

С.И. Гуров

УПОРЯДОЧЕННЫЕ МНОЖЕСТВА И
АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

МОСКВА

УДК 512 (075.8) ??

ББК 22.144

Г 95

Рецензенты:

д.ф.-м.н, профессор *В.К. Леонтьев*

д.ф.-м.н, профессор *С.С. Марченков*

Гуров С.И.

УПОРЯДОЧЕННЫЕ МНОЖЕСТВА И АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

Главными инструментами математической кибернетики являются дискретная математика и алгебра. Основные понятия и свойства математических структур этих наук — частично упорядоченные множества, решётки, булевы алгебры, алгебраические системы — являются рабочим инструментом учёных в различных областях прикладной математики (распознавание образов и прогнозирование, оптимальное управление, автоматизация научных исследований, теоретическое и прикладное программирование и т.д.). Цель книги — восполнить практическое отсутствие, либо труднодоступность научной литературы по данной тематике.

Книга предназначена для научных работников, аспирантов, и инженеров, применяющих рассматриваемые алгебраические методы в своих исследованиях. Может также быть использована в качестве учебного пособия для студентов университетов и высших технических учебных заведений, а также при самообразовании.

Оглавление

Предисловие	4
1 Булевы алгебры	6
1.1 Определение булевой алгебры. Алгебраические системы	6
1.2 Алгебры множеств	10
1.3 Изоморфизмы булевых алгебр	15
1.4 Теорема Стоуна	19
2 Отношения и соответствия	22
2.1 Декартово произведение множеств и отношения	22
2.2 Однородные отношения	26
2.3 Отношение эквивалентности	31
2.4 Пространства толерантности	37
2.5 Основные свойства и типы соответствий	45
2.6 Отображения и их основные свойства	46
3 Частично упорядоченные множества	53
3.1 Предпорядки и порядки	53
3.2 Особые элементы и основные свойства ч.у. множеств	60
3.3 Грани, изотонные отображения и порядковые идеалы	65
3.4 Операции над ч.у. множествами	69
3.5 Линеаризация и размерность	76
3.6 Вполне упорядоченные множества и смежные вопросы	84
4 Решётки	91
4.1 Решёточно упорядоченные множества и решётки	91
4.2 Основные свойства решёток. Решёточные гомоморфизмы, идеалы и фильтры	97
4.3 Модулярные решётки	105
4.4 Дистрибутивные решётки	108
4.5 Факторрешётки. Решётки с дополнениями	119
5 Булевы алгебры (продолжение)	125
5.1 Булевы алгебры как решётки. Булевы гомоморфизмы и подалгебры	125
5.2 Булевы кольца и структуры	127
5.3 Идеалы, фильтры и конгруэнции в булевой алгебре	130
5.4 Булевы многочлены	137
5.5 Уравнения в булевых алгебрах	140
6 Алгебраические системы	143
6.1 Основные определения. Модели и алгебры	143
6.2 Подсистемы. Прямое произведение АС	146
6.3 Гомоморфизмы АС	148
6.4 Конгруэнции и факторсистемы	151
6.5 Теоремы о гомоморфизмах и изоморфизмах АС	154
6.6 Многоосновные системы	157
Приложение	159
Список литературы	162

Предисловие

Мы, конечно, не предполагаем бесполезно мучить людей, но, вместе с тем, мы не можем стремиться к тому, чтобы убрать все тернии с пути, ведущего к науке, добродетели и славе; это нам не удастся ни при каких условиях.

Дени Дидро. План университета или школы публичного преподавания всех наук.

Главными инструментами математической кибернетики являются, очевидно, дискретная математика и алгебра. Основные понятия и свойства математических структур этих наук — частично упорядоченные множества, решётки, булевы алгебры, алгебраические системы — являются рабочим инструментом учёных в различных областях прикладной математики (распознавание образов и прогнозирование, оптимальное управление, автоматизация научных исследований, теоретическое и прикладное программирование и т.д.).

В зарубежных издательствах выпускается большое число книг, учебников и монографий по данной тематике, с систематическим изложением основных сведений из указанных разделов и ориентированных на исследователей-практиков, работающих с указанными структурами алгебры и дискретной математики. Кроме того, данная тематика затрагивается во многих журналах, сборниках статей и трудов конференций с изложением результатов последних исследований. Имеются и специализированные периодические издания по теории упорядоченных множеств и решёток, универсальным алгебрам и смежным вопросам (журналы *Order*, *Discrete Mathematics*, *Discrete Applied Mathematics*, *Algebra Universalis* и др., а также многочисленные издания по комбинаторике, вплоть до *Electronic Journal of Combinatorics*). На русском языке аналогичных публикаций крайне мало. Автор ставил своей целью восполнить, в некоторой степени, указанный пробел, описав понятия и структуры, активно используемые исследователями в различных областях прикладной математики.

В данной монографии вводимые понятия и утверждения, как доказываемые, так и не доказываемые, иллюстрируются большим количеством примеров. Как правило, отсутствие доказательств некоторых (весьма немногочисленных) утверждений связано с нежеланием чрезмерно увеличивать объём монографии или уводить читателя в сторону от основных идей, при этом всегда даётся ссылка на источник, где такое доказательство может быть найдено. В списке литературы указаны работы как непосредственно использованные при написании текста, так и могущие быть полезными при более углублённой проработке материала.

Книга предназначена для научных работников, аспирантов, и инженеров, применяющих рассматриваемые алгебраические методы в своих исследованиях. При этом автор пытался подготовить её так, чтобы она могла быть использована и при самообразовании. Желательно лишь знакомство с основными понятиями алгебры и дискретной математики в объёме младших курсов университетов.

Приведём, хотя они и традиционны, основные обозначения, используемые книге. Символы \mathbb{N} , \mathbb{Z} , \mathbb{Q} , \mathbb{R} обозначают множества натуральных, целых, рациональных и действительных чисел соответственно; $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ — пополненный натуральный ряд. НОК и НОД — это наименьшее общее кратное и наибольший общий делитель соответственно. Множество целых, кратных n обозначается $n\mathbb{Z}$. Как обычно, \mathbb{Z}_n обозначает циклическую n -элементную группу (по сложению).

Булевы константы (истинностные значения) «истина» и «ложь» обозначаются соответственно $\mathbf{1}$ и $\mathbf{0}$, а n -мерный единичный куб — B^n или $\mathbf{2}^n$. Символ \triangleq означает «равно»

по определению», \supset — логическую операцию импликации, \equiv_n — «равно по $\text{mod } n$ » и если \circ_n — инфиксный символ бинарной операции на \mathbb{Z} или \mathbb{N} , то $x \circ_n y$ означает, что результат берётся по $\text{mod } n$ (например, $2 +_3 1 = 0$). Символ \mapsto обозначает подстановку элементов, символ \leftrightarrow — их перестановку, а \leftarrow — оператор присваивания.

Стрелки \Rightarrow и \Leftrightarrow служат сокращениями для выражений русского языка «влечёт», «если ..., то ...» и «эквивалентно», «... если и только если ...» соответственно. Кванторы существования и всеобщности переменной x по множеству X обозначаются $\exists x$ и $\forall x$ соответственно; впрочем, указание на X опускается, когда это не ведёт к двусмысленности. Совместное выполнение условий обозначается, как обычно, левой фигурной, а выполнение хотя бы одного условия — левой квадратной скобками.

Автор выражает особую признательность академику РАН Ю.И. Журавлёву, прочитавшему первоначальный вариант данного труда и поддерживавшему автора на протяжении всей работы. Выражаю также искреннюю благодарность рецензентам профессорам В.К. Леонтьеву и С.С. Марченкову, внимательно прочитавшим рукопись, указавшим на ряд неточностей и сделавшим много ценных замечаний. О.М. Васильев и Н.О. Пташко тщательно проработали текст и выявили значительное количество пропущенных при предыдущих чтениях описок и несоответствий, за что я им глубоко благодарен. Ответственность за возможные оставшиеся погрешности несёт, безусловно, автор.

«Писание математических текстов — сложное искусство, и даже лучшие из математиков не всегда оказываются на высоте, а уж большинство математических публикаций (будь то научные статьи, или учебники, даже для средней или начальной школы) вообще не выдерживают никакой критики» [В.И. Арнольд. Что такое математика?]. Насколько данная книжка оказалась удачной — судить читателю.

С. Гуров

Глава 1

Булевы алгебры

Булевы алгебры представляют собой удобную формализацию фрагмента теории множеств, служащей основой большинства современных разделов математики, что и определяет широкое их применение во многих математических конструкциях.

С.С. Гончаров. Счётные булевы алгебры.

1.1 Определение булевой алгебры. Алгебраические системы

Определение 1.1. Булевой алгеброй \mathfrak{B} называется множество B , содержащее по крайней мере два элемента — o (нуль) и ι (единица), с заданными на нём бинарными операциями¹ \sqcup (объединения), \sqcap (пересечения) и унарной операцией $'$ (дополнения). При этом для любых x, y и z из B выполняются следующие законы (аксиомы) булевой алгебры:

$$Com \sqcup: x \sqcup y = y \sqcup x;$$

$$Com \sqcap: x \sqcap y = y \sqcap x;$$

$$Dtr1: (x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z);$$

$$Dtr2: (x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z);$$

$$\sqcup o: x \sqcup o = x;$$

$$\sqcap \iota: x \sqcap \iota = x;$$

$$Cmp': x \sqcup x' = \iota;$$

$$Isl': x \sqcap x' = o;$$

$$Inv': (x')' = x;$$

$$\iota': \iota' = o;$$

$$o': o' = \iota;$$

$$DeM1: (x \sqcup y)' = x' \sqcap y';$$

$$DeM2: (x \sqcap y)' = x' \sqcup y';$$

$$\sqcup \iota: x \sqcup \iota = \iota;$$

$$\sqcap o: x \sqcap o = o;$$

$$Ass \sqcup: x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z;$$

$$Ass \sqcap: x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z;$$

$$Id \sqcup: x \sqcup x = x;$$

$$Id \sqcap: x \sqcap x = x;$$

$$Abs1: x \sqcap (x \sqcup y) = x;$$

$$Abs2: x \sqcup (x \sqcap y) = x.$$

Множество B называется носителем булевой алгебры \mathfrak{B} , а o и ι — выделенными элементами или универсальными гранями.

В булевой алгебре для объединения и пересечения выполняются пары законов коммутативности (Com), первый и второй дистрибутивные законы ($Dtr1, 2$), законы ассоциативности (Ass), идемпотентности² (Id) и поглощения (Abs). Понятно, что в булевой алгебре определены объединения и пересечения любой конечной совокупности элементов. При этом законы ассоциативности обеспечивают эквивалентность произвольных скобочных структур конечных объединений и пересечений. Далее при выводе соотношений мы,

¹Напомним, что задание бинарной операции на некотором множестве означает указание правила, ставящего в соответствие каждой упорядоченной паре элементов множества третьего его элемента. Аналогично задание унарной операции означает указание правила, по которому каждому элементу множества ставится в соответствие некоторый (как правило, отличный от заданного) элемент.

²От лат. *idem* — тот же самый, *potentia* — сила.

как правило, не будем специально отмечать применение законов ассоциативности и коммутативности.

Законы $\sqcup o$, $\sqcap \iota$, $\sqcup \iota$ и $\sqcap o$ описывают нейтральные и поглощающие свойства особых элементов булевой алгебры по отношению к объединению и пересечению. Свойства ι' , o' указывают на взаимную дополнительность этих элементов. Законы $Стр'$ и Isl' являются основными законами, описывающие свойства дополнения; они постулируют, соответственно, его полноту и обособленность. Закон Inv' указывает на инволютивность дополнения. Взаимные свойства бинарных операций и дополнения описываются законами Де Моргана (*DeM1*, 2).

Введённые операции называют *абстрактными*, поскольку ни они сами, ни носитель, на котором они определены никак не конкретизируются и никаких иных требований, кроме удовлетворения вышеприведённым законам, к ним не предъявляется. В приложениях элементы булевой алгебры интерпретируются как подмножества некоторых множеств, как события, высказывания, сигналы и др.

Лемма 1.1. *Для любых элементов x и y булевой алгебры справедливы следующие соотношения:*

$$1) \quad x \sqcup y = 0 \Leftrightarrow x = y = 0 \quad \text{и} \quad x \sqcap y = 1 \Leftrightarrow x = y = 1;$$

2) *следующие четыре соотношения эквивалентны —*

$$x \sqcap y = x, \quad x \sqcup y = y, \quad x' \sqcup y = \iota, \quad x \sqcap y' = o;$$

3) $(x \sqcap y = o) \& (x \sqcup y = \iota) \Leftrightarrow y = x'$ — *лемма о единственности дополнения*³.

Доказательство.

1. Беря пересечение обеих частей равенства $x \sqcup y = 0$ с x , получим $x \sqcap (x \sqcup y) = 0$, откуда по *Abs1* получаем $x = o$; аналогично показывается, что $y = o$.

Беря объединение обеих частей равенства $x \sqcap y = 1$ с x , получим $x \sqcup (x \sqcap y) = 1$, откуда по *Abs2* получаем $x = \iota$; аналогично показывается, что $y = \iota$.

Обратные следования очевидны (законы $\sqcup o$ и $\sqcap \iota$).

2. Пусть $x \sqcap y = x$. Но по *Abs2* имеем $y \sqcup (x \sqcap y) = y$, т.е. $x \sqcup y = y$. С учётом этого имеем

$$x' \sqcup y = x' \sqcup (x \sqcup y) = (x' \sqcup x) \sqcup y = \iota \sqcup y = \iota.$$

Из полученного $x' \sqcup y = \iota$ по *DeM1* следует, что

$$x \sqcap y' = o.$$

И наконец с учётом последнего, применяя законы дистрибутивности, имеем

$$x \sqcap y = (x \sqcap y) \sqcup o = (x \sqcap y) \sqcup (x \sqcap y) = x \sqcap (y \sqcup y') = x \sqcap \iota = x.$$

Таким образом мы циклически вывели требуемые соотношения друг из друга.

³В некоторых аксиоматизациях дополнение вводится как элемент, удовлетворяющий условиям комплиментарности и изолированности. Но тогда необходимо доказывать его единственность, чем и объясняется название леммы.

3. (\Rightarrow , достаточность)

$$\begin{aligned} y \stackrel{\sqcap \iota}{=} y \sqcap \iota \stackrel{Cmp'}{=} y \sqcap (x \sqcup x') \stackrel{Com \sqcap, Dtr1}{=} (y \sqcap x) \sqcup (y \sqcap x') &= \\ = o \sqcup (y \sqcap x') \stackrel{Isl'}{=} (x \sqcap x') \sqcup (y \sqcap x') \stackrel{Dtr, Abs, Com}{=} & \\ = (x \sqcup y) \sqcap x' = \iota \sqcap x' \stackrel{\sqcap \iota}{=} x'. & \end{aligned}$$

(\Leftarrow , необходимость) очевидна — законы Cmp' и Isl' .

□

Отдельный элемент булевой алгебры, а также формула, описывающая применение конечного числа указанных операций к элементам носителя, записанное в виде соответствующей формулы, будем называть *булевым выражением*. Ясно, что булево выражение определяет некоторый элемент булевой алгебры как значение функции от переменных, вместо которых подставляются те или иные конкретные элементы. Два выражения, связанные знаком ($=$) представляют собой *булево равенство*. Булево равенство может быть как истинным, так и ложным в зависимости от того, определяют ли левая и правая его части один и тот же элемент носителя. Точное определение данных понятий будет дано в п. 5.4. Приведённые выше законы булевой алгебры истинны именно в этом смысле.

Пусть V — выражение или равенство булевой алгебры. Результаты одновременной замены всех символов $\sqcap \leftrightarrow \sqcup$ и $\iota \leftrightarrow o$ в V будем обозначать V^{\natural} , а $x \leftrightarrow x'$, где x — некоторый элемент носителя, не являющийся универсальной гранью — V^b . Если же в V производятся обе указанные замены, то их результат обозначим V^* . В булевой алгебре справедлив следующий

Принцип двойственности (для булевой алгебры). 1. Если V — булево равенство, истинное для любых входящих в него элементов, то равенства V^{\natural} , V^b и V^* также истинны.

2. Если V — выражение булевой алгебры, то $V^* = V'$.

Действительно, приведённые выше законы, кроме Inv' , разбиваются на пары (последовательно записанных) взаимодвойственных, переходящих друг в друга при замене $^{\natural}$; при этом Inv' переходит сам в себя. Преобразование b переводит все законы, кроме Inv' , или с точностью до обозначений в себя, или в двойственные, а Inv' переходит в тождество $x' = x'$. Поэтому и при замене * истинность булева равенства сохранится. В результате утверждение (1) доказано. Справедливость утверждения (2) следует из равенства $V = z$, где z — соответствующий элемент булевой алгебры: $V = z \Rightarrow V^* = z' \Rightarrow V^* = V'$. Впервые принцип двойственности был сформулирован Э. Шредером в 1877 г.

Нетрудно обнаружить, что приведённая система из 21-ой аксиомы избыточна.

- Законы идемпотентности вытекают из законов поглощения. Действительно, для любого $x \in B$ имеет место

$$x \sqcup x \stackrel{Abs1}{=} x \sqcup (x \sqcap (x \sqcup x)) \stackrel{Abs2}{=} x.$$

Идемпотентность пересечения следует из только что доказанного по принципу двойственности⁴.

⁴Для нас указанные следования почти очевидны, однако они были установлены выдающимся немецким математиком Р. Дедекиндом.

- Законы поглощения влекут эквивалентность дистрибутивных законов. Действительно, для любых элементов x, y, z булевой алгебры имеем

$$\begin{aligned} (x \sqcup z) \sqcap (y \sqcup z) &\stackrel{Dtr1}{=} (x \sqcap (y \sqcup z)) \sqcup (z \sqcap (y \sqcup z)) \stackrel{Abs1, Dtr1}{=} \\ &= (x \sqcap y) \sqcup (x \sqcap z) \sqcup z \stackrel{Abs2}{=} (x \sqcap y) \sqcup z. \end{aligned}$$

т.е. $Dtr1 \Rightarrow Dtr2$. Двойственно показывается, что $Dtr2 \Rightarrow Dtr1$.

- Используя законы дистрибутивности, ассоциативности, свойства дополнения и единицы показывается, что для любых $x, y \in B$ справедливо

$$(x \sqcap y) \sqcup (x' \sqcup y') = \iota \quad \text{и} \quad (x \sqcap y) \sqcap (x' \sqcup y') = o.$$

В соответствии с леммой о единственности дополнения это означает, что $x' \sqcup y'$ — дополнение к $x \sqcap y$, т.е. из указанных законов выведен закон $DeM1$. Аналогичная выводимость $DeM2$ следует из принципа двойственности.

Избыточность системы аксиом обычно не является помехой в практической работе. При определении булевой алгебры удобно задавать именно приведённый набор аксиом, как содержащий все основные характерные соотношения, раскрывающие содержательные свойства определяемого объекта. Вопрос же о избыточной системе аксиом для булевой алгебры оказался не таким простым, как могло бы показаться на первый взгляд. В ходе его исследования был обнаружен ряд интересных фактов, с некоторыми из которых мы встретимся в дальнейшем.

Укажем ещё две системы аксиом для булевой алгебры.

- Пары аксиом коммутативности, дистрибутивности, нейтральных свойств особых элементов, а также основные законы дополнения, т.е. первые восемь из приведенных выше законов.

Данная система не является независимой: можно показать, что каждый из законов $\sqcup o$, $\sqcap \iota$ выводим из остальных семи. Данная аксиоматика, часто используемая на практике как наиболее легко проверяемая, восходит к работам американского математика Э. Хантингтона⁵.

- Пары законов пары законов Dtr , Abs вместе с $Сmp'$ и Isl' .

Это единственная кратчайшая (шесть аксиом) известная безызыточная самодвойственная система аксиом булевой алгебры.

Понятно, что такие и подобные им системы имеет более формальный характер по сравнению с приведённой в определении 1.1.

Булева алгебра является примером *алгебраической системы* (AC), точнее, частного случая AC — *алгебры*. Произвольная AC \mathfrak{A} задается парой множеств A и σ_A , т.е. $\mathfrak{A} = \langle A, \sigma_A \rangle$. Здесь A — *носитель*, а σ_A — *сигнатура* AC с носителем A . Носитель AC есть некоторое непустое множество. Сигнатура σ_A алгебры с носителем A есть упорядоченная совокупность символов операций, отношений и особых элементов из A . Если нужно явно указать местность или арность операций и отношений, их записывают как верхние индексы у соответствующих символов (символы особых элементов имеют нулевую местность). Если результат некоторой операции над элементами множества всегда

⁵Huntington E. V. Sets of independent postulates for algebra of logic. — Amer. Math. Soc., 1904, **5**, p. 288-309. Подробности см. в [33].

лежит в этом множестве, то говорят, что множество *устойчиво* относительно данной операции, а операция *устойчива* на данном множестве. В определении алгебры требуется, чтобы все операции были устойчивы на её носителе. Здесь приведено неформальное пояснение понятия АС, точные определения будут даны в п. 6.1. Как синонимом понятия АС мы будем пользоваться термином «структура».

Для случая булевой алгебры с носителем B имеем $\sigma_B = \langle \sqcup^2, \sqcap^2, '1, o^0, \iota^0 \rangle$ (сигнатура не содержит символов отношений), и свойства указанных операций и выделенных элементов носителя описываются указанными выше законами. Ясно, что выделенные элементы o и ι суть некоторые нульместные операции на носителе. Если рассматривается АС заданной сигнатуры, то, стремясь к краткости, для её обозначения часто используют просто символ носителя. Мы будем так поступать, когда это не приводит к недоразумениям.

Отметим, что основные законы булевой алгебры были сформулированы Дж. Булем в 1847 г. в основополагающей работе «Математический анализ логики». Однако точного определения предложенной им алгебры Буль не дал. Алгебраическая система, эквивалентная булевой алгебре в современном её понимании, впервые приведена в вышедшем в том же году третьем томе трактата А. де Моргана «Формальная логика». В работе Т. Хельперина, прямо озаглавленной «Алгебра Буля не есть булева алгебра» (*Heilperin T. Bool's algebra isn't boolean algebra. Math. Mag., 1981, 54, 4, 173–184*), показано, что алгебра логики, предложенная Булем, является коммутативным кольцом с единицей, без нильпотентных элементов и обладающая идемпотентами. Такая система применима для изучения теории мультимножеств и псевдобулевых функций. Системы Буля и де Моргана, очевидно, различаются. Идеи последнего нашли отражение в современных теориях нечёткой логики и алгебрами де Моргана⁶.

1.2 Алгебры множеств

Рассмотрим непустое множество A и некоторую совокупность $\mathcal{S}(A)$ его подмножеств, устойчивую относительно операций объединения (\cup), пересечения (\cap) и дополнения до A ($-$). Множество всех подмножеств (*булеан*) A будем обозначать $\mathcal{P}(A)$. Понятно, что $\{\emptyset, A\} \subseteq \mathcal{S}(A) \subseteq \mathcal{P}(A)$.

Алгебраическая система $\langle \mathcal{S}(A), \cup, \cap, -, \emptyset, A \rangle$ называется *алгеброй множеств* (*полем множеств, алгеброй классов*). Алгебру множеств с носителем $\mathcal{P}(A)$ будем называть *тотальной (над A)*, а с двухэлементным носителем $\{\emptyset, A\}$ — *тривиальной алгебрами множеств*.

Нетрудно показать, что имеет место

Утверждение 1.1. *Всякая алгебра множеств $\mathcal{S}(A)$ есть булева алгебра с нулём \emptyset и единицей A .*

Доказательство. Достаточно убедиться, что в любой алгебре $\mathcal{S}(A)$ множеств выполняются первые восемь законов булевой алгебры в формулировке которых произведены подстановки $\sqcup \mapsto \cap, \sqcap \mapsto \cup, ' \mapsto -, \iota \mapsto A, o \mapsto \emptyset$.

Законы коммутативности, $\sqcup o, \sqcap \iota$ и *Смп'*, *Isl'* описывают элементарные свойства теоретико-множественных операций.

В силу принципа двойственности достаточно доказать справедливость для алгебры множеств первого закона дистрибутивности: $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$

⁶Псевдобулева функция есть некоторая нумерация вершин единичного куба. Алгебра де Моргана задаётся парами аксиом коммутативности, ассоциативности, дистрибутивности, законов Де Моргана, $\sqcup o, \sqcap \iota$ и *Inv'*.

для любых подмножеств $X, Y, Z \in \mathcal{S}(A)$. Для этого рассмотрим произвольный элемент $w \in (X \cup Y) \cap Z$. Он принадлежит Z , а также либо X , либо Y . В первом случае $w \in X \cap Z$, а во втором — $w \in Y \cap Z$. Следовательно, $w \in (X \cap Z) \cup (Y \cap Z)$. Пусть теперь $w \in (X \cap Z) \cup (Y \cap Z)$. Тогда $w \in X \cap Z$ или $w \in Y \cap Z$, откуда $w \in Z$ и либо $w \in X$, либо $w \in Y$, т.е. $w \in (X \cup Y) \cap Z$. \square

Пример 1.1. σ -алгебра подмножеств пространства элементарных событий, используемая в аксиоматике теории вероятностей, есть алгебра множеств и, следовательно, булева алгебра.

Заметим, что система подмножеств некоторого множества может оказаться булевой алгеброй, не являясь при этом алгеброй множеств. Это будет, когда хотя бы одна из операций на данной системе не является соответствующей теоретико-множественной. Ниже такие системы встретятся.

Проверку равенств булевой алгебры легче всего проводить, используя известные диаграммы Эйлера-Венна⁷, в которых множество A изображается прямоугольником, а его подмножества — различными кругами или овалами общего положения в этом прямоугольнике. При этом объединению элементов соответствует объединение, а пересечению — общая часть фигур, связанных с данными элементами. Такие диаграммы строят отдельно для левых и правых частей проверяемого равенства, а интересующую при данной проверке область заштриховывают. Если на соответствующей паре диаграмм заштрихованными оказались одинаковые области, то, рассматривая различные подобласти A получающиеся в результате пересечения фигур, можно провести формальное доказательство, подобное приведённому выше.

Впрочем, на практике можно просто ограничиться указанной констатацией, если соответствующие построения проводить для “правильно построенных” диаграмм Эйлера-Венна. Ниже данное понятие формализуется.

Определение 1.2. Пусть дано непустое множество U и система его подмножеств $\{X_1, \dots, X_n\}$. Составляющие s_1, \dots, s_k данной системы множеств задаются следующим индуктивным определением:

- 1) составляющие системы $\{X_1\}$ суть X_1 и \bar{X}_1 ;
- 2) если s — составляющая системы $\{X_1, \dots, X_{n-1}\}$, то $s \cap X_n$ и $s \cap \bar{X}_n$ — составляющие системы $\{X_1, \dots, X_{n-1}, X_n\}$.

Система множеств X называется *независимой*, если все её составляющие непусты.

Пример 1.2. Рассмотрим множество $U = \{a, b, c, d\}$.

1. Составляющие системы $X_1 = \{a, b\}$, $X_2 = \{b\}$ суть $\{b\}$, \emptyset , $\{a\}$, $\{c, d\}$, и, следовательно, данная система множеств не является независимой.
2. Составляющие системы $X_1 = \{a, b\}$, $X_2 = \{b, c\}$ суть $\{b\}$, $\{c\}$, $\{a\}$, $\{d\}$, и, следовательно, данная система множеств независима.

Для $\sigma \in \{0, 1\}$ и множества X введём обозначение X^σ : X^σ есть X , если $\sigma = 1$ и \bar{X} , если $\sigma = 0$. Булево выражение вида $\bigcap_{j=1}^m X_j^{\sigma_j}$, где X_1, \dots, X_m суть попарно различные подмножества некоторого множества, а $\sigma_j \in \{0, 1\}$, называется их *элементарным пересечением*. Понятно, что элементарные пересечения либо совпадают, либо не пересекаются.

⁷См., например, Кузичев А.С. Диаграммы Венна. — М., 1968, или [5].
Джон Венн (John Venn, 1834–1923) — английский математик и логик.

- Лемма 1.2 (свойства составляющих системы множеств).** 1. Произвольная составляющая системы множеств $\{X_1, \dots, X_n\}$, $X_i \in U$, $i = \overline{1, n}$, представима в виде элементарного пересечения u , следовательно, неравные составляющие не пересекаются.
2. Независимая система из n множеств имеет 2^n различных составляющих.
3. Объединение всех составляющих совпадает с универсальным множеством U .

Доказательство пп. 1 и 3) легко проводятся по индукции, а 2) следует из 1). \square

Из леммы следует, что получаемая в соответствии с определением совокупность составляющих некоторой системы множеств не зависит от порядка выбора этих множеств и, таким образом, определение набора составляющих корректно.

Итак, все составляющие системы множеств суть элементарные пересечения. Выражение F_M , задающее некоторое подмножество M алгебры множеств в виде объединения различных элементарных пересечений называется *нормальной формой Кантора* для M над соответствующими попарно различными множествами. Две нормальные формы Кантора, отличающиеся порядком объединения элементарных пересечений, будем считать эквивалентными, поскольку они, очевидно, задают одно и то же множество.

Теорема 1.1 (Венн). Если в алгебре множеств булево равенство выполнено для некоторой независимой системы подмножеств, то оно справедливо для любой системы подмножеств.

Доказательство. Заметим, что любая составляющая s системы $\{X_1, \dots, X_n\}$ однозначно определяет значения всех формул вида $c \in X_i$, что легко устанавливается по индукции. Далее, если Y — булева формула с переменными $\{X_1, \dots, X_n\}$ и s — составляющая этой системы, то s либо подмножество множества, соответствующего Y , либо с ним не пересекается. Это вытекает из того, что значение характеристического свойства Y полностью определяется значениями всех $c \in X_i$. Значит, в независимой системе любая булева комбинация однозначно разлагается на составляющие (т.е. представляется как объединение составляющих) и это разложение сохраняется и для других систем множеств (конечно, для зависимых систем могут появиться и другие разложения). Поэтому если в независимой системе две булевы комбинации имеют одни и те же составляющие, они будут иметь одинаковые значения и в любой другой системе. \square

Из теоремы следует, что равенство в алгебре множеств достаточно проверить на одной диаграмме Эйлера-Венна с независимой системой множеств. Их и называют множествами общего положения. Интерпретация же выражений любой булевой алгебры соотношениями множеств обосновывается приведённой ниже теоремой 1.3.

Объединение, пересечение и дополнение будем считать основными теоретико-множественными операциями. Обычно вводят и производные операции над множествами. Например, операция \setminus (*разности*) множеств X и Y определяется как $X \setminus Y = X \cap \bar{Y}$, а операция \oplus (*их симметрической разности*) как $X \oplus Y = (X \cap \bar{Y}) \cup (\bar{X} \cap Y)$. Можно показать, что $X \oplus Y = (X \cup Y) \setminus (X \cap Y)$. Следующие свойства введённых операций легко проверяются:

$$\begin{aligned} X \setminus (Y \setminus Z) &= (X \setminus Y) \cup (X \cap Z); \\ X \setminus (Y \cap Z) &= (X \setminus Y) \cup (X \setminus Z); \\ X \setminus (Y \cup Z) &= (X \setminus Y) \cap (X \setminus Z); \\ X \oplus (Y \oplus Z) &= (X \oplus Y) \oplus Z; \\ X \oplus Y &= Y \oplus X; \\ (X \oplus Y) \cap Z &= (X \cap Y) \oplus (Y \cap Z). \end{aligned}$$

При этом операция симметрической разности обладает свойствами метрики:

$$\begin{aligned} X \oplus Y = 0 &\Leftrightarrow X = Y; \\ X \oplus Y &= Y \oplus X; \\ X \oplus Y &\subseteq (X \oplus Z) \cup (Z \oplus Y). \end{aligned}$$

Также часто используют отношение \subseteq включения множеств. Очевидно

$$X \subseteq Y \Leftrightarrow X \cap Y = X \Leftrightarrow X \cup Y = Y.$$

При $X \subseteq Y$, напомним, X называют подмножеством Y , а Y — надмножеством X .

В дальнейшем мы будем использовать обозначение $\mathcal{P}^*(A)$ для совокупности всех непустых подмножеств множества A .

Далее в данном разделе мы рассмотрим практически важную задачу подсчёта числа элементов в подмножествах с помощью формул включений-исключений и обращения.

Пусть X_1, \dots, X_n — конечные множества. Легко видеть, что

$$|X_1 \cup X_2| = |X_1| + |X_2| - |X_1 \cap X_2|$$

и далее

$$|X_1 \cup X_2 \cup X_3| = |X_1| + |X_2| + |X_3| - |X_1 \cap X_2| - |X_2 \cap X_3| - |X_3 \cap X_1| + |X_1 \cap X_2 \cap X_3|.$$

Применяя математическую индукцию, получим *формулу включений и исключений*

$$\begin{aligned} \left| \bigcup_{i=1}^n X_i \right| &= \sum_{1 \leq i \leq n} |X_i| - \sum_{1 \leq i_1 < i_2 \leq n} |X_{i_1} \cap X_{i_2}| + \\ &+ \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |X_{i_1} \cap X_{i_2} \cap X_{i_3}| - \dots + (-1)^{n-1} \sum_{1 \leq i_1 < \dots < i_n \leq n} |X_{i_1} \cap \dots \cap X_{i_n}| = \\ &= \sum_{k=1}^n (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |X_{i_1} \cap \dots \cap X_{i_k}|. \end{aligned}$$

Пример 1.3. Задача. В группе студентов 10 москвичей, а остальные — иногородние. Известно, что пятеро москвичей и семеро иногородних любят читать детективы, а двое москвичей — не любят. Спрашивается, сколько человек насчитывает вся группа?

Решение. Пусть A , B и C — множества москвичей, иногородних и любителей детективов соответственно. Имеем: $|A| = 10$, $|B| = 9$, $|C| = 12$, $A \cap B = \emptyset$, $|A \cap C| = 5$, $|B \cap C| = 7$, $A \cap B \cap C = \emptyset$. Поэтому

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| = \\ &= 10 + 9 + 12 - 0 - 7 - 5 + 0 = 19. \end{aligned}$$

Применим формулу включения и исключения для решения следующей, весьма общей, задачи. Пусть имеется N элементов и некоторое число свойств $P(1), \dots, P(n)$. Ясно, что свойства задают некоторые подмножества исходного множества. Пусть далее N_i — число элементов со свойством $P(i)$ и вообще $N_{i_1 i_2 \dots i_r}$ — число элементов со свойствами $P(i_1), \dots, P(i_r)$, а также, возможно, какими-то ещё. Тогда число элементов $N(0)$, не обладающих ни одним из указанных свойств, будет задаваться *формулой обращения*

$$\begin{aligned} N(0) &= N - \sum_i N_i + \sum_{i_1 < i_2} N_{i_1 i_2} - \dots \\ &\dots + (-1)^k \sum_{i_1 < i_2 < \dots < i_k} N_{i_1 i_2 \dots i_k} + \dots + (-1)^n N_{1,2,\dots,n}. \end{aligned} \quad (1.1)$$

Формула (1.1) содержит, очевидно, 2^n слагаемых. Но в некоторых случаях удаётся получить ответ с меньшим числом слагаемых. Это будет, когда число $N_{t_1 t_2 \dots t_r}$ элементов со свойствами $P(i_1), \dots, P(i_r)$ не зависит от самих этих свойств, а лишь от количества одновременно выполняемых свойств, т.е.

$$\begin{aligned} N_1 &= N_2 = \dots = N_n = N^{(1)}, \\ N_{1,2} &= N_{1,3} = \dots = N_{1,n} = N_{2,3} = \dots = N_{n-1,n} = N^{(2)}, \\ &\dots\dots\dots \\ N_{1,2,\dots,n} &= N^{(n)}. \end{aligned}$$

Поэтому в рассматриваемом случае формула включений и исключений принимает вид

$$N(0) = N - C_n^1 N^{(1)} + C_n^2 N^{(2)} - \dots\dots\dots + (-1)^k C_n^k N^{(k)} + \dots + (-1)^n N^{(n)}. \quad (1.2)$$

В качестве примера подсчитаем число булевых функций, существенно зависящих от n переменных. Напомним, что булева функция $f(x_1, \dots, x_n)$ существенно зависит от переменной x_i , если найдётся набор $\alpha_1, \dots, \alpha_{n-1}$ из 0 и 1 такой, что

$$f(\alpha_1, \dots, \alpha_{i-1}, 0, \alpha_i, \dots, \alpha_{n-1}) \neq f(\alpha_1, \dots, \alpha_{i-1}, 1, \alpha_i, \dots, \alpha_{n-1}).$$

Известно, что имеется различных 2^{2^n} булевых функций, зависящих от n переменных. Пусть $P(i)$ — свойство функции иметь i фиктивных переменных, $i = 0, 1, \dots, n$. Тогда число существенных переменных — $n - i$ из n , причём i несущественных переменных можно выбрать C_n^i способами. Поэтому $\sum_{i_1 < i_2 < \dots < i_k} N_{i_1 i_2 \dots i_k} = C_n^k 2^{2^{n-k}}$ и по формуле (1.1):

$$\begin{aligned} N(0) &= C_n^0 2^{2^n} - C_n^1 2^{2^{n-1}} + \dots + (-1)^k C_n^k 2^{2^{n-k}} + \dots \\ &\dots + (-1)^k C_n^k 2^{2^{n-k}} = \sum_{k=0}^n (-1)^k C_n^k 2^{2^{n-k}}. \quad (1.3) \end{aligned}$$

Количества $b(n)$ всех булевых функций от n переменных и $i(n)$ булевых функций, существенно зависящих от всех переменных для первых значений n приведено в нижеследующей таблице.

n	0	1	2	3	4	5
$b(n)$	2	4	16	256	65 536	4 294 967 296
$i(n)$	2	2	10	218	64 594	4 294 642 034

Введём следующие удобные обозначения. Пусть

- $N_{[s]}$ — число элементов, обладающих ровно r свойствами (неважно, конкретно какими). Обычно эти значения для $s = 1, 2, \dots, n$ и требуется определить, т.к. зная их можно найти мощности подмножеств во всевозможными комбинациями свойств. Ясно, например, что $N(0) = N_{[0]}$.
- $N_{(s)}$ — число элементов, обладающих не менее r свойствами (неважно, конкретно какими). Понятно, что $N_{(s)} = \sum_{i_1 < i_2 < \dots < i_s} N_{i_1 i_2 \dots i_s}$, $s = 1, 2, \dots, n$ и $N_{(0)} = N$.

Ясно, что в этих обозначениях формула обращения (1.1) приобретает вид

$$N_{[0]} = N_{(0)} - N_{(1)} + N_{(2)} - \dots + (-1)^s N_{(s)} + \dots + (-1)^n N_{(n)}. \quad (1.4)$$

Существует простое мнемоническое правило для запоминания принципа включения-исключения: пусть 1 соответствует объектам, обладающим всеми свойствами, тогда $1 - c_1$ — выражение для объектов, не обладающих свойством c_1 , $1 - c_2$ — выражение для объектов, не обладающих свойством c_2 и т.д. Выражение для объектов, не обладающих ни одним из свойств c_1, \dots, c_m будет иметь вид

$$(1 - c_1)(1 - c_2) \dots (1 - c_m).$$

Откуда, раскрывая скобки, получаем

$$(1 - c_1)(1 - c_2) \dots (1 - c_m) = 1 - c_1 - c_2 - \dots - c_m + c_1c_2 + \dots - c_1c_2c_3 \dots \quad (1.5)$$

Можно показать, что справедлива *общая формула включений и исключений*

$$N_{[m]} = C_m^m N_{(m)} - C_{m+1}^m N_{(m+1)} + C_{m+2}^m N_{(m+2)} - \dots \\ \dots + (-1)^s C_{m+s}^m N_{(m+s)} + \dots + (-1)^{n-m} C_n^m N_{(n)}. \quad (1.6)$$

Часто именно эту последнюю наиболее общую формулу и считают выражением принципа включений и исключений.

Пример 1.4. Задача. При обследовании читательских вкусов оказалось, что 60% студентов читают журнал А, 50% — журнал В, 50% — журнал С, 30% — журналы А и В, 20% — журналы В и С, 40% — журналы А и С, 10% — журналы А, В и С. Сколько процентов студентов:

- 1) не читает ни одного журнала?
- 2) читает в точности 2 журнала?
- 3) читает не менее 2-х журналов?

Решение.

1. По принципу включения и исключения

$$N_{[0]} = N_{(0)} - N_{(1)} + N_{(2)} - N_{(3)} = \\ = 100\% - (60\% + 50\% + 50\%) + (30\% + 20\% + 40\%) - 10\% = 20\%.$$

2. По общей формуле включений и исключений

$$N_{[2]} = C_2^2 N_{(2)} - C_3^2 N_{(3)} = 1 \cdot (30\% + 20\% + 40\%) - 3 \cdot 10\% = 60\%.$$

3. По общей формуле включений и исключений

$$N_{[2]} + N_{[3]} = C_2^2 N_{(2)} - C_3^2 N_{(3)} + C_3^3 N_{(3)} = \\ = 1 \cdot (30\% + 20\% + 40\%) - 3 \cdot 10\% + 10\% = 70\%.$$

1.3 Изоморфизмы булевых алгебр

Хотя алгебры множеств являются, как мы увидим, в некотором смысле, основными примерами булевых алгебр, последние ими не исчерпываются.

