и, следовательно, $f \notin \Sigma$; обратно, модельно-замкнутое множество, не являющееся теорией, имеет вид $\varnothing^* = \overline{\Omega}_I$. Эквивалентно этому Σ будет теорией тогда и только тогда, когда $f \notin \Sigma$.

При изучении структур с отношениями решающее значение имеет тот факт, что система модельно-замкнутых множеств образует алгебраическую систему замыканий. В формальной логике это доказывается определением в явном виде множества конечноместных операторов. Эти операторы имеют вид правил вывода (позволяющих выводить новые истинные формулы из данных):

(i) Если $M \vdash (P \Rightarrow Q)$ и $M \vdash P$, то $M \vdash Q$.

(ii) Если $M \vdash P$, то $M \vdash \bigwedge_i P$.

Связь с моделями устанавливается теоремой Гёделя о полноте, которая утверждает, что множество формул, замкнутое относительно правил вывода и являющееся собственным подмножеством множества $\overline{\Omega}_I$, обязательно обладает моделью. Полное изложение этих вопросов, включая доказательство теоремы Гёделя, можно найти у Чёрча [56].

Здесь мы не будем доказывать теорему Гёделя, поскольку в § V. 5 будет дано независимое доказательство того факта, что модельно-замкнутые множества образуют алгебраическую систему замыканий. Сейчас мы лишь укажем, каким образом из теоремы Гёделя вытекает, что всякое множество формул, замкнутое относительно правил вывода, модельно-замкнуто.

Пусть Σ — множество формул, замкнутое относительно всех правил вывода; нам нужно показать, что $\Sigma = \Sigma^{**}$. Так как, очевидно, $\Sigma \subseteq \Sigma^{**}$, то нужно только доказать, что $\Sigma^{**} \subseteq \Sigma$; итак, если задана некоторая формула $P \notin \Sigma$, то нужно найти модель для Σ, в которой P не будет истинной. Здесь, не ограничивая общности, можно считать P предложением; тогда нам нужно найти модель для $\Sigma \cup \{\sim P\}$. В силу теоремы Гёделя достаточно показать, что не всякое предложение может быть выведено из $\Sigma \cup \{\sim P\}$. Предположим, что f может быть выведено из Σ и $\sim P$. В силу конечного характера правил вывода отсюда вытекает, что f можно вывести из $S_1, \ldots, S_n, \sim P$ $(S_i \in \Sigma)$. Применяя теорему дедукции (см. Чёрч [56], стр. 186; это по существу обращение правила вывода (i)), находим, что из $S_1, \ldots, S_n$ можно вывести $(\sim P) \Rightarrow f$, а так как Σ замкнуто относительно правил вывода, то $[(\sim P) \Rightarrow f] \in \Sigma$, но

$$[(\sim P) \Rightarrow f] = [(\sim \sim P) \vee f] = P \vee f = P;$$

итак, $P \in \Sigma$, что противоречит выбору формулы P. ∎

Так как замкнутое множество формул замкнуто относительно всех правил вывода, то отсюда вытекает, что модельно-замкнутыми множествами являются в точности те множества, которые замкнуты относительно правил вывода. Такое положение вещей (так же как и сама теорема Гёделя) имеет место только в исчислении предикатов первой ступени. В более общих ситуациях, таких, как исчисление предикатов второй ступени, где кванторы могут применяться к предикатным переменным, система замыканий, состоящая из модельно-замкнутых множеств формул, не будет *больше алгебраической* и поэтому не может быть описана правилами вывода конечного характера. Здесь подразумевается, что во всякой модели переменные n-арные предикаты определены *для всех* наборов из n элементов (что приводит к понятию так называемой *стандартной модели*).

Если допускаются более общие модели, где предикаты могут быть определены лишь для некоторых вполне определенных наборов из n элементов, то снова имеет место аналог теоремы Гёделя о полноте и так же, как и выше, отсюда следует, что система замыканий, состоящая из модельно-замкнутых множеств, будет алгебраической (см. Хенкин [50]). Однако знаменитая теорема Гёделя о неполноте (см., например, Клини [52]) утверждает, что для всякого непротиворечивого множества формул, обладающего моделью целых чисел, существуют предложения P, которые неразрешимы в том смысле, что ни P, ни $\sim P$ не могут быть выведены из формул этой системы. Итак, для всякой аксиоматизируемой системы, содержащей целые числа, существуют некоторые (неэлементарные) предложения, которые выполняются во всех стандартных моделях, но недоказуемы и поэтому не выполняются во всех моделях.

Соответствие Галуа, описанное в теореме 4.1, может быть использовано в двух направлениях: либо для изучения строения формул над Ω с помощью их моделей, либо для изучения Ω-структур посредством их теорем. Однако этот метод несколько ограничен; так, он не дает возможности различать две формулы, имеющие одни и те же модели, или две Ω-структуры, имеющие одни и те же теоремы. Поэтому введем определения:

(i) Две формулы P и Q называются *конгруэнтными*, $P \approx Q$, если для каждой Ω-структуры M и каждого отображения θ: $I \to M$

$$M \models P\theta \text{ тогда и только тогда, когда } M \models Q\theta.$$

(ii) Две Ω-структуры M и N называются *элементарно эквивалентными* или *неразличимыми*, $M \equiv N$, если

$$M \vdash P \text{ тогда и только тогда, когда } N \vdash P \text{ для всех } P \in \bar{\Omega}_I.$$

Очевидно, для элементарной эквивалентности достаточно выяснить, выполняется ли это последнее условие для всех предложений P. Так как для любого предложения P либо $M \vdash P$, либо $M \vdash \sim P$, то отсюда вытекает, что $M \equiv N$, если $N \vdash P$, как только $M \vdash P$.

Легко проверить, что отношение $\approx$, ограниченное на подалгебре всех предложений, будет эквивалентностью и на самом деле конгруэнцией, т. е. если $P_1 \approx Q_1$ и $P_2 \approx Q_2$, то $P_1 \wedge P_2 \approx Q_1 \wedge Q_2$ и $\sim P_1 \approx \sim Q_1$. Факторалгебра по этой конгруэнции обозначается через $\mathscr{L}(\Omega)$ и называется *алгеброй Линденбаума* над Ω. Ее элементы обычно будут обозначаться строчными греческими буквами; будем также писать (P) для обозначения класса этой конгруэнции, содержащего предложение P, и положим $M \vdash \alpha$, чтобы обозначить $M \vdash P$ для некоторого (и, следовательно, для всех) $P \in \alpha$. Свойства алгебры $\mathscr{L}(\Omega)$ собраны в следующей теореме:

***Теорема* 4.2.** *Алгебра Линденбаума $\mathscr{L}(\Omega)$ является булевой алгеброй, гомоморфным образом алгебры всех предложений над Ω. Каждый элемент алгебры $\mathscr{L}(\Omega)$ определяет элементарный класс моделей, и различные элементы алгебры $\mathscr{L}(\Omega)$ определяют различные классы моделей. Далее, если $\alpha, \beta \in \mathscr{L}(\Omega)$, то*

$$\alpha \leqslant \beta \text{ *тогда и только тогда, когда* } M \vdash \beta$$

$$\text{*для любой такой структуры* } M, \text{ *что* } M \vdash \alpha.$$

Доказательства требует только последнее утверждение теоремы. Утверждение, что $M \vdash \beta$, как только $M \vdash \alpha$, означает, что $M \vdash \alpha$ тогда и только тогда, когда $M \vdash \alpha \wedge \beta$, т. е. $\alpha = \alpha \wedge \beta$, а это как раз и означает, что $\alpha \leqslant \beta$. ∎

Вместо $\mathscr{L}(\Omega)$ можно было бы рассматривать $\bar{\Omega}_I$, булеву алгебру всех производных предикатов, но тогда нужно принимать в расчет дополнительную структуру, появляющуюся благодаря присутствию кванторов. Получающиеся при этом структуры называются *полиадическими алгебрами* и изучались Халмошем [62] и другими. При построении в такой структуре отношения равенства $=$ получаются по существу *цилиндрические алгебры* Тарского (см. Хенкин и Тарский [61]); краткую сводку определений, а также о связи между этими двумя понятиями см. Геллер [57].

Возвращаясь к (ii), видим, что $\equiv$ будет эквивалентностью на классе $[\Omega]$ всех Ω-структур. Классы этой эквивалентности являются в точности минимальными аксиоматизируемыми классами Ω-структур; они называются *аксиоматизируемыми типами*. Множество всех аксиоматизируемых типов называется *пространством моделей* над Ω и будет обозначаться через $\mathcal{T}[\Omega]$. Природа этой эквивалентности в дальнейшем будет интересовать нас гораздо больше, но она значительно сложнее рассмотренной конгруэнции между предложениями, и про нее известно не так уж много. Мы отметим только

***Предложение* 4.3.** *Если M и N — некоторые неразличимые Ω-структуры и M конечна, то N конечна и $|M|=|N|$.*

Для доказательства этого утверждения нужно только записать производный предикат, выражающий тот факт, что M имеет по крайней мере n элементов. Для любого целого n запишем

$$E(n)=\bigvee(i_1\neq i_2)\wedge(i_1\neq i_3)\wedge\ldots\wedge(i_1\neq i_n)\wedge(i_2\neq i_3)\wedge\ldots\wedge(i_{n-1}\neq i_n);$$

тогда $E(n)$ выполняется в M тогда и только тогда, когда M имеет по крайней мере n элементов. Поэтому если M конечна с m элементами, то $E(n)$ выполняется в M в точности для $n=1, \ldots, m$. То же самое должно быть верно для N, и потому N также имеет m элементов. ∎

Из приведенных выше определений ясно, что соответствие Галуа, установленное в теореме 4.1, можно также рассматривать как соответствие Галуа между алгеброй Линденбаума и пространством моделей. Наша очередная задача состоит в том, чтобы отождествить соответствующие системы замыканий. Будет выяснено, что теории соответствуют фильтрам в алгебре Линденбаума (теорема 5.4), тогда как система замыканий аксиоматизируемых классов определяет на пространстве моделей некоторую топологию, которая будет предметом изучения в §V.6.

УПРАЖНЕНИЯ

1. Показать, что никакие две различные атомные формулы не конгруэнтны.

2. Показать, что всякая формула конгруэнтна своему универсальному замыканию; вывести отсюда, что $\approx$ не является конгруэнцией на всем $\overline{\Omega}_I$.

3. Проверить, что классы предложений, конгруэнтных предложениям данной теории, образуют фильтр в алгебре Линденбаума.

5. УЛЬТРАПРОИЗВЕДЕНИЯ И ТЕОРЕМА КОМПАКТНОСТИ

Рассмотрим снова произведение семейства $(M_\lambda)_{\lambda\in\Lambda}$ Ω-структур: $M=\prod M_\lambda$ с проекциями ε_λ: $M\to M_\lambda$. Напомним, что Ω-структура на M определяется следующим правилом:

$$M\models\omega\theta \text{ тогда и только тогда, когда } M_\lambda\models\omega\theta\varepsilon_\lambda \text{ для всех } \lambda\in\Lambda, \quad (1)$$

а определение равенства в M может быть записано в виде

$$M\models\varepsilon\theta \text{ тогда и только тогда, когда } M_\lambda\models\varepsilon\theta\varepsilon_\lambda \text{ для всех } \lambda\in\Lambda. \quad (2)$$

Здесь θ: $I\to M$ — произвольное отображение. Нас теперь интересует вопрос, для каких производных предикатов имеет место утверждение

$$M\models P\theta \text{ тогда и только тогда, когда } M_\lambda\models P\theta\varepsilon_\lambda \text{ для всех } \lambda\in\Lambda. \quad (3)$$

Оно, конечно, выполняется для всех положительных формул; нужно только показать, что

$$M\models P\theta \text{ или } M\models Q\theta \text{ тогда и только тогда, когда } M\models P\theta\vee Q\theta,$$

$$M\models P\theta \text{ и } M\models Q\theta \text{ тогда и только тогда, когда } M\models P\theta\wedge Q\theta,$$

а это ясно из определений. Аналогично можно показать, что если (3) выполняется для P, то оно выполняется для $\bigvee_i P$ и $\bigwedge_i P$; но для формул, содержащих отрицание, (3) уже не верно. Так, для любой формулы P

$$M\models\sim P\theta \text{ означает, что } M\models\sim P\theta\varepsilon_\lambda \text{ для всех } \lambda\in\Lambda,$$

тогда как

$$M\sim\models P\theta \text{ означает, что } M_\lambda\models\sim P\theta\varepsilon_\lambda \text{ для некоторого } \lambda\in\Lambda.$$

Два утверждения справа неэквивалентны, за исключением тривиальных случаев; наша цель состоит в том, чтобы устранить этот дефект, т. е. так усовершенствовать определение произведения структур, чтобы $M\models\sim P\theta$ означало то же самое, что и $M\sim\models P\theta$. Это достигается введением понятия приведенного произведения структур.

Пусть $(M_\lambda)_{\lambda\in\Lambda}$ — семейство Ω-структур; тогда для любого фильтра $\mathscr{D}$ над множеством индексов Λ *приведенным произведением* $M_{\mathscr{D}}$ Ω-структур M_λ (по модулю $\mathscr{D}$) называется фактормножество декартова произведения $M=\prod M_\lambda$, определяемое по правилу

$$a\mathscr{D}=b\mathscr{D} \text{ тогда и только тогда, когда } \{\lambda\in\Lambda\mid a\varepsilon_\lambda=b\varepsilon_\lambda\}\in\mathscr{D}. \quad (4)$$

вместе с Ω-структурой, определяемой по правилу

$$M_{\mathscr{D}} \models \omega\theta \text{ тогда и только тогда, когда } \{\lambda \in \Lambda \mid M_\lambda \models \omega\theta\varepsilon_\lambda\} \in \mathscr{D}. \quad (5)$$

Естественное отображение $M \to M_{\mathscr{D}}$ будет обозначаться через $a \to a\mathscr{D}$ или $\mathrm{nat}\,\mathscr{D}$, и мы будем также писать $M/\mathscr{D}$ вместо $M_{\mathscr{D}}$ и $a \equiv b \pmod{\mathscr{D}}$ вместо $a\mathscr{D} = b\mathscr{D}$. Легко видеть, что приведенное произведение, взятое по модулю главного фильтра, изоморфно прямому произведению некоторых из сомножителей; такое произведение называется *тривиальным*. Приведенное произведение, взятое по модулю ультрафильтра, называется *ультрапроизведением* или в случае, когда все сомножители совпадают, *ультрастепенью*. Насколько полезны ультрапроизведения, показывают следующие фундаментальные результаты (Фрейн, Морел и Скотт [62], Кочен [61]):

***Теорема* 5.1. (*Теорема об ультрапроизведениях.*)** *Пусть* $(M_\lambda)_{\lambda \in \Lambda}$ — *семейство* Ω-*структур,* $\mathscr{D}$ — *ультрафильтр над* Λ, *и пусть* $M = \prod M_\lambda$, $M_{\mathscr{D}} = \prod M_\lambda/\mathscr{D}$. *Тогда для любой формулы* P *и любого* $\theta\colon I \to M$

$$M_{\mathscr{D}} \models P\theta(\mathrm{nat}\,\mathscr{D}) \text{ тогда и только тогда, когда}$$
$$\{\lambda \in \Lambda \mid M_\lambda \models P\theta\varepsilon_\lambda\} \in \mathscr{D}. \quad (6)$$

Доказательство. Пусть Σ — множество всех формул, для которых имеет место (6); тогда по определению ультрапроизведения (см. (4) и (5)) Σ содержит t и все атомные формулы; поэтому, чтобы показать, что $\Sigma = \overline{\Omega}_I$, нужно только проверить замкнутость Σ относительно $\wedge$, $\sim$ и $\bigvee\limits_i$.

Если заданы произвольные $P, Q \in \Sigma$ и некоторое $\theta\colon I \to M$, то запишем

$$X = \{\lambda \in \Lambda \mid M_\lambda \models P\theta\varepsilon_\lambda\}, \qquad Y = \{\lambda \in \Lambda \mid M_\lambda \models Q\theta\varepsilon_\lambda\},$$
$$Z = \{\lambda \in \Lambda \mid M_\lambda \models P\theta\varepsilon_\lambda \wedge Q\theta\varepsilon_\lambda\}. \quad (7)$$

Ясно, что $Z = X \cap Y$; теперь $M_{\mathscr{D}} \models P\theta(\mathrm{nat}\,\mathscr{D}) \wedge Q\theta(\mathrm{nat}\,\mathscr{D})$ тогда и только тогда, когда $M_{\mathscr{D}} \models P\theta(\mathrm{nat}\,\mathscr{D})$ и $M_{\mathscr{D}} \models Q\theta(\mathrm{nat}\,\mathscr{D})$, т. е. тогда и только тогда, когда $X \in \mathscr{D}$ и $Y \in \mathscr{D}$ (так как P, Q удовлетворяют (6)). Но это верно в том и только том случае, если $Z = X \cap Y \in \mathscr{D}$, и поэтому (6) выполняется для $P \wedge Q$.

Далее, если $P \in \Sigma$, то $M_{\mathscr{D}} \models {\sim} P\theta(\mathrm{nat}\,\mathscr{D})$ тогда и только тогда, когда $M_{\mathscr{D}} {\sim} \models P\theta(\mathrm{nat}\,\mathscr{D})$, т. е. $X \notin \mathscr{D}$, где X задано формулой (7); и поскольку $\mathscr{D}$ — ультрафильтр, то это имеет место тогда и только тогда, когда $\Lambda \setminus X \in \mathscr{D}$, т. е. $\{\lambda \in \Lambda \mid M_\lambda \models {\sim} P\theta(\mathrm{nat}\,\mathscr{D})\} \in \mathscr{D}$. Поэтому ${\sim} P \in \Sigma$.

Наконец, пусть $P \in \Sigma$ и предположим, что $M_{\mathscr{D}} \models \bigvee_i P\theta\,(\mathrm{nat}\,\mathscr{D})$; тогда существует такое $\theta'\colon I \to M$, что $j\theta' = j\theta$ для $j \neq i$ и $M_{\mathscr{D}} \models P\theta'\,(\mathrm{nat}\,\mathscr{D})$; отсюда $\{\lambda \in \Lambda \mid M_\lambda \models P\theta'\varepsilon_\lambda\} \in \mathscr{D}$, т. е.

$$X_0 = \{\lambda \in \Lambda \mid M_\lambda \models \bigvee_i P\theta\varepsilon_\lambda\} \in \mathscr{D}. \tag{8}$$

Обратно, если имеет место (8), то выберем такое $\theta'\colon I \to M$, что $j\theta' = j\theta$ для $j \neq i$ и $M_\lambda \models P\theta'\varepsilon_\lambda$ для $\lambda \in X_0$. Такое θ' существует в силу (8), так как ни одно M_λ не пусто. Тогда, в силу выбора θ', $\{\lambda \in \Lambda \mid M_\lambda \models P\theta'\varepsilon_\lambda\} = X_0$ и поэтому $M_{\mathscr{D}} \models P\theta'\,(\mathrm{nat}\,\mathscr{D})$, т. е. $M_{\mathscr{D}} \models \bigvee_i P\theta\,(\mathrm{nat}\,\mathscr{D})$. ∎

Если в теореме 5.1 взять замкнутую формулу P и положить $\{P\}^* = \mathscr{K}$, то получим

***Следствие* 5.2.** *Если $\mathscr{K}$ — элементарный класс, то $\prod M_\lambda/\mathscr{D} \in \mathscr{K}$ тогда и только тогда, когда $\{\lambda \in \Lambda \mid M_\lambda \in \mathscr{K}\} \in \mathscr{D}$.* ∎

В частности, если каждое $M_\lambda \in \mathscr{K}$, то $M_{\mathscr{D}} \in \mathscr{K}$. Вообще, если $\mathscr{K}$ — аксиоматизируемый класс, скажем $\mathscr{K} = \Sigma^*$, то $\mathscr{K} = \bigcap_{\alpha \in \Sigma} \{\alpha\}^*$, т. е. $\mathscr{K}$ будет пересечением элементарных классов, и мы получаем

***Следствие* 5.3.** *Всякий аксиоматизируемый класс замкнут относительно ультрапроизведений.* ∎

Можно показать на примерах, что в общем случае для аксиоматизируемых классов следствие 5.2 не имеет места (см. упражнение 4).

Теперь, используя ультрапроизведения, можно показать, что система замыканий, состоящая из модельно-замкнутых множеств формул, будет алгебраической. Достаточно будет доказать это в алгебре Линденбаума $\mathscr{L}(\Omega)$, а не в самой алгебре формул $\overline{\Omega}_I$. На самом деле мы докажем более точный результат:

***Теорема* 5.4.** *Пусть Σ — некоторое подмножество алгебры Линденбаума $\mathscr{L}(\Omega)$; тогда дуальный идеал, порожденный множеством Σ, будет в точности модельным замыканием Σ^{**}.*

Доказательство. Через $\overline{\Sigma}$ обозначим дуальный идеал, порожденный множеством Σ; таким образом, $\overline{\Sigma}$ состоит из всех $\alpha \in \mathscr{L}(\Omega)$, удовлетворяющих неравенству

$$\alpha \geqslant \beta_1 \wedge \ldots \wedge \beta_n \qquad (\beta_r \in \Sigma).$$

Ясно, что всякая Σ-модель будет также $\overline{\Sigma}$-моделью, так что

$$\overline{\Sigma} \subseteq \Sigma^{**}; \tag{9}$$

остается установить обратное включение. Пусть Φ — семейство множеств, в которых главные идеалы, порожденные элементами множества Σ, пересекаются с $\bar{\Sigma}$; тогда Φ обладает свойством конечных пересечений (поскольку точная нижняя грань любого конечного подмножества множества Σ принадлежит множеству $\bar{\Sigma}$); поэтому Φ содержится в некотором ультрафильтре $\mathscr{D}$ над $\bar{\Sigma}$ (как множеством). Теперь, чтобы доказать, что в (9) имеет место равенство, возьмем произвольное $\lambda \notin \bar{\Sigma}$; тогда для каждого $\alpha \in \bar{\Sigma}$ имеем $\alpha \not\leqslant \lambda$, и, следовательно (по теореме 4.2), существует Ω-структура M_α, в которой α истинно, а λ не истинно. Положим

$$M_{\mathscr{D}} = \prod_{\alpha \in \bar{\Sigma}} M_\alpha / \mathscr{D};$$

тогда, если дано $\alpha \in \bar{\Sigma}$, то $M_\beta \vdash \alpha$ для всех таких $\beta \in \bar{\Sigma}$, что $\beta \leqslant \alpha$, и поэтому $M_{\mathscr{D}} \vdash \alpha$ по построению семейства Φ. Это имеет место для всех $\alpha \in \Sigma$; следовательно, $M_{\mathscr{D}} \in \Sigma^*$. С другой стороны, $M_\alpha \sim\vdash \lambda$ для всех $\alpha \in \bar{\Sigma}$; поэтому $M_{\mathscr{D}} \sim\vdash \lambda$. Этим доказано, что $\lambda \notin \Sigma^{**}$, т. е. в (9) имеет место равенство. ∎

Эта теорема показывает, что модельно-замкнутые множества являются в точности дуальными идеалами алгебры $\mathscr{L}(\Omega)$; кроме того, фильтры в $\mathscr{L}(\Omega)$ являются теориями. Теория называется *полной*, если она максимальна в множестве всех теорий. Из теорем 5.4, II.5.2 и V.2.7 мы получаем теперь следующую теорему:

***Теорема* 5.5.** *Система замыканий, состоящая из модельно-замкнутых множеств формул, является алгебраической. Кроме того, каждую теорию можно расширить до полной теории.* ∎

Множество формул называется *непротиворечивым*, если оно обладает моделью. Итак, Σ непротиворечиво тогда и только тогда, когда $f \notin \Sigma^{**}$, или, эквивалентно этому, когда Σ можно расширить до теории. По теореме 5.5 и определению алгебраической системы замыканий теперь имеем

***Следствие* 5.6.** *Множество формул непротиворечиво тогда и только тогда, когда каждое его конечное подмножество непротиворечиво.* ∎

Этот результат иногда называется *теоремой компактности* по причинам, которые будут выяснены в § V.6. Впервые этот результат был получен Гёделем как теорема в логике (с помощью его теоремы полноты) и независимо Сколемом и Мальцевым (см. Чёрч [56]).

УПРАЖНЕНИЯ

1. Показать, что при соответствии Галуа, установленном в теореме 5.1, полные теории соответствуют аксиоматизируемым типам.

2. Проверить, что ультрапроизведение по модулю главного фильтра изоморфно одному из сомножителей (этим объясняется, почему ультрапроизведения представляют интерес только в случае бесконечного числа сомножителей).

3. Показать, что если $\mathcal{K}$ — аксиоматизируемый класс Ω-структур, то бесконечные $\mathcal{K}$-структуры снова образуют аксиоматизируемый класс. (Использовать формулы $E(n)$, определенные в предложении 4.3.)

4. Пусть $\mathcal{K}$ — некоторый аксиоматизируемый класс Ω-структур; показать, что если $\mathcal{K}$ содержит конечные структуры со сколь угодно большим числом элементов, то следствие 5.2 не выполняется для $\mathcal{K}$.

5. Показать, что любая ультрастепень конечной структуры, содержащей n элементов, содержит снова n элементов.

6. Показать, что любое ультрапроизведение бесконечных структур снова бесконечно.

7. Показать, что теория полна тогда и только тогда, когда для каждого предложения P либо P, либо $\sim P$ принадлежит этой теории. Вывести отсюда, что для любой Ω-структуры M множество предложений, истинных в M, будет полной теорией.

8. Показать, что если Θ — некоторая теория и P — такое предложение, что $\Theta \cup \{\sim P\}$ противоречиво, то $P \in \Theta$.

6. ПРОСТРАНСТВО МОДЕЛЕЙ

Рассмотрим теперь более детально систему замыканий, состоящую из аксиоматизируемых классов моделей. Поскольку формулы не дают возможности различать Ω-структуры данного типа, то в качестве объектов исследования следует взять аксиоматизируемые типы, а не индивидуальные Ω-структуры. Таким образом, имеем естественное отображение $M \to (M)$ из $[\Omega]$ в $\mathcal{T}[\Omega]$, сопоставляющее каждой Ω-структуре ее тип. Полными прообразами подмножеств из $\mathcal{T}[\Omega]$ при этом отображении будут те классы Ω-структур, которые являются объединениями типов. Эти классы называются для краткости *типовыми классами*. Итак, типовым классом будет такой класс $\mathcal{K}$ Ω-структур, что

$$\text{если} \quad M \in \mathcal{K} \quad \text{и} \quad M \equiv N, \quad \text{то } N \in \mathcal{K}.$$

Аксиоматизируемыми классами моделей можно воспользоваться для определения на множестве $\mathcal{T}[\Omega]$ некоторой топологии, которая описана в следующей теореме:

***Теорема* 6.1.** *Аксиоматизируемые классы моделей образуют топологическую систему замыканий на пространстве моделей $\mathcal{T}[\Omega]$. При соответствующей топологии $\mathcal{T}[\Omega]$ будет вполне несвязным компактным хаусдорфовым пространством.*

Топологическое пространство с перечисленными свойствами называется иногда *булевым пространством.*

Доказательство. Пусть $\mathscr{C}_1$, $\mathscr{C}_2$ — аксиоматизируемые классы моделей, скажем $\mathscr{C}_r = \Sigma_r^*$ ($r = 1, 2$); мы утверждаем, что класс $\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2$ аксиоматизируем. Достаточно показать, что $\mathscr{C}^{**} \subseteq \mathscr{C}$. Пусть M есть Ω-структура, не принадлежащая $\mathscr{C}$; тогда $M \notin \mathscr{C}_r$ ($r = 1, 2$) и поэтому существует $\mathscr{C}_r$-теорема P_r, которая неистинна в M. Отсюда $P_1 \vee P_2$ является $\mathscr{C}$-теоремой, которая неистинна в M, т. е. $M \notin \mathscr{C}^{**}$. Итак, $\mathscr{C}^{**} = \mathscr{C}$, откуда следует, что аксиоматизируемые классы образуют топологическую систему замыканий. Кроме того, пустой класс аксиоматизируем, поскольку он может быть определен, скажем формулой f, и поэтому мы получаем топологию. Замкнутыми множествами будут пересечения множеств вида $\{P\}^*$, где P — произвольное предложение. Так как дополнение к $\{P\}^*$ имеет тот же вид, а именно $\{\sim P\}^*$, то отсюда вытекает, что существует база, состоящая из замкнутых и открытых множеств (открыто-замкнутых множеств), так что данная топология вполне несвязна. Далее, если (M) и (N) — различные типы, то существует предложение P, истинное в M, но неистинное в N. Следовательно, $\sim P$ истинно в N, но неистинно в M, и $\{P\}^*$, $\{\sim P\}^*$ будут непересекающимися окрестностями типов (M) и (N) соответственно, т. е. показано, что мы имеем хаусдорфово пространство.

Для доказательства компактности возьмем семейство замкнутых множеств $(\mathscr{C}_\lambda)_{\lambda \in \Lambda}$ со свойством конечных пересечений. Если $\mathscr{C}_\lambda = \Sigma_\lambda^*$, то для всякого конечного подмножества Λ_0 множества Λ

$$\Bigl(\bigcup_{\Lambda_0} \Sigma_\lambda\Bigr)^* = \bigcap_{\Lambda_0} \mathscr{C}_\lambda \neq \varnothing;$$

в частности, всякое конечное подмножество $\Sigma = \bigcup \Sigma_\lambda$ непротиворечиво. Поэтому в силу следствия 5.6 Σ само непротиворечиво, и, следовательно,

$$\bigcap \mathscr{C}_\lambda = \Sigma^* \neq \varnothing.$$

Этим установлена компактность. ∎

Следствие 6.2. *Элементарные классы соответствуют тем подмножествам из $\mathcal{T}[\Omega]$, которые одновременно открыты и замкнуты. Иными словами, аксиоматизируемый класс моделей будет элементарным тогда и только тогда, когда его дополнение также аксиоматизируемо.*

В самом деле, ясно, что всякий элементарный класс определяет подмножество из $\mathcal{T}[\Omega]$, которое одновременно открыто и замкнуто. Обратно, предположим, что $\mathscr{C}$ и открыто, и замкнуто; будучи открытым, $\mathscr{C}$ может быть представлено в виде объединения элементарных классов, скажем $\mathscr{C} = \bigcup \mathscr{C}_\lambda$. Так как $\mathscr{C}$ в то же время замкнуто, то оно компактно и поэтому покрывается конечным подсемейством семейства $\mathscr{C}_\lambda$, скажем $\mathscr{C} = \mathscr{C}_1 \cup \ldots \cup \mathscr{C}_n$; следовательно, класс $\mathscr{C}$ сам элементарен. ∎

В связи с этим следствием отметим, это элементарные классы соответствуют элементам алгебры Линденбаума $\mathscr{L}(\Omega)$ и в действительности это соответствие взаимно однозначно.

Операция замыкания в пространстве моделей может быть описана на языке ультрапроизведений следующим образом (Тайманов [62]):

***Предложение* 6.3.** *Пусть S — некоторое подмножество из $\mathcal{T}[\Omega]$ и N — произвольная Ω-структура; тип (N) принадлежит замыканию множества S тогда и только тогда, когда существует такое семейство S-структур $(M_\lambda)_{\lambda \in \Lambda}$ и такой ультрафильтр $\mathscr{D}$ на Λ, что*

$$N \equiv \prod M_\lambda/\mathscr{D}. \tag{1}$$

Доказательство. По определению $(N) \in \overline{S}$ тогда и только тогда, когда каждая S-теорема истинна в N. Поэтому если (1) имеет место, то по теореме об ультрапроизведениях (теорема 5.1) отсюда вытекает, что $(N) \in \overline{S}$. Обратно, пусть $(N) \in \overline{S}$ и в каждом типе λ, принадлежащем S, возьмем модель M_λ. Так как каждая S-теорема истинна в N, то всякое предложение P, истинное в N, обладает моделью в S (поскольку в противном случае $\sim P$ было бы S-теоремой). Для каждого такого $\alpha \in \mathscr{L}(\Omega)$, что $N \vdash \alpha$, определим подмножество E_α множества Λ равенством

$$E_\alpha = \{\lambda \in \Lambda \mid M_\lambda \vdash \alpha\};$$

тогда $E_\alpha \neq \varnothing$ и множество всех E_α замкнуто относительно конечных пересечений, так как если $P \in \alpha$, $Q \in \beta$, то $E_\alpha \cap E_\beta = E_\gamma$, где $\gamma = (P \wedge Q)$. Следовательно, существует ультрафильтр $\mathscr{D}$ на Λ, содержащий все E_α. Мы утверждаем, что при таком выборе $M_{\mathscr{D}} = \prod M_\lambda/\mathscr{D}$ имеет место (1). Действительно, если $N \vdash \alpha$, то $E_\alpha \in \mathscr{D}$ и отсюда $M_{\mathscr{D}} \vdash \alpha$; итак, $N \equiv M_{\mathscr{D}}$, т. е. выполняется (1). ∎

Из этого предложения получается следующее обобщение следствия 5.3:

***Следствие* 6.4.** *Типовой класс аксиоматизируем тогда и только тогда, когда он замкнут относительно ультрапроизведений.* ∎

Более полный результат содержится в § VI.6; здесь мы ограничимся указанием другого следствия из предложения 6.3. Аксиоматизируемый тип является просто точкой пространства $\mathcal{T}[\Omega]$ и поэтому замкнут. Так как ультрастепени представляют собой частный случай ультрапроизведений, взятых внутри одного типа, то из следствия 6.4 получается

***Следствие* 6.5.** *Всякий типовой класс замкнут относительно ультрастепеней.* ▮

Всякий аксиоматизируемый класс $\mathscr{K}$ является замкнутым подпространством пространства $\mathscr{T}[\Omega]$ и при топологии, индуцируемой топологией всего пространства, снова превращается в вполне несвязное компактное хаусдорфово пространство. Пересечение произвольного аксиоматизируемого (или элементарного) класса с $\mathscr{K}$ мы будем называть *относительно аксиоматизируемым* (или *элементарным*) классом в $\mathscr{K}$. Относительные классы приносят наибольшую пользу в случае Ω-структур, являющихся алгебрами относительно подобласти Ω^* области Ω. Нам нужно показать, что класс Ω-структур, являющихся алгебрами относительно Ω^*, аксиоматизируем. Это делается с помощью построения предложений, выражающих тот факт, что предикаты из Ω^* определяют операции (а не просто отношения). Пусть $\omega \in \Omega$ — некоторый $(n+1)$-арный предикат. Тогда предложение

$$\bigwedge \bigvee_j \omega(i_1, \ldots, i_n, j) \qquad (2)$$

называется *условием определенности* для ω. Оно истинно в Ω-структуре M тогда и только тогда, когда для каждого набора из n элементов $(a_1, \ldots, a_n)$ из M существует по крайней мере одно такое $b \in M$, что $\omega(a_1, \ldots, a_n, b)$ *выполняется; иными словами*, когда ω определяет — возможно многозначную — операцию в M. Чтобы получить операцию в нашем смысле, нужно второе предложение, *условие единственности* для ω:

$$\bigwedge [(\omega(i_1, \ldots, i_n, j) \wedge \omega(i_1, \ldots, i_n, k)) \Rightarrow (j = k)]. \qquad (3)$$

Это предложение выражает тот факт, что для каждого набора из n элементов $(a_1, \ldots, a_n)$ из M существует не больше одного такого $b \in M$, что $M \models \omega(a_1, \ldots, a_n, b)$. Итак, (2) и (3) вместе утверждают, что ω определяет n-арную операцию в M.

Пусть теперь Ω^* — подобласть области Ω и Σ — множество, состоящее из условий определенности и единственности для всех элементов из Ω^*. Тогда аксиоматизируемый класс, определенный множеством Σ, будет как раз классом всех Ω-структур, являющихся Ω^*-алгебрами. Таким образом, применяя теорему 6.1, получаем следующую теорему:

***Теорема* 6.6.** *Типы всех Ω-структур, являющихся Ω^*-алгебрами, образуют замкнутое (и, следовательно, компактное) подпространство пространства моделей $\mathscr{T}[\Omega]$. Некоторый аксиоматизируемый класс алгебр относительно элементарен тогда и* *только тогда, когда его дополнение также относительно элементарно.* ∎

На практике мы будем записывать операторы в функциональной форме, как в главе II, а не в использованной здесь форме отношений. Это делается лишь для удобства; читатель может при желании переписать все предложения только с помощью отношений. Например, если ω — тернарное отношение, определяющее на некоторой структуре M бинарную операцию, то закон коммутативности для этой операции, выписанный полностью, читается так:

$$\bigwedge [(\omega(i_1, i_2, i_3) \wedge \omega(i_2, i_1, i_4)) \Rightarrow (i_3 = i_4)],$$

тогда как закон ассоциативности записывается в виде

$$\bigwedge [(\omega(i_1, i_2, i_4) \wedge \omega(i_4, i_3, i_5) \wedge \omega(i_2, i_3, i_6) \wedge \omega(i_1, i_6, i_7)) \Rightarrow (i_5 = i_7)].$$

Можно заметить что оба эти закона описываются универсальными предложениями, хотя условие определенности, нужное для определения ω как операции, не универсально.

Приведем теперь несколько примеров относительно аксиоматизируемых классов.

(i) *Упорядоченные множества.* Пусть Ω состоит из одного бинарного отношения ρ; тогда элементарный класс, определяемый предложениями

$$\bigwedge [\sim \rho(i, i)], \tag{4}$$

$$\bigwedge [(\rho(i, j) \wedge \rho(j, k)) \Rightarrow \rho(i, k)], \tag{5}$$

будет по существу классом упорядоченных множеств. Структуры могут быть выделены из этого класса добавлением аксиом

$$\bigwedge \bigvee_k \bigwedge_l [(\rho_r(i, k) \wedge \rho_r(j, k)) \wedge (\rho_r(i, l) \wedge \rho_r(j, l)) \Rightarrow \rho_r(k, l)] \quad (6)_r$$

$$(r = 1, 2).$$

Здесь для краткости записано $\rho_1(i, j)$ вместо $\rho(i, j) \vee (i = j)$ и $\rho_2(i, j)$ вместо $\rho_1(j, i)$. При этом важно помнить о различии между подструктурами и подалгебрами; именно, подструктура в смысле § V.1 определенной таким образом структуры не будет в общем случае подструктурой в смысле § II.4.

(ii) *Упорядоченные группы.* Возьмем теперь область Ω, состоящую из групповых операторов и бинарного предиката ρ. Тогда упорядоченные группы можно определить групповыми аксиомами вместе с предложениями (4) и (5), приведенными выше, и

$$\bigwedge [\rho(i, j) \Rightarrow (\rho(ik, jk) \wedge \rho(ki, kj))]. \tag{7}$$

(iii) *Поля.* Поле можно определить как коммутативное (и ассоциативное) кольцо, удовлетворяющее условию

$$\bigwedge \bigvee_k [(i \neq 0) \Rightarrow (ik = j)]. \tag{8}$$

Как правило, кольцо, состоящее из одного нуля, исключается, например, добавлением предложения

$$\bigvee (i \neq 0). \tag{9}$$

В качестве следующего примера рассмотрим поля данной конечной характеристики. Для каждого натурального числа n во всяком поле (как и во всякой аддитивной группе) имеем производный оператор $x \to nx$, где

$$nx = x + x + \ldots + x \qquad (n \text{ слагаемых}).$$

Теперь поле характеристики n можно определить предложениями

$$\bigwedge (ni = 0), \tag{10}$$

$$\bigvee [(i \neq 0) \wedge (2i \neq 0) \wedge \ldots \wedge ((n-1)\, i \neq 0)]. \tag{11}$$

Как хорошо известно (см., например, Ван дер Варден [37]), этот класс непуст тогда и только тогда, когда n — простое. Поля характеристики нуль можно определить, взяв все предложения (11) для $n = 1, 2, \ldots$. Следовательно, они также образуют аксиоматизируемый класс, но, как мы вскоре увидим, этот класс уже не будет элементарным.