Пример 1.5. 1. Рассмотрим двоичное множество истинностных значений $B = \{1, 0\}$ и сигнатуру $\sigma = \langle \vee, \&, \neg, 0, 1 \rangle$, состоящую из логических операций дизъюнкции, конъюнкции и отрицания, а также символов элементов B — логического нуля 0 («ложь») и логической единицы 1 («истина»). Полученная АС $\langle B, \sigma \rangle$ является, как нетрудно видеть, булевой алгеброй. Эта простейшая булева алгебра играет фундаментальную роль в логике. Она называется *алгеброй высказываний*; будем обозначать её **2**. Заметим, что *Стр'* и *Isl'* (основные законы, описывающие свойства дополнения) в логике называются соответственно законами «исключенного третьего» и «противоречия».

2. АС $\langle B^n, \vee, \&, \neg, \tilde{0}, \tilde{1} \rangle$, где B^n — n -мерный единичный куб, $\tilde{0}$ и $\tilde{1}$ — обозначения нулевого $(0 \dots 0)$ и единичного $(1 \dots 1)$ векторов соответственно, а сигнатурные операции применяются к булевым векторам покомпонентно, называют *булевой алгеброй n -мерных двоичных векторов*.

3. Обозначим через P_2 множество всех двузначных булевых функций, а через 0 и 1 — функции «тождественный нуль» и «тождественная единица» соответственно. Тогда АС $\langle P_2, \vee, \&, \neg, 0, 1 \rangle$ есть булева алгебра. Её называют *булевой алгеброй логических функций*.

4. Пусть N — свободное от квадратов натуральное число. Это означает, что справедливо представление $N = p_1 \cdot \dots \cdot p_k$ (*примарное разложение*), где p_1, \dots, p_k — различные простые числа. Совокупность всех натуральных делителей N обозначим $D(N)$. Например, для $N = 30 = 2 \cdot 3 \cdot 5$ имеем $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$.

Наименьшее общее кратное чисел m и n обозначим $m \vee n$, а их наибольший общий делитель — $m \wedge n$. Положим $m' = \frac{N}{m}$. Тогда АС $\langle D(N), \vee, \wedge, ', 1, N \rangle$, как нетрудно проверить, есть булева алгебра. Данная булева алгебра широко используется в теории чисел⁸.

5. Рассмотрим множество электрических выключателей, или контактов, которые могут находиться в одном из двух состояний — замкнутым (проводящим) или разомкнутым (не проводящим). У таких контактов различают входной и выходной полюсы, которые можно соединять с полюсами других контактов, строя электрические двухполюсные (один вход и один выход) цепи.

Если соединять друг с другом только входные и выходные полюсы, то имеется только два способа объединения таких цепей: последовательное и параллельное. При последовательном соединении цепей A и B выходной полюс цепи A присоединяется к входному полюсу цепи B , при параллельном — попарно объединяются входные и выходные цепи A и B (в обоих случаях входной и выходной полюсы полученной цепи определяются входным полюсом A и выходным полюсом B соответственно). Таким образом, получают класс т.н. параллельно-последовательных контактных схем. Их ещё называют π -схемами.

Под произведением $A \cdot B$ будем понимать цепь, образованную последовательным, а под суммой $A + B$ — параллельным соединением цепей A и B . Под цепью \bar{A} будем понимать цепь, полученную размыканием всех замкнутых контактов A и замыканием всех её разомкнутых контактов.

Проводимость двухполюсной цепи может быть описана некоторой булевой функцией, точнее — функцией, представимой т.н. *бесповторной формулой* над множеством логических связок $\{\vee, \&, \neg\}$, соответствующих операциям $\{+, \cdot, \bar{}\}$, в которой каждому контакту цепи соответствует выражающая его проводимость пропозициональная переменная, встречающаяся в формуле ровно один раз.

Две цепи будем считать одинаковыми, если можно так сопоставить контактам переменные, что при одном и том же состоянии контактов, соответствующим одной

⁸В частности, отсюда следует, что максимальное число взаимно простых делителей свободного от квадратов числа N есть $\binom{N}{[N/2]}$

переменной и всех произвольных состояниях остальных контактов, обе рассматриваемые цепи являются одновременно либо проводящими, либо не проводящими. Введенное отношение, очевидно, является отношением эквивалентности на множестве цепей. Обозначим через I постоянно замкнутый, а через O — постоянно разомкнутый контакты. Обозначим через C множество всех попарно неэквивалентных π -схем (двухполюсных электрических цепей). Тогда АС $\langle C, +, \cdot, -, O, I \rangle$ есть, как нетрудно видеть, булева алгебра.

Применение формульного аппарата булевых алгебр для анализа и синтеза электрических схем имеет огромное прикладное значение.

Системы данного примера являются *представлениями* или *реализациями* булевой алгебры.

Пример 1.6. 1. Кроме параллельно-последовательных, существуют ещё т.н. мостиковые схемы, когда входные или выходные контакты одной цепи присоединяется к внутреннему полюсу другой, образуя, тем не менее, двухполюсную цепь — простейшая мостиковая схема изображена на рис. 1.1.

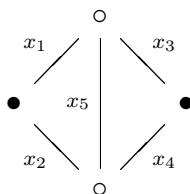


Рис. 1.1: Мостиковая схема (входной и выходной полюсы выделены)

Эти схемы не являются параллельно-последовательными и для их описания язык булевой алгебры оказывается недостаточным: «не удаётся так усовершенствовать обычный булев аппарат алгебры логики, добавив к нему ещё несколько (конечное число!) операций так, чтобы он стал содержать средства для описания строения не только параллельно-последовательных, но и мостиковых схем, притом описания адекватного, т.е. такого, при котором каждому контакту в схеме соответствует ровно одна буква в формуле, выражающая проводимость данной схемы»⁹.

Действительно, проводимость мостиковой схемы на рис. 1.1 описывается булевой функцией, которая может быть задана формулой $F = x_1 \& (x_3 \vee (x_4 \& x_5)) \vee x_2 \& (x_4 \vee (x_3 \& x_5))$, не являющейся неповторной, и никакое эквивалентное преобразование F не приведёт, как можно показать, к неповторной форме над множеством связок $\{\vee, \&, \neg\}$ ¹⁰.

Отметим, что попытка построения подобного булевой алгебре формализованного формульного языка, пригодного для адекватного описания двухполюсных цепей общего вида предпринята в работе [9].

2. Для действительных чисел a, b из отрезка $[0, 1]$ положим

$$a \oplus b = \max\{a, b\}, \quad a \otimes b = \min\{a, b\}, \quad \ominus a = 1 - a.$$

⁹ Кузнецов А.В. О неповторных контактных схемах и неповторных суперпозициях функций алгебры логики // Труды матем. ин-та им. В.А. Стеклова, т. LI. — М.: 1958.

¹⁰ Это утверждение неоднократно высказывалось В.И. Шестаковым, начиная с 1930-х годов. Однако на семинаре по математической логике в МГУ в начале 1950-х годов П.С. Новиков указал на отсутствие математического доказательства данного факта. Такое доказательство было позже приведено А.В. Кузнецовым.

Систему $\langle [0, 1], \oplus, \otimes, \ominus, 0, 1 \rangle$ называют *максиминной алгеброй*. Она не будет являться булевой алгеброй, поскольку в ней не выполняются законы *Стр'* и *Isl'*. Отметим, что в приведённой выше системе из 21-ой аксиомы не выполняются только данные законы. Последнее доказывает их независимость от остальных и необходимость их присутствия в любой системе аксиом для булевой алгебры.

Отметим, что дополнения в максиминной алгебре единственны. Таким образом, указанная структура чрезвычайно близка к булевой алгебре, но ей всё-таки не является.

Определение 1.3. Пусть даны две булевы алгебры B_1 и B_2 и взаимно-однозначная функция¹¹ $\varphi: B_1 \rightarrow B_2$ такая, что равенства

$$1) \varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y), \quad 2) \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y), \quad 3) \varphi(x') = \varphi(x)'$$

справедливы для всех x и y из B_1 . Тогда говорят, что φ — *булев изоморфизм* между B_1 и B_2 , данные алгебры *булево изоморфны* (символически $B_1 \cong_b B_2$).

Замечание. Легко показать, что из 1)–3) следует

$$4) \varphi(o) = o \quad \text{и} \quad 5) \varphi(\iota) = \iota.$$

Действительно, имеем $\varphi(o) = \varphi(x \sqcap x') = \varphi(x) \sqcap \varphi(x') = \varphi(x) \sqcap \varphi(x)' = o$ и аналогично для $\varphi(\iota)$.

Мы видим, что булев изоморфизм — это взаимно-однозначное отображение носителей булевых алгебр, сохраняющее операции и особые элементы o и ι .

В записи булевых алгебр B_1 и B_2 мы использовали одинаковые обозначения и для соответствующих операций, и для выделенных элементов. Стремясь не усложнять обозначения, так обычно и поступают. При внимательном чтении путаницы относительно принадлежности операций и выделенных элементов к одной или другой алгебре возникнуть не должно.

Пример 1.7. 1. Алгебра высказываний, очевидно, изоморфна тривиальной алгебре множеств.

2. Тотальная алгебра над n -элементным множеством $A = \{a_1, \dots, a_n\}$ изоморфна булевой алгебре n -мерных двоичных векторов B^n . Булевым изоморфизмом здесь будет является отображение $\varphi: B^n \rightarrow \mathcal{P}(A)$, ставящее в соответствие булеву вектору $(\alpha_1, \dots, \alpha_n)$ подмножество $\{a_{i_k} \mid \alpha_{i_k} = 1, k = \overline{1, n}\}$ множества A .

Существует простой критерий изоморфности тотальных алгебр множеств.

Теорема 1.2. Для того чтобы тотальные алгебры множеств $\mathcal{P}(A)$ и $\mathcal{P}(B)$ были изоморфны, необходимо и достаточно, чтобы A и B имели одинаковую мощность¹².

Доказательство. (\Leftarrow) Пусть существует изоморфизм φ между алгебрами $\mathcal{P}(A)$ и $\mathcal{P}(B)$. Тогда φ — взаимно-однозначное соответствие между множествами A и B , откуда следует их равномощность.

(\Rightarrow) Пусть множества A и B равномощны. Тогда между их элементами можно установить взаимно-однозначное соответствие f . Однако, элементами $\mathcal{P}(A)$ и $\mathcal{P}(B)$ служат подмножества A и B соответственно и f не является искомым изоморфизмом. Поэтому распространим отображение f на подмножества данных множеств, поставив в соответствие произвольному подмножеству X множества A его образ $\varphi(X) = \bigcup_{a \in X} f(a) \subseteq B$. Простая проверка показывает, что φ является булевым изоморфизмом между $\mathcal{P}(A)$ и $\mathcal{P}(B)$. \square

Равномощные множества называют, напомним, *эквивалентными*.

¹¹Точное определение взаимно-однозначной функции или биекции см. в п. 2.6.

¹²т.е. чтобы между ними существовало взаимно-однозначное отображение.

1.4 Теорема Стоуна

Справедлива следующая фундаментальная теорема о представлении произвольных булевых алгебр алгебрами множеств. Она показывает, что элементы любой булевой алгебры можно считать подмножествами некоторого множества, а булевы операции отождествлять с одноимёнными теоретико-множественными.

Теорема 1.3 (Стоун). *Всякая булева алгебра изоморфна подходящей алгебре множеств.*

Иными словами, теорема Стоуна утверждает существование вложения любой булевой алгебры в некоторую тотальную алгебру множеств. Мы докажем эту теорему для конечного случая. Для этого нам потребуются ввести новое понятие.

Определение 1.4. Ненулевой элемент a булевой алгебры называется *атомом*, если для любого её элемента x справедливо либо $a \sqcap x = o$, либо $a \sqcap x = a$. В последнем случае говорят, что *элемент x содержит атом a* .

Например, в булевой алгебре всех n -мерных двоичных векторов атомы суть двоичные наборы единичного веса. В тотальной алгебре множеств атомами будут являться все одноэлементные подмножества.

Лемма 1.3. *В конечной булевой алгебре каждый ненулевой элемент содержит хотя бы один атом.*

Доказательство. Пусть $B = \{b_1, b_2, \dots, b_m\}$ — носитель булевой алгебры и x — его ненулевой элемент (в дальнейшем будет установлено, что $m = 2^n$ для некоторого натурального n). Приведём алгоритм, обнаруживающий атом, содержащийся в x .

Шаг 1. Положить $a \leftarrow x$, $k \leftarrow 1$.

Шаг 2. Вычислить $b = a \sqcap b_k$. Если $b = o$ или $b = a$, то переход к шагу 3, иначе — к шагу 4.

Шаг 3. Если $k = n$, то конец. Иначе $k \leftarrow k + 1$ и переход к шагу 2.

Шаг 4. Положить $a \leftarrow b$. Если $k = n$, то конец, иначе $k \leftarrow k + 1$ и переход к шагу 2.

После окончания работы алгоритма в a будет записан атом, содержащийся в x . В самом деле, алгоритм пропускает через a конечную (длины $< n$) последовательность ненулевых элементов $x, x \sqcap b_{i_1}, x \sqcap b_{i_1} \sqcap b_{i_2}, \dots$, последний из которых

$$y = x \sqcap b_{i_1} \sqcap b_{i_2} \dots \sqcap b_{i_n}$$

обладает тем свойством, что $y \sqcap z = o$ или $y \sqcap z = y$ для любого $z \in B$. Кроме того,

$$y \sqcap x = x \sqcap y = x \sqcap (x \sqcap b_{i_1} \sqcap b_{i_2} \dots \sqcap b_{i_n}) = x \sqcap b_{i_1} \sqcap b_{i_2} \dots \sqcap b_{i_n} = y.$$

Это означает, что y содержится в x и, таким образом, y — искомый атом. □

Утверждение 1.2 (Основное свойство атомов). *Если a_1 и a_2 — различные атомы булевой алгебры, то*

$$a_1 \sqcap a_2 = o. \tag{1.7}$$

Доказательство. Если $a_1 \sqcap a_2 = b \neq o$, то согласно определению, должно быть $b = a_1$ и $b = a_2$. \square

Булева алгебра, в которой каждый ненулевой элемент содержит атом, называется *атомной*. Все рассмотренные выше алгебры атомные. Из леммы 1.3 следует, что конечная булева алгебра является атомной. Булеву алгебру, не содержащую ни одного атома называют *безатомной* или *непрерывной*. Пример безатомной булевой алгебры будет приведён в п. 5.1.

Множество всех атомов, содержащихся в элементе x обозначим $At(x)$ и формально считать, что $At(o) = \emptyset$. Совокупность всех атомов булевой алгебры B будем обозначать $At(B)$.

Лемма 1.4. *Всякий ненулевой элемент конечной булевой алгебры может быть представлен в виде объединения содержащихся в нём атомов:*

$$x = \bigsqcup_{a \in At(x)} a. \quad (1.8)$$

Например, в тотальной алгебре над множеством $\{1, 2, 3, 4\}$ элемент $x = \{1, 2, 3\}$ содержит атомы $\{1\}, \{2\}, \{3\}$ и равен их объединению: $x = \{1\} \cup \{2\} \cup \{3\}$. При $At(x) = \{a\}$ формально полагают $x = a$, а при $At(x) = \emptyset$ — $x = o$. Понятно, что единица ι есть объединение всех атомов булевой алгебры B . Действительно, пусть $b = \bigsqcup_{a \in At(B)} a$, тогда

$$o = b' \sqcap b = b' \sqcap \bigsqcup_{a \in At(B)} a = \bigsqcup_{a \in At(B)} (b' \sqcap a),$$

и, следовательно, $b' \sqcap a = o$ для любого атома из $At(B)$, т.е. b' не содержит ни одного атома. По лемме 1.3 это означает, что $b' = o$, т.е. $b = \iota$.

Доказательство этой простой леммы отложим до п. 5.2.

Для конечного случая теорема Стоуна допускает следующее усиление.

Теорема 1.4. *Всякая конечная булева алгебра изоморфна подходящей тотальной алгебре множеств.*

Доказательство. Пусть B — конечная булева алгебра. Построим тотальную алгебру множеств над $At(B)$ и покажем, что она изоморфна B . При этом будем постоянно пользоваться утверждением леммы 1.4.

Рассмотрим функцию φ , сопоставляющую каждому элементу x из B множество $At(x)$ содержащихся в нём атомов. Покажем, что φ является искомым изоморфизмом между B и $\mathcal{P}(At(B))$.

Убедимся сначала, что $\varphi(x) = At(x)$ — биекция¹³ между B и $\mathcal{P}(At(B))$. Из разложения (1.8) следует, что

- 1) элемент x однозначно определяется множеством $At(x)$ своих атомов и наоборот, т.е. отображение $\varphi(x)$ инъективно;
- 2) для произвольного подмножества A атомов булевой алгебры можно определить элемент x по соотношению $x = \bigsqcup_{a \in A} a$, тогда $\varphi(x) = A$ и φ — сюръективно.

¹³Читателю должны быть известны свойства инъективности, сюръективности и биективности отображений. Их алгебраические определения будут даны в п. 2.6.

Таким образом, биективность отображения φ показана.

Теперь удостоверимся, что для φ выполнены свойства (1)–(3) определения 1.3 (нижеприведённые выкладки проведены для произвольных элементов x, y из B).

Во-первых, очевидно, что

$$x \sqcup y = \bigsqcup_{a_1 \in At(x)} a_1 \sqcup \bigsqcup_{a_2 \in At(y)} a_2 = \bigsqcup_{a \in At(x) \cup At(y)} a,$$

откуда $\varphi(x \sqcup y) = \varphi(x) \cup \varphi(y)$.

Во-вторых,

$$x \sqcap y = \bigsqcup_{a_1 \in At(x)} a_1 \sqcap \bigsqcup_{a_2 \in At(y)} a_2 \stackrel{Dtr1}{=} \bigsqcup_{\substack{a_1 \in At(x) \\ a_2 \in At(y)}} (a_1 \sqcap a_2) \stackrel{(1.7)}{=} \bigsqcup_{a \in At(x) \cap At(y)} a,$$

т.е. $\varphi(x \sqcap y) = \varphi(x) \cap \varphi(y)$.

В-третьих, подставляя в полученные выше равенства $y = x'$ имеем

$$At(x) \cup At(x') = At(B) \quad \text{и} \quad At(x) \cap At(x') = \emptyset,$$

откуда по лемме 1.1 $At(x') = At(B) \setminus At(x)$ и $\varphi(x') = \overline{\varphi(x)}$. □

Доказанная теорема имеет следующие простые

Следствия. 1. Если конечная булева алгебра имеет n атомов, то общее число её элементов равно 2^n .

2. Любая конечная булева алгебра изоморфна подходящей алгебре n -мерных двоичных векторов.

Первое следует из того, что мощность множества всех подмножеств совокупности из атомов n есть 2^n , а второе — из примера 1.7.2.

Теорема Стоуна показывает, что элементы любой булевой алгебры можно считать подмножествами некоторого множества, а булевы операции отождествлять с одноимёнными теоретико-множественными.

Если в булевой алгебре определены объединение и пересечение произвольной совокупности её элементов, то такая булева алгебра называется *полной*. Легко показывается, что в полной атомной булевой алгебре $At(B) = At(\iota)$. Ясно, что полной булевой алгеброй является любая алгебра множеств, а σ -алгебра, где эти операции могут быть взяты лишь по счётной совокупности множеств, является “промежуточной” между обычной и полной булевыми алгебрами.

Приведённое доказательство останется справедливым для полных атомных алгебр, и справедливой является следующая

Теорема 1.5 (о представлении полных атомных булевых алгебр). Пусть B — полная атомная булева алгебра. Тогда

$$B \cong_b \mathcal{P}(At(B)).$$

Таким образом, с точностью до изоморфизма полные атомные булевы алгебры исчерпываются тотальными алгебрами подходящих множеств.

Заметим, что для доказательства теоремы Стоуна в случае бесконечных булевых алгебр используется понятие ультрафильтра (см. п. 4.2).

Глава 2

Отношения и соответствия

Понятие отображения является настолько общим, что, вообще говоря, любое алгебраическое построение в явной или неявной форме основывается на понятии отображения. Поэтому любая работа по алгебре в той или иной степени посвящена изучению отображений множеств.

И.И. Валуце. Отображения. Алгебраические аспекты теории.

2.1 Декартово произведение множеств и отношения

Пусть $I = \{1, \dots, n\}$ — множество индексов и каждому $i \in I$ сопоставлено непустое множество A_i . Декартовым (или прямым) произведением множеств $\{A_i\}_{i \in I}$ называют множество конечных последовательностей (a_1, a_2, \dots, a_n) , где $a_i \in A_i$, $i \in I$. Декартово произведение обычно определяют для произвольной, а не только конечной, совокупности индексов. Нам, однако, будет достаточно данного определения и в дальнейшем мы будем обозначать декартово произведение

$$A_1 \times A_2 \times \dots \times A_n \quad \text{или} \quad \prod_{i=1}^n A_i.$$

Заметим, что $A \times B \neq B \times A$; также $A \times B \times C$, $(A \times B) \times C$ и $A \times (B \times C)$ суть разные множества.

Декартово произведение n экземпляров множества A обозначают A^n и называют n -ой декартовой степенью множества A . Естественно полагают $A^1 = A$, а под A^0 понимают некоторое одноэлементное подмножество A . Ясно, что $A^m \times A^n \neq A^{m+n}$.

Определение 2.1. Отношения суть подмножества декартовых произведений множеств.

Число множеств в соответствующем декартовом произведении определяет *местность* или *арность* отношения. Говорят об унарных, бинарных, тернарных, кватернарных и т.д. отношениях. Понятно, что отношение $\rho \subseteq A_1 \times \dots \times A_n$ определяет совокупность n -ок $(a_1, \dots, a_n) \in \rho$, $a_i \in A_i$, $i = 1, \dots, n$.

Определение 2.2. Если ρ — отношение на $A_1 \times \dots \times A_n$, то совокупность всех элементов $a_1 \in A_1$ для которых найдутся такие $a_2 \in A_2, \dots, a_n \in A_n$, что $(a_1, a_2, \dots, a_n) \in \rho$, называют *проекцией отношения ρ на множество A_1* или *первой проекцией*. Аналогично определяют вторые, третьи и т.д. проекции. Символически i -я проекция ρ обозначается $Pr_i \rho$.

Таким образом, i -я проекция отношения состоит из всех элементов, стоящих на i -м месте в n -ках из данного отношения.

Отношения можно рассматривать как предикаты, т.е. функции, принимающие два значения — «истина» (**1**) и «ложь» (**0**), а именно, $\rho(a_1, \dots, a_n)$ истинно, если $(a_1, \dots, a_n) \in \rho$ и ложно в противном случае. Поэтому к отношениям можно применять операции алгебры логики: дизъюнкции (\vee), конъюнкции ($\&$), отрицания (\neg), тождества (\equiv), импликации

(\supset) и др. При чтении соответствующих формул следует иметь в виду, что, поскольку приоритет отношений выше приоритета операций алгебры логики, скобки вокруг отношений, как правило, опускают.

Унарные отношения на некотором множестве определяют те или иные свойства его элементов.

Бинарные отношения на декартовом произведении множеств A и B называют отношениями *между* A и B или *соответствиями* между данными множествами — их называют *базисными*. Заметим, что первое изложение теории бинарных отношений применительно к математической логике дал в 1895 г. Э. Шрёдер. Основы современного систематического изложения данной теории заложены в работах Ж. Риге [30], В. Вагнера [6] и, отчасти, И. Валуце [7].

Для соответствия $\rho \subseteq A \times B$ удобно пользоваться обозначением $a\rho b$, если $(a, b) \in \rho$. Соответствия удобно задавать направленным двудольным графом¹ $\vec{G}(\rho)$, вершинами которого служат элементы A и B , причём, если $a\rho b$, то из вершины, соответствующей $a \in A$, дуга ведёт в вершину, соответствующую $b \in B$. На рис. 2.1 показан пример такого графа для отношения $\{(a_1, b_1), (a_1, b_2)\}$ на $\{a_1, a_2\} \times \{b_1, b_2\}$.

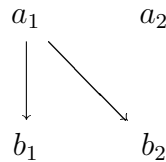


Рис. 2.1: Граф бинарного отношения

Первая проекция соответствия ρ называется его *областью определения*, а вторая — *областью значений*, которые обозначаются $\text{Dom } \rho$ и $\text{Im } \rho$ соответственно. Для $a \in A$ множество $\rho(a) = \{b \in B \mid a\rho b\}$ называется *образом элемента* a при соответствии ρ . Если $X \subseteq A$, то множество $\rho(X) = \bigcup_{x \in X} \rho(x)$ называется *образом множества* X при соответствии ρ .

Поскольку отношения суть подмножества, то для бинарных отношений определена тотальная алгебра над декартовым произведением своих базисных множеств. Ясно, что теоретико-множественные операции, применённые к соответствиям $\alpha, \beta \subseteq A \times B$, для $a \in A, b \in B$ имеют следующие свойства:

- 1) $a(\alpha \cup \beta)b \Leftrightarrow a\alpha b \vee a\beta b \Leftrightarrow (a, b) \in \alpha$ или $(a, b) \in \beta$;
- 2) $a(\alpha \cap \beta)b \Leftrightarrow a\alpha b \& a\beta b \Leftrightarrow (a, b) \in \alpha$ и $(a, b) \in \beta$;
- 3) $a\bar{\alpha}b \Leftrightarrow \neg(a\alpha b) \Leftrightarrow (a, b) \notin \alpha$.

Легко показывается, что

$$\begin{cases} \alpha \subseteq \beta \\ \gamma \subseteq \delta \end{cases} \Rightarrow \begin{cases} \alpha \cup \gamma \subseteq \beta \cup \delta, \\ \alpha \cap \gamma \subseteq \beta \cap \delta \end{cases}$$

(α, β, γ и δ суть соответствия одной и той же пары множеств).

¹Граф называется двудольным, если его вершины могут быть разбиты на два непересекающихся множества, и при таком разбиении ребра соединяют вершины из разных множеств. Если двудольный граф направленный, то дуги (направленные рёбра) исходят из вершин первого множества и входят в вершины второго.

Отношение $\bar{\rho}$ называют *дополнительным* к ρ .

Теперь мы введём две новые операции для бинарных отношений (соответствий): унарную псевдообращения и бинарную произведения.

Определение 2.3. Пусть $\rho \subseteq A \times B$. Операция $\#$ (псевдообращения) соответствия ρ задаёт псевдообратное к нему соответствие $\rho^\# \subseteq B \times A$, определяемое как $b\rho^\#a \Leftrightarrow a\rho b$ для любых $a \in A, b \in B$.

Ясно, что псевдообратное к данному отношению существует всегда. Для псевдообращения часто употребляют также термины *противоположное, обратное, транспонированное, инверсное, симметричное* или *дуальное* отношение и пользуются обозначениями ρ^{-1}, ρ', ρ^d и др. Легко установить следующие свойства псевдообращения относительно теоретико-множественных операций и отношения включения:

$$\begin{aligned} (\rho^\#)^\# &= \rho \quad (\text{инволютивность псевдообращения}), \\ \overline{\rho^\#} &= (\bar{\rho})^\#, \\ \alpha \subseteq \beta &\Rightarrow \alpha^\# \subseteq \beta^\# \quad (\text{монотонность псевдообращения}), \\ (\alpha \cup \beta)^\# &= \alpha^\# \cup \beta^\#, \\ (\alpha \cap \beta)^\# &= \alpha^\# \cap \beta^\#. \end{aligned}$$

Покажем, например, справедливость последнего равенства (a и b — произвольные элементы соответствующих множеств):

$$b(\alpha \cap \beta)^\#a = a(\alpha \cap \beta)b = a\alpha b \& a\beta b = b\alpha^\#a \& b\beta^\#a = b(\alpha^\# \cap \beta^\#)a.$$

Для $\rho \subseteq A \times B$ и $b \in B$ множество $\rho^\#(b) = \{a \in A \mid a\rho b\}$ называется *прообразом элемента b* при соответствии ρ . Если $Y \subseteq B$, то множество $\rho^\#(Y) = \bigcup_{y \in Y} \rho^\#(y)$ называется *прообразом множества Y* .

Определение 2.4. Пусть A, B и C — непустые множества, $\alpha \subseteq A \times B$ и $\beta \subseteq B \times C$. Тогда *произведение* или *умножение* $\alpha \diamond \beta$ соответствий α и β определяется для произвольных $a \in A, c \in C$ как

$$a(\alpha \diamond \beta)c \Leftrightarrow \exists b \underset{B}{(a\alpha b \& b\beta c)}.$$

Часто знак \diamond опускают и вместо $\alpha \diamond \beta$ пишут просто $\alpha\beta$.

Кроме приведённого в определении, имеются ещё два выражения для произведения отношений $\alpha \subseteq A \times B$ и $\beta \subseteq B \times C$:

$$\begin{aligned} \alpha \diamond \beta &= \{ (a, c) \in A \times C \mid \alpha(a) \cap \beta^\#(c) \neq \emptyset \}; \\ \alpha \diamond \beta &= \bigcap_{b \in B} \alpha^\#(b) \times \beta(b). \end{aligned} \tag{2.1}$$

Понятно, что в общем случае произведение соответствий может и не существовать. В случае же существования оно обладает следующими свойствами:

$$\begin{aligned} \alpha(\beta\gamma) &= (\alpha\beta)\gamma \quad (\text{ассоциативность произведения соответствий}), \\ (\alpha\beta)^\# &= \beta^\#\alpha^\#, \\ \left\{ \begin{array}{l} \alpha \subseteq \beta \\ \gamma \subseteq \delta \end{array} \right. &\Rightarrow \alpha\gamma \subseteq \beta\delta \quad (\text{монотонность умножения соответствий}), \\ \alpha(\beta \cup \gamma) &= \alpha\beta \cup \alpha\gamma \quad \text{и} \quad (\alpha \cup \beta)\gamma = \alpha\gamma \cup \beta\gamma, \quad \text{откуда} \\ &(\alpha \cup \beta)(\gamma \cup \delta) = \alpha\gamma \cup \alpha\delta \cup \beta\gamma \cup \beta\delta, \\ \alpha(\beta \cap \gamma) &\subseteq \alpha\beta \cap \alpha\gamma \quad \text{и} \quad (\alpha \cap \beta)\gamma \subseteq \alpha\gamma \cap \beta\gamma. \end{aligned} \tag{2.2}$$

Ассоциативность произведения соответствий следует из ассоциативности логической операции $\&$ и правил её взаимодействия с квантором существования. Докажем справедливость правила $(\alpha\beta)^\# = \beta^\#\alpha^\#$: для произвольных элементов a и c соответствующих множеств имеем

$$c(\alpha\beta)^\#a = a(\alpha\beta)c = \exists b (a\alpha b \& b\beta c) = \exists b (c\beta^\#b \& b\alpha^\#a) = c(\beta^\#\alpha^\#)a.$$

Покажем справедливость свойства монотонности умножения соответствий. Действительно, для произвольных элементов a и c соответствующих множеств имеем

$$a(\alpha\gamma)c = \exists b (a\alpha b \& b\gamma c) \Rightarrow \exists b (a\beta b \& b\delta c) = a(\beta\delta)c.$$

Докажем теперь, что $(\alpha \cap \beta)\gamma \subseteq \alpha\gamma \cap \beta\gamma$. Действительно, для произвольных элементов a и c соответствующих множеств будем иметь

$$\begin{aligned} a[(\alpha \cap \beta)\gamma]c &= \exists b (a(\alpha \cap \beta)b \& b\gamma c) = \exists b (a\alpha b \& a\beta b \& b\gamma c) = \\ &= \exists b ((a\alpha b \& b\gamma c) \& (a\beta b \& b\gamma c)) \Rightarrow \exists x (a\alpha x \& x\gamma c) \& \exists y (a\beta y \& y\gamma c) = \\ &= a(\alpha\gamma)c \& a(\beta\gamma)c = a(\alpha\gamma \cap \beta\gamma)c. \end{aligned}$$

Соотношение $\alpha(\beta \cap \gamma) \subseteq \alpha\beta \cap \alpha\gamma$ доказывается аналогично.

Существует удобный способ представления соответствий конечных множеств в виде $(0,1)$ -матриц. Пусть ρ — соответствие между $A = \{a_1, \dots, a_m\}$ и $B = \{b_1, \dots, b_n\}$. Зафиксируем указанный порядок следования элементов в множествах A и B . Тогда матрица $M(\rho)$ отношения ρ имеет размеры $m \times n$ и её элемент r_{ij} равен 1, если $a_i\rho b_j$ и 0 иначе.

Множество всех $(0,1)$ -матриц размера $m \times n$ будем обозначать $\mathcal{M}_{m \times n}$, опуская индекс, когда соответствующий размер подразумевается. Во введённом множестве выделяются матрица, у которой все элементы равны 1 и матрица, у которой все элементы равны 0. Их называют *универсальной* и *нуль-матрицей* и обозначают I и O соответственно. К любой матрице из \mathcal{M} можно поэлементно применить логическую операцию \neg , а к матрицам одинакового размера — логические операции \vee и $\&$ по правилам алгебры $\mathbf{2}$ (полагая $1 = \mathbf{1}$ и $0 = \mathbf{0}$). Легко видеть, что АС $\langle \mathcal{M}_{m \times n}, \vee, \&, \neg, O, I \rangle$ является булевой алгеброй, изоморфной в нашем случае тотальной алгебре $\mathcal{P}(A \times B)$. Изоморфизм следует из следующих равенств:

$$M(\alpha \cup \beta) = M(\alpha) \vee M(\beta); \quad M(\alpha \cap \beta) = M(\alpha) \& M(\beta); \quad M(\bar{\alpha}) = \neg M(\alpha).$$

Понятно, что матрица $M(\alpha^\#) \in \mathcal{M}_{n \times m}$ получается из матрицы $M(\alpha) \in \mathcal{M}_{m \times n}$ транспонированием.

Пусть $M_1 \in \mathcal{M}_{m \times n}$, $M_2 \in \mathcal{M}_{n \times k}$. Определим *произведение* $M_1 \times M_2 \in \mathcal{M}_{m \times k}$ данных матриц как обычное матричное произведение с заменой операции суммирования на \vee , а операции умножения — на $\&$. Обычным образом вводится натуральная степень M^n матрицы M как результат перемножения $n \in \mathbb{N}$ экземпляров данной матрицы. Легко показывается, что если $\alpha \subseteq A \times B$ и $\beta \subseteq B \times C$, где A, B, C — конечные множества, то справедливо равенство

$$M(\alpha \diamond \beta) = M(\alpha) \times M(\beta)$$

и поэтому $M(\alpha^n) = M^n(\alpha)$.

Определим теперь понятия смежных классов соответствия и его фактормножества.

Определение 2.5. Для соответствия $\rho \subseteq A \times B$ прообразы $\rho^\#(b)$ элементов $b \in B$ называются *смежными классами A по ρ* , а образы элементов $a \in A$ — *смежными классами B по $\rho^\#$* .

Фактормножествами A/ρ и $B/\rho^\#$ называются множества, элементами которых являются смежные классы A по ρ и B по $\rho^\#$ соответственно.

Таким образом, для $\rho \subseteq A \times B$ имеем $A/\rho = \{\rho^\#(b) \mid b \in B\}$, $B/\rho^\# = \{\rho(a) \mid a \in A\}$, и, например, элементы $a_1, a_2 \in A$ принадлежат одному смежному классу A по ρ , если

$$\exists b \in B (a_1 \rho b = a_2 \rho b) \quad (2.3)$$

Легко заметить, что объединение всех смежных классов A по ρ есть область определения $\text{Dom}(\rho) \subseteq A$ (возможно, понятно, и строгое включение).

Говорят, что совокупность \mathcal{C} непустых подмножеств множества A образует его *покрытие*, если объединение всех подмножеств из \mathcal{C} совпадает с A . При этом подмножества из \mathcal{C} могут иметь непустые попарные пересечения. Ясно, что совокупность A_1, A_2, \dots всех смежных классов A по ρ образует покрытие множества $\text{Dom}(\rho)$:

$$\text{Dom}(\rho)A = A_1 \cup A_2 \cup \dots \subseteq A.$$

Пример 2.1. Пусть $A = \{0, 1, 2, 3\}$, $B = \{a, b, c\}$ и на $A \times B$ задано соответствие $\rho = \{(0, a), (0, b), (1, a), (2, b)\}$, граф $\vec{G}(\rho)$ которого показан на рис. 2.2. Здесь

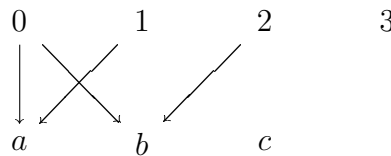


Рис. 2.2: К примеру 2.1

$\text{Dom}(\rho) = \{0, 1, 2\} \subset A$, а A/ρ составляют смежные классы $\{0, 1\}$ и $\{0, 2\}$, имеющие общий элемент 0 и $\{0, 1\} \cup \{0, 2\} = \text{Dom}(\rho)$.

2.2 Однородные отношения

Отношение $\rho \subseteq A^2$ называется *бинарным на A* или *однородным*. Множество всех бинарных на A отношений обозначим $\mathcal{R}(A)$.

Однородные отношения $\rho \in \mathcal{R}(A)$ удобно (особенно в случае, когда A — конечное множество с небольшим числом элементов) изображать в виде ориентированного графа $\vec{G}(\rho)$, вершинам которого соответствуют элементы A , а дуга ведёт из x в y , если $x\rho y$. Если $x\rho x$, то у вершины x рисуют петлю. Когда $x\rho y$ и $y\rho x$, вместо пары дуг противоположной направленности между x и y рисуют (ненаправленное) ребро. На рис. 2.3 показан пример такого графа для отношения $\{(1, 3), (1, 4), (4, 2), (2, 4)\}$ на множестве $\{1, 2, 3, 4\}$.

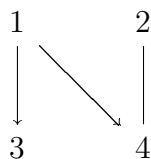


Рис. 2.3: Граф однородного отношения

Понятие класса смежности переносится на однородные отношения: в определении (2.5) полагают $B = A$.

Поскольку в $\mathcal{R}(A)$ произведение всегда определено, то в силу ассоциативности произведения соответствий алгебра $\langle \mathcal{R}(A), \diamond \rangle$ есть полугруппа. Если $\rho \in \mathcal{R}(A)$ и $\emptyset \neq B \subseteq A$, то отношение $\rho \cap B^2$ называют *сужением* или *ограничением отношения ρ на подмножество B* и обозначают $\rho|_B$.

Для натурального k вводят естественное обозначение $\alpha^k = \alpha \diamond \dots \diamond \alpha$ (k раз, $\alpha^1 = \alpha$). Разумеется,

$$\alpha \subseteq \beta \Rightarrow \alpha^k \subseteq \beta^k, \quad k = 1, 2, \dots$$

Покажем, что

$$(\alpha \cap \beta)^2 \subseteq \alpha^2 \cap \beta^2. \quad (2.4)$$

Действительно, если $\alpha, \beta \in \mathcal{R}(A)$, то для любых $a, b \in A$ получим

$$\begin{aligned} a[(\alpha \cap \beta)(\alpha \cap \beta)]c &= \exists b [a(\alpha \cap \beta)b \& b(\alpha \cap \beta)c] = \\ &= \exists x (a\alpha x \& a\beta x \& x\alpha b \& x\beta c) \Rightarrow \exists x (a\alpha x \& x\alpha b) \& \exists y (a\beta y \& y\beta c) = \\ &= a\alpha^2 c \& a\beta^2 c = a(\alpha^2 \cap \beta^2)c. \end{aligned}$$

Отношение $\sigma_\alpha = \frac{\alpha \cup \alpha^\sharp}{\alpha \cup \alpha^\sharp} = \alpha \cup \alpha^\sharp$ называют *отношением сравнимости*, а $\iota_\alpha = A^2 \setminus \sigma_\alpha = \alpha \cup \alpha^\sharp = \bar{\alpha} \cap \bar{\alpha}^\sharp$ — *отношением несравнимости* для отношения $\alpha \in \mathcal{R}(A)$. Если $a\sigma_\alpha b$ [$a\iota_\alpha b$], то говорят, что элементы a и b *сравнимы* [соответственно, *несравнимы*].

Проиллюстрируем действие введённых операций на однородные отношения.

Пример 2.2. Рассмотрим отношение $\alpha = <$ (строго меньше) на \mathbb{N} .

α^\sharp : Имеем $m <^\sharp n \Leftrightarrow n < m \Leftrightarrow m > n$. Таким образом, псевдообращением отношения «строго меньше» будет отношение «строго больше».

σ_α : Поскольку $m < n \vee n < m \Leftrightarrow m \neq n$, то отношением сравнимости для отношения «строго меньше» будет отношение неравенства.

ι_α : Отношением несравнимости для отношения «строго меньше» будет отношение равенства.

α^2 : Имеем $m <^2 n \Leftrightarrow \exists x \underset{\mathbb{N}}{(m < x \& x < n)} \Leftrightarrow m + 1 < n$. Понятно, что $m <^k n \Leftrightarrow m + k - 1 < n$ для $k \geq 1$.

$\alpha \diamond \alpha^\sharp$: Имеем $m(< \diamond >)n \Leftrightarrow \exists x \underset{\mathbb{N}}{(m < x \& x > n)} \Leftrightarrow \exists x \underset{\mathbb{N}}{(x > \max\{m, n\})} \Leftrightarrow \mathbf{1}$, т.е. отношение $< \diamond >$ на множестве натуральных чисел истинно всегда.

$\alpha^\sharp \diamond \alpha$: Имеем

$$\begin{aligned} m(> \diamond <)n &\Leftrightarrow \exists x \underset{\mathbb{N}}{(m > x \& x < n)} \Leftrightarrow \\ &\Leftrightarrow \exists x \underset{\mathbb{N}}{(x < \min\{m, n\})} \Leftrightarrow \begin{cases} \mathbf{1}, & \text{если } \min\{m, n\} > 1, \\ \mathbf{0}, & \text{иначе.} \end{cases} \end{aligned}$$

Мы видим, что, вообще говоря, $\alpha\beta \neq \beta\alpha$. При $\alpha\beta = \beta\alpha$ соответствующие отношения называются *перестановочными*.

Определение 2.6. Однородное на множестве A отношение ρ называется:

(∇) *аморфным*, если $\rho = A^2$.

(\emptyset) *пустым*, если $\rho = \emptyset$.

Аморфное отношение вместе с пустым называют *несобственными* отношениями на данном множестве. Ясно, что для любого отношения ρ имеет место $\emptyset \subseteq \rho \subseteq \nabla$.

(Δ) *диагональным* или *единичным*, если $xry \Leftrightarrow x = y$. Здесь и далее x, y и z — произвольные элементы множества A .

По определению для произвольного однородного отношения ρ полагают $\rho^0 = \Delta$. Очевидно $\rho = \rho \Delta = \Delta \rho$.

(F) *полным*, если $\rho \cup \rho^\# = \nabla$ (т.е. $xry \vee xr^\#y$, или из любых двух элементов A по крайней мере один находится в отношении ρ с другим).

(R) *рефлексивным*, если $\Delta \subseteq \rho$ (что означает xrx).

(AR) *антирефлексивным*, если $\rho \cap \Delta = \emptyset$ (что означает $x\bar{r}x$).

(S) *симметричным*, если $\rho^\# \subseteq \rho$. Из $(\rho^\#)^\# = \rho$ сразу следует, что симметричность отношения можно задать равенством $\rho^\# = \rho$ (т.е. $xry = yrx$).

(AS) *антисимметричным*, если $\rho \cap \rho^\# \subseteq \Delta$, (т.е. $xry \& yrx \Rightarrow x = y$).

(NS) *асимметричным* или *несимметричным*, если $\rho \cap \rho^\# = \emptyset$ (т.е. $x\bar{r}y \vee y\bar{r}x$, или из двух соотношений ρ и $\rho^\#$ хотя бы одно не выполнено).

(T) *транзитивным*, если $\rho^2 \subseteq \rho$, (что означает $xry \& yrz \Rightarrow xrz$).

Поскольку $\rho^2 \subseteq \rho \Rightarrow \rho^3 \subseteq \rho^2 \subseteq \rho$, то для транзитивного отношения ρ имеем $\rho^n \subseteq \rho$, $n = 1, 2, \dots$

Пустое отношение \emptyset обычно также считают транзитивным.

(C) *содержащим цикл*, если для некоторых x и $k > 1$ справедливо xr^kx ; в противном случае говорят, что ρ — отношение *без циклов*.

В обозначениях однородных отношений, когда это необходимо, подстрочным символом указывают множество, на котором они определены (например, ∇_A). Ясно, что Δ_A — единица в полугруппе однородных отношений и АС $\langle \mathcal{R}(A), \diamond, \Delta_A \rangle$ есть моноид².

Почти очевидна следующая

Теорема 2.1 (о сохранении свойств отношения при сужении). Пусть $\emptyset \neq B \subseteq A$ и $\rho \in \mathcal{R}(A)$. Тогда, если ρ обладает одним из следующих свойств: (F), (R), (AR), (S), (AS), (T) — это свойство выполняется и для сужения $\rho|_B$.

Очевидно, полное отношение рефлексивно.

Теорема 2.2. Симметричное и транзитивное отношение на множестве A , первая проекция которого совпадает с A , рефлексивно.

Доказательство. Пусть ρ — однородное на A отношение, обладающее указанными свойствами. $Pr_1\rho = A$ означает существование для любого x такого y , что xry , откуда по симметричности и yrx . Таким образом, для произвольного x справедливо

$$\exists y (xry \& yrx) \Leftrightarrow xr^2x \Rightarrow xrx,$$

что и означает $\Delta \subseteq \rho$. □

Замечание. В силу симметричности $Pr_1\rho = A$ эквивалентно $Pr_2\rho = A$.

Теорема 2.3 (свойства произведения отношений). Пусть α, β и γ — однородные отношения. Тогда справедливы следующие утверждения.

1. Если β рефлексивно, то $\alpha \subseteq \alpha\beta$ и $\alpha \subseteq \beta\alpha$. Отсюда $\Delta \subseteq \alpha^n$ для рефлексивного α , $n = 0, 1, 2, \dots$
2. Если α рефлексивно и транзитивно, то $\alpha^n = \alpha$, $n = 1, 2, \dots$
3. Если $\alpha, \beta \subseteq \gamma$ и γ транзитивно, то $\alpha\beta \subseteq \gamma$.

²Понятно, что ни отношение $\rho\rho^\#$, ни $\rho^\#\rho$ могут не быть равными единичному. Это объясняет выбор термина “псевдообратное” для отношения $\rho^\#$.

Доказательство.

1. Если β рефлексивно, то $\alpha = \alpha \Delta \subseteq \alpha\beta$ и аналогично для другого включения. Второе утверждение следует из первого при $\alpha = \beta$ по монотонности произведения соответствий.
2. Если $\alpha^2 \subseteq \alpha$ и α рефлексивно, то из предыдущего $\alpha \subseteq \alpha^2$, т.е. $\alpha = \alpha^2$, откуда и следует требуемое.
3. Для транзитивного γ имеем $\alpha\beta \subseteq \gamma\gamma = \gamma^2 \subseteq \gamma$. □

Определение 2.7. Однородное отношение ρ на множестве A называется *стабильным относительно операции f местности n* на A , если при $n > 0$ для любых элементов $a_1, a_1', \dots, a_n, a_n' \in A$ справедливо

$$\bigotimes_{i=1}^n (a_i \rho a_i') \Rightarrow f(a_1, \dots, a_n) \rho f(a_1', \dots, a_n'),$$

а при $n = 0$ — ρ рефлексивно.

Стабильность отношения означает, что если наборы аргументов функции находятся в данном отношении, то и результаты операции также находятся в этом отношении.

Рассмотрим стабильность “положительных” и “отрицательных” свойств отношений относительно основных теоретико-множественных операций и специфических операций над отношениями.

Теорема 2.4 (о стабильности “положительных” свойств отношений). *Для однородных отношений*

- 1) рефлексивность стабильна относительно $\cup, \cap, \#$ и \diamond ;
- 2) симметричность стабильна относительно $\bar{}, \cup, \cap$ и $\#$, а относительно \diamond — если и только если отношения перестановочны;
- 3) транзитивность стабильна относительно \cap и $\#$, а относительно \diamond — если отношения перестановочны.

Доказательство.

1. Первые три свойства очевидны. Стабильность рефлексивности отношений относительно произведения следует из п. 1 теоремы 2.3 о свойствах произведения отношений.
2. Свойство $\overline{\rho^\#} = (\overline{\rho})^\#$ влечёт стабильность симметричности относительно теоретико-множественной операции дополнения.

Пусть α, β — однородные отношения и $\alpha^\# = \alpha, \beta^\# = \beta$. Для объединения и пересечения имеем

$$(\alpha \cup \beta)^\# = \alpha^\# \cup \beta^\# = \alpha \cup \beta \quad \text{и} \quad (\alpha \cap \beta)^\# = \alpha^\# \cap \beta^\# = \alpha \cap \beta.$$

Симметричность отношения означает его стабильность относительно операции псевдообращения.

Для произведения симметричных отношений α и β имеем:

- если $\alpha\beta = \beta\alpha$, то $(\alpha\beta)^\# = \beta^\#\alpha^\# = \beta\alpha = \alpha\beta$;
- если $\alpha\beta$ симметрично, то $\alpha\beta = (\alpha\beta)^\# = \beta^\#\alpha^\# = \beta\alpha$.

3. Пусть α, β — однородные отношения и $\alpha^2 \subseteq \alpha, \beta^2 \subseteq \beta$.

Сразу имеем $\alpha^2 \cap \beta^2 \subseteq \alpha \cap \beta$, а (2.4) обеспечивает $(\alpha \cap \beta)^2 \subseteq \alpha^2 \cap \beta^2$, откуда $(\alpha \cap \beta)^2 \subseteq \alpha \cap \beta$.

Для псевдообращения имеем

$$\alpha^2 = \alpha\alpha \subseteq \alpha \Leftrightarrow (\alpha\alpha)^\# \subseteq \alpha^\# \Leftrightarrow \alpha^\#\alpha^\# \subseteq \alpha^\# \Leftrightarrow (\alpha^\#)^2 \subseteq \alpha^\#.$$

Для произведения отношений, если $\alpha\beta = \beta\alpha$, то

$$(\alpha\beta)^2 = \alpha\beta\alpha\beta = \alpha\alpha\beta\beta = \alpha^2\beta^2 = \alpha\beta. \quad \square$$

Теорема 2.5 (о стабильности “отрицательных” свойств отношений). Для однородных отношений α и β

- 1) антирефлексивность стабильна относительно \cup, \cap и $^\#$; а относительно произведения $\alpha\beta$ — если и только если $\alpha \cap \beta^\# = \emptyset$;
- 2) антисимметричность стабильна относительно \cap и $^\#$;
- 3) асимметричность стабильна относительно \cap и $^\#$; а относительно \cup — если и только если $\alpha \cap \beta^\# = \alpha^\# \cap \beta = \emptyset$.

Доказательство.

1. Стабильность антирефлексивности относительно $\cup, \cap, ^\#$ очевидна.

Антирефлексивность произведения $\alpha\beta$ отношений α и β означает, что ни для одного элемента a не найдётся элемента x с одновременной справедливостью ax и $x\beta a$. Но это означает ложность $a(\alpha \cap \beta^\#)x$ для всех a и x , что эквивалентно требуемому.

2. Стабильность антисимметричности ($\alpha \cap \alpha^\# = \Delta$) относительно псевдообращения очевидна, а относительно пересечения её доказывают равенства

$$(\alpha \cap \beta) \cap (\alpha \cap \beta)^\# = \alpha \cap \beta \cap \alpha^\# \cap \beta^\# = (\alpha \cap \alpha^\#) \cap (\beta \cap \beta^\#) \subseteq \Delta \cap \Delta = \Delta.$$

3. Стабильность асимметричности ($\rho \cap \rho^\# = \emptyset$) относительно $^\#$ очевидна.

Для пересечения имеем

$$(\alpha \cap \beta) \cap (\alpha \cap \beta)^\# = \alpha \cap \beta \cap \alpha^\# \cap \beta^\# = (\alpha \cap \alpha^\#) \cap (\beta \cap \beta^\#) = \emptyset.$$

Для объединения:

$$\begin{aligned} (\alpha \cup \beta) \cap (\alpha \cup \beta)^\# &= (\alpha \cup \beta) \cap (\alpha^\# \cup \beta^\#) = \\ &= (\alpha \cap \alpha^\#) \cup (\beta \cap \beta^\#) \cup (\alpha \cap \beta^\#) \cup (\beta \cap \alpha^\#) = \\ &= (\alpha \cap \beta^\#) \cup (\beta \cap \alpha^\#). \end{aligned}$$

Это выражение будет равно \emptyset если и только если $\alpha \cap \beta^\# = \alpha^\# \cap \beta = \emptyset$. \square

Очевидно, на n -элементном множестве определены 2^{n^2} всевозможных однородных отношений, из которых 2^{n^2-n} рефлексивных. Для числа транзитивных отношений не известна общей формулы. Значения $u(n)$, $r(n)$ и $t(n)$ числа, соответственно, всевозможных, рефлексивных и транзитивных однородных отношений на n -элементном множестве для первых значений n приведены в нижеследующей таблице.

n	1	2	3	4	5	6	7
$u(n)$	2	16	512	6 5536	33 554 432	$\approx 6,87 \cdot 10^{10}$	$\approx 5,63 \cdot 10^{14}$
$r(n)$	1	4	64	4 096	104 8576	1 073 741 824	4 398 046 511 104
$t(n)$	2	13	171	3 994	15 4303	9 415 189	878 222 530

Различные встречающиеся в приложениях отношения обладают теми или иными из указанных выше элементарных свойств. Например, однородное антирефлексивное и антисимметричное отношение называют отношением *предпочтения* (иногда предполагая у него и наличие свойства транзитивности); оно играет важную роль в теориях выбора, статистических решений, стратегических игр и др. Ниже в п. 2.4 будет рассмотрено отношение толерантности, обладающее свойствами рефлексивности и антисимметричности и используемое, например, в теории распознавания образов. Там важную роль играет понятие близости объектов, являющееся толерантностью.

Исключительную роль в математике и приложениях играет отношение эквивалентности.

2.3 Отношение эквивалентности

Определение 2.8. Однородные рефлексивные, симметричные и транзитивные отношения называют *отношениями эквивалентности*.

Ясно, что аморфное ∇ и диагональное Δ отношения являются эквивалентностями. В то же время, эквивалентность элементов какого-либо множества, вообще говоря, не означает их тождества. Эквивалентностями являются, например, отношение параллельности на множестве прямых обычного пространства (если считать прямую параллельной самой себе), отношение подобия геометрических фигур, отношение равенства по модулю n целых чисел и др.

Отношение эквивалентности обычно будем называть просто эквивалентностью и часто обозначать знаком \sim . Согласно определению

$$\Delta \subseteq \sim = \sim^\# = \sim^2$$

(второе равенство в силу п. 2 теоремы 2.3 следует из рефлексивности \sim). Множество всех эквивалентностей на (непустом) множестве A будем обозначать $\mathcal{E}(A)$.

Для данной эквивалентности \sim на множестве A каждому $a \in A$ можно сопоставить множество $[a]_\sim$ эквивалентных ему элементов — *классов эквивалентности* или *смежных классов*: $[a]_\sim = \{x \in A \mid x \sim a\}$. Ясно, что это суть смежные классы по определению (2.5) с учетом однородности и свойств отношения эквивалентности. Если эквивалентность фиксирована, то смежный класс элемента a обозначаем $[a]$.

Формирование смежных классов происходит в ходе выполнения т.н. операции *абстракции отождествления* по данной эквивалентности, при которой отвлекаются от индивидуальных характеристик элементов, выделяя лишь их общность. Понятно, что при этом каждый $x \in A$ попадает в один и только один класс эквивалентности, и классы эквивалентности или совпадают, или не пересекаются, накрывая в совокупности всё множество A .

Говорят, что совокупность $\mathcal{D} = \{A_1, A_2, \dots\}$ непустых подмножеств множества A образует его *разбиение*, если объединение всех подмножеств из \mathcal{D} совпадает с A и все они попарно не пересекаются:

$$A = A_1 + A_2 + \dots, \quad A_i \cap A_j = \emptyset \text{ при } i \neq j \quad (2.5)$$

(использование знака $+$ вместо \cup подчёркивает, что рассматривается именно разбиение множества). Элементы A_1, A_2, \dots разбиения \mathcal{D} называют *блоками*. Конечное разбиение $A = A_1 + A_2 + \dots + A_k$ обычно записывают в виде $(A_1 | A_2 | \dots | A_k)$.

Пусть задано разбиение множества A . Тогда можно определить отношение эквивалентности на A так, что элементы разбиения A будут смежными классами данной эквивалентности. Ясно, что такая эквивалентность единственна. Таким образом, между отношением эквивалентности и разбиениями существует взаимно-однозначное соответствие.

Приведённые рассуждения можно оформить в виде простой, но очень важной теоремы.

Теорема 2.6 (о классах эквивалентности). Пусть A — непустое множество. Если на A задана эквивалентность, то множество классов эквивалентности образует разбиение A . И обратно, если задано разбиение A на классы, то можно единственным образом определить эквивалентность \sim на A так, что для любой пары a, b элементов A $a \sim b \Leftrightarrow$ « a и b находятся в одном классе разбиения».

«Теорема о классах эквивалентности находит в математике широчайшее применение, и её по праву можно считать одной из главных (а то и самой главной) теоремой»³. Она позволяет задавать эквивалентности разбиениями, что мы часто будем делать.

Пусть дано разбиение \mathcal{D} непустого множества A на классы $(A_1 | A_2 | \dots)$. Замкнём \mathcal{D} относительно основных теоретико-множественных операций, т.е. построим \mathcal{D} до множества S так, чтобы операции $\cup, \cap, -$ стали устойчивы на S . Тогда S будет алгеброй подмножеств множества A , причём её атомами будут A_1, A_2, \dots .

Эквивалентность на конечном множестве можно задавать $(0,1)$ -матрицей (см. п. 2.1). Ясно, что соответствующая матрица будет симметрична и содержать 1 на главной диагонали, но не каждая такая матрица будет задавать эквивалентность.

Определение 2.9. Множество, элементами которого являются классы эквивалентности множества A по отношению эквивалентности \sim называется *фактормножеством* и обозначается A/\sim .

Пример 2.3. 1. Если A — множество зёрен, насыпанных в мешки, и для зёрен a и b положить $a \sim b$, если они лежат в одном мешке, то классами эквивалентности являются множества зёрен, лежащих в одном мешке, а фактормножеством A/\sim — множество мешков.

2. Если W — множество слов русского языка и для слов u и v положить $u \sim v$, если они начинаются с одной и той же буквы (в русском языке 33 буквы), то классами эквивалентности будут множества слов, начинающихся на данную букву, а фактормножеством W/\sim — множество соответствующих букв (заметим, что $|W/\sim| = 31$).

Исследуем теперь стабильность эквивалентности. Разумеется, эквивалентность не стабильна относительно взятия дополнения, поскольку дополнение эквивалентности не содержит диагонального отношения. С другой стороны, эквивалентность стабильна относительно операции перехода к псевдообратному отношению: это следует из теоремы 2.4 о стабильности «положительных» свойств отношений. Из этой же теоремы вытекает

Теорема 2.7 (стабильность пересечения эквивалентностей). Отношение эквивалентности стабильно относительно пересечения.

Из теоремы следует, что пересечение эквивалентностей из произвольной непустой (возможно бесконечной) совокупности есть эквивалентность.

Эквивалентности α и β на некотором множестве назовём *когерентными*, если для любой пары смежных классов по α и по β соответственно справедливо утверждение «либо один из данных классов лежит в другом, либо они не пересекаются».

³ Успенский В.А. Что такое аксиоматический метод. — Ижевск, 2000.

Теорема 2.8 (стабильность объединения эквивалентностей). Пусть α и β — эквивалентности. Тогда

- 1) объединение $\alpha \cup \beta$ является эквивалентностью, если и только если α и β когерентны;
- 2) если $\alpha \cup \beta$ — эквивалентность, то $\alpha \cup \beta = \alpha\beta$.

Доказательство.

1. В силу теоремы 2.4 достаточно показать указанный критерий относительно транзитивности.

(\Leftarrow) Пусть α и β — когерентные эквивалентности на множестве A . Рассмотрим всевозможные образы $\{b \in A \mid a(\alpha \cup \beta)b\}$ по всем элементам $a \in A$. Легко видеть, что при указанном условии данные подмножества A либо совпадают, либо не пересекаются и их объединение совпадает A . Таким образом, они образуют разбиение множества A , задавая эквивалентность не нём.

(\Rightarrow) Пусть теперь данные эквивалентности не когерентны, т.е. найдутся смежные классы $[a]_\alpha$ и $[b]_\beta$ не лежащие один в другом и содержащие общий элемент c . Можно считать, что $a \in [a]_\alpha \setminus [b]_\beta$ и $b \in [b]_\beta \setminus [a]_\alpha$ (см. рис. 2.4). Пары (a, c) и (c, b)

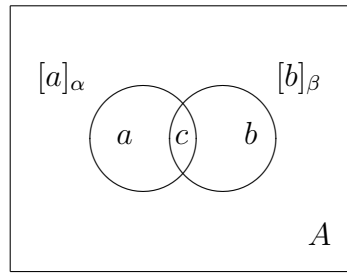


Рис. 2.4: К доказательству теоремы 2.8

содержатся в $\alpha \cup \beta$. Если бы это отношение было эквивалентностью, то оно, в силу транзитивности, содержало бы и пару (a, b) . Последнее означает справедливость либо $a\alpha b$, либо $a\beta b$. Это, однако, не имеет места и, следовательно, $\alpha \cup \beta$ — не эквивалентность.

2. Пусть α , β и $\alpha \cup \beta$ — эквивалентности. Тогда по теореме 2.3 о свойствах произведения отношений получим:

из п. 1) — поскольку α и β рефлексивны, то $\alpha \subseteq \alpha\beta$ и $\beta \subseteq \alpha\beta$, откуда $\alpha \cup \beta \subseteq \alpha\beta$ по монотонности объединения;

из п. 3) — поскольку $\alpha \subseteq \alpha \cup \beta$ и $\beta \subseteq \alpha \cup \beta$, а $\alpha \cup \beta$ транзитивно, то $\alpha\beta \subseteq \alpha \cup \beta$.

Следовательно, $\alpha \cup \beta = \alpha\beta$. □

Пример 2.4. Пусть α и β — эквивалентности на множестве $A = \{a, b, c, d\}$ со смежными классами $A/\alpha = (a \mid b \mid c, d)$ и $A/\beta = (a, b \mid c \mid d)$.

1. Тогда $\alpha \cup \beta$ есть эквивалентность и $A/(\alpha \cup \beta) = (a, b \mid c, d)$.
2. Возьмём два элемента из одного класса эквивалентности по $\alpha \cup \beta$, например, a и b . Тогда справедливо $a(\alpha\beta)b$, поскольку справедливы отношения $a\alpha b$ и $b\beta b$.

Теперь возьмём два элемента из разных классов эквивалентности по $\alpha \cup \beta$, например, a и c . Тогда $a(\alpha\beta)c$ несправедливо, поскольку не существует элемента x такого, что отношения $a\alpha x$ и $x\beta c$ справедливы одновременно.

Мы уже отмечали, что отношения могут быть, а могут и не быть перестановочными. Покажем, это остаётся справедливым и для эквивалентностей.

Пример 2.5. 1. Пусть α и β — эквивалентности на множестве $A = \{a, b, c, d\}$ со смежными классами $D_\alpha = (a, b \mid c, d)$ и $D_\beta = (a, c \mid b, d)$ соответственно. Тогда $\alpha \cup \beta = \nabla = \alpha\beta = \beta\alpha$ и α и β перестановочны.

2. Пусть α и β — эквивалентности на множестве $A = \{a, b, c\}$ со смежными классами $D_\alpha = (a, b \mid c)$ и $D_\beta = (a \mid b, c)$ соответственно. Тогда $a(\alpha\beta)c$, но неверно, что $a(\beta\alpha)c$, и данные эквивалентности не перестановочны. Отметим, что при этом ни $\alpha\beta$, ни $\beta\alpha$ не являются эквивалентностями.

Следствием теоремы теоремы 2.3 является

Теорема 2.9 (стабильность произведения эквивалентностей). *Произведение эквивалентностей будет эквивалентностью, если и только если они перестановочны.*

Объединяя утверждения данной теоремы и теоремы 2.8 (об объединении эквивалентностей) для перестановочных эквивалентностей α и β и замечая, что объединение двух множеств есть наименьшее множество их содержащее, получаем, что $\alpha \cup \beta = \alpha\beta$, т.е. справедлива

Теорема 2.10 (произведение перестановочных эквивалентностей). *Для перестановочных эквивалентностей произведение является наименьшей эквивалентностью, их содержащей.*

Укажем теперь способ построения наименьшей эквивалентности, содержащей данное отношение. Оно использует понятие замыкания, в данном случае — замыкания отношения. Вообще, понятие замыкания (неформально — присоединения некоторого количества новых объектов к данному множеству) является фундаментальным и часто используется в различных областях математики.

Определение 2.10. *Оператором замыкания на непустом множестве M называют отображение C множества всех подмножеств M в себя, обладающее для всех $X, Y \subseteq M$ следующими свойствами:*

1. $X \subseteq C(X)$ — рефлексивность,
2. $X \subseteq Y \Rightarrow C(X) \subseteq C(Y)$ — монотонность,
3. $C(C(X)) = C(X)$ — идемпотентность.

Множество X называется *замкнутым*, если $C(X) = X$.

Если S — некоторое свойство элементов множества A , то *наименьшим подмножеством, обладающим свойством S* называется пересечение всех подмножеств множества A , элементы которых обладают данным свойством.

Определение 2.11. *Наименьшее рефлексивное отношение ρ^r , содержащее отношение ρ , называется рефлексивным замыканием ρ . Наименьшее симметричное отношение ρ^s , содержащее отношение ρ , называется симметричным замыканием ρ . Наименьшее транзитивное отношение ρ^t , содержащее отношение ρ , называется транзитивным замыканием ρ . Наименьшая эквивалентность ρ^e , содержащая отношение ρ , называется эквивалентным замыканием ρ .*

Легко видеть, что получение введённые отношения–замыкания данного можно представить как результат действия соответствующих операторов замыкания.

Рефлексивное и симметричные замыкания данного отношения легко строятся. Очевидно, что

$$\rho^r = \rho \cup \Delta \quad \text{и} \quad \rho^s = \rho \cup \rho^\#.$$

Введём обозначение $\rho^+ \triangleq \bigcup_{n=1}^{\infty} \rho^n$. Очевидно, справедливость $a\rho^+b$ означает существование таких элементов x_1, \dots, x_n ($n \geq 1$) соответствующего множества, что

$$a\rho x_1 \& x_1\rho x_2 \& \dots \& x_n\rho b.$$

Ясно, что ρ^+ всегда транзитивно и из $\alpha \subseteq \beta$ следует $\alpha^+ \subseteq \beta^+$.

Утверждение 2.1. Для произвольного однородного отношения ρ справедливо $\rho^t = \rho^+$.

Доказательство. Если отношение ρ транзитивно, то для любого натурального n имеем $\rho^n \subseteq \rho$, откуда $\rho = \rho^+$. Поэтому применяя операцию $+$ к $\rho \subseteq \rho^t \subseteq \rho^+$, получим $\rho^+ \subseteq \rho^t \subseteq \rho^+$, что означает $\rho^t = \rho^+$. \square

Теперь можно конструктивно определить эквивалентное замыкание отношения. Во-первых, очевидно,

$$(\rho^t)^r = (\rho^r)^t \triangleq \rho^* = \Delta \cup \rho^+ = \bigcup_{n=0}^{\infty} \rho^n.$$

для любого $\rho \in \mathcal{R}(A)$. Отношение ρ^* называют рефлексивно-транзитивным замыканием однородного отношения ρ .

Во-вторых, из определения эквивалентного замыкания также вытекает, что

$$(\rho^\#)^e = \rho^e, \quad (\rho^2)^e = \rho^e.$$

Введём обозначение $\rho^\circ \triangleq (\rho \cup \rho^\# \cup \Delta)^t$. Ясно, что ρ° всегда есть эквивалентность.

Утверждение 2.2. Для произвольного однородного отношения ρ справедливо $\rho^e = \rho^\circ$.

Доказательство. Для эквивалентности ρ , очевидно, имеем $\rho^\circ = \rho$. Поэтому применяя операцию $^\circ$ к $\rho \subseteq \rho^e \subseteq \rho^\circ$, получим $\rho^\circ \subseteq \rho^e \subseteq \rho^\circ$, что означает $\rho^e = \rho^\circ$. \square

Замыкание совокупности отношений есть замыкание их объединения.

Теорема 2.11. Эквивалентное замыкание совокупности эквивалентностей совпадает с объединением всевозможных произведений этих эквивалентностей.

Доказательство. Пусть R — совокупность эквивалентностей и E — объединение всевозможных их произведений. Тогда для любой эквивалентности \sim из R согласно п. 1 теоремы 2.3 о свойствах произведения отношений имеем $\sim \subseteq E$, а согласно её п. 3 — $E \subseteq \sim$, откуда и следует требуемое. \square

Следствия. 1. Эквивалентное замыкание $\{\alpha, \beta\}^e$ двух эквивалентностей α и β совпадает с объединением всевозможных произведений вида $\alpha\beta, \beta\alpha, \alpha\beta\alpha, \beta\alpha\beta, \dots$

2. Если α и β — перестановочные эквивалентности, то $\{\alpha, \beta\}^e = \alpha \cup \beta = \alpha\beta$ (последнее равенство есть утверждение теоремы 2.10).

Пример 2.6. 1. Если α — отношение на множестве натуральных чисел, определяемое правилом $m\alpha n \triangleq m+1 = n$, то $\alpha^t = <$ и $\alpha^* = \leq$.

2. Пусть на множестве $A = \{1, \dots, 8\}$ заданы эквивалентности α и β со смежными классами соответственно $D_\alpha = (1, 2 \mid 3, 4 \mid 5, 6, 7 \mid 8)$ и $D_\beta = (1, 4 \mid 2, 3 \mid 5, 6 \mid 7 \mid 8)$. Тогда эквивалентность $(\alpha \cup \beta)^e$ порождает смежные классы $(1, 2, 3, 4 \mid 5, 6, 7 \mid 8)$.

3. Пусть на множестве $A = \{a, b, c, d, e, f\}$ заданы эквивалентности α и β со смежными классами $D_\alpha = (a, b \mid c \mid d \mid e, f)$ и $D_\beta = (a \mid b, c \mid d, e \mid f)$ соответственно. Тогда $(a, c) \in \alpha\beta$, но $(c, a) \notin \alpha\beta$ и $(c, a) \in \beta\alpha$, но $(a, c) \notin \beta\alpha$. Таким образом, эквивалентности α и β не перестановочны и ни $\alpha\beta$, ни $\beta\alpha$ эквивалентностями не являются. Эквивалентное замыкание $\{\alpha, \beta\}^e$ (совпадающее с $\alpha\beta \cup \beta\alpha$) имеет смежные классы $\{a, b, c\}$ и $\{d, e, f\}$.

Пусть α и β — две эквивалентности на множестве A . Отношение включения $\beta \subseteq \alpha$ для них означает, что любой смежный класс по β лежит в некотором смежном классе по α . Иными словами, разбиение множества A на смежные классы по β есть подразбиение его разбиения на смежные классы по α . Говорят также, что разбиение по β есть *измельчение* разбиения по α . Для таких эквивалентностей определим на фактормножестве A/β *дробную эквивалентность* α/β по правилу

$$[x]_\beta (\alpha/\beta) [y]_\beta \triangleq [x]_\alpha = [y]_\alpha$$

для произвольных $x, y \in A$. Таким образом, два смежных класса по β эквивалентны по α/β , если они находятся в одном смежном классе по эквивалентности α (или $x\alpha y$).

Введём теперь важные понятия ядра и коядра бинарного отношения.

Определение 2.12. Пусть A и B — непустые множества и $\rho \in A \times B$ — непустое соответствие между ними. Тогда *ядром соответствия* ρ называется однородное на A отношение $\text{Ker } \rho$, определяемое соотношением

$$a_1(\text{Ker } \rho) a_2 \triangleq \forall b \in B (a_1\rho b = a_2\rho b) \quad (2.6)$$

для $a_1, a_2 \in A$. Двойственно, *коядро соответствия* ρ — это однородное на B отношение $\text{CoKer } \rho$, определяемое соотношением

$$\text{CoKer } \rho \triangleq \text{Ker } \rho^\#.$$

Ясно, что два элемента A находятся в отношении $\text{Ker } \rho$, если совпадают их образы, а два элемента B в отношении $\text{CoKer } \rho$, — если совпадают их прообразы. Легко проверяется, что $\text{Ker } \rho$ и $\text{CoKer } \rho$ суть отношения эквивалентности на соответствующих множествах — их свойства рефлексивности, симметричности и транзитивности очевидны. Поэтому $\text{Ker } \rho$ часто называют *ядерной эквивалентностью*. Смежные классы указанных эквивалентностей называются *ядрами* и *коядрами* соответственно. Таким образом, ядро соответствия — это отношение эквивалентности, а «просто» ядра — смежные классы этого отношения. Ядро, содержащее элемент $a \in A$ будем обозначать $\text{Core}(a)$; соответственно, $\text{CoCore}(b)$ — коядро, содержащее элемент $b \in B$. Понятно, что в наших обозначениях $\text{Core}(a) = [a]_{\text{Ker } \rho}$. При задании отношения матрицей, ядрам будут соответствовать совокупности одинаковых строк.

Понятие ядерной эквивалентности и ядра может быть использовано для частного случая однородного отношения: два элемента множества A находятся в отношении $\text{Ker } \rho$, если они связаны исходным отношением $\rho \in \mathcal{R}(A)$ в точности с одними и теми же элементами A (в соотношении (2.6) полагают $B = A$). Для отношения на множестве $\{1, \dots, 4\}$ заданного матрицей (2.7)

$$\begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \quad (2.7)$$

ядрами будут $\{1, 2\}$ и $\{3, 4\}$.

Ядром отношения эквивалентности, очевидно, является оно само.

Число Белла $B(n)$ называется число всевозможных разбиений n -элементного множества (см., например, [15]). В силу взаимно-однозначного соответствия между отношением эквивалентности и разбиениями, $B(n)$ будет числом всевозможных эквивалентностей на n -элементном множестве. Числа Белла растут очень быстро: например, $B(20) = 51\,724\,158\,235\,372$. Значения $B(n)$ для $n \leq 10$ приведены в нижеследующей таблице.

n	1	2	3	4	5	6	7	8	9	10
$B(n)$	1	2	5	15	52	203	877	4 140	21 147	115 975

Удобно формально считать, что $B(0) = 1$. Для $B(n)$ справедлива формула Добинского

$$B(n) = \frac{1}{e} \cdot \sum_{k=0}^{\infty} \frac{k^n}{k!}.$$

2.4 Пространства толерантности

Определение 2.13. Однородные рефлексивные и симметричные отношения называют отношениями толерантности или псевдоэквивалентностями.

Отношение толерантности будем обычно обозначать \simeq или τ . Согласно определению для произвольного отношения толерантности \simeq справедливо

$$\Delta \subseteq \simeq = \simeq^\#.$$

Введённое отношение толерантности⁴ — математическое уточнение понятие сходства, неразличимости. Как уже упоминалось, понятие близости объектов, используемое в теории распознавания образов, есть отношение толерантности между ними. Отношения толерантности часто называют просто толерантностями, а пару элементов, связанных указанным отношением — толерантными.

Пример 2.7. Описанные ниже отношения τ суть толерантности.

1. A и B — точки евклидова пространства и $A\tau B \Leftrightarrow |A - B| < r$, где r — фиксированное положительное число.
2. Слова русского языка находятся в отношении τ , если они отличаются не менее, чем на определённое количество букв (например, на одну).
3. Для элементов x и y некоторого кольца $x\tau y \Leftrightarrow$ «элемент $x - y$ необратим».

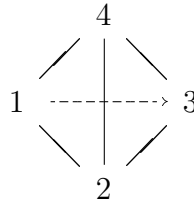
Определение 2.14. Пару $\mathfrak{T} = \langle A, \simeq \rangle$, где A — непустое множество, а \simeq — толерантность на нём, называют пространством толерантности.

Пример 2.8. Пусть A — непустое множество и $\mathcal{P}^*(A)$ — совокупность всех его непустых подмножеств. Для произвольных $X, Y \in \mathcal{P}^*(A)$ положим $X \simeq Y = (X \cap Y \neq \emptyset)$. Тогда $\langle \mathcal{P}^*(A), \simeq \rangle$ — пространство толерантности.

⁴От лат. toleratia — терпение. Употребление данного термина поясняется свойствами классов толерантности образовывать не разбиение, как у эквивалентности, а покрытие исходного множества (см. ниже).

Приведённую аксиоматизацию понятия сходства и родственного ему понятия неразличимости ввёл английский математик Э. Зиманн (см., например, Э. Зиманн, О. Бьюнеман. Толерантные пространства и мозг. / На пути к теоретической биологии. — М.: Мир, 1970).

Множество $\mathcal{P}^*(A)$ при $A = \{1, \dots, n\}$ будем обозначать S^n . Его называют $(n-1)$ -мерным симплексом. Это понятие обобщает понятия отрезка, треугольника, тетраэдра на многомерный случай. Числа $1, \dots, n$ интерпретируются как *вершины* симплекса. Двухэлементные подмножества — как *рёбра*, трёхэлементные — как *плоские (двумерные) грани*, и вообще, k -элементные подмножества — как $(k-1)$ -мерные грани. На рис. 2.5 изображен симплекс S_4 . Толерантность граней симплекса S^n означает их геометрическую инцидент-

Рис. 2.5: Симплекс S^4

ность — наличие общих вершин. Число всех элементов S^n равно, разумеется, $2^n - 1$.

На конечном множестве толерантность можно, как и любое отношение, задавать $(0,1)$ -матрицей. Ясно, что соответствующая матрица будет симметрична и содержать 1 на главной диагонали, а любая такая матрица — задавать толерантность.

Также толерантность, как и любое бинарное отношение, задают в виде графа. При этом вершины x и y графа $G(\tau)$ при $x\tau y$ соединяют неориентированным ребром (симметричность), а петли в каждой вершине (рефлексивность) опускают. На рис. 2.6 показано задание матрицей и графом толерантности на трёхэлементном множестве $\{1, 2, 3\}$.

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad 1 \text{ — } 2 \text{ — } 3$$

Рис. 2.6: Толерантность, заданная матрицей и графом.

Рассмотрим теперь алгебраические свойства операций над толерантностями. Ясно, например, что транзитивное замыкание толерантности есть эквивалентность. Так, для толерантности \simeq , заданной вышеприведённой матрицей M отношение \simeq^t есть аморфная эквивалентность.

Утверждение 2.3. Если \simeq — толерантность, а \sim — эквивалентность на некотором множестве такие, что $\simeq \subseteq \sim$, то $\simeq^t \subseteq \sim$.

Доказательство получается применением операции транзитивного замыкания к обеим частям исходного включения. \square

Следствие. Транзитивное замыкание отношения толерантности есть минимальная эквивалентность, включающая эту толерантность.

Для эквивалентного замыкания системы толерантностей справедливо почти очевидное

Утверждение 2.4. Пусть S — совокупность толерантностей на множестве A . Тогда $a S^e b$ для $a, b \in A$, если и только если в A существует конечная цепочка элементов a_1, \dots, a_n , связанных отношениями

$$a\tau_1 a_1 \tau_2 a_2 \tau_3 \dots a_n \tau_{n+1} b,$$

где $\tau_1, \dots, \tau_{n+1}$ — какие-то (возможно, повторяющиеся) отношения из S .

Введём ещё одну бинарную операцию (\circ) над однородными отношениями α и β — симметризованное произведение:

$$\alpha \circ \beta \triangleq \alpha\beta \cup \beta\alpha.$$

Теорема 2.12 (свойства толерантности).

1. Толерантность стабильна относительно \cup , \cap , $\#$, а относительно \diamond — если и только если толерантности перестановочны (и в этом случае $\alpha \diamond \beta = \alpha \circ \beta$).
2. Толерантность стабильна относительно \circ .
3. Если τ — толерантность, то и $\bar{\tau} \cup \Delta$ толерантность.
4. Если α — рефлексивное однородное отношение, то $\alpha \cup \alpha^\#$, $\alpha \cap \alpha^\#$ и $\alpha \circ \alpha^\#$ суть толерантности.

Доказательство.

1. Все утверждения следуют из п. 1) и 2) теоремы 2.4 о стабильности “положительных” свойств однородных отношений.
2. Пусть α и β — толерантности. Тогда
R: рефлексивность $\alpha \circ \beta$ следует из п. 1) теоремы 2.4;
S: $(\alpha \circ \beta)^\# = (\alpha\beta \cup \beta\alpha)^\# = (\alpha\beta)^\# \cup (\beta\alpha)^\# = \beta^\# \alpha^\# \cup \alpha^\# \beta^\# = \beta\alpha \cup \alpha\beta = \alpha \circ \beta$.
3. Утверждение следует из того, что дополнение сохраняет свойство симметричности, но превращает рефлексивное отношение антирефлексивное.
4. Легко видеть, что отношения, являющиеся результатами указанных операций наследуют рефлексивность α и приобретают свойство симметричности (для \circ — следствие п. 2)). □

Понятие толерантности, очевидно, является обобщением понятия эквивалентности. С последней связано фундаментальное понятие класса эквивалентности. Довольно часто в математике встречающаяся ситуация, когда при переходе от частного понятия к общему происходит расщепление понятий. Такое расщепление происходит, например, при переходе от эквивалентности к толерантности. При этом понятие класса эквивалентности расщепляется на два разных понятия: ядро и класс толерантности. Рассмотрим эти новые понятия.

Пусть на некотором множестве задана толерантность τ . Тогда по (2.6) определено ядро $\text{Кег } \tau$ отношения τ . Ясно, что два элемента принадлежат одному классу эквивалентности (ядру) по $\text{Кег } \tau$, если они толерантны одним и тем же объектам.

- Пример 2.9.**
1. Для толерантности, приведённой на рис. 2.6, ядра суть $\{1\}$, $\{2\}$ и $\{3\}$.
 2. Для толерантности τ , заданной графом, приведённым на рис. 2.7, классами будут множества $\text{Core}(a) = \{a, b\}$, $\text{Core}(x) = \{x\}$ и $\text{Core}(y) = \{y\}$. При этом элементы x и y не могут быть объединены в ядро, т.к. $x\tau x$, но неверно, что $y\tau x$.

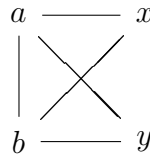


Рис. 2.7: Толерантность на четырёхэлементном множестве

Понятно, что в конечном случае задания толерантности $(0,1)$ -матрицей в одно ядро будут объединены элементы, соответствующие её одинаковым строкам или столбцам.

Фактормножество $A^* = A/\text{Кер } \tau$ пространства $\langle A, \tau \rangle$ состоит из его ядер. Назовём A^* *фактормножеством пространства толерантности по его ядру*. Введём на A^* отношение τ^* по правилу

$$\text{Core}(x) \tau^* \text{Core}(y) \Leftrightarrow xty. \quad (2.8)$$

Корректность данного определения определяется независимостью от выбора представителя в ядре. Отсюда вытекает, что отображение

$$\varphi: A \rightarrow A/\text{Кер } \tau, \quad \varphi(x) = \text{Core}(x)$$

ставящее в соответствие каждому элементу его ядро, обладает свойством

$$xty \equiv \varphi(x) \tau^* \varphi(y).$$

В таких случаях будем говорить, отображение φ *тождественно согласованно* с парой отношений τ и τ^* на множествах A и $A/\text{Кер } \tau$ соответственно.