Отметим сначала следующий результат, вытекающий из теоремы 6.6 (см. Робинсон [63]):

***Теорема* 6.7.** *Пусть Σ — некоторое множество предложений относительно полей. Если существуют поля произвольно большой характеристики, удовлетворяющие Σ, то существуют поля характеристики нуль, удовлетворяющие Σ.*

Доказательство. Пусть $\mathcal{K}_n$ — класс полей, определяемых множеством Σ и (11); таким образом, $\mathcal{K}_n$ состоит из всех Σ-полей характеристики не меньше n. Поля характеристики нуль, удовлетворяющие Σ, составляют пересечение $\bigcap \mathcal{K}_n$. Теперь по предположению

$$\mathcal{K}_1 \supseteq \mathcal{K}_2 \supseteq \ldots$$

является цепью непустых замкнутых подмножеств компактного пространства; следовательно, их пересечение также непусто, что мы и хотели показать. ∎

Пусть P — некоторое предложение, истинное в каждом поле характеристики нуль. Если мы применим нашу теорему для $\Sigma = \{\sim P\}$, то получим

***Следствие* 6.8.** *Элементарное предложение, выполняющееся в каждом поле характеристики нуль, выполняется также в каждом поле достаточно большой характеристики.* ∎

Теперь, если бы класс всех полей характеристики нуль был элементарным, то существовало бы предложение P, определяющее этот класс. По следствию 6.8 P выполнялось бы тогда во всех полях, характеристика которых больше некоторого числа n_0; другими словами, не существовало бы полей конечной характеристики, большей чем n_0. Мы получили противоречие, доказывающее

***Следствие* 6.9.** *Класс полей характеристики нуль не является относительно элементарным.* ∎

УПРАЖНЕНИЯ

1. Показать, что пространство моделей $\mathcal{T}[\Omega]$ имеет счетную базу тогда и только тогда, когда Ω не более чем счетно.

2. Пусть A — булева алгебра и через A^* обозначено подмножество множества 2^A, состоящее из всех гомоморфизмов $A \to 2$. Показать, что A^* будет булевым пространством относительно топологии, индуцируемой топологией произведения 2^A. Используя этот факт, дать другое доказательство теоремы 6.1.

3. Если X — булево пространство, то множество X^* открыто-замкнутых множеств образует булеву алгебру. В частности, если $X = A^*$ для некоторой булевой алгебры A (см. упражнение 2), то $A^{**} \cong A$; кроме того, X^{**} гомеоморфно X.

4. Показать, что классы моделей, замкнутые относительно ультрапроизведений, образуют топологическую систему замыканий и что получающаяся топология компактна.

5. Показать, что типовой класс $\mathcal{K}$ элементарен тогда и только тогда, когда $\mathcal{K}$ и его дополнение в $\mathcal{T}[\Omega]$ оба замкнуты относительно ультрапроизведений.

6. Показать, что класс полей конечной характеристики не аксиоматизируем.

7. Показать, что класс всех конечных групп не аксиоматизируем.

8. Показать, что класс всех конечных упорядоченных множеств, удовлетворяющих аксиоме

$$\bigwedge \bigvee_k [(\rho(i, k) \wedge \rho(k, j)) \vee (\rho(j, k) \wedge \rho(k, i)) \vee (i = j)],$$

является элементарным.

ГЛАВА VI

АКСИОМАТИЗИРУЕМЫЕ КЛАССЫ МОДЕЛЕЙ

Как мы показали в главе V, некоторые свойства Ω-структур можно выразить посредством элементарных предложений, тогда как другие нельзя. Сделаем теперь еще один шаг в нашей теории: рассмотрим различные свойства аксиоматизируемых классов моделей и выясним, до какой степени их можно охарактеризовать формой определяющих предложений. В заключение этой главы приведем изящную характеризацию аксиоматизируемых классов моделей на языке ультрапроизведений, принадлежащую Кейслеру [61].

1. ОГРАНИЧЕНИЯ И РАСШИРЕНИЯ

Пусть Ω — некоторая область предикатов и $\mathscr{L}$ — аксиоматизируемый класс моделей, который в дальнейшем мы будем считать фиксированным. Предложения, определяющие $\mathscr{L}$, будут называться *базисными аксиомами*; $\mathscr{L}$-структуры будут называться просто *моделями*, а все *подмодели*, *фактормодели* и т. д. будут считаться принадлежащими $\mathscr{L}$, если не сказано ничего другого. Все классы Ω-структур будем рассматривать в дальнейшем относительно $\mathscr{L}$; таким образом, если $\mathscr{C}$ — некоторый класс Ω-структур, то под $\mathscr{C}$-моделью подразумевается элемент класса $\mathscr{C} \cap \mathscr{L}$. Здесь $\mathscr{L}$ может быть классом всех Ω-алгебр, или вообще классом Ω-структур, являющихся алгебрами относительно $\Omega^* \subseteq \Omega$, или также классом всех Ω-структур.

Если Ω' — некоторая подобласть области Ω, то каждой модели M соответствует единственная Ω'-структура $M \mid \Omega'$, которая называется *Ω'-ограничением* модели M и которая получается из M, если забыть о предикатах, не принадлежащих Ω', и о базисных аксиомах, содержащих такие предикаты. В частности, *конечным ограничением* модели M называется ограничение $M \mid \Omega_f$, где Ω_f — конечное подмножество области Ω. Наоборот, если дана Ω'-структура N и если существует модель M, для которой N является Ω'-ограничением, то M называется *Ω-расширением* структуры N. Такое расширение называется *конечным*, если $\Omega \setminus \Omega'$ конечно, и *унарным*, если $\Omega \setminus \Omega'$

состоит только из унарных предикатов; сама область Ω будет называться также расширением области Ω'.

Как и для Ω-алгебр, определим для классов моделей операции замыкания. Класс моделей будет называться *абстрактным*, если с каждой моделью в нем содержатся все ее изоморфные образы; для любого абстрактного класса моделей $\mathscr{C}$ обозначим через

$\mathbf{S}\mathscr{C}$ — класс подмоделей $\mathscr{C}$-моделей.
$\mathbf{H}\mathscr{C}$ — класс гомоморфных образов $\mathscr{C}$-моделей.
$\mathbf{P}\mathscr{C}$ — класс произведений $\mathscr{C}$-моделей.
$\mathbf{L}\mathscr{C}$ — класс локальных $\mathscr{C}$-моделей: $M \in \mathbf{L}\mathscr{C}$ тогда и только тогда, когда M обладает локальной системой $\mathbf{S}\mathscr{C}$-моделей.
$\bar{\mathbf{L}}\mathscr{C}$ — класс сублокальных $\mathscr{C}$-моделей: $M \in \bar{\mathbf{L}}\mathscr{C}$ тогда и только тогда, когда каждую конечную подструктуру модели M можно вложить в $\mathscr{C}$-модель.

$\mathbf{S}$-замкнутый класс называется *наследственным*; из контекста обычно будет ясно, относится ли это понятие к подалгебрам или к подструктурам. $\mathbf{L}$-замкнутый класс называется *локально определимым*, а $\bar{\mathbf{L}}$-замкнутый класс — *сублокально определимым*.

Ясно, что

$$\mathbf{L}\mathscr{C} \subseteq \bar{\mathbf{L}}\mathscr{C},$$

но равенство не обязательно выполняется. Например, если $\mathscr{L}$ — класс абелевых групп и $\mathscr{C}$ — класс периодических групп (в $\mathscr{L}$), то $\mathbf{L}\mathscr{C} = \mathscr{C}$, тогда как $\bar{\mathbf{L}}\mathscr{C} = \mathscr{L}$. Вообще всякая локальная $\mathscr{C}$-модель будет сублокальной $\mathscr{C}$-моделью и каждый сублокально определимый класс — локально определимым классом.

Если $\mathscr{C}$ — некоторый класс моделей и $\Omega' \subseteq \Omega$, то обозначим через $\mathscr{C} \mid \Omega'$ класс всех Ω'-ограничений $\mathscr{C}$-моделей. Легко проверить, что для всякого аксиоматизируемого класса $\mathscr{C}$ M будет $\mathscr{C}$-моделью тогда и только тогда, когда для каждой конечной подобласти Ω_f области Ω ограничение $M \mid \Omega_f$ будет $(\mathscr{C} \mid \Omega_f)$-моделью. Из этого замечания вытекает, что аксиоматизируемый класс $\mathscr{C}$ замкнут относительно любой из операций $\mathbf{S}$, $\mathbf{H}$, $\mathbf{P}$, $\mathbf{L}$, $\bar{\mathbf{L}}$ тогда и только тогда, когда для любой конечной подобласти Ω_f области Ω класс $\mathscr{C} \mid \Omega_f$ замкнут в пределах $\mathscr{L} \mid \Omega_f$ относительно той же операции. Довольно часто это позволяет свести рассмотрение к случаю, когда Ω конечно. Однако в большинстве алгебраических систем Ω, как правило, конечно; исключение составляет класс векторных пространств над бесконечным полем.

Часто оказывается полезным следующий критерий локальной определимости наследственных классов. Напомним, что класс называется *индуктивным*, если он замкнут относительно верхних граней, т. е. относительно объединений цепей.

***Предложение* 1.1.** *Пусть $\mathscr{C}$ — наследственный класс моделей; тогда $\mathscr{C}$ локально определим тогда и только тогда, когда он индуктивен.*

Доказательство. Предположим, что $\mathscr{C}$ локально определим, и пусть $(M_\lambda)_{\lambda \in \Lambda}$ — некоторая цепь $\mathscr{C}$-моделей. Если такая цепь допустима, то, рассматриваемая как семейство множеств, она должна принадлежать нашему универсальному множеству U; это будет в том случае, если $M_\lambda \in U$ для каждого $\lambda \in \Lambda$ и $\Lambda \in U$ (см. § I.10), откуда вытекает, что $M = \bigcup M_\lambda \in U$. Пусть теперь (M_λ) — локальная система $\mathscr{C}$-моделей для M; тогда $M \in \mathrm{L}\mathscr{C} = \mathscr{C}$. Обратно, предположим, что $\mathscr{C}$ индуктивен, и пусть M — модель с локальной системой $\mathscr{C}$-моделей ($= \mathrm{S}\mathscr{C}$-моделей). В силу предложения I.5.9 $\mathscr{C}$ замкнут относительно объединений направленных множеств, и поэтому $M \in \mathscr{C}$. ▌

Описание предложений, определяющих индуктивные классы моделей, было дано Чжаном [59].

УПРАЖНЕНИЯ

1. Пусть A — некоторый оператор замыкания на классах моделей; определим оператор A_f по правилу: $M \in \mathrm{A}_f \mathscr{C}$ тогда и только тогда, когда $M \mid \Omega_f \in \mathrm{A}(\mathscr{C} \mid \Omega_f)$ для всех конечных подобластей Ω_f области Ω. Выяснить, какие из операторов, определенных в § VI. 1, удовлетворяют равенству $\mathrm{A}_f = \mathrm{A}$.

2. Класс $\mathscr{C}$ Ω-структур называется ограниченным, если $M \in \mathscr{C}$ тогда и только тогда, когда $M \mid \Omega_f \in \mathscr{C} \mid \Omega_f$ для всех конечных подобластей Ω_f области Ω. Показать, что $\mathrm{A}_f \mathscr{C} = \mathrm{A}\mathscr{C}$ для любого ограниченного класса $\mathscr{C}$ и любого оператора A.

2. ЛОКАЛЬНАЯ ОПРЕДЕЛИМОСТЬ КЛАССОВ

Аксиоматизируемые классы обладают важным свойством локальной определимости в том смысле, что $\mathrm{S}\mathscr{C}$ сублокально определим для любого аксиоматизируемого класса $\mathscr{C}$. Естественно, это особенно интересно для наследственных классов; более того, существует простой критерий аксиоматизируемости таких классов. Эти два результата не связаны между собой непосредственно, но оба основаны на возможности описания понятия вложения с помощью элементарных предложений. Поэтому начнем с этого описания.

Пусть M — произвольная модель и Λ — множество, содержащее носитель модели M. Наша цель состоит в том, чтобы над областью предикатов $\Omega \sqcup \Lambda$, где элементы множества Λ — различные унарные предикаты, построить такое множество предложений Δ, что моделями системы Δ будут в точности расширения модели с носителем Λ, в которую M вложена как подмодель. Таким образом, Δ состоит из условий определенности и единственности для Λ,

$$\bigvee \lambda(i) \quad (\lambda \in \Lambda), \tag{1}$$

$$\bigwedge \{(\lambda(i) \wedge \lambda(j)) \Rightarrow (i = j)\} \quad (\lambda \in \Lambda), \tag{2}$$

вместе с предложениями, выражающими тот факт, что различные элементы из Λ определяют различные предикаты:

$$\bigwedge \{(\lambda(i) \wedge \mu(j)) \Rightarrow (i \neq j)\} \text{ для всех таких } \lambda,\ \mu \in \Lambda, \text{ что } \lambda \neq \mu. \tag{3}$$

В частности, каждому элементу $a \in M$ сопоставлен унарный предикат $a(i)$. Теперь для каждого $a = (a_1, \ldots, a_n) \in M^n$ и каждого $\omega \in \Omega(n-1)$ включим в Δ предложения вида

$$\bigwedge \{a_1(i_1) \wedge \ldots \wedge a_n(i_n) \Rightarrow \omega(i_1, \ldots, i_n)\}, \text{ если } M \models \omega(a_1, \ldots, a_n), \tag{4}$$

$$\bigwedge \{a_1(i_1) \wedge \ldots \wedge a_n(i_n) \Rightarrow \sim \omega(i_1, \ldots, i_n)\}, \quad \text{если } M \sim \models \omega(a_1, \ldots, a_n). \tag{5}$$

Если мы отождествим тот единственный элемент, для которого λ истинен, с λ, то увидим, что каждая Δ-модель N содержит Λ в качестве подмножества. Кроме того, (4) и (5) утверждают, что ограничение на M вложения $\Lambda \to N$ на самом деле будет вложением модели M в модель N. Множество предложений (1) — (5) называется *диаграммой модели M с константами* Λ. Ясно, что (4) и (5) выполняются, если в них подставить вместо ω любую открытую формулу. Множество $\bar{\Delta}$, составленное из предложений вида (1) — (3) и (4), (5), записанных для *каждой* формулы над $\Omega \sqcup \Lambda$ (не обязательно открытой), называется *полной диаграммой* модели M с константами Λ. Модель полной диаграммы модели M является примером элементарного расширения модели M, которые будут изучаться в § VI.3.

С помощью понятия диаграммы можно сформулировать следующий *принцип локализации* (Хенкин [53], Робинсон [63]):

***Теорема* 2.1.** *Если $\mathscr{C}$ — некоторый аксиоматизируемый класс моделей, то класс $S\mathscr{C}$ сублокально определим.*

Доказательство. Пусть $\mathscr{C} = \Sigma^*$ и рассмотрим произвольную модель M. Нужно показать, что $M \in S\mathscr{C}$, если только каждая конечная подмодель модели M вложима в $\mathscr{C}$-модель. Пусть Δ — диаграмма модели M с константами M; тогда $M \in S\mathscr{C}$ при условии, что система $\Sigma \cup \Delta$ непротиворечива, но в силу теоремы компактности (следствие V.5.6) это будет верно, если только каждое конечное подмножество системы $\Sigma \cup \Delta$ непротиворечиво. Пусть $\Sigma_f \cup \Delta_f$ — такое подмножество (где $\Sigma_f \subseteq \Sigma$ и $\Delta_f \subseteq \Delta$), и пусть N — подмножество (конечное) тех элементов из M, которые участвуют в Δ_f в качестве констант; тогда расширение модели N будет Δ_f-моделью. По предположению относительно M модель $N \in \mathbf{S}\mathscr{C}$; таким образом, существует $\mathscr{C}$-модель, содержащая N. Эта $\mathscr{C}$-модель удовлетворяет Σ и Δ_f; следовательно, система $\Sigma_f \cup \Delta_f$ непротиворечива. Отсюда вытекает, что $\Sigma \cup \Delta$ непротиворечива, и поэтому существует Σ-модель, являющаяся расширением модели M. ∎

Этот результат можно использовать в двух направлениях. Во-первых, мы получаем локальные теоремы для классов вида $\mathbf{S}\mathscr{C}$, где $\mathscr{C}$ — аксиоматизируемый класс, и в частности для наследственных аксиоматизируемых классов. Во-вторых, если $\mathscr{C}$ — такой класс, что $\mathbf{S}\mathscr{C}$ не будет сублокально определимым, то теорема 2.1 показывает, что $\mathscr{C}$ не аксиоматизируем. Однако отметим, что условие теоремы 2.1, необходимое для аксиоматизируемости класса $\mathscr{C}$, не является достаточным (см. Ершов [62]).

Можно применить теорему 2.1 к алгебрам, выделяя подобласть Ω^* области Ω и рассматривая те Ω-структуры, которые являются Ω^*-алгебрами.

***Следствие* 2.2.** *Пусть $\mathscr{K}$ — аксиоматизируемый класс Ω-структур, являющихся Ω^*-алгебрами; тогда Ω-модель M можно вложить в $\mathscr{K}$-алгебру в том и только том случае, если каждую конечную подмодель модели M можно вложить в $\mathscr{K}$-алгебру.* ∎

Обычно та структура, которую требуется вложить, сама является алгеброй (возможно, с другой областью операторов), и в этом случае часто достаточно применить следующий результат, вытекающий из следствия 2.2:

***Следствие* 2.3.** *Пусть $\mathscr{K}$ — аксиоматизируемый класс Ω-структур, являющихся Ω^*-алгебрами, и пусть $\mathscr{L}$ — класс алгебр, представленный в $\mathscr{K}$. Тогда $\mathscr{L}$-алгебру B можно вложить в $\mathscr{K}$-алгебру при условии, что для каждого конечного подмножества X из B существует такая $\mathscr{K}$-алгебра A_X и такое допустимое отображение θ: $X \to A_X$, что ограничение $\theta \mid X$ взаимно однозначно.* ∎

Вернемся теперь к проблеме описания наследственных классов. В этом описании будет использована диаграмма конечного ограничения конечной структуры, и здесь важно представить эту диаграмму (без констант) в виде одного элементарного предложения. Это сделано в следующей лемме:

***Лемма* 2.4.** *Пусть M — конечная Ω-структура, где Ω — конечная область предикатов. Тогда существует такое экзистенциальное предложение P от некоторых переменных, число которых не превосходит $|M|$, что класс P-моделей состоит из тех и только тех моделей, которые содержат подмодель, изоморфную M.*

Доказательство. Пусть $M=\{a_1, \ldots, a_k\}$; рассмотрим следующее множество формул от переменных $1, 2, \ldots, k$:

$$i \neq j \text{ для любой пары } (i, j) \text{ различных переменных,} \tag{6}$$

и для каждого $\omega \in \Omega(n-1)$ и любого набора $(i_1, \ldots, i_n)$ $(1 \leqslant i_r \leqslant k)$

$$\omega(i_1, \ldots, i_n), \quad \text{если} \quad M \models \omega(a_1, \ldots, a_n), \tag{7}$$

$$\sim\omega(i_1, \ldots, i_n), \quad \text{если} \quad M \sim\models \omega(a_1, \ldots, a_n). \tag{8}$$

Так как Ω и M конечны, то совокупность всех формул (6)—(8) конечна. Если мы возьмем конъюнкцию этих формул и свяжем каждое из переменных квантором существования, то получим, очевидно, предложение требуемого вида. ∎

***Предложение* 2.5.** *Класс моделей $\mathscr{C}$ будет элементарным классом, определяемым универсальным предложением, в том и только том случае, если $\mathscr{C}$ — абстрактный и наследственный класс и существуют такая конечная подобласть Ω_f области Ω и такое целое положительное число n, что модель M принадлежит $\mathscr{C}$, если только для каждой подмодели N модели M, содержащей не более n элементов, $N|\Omega_f$ может быть вложена в $(\mathscr{C}\,|\,\Omega_f)$-модель.*

Доказательство. Пусть P — универсальное предложение, определяющее $\mathscr{C}$. Если $M \vdash P$, то P истинно во всякой модели, изоморфной M, и во всякой подмодели модели M; третье условие также удовлетворяется, если в качестве Ω_f взять множество предикатов, участвующих в записи P, а в качестве n—число переменных в P.

Пусть теперь $\mathscr{C}$ — некоторый класс, удовлетворяющий всем условиям предложения 2.5 с данными Ω_f и n. Число открытых формул над Ω_f не более чем от n переменных конечно; поэтому можно взять конъюнкцию P_0 всех таких формул, истинных в каждой $(\mathscr{C}\,|\,\Omega_f)$-модели. Пусть $\mathscr{D}$ — класс моделей, определяемый формулой P_0; тогда $\mathscr{D}$ можно определить также универсальным предложением, скажем P, соответствующим предложению P_0 (которое получается из P_0 применением универсальных кванторов); следовательно, в силу первой части доказательства $\mathscr{D}$ удовлетворяет условиям данного предложения. Мы закончим доказательство, если покажем, что

$$\mathscr{C}=\mathscr{D}. \tag{9}$$

Если $M \in \mathscr{C}$, то $M\,|\,\Omega_f$ принадлежит $\mathscr{C}\,|\,\Omega_f$ и поэтому является P-моделью. Так как в записи P участвуют только предикаты из Ω_f, то отсюда вытекает, что модель M сама будет P-моделью, т. е. $M \in \mathscr{D}$. Этим доказано включение $\mathscr{C} \subseteq \mathscr{D}$. Пусть теперь $M \in \mathscr{D}$, т. е $M \vdash P$, и возьмем произвольную подмодель N модели M, содержащую не больше n элементов. Поскольку P — универсальное предложение, имеем

$$N \vdash P. \tag{10}$$

Применяя лемму к $N \mid \Omega_f$, получим экзистенциальное предложение Q не более чем от n переменных, истинное в тех и только тех Ω_f-моделях, которые обладают подмоделью, изоморфной $N \mid \Omega_f$. Как легко видеть, отрицание $\sim Q$ предложения Q эквивалентно универсальному предложению Q' не более чем от n переменных. В силу (10) Q' не вытекает из P, так как Q' не выполняется в N. По определению предложения P это означает, что Q' не выполняется в $\mathscr{C} \mid \Omega_f$; итак, существует $(\mathscr{C} \mid \Omega_f)$-модель, скажем N', в которой Q' неистинно. Отсюда Q истинно в N'; но Q было предложением, описывающим $N \mid \Omega_f$; поэтому мы получили $(\mathscr{C} \mid \Omega_f)$-модель N', в которую можно вложить $N \mid \Omega_f$. По предположению это означает, что $M \in \mathscr{C}$, т. е. имеет место (9). ▌

Отметим два простых следствия из этого результата.

***Следствие* 2.6.** *Элементарное предложение определяет наследственный класс в том и только том случае, если оно конгруэнтно универсальному предложению.*

В самом деле, очевидно, что универсальное предложение и, следовательно, всякое предложение, ему конгруэнтное, определяет наследственный класс. Обратно, если P определяет наследственный класс, то $\{P\}^*$ удовлетворяет всем условиям предложения 2.5 и поэтому может быть определен универсальным предложением Q. Теперь ясно, что P и Q конгруэнтны. ▌

Свойство называется *стойким*, если оно выполняется в модели M, как только оно выполняется в некоторой подмодели модели M. Переходя к отрицанию, из следствия 2.6 получаем:

***Следствие* 2.7.** *Элементарное предложение выражает стойкое свойство в том и только том случае, если оно конгруэнтно экзистенциальному предложению.* ▌

Наследственные аксиоматизируемые классы можно охарактеризовать следующим образом (Лось [55], Робинсон [63]):

***Теорема* 2.8.** *Для любого класса моделей $\mathscr{C}$ следующие условия эквивалентны:*

(i) *$\mathscr{C}$ — наследственный и аксиоматизируемый класс;*

(ii) *$\mathscr{C}$ — наследственный и $\mathscr{C} \mid \Omega_f$ — сублокально определимый классы для каждой конечной подобласти Ω_f области Ω;*

(iii) *$\mathscr{C}$ определяется множеством универсальных предложений.*

Класс, удовлетворяющий (iii) (и, следовательно, (i) и (ii)), называется *универсальным классом* или также *классом открытых* *предложений*, поскольку его можно определить открытыми формулами.

Доказательство. Импликация (i)$\Rightarrow$(ii) вытекает из теоремы 2.1. Для доказательства того, что (ii)$\Rightarrow$(iii), возьмем класс $\mathscr{C}$, удовлетворяющий (ii), и для каждого конечного подмножества Ω_f множества Ω и каждого целого положительного числа n через $\mathscr{C}(\Omega_f, n)$ обозначим класс всех таких моделей M, для которых Ω_f-ограничение любой подмодели, содержащей не больше n элементов, можно вложить в $(\mathscr{C} \mid \Omega_f)$-модель. Тогда класс $\mathscr{C}(\Omega_f, n)$ удовлетворяет условиям предложения 2.5 и поэтому может быть определен универсальным предложением. В силу (ii) $M \in \mathscr{C}$ тогда и только тогда, когда $M \in \mathscr{C}(\Omega_f, n)$ для всех Ω_f и всех n, т. е.

$$\mathscr{C} = \bigcap \mathscr{C}(\Omega_f, n),$$

где пересечение берется по всевозможным парам (Ω_f, n). Следовательно, $\mathscr{C}$ можно определить множеством универсальных предложений. Наконец, очевидно, что (iii)$\Rightarrow$(i). ∎

Если перейти к алгебрам, считая предикаты подобласти Ω^* операторами, то мы получим критерий аксиоматизируемости класса алгебр, замкнутого относительно подалгебр. Мы оставляем формулировку этого результата читателю и упомянем только

Следствие 2.9. *Если $\mathscr{C}$ — универсальный класс алгебр, то $A \in \mathscr{C}$ тогда и только тогда, когда каждая конечнопорожденная подалгебра алгебры A принадлежит $\mathscr{C}$.* ∎

Это следствие гораздо слабее теоремы 2.8 даже для конечного Ω^*. Например, класс периодических групп локально определим, но не сублокально определим; таким образом, он не является универсальным классом (он даже не аксиоматизируем), хотя условия следствия 2.9 выполнены.

УПРАЖНЕНИЯ

1. Доказать, что универсальный класс будет элементарным тогда и только тогда, когда его можно определить одним универсальным предложением.

2. Показать, что класс периодических групп не аксиоматизируем. (Применить следствие 2.2, взяв в качестве M бесконечную циклическую группу; заметить, что следствие 2.3 не может быть здесь использовано.)

3. Показать, что если $\mathscr{C}$ — аксиоматизируемый класс, то $S\mathscr{C}$ — универсальный класс.

4. Если $\mathscr{C}$ — элементарный класс, так что $S\mathscr{C}$ — универсальный, то сам класс $S\mathscr{C}$ не обязан быть элементарным. Например, класс $\mathscr{C}$ таких полугрупп, что

$$\bigvee_h \bigwedge_{i,j} \bigvee_{k,l} [(h = h) \wedge (ik = j) \wedge (li = j)],$$

состоит из всех групп, рассматриваемых как полугруппы, допускающие деление. Проверить, что если $\mathscr{C}$ считать классом алгебр, то $S\mathscr{C}$ состоит из всех полугрупп, вложимых в группы. (Множество универсальных предложений, определяющих $S\mathscr{C}$, было построено Мальцевым [39] (см. § VII. 3), который показал также, что класс $S\mathscr{C}$ не является элементарным (Мальцев [40]).)

5. (Мальцев.) Показать, что класс свободных групп не аксиоматизируем.

6. (Каргаполов.) Показать, что класс локально свободных групп не аксиоматизируем.

7. Говорят, что группа G удовлетворяет *нормализаторному условию*, если каждая собственная подгруппа отлична от ее нормализатора. Проверить, что класс групп, удовлетворяющих нормализаторному условию, наследствен (см. Курош [53]; этот класс не является локально определимым и поэтому не аксиоматизируем).

8. Показать, что если $\mathscr{L}$ — класс всех Ω-алгебр и $\mathscr{C}$ — произвольный класс Ω-алгебр, то алгебра A будет сублокальной $\mathscr{C}$-алгеброй при условии, что для каждого конечного подмножества X алгебры A подалгебра $J(X)$, порожденная множеством X, обладает такой конгруэнцией $\mathfrak{q}$, разделяющей X, что $J(X)/\mathfrak{q} \in \mathscr{C}$.

3. ЭЛЕМЕНТАРНЫЕ РАСШИРЕНИЯ

Мы видели, что понятие гомоморфизма не инвариантно при переходе к производным предикатам. Этот дефект можно исправить, если ввести элементарные отображения. Отображение между Ω-структурами

$$\varphi\colon M \to N$$

называется *элементарным* при условии, что для любой формулы P и любого $\theta\colon I \to M$

$$N \models P\theta\varphi, \quad \text{если} \quad M \models P\theta. \tag{1}$$

Ясно, что элементарное отображение будет гомоморфизмом, но в действительности можно сказать больше:

***Предложение* 3.1.** *Если $\varphi\colon M \to N$ — элементарное отображение, то φ взаимно однозначно и для каждой формулы P и $\theta\colon I \to M$*

$$M \models P\theta \text{ тогда и только тогда, когда } N \models P\theta\varphi. \tag{2}$$

Чтобы убедиться в том, что φ взаимно однозначно, нужно только применить (1) с формулой «$i \neq j$» в качестве P. Теперь одна половина утверждения (2) является повторением (1), тогда как другая половина вытекает из (1), если формулу P в (1) заменить на $\sim P$. ∎

Пусть N — некоторая Ω-структура и M — подструктура структуры N. Тогда N называется *элементарным расширением* структуры M, если вложение $\iota\colon M \to N$ элементарно. Будем обозначать это отношение между M и N так: $M \prec N$. Если $M \prec N$ и $N \prec M$, то это означает, что M и N имеют один и тот же носитель и тождественное отображение между ними является изоморфизмом. Как и в случае алгебр, будем считать M и N в этом случае одной и той же структурой, так что $\prec$ определяет упорядоченность на $[\Omega]$. При этой упорядоченности $[\Omega]$ будет индуктивным классом; действительно, если $(M_\lambda)_{\lambda \in \Lambda}$ — некоторая цепь, то обозначим через M ее объединение и определим Ω-структуру на M так, чтобы вложения $M_\lambda \to M$ были элементарными. Тогда M превращается в Ω-структуру, являющуюся элементарным расширением каждого M_λ.

Если $\varphi\colon M \to N$ — элементарное отображение между Ω-структурами, то M и N неразличимы, что вытекает из предложения 3.1, если в качестве P взять в нем произвольное предложение. Может случиться, однако, что расширение N/M Ω-структур неэлементарно даже в том случае, когда M и N неразличимы. Например, целые положительные числа и положительные четные числа как упорядоченные множества неразличимы, и они образуют расширение, но неэлементарное расширение, поскольку 2 обладает предшествующим элементом в одной модели и не обладает им в другой.

Приведем теперь несколько критериев того, что расширения элементарны (эти и другие критерии см. в работе Тарского и Вота [57]).

Если M — некоторая Ω-структура и X — подмножество в M, то через $\langle M, X\rangle$ обозначим унарное расширение модели M, которое получается, если считать элементы множества X постоянными операторами (определяемыми унарными предикатами, соответствующими элементам множества X). Так, например, для $X = M$, $\langle M, M\rangle$ будет моделью диаграммы Ω-структуры M с константами M.

***Теорема* 3.2.** *Для любого расширения N/M Ω-структур следующие три условия эквивалентны:*

(i) $M \prec N$;

(ii) *для каждой формулы P и каждого $\theta\colon I \to M$, если $N \models \left(\bigvee_i P\right)\theta$, то существует такое $\theta'\colon I \to M$, что $j\theta' = j\theta$ для $j \neq i$ и $N \models P\theta'$;*

(iii) *для каждого конечного подмножества X модели M*

$$\langle M, X\rangle \equiv \langle N, X\rangle.$$

Доказательство. (ii)$\Rightarrow$(i). Пусть Φ — множество всех таких формул P, что

$$\text{для каждого } \theta\colon I \to M, \text{ если } N \models P\theta, \text{ то } M \models P\theta. \tag{3}$$

Нужно показать, что Φ содержит все формулы. Ясно, что каждая открытая формула принадлежит Φ; далее, если $P \in \Phi$, то $\bigwedge_i P \in \Phi$, а в силу (ii) также $\bigvee_i P \in \Phi$. Итак, (3) выполняется для всех P, откуда $M \prec N$.

(i)$\Rightarrow$(iii). Пусть $\langle N, X\rangle \vdash P$, где P имеет вид

$$P = P(x_1, \ldots, x_n) \quad (x_\nu \in X).$$

Возьмем элементы $i_1, \ldots, i_n \in I$, не участвующие в записи P; если $Q = P(i_1, \ldots, i_n)$, то для любого $\theta\colon I \to M$, при котором $a_{i_1} = x_1, \ldots$ $\ldots, a_{i_n} = x_n$,

$$N \models (\bigvee Q)\,\theta \text{ и потому } M \models (\bigvee Q)\,\theta,$$

т. е. $\langle M, X\rangle \vdash P$. Заменив P на $\sim P$ и повторяя те же рассуждения, получим обратное утверждение: если $\langle M, X\rangle \vdash P$, то $\langle N, X\rangle \vdash P$.

(iii)$\Rightarrow$(ii). Предположим, что выполняется (iii), и пусть заданы такие P, $i \in I$ и $\theta\colon I \to M$, что $N \models \left(\bigvee_i P\right)\theta$. Пусть J — подмножество множества I, элементы которого участвуют в P, и через X обозначим образ множества $J \setminus \{i\}$ при θ; тогда $\langle N, X\rangle \models \left(\bigvee_i P\right)\theta$, где в правой части формулы все элементы $j\theta$ $(j \neq i)$ считаются константами. Отсюда $\langle M, X\rangle \models \left(\bigvee_i P\right)\theta$, т. е. для некоторого $\theta'\colon I \to M$, при котором $j\theta' = j\theta$ для всех $j \neq i$ $(j \in J)$, имеем $M \models P\theta'$; и это будет выполняться, если мы положим $j\theta' = j\theta$ для всех $j \neq i$. Поэтому (ii) удовлетворяется. ∎

***Следствие* 3.3.** *Пусть $B|A$ — расширение Ω-структур, являющихся Ω^*-алгебрами. Если для каждой конечнопорожденной подалгебры A_f алгебры A и любого $b \in B$ существует автоморфизм алгебры B, который элементы подалгебры A_f оставляет неподвижными и отображает b в A, то $A \prec B$.*

Это вытекает из теоремы 3.2, если проверить, что выполняется условие (ii) этой теоремы. ∎.

Понятие элементарного расширения можно использовать для построения из данной Ω-структуры M других неразличимых с M структур нужной мощности λ. Имеется по существу два результата (оба принадлежат Тарскому и Воту [57]), соответствующие тем случаям, когда λ больше или меньше, чем $|M|$. Чтобы избежать тривиальных утверждений, нужно, конечно, предполагать, что все рассматриваемые мощности бесконечны (см. предложение V. 4.3).

***Теорема* 3.4.** *Пусть M — бесконечная Ω-структура, X — некоторое подмножество в M и λ — такая бесконечная мощность, что*

$$\max(|\Omega|, |X|) \leqslant \lambda \leqslant |M|.$$

Тогда существует такая Ω-структура L мощности λ, что

$$X \subseteq L \prec M.$$

Доказательство. Из предположений вытекает, что в M существует подмножество Y мощности λ, содержащее X. Пусть Y — такое множество; для каждой формулы P, в записи которой участвует конечное подмножество J из I, каждого $i \in I$ и каждого θ: $J \to Y$, для которых $M \models \left(\bigvee_i P\right)\theta$, выберем такой определенный $x \in M$, что $M \models P\theta'$, где θ': $J \to M$ задано равенством

$$j\theta' = \begin{cases} x, & \text{если} \quad j = i, \\ j\theta, & \text{если} \quad j \neq i. \end{cases}$$

Пусть Y' — множество всех таких $x \in M$; тогда $|Y'| = \lambda$, поскольку число формул равно $\max\{|\Omega|, \aleph_0\} \leqslant \lambda$. Кроме того, взяв «$i = j$» в качестве P, видим, что $Y \subseteq Y'$. Если применить такое же построение к Y', то мы получим множество Y'' и, продолжая таким образом, получим возрастающую цепь

$$Y \subseteq Y' \subseteq Y'' \subseteq \ldots .$$

Объединение L этой цепи снова будет иметь мощность λ и будет содержать X. Кроме того, $L \prec M$ по условию (ii) теоремы 3.2. ∎

Взяв $X = \varnothing$, мы получим

***Следствие* 3.5.** *Каждая бесконечная Ω-структура над конечной или счетной областью Ω является элементарным расширением счетной Ω-структуры.* ∎

В частности, отсюда вытекает хорошо известная

Теорема Лёвенгейма — Сколема. *Каждая непротиворечивая теория над счетной областью предикатов обладает счетной моделью.* ∎

Вообще отсюда вытекает, что всякая непротиворечивая теория обладает моделью, мощность которой не превосходит $\max(|\Omega|, \aleph_0)$. Это показывает, в частности, что пространство моделей, введенное в § V.6, не зависит от выбранного универсального множества, а зависит только от Ω.

Для получения Ω-структур большей мощности воспользуемся следующей теоремой:

***Теорема* 3.6.** *Пусть M — бесконечная Ω-структура и λ — такая мощность, что $\lambda \geqslant \max(|M|, |\Omega|)$; тогда M обладает элементарным расширением мощности λ.*

Доказательство. Пусть Λ — некоторое множество мощности λ, содержащее M, и через Δ обозначим полную диаграмму модели M с константами Λ (см. § VI.2). Каждое конечное подмножество из Δ обладает моделью, а именно M; нужно только выбрать подходящие элементы из M, чтобы поставить их в соответствие конечному числу используемых элементов из Λ. Поэтому в силу компактности Λ обладает моделью N. По построению N содержит Λ и является элементарным расширением модели M. Следовательно, ее мощность не меньше λ, и по теореме 3.4 существует расширение L мощности λ, содержащее M. Поскольку $M \prec N$, $L \prec N$, $M \subseteq L$, отсюда вытекает, что $M \prec L$. ∎

***Следствие* 3.7.** *Если M — некоторая бесконечная Ω-структура и $\lambda \geqslant \max\{|\Omega|, \aleph_0\}$, то существует Ω-структура мощности λ, которая неразличима с M.* ∎

В качестве приложения приведем простой критерий полноты теории, принадлежащий Воту [54]. Напомним, что полной теорией называется максимальное непротиворечивое множество предложений. Другими словами, теория полна тогда и только тогда, когда все ее модели неразличимы. Итак, чтобы получить полную теорию, нужно только выбрать некоторую Ω-структуру M и взять множество всех предложений, истинных в M. Однако это не дает простого критерия, который мог бы быть применен к данному множеству аксиом. Чтобы привести критерий Вота, нам понадобится понятие категоричности. Вообще теория называется *категоричной*, если все ее модели изоморфны. Ясно, что всякая категоричная теория полна, но элементарные теории, которые мы изучаем, никогда не могут быть категоричными (в силу следствия 3.7), за исключением тривиального случая полной теории, обладающей конечной моделью (предложение V. 4.3). Поэтому назовем теорию Θ *α-категоричной*, где α — данная мощность, если любые две Θ-модели мощности α изоморфны. С помощью этого определения получаем следующий критерий:

***Теорема* 3.8. (Вот [54].)** *Пусть Θ—некоторая элементарная теория без конечных моделей, которая α-категорична для некоторой мощности α, где*

$$\alpha \geqslant \max\{|\Omega|, \aleph_0\}.$$

Тогда Θ полна.

Доказательство. Если Θ не полна, то для некоторого предложения P ни P, ни $\sim P$ не принадлежат Θ, а поэтому и $\Theta \cup \{P\}$, и $\Theta \cup \{\sim P\}$ непротиворечивы (см. § V. 5). Пусть M_1 — модель для $\Theta \cup \{P\}$, а M_2 — модель для $\Theta \cup \{\sim P\}$. Обе эти модели будут Θ-моделями и поэтому бесконечны; в силу следствия 3.7 существуют Ω-структуры N_1, V_2 мощности α, неразличимые с M_1, M_2 соответственно. Но тогда N_1 и N_2 являются Θ-моделями и, следовательно, изоморфны, что противоречит тому факту, что $N_1 \vdash P$, $N_2 \vdash \sim P$. ∎

УПРАЖНЕНИЯ

1. Показать, что если M — некоторая Ω-структура, то любая ультрастепень структуры M будет ее элементарным расширением.