По (2.8) τ^* оказывается отношением толерантности, а $\langle A/\text{Кер } \tau, \tau^* \rangle$ — пространством толерантности. Для толерантности, задаваемой на рис. 2.6 будем, очевидно, иметь $M(\tau^*) = M(\tau)$. Если для толерантности \simeq , заданной рис. 2.7, ядра перечислить в порядке $\text{Core}(x), \text{Core}(a), \text{Core}(y)$, то $M(\simeq^*) = M(\tau)$.

Пример 2.10. Пусть толерантность τ на множестве $A = \{1, \dots, 9\}$ задана матрицей

$$M(\tau) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}. \quad (2.9)$$

Ядра τ суть

$$\begin{aligned} C_1 = \text{Core}(1) &= \{1, 2\}, & C_2 = \text{Core}(3) &= \{3\}, \\ C_3 = \text{Core}(4) &= \{4, 6\}, & C_4 = \text{Core}(5) &= \{5\}, \\ C_5 = \text{Core}(7) &= \{7, 9\}, & C_6 = \text{Core}(8) &= \{8\}. \end{aligned} \quad (2.10)$$

Матрица толерантности τ^* на фактормножестве $A^* = A/\text{Кер } \tau = \{C_1, \dots, C_6\}$ есть

$$M(\tau^*) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Ясно, что в частном случае, когда толерантность оказывается эквивалентностью, понятие фактормножества толерантности по ядру совпадает с понятием фактормножества по эквивалентности (см. п. (2.3)).

Перейдём теперь к другому обобщению понятия класса эквивалентности — классам толерантности. Они обладают рядом интересных свойств и оказывающиеся подобными ядрам. В частности, через классы определяются базисы толерантности, по которым оказывается возможным задавать фактормножества пространств толерантности, аналогично фактормножествам по ядрам. Фактормножества также можно задавать по эквивалентностям, определяемым через базисы толерантности.

Определение 2.15. Пусть $\langle A, \tau \rangle$ — пространство толерантности. Подмножество $K \subseteq A$ называют *предклассом толерантности в A* или *τ -предклассом*, если в нём все пары элементов толерантны. Максимальный (по включению) предкласс называют *классом толерантности в A* или *τ -классом*.

Понятно, что классы и предклассы толерантности являются классами соответствия толерантности согласно определению 2.5, но не наоборот (см. ниже п. 3 примера 2.11). Для краткости, рассматривая пространства толерантности часто будем говорить просто «класс» и «предкласс», имея ввиду классы и предклассы толерантности.

Пример 2.11. 1. Тривиальным примером предкласса является любое одноэлементное множество пространства толерантности.

2. Для толерантности, задаваемой на рис. 2.6 классы толерантности суть $\{1, 2\}$ и $\{2, 3\}$.

3. Для толерантности τ на четырёхэлементном множестве $\{a, b, x, y\}$, заданной на рис. 2.7 классы толерантности суть $\{a, b, x\}$ и $\{a, b, y\}$. При этом элементы x и y не образуют τ -предкласса, однако составляют класс соответствия по τ (см. определение (2.5)), поскольку имеется, например, элемент a такой, что $x\tau a$ и $y\tau a$.

4. Рассмотрим пространство толерантности $\langle S^n, \simeq \rangle$. Обозначим через \tilde{K}_i множество некоторых граней, содержащих элемент i , $1 \leq i \leq n$.

Понятно, что \tilde{K}_i — предкласс. Пусть теперь K_i объединяет все грани, содержащие элемент i . Тогда предкласс \tilde{K}_i нерасширяем, и K_i — класс толерантности в S^n .

Геометрически класс K_i состоит, очевидно, из всевозможных граней симплекса, содержащих вершину i . Так, для S^3 получим, например, $K_1 = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}$.

Ясно, что совокупность всех предклассов толерантности пространства $\langle A, \tau \rangle$ образует покрытие множества A , т.к. объединение всех одноэлементных предклассов уже образует покрытие (точнее, разбиение) A . С другой стороны, если заданы некоторое непустое множество A и покрытие его подмножествами, то тем самым задана и толерантность τ на A , если считать толерантными любую пару элементов A , принадлежащих одному из подмножеств покрытия. При этом данные подмножества будут τ -предклассами (ср. с теоремой (2.6) о классах эквивалентности).

Особый интерес представляют классы толерантности. Здесь справедлива

Лемма 2.1. *Для всякого предкласса существует содержащий его класс.*

Доказательство (для конечного случая). Рассмотрим некоторый τ -предкласс K и всевозможные τ -предклассы, его содержащие. Любая цепь вложенных друг в друга таких предклассов, начинающаяся с K , будет конечной. Заключительный предкласс будет уже классом толерантности. \square

Полное доказательство отложим до п. 3.6. Из данной леммы следует

Теорема 2.13. Для всякой пары элементов пространства толерантности $\langle A, \tau \rangle$, находящихся в отношении τ , существует класс толерантности, их содержащий.

Для доказательства заметим, что указанная в условии пара элементов образует предкласс. Важным следствием данной теоремы является следующие

Утверждение 2.5. Если K_1, K_2, \dots, K_m — все классы толерантности τ , то

$$\tau = \bigcup_{i=1}^m K_i^2. \quad (2.11)$$

Пример 2.12. Продолжение примера 2.11. Поскольку для толерантности, задаваемой матрицей (2.6) классы толерантности суть $K_1 = \{1, 2\}$ и $K_2 = \{2, 3\}$, то $K_1^2 = \{(1, 1), (1, 2), (2, 1), (2, 2)\}$ и $K_2^2 = \{(2, 2), (2, 3), (3, 2), (3, 3)\}$. При задании $(0, 1)$ -матрицами толерантности и отношений K^2 — «находиться в одном данном классе K », имеем

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \vee \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Представление (2.11) толерантности в виде объединения декартовых квадратов своих классов называется *разложением на квадраты*. Говорят, что такое разложение *неприводимо*, если ни один квадрат нельзя исключить без нарушения данного равенства.

Пример 2.13. Пусть на множестве $A = \{1, \dots, 6\}$ задана толерантность τ , представленная в виде графа на рис. 2.8. Классами толерантности здесь будут множества

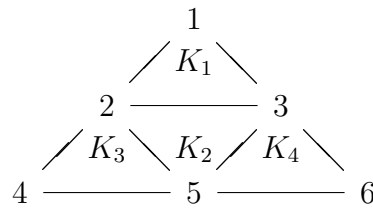


Рис. 2.8: К примеру 2.13

$$\begin{aligned} K_1 &= \{1, 2, 3\}, & K_2 &= \{2, 3, 5\}, \\ K_3 &= \{2, 4, 5\}, & K_4 &= \{3, 5, 6\}. \end{aligned}$$

Разложение $\tau = K_1^2 \cup \dots \cup K_4^2$ избыточно, т.к. любая пара элементов, входящая в декартов квадрат K_2^2 , содержится в одном из остальных квадратов. В тоже время, разложение $\tau = K_1^2 \cup K_3^2 \cup K_4^2$ уже неприводимо: например, пара $(1, 1)$ содержится только в K_1^2 , пара $(4, 4)$ — только в K_3^2 , а пара $(6, 6)$ — только в K_4^2 .

Определение 2.16. Базисом $\mathcal{B}(\tau)$ толерантности τ на конечном множестве называется всякий набор классов, определяющий неприводимое разложение данной толерантности на квадраты.

Ясно, что при удалении из базиса любого класса оставшиеся элементы уже не образуют покрытия исходного множества. Для краткости в рамках данного пункта базис толерантности будем именовать просто базисом. Так, в предыдущем примере единственный базис толерантности τ состоит из её классов K_1 , K_3 и K_4 .

Когда толерантность оказывается эквивалентностью \sim , её базис, очевидно, единственен и его составляют смежные классы по \sim . В общем случае толерантность может иметь несколько базисов с различным числом входящих в них классов.

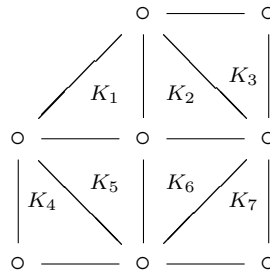


Рис. 2.9: К примеру 2.14

Пример 2.14. Граф, представленный на рис. 2.9 задаёт толерантность на восьмиэлементном множестве. Легко видеть, что классы K_1 – K_5 и K_7 образуют шестиэлементный, а классы K_1 , K_3 , K_4 , K_6 и K_7 — пятиэлементный базисы данного пространства толерантности.

Ясно, что в частном случае, когда толерантность оказывается эквивалентностью, то её базис единственен и его составляют смежные классы.

Определение 2.17. Пусть $\mathcal{B}(\tau)$ — базис в пространстве толерантности $\langle A, \tau \rangle$. *Фактормножеством пространства A по базису $\mathcal{B}(\tau)$* называется множество обозначаемое $A/\mathcal{B}(\tau)$, элементами которого являются классы из $\mathcal{B}(\tau)$ и их всевозможные (не обязательно попарные) непустые пересечения.

Ясно, что в частном случае, когда толерантность оказывается эквивалентностью, понятие фактормножества толерантности совпадает с понятием фактормножества по эквивалентности (см. п. (2.3)).

Если пространство толерантности $\langle A, \tau \rangle$ имеет единственный базис, то вместо $A/\mathcal{B}(\tau)$ будем писать A/τ .

Пример 2.15. 1. *Продолжение примера 2.10.* Пусть толерантность τ на множестве $A = \{1, \dots, 9\}$ задана матрицей (2.9). Единственным базисом толерантности τ является совокупность подмножеств

$$K_1 = \{1, 2, 3, 4, 6\}, \quad K_2 = \{1, 2, 3, 5, 7, 9\}, \quad K_3 = \{1, 2, 5, 8\}.$$

Находим пересечения непустые непарные пересечения данных классов:

$$\begin{aligned} K_1 \cap K_2 &= \{1, 2, 3\} = K_4, \\ K_1 \cap K_3 &= \{1, 2\} = K_1 \cap K_2 \cap K_3 = K_5, \\ K_2 \cap K_3 &= \{1, 2, 5\} = K_6. \end{aligned}$$

Таким образом, $A/\tau = \{K_1, \dots, K_6\}$.

Заметим, что данное фактормножество имеет лишь один общий элемент $\{1, 2\}$ с также шестиэлементным фактормножеством $A/\text{Ker } \tau$ рассматриваемого пространства по его ядру (см. (2.10)) и поэтому $A/\tau \neq A/\text{Ker } \tau$.

2. *Продолжение примера 2.11.* Для пространства $\mathfrak{A} = \langle \{1, 2, 3\}, \tau \rangle$, в котором толерантность задана матрицей (2.6), τ -классы суть $K_1 = \{1, 2\}$ и $K_2 = \{2, 3\}$; они и составляют единственный базис \mathfrak{A} . Добавив к этим классам множество $K_3 = K_1 \cap K_2 = \{2\}$, получим фактормножество $A/\simeq = \{K_1, K_2, K_3\}$. Заметим, что в данном случае $A/\tau = A/\text{Ker } \tau$.

Понятие фактормножества по базису толерантности оказывается особенно полезным в случаях, когда базис содержит небольшое множество элементов. Оно используется, в частности, при минимизации конечных автоматов.

Заметим, что на фактормножестве пространства толерантности $\langle A, \tau \rangle$ по его базису $\mathcal{B}(\tau)$ невозможно (кроме тривиального случая $A/\tau = A/\text{Кег } \tau$) естественно задать некоторую толерантность τ^* так, чтобы отображение φ , ставящее в соответствие каждому элементу $x \in A$ некоторый содержащий его класс $K \in \mathcal{B}(\tau)$ было тождественно согласованно с парой отношений τ и τ^* на множествах A и $A/\mathcal{B}(\tau)$ соответственно. Например, как следует из п. 1 примера 2.15, для рассматриваемой там толерантности τ пересечение всех классов базиса непусто (элементы 1 и 2 входят во все классы), и ни отображение $\varphi : x \rightarrow \mathcal{B}(\tau)$, ни толерантность на $\mathcal{B}(\tau)$ не могут быть заданы без привлечения дополнительных условий.

Для пространства толерантности $\langle A, \tau \rangle$ выше были определены фактормножества $A/\text{Кег } \tau$ — по ядерной эквивалентности $\text{Кег } \tau$ согласно общему определению 2.9 и $A/\mathcal{B}(\tau)$ — по базису $\mathcal{B}(\tau)$ в соответствии с определением 2.17. Также можно задавать фактормножества по эквивалентностям, определяемым через базисы толерантности.

Для этого свяжем с каждым базисом $\mathcal{B}(\tau)$ пространства $\langle A, \tau \rangle$ эквивалентность $\sim_{\mathcal{B}(\tau)}$ по правилу:

$$x \sim_{\mathcal{B}(\tau)} y \triangleq \bigvee_{K \in \mathcal{B}(\tau)} (x \in K \Leftrightarrow y \in K).$$

Иными словами, элементы x и y считаются эквивалентными, если они входят в одни и те же классы данного базиса. Для приложений важным является следующее замечание: если считать, что классы из $\mathcal{B}(\tau)$ — некоторые свойства, по которым ведётся классификация, то эквивалентность элементов означает, что они обладают одинаковым набором свойств.

В случае единственности базиса вместо $\sim_{\mathcal{B}(\tau)}$ естественно писать \sim_τ . Например, для толерантности, задаваемой матрицей (2.9) из примера 2.10 базис $\mathcal{B}(\tau)$ единственен и эквивалентность \sim_τ совпадает с $\text{Кег } \tau$; в данном случае, следовательно, $A/\sim_\tau = A/\text{Кег } \tau \neq A/\tau$.

Пусть пространство толерантности $\langle A, \tau \rangle$ имеет базис $\mathcal{B}(\tau) = \{K_1, K_2, \dots\}$. Через $\mathcal{K}(x)$ обозначим все элементы базиса, содержащие элемент $x \in A$. Базис $\mathcal{B}(\tau)$ определяет эквивалентность $\sim_{\mathcal{B}(\tau)}$ со смежными классами E_1, E_2, \dots ; они являются элементами фактормножества $A/\sim_{\mathcal{B}(\tau)}$. Через $E(x)$ обозначим (единственный) смежный класс, содержащий элемент x . Таким образом задано отображение $\varphi(x) = E(x)$ из A на $A/\sim_{\mathcal{B}(\tau)}$. На данном фактормножестве определим отношение τ^* по правилу

$$E(x)\tau^*E(y) \equiv \mathcal{K}(x) \cap \mathcal{K}(y) \neq \emptyset.$$

Легко видеть, что данное отношение есть толерантность. Заметим, что

$$E(x)\tau^*E(y) \Leftrightarrow \exists_{K \in \mathcal{B}(\tau)} (x, y \in K),$$

где $A/\mathcal{B}(\tau)$ — фактормножество A по базису $\mathcal{B}(\tau)$. Отсюда следует, что

$$\varphi(x)\tau^*\varphi(y) \Rightarrow x\tau y.$$

Последнее соотношение описывает *сильную согласованность* φ с парой отношений τ и τ^* на A и $A/\sim_{\mathcal{B}(\tau)}$ соответственно.

2.5 Основные свойства и типы соответствий

Будем рассматривать соответствия $\rho \subseteq A \times B$ между непустыми базисными множествами A и B .

Для любых отношений $\rho, \alpha, \beta \subseteq A \times B$ и $\sigma \subseteq B \times C$ и подмножеств $X, Y \subseteq A$ справедливы следующие утверждения:

$$\begin{aligned} \rho(A) &= \text{Im } \rho, & \rho^\#(B) &= \text{Dom } \rho; \\ X \subseteq Y &\Rightarrow \rho(X) \subseteq \rho(Y); & \alpha \subseteq \beta &\Rightarrow \alpha(X) \subseteq \beta(X); \\ \alpha \subseteq \beta &\Rightarrow \begin{cases} \text{Dom } \alpha \subseteq \text{Dom } \beta \\ \text{Im } \alpha \subseteq \text{Im } \beta \end{cases}; \\ \text{Dom } \rho^\# &= \text{Im } \rho, & \text{Im } \rho^\# &= \text{Dom } \rho. \end{aligned}$$

Эти свойства вполне очевидны. Далее, справедливы соотношения

$$\begin{aligned} \rho(X \cup Y) &= \rho(X) \cup \rho(Y); & \rho(X \cap Y) &\subseteq \rho(X) \cap \rho(Y); \\ (\alpha \cup \beta)(X) &= \alpha(X) \cup \beta(X); & (\alpha \cap \beta)(X) &\subseteq \alpha(X) \cap \beta(X); \\ (\rho \diamond \sigma)(X) &= \sigma(\rho(X)); \\ \text{Dom } (\rho\sigma) &= \rho^\#(\text{Dom } \sigma), & \text{Im } (\rho\sigma) &= \sigma(\text{Im } \rho). \end{aligned}$$

Докажем последние два свойства. Запишем прообраз C и образ A через проекции соответствий:

$$\text{Dom } \sigma = \sigma^\#(C) \quad \text{и} \quad \text{Im } \rho = \rho(A)$$

(см. соотношения 2.1). Пользуясь свойствами соответствий и их псевдообращений получим

$$\begin{aligned} \text{Dom } (\rho\sigma) &= (\rho\sigma)^\#(C) = (\sigma^\# \rho^\#)(C) = \rho^\#(\sigma^\#(C)) = \rho^\#(\text{Dom } \sigma); \\ \text{Im } (\rho\sigma) &= (\rho\sigma)(A) = \sigma(\rho(A)) = \sigma(\text{Im } \rho). \end{aligned}$$

Доказательство остальных свойств элементарны (их можно найти, например, в [3]).

Соответствие $\rho \subseteq A \times B$ назовём *вполне эффективным*, если $\text{Dom}(\rho) = A$ и $\text{Im}(\rho) = B$. Для конечного случая $|A| = m \geq 2$ и $|B| = n \geq 0$ известна [17] формула числа $f(m, n)$ вполне эффективных соответствий:

$$f(m, n) = \sum_{i=0}^n (-1)^{n-i} \binom{n}{i} (2^i - 1)^m.$$

Ясно, что всегда справедливо включение $\rho \subseteq \rho\rho^\#\rho$. Действительно, для произвольных $a \in A$ и $b \in B$ имеем $a\rho b = a\rho b \& b\rho^\#a \& a\rho b \Rightarrow a(\rho\rho^\#\rho)b$.

Выделим теперь основные типы соответствий, обладающие особыми свойствами.

Определение 2.18. Соответствие ρ между множествами A и B называется

- *многозначным отображением* или *всюду определённым соответствием*, если $\Delta_A \subseteq \rho\rho^\#$. Ясно, что это условие эквивалентно $\text{Dom } \rho = A$, и в графе $\vec{G}(\rho)$ из каждой вершины A выходит хотя бы одна дуга.
- *частичным отображением A в B* , если $\rho^\#\rho \subseteq \Delta_B$. Легко видеть, что это условие эквивалентно $a\rho b_1 \& a\rho b_2 \Rightarrow b_1 = b_2$ для $a \in A$ (при этом $\text{Dom } \rho \subseteq A$), и в графе $\vec{G}(\rho)$ из каждой вершины A выходит не более одной дуги.

- *функциональным* или *отображением* A в B , если $\Delta_A \subseteq \rho\rho^\# \& \rho^\#\rho \subseteq \Delta_B$. Ясно, что это условие эквивалентно существованию для любого $a \in A$ единственного $b \in B$ такого, что $a\rho b$, и в графе $\vec{G}(\rho)$ из каждой вершины A выходит ровно одна дуга.
- *дифункциональным* или *квазиоднозначным*, если $\rho\rho^\#\rho \subseteq \rho$ или, с учётом доказанного выше, $\rho\rho^\#\rho = \rho$.

Для отношения $\rho \subseteq A \times B$ справедливы следующие утверждения (см. [30] или [23]): любых $a \in A$, $b \in B$ если

- $\rho^\#(b_1) \neq \rho^\#(b_2) \Rightarrow \rho^\#(b_1) \cap \rho^\#(b_2) = \emptyset$ или $\rho(a_1) \neq \rho(a_2) \Rightarrow \rho(a_1) \cap \rho(a_2) = \emptyset$ (смежные классы A по ρ или B по $\rho^\#$ попарно не пересекаются), то ρ дифункционально;
- ρ дифункционально, то $\rho^\#(b_1) \neq \rho^\#(b_2) \Rightarrow \rho^\#(b_1) \cap \rho^\#(b_2) = \emptyset$ и $\rho(a_1) \neq \rho(a_2) \Rightarrow \rho(a_1) \cap \rho(a_2) = \emptyset$ (смежные классы A по ρ и B по $\rho^\#$ попарно не пересекаются).

Функциональные отображения будут рассмотрены ниже. В качестве иллюстрации использования многозначных отображений приведём без доказательства (которое может быть найдено в [37]) следующую теорему.

Теорема 2.14 (Кальмар-Якубович). *Произвольное отношение толерантности \simeq на множестве A может быть задано с помощью подходящего многозначного отображения φ из A на совокупность всевозможных классов толерантности как*

$$x \simeq y \Leftrightarrow \varphi(x) \cap \varphi(y) \neq \emptyset.$$

2.6 Отображения и их основные свойства

Широчайшее применение находят функциональные соответствия (отображения). Рассмотрим их подробнее.

Отображение φ из A в B будем называть также *функцией* из A в B или *операцией* на A^5 . При этом используют обозначения $\varphi: A \rightarrow B$ или $A \xrightarrow{\varphi} B$. Тот факт, что $a\varphi b$ записывают как $\varphi(a) = b$ или $a \xrightarrow{\varphi} b$; при теоретических выкладках удобна запись $a\varphi = b$ или даже $a^\varphi = b$. Множество всех отображений $A \rightarrow B$ будем обозначать $Fun(A, B)$. При $A = B$ будем пользоваться обозначением $Fun(A)$ и говорить, что $Fun(A)$ составляют *преобразования* множества A .

Ясно, что отображение $\varphi: A \rightarrow B$ задаётся направленным двудольным графом $\vec{G}(\varphi)$, вершинами которого служат элементы A и B , причём из вершины, соответствующей $a \in A$, единственная дуга ведёт в вершину, соответствующую $b \in B$, если $\varphi(a) = b$. Далее мы не будем различать элементы множеств A и B и вершины $\vec{G}(\varphi)$.

В соответствии с определениями для соответствий, если $\varphi: A \rightarrow B$, то элемент b , $b = \varphi(a)$ называют *образом элемента a* , а элемент a — *прообразом элемента b* . Совокупность (возможно пустая) всех прообразов элемента $b \in B$ называется *полным прообразом b* .

Если $A' \subset A$ и $\varphi: A \rightarrow B$, то про отображение $\varphi': A' \rightarrow B$, где $\varphi(x) = \varphi'(x)$ для всех $x \in A'$, говорят, что оно является *сужением* или *ограничением отображения φ на A'* , а про отображение φ — что оно является *продолжением* или *расширением отображения φ'* . Заметим, что в общем случае сужения отображения может не существовать.

⁵Таким образом, мы не различаем понятия функционального соответствия (отображения) и функции, хотя они не тождественны друг другу. Пример для знакомых с теорией алгоритмов: невычислимые функции, строго говоря, являются лишь функциональными соответствиями, а не функциями.

Поскольку отображения являются отношениями, к ним можно попытаться применять теоретико-множественные операции. Однако во-первых, отрицание отображения, очевидно, отображением не является, а во-вторых — справедлива следующая

Утверждение 2.6. *Объединение [пересечение] двух отображений $\varphi: A \rightarrow B$ и $\psi: A \rightarrow B$ является отображением, если и только если $\varphi = \psi$.*

Доказательство. Поскольку φ и ψ — отображения из A в B , для каждого $a \in A$ φ и ψ содержат лишь по одной паре (a, b_1) и (a, b_2) соответственно, где $b_1, b_2 \in B$. Если предположить, что $b_1 \neq b_2$, то $\varphi \cup \psi$ содержит две, а $\varphi \cap \psi$ — не содержит ни одной пары с первым элементом, равным a . \square

Таким образом, применение к отображениям обычных теоретико-множественных операций интереса не представляет. Рассмотрим теперь операцию произведения отношений, применённую к отображениям.

Теорема 2.15. *Если A, B и C — непустые множества, φ — отображение из A в B , а ψ — отображение из B в C , то $\varphi\psi$ — отображение из A в C .*

Доказательство.

$$\begin{aligned} \left\{ \begin{array}{l} \Delta_A \subseteq \varphi\varphi^\#, \varphi^\#\varphi \subseteq \Delta_B \\ \Delta_B \subseteq \psi\psi^\#, \psi^\#\psi \subseteq \Delta_C \end{array} \right. &\Rightarrow \Delta_A \subseteq \varphi\varphi^\# = \\ &= \varphi \Delta_B \varphi^\# \subseteq \varphi(\psi\psi^\#)\varphi^\# = (\varphi\psi)(\psi^\#\varphi^\#) = (\varphi\psi)(\varphi\psi)^\#, \end{aligned}$$

т.е. $\Delta_A \subseteq (\varphi\psi)(\varphi\psi)^\#$. Включение $(\varphi\psi)^\#(\varphi\psi) \subseteq \Delta_C$ показывается аналогично. \square

Произведение функций как отображений принято записывать как их композицию $*$: $(\varphi \circ \psi)(x) \triangleq (\varphi * \psi)(x) = \psi(\varphi(x))$ ⁶.

Рассмотрим специальные виды отображений. Единичное отношение Δ_A , рассматриваемое как отображение A на себя, называют *тождественным*. Для тождественного отображения будем употреблять обозначение id_A .

Определение 2.19. Отображение $\varphi: A \rightarrow B$ называется

- *постоянным* или *константой*, если $\varphi\varphi^\# = \nabla_A$.

Легко видеть, что данное соотношение эквивалентно $\varphi(a) = b \in B$ для всех $a \in A$. В графовой интерпретации отображения это означает, что дуги, исходящие из всех вершин $a \in A$ графа $\vec{G}(\varphi)$, входят в единственную вершину $b \in B$.

- *вложением* или *инъективным отображением* A в B , если $\text{id}_A = \varphi\varphi^\#$, что записывают как $A \xrightarrow{\varphi} B$.

Понятно, что при вложении различные элементы A переходят в различные элементы B и прообраз $\varphi^\#(y)$ элемента $y \in Y$ — не более, чем одноэлементное множество. В графовой интерпретации это означает, что в каждую вершину $b \in B$ входит не более одной дуги.

Если $A \subseteq B$, то вложение $A \xrightarrow{\varphi} B$ такое, что $\varphi(x) = x$, называется *естественным вложением* множества A в множество B .

- *наложением* или *сюръективным отображением* A в B , если $\varphi^\#\varphi = \text{id}_B$.

При наложении каждый элемент множества B имеет свой прообраз. В графовой интерпретации это означает, что в каждую вершину $b \in B$ входит хотя бы одна дуга.

⁶Здесь становится очевидным удобство записи $\psi(\varphi(x)) = x\varphi\psi$. В этом случае приведённое соотношение означает просто возможность опускания скобок в записи вида $x\varphi\psi$.

Ясно, что для $A = A_1 \times \dots \times A_n$ отображения $A \xrightarrow{\pi_i} A_i$, определяемые как $(a_1, \dots, a_i, \dots, a_k) \xrightarrow{\pi_i} a_i$, $i = \overline{1, n}$ сюръективны. Они называются *отображениями проектирования*.

- *биекцией* (биективным, взаимно-однозначным отображением), если $\text{id}_A = \varphi^\# \& \varphi^\# \varphi = \text{id}_B$, т.е. оно является одновременно и вложением, и наложением.

В графовой интерпретации отображения это означает, что все вершины двудольного графа $\vec{G}(\varphi)$ оказываются разбитыми на пары (a, b) , $a \in A$, $b \in B$ так, что из a в b идёт дуга. Понятно, что в конечном случае это означает $|A| = |B|$.

Множество всех биективных отображений из A в B будем обозначать $\text{Bij}(A, B)$, а в случае $A = B$ — пользоваться обозначением $\text{Bij}(A)$.

Псевдообратное к отображению $\varphi: A \rightarrow B$ соответствие $\varphi^\#$, понятно, может и не оказаться отображением из B в A . Отображение $\psi: B \rightarrow A$ называется *обратным отображением* $\varphi: A \rightarrow B$, если $\text{id}_A = \varphi\psi \& \psi\varphi = \text{id}_B$. Ясно, что если φ — биекция, то однозначно определяемое псевдообратное к ней отношение $\varphi^\#$ является отображением и, более того, биекцией. Также легко видеть, что этим случаем исчерпываются возможности отображения иметь обратное. Для биекции, обратной к биекции φ естественно использовать обозначение φ^{-1} , а не $\varphi^\#$.

Моноид $\langle \text{Fun}(A), *, \text{id}_A \rangle$ называют *моноидом эндоморфизмов множества A* и обозначают $\text{End } A$. Симметрическую группу $\text{Sym}_A = \langle \text{Bij}(A), *,^{-1}, \text{id}_A \rangle$ называют также *группой автоморфизмов множества A* и обозначают $\text{Aut } A$.

Рассмотрим применение к отображениям операции произведения (композиции). Нетрудно показать, что произведение двух вложений, наложений или биекций также является, соответственно, вложением, наложением или биекцией: доказательства повторяют доказательство теоремы 2.15 с заменой символа \subseteq на $=$.

Следующие две теоремы характеризуют вложение и наложение через свойства их произведений (композиций).

Теорема 2.16. *Отображение $f: X \rightarrow Y$ — инъекция если и только если для любых двух отображений g_1, g_2 из некоторого множества Z в X*

$$g_1 * f = g_2 * f \Leftrightarrow g_1 = g_2.$$

Доказательство. (\Rightarrow) Пусть f — инъекция из множества X в Y и для любых двух отображений g_1, g_2 из Z в X справедливо $g_1 * f = g_2 * f$. Но тогда же справедливо $g_1 * f * f^\# = g_2 * f * f^\#$ или $g_1 * \text{id}_X = g_2 * \text{id}_X$, откуда $g_1 = g_2$.

(\Leftarrow) Пусть для любых двух отображений g_1, g_2 из Z в X справедлива равносильность $g_1 * f = g_2 * f \Leftrightarrow g_1 = g_2$, но f не является вложением. Тогда найдутся x_1 и x_2 из X , что $x_1 \neq x_2$, но $f(x_1) = f(x_2)$. Возьмём в качестве Z одноэлементное множество $\{z_0\}$ и построим два отображения g_1, g_2 из Z в X такие, что $g_1(z_0) = x_1$, $g_2(z_0) = x_2$. Поскольку $f(g_1(z_0)) = f(g_2(z_0))$, а других значений аргумента нет, то $g_1 * f = g_2 * f$, $g_1 = g_2$ и $x_1 = x_2$. Противоречие. \square

Теорема 2.17. *Отображение $f: X \rightarrow Y$ — сюръекция если и только если для любых двух отображений g_1, g_2 из Y в некоторое множество Z*

$$f * g_1 = f * g_2 \Leftrightarrow g_1 = g_2.$$

Доказательство. (\Rightarrow) Пусть f — сюръекция из множества X в Y и для любых двух отображений g_1, g_2 из Y в Z справедливо $f * g_1 = f * g_2$. Из того, что f — наложение

следует непустота $f^\sharp(y)$ для любого $y \in Y$. Пусть $x \in f^\sharp(y)$ ⁷. Тогда

$$g_1(y) = g_1(f(x)) = g_2(f(x)) = g_2(y),$$

что в виду произвольности элемента y влечёт $g_1 = g_2$.

(\Leftarrow) Пусть для любых двух отображений g_1, g_2 из Y в Z справедлива равносильность $f * g_1 = f * g_2 \Leftrightarrow g_1 = g_2$, но f не является наложением. Тогда найдётся элемент y из области $Y \setminus \text{Im}(f)$. Зафиксируем в Y элемент $y_0 \neq y$ и рассмотрим отображение $g_2 : Y \rightarrow Y$, определяемое условием

$$g_2(t) = \begin{cases} t, & \text{если } t \neq y \\ y_0, & \text{если } t = y, \end{cases}$$

Ясно, что $g_2 \neq \text{id}_Y$, в силу чего $f * g_2 \neq f * \text{id}_Y$. Однако для всех $x \in X$ имеем

$$g_2(f(x)) = f(x) = \text{id}_Y(f(x)).$$

Противоречие. □

С помощью биекций описываются фундаментальные свойства множеств. Напомним, что множества называют *равномощными*, если между ними существует биективное отображение.

Теорема 2.18 (Кантора-Шрёдера-Бернштейна⁸). *Если каждое из множеств A и B равномощно подмножеству другого, то они равномощны.*

Доказательство. Теорема утверждает, что если для двух множеств A и B существуют биекции θ_1 между A и подмножеством B и θ_2 между B и подмножеством A , то существует биекция между A и B .

Обозначим $A_0 = A$ и $\text{Im}(\theta_2) = A_1$. Ясно, что можно считать $A_0 \supset A_1$ и $\text{Im}(\theta_1) \subset B$, иначе теорема тривиально справедлива. Также ясно, что в этом случае A и B — бесконечные множества.

Последовательное применение отображений, указанных в формулировке теоремы, даёт взаимно-однозначное отображение $\theta = \theta_1 * \theta_2$ множества A_0 на своё подмножество A_2 и $A_1 \supset A_2$. Обозначим $\theta(A_i) = A_{i+2}$, $i = 0, 1, 2, \dots$. Получим цепочку строго содержащихся друг в друге подмножеств A : $A = A_0 \supset A_1 \supset A_2 \supset \dots$.

Обозначим $C_i = A_i \setminus A_{i+1}$, $i = 0, 1, 2, \dots$ и $C = \bigcap_{i \geq 0} A_i$. По построению между множествами C_0, C_2, C_4, \dots существует взаимно-однозначное соответствие θ : $C_{2i+2} = \theta(A_{2i}) \setminus \theta(A_{2i+1}) = \theta(C_{2i})$.

Построим теперь взаимно-однозначное отображение φ между A_0 и A_1 . Положим

$$\varphi(x) = \begin{cases} \theta(x), & \text{если } x \in C_{2i}, i = 0, 1, \dots \\ x, & \text{иначе} \end{cases} \quad (\text{см. рис. 2.10}).$$

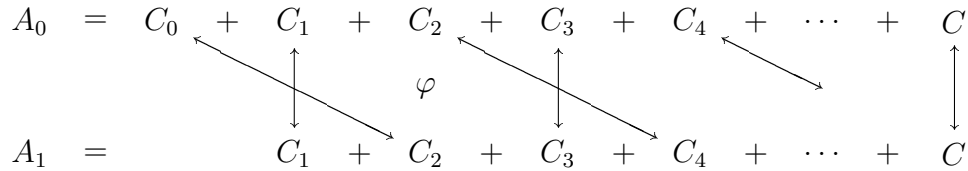
Таким образом, имеем взаимно-однозначные соответствия $A \xrightarrow{\varphi} A_1 \xrightarrow{\theta_2^{-1}} B$ и $\varphi * \theta_2^{-1}$ — искомая биекция. □

Отметим, важное свойство преобразований конечных множеств.

Теорема 2.19 (свойство преобразования конечного множества). *Пусть множество A конечно. Тогда для его преобразования $\varphi \in \text{Func}(A)$ сюръективность, инъективность и биективность функций из $\text{Func}(A)$ — равносильные условия.*

⁷Заметим, что возможность указания такого x эквивалентна принятию аксиомы выбора (см. п. 3.6).

⁸Теорема была приведена без доказательства в работе Г. Кантора 1883 г. и доказана позднее Э. Шрёдером и Ф. Бернштейном.

Рис. 2.10: Схема соответствия между множествами A_0 и A_1

Доказательство. Если множество A имеет n элементов, то граф $\vec{G}(\varphi)$, соответствующей преобразованию φ , имеет n вершин и n дуг, причём из каждой вершины исходит ровно одна дуга.

Сюръективность φ означает, что в каждую вершину $\vec{G}(\varphi)$ входит дуга. Поскольку дуг столько же сколько вершин, это означает, что в каждую вершину входит ровно одна дуга, т.е. φ — инъективно.

Если же в каждую вершину в каждую вершину $\vec{G}(\varphi)$ входит ровно одна дуга, то, поскольку одна дуга исходит из каждой вершины, с каждой вершиной $\vec{G}(\varphi)$ связаны ровно по одной входящей и исходящей дуги, т.е. φ — биективно.

Биективность отображения по определению влечёт сюръективность. \square

Пусть \sim — эквивалентность на A . Тогда существует функция $\pi : A \rightarrow A/\sim$, ставящая в соответствие каждому элементу $a \in A$ его класс эквивалентности, т.е. $\pi(a) = [a]_{\sim}$. Такое отображение называется *естественным (каноническим, натуральным)*. Каноническое отображение мы будем обозначать $nat(A, \sim)$ или просто $nat(\sim)$, если множество A фиксировано при данном рассмотрении. Понятно, что $nat(\sim)$ — наложение.

Пример 2.16. Для примера 2.3 имеем:

1. $\pi(a)$ — мешок, в котором лежит зерно a .
2. $\pi(u)$ — начальная буква слова u .

Пусть дано отображение $\varphi : A \rightarrow B$. Его *ядром* называется отношение $\text{Ker } \varphi \in \mathcal{R}(A)$, заданное как

$$a_1(\text{Ker } \varphi)a_2 \Leftrightarrow \varphi(a_1) = \varphi(a_2). \quad (2.12)$$

Понятно, что ядро отображения есть частный случай понятия ядра соответствия (2.6) и является *ядерной эквивалентностью*. Легко установить, что

$$\text{Ker } \varphi = \varphi\varphi^\#.$$

С ядерной эквивалентностью отображения φ из A связано фактормножество $A/\text{Ker } \varphi$ и натуральное отображение $nat(A, \text{Ker } \varphi)$, для которого $nat(A, \text{Ker } \varphi)(x) = [x]_{\text{Ker } \varphi}$. Заметим, что отображения $\varphi : A \rightarrow B$ и $nat(A, \text{Ker } \varphi)$ имеют общую ядерную эквивалентность, но отображают A в разные множества: соответственно в B и в $A/\text{Ker } \varphi$. Также нетрудно видеть, что $\text{Ker } \varphi = \varphi\varphi^\#$. Ясно, что если ядро отображения φ из A в B есть диагональное отношение на A , то φ — вложение A в B .

Далее мы будем пользоваться следующим удобным изображением соответствий. Если A, B, C, D — некоторые множества и

$$\begin{array}{ccccccc}
 \alpha : A \rightarrow B, & \beta : B \rightarrow C, & \gamma : A \rightarrow C, \\
 \delta : B \rightarrow D, & \varepsilon : C \rightarrow D.
 \end{array}$$



Рис. 2.11: Диаграммы отображений множеств

то указанные отображения на них наглядно задают в виде диаграмм, приведённых на рис. 2.11.

Говорят, что эти диаграммы *коммутативны*, если $\gamma = \alpha\beta$ и $\alpha\delta = \gamma\epsilon$ соответственно. Аналогично определяется коммутативность и для более сложных диаграмм. Биективные отображения будем обозначать на диаграммах двунаправленными стрелками \leftrightarrow .

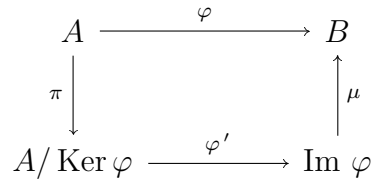
Сформулируем теперь основную теорему о разложении отображений.

Теорема 2.20 (о разложении отображений). Пусть даны непустые множества A , B и отображение $\varphi: A \rightarrow B$. Тогда для отображения φ справедливо разложение

$$\varphi = \pi * \varphi' * \mu, \quad (2.13)$$

где $\pi = \text{nat}(\text{Ker } \varphi)$, φ' — биекция между $A/\text{Ker } \varphi$ и $\text{Im } \varphi$ и μ — вложение $\text{Im } \varphi$ в B .

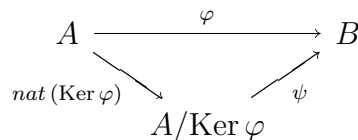
Доказательство. Утверждение теоремы будет справедливо в случае коммутативности диаграммы



Ясно, что $\text{Im } \varphi$ есть подмножество B . В качестве μ возьмём естественное вложение. Из определения $\text{Ker } \varphi$ следует, что отображение $\varphi': A/\text{Ker } \varphi \rightarrow \text{Im } \varphi$ биективно. Отсюда следует справедливость разложения (2.13), если в качестве π взять $\text{nat}(\text{Ker } \varphi)$. При этом все элементы разложения (2.13) определены однозначно. \square

Следующая теорема является следствием только что доказанной.

Теорема 2.21 (основное свойство отображений). Пусть даны непустые множества A , B и отображение $\varphi: A \rightarrow B$. Тогда имеется единственное отображение $\psi: A/\text{Ker } \varphi \rightarrow B$ являющееся вложением, и такое, что диаграмма



коммутативна.

Доказательство. Положим в (2.13) $\psi = \varphi' * \mu$. Тогда ψ заданное как $\psi([a]_{\text{Ker } \varphi}) = \varphi(a)$ — однозначно определённое вложение $\text{Ker } \varphi$ в B . \square

Из данной теоремы следует, что для любого отображения $\varphi: A \rightarrow B$ справедливо *каноническое разложение* $\varphi = \pi * \psi$, где $\pi = \text{nat}(A, \text{Ker } \varphi)$ — наложение, а ψ — вложение.

Такое разложение, очевидно, единственно. Это свойство и называют *основным свойством отображений*.