2. Показать, что теория без конечных моделей будет полной при условии, что для некоторого $\alpha \geqslant \max\{|\Omega|, \aleph_0\}$ все ее модели мощности α неразличимы.

3. Применяя критерий Вота, показать, что следующие теории полны:

(i) Плотно упорядоченные множества (с концевыми точками или без концевых точек). (См. упражнение I.5.9.)

(ii) Бесконечномерные векторные пространства над данным полем.

(iii) Алгебраически замкнутые поля данной характеристики. (См. § VII. 2.)

(iv) Нетривиальные булевы алгебры без атомов. (См. упражнение V. 2.10.)

4. Р-ЗАМКНУТЫЕ КЛАССЫ И КВАЗИМНОГООБРАЗИЯ

Рассмотрим теперь более подробно вид, который могут принимать универсальные предложения. Всякое универсальное предложение над Ω имеет вид

$$\bigwedge P, \tag{1}$$

где P — открытая формула с конечным числом свободных переменных. Таким образом, P составлена из атомных формул посредством $\sim$, $\vee$ и $\wedge$. При помощи конъюнктивной нормальной формы можно представить P как конъюнкцию формул типа

$$Q = E_1 \vee \cdots \vee E_r, \tag{2}$$

где каждая формула E_k — атомная формула или отрицание атомной формулы. Соответственно этому назовем E_k *положительной* или *отрицательной* составляющей формулы Q. Теперь P истинна в данной структуре M тогда и только тогда, когда в M истинны все формулы Q, из которых составлена P; поэтому можно ограничиться рассмотрением формул вида (2). Для каждой формулы Q вида (2) запишем

$$Q^{(k)} = E_1 \vee \cdots \vee E_{k-1} \vee E_{k+1} \vee \cdots \vee E_r \quad (k = 1, \ldots, r).$$

Пусть Σ — произвольное множество универсальных предложений; так как нас интересует только класс моделей, определяемый множеством Σ, то все предложения в Σ можно заменить соответствующими открытыми формулами (которые получаются, если опустить все кванторы), а последние могут быть заменены своими конъюнктивными компонентами (2). Таким образом, можно предполагать, что Σ состоит из формул вида (2). Формула Q в Σ называется *сократимой в* Σ, если Q имеет больше одной компоненты и $Q^{(k)} \in \Sigma$ для некоторого $k = 1, \ldots, r$; в противном случае Q называется *несократимой в* Σ. Итак, высказывание, что Q несократима в Σ, означает, что Q имеет только одну компоненту или что для любого $k = 1, \ldots, r$ существует такая Σ-модель M_k, что $M_k \sim\vdash Q^{(k)}$.

Предложение **4.1.** *Каждый универсальный класс может быть определен множеством Σ открытых формул, которые несократимы в Σ.*

Действительно, мы видели, что универсальный класс $\mathcal{K}$ может быть определен множеством Σ формул вида (2). Теперь всякую сократимую в Σ формулу можно заменить формулой с меньшим числом компонент, не изменяя $\mathcal{K}$; повторяя, если нужно, этот процесс, получим таким образом формулу, несократимую в Σ. ∎

Лемма **4.2.** *Пусть Σ — множество таких несократимых открытых формул, что класс моделей, определяемый множеством Σ,* **Р**-*замкнут. Тогда ни одна формула в Σ не может иметь больше одной положительной компоненты.*

Доказательство. Предположим, что Σ содержит формулу $Q = E_1 \vee E_2 \vee \cdots \vee E_r$, где E_1 и E_2 положительны. Пусть M_k есть Σ-модель, к которой формула $Q^{(k)}$ не является истинной. Таким образом,

$$M_1 \vdash \bigwedge (E_1 \vee E_2 \vee \cdots \vee E_r)$$

и

$$M_1 \vdash \bigvee (\sim E_2 \wedge \sim E_3 \wedge \cdots \wedge \sim E_r),$$

а поэтому

$$M_1 \vdash \bigvee (E_1 \wedge \sim E_2 \wedge \cdots \wedge \sim E_r);$$

аналогично

$$M_2 \vdash \bigvee (\sim E_1 \wedge E_2 \wedge \sim E_3 \wedge \cdots \wedge \sim E_r).$$

Выберем такое $\theta_1 \colon I \to M_1$, что

$$M_1 \models (E_1 \wedge \sim E_2 \wedge \cdots \wedge \sim E_r)\,\theta_1,$$

и такое $\theta_2 \colon I \to M_2$, что

$$M_2 \models (\sim E_1 \wedge E_2 \wedge \sim E_3 \wedge \cdots \wedge \sim E_r)\,\theta_2;$$

тогда

$$M_1 \times M_2 \models (\sim E_1 \wedge \sim E_2 \wedge \cdots \wedge \sim E_r)(\theta_1, \theta_2),$$

где через (θ_1, θ_2) обозначено отображение $i \to (i\theta_1, i\theta_2)$. Но это означает, что $M_1 \times M_2 \sim\vdash Q$, что противоречит **Р**-замкнутости Σ. ∎

Отметим, что при доказательстве было использовано только произведение двух сомножителей; в действительности всякий класс, замкнутый относительно прямых произведений двух сомножителей, очевидно, замкнут относительно прямых произведений любого конечного числа сомножителей, и в силу результата Вота [54″] если этот класс аксиоматизируем, то он замкнут относительно прямых произведений любого числа сомножителей.

Эта лемма показывает, что любая формула в Σ имеет вид

$$\sim A_1 \vee \sim A_2 \vee \cdots \vee \sim A_r \tag{3}$$

или

$$A_1 \wedge \cdots \wedge A_s \Rightarrow A, \tag{4}$$

где все A — атомные формулы. Теперь ясно, что если (M_λ) — семейство Ω-структур, удовлетворяющих данной формуле вида (3) или (4), то их прямое произведение $\prod M_\lambda$ также удовлетворяет этой формуле; таким образом, получаем следующую теорему (см. Маккинси [43], Когаловский [59]):

***Теорема* 4.3.** *Универсальный класс моделей замкнут относительно прямых произведений тогда и только тогда, когда он определяется системой формул вида* (3) *или* (4). ▮

Тот же самый результат имеет место, если заменить «класс моделей» на «класс алгебр», что вытекает из относительности доказательства теоремы (см. § VI.1).

Формула вида (4) называется *хорновской формулой* (Хорн [51]), и всякое предложение, не обязательно универсальное, полученное из хорновской формулы применением кванторов, называется *хорновским предложением*. Далее, *хорновским классом* называется класс моделей, определяемый хорновскими предложениями. Универсальный хорновский класс алгебр называется *квазимногообразием* (или квазипримитивным классом). Теорема 4.3 показывает, что каждое квазимногообразие замкнуто относительно прямых произведений; наоборот, универсальный класс, замкнутый относительно прямых произведений, будет квазимногообразием, если в определяющих его формулах нет формул вида (3). Далее, тривиальная Ω-структура (т. е. полная одноэлементная Ω-структура) удовлетворяет каждой формуле (4), но не удовлетворяет формуле (3). Итак, получаем, что универсальный класс будет хорновским классом тогда и только тогда, когда он замкнут относительно прямых произведений и содержит тривиальную структуру [1]). Для алгебр это утверждение превращается в

***Следствие* 4.4.** *Универсальный класс алгебр является квазимногообразием тогда и только тогда, когда он замкнут относительно прямых произведений и содержит полную тривиальную алгебру.* ▮

В качестве примеров квазимногообразий упомянем полугруппы с сокращением, полугруппы, вложимые в группы (см. упражнение

---

[1]) См. также Кейслер (*Tran. Amer. Math. Soc.*, **117** (1965), 307—328), А. Д. Тайманов (*Изв. АН СССР*, серия матем., **30** (1966), 523—524). — *Прим. ред.*

2.4 и § VII.3), а также упорядоченные *полугруппы*. С *другой стороны*, линейно упорядоченные полугруппы не образуют квазимногообразия; не образуют квазимногообразия и области целостности.

Так как квазимногообразия замкнуты относительно подалгебр и прямых произведений, то в силу следствия III.5.2 получаем

***Предложение* 4.5.** *Каждое квазимногообразие обладает свободными алгебрами.* ∎

За дальнейшими результатами о квазимногообразиях, включая их абстрактную характеризацию (на языке категорий), отсылаем читателя к работам Мальцева [56], [58″].

Замечания, предшествующие следствию 4.4, дают удобную характеризацию универсальных **P**-замкнутых классов; для произвольных **P**-замкнутых классов не известно никакого столь же простого критерия. Любое хорновское предложение сохраняется при переходе к прямым произведениям и даже при переходе к приведенным произведениям (см. § V.5). Это было доказано Чжаном и Морелом [58], которые показали также, что существуют предложения, сохраняющиеся при переходе к прямым произведениям, но неэквивалентные никакому хорновскому предложению (см. упражнение 3). Кейслер [65] доказал, что класс моделей первого порядка замкнут относительно приведенных произведений тогда и только тогда, когда он является хорновским классом.

УПРАЖНЕНИЯ

1. Показать, что если $\mathcal{K}$ — универсальный класс алгебр, то подпрямые произведения $\mathcal{K}$-алгебр образуют квазимногообразие. Показать, что квазимногообразие, порожденное областями целостности, состоит из всех коммутативных колец без нильпотентных элементов (кроме нуля).

2. Показать, что каждое квазимногообразие порождается своими подпрямо неразложимыми элементами.

3. Получить элементарное предложение, выражающее тот факт, что булева алгебра тривиальна или содержит атом. Показать, что это предложение сохраняется при переходе к прямым произведениям, но не сохраняется при переходе к приведенным произведениям (Чжан и Морел [58]; в силу результата, упомянутого выше, это предложение неэквивалентно никакому хорновскому предложению.)

5. КЛАССЫ, ЗАМКНУТЫЕ ОТНОСИТЕЛЬНО ГОМОМОРФНЫХ ОБРАЗОВ

В силу «двойственности» между подмножествами и фактормножествами должна была бы существовать характеризация аксиоматизируемых **H**-замкнутых классов моделей. Такая характеризация действительно существует, но ни этот результат, ни его доказательство никоим образом не двойственны случаю наследственных классов, рассмотренному в § VI.2. Назовем предложение *положительным*, если оно получено из положительной формулы применением кванторов, и *отрицательным*, если оно может быть представлено как отрицание положительного предложения. Линдон [59′] показал, что аксиоматизируемый класс моделей **H**-замкнут тогда и только тогда, когда его можно определить положительными предложениями. При доказательстве требуется довольно тонкий анализ структуры формул, которые могут встретиться, и поэтому здесь мы ограничимся частным случаем универсальных классов над конечной областью предикатов. К этим классам применим принцип локализации (теорема 2.1), и можно дать доказательство, чем-то напоминающее доказательство теоремы 2.8, характеризующей наследственные аксиоматизируемые классы. В то же время это показывает ограниченность упомянутой выше двойственности. Начнем с леммы, которая играет роль леммы 2.4.

***Лемма* 5.1.** *Пусть Ω — конечная область и M — конечная Ω-структура. Тогда существует такое положительное универсальное предложение P, что P-моделями будут те и только те структуры, которые не обладают подструктурами, гомоморфно отображающимися на M.*

Доказательство. Пусть $M = \{a_1, \ldots, a_m\}$, и пусть N есть Ω-структура, которая обладает подструктурой, гомоморфно отображающейся на M. Это означает, что N содержит такие m элементов $b_1, \ldots, b_m$, что в N выполняются следующие условия:

$$b_i \neq b_j, \quad \text{если} \quad i \neq j, \tag{1}$$

$$\sim \omega(b_{i_1}, \ldots, b_{i_n}), \quad \text{если} \quad M \models \sim \omega(a_{i_1}, \ldots, a_{i_n}). \tag{2}$$

Действительно, в качестве b_i нужно только выбрать элемент структуры N, отображающийся в a_i при данном гомоморфизме. Обратно, если все формулы (1), (2) выполняются в N, то $b_i \to a_i$ будет гомоморфизмом подструктуры структуры N на M. Теперь число всех формул (1), (2) конечно, и каждая из формул является отрицанием атомной формулы. Поэтому их конъюнкция имеет вид $\sim P(b_1, \ldots, b_m)$, где P — положительная формула. По построению формулы P структура N обладает подструктурой, гомоморфно отображающейся на M, тогда и только тогда, когда

$$N \vdash \bigvee \sim P(i_1, \ldots, i_m),$$

и поэтому N не обладает такой подструктурой тогда и только тогда, когда

$$N \vdash \bigwedge P(i_1, \ldots, i_m).$$

Поскольку P — положительная формула, то это и есть предложение нужного вида. ∎

***Теорема* 5.2.** *Универсальный класс моделей над конечной областью предикатов тогда и только тогда замкнут относительно гомоморфных образов, когда его можно определить посредством универсальных положительных предложений.*

Доказательство. Ясно, что положительное предложение, выполняющееся в данной Ω-модели, выполняется и во всех ее гомоморфных образах; поэтому универсальный класс моделей, определяемый положительными предложениями, замкнут относительно гомоморфных образов (без всяких ограничений на размер Ω).

Пусть теперь $\mathscr{C}$ — универсальный класс моделей (над конечной областью Ω), замкнутый относительно гомоморфных образов. Ясно, что если $\mathscr{D}$ — класс моделей, определяемый всеми универсальными положительными предложениями, выполняющимися в $\mathscr{C}$, то

$$\mathscr{C} \subseteq \mathscr{D}; \tag{3}$$

доказательство будет завершено, если мы покажем, что в (3) имеет место равенство. Итак, предположим, что существует такая Ω-модель M, что

$$M \in \mathscr{D}, \quad M \notin \mathscr{C}. \tag{4}$$

Поскольку $\mathscr{C}$ сублокально определим (теорема 2.1), существует конечная подмодель модели M, не принадлежащая $\mathscr{C}$. Но всякая подмодель модели M снова лежит в $\mathscr{D}$, и, таким образом, в (4) можно считать M конечной. Пусть P—универсальное положительное предложение, характеризующее те Ω-модели, которые не обладают подмоделями, гомоморфно отображающимися на M. Если существует $\mathscr{C}$-модель, скажем N, для которой P не выполняется, то M является гомоморфным образом подмодели модели N и поэтому принадлежит $\mathscr{C}$. Но это противоречит (4); следовательно, каждая $\mathscr{C}$-модель удовлетворяет P. По определению класса $\mathscr{D}$ каждая $\mathscr{D}$-модель также должна удовлетворять P, тогда как M, очевидно, не удовлетворяет P. Последнее противоречит тому факту, что $M \in \mathscr{D}$, так что (4) невозможно, т. е. $\mathscr{C} = \mathscr{D}$. ∎

Если мы будем рассматривать только Ω-модели, являющиеся алгебрами (относительно некоторой подобласти Ω^*), то получим

***Следствие* 5.3.** *Универсальный класс Ω^*-алгебр (над конечной областью предикатов, содержащей Ω^*) замкнут относительно гомоморфных образов (алгебр) тогда и только тогда, когда его можно определить (относительно класса всех Ω^*-алгебр) положительными универсальными предложениями.* ∎

УПРАЖНЕНИЕ

1. Показать, что если P — универсальное предложение, то класс P-моделей замкнут относительно гомоморфных образов тогда и только тогда, когда P эквивалентно некоторому универсальному положительному предложению. (Воспользоваться следствием V.6.2 и компактностью.)

6. ХАРАКТЕРИЗАЦИЯ АКСИОМАТИЗИРУЕМЫХ КЛАССОВ МОДЕЛЕЙ

В силу теоремы V.6.4 типовой класс, т. е. объединение типов, аксиоматизируем тогда и только тогда, когда он замкнут относительно ультрапроизведений, но этот результат ничего не говорит нам о связях между Ω-структурами, принадлежащими одному и тому же типу. Покажем теперь, что две Ω-структуры принадлежат одному и тому же типу (т. е. неразличимы) тогда и только тогда, когда они обладают изоморфными ультрастепенями. Отсюда легко вывести критерий аксиоматизируемости произвольного класса моделей, не предполагая, что это типовой класс. Эти результаты принадлежат Кейслеру [61]; основной теоремой, из которой выводятся все остальные, является теорема 6.2, приведенная ниже. Однако при доказательстве этой теоремы (и ее следствий) придется сделать одно дополнительное предположение, которое мы сейчас обсудим.

Если α — некоторое бесконечное кардинальное число, то существуют кардинальные числа, большие α, например 2^α, и, следовательно, существует наименьшее такое кардинальное число. Это наименьшее кардинальное число, большее чем α, мы обозначим через α^+; по теореме I.5.6 имеем

$$\alpha^+ \leqslant 2^\alpha. \tag{1}$$

В частности, если $\alpha = \aleph_0$, то $2^{\aleph_0}$ — мощность действительной прямой («континуум»), и канторова *гипотеза континуума* утверждает, что для $\alpha = \aleph_0$ в (1) имеет место равенство, т. е. (после подстановки $\aleph_1$ вместо $\aleph_0^+$)

$$\aleph_1 = 2^{\aleph_0}. \tag{2}$$

Утверждение

$$\alpha^+ = 2^\alpha \text{ для любого бесконечного кардинального числа } \alpha \tag{3}$$

называется *обобщенной гипотезой континуума*. Эта гипотеза до сих пор не доказана даже для $\alpha = \aleph_0$, хотя Гёдель [40] показал ее непротиворечивость с аксиомами теории множеств в предположении, что эти аксиомы непротиворечивы. При этом не обязательно включать аксиому выбора; ее непротиворечивость доказывается тем же способом. Далее, вместо существования универсальных множеств Гёдель предполагает только существование бесконечных множеств. Поэтому если принять аксиоматическую точку зрения, то имеет смысл включить (3) в качестве аксиомы (особенно ввиду того, что (3) не зависит от других аксиом теории множеств, как показал Коэн [63]). Существует также более наивная точка зрения, утверждающая, что при более тонком анализе интуитивного понятия множества можно будет выделить дополнительное утверждение о множествах, которое интуитивно «очевидно» и которое, взятое в качестве аксиомы, будет обеспечивать вместе с другими аксиомами справедливость равенства (3). (Однако если кто-либо готов положиться на интуицию, то он должен также быть готовым к противоположному заключению, что (3) может оказаться «очевидным образом» ложным.) Читатель может найти более подробное обсуждение этого вопроса в работе Гёделя [47]; здесь мы не будем придерживаться этой точки зрения, но впредь будем предполагать выполненным (3). Всякий результат, при доказательстве которого используется (3), будет помечен символом ОГК (обобщенная гипотеза континуума).

Прежде чем переходить к основному результату, докажем лемму, обобщающую предложение I.5.8. Если α — некоторое порядковое число, то под α-последовательностью будем подразумевать семейство, заиндексированное с помощью α. Отождествим, далее, любое кардинальное число α с первым порядковым числом мощности α.

***Лемма* 6.1.** *Пусть α — бесконечное кардинальное число, β — такое порядковое число, что $\beta \leqslant \alpha$, и $(X_\xi)_{\xi<\beta}$ есть β-последовательность множеств, каждое из которых имеет мощность α. Тогда каждое X_ξ содержит такое подмножество Y_ξ снова мощности α, что (Y_ξ) образует непересекающееся семейство.*

Заметим, что если через $\Phi_{\alpha\beta}$ обозначить утверждение леммы, то $\Phi_{\alpha\beta}$ влечет равенство

$$\alpha\beta = \alpha \quad \text{для} \quad \beta \leqslant \alpha \ (\text{и } \alpha \geqslant \aleph_0), \tag{4}$$

и, в частности,

$$\alpha^2 = \alpha \qquad (\alpha \geqslant \aleph_0). \tag{5}$$

Действительно, если взять какое-либо множество X мощности α и положить $X_\xi = X$ для $\xi < \beta$, то в силу $\Phi_{\alpha\beta}$ существует β-последовательность непересекающихся подмножеств множества X, каждое из которых мощности α, откуда $\alpha\beta \leqslant \alpha$. Так как обратное неравенство очевидно, то отсюда вытекает (4).

Для доказательства леммы достаточно, очевидно, рассмотреть случай $\beta = \alpha$; воспользуемся трансфинитной индукцией по α. Пусть γ — такое произвольное порядковое число, что $\gamma < \alpha$, и предположим, что для каждой пары ξ, η порядковых чисел, меньших γ, мы имеем такую η-последовательность $Y_{\xi\eta}$, что

(i) $Y_{\xi\eta}$ — последовательность различных элементов множества X_ξ;

(ii) если $\eta' < \eta$, то $Y_{\xi\eta'}$ — левый отрезок последовательности $Y_{\xi\eta}$;

(iii) для $\xi' \neq \xi$ $\quad Y_{\xi'\eta'} \cap Y_{\xi\eta} = \varnothing$.

Если γ — предельное порядковое число, то определим $Y_{\xi\gamma}$ по формуле

$$Y_{\xi\gamma} = \bigcup_{\eta < \gamma} Y_{\xi\eta};$$

тогда все $Y_{\xi\gamma}$ снова попарно не пересекаются и каждое $Y_{\xi\gamma}$ является γ-последовательностью различных элементов множества X_ξ. Если γ — не предельное порядковое число, скажем $\gamma = \delta + 1$, то определим $Y_{\xi\gamma}$ (трансфинитной индукцией по ξ), присоединяя к $Y_{\xi\delta}$ один элемент из X_ξ таким образом, чтобы оставались справедливыми условия (i) — (iii) для $\eta = \gamma$. Это всегда возможно, поскольку в силу (5) $\left|\bigcup_\xi Y_{\xi\gamma}\right| = |\gamma|^2 = |\gamma|$ (используется предположение индукции относительно γ), тогда как $|X_\xi| = \alpha > |\gamma|$. Определив $Y_{\xi\gamma}$, можно теперь определить $Y_{\gamma\gamma}$, выбирая некоторую последовательность различных элементов множества X_γ, не принадлежащих $\bigcup Y_{\xi\gamma}$. Это снова возможно в силу (5), и $Y_{\gamma\eta}$ для $\eta < \gamma$ определяется как подходящий левый отрезок последовательности $Y_{\gamma\gamma}$. Таким образом, по индукции для каждой пары ξ, $\eta < \alpha$ получаем $Y_{\xi\eta}$, удовлетворяющие условиям (i) — (iii). Положим теперь

$$Y_\xi = \bigcup_{\eta < \alpha} Y_{\xi\eta};$$

тогда Y_ξ есть α-последовательность различных элементов множества X_ξ, причем в силу (iii) $Y_\xi \cap Y_{\xi'} = \varnothing$ для $\xi \neq \xi'$, что и требовалось. ∎

Теорема 6.2 (ОГК). (Кейслер [61].) *Пусть α — кардинальное число, не меньшее $\max\{|\Omega|, \aleph_0\}$, и пусть I — некоторое множество мощности α. Тогда для любых двух семейств $(A_i)_{i\in I}$, $(B_i)_{i\in I}$ Ω-структур мощности, не большей α^+, следующие два утверждения эквивалентны:*

(i) *существуют такие ультрафильтры Фреше $\mathscr{D}$, $\mathscr{E}$ на I, что*

$$\prod A_i/\mathscr{D} \cong \prod B_i/\mathscr{E};$$

(ii) *для любого элементарного предложения P либо*

$$|\{i \in I \mid A_i \vdash P\}| = \alpha, \tag{6}$$

либо

$$|\{i \in I \mid B_i \vdash \sim P\}| = \alpha. \tag{7}$$

Доказательство. (i)$\Rightarrow$(ii). Если P выполняется меньше чем на α структурах A_i, то $\sim P$ выполняется для всех A из некоторого $\mathscr{D}$-множества и поэтому выполняется в ультрапроизведении. В силу изоморфизма (i) $\sim P$ выполняется во всех B из некоторого $\mathscr{E}$-множества, откуда вытекает (7).

(ii) $\Rightarrow$ (i). Положим $A = \prod A_i$, $B = \prod B_i$ и через ε_i: $A \to A_i$, ζ_i: $B \to B_i$ обозначим соответствующие проекции. Затем вполне упорядочим A и B: $A = (a_\xi)_{\xi < \alpha^+}$, $B = (b_\xi)_{\xi < \alpha^+}$; отметим, что здесь была использована ОГК при проверке того, что A и B могут быть заиндексированы порядковыми числами, меньшими чем α^+. Однако каждое порядковое число может быть однозначно представлено в виде $\lambda + n$, где λ — предельное порядковое число (или нуль) и n — натуральное число (см. упражнение I.5.5). Наша первая задача состоит в том, чтобы построить такие α-последовательности (a'), (b') в A и B соответственно, что для любого предельного порядкового числа λ и любого натурального n

(a) $a'_{\lambda+2n} = a_{\lambda+n}$;

(b) $b'_{\lambda+2n+1} = b_{\lambda+n}$;

(c) для любого элементарного предложения P над Ω и α-последовательности унарных предикатов через $\langle A_i, a'\varepsilon_i\rangle$ обозначим унарное расширение Ω-структуры A_i, в котором унарные предикаты являются постоянными операторами со значениями $a'_\xi\varepsilon_i$, и аналогично для $\langle B_i, b'\zeta_i\rangle$; тогда либо

$$|\{i \in I \mid \langle A_i, a'\varepsilon_i\rangle \vdash P\}| = \alpha, \tag{8}$$

либо

$$|\{i \in I \mid \langle B_i, b'\zeta_i\rangle \vdash \sim P\}| = \alpha. \tag{9}$$

Это построение можно выполнить с помощью трансфинитной индукции: если (a'_ξ), (b'_ξ) уже построены для $\xi < \gamma$, так что выполняются условия (a) — (c), то определим a'_γ и b'_γ следующим образом:

а) $\gamma = \lambda + 2n$, *где* λ — *предельное порядковое число или нуль, а* n — *натуральное число*. Положим $a'_{\lambda+2n} = a_{\lambda+n}$ и обозначим через Γ множество, состоящее из формул $P(k)$ над Ω и такой γ-последовательности $(\rho_\xi)_{\xi<\gamma}$ унарных предикатов, что мощность множества индексов $i \in I$, для которых

$$\langle A_i, a'\varepsilon_i\rangle \sim\vdash \bigvee_k (\rho_\gamma(k) \wedge P(k)), \tag{10}$$

т. е.

$$\langle A_i, (a'_\xi\varepsilon_i)_{\xi<\gamma}\rangle \models \sim P(a_{\lambda+n}\varepsilon_i),$$

меньше α. Поскольку $|\gamma| \leqslant \alpha$ и мощность множества всех формул не превосходит α, отсюда вытекает, что $|\Gamma| \leqslant \alpha$. Для каждого $P \in \Gamma$ положим

$$X_P = \left\{ i \in I \mid \langle B_i, b'\zeta_i\rangle \vdash \bigvee_k P(k)\right\}. \tag{11}$$

В силу (c) для $\bigvee_k P(k)$ вместо P видим, что $|X_P| = \alpha$, если только $P \in \Gamma$. Воспользуемся теперь леммой 6.1, чтобы заменить X_P таким подмножеством X'_P, что $|X'_P| = \alpha$ и X'_P попарно не пересекаются. Тогда в силу (11) существует такой элемент $f \in B$, что

$$\langle B_i, b'\zeta_i\rangle \vDash P(f\zeta_i) \quad \text{для} \quad i \in X'_P. \tag{12}$$

Если мы определим $b'_{\lambda+2n}$ равенством

$$b'_{\lambda+2n} = f,$$

то (c) выполняется для $\gamma = \lambda + 2n$. Действительно, если $\sim P$ выполняется меньше чем в α структурах $\langle A_i, (a'_\xi \varepsilon_i)_{\xi < \gamma+1}\rangle$ и если ρ_γ не встречается в P, то по предположению индукции (в силу (c)) *P выполняется в α структурах $\langle B_i, (b'_\xi \zeta_i)_{\xi < \gamma+1}\rangle$, тогда как если ρ_γ* встречается в P, скажем $P = P(\rho_\gamma)$, то в силу (10) $P(k) \in \Gamma$ и поэтому (12) показывает, что P выполняется в α структурах $\langle B_i, (b'_\xi \zeta_i)_{\xi < \gamma+1}\rangle$.

b) $\gamma = \lambda + 2n + 1$. Здесь мы просто повторим то же построение, поменяв ролями a' и b'.

Для $\gamma = 1$ предположение (c) превращается в точности в условие (ii), которое, как предполагалось, выполняется, и поэтому мы получаем структуры $A_i^* = \langle A_i, a'\varepsilon_i\rangle$ и $B_i^* = \langle B_i, b'\zeta_i\rangle$ над Ω^*, унарным расширением Ω при помощи α унарных предикатов. Для каждого элементарного предложения P над Ω^* определим два подмножества множества I:

$$Y_P = \{i \in I \mid A_i^* \vdash P\},$$
$$Z_P = \{i \in I \mid B_i^* \vdash P\}.$$

Ясно, что $Y_{\sim P} = I \setminus Y_P$, $Y_{P \wedge Q} = Y_P \cap Y_Q$ и аналогично для Z. Кроме того, в силу (c) либо P выполняется для α структур A_i^*, либо $\sim P$ выполняется для α структур B_i^*; итак, если через $\Phi(I)$ обозначим минимальный фильтр Фреше на I, то либо $Y_{\sim P} \notin \Phi(I)$, либо $Z_P \notin \Phi(I)$. При замене P на $\sim P$ это показывает, что

$$\text{если } Y_P \in \Phi(I), \text{ то } Z_{\sim P} \notin \Phi(I). \tag{13}$$

Пусть $\mathscr{E}_0$ — множество всех таких Z_P, что $Y_P \in \Phi(I)$. Тогда $\mathscr{E}_0$ *замкнуто относительно конечных* пересечений, а в силу (13) каждое $\mathscr{E}_0$-множество имеет мощность α. Следовательно, по предложению V. 2.10 существует ультрафильтр Фреше $\mathscr{E}$, содержащий $\mathscr{E}_0$. Далее, пусть $\mathscr{D}_0$ — множество всех таких Y_P, что $Z_P \in \mathscr{E}$; тогда $\mathscr{D}_0$ снова будет базой фильтра, и каждое $\mathscr{D}_0$-множество имеет мощность α, поскольку любое $J \in \mathscr{D}_0$ имеет вид $J = Y_P$, где $Z_P \in \mathscr{E}$, откуда $Z_{\sim P} \notin \mathscr{E}_0$, и поэтому, в силу определения $\mathscr{E}_0$, $Y_{\sim P} \notin \Phi(I)$, т. е. $|J| = \alpha$. Отсюда вытекает, что существует ультрафильтр Фреше $\mathscr{D}$, содержащий $\mathscr{D}_0$.

Если P — некоторое предложение над Ω^*, то

$$Y_P \in \mathscr{D} \text{ тогда и только тогда, когда } Z_P \in \mathscr{E}.$$

Действительно, если $Y_P \in \mathscr{D}$, то $Y_{\sim P} \notin \mathscr{D}$, откуда $Y_{\sim P} \notin \mathscr{D}_0$, и поэтому $Z_{\sim P} \notin \mathscr{E}$; следовательно, $Z_P \in \mathscr{E}$. Обратно, если $Z_P \in \mathscr{E}$, то $Y_P \in \mathscr{D}_0$ и поэтому $Y_P \in \mathscr{D}$. Рассмотрим теперь соответствие $a'_\xi \longleftrightarrow b'_\xi$ между A и B. Если $a'_\xi \equiv a'_\eta (\operatorname{mod} \mathscr{D})$, то предложение

$$\bigvee_k (\rho_\xi(k) \wedge \rho_\eta(k))$$

выполняется на $\mathscr{D}$-множестве структур $\overset{*}{A_i}$, и поэтому оно выполняется на $\mathscr{E}$-множестве структур $\overset{*}{B_i}$, т. е. $b'_\xi \equiv b'_\eta (\operatorname{mod} \mathscr{E})$; в силу симметрии справедливо также обратное утверждение. Это означает, что соответствие $a'_\xi \to b'_\xi$ индуцирует взаимно однозначное соответствие между $A/\mathscr{D}$ и $B/\mathscr{E}$. Кроме того, предложение P выполняется в $\langle A/\mathscr{D}, a'/\mathscr{D}\rangle$ тогда и только тогда, когда $Y_P \in \mathscr{D}$, т. е. $Z_P \in \mathscr{E}$, т. е. тогда и только тогда, когда P выполняется в $\langle B/\mathscr{E}, b'/\mathscr{E}\rangle$. Поэтому соответствие $a'_\xi/\mathscr{D} \longleftrightarrow b'_\xi/\mathscr{E}$ является изоморфизмом, т. е. $A/\mathscr{D} \cong B/\mathscr{E}$. ∎

Из теоремы 6.2 вытекают следующие утверждения (Кейслер [61]):

***Теорема* 6.3 (*ОГК*).** *Две Ω-структуры M и N неразличимы тогда и только тогда, когда существуют изоморфные ультрастепени $M^I/\mathscr{D}$ и $N^I/\mathscr{E}$ Ω-структур M и N соответственно. Здесь I можно считать произвольным множеством мощности α, где $\alpha \geqslant \max\{|\Omega|, \aleph_0\}$ и $\alpha^+ \geqslant \max\{|M|, |N|\}$.*

Это вытекает из теоремы 6.2, если взять $A_i = M$, $B_i = N$. ∎

В следующих результатах для любого класса моделей $\mathscr{K}$ через $\mathscr{K}'$ обозначается класс всех структур, не принадлежащих $\mathscr{K}$.

***Следствие* 6.4 (*ОГК*).** *Класс моделей $\mathscr{K}$ является типовым классом тогда и только тогда, когда оба класса $\mathscr{K}$ и $\mathscr{K}'$ замкнуты относительно ультрастепеней.*

Действительно, если $\mathscr{K}$ — типовой класс, то $\mathscr{K}'$ — также типовой класс, а всякий типовой класс замкнут относительно ультрастепеней в силу следствия V.6.5. Обратно, если оба класса $\mathscr{K}$ и $\mathscr{K}'$ замкнуты относительно ультрастепеней, то по теореме 6.3 каждая $\mathscr{K}$-модель различима с каждой $\mathscr{K}'$-моделью, откуда $\mathscr{K}$ — типовой класс. ∎

***Следствие* 6.5 (*ОГК*).** *Класс моделей $\mathscr{K}$ аксиоматизируем тогда и только тогда, когда $\mathscr{K}$ замкнут относительно ультрапроизведений и $\mathscr{K}'$ замкнут относительно ультрастепеней.*

В самом деле, эти условия необходимы в силу следствия V.6.4; если же они выполняются, то $\mathscr{K}$ — типовой класс в силу следствия 6.4 и, следовательно, аксиоматизируем в силу следствия V.6.4. ∎

***Следствие* 6.6 (*ОГК*).** *Класс моделей $\mathscr{K}$ элементарен тогда и только тогда, когда оба класса $\mathscr{K}$ и $\mathscr{K}'$ замкнуты относительно ультрапроизведений.*

Это вытекает из предыдущего результата и следствия V.6.2. ∎

В качестве еще одного следствия теоремы 6.3 отметим, что для любой бесконечной Ω-структуры M и любой данной мощности α существует ультрастепень Ω-структуры M, мощность которой больше α. Действительно, в силу следствия 3.7 существует Ω-структура N мощности, большей α, неразличимая с M. Теперь любая ультрастепень Ω-структуры N имеет мощность не меньше $|N|$ (см. упражнение 3.1), и поэтому сформулированный результат вытекает из теоремы 6.3. Получаемая отсюда информация не очень определенна, но во всяком случае интересна тем, что дает более прямую оценку мощности ультрастепени. В простейшем случае получаем следующий результат, принадлежащий Халмошу и Кочену, доказательство которого не связано с предшествующими теоремами (Кочен [61]; относительно близких результатов см. Фрейн, Морел и Скотт [62]).

***Теорема* 6.7.** *Пусть $(M_n)_{n \in N}$ — такая последовательность конечных множеств, что для каждого конечного числа k лишь конечное число множеств M_n имеет мощность k. Тогда если $\mathscr{D}$ — некоторый неглавный ультрафильтр на множестве положительных целых чисел N, то $M_{\mathscr{D}} = \prod M_n/\mathscr{D}$ имеет мощность $2^{\aleph_0}$.*

Доказательство. Ясно, что

$$|M_{\mathscr{D}}| \leqslant |\prod M_n| = 2^{\aleph_0},$$

поэтому для завершения доказательства нужно только построить взаимно однозначное отображение $2^N \to M_{\mathscr{D}}$. Можно предполагать, что множества M_n упорядочены по величине, т. е. перенумерованы так, что $m \leqslant n$ влечет $|M_m| \leqslant |M_n|$. Положим $\Gamma = 2^N$; тогда Γ может быть реализовано в виде множества всех последовательностей из 0 и 1; через Γ_k обозначим множество конечных последовательностей длины k. Каждое Γ_k конечно, и для данного n через k_n обозначим такое наибольшее целое число k, что $|\Gamma_k| \leqslant |M_n|$. Отсюда вытекает, что существует взаимно однозначное отображение

$$\varphi_n\colon \Gamma_{k_n} \to M_n$$

и, кроме того,

$$|\Gamma_{k_n}| \leqslant |M_{n'}| \text{ для всех } n' \geqslant n.$$

Определим теперь φ: $\Gamma \to \prod M_n$ следующим образом. Если $\gamma \in \Gamma$ и γ_k состоит из первых k членов последовательности γ, то положим

$$(\gamma\varphi)_n = \gamma_{k_n}\varphi_n.$$

Если h: $\prod M_n \to \prod M_n/\mathscr{D}$ — естественное отображение nat $\mathscr{D}$, то мы утверждаем, что φh: $\Gamma \to M_{\mathscr{D}}$ взаимно однозначно. Действительно, если γ, $\delta \in \Gamma$ и $\gamma \neq \delta$, то для некоторого n_0 $\gamma_n \neq \delta_n$ для всех $n \geqslant n_0$, и так как дополнение любого конечного множества лежит в $\mathscr{D}$, то $\gamma\varphi h \neq \delta\varphi h$. ∎

Если даны два семейства множеств (M_i), (N_i) над одним и тем же множеством индексов I и ультрафильтр $\mathscr{D}$ на I, то мы можем построить ультрапроизведения $M_{\mathscr{D}} = \prod M_i/\mathscr{D}$ и $N_{\mathscr{D}} = \prod N_i/\mathscr{D}$. Ясно, что любое семейство отображений φ_i: $M_i \to N_i$ продолжается до отображения произведений φ: $\prod M_i \to \prod N_i$; более того, элементы, сравнимые друг с другом по mod $\mathscr{D}$, отображаются в элементы, сравнимые по mod $\mathscr{D}$, так что мы получаем отображение $\varphi_{\mathscr{D}}$: $M_{\mathscr{D}} \to N_{\mathscr{D}}$. Заметим, что $\varphi_{\mathscr{D}}$ взаимно однозначно тогда и только тогда, когда φ_i взаимно однозначно для всех i, принадлежащих некоторому $\mathscr{D}$-множеству; в частности, если каждое φ_i взаимно однозначно, то $\varphi_{\mathscr{D}}$ также взаимно однозначно. Отсюда вытекает, что мощность $|M_{\mathscr{D}}|$ является возрастающей функцией мощности каждого из сомножителей. Выбирая I и каждое M_i счетными и применяя теорему 6.7, получаем

***Следствие* 6.8.** *Любое ультрапроизведение счетного семейства счетных множеств относительно неглавного ультрафильтра имеет мощность* $2^{\aleph_0}$. ∎

Это применимо, в частности, к счетным ультрастепеням счетных множеств.

УПРАЖНЕНИЕ

1. Показать, что теорема 6.7 не имеет места, если имеется бесконечно много множеств данной (конечной) мощности k. (Построить ультрафильтр Фреше, содержащий N_0, где N_0 — множество индексов, для которых $|M_n| = k$.)

ГЛАВА VII

ПРИЛОЖЕНИЯ

В первых шести главах был рассмотрен ряд приложений общей теории к частным случаям. Однако чаще всего конкретная проблема распадается на две части, одна из которых, относящаяся к универсальной алгебре, сравнительно проста, но после ее решения остается еще сделать более существенную часть работы. Типичным примером является задача об универсальном отображении, в которой доказательство того, что универсальный функтор инъективен, часто оказывается наиболее трудной частью, и универсальная алгебра здесь мало чем может помочь. Тем не менее использование универсальной алгебры часто помогает упростить доказательство, выявляя истинную природу того, что нужно доказать. Эта точка зрения иллюстрируется приложениями, которые изложены в этой главе.