Основное свойство отображений можно обобщить, если заметить, что для произвольной эквивалентности \sim , содержащейся в $\text{Кер } \varphi$ существует единственное отображение $\chi: A/\sim \rightarrow B$.

Теорема 2.22 (о фактормножествах). Пусть даны непустые множества A, B с отображением $\varphi: A \rightarrow B$ и эквивалентность \sim на A такая, что $\sim \subseteq \text{Кер } \varphi$. Тогда имеется единственное отображение $\chi: A/\sim \rightarrow B$ такое, что диаграмма

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \text{nat}(\sim) \searrow & & \nearrow \chi \\ & A/\sim & \end{array}$$

коммутативна.

Доказательство. Коммутативность диаграммы обеспечивается при задании χ правилом $\chi([a]_{\sim}) = \varphi(a)$, $a \in A$. Такое задание корректно, поскольку, в силу $\sim \subseteq \text{Кер } \varphi$, всем элементам x из $[a]_{\sim}$ соответствует единственное значение $\chi(x) = \varphi(a)$. Ядерная эквивалентность отображения χ — единичное отношение на A/\sim лишь при $\sim = \text{Кер } \varphi$, и поэтому χ , вообще говоря, не есть вложение. Единственность χ следует из теоремы о классах эквивалентности. \square

Из данной теоремы следует, что для любого отображения $\varphi: A \rightarrow B$ и эквивалентности \sim на A такой, что $\sim \subseteq \text{Кер } \varphi$, справедливо *обобщённое разложение* $\varphi = \pi * \chi$, где $\pi = \text{nat}(A, \sim)$ — наложение. Такое разложение, вообще говоря, не единственно, поскольку возможны различные измельчения классов эквивалентностей по $\text{Кер } \varphi$. Иногда данную теорему коротко формулируют как утверждение о возможности факторизации любого отображения по эквивалентности, содержащейся в его ядре.

Из основного свойства отображений вытекает

Теорема 2.23 (о дробных эквивалентностях). Пусть дано множество A и эквивалентности α, β на нём такие, что $\beta \subseteq \alpha$. Тогда существуют отображение $\varphi: A/\beta \rightarrow A/\alpha$ и биекция $\psi: (A/\beta)/(\alpha/\beta) \rightarrow A/\alpha$ такие, что диаграмма

$$\begin{array}{ccc} & A & \\ \text{nat } \beta \swarrow & & \searrow \text{nat } \alpha \\ A/\beta & \xrightarrow{\varphi} & A/\alpha \\ \text{nat}(\alpha/\beta) \searrow & & \nearrow \psi \\ & (A/\beta)/(\alpha/\beta) & \end{array}$$

коммутативна.

Доказательство. Зададим функцию φ правилом $\varphi([a]_{\beta}) = [a]_{\alpha}$. Нетрудно видеть, что такое задание корректно, т.к. каждому классу эквивалентности $[a]_{\beta}$ соответствует единственный класс эквивалентности $[a]_{\alpha}$. Далее применим теорему 2.21 к нижней части диаграммы. Поскольку φ , как легко видеть, накрытие, то $\psi([a]_{\beta}/(\alpha/\beta)) = \varphi([a]_{\beta}) = [a]_{\alpha}$ — биекция. \square

Глава 3

Частично упорядоченные множества

Понятие частично упорядоченного множества является фундаментальным для современной теоретико-множественной математики и встречается во многих прикладных вопросах.

Л. А. Скорняков. Предисловие редактора русского перевода книги Л. Берана «Упорядоченные множества».

3.1 Предпорядки и порядки

Определение 3.1. *Предпорядками (или квазипорядками) называют рефлексивные и транзитивные однородные отношения.*

Пример 3.1. Предпорядками, например, являются следующие отношения.

1. Отношение делимости на множестве $\mathbb{Z} \setminus \{0\}$;
2. Отношение ρ на множестве действительных функций, задаваемое условием « $f\rho h \Leftrightarrow$ множество нулей функции f содержится во множестве нулей функции h ».
3. Отношение выводимости \vdash в логике: если из формулы A выводится формула B , то пишут $A \vdash B$.
4. В экономике: отношение предпочтения (например, по цене и полезности) на наборах товаров.

Для предпорядков ρ по теореме 2.3 имеем $\rho = \rho^n$, $n \in \mathbb{N}$, поэтому для них

$$\Delta \subseteq \rho = \rho^2.$$

Легко показать, что согласно (2.6), ядерной эквивалентностью $\text{Кер } \rho$ предпорядка ρ будет его *симметрическая часть* $\text{Кер } \rho = \rho \cap \rho^\sharp$.

Определение 3.2. Рефлексивные, антисимметричные и транзитивные бинарные отношения называют отношениями *частичного порядка*.

Иногда для простоты вместо «частичный порядок» будем говорить просто «порядок». Понятно, что для порядка ρ справедливо

$$\rho \cap \rho^\sharp \subseteq \Delta \subseteq \rho = \rho^2.$$

Очевидно, ядерной эквивалентностью частичного порядка будет подмножество диагонального отношения Δ .

Пример 3.2. Все предпорядки из примера 3.1 не являются частичными порядками ввиду отсутствия у них свойства антисимметричности:

- 1) из $m \mid n$ и $n \mid m$ следует не $m = n$, а лишь $|m| = |n|$;
- 2) совпадение множеств нулей функций не означает равенства последних;
- 3) возможно $A \vdash B$ и $B \vdash A$, но $A \neq B$ (формулы A и B не совпадают как строки символов): например, при $A = x \supset y$ и $B = \neg x \vee y$;
- 4) ясно, что одинаковые цену и полезность могут иметь разные товары.

Важнейшим примером частичного порядка является отношение включения на совокупности подмножеств некоторого множества. При этом говорят, что такая совокупность *упорядочена по включению*. Диагональное отношение на произвольном множестве можно рассматривать не только как эквивалентность, но и как частичный порядок. Множество с таким порядком называют *тривиально упорядоченным* или *дискретным*.

Из предпорядка ρ всегда можно построить порядок, если отождествить элементы a и b , для которых одновременно $a\rho b$ и $b\rho a$.

Теорема 3.1. *Если \preceq — предпорядок на множестве P , то*

- 1) *бинарное отношение ε на P , определяемое условием*

$$a\varepsilon b \Leftrightarrow a \preceq b \ \& \ b \preceq a$$

является эквивалентностью;

- 2) *бинарное отношение \leq на фактормножестве P/ε , определяемое условием*

$$[a]_\varepsilon \leq [b]_\varepsilon \Leftrightarrow a \preceq b$$

является частичным порядком.

Доказательство.

- 1) Согласно своему определению, отношение ε приобретает свойство симметричности в дополнение к свойствам рефлексивности и транзитивности, наследуемых от \preceq .
- 2) Свойства рефлексивности и транзитивности \leq наследуются от отношения \preceq . В силу свойства классов эквивалентности по ε , оно оказывается ещё и антисимметричным.

□

Пример 3.3. Для примера 3.1 в обозначениях теоремы 3.1 получим следующее.

1. $[n]_\varepsilon = \{n, -n\}$ и частичный порядок \leq есть отношение делимости $|$ на фактормножестве $\{\mathbb{Z} \setminus \{0\}\}/\varepsilon = \mathbb{N}$.
2. $f\varepsilon h \Leftrightarrow$ множество нулей функций f и h совпадают; $[f]_\varepsilon \leq [h]_\varepsilon \Leftrightarrow$ множество нулей любой функции из $[f]_\varepsilon$ содержится во множестве нулей любой функции из $[h]_\varepsilon$.
3. Если на множестве формул \mathcal{A} ввести отношение \simeq дедуктивной эквивалентности по правилу

$$A \vdash B \ \text{и} \ B \vdash A \Leftrightarrow A \simeq B,$$

(нетрудно проверить, что это действительно эквивалентность), то \mathcal{A}/\simeq — фактормножество классов дедуктивно эквивалентных формул, а отношение выводимости, перенесённое на классы означает, что из любой формулы класса $[A]$ выводится любая формула класса $[B]$, что (в полученной алгебре Линденбаума-Тарского) записывают как $[A] \leq [B]$.

4. Ситуацию с отношением предпочтения в экономике оставляем для самостоятельного разбора.

Отношения частичного порядка будем, как правило, обозначать \sqsubseteq , иногда, впрочем, употребляя обозначения \leq , \preceq и т.д. Когда $x \sqsubseteq y$ и $x \neq y$, то будем писать $x \sqsubset y$ (и аналогично для других обозначений) и говорить об отношении *строгого порядка*. Понятно, что строгий порядок транзитивен, антирефлексивен и асимметричен ($\sqsubset \cap \sqsupset = \emptyset$). Часто удобно рассматривать двойственные частичные порядки: $\sqsupset \triangleq \sqsubset^\#$, т.е. запись $x \sqsupset y$ означает, что $y \sqsubseteq x$ и аналогично для строгого порядка. Отношение несравнимости ι_{\sqsubseteq} для данного порядка \sqsubseteq обозначаем инфексным символом \parallel .

- Утверждение 3.1.** 1. $x_1 \sqsubseteq x_2 \sqsubseteq \dots \sqsubseteq x_n \sqsubseteq x_1 \Rightarrow x_1 = x_2 = \dots = x_n$ (антициклическость порядка).
2. Отношение сравнимости для частичного порядка есть эквивалентность.
3. Отношение несравнимости для строгого частичного порядка есть отношение толерантности.

Доказательство.

1. Если хотя бы одно отношение есть строгий порядок то, в силу его антирефлексивности, выполнение $x_1 = x_2 = \dots = x_n$ станет невозможным.
2. Отношение сравнимости для частичного порядка, очевидно, рефлексивно, симметрично и транзитивно.
3. Рефлексивность несравнимости для строгого порядка следует из антирефлексивности последнего. Следование

$$x \iota_{\sqsubseteq} y = x(\overline{\sqsubseteq} \cap \overline{\sqsupset})y = y(\overline{\sqsubseteq} \cap \overline{\sqsupset})^{\#}x = y(\overline{\sqsubseteq}^{\#} \cap \overline{\sqsupset}^{\#})x = y(\overline{\sqsupset} \cap \overline{\sqsubseteq})x = y \iota_{\sqsubseteq} x$$

доказывает симметричность ι_{\sqsubseteq} .

□

Если $a \sqsubseteq b$, то говорят, что a предшествует b или b следует за a или содержит a . При $a \sqsubseteq b$ определяют множество $\{x \mid a \sqsubseteq x \ \& \ x \sqsubseteq b\}$, которое называют интервалом¹ и обозначают $[a, b]$. Если $[a, b] = \{a, b\}$, то говорят, что a непосредственно предшествует b и что b непосредственно следует за a или покрывает, доминирует над a (символически $a \leq b$).

Выясним стабильность порядков относительно теоретико-множественных операций и специальных операций над отношениями. Из теорем 2.4 и 2.5 следует, что если α и β — порядки, то $\alpha^{\#}$ и $\alpha \cap \beta$ — также порядки.

Объединение порядков в общем случае не является порядком. Приведённая ниже теорема описывает критерий того, что объединение порядков является порядком.

Теорема 3.2. Объединение $\alpha \cup \beta$ частичных порядков α и β есть частичный порядок, если и только если

$$\begin{cases} \alpha\beta \cup \beta\alpha \subseteq \alpha \cup \beta, \\ \alpha \cap \beta^{\#} = \Delta. \end{cases} \quad (3.1)$$

Доказательство. Рассмотрим произвольные частичные порядки α и β на некотором множестве.

(\Leftarrow) Пусть условия (3.1) выполнены.

R: Рефлексивность объединения $\alpha \cup \beta$ следует из рефлексивности каждого из порядков.

AS: Второе свойство из (3.1) обеспечивает равенства

$$\begin{aligned} (\alpha \cup \beta) \cap (\alpha \cup \beta)^{\#} &= (\alpha \cup \beta) \cap (\alpha^{\#} \cup \beta^{\#}) \stackrel{Dtr}{=} \\ &= \underbrace{(\alpha \cap \alpha^{\#})}_{\subseteq \Delta} \cup \underbrace{(\beta \cap \beta^{\#})}_{\subseteq \Delta} \cup (\beta \cap \alpha^{\#}) \cup \underbrace{(\alpha \cap \beta^{\#})}_{\Delta} = \Delta \cup (\alpha \cap \beta^{\#})^{\#} = \Delta. \end{aligned} \quad (3.2)$$

¹хотя с точки зрения словоупотребления, принятого в математическом анализе, здесь следовало бы говорить «отрезок»

Т: Рефлексивность и симметричность порядков влечёт $\alpha^2 = \alpha$ и $\beta^2 = \beta$. С учётом первого свойства из (3.1) имеем

$$\begin{aligned} (\alpha \cup \beta)^2 &= (\alpha \cup \beta)(\alpha \cup \beta) \stackrel{(2.2)}{=} \alpha^2 \cup \alpha\beta \cup \beta\alpha \cup \beta^2 = \\ &= (\alpha \cup \beta) \cup (\alpha\beta \cup \beta\alpha) \subseteq \alpha \cup \beta. \end{aligned} \quad (3.3)$$

(\Rightarrow) Пусть $\alpha \cup \beta$ — частичный порядок. Тогда, в силу его транзитивности, справедливо условие (3.3), откуда $\alpha\beta \cup \beta\alpha \subseteq \alpha \cup \beta$.

Поскольку $\alpha \cup \beta$ антисимметрично, из (3.2) следует, что $\alpha \cap \beta^\# \subseteq \Delta$. Но $\alpha \cap \beta^\#$ — частичный порядок, и поэтому $\Delta \subseteq \alpha \cap \beta^\#$, откуда следует $\alpha \cap \beta^\# = \Delta$. \square

Замечание. Если α и β — строгие порядки, то для того, чтобы их объединение также было строгим порядком, необходимо и достаточно выполнение условия $\alpha\beta \cup \beta\alpha \subseteq \alpha \cup \beta$.

Произведение порядков также, вообще говоря, не является порядком (исключениями будут, например, тривиальные случаи $\alpha\beta = \Delta$, $\alpha\beta = \alpha$ или $\alpha\beta = \beta$). Для строгих порядков справедлива следующая

Теорема 3.3. Если α и β — строгие порядки и выполнены соотношения

$$\begin{cases} \alpha\beta = \beta\alpha, \\ \alpha \cap \beta^\# = \emptyset, \end{cases}$$

то $\alpha\beta$ — строгий порядок.

Определение 3.3. Пару $\mathfrak{P} = \langle P, \sqsubseteq \rangle$, где P — непустое множество, а \sqsubseteq — частичный порядок на нём, называют *частично упорядоченным множеством* (сокращённо *ч.у. множеством*).

Аксиомы порядка около 1690 г. рассматривал ещё Г. В. Лейбниц. Понятие ч.у. множества в математику введено Ф. Хаусдорфом в 1914 г. Развитие теории ч.у. множеств как самостоятельного предмета началось с работ Г. Биркгофа в 1930-х годах.

Ч.у. множество представляет собой пример нового типа алгебраической системы, а именно *модели*. АС является моделью, если в ней отсутствуют операции на носителе, но имеются отношения на нём. Любое множество можно превратить в частично упорядоченное, задав на нём некоторый порядок. Например, на двухэлементном множестве $\{x, y\}$ можно построить 3 различных порядка: тривиальный, $x \sqsubseteq y$ и $y \sqsubseteq x$.

Пример 3.4. 1. Модели $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{Q}, \leq \rangle$, $\langle \mathbb{N}, \leq \rangle$, $\langle \mathbb{N}, | \rangle$, $\langle B^n, \preceq \rangle$ и $\langle \mathcal{P}(\cdot), \subseteq \rangle$ суть ч.у. множества, причём последнее считается классическим примером этого понятия.

Ясно, что элемент y покрывает элемент x в $\langle \mathbb{N}, \leq \rangle$, если $y = x + 1$, в $\langle \mathbb{N}, | \rangle$ — если $\frac{y}{x}$ — простое число, в $\langle \mathcal{P}(A), \subseteq \rangle$ при конечном A , если $|y| = |x| + 1$.

Заметим, что если выбор любого подмножества n -элементного множества A равновероятен, то вероятность того, что два случайно выбранных из $\mathcal{P}(A)$ множества сравнимы (в том числе и совпадают), есть $\frac{2 \cdot 3^n - 2^n}{4^n}$ [12].

2. Совокупность лучей на прямой с отношением включения — ч.у. множество.
3. Для $A \neq \emptyset$ модель $\langle \mathcal{E}(A), \subseteq \rangle$ есть ч.у. множество, состоящее из разбиений множества A (имея в виду взаимно-однозначную связь между разбиениями множества и отношениями эквивалентности на нём) и *упорядоченных по измельчению*.
4. Множество конечных возрастающих последовательностей натуральных чисел, где

$$(a_1, \dots, a_k) \sqsubseteq (b_1, \dots, b_l)$$

означает, что $k \leq l$ и $a_i = b_i$ при $1 \leq i \leq k$.

Далее будут приведены и другие примеры порядков специального вида.

Ясно, что если $\langle P, \sqsubseteq \rangle$ — ч.у. множество, $Q \subseteq P$ и $\sqsubseteq|_Q$ — сужение отношения \sqsubseteq на Q , то и $\langle Q, \sqsubseteq|_Q \rangle$ — ч.у. множество. В этом случае Q называем *ч.у. подмножеством* P и, допуская некоторую вольность, порядок на P и его сужение на Q будем иногда обозначать одним и тем же символом.

Если на множестве P заданы порядки \sqsubseteq_1 и \sqsubseteq_2 и $\sqsubseteq_1 \subseteq \sqsubseteq_2$ (из $x \sqsubseteq_1 y$ следует $x \sqsubseteq_2 y$ для всех $x, y \in P$), то говорят, что *порядок \sqsubseteq_1 содержится в порядке \sqsubseteq_2* . При построении порядка, содержащего данный, говорят о *продолжении* последнего. Например, тривиальный порядок на одноэлементном множестве содержится в любом другом и может быть продолжен до него.

В зависимости от мощности P различают конечные и бесконечные ч.у. множества. Частично упорядоченное множество, все интервалы которого конечны, называется *локально конечным*. Например, ч.у. множество $\langle \mathbb{N}, \leq \rangle$ бесконечно, но локально конечно, а ч.у. множество $\langle \mathbb{Q}, \leq \rangle$ — не локально конечное.

Утверждение 3.2. Пусть $\langle P, \sqsubseteq \rangle$ — локально конечное ч.у. множество, и $x, y \in P$. Тогда $x \sqsubseteq y$, если и только если в P существуют такие элементы z_0, \dots, z_n (для некоторого $n \in \mathbb{N}_0$), что $x = z_0$, $y = z_n$ и $z_i \sqsubset z_{i+1}$ для всех $i = \overline{0, n-1}$.

Доказательство проводится индукцией по числу элементов n . □

Определение 3.4. Полный частичный порядок \leq на неединичном множестве P называется *линейным*. В этом случае ч.у. множество $\langle P, \leq \rangle$ называется *линейно упорядоченным* или *цепью*.

Иногда линейно упорядоченное множество называют *совершенно упорядоченным*; согласно определению, любые два его элемента сравнимы. Подмножество линейно упорядоченного множества само является линейно упорядоченным. Считается, что цепь содержит не менее двух элементов. Для строгого линейного порядка будем пользоваться обозначением $<$. n -элементная цепь обозначается \mathbf{n} ; иногда (из-за полиграфических трудностей) используют обозначение \underline{n} . Цепь $v_1 < \dots < v_n$ будем записывать как $[v_1, \dots, v_n]$. Обозначим $[n] = [1, \dots, n]$.

Длина цепи \mathbf{n} есть число $n - 1$. Одноэлементное ч.у. множество $\mathbf{1}$ называется *тривиальным*.

Все нетривиально упорядоченные ч.у. множества содержат цепи в качестве подмножеств. Цепь в ч.у. множестве называется *максимальной* или *насыщенной*, если её объединение с любым, не принадлежащим ей элементом, цепью не является. В ч.у. множестве $\langle \mathbb{N}, | \rangle$ цепью будет, например, совокупность некоторых степеней простого числа; $\{2^n \mid n \in \mathbb{N}\}$ — пример максимальной цепи.

Для наглядного представления конечных ч.у. множеств, имеющих небольшое число элементов, используют *диаграммы (Хассе)²* или *диаграммы покрытий*. На них изображают элементы ч.у. множеств, причём если элемент a предшествует элементу b , то a рисуют ниже b и соединяют их отрезком, если это предшествование непосредственное.

Следует отличать диаграммы Хассе от представления ч.у. множества в виде направленного графа: для последних требуется соединять дугой любую упорядоченную пару элементов, удовлетворяющую данному отношению, в то время как для первых предполагается отсутствие петель у вершин, транзитивность рёберных связей (в силу чего достаточно соединять вершины, соответствующие лишь покрывающим один другого элементам)

²Хельмут Хассе (Helmut Hasse, 1898–1979) — немецкий математик, автор фундаментальных работ по алгебре и теории чисел.

и отображение направленности рёбер взаимным расположением вершин (выше или ниже одна другой). Отметим, что ненаправленный граф, вершинам которого сопоставлены элементы ч.у. множества P , а две различные вершины смежны, если соответствующие элементы сравнимы, называется *графом сравнимости* P .

На рис. 3.1 приведены диаграммы Хассе: на а) — цепи $\mathbf{4}$, а на б) и в) — булеан трёхэлементного множества (или B^3). Последние две изображения показывают, что данного

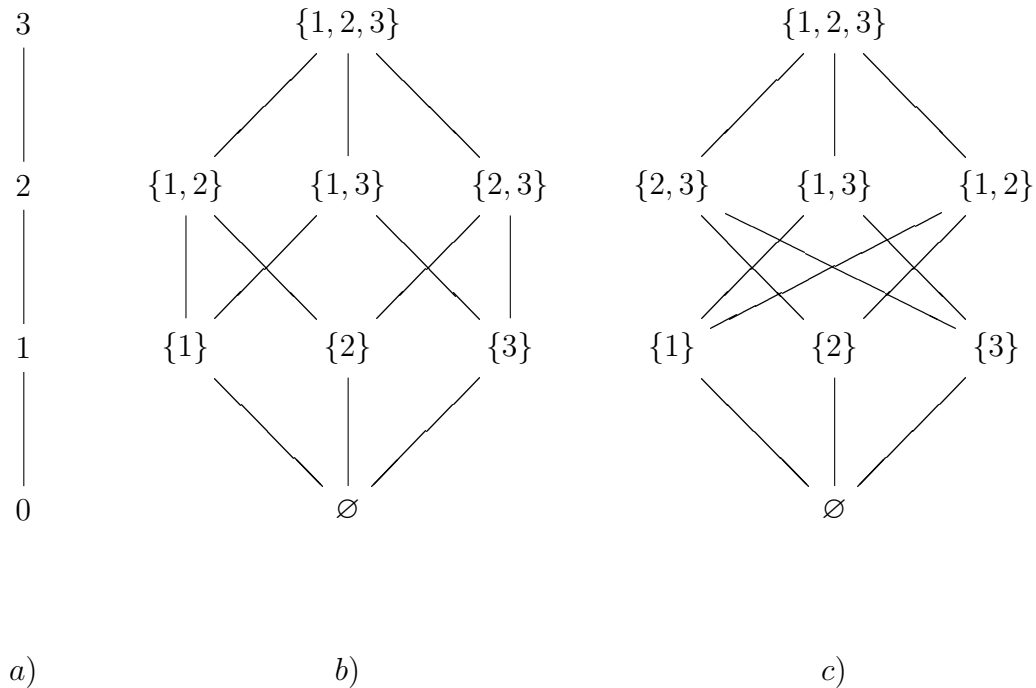


Рис. 3.1: Диаграммы (а) — цепи $\mathbf{4}$, (б) и (в) — булевой алгебры B^3

ч.у. множества можно построить много визуально отличающихся друг от друга диаграмм. По возможности, их стараются рисовать без самопересечений, например, на рис. 3.1б) приведено стандартное изображение булевой алгебры B^3 . Диаграммой Хассе ч.у. множества, определённого в п. 4 примера 3.4 будет некоторое дерево.

Обозначим через $D(N)$ — совокупность всех натуральных делителей числа N . На рис. 3.2 показаны одна из максимальных цепей ($\circ_1 \leftarrow \circ_2$ означает $\circ_1 < \circ_2$) и интервал $[3, 60]$ для ч.у. множества $D(180)$.

Пусть $h(n)$ — число неизоморфных как графов диаграмм n -элементных ч.у. множеств. Легко установить, что $h(1) = 1$, $h(2) = 2$ и $h(3) = 5$ (диаграммы тривиально упорядоченного множества и изображённые на рис. 3.3). В нижеследующей таблице для $n \leq 7$ приведены значения $h(n)$ и, для сравнения, числа $p(n)$ и $k(n)$ различных n -элементных частичных порядков и предпорядков соответственно.

n	1	2	3	4	5	6	7
$h(n)$	1	2	5	16	63	318	2045
$p(n)$	1	3	19	219	4231	130023	6129856
$k(n)$	1	3	29	355	6942	209527	9535241

Ясно, что эти числа $h(n)$, $p(n)$ и $k(n)$ растут очень быстро. “Компактных” (не содержащих суммирования и не подразумевающих перебора всех или почти всех элементов)

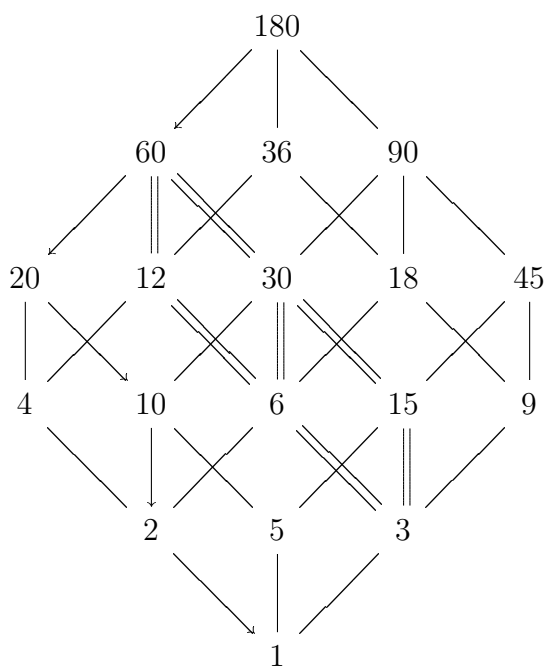


Рис. 3.2: Диаграмма Хассе для $D(180)$

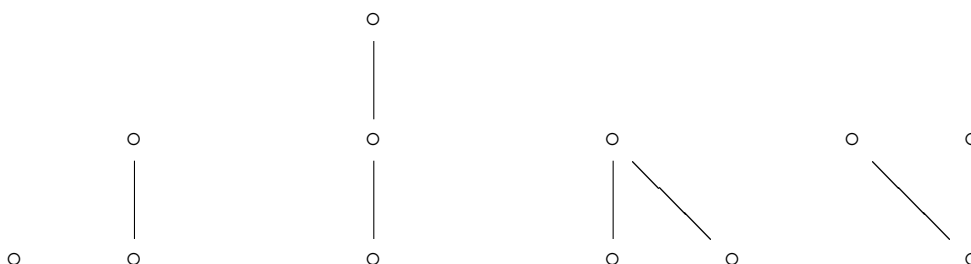


Рис. 3.3: Диаграммы нетривиальных трёхэлементных ч.у. множеств

формул для них $h(n)$, $p(n)$ и $k(n)$ неизвестно, и вряд ли они существуют. В первом приближении для $h(n)$ справедлива асимптотика

$$\ln h(n) \sim \frac{n^2}{4} \ln 2.$$

(здесь $g(n) \sim f(n)$ означает $\lim_{n \rightarrow \infty} g(n)/f(n) = 1$).

Иногда диаграммы Хассе рисуют и для бесконечных ч.у. множеств. Конечно, все элементы такого множества изобразить невозможно, но получающиеся рисунки дают ясное представление об его устройстве. На рис. 3.4.a) представлена бесконечная цепь $\langle \mathbb{N}_0, \leq \rangle$, а на рис. 3.4.b) — бесконечное ч.у. множество, все цепи которого конечны. Некоторые диаграммы имеют свои традиционные названия. Этими же именами мы будем пользоваться и для обозначения соответствующих ч.у. множеств. И вообще, когда это не приводит к двусмысленности, мы не будем различать ч.у. множество и его диаграмму.

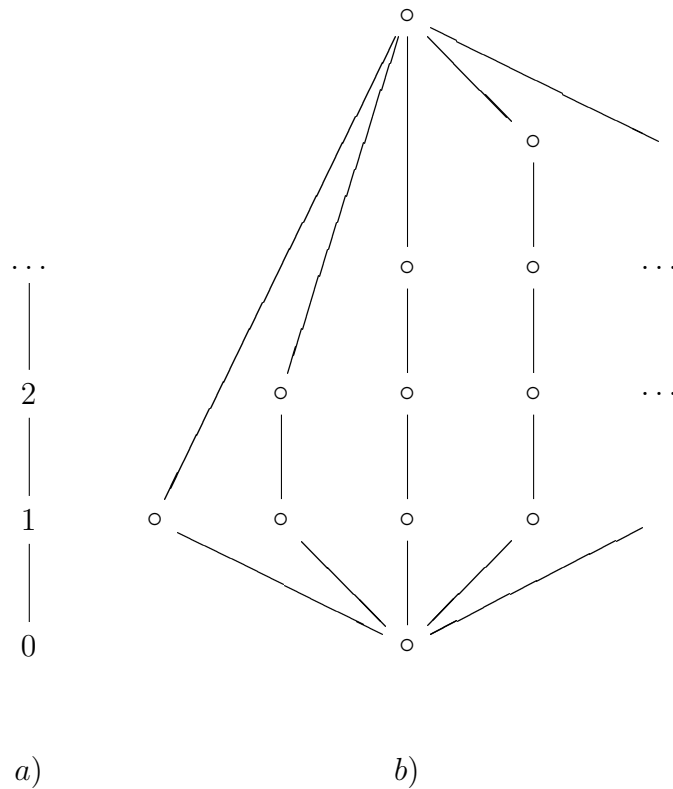


Рис. 3.4: Диаграммы Хассе бесконечных ч.у. множеств

3.2 Особые элементы и основные свойства ч.у. множеств

В ч.у. множествах выделяют особые элементы.

Определение 3.5. Элемент $u \in P$ ч.у. множества $\langle P, \sqsubseteq \rangle$ называют:

- *максимальным*, если $u \sqsubseteq x \Rightarrow u = x$,
- *минимальным*, если $u \sqsupseteq x \Rightarrow u = x$,
- *наибольшим*, если $x \sqsubseteq u$,
- *наименьшим*, если $x \sqsupseteq u$

для любых $x \in P$.

Из определений ясно, что элемент наибольший, если все другие элементы содержатся в нём, и он максимальный, если нет элементов, содержащих его (аналогично для наименьшего и минимального элементов).

Легко видеть, что ч.у. множество может иметь не более, чем по одному наибольшему и наименьшему элементу. Их называют соответственно *единицей* и *нулём*, а также *универсальными гранями* данного ч.у. множества; мы будем использовать для них обозначения 1 и 0 соответственно. Ч.у. множество с универсальными гранями называется *ограниченным ч.у. множеством*, или, короче, *ограниченным порядком*. Понятно, что наибольший [наименьший] элемент есть одновременно и единственный максимальный [минимальный]. С другой стороны, максимальных или минимальных элементов может быть несколько, а может и не быть совсем. Например, ч.у. множество, изображённое на рис. 3.6 имеет один наименьший (он же минимальный) и 3 максимальных элемента. Заметим, что в приложениях совокупность максимальных элементов ч.у. множества называют

множеством Парето. В ч.у. множестве с o интервалы вида $[o, x]$ называют *начальными*; двойственно, в ч.у. множестве с ι интервалы вида $[x, \iota]$ называют *финальными*.

Говорят, что *высота* ч.у. множества P равна n (символически $h(P) = n$) если в P существует цепь, содержащая $n + 1$ элемент, и нет цепей, содержащих большее число элементов. *Высотой элемента v* (символически $h(v)$) в конечном упорядоченном множестве называется наибольшая из длин цепей $[v_0, \dots, v]$, где v_0 — минимальный элемент. Понятно, что все минимальные элементы имеют высоту 0.

Антицепь (семейство Шпернера, клаттер) есть непустое подмножество A ч.у. множества P , в котором любые два элемента или равны, или несравнимы. Например, в ч.у. множестве $\langle \mathbb{N}, | \rangle$ антицепью является произвольное подмножество попарно некрратных чисел, а в множестве $\langle B^n, \preceq \rangle$ — совокупности верхних нулей либо нижних единиц некоторой (не тождественной константам) монотонной булевой функции. Одноэлементное подмножество ч.у. множества называют *тривиальной антицепью*.

Задача определения количества $\psi(n)$ антицепей (включая пустую) в B^n называется *проблемой Дедекинда*. Данной тематике посвящена обширная литература³. Первые значения $\psi(n)$ приведены в нижеследующей таблице

n	1	2	3	4	5	6	7
$\psi(n)$	3	6	20	168	7 581	7 828 354	2 414 682 040 998

Точной формулы для $\psi(n)$ неизвестно и вряд ли она существует. Найдены, однако, приближённые формулы для $\psi(n)$: например, для чётных n для $\psi(n)$ справедлива приближённая формула

$$\psi(n) \sim 2^{\binom{n}{n/2}} \exp \left\{ \binom{n}{n/2-1} \left(\frac{1}{2^{n/2}} + \frac{n^2-2n}{2^{n+5}} \right) \right\},$$

которая для $n = 6$ даёт 7 996 118.

Говорят, что *ширина* ч.у. множества P равна n (символически $w(P) = n$) если в P существует антицепь, содержащая n элементов, и нет антицепей, содержащих большее число элементов.

Теорема 3.4 (Дилоурс⁴). *Ч.у. множество ширины w может быть разбито на w цепей. Ч.у. множество высоты h может быть разбито на h антицепей.*

В теории ч.у. множеств известно следующее

Цепное условие Жордана–Дедекинда. *Все максимальные цепи между двумя данными элементами ч.у. множества имеют одинаковую (конечную) длину.*

Если максимальные цепи ч.у. множества P имеют одну и ту же длину n , то говорят, что данное ч.у. множество — *градуированное (ранжированное) ранга n* . Легко показать [1], что цепное условие Жордана–Дедекинда выполняется для всех градуированных ч.у. множеств и только для них. Ч.у. множество не ранжировано, если оно содержит $\mathbf{1} + \mathbf{2}$ в качестве ч.у. подмножества.

Для градуированных множеств существует единственная *ранговая функция* $\rho : P \rightarrow \{0, 1, \dots, n\}$ такая, что $\rho(x) = 0$, если x — минимальный элемент P и $\rho(y) = \rho(x) + 1$, если y покрывает x . Если $\rho(x) = k$, то говорят, что элемент x имеет *ранг k* . Элементы одного ранга образуют *слой* соответствующего градуированного ч.у. множества.

³См., например, *Коршунов А.Д.* Решение проблемы Дедекинда о числе монотонных функций булевых функций // Докл. АН СССР. — 223, № 4, с. 543–546 и *Сапоженко А.А.* Проблема Дедекинда и метод граничных функционалов. М.: ФИЗМАТЛИТ, 2009.

⁴*Dilworth R.* A decomposition theorem for partially ordered sets. Annals of Mathematics, **51**, 161–166.

Пример 3.5. 1. Цепь и булеан, изображённые на рис. 3.1, суть градуированные множества ранга 3, вес первого есть 1, а второго — 3.

2. *Разбиением натурального числа n* называется его представление неупорядоченной суммой натуральных невозрастающих слагаемых: $n = n_1 + \dots + n_r$, при этом слагаемые n_i называются *частями*, а их число r — рангом разбиения. Записываются разбиения обычно в векторной форме: (n_1, \dots, n_r) .

На множестве $P(n)$ всех разбиений числа n устанавливается частичный порядок по их *вложимости*. Говоря, что разбиение $a = (n_1, \dots, n_t)$ вложимо в разбиение $b = (m_1, \dots, m_r)$ (символически $a \preceq b$), если a может быть получено из b подразбиением некоторых своих элементов. Например, $(2, 2, 2) \preceq (4, 2)$, но $(2, 2, 2) \not\preceq (3, 3)$. Очевидно, $P(n)$ — градуированное множество и $n - r$ есть ранг элемента (n_1, \dots, n_r) в ч.у. множестве $P(n)$. Диаграмма Хассе ч.у. множества $P(6)$ представлена на рис. 3.5. Ясно, что $P(n)$ — ограниченный порядок.

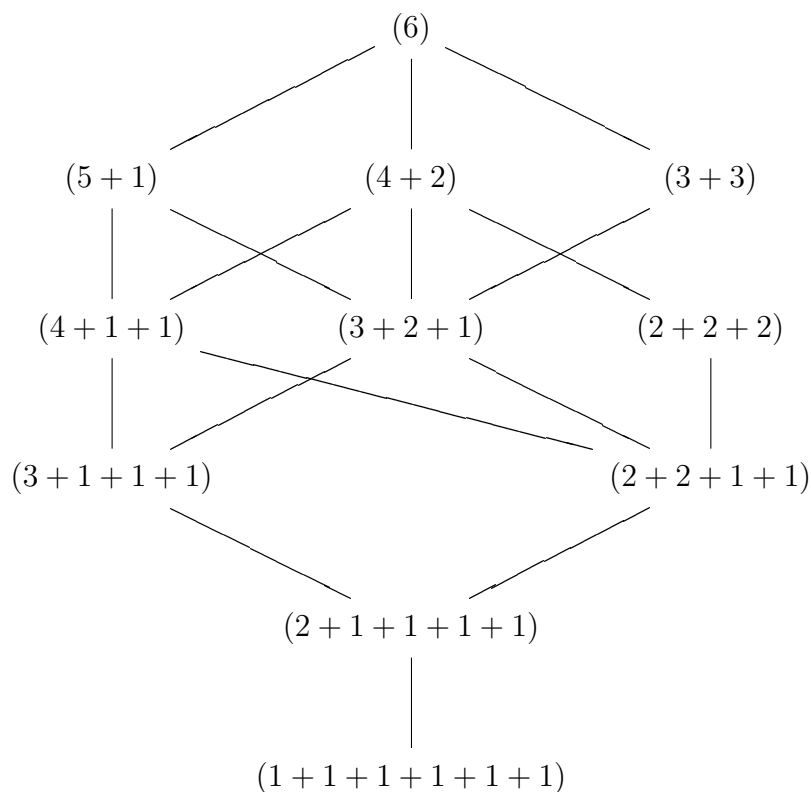


Рис. 3.5: $P(6)$

3. Ч.у. множество $\langle \mathbb{N}, | \rangle$ ранжировано. Все его уровни, за исключением нулевого, содержат счетное число элементов, причем k -й уровень состоит из всех тех натуральных чисел, примарное разложение которых содержит k (не обязательно различных) простых множителей.

Ясно, что слой градуированного ч.у. множества есть антицепь — например, слой $\{(5 + 1), (4 + 2), (3 + 3)\}$ ранга 4 ч.у. множества $P(6)$ на рис. 3.5. Однако не всякая антицепь есть слой: на рис. 3.6 представлено градуированное ч.у. множество, у которого элементы максимальной антицепи, обозначенные \bullet , не принадлежат какому-то одному слою.

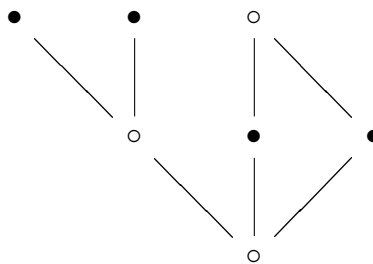


Рис. 3.6: Ч.у. множество, не обладающее свойством Шпернера

Число элементов в k -м слое градуированного ч.у. множества P обозначают $W_k(P)$ и называют *числом Уитни*⁵ ч.у. множества P . Говорят, что конечное градуированное ч.у. множество P обладает свойством Шпернера, если

$$\max_k W_k(P) = w(P).$$

(при этом ясно, что всегда $\max_k W_k(P) \leq w(P)$). Например, ч.у. множество, изображённое на рис. 3.6, не обладает свойством Шпернера, т.к. у него $\max_k W_k(P) = 3$, а $w(P) = 4$.

Определение 3.6 (LYM-свойство⁶). Пусть Q — подмножество элементов ранжированного ч.у. множества P с ранговой функцией ρ . Говорят, что для Q выполняется LYM-неравенство, если

$$\sum_{x \in Q} \frac{1}{W_{\rho(x)}} \leq 1.$$

Ч.у. множество обладает LYM-свойством (или является LYM-порядком), если любая антицепь в P удовлетворяет LYM-неравенству.

Легко показывается, что ч.у. множество, обладающее LYM-свойством, обладает и свойством Шпернера. Первоначально было установлено, что LYM-свойству удовлетворяет булев куб, т.е. если антицепь в B^n имеет a_k элементов в k -м слое B^n , то выполняется неравенство

$$\sum_{k=0}^n \frac{a_k}{\binom{n}{k}} \leq 1.$$

Решётка делителей $D(N)$ обладает LYM-свойством, а решётка разбиений Π_n обладает им только при $n < 20$. Заметим, что декартово произведение LYM-порядков может потерять данное свойство.

Теорема 3.5. В конечном ч.у. множестве каждый элемент содержится в некотором максимальном элементе и содержит некоторый минимальный элемент.

Доказательство. Пусть x — произвольный элемент ч.у. множества $\langle P, \sqsubseteq \rangle$. Если x не максимален, то найдётся такой элемент $x_1 \in P$, что $x \sqsubseteq x_1$. Повторяя рассуждения

⁵Точнее, числом Уитни второго рода. О числах Уитни первого рода см., например, [36].