1. НАТУРАЛЬНЫЕ ЧИСЛА

Натуральные числа бегло рассматривались уже в главе I, где в общих чертах был изложен способ их определения в пределах основ общей теории множеств. Кроме этого метода, идущего от Фреге, существует аксиоматический подход, принадлежащий Пеано. По духу этот подход ближе к абстрактной алгебре, и теперь мы рассмотрим натуральные числа с этой точки зрения. В основном мы будем придерживаться очень прозрачного изложения Хенкина [60], к которому отсылаем читателя за дальнейшими деталями и ссылками.

В основу своей теории Пеано полагает следующие пять аксиом:

P. 1. *0 есть натуральное число.*

P. 2. *Каждое натуральное число x обладает однозначно определенным, непосредственно следующим за ним натуральным числом x'.*

P. 3. $x' \neq 0$ *для любого* x.

P. 4. *Если* $x' = y'$, *то* $x = y$.

P. 5 (принцип индукции). *Любое множество натуральных чисел, содержащее 0 и вместе с каждым натуральным числом x содержащее* непосредственно следующее за ним число x', содержит все натуральные числа.

Первые четыре аксиомы можно записать в виде элементарных предложений; возьмем унарный предикат ν (который будет играть роль 0) и бинарный предикат σ (который будет играть роль функции «непосредственного следования за»). Тогда эти аксиомы примут вид

P′.1. $\bigvee_i \bigwedge_j [\nu(i) \wedge (\nu(j) \Rightarrow (i = j))]$.

P′.2. $\bigwedge_i \bigvee_j \bigwedge_k [\sigma(i, j) \wedge (\sigma(i, k) \Rightarrow (j = k))]$.

P′.3. $\bigwedge [\sigma(i, j) \Rightarrow \sim \nu(j)]$.

P′.4. $\bigwedge [(\sigma(i, k) \wedge \sigma(j, k)) \Rightarrow (i = j)]$.

Для принципа индукции (P.5) никакая такая запись невозможна, поскольку, как мы увидим в дальнейшем, существуют системы, удовлетворяющие всем элементарным предложениям, выполняющимся для натуральных чисел, но не удовлетворяющие принципу индукции.

Мы не будем здесь заниматься вопросом, существуют ли системы, удовлетворяющие аксиомам P.1—5; для нас этот вопрос решен положительно аксиомами теории множеств в главе I. Пусть N — некоторая система, удовлетворяющая P.1—5; в этом случае P.2 утверждает, что существует унарная операция, определенная на N, тогда как P. 1 постулирует существование в N отмеченного элемента, т. е. постоянного оператора. Поэтому можно считать N алгеброй с 0-арным оператором, нулем, и унарным оператором, функцией «непосредственного следования за». Иными словами, P.5 утверждает, что в N нет собственных подалгебр или, эквивалентно этому, что N порождается пустым множеством.

Руководствуясь этими рассмотрениями, определим *индуктивную алгебру* как алгебру с постоянным оператором (обозначаемым 0), унарным оператором (обозначаемым $x \to x'$) и с пустым множеством как множеством образующих. Индуктивная алгебра называется *числовой*, если она удовлетворяет также P. 3—4. Теперь обычное развитие теории целых чисел на основе аксиом Пеано показывает, что на самом деле существует единственная числовая алгебра. Мы получим этот результат в качестве следствия теоремы:

***Теорема* 1.1.** *Всякая числовая алгебра является свободной индуктивной алгеброй с $\varnothing$ в качестве множества свободных образующих.*

Будем доказывать эту теорему с помощью следующей леммы.

Лемма. *Каждый элемент $\neq 0$ индуктивной алгебры A является непосредственно следующим за некоторым элементом алгебры A.*

Действительно, множество элементов, непосредственно следующих за каким-либо элементом алгебры A, вместе с 0 является подалгеброй и, следовательно, совпадает с A. ∎

Для доказательства теоремы возьмем числовую алгебру N и произвольную индуктивную алгебру I. Нужно найти гомоморфизм $N \to I$; этот гомоморфизм обязательно будет эпиморфизмом, и отсюда будет следовать сформулированный результат. Построим прямое произведение $N \times I$; подалгебра H, порожденная пустым множеством $\varnothing$, снова будет индуктивной алгеброй. Пусть теперь ε — ограничение проекции $N \times I \to N$ на H. Образ подалгебры H будет подалгеброй в N и, следовательно, должен совпадать с N. Мы утверждаем, что ε взаимно однозначно; это равносильно утверждению: для каждого $x \in N$

$$\text{существует такой единственный } y \in I, \text{ что } (x, y) \in H. \tag{1}$$

Пусть S — подмножество алгебры N, состоящее из всех элементов $x \in N$, удовлетворяющих (1); тогда если мы покажем, что S — подалгебра в N, то из этого будет вытекать, что $S = N$, а это и нужно показать.

(i) $0 = (0, 0) \in H$; если $(0, y) \in H$ для некоторого $y \neq 0$, то $(0, y) \neq 0$ и, следовательно, по лемме $(0, y) = (u, v)' = (u', v')$, т. е. $u' = 0$. Но это противоречит P.3; поэтому $(0, y) \in H$ только в том случае, если $y = 0$, откуда вытекает, что $0 \in S$.

(ii) Если $x \in S$, то существует такой y, что $(x, y) \in H$ и, следовательно, $(x', y') \in H$. Предположим, что (x', y_1), $(x', y_2) \in H$; тогда, поскольку $x' \neq 0$, отсюда вытекает, что $(x', y_i) \neq 0$, и поэтому (x', y_i) непосредственно следует за некоторым элементом в H, скажем $(x', y_i) = (u_i, v_i)' = (u_i', v_i')$, где $(u_i, v_i) \in H$. Теперь $u_1' = x' = u_2'$ и в силу P.4 $u_1 = u_2 = x$. Так как $x \in S$ и $(x, v_i) \in H$ $(i = 1, 2)$, то отсюда вытекает, что $v_1 = v_2$; поэтому $v_1' = v_2'$, т. е. $y_1 = y_2$. Итак, x' удовлетворяет (1), и поэтому $x' \in S$.

Теперь мы показали, что $S = N$, т. е. (1) имеет место для всех $x \in N$. Пусть $x\theta$ — тот единственный элемент y алгебры I, который определяется в силу (1); тогда $\theta\colon N \to I$ — нужный гомоморфизм. ∎

Поскольку числовые алгебры существуют, отсюда вытекает, что свободная индуктивная алгебра (которая единственна с точностью до изоморфизма) удовлетворяет P.3—4, и мы получаем

***Следствие* 1.2.** *Числовая алгебра единственна с точностью до изоморфизма.* ∎

На теореме 1.1 основано понятие определения по индукции. Это проще всего объяснить на примере сложения. Пусть N — числовая алгебра, и для любого $a \in N$ через N_a обозначим подмножество алгебры N, порожденное элементом a с помощью функции непосредственного следования. Это множество N_a само можно считать индуктивной алгеброй с элементом a в качестве нулевого элемента. Следовательно, по теореме 1.1 существует гомоморфизм α_a: $N \to N_a$. Подробнее это означает, что

$$0\alpha_a = a, \quad x'\alpha_a = (x\alpha_a)'.$$

Если гомоморфизм α_a обозначить через $+a$, то эти равенства примут привычную форму

$$0 + a = a, \qquad x' + a = (x + a)'.$$

Важно отметить, что, тогда как для метода доказательства по индукции нужна только аксиома P.5 и поэтому этот метод применим в любой индуктивной алгебре, определение по индукции обычно требует дополнительной проверки его корректности. Например, при определении сложения в N нужно показать, что гомоморфизм из N на N_a существует; конечно, это сразу вытекает из находящейся в нашем распоряжении теоремы 1.1 (в большинстве случаев проводится непосредственная проверка на основе аксиом P.3—4).

Рассмотрим теперь определение умножения в N; умножение является отображением μ_a алгебры N в себя (для каждого $a \in N$), удовлетворяющим равенствам

$$0\mu_a = 0, \qquad x'\mu_a = x\mu_a + a.$$

Поскольку N в действительности является алгеброй слов, то существует единственное отображение μ_a: $N \to N$, удовлетворяющее этим равенствам (см. упражнение III.7.6). Аналогичное определение можно получить для любой функции на N. Предоставляем читателю провести подробно соответствующие рассуждения.

В заключение приведем пример структуры, неразличимой со структурой натуральных чисел, но и неизоморфной ей. Такая структура называется *нестандартной моделью* натуральных чисел. Пусть N — множество натуральных чисел, рассматриваемое как числовая алгебра, а $M = N^N/\mathscr{D}$ — ультрастепень относительно неглавного ультрафильтра $\mathscr{D}$ на N. Тогда по теореме об ультрапроизведениях (теорема V.5.1) M и N неразличимы, но и неизоморфны, поскольку в силу следствия VI.6.8 M несчетна и поэтому даже не равномощна N. Можно также непосредственно проверить, что M не удовлетворяет P.5; подалгебра алгебры M, порожденная пустым множеством $\varnothing$, состоит из всевозможных отображений $N \to N$, постоянных на некотором $\mathscr{D}$-множестве. Но $\mathscr{D}$ — неглавный ультрафильтр и поэтому не содержит конечных множеств; таким образом, тождественное отображение на N не постоянно ни на каком $\mathscr{D}$-множестве и поэтому не принадлежит минимальной подалгебре алгебры M; следовательно, M обладает собственной подалгеброй, что противоречит P.5.

Аналогично можно построить нестандартные модели теории множеств, аксиоматически определенные с помощью бинарного отношения $\in$ (и отношения равенства). Например, если $\mathfrak{S}$ — класс всех порядковых чисел в данном универсальном множестве, то $\mathfrak{S}$ будет моделью теории множеств в этом смысле, и всякая ультрастепень модели $\mathfrak{S}$ снова будет моделью теории множеств. Однако эта ультрастепень будет в общем случае упорядочена, но не вполне упорядочена (см. Вопенка [62]; также см. упражнение 8 ниже). В главе I мы миновали эти трудности, допустив относительно наивную точку зрения, согласно которой аксиомы рассматривались как самоочевидные утверждения об интуитивно известных понятиях. Взглянув на эти аксиомы, читатель убедится, что, конечно, не все они могут быть записаны в виде элементарных предложений, и было бы бесполезно допускать неэлементарные аксиомы, если это не может быть сделано без предположения существования теории множеств.

Возвращаясь к натуральным числам, мы могли бы попытаться формализовать Р.5, допустив кванторы над множествами элементов, так же как над самими элементами. Но даже и тогда нужно оговорить, что используется стандартная интерпретация, в которой переменные множества пробегают все подмножества данной структуры, а это требование нельзя формализовать внутри этой системы, по крайней мере не расширяя ее нежелательным образом.

УПРАЖНЕНИЯ

1. Показать, что любая индуктивная алгебра I, не являющаяся свободной, определяется однозначно с точностью до изоморфизма такими двумя числами r, n ($r \geqslant 0$, $n \geqslant 1$), что если через θ: $N \to I$ обозначен тот единственный гомоморфизм, который был построен в теореме 1.1, то $x\theta = y\theta$ тогда и только тогда, когда $x \geqslant r$, $y \geqslant r$ и $x \equiv y \pmod n$. В следующих ниже упражнениях так определенная индуктивная алгебра обозначается через $I_{r,\,n}$.

2. Показать, что всякая индуктивная алгебра I относительно свободна; вывести отсюда, что к эндоморфизмам алгебры I можно применить определение по индукции, и воспользоваться этим для определения сложения в I. Можно ли определить в I умножение? Можно ли определить в I возведение в степень?

3. Доказать непосредственно, что всякая индуктивная алгебра удовлетворяет либо Р.3, либо Р.4.

4. Описать все индуктивные алгебры, удовлетворяющие Р.6: $x' \neq x$ для всех x.

5. Провести подробное доказательство возможности индуктивного определения для свободных индуктивных алгебр, т. е. показать, что если N — свободная индуктивная алгебра, то для любых $a \in N$ и $f \in I^N$ (где I — некоторая индуктивная алгебра) существует единственное отображение θ: $N \to I$, для которого $0\theta = a$, $x'\theta = f(x)$.

6. Доказать непосредственно, что свободная индуктивная алгебра удовлетворяет Р. 3—4. (Рассмотреть подходящие отображения этой алгебры в $I_{0,2}$.)

7. Используя только 0 и функцию непосредственного следования, записать в виде элементарных предложений тот факт, что натуральные числа образуют линейно упорядоченное множество. Вывести отсюда, что всякая ультрастепень натуральных чисел линейно упорядочена.

8. Доказать, что нельзя записать в виде элементарных предложений тот факт, что натуральные числа вполне упорядочены. (Построить ультрастепень, не являющуюся вполне упорядоченной.)

9. Показать, что во всякой модели натуральных чисел любой ненулевой элемент является непосредственно следующим за некоторым элементом.

10. (Хенкин.) Показать, что существуют счетные нестандартные модели натуральных чисел. (Применить теорему VI.3.4 к подходящей ультрастепени натуральных чисел.)

11. Пусть Q — множество неотрицательных рациональных чисел и Z — множество всех целых чисел с их естественной упорядоченностью; рассмотрим подмножество A множества $Q \times Z$, состоящее из всех пар (x, y), кроме тех, для которых $x = 0$, $y < 0$. Если A упорядочено лексикографически, т. е. $(x, y) \leqslant (z, t)$ тогда и только тогда, когда $x < z$ или $x = z$ и $y \leqslant t$, то каждый элемент из A обладает непосредственно следующим. Показать, что A — нестандартная модель натуральных чисел и что каждая счетная нестандартная модель изоморфна A. (Воспользоваться упражнениями 10 и I.5.9.)

2. АБСТРАКТНЫЕ ОТНОШЕНИЯ ЗАВИСИМОСТИ

Теория линейной зависимости в векторном пространстве над полем имеет так много общих черт с теорией алгебраической зависимости в поле над данным основным полем, что общие теоремы обычно выводятся из нескольких аксиом, одних и тех же для обеих теорий (Ван дер Варден [37], Зарисский и Самюэль [58]). Поэтому естественно сформулировать эти аксиомы на языке универсальной алгебры. Это дает возможность объединить оба эти случая в одну теорию, включающую понятие алгебраического замыкания.

Абстрактное отношение зависимости на множестве S задается системой $\mathscr{D}$ таких подмножеств множества S, что

> подмножество X множества S принадлежит системе $\mathscr{D}$ тогда и только тогда, когда некоторое конечное непустое подмножество множества X принадлежит $\mathscr{D}$. (1)

Подмножество множества S называется *зависимым*, если оно принадлежит $\mathscr{D}$, и *независимым* в противном случае. Из (1) ясно, что всякое подмножество множества S, содержащее зависимое множество, само зависимо; иными словами, всякое подмножество независимого множества независимо. Кроме того, пустое множество независимо.

Пусть S — множество с отношением зависимости; говорят, что элемент a множества S *зависит от подмножества* X множества S, если $a \in X$ или существует такое независимое подмножество X' множества X, что $X' \cup \{a\}$ зависимо. Множество всех элементов, зависящих от X, называется *оболочкой* множества X и обозначается через $\langle X\rangle$. Если $\langle X\rangle = S$, то X называется *порождающим множеством* множества S; независимое порождающее подмножество множества S называется *базисом* множества S.

Понятие линейной зависимости в векторном пространстве над телом (не обязательно коммутативным), очевидно, представляет собой пример отношения зависимости. Далее, если E—коммутативное поле, то обычное понятие алгебраической зависимости (над фиксированным подполем F поля E) является другим примером отношения зависимости. В этих двух примерах отношения зависимости обладают тем свойством, что

$$\langle\langle X\rangle\rangle = \langle X\rangle. \tag{2}$$

Если имеет место (2), то отношение зависимости называется *транзитивным*. Такое отношение зависимости может быть описано также алгебраическим оператором замыкания некоторого типа.

***Предложение* 2.1.** *Для любого транзитивного отношения зависимости отображение $X \to \langle X\rangle$ является алгебраическим оператором замыкания со следующим свойством замещения:*

$$\textit{если } y \notin \langle X\rangle \textit{ и } y \in \langle X \cup \{z\}\rangle, \textit{ то } z \in \langle X \cup \{y\}\rangle. \tag{3}$$

Обратно, любой алгебраический оператор замыкания со свойством замещения (3) *получается таким способом из некоторого транзитивного отношения зависимости.*

Доказательство. Временно будем называть подмножество T множества S *замкнутым*, если $\langle T\rangle = T$. Покажем сначала, что замкнутые подмножества образуют систему замыканий. В самом деле, если $B = \bigcap C_\lambda$, где (C_λ) — семейство замкнутых множеств, то пусть B_0 — такое независимое подмножество множества B, что $B_0 \cup \{y\}$ зависимо; поскольку $B_0 \subseteq C_\lambda$ для всех λ, имеем $y \in \langle C_\lambda\rangle = C_\lambda$, откуда $y \in \bigcap C_\lambda = B$, а это показывает, что B замкнуто. Далее, если $y \in \langle X\rangle$, то по определению множества $\langle X\rangle$ существует такое независимое подмножество X' множества X, что $X' \cup \{y\}$ зависимо. По предположению $X' \cup \{y\}$ должно обладать конечным зависимым подмножеством, скажем Y. Если $y \notin Y$, то $Y \subseteq X'$, что противоречит независимости X'. Следовательно, $y \in Y$, т. е. Y имеет вид $Y' \cup \{y\}$, где $Y' \subseteq X'$, и поэтому Y' независимо. Итак, $y \in \langle Y'\rangle$, где Y' — конечное подмножество множества X. Этим доказано, что замкнутые подмножества образуют алгебраическую систему замыканий, и, поскольку $\langle X\rangle$ замкнуто в силу (2), получаем алгебраический оператор замыкания. Чтобы проверить (3), отметим как непосредственное следствие из определений, что

$$\text{если } X \text{ независимо и } X \cup \{y\} \text{ зависимо, то } y \in \langle X\rangle. \tag{4}$$

Предположим теперь, что $y \notin \langle X \rangle$, $y \in \langle X \cup \{z\} \rangle$. Так как y зависит от $X \cup \{z\}$, то y зависит от конечного подмножества Y множества $X \cup \{z\}$, и, взяв минимальное Y с этим свойством, убеждаемся, что Y независимо. Теперь, если бы $z \notin Y$, то Y было бы подмножеством множества X и поэтому $y \in \langle X \rangle$, что противоречило бы нашему предположению. Поэтому $z \in Y$, скажем $Y = Y' \cup \{z\}$, где $Y' \subseteq X$. Теперь $Y' \cup \{y\}$ независимо, так как $y \notin \langle Y' \rangle$, а $Y' \cup \{y, z\} = Y \cup \{y\}$ зависимо, откуда $z \in \langle Y' \cup \{y\} \rangle \subseteq \langle X \cup \{y\} \rangle$.

Обратно, пусть $X \to [X]$ — алгебраический оператор замыкания со свойством замещения; будем считать X *зависимым*, если $y \in [X \setminus \{y\}]$ для некоторого $y \in X$, и *независимым* в противном случае. Так как оператор алгебраический, то отсюда вытекает, что всякое зависимое множество обладает конечным зависимым подмножеством, и поскольку очевидно, что всякое множество, содержащее зависимое множество, само зависимо, то (1) выполняется. Условие (2) выполняется по определению, и это показывает, что мы имеем транзитивное отношение зависимости. Теперь для любых $X \subseteq S$, $y \in S$ имеем $y \in [X]$ тогда и только тогда, когда $y \in [X']$ для некоторого конечного подмножества X' множества X; выбирая X' минимальным, можем предполагать, что X' независимо. Отсюда вытекает, что $y \in \langle X' \rangle \subseteq \langle X \rangle$ и, следовательно, $[X] \subseteq \langle X \rangle$. Обратно, если $y \in \langle X \rangle$, то снова $y \in \langle X' \rangle$ для некоторого конечного независимого подмножества X' множества X. Это означает, что $X' \cup \{y\}$ зависимо, т. е. $z \in [X' \cup \{y\} \setminus \{z\}]$ для некоторого $z \in X' \cup \{y\}$; в силу свойства замещения отсюда вытекает, что $y \in [X']$ и $[X'] \subseteq [X]$; поэтому $[X] = \langle X \rangle$. ∎

Когда нам придется иметь дело с отношениями зависимости на Ω-алгебрах, то обычно это отношение будет определено не на одной алгебре, а на целом классе алгебр. Отношение зависимости на алгебрах некоторой категории $\mathcal{K}$ Ω-алгебр и гомоморфизмов называется *алгебраическим*, если оно транзитивно и

(i) каждое замкнутое подмножество $\mathcal{K}$-алгебры снова является $\mathcal{K}$-алгеброй,

(ii) для любого $\mathcal{K}$-гомоморфизма θ: $A \to B$ и любого $X \subseteq A$ $\langle X \rangle \theta \subseteq \langle X\theta \rangle$.

Отметим, что так как $X \subseteq \langle X \rangle$, то $X\theta \subseteq \langle X \rangle \theta$ и поэтому во всяком случае имеет место включение $\langle X\theta \rangle \subseteq \langle X \rangle \theta$. Следовательно, если (ii) выполняется, то

$$\langle X \rangle \theta = \langle X\theta \rangle.$$

Предположим, что $\mathcal{K}$ — категория со свободными алгебрами. Если задана некоторая $\mathcal{K}$-алгебра A и подмножество X алгебры A, то пусть φ: $F_X \to A$ — гомоморфизм свободной $\mathcal{K}$-алгебры F_X над X в A, продолжающий тождественное отображение множества X. Будем считать X *независимым*, если этот гомоморфизм взаимно однозначен, и *зависимым* в противном случае. Другими словами, X независимо тогда и только тогда, когда подалгебра алгебры A, порожденная множеством X, свободна над X. Легко проверить, что так определенная зависимость удовлетворяет (1); она не всегда удовлетворяет (2), однако известно, что это имеет место во многих часто встречающихся классах алгебр. Отношение, определенное таким образом, будем называть *стандартной зависимостью* на A (относительно $\mathscr{K}$). Оно всегда удовлетворяет вышеприведенному условию (ii), но не всегда — условию (i), хотя опять оно имеет место во многих частных случаях[1]. Приведем теперь несколько примеров стандартной зависимости в алгебрах.

(i) *Категория R-модулей, где R — некоторое кольцо.* Для R-модулей стандартная зависимость превращается в линейную зависимость, которая обобщает понятие линейной зависимости над полем. Эта зависимость будет алгебраической, если, например, R — коммутативная область целостности с 1, действующей унитарно.

(ii) *Категория линейных K-алгебр, где K — коммутативное кольцо с* 1. Стандартная зависимость обобщает понятие алгебраической зависимости (с K в качестве области коэффициентов). Если K—область целостности и берутся коммутативные K-алгебры, то зависимость будет алгебраической.

(iii) *Категория расширений фиксированной $\mathscr{K}$-алгебры.* Пусть $\mathscr{K}$ — некоторая категория Ω-алгебр и C — фиксированная $\mathscr{K}$-алгебра; тогда $\mathscr{K}$-алгебры над C можно считать алгебрами над унарным расширением области Ω (с постоянным оператором, соответствующим каждому элементу алгебры C); таким образом, мы получаем новую категорию $\mathscr{K}_C$. В $\mathscr{K}_C$ можно определить стандарную зависимость, если только $\mathscr{K}$ замкнута относительно свободных объединений; эту зависимость называют также стандартной зависимостью в $\mathscr{K}$ над C.

(iv) *Категория свободных групп и гомоморфизмов.* Подмножество X свободной группы F независимо тогда и только тогда, когда $\mathrm{Gp}(X)$ свободна над X как над множеством свободных образующих. Для любого x группы F через $l(x)$ обозначим длину x (относительно некоторого фиксированного множества свободных образующих группы F) и вообще для любого конечного подмножества $X=\{x_1, \ldots, x_k\}$ группы F запишем $l(X)=\sum l(x_i)$. Определим предупорядоченность на конечных подмножествах группы F, полагая $X \prec Y$, как только $\mathrm{Gp}(X)=\mathrm{Gp}(Y)$ и $l(X) \leqslant l(Y)$. Тогда можно показать, что (i) конечные подмножества группы F удовлетворяют условию минимальности относительно этой предупорядоченности и (ii) всякое минимальное множество независимо. Отсюда вытекает, что каждая конечнопоро-

[1]) Обзор теории зависимости в универсальных алгебрах можно найти у Марчевского (*Coll. Math.*, **14** (1966), 169—188). — *Прим. ред.*

жденная подгруппа свободной группы свободна. Этот частный случай теоремы Шрейера (все подгруппы свободной группы свободны) доказан Нильсеном; относительно деталей его метода и других приложений см. М. Холл [59]. Тот же самый метод можно применить в случае свободных алгебр Ли над полем (см. Кон [64])[1]).

Вернемся теперь к общим транзитивным отношениям зависимости. Наша первая задача состоит в том, чтобы вывести существование базиса и инвариантность размерности; доказательства проводятся способом, обычным для линейной алгебры.

***Лемма* 2.2.** *Пусть S — множество с транзитивным отношением зависимости, и пусть X — подмножество множества S. Тогда следующие три утверждения эквивалентны:*

(i) *X — максимальное независимое подмножество в S;*
(ii) *X — минимальное порождающее множество в S;*
(iii) *X — базис в S.*

Доказательство почти очевидно; действительно, базис одновременно является максимальным независимым и минимальным порождающим множеством. Обратно, если X — максимальное независимое множество, то всякий элемент y множества S либо принадлежит X, либо таков, что $X \cup \{y\}$ зависимо, а поэтому $y \in \langle X \rangle$ в том и другом случае. Если X — минимальное порождающее множество, то оно не может быть зависимым, так как в противном случае его можно было бы заменить собственным подмножеством, все еще порождающим S. ∎

***Лемма* 2.3. (*Лемма о замещении.*)** *Пусть S — множество с транзитивным отношением зависимости. Если X — независимое множество и Y — порождающее множество в S, то существует такое подмножество Y' множества Y, что $X \cap Y' = \varnothing$ и $X \cup Y'$ — базис для S.*

Доказательство. Рассмотрим систему $\mathcal{J}$ таких независимых подмножеств Z множества S, что

$$X \subseteq Z \subseteq X \cup Y. \tag{5}$$

Так как X независимо, то такие множества существуют; кроме того, если (Z_λ) — некоторая цепь множеств из $\mathcal{J}$, то ее объединение $Z = \bigcup Z_\lambda$ снова принадлежит $\mathcal{J}$, поскольку Z, очевидно, удовлетворяет (5), и если Z зависимо, то некоторое конечное подмножество множества Z должно было бы быть зависимым; это подмножество содержалось бы в некотором члене цепи (Z_λ) в противоречии с тем

[1]) Теорема о том, что всякая подалгебра свободной лиевой алгебры над полем сама свободна, доказана А. И. Ширшовым (*Матем. сб.*, **33** (1953), 441—452) и независимо Виттом (*Math. Zeitschr.*, **64** (1956), 195—216). — *Прим. ред.*

фактом, что все Z_λ независимы. По лемме Цорна $\mathcal{J}$ имеет максимальный элемент M; в силу максимальности каждый элемент множества Y либо принадлежит M, либо зависит от M, откуда $\langle M\rangle = \langle Y\rangle = S$. Этим доказано, что M—базис в S. Так как $X \subseteq M \subseteq X \cup Y$, то M имеет вид $M = X \cup Y'$, где $Y' = M \setminus X$ удовлетворяет условиям $Y' \subseteq Y$, $Y' \cap X = \varnothing$. ∎

Лемма о замещении показывает, в частности, что S обладает базисом.

***Теорема* 2.4.** *Пусть S — множество с транзитивным отношением зависимости. Тогда S обладает базисом; точнее, если X — произвольное независимое множество и Y — такое порождающее множество, что $X \subseteq Y$, то существует такой базис B в S, что*

$$X \subseteq B \subseteq Y. \tag{6}$$

Кроме того, любые два базиса равномощны.

Доказательство. Пусть даны X и Y, удовлетворяющие условиям теоремы; тогда $X \cup Y = Y$ и поэтому в силу леммы 2.3 существует базис, удовлетворяющий (6). В частности, выбирая $X = \varnothing$, $Y = S$, видим, что базис всегда существует.

Пусть теперь B, C — любые два базиса в S. Если один из базисов B или C бесконечен, то другой базис также бесконечен, и оба базиса имеют одну и ту же мощность по предложению II.5.5, если использовать теорему II.5.2 для представления системы замыканий на S в качестве системы подалгебр. Если B и C оба конечны, то пусть $B \cap C = \{a_1, \ldots, a_n\}$, $B = \{a_1, \ldots, a_n, b_1, \ldots, b_r\}$ и $C = \{a_1, \ldots, a_n, c_1, \ldots, c_s\}$, где различные элементы обозначены различными буквами или снабжены различными индексами. Применим индукцию по $\max(r, s)$. Если $r = 0$ или $s = 0$, то $B \subseteq C$ или $C \subseteq B$, и результат очевиден. Поэтому можно предполагать, что $r \geqslant 1$, $s \geqslant 1$; далее, без ограничения общности можно считать, что $r \geqslant s$, так что на самом деле $r > 1$. По лемме 2.3 множество $\{a_1, \ldots, a_n, b_1\}$ можно дополнить до базиса D элементами базиса C, скажем

$$D = \{a_1, \ldots, a_n, b_1, c_{i_1}, \ldots, c_{i_t}\}, \quad t \leqslant s < r.$$

Теперь пересечение D с B состоит из $n+1$ элемента, и D содержит, кроме того, еще t $(< r)$ элементов, тогда как B содержит, кроме этого пересечения, еще $r-1$ элементов, так что по предположению индукции $|B| = |D|$, т. е.

$$r = t + 1.$$

Поскольку $r > 1$, отсюда вытекает, что $t \geqslant 1$, и поэтому пересечение D с C содержит не меньше чем $n+1$ элементов. Используя еще раз предположение индукции, находим, что

$$s = t + 1,$$

и, следовательно, $r = s$. ∎

Чтобы ввести понятие алгебраического замыкания, нужно поступить следующим образом. Пусть $\mathcal{K}$ — категория Ω-алгебр с алгебраическим отношением зависимости. Расширение E/A $\mathcal{K}$-алгебр называется *алгебраическим*, если A порождает E. Теперь естественно было бы считать $\mathcal{K}$-алгебру алгебраически замкнутой, если у нее нет собственных алгебраических расширений; такое определение встретило бы, однако, ряд трудностей, так как обычно алгебраически замкнутых алгебр в этом смысле не существует просто потому, что всегда можно присоединить к A элементы, алгебраические над $\varnothing$. Эти трудности можно обойти, исключая такие элементы и допуская только такие расширения алгебры A, из которых нельзя исключить ни одного элемента, не изменяя алгебру A.

Определение. Расширение E/A $\mathcal{K}$-алгебр называется *сжимаемым*, если существует гомоморфизм θ: $E/A \to F/A$, не являющийся взаимно однозначным; образ при гомоморфизме θ называется также *сжатием* расширения E/A. Если такого гомоморфизма не существует, то это расширение называется *несжимаемым*. Далее, E/A называется *алгебраическим* расширением (относительно некоторого алгебраического отношения зависимости), если A порождает E.

***Предложение* 2.5.** *Пусть $\mathcal{K}$ — категория Ω-алгебр, замкнутая относительно гомоморфных образов. Тогда любое расширение E/A $\mathcal{K}$-алгебр обладает сжатием, которое само несжимаемо.*

Доказательство. Рассмотрим конгруэнции на E, разделяющие A; по следствию II.6.4 существует максимальная такая конгруэнция, скажем $\mathfrak{q}$. Ограничение на A естественного гомоморфизма $E \to E/\mathfrak{q} = \bar{E}$ взаимно однозначно, и поэтому им можно воспользоваться для вложения A в $\bar{E}$. Полученное расширение $\bar{E}/A$ несжимаемо; действительно, в противном случае на $\bar{E}$ существовала бы такая нетривиальная конгруэнция $\bar{\mathfrak{r}}$, разделяющая A, что конгруэнция $\mathfrak{r}$ на E, которой соответствует в силу следствия II.3.12 конгруэнция $\bar{\mathfrak{r}}$, содержит $\mathfrak{q}$, отлична от $\mathfrak{q}$ и разделяет A, что противоречит определению конгруэнции $\mathfrak{q}$. ∎

Пусть $\mathcal{K}$ — категория алгебр с алгебраическим отношением зависимости. Тогда расширение E/A $\mathcal{K}$-алгебр называется *алгебраически замкнутым*, если E/A является алгебраическим и несжимаемым и для любого данного алгебраического несжимаемого расширения C/B любое вложение $B \to A$ продолжается до вложения $C \to E$. Из этого определения немедленно вытекает, что если θ: $B \to A$ — мономорфизм и C/B — алгебраическое расширение, то θ можно продолжить до гомоморфизма θ': $C \to E$. Действительно, если C'/B — несжимаемое сжатие расширения C/B, то C'/B все еще будет алгебраическим расширением и поэтому может быть вложено в E/A; применяя последовательно естественный гомоморфизм $C \to C'$ и это вложение, получим нужный гомоморфизм.

Если применить это определение в случае стандартной зависимости в векторных пространствах (т. е. линейной зависимости), то мы увидим, что никакое собственное расширение векторного пространства не может быть алгебраическим; этим объясняется, почему понятие алгебраического замыкания, как оно было здесь определено, обычно не играет никакой роли при изучении векторных пространств. Рассмотрев затем случай стандартной зависимости в расширениях поля (т. е. алгебраической зависимости в обычном смысле), видим, что каждое расширение поля E/F несжимаемо, так что наше определение алгебраически замкнутого расширения совпадает здесь с обычным понятием.

Наша цель — показать, что при подходящих условиях на $\mathcal{K}$ каждая $\mathcal{K}$-алгебра A обладает алгебраически замкнутым расширением и что это расширение определяется алгеброй A однозначно с точностью до изоморфизма. Чтобы установить этот результат, нужно сделать еще одно предположение, которое в большинстве случаев выполняется. Будем считать отношение зависимости таким, что

I. Мощность любого алгебраического несжимаемого расширения алгебры A не превосходит $\max(|A|, |\Omega|, \aleph_0)$.

Далее, категория алгебр $\mathcal{K}$ называется *направленной*, если для любых двух расширений алгебры A существует третье, содержащее оба эти расширения. Теперь мы можем сформулировать условия существования алгебраических замыканий:

***Теорема* 2.6.** *Пусть $\mathcal{K}$ — направленная локальная категория Ω-алгебр, замкнутая относительно гомоморфных образов. Предположим, что на $\mathcal{K}$ задано алгебраическое отношение зависимости, удовлетворяющее условию* I. *Тогда для каждой $\mathcal{K}$-алгебры A существует алгебраически замкнутое расширение $\bar{A}/A$ и $\bar{A}$ определяется $\mathcal{K}$-алгеброй A однозначно с точностью до изоморфизма.*

Доказательство. Пусть $\gamma = \max(|A|, |\Omega|, \aleph_0)$; по предположению мощность любого алгебраического несжимаемого расширения алгебры A не больше γ. Далее, поскольку $\mathcal{K}$ направлена, любые два расширения E_i/A $(i = 1, 2)$ содержатся в третьем, скажем E/A. Если E_i/A — алгебраические расширения, то, заменяя E множеством элементов, зависящих от A в E, можно предполагать, что E/A — тоже алгебраическое. Если к тому же расширения E_i/A несжимаемы, то любая конгруэнция на E, разделяющая A, будет также разделять E_i, и факторизуя по максимальной такой конгруэнции, получим несжимаемое расширение, которое останется алгебраическим и в которое E_i снова могут быть вложены. Итак, семейство алгебраических несжимаемых расширений $\mathscr{K}$-алгебры A направлено по включению. Пусть (E_λ/A) — семейство таких алгебраических несжимаемых расширений $\mathscr{K}$-алгебры A, что любое алгебраическое несжимаемое расширение алгебры A изоморфно некоторому E_λ/A; определим упорядоченность, полагая $E_\lambda \prec E_\mu$, если только существует мономорфизм $E_\lambda \to E_\mu$ (над A); тогда E_λ образуют направленное семейство, предел которого E можно считать Ω-алгеброй (упражнение III.1.5), и эта Ω-алгебра будет на самом деле $\mathscr{K}$-алгеброй, содержащей A, так как $\mathscr{K}$ локальна. Каждый элемент алгебры E принадлежит некоторому E_λ и поэтому зависит от A; кроме того, E/A несжимаемо, так как всякий гомоморфизм θ расширения E/A, не являющийся взаимно однозначным, должен отождествлять пару различных элементов, скажем x, y, из E, и если E_λ содержит x и y, то $\theta \mid E_\lambda$ не будет взаимно однозначным, что противоречит несжимаемости E_λ. Этим доказано, что E/A — алгебраическое несжимаемое расширение. Чтобы доказать, что E/A алгебраически замкнуто, нужно показать, что для любого алгебраического несжимаемого расширения C/B и любого вложения θ: $B \to A$ существует вложение θ': $C \to E$, продолжающее θ. Отождествляя алгебру B с ее образом при θ, можно считать E расширением алгебры B. Пусть F/B — расширение, содержащее C/B и E/B; тогда F содержит A, и поэтому F можно считать расширением алгебры A. Так как расширения E/A и C/B — алгебраические, то F/A можно выбрать также алгебраическим. Если $\mathfrak{q}$ — некоторая конгруэнция на F, разделяющая A, то $\mathfrak{q}$ также разделяет B и, следовательно, разделяет C. Поэтому несжимаемое сжатие расширения F/A все еще содержит C. Но E/A было максимальным алгебраическим несжимаемым расширением, поэтому F вложимо в E, и, следовательно, C также вложимо в E.

Чтобы показать, что E определяется алгеброй A однозначно с точностью до изоморфизма, докажем сначала, что E/A — минимальное алгебраически замкнутое расширение алгебры A. Действительно, предположим, что F/A — собственное подрасширение расширения E/A, которое также алгебраически замкнуто. Тогда E/A может быть вложено в F/A, и, заменяя F образом E при этом вложении, можем предположить, что F/A изоморфно E/A. Таким образом, из этого вытекает, что E/A обладает собственным расширением E'/A, изоморфным E/A и поэтому алгебраическим и несжимаемым. Повторяя этот процесс, получаем возрастающую вполне упорядоченную последовательность расширений алгебры A, каждое из которых алгебраическое и несжимаемое:

$$E/A \subset E'/A \subset E''/A \subset \ldots \subset E^{(\alpha)}/A \subset \ldots .$$

Для предельного порядкового числа имеем алгебраическое несжимаемое расширение алгебры A, которое снова можно вложить в E/A, и поэтому процесс можно продолжать. Если продолжать эту последовательность до такого порядкового числа, кардинальное число которого превосходит γ, получим расширение $E^{(\alpha)}/A$, алгебраическое и несжимаемое, но мощность которого больше γ, что противоречит условию I. Поэтому никакое собственное подрасширение расширения E/A не может быть алгебраически замкнутым.

Пусть теперь E/A, F/A — любые два алгебраически замкнутых расширения алгебры A. Тогда F/A можно вложить в E/A; при этом образ расширения F/A будет снова алгебраически замкнутым расширением и, следовательно, в силу минимальности E совпадает с E. Это показывает, что $E/A \cong F/A$. ∎

Алгебраически замкнутое расширение алгебры A, определенное алгеброй A однозначно с точностью до изоморфизма, называется *алгебраическим замыканием* алгебры A. При доказательстве теоремы 2.6 мы получили

Следствие 2.7. *Если E/A — некоторое расширение алгебры A, содержащее алгебраическое замыкание $\bar{A}$ алгебры A, то $\bar{A}$ однозначно определяется в E как множество элементов из E, зависящих от A.* ∎

Например, категория (коммутативных) полей данной характеристики локальна, направлена и замкнута относительно гомоморфных образов (единственными гомоморфными образами здесь являются изоморфные образы; иными словами, каждое поле является несжимаемым расширением своего простого поля и, следовательно, каждое расширение поля несжимаемо). Поскольку уравнение степени n не может иметь больше чем n корней и над полем F бесконечной мощности γ существует $\aleph_0\gamma = \gamma$ уравнений, то отсюда вытекает, что мощность любого алгебраического расширения поля F (всегда несжимаемого) не больше γ. Итак, условие I выполняется, и можно применить теорему 2.6, чтобы вывести существование алгебраического замыкания данного поля.