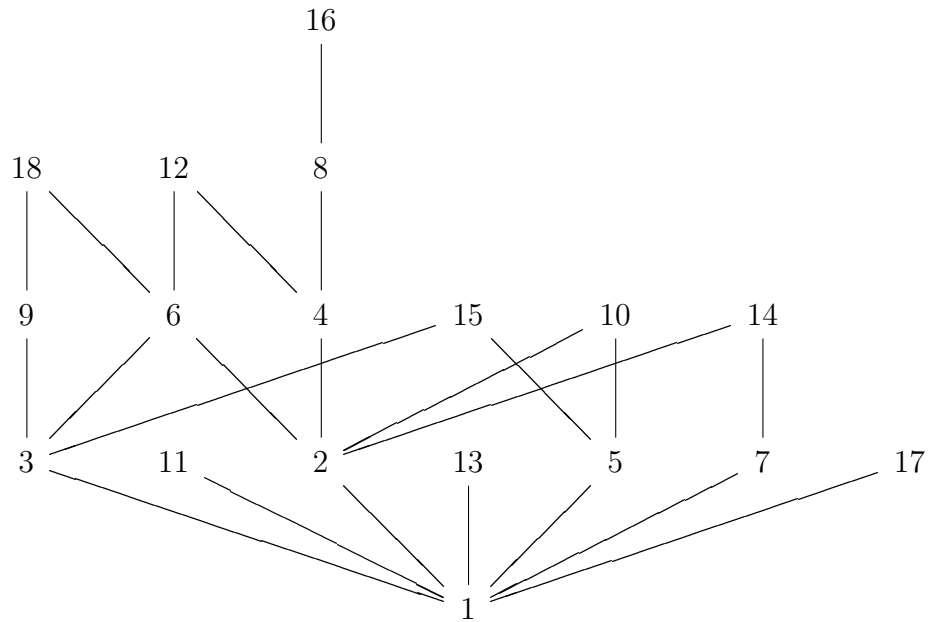
⁶Или *неравенство Любеля-Ямамото-Мешалкина*. См. Lubell, D. A short proof of Sperner's lemma. Journal of Combinatorial Theory 1, (1966) 299; Мешалкин Л.Д. Обобщение теоремы Шпернера о числе подмножеств конечного множества // Теория вероятностей и её применение — № 8, 1963. — с. 219–220 и Yamamoto, K. Logarithmic order of free distributive lattices. Journal of the Mathematical Society of Japan 6, (1954) 343–353 (т.е. первым был всё-таки К. Ямамото).

для новых элементов, получаем возрастающую цепь $x \sqsubseteq x_1 \sqsubseteq \dots$. Поскольку множество P конечно, то и данная цепь конечна. Её последний элемент x_n , по определению будет максимальным элементом P и $x \sqsubseteq x_n$.

Для нахождения минимального элемента рассуждения аналогичны, при этом строится убывающая цепь. \square

Пример 3.6. 1. Рассмотрим ч.у. множество $\langle N_f^1, \preceq \rangle$, где N_f^1 — множество единичных наборов монотонной булевой функции $f(x_1, x_2, x_3, x_4, x_5) = x_1 \vee x_2x_3 \vee x_3x_4x_5$. Для N_f^1 нижние единицы (10000), (01100) и (00111) функции f будут минимальными элементами, $\tilde{1} = (11111)$ — максимальным и наибольшим элементом, а наименьший элемент в N_f^1 отсутствует.

2. Ч.у. множество $\langle \{1, \dots, 18\}, | \rangle$ имеет следующую диаграмму:



Здесь 1 — наименьший элемент, 10, ..., 18 — максимальные, а наибольшего элемента нет.

3. В ограниченном ч.у. множестве $\langle \mathcal{P}(A), \subseteq \rangle$ наименьшим элементом является пустое множество \emptyset , а наибольшим — само множество A .

В ч.у. множестве $\langle \mathcal{P}^*(A), \subseteq \rangle$ при $|A| > 1$ нет наименьшего элемента, а минимальными являются все одноэлементные подмножества.

Будем обозначать через $\mathcal{P}_0(A)$ совокупность всех конечных подмножеств бесконечного множества A . В ч.у. множестве $\langle \mathcal{P}_0(A), \subseteq \rangle$ наименьшим элементом будет пустое подмножество, а максимальных (следовательно, и наибольшего) элементов нет.

Сечением цепи $\langle C, \leq \rangle$ называют разбиение её на два подмножества A (нижний класс сечения) и B (верхний класс сечения) так, что $a < b$ для любых $a \in A$ и $b \in B$. Различают следующие виды сечений:

- *скачок* — в нижнем классе имеется наибольший элемент, а в верхнем классе — наименьший;
- *дедекиндово сечение* — либо в нижнем классе имеется наибольший элемент, а в верхнем классе наименьшего элемента нет, либо в верхнем классе имеется наименьший элемент, а в нижнем классе наибольшего элемента нет;
- *цель* — в нижнем классе нет наибольшего элемента, а в верхнем — наименьшего.

Цепь называется *непрерывной*, если все её сечения дедекиндовы.

Если ч.у. множество имеет наименьший элемент, то элементы, непосредственно следующие за ним, называют *атомами*. Понятно, что таковых может и не оказаться. Легко показывается, что данное определение атома ч.у. множества совпадает с определением 1.4 атома булевой алгебры, если в ней принять $x \sqsubseteq y \Leftrightarrow x = x \sqcap y$ (см. утверждение 5.1).

Двойственно определяются *дуальные атомы* или *коатомы* или *антиатомы*: это элементы, непосредственно предшествующие наибольшему элементу (в предположении, что таковой существует).

Пример 3.7. 1. Конечная нетривиальная цепь содержит единственные атом и коатом.
2. Положим формально, что $0|0$. Тогда в ч.у. множестве $\langle \mathbb{N}_0, | \rangle$ наименьшим элементом является 1, наибольшим — 0, атомы суть простые числа, а коатомы отсутствуют.

3.3 Грани, изотонные отображения и порядковые идеалы

Определение 3.7. Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $\emptyset \neq A \subseteq P$. Множества A^Δ и A^∇ определяемые условиями

$$A^\Delta = \{x \in P \mid \forall_A (a \sqsubseteq x)\} \quad \text{и} \quad A^\nabla = \{x \in P \mid \forall_A (x \sqsubseteq a)\}$$

называются *верхним* и *нижним конусами* множества A , а их элементы — *верхними* и *нижними гранями* множества A соответственно. Верхний [нижний] конус одноэлементного множества $A = \{a\}$ обозначают a^Δ [a^∇].

Верхним и нижним конусами пустого подмножества элементов P считают само множество P .

Понятно, например, что если $a \sqsubseteq b$, то $a^\Delta \cap b^\nabla = [a, b]$. Иногда верхние [нижние] грани называют *мажорантами* [*минорантами*] соответствующего множества.

Теорема 3.6 (основные свойства верхнего и нижнего конусов). Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество, $A, B \subseteq P$ и $x, y \in P$. Тогда

- 1) $A \subseteq B \Rightarrow B^\nabla \subseteq A^\nabla$ и $B^\Delta \subseteq A^\Delta$ (антимонотонность конусов подмножеств по включению);
- 2) $A \subseteq A^{\Delta\nabla} \cap A^{\nabla\Delta}$;
- 3) $A^\Delta = A^{\Delta\nabla\Delta}$;
- 4) $A^\nabla = A^{\nabla\Delta\nabla}$;
- 5) $(A \cup B)^\Delta = A^\Delta \cap B^\Delta$;
- 6) $(A \cup B)^\nabla = A^\nabla \cap B^\nabla$;
- 7) $x \sqsubseteq y \Leftrightarrow x^\nabla \subseteq y^\nabla$ и $y^\Delta \subseteq x^\Delta$.

Доказательство.

- 1) Это свойство (антимонотонность операций перехода к верхнему и нижнему конусам по включению множеств) вытекает непосредственно из определения.
- 2) Так как для любых $x \in A$ и $y \in A^\Delta$ справедливо $x \sqsubseteq y$, то $A \subseteq A^{\Delta\nabla}$. Аналогично показывается $A \subseteq A^{\nabla\Delta}$, откуда и следует требуемое.
- 3), 4) $A^\Delta \stackrel{(2)}{\subseteq} (A^\Delta)^{\nabla\Delta} = (A^{\Delta\nabla})^\Delta \stackrel{(1)}{\subseteq} A^\Delta$ и аналогично для (4).
- 5), 6) Включение $(A \cup B)^\Delta \subseteq A^\Delta \cap B^\Delta$ вытекает из (1). Если же $x \in A^\Delta \cap B^\Delta$, то $y \sqsubseteq x$ для всех $y \in A$ и $y \in B$, откуда следует справедливость свойства (5). Аналогично для (6).

- 7) Свойство (монотонность и антимонотонность операций взятия соответственно главного идеала и главного фильтра) сразу следует из определений. \square

Определение 3.8. Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $A \subseteq P$. Если в A^Δ существует наименьший элемент, то он называется *точной верхней гранью множества A* и обозначается $\sup A$. Если в A^∇ существует наибольший элемент, то он называется *точной нижней гранью множества A* и обозначается $\inf A$ ⁷.

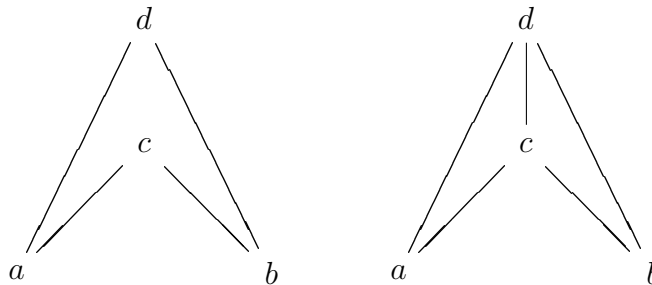
Точной верхней [нижней] гранью пустого множества считают наименьший [наибольший] элемент ч.у. множества.

Понятно что

$$\inf A \sqsubseteq a \sqsubseteq \sup A \quad \text{для всех } a \in A.$$

Также, если $\sup A$ или $\inf A^\Delta$ существует, то $\sup A = \inf A^\Delta$ и двойственно, если $\inf A$ или $\sup A^\nabla$ существует, то $\inf A = \sup A^\nabla$.

Пример 3.8. 1. Пусть $P = \{a, b, c, d\}$ и два различных порядка на P задаются следующими диаграммами:



Для $A = \{a, b\}$ имеем $A^\Delta = \{c, d\}$ в обоих случаях, но в первом случае $\sup A$ отсутствует, а во втором $\sup A = c$ (строго говоря, вторая диаграмма не есть диаграмма Хассе: линии, соединяющие d с a и b здесь излишни).

2. Для элемента $\tilde{\alpha}$ ч.у. множества $\langle B^n, \preceq \rangle$ имеем

$$\tilde{\alpha}^\Delta = [\tilde{\alpha}, \tilde{1}], \quad \tilde{\alpha}^\nabla = [\tilde{0}, \tilde{\alpha}]; \quad \sup \tilde{\alpha} = \inf \tilde{\alpha} = \tilde{\alpha}.$$

3. Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $A \subseteq B \subseteq P$. Если существуют $\sup A$ и $\sup B$ ($\inf A$ и $\inf B$), то $\sup A \sqsubseteq \sup B$ ($\inf A \supseteq \inf B$).

4. Для ч.у. множества рациональных чисел \mathbb{Q} с естественным упорядочением имеем

- $\sup \{x \in \mathbb{Q} \mid x < 0\} = 0$;
- $\sup \{x \in \mathbb{Q} \mid x^2 < 2\}$ не существует;
- $\sup \{x \in \{\mathbb{Q} \cup \{\sqrt{2}\}\} \mid x^2 < 2\} = \sqrt{2}$.

5. Если S — совокупность подмножеств некоторого множества, то, по включению, $\sup S$ совпадает с объединением, а $\inf S$ — с пересечением всех подмножеств из совокупности S .

Определение 3.9. Пусть P и P' — ч.у. множества и x, y — произвольные элементы из P . Отображение $\varphi: P \rightarrow P'$ называется соответственно

- *изотонным* отображением, если $x \sqsubseteq y \Rightarrow \varphi(x) \sqsubseteq \varphi(y)$, изотонные отображения называют также *монотонными* или *порядковыми гомоморфизмами*;
- *обратно изотонным* отображением, если $\varphi(x) \sqsubseteq \varphi(y) \Rightarrow x \sqsubseteq y$;

⁷Названия происходят от лат. *supremum* — самый высокий и *infimum* — самый низкий.

- *антиизотонным*, если $x \sqsubseteq y \Rightarrow \varphi(x) \supseteq \varphi(y)$.

Если φ изотонно, обратно изотонно и инъективно, то его называют *вложением* или (*порядковым*) *мономорфизмом* ч.у. множества P в ч.у. множество P' , что обозначают $P \xrightarrow{\varphi} P'$.

Сюръективный мономорфизм ч.у. множеств называют (*порядковым*) *изоморфизмом* (символически $P \cong P'$ или, с указанием на отображение — $P \xrightarrow{\cong} P'$).

Понятно, что для ч.у. множеств P и P' отображение $\varphi: P \rightarrow P'$ есть порядковый изоморфизм, если и только если P — изотонная и обратно изотонная биекция, т.е. для любых $x, y \in P$ справедливо $x \sqsubseteq y \Leftrightarrow \varphi(x) \sqsubseteq \varphi(y)$. Заметим, что биективность φ может быть выведена из последнего условия.

Пример 3.9. 1. Ч.у. множество a), изображённое на рис. 3.1 является изотонным образом ч.у. множества b), если в качестве отображения взять функцию $\varphi(x) = |x|$. Это отображение не инъективно и, следовательно, вложением не является.

2. Тожественное отображение ч.у. множества $\langle \mathbb{N}, | \rangle$ во множество натуральных чисел с естественным порядком изотонно, но не обратно изотонно и, следовательно, вложением также не является.

3. При продолжении любого частичного порядка \sqsubseteq на до линейного \leq естественное вложение $\langle M, \sqsubseteq \rangle \xrightarrow{\text{id}} \langle M, \leq \rangle$ изотонно и взаимно-однозначно, но не является мономорфизмом из-за отсутствия обратной изотонности и, тем более, не является изоморфизмом.

В частности, если Q — одноэлементное ч.у. множество с тривиальным порядком, а Q' — то же самое множество с произвольным нетривиальным порядком, то тождественное отображение Q на себя является изотонным и взаимно-однозначным, но не обратно изотонным.

4. Естественное вложение $n\mathbb{Z}$ в \mathbb{Z} для натурального n есть мономорфизм.

5. Отображение φ булеана непустого множества X в себя такое, что $\varphi(A) = \bar{A}$ для $A \subseteq X$, есть антиизотонное отображение.

6. $\mathbf{n} \cong [1, \dots, n]$ (т.е. любая n -элементная цепь изоморфна цепи целых чисел от 1 до n с естественным порядком).

Утверждение 3.3. Пусть $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — ч.у. множества, φ — изотонное отображение из P в Q , $A \subseteq P$ и существуют как $\sup A$ в P , так и $\sup \varphi(A)$ в Q , то $\sup \varphi(A) \sqsubseteq_Q \varphi(\sup A)$.

Определение 3.10. Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество. Подмножество I элементов P называется его *порядковым идеалом*, если

$$x \in I \ \& \ y \sqsubseteq x \Rightarrow y \in I.$$

Подмножество F элементов P называется его *порядковым фильтром* или *двойственным порядковым идеалом*, если

$$x \in F \ \& \ x \sqsubseteq y \Rightarrow y \in F.$$

Таким образом, порядковые идеалы ч.у. множества суть такие его подмножества, которые вместе с каждым своим элементом содержат все элементы, предшествующие ему. Двойственно, порядковые фильтры ч.у. множества суть такие его подмножества, которые вместе с каждым своим элементом содержат все элементы, следующие за ним. Порядковые идеалы [фильтры] называют также *полуидеалами* или *нижними множествами*

[полуфильтрами, верхними множествами]. Согласно определению, пустое множество также является порядковым идеалом и фильтром любого ч.у. множества.

Ясно, что объединение и пересечение порядковых идеалов есть порядковый идеал. Очевидно, x^∇ и x^Δ для любого элемента x ч.у. множества P являются порядковыми идеалом и фильтром соответственно. Такие идеалы и фильтры называют *главными*. Далее используется обозначение $J(x) = x^\nabla$.

Множество всех порядковых идеалов ч.у. множества P , упорядоченное по включению, образует ч.у. множество, которое мы будем обозначать $J(P)$. Например, если $P = \mathbf{n}$, т.е. является n -элементной цепью, то $J(\mathbf{n}) \cong (\mathbf{n} + \mathbf{1})$ (причина заключения $\mathbf{n} + \mathbf{1}$ в скобки будет ясна из дальнейшего). В другом крайнем случае, если P — n -элементная антицепь, то любое подмножество в P есть его порядковый идеал, $J(P)$ будет булеаном P и $J(P) \cong B^n$. Понятно также, что $J(P^\#) = J^\#(P)$.

Обозначим $J_0(P) = \bigcup_{x \in P} J(x)$. Ясно, что $J_0(P)$ — ч.у. подмножество $J(P)$.

Теорема 3.7 (о представлении ч.у. множеств). *Любое ч.у. множество может быть вложено в булеан подходящего множества, упорядоченный по включению.*

Доказательство. Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество. Докажем, что $\varphi(x) = x^\nabla$ будет изоморфизмом между P и $J_0(P)$.

Покажем сначала, что φ — биекция. Действительно,

$$\varphi(x) = \varphi(y) \Leftrightarrow (x^\nabla = y^\nabla) \Leftrightarrow (x \in y^\nabla) \& (y \in x^\nabla) \Leftrightarrow (x \sqsubseteq y) \& (y \sqsubseteq x) \Leftrightarrow x = y,$$

т.е. φ — вложение. Также очевидно, что каждому главному идеалу x^∇ соответствует порождающий его элемент x и поэтому φ — наложение.

Изотонность и обратная изотонность φ устанавливается п. 7) теоремы 3.6:

$$x \sqsubseteq y \Leftrightarrow x^\nabla \subseteq y^\nabla \Leftrightarrow \varphi(x) \subseteq \varphi(y).$$

Таким образом, $P \cong J_0(P) \xrightarrow{id} J(P) \xrightarrow{id} \mathcal{P}(P)$. □

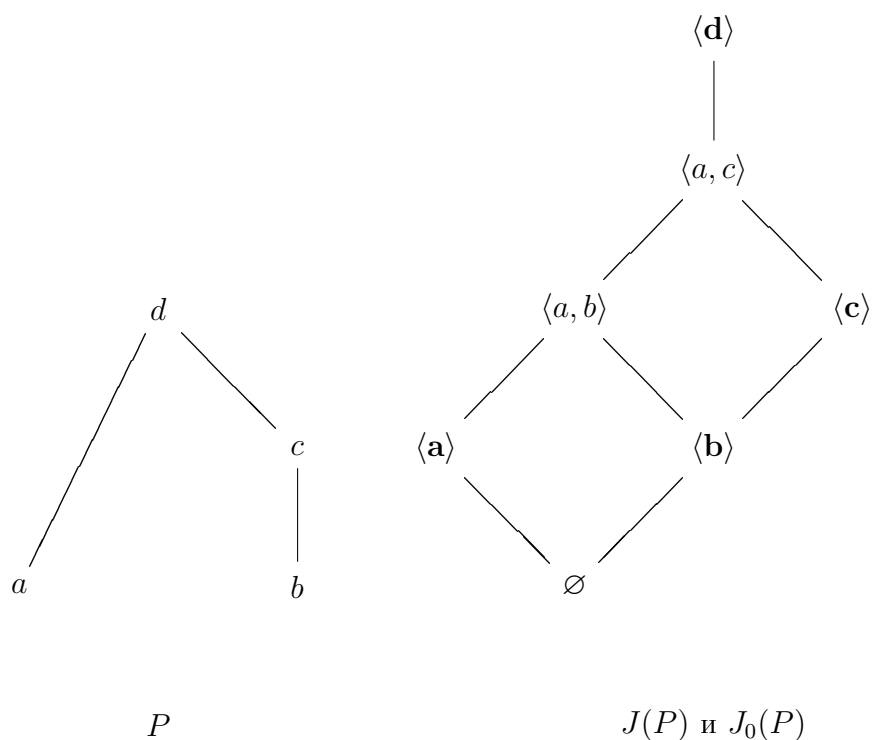
Заметим, что установленный изоморфизм $P \cong^{x^\nabla} J_0(P)$ часто используется при доказательствах различных свойств ч.у. множеств.

Подчеркнём взаимно-однозначное соответствие между его анитцепями и порядковыми идеалами конечного ч.у. множества. Действительно, с одной стороны, множество M максимальных элементов идеала I есть антицепь (возможно, тривиальная), а с другой — $I = \bigcup_{a \in M} a^\nabla$. Если некоторое подмножество A ч.у. множества и его идеал I связаны таким соотношением, то говорят, что A порождает I . В случае $A = \{a_1, \dots, a_k\}$ пишут $I = \langle a_1, \dots, a_k \rangle$ и говорят, что идеал I *конечнопорождённый*. Ясно, что $J(a) = \langle a \rangle$.

Пример 3.10. На рис. 3.7 показаны диаграммы четырёхэлементного ч.у. множества P и множества его порядковых идеалов $J(P) = \{\emptyset, \{a\} = \langle a \rangle, \{b\} = \langle b \rangle, \{a, b\} = \langle a, b \rangle, \{c, b\} = \langle c \rangle, \{a, b, c\} = \langle a, c \rangle, \{a, b, c, d\} = \langle d \rangle\}$. Множество $J_0(P)$ выделено жирным шрифтом и изоморфизм $P \cong J_0(P)$ легко проверяется. Каждому порядковому идеалу из $J(P)$ соответствует антицепь P , его порождающая.

Теорема 3.8. *Если P — ч.у. множество, то $J(P)$ — градуированное ч.у. множество ранга n , причём, если $\rho(I)$ — ранг идеала $I \in J(P)$, то $\rho(I) = |I|$.*

Доказательство. Утверждение теоремы следует из того, что порядковые идеалы, являющиеся надмножествами данного идеала I суть идеалы вида $I \cup \{x\}$, где x — минимальный элемент множества $P \setminus I$. □

Рис. 3.7: Ч.у. множества P и $J(P)$ (подмножество $J_0(P)$ выделено)

3.4 Операции над ч.у. множествами

Для однородных отношений можно⁸ вводить различные операции. Мы будем рассматривать только операции над конечными ч.у. множествами.

Присоединение универсальных граней. \widehat{P} — ч.у. множество, полученное из P присоединением универсальных граней o и/или ι , если последнее соответствующего элемента не содержит — см. пример на рис. 3.8.

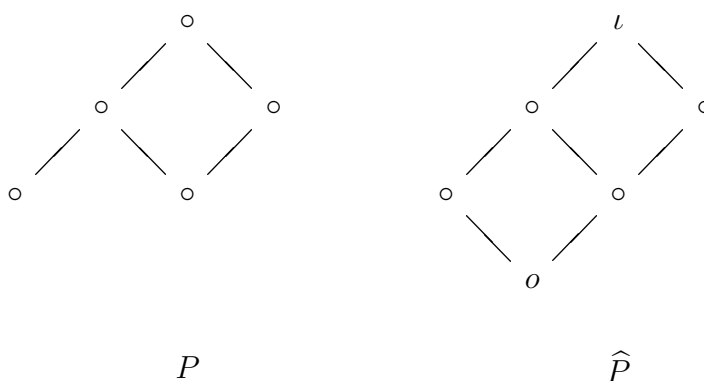


Рис. 3.8: Присоединение универсальных граней

⁸См. Уайтхед А.Н., Рассел Б. Основания математики: в 3 т. — Самара: Книга, 2005—2006.

Двойственность. Если P — ч.у. множество с порядком \sqsubseteq , то ч.у. множество с тем же носителем и порядком \supseteq назовём *дуальным* или *двойственным* к P и обозначим P^\sharp .

Диаграмма Хассе множества P^\sharp есть диаграмма ч.у. множества P перевернутая “вверх ногами”, при этом диаграммы самодвойственных множеств не изменятся.

Если $P \cong P^\sharp$, то ч.у. множество P называют *самодвойственным*. Показанные на рис. 3.9 ч.у. множества будем называть зигзагами; два первые ч.у. множества двойственны друг другу, а последнее — самодвойственно. На рис. 3.10 показаны диаграммы

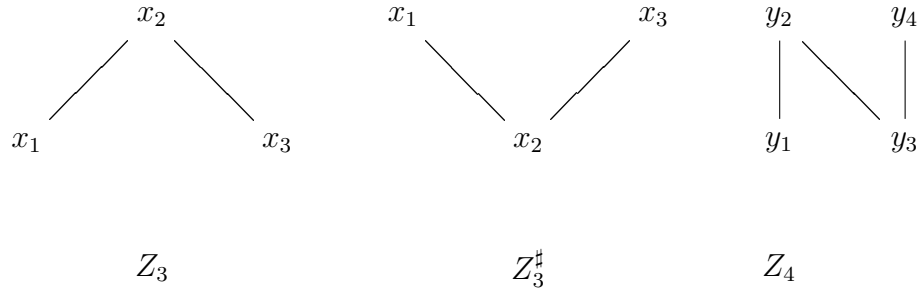


Рис. 3.9: Диаграммы Хассе зигзагов

самодвойственных ч.у. множеств.



Рис. 3.10: Пятиэлементные самодвойственные ч.у. множества

Ясно, что к ч.у. множествам применим следующий

Принцип двойственности (для частично упорядоченных множеств). *Любое утверждение, истинное для произвольных элементов ч.у. множества, остаётся таковым в ч.у. множестве, дуальном к нему.*

Пересечение. Пусть $\langle P, \sqsubseteq_1 \rangle$ и $\langle P, \sqsubseteq_2 \rangle$ — два ч.у. множества, имеющие общий носитель. *Пересечением* этих ч.у. множеств будет ч.у. множество $\langle P, \sqsubseteq \rangle$ с тем же носителем P и порядком $\sqsubseteq = \sqsubseteq_1 \cap \sqsubseteq_2$. При построении диаграммы ч.у. множества $\langle P, \sqsubseteq_1 \cap \sqsubseteq_2 \rangle$ вершину x рисуют ниже вершины y и соединяют их отрезком, если y покрывает x как по \sqsubseteq_1 , так и по \sqsubseteq_2 ; пример см. на рис. 3.11.

Заметим, что свойства ч.у. множеств могут не сохраняться при пересечении. Например, это относится к свойству «быть линейным порядком»: пусть P — цепь, тогда P^\sharp — также цепь, а $P \cap P^\sharp$ — тривиально упорядоченное множество.

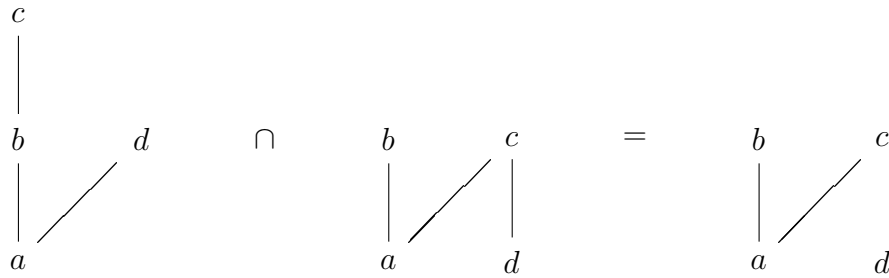


Рис. 3.11: Пересечение ч.у. множеств

Прямая сумма. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч.у. множества с непересекающимися носителями, то их *прямой* или *кардинальной суммой* $P+Q$ называется множество $P \cup Q$ с частичным порядком \sqsubseteq таким, что $x \sqsubseteq y$ когда либо $x \sqsubseteq_P y$, либо $x \sqsubseteq_Q y$.

Очевидно, справедливы соотношения

$$P + Q \cong P + R \Rightarrow Q \cong R \quad \text{и} \quad (P + Q)^\# \cong P^\# + R^\#.$$

Прямая сумма n ч.у. множеств P обозначается nP . n -элементная антицепь изоморфна $n\mathbf{1}$.

Диаграмма прямой суммы состоит из двух диаграмм соответствующих ч.у. множеств, рассматриваемых как единая диаграмма. Ч.у. множество, не являющееся прямой суммой некоторых двух других ч.у. множеств, называется *связным*. Прямую сумму двух цепей называют *бицепью*.

Порядковая сумма. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — также два ч.у. множества с непересекающимися носителями, то их *порядковой* или *ординальной суммой* $P \oplus Q$ называется множество $P \cup Q$ с частичным порядком \sqsubseteq таким, что $x \sqsubseteq y$ когда либо $x \sqsubseteq_P y$, либо $x \sqsubseteq_Q y$, либо $x \in P$ и $y \in Q$.

Понятно, что операция порядковой суммы ассоциативна, но не коммутативна. n -элементная цепь изоморфна $\mathbf{1} \oplus \dots \oplus \mathbf{1}$ (n раз).

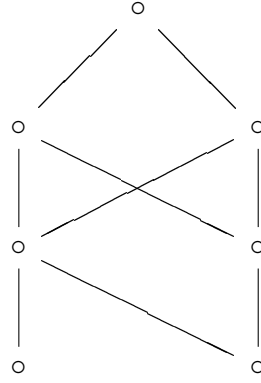
Диаграмма порядковой суммы $P \oplus Q$ состоит из диаграмм соответствующих ч.у. множеств, причём диаграмма P располагается под диаграммой Q , и в которой добавлены отрезки, соединяющие максимальные элементы P с минимальными элементами Q (корректность такого построения обеспечивается теоремой 3.5). На рис. 3.12 показана порядковая сумма двух зигзагов из 4 и 3 элементов.

Ч.у. множество, не представимое в виде кардинальной [ординальной] суммы своих подмножеств, называется *кардинально* [ординально] *неразложимым*.

Теорема 3.9. *Всякое ч.у. множество является кардинальной суммой своих кардинально неразложимых подмножеств.*

Верна также аналогичная теорема для ординальной суммы. Доказательство обеих теорем имеется в [34]. Ч.у. кардинально и/или ординально разложимые множества называются последовательно-параллельными ч.у. множествами.

Упорядоченная сумма. Пусть $\langle P, \sqsubseteq_P \rangle$ — ч.у. множество, каждому элементу x которого сопоставлено ч.у. множество $\langle Q_x, \sqsubseteq_x \rangle$. Семейство всех ч.у. множеств Q_x , индексированных элементами P , обозначим \mathcal{F} .

Рис. 3.12: Порядковая сумма $Z_4 \oplus Z_3$

Упорядоченная (лексикографической) суммой $\sum_P Q_x$ семейства ч.у. множеств \mathcal{F} над ч.у. множеством $\langle P, \sqsubseteq_P \rangle$ называется ч.у. множество $\langle R, \sqsubseteq \rangle$, с носителем $R = \{(x, q) \mid x \in P, q \in Q_x\}$ и порядком на нём, задаваемым соотношением $(x, q) \sqsubseteq (x', q')$, если либо $x \sqsubseteq_P x'$, либо $x = x'$ и $q \sqsubseteq_x q'$.

Для того, чтобы получить диаграмму упорядоченной суммы $\sum_P Q_p$

- 1) строят диаграмму ч.у. множества P ;
- 2) отбрасывают отрезки между элементами P ;
- 3) заменяют каждый элемент $x \in P$ диаграммой Q_x ;
- 4) соединяют отрезками все максимальные элементы Q_x со всеми минимальными элементами Q_y , если x непосредственно предшествует y в P .

На рис. 3.13 приведены ч.у. множество $P = \{a, b, c\}$, семейство $\mathcal{F} = \{Q_a, Q_b, Q_c\}$ ч.у. множеств, индексированных элементами P и упорядоченная сумма семейства \mathcal{F} над P .

Упорядоченная сумма $\sum_P Q_p$ тривиальна, если ч.у. множество P или все множества семейства \mathcal{F} одноэлементны. Понятно, что в этом случае $\sum_P Q_p$ изоморфно либо Q , либо P . Ч.у. множество *разложимо в упорядоченную сумму*, если оно изоморфно некоторой нетривиальной упорядоченной сумме, в противном случае оно *неразложимо в упорядоченную сумму*.

Легко видеть, что кардинальная (прямая) и ординальная (порядковая) суммы являются частными случаями порядковой суммы $\sum_P Q_x$: первая из них получается, если P — тривиальное ч.у. множество, а вторая, если P — цепь.

Прямое произведение. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч.у. множества, то их *прямым* или *декартовым произведением* называется множество $P \times Q$ с частичным порядком \sqsubseteq таким, что $(p, q) \sqsubseteq (p', q')$ только когда $p \sqsubseteq_P p'$ и $q \sqsubseteq_Q q'$.

Если ч.у. множества P и Q градуированы и их ранговые функции суть ρ_P и ρ_Q , то их прямое произведение также градуировано. При этом

- ранг элемента $x = (x_1, x_2)$ есть $\rho(x) = \rho_P(x_1) + \rho_Q(x_2)$;
- для чисел Уитни W_k справедливо равенство $W_k(P \times Q) = \sum_i W_i(P) W_{k-i}(Q)$.

Очевидно, $W_k(2^n) = \binom{n}{k}$.

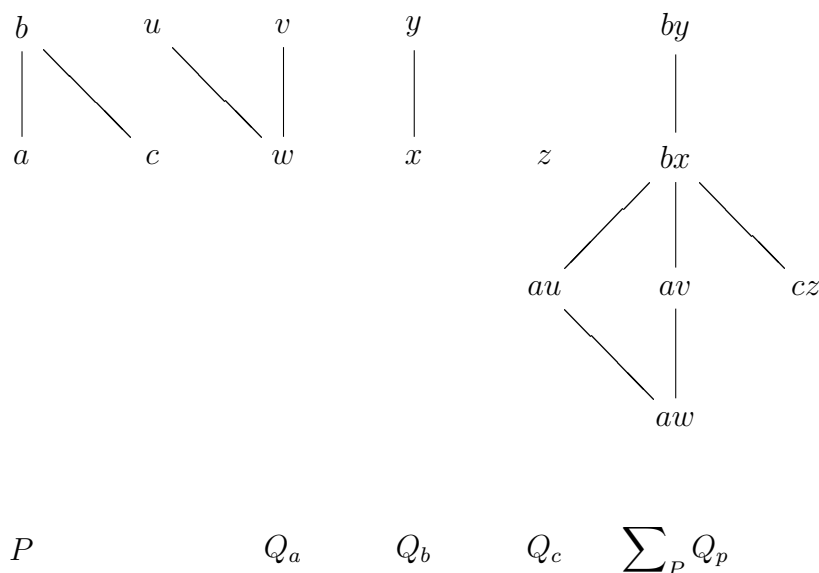


Рис. 3.13: Ч.у. множество P , семейство ч.у. множеств $F = \{Q_a, Q_b, Q_c\}$, индексированных элементами P и лексикографическая сумма $\sum_P Q_p$.

Прямое произведение n экземпляров ч.у. множеств P обозначают P^n . Справедливы соотношения

$$P \times R \cong Q \times R \Rightarrow P \cong Q, \quad \text{откуда} \quad P^n \cong Q^n \Rightarrow P \cong Q, \\ (P \times Q)^\# \cong P^\# \times Q^\#.$$

Для того, чтобы получить диаграмму прямого произведения ч.у. множеств P и Q

- 1) строят диаграмму ч.у. множества P ;
- 2) отбрасывают отрезки между элементами P ;
- 3) заменяют каждый элемент $x \in P$ копией Q_x диаграммы Q ;
- 4) соединяют отрезками копии элементов из Q в Q_x и Q_y , если x непосредственно предшествует y в P .

На рис. 3.14 показано прямое произведение трёх- и четырёхэлементного зигзагов.

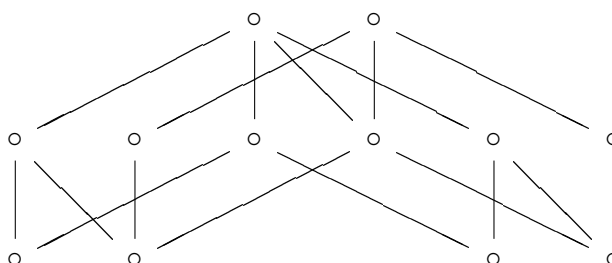
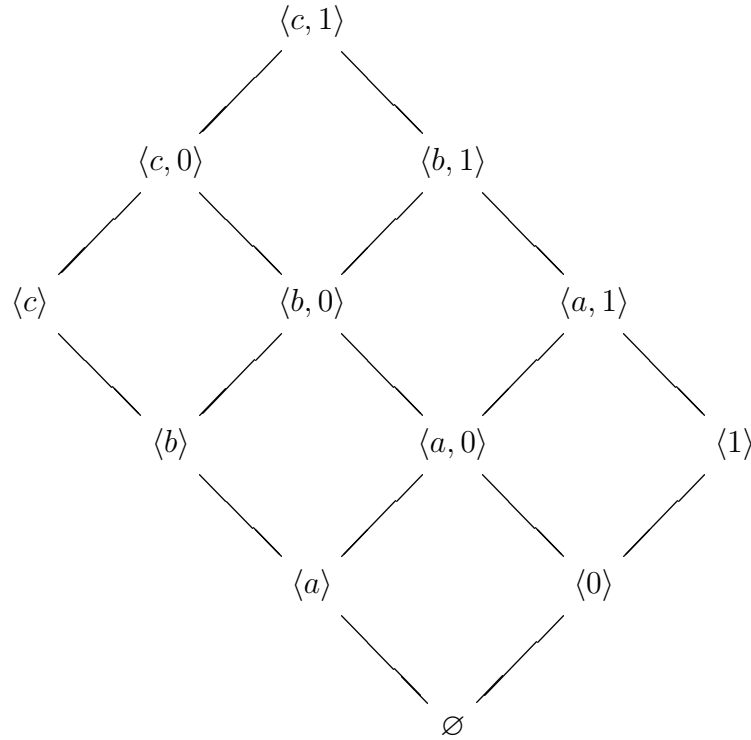


Рис. 3.14: Прямое произведение $Z_3 \times Z_4$

Заметим, что диаграммы изоморфных множеств $P \times Q$ и $Q \times P$ обычно выглядят совершенно не похожими друг на друга.

- Пример 3.11.** 1. $J(P + Q) \cong J(P) \times J(Q)$. В частности, $B^n \cong J(n\mathbf{1}) \cong J(\mathbf{1}^n) \cong \mathbf{2}^n$, что уже отмечалось выше.
2. Обозначим через $[0, m]$ — цепь $[0, 1, \dots, m]$. Тогда $D(N) \cong [0, m_1] \times \dots \times [0, m_k]$, если $N = p_1^{m_1} \cdot \dots \cdot p_k^{m_k}$ — примарное разложение N .
3. $J(\mathbf{m}_1 + \dots + \mathbf{m}_k) = (\mathbf{m}_1 + \mathbf{1}) \times \dots \times (\mathbf{m}_k + \mathbf{1})$. Как иллюстрация, на рис. 3.15 представлена диаграмма порядковых идеалов прямой суммы 3- и 2-элементных цепей.

Рис. 3.15: $J([a, b, c] + [0, 1])$

Заметим, что если два ч.у. множества обладают ЛУМ-свойством, то их прямое произведение этим свойством может и не обладать. С другой стороны, свойство Шпернера при прямых произведениях сохраняется.

Теорема 3.10 (Оре [26]). *Каждый частичный порядок изоморфен некоторому подмножеству декартова произведения цепей.*

Определение 3.11. *Мультипликативной размерностью ч.у. множества P называется наименьшее число k линейных порядков C_i таких, существует вложение $P \hookrightarrow C_1 \times \dots \times C_k$.*

Степень. Если $\langle P, \sqsubseteq_P \rangle$ и $\langle Q, \sqsubseteq_Q \rangle$ — два ч.у. множества, то обозначим через Q^P множество всех изотонных отображений из P в Q . Введём на Q^P порядок \sqsubseteq , положив $f \sqsubseteq g$ для $f, g \in Q^P$, если $f(x) \sqsubseteq_Q g(x)$ для всех $x \in P$. Таким образом, $\langle Q^P, \sqsubseteq \rangle$ есть ч.у. множество.

Легко показывается справедливость соотношения

$$\mathbf{2}^n \cong (\mathbf{n} + \mathbf{1}) \quad (3.4)$$

(мы заключаем $\mathbf{n} + \mathbf{1}$ в скобки, чтобы отличить $n + 1$ -элементную цепь от прямой суммы n -элементной цепи и тривиального ч.у. множества).

На рис. 3.16 показано ч.у. множество $Z_4^{Z_3}$, где выделенному элементу \bullet соответствует отображение $f: Z_3 \rightarrow Z_4$ такое, что $f(x_1) = f(x_3) = y_3$, $f(x_2) = y_4$ (см. рис. 3.9).

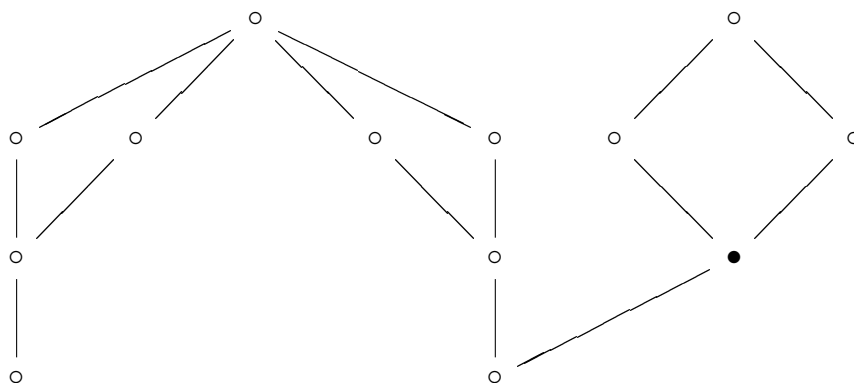


Рис. 3.16: Степень $Z_4^{Z_3}$

Можно показать, что для нетривиально упорядоченного ч.у. множества P и произвольных ч.у. множеств Q и R

$$R^P \cong R^Q \Rightarrow P \cong Q, \quad (Q^P)^\# \cong (Q^\#)^{P^\#}.$$

Г. Биркгоф предположил, что для конечных множеств справедливо

$$P^R \cong Q^R \Rightarrow P \cong Q$$

(т.н. “предположение об экспоненциальном сокращении”), однако доказательство этого до сих пор не найдено.

Вводят и другие операции над ч.у. множествами, но мы ограничимся приведёнными.

Можно убедиться [4], что для введённых выше операций $+$, \times над ч.у. множествами выполняются законы ассоциативности, коммутативности (для \times — с точностью до изоморфизма), первый дистрибутивный закон

$$P \times (Q + R) \cong (P \times Q) + (P \times R)$$

и для степени — соотношения

$$R^{P+Q} \cong R^P \times R^Q, \quad (P^Q)^R \cong P^{Q \times R}, \quad (P \times Q)^R \cong P^R \times Q^R.$$

Здесь предполагается, что соответствующие прямые суммы существуют. Также справедливы соотношения для «единицы» $\mathbf{1}$:

$$\mathbf{1} \times P \cong P, \quad \mathbf{1}^P \cong \mathbf{1}.$$

Указанные соотношения, вместе с приведёнными выше при определении операций, называются правилами *арифметики кардиналов*. В частности, в ней справедливо (см. (3.4)) важное для практических приложений соотношение

$$\mathfrak{n}^P \cong (2^{\mathfrak{n}-1})^P \cong 2^{P \times (\mathfrak{n}-1)}.$$

Следует сказать, что класс всех неразложимых в прямую сумму или произведение ч.у. множеств также необозрим, как и всех исходных. Поэтому представление совокупности ч.у. множеств в виде АС с операциями $+$ и \times не решает проблемы их «хорошего» описания. Эти и прочие описанные операции полезны при построении ч.у. множеств со специальными свойствами.

3.5 Линеаризация и размерность

Рассмотрим теперь представление частичных порядков в виде пересечения цепей. Основной здесь является

Теорема 3.11 (Шпильрайна-Дашника-Миллера [59, 47]). *Любой частичный порядок может быть продолжен до линейного на том же множестве. Каждый порядок есть пересечение всех своих линейных продолжений.*

Доказательство (для конечного случая). Пусть $\langle M, \sqsubseteq \rangle$ — ч.у. множество. Построим линейный порядок \leq , содержащий данный частичный.

По условию M — не цепь, и значит в M найдутся несравнимые элементы a и b . Произвольно определим порядок на них. Для определённости положим, например, $a \leq b$. Далее для всех $x \sqsubseteq a$ и $b \sqsubseteq y$ полагаем $x \leq y$. Если $\langle M, \leq \rangle$ ещё не цепь, то выберем новую пару несравнимых элементов и поступаем, как указано выше. Через конечное число шагов получаем линейный порядок.

Поскольку возможен различный выбор пар несравнимых элементов a и b и при каждом выборе можно полагать как $a \leq b$, так и $b \leq a$, то действуя указанным образом можно получить различные возможные продолжения исходного частичного порядка \sqsubseteq до линейного \leq (т.е. если $x \sqsubseteq y$, то и $x \leq y$).

Пересечение всех таких цепей даст исходное ч.у. множество. Действительно, если $x \sqsubseteq y$, то аналогичное следование будет и во всех полученных линейных порядках, а при несравнимых x и y всегда найдётся пара цепей с противоположным их следованием, что в пересечении цепей и даст несравнимость этих элементов. \square

Для счетного бесконечного упорядоченного множества доказательство проводится методом математической индукции. В общем случае доказательство первого утверждения может опираться [47, 26] на лемму Куратовского-Цорна или трансфинитную индукцию (см. ниже). Можно показать, что любое отношение без циклов может быть продолжено до линейного порядка. Для конечных множеств поиск такого продолжения в теоретическом программировании называют «топологической сортировкой»⁹.

Пусть M — непустое множество и \leq_1, \dots, \leq_n — некоторые линейные порядки на нём. Тогда на M определён частичный порядок \sqsubseteq по правилу

$$x \sqsubseteq y \Leftrightarrow \bigwedge_{i=1}^n (x \leq_i y)$$

⁹Заметим, что данный термин очень неудачен: указанная процедура не имеет никакого отношения ни к сортировке (упорядочение элементов в списке по возрастанию/убыванию значений какого-либо атрибута), ни к топологии (раздел математики, изучающий в самом общем виде явление непрерывности).

для произвольных $x, y \in M$. Понятно, что $\langle M, \sqsubseteq \rangle = \langle M, \bigcap_{i=1}^n \leq_i \rangle$.

Линейный порядок \leq , включающий в себя данный частичный порядок \sqsubseteq (т.е. $\sqsubseteq \subseteq \leq$) на некотором множестве называют *линеаризацией* или *линейным расширением* исходного порядка. Из доказанной теоремы следует простой алгоритм построения некоторой линеаризации конечного ч.у. множества P : выделяем множество минимальных элементов P и линейно упорядочиваем его произвольным образом, исключаем это множество из P , образуя ч.у. подмножество $P' \subset P$, в котором вновь выделяем минимальные элементы, линейно упорядочиваем их и т.д. Однако, могут существовать линеаризации, которые не могут быть получены таким способом¹⁰.

Произвольным образом занумеруем элементы P первыми n натуральными числами. Отождествим линейное расширение $\sigma : P \rightarrow \mathbf{n}$ ч.у. множества P с перестановкой $(\sigma^{-1}(1), \dots, \sigma^{-1}(n))$ множества $[1, \dots, n]$. Совокупность всех перестановок множества $[n]$, полученных таким образом, называется *множеством Гёльдера* ч.у. множества P . Определение мощности множества Гёльдера для данного n -элементного ч.у. множества составляет т.н. *проблему Рейни*. Для $n > 5$ она решена лишь для очень немногих типов ч.у. множеств.

Введём ещё два типа ч.у. множеств. Частично упорядоченные множества с диаграммами Хассе, являющимися двудольными графами с числами элементами m и n в верхней и нижней доле соответственно, будем называть *двудольными ч.у. множествами*. $K_{m,n}$ — обозначение для двудольного ч.у. множества, у которого любой максимальный элемент покрывает любой минимальный.

Двудольные ч.у. множества, состоящие из $n > 2$ элементов $\{v_1, \dots, v_n\}$ с отношениями включения $v_{2i-1} < v_{2i}$ и $v_{2i} > v_{2i+1}$ (последнее включение при чётном n и $i = n/2$ отсутствует) и двойственные им назовём *заборами* и будем обозначать Z_n . Обычно элементы нижней и верхней долей множества Z_n обозначают соответственно символами a и b с индексами. Множества Z_n имеют диаграммы Хассе, изображённые на рис. 3.17а), рис. 3.17б) и двойственные к последней. Если в $2n$ -элементном заборе при $n \geq 3$ доба-

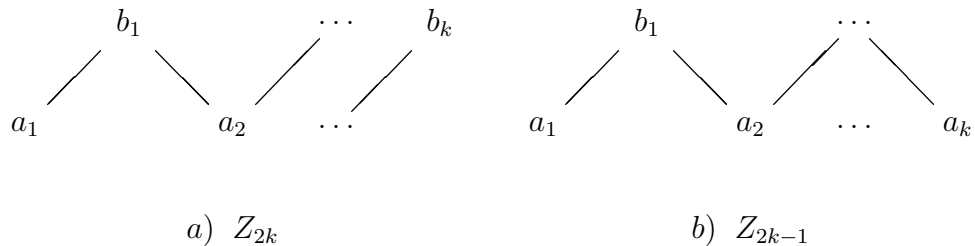


Рис. 3.17: Зигзаги с чётным а) и нечётным б) числом элементов

вить условие «последний элемент покрывает первый», то получим ч.у. множество, которое назовём *малой короной* s_n , диаграмма которой изображена на рис. 3.18. Понятно, что корона s_n изоморфна упорядоченной по включению совокупности всех одноэлементных $\{v_1\}, \dots, \{v_n\}$ и двухэлементных подмножеств вида $\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_n, v_1\}$ n -элементного множества $\{v_1, \dots, v_n\}$. Короны и заборы часто появляются при исследовании конечных ч.у. множеств [46].

Число всевозможных линеаризаций ч.у. множества P обозначают $e(P)$. Оно может

¹⁰Эффективные алгоритмы построения всех линеаризаций ч.у. множества описаны в Novak V., Novotny M. Linear extensions of orderings // Czechoslovak Mathematical Journal, **50** (125) (2000), Praha. 853–864 (здесь приведён также алгоритм нахождения всех порядков, имеющих данную линеаризацию) и Korsh J.F., Lafollette P.S. Loopless Generation of Linear Extensions of a Poset // Order, **19** (2002) 115–126.

интерпретироваться как некоторая оценка сложности P^{11} (ясно, что $e(P)$, совпадает с мощностью множества Гёльдера для P). Понятно, что $e(n\mathbf{1}) = n!$ и $e(C) = 1$ для цепи C (очевидно, это максимально и минимально возможные значения $e(\cdot)$). Легко показывается справедливость формул

$$e(P \oplus Q) = e(P)e(Q), \quad e(P + Q) = \binom{m+n}{m} e(P)e(Q)$$

для произвольных ч.у. множеств P и Q (для второй формулы — мощностей m и n соответственно). Также установлено, что

- $e(\mathbf{2} \times \mathbf{n}) = \frac{1}{n+1} \binom{2n}{n}$ — числа Каталана; например, для $e(\mathbf{2} \times \mathbf{3}) = 5$ — см. рис. 3.19;
- для зигзагов Z_n справедливо¹² представление

$$\sum_{n \geq 0} \frac{e(Z_n) x^n}{n!} = \operatorname{tg} x + \sec x, \quad (3.5)$$

при этом значения $e(Z_n)$ при чётных n называют *числами секанса*, а при нечётных — *числами тангенса*¹³.

Отметим, что значение $e(Z_n)$ подсчитано как мощность множества Гёльдера для Z_n : в данном случае его элементами будут т.н. *up-down перестановки*. Такие перестановки, называемые ещё *пилообразными*, образуют первые n натуральных чисел, переставленные так, каждый элемент либо больше, ибо меньше обоих своих соседей.

В общем случае вычисление значения $e(P)$ — сложная комбинаторная задача (в [42] показана её NP-полнота). Существуют различные подходы к её решению. Один из них связан с подсчётом числа изотонных отображений специального вида. Обозначим через $O_m(P)$ число порядковых гомоморфизмов из данного n -элементного ч.у. множества P в m -элементную цепь. Тогда [57]

$$\lim_{m \rightarrow \infty} \frac{O_m(P)}{m^n} = \frac{e(P)}{n!}.$$

¹¹В [36] даже указывается, что $e(P)$ «является, вероятно, единственным весьма полезным числом, измеряющим “сложность” ч.у. множества P », однако автор не разделяет этой крайней точки зрения — см. 81.

¹²Впервые установлено в *André D. Sur les permutations alternées // J. de Math.* **7** (3) (1881) 167–184.

¹³Как известно,

$$\operatorname{tg} x = x + \frac{1}{3} x^3 + \frac{2}{15} x^5 + \frac{17}{315} x^7 + \frac{62}{2835} x^9 + \dots + \frac{2^{2n}(2^{2n}-1)B_n}{(2n)!} x^{2n-1} + \dots,$$

$$\sec x = 1 + \frac{x^2}{2} + \frac{5}{24} x^4 + \frac{61}{720} x^6 + \frac{277}{8064} x^8 + \dots + \frac{E_n}{(2n)!} x^{2n} + \dots,$$

где B_n и E_n — числа Бернулли и Эйлера соответственно [16].

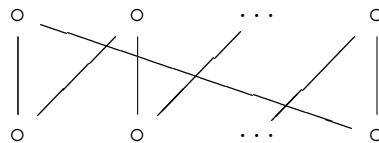
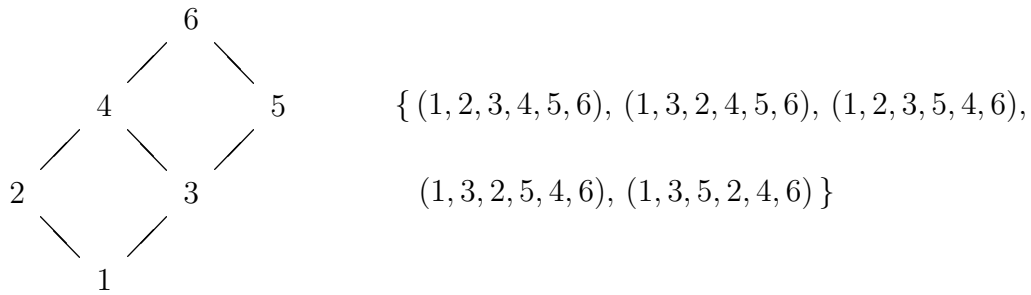


Рис. 3.18: Малая корона s_n

Рис. 3.19: Ч.у. множество $\mathbf{2} \times \mathbf{3}$ и его 5-элементное множество Гёльдера

Другой метод определения $e(P)$ использует вероятностный подход. Пусть $P = \{v_1, \dots, v_n\}$ — носитель ч.у. множества $\langle P, \sqsubseteq \rangle$. В n -мерном евклидовом пространстве \mathbb{R}^n определим многогранник \mathcal{P} :

$$\mathcal{P} = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid 0 \leq x_i \leq 1, v_i \sqsubseteq v_j \Rightarrow x_i \leq x_j\}.$$

Показано, что $e(P) = n! \cdot \text{vol}(\mathcal{P})$, где $\text{vol}(\mathcal{P})$ — объём многогранника \mathcal{P} .

Пример 3.12. Рассмотрим ч.у. множество $P = \{v_1, v_2, v_3\} \cong Z_3^\#$ в котором $v_1 \sqsubseteq v_2$, $v_1 \sqsubseteq v_3$ и $v_2 \parallel v_3$. Тогда вышеопределённый многогранник \mathcal{P} есть четырёхугольная пирамида, основанием которой служит квадрат $(000), (001), (011), (010)$, вершиной — точка (111) , а высота совпадает с боковым ребром $(111) - (011)$. Таким образом, $\text{vol}(\mathcal{P}) = \frac{1}{3}$. Отсюда $e(P) = \frac{3!}{3} = 2$ и множество линейных продолжений P состоит из двух цепей $[v_1, v_2, v_3]$ и $[v_1, v_3, v_2]$.

Понятно, что в общем случае \mathcal{P} есть многогранное множество в \mathbb{R}^n , ограниченное гиперплоскостями вида $x_i = x_j$ (для каждых i, j таких, что v_i непосредственно предшествует v_j или наоборот) и заключённое в единичный куб. Задача, таким образом, сводится к вычислению объёма указанного многогранника¹⁴.

Для практических целей (решение задач комбинаторики, дискретной оптимизации и др.) часто рассматривают связанное с ч.у. множеством $\langle P, \sqsubseteq \rangle$ вероятностное пространство на множестве всех $e(P)$ его линеаризаций, в котором каждая линеаризация равновероятна. В этом пространстве для $x, y, z \in P$ рассматривают события E вида $x \sqsubseteq y$, $(x \sqsubseteq y) \& (x \sqsubseteq z)$ и т.д. Для них определяют вероятности $\text{Pr}[E]$ как отношение числа линеаризаций $N(E)$, в которых имеет место E к $e(P)$. Важным результатом здесь является¹⁵

Теорема 3.12 (XYZ-теорема). Пусть $\langle P, \sqsubseteq \rangle$ — ч.у. множество и $x, y, z \in P$. Тогда

$$\text{Pr}[(x \sqsubseteq y) \& (x \sqsubseteq z)] \geq \text{Pr}[x \sqsubseteq y] \cdot \text{Pr}[x \sqsubseteq z].$$

Заметим, что иногда утверждение XYZ-теоремы записывают в виде

$$\text{Pr}[x \sqsubseteq y] \leq \text{Pr}[x \sqsubseteq y \mid x \sqsubseteq z].$$

Так называемое « $1/3 - 2/3$ предположение» утверждает, что любое ч.у. множество содержит пару несравнимых элементов x и y , для которых

$$\frac{1}{3} \leq \text{Pr}[x \sqsubseteq y] \leq \frac{2}{3}.$$

¹⁴Для этого возможно применение метода Монте-Карло с получением оценок $\text{vol}(\mathcal{P})$ вероятностного типа.

¹⁵См., например, Алон Н., Спенсер Дж. Вероятностный метод. — М.: БИНОМ, 2007.

Наиболее сильным результатом¹⁶ здесь является утверждение, что

$$0,2764 \approx \frac{5 - \sqrt{5}}{10} \leq \Pr[x \sqsubset y] \leq \frac{5 + \sqrt{5}}{10} \approx 0,7236.$$

для некоторых несравнимых элементов x и y любого ч.у. множества.

Пример 3.13. Изоморфное Z_3 ч.у. множество, представленное на рис. 3.20 имеет пять

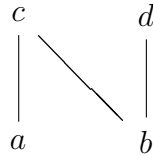
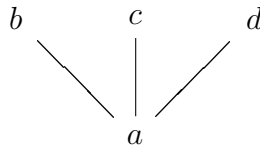


Рис. 3.20: К примеру 3.13

линейных расширений, а именно $[a, b, c, d]$, $[a, b, d, cd]$, $[b, a, c, d]$, $[b, a, d, c]$, $[b, d, a, c]$, и поэтому $\Pr[a \sqsubseteq b] = \frac{2}{5}$.

Перейдём теперь к понятию размерности ч.у. множества. Ясно, что ч.у. множество P совпадает с пересечением всех $e(P)$ своих возможных линейаризации. Однако, тот же результат можно получить, взяв значительно меньшее число линейных продолжений. Например, ч.у. множество



имеющее 6 линейаризаций, может быть представлено в виде пересечения двух цепей $[a, b, c, d]$ и $[a, d, c, b]$.

Пусть P — ч.у. множество и $\mathcal{R} = \{C_1, \dots, C_k\}$ — совокупность цепей такая, что $P = \bigcap_{i=1}^k C_i$. Тогда говорят, что \mathcal{R} реализует ч.у. множество P .

Пример 3.14. $\mathcal{R} = \{C_1, C_2, C_3\}$ реализует ч.у. множество P , изображённое на рис. 3.21.

$$\begin{aligned} C_1 &= [13, 2, 10, 8, 1, 3, 11, 12, 9, 6, 4, 5, 7], \\ C_2 &= [13, 6, 7, 12, 11, 10, 9, 8, 4, 1, 5, 2, 3], \\ C_3 &= [6, 7, 10, 11, 12, 8, 9, 1, 13, 2, 4, 3, 5]. \end{aligned}$$

Классическая проблема сортировки состоит в определении неизвестной линейаризации L ч.у. множества P с помощью минимального количества вопросов вида «верно ли, что $x < y$ в L ?».

Определение 3.12. Наименьшее число линейных порядков, дающее в пересечении данное ч.у. множество P называется (*порядковой*) *размерностью* последнего и обозначается $\dim(P)$.

Понятно, что для ч.у. множества, изображённого на рис. 3.21 $\dim(P) \leq 3$.

Справедлива

¹⁶См. *Brightwell G.R., Felsner S., Trotter W.T.* Balancing pairs and the cross product conjecture. Order **12** (1995), 321–335.

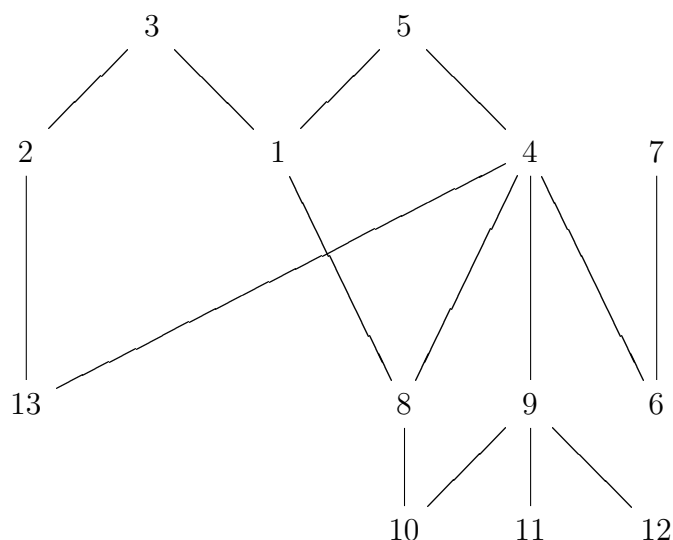
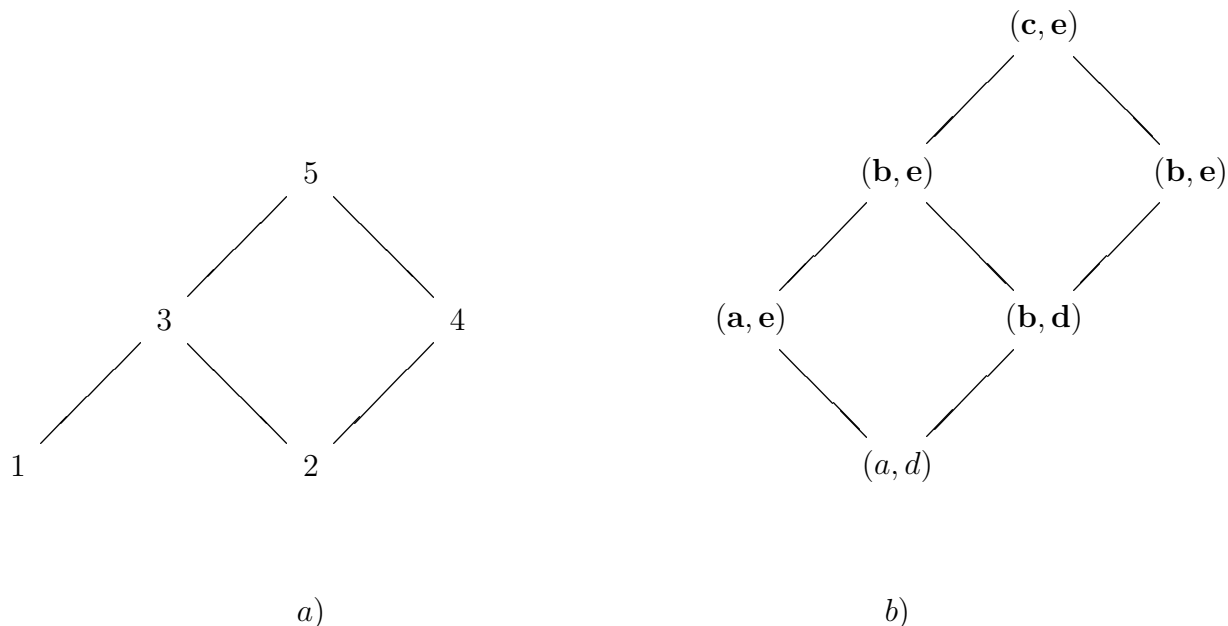


Рис. 3.21: К примеру 3.14

Теорема 3.13 (Оре [26]). *Порядковая и мультипликативная размерности ч.у. множества совпадают.*

На рис. 3.22 представлено ч.у. множество P и его вложение в (выделено жирным шрифтом) в произведение двух цепей $[a, b, c]$ и $[d, e]$. В то же время P представляется

Рис. 3.22: Ч.у. множество P (a) и его вложение в $[a, b, c] \times [d, e]$ (b)

в виде пересечения цепей $[1, 2, 3, 4, 5]$ и $[2, 1, 4, 3, 5]$.

Приведённая теорема Оре позволяет не различать указанные виды размерности и пользоваться для её обозначения единым символом $\dim(P)$. Значение $\dim(P)$ является более тонкой оценкой сложности ч.у. множества P , чем $e(P)$.

Размерность 1 имеют только цепи, а размерность тривиально упорядоченных множеств равна 2 (они могут быть представлены в виде пересечения любого линейного упорядочения своих элементов с двойственным упорядочиванием). Последнее показывает, что размерность не может интерпретироваться как мера отличия данного ч.у. множества от линейного. Размерность всех (отличных от цепей) ч.у. множеств, имеющих не более пяти элементов, также равна 2. Легко видеть, что $\dim(Z_n) = 2$ (например, пара цепей $[a, b, c, d]$ и $[b, a, d, c]$ реализует ч.у. множество, представленное на рис. 3.20).

Размерность 2 имеют и все 6-элементные (кроме цепи **6**) ч.у. множества, не изоморфные т.н. “короне” s_3 , “шеvronу” sh и sh^\sharp (см. рис. 3.23), имеющих размерность 3. Приве-

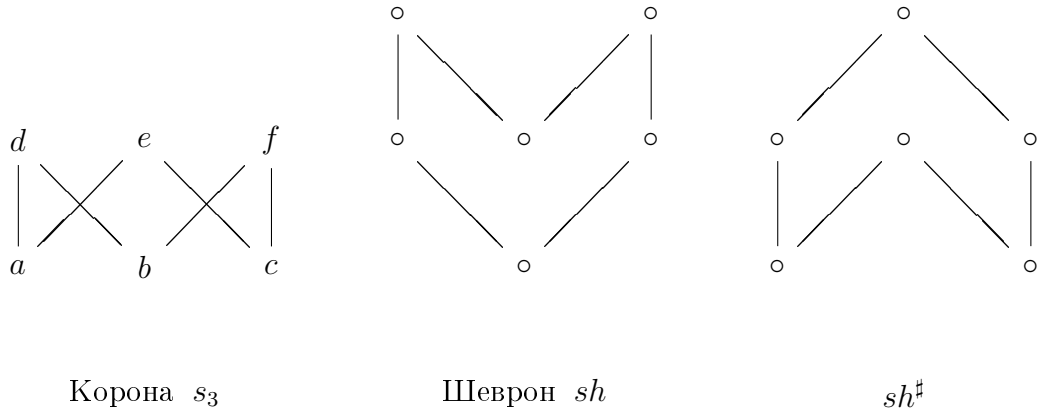


Рис. 3.23: 6-элементные ч.у. множества размерности 3

дём разложение s_3 (обозначение элементов — на указанном рисунке) в пересечение цепей:

$$[a, b, d, c, e, f] \cap [c, a, e, b, f, d] \cap [c, b, f, a, e, d].$$

Легко установить, что $\dim(s_n) = 3$. Приведённые на рис. 3.24 и рис. 3.25 ч.у. множества P_1 и P_2 имеют размерность 3.

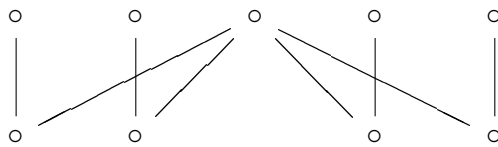
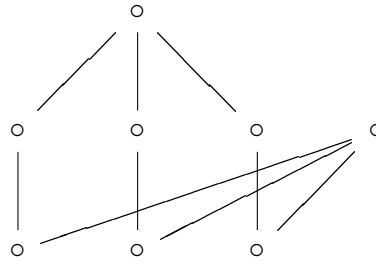
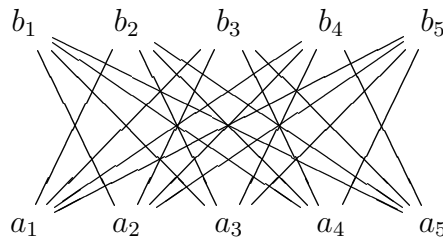


Рис. 3.24: Ч.у. множество P_1 размерности 4

Будем далее пользоваться обозначением $\pi(X)$ для мощность множества Парето (числа максимальных элементов) ч.у. множества P . Упорядоченную пару (x, y) несравнимых элементов x и y ч.у. множества P называют *критической*, если $u < x \Rightarrow u < y$ и $y < v \Rightarrow x < v$ для всех $u, v \in P$. Множество всех критических пар ч.у. множества P обозначают $\text{crit}(P)$.

Для $n \geq 3$ определяют ч.у. множество S_n , которое называют (полной) короной: это $2n$ -элементное *двудольное ч.у. множество*, т.е. $S_n = A \cup B$, где $A = \{a_1, \dots, a_n\}$ — множество минимальных, а $B = \{b_1, \dots, b_n\}$ — множество максимальных элементов. Порядок \sqsubseteq на S_n задаётся следующим образом: для элементов $a_i \in A$ и $b_j \in B$ полагают $a_i \sqsubseteq b_j$ для всех $i \neq j$, $i, j = 1, \dots, n$ (и, естественно, \sqsubseteq рефлексивен).

Рис. 3.25: Ч.у. множество P_2 размерности 4Рис. 3.26: Корона S_5

Ясно, что $S_3 = s_3$. На рис. 3.26 изображена корона S_5 . Рассмотрим n -элементное, $n \geq 3$, множество и совокупность $\mathcal{S}_n(1, n-1)$ из его одноэлементных и $(n-1)$ -элементных подмножеств. Тогда множество $\mathcal{S}_n(1, n-1)$, упорядоченное по включению, изоморфно S_n .

Установлено [47], что $\dim(S_n) = n$, и корона S_n считается стандартным примером ч.у. множества размерности n . Например, пять цепей

$$\begin{aligned} & [a_5, a_4, a_3, a_2, b_1, a_1, b_2, b_3, b_4, b_5], & [a_1, a_5, a_4, a_3, b_2, a_2, b_3, b_4, b_5, b_1] \\ & [a_2, a_1, a_5, a_4, b_3, a_3, b_4, b_5, b_1, b_2], & [a_3, a_2, a_1, a_5, b_4, a_4, b_5, b_1, b_2, b_3] \\ & [a_4, a_3, a_2, a_1, b_5, a_5, b_1, b_2, b_3, b_4] \end{aligned}$$

реализуют представленную на рис. 3.26 корону S_5 .

Для ч.у. множеств P и Q справедливы следующие соотношения (см., например, [62]).

1. $\emptyset \neq Q \subseteq P \Rightarrow \dim(Q) \leq \dim(P)$ (монотонность размерности по мощности вложенных ч.у. подмножеств); при этом при удалении из ч.у. множества одного элемента его размерность уменьшается не более, чем на 1 (теорема об удалении одного элемента [50]).
2. $\dim(P + Q) = \max \{ \dim(P), \dim(Q) \}$, если хотя бы одно из множеств не является цепью и $\dim(P + Q) = 2$, иначе.
3. $\dim(P \times Q) \leq \dim(P) + \dim(Q)$, причём равенство достигается, когда и P , и Q — ограниченные неоднородные множества (но не только в этом случае). В частности:

- размерность декартова произведения n цепей (напомним, мы не считаем одноэлементные множества цепями) есть n ; отсюда следует, что размерность n -мерного евклидова пространства \mathbb{R}^n , рассмотренного как декартово произведение линейных порядков \mathbb{R} (т.е. для $x = (x_1, \dots, x_n)$ и $y = (y_1, \dots, y_n)$ из \mathbb{R}^n полагаем $x \leq y$, если $x_i \leq y_i$ для всех $i = \overline{1, n}$) равна n ;

- $\dim(\mathbf{2}^n) = n$;
 - $\dim(S_n \times S_n) = 2n - 2$.
4. $\dim(P) \leq |P|/2$ при $|P| \geq 4$ (теорема Хирагучи [50]).
 5. $\dim(P) \leq 2 \cdot \dim(P - C) + 1$, где C — подцепь, не совпадающая со всем множеством P .
 6. $\dim(P) \leq |P - A|$, где A — антицепь в P такая, что $|P - A| \geq 2$.
 7. $\dim(P) \leq w(P)$.
 8. $\dim(P) \leq w(X - \pi(X)) + 1$.
 9. $\dim(P) \leq |\text{crit}(P)|$.

Для бесконечных ч.у. множеств справедлива «теорема компактности»:

Теорема 3.14. Пусть P — такое ч.у. множество, что любое его конечное ч.у. подмножество имеет размерность, не превосходящую d . Тогда $\dim(P) \leq d$.

Доказательство может быть найдено в Harzheim E. Ein Endlichkeitssatz über die Dimension teilweise geordneter Mengen, Math. Nachr. 46 (1970), 183-188 или [48]. \square

Ч.у. множество P называется d -несводимым для некоторого $d \geq 2$, если $\dim(P) = d$ и $\dim(P') < d$ для любого собственного ч.у. подмножества $P' \subset P$. Единственное 2-несводимое множество есть двухэлементная антицепь. Ч.у. множества, представленные на рис. 3.23 являются 3-несводимыми. Они далеко не исчерпывают всех 3-несводимых ч.у. множеств, которые полностью описаны [51]. В частности, имеется 3 (s_3 , sh и sh^d) шестиэлементных и 21 семиэлементных 3-несводимых ч.у. множества [41, 62]. Установлено [52], что для любого натурального w и $d \geq 6$ существует d -несводимое ч.у. множество ширины w . Для $d = 3$ это не так, а для $d = 4$ и $d = 5$ ответ неизвестен.

Единственное n -несводимое $2n$ -элементное множество есть корона S_n . Показано, что для $d \geq 4$ не существует d -несводимого множества с числом элементов $n = 2d + 1$. Также известно, что каждое d -несводимое ч.у. множество является ч.у. подмножеством некоторого $d + 1$ -несводимого ч.у. множества [56].

Утверждение 3.4. Если ч.у. множество является d -несводимым для некоторого $d \geq 2$, то оно неразложимо в лексикографическую сумму.

В 1990 г. ленинградским учёным В.Д. Ногиным поставлена [24] проблема:

Каково наибольшее значение $\mu(d, n)$ мощности множества Парето d -несводимого ч.у. множества при $d \geq 4$, имеющего n элементов?

Данная проблема до сих пор остаётся открытой. Можно показать только, что

Теорема 3.15 ([14]). $\mu(d, n) \leq n - d$.

Доказательство. Пусть A — максимальная антицепь в d -несводимом n -элементном ч.у. множестве P . Тогда $|A| = w(P)$ и $|P - A| \geq 2$. Поэтому, $d = \dim(P) \leq n - w(P)$ и $w(P) \leq n - \dim(P)$. Но, очевидно, $\pi(P) \leq w(P)$, откуда $\pi(P) \leq n - \dim(P)$. \square

3.6 Вполне упорядоченные множества и смежные вопросы

В ходе исследований ч.у. множеств были сформулированы следующие утверждения.

Лемма Куратовского-Цорна (принцип максимальности). Если в ч.у. множестве все цепи имеет верхние грани, то любой его элемент содержится в некотором максимальном.

Принцип Хаусдорфа. Всякая цепь ч.у. множества может быть вложена в некоторую максимальную цепь.

Данные утверждения часто применяют при доказательстве свойств ч.у. множеств. Например, для доказательства теоремы 3.11 в общем случае нужно рассмотреть семейство всех продолжений порядка, упорядоченных по включению и с помощью леммы Куратовского-Цорна вывести существование максимального элемента.

Оказалось, что приведённые утверждения эквивалентны — одно может быть выведено из другого. Более того, они также эквивалентны приводимым ниже фундаментальным теоретико-множественным аксиомам выбора и о полном упорядочении.

Аксиома выбора (АС). Существует отображение, сопоставляющее каждому непустому подмножеству B множества A элемент из B .

Таким образом, аксиома выбора (общепринятое обозначение АС есть аббревиатура англ. «axiom of choice») обеспечивает существование для каждого непустого множества A функции f_A такой, что $f_A(B) \in B$ для любого $B \in \mathcal{P}^*(A)$.

Для формулировки следующей аксиомы нам потребуются новое понятие.

Определение 3.13. Линейно упорядоченное множество называют *вполне упорядоченным*, если каждое его непустое подмножество содержит наименьший элемент.

Ч.у. множество также называют *фундированным* когда в нём не существует бесконечных строго убывающих последовательностей элементов (*условие минимальности*). Понятно, что выполнение условия минимальности есть критерий для ч.у. множества быть вполне упорядоченным; элементы вполне упорядоченного множества иногда называют *трансфинитами*. Рассматриваемые понятия введены Г. Кантором в 1833 г.

Элементы вполне упорядоченного множества традиционно обозначают строчными греческими булавами α, β, \dots . Ясно, что вполне упорядоченное множество всегда содержит наименьший элемент. Во вполне упорядоченном множестве каждый элемент α , (1) если только он не является наибольшим, имеет единственный непосредственно следующий, обозначаемый $\alpha + 1$, и (2) если только он не наименьший, может иметь не более одного непосредственно предшествующего. В последнем случае, если α не имеет непосредственно предшествующего элемента, он называется *предельным*.

Пример 3.15. 1. Очевидно, вполне упорядочены все конечные цепи, а так же цепь \mathbb{N} с естественным порядком. В этих цепях нет предельных элементов.

Множество целых чисел \mathbb{Z} не является вполне упорядоченным относительно естественного порядка, поскольку оно не имеет наименьшего элемента. Интервал $[0, 1]$ действительных чисел с обычным порядком — также не есть вполне упорядоченное множество.

2. Множество

$$\{ 0, 1/2, 2/3, 3/4, \dots, 1, 1 + 1/2, 1 + 2/3, \dots, m, m + 1/2, m + 2/3, \dots \}$$

с естественным порядком является вполне упорядоченным. Его предельные элементы суть натуральные числа.

Теорема Цёрмело (принцип полного упорядочения). Любое непустое множество можно вполне упорядочить.

Пример 3.16. Множество целых чисел \mathbb{Z} можно вполне упорядочить считая, например, что

$$0 < 1 < -1 < 2 < -2 < 3 \dots \quad \text{или} \quad 1 < 2 < \dots < 0 < -1 < -2 < \dots$$

(в последнем случае 0 — предельный элемент).

Покажем, к примеру, как аксиому выбора можно получить из теоремы Цермело. Пусть A — непустое множество; по аксиоме о полном упорядочении его можно считать вполне упорядоченным. Тогда в определено отображение, ставящее в соответствие каждому непустому подмножеству A его элемент, а именно — наименьший.

Отметим, что известны и другие утверждения, эквивалентные приведённым: например, о равносильности множеств X и $X \times X$ или о непустоте декартова произведения произвольной совокупности непустых множеств. Доказательство эквивалентности упомянутых утверждений можно найти, например, в [34].

Таким образом, истинными или ложными все эти утверждения могут быть только одновременно. Что же имеет место “в действительности”? Ответ на поставленный вопрос зависит от того, какими свойствами мы наделяем понятие множества. В наиболее общей форме проблема выражена в аксиоме выбора, предложенной Э. Цермело в 1904 г. при разработке *аксиоматической теории множеств*. Для конечных множеств её справедливость очевидна. Однако при рассмотрении бесконечных совокупностей бесконечных множеств эта очевидность теряется. Все же попытки свести АС к другим фундаментальным принципам оказались безуспешными: не выводимы ни отрицание аксиомы выбора (в аксиоматике Бернаиса-Гёделя Σ , К. Гёдель, 1939), ни она сама (в аксиоматике Цермело-Френкеля ZF , П. Коэн, 1963). Таким образом, АС является независимым от остальных аксиом утверждением, и добавление к ним как самой этой аксиомы, так и её отрицания порождает две равноправные непротиворечивые аксиоматики теории множеств¹⁷. Поэтому при практических, не связанных с вопросами оснований математики и теории множеств исследованиях можно как принять аксиому выбора, так и отказаться от неё. Последствия же такого решения суть следующие.

Отклонение аксиомы выбора обедняет содержание конкретных математических теорий. Например, без привлечения АС, кроме условия существования максимальных элементов ч.у. множеств, не удастся доказать ни наличия базиса у произвольного векторного пространства, ни эквивалентности двух определений непрерывности функции в точке (на языке ε - δ и через пределы последовательностей), ни некоторых других важных и привычных свойств различных математических объектов.

Принятие аксиомы выбора имеет свои “отрицательные” последствия в виде существования объектов с парадоксальными свойствами: неизмеримого по Лебегу множества действительных чисел; такого разбиения шара на четыре части, что из них движениями в пространстве оказывается возможным составить два таких же шара и др. Однако все эти объекты неконструктивны и обосновываются теоремами чистого существования¹⁸. Кроме того, за принятие аксиомы выбора говорит и следующий, весьма сильный, аргумент. Как отмечалось выше, Гёдель показал, что присоединение АС к системе аксиом теории множеств не увеличивает опасности впасть в противоречие, т.е. если в полученной расширенной системе встретилось противоречие, то причина его в исходной системе, а не в аксиоме выбора. Из результата Гёделя также вытекает, что всякое свойство натуральных

¹⁷Естественно, при условии непротиворечивости самих аксиоматических системы теории множеств, что, как известно, является открытым вопросом (при этом системы Σ и ZF равнонепротиворечивы). Отметим, что результаты Гёделя и Коэна об АС имеют место и относительно т.н. континуум-гипотезы. Подробнее см., например, *Френкель А., Бар-Хиллел И. Основания теории множеств*. — М., 1966 и *Гильберт Д., Бернаис П. Основания математики. Теория доказательств*. — М., 1982.

¹⁸Обычно используемое выражение «чистая теорема существования» является неточным переводом с немецкого.

чисел, доказываемое с помощью аксиомы выбора, может быть доказано и без неё. В силу этого, по крайней мере в теории натуральных чисел, аксиому выбора можно рассматривать лишь как вспомогательное средство, нужное лишь для упрощения доказательств.

Последние из приведённых соображений обычно перевешивают, и при конкретных математических исследованиях аксиому выбора, как правило, принимают¹⁹. При этом доказательства, не использующие аксиому выбора (или эквивалентные ей утверждения) называют *эффективными*.