Было бы чрезвычайно интересно установить аналогичный результат для тел. Используя стандартную зависимость над подтелом, нужно было бы показать, что (i) это алгебраическое отношение зависимости, что (ii) выполняется условие I и что (iii) эта категория направлена, т. е. для любых двух расширений тел существует третье, содержащее оба эти расширения. В настоящее время неизвестно решение ни одной из этих трех проблем.

Доказательство теоремы 2.6 можно упростить, если A обладает таким расширением I/A, что I алгебраически замкнуто как расширение самого себя. Алгебра I с этим свойством называется *инъективной*; итак, алгебра I инъективна, если любое вложение $B \to I$

может быть продолжено для любого алгебраического несжимаемого расширения C алгебры B.

***Предложение* 2.8.** *Если A содержится в инъективной алгебре I, то любое максимальное алгебраическое несжимаемое подрасширение расширения I/A является алгебраическим замыканием алгебры A.*

Доказательство. Алгебраические несжимаемые подрасширения расширения I/A образуют индуктивную систему; следовательно, существует максимальное такое подрасширение, скажем E/A. Теперь, если B/A — произвольное алгебраическое несжимаемое подрасширение расширения I/A, то существует некоторое алгебраическое подрасширение C/A расширения I/A, содержащее оба расширения E/A и B/A. Пусть C'/A — несжимаемое сжатие расширения C/A; тогда C'/A снова будет алгебраическим и B/A, E/A могут быть вложены в C'/A. Теперь вложение $E \to I$ можно продолжить до вложения C' в I, так как I инъективна. В силу максимальности расширения E отсюда вытекает, что $C' = E$; это означает, что B/A можно вложить в E/A. Если C/B — некоторое алгебраическое несжимаемое расширение, то любое вложение $B \to A$ можно продолжить до гомоморфизма $C \to I$, который обязательно будет вложением, и, следовательно, C может быть вложено в E. Этим доказано, что E/A алгебраически замкнуто. Единственность расширения E доказывается теперь следующим образом. Заметим, что алгебра E на самом деле инъективна, поскольку любое алгебраическое несжимаемое расширение алгебры E может быть вложено в I и затем может быть вложено в E. Как при доказательстве теоремы 2.6, сформулированный результат будет доказан, если мы сможем показать, что E — минимальная инъективная подалгебра алгебры I, содержащая E. Итак, пусть F/A — некоторое подрасширение расширения E/A, которое также инъективно; тогда тождественное на F отображение продолжается до вложения $E \to F$, которое возможно, если только $F = E$; следовательно, E минимальна, как и утверждалось. ▮

Для иллюстрации предложения 2.8 возьмем в качестве $\mathscr{K}$ категорию унитарных R-модулей (над ассоциативным кольцом R с 1) и будем считать зависимыми все непустые подмножества произвольного модуля. Тогда каждый модуль может быть вложен в инъективный модуль (см., например, Маклейн [63]), и поэтому каждый модуль обладает алгебраическим замыканием, которое однозначно определено (с точностью до изоморфизма) как максимальное несжимаемое расширение или, эквивалентно этому, как минимальное инъективное расширение. Это расширение называется обычно *инъективной оболочкой* данного модуля.

Возможны еще и другие определения алгебраического замыкания. В частности, делая более сильные предположения, можно вывести из них условие I (или совсем его избежать). Например, В. Скотт [51] называет алгебру A слабо алгебраически замкнутой, если каждое конечнозаданное расширение алгебры A обладает сжатием на A; при этом определении предположения типа условия I не требуются. Другой вид условий, которые влекут за собой I, рассматривался Йонсоном [62] (см. упражнение 6).

УПРАЖНЕНИЯ

1. Пусть R — некоммутативная область целостности; показать, что стандартная зависимость в R-модулях будет алгебраической тогда и только тогда, когда любые два ненулевых правых идеала в R имеют ненулевое пересечение.

2. (Уитни.) Пусть Γ — некоторый граф; подграф Γ_0 графа Γ называется *зависимым*, если Γ_0 содержит цикл. Проверить, что это транзитивное отношение зависимости.

3. Показать, что выпуклые подмножества плоскости образуют систему замыканий, которая не обладает свойством замещения.

4. Для любого R-модуля M (над фиксированным кольцом R) семейство подмодулей будем считать зависимым, если их сумма не является прямой. Показать, что это будет отношением зависимости на множестве всех подмодулей модуля M, которое в общем случае не транзитивно.

5. (Кертес.) Если дана группа G, то через G_0 обозначим подмножество таких элементов a группы G, что нормальный делитель группы G, порожденный элементом a, минимален (среди нетривиальных нормальных делителей). Показать, что если оболочка множества $X \subseteq G_0$ определена как нормальный делитель, порожденный множеством X, то это определяет транзитивное отношение зависимости на G_0. Вывести отсюда, что любые два разложения группы G в прямое произведение простых групп (если такие разложения существуют) имеют одно и то же число сомножителей.

6. Два элемента x и y расширения E/A называются *A-изоморфными*, если отображение $x \to y$ продолжается до изоморфизма $A(x) \to A(y)$, оставляющего элементы алгебры A неподвижными. Показать, что если при стандартном отношении зависимости каждый алгебраический над A элемент A-изоморфен лишь конечному числу элементов, то эта зависимость удовлетворяет условию I (см. Йонсон [62]).

3. ПРОБЛЕМА ДЕЛЕНИЯ ДЛЯ ПОЛУГРУПП И КОЛЕЦ

Группу можно рассматривать как полугруппу, допускающую деление. Следовательно, можно поставить вопрос, существует ли для данной полугруппы содержащая ее группа. Выражаясь более формально, многообразие Gp (групп) подчинено многообразию Sg (полугрупп), и поэтому многообразие Sg может быть представлено в Gp. Кроме того, по следствию IV.4.3 это представление обладает универсальным функтором. Это означает, что каждой полугруппе S сопоставлена такая группа $U(S)$ и такой гомоморфизм

$$u\colon S \to U(S), \tag{1}$$

что каждый гомоморфизм φ полугруппы S в группу G можно однозначно представить в виде произведения гомоморфизма u и гомоморфизма $\bar{\varphi}$: $U(S) \to G$. Будем называть $U(S)$ *универсальной группой* полугруппы S.

Ясно, что S можно вложить в группу тогда и только тогда, когда гомоморфизм (1) будет взаимно однозначным. Проблема деления для полугрупп состоит в нахождении практических критериев для вложимости полугруппы в группу. Хотя нахождение таких критериев может вывести за пределы универсальной алгебры, однако абстрактная точка зрения очень помогает упростить доказательство такого критерия, если он найден. Проиллюстрируем это на двух примерах: во-первых, докажем необходимые и достаточные условия Мальцева для вложимости полугруппы в группу, и, во-вторых, рассмотрим полугруппы эндоморфизмов алгебры A и получим условия, при которых A обладает расширением A^* с автоморфизмами, индуцирующими данные эндоморфизмы.

Пусть S — произвольная полугруппа и G — группа, содержащая S и ею порожденная; тогда ясно, что G будет гомоморфным образом универсальной группы $U(S)$ по конгруэнции, разделяющей S, т. е. по некоторому нормальному делителю группы $U(S)$, имеющему в пересечении с S не больше одного элемента (а именно единичного элемента) [1]. Обратно, если G—некоторый гомоморфный образ группы $U(S)$ по конгруэнции, разделяющей S (в предположении, что S вложена в $U(S)$), то u можно использовать для вложения S в G таким образом, чтобы S порождала G. Любая такая группа G будет называться *группой дробей* полугруппы S. В противоположность универсальной группе группа дробей не всегда существует, а когда существует, то не обязательно единственна (см. упражнение 3).

Первый шаг при вложении полугруппы в группу состоит в присоединении единичного элемента, если его еще там нет. Это всегда можно сделать; возьмем элемент 1 и определим на множестве $S^1 = S \sqcup \{1\}$ умножение, сохраняя на S то умножение, которое было определено раньше, и полагая

$$a1 = 1a = a \quad (a \in S^1).$$

Теперь ясно, что если S может быть вложена в группу, то либо S обладает единичным элементом, либо S^1 может быть вложена в группу. Поэтому мы можем сконцентрировать наше внимание на полугруппах с 1. Итак, вместо многообразия Sg мы будем иметь дело только с Sg*, многообразием полугрупп с 1 (считая 1 постоянным оператором), и будем предполагать, что все полугруппы, встречающиеся в дальнейшем, принадлежат Sg*.

[1] Понятно, что не всякий нормальный делитель группы $U(S)$, пересечение которого с S содержит не больше одного элемента, будет определять конгруэнцию, разделяющую S. — *Прим. ред.*

Если S — некоторая полугруппа, то подмножество M полугруппы S называется *потенциально обратимым*, если существует мономорфизм полугруппы S в полугруппу с сокращениями T, в которой все элементы множества M обладают обратными. Итак, S имеет группу дробей тогда и только тогда, когда S сама потенциально обратима. В силу принципа локализации S обладает группой дробей, если каждое конечное подмножество полугруппы S потенциально обратимо. Это условие можно еще несколько ослабить:

***Предложение* 3.1.** *Полугруппа S обладает группой дробей, если каждый элемент полугруппы S потенциально обратим.*

Действительно, пусть $\{a_1, \ldots, a_n\}$ — конечное подмножество полугруппы S; тогда по предположению произведение $a_1 \cdots a_n$ потенциально обратимо, т. е. существует такой мономорфизм T: $x \to x'$ в полугруппу с сокращениями, что $(a_1 \cdots a_n)'$ обратимо. Положим

$$b_i = a'_{i+1} \cdots a'_n \left[(a_1 \cdots a_n)'\right]^{-1} a'_1 \cdots a'_{i-1};$$

тогда $a'_i b_i = b_i a'_i = 1$; это показывает, что $\{a_1, \ldots, a_n\}$ потенциально обратимо, и сформулированный результат вытекает из принципа локализации. ∎

Несмотря на этот результат, иногда удобнее рассматривать потенциальную обратимость множеств, а не элементов. В частности, так обстоит дело, когда нас интересует множество образующих полугруппы S. Итак, даны полугруппа S и ее подмножество P, и наша задача состоит в выяснении, будет ли P потенциально обратимым. Для каждого элемента p множества P присоединим к S неизвестное p^- и обозначим так полученную полугруппу через $S(P)$. Пусть $\mathfrak{q}$ — конгруэнция на $S(P)$, порожденная всевозможными парами $(pp^-, 1)$, $(p^-p, 1)$, где $p \in P$; тогда факторполугруппа $S(P)/\mathfrak{q}$ будет универсальной полугруппой для S с обратными элементами для элементов множества P, и нам нужно найти условия, при которых отображение $\operatorname{nat}\mathfrak{q}$, ограниченное на S, взаимно однозначно. Эта задача аналогична проблеме тождества (§ III.9), и не известно никакого критерия, который был бы применим в общем случае, практически полезен и *одновременно* прост. Однако общие условия такого рода были записаны в неожиданной форме, которая хотя и не проста, но полезна в некоторых случаях. Наше изложение следует с некоторыми упрощениями статье Мальцева [39].

Ключом к решению является некоторое изменение конструкции построенной выше полугруппы $S(P)$. Если даны полугруппа S и подмножество P, то для каждого $p \in P$ возьмем два неизвестных p^- и p^+ и через $S(P)$ обозначим полугруппу, полученную присоединением к S всех этих элементов. Пусть $\mathfrak{q}$ — конгруэнция на $S(P)$, порожденная всевозможными парами $(p^-p, 1)$, $(pp^+, 1)$, где $p \in P$; тогда факторполугруппа $S(p)/\mathfrak{q}$ снова будет универсальной полугруппой для S, в которой элементы множества P обладают обратными; действительно, если образы элементов p, p^-, p^+ при $\operatorname{nat}\mathfrak{q}$ обозначить через a, a^-, a^+, то $a^-a = aa^+ = 1$ и, следовательно,

$$a^- = a^-aa^+ = a^+.$$

Чтобы описать $\mathfrak{q}$ подробнее, представим элементы полугруппы $S(P)$ в виде вершин графа, в котором отрезки определяются следующими преобразованиями:

$($: заменяет 1 на p^-p; $[$: заменяет 1 на pp^+;

$)$: заменяет p^-p на 1; $]$: заменяет pp^+ на 1.

Так, например, преобразование $($ может быть применено к любому элементу w полугруппы $S(P)$, представленному некоторым способом в виде произведения $w = uv$, и определяет отрезок из uv в up^-pv; это же верно для $[$, тогда как преобразования $)$, $]$ могут быть применены только к элементам полугруппы $S(P)$, содержащим p^-p, pp^+ соответственно. Таким образом, получается в точности графическое представление, описанное в § III.9, и ясно, что различные $\mathfrak{q}$-классы являются связными компонентами этого графа. Отсюда вытекает, что P потенциально обратимо тогда и только тогда, когда различные элементы полугруппы S лежат в разных компонентах этого графа. Чтобы уточнить это утверждение, возьмем любые два элемента u, v полугруппы $S(P)$, лежащие в одной и той же компоненте, и рассмотрим путь из u в v. Он задается цепочкой элементов полугруппы $S(P)$

$$w_0 = u, \quad w_1, \ \ldots, \ w_n = v, \tag{2}$$

где два рядом стоящих элемента w_{i-1}, w_i получаются друг из друга с помощью некоторого преобразования. Поскольку p^- есть неизвестное, то каждое p^-, встречающееся на некотором месте в w_i, либо было введено с помощью некоторого преобразования при переходе от w_{i-1} к w_i, либо встречалось уже в w_{i-1}; аналогично p^- будет присутствовать в w_{i+1}, если не исчезнет после некоторого преобразования при переходе от w_i к w_{i+1}. Во всяком случае, можно проследить каждое вхождение элемента p^- и аналогично каждое вхождение элемента p^+ от его первого появления в цепи (2) до его исчезновения. Остановим теперь наше внимание на определенном вхождении элемента p^-. Если предположить, что в (2) u, $v \in S$, то p^- не может входить в u или v, поэтому он должен появиться на некотором шаге, скажем при i-м преобразовании:

$$(: \ w_{i-1} = ab, \quad w_i = ap^-pb \qquad (a, \ b \in S(P)),$$

а несколько позже должен исчезнуть, скажем при j-м преобразовании:

$$): \ w_{j-1} = a'p^-pb', \quad w_j = a'b' \qquad (a', \ b' \in S(P)).$$

Преобразования с номерами от i до $j-1$ переводят a в a' и pb в pb', причем каждое из них применяется либо к первому, либо ко второму элементу. Рассмотрение изменений, происходящих с pb', нельзя отложить до того момента, когда будет произведено j-е преобразование, так как после него pb' уже исчезнет, однако изменения, происходящие с a', *можно* рассмотреть после j-го преобразования, поскольку при этом преобразовании a' не изменяется. В частности, все преобразования, при помощи которых a превращается в a' до того шага, после которого исчезает p^-, можно рассмотреть после j-го преобразования. Итак, когда p^- исчезает, имеем

$$ap^-pb \to ab',$$

и затем следует ряд преобразований, переводящих ab' в $a'b'$.

Чтобы описать эту ситуацию, назовем часть, находящуюся слева от некоторого вхождения p^- (или справа от некоторого вхождения p^+) *пассивной частью*, а часть, находящуюся справа (или в случае p^+ слева), — *активной частью*. Таким образом, мы показали, что любые изменения в пассивной части относительно некоторого вхождения p^- можно рассматривать после исчезновения p^-. Временно будем называть вхождение p^- или p^+ в некоторый член цепи (2) *регулярным*, если никакие изменения не затрагивают его пассивной части. Покажем теперь, что путь, связывающий два элемента полугруппы S, всегда можно заменить путем, в котором все вхождения регулярны.

Лемма **3.2.** *Если дана цепь*

$$w_0 = u,\ w_1,\ \ldots,\ w_n = v, \tag{2}$$

связывающая два элемента u, v полугруппы S, то существует цепь той же длины

$$w_0 = u,\ w_1',\ \ldots,\ w_{n-1}',\ w_n = v,$$

которая связывает u, v и в которой все вхождения регулярны.

Доказательство. Рассмотрим первое преобразование, при котором появляется нерегулярное вхождение; пусть это будет вхождение элемента p^-, который появляется при i-м преобразовании: $w_{i-1} \to w_i$, и исчезает при j-м преобразовании. Часть нашей цепи от i до j имеет вид

$$ab,\ ap^-pb,\ \ldots,\ a'p^-pb',\ a'b',$$

и, как мы видели, ее можно заменить цепью

$$ab,\ ap^-pb,\ \ldots,\ ap^-pb',\ ab',\ \ldots,\ a'b'.$$

Новая цепь снова будет длины n, и данное вхождение p^- теперь регулярно. Кроме того, число нерегулярных вхождений не возросло, так как любой p^+, входящий в a, должен был входить нерегулярно с самого начала, а любой p^-, входящий в a регулярно, будет входить регулярно и в новую цепь. Итак, число нерегулярных вхождений уменьшится по крайней мере на единицу, и по индукции мы получаем сформулированный результат. ▮

В силу этой леммы любые элементы u и v полугруппы S, сравнимые по mod $\mathfrak{q}$, могут быть связаны цепью, в которой все вхождения регулярны, т. е. все изменения происходят на активной части любого вхождения p^- или p^+. Итак, в любом члене w_i данной цепи изменение происходит в части, лежащей между самым правым p^- и самым левым p^+ (ясно, что любой p^+ должен лежать правее любого p^-). Будем называть эту часть *активной областью*. Любое изменение при переходе от некоторого члена цепи к следующему происходит в его активной области, и это изменение задается следующей таблицей, в которой через $R(*)$ и $L(*)$ обозначены активные области до и после преобразования * соответственно:

	(	)	[	]
$R(*)$	ab	pb'	cd	$c'q$
$L(*)$	pb	ab'	cq	$c'd$

Эту таблицу легко получить, если рассмотреть часть цепи, выписанной при доказательстве леммы 3.2. Так, например, для (эта область превращается из ab в pb, а для) она превращается из pb' в ab', где для некоторого данного вхождения a, b, b' имеют фиксированные значения. Конечно, различные вхождения в общем случае будут иметь различные элементы a, b, b', так что их придется различать с помощью индексов. Часть этой таблицы, относящаяся к [и], строится аналогично на основе вхождения q^+ $(q \in P)$.

Теперь, если преобразования в цепи, связывающей u и v, обозначены через $\alpha_1, \ldots, \alpha_n$, то мы имеем равенства

$$L(\alpha_1) = R(\alpha_2),\ L(\alpha_2) = R(\alpha_3),\ \ldots,\ L(\alpha_{n-1}) = R(\alpha_n), \qquad (3)$$

которые выражают тот факт, что после того, как выполнено $(i-1)$-е преобразование, активная область будет той же самой, что и перед выполнением i-го преобразования. Поскольку изменяются только активные области, то равенства (3) выражают в точности тот факт, что цепь (2) (с регулярными вхождениями), связывающая u и v, существует. В начале и конце этой цепи активными областями являются u и v соответственно, и для вложимости они должны быть равны; это выражается равенством

$$L(\alpha_n) = R(\alpha_1). \qquad (4)$$

Итак, последовательности преобразований $\alpha_1, \ldots, \alpha_n$ мы сопоставляем условие (3)$\Rightarrow$(4). Если все эти условия выполняются, то конгруэнция $\mathfrak{q}$ разделяет S и вложение возможно. Ясно, что эти условия также необходимы.

Чтобы найти все последовательности $\alpha_1, \ldots, \alpha_n$, которые могут возникнуть, заметим, что такая последовательность должна содержать столько же (, сколько). Если преобразования (перенумерованы скажем от 1 до r в порядке их появления, и если два соответствующих элемента p_k^- появляются в одном и том же члене w_i, то один из них с бо́льшим индексом должен быть правее другого, так как слева от последнего находится пассивная область. Отсюда вытекает, что элемент с бо́льшим индексом должен исчезнуть тоже первым (в противном случае *его* пассивная область была бы затронута преобразованием). Кроме того, в любом левом отрезке $\alpha_1, \ldots$ $\ldots, \alpha_\nu$ должно быть по крайней мере столько же преобразований (, сколько). Итак, члены (,) входят в данную последовательность попарно таким образом, что никакая пара не разделяет другую пару; назовем это для краткости *нормальным распределением скобок* (Тамари [62]). Аналогичные рассуждения применимы к [и], и мы получаем следующую теорему:

***Теорема* 3.3. (*Мальцев* [39].)** *Пусть S—полугруппа и P—некоторое подмножество полугруппы S. Каждой конечной последовательности $\alpha_1, \ldots, \alpha_n$ таких пар скобок* (,) *и* [,], *что как круглые скобки, так и квадратные образуют нормальное распределение скобок, сопоставим условие*

$$L(\alpha_1) = R(\alpha_2), \ \ldots, \ L(\alpha_{n-1}) = R(\alpha_n) \Rightarrow L(\alpha_n) = R(\alpha_1) \qquad (5)$$

для любых $a, b, b', c, c', d \in S$ и $p, q \in P$, причем эти буквы снабжены индексами соответствующей скобки и $L(*)$, $R(*)$ берутся из вышеприведенной таблицы. Тогда условия (5), *взятые для всех таких последовательностей, необходимы и достаточны для того, чтобы множество P было потенциально обратимым.* ∎

В частности, если в качестве P мы возьмем саму полугруппу S или в более общем случае множество образующих полугруппы S, то получим необходимые и достаточные условия, при которых S обладает группой дробей.

В качестве примера рассмотрим простейшее условие, соответствующее последовательности ( ). Это условие читается так:

$$pb = pb' \Rightarrow ab' = ab$$

и по существу выражает возможность левого сокращения на элементы множества P (в чем легко убедиться, взяв $a = 1$). Аналогично последовательность [ ] соответствует правому сокращению. Далее, условие, соответствующее последовательности ([ )], утверждает, что

$$pb = cd, \quad cq = pb', \quad ab' = c'q \tag{6}$$

влечет

$$c'd = ab. \tag{7}$$

Нетрудно проверить, что полугруппа с образующими a, b, c, d, b', c', p, q и соотношениями (6) является полугруппой с сокращениями, но не удовлетворяет (7); эта полугруппа дает пример полугруппы, допускающей сокращения, но не вложимой в группу (Мальцев [37]). Вообще можно показать (Мальцев [40]), что для каждого натурального числа n существуют условия (5) длины n, которые не вытекают из всех более коротких условий, вместе взятых. Таким образом, в общем случае бесконечное множество условий в теореме 3.3 не может быть заменено конечным подмножеством.

Группы возникают естественным образом как подстановки множества, точно так же полугруппы возникают как отображения множества в себя.

Проблему деления можно поэтому сформулировать следующим образом. Пусть задано множество A и полугруппа Σ отображений множества A в себя; при каких условиях существует множество A^*, содержащее A, вместе с группой подстановок, индуцирующих данные отображения на A? Очевидное необходимое условие состоит в том, чтобы данные отображения на A были взаимно однозначными; как только это выполнено, множество A^* с нужной группой подстановок строится почти тривиально. В частности, данная полугруппа совсем не обязательно должна вкладываться в группу; тем не менее возможность построения нужного множества основывается в этом случае на том факте, что различные подстановки множества A^* могут индуцировать одно и то же отображение на A. Таким образом, поставленная задача не очень близка проблеме деления в полугруппах, если только мы не устанавливаем взаимно однозначного соответствия между данной полугруппой отображений множества A и некоторой группой подстановок множества A^*. Если попытаться найти необходимые и достаточные условия для этого, то мы снова придем к условиям типа условий Мальцева (теорема 3.3); наложим поэтому дальнейшие ограничения, чтобы найти подходящие достаточные условия.

Естественное ограничение, которое в то же время расширяет область применимости данного метода, состоит в том, что множество A снабжается некоторой структурой и рассматриваются только те отображения, которые согласованы с этой структурой; итак, будем предполагать, что A является Ω-алгеброй с полугруппой эндоморфизмов. Рассмотрим сначала случай одного эндоморфизма θ и предположим, что θ — взаимно однозначный эндоморфизм. Тогда θ определяет изоморфизм между A и подалгеброй A' алгебры A. Поэтому можно определить θ^{-1} на A', а так как $A' \simeq A$, то отображение θ^{-1} можно продолжить до изоморфизма алгебры A на алгебру A_1, содержащую A. Продолжая таким образом, получим возрастающую последовательность алгебр, содержащих A (и изоморфных A, что несущественно); их объединение A^* будет нужным расширением.

Эту конструкцию можно обобщить, если вместо возрастающей последовательности рассматривать направленную систему. Соответственно это позволит применить данный метод к полугруппам, направленным относительно делимости слева, т. е. к таким полугруппам Σ, что

$$\begin{gathered}\text{если даны } \alpha,\ \beta \in \Sigma, \text{ то существуют}\\ \text{такие } \alpha',\ \beta' \in \Sigma, \text{ что } \alpha\beta' = \beta\alpha'.\end{gathered} \tag{8}$$

Полугруппа, удовлетворяющая этому условию, называется *направленной*. Отметим, что всякая коммутативная полугруппа, в частности всякая полугруппа, порожденная одним элементом, всегда направлена.

Пусть A есть $\mathscr{K}$-алгебра, где $\mathscr{K}$ — некоторая категория Ω-алгебр. Тогда говорят, что полугруппа Σ *действует на A взаимно однозначно*, если каждому $\alpha \in \Sigma$ сопоставлен такой взаимно однозначный эндоморфизм θ_α Ω-алгебры A, что

$$\theta_{\alpha\beta} = \theta_\alpha\theta_\beta, \quad \theta_1 = \iota,$$

где через ι обозначено тождественное отображение на A. Для краткости будем писать просто $x\alpha$ вместо $x\theta_\alpha$. Теперь результат, который нужно доказать, можно сформулировать следующим образом:

Теорема 3.4. *Пусть A есть $\mathscr{K}$-алгебра, и пусть Σ — полугруппа, действующая на A взаимно однозначно. Если Σ — направленная полугруппа с двусторонним сокращением, то существует локальная $\mathscr{K}$-алгебра A^*, обладающая следующими свойствами:*

(i) *A — подалгебра алгебры A^*.*

(ii) *Σ действует на A^* автоморфизмами, продолжая действие Σ на A.*

(iii) *Каждый элемент алгебры A^* имеет вид $a\theta_\alpha^{-1}$ для некоторых $a \in A$ и $\alpha \in \Sigma$.*

Кроме того, алгебра A^* определяется условиями (i) — (iii) *однозначно с точностью до изоморфизма.*

Доказательство. Будем писать $\alpha | \beta$ для обозначения того, что $\alpha\lambda = \beta$ для некоторого $\lambda \in \Sigma$; отношение $|$ будет предупорядоченностью полугруппы Σ, при которой по предположению множество Σ направлено. Сделаем это отношение более тонким, считая $\alpha \leqslant \beta$, если существуют такие α', $\beta' \in \Sigma$, что

$$\alpha\beta' = \beta\alpha' \quad \text{и} \quad A\beta' \subseteq A\alpha'.$$

Ясно, что если $\alpha|\beta$, то $\alpha\leqslant\beta$, откуда вытекает, что отношение $\leqslant$ рефлексивно. Мы утверждаем, что это отношение снова будет предупорядоченностью на Σ, при которой множество Σ направлено. Действительно, предположим, что $\alpha\leqslant\beta$, $\beta\leqslant\gamma$, и возьмем такие λ, μ, λ', $\mu'\in\Sigma$, что $\alpha\lambda=\beta\mu$, $A\lambda\subseteq A\mu$, $\beta\lambda'=\gamma\mu'$, $A\lambda'\subseteq A\mu'$. Пусть $\mu, \lambda'|\nu$, скажем $\nu=\mu\varkappa'=\lambda'\varkappa$; тогда $\alpha\lambda\varkappa'=\beta\nu=\gamma\mu'\varkappa$ и

$$A\lambda\varkappa'\subseteq A\mu\varkappa'=A\nu\subseteq A\mu'\varkappa.$$

Поэтому $\alpha\leqslant\gamma$, т. е. $\leqslant$ является предупорядоченностью на Σ. Если теперь $\alpha, \beta\in\Sigma$, то $\alpha, \beta|\gamma$ для некоторого $\gamma\in\Sigma$; отсюда $\alpha, \beta\leqslant\gamma$ и поэтому относительно $\leqslant$ множество Σ снова направлено. Заметим, что, как и отношение $|$, отношение $\leqslant$ также сохраняется при умножении слева.

Пусть λ, $\mu\in\Sigma$ таковы, что

$$A\lambda\subseteq A\mu; \tag{9}$$

тогда существует такое однозначно определенное вложение α алгебры A в себя, что

$$x\alpha\mu=x\lambda \qquad (x\in A); \tag{10}$$

действительно, каждый элемент $x\lambda$ представим в виде $y\mu$, где элемент y однозначно определен. Обозначим этот эндоморфизм α более коротко через $\lambda\mu^{-1}$, помня, однако, что это обозначение оправдано только в предположении (9). Применяя к (10) произвольное $\nu\in\Sigma$, получим

$$x\alpha\mu\nu=x\lambda\nu. \tag{11}$$

Обратно, (11) влечет (10), поскольку эндоморфизм ν взаимно однозначен. Это показывает, что

$$\alpha=\lambda\mu^{-1}=(\lambda\nu)(\mu\nu)^{-1}, \tag{12}$$

где α — вложение, определенное равенством (10).

Теперь для каждого $\alpha\in\Sigma$ возьмем по экземпляру A_α алгебры A вместе с изоморфизмом η_α: $A\to A_\alpha$ и вложим A в A_α с помощью мономорфизма φ_α:

$$x\varphi_\alpha=(x\alpha)\eta_\alpha \qquad (x\in A). \tag{13}$$

Если заданы такие α, $\beta\in\Sigma$, что $\alpha\leqslant\beta$, то определим мономорфизм

$$\varphi_{\alpha\beta}\colon A_\alpha\to A_\beta \tag{14}$$

следующим образом: пусть $\alpha\lambda=\beta\mu$, $A\lambda\subseteq A\mu$; тогда положим $x\varphi_{\alpha\beta}=$ $=x\eta_\alpha^{-1}\lambda\mu^{-1}\eta_\beta$. Это определение не зависит от выбора λ, μ; действительно, если в то же время $\alpha\lambda'=\beta\mu'$ и $A\lambda'\subseteq A\mu'$, то пусть $\mu\nu'=\mu'\nu$;

тогда $\alpha\lambda\nu' = \beta\mu\nu' = \beta\mu'\nu = \alpha\lambda'\nu$, откуда после сокращения слева $\lambda\nu' = \lambda'\nu$, и поэтому

$$\lambda\mu^{-1} = (\lambda\nu')(\mu\nu')^{-1} = (\lambda'\nu)(\mu'\nu)^{-1} = \lambda'\mu'^{-1}.$$

Заметим, что на самом деле $\varphi_{\alpha\beta} = \varphi_\alpha^{-1}\varphi_\beta$; следовательно,

$$\varphi_{\alpha\beta}\varphi_{\beta\gamma} = \varphi_{\alpha\gamma} \quad (\alpha \leqslant \beta \leqslant \gamma) \quad \text{и} \quad \varphi_{\alpha\alpha} = 1.$$

Это показывает, что (14) определяет направленную систему $\mathcal{K}$-алгебр и мономорфизмов. Пусть A^* — прямой предел этой системы; A^* будет локальной $\mathcal{K}$-алгеброй с такими мономорфизмами

$$\varepsilon_\alpha\colon A_\lambda \to A^*, \tag{15}$$

что

$$\varepsilon_\alpha = \varphi_{\alpha\beta}\varepsilon_\beta \quad (\alpha \leqslant \beta). \tag{16}$$

В силу (16) и (13) имеем

$$\varepsilon_\alpha = \varphi_{\alpha,\alpha\lambda}\varepsilon_{\alpha\lambda} = \eta_\alpha^{-1}\lambda\eta_{\alpha\lambda}\varepsilon_{\alpha\lambda},$$

откуда

$$\eta_\alpha\varepsilon_\alpha = \lambda\eta_{\alpha\lambda}\varepsilon_{\alpha\lambda}.$$

Обозначим мономорфизм $\eta_\alpha\varepsilon_\alpha\colon A \to A^*$ через ζ_α; тогда последнее равенство принимает вид $\zeta_\alpha = \lambda\zeta_{\alpha\lambda}$; отсюда вытекает, что для любого $x \in A$ и любых α, β, $\lambda \in \Sigma$

$$(x\alpha)\zeta_\beta = (x\alpha\lambda)\zeta_{\beta\lambda}. \tag{17}$$

Чтобы определить действие Σ на A^*, возьмем произвольное $\alpha \in \Sigma$ и произвольный $x \in A^*$, скажем $x = y\zeta_\beta$ $(\beta \in \Sigma)$. По предположению $\alpha\lambda = \beta\mu$ для некоторых λ, $\mu \in \Sigma$; определим $x\alpha$, полагая

$$x\alpha = (y\mu)\zeta_\lambda. \tag{18}$$

Если бы в то же время мы имели $\alpha\lambda' = \beta\mu'$ $(\lambda', \mu' \in \Sigma)$, то $\mu\nu' = \mu'\nu$ для некоторых ν, $\nu' \in \Sigma$, откуда $\alpha\lambda'\nu = \beta\mu'\nu = \beta\mu\nu' = \alpha\lambda\nu'$, т. е. $\lambda'\nu = \lambda\nu'$, и поэтому в силу (17)

$$(y\mu)\zeta_\lambda = (y\mu\nu')\zeta_{\lambda\nu'} = (y\mu'\nu)\zeta_{\lambda'\nu} = (y\mu')\zeta_{\lambda'}.$$

Это показывает, что правая часть равенства (18) не зависит от выбора λ и μ. Теперь (18) определяет действие полугруппы Σ на A^*; в самом деле, если α, $\beta \in \Sigma$ и $x = y\zeta_\gamma$, то пусть $\gamma\lambda = \alpha\mu$, $\mu\rho = \beta\nu$; тогда $\gamma\lambda\rho = \alpha\mu\rho = \alpha\beta\nu$ и, следовательно,

$$(x\alpha)\beta = (y\zeta_\gamma\alpha)\beta = (y\lambda\zeta_\mu)\beta = y\lambda\rho\zeta_\nu = (y\zeta_\gamma)\alpha\beta = x(\alpha\beta),$$
$$x \cdot 1 = y\zeta_\gamma = x.$$

Далее, если x имеет вид $y\zeta_1$, то (18) превращается в равенство

$$(y\zeta_1)\alpha = (y\alpha)\zeta_1.$$

Поэтому, если мы вложим A в A^*, отождествляя $x \in A$ с $x\zeta_1$, то действие полугруппы Σ на A^*, ограниченное на A, совпадает с заданным действием этой полугруппы на A. Кроме того, так как

$$(x\zeta_\alpha)\alpha = (x\alpha)\zeta_\alpha = x\zeta_1 = x,$$

то отсюда вытекает, что каждому $x \in A^*$ соответствует такой эндоморфизм $\alpha \in \Sigma$, что $x\alpha \in A$, т. е. каждый элемент алгебры A^* имеет вид $a\alpha^{-1}$, где $a \in A$. То же самое равенство показывает, что ζ_α является обратным к α, который поэтому будет автоморфизмом.

Чтобы установить единственность алгебры A^*, обозначим через U универсальную Ω-алгебру, обладающую свойством (ii) данной теоремы (где A^* заменено на U); ясно, что такая алгебра существует (в силу следствия IV.4.3, если в качестве $\mathcal{S}$ взять категорию, состоящую из всех алгебр, изоморфных A, и мономорфизмов между ними), и так как найденная алгебра A^* удовлетворяет (ii) и (i), то канонический гомоморфизм $A \to U$ будет взаимно однозначным; поскольку A^* удовлетворяет (iii), она порождается алгеброй A (с помощью элементов полугруппы Σ и обратных к ним), и поэтому A^* является гомоморфным образом алгебры U. Если это собственный гомоморфный образ, то предположим, что в A^*

$$x\alpha^{-1} = y\beta^{-1}, \tag{19}$$

и пусть $\alpha\lambda = \beta\mu$; тогда

$$x\lambda = x\alpha^{-1}\alpha\lambda = y\beta^{-1}\beta\mu = y\mu;$$

отсюда вытекает, что $x\lambda = y\mu$ в A и, следовательно, в U; применяя $(\alpha\lambda)^{-1}$, видим, что (19) выполняется уже в U; таким образом, алгебра A^* является изоморфным образом алгебры U и поэтому единственна с точностью до изоморфизма. ∎

Этот результат дает простое достаточное условие, при котором для абстрактной полугруппы существует группа дробей (см. Дюбрей [43]).

***Предложение* 3.5.** *Пусть S — некоторая направленная полугруппа с сокращениями; тогда S обладает группой дробей G; кроме того, G определяется полугруппой S однозначно с точностью до изоморфизма и $G = SS^{-1}$. Обратно, любая полугруппа S с группой дробей $G = SS^{-1}$ направлена.*

Для доказательства этого результата нужно только предположить, что полугруппа S действует на самой себе посредством правого умножения, и применить теорему 3.4. Последнее утверждение предложения 3.5 получается следующим образом: если S обладает группой дробей вида SS^{-1}, то для любых $a, b \in S$ $a^{-1}b$ представим в виде uv^{-1}, т. е. $a^{-1}b = uv^{-1}$, и после умножения получаем $bv = au$, откуда S направлена. ∎

Возвращаясь к ситуации теоремы 3.4, заметим, что любой постоянный элемент алгебры A, т. е. значение 0-арного оператора в A, будет обязательно неподвижным при каждом эндоморфизме алгебры A. Будем говорить, что Σ действует на A *регулярно*, если результаты применения любых двух различных элементов полугруппы Σ к любому непостоянному элементу алгебры A различны. Тогда имеем

Следствие 3.6. *Если Σ, A и A^* — такие же, как в теореме 3.4, и Σ действует на A регулярно, то Σ действует на A^* также регулярно.*

Действительно, предположим, что $x \in A$ и $\alpha, \beta, \gamma \in \Sigma$ таковы, что

$$x\gamma^{-1}\alpha = x\gamma^{-1}\beta, \quad \text{где} \quad x\gamma^{-1} \text{ — непостоянный элемент;} \tag{20}$$

тогда либо $x\gamma \neq x$, либо $\gamma = 1$ и $x \in A$. В последнем случае $\alpha = \beta$ по предположению. В первом случае существуют такие λ, μ, λ', $\mu' \in \Sigma$, что $\alpha\lambda = \gamma\mu$, $\beta\lambda' = \gamma\mu'$ и, следовательно, существуют такие ν, $\nu' \in \Sigma$, что $\lambda\nu' = \lambda'\nu = \rho$, скажем. Отсюда вытекает, что

$$\gamma\mu\nu' = \alpha\rho, \quad \gamma\mu'\nu = \beta\rho, \tag{21}$$

и, умножая (20) на ρ, получаем

$$x\mu\nu' = x\gamma^{-1}\alpha\rho = x\gamma^{-1}\beta\rho = x\mu'\nu.$$

Так как $x\gamma \neq x$, то x не является постоянным элементом; поэтому $\mu\nu' = \mu'\nu$, и в силу (21)

$$\alpha\rho = \gamma\mu\nu' = \gamma\mu'\nu = \beta\rho;$$

поэтому $\alpha = \beta$, что и утверждалось. ∎

Проблема деления для колец, а именно получение условий, при которых ассоциативное кольцо вложимо в тело (не обязательно коммутативное), гораздо труднее, чем соответствующая проблема для полугрупп. Не ограничивая общности, снова можем рассматривать лишь кольца с единицей 1 и можем предполагать, кроме того, что $1 \neq 0$. *Телом дробей* кольца R будем называть любое тело, которое содержит R в качестве подкольца и порождается кольцом R.

Прежде всего мы не можем утверждать существования универсального тела для данного кольца (даже если тело дробей существует), ссылаясь на универсальную алгебру, поскольку тела не образуют многообразия. На самом деле, взяв категорию тел и гомоморфизмов, можно показать, что в общем случае универсального тела не существует. В частном случае коммутативных колец и полей можно установить существование универсального поля для данного кольца, если действовать не в категории полей и гомоморфизмов, а в категории полей и точек, т. е. обобщенных гомоморфизмов, отображающих некоторые из элементов поля в бесконечность (см., например, Ленг [58]). При определении точек для тел не возникает никаких трудностей, но в настоящее время не известно даже, будет ли полученная категория обладать чем-нибудь, соответствующим свободным полям.

Вторая трудность, которая также не возникает для полугрупп, состоит в том, что если мы присоединим обратные элементы для всех ненулевых элементов кольца R (предполагая, что R обладает телом дробей), то кольцо, порожденное всеми этими элементами, не обязано быть телом; например, если $a, b \in R$, $ab \neq 0$, то $ab^{-1} + ba^{-1}$ *может* не *иметь* обратного элемента вида uv^{-1}, где $u, v \in R$. Однако в частном случае, когда R обладает телом дробей, все элементы которого представимы в виде uv^{-1} ($u, v \in R$, $v \neq 0$), все эти трудности исчезают, и получается следующий изящный результат, принадлежащий Оре [31]:

Теорема 3.7. *Пусть R — ассоциативное кольцо (с единицей $1 \neq 0$), ненулевые элементы которого образуют по умножению направленную полугруппу; тогда существует такое тело K, содержащее R в качестве подкольца, что каждый элемент из K представим в виде ab^{-1} $(a, b \in R)$. Кроме того, тело K определяется кольцом R однозначно с точностью до изоморфизма.*

Кольцо R, удовлетворяющее условиям теоремы 3.7, называется *(правой) областью Оре.*

Доказательство. Через R^* обозначим множество ненулевых элементов кольца R. По предположению $R^* \neq \varnothing$, и R^* будет полугруппой по умножению тогда и только тогда, когда в R нет делителей нуля; в этом случае R^* будет полугруппой с сокращениями: $ab = ac$ влечет $a(b - c) = 0$ и если $a, b, c \in R^*$, то это означает, что $b = c$; возможность правостороннего сокращения получается аналогично. Будем рассматривать теперь R как абелеву группу (по сложению) вместе с R^* как полугруппой правых умножений. По теореме 3.4 существует абелева группа S, являющаяся расширением группы R, причем элементы из R^* действуют на S как автоморфизмы. Если через a_r обозначен автоморфизм группы S, определяемый элементом $a \in R^*$, то $1_r = 1$, $(ab)_r = a_r b_r$. Единственным постоянным элементом в R (как в абелевой группе) является 0; следовательно, любые два автоморфизма, совпадающие на ненулевом элементе группы S, равны, и это показывает, что $(a + b)_r = a_r + b_r$. Итак, мы имеем гомоморфизм кольца R в кольцо эндоморфизмов группы S, при котором ненулевые элементы кольца R отображаются в обратимые элементы. Пусть K — мультипликативная группа, порожденная образами элементов полугруппы R^*, вместе с 0. Тогда каждый ненулевой элемент из K представим в виде ab^{-1}, где $a, b \in R^*$. Отсюда вытекает, что K замкнуто относительно операции $x \to x + 1$; действительно, если

$x = ab^{-1}$, то $x+1=(a+b)b^{-1}$. Чтобы доказать, что K — тело, нужно только показать, что K замкнуто относительно сложения. Пусть $x, y \in K$; тогда

$$x+y=\begin{cases} x, & \text{если} \quad y=0, \\ (xy^{-1}+1)y, & \text{если} \quad y \neq 0. \end{cases}$$

Итак, R вложено в тело нужного вида. Кроме того, K^* — множество ненулевых элементов тела K — однозначно определено как группа дробей полугруппы R^*, и, следовательно, тело K единственно (с точностью до изоморфизма). ∎

Построение, приведенное в теореме 3.7, было обобщено на кольца, мультипликативные полугруппы которых удовлетворяют условиям теоремы 3.7 резидуально (Кон [61]). Это дает возможность вкладывать свободные ассоциативные алгебры в тела. Другой метод вложения свободных ассоциативных алгебр в тела, принадлежащий Мальцеву [48] и Нейману [49], основан на том, что свободная группа может быть линейно упорядочена (Нейман [49′]) и что групповая алгебра (над полем F) свободной группы над X содержит в качестве подалгебры свободную ассоциативную алгебру над F с множеством свободных образующих X. Теперь вложение осуществляется при помощи следующей теоремы:

Теорема 3.8. (Мальцев, Нейман.) *Групповая алгебра над полем F линейно упорядоченной группы G может быть вложена в тело.*

Доказательство (Хигмэн [52]). Рассмотрим прямую степень F^G как векторное пространство над F. Каждому элементу $f \in F^G$ сопоставим подмножество $D(f)$ группы G, его *опору*, определяемое равенством

$$D(f)=\{s \in G \mid f(s) \neq 0\}.$$

Пусть A — подмножество прямой степени F^G, состоящее из всех элементов, которые обладают вполне упорядоченными опорами. Формально всякий элемент множества A может быть записан в виде степенного ряда: $f=\sum f(s)s$. Сумма двух таких степенных рядов снова принадлежит множеству A, так как объединение двух вполне упорядоченных множеств снова вполне упорядочено. Определим в A произведения, полагая

$$fg=\left(\sum f(s)s\right)\left(\sum g(t)t\right)=\sum\left(\sum_{st=u} f(s)g(t)\right)u. \tag{22}$$

Для данного $u \in G$ уравнение $st=u$ имеет лишь конечное множество решений (s, t) в $D(f) \times D(g)$, так как обе опоры вполне упорядочены.

Это показывает, что внутренняя сумма правой части равенства (22) конечна; теперь $D(fg)$ является образом множества $D(f) \times D(g)$ при отображении $(s, t) \to st$ и вполне упорядочено (как образ частично вполне упорядоченного множества, см. § III. 2). Следовательно, элемент fg, определенный равенством (22), лежит в A, и легко проверить, что при этих определениях A образует алгебру над F, содержащую групповую алгебру группы G в качестве подалгебры (а именно подалгебры элементов с конечными опорами).

Рассмотрим теперь элемент алгебры A вида $1 - f$, где $f(s) = 0$ для $s < 1$. Мы утверждаем, что $1 + f + f^2 + \ldots$ можно представить в виде степенного ряда. Действительно, свободная полугруппа над $D(f)$ с упорядоченностью по делимости частично вполне упорядочена ввиду теоремы III. 2.9; отсюда вытекает, что $\bigcup D(f^n)$ частично вполне упорядочено, и, кроме того, никакой элемент группы G не может принадлежать бесконечному множеству носителей $D(f^n)$, поскольку решения $(s_1, \ldots, s_n)$ уравнения

$$s_1 \cdots s_n = u$$

при фиксированном u являются попарно несравнимыми элементами частично вполне упорядоченного множества. Это показывает, что $1 + f + f^2 + \ldots$ принадлежит множеству A, и легко проверить, что на самом деле этот элемент будет обратным к $1 - f$. Теперь каждый ненулевой элемент множества A представим в виде $\alpha u(1 - f)$, где $\alpha \in F$, $\alpha \neq 0$, $u \in G$ и $f(s) = 0$ для $s < 1$. Таким образом, этот элемент обладает обратным в A, и это показывает, что A — тело. ∎

Ни один из этих методов вложения свободной ассоциативной алгебры в тело не является чисто алгебраическим, так как все эти методы используют предельные переходы, и это создает трудности при решении вопроса, будут ли полученные тела «универсальными» в некотором смысле. Однако, сравнивая эти конструкции с более ранними алгебраическими конструкциями Муфанг [37], можно получить два неизоморфных тела дробей для данной свободной ассоциативной алгебры.

В заключение отметим, что не известно ни одного кольца R, не вложимого в тело, ненулевые элементы которого образуют полугруппу, вложимую в группу [1]).

УПРАЖНЕНИЯ

1. Показать, что идемпотентный элемент полугруппы с сокращениями S будет обязательно единицей полугруппы S, и вывести отсюда, что полугруппа с сокращениями имеет не больше одного идемпотента.

---

[1]) К настоящему времени существование примеров таких колец уже анонсировано несколькими авторами. — *Прим. ред.*

2. Проверить, что полугруппа, определяемая соотношениями (6), допускает двусторонние сокращения. (Воспользоваться теоремой III. 9.3 для получения нормальной формы слов.)

3. (Мальцев.) Показать, что свободная полугруппа S с двумя свободными образующими a, b может быть вложена в $G = \mathrm{Gp}\{a, b \mid (ab^{-1})^2 = 1\}$ и в $H = \mathrm{Gp}\{a, b \mid (ab^{-1})^3 = 1\}$ и что G и H будут неизоморфными группами дробей для S. Показать, что S обладает неизоморфными группами дробей, которые несжимаемы как расширения полугруппы S. (Применить предложение VII. 2.5 к G и H.)

4. Доказать предложение 3.1 непосредственно, используя ультрапроизведения. (В качестве множества индексов взять систему конечных подмножеств полугруппы S.)

5. Будем называть последовательность преобразований *допустимой*, если она имеет вид, описанный в теореме 3.3. Показать, что в теореме 3.3 достаточно взять только такие последовательности, которые не содержат никаких допустимых собственных подпоследовательностей.

6. Непосредственно проверить условия теоремы 3.3 для направленных полугрупп с сокращениями.

7. Пусть S — полугруппа с сокращениями, в которой любые два элемента с общим правым кратным обладают наименьшим общим правым кратным (единственным с точностью до умножения справа на обратимые элементы). Показать, что при применении теоремы 3.3 нужно рассматривать только допустимые последовательности, не содержащие подпоследовательности вида ([ ). (Записать условие (5) теоремы 3.3 для последовательности ... ([ ) ... и показать, что его можно заменить таким же условием для последовательности ... [... .)

8. Пусть S — полугруппа и p — такой элемент полугруппы S, что $ap = pa'$ для некоторых $a, a' \in S$ влечет либо $a = a' = 1$, либо $a = pb$, $a' = bp$. Показать, что p потенциально обратим.

9. Пусть S — полугруппа и C—такое подмножество центра полугруппы S, что в S возможно сокращение на каждый элемент множества C. Показать, что C потенциально обратимо.

10. Показать, что полугруппа $S = \mathrm{Sg}^*\{a, b \mid ba = ab^r\}$ (где r — целое положительное число) удовлетворяет законам сокращения и направлена. (Получить нормальную форму для элементов полугруппы S.)

11. Показать, что подпрямое произведение двух направленных полугрупп не обязательно будет направленной полугруппой. (Рассмотреть полугруппы из упражнения 10 для различных чисел r.)

12. Показать, что всякое (ассоциативное) кольцо может быть вложено в кольцо с 1. Пусть через R^1 обозначено универсальное «кольцо с 1» для R. Получить необходимые и достаточные условия для R, при которых R^1 не имеет делителей 0.

13. (Голди.) Показать, что каждая область целостности с условием максимальности для правых идеалов будет правой областью Оре. (Показать, что если a, b не имеют общего правого кратного, то правые идеалы, порожденные $b, ab, \ldots, a^n b$, образуют строго возрастающую цепь.)

14. (Алберт.) Показать, что никакое линейно упорядоченное кольцо не имеет делителей нуля. Показать, что если такое кольцо является областью Оре, то данная упорядоченность имеет единственное продолжение в теле дробей.

15. (Амицур.) Показать, что кольцо без делителей нуля, которое удовлетворяет некоторому тождеству, выполняющемуся не во всех кольцах, вкладывается в тело.

16. Пусть R — некоторое кольцо с 1 и M — мультипликативно замкнутое подмножество кольца R, содержащее 1, но не содержащее делителей нуля и направленное относительно делимости слева. Показать, что если для каждого $a \in M$ существует такое $b \in M$, что $Rb \subseteq aR$ и, кроме того, $Mx \cap M \neq \varnothing$ влечет $x \in M$, то R может быть вложено в такое кольцо S, что элементы множества M обратимы в S и каждый элемент кольца S представим в виде am^{-1} ($a \in R$, $m \in M$).

17. Показать, что для любого тела K с эндоморфизмом θ существует расширение L с автоморфизмом, индуцирующим θ. (Заметить, что по определению каждый эндоморфизм оставляет единицу 1 неподвижной.)

18. Пусть $F(x)$ — поле рациональных функций от x над полем F, а через α, β, γ обозначим эндоморфизмы, порожденные отображениями $x \to -x$, $x \to x^2$, $x \to x^3$ соответственно. Тогда $F(x)$ может быть вложено в тело E, которое обладает автоморфизмами α', β', γ', индуцирующими на $F(x)$ соответственно α, β, γ, но не существует полугруппы автоморфизмов тела E, которая после ограничения на $F(x)$ индуцирует действие полугруппы, порожденной эндоморфизмами α, β, γ.

4. ПРОБЛЕМА ДЕЛЕНИЯ ДЛЯ ГРУППОИДОВ

Проблема деления, которая обсуждалась в § VII.3, как это ни странно, становится значительно проще, если отбросить условие ассоциативности. Теперь задача состоит в том, чтобы группоид вложить в квазигруппу. Так как в квазигруппе однозначно определено левое и правое деление, то для вложимости группоида G в квазигруппу, очевидно, необходимо, чтобы G удовлетворял законам правостороннего и левостороннего сокращения. Это условие также достаточно для того, чтобы вложение было возможно (Бейтс [47], Ивенс [51]). Для установления этого факта воспользуемся представлением алгебр в полугруппах (предложение IV.4.6). При доказательстве удобно рассматривать правое и левое деление отдельно; итак, будем называть группоид G *правой квазигруппой*, если уравнение

$$xa = b \tag{1}$$

обладает единственным решением в G для $a, b \in G$. Ясно, что во всякой правой квазигруппе и, в более общем случае, во всяком группоиде, содержащемся в правой квазигруппе в качестве подгруппоида, возможно правостороннее сокращение:

$$\text{если} \quad ac = bc, \quad \text{то} \quad a = b. \tag{2}$$

***Лемма* 4.1.** *Пусть G — группоид с правосторонним сокращением; тогда G может быть вложен в правую квазигруппу G^*. Если, кроме того, G удовлетворяет закону левостороннего сокращения, то G^* также удовлетворяет этому закону.*

Доказательство. Построим сначала расширение G_1 группоида G, в котором уравнение (1) разрешимо для всех $a \in G$ и всех

$b \in G_1$. Пусть S — свободная полугруппа (с 1) над множеством G и двумя дополнительными элементами μ, ρ (отличными от элементов множества G) как множеством свободных образующих. Через $\mathfrak{q}$ обозначим конгруэнцию на S, порожденную парами $(a\mu a\rho, 1)$, $(a\rho a\mu, 1)$, $(ab\mu, c)$, $(cb\rho, a)$, где a, b, c пробегают все такие элементы группоида G, что $ab = c$ в G. Записывая $S' = S/\mathfrak{q}$, видим, что естественный гомоморфизм $x \to x'$ полугруппы S на S' обладает свойствами

$$(ab)' = a'b', \quad a, b \in G,$$
$$u'a'\mu'a'\rho' = u'a'\rho'a'\mu' = u', \quad u \in S.$$

Таким образом, интерпретируя μ и ρ как операторы умножения и правого деления, мы получим вложение нужного вида, если сможем показать, что $\mathfrak{q}$ разделяет G и выполняются условия сокращения.

Рассмотрим граф, определенный данным представлением полугруппы S'; отрезки этого графа получаются при выполнении преобразований

$$ua\mu a\rho v \to uv, \tag{3}$$
$$ua\rho a\mu v \to uv, \tag{4}$$
$$uab\mu v \to ucv, \tag{5}$$
$$ucb\rho v \to uav \tag{6}$$

и обратных к ним, где u, $v \in S$, a, b, $c \in G$ и $ab = c$ в G. Отметим, что в силу правостороннего сокращения a однозначно определяется элементами b и c, так что преобразование (6), когда оно возможно, полностью определяется своей исходной вершиной $ucb\rho v$.

Наша цель состоит в том, чтобы проверить условия теоремы III.9.3. Ясно, что каждое преобразование (3) — (6) уменьшает длину любого слова w, к которому оно применяется; поэтому мы получим приведенное слово через конечное число шагов, которое ограничено длиной слова w. Предположим теперь, что каждое из двух слов w_1, w_2 получено с помощью преобразований (3) — (6) из одного и того же слова w; нам нужно показать, что, применяя дальнейшие преобразования к w_1 и w_2, можно получить одно и то же слово из обоих этих слов. Это ясно, если части слова w, затронутые преобразованиями, которые приводят к w_1 и w_2, не перекрываются. Далее, перекрытие может произойти только для следующих пар преобразований: (3) и (4), (3) и (5), (4) и (6). Если перекрываются (3) и (4), то w должно иметь вид $w = ua\mu a\rho a\mu v$ или $w = ua\rho a\mu a\rho v$, скажем первый. Применяя либо (3), либо (4), получаем $ua\mu v$, и поэтому в этом случае $w_1 = w_2$; тот же самый вывод получается, если $w = ua\rho a\mu a\rho v$. Далее, пусть перекрываются (3) и (5); тогда $w = uab\mu b\rho v$; применяя (3) и (5), получим $w_1 = uav$ и $w_2 = ucb\rho v$ соответственно, где $c = ab$. Если к w_2 мы применим (6), то получим $uav = w_1$. Случай, когда перекрываются (4) и (6), рассматривается аналогично.

Итак, условия теоремы III.9.3 выполняются, и мы заключаем отсюда, что приведенные слова в S образуют трансверсал для S'. Так как каждый элемент группоида G, очевидно, является приведенным словом, то это показывает, что G вложен в S'. Пусть T — подалгебра в S относительно операторов μ и ρ, порожденная группоидом G. Ее образ T' при $\operatorname{nat} \mathfrak{q}$ будет группоидом, содержащим G, в котором возможно правое деление на все элементы из G, т. е. уравнение

$$xa\mu = g \quad (a \in G, \ g \in T')$$

обладает единственным решением в T', а именно

$$x = ga\rho.$$

Здесь мы отождествили элементы множества G и μ, ρ с их образами при $\operatorname{nat} \mathfrak{q}$. Чтобы проверить возможность правостороннего сокращения в T', возьмем такие u, v, $w \in T$, что

$$uw\mu \equiv vw\mu \pmod{\mathfrak{q}}. \tag{7}$$

Без ограничения общности можно считать u, v и w приведенными словами; если в (7) в обеих частях стоят приведенные слова, то они должны быть равны, и поэтому $u = v$ *в силу возможности* сокращения в свободной полугруппе S. Остается случай, когда в (7) хотя бы с одной стороны стоит неприведенное слово. Теперь T является просто алгеброй $\{\mu, \rho\}$-слов над G; поэтому всякое собственное подслово слова $uw\mu$ должно быть подсловом в u или w (следствие III.2.5); но каждое преобразование (3) — (6) состоит в том, что некоторое слово заменяется другим словом. Поэтому любое преобразование над собственным подсловом слова $uw\mu$ происходит целиком в пределах u или w и поэтому может уже считаться выполненным в u или w соответственно. Так как u и w — приведенные слова, то отсюда вытекает, что $uw\mu$ будет приведенным словом, за исключением того случая, когда u, $w \in G$, и тогда $uw\mu = c \in G$. *При этом* $vw\mu$ *также* не является приведенным словом, поскольку в противном случае мы получили бы равенство $vw\mu = c$ между приведенными словами — противоречие (например, при сравнении длин). Поэтому v также должно принадлежать G; в силу (7) имеем $uw = vw$ в G и, сокращая в G, находим, что $u = v$.

Предположим теперь, что G удовлетворяет закону левостороннего сокращения, и пусть

$$uv\mu \equiv uw\mu \pmod{\mathfrak{q}}, \tag{8}$$

где u, v, w являются снова приведенными элементами в T. Те же самые рассуждения показывают, что если в (8) с одной стороны получается приведенное слово, то также и с другой, и u, v, $w \in G$; равенство $v = w$ теперь вытекает из возможности сокращения в G.

Мы построили группоид T', содержащий G, в котором уравнение (1) обладает единственным решением для любых $a \in G$, $b \in T'$, при этом в T' можно производить (левосторонние или правосторонние) сокращения, если только их можно производить в G. Положим $G_1 = T'$ и применим тот же самый процесс к G_1; повторяя эту конструкцию, получим возрастающую цепь

$$G \subseteq G_1 \subseteq G_2 \subseteq \ldots$$

группоидов, каждый из которых с правосторонним сокращением; прямой предел G^* этой цепи будет снова группоидом с правосторонним сокращением. Кроме того, если дано произвольное уравнение (1) в G^*, то можно найти такое n, что a, $b \in G_n$, и по построению (1) обладает решением в G_{n+1} и потому в G^*. Благодаря закону правостороннего сокращения, это решение будет единственным. Итак, G^* — правая квазигруппа, содержащая G. Если теперь G удовлетворяет закону левостороннего сокращения, то G_1, G_2, ..., а поэтому и их прямой предел G^* также удовлетворяют закону левостороннего сокращения (так как это является локальным свойством). ∎

Из соображений симметрии ясно, что будет справедлива соответствующая лемма, если всюду слова «правое» и «левое» поменять местами (при очевидном определении левой квазигруппы). Поэтому если мы возьмем группоид G с двусторонним сокращением, то можно вложить G в правую квазигруппу с левосторонним сокращением, а эту квазигруппу в свою очередь можно вложить в левую квазигруппу с правосторонним сокращением, скажем G'. Тогда любое уравнение

$$xa = b \quad \text{или} \quad ay = b, \tag{9}$$

где a, $b \in G$, обладает решением в G'. Повторяя эту конструкцию, снова получим возрастающую цепь

$$G \subseteq G' \subseteq G'' \subseteq \ldots,$$

прямой предел которой H будет квазигруппой, содержащей G. Действительно, если дано некоторое уравнение вида (9) в H, то можно взять такое n, что a, $b \in G^{(n)}$, и затем решить это уравнение в $G^{(n+1)}$; итак, данное уравнение обладает решением в H, и это решение единственно, поскольку H удовлетворяет закону двустороннего сокращения. Этим доказана

Теорема 4.2. *Всякий группоид с двусторонним сокращением может быть вложен в квазигруппу.* ∎

Отметим, что результат, аналогичный лемме 4.1 относительно одностороннего деления, тем же методом может быть доказан для полугрупп (Кон [56]), но получающаяся полугруппа не будет удовлетворять законам сокращения, даже если мы начнем с полугруппы с сокращениями. По этой причине данный метод не может быть распространен на случай двустороннего деления — ограничение, которое следовало ожидать ввиду теоремы Мальцева (теорема 3.3).

В случае неассоциативных колец (для краткости, NA-колец) также существуют простые необходимые и достаточные условия вложимости в NA-тело (т. е. кольцо, ненулевые элементы которого образуют квазигруппу по умножению) (Нейман [51]). Как и в коммутативном случае, можно определить категорию NA-тел и T-гомоморфизмов и можно показать, что представление NA-колец в этой категории обладает универсальным функтором (Скорняков [57])[1]).

УПРАЖНЕНИЯ

1. Показать, что каждый группоид с единицей, удовлетворяющий законам сокращения, может быть вложен в лупу.

2. Показать, что всякий группоид может быть вложен в группоид, в котором каждое уравнение $xa = b$ или $ay = b$ обладает по крайней мере одним решением.

3. Получить нормальную форму для элементов свободной квазигруппы с одним свободным образующим. (Воспользоваться теоремой III. 2.3 и предложением IV. 4.6.)

5. ЛИНЕЙНЫЕ АЛГЕБРЫ

Одно из главных приложений теории представлений, развитой в § IV.4, состоит в применении ее к представлению лиевых и йордановых алгебр в ассоциативных алгебрах. Хотя в основном в лиевом и йордановом случае ситуация одинакова, однако детали во многом различны, и каждая теория имеет свои собственные особые трудности, которые объясняются главным образом наличием закона ассоциативности. Поэтому мы посвятим этот параграф случаю линейных алгебр, не обязательно ассоциативных, а в следующих параграфах рассмотрим влияние ассоциативности.

Пусть K — некоторое коммутативное и ассоциативное кольцо с 1, и через (K) обозначим категорию всех линейных K-алгебр (не обязательно ассоциативных). Когда $K = Z$, кольцу целых чисел, (Z)

---

[1]) Теорию свободных разложений в указанной категории, построенную Л. А. Скорняковым, на случай мультиоператорных алгебр с делением обобщил И. С. Иванов (*ДАН СССР*, **165** (1965), 28—30). При этом понятие мультиоператорной алгебры над полем есть обобщение понятия алгебры над полем, состоящее в том, что бинарное умножение заменяется произвольной системой Ω операций произвольной арности, не меньшей двух, притом полилинейных относительно аддитивного векторного пространства (см. А. Курош, *Сиб. матем. журн.*, **1** (1960), 62—70, 638). — *Прим. ред.*

будет по существу категорией всех колец. В обозначениях главы II умножение в K-алгебре может быть обозначено символом оператора μ

$$ab\mu; \tag{1}$$

обычно этот символ совсем опускают, но так как закон ассоциативности не обязан выполняться, то теперь при повторных произведениях необходимо использовать скобки, чтобы различать, например, $(ab)c$ и $a(bc)$. Мы примем компромиссное обозначение, используя скобки, но отбрасывая левую скобку. Итак, произведение a на b будет записываться так:

$$ab). \tag{2}$$

На самом деле это совпадает с обозначением (1), где μ заменено на). Итак, закон ассоциативности должен теперь читаться так: $ab)\,c) = abc))$.

Рассмотрим теперь произвольное тождество в K-алгебре; такое тождество можно привести к виду

$$f = 0, \tag{3}$$

где f — слово в свободной K-алгебре, скажем K_X, над некоторым алфавитом X. Как и в § IV.2, можно показать, что K_X является группоидной алгеброй над K свободного группоида Γ_X над X. Итак, каждый элемент алгебры K_X единственным образом может быть представлен в виде

$$f = \sum f(s)\, s,$$

где $f(s) \in K$, $s \in \Gamma_X$ и $f(s) = 0$ для всех элементов s, за исключением конечного числа. Каждому элементу s группоида Γ_X сопоставлено целое положительное число $l(s)$, его *длина*, равное числу сомножителей (или, эквивалентно этому, на единицу большее, чем число скобок). С помощью длины определим *степень* элемента f следующим образом:

$$d(f) = \max\{l(s) \mid f(s) \neq 0\}.$$

Для $f = 0$ степень примем равной $-\infty$.

Всякое систематическое изучение многообразий линейных K-алгебр должно исходить из рассмотрения возможных множеств тождеств. Теперь тождества (3) можно классифицировать по их степени. Для произвольной степени n это трудная задача, охватывающая теорию представлений симметрической группы n-й степени и общей линейной группы над K (см. Мальцев [50], Шпехт [50], Кон [52]), и если не иметь в виду определенной задачи, такая классификация вряд ли оправдала бы затраченные усилия. Поэтому ограничимся простейшим случаем, когда $n \leqslant 2$ и K — поле. Тогда полная классификация дается следующей теоремой:

Теорема 5.1. *Пусть K — произвольное поле; тогда всякое тождество степени не выше двух, которое выполняется не во всех* *линейных K-алгебрах, эквивалентно для K-алгебр одному из следующих тождеств*: (i) $x=0$; (ii) $xy)=0$; (iii) $x^2)-x=0$ (*закон идемпотентности*); (iv) $x^2)=0$ (*закон альтернативности*); (v) $xy)-yx)=0$ (*закон коммутативности*). *Кроме того, случай* (iii) *возможен только тогда, когда K — поле из двух элементов.*

Доказательство. Всякое тождество содержит лишь конечное число различных неизвестных; наиболее общее тождество степени два от $x_1, \ldots, x_n$ имеет вид

$$\sum x_i\alpha_i + \sum x_ix_j)\beta_{ij} = 0. \tag{4}$$

Если мы зафиксируем k и положим в (4) $x_i = 0$ для $i \neq k$, то получим

$$x_k\alpha_k + x_k^2)\beta_{kk} = 0 \quad (k = 1, \ldots, n); \tag{5}$$

вычитая равенства (5) из (4), получаем

$$\sum_{i \neq j} x_ix_j)\beta_{ij} = 0. \tag{6}$$

Итак, (4) влечет (5) и (6), и, обратно, если выполняются (5) и (6), то можно вывести (4), так что (4) эквивалентно (5) и (6).

Предположим теперь, что не все α_i равны нулю, скажем $\alpha_1 \neq 0$. Тогда, разделив на α_1, из (5) получаем

$$x + x^2)\gamma = 0, \tag{7}$$

где мы написали x вместо x_1. Таким образом, если $\gamma = 0$, то мы получаем тождество $x = 0$, которое, очевидно, влечет (4), так что мы имеем случай (i). В любом случае, если в (7) заменить x на $x\lambda$ ($\lambda \in K$) и полученное равенство вычесть из равенства (7), умноженного на λ^2, мы получим $x(\lambda^2 - \lambda) = 0$; это снова дает (i), за исключением того случая, когда $\lambda^2 = \lambda$ для всех элементов λ поля K, что может быть только тогда, когда K состоит из двух элементов. Следовательно, если это так и случай (i) не выполняется, то имеем

$$x^2) - x = 0. \tag{8}$$

Если в (8) заменить x на $x+y$ и затем упростить, используя (8) (как в § V.2), то получим

$$xy) + yx) = 0. \tag{9}$$

Итак, используя одно равенство (8), можно привести (4) к виду

$$\sum_{i<j} x_ix_j)\gamma_{ij} = 0. \tag{10}$$

Если это не тождественный нуль, то пусть $\gamma_{ij} \neq 0$; тогда, полагая $x_i = x_j = x$, $x_k = 0$ ($k \neq i, j$), получаем $x^2) = 0$, а вместе с (8) это показывает, что $x=0$, т. е. имеем случай (i). В противном случае (10) равно нулю тождественно, т. е. (8) влечет (6), и остается только (5). Но мы уже видели, что это может дать только случай (i) или случай (iii), и в последнем случае K — поле из двух элементов.

Остается обсудить случай, когда все α_i в (4) равны нулю. Полагая все переменные, кроме двух, равными нулю, из (6) получаем тождества

$$x_i x_j)\beta_{ij} + x_j x_i)\beta_{ji} = 0 \quad (i,\ j = 1,\ \ldots,\ n), \tag{11}$$

которые все вместе эквивалентны (6). Если $\beta_{kk} \neq 0$ для некоторого k или если $\beta_{ij} + \beta_{ji} \neq 0$ для некоторых i, j, то из (5) или (11) соответственно (помня, что теперь $\alpha_k = 0$ в (5)) можно вывести тождество

$$x^2) = 0. \tag{12}$$

Из (12) получаем (9) (заменяя x на $x+y$ и используя (12) для упрощения полученного тождества), и этим снова можно воспользоваться для приведения (4) к виду (10). Если (10) не тождественный нуль, скажем $\gamma_{ij} \neq 0$, то, полагая все неизвестные, за исключением x_i и x_j, равными нулю, выведем тождество

$$xy) = 0, \tag{13}$$

и, наоборот, (13) влечет (4) (в предположении, что все α_k равны нулю). Итак, имеем случай (ii); с другой стороны, если (10) получилось тождественно равным нулю, то это означает, что (12) влечет (4) и поэтому эквивалентно (4), т. е. случай (iv).

Остался только случай, когда $\beta_{kk} = 0$ для всех k в (5), так что (5) выполняется тождественно, и в (11) $\beta_{ij} + \beta_{ji} = 0$ для всех i, j. Так как (4) не удовлетворяется тождественно, то некоторое β_{ij} отлично от нуля, и таким образом получаем

$$xy) - yx) = 0;$$

обратно, этим тождеством можно воспользоваться для приведения (6) к нулю, и поэтому оно эквивалентно нашему исходному тождеству (4), т. е. имеем случай (v). ∎

Для $\alpha = \text{i}, \ldots, \text{v}$ через $(K)_\alpha$ обозначим многообразие линейных K-алгебр, определяемое тождеством (α) теоремы 5.1. Ясно, что $(K)_{\text{i}}$ — тривиальное многообразие и $(K)_{\text{ii}}$ — многообразие «нулевых алгебр», т. е. K-модулей, которые рассматриваются как линейные алгебры с нулевым умножением. $(K)_{\text{iii}}$ — многообразие *идемпотентных* алгебр; при наличии закона ассоциативности эти алгебры будут просто булевыми алгебрами (см. § V.2), однако легко построить неассоциативные алгебры в $(K)_{\text{iii}}$ (см. упражнение 2). На самом деле были построены общие (т. е. нелинейные) алгебры, все подалгебры которых с двумя образующими являются булевыми алгебрами, но сами эти алгебры не являются булевыми (Даймонд и Маккинси [47]). Такие алгебры не могут быть линейными в силу результата упражнения 1, приведенного ниже. Это показывает, что аксиоматический ранг булевых алгебр не меньше трех (см. § IV.3); *поскольку булевы алгебры могут быть определены тождествами от трех переменных*, то на самом деле их аксиоматический ранг равен трем.

Алгебры многообразия $(K)_{\mathrm{lv}}$ называются *антикоммутативными*[1]) или $(-)$-*алгебрами*. Существует естественный способ представления $(-)$-алгебр в линейных K-алгебрах, который мы теперь опишем. Каждой K-алгебре A можно сопоставить другую K-алгебру A^-, на которой структура K-модуля такая же, как и на A, но в которой умножение задается равенством

$$xy] = xy) - yx). \tag{14}$$

Алгебру A^- будем называть $(-)$-алгеброй, соответствующей алгебре A; ясно, что на самом деле A^- будет $(-)$-алгеброй, операции которой являются производными от операций алгебры A. Таким образом, категория (K) всех линейных K-алгебр оказывается подчиненной категории $(K)_{\mathrm{lv}}$. Теперь в силу следствия IV.4.3 представление (14) $(-)$-алгебр в K-алгебрах обладает универсальным функтором, сопоставляющим каждой $(-)$-алгебре B линейную K-алгебру $U(B)$ и гомоморфизм

$$u\colon\ B \to U(B)^-, \tag{15}$$

который универсален для гомоморфизмов алгебры B в алгебры вида A^-. Предположим теперь, что характеристика поля K отлична от двух; тогда на любой $(-)$-алгебре B с умножением $xy]$ можно определить второе умножение $xy)$, полагая

$$xy) = \frac{1}{2}\, xy]. \tag{16}$$

Если полученную таким образом алгебру обозначить через $B^\natural$, то тождественное отображение определяет представление алгебры B в алгебре $B^\natural$, так как

$$xy) - yx) = \frac{1}{2}(xy] - yx]) = xy].$$

Итак, каждая $(-)$-алгебра обладает точным представлением (14), и отсюда вытекает, что (15) будет вложением. По этой причине $U(B)$ называется *универсальной линейной K-оболочкой* $(-)$-алгебры B даже в случае произвольного основного кольца, когда (15) не обязано быть взаимно однозначным. Мы можем сформулировать наш результат в виде следующей теоремы:

---

[1]) С некоторых точек зрения естественнее было бы называть эти алгебры *альтернирующими*; *мы избегаем* этого названия из-за возможной путаницы с альтернативными алгебрами (см. упражнение 6).

***Теорема* 5.2.** *Пусть K — произвольное поле, характеристика которого не равна двум; тогда всякая антикоммутативная K-алгебра может быть вложена в $(-)$-алгебру подходящей линейной K-алгебры, и для всех таких вложений существует универсальная K-алгебра, универсальная линейная K-оболочка антикоммутативной алгебры B.* ∎

Этот результат справедлив для любого поля, но не для любого кольца (см. упражнения 3 и 4). Им можно воспользоваться, например, для доказательства того, что подалгебры свободных $(-)$-алгебр (над полем) снова свободны (Ширшов [54]), используя при этом соответствующий результат для линейных алгебр (Курош [47], Витт [53]), но мы не будем входить в детали доказательства.

Алгебры многообразия $(K)_{\mathrm{v}}$ являются просто коммутативными (но не обязательно ассоциативными) алгебрами. Каждой K-алгебре A сопоставим коммутативную алгебру A^{+}, ее $(+)$-алгебру, взяв K-модуль A с умножением

$$xy\} = xy) + yx). \tag{17}$$

Как и раньше, это определяет универсальный функтор, сопоставляющий каждой коммутативной алгебре C линейную K-алгебру $V(C)$ и гомоморфизм

$$v\colon\ C \to V(C)^{+}, \tag{18}$$

который универсален для гомоморфизмов алгебры C в алгебры вида A^{+}, где A — линейная K-алгебра. Если характеристика поля K отлична от двух, то тождественное отображение алгебры C в алгебру $C^{\natural}$, которая определяется так же, как в (16), снова дает точное представление, и, таким образом, мы получаем следующую теорему:

***Теорема* 5.3.** *Пусть K — произвольное поле, характеристика которого не равна двум; тогда всякая коммутативная K-алгебра может быть вложена в $(+)$-алгебру подходящей линейной K-алгебры, и для всех таких вложений существует универсальная K-алгебра.* ∎

УПРАЖНЕНИЯ

1. Показать, что всякое кольцо с 1 (ассоциативность не предполагается), удовлетворяющее тождеству $xy)\,y) = xy)$, будет булевой алгеброй.

2. Показать, что коммутативная алгебра с единицей 1 над основным полем из двух элементов с базисом $1, a, b, c$ и соотношениями $a^2) = a$, $b^2) = b$, $ab) = ac) = c^2) = c$, $bc) = 0$ неассоциативна и принадлежит многообразию $(K)_{\mathrm{III}}$.

3. Показать, что для основного поля характеристики два универсальные функторы U и V для представлений $(-)$- и $(+)$-алгебр также будут инъективными. (Использовать линейно упорядоченный базис для построения точного представления.)

4. Пусть F — поле характеристики два и K — ассоциативная и коммутативная F-алгебра, порожденная элементами α, β, γ с соотношениями $\alpha^2 = \beta^2 = \gamma^2 = 0$. Показать, что универсальный функтор U не будет инъективным в этом случае. (Взять (—)-алгебру с образующими a, b, c и соотношениями $a\alpha + b\beta = c\gamma$ и показать, что каждое представление отображает $ab]\,\alpha\beta$ в нуль.)

5. (Капланский.) Показать, что в линейной алгебре над полем характеристики нуль всякое тождество эквивалентно системе тождеств, линейных и однородных относительно каждого переменного.

6. Показать, что всякое многообразие линейных алгебр с 1 над полем характеристики нуль, определяемое тождествами степени не выше трех, определяется одним или несколькими из следующих тождеств, где $A(x, y, z) = xy)\,z) - xyz)\,)$, $xy] = xy) - yx)$:

(i) $xy) = yx)$,

(ii) $x^2)\,x) = xx^2)\,)$,

(iii) $xy]\,z] + yz]\,x] + zx]\,y] = 0$ (тождество Якоби),

(iv) $A(x, y, z) = 0$ (закон ассоциативности),

(v) $A(x, y, x) = 0$ (закон эластичности),

(vi) $A(x, y, y) = 0$ (закон правой альтернативности),

(vii) $xy]\,y] = 0$,

(viii) $xy]\,z] = xz]\,y]$,

(ix) $A(x, y, z) = A(z, y, x)$,

(x) $xy)\,z) - xz)\,y) - yz)\,x) + zy)\,x) = \lambda\,\{xyz)\,) - xzy)\,) - yzx)\,) + zyx)\,)\}$,

тождества, полученные из (vi) и (x) изменением порядка сомножителей (т. е. применением антиизоморфизма).

7. Показать, что в ассоциативной алгебре, удовлетворяющей тождеству $xy]z] = 0$, прозводная операция $\alpha xy) + \beta yx)$ определяет ассоциативное умножение для всех α, β.

8. *Пусть A есть* (+)*-алгебра* (с коэффициентами из кольца K); тогда K-модуль M с отображением ν: $A \times M \to M$, которое линейно по каждому аргументу, называется *A-модулем*. Показать, что если умножение в A обозначено через μ, то прямое произведение $E = A \times M$ с умножением

$$(a, x) \cdot (b, y) = (ab\mu, ay\nu + bx\nu)$$

будет (+)-алгеброй, содержащей A в *качестве* подалгебры и M в качестве идеала. (Алгебра E называется *расщепляемым нулевым расширением* M при помощи A.)

9. (Тамари [62].) Показать, что если неассоциативные произведения выделяются заключением второго сомножителя в скобки, то различные распределения из r пар скобок (,) определяют различные произведения из $r + 1$ сомножителей и что таким образом получаются все возможные произведения. Вывести формулу

$$b_r = \binom{2r}{r} - \binom{2r}{r-1}$$

для числа b_r способов распределения скобок в произведении из $r + 1$ сомножителей. (Если s_k^h означает число всех последовательностей из h членов (и k членов), то, заменяя в каждой последовательности последнюю не имеющую пары скобку) на (, показать, что $s_r^r - b_r = s_{r-1}^{r+1}$.)

6. ЛИЕВЫ АЛГЕБРЫ

Пусть K — некоторое ассоциативное и коммутативное кольцо с 1, а через $\mathrm{As}(K)$ обозначена категория ассоциативных K-алгебр. Поскольку $\mathrm{As}(K)$ является (полной) подкатегорией категории (K), она снова будет подчинена категории антикоммутативных алгебр, которую здесь мы будем обозначать через $(K)^{-}$ (вместо $(K)_{\mathrm{Iv}}$). Поэтому мы имеем естественное представление категории $(K)^{-}$ в категории $\mathrm{As}(K)$. Допустимыми отображениями будут те и только те K-линейные отображения μ, для которых

$$\mu(xy]) = \mu(x)\mu(y) - \mu(y)\mu(x). \tag{1}$$

Таким образом, допустимые отображения определяются тождествами, и отсюда вытекает (по следствию IV.4.2), что существует универсальный функтор, сопоставляющий каждой (—)-алгебре X единственную ассоциативную алгебру $U(X)$, *универсальную ассоциативную оболочку* (—)-алгебры X, с каноническим гомоморфизмом

$$u\colon X \to U(X). \tag{2}$$

Обычно этот гомоморфизм не является взаимно однозначным; действительно, легко проверить, что всякий элемент вида

$$xy]z] + yz]x] + zx]y] \tag{3}$$

отображается в нуль. Поэтому ограничимся рассмотрением (—)-алгебр, в которых это выражение тождественно равно нулю, и дадим такое определение:

Лиевой алгеброй называется (—)-алгебра, удовлетворяющая тождеству

$$xy]z] + yz]x] + zx]y] = 0 \quad \text{(тождество Якоби).} \tag{4}$$

Предыдущее замечание показывает, что алгебра X должна быть лиевой, чтобы гомоморфизм (2) был взаимно однозначным; всякая лиева алгебра с этим свойством называется *специальной*. Каждая лиева алгебра над полем как областью коэффициентов специальна. Это вытекает из теоремы Биркгофа — Витта, в которой, кроме того, базис универсальной ассоциативной оболочки лиевой алгебры L выражается через базис алгебры L. Ниже мы приведем доказательство этого результата, но сначала рассмотрим частный случай свободной лиевой алгебры. Мы докажем несколько больше, а именно выразим базис этой алгебры через множество свободных образующих. В частности, этим будет решена проблема тождества для свободных лиевых алгебр.

Пусть X — некоторое линейно упорядоченное множество; рассмотрим свободную полугруппу Φ_X над X. Элементы полугруппы Φ_X, называемые *словами* над X, являются конечными наборами элементов множества X и могут быть упорядочены лексикографически. Точнее, если $u = u_1 \cdots u_r$, $v = v_1 \cdots v_s$ (u_i, $v_j \in X$), то положим $u < v$, если только $u_i = v_i$ для $i = 1, \ldots, k-1$ и $u_k < v_k$. При таком определении Φ_X будет линейно упорядоченной; если, например, $x_1 < x_2 < x_3$, то $x_1x_3x_2^2x_1 < x_1x_3x_2$. Два слова u, v называются *циклически сопряженными*, если $u = ab$, $v = ba$. Слово u называется *правильным*, если для любого разложения $u = ab$ (a, $b \neq 1$) имеем $u > ba$; таким образом, слово правильно, если оно следует за всеми циклически сопряженными с ним. Отметим, что для правильного слова представление $u = a^k$, где $k > 1$, невозможно; далее, заметим, что

$$\text{если } u \text{ — правильное и } u < v, \text{ то } uv < vu. \tag{5}$$

Действительно, если $u < v$ и $uv \geqslant vu$, то $u = vz$ и поэтому $vzv \geqslant vvz$, т. е. $zv \geqslant vz$, что противоречит правильности u.

Воспользуемся теперь правильными словами для определения неассоциативных «базисных произведений», которые будут служить базисом нашей свободной лиевой алгебры. Пусть Γ_X — свободный группоид над X; его элементы представляют собой наборы элементов из X с некоторой расстановкой скобок. Будем обозначать такие произведения через $[u]$; если u имеет степень n, то в $[u]$ имеется $n-1$ пара скобок (или $n-2$ пары, если мы опускаем внешнюю пару скобок, как иногда будем делать).

Определение. Произведение $[u]$ называется *базисным* при условии, что либо $u \in X$, либо выполняются следующие условия:

(i) если $[u] = [v][w]$, то $[v]$, $[w]$ — базисные и $v > w$,

(ii) если $[u] = [[v_1][v_2]][w]$, то $v_2 \leqslant w$.

Этим базисные произведения определены индукцией по степени. Например, если $X = \{x, y\}$, где $x < y$, то базисные произведения включают

$$x,\ y,\ [yx],\ [[yx]x],\ \ldots,\ [[yx][yx]x]],\ \ldots.$$

Эти обозначения скоро становятся громоздкими, но положение исправляется следующей леммой:

Лемма **6.1.** *В каждом слове u над X можно расставить скобки единственным способом так, что оно примет вид*

$$u = [b_1][b_2] \cdots [b_r], \quad b_1 \leqslant b_2 \leqslant \ldots \leqslant b_r, \tag{6}$$

где каждое слово $[b_i]$ — базисное.

Кроме того, если в базисном произведении $[u]$ отбросить скобки, то полученное слово будет правильным, и, обратно, в каждом правильном слове u можно расставить скобки единственным способом так, что оно превратится в базисное произведение.

Доказательство. Воспользуемся индукцией по длине (=степени) слова u. Пусть x_1 — первый элемент множества X (в смысле данной упорядоченности), встречающийся в u. Если x_1 встречается в u на первом месте, то имеем

$$u = x_1 v,$$

где v имеет меньшую длину, и по предположению индукции $v = [b_2] \cdots [b_r]$, где $b_2 \leqslant \ldots \leqslant b_r$; отсюда

$$u = [x_1][b_2] \cdots [b_r]. \tag{7}$$

Теперь единственным базисным произведением, начинающимся с x_1, которое является сомножителем слова u, может быть только сам x_1 (в силу (ii) определения базисных произведений). Отсюда $r > 1$, за исключением того случая, когда $u = x_1$; кроме того, $x_1 \leqslant b_2$. Это показывает, что запись (7) нужного вида и единственна.

Далее, предположим, что x_1 встречается в u не на первом месте, так что

$$u = x_i \cdots x_1 \cdots x_1 \cdots \quad (x_i > x_1).$$

Во всяком разложении слова u на базисные произведения единственным базисным произведением, начинающимся с x_1, будет сам x_1, как мы только что видели. Но первое базисное произведение начинается с x_i и поэтому следует за x_1. Итак, не существует разложения вида (6) с x_1 в качестве сомножителя. Теперь возьмем некоторый x_1 в u, которому предшествует $x_j \neq x_1$. Так как x_1 не является начальной буквой базисного произведения (ни в каком разложении вида (6)), то он может быть только конечной буквой некоторой части (также базисной) некоторого базисного произведения: $[[w]\, x_1]$ например. Но если степень w больше единицы, скажем $w = w_1 w_2$, то $w_2 > x_1$, а это противоречит тому факту, что $[w]\, x_1$ — базисное слово. Итак, $w = x_j$ и в любом разложении слова u на базисные произведения базисное слово $x_j x_1$ должно появиться в качестве сомножителя. Заключая $x_j x_1$ в скобки и обозначая этот сомножитель одной буквой, получаем более короткое слово, и, используя предположение индукции, получаем разложение (6) слова u.

Если в (6) $r > 1$, то, используя (5), имеем $b_i \leqslant b_j$ для $i < j$ и, следовательно, $b_i b_j \leqslant b_j b_i$. Это показывает, что

$$b_1 b_2 \cdots b_r \leqslant b_2 b_1 b_3 \cdots b_r \leqslant b_2 b_3 \cdots b_r b_1;$$

отсюда, если $r > 1$, то u не может быть правильным. Итак, если u правильно, то существует один и только один способ расстановки скобок в u для получения базисного произведения $[u]$. Обратно, если $[u]$ — базисное произведение, то либо u имеет степень 1 и поэтому правильно, либо степень u больше 1 и x_1 — наименьшая буква, встречающаяся в u; тогда первый раз x_1 входит в $[u]$ в сочетании $[x_i x_1]$, где $x_i > x_1$.

Обозначая $[x_i x_1]$ новой буквой и используя индукцию по степени, видим, что любое слово, циклически сопряженное с u, должно предшествовать u, за исключением, быть может, одного, начинающегося с самого x_1. Но оно также предшествует u, так как u, очевидно, не может начинаться с x_1. Итак, u правильно, как и утверждалось. ∎

Теперь мы можем доказать теорему, в которой строится канонический базис для свободных лиевых алгебр. Доказательство (так же как и доказательство леммы 6.1) основано на доказательстве Ширшова [58] (см. также М. Холл [50] и Ф. Холл [58]).

***Теорема* 6.2.** *Пусть L — свободная лиева алгебра над линейно упорядоченным множеством X. Тогда базисные произведения над X образуют базис в L как в свободном K-модуле.*

Доказательство. Покажем сначала, что базисные произведения над X порождают L. Всякий элемент в L степени, большей единицы, является линейной комбинацией членов $[v][w]$, где по предположению индукции $[v]$ и $[w]$ можно считать базисными и в силу антикоммутативности можно предполагать, что $v > w$. Если $[v]$ имеет степень 1 или если $[v] = [v_1][v_2]$, где $v_2 \leqslant w$, то $[v][w]$ будет также базисным. В противном случае $v_2 > w$, и в силу тождества Якоби имеем

$$[v][w] = -[[v_2][w]][v_1] + [[v_1][w]][v_2]. \tag{8}$$

Теперь v_1, v_2 и w правильны и $v_1 > v_2 > w$, откуда $v_1 v_2 > v_2 v_1$ и $v_1 w > w v_1$; следовательно,

$$v_1 v_2 w > v_2 v_1 w > v_2 w v_1.$$

Кроме того, $v_2 w > w v_2$ и поэтому $v_1 v_2 w > v_1 w v_2$. Индукцией по порядку членов одинаковой степени члены в правой части равенства (8) можно выразить через базисные произведения, а потому $[v][w]$ также можно выразить через базисные произведения. Это показывает, что базисные произведения порождают L.

Для доказательства независимости базисных произведений возьмем свободную ассоциативную алгебру A над X и подалгебру $[X]$ алгебры A^-, порожденную множеством X. Тогда $[X]$ — лиева алгебра над X, и, поскольку L свободна над X, тождественное отображение множества X можно продолжить до гомоморфизма

$$L \to [X]. \tag{9}$$

Мы завершим доказательство теоремы, если покажем, что базисные произведения линейно независимы в $[X]$ над K. Этим будет показано попутно, что (9) — изоморфизм. Всякое базисное произведение имеет вид $[u]$, где u правильно. Мы утверждаем, что если $[u]$ выражено через ассоциативные слова в A, то

$$[u] = u + \text{слова, предшествующие } u \text{ в данной упорядоченности.} \tag{10}$$

Действительно, пусть $[u]=[v][w]$; тогда $[v]$ и $[w]$ (индукцией по степени) можно считать базисными, поскольку

$$[v]=v+v^*, \quad [w]=w+w^*,$$

где через v^* обозначены члены, предшествующие v, а через w^* обозначены члены, предшествующие w. Теперь

$$[u]=[v+v^*,\ w+w^*]=vw+v^*w+vw^*+v^*w^*-$$
$$-wv-wv^*-w^*v-w^*v^*.$$

Справа все члены первой строки предшествуют vw, а все члены второй строки предшествуют wv, который в силу правильности u сам предшествует vw. Этим доказано (10). Если теперь мы имеем соотношение

$$\sum \alpha_i u_i = 0 \quad (\alpha_i \in K) \tag{11}$$

между различными базисными произведениями, то пусть $[u_k]$ — последнее базисное произведение (в смысле данной упорядоченности), участвующее в (11) с ненулевым коэффициентом. Выражая (11) через ассоциативные слова, находим, что

$$\alpha_k u_k + \text{предшествующие слова} = 0,$$

что приводит к противоречию. Следовательно, базисные произведения независимы. ∎

***Теорема* 6.3. (*Биркгоф* [37], *Витт* [37].)** *Пусть L — лиева алгебра над полем K с базисом B. Если базис B линейно упорядочен некоторым образом, то универсальная ассоциативная оболочка $U(L)$ лиевой алгебры L обладает базисом, состоящим из возрастающих произведений*

$$b_1 b_2 \cdots b_r \quad (b_i \in B,\ b_1 \leqslant \ldots \leqslant b_r). \tag{12}$$

В частности, L специальна.

Доказательство. Предположим сначала, что L свободна над X; тогда имеем гомоморфизм

$$\varphi\colon\ L \to [X] \tag{13}$$

алгебры L в лиеву алгебру, порожденную в A^- множеством X, где A — свободная ассоциативная алгебра над X. Далее, всякое допустимое отображение α алгебры L в ассоциативную алгебру C (т. е. всякий гомоморфизм $\alpha\colon L \to C^-$) индуцирует отображение $\alpha_0\colon X \to C$. Это отображение может быть продолжено до гомоморфизма $\alpha'\colon A \to C$, поскольку A свободна. Теперь $\varphi\alpha'$ и α — два гомоморфизма алгебры L в C^-, которые совпадают на X и, следовательно, на L. Итак, $\varphi\alpha' = \alpha$

и отображение α', ограниченное на $[X]$, единственно, так как оно определяется своими значениями на X. Это показывает, что $[X]$ с каноническим отображением (13) является универсальной ассоциативной оболочкой алгебры L; покажем, что произведения

$$[b_1] \cdots [b_r] \quad ([b_i] \text{ — базисное, } b_1 \leqslant \ldots \leqslant b_r) \tag{14}$$

образуют базис алгебры A. При доказательстве теоремы 6.2 мы видели, что всякое базисное произведение $[b]$ имеет вид

$$[b] = b + \text{члены, предшествующие } b.$$

Отсюда, если u — некоторое слово над X, то по лемме 6.1

$$u = b_1 b_2 \cdots b_r \quad (b_1 \leqslant \ldots \leqslant b_r);$$

итак,

$$u = [b_1][b_2] \cdots [b_r] + \text{предшествующие члены.} \tag{15}$$

Теперь различные слова u образуют базис алгебры A, и в силу (15) эти базисные элементы могут быть выражены последовательно через произведения (14); поэтому последние снова образуют базис. Выбирая $r = 1$, видим, что отображение (13) взаимно однозначно, и потому алгебра L может быть отождествлена с подпространством алгебры A. Пусть L^r — подпространство алгебры A, порожденное всеми произведениями (14), состоящими не более чем из r сомножителей. Так как для любых двух базисных произведений b_i, b_j

$$b_i b_j = b_j b_i + \sum \gamma_{ijk} b_k \quad (\gamma_{ijk} \in K),$$

то отсюда вытекает, что во всяком произведении из r базисных произведений сомножители перестановочны $\left(\text{по } \operatorname{mod} L^{r-1}\right)$, так что L^r содержит все выражения степени r, составленные из базисных произведений в произвольном порядке. В частности, если B — произвольный базис алгебры L, некоторым образом упорядоченный, то возрастающие произведения степени r над B образуют базис подпространства L^r $\left(\text{по } \operatorname{mod} L^{r-1}\right)$.

Пусть теперь L — произвольная лиева алгебра; запишем $L = F/N$, где F — свободная лиева алгебра и N — идеал в F. Если B — некоторый базис алгебры F вида $B = B' \cup B''$, где B' — базис идеала N и B'' — базис дополнения идеала N в F, то в $U(F)$ базис образуют элементы

$$v'v'', \tag{16}$$

когда v', v'' пробегают возрастающие произведения над B', B'' соответственно. Так как N — идеал в F, то подпространство V алгебры $U(F)$, порожденное элементами (16), в которых $v' \neq 1$, образует идеал в $U(F)$. В самом деле, если $v'v''$ имеет степень r, скажем $v' = b_1 b_2 \cdots b_s$, $v'' = b_{s+1} \cdots b_r$ $(s \geqslant 1)$ и $b \in B$, то предположим, что $b_{i-1} \leqslant b \leqslant b_i$; тогда индукцией по r получаем

$$b_1 \cdots b_r b = b_1 \cdots b_{i-1} b b_i \cdots b_r \pmod{V \cap F^{r-1}}.$$

Здесь правая часть принадлежит V, откуда $b_1 \cdots b_r b \in V$ и аналогично $bb_1 \cdots b_r \in V$. Это показывает, что V замкнуто относительно умножения на любые элементы из B и, следовательно, на любые элементы из F, т. е. V — идеал. Факторалгебра $U(F)/V$ обладает базисом, состоящим из элементов v'', т. е. из всевозможных возрастающих произведений над B'', и так как $V \supseteq N$, то естественное отображение $F \to U(F)$ индуцирует такое отображение $L \to U(F)/V$, что диаграмма

$$\begin{tikzcd} F \arrow[r] \arrow[d] & U(F) \arrow[d] \\ L \arrow[r] & U(F)/V \end{tikzcd}$$

коммутативна. Итак, имеем гомоморфизм $U(L) \to U(F)/V$, и поскольку возрастающие произведения над B'' линейно независимы в $U(F)/V$, то они независимы также в $U(L)$; ясно, что они порождают $U(L)$ и, следовательно, образуют базис. ∎

Отметим, что можно также доказать эту теорему, не используя теоремы 6.2, непосредственными, хотя и несколько более длинными, выкладками (см., например, Картан и Эйленберг [56], гл. 13). Этот метод имеет то преимущество, что применим к любой лиевой алгебре, которая свободна как K-модуль, так что нет необходимости предполагать, что K — поле. Теорема Биркгофа — Витта была сформулирована для произвольных лиевых K-алгебр и была доказана для лиевых алгебр над кольцом главных идеалов без делителей нуля (Лазар [54]) и, в более общем случае, над произвольным дедекиндовым кольцом без делителей нуля (Картье [58]). Но она не может иметь места во всех случаях, поскольку существуют лиевы алгебры, не являющиеся специальными (Картье [58], Ширшов [53]). Во всех примерах неспециальных лиевых алгебр аддитивная группа алгебры L обладает кручением, и, действительно, было показано, что лиева алгебра без кручения обязательно специальна (Кон [63]).

В заключение вернемся к свободной лиевой алгебре F и вычислим размерность ψ_n пространства F_n, компоненты степени n алгебры F, в случае когда F — алгебра ранга q. Если дано некоторое слово u длины n, то либо все слова, циклически сопряженные с u, различны, и в этом случае u сопряжено в точности с одним правильным словом, либо u имеет вид v^k, где v имеет длину $d = n/k$ и сопряжено только с одним правильным словом. Поэтому если мы переберем все q^n слов длины n, то для каждого делителя d числа n получим все правильные слова длины d, каждое из которых повторено d раз. Итак,

$$q^n = \sum_{d \mid n} d\psi_d;$$

чтобы разрешить это равенство относительно ψ_n, запишем его для всех делителей данного n и разрешим последовательно относительно $n\psi_n$:

$$n\psi_n = q^n - \sum_{p_1 \mid n} q^{n/p_1} + \sum_{p_1 p_2 \mid n} q^{n/p_1 p_2} - \ldots, \tag{17}$$

где $p_1, p_2, \ldots$ пробегают все различные простые делители n. Чтобы записать это равенство короче, введем функцию Мёбиуса

$$\mu(r) = \begin{cases} (-1)^k, & \text{если } r = p_1 p_2 \cdots p_k \text{ (где } p_1, p_2, \ldots, p_k \text{ — различные простые)}, \\ 0 & \text{в противном случае.} \end{cases}$$

Тогда из (17) вытекает следующая

***Теорема* 6.4. (*Формула Витта.*)** *Пусть F — свободная лиева алгебра над $x_1, \ldots, x_q$ и F_n — компонента степени n алгебры F; тогда размерность пространства F_n определяется по формуле*

$$\psi_n = \frac{1}{n} \sum_{d \mid n} \mu(d) q^{n/d}. \blacksquare$$

УПРАЖНЕНИЯ

1. Пусть L — лиева алгебра, и через ρ_a обозначим правое умножение $x \to xa$]. Показать, что $a \to \rho_a$ будет допустимым отображением из L в $\mathscr{L}(L)$, кольцо K-линейных отображений на L.

2. Показать, что ненулевая лиева алгебра не может обладать единицей.

3. Показать, что если X — множество образующих лиевой алгебры L, то пространство L порождается левонормированными произведениями над X (произведение называется *левонормированным*, если всякий его сомножитель имеет степень 1 или является произведением, в котором правый сомножитель имеет степень 1).

4. Показать, что если X — множество образующих лиевой алгебры L и X линейно упорядочено, то L порождается базисными произведениями над X. (Заметим, что базисные произведения не являются в общем случае левонормированными.)

5. Показать, что в свободной лиевой алгебре над $\{x\} \cup Y$ левонормированные произведения, получаемые из элементов $xy_1 \cdots y_n$ $(y_i \in Y)$ с помощью соответствующей расстановки скобок, образуют базис для элементов степени $n+1$ относительно x.

6. Показать, что в свободной лиевой алгебре над $x_1, \ldots, x_q$ размерность пространства элементов степени n_i относительно x_i равна

$$\frac{1}{n}\sum_{d \mid n_i} \mu(d) \frac{\left(\frac{n}{d}\right)!}{\left(\frac{n_1}{d}\right)! \ldots \left(\frac{n_q}{d}\right)!},$$

где $n = \sum n_i$.

7. ЙОРДАНОВЫ АЛГЕБРЫ

Рассмотрим теперь естественное представление категории $(K)_v$ коммутативных алгебр в $\mathrm{As}(K)$. Для краткости произведение в $(+)$-алгебрах обозначим через $x \cdot y$, а в ассоциативных алгебрах—через xy (как и раньше). Кроме того, будем предполагать, что K содержит элемент $1/2$, удовлетворяющий равенству

$$\frac{1}{2}+\frac{1}{2}=1.$$

Это выполняется, например, если K — поле характеристики, не равной двум. Допустимыми отображениями будут K-линейные отображения μ, удовлетворяющие равенству

$$\mu(a \cdot a) = 2\mu(a)^2. \tag{1}$$

В силу линейности и коммутативности имеем

$$a \cdot b = \frac{1}{2}\{(a+b)\cdot(a+b) - a \cdot a - b \cdot b\}.$$

Подставляя в (1) и используя линейность отображения μ, получаем

$$\mu(a \cdot b) = \mu(a)\mu(b) + \mu(b)\mu(a). \tag{2}$$

Процесс, при котором из (1) было получено (2), называется *линеаризацией*; будем говорить также, что (2) получается *линеаризацией* (1).

Снова существует универсальный функтор, сопоставляющий каждой $(+)$-алгебре X ассоциативную алгебру, которую мы обозначим через $V'(X)$, и каноническое отображение

$$v'\colon X \to V'(X). \tag{3}$$

Чтобы определить, когда v' взаимно однозначно, найдем опять элементы в свободной $(+)$-алгебре, отображающиеся в нуль при v'. Оказывается, не существует таких элементов степени, меньшей четырех. Самым общим элементом[1]) четвертой степени, который отображается в нуль при v', будет

$$(x \cdot y) \cdot y^{\cdot 2} - (x \cdot y^{\cdot 2}) \cdot y. \tag{4}$$

Соответствующее тождество

$$(x \cdot y) \cdot y^{\cdot 2} - (x \cdot y^{\cdot 2}) \cdot y = 0 \tag{5}$$

называется *йордановым тождеством*, и всякая (+)-алгебра, удовлетворяющая тождеству (5), называется *йордановой алгеброй*. В силу сказанного выше, если v' взаимно однозначно, то алгебра X должна быть йордановой; такая йорданова алгебра называется *специальной*. K-линейное отображение, удовлетворяющее (1), будем называть *специальным представлением*.

Читатель может теперь ожидать развития теории йордановых алгебр, параллельной теории лиевых алгебр. Однако оказывается, что имеются существенные различия, которые приводят к совершенно иному развитию теории йордановых алгебр. Одно из этих различий, кажущееся незначительным, состоит в том, что степень йорданова тождества равна четырем, тогда как степень тождества Якоби равна трем (т. е. равна степени закона ассоциативности). Уже поэтому нет оснований ожидать, что йорданово тождество полностью заменит закон ассоциативности. Так, даже когда K — поле характеристики нуль, существуют йордановы алгебры, не являющиеся специальными. Среди этих «исключительных» йордановых алгебр лучше всего известна алгебра M_3^8 эрмитовых матриц порядка 3×3 над алгеброй Кэли — Диксона (Алберт [34], [50]). Класс специальных йордановых алгебр, очевидно, замкнут относительно подалгебр и прямых произведений, но не образует многообразия, как будет показано в предложении 7.9 на примере одной исключительной йордановой алгебры, являющейся гомоморфным образом специальной йордановой алгебры (Кон [54]). Итак, если $\mathcal{J}$ — многообразие всех йордановых алгебр и $\mathcal{J}'$ — класс специальных йордановых алгебр, то имеем

$$\mathcal{J}' \subseteq \mathrm{V}\mathcal{J}' \subseteq \mathcal{J}. \tag{6}$$

Здесь первое неравенство будет строгим в силу сказанного выше. Далее Алберт и Пейдж [59] показали, что исключительная йорданова алгебра M_3^8 не является гомоморфным образом никакой специальной йордановой алгебры и поэтому не принадлежит $\mathrm{V}\mathcal{J}'$. Это показывает, что второе неравенство в (6) должно быть строгим. На самом деле это означает, что существуют тождества, которые выполняются во всех специальных йордановых алгебрах, но не во всех йордановых

[1]) В том смысле, что вполне инвариантный идеал, порожденный словом (4), содержит всякий элемент четвертой степени, отображающийся в 0 при v'.

алгебрах. Доказательство Алберта и Пейджа не дало явных тождеств, хотя из доказательства явствует, что степень таких тождеств не может превосходить 45. В действительности некоторые тождества (степеней 8 и 9), выполняющиеся в специальных йордановых алгебрах, но не во всех йордановых алгебрах, в настоящее время найдены Гленни [63].

В любой йордановой алгебре J через R_a обозначим правое умножение

$$R_a\colon\ x \to x \cdot a. \tag{7}$$

Это называется также *регулярным представлением* алгебры J. В противоположность случаю лиевых алгебр это отображение алгебры J в $\mathscr{L}(J)$, кольцо K-линейных преобразований алгебры J, не будет, вообще говоря, допустимым. Однако оно удовлетворяет некоторым тождествам, которые вытекают из йорданова тождества. Во-первых, из (5) имеем

$$R_y R_{y\cdot 2} = R_{y\cdot 2} R_y; \tag{8}$$

во-вторых, мы можем линеаризовать (5) и выразить его как равенство операторов, применяемых к одному из переменных, заменяющих y. Так, обозначая левую часть равенства (5) через $f(y)$, рассмотрим выражение $f(u+v+w)-f(u+v)-f(v+w)-f(w+u)+f(u)+$ $+f(v)+f(w)$. Обращение этого выражения в нуль равносильно равенству

$$x \cdot u) \cdot v \cdot w))+x \cdot v) \cdot w \cdot u))+x \cdot w) \cdot u \cdot v))=$$
$$=u \cdot v) \cdot x) \cdot w)+v \cdot w) \cdot x) \cdot u)+w \cdot u) \cdot x) \cdot v).$$

Записывая его в виде равенства операторов, применяемых к w, получаем

$$R_v R_{x\cdot u}+R_u R_{x\cdot v}+R_x R_{u\cdot v}=R_{u\cdot v)\cdot x)}+R_v R_x R_u+R_u R_x R_v. \tag{9}$$

Всякое K-линейное отображение йордановой алгебры в ассоциативную алгебру, удовлетворяющее тождествам (8), (9), называется *йордановым представлением* или *общим представлением* алгебры J. Легко проверить, что специальное представление йордановой алгебры будет в то же время общим представлением (см. упражнение 2).

Рассмотрим специальную йорданову алгебру B, содержащуюся в ассоциативной алгебре A. Если обозначить правое и левое умножение на $a \in A$ через ρ_a и λ_a соответственно, а регулярное представление в B через R_a, то, так как $x \cdot y = xy + yx$, отсюда вытекает, что

$$R_a = \lambda_a + \rho_a. \tag{10}$$

Теперь ясно, что оба умножения λ_a и ρ_a, ограниченные на B, будут специальными предствлениями, и, кроме того, закон ассоциативности в A: $(ax)b=a(xb)$ может быть записан в виде

$$\lambda_a\rho_b=\rho_b\lambda_a. \tag{11}$$

Это выражает тот факт, что представления λ и ρ перестановочны, и этим показано, что регулярное представление $a\to R_a$ в B является суммой двух перестановочных специальных представлений. Вообще будем называть K-линейное отображение йордановой алгебры *полуспециальным представлением*, если это отображение может быть разложено в сумму двух перестановочных специальных представлений. Доказанный результат может быть сформулирован следующим образом:

***Предложение* 7.1.** *Регулярное представление специальной йордановой алгебры полуспециально.* ∎

Так как регулярное представление любой йордановой алгебры будет йордановым представлением, то в силу предложения 7.1 кажется правдоподобным, что всякое полуспециальное представление будет йордановым представлением, и в этом легко убедиться непосредственной проверкой, которая может быть предоставлена читателю. Кроме того, специальное представление может быть тривиальным образом выражено в виде суммы двух специальных представлений

$$\mu(a)=\mu(a)+0$$

и является поэтому полуспециальным. Итак, мы имеем три типа представлений йордановых алгебр в убывающем порядке общности:

(i) общие представления,
(ii) полуспециальные представления,
(iii) специальные представления.

Из них (i) и (iii) определяются тождествами и, следовательно, обладают универсальными функторами. Чтобы установить, что полуспециальные представления также обладают универсальным функтором, в силу теоремы III.4.2 осталось только показать, что эти представления резидуальны. Итак, пусть μ: $J\to A$ — отображение йордановой алгебры J в ассоциативную алгебру A, и предположим, что A — подпрямое произведение алгебр A_λ с такими проекциями ε_λ, что $\mu\varepsilon_\lambda$ полуспециальны, скажем

$$\mu\varepsilon_\lambda=\alpha_\lambda+\beta_\lambda,\quad \text{где}\quad \alpha_\lambda\beta_\lambda=\beta_\lambda\alpha_\lambda.$$

Запишем $P=\prod A_\lambda$, так что A можно отождествить с подалгеброй алгебры P. Отображение α: $J\to P$, определяемое равенством $\alpha(x)=(\alpha_\lambda(x))$ $(x\in J)$, будет специальным представлением, так же как и отображение β, определяемое равенством $\beta(x) = (\beta_\lambda(x))$. Ясно, что α и β перестановочны и для любого $x \in J$

$$\mu(x) = \alpha(x) + \beta(x),$$

откуда μ полуспециально. Этим показано, что полуспециальные представления резидуальны.

Обозначим универсальные функторы для общих, полуспециальных и специальных представлений йордановой алгебры J через $V(J)$, $V''(J)$ и $V'(J)$ соответственно, а соответствующие канонические отображения v, v'' и v' будем называть *универсальным общим, полуспециальным* и *специальным представлением* соответственно. Здесь (V', v') совпадает с функтором на $(+)$-алгебрах, введенным раньше. Поскольку данные представления расположены в убывающем порядке общности, то мы имеем естественные гомоморфизмы σ: $V(J) \to V''(J)$ и τ: $V''(J) \to V'(J)$, которые вместе с каноническими отображениями v, v'', v' образуют коммутативную диаграмму

$$\begin{tikzcd} J \arrow[r] \arrow[d, "v"'] & J \arrow[r] \arrow[d, "v''"'] & J \arrow[d, "v'"] \\ V(J) \arrow[r, "\sigma"'] & V''(J) \arrow[r, "\tau"'] & V'(J) \end{tikzcd}$$

Так как каждая алгебра $V(J)$, $V''(J)$, $V'(J)$ порождается образом алгебры J, то оба отображения σ, τ являются эпиморфизмами. Будут ли они мономорфизмами, зависит от того, будут ли канонические отображения взаимно однозначными, и поэтому мы начнем с рассмотрения этого вопроса.

Универсальное специальное представление v' взаимно однозначно тогда и только тогда, когда J специальна, по определению специальной йордановой алгебры. Отсюда непосредственно вытекает, что для специальных йордановых алгебр v'' также взаимно однозначно; обратно, если v'' взаимно однозначно, то J обладает точным полуспециальным представлением и, следовательно, точным специальным представлением в прямом произведении двух ассоциативных алгебр, если заменить представление $a \to \mu(a) = \alpha(a) + \beta(a)$, где α, β специальны, представлением $a \to (\alpha(a), \beta(a))$. Итак, J снова специальна. Возвращаясь теперь к v, покажем, что для любой йордановой алгебры J оно всегда взаимно однозначно по построению, т. е. является точным общим представлением. Пусть $J^1 = J \times (u)$ — прямое произведение алгебры J и свободного K-модуля, порожденного элементом u; определим умножение в J^1 равенством

$$(a, \alpha u) \cdot (b, \beta u) = (a \cdot b + \alpha b + \beta a, \alpha\beta u) \quad (a, b \in J; \ \alpha, \beta \in K).$$

Итак, J^1 является в точности алгеброй, полученной присоединением единичного элемента u к J. Легко проверить, что J^1 снова будет йордановой алгеброй; следовательно, ее регулярное представление будет йордановым представлением. Теперь $a \to R_a$ является взаимно однозначным отображением J в $\mathcal{L}(J^1)$, так как $R_a = R_b$ влечет $a = u \cdot a = u \cdot b = b$; итак, R_a — точное йорданово представление алгебры J. Суммируя сказанное, получаем

***Предложение* 7.2.** *Универсальное йорданово представление v всегда взаимно однозначно, тогда как универсальное полуспециальное представление v'' и универсальное специальное представление v' взаимно однозначны тогда и только тогда, когда йорданова алгебра специальна.* ∎

***Следствие* 7.3.** *Отображение σ: $V(J) \to V''(J)$ не является взаимно однозначным, за исключением, быть может, того случая, когда алгебра J специальна.*

Действительно, если σ взаимно однозначно, то $v\sigma = \sigma''$ взаимно однозначно, а это может случиться только если J специальна. ∎

Отметим, что σ не обязано быть взаимно однозначным, даже когда J специальна, в чем можно убедиться, если рассмотреть йорданову алгебру эрмитовых матриц порядка 3×3 над кватернионами (см. Джекобсон [54]); позже будет указан другой пример.

В противоположность σ отображение τ не является взаимно однозначным никогда, кроме тривиальных случаев. Итак, пусть J — йорданова алгебра над полем K, и предположим, что τ — взаимно однозначно. Пусть $W = V' \otimes V'$ — тензорное произведение (над K) алгебры $V' = V'(J)$ на себя; рассмотрим представление J в W:

$$a \to v'(a) \otimes 1 + 1 \otimes v'(a). \tag{12}$$

Это представление полуспециально (поскольку является суммой двух перестановочных специальных представлений), и так как τ взаимно однозначно, то (12) должно быть специальным. Итак,

$$v'(a^{\cdot 2}) \otimes 1 + 1 \otimes v'(a^{\cdot 2}) = 2(v'(a) \otimes 1 + 1 \otimes v'(a))^2, \tag{13}$$

и так как v' само специально, то $v'(a^{\cdot 2}) = 2v'(a)^2$. Подставляя это в (13) и вычисляя правую часть, после некоторых упрощений получаем $4v'(a) \otimes v'(a) = 0$, т. е.

$$v'(a) \otimes v'(a) = 0.$$

Это возможно, только если $v'(a) = 0$ для всех $a \in J$, т. е. $V'(J) = 0$. Отметим, что J может все же быть ненулевой алгеброй, даже если $V'(J) = 0$. Например, исключительная йорданова алгебра M_3^8, упомянутая ранее, проста; так как ядро универсального специального представления v' является, очевидно, идеалом в M_3^8, то, будучи ненулевым, этот идеал должен совпадать со всей алгеброй. Итак, $\operatorname{im} v' = 0$, и так как $\operatorname{im} v'$ порождает $V'(J)$, то $V'(M_3^8) = 0$.

Так же как для ассоциативных и лиевых алгебр, мы имеем соответствие между представлениями и модулями. Итак, если J — произвольная йорданова алгебра, то под йордановым модулем для J понимают K-модуль M вместе с йордановым представлением $J \to \mathscr{L}(M)$. Если задан йорданов модуль M для J с представлением $a \to \mu(a)$, то можно образовать *расщепляемое нулевое расширение* $E = J \times M$ с умножением

$$(a, x) \cdot (b, y) = (a \cdot b, y\mu(a) + x\mu(b)) \quad (a, b \in J; x, y \in M)$$

(см. упражнение 5.8) и нетрудно проверить при помощи (8) и (9), что E будет опять йордановой алгеброй. В терминах E существует простой критерий того, чтобы представление алгебры J было полуспециальным (Джекобсон [54]):

Предложение 7.4. *Пусть J — специальная йорданова алгебра и M есть J-модуль; тогда представление, определяемое M, полуспециально тогда и только тогда, когда расщепляемое нулевое расширение $J \times M$ является специальной йордановой алгеброй.*

Доказательство. Пусть $a \to \mu(a)$ — представление, определяемое M; если оно полуспециально, то пусть $\mu(a) = \alpha(a) + \beta(a)$, где α, β — перестановочные специальные представления алгебры J линейными преобразованиями модуля N, содержащего M. Так как J специальна, то можно считать, что она вложена в $V'(J)$ (т. е. является подалгеброй алгебры $(V'(J))^+$). Возьмем теперь произведение $V'(J) \times N$ с умножением

$$(a, x)(b, y) = (ab, x\alpha(b) + y\beta(a)) \quad (a, b \in J; x, y \in N).$$

Так как $V'(J)$ универсальна для специальных представлений, то это определяет структуру ассоциативной алгебры на $A = V'(J) \times N$, и легко видеть, что $E = J \times M$ является подалгеброй в A^+. Обратно, если E вложена в $(+)$-алгебру некоторой ассоциативной алгебры A, то для любых $x \in M$, $a \in J$ имеем

$$x \cdot a = xa + ax \text{ в } A,$$

откуда $\mu(a) = \rho_a + \lambda_a$, и это показывает, что μ полуспециально. ∎

До сих пор предполагалось, что все ассоциативные алгебры обладают единицей 1. Однако йорданова алгебра сама может обладать единицей, которую мы обозначаем через u во избежание недоразумений. Это приводит к дальнейшей классификации представлений по их действию на u. Пусть μ — произвольное йорданово представление; запишем $\mu_1 = \mu(u)$; тогда в силу (9)

$$\mu_1 + 2\mu_1^3 - 3\mu_1^2 = 0,$$

т. е.

$$\mu_1(\mu_1 - 1)(2\mu_1 - 1) = 0.$$

Итак, для любого йорданова представления (над полем) матрица, представляющая u, обладает собственными значениями 0, 1/2 и 1. В частности, если 1 — единичный элемент алгебры $V(J)$, то имеем разложение единицы

$$1 = 1_0 + 1_{1/2} + 1_1$$

на попарно ортогональные идемпотенты и соответствующее разложение алгебры $V(J)$

$$V(J) = V_0(J) \otimes V_{1/2}(J) \otimes V_1(J), \tag{14}$$

где $V_i(J)$ — универсальная ассоциативная оболочка для таких представлений $a \to \mu(a)$, что

$$\mu(u) = i1 \qquad \left(i = 0,\ \frac{1}{2},\ 1\right). \tag{15}$$

Представление μ называется *унитальным, специальным унитальным* или *нулевым представлением* соответственно тому, выполняется ли (15) для $i = 1$, 1/2 или 0. Ясно, что нулевое представление алгебры J тождественно равно нулю на J:

$$\mu(a) = \mu(a \cdot u) = \mu(a)\mu(u) + \mu(u)\mu(a) = 0.$$

Если μ — специальное унитальное, то в силу (9)

$$\mu(a^{\cdot 2}) = \mu(a^{\cdot 2} \cdot u) = 2\mu(a)\mu(a \cdot u) + \mu(u)\mu(a^{\cdot 2}) - 2\mu(a)\mu(u)\mu(a) =$$
$$= 2\mu(a)^2 + \frac{1}{2}u(a^{\cdot 2}) - \mu(a)^2,$$

откуда $\mu(a^{\cdot 2}) = 2\mu(a)^2$, т. е. μ на самом деле специально. Рассмотрим теперь $V'(J)$ и $V''(J)$; они обладают разложениями, совершенно аналогичными разложению (14). Так как каждое нулевое представление и каждое специальное унитальное представление специально и тем более полуспециально, то мы получаем канонические изоморфизмы

$$V'_0(J) \cong V''_0(J) \cong V_0(J),$$

$$V'_{1/2}(J) \cong V''_{1/2}(J) \cong V_{1/2}(J).$$

В частности, отсюда вытекает, что каноническое отображение

$$\sigma\colon\ V(J)\to V''(J)$$

будет изоморфизмом тогда и только тогда, когда индуцированное им отображение

$$\sigma_1\colon\ V_1(J)\to V_0''(J)$$

является изоморфизмом (Джекобсон [54]). Этот результат можно сформулировать следующим образом:

***Предложение* 7.5.** *Универсальное общее представление йордановой алгебры J с единицей полуспециально тогда и только тогда, когда универсальное унитальное представление алгебры J полуспециально.* ∎

Структурная теория йордановых алгебр дальше всего продвинута в случае конечномерных йордановых алгебр над полем (Алберт [47]). Мы не будем углубляться в эту теорию (главным образом потому, что универсальная алгебра почти не имеет к ней отношения), но вместо этого применим теорию § IV.4 для построения неспециальных йордановых алгебр и неполуспециальных представлений. Впредь будем считать, что все йордановы алгебры являются алгебрами над полем K характеристики, не равной двум.

Пусть A — свободная ассоциативная алгебра над X; через $(X)^+$ обозначим подалгебру алгебры A^+, порожденную множеством X; элементы алгебры $(X)^+$ называются также *йордановыми элементами* над X. Наша первая задача состоит в нахождении критерия того, чтобы элемент алгебры A был йордановым элементом. Такой критерий известен только в случае, когда X имеет не больше трех элементов, и получается следующим образом. Определим на A линейное отображение $a\to a^*$, *обращающий оператор*, посредством равенства

$$(x_1x_2\cdots x_n)^*=x_n\cdots x_2x_1\qquad(x_i\in X)\tag{16}$$

при условии линейности. Этим отображение полностью определено, так как одночлены $x_1x_2\cdots x_n$ образуют базис для A. Заметим, что

$$(ab)^*=b^*a^*,\quad a^{**}=a\qquad(a,\ b\in A).$$

Элемент $a\in A$, удовлетворяющий равенству $a^*=a$, называется *неподвижным*. Для любого $a\in A$ запишем

$$\{a\}=\frac{1}{2}(a+a^*);$$

из этого определения ясно, что $\{a\}$ неподвижен для всех элементов $a\in A$. Множество всех неподвижных элементов алгебры A обозначим через H; оно будет подалгеброй в A^+, содержащей $(X)^+$, но не обязательно совпадающей с ней. Чтобы проверить это, предположим, что X имеет по крайней мере четыре различных элемента x_1, x_2, x_3, x_4, и рассмотрим

$$\{x_1x_2x_3x_4\}. \tag{17}$$

Ясно, что этот элемент лежит в H, но не принадлежит $(X)^+$; действительно, если мы применим к (17) все 24 перестановки π из переменных $x_1, \ldots, x_4$, умножим на знак перестановки π и просуммируем, то из (17) получим

$$\sum (\operatorname{sign} \pi)\, x_{1\pi}x_{2\pi}x_{3\pi}x_{4\pi},$$

так как (1, 2, 3, 4) отличается от (4, 3, 2, 1) на четную перестановку. С другой стороны, та же самая операция, примененная к йорданову элементу, линейному по каждому из x_1, x_2, x_3, x_4, дает нуль, так как всякий такой элемент является суммой членов, содержащих сомножитель $\{x_iy_j\}$. Однако мы получим всю алгебру H, как только включим элементы вида (17) в множество образующих (Кон [54]).

Теорема 7.6. *$(+)$-алгебра H неподвижных элементов алгебры A порождается множеством X и всеми элементами* (17), *где $x_i \in X$.*

Доказательство. Пусть H' — подалгебра алгебры A^+, порожденная множеством X и элементами (17); тогда ясно, что $H' \subseteq H$; для доказательства равенства нужно только показать, что $p_n = \{x_1 \cdots x_n\} \in H'$ для любых $x_i \in X$. Для $n = 0, 1, 2$ это очевидно, поэтому можно применить индукцию по n. Итак, для $n \geqslant 3$ по предположению индукции

$$\{x_1x_2 \cdots x_n\} + \{x_2 \cdots x_nx_1\} = x_1 \cdot \{x_2 \cdots x_n\} \equiv 0 \pmod{H'}. \tag{18}$$

Таким образом, по $\operatorname{mod} H'$ произведение p_n меняет знак при перестановке $(1, \ldots, n)$; в частности, если n нечетно, то этим доказано, что $p_n \in H'$. Для четных n, больших двух, имеем

$$\{x_1x_2\} \cdot \{x_3 \cdots x_n\} \equiv 0 \pmod{H'},$$

откуда

$$\{x_1x_2x_3 \cdots x_n\} + \{x_3x_4 \cdots x_nx_1x_2\} + \{x_2x_1x_3 \cdots x_n\} + \\ + \{x_3 \cdots x_nx_2x_1\} \equiv 0 \pmod{H'},$$

или, используя (18),

$$\{x_1x_2 \cdots x_n\} \equiv -\{x_2x_1x_3 \cdots x_n\} \pmod{H'}. \tag{19}$$

Так как перестановки $(12 \cdots n)$ и (12) порождают симметрическую группу, то путем повторного применения (18) и (19) получаем, что p_n кососимметричен $(\operatorname{mod} H')$. Отсюда $p_n \in H'$, если не все $x_1, \ldots, x_n$ различны. Для $n = 4$ этим способом все произведения приводятся к виду (17) с различными аргументами, так что можно предполагать, что $n \geqslant 6$ и n четно. Тогда

$$\{x_1x_2x_3x_4\} \cdot \{x_5 \cdots x_n\} \equiv 0 \pmod{H'},$$

т. е.

$$\{x_1x_2x_3x_4x_5 \cdots x_n\} + \{x_4x_3x_2x_1x_5 \cdots x_n\} \equiv 0 \pmod{H'}$$

и отсюда $p_n \in H'$; этим показано, что $H' = H$. ∎

Если X имеет меньше четырех элементов, то элементов вида (17) не существует, и мы получаем

Следствие 7.7. *В свободной ассоциативной алгебре с тремя свободными образующими x, y, z множество H неподвижных элементов является в точности йордановой подалгеброй, порожденной элементами x, y, z.* ∎

Другими словами, выражение от x, y, z является йордановым элементом тогда и только тогда, когда оно неподвижно. В качестве следствия получаем следующий результат:

Теорема 7.8. *Любой гомоморфный образ специальной йордановой алгебры с двумя образующими является специальной алгеброй.*

Доказательство. Пусть A — свободная ассоциативная алгебра над x и y; через J обозначим подалгебру алгебры A^+, порожденную элементами x и y; таким образом, J — свободная специальная йорданова алгебра над x и y. Нам нужно показать, что любой гомоморфный образ алгебры J будет специальной алгеброй, а в силу теоремы IV.4.5 для этого достаточно показать, что для любого идеала N алгебры J

$$ANA \cap J = N. \tag{20}$$

Любой элемент из $ANA \cap J$ является суммой членов $aub + b^*ua^*$, где $a, b \in A$ и $u \in N$. Рассмотрим теперь элемент $azb + b^*za^*$ в свободной ассоциативной алгебре над x, y, z. Ясно, что этот элемент неподвижен, и в силу следствия 7.7 его можно представить как йорданов элемент от x, y, z:

$$azb + b^*za^* = f(x, y, z).$$

Отсюда

$$aub + b^*ua^* = f(x, y, u) \in N.$$

Так как во всяком случае $N \subseteq ANA \cap J$, то этим доказано (20), и отсюда вытекает утверждение теоремы. ∎

Эта теорема вместе с результатом Ширшова [56] о том, что свободная йорданова алгебра с двумя свободными образующими специальна, показывает, что на самом деле каждая йорданова алгебра с двумя образующими специальна. В связи с этим интересно отметить, что исключительная йорданова алгебра M_3^8 может быть порождена тремя элементами. Мы не будем доказывать ни того, что эта алгебра является исключительной, ни даже того, что эта алгебра йорданова, но вместо этого построим гомоморфный образ одной специальной йордановой алгебры, который является исключительной алгеброй. Пусть A — свободная ассоциативная алгебра над x, y, z и J — йорданова алгебра, порожденная x, y, z. Рассмотрим идеал P в J, порожденный элементом $u = x \cdot y \left(= \frac{1}{2}(xy + yx)\right)$; если бы J/P была специальной, то мы имели бы $APA \cap J = P$, откуда

$$\{uxyz\} \in P.$$

Это означает, что существует йорданов элемент $f(u, x, y, z)$ от четырех свободных переменных, который превращается в $\{uxyz\}$, если мы положим $u = x \cdot y$. Следовательно, f должен быть линейной комбинацией неподвижных элементов, которые однородны и линейны по каждому из u, x, y, z. Выбирая только члены, кончающиеся на z, видим, что эти требования выполняются только для $v_1 = \{uxyz\}$, $v_2 = \{uyxz\}$, $v_3 = \{xyuz\}$, $v_4 = \{yxuz\}$, $v_5 = \{xuyz\}$, $v_6 = \{yuxz\}$. Если мы подставим $u = x \cdot y$, то только v_5 содержит член x^2y^2z и только v_6 содержит член y^2x^2z, так что ни v_5, ни v_6 не могут встречаться в f. Теперь xy^2xz встречается только в v_2 и v_3, так что они должны входить с противоположными коэффициентами, скажем α и $-\alpha$ соответственно. Аналогично $yxyxz$ встречается только в v_2 и v_4, так что v_4 имеет коэффициент $-\alpha$. Но вхождения $xyxyz$ и yx^2yz должны совпадать, а это может случиться, только если $\alpha = 0$; остается лишь v_1, но мы видели, что $v_1 = \{uxyz\}$ не является йордановым элементом от u, x, y, z. Этим доказано

***Предложение* 7.9.** *Гомоморфный образ свободной специальной йордановой алгебры над x, y, z, полученный присоединением соотношения $x \cdot y = 0$, является исключительной алгеброй. В частности, класс $\mathscr{J}'$ специальных йордановых алгебр не является многообразием.* ∎

Тем же способом можно показать, что йорданова алгебра, порожденная элементами x, y, z, с соотношениями $x \cdot y = 0$ и $Z^{\cdot 2} = 0$, где Z — идеал, порожденный элементом z, является исключительной. Но эта алгебра в точности совпадает с расщепляемым нулевым расширением алгебры

$$\mathscr{J}\{x, y \mid x \cdot y = 0\} \tag{21}$$

при универсальном общем представлении. Следовательно, в силу предложения 7.4 это представление не будет полуспециальным; итак, в (21) мы имеем специальную йорданову алгебру, для которой каноническое отображение σ: $V(J) \to V''(J)$ не является изоморфизмом. Этот результат особенно интересен ввиду теоремы Макдональда (Макдональд [60] или также Джекобсон [62]), которая утверждает, что любое тождество от x, y, z, линейное по z, выполняющееся во всех специальных йордановых алгебрах, выполняется во всех йордановых алгебрах. Эквивалентная формулировка этой теоремы утверждает, что универсальное общее представление свободной йордановой алгебры F_2 с двумя свободными образующими полуспециально (в частности, отсюда вытекает теорема Ширшова, упомянутая ранее). Отсюда можно вывести, используя ту же технику, что и при доказательстве теоремы 7.8, что *все* представления алгебры F_2 полуспециальны в противоположность представлениям алгебры (21).

УПРАЖНЕНИЯ

1. Показать, что каждая йорданова алгебра удовлетворяет тождеству

$$(a^{\cdot 2} \cdot b) \cdot c - (a^{\cdot 2} \cdot c) \cdot b = 2a \cdot b) \cdot c) \cdot a - 2a \cdot c) \cdot b) \cdot a.$$

Эквивалентно ли это тождество (в (+)-алгебрах) йорданову тождеству?

2. Проверить, что каждое полуспециальное представление является йордановым представлением.

3. Проверить, что расщепляемое нулевое расширение A-модуля M, где A есть (+)-алгебра (см. упражнение 5.8), является йордановой алгеброй тогда и только тогда, когда A — йорданова алгебра и M определяет йорданово представление.

4. Проверить, что если N — ядро общего представления йордановой алгебры J, то $A(k, a, b) \equiv A(a, k, b) \equiv A(a, b, k) \equiv 0 \pmod N$ для всех $a, b \in J$, $k \in N$, где $A(a, b, c) = (a \cdot b) \cdot c - a \cdot (b \cdot c)$. Показать, что если это представление специально, то, кроме того, N является идеалом в J.

5. Показать, что йорданова алгебра с одним образующим ассоциативна.

6. Показать, что если J — йорданова алгебра с одним образующим, то $V'(J)$ коммутативна; привести пример ассоциативной йордановой алгебры, универсальная ассоциативная оболочка которой для специальных представлений не коммутативна.

7. Показать, что если A — ассоциативная алгебра с 1 над полем характеристики, не равной двум, то элемент $a \in A$ обладает обратным b в A тогда и только тогда, когда в A^+ выполняются равенства $a \cdot b = 1$, $a^{\cdot 2} \cdot b = a$.

БИБЛИОГРАФИЯ

Алберт (Albert A. A.)

[34] On a certain algebra of quantum mechanics, *Ann. of Math.*, **35** (1934), 65—73.

[47] A structure theory for Jordan algebras, *Ann. of Math.*, **48** (1947), 546—567.

[50] A note on the exceptional Jordan algebra, *Proc. Nat. Acad. Sci. USA*, **36** (1950), 372—374.

Алберт, Пейдж (Albert A. A., Paige L. J.)

[59] On a homomorphism property of certain Jordan algebras, *Trans. Amer. Math. Soc.*, **93** (1959), 20—29.

Артин, Несбит, Тролл (Artin E., Nesbitt C. J., Thrall R. M.)

[44] Rings with minimum condition, Ann. Arbor, 1944.

Бейтс (Bates G. E.)

[47] Free nets and loops and their generalizations, *Amer. J. Math.*, **69** (1947), 499—550.

Бинг (Bing K.)

[55] On arithmetical classes not closed under direct union, *Proc. Amer. Math. Soc.*, **6** (1955), 836—846.

Биркгоф (Birkhoff G.)

[33] On the combination of subalgebras, *Proc. Cambridge Phil. Soc.*, **29** (1933), 441—464.

[35] On the structure of abstract algebras, *Proc. Cambridge Phil. Soc.*, **31** (1935), 433—454.

[37] Representability of Lie algebras and Lie groups by matrices, *Ann. of Math.*, **38** (1937), 526—532.

[44] Subdirect unions in universal algebras, *Bull. Amer. Math. Soc.*, **50** (1944), 764—768.

[46] Universal algebra, Proc. Canad. Math. Cong., Montreal, 1946, 310—326

[48] Lattice theory, rev. ed., New York, 1948. (Русский перевод: Биркгоф Г., Теория структур, ИЛ, М., 1951.)

Биркгоф, Уитмен (Birkhoff G., Whitman P. M.)

[49] Representation of Jordan and Lie algebras, *Trans. Amer. Math. Soc.*, **65** (1949), 116—136.

Биркгоф, Фринк (Birkhoff G., Frink O.)

[48] Representation of lattices by sets, *Trans. Amer. Math. Soc.*, **64** (1948), 299—316.

Бриттон (Britton J. L.)

[58] The word problem for groups, *London Math. Soc.*, **8**, (3), (1958), 493—506.

Бун (Boone W. W.)
[57] Certain simple unsolvable problems of group theory, *Indag. Math.*, **19** (=*Proc. Kon. Ned. Akad.* (A), **60**) (1957), 22—27, 227—232.

Бурбаки (Bourbaki N.)
[51] Topologie générale, Paris, 1951, chs. III—IV. (Русский перевод: Бурбаки Н., Общая топология. Основные структуры, Физматгиз, М., 1958.)
[54] Théorie des ensembles, Paris, 1954, chs. I—II. (Русский перевод: Бурбаки Н., Теория множеств, изд-во «Мир», М., 1965.)

Ван дер Варден (v. d. Waerden B. L.)
[37] Moderne Algebra, I, Leipzig, 1937. (Русский перевод: Ван дер Варден Б. Л., Современная алгебра, ОГИЗ, М. — Л., 1947.)

Ван Хао, Макнотон (Wang H., McNaughton R.)
[53] Les systèmes axiomatiques de la théorie des ensembles (Paris, 1953. (Русский перевод. Ван Хао, Мак-Нottoн, Аксиоматические системы теории множеств, ИЛ, М., 1963.)

Витт (Witt E.)
[37] Treue Darstellung Liescher Ringe, *J. reine angew. Math.*, **177** (1937), 152—160.
[53] Über freie Ringe und ihre Unterringe, *Math. Zeits.*, **58** (1953), 113—114.

Вопенка (Vopenka P.)
[62] A method of constructing a non-standard model of the Bernays-Gödel axiomatic theory of sets, *ДАН СССР*, **143** (1962), 11—12.

Вот (Vaught R. L.)
[54] Applications of the Löwenheim-Skolem-Tarski theorem to problems of completeness and decidability, *Indag. Math.*, **16** (1954), 467—472.
[54'] Remarks on universal classes of relational systems, *Indag. Math.*, **16** (1954), 589—591.
[54''] On sentences holding in direct products of relational systems, Proc. Int. Cong. Math., vol. 2, Amsterdam (1954), 409—410.
[63] Models of complete theories, *Bull. Amer. Math. Soc.*, **69** (1963), 299—313.

Габриэль (Gabriel P.)
[62] Des catégories abéliennes, *Bull. Soc. Math. France*, **90** (1962), 323—448.

Геллер (Galler B. A.)
[57] Cylindric and polyadic algebras, *Proc. Amer. Math. Soc.*, **8** (1957), 176—183.

Гёдель (Gödel K.)
[40] The consistency of the axiom of choice and of the generalized continuum hypothesis with the axioms of set theory, Princeton, 1940.
[47] What is Cantor's continuum problem? *Amer. Math. Monthly*, **44** (1947), 515—525.

Гленни (Glennie C. M.)
[63] Identities in Jordan algebras, Ph. D. thesis, Yale University, 1963.

Голди (Goldie A. W.)
[52] The scope of the Jordan-Hölder theorem in abstract algebra, *Proc. London Math. Soc.* (3), **2** (1952), 349—368.

Грин (Green J. A.)
[52] A duality in abstract algebra, *J. London Math. Soc.*, **27** (1952), 64—73.

Даймонд, Маккинси (Diamond A. H., McKinsey J. C. C.)
[47] Algebras and their subalgebras, *Bull. Amer. Math. Soc.*, **53** (1947), 959—962.

Двингер (Dwinger Ph.)
[61] Introduction to Boolean algebras, Würzburg, 1961.

Двингер, Якуб (Dwinger Ph., Yaqub F. M.)
[63] Generalized free products of Boolean algebras with an amalgamated subalgebra, *Indag. Math.*, **25** (1963), 225—231.

Девис (Davis Anne C.)
[55] A characterization of complete lattices, *Pacific J. Math*, **5** (1955), 311—319.

Дедекинд (Dedekind R.)
[00] Über die von drei Moduln erzeugte Dualgruppe, *Math. Ann.*, **53** (1900), 371—403. (Ges. Werke, II, 236—271.)

Джекобсон (Jacobson N.)
[54] Structure of alternative and Jordan bimodules, *Osaka Math. J.*, **6** (1954), 1—71.
[56] Structure of rings, Providence, 1956. (Русский перевод: Джекобсон Н., Строение колец, ИЛ, М., 1961.)
[62] MacDonald's theorem on Jordan algebras, *Arch. Math.*, **13** (1962), 241—250.

Дик (Dyck W.)
[1882] Gruppentheoretische Studien, *Math. Ann.*, **20** (1882), 1—44.

Дилуорс, Глисон (Dilworth R. P., Gleason A. M.)
[62] A generalized Cantor theorem, *Proc. Amer. Math. Soc.*, **13** (1962), 704—705.

Дюбрей (Dubreil P.)
[43] Sur les problèmes d'immersion et la théorie des modules, *C. R. Acad. Sci. Paris*, **216** (1943), 625—627.

Ершов Ю. Л.
[62] Об аксиоматизируемых классах моделей с бесконечной сигнатурой, *Алгебра и логика*, Семинар, **1**, № 4 (1962), 32—44.

Зарисский, Самюэль (Zariski O., Samuel P.)
[58] Commutative algebra, I, Princeton, 1958. (Русский перевод: Зарисский О., Самюэль П., Коммутативная алгебра, I, ИЛ, М., 1963.)

Зоннер (Sonner J.)
[62] The formal definition of categories, *Math. Zeits.*, **80** (1962), 163—176.

Ивенс (Evans T.)
[51] On multiplicative systems defined by generators and relations, I. Normal form theorems, *Proc. Cambridge Phil. Soc.*, **47** (1951), 637—649.
[53] Embeddability and the word problem, *J. London Math. Soc.*, **28** (1953), 76—80.

Йонсон (Jónsson B.)
[57] On direct decompositions of torsionfree abelian groups, *Math. Scand.*, **5** (1957), 230—235.
[62] Algebraic extensions of relational systems, *Math. Scand.*, **11** (1962), 197—205.

Йонсон, Тарский (Jónsson B., Tarski A.)
[47] Direct decompositions of finite algebraic systems, Notre Dame, 1947.
[61] On two properties of free algebras, *Math. Scand.*, **9** (1961), 95—101.

Калицкий, Скотт (Kalicki J., Scott D. S.)
[55] Equational completeness in abstract algebras, *Indag. Math.*, **17** (1955), 650—659.

Кармайкл (Carmichael R.)
[37] Introduction to the theory of groups of finite order, Boston, 1937.

Картан, Эйленберг (Cartan H., Eilenberg S.)
[56] Homological algebra, Princeton, 1956. (Русский перевод: Картан А., Эйленберг С., Гомологическая алгебра, ИЛ, М., 1960.)

Картье (Cartier P.)
[58] Remarques sur le théorème de Birkhoff-Witt, *Ann. scuola norm sup. Pisa, Sci. fis. mat.*, III, Ser. **12**, (1958), 1—4.

Кейслер (Keisler H. J.)
[61] Ultraproducts and elementary classes, *Indag. Math.*, **23** (1961), 477—495.
[61'] On some results of Jónsson and Tarski concerning free algebras, *Math. Scand.*, **9** (1961), 102—106.
[65] Reduced products and Horn classes, *Trans. Amer. Math. Soc.*, **117**, № 5 (1965), 307—328.

Келли (Kelley J. L.)
[55] General topology, New York, 1955. (Русский перевод: Келли Дж. Л., Общая топология, «Наука», М., 1968.)

Кертес (Kertész A.)
[60] On independent sets of elements in an algebra, *Acta Sci. Math. Szeged*, **21** (1960), 260—269.

Клини (Kleene S. C.)
[52] Introduction to metamathematics, Amsterdam, 1952. (Русский перевод: Клини С., Введение в метаматематику, ИЛ, М., 1957.)

Когаловский С. Р.
[59] Об универсальных классах алгебр, замкнутых относительно прямых произведений, *Изв. высш. учебн. заведений*, математика, (1959), 88—96.

Кон (Cohn P. M.)
[52] A theorem on the structure of tensor spaces, *Ann. of Math.*, **56** (1952), 254—268.
[54] On homomorphic images of special Jordan algebras, *Canad. J. Math.*, **6** (1954), 253—264.
[56] Embeddings in semigroups with one-sided division, *J. London Math. Soc.*, **31** (1956), 169—181.
[59] On the free product of associative rings, *Math. Zeits.*, **71** (1959), 380—398.
[61] On the embedding of rings in skew fields, *Proc. London Math. Soc.*, (3), **11** (1961), 511—530.
[63] A remark on the Birkhoff-Witt theorem, *J. London Math. Soc.*, **38** (1963), 197—203.
[64] Subalgebras of free associative algebras, *Proc. London Math. Soc.*, (3), **14** (1964), 618—632.

Кочен (Kochen S. B.)
[61] Ultraproducts in the theory of models, *Ann. of Math.*, **74** (1961), 221—261.

Коэн (Cohen P. J.)
[63] The independence of the continuum hypothesis, *Proc. Nat. Acad Sci. USA*, **50** (1963), 1143—1148; **51** (1964), 105—110. (Русский перевод: сб. *Математика*, **9** : 4 (1965).)

Краскэл (Kruskal J. B.)
[60] Well-quasi-ordering, the tree theorem and Vazsonyi's conjecture, *Trans. Amer. Math. Soc.*, **95** (1960), 210—225.

Курош А. Г.
[35] Durchschnittsdarstellungen mit irreduziblen Komponenten in Ringen und sogenannten Dualgruppen, *Матем. сб.*, **42** (1935), 613—616
[47] Неассоциативные свободные алгебры и свободные произведения алгебр, *Матем. сб.*, нов. сер., **20** (62) (1947), 239—262.
[53] Теория групп, ГИТТЛ, М., 1953.
[62] Лекции по общей алгебре, Физматгиз, М., 1962.

Лазар (Lazard M.)
[54] Sur les algèbres enveloppantes universelles de certaines algèbres de Lie, *Publ. Sci. Univ. Alger*, Ser. A, **1** (1954), 281—294.

Ленг (Lang S.)
[58] Introduction to algebraic geometry, New York, 1958.

Линдон (Lyndon R. C.)
[54] Identities in finite algebras, *Proc Amer. Math. Soc.*, **5** (1954), 8—9.
[59] Properties preserved under algebraic constructions, *Bull. Amer. Math. Soc.*, **65** (1959), 287—299.
[59′] Properties preserved under homomorphism, *Pacific J. Math.*, **9** (1959), 143—154.
[59″] Properties preserved in subdirect products, *Pacific J. Math.*, **9** (1959), 155—164.

Лоренцен (Lorenzen P.)
[53] Eine Bemerkung über die Abzählbarkeitsvoraussetzung in der Algebra, *Math. Zeits.*, **57** (1953), 241—243.

Лось (Łoś J.)
[55] On the extending of models, I, *Fund. Math.*, **42** (1955), 38—54.
[55′] Quelques rémarques, théorèmes et problèmes sur les classes définissables d'algèbres, Math. Interpretation of Formal Systems, Amsterdam, 1955, 98—113.

Макдональд (MacDonald I. G.)
[60] Jordan algebras with three generators, *Proc. London Math. Soc.* *(3)*, ***10*** *(1960), 395—408.*

Маккинси (McKinsey J. C. C.)
[43] The decision problem for some classes of sentences without quantifiers, *J. symb. Logic*, **8** (1943), 61—76.

Маклейн (MacLane S.)
[63] Homology, Berlin, 1963. (Русский перевод: Маклейн С., Гомология, изд-во «Мир», М., 1966.)

Мальцев А. И.
[37] On the immersion of an algebraic ring into a field, *Math. Ann.*, **113** (1937), 686—691.

[39] О вложении ассоциативных систем в группы, I, *Матем. сб.*, нов. серия, **6** (48), (1939), 331—336.
[40] О вложении ассоциативных систем в группы, II, *Матем. сб.*, нов. серия, **8** (50), (1940), 251—264.
[48] О вложении групповых алгебр с делением, *ДАН СССР*, **60** (1948), 1499—1501.
[50] Об алгебрах с тождественными определяющими соотношениями, *Матем. сб.*, **26** (68) (1950), 19—33.
[52] О представлении ассоциативных колец, *УМН*, **7** (1952), 181—185.
[54] К общей теории алгебраических систем, *Матем. сб.*, новая серия, **35** (77) (1954), 3—20.
[56] Подпрямые произведения моделей, *ДАН СССР*, **109** (1956), 264—266.
[58] Определяющие соотношения в категориях, *ДАН СССР*, **119** (1958), 1095—1098.
[58′] Структурная характеристика некоторых классов алгебр, *ДАН СССР*, **120** (1958), 29—32.
[58″] О некоторых классах моделей, *ДАН СССР*, **120** (1958), 245—248.
[62] Аксиоматизируемые классы локально свободных алгебр некоторых типов, *Сибирск. матем. ж.*, **3** (1962), 729—743.

Марчевский (Marczewski E.)
[51] Sur les congruences et les propriétés positives d'algèbres abstraites, *Colloq. Math.*, **2** (1951), 220—228.

Мостовский (Mostowski E.)
[55] The present state of investigations on the foundations of mathematics, *Rozprawy Mat.*, **9** (1955).
[57] A generalization of quantifiers, *Fund. Math.*, **44** (1957), 12—36.

Муфанг (Moufang R.)
[57] Einige Untersuchungen über geordnete Schiefkörper, *J. reine angew. Math.*, **176** (1937), 203—223.

Нейман Б. (Neumann B. H.)
[37] Identical relations in groups, I, *Math. Ann.*, **114** (1937), 506—526.
[37′] Some remarks on infinite groups, *J. London Math. Soc.*, **12** (1937), 120—127.
[49] On ordered division rings, *Trans. Amer. Math. Soc.*, **66** (1949), 202—252.
[49′] On ordered groups, *Amer. J. Math.*, **71** (1949), 1—18.
[51] Embedding non-associative rings in division rings, *Proc. London Math. Soc.* (3), **1** (1951), 241—256.
[54] An essay on free products of groups with amalgamations, *Phil. Trans. Roy. Soc.*, Ser. A, **246** (1954), 503—554.

Нейман Б., Нейман Х., Нейман П. (Neumann B. H., Neumann H., Neumann P. M.)
[62] Wreath products and varieties of groups, *Math. Zeits.*, **80** (1962), 44—62.

Нейман Х. (Neumann H.)
[56] On varieties of groups and their associated nearrings, *Math. Zeits.*, **65** (1956), 36—69.

Нётер (Noether E.)
[21] Idealtheorie in Ringbereichen, *Math. Ann.*, **83** (1921), 24—66.

Новиков П. С.
[55] Алгоритмическая неразрешимость проблемы слов в теории групп, Труды Мат. Инст. им. Стеклова, АН СССР 44 (1955).

Нэш-Вильямс (Nash-Williams C. St. J. A.)
[63] On well-quasi-ordering finite trees, *Proc. Cambridge Phil. Soc.*, **59** (1963), 833—835.

Ньюмен (Newman M. H. A.)
[42] On theories with a combinatorial definition of "equivalence" *Ann. of Math.*, **43** (1942), 223—243.

Оре (Ore O.)
[31] Linear equations in non-commutative fields, *Ann. of Math.*, **32** (1931), 463—477.
[35] On the foundation of abstract algebra, I, *Ann. of Math.*, **36** (1935), 406—437.
[36] On the foundation of abstract algebra, II, *Ann. of Math.*, **37** (1936), 265—292.
[42] Theory of equivalence relations, *Duke Math. J.*, **9** (1942), 573—627.
[44] Galois connexions, *Trans. Amer. Math. Soc.*, **55** (1944), 493—513.

Расёва (Rasiowa H.)
[52] A proof of the compactness theorem for arithmetical classes, *Fund. Math.*, **39** (1952), 8—14.
[55] Algebraic models of axiomatic theories, *Fund. Math.*, **41** (1955), 291—310.

Расёва, Сикорский (Rasiowa H., Sikorski R.)
[50] A proof of the completeness theorem of Gödel, *Fund. Math.*, **37** (1950), 193—200.
[51] A proof of the Skolem-Löwenheim theorem, *Fund. Math.*, **38** (1951), 230—232.

Рассел (Russell B.)
[19] Introduction to mathematical philosophy, London, 1919.

Робинсон (Robinson A.)
[63] Introduction to model theory and to the metamathematics of algebra, Amsterdam, 1963.

Розенблюм (Rozenbloom P. C.)
[50] The elements of mathematical logic, New York, 1950.

Самюэль (Samuel P.)
[48] On universal mappings and free topological groups, *Bull. Amer. Math. Soc.*, **54** (1948), 591—598.

Серпинский (Sierpiński W.)
[58] Cardinal and ordinal numbers, Warsaw, 1958.

Сикорский (Sikorski R.)
[53] Products of abstract algebras, *Fund Math.*, **39** (1953), 211—228.
[60] Boolean algebras, Berlin, 1960. (Готовится перевод второго издания: Сикорский П., Булевы алгебры, изд-во «Мир», М.).

Скорняков Л. А.,
[57] T-гомоморфизмы колец, *Матем. сб.*, 42 (84) (1957), 425—440.

Скотт Д. (Scott D.)
[56] Equationally complete extensions of finite algebras, *Indag. Math.*, **18** (1956), 35—38.

Скотт В. (Scott W. R.)
[51] Algebraically closed groups, *Proc. Amer. Math. Soc.*, **2** (1951), 118—121.

С л о м и н с к и й (S ł o m i ń s k i J.)
[59] The theory of abstract algebras with infinitary operations, *Rozprawy Mat.*, **18** (1959).

С у д з у к и (S u z u k i M.)
[56] Structure of a group and the structure of its lattice of subgroups, Berlin, 1956. (Русский перевод: С у д з у к и М., Строение групп и строение структуры ее подгрупп, ИЛ, М., 1960.)

Т а й м а н о в А. Д.
[53] Класс моделей, замкнутый относительно прямых объединений, *ДАН СССР*, **127** (1959), 1173—1175.
[62] Характеризация аксиоматизируемых классов моделей, *Алгебра и логика*, Семинар, **1**, № 4 (1962), 5—31.

Т а м а р и (T a m a r i D.)
[62] The algebra of bracketings and their enumeration, *Nieuw. Arch. v. Wiskunde* (3), **10** (1962), 131—146.

Т а р с к и й (T a r s k i A.)
[36] Der Wahrheitsbegriff in den formalisierten Sprachen, *Studia Philos.*, **1** (1936), 261—405.
[46] A remark on functionally free algebras, *Ann. of Math.*, **47** (1946), 163—165.
[50] Some notions and methods on the borderline of algebra and metamathematics, Proc. Int. Cong. Math., vol. I, Cambridge, Mass., 1950, 705—720.
[54] Contributions to the theory of models, *Indag. Math.*, **16** (1954), 572—588; **17** (1955), 56—64.
[55] A lattice-theoretic fixpoint theorem and its applications, *Pacific J. Math.*, **5** (1955), 285—309.
[56] Equationally complete rings and relation algebras, *Indag. Math.*, **18** (1956), 39—46.
[58] Remarks on predicate logic with infinitely long expressions, *Colloq. Math.*, **6** (1958), 171—176.

Т а р с к и й, В о т (T a r s k i A., V a u g h t R. L.)
[57] Arithmetical extensions of relational systems, *Comp. Math.*, **13** (1957), 81—102.

У а й т х е д (W h i t e h e a d A. N.)
[1898] A treatise on universal algebra, with application, I, Cambridge, 1898; reprinted New York, 1960.

Ф о с т е р (F o s t e r A. L.)
[55] The identities of — and unique subdirect factorization within — classes of universal algebras, *Math. Zeits.*, **62** (1955), 171—188.
[59] An existence theorem for functionally complete universal algebras, *Math. Zeits.*, **71** (1959), 69—82.

Ф р е й н, М о р е л, С к о т т (F r a y n e T., M o r e l A., S c o t t D.)
[62] Reduced direct products. *Fund. Math.*, **51** (1962), 195—228.

Х а л м о ш (H a l m o s P. R.)
[61] Naive set theory, Princeton, 1961.
[62] Algebraic logic, New York, 1962. (Сборник статей автора о монадических и полиадических алгебрах за 1954—1959 гг.)

Х а у с д о р ф (H a u s d o r f f F.)
[14] Mengenlehre, Berlin, 1914. (Русский перевод: Х а у с д о р ф Ф., Теория множеств, М., Гостехиздат, 1937.)

Хенкин (Henkin L.)
[49] The completeness of the first order functional calculus, *J. symb. Logic*, **14** (1949), 159—166.
[50] Completeness in the theory of types, *J. symb. Logic*, **15** (1950), 81—91.
[53] Some interconnections between modern algebra and mathematical logic, *Trans. Amer. Math. Soc.*, **74** (1953), 410—427.
[60] On mathematical induction, *Amer. Math. Monthly*, **67** (1960), 323—338.

Хенкин, Тарский (Henkin L., Tarski A.)
[61] Cylindric algebras, Proc. Symp. on Pure Math., II; Lattice theory (1961), 83—113.

Хиггинс (Higgins P. J.)
[56] Groups with multiple operators, *Proc. London Math. Soc.*, (3) **6** (1956), 366—416.
[63] Algebras with a scheme of operators, *Math. Nachr.*, **27** (1963), 115—132.

Хигмэн (Higman G.)
[52] Ordering by divisibility in abstract algebras, *Proc. London Math. Soc.* (3), **2** (1952), 326—336.
[59] Some remarks on varieties of groups, *Quarterly J. Math.*, (2) **10** (1959), 165—178.
[61] Subgroups of finitely presented groups, *Proc. Roy. Soc.*, **A 262** (1961), 455—475.

Хигмэн, Нейман Б. (Higman G., Neumann B. H.)
[52] Groups as groupoids with one law, *Publ. Math. Debrecen*, **2** (1952), 215—221.

Холл М. (Hall M., jr.)
[50] A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.*, **1** (1950), 575—581.
[59] The theory of groups, New York, 1959. (Русский перевод: Холл М., Теория групп, ИЛ, М., 1962.)

Холл Ф. (Hall P.)
[58] Some word problems, *J. London Math. Soc.*, **33** (1958), 482—496.

Хорн (Horn A.)
[51] On sentences which are true of direct unions of algebras, *J. symb. Logic*, **16** (1951), 14—21.

Чёрч (Church A.)
[56] Introduction to mathematical logic, vol. I, Princeton, 1956. (Русский перевод: Чёрч А., Введение в математическую логику, т. I, ИЛ, М., 1960.)

Чжан (Chang C. C.)
[59] On unions of chains of models, *Proc. Amer. Math. Soc.*, **10** (1959), 120—127.

Чжан, Морел (Chang C. C., Morel A. C.)
[58] On closure under direct product, *J. symb. Logic*, **23** (1958), 149—154.

Ширшов А. И.
[53] О представлении лиевых колец в ассоциативных кольцах, *УМН*, **5** (1953), 173—175.
[54] Подалгебры свободных коммутативных и свободных антикоммутативных алгебр, *Матем. сб.*, новая серия, **34** (76), (1954), 81—88.
[56] Специальные *J*-кольца, *Матем.* сб., новая серия, **38** (80), (1956).

[58] Свободные лиевы кольца, *Матем. сб.*, новая серия, **45** (87), (1958), 113—122.

Шмидт (Schmidt J.)

[52] Über die Rolle der transfiniten Schlussweisen in einer allgemeinen Idealtheorie, *Math. Nachr.*, **7** (1952), 165—182.

[55] Eine verallgemeinerte Wohlordnung und die Endlichkeitsbedingungen der Wohlordnungstheorie, *Arch. Math.*, **6** (1955), 374—381.

Шода (Shoda K.)

[49] Allgemeine Algebra, *Osaka Math. J.*, **1** (1949), 182—225.

Шпехт (Specht W.)

[50] Gesetze in Ringen, I, *Math. Zeits.*, **52** (1950), 557—589.

Эйленберг, Маклейн (Eilenberg S., MacLane S.)

[45] General theory of natural equivalences, *Trans. Amer. Math. Soc.*, **58** (1945), 231—294.

Эренфойхт (Ehrenfeucht A.)

[61] An application of games to the completeness problem for formalized theories, *Fund. Math.*, **49** (1961), 129—141.

УКАЗАТЕЛЬ ОБОЗНАЧЕНИЙ

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

ОГЛАВЛЕНИЕ