Заметим, что изложение в данной монографии остаётся в рамках т.н. *наивной теории множеств*, которая позволяет рассматривать множества, задаваемые произвольным свойством. Неограниченное применение этого принципа, как известно, может привести к противоречиям (парадоксам). Приведём здесь *парадокс Рассела*²⁰: множество Рассела $R = \{x \mid x \notin x\}$, корректно заданное в рамках наивной теории множеств, характеризуется справедливостью соотношения $z \in R \Leftrightarrow z \notin z$ для любого множества z , что при $z = R$ приводит к противоречию $R \in R \Leftrightarrow R \notin R$. Приведём для примера множество, содержащее себя: зафиксируем некоторый объект a и рассмотрим совокупность N_a всех множеств, не содержащих a ; тогда получается, что $N_a \in N_a$. В аксиоматических теориях множеств ZF и Σ ни R , ни множество, содержащее себя в качестве своего элемента, не могут быть построены.

Для вполне упорядоченного множества определяют множество $[o, \alpha) \triangleq \alpha^\nabla \setminus \{\alpha\}$, которое называют *начальным отрезком* α . Символ $[o, o)$ понимается как пустое множество. Предельный элемент α вполне упорядоченного множества $\langle C, \leq \rangle$ определяется условиями $\alpha \neq o$ и отсутствием в $[o, \alpha)$ наибольшего элемента. Следующий за α элемент $\alpha + 1$ — наименьший во множестве $\alpha^\Delta \setminus \{\alpha\}$.

Отметим важнейшие свойства вполне упорядоченных множеств $\langle C, \leq \rangle$.

Теорема 3.16. Пусть C — вполне упорядоченное множество. Тогда

- 1) если $C^\#$ также вполне упорядочено, то C — конечная цепь.
- 2) если α — предельный элемент вполне упорядоченного множества, то

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

Доказательство.

1. Поскольку C и $C^\#$ вполне упорядочены, то C содержит универсальные грани o и ι , каждый её элемент, отличный от ι имеет последующий, а каждый элемент, отличный от o — предшествующий. Таким образом, в C отсутствуют предельные элементы, все её сечения — скачки, что вместе с наличием универсальных граней означает конечность C .
2. Если $\gamma \in [o, \alpha)$, то поскольку между γ и $\gamma + 1$ элементов нет, $\gamma + 1 \leq \alpha$. Однако, в силу предельности α , равенство невозможно. Таким образом, $\gamma \in [o, \gamma + 1) \subseteq \bigcup_{\beta < \alpha} [o, \beta)$, т.е. $[o, \alpha) \subseteq \bigcup_{\beta < \alpha} [o, \beta)$. Обратное включение очевидно.

¹⁹Д. Гильберт назвал аксиому выбора общим, «необходимым и неопределимым для математики принципом». С другой стороны, её применение вызвало негодование многих ведущих математиков начала XX в.

²⁰Парадокс был обнаружен Б. Расселом и сообщён в 1902 г. в письме к математику и логика Г. Фреге, что привело последнего к умственному расстройству.

Одна из неформальных интерпретаций парадокса Рассела: «В одной стране вышел указ: «Мэры всех городов должны жить не в своем городе, а в специальном Городе мэров»; спрашивается, где должен жить мэр Города мэров?».

□

Решающим моментом, обеспечивающим возможность сравнивать произвольные множества является

Теорема 3.17 (о сравнении вполне упорядоченных множеств). Пусть A и B — два вполне упорядоченных множества. Тогда имеется лишь одна из следующих возможностей:

- 1) $A \cong B$;
- 2) A изоморфно начальному отрезку B ;
- 3) B изоморфно начальному отрезку A .

Доказательство этой теоремы имеется, например, в [35].

Факт равномогности множеств A и B будем обозначать $\overline{\overline{A}} = \overline{\overline{B}}$, а неравномогности — $\overline{\overline{A}} \neq \overline{\overline{B}}$. Здесь под $\overline{\overline{X}}$ понимается новый объект, связанный с множеством X , называемый *кардинальным числом* X или *кардиналом*. Определение такого объекта возможно по *принципу абстракции*, согласно которому эквивалентным множествам можно сопоставить некоторый абстрактный объект (кардинальное число) — то общее, что делает их эквивалентными.

Теорема 3.18 (о сравнении множеств — закон трихотомии). Для любых множеств A и B имеется лишь одна из следующих возможностей:

- 1) $\overline{\overline{A}} = \overline{\overline{B}}$ (A эквивалентно B);
- 2) $\overline{\overline{A}} = \overline{\overline{B'}}$ для некоторого $B' \subseteq B$, но $\overline{\overline{A'}} \neq \overline{\overline{B}}$ для любого $A' \subseteq A$;
- 3) $\overline{\overline{B}} = \overline{\overline{A'}}$ для некоторого $A' \subseteq A$, но $\overline{\overline{B'}} \neq \overline{\overline{A}}$ для любого $B' \subseteq B$.

Доказательство. Отметим, что утверждения теоремы попарно несовместимы. Далее, используя аксиому о полном упорядочении заключаем, что для A и B справедлива теорема 3.17. Отсюда либо справедливы утверждения 2)–3) данной теоремы, либо выполняются условия теоремы 2.18 Кантора-Шрёдера-Бернштейна. Последнее же влечёт выполнение условия 1). □

Данная теорема лежит в основе учения о мощности множеств. Она позволяет ввести порядок на множестве кардинальных чисел, а именно считать, что $\overline{\overline{A}} < \overline{\overline{B}}$ и $\overline{\overline{A}} > \overline{\overline{B}}$ соответственно в случаях 2) и 3) данной теоремы (понятно, что если $A \subseteq B$, то $\overline{\overline{A}} \leq \overline{\overline{B}}$, при этом возможен случай $\overline{\overline{A}} = \overline{\overline{B}}$).

Теорема 3.19 (Кантор). $\overline{\overline{A}} < \overline{\overline{\mathcal{P}(A)}}$.

Доказательство. Сопоставив каждому элементу $a \in A$ одноэлементное подмножество $\{a\}$ множества A , получим вложение A в $\mathcal{P}(A)$, и поэтому $\overline{\overline{A}} \leq \overline{\overline{\mathcal{P}(A)}}$.

Допустим теперь, что существует взаимно-однозначное отображение φ множества A в $\mathcal{P}(A)$. Во множестве A определим подмножество M :

$$M = \{a \in A \mid a \notin \varphi(a)\} \in \mathcal{P}(A).$$

По определению φ , должен существовать элемент $m \in A$ такой, что $\varphi(m) = M$. При попытке выяснить, принадлежит ли m множеству M , получаем противоречие: действительно, если предположить $m \in M$, то получим $m \notin \varphi(m) = M$, а если $m \notin M$ — то $m \in \varphi(m) = M$. □

Доказательства более общего факта см. в [7].

Заметим, что из теоремы Кантора сразу следует *парадокс Кантора*, показывающий, что множества всех множеств не существует. Действительно, для множества всех множеств V справедливо $\mathcal{P}(V) \subseteq V$ и, следовательно, $\overline{\overline{\mathcal{P}(V)}} \leq \overline{V}$, что противоречит теореме Кантора. Множество V можно формально определить как $V = \{x \mid x = x\}$, и мы ещё раз, как и в случае с множеством Рассела, убеждаемся, что не всякое свойство, вообще говоря, определяет множество.

Далее в теории множеств показывается, что множество кардинальных чисел вполне упорядочено, откуда получают много важных и интересных следствий.

Важность вполне упорядоченных множеств определяется главным образом тем, что для них справедлив

Теорема 3.20 (принцип трансфинитной индукции). Пусть C — вполне упорядоченное множество с каждым элементом α которого связано утверждение S_α , образующие совокупность S . Тогда, если из справедливости S_β для всех $\beta \in [o, \alpha)$ следует справедливость S_α , то верны все утверждения из S .

Доказательство. Пусть среди S имеется неверное утверждение. Тогда непусто множество E неверных утверждений. Пусть α — наименьший элемент E , который всегда существует в силу полного порядка на C . Но тогда, поскольку S_β справедливо для всех $\beta \in [o, \alpha)$, то справедливо и S_α . Противоречие. \square

При доказательстве свойств ч.у. множеств метод трансфинитной индукции является альтернативным использованию леммы Куратовского-Цорна. С его помощью докажем теорему 2.13, утверждающую, что для всякой толерантной пары элементов существует класс толерантности, её содержащий.

Лемма 3.1. Пусть $\langle A, \simeq \rangle$ — пространство толерантности, а $\langle C, \leq \rangle$ — вполне упорядоченное множество, каждому элементу α которого сопоставлен предкласс толерантности $E_\alpha \subseteq A$ так, что из $\alpha_1 < \alpha_2$ следует $E_{\alpha_1} \subseteq E_{\alpha_2}$. Тогда объединение $\bigcup E_\alpha = E$ является предклассом толерантности в A .

Доказательство. Пусть x , и y — произвольные элементы множества $E = \bigcup E_\alpha$. Определим подмножество $C(x) \subseteq C$ правилом

$$C(x) = \{\omega \in C \mid x \in E_\omega\}.$$

Очевидно, что из $\alpha \in C(x)$ и $\alpha < \beta$ следует $\beta \in C(x)$.

Обозначим через $\alpha(x)$ наименьший элемент множества $C(x)$. Пусть для определённости $\alpha(y) \leq \alpha(x)$. Так как $y \in E_{\alpha(y)}$, а $E_{\alpha(y)} \subseteq E_{\alpha(x)}$, то $y \in E_{\alpha(x)}$. Следовательно, x и y входят в общий предкласс, а значит $x \simeq y$. \square

Доказательство теоремы 2.13 проведём с помощью трансфинитной индукции.

1°. *Базис индукции.* Возьмём $E_1 = \{x\}$. В силу рефлексивности \simeq , E_1 есть предкласс. Если нет $y \neq x$ таких, что $x \neq y$, то E_1 есть класс толерантности. Если же такой y существует, то выполняем шаг индукции.

2°. *Шаг индукции.* Если α не является предельным элементом C , то, поскольку $E_{\alpha-1}$ определено, получаем, что либо $E_{\alpha-1}$ уже есть класс, либо существует $y \in E_{\alpha-1}$, толерантный ко всем $x \in E_{\alpha-1}$ и тогда полагаем $E_\alpha = E_{\alpha-1} \cup \{y\}$.

Если α — предельный элемент C , то, поскольку E_β определены при всех $\beta < \alpha$, полагаем $E_\alpha = \bigcup_{\beta < \alpha} E_\beta$. Согласно лемме 3.1 E_α есть предкласс.

Для завершения доказательства достаточно положить $K = \bigcup E_\alpha$, где объединение берётся по всем элементам ч.у. множества α , для которых E_α определено. Очевидно, K есть максимальный предкласс, содержащий элемент x . \square

Из этого доказательства выводятся две леммы.

Лемма 3.2. *Для того, чтобы выполнялось $x \simeq y$, необходимо и достаточно существование класса толерантности K , одновременно содержащего x и y .*

Доказательство. Достаточность следует из определения класса, а необходимость получается из приведённого доказательства теоремы 2.13, если на этапе базиса индукции взять элемент x , а на втором присоединить y . □

Лемма 3.3 (о классах толерантности). *Для всякого предкласса существует содержащий его класс.*

Доказательство сводится к замечанию, что базис индукции может быть начат с любого класса. □

Глава 4

Решётки

Красота теории решёток отчасти объясняется исключительной простотой её основных понятий: упорядочения, точной верхней и точной нижней граней. В этом отношении она очень напоминает теорию групп. Теоретико-решёточными понятиями пронизана вся современная алгебра, хотя во многих учебниках это обстоятельство явным образом не отмечается.

С.С. Гончаров. Счётные булевы алгебры.

4.1 Решёточно упорядоченные множества и решётки

Определение 4.1. Ч.у. множество, в котором для любых элементов a и b существуют $\inf \{a, b\}$ и $\sup \{a, b\}$ называют *решёточно упорядоченным* или *бинаправленным*.

Ясно, что в решёточно упорядоченном множестве точные верхние и нижние грани существуют для любого конечного подмножества элементов.

Пример 4.1. 1. Модели, изображённые на рис. 3.1 суть решёточно упорядоченные множества.

2. Любая цепь решёточно упорядочена. Модели $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{N}, | \rangle$ и $\langle \mathcal{P}(A), \subseteq \rangle$ суть решёточно упорядоченные множества: парами (инфинум, супремум) для них будут (\min, \max) , (НОК, НОД) и (\cap, \cup) соответственно.

3. На рис. 4.1 представлены два ч.у. множества, причем лишь первое из них является решёточно упорядоченным, т.к. во втором не существуют $\sup \{a, b\}$ и $\inf \{c, d\}$.

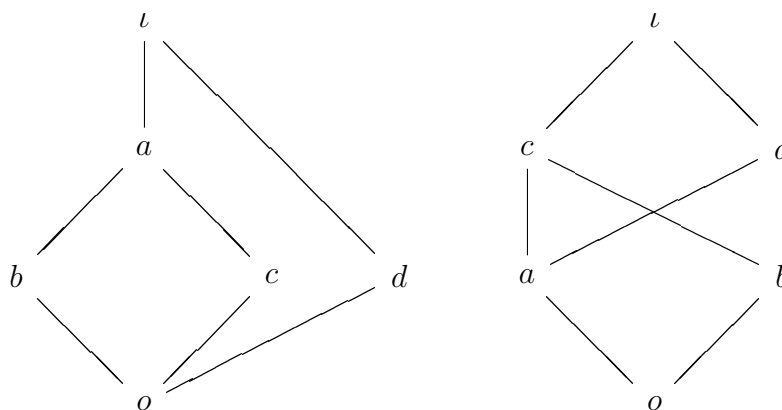
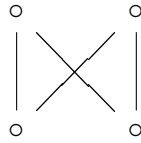


Рис. 4.1: 6-элементные ч.у. множества

Четырёхэлементное ч.у. множество с диаграммой, изображённой на рис. 4.2 обозначим K_2 . Пусть в некотором ч.у. множестве с диаграммой H за элементом a непосредственно следует элемент b . Модифицируем данное множество, добавив между элементами a и b новые элементы a_1, \dots, a_k , образовав подцепь $[a, a_1, \dots, a_k, b]$. Обозначим диаграмму полученного ч.у. множества через H' . Диаграммы H и H' называют *гомеоморфными*.

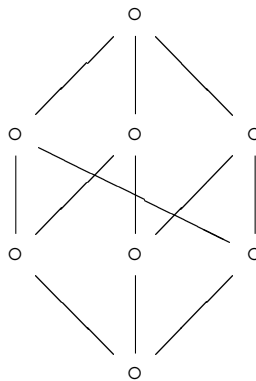
Рис. 4.2: Ч.у. множество K_2

Очевидно диаграмма H не определяет решётку, если она содержит поддиаграмму, гомеоморфную диаграмме K_2 .

Мы ввели понятие решёточно упорядоченного множества, отталкиваясь от отношения порядка. Однако возможен другой, эквивалентный данному подход, опирающийся на алгебраические операции.

Определение 4.2. Решёткой \mathfrak{L} называется множество L с заданными на нём двумя бинарными операциями: \sqcup (объединения) и \sqcap (пересечения), подчиняющимися двойственным парам законов Ass , Com , Id и Abs (см. п. 1.1).

Например, ч.у. множество, представленное на рис. 4.3 есть решётка. Ясно, что в ре-

Рис. 4.3: Восьмизлементная решётка \widehat{s}_3

шётке объединения и пресечения существуют для любого конечного подмножества её элементов.

Отметим, что раньше вместо термина «решётка» часто употреблялся термин *структура*. Теперь под структурой обычно понимают алгебраическую систему. При этом часто удобно считать решёткой пустое множество.

Приведённое выше определение утверждает, что решётка есть АС $\langle L, \sqcup, \sqcap \rangle$, двухместные операции \sqcup и \sqcap которой удовлетворяют указанным законам. Ранее было показано, что законы идемпотентности вытекают из законов поглощения, и поэтому указанная система аксиом избыточна. Использование именно такой системы аксиом традиционно. Следствием её двойственности является

Принцип двойственности (для решёток). *Любое утверждение, истинное для любых произвольных элементов решётки, остаётся таковым при замене $\sqcap \leftrightarrow \sqcup$.*

Ясно, что бесконечная решётка может содержать, а может и не содержать универсальные грани; при этом конечная решётка их обязательно содержит: 0 есть пересечение, а 1 — объединение всех элементов конечной решётки.

На рис. 4.4 изображены все, за исключением линейного порядка, решётки с пятью элементами. Последние две решётки традиционно называют “пятиугольник” и “ромб” и обозначают соответственно N_5 и M_3 .

Пример 4.2. 1. Очевидно, любая булева алгебра есть решётка. С другой стороны, любая цепь есть решётка, являясь булевой алгеброй лишь при числе элементов, равном 2.

N_5 показывает, что решётка не обязательно есть ранжированное множество.

2. Ч.у. множество $\langle \mathcal{E}(A), \subseteq \rangle$ всех отношений эквивалентности на множестве A , рассмотренное в примере 3.4.3, есть решётка с универсальными гранями $o = \Delta_A$ и $\iota = \nabla_A$. Здесь для эквивалентностей α и β в качестве объединения выступает $\{\alpha, \beta\}^e$, а в качестве пересечения — обычное теоретико-множественное пересечение $\alpha \cap \beta$, поскольку оно всегда есть эквивалентность. Эту решётку называют также *решёткой всех разбиений* множества. Решётку всех разбиений множества $\{1, \dots, n\}$ обозначают Π_n .

Пусть, например, на множестве $\{1, \dots, 11\}$ заданы эквивалентности α и β , определяющие разбиения

$$D_\alpha = (1, 2 \mid 3, 4, 5 \mid 6, 7, 8 \mid 9, 10, 11) \quad \text{и} \quad D_\beta = (1, 3, 4 \mid 2, 5 \mid 6, 7, 11 \mid 8 \mid 9, 10).$$

Тогда эквивалентность $\alpha \sqcup \beta$ задаётся разбиением $(1, 2, 3, 4, 5 \mid 6, 7, 8, 9, 10, 11)$, а эквивалентность $\alpha \sqcap \beta$ — разбиением $(1 \mid 2 \mid 3, 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9, 10 \mid 11)$.

Легко видеть, что $\Pi_3 \cong M_3$. Решётка Π_4 показана на рис. 4.5.

Число элементов решётки Π_n обозначают $B(n)$ — это комбинаторные числа Белла (поэтому Π_n иногда называют *беллианом* n -элементного множества). Из предыдущего ясно, что $B(3) = 5$ и $B(4) = 15$. Числом Стирлинга второго рода $S(n, k)$ для $n, k \geq 1$ называется число разбиений n -элементного множества на k блоков. Для них $S(n, k) = 0$ при $n < k$, $S(n, 0) = 0$ при $n \neq 0$ и формально полагают $S(0, k) = 0$, $n, k \in \mathbb{N}_0$.

Ясно, что в решётке всех разбиений n -элементного множества $W_k = S(n, k)$ и

$$B(n) = \sum_{k=0}^n S(n, k).$$

Для чисел Стирлинга второго рода при $k \geq 2$ справедливо соотношение

$$S(n, k) = \sum_{i=k-1}^{n-1} C_{n-1}^i S(i, k-1).$$

Числа Стирлинга второго рода растут очень быстро: так, например, $S(10, 5) = 42\,525$.

3. Множество $\text{Sub } G$ всех подгрупп группы G с операциями $x \sqcup y = \langle x, y \rangle$ (подгруппа порожденная объединением подгрупп x и y) и $x \sqcap y = x \cap y$ (это множество, как известно, всегда является группой) есть решётка. Здесь $o = E$ (единичная группа) и $\iota = G$.

Утверждение 4.1. Для любых элементов x и y решётки $\langle L, \sqcup, \sqcap \rangle$ справедливо

$$x \sqcup y = y \Leftrightarrow x \sqcap y = x.$$

Доказательство. Имеем $x \sqcup y = y \Rightarrow (x \sqcup y) \sqcap x = x \sqcap y \stackrel{(Abs)}{\Leftrightarrow} x = x \sqcap y$, и аналогично показывается $x \sqcap y = x \Rightarrow x \sqcup y = y$. \square

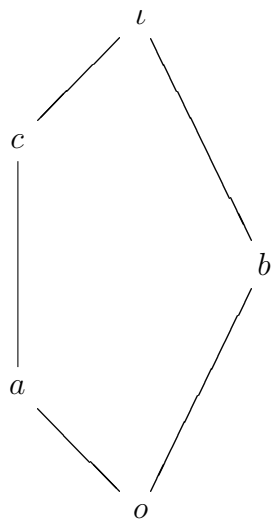
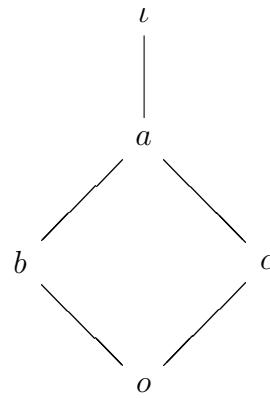
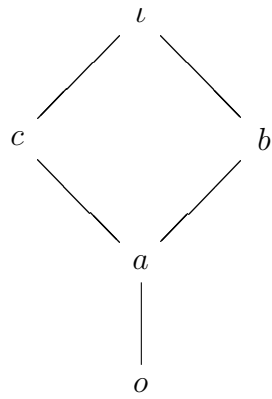
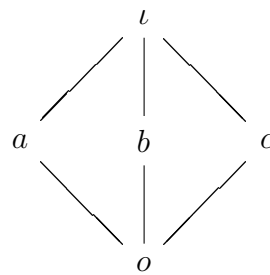
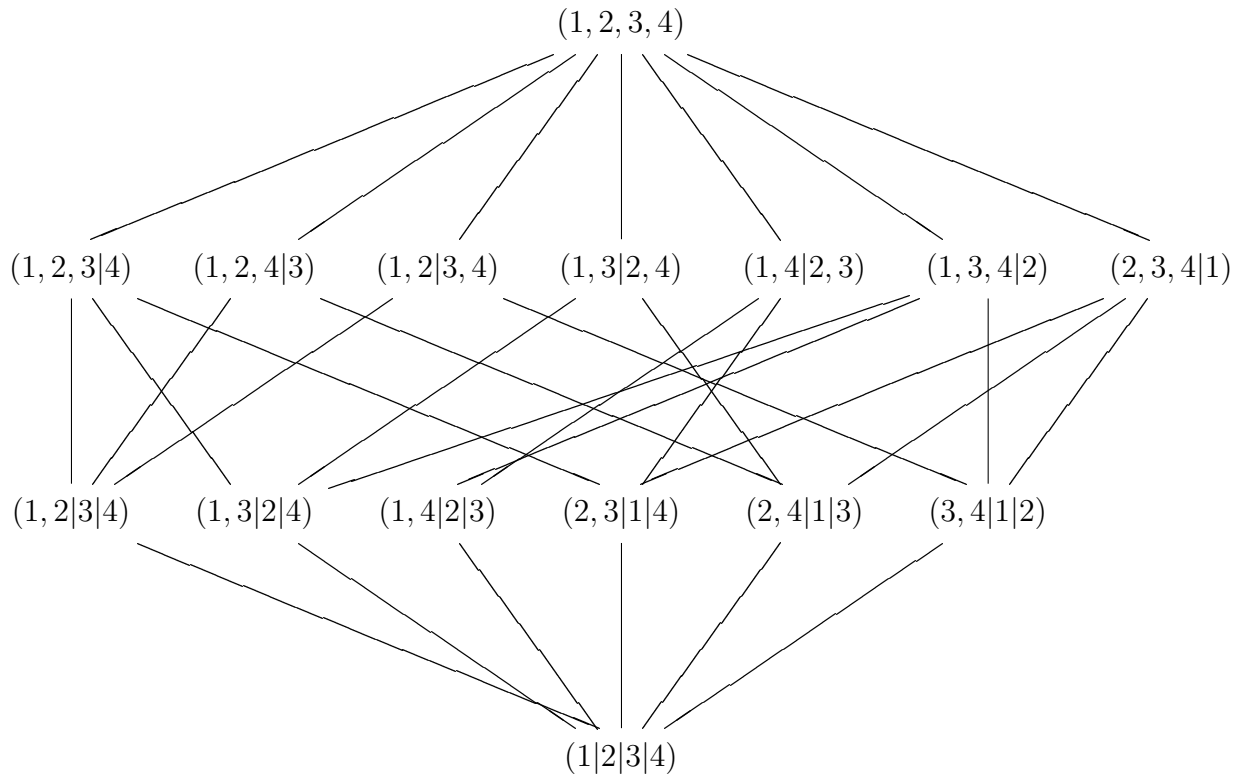
 N_5  M_3

Рис. 4.4: Все, кроме линейного порядка, 5-элементные решётки

Рис. 4.5: Решётка разбиений множества $\{1, \dots, 4\}$

Если L и M — решётки, то таковыми же являются L^\sharp , $L \oplus M$ и $L \times M$ (в частности, произведение любых цепей есть решётка). При этом $L + M$ никогда не будет решёткой, если только одно из множеств L и M непусто. Однако, если к $L + M$ добавить универсальные грани, то полученное множество станет решёткой. Например, $N_5 = \widehat{\mathbf{1} + \mathbf{2}}$ и $M_3 = \widehat{\mathbf{31}}$.

Рассмотрим решёточно упорядоченное множество $\langle \mathbb{N}, | \rangle$. В нём для любой пары натуральных чисел m и n существуют наименьшее общее кратное $m \vee n$ и наибольший общий делитель $m \wedge n$, из определений которых следует, что $m \vee n = \sup \{m, n\}$ и $m \wedge n = \inf \{m, n\}$. Таким образом, рассматриваемое ч.у. множество решёточно упорядоченно. С другой стороны, операции \vee и \wedge удовлетворяют законам коммутативности, ассоциативности, поглощения и идемпотентности, и поэтому $\langle \mathbb{N}, \vee, \wedge \rangle$ — решётка. Наконец, если в данной решётке ввести отношение δ по правилу $m \delta n \triangleq m \wedge n = m$, то оказывается $\delta = |$ и, таким образом, $\langle \mathbb{N}, \delta \rangle$ — решёточно упорядоченное множество.

Данное рассмотрение наводит на мысль, что решётки и решёточно упорядоченные множества тесно связаны. Это действительно так, и данная связь устанавливается следующей теоремой.

Теорема 4.1 (эквивалентность решёточно упорядоченных множеств и решёток).

1. Пусть $\langle P, \sqsubseteq \rangle$ — решёточно упорядоченное множество. Если для любых элементов x и y из P положить

$$x \sqcup y \triangleq \sup \{x, y\}, \quad x \sqcap y \triangleq \inf \{x, y\},$$

то структура $\langle P, \sqcup, \sqcap \rangle$ будет решёткой.

2. Пусть $\langle L, \sqcup, \sqcap \rangle$ — решётка. Если для любых элементов x и y из L положить

$$x \sqsubseteq y \triangleq x \sqcap y = x \quad (\text{или } x \sqsubseteq y \triangleq x \sqcup y = y), \quad (4.1)$$

то структура $\langle L, \sqsubseteq \rangle$ будет решёточно упорядоченным множеством.

Доказательство.

1. Необходимо проверить справедливость аксиом решётки для введённых операций \sqcup и \sqcap в решёточно упорядоченном множестве P . Выполнение законов коммутативности и ассоциативности очевидно. Покажем справедливость законов поглощения.

Пусть x и y — произвольные элементы P .

Abs1: $x \sqcap (x \sqcup y) = \inf \{x, \sup \{x, y\}\}$; имеем $x \sqsubseteq \sup \{x, y\} = z$ и поэтому $\inf \{x, z\} = x$.

Abs2: По двойственности.

2. Удостоверимся в справедливости свойств рефлексивности, антисимметричности и транзитивности у введённого отношения \sqsubseteq в решётке L . Для произвольных элементов $x, y, z \in L$ имеем

$$\text{R: } x \sqsubseteq x \Leftrightarrow x \sqcap x = x;$$

$$\text{AS: } \begin{cases} x \sqsubseteq y \\ y \sqsubseteq x \end{cases} \Leftrightarrow \begin{cases} x \sqcap y = x \\ y \sqcap x = y \end{cases} \Leftrightarrow x = y;$$

T:

$$\begin{cases} x \sqsubseteq y \\ y \sqsubseteq z \end{cases} \Leftrightarrow \begin{cases} x \sqcup y = y \\ y \sqcup z = z \end{cases} \Rightarrow x \sqcup y \sqcup z = y \sqcup z \Leftrightarrow x \sqcup z = z \Leftrightarrow x \sqsubseteq z.$$

Таким образом, $\langle L, \sqsubseteq \rangle$ есть ч.у. множество. Убедимся, что оно решёточно упорядочено. Пусть z — верхняя грань элементов x и y . Тогда

$$\begin{cases} x \sqsubseteq z \\ y \sqsubseteq z \end{cases} \Leftrightarrow \begin{cases} x \sqcup z = z \\ y \sqcup z = z \end{cases} \Rightarrow (x \sqcup y) \sqcup z = z \Leftrightarrow (x \sqcup y) \sqsubseteq z.$$

Поэтому супремум множества $\{x, y\}$ существует и $\sup \{x, y\} = x \sqcup y$.

Аналогично показывается, что $\inf \{x, y\} = x \sqcap y$. Следовательно, $\langle L, \sqsubseteq \rangle$ — решёточно упорядоченное множество.

Заметим, что следование \Rightarrow может быть заменено на равносильность \Leftrightarrow в доказательстве (T) — на основании свойства 2 теоремы 2.3, а в последнем выводе — на основании пункта 3 доказываемого ниже утверждения 4.3. \square

Следствие. Для $x, y \in \langle P, \sqsubseteq \rangle$ справедливо $x \sqcap y \sqsubseteq x \sqsubseteq x \sqcup y$, причём $x \sqcup y$ — наименьший, а $x \sqcap y$ — наибольший элементы, содержащие как x , так и y .

Теорема 4.1 устанавливает взаимно-однозначное соответствие между решёточно упорядоченными множествами и решётками: из одной АС всегда можно получить другую. Поэтому термин «решётка» применяют для обоих понятий, имея в виду, что любую решётку можно представить либо как ч.у. множество, либо как алгебру. Например, решёточно упорядоченные множества $\langle \mathbb{R}, \leq \rangle$, $\langle \mathbb{N}, | \rangle$ и $\langle \mathcal{P}(A), \subseteq \rangle$ примера 4.1 можно записать в виде решёток $\langle \mathbb{R}, \max, \min \rangle$, $\langle \mathbb{N}, \vee, \wedge \rangle$ и $\langle \mathcal{P}(A), \cup, \cap \rangle$ соответственно. Возможность такого

рассмотрения решёток позволяет вводить в них как порядковые, так и алгебраические операции, что приводит к богатой и многообразной в приложениях теории.

Атомы [коатомы] решётки есть её атомы [коатомы] как ч.у. множества.

Решётка называется *полной*, если любое подмножество её элементов имеет точные верхнюю и нижнюю грани (ср. с определением полной булевой алгебры на с. 21). Например, отрезок $[0, 1]$ с обычным порядком и произвольная тотальная алгебра множеств являются полными решётками, а решётки $\langle \mathbb{N}, | \rangle$ и $\langle \mathbb{Z}, \leq \rangle$ не являются полными, т.к. ни одно бесконечное подмножество в первой них не имеет точной верхней грани, а во второй — не имеет хотя бы одной из точных граней. Ясно также, что все полные решётки должны иметь универсальные грани.

В приложениях часто используется в приложениях следующая

Теорема 4.2. *Частично упорядоченное множество является полной решёткой, если и только если*

- 1) оно имеет наибольший элемент ι ;
- 2) для любого его непустого подмножества A существует точная нижняя грань $\inf A$.

Доказательство. (\Leftarrow) Пусть $\langle P, \sqsubseteq \rangle$ — полная решётка. Тогда каждое о непустое подмножество $A \subseteq P$ имеет и точную нижнюю грань $\inf A$, и точную верхнюю грань $\sup A$. В частности, существует $\sup P = \iota$.

(\Rightarrow) Покажем, что в условиях теоремы каждое непустое подмножество $A \subseteq P$ имеет точную верхнюю грань. Рассмотрим A^Δ — совокупность всех верхних граней A .

Очевидно, $\iota \in A^\Delta$, так что $A^\Delta \neq \emptyset$. По условию существует элемент $b = \inf A^\Delta$. Этот элемент и будет точной верхней гранью подмножества A , откуда заключаем, что рассматриваемая решётка полная. \square

Следствие. *Конечное ч.у. множество является решёткой, если и только если:*

- 1) оно имеет наибольший элемент;
- 2) для любых двух его элементов существует точная нижняя грань.

В практических ситуациях проверка наличия точных нижних граней у подмножеств ч.у. множества обычно не вызывает затруднений, в то время как отыскание точных верхних граней, как правило, требует значительных усилий. Теорема 4.2 и следствие из неё являются эффективными критериями решёточности порядков.

В частности, справедливо

Утверждение 4.2. *Решётка всех разбиений множества является полной.*

Доказательство. Точной нижней гранью любой совокупности эквивалентностей является их пересечение (всегда эквивалентность), а единицей решётки всех эквивалентностей (разбиений) множества служит аморфная эквивалентность ∇ . Осталось применить теорему 4.2. \square

4.2 Основные свойства решёток. Решёточные гомоморфизмы, идеалы и фильтры

Легко показываются нижеследующие элементарные свойства решёток.

Утверждение 4.3. Для любых элементов x, y, u, v решётки $\langle L, \sqcup, \sqcap \rangle$ справедливы следующие соотношения:

1.

$$\left\{ \begin{array}{l} x \sqsubseteq y \\ u \sqsubseteq v \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x \sqcup u = y \sqcup v \\ y \sqcap u = y \sqcap v \end{array} \right. ;$$

2.

$$x \sqsubseteq y \Rightarrow \left\{ \begin{array}{l} x \sqcup u \sqsubseteq y \sqcup u \\ x \sqcap u \sqsubseteq y \sqcap u \end{array} \right. ;$$

3.

$$\left\{ \begin{array}{l} x \sqsubseteq z \\ y \sqsubseteq z \end{array} \right\} \Leftrightarrow x \sqcup y \sqsubseteq z, \quad \left\{ \begin{array}{l} x \sqsubseteq y \\ x \sqsubseteq z \end{array} \right\} \Leftrightarrow x \sqsubseteq y \sqcap z.$$

Доказательство. Докажем, например, последнее соотношение, оставив остальные в качестве простого упражнения. Имеем, во-первых

$$\left\{ \begin{array}{l} x \sqsubseteq y \\ x \sqsubseteq z \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x \sqcap y = x \\ x \sqcap z = x \end{array} \right\} \Rightarrow x \sqcap (y \sqcap z) = x \Leftrightarrow x \sqsubseteq y \sqcap z$$

и, во-вторых,

$$x \sqsubseteq y \sqcap z \Leftrightarrow x \sqcap (y \sqcap z) = x \Rightarrow x = \inf \{x, y, z\} \Rightarrow \left\{ \begin{array}{l} x \sqsubseteq y \\ x \sqsubseteq z \end{array} \right. .$$

□

Теорема 4.3. Элементы x, y и z любой решётки удовлетворяют следующим неравенствам полудистрибутивности

$$\begin{aligned} Dtr1 \sqsupseteq: & (x \sqcup y) \sqcap z \sqsupseteq (x \sqcap z) \sqcup (y \sqcap z); \\ Dtr2 \sqsubseteq: & (x \sqcap y) \sqcup z \sqsubseteq (x \sqcup z) \sqcap (y \sqcup z) \end{aligned}$$

и полумодулярности

$$\begin{aligned} Mod \sqsubseteq: & x \sqsubseteq y \Rightarrow x \sqcup (y \sqcap z) \sqsubseteq y \sqcap (x \sqcup z) = (x \sqcap y) \sqcup (y \sqcap z); \\ Mod \sqsupseteq: & x \sqsupseteq y \Rightarrow x \sqcap (y \sqcup z) \sqsupseteq y \sqcup (x \sqcap z) = (x \sqcup y) \sqcap (y \sqcup z). \end{aligned}$$

Доказательство. Для произвольных элементов x, y и z решётки имеем

$$\left. \begin{array}{l} x \sqcap z \sqsubseteq x \sqsubseteq x \sqcup y \\ x \sqcap z \sqsubseteq z \end{array} \right\} \Rightarrow x \sqcap z \sqsubseteq (x \sqcup y) \sqcap z$$

и

$$\left. \begin{array}{l} y \sqcap z \sqsubseteq y \sqsubseteq x \sqcup y \\ y \sqcap z \sqsubseteq z \end{array} \right\} \Rightarrow y \sqcap z \sqsubseteq (x \sqcup y) \sqcap z.$$

Таким образом, $(x \sqcup y) \sqcap z$ есть верхняя грань для $x \sqcap z$ и $y \sqcap z$. Это означает, что

$$(x \sqcap z) \sqcup (y \sqcap z) \sqsubseteq (x \sqcup y) \sqcap z,$$

и следование $Dtr1 \sqsupseteq$ доказано. Второе неравенство полудистрибутивности следует из только что доказанного по принципу двойственности.

Неравенства полумодулярности есть частный случай неравенств полудистрибутивности. □

Используя неравенства полудистрибутивности, можно усилить свойства порядка, приведённые в утверждении 4.3.

Лемма 4.1 (о четырёх элементах). Для любых элементов x, y, u, v решётки $\langle L, \sqcup, \sqcap \rangle$ справедливо соотношение

$$x, y \sqsubseteq u, v \Rightarrow x \sqcup y \sqsubseteq u \sqcap v.$$

Доказательство. В $Dtr2 \sqsubseteq$ произведя замены $x \mapsto u, y \mapsto v$ и $z \mapsto x$, получим

$$(u \sqcap v) \sqcup x \sqsubseteq (u \sqcup x) \sqcap (v \sqcup x).$$

Далее, поскольку $u \sqcup x = u, v \sqcup x = v$ и $y \sqsubseteq u \sqcap v$, получим требуемое. \square

Определение 4.3. Отображение φ решётки L в решётку L' называется *алгебраическим* или *решёточным гомоморфизмом*, если для любых $x, y \in L$ справедливы равенства

$$\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y) \quad \text{и} \quad \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y).$$

Биективный решёточный гомоморфизм есть *решёточный изоморфизм*. Изоморфизм решётки в себя называется *автоморфизмом*.

Инъективные и сюръективные решёточные гомоморфизмы называют *решёточными* (или *алгебраическими*) *мономорфизмами* (*вложениями*) и *эпиморфизмами* соответственно.

Порядковые гомоморфизмы решёток как ч.у. множеств, вообще говоря, не являются алгебраическими. Действительно, для упорядоченных по включению конечных подмножеств множества M отображение $\varphi: \mathcal{P}_0(M) \rightarrow \mathbb{N}_0$ такое, что $\varphi(X) = |X|$ для $X \subseteq M$, являясь изотонным, не сохраняет ни одну из решёточных операций, поскольку, например, для произвольных подмножеств A и B

$$\varphi(A \cup B) = |A \cup B| \neq \max\{|A|, |B|\} = \max\{\varphi(A), \varphi(B)\}.$$

Напротив, любое отображение одной решётки на другую, сохраняющее хотя бы одну из решёточных операций, изотонно, т.е. является порядковым гомоморфизмом. Действительно, если φ сохраняет пересечение, то для любых $x, y \in L$ имеем

$$x \sqsubseteq y \Leftrightarrow x = x \sqcap y \stackrel{(*)}{\Rightarrow} \varphi(x) = \varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y) \Leftrightarrow \varphi(x) \sqsubseteq \varphi(y), \quad (4.2)$$

и, значит, φ изотонно. Аналогично изотонность φ следует и из сохранения объединения.

В случае изоморфизма проблемы снимаются.

Теорема 4.4 (об эквивалентности двух видов изоморфизма решёток). Две решётки алгебраически изоморфны, если и только если они изоморфны как ч.у. множества.

Доказательство. (\Leftarrow) Пусть φ — алгебраический изоморфизм решётки L на некоторую другую решётку. Так как отображение φ взаимно-однозначно и изотонно, остаётся убедиться в его обратной изотонности. Это устанавливается обращением следования $\stackrel{(*)}{\Rightarrow}$ в (4.2), что можно сделать в силу взаимно-однозначности φ .

(\Rightarrow) Пусть L_1 и L_2 — две решётки, изоморфные как порядки. Докажем согласованность операции \sqcap относительно порядкового изоморфизма φ , т.е. что $\varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y)$ при условии $x \sqsubseteq y \Leftrightarrow \varphi(x) \sqsubseteq \varphi(y)$ и биективности φ .

Для произвольных элементов $x, y \in L_1$ в силу изотонности φ в решётке L_2 элемент $\varphi(x \sqcap y)$ будет нижней гранью и элемента $\varphi(x)$, и элемента $\varphi(y)$: $\varphi(x \sqcap y) \sqsubseteq \varphi(x)$ и

$\varphi(x \sqcap y) \sqsubseteq \varphi(y)$. Пусть b также есть нижняя грань этих элементов в L_2 . Тогда, в силу сюръективности φ , в L_1 найдется прообраз b — элемент a и

$$\begin{cases} b = \varphi(a) \sqsubseteq \varphi(x) \\ b = \varphi(a) \sqsubseteq \varphi(y) \end{cases} \Leftrightarrow \begin{cases} a \sqsubseteq x \\ a \sqsubseteq y \end{cases}.$$

Отсюда далее имеем

$$a \sqsubseteq x \sqcap y \Leftrightarrow b = \varphi(a) \sqsubseteq \varphi(x \sqcap y).$$

Таким образом, $\varphi(x \sqcap y)$ будет наибольшей нижней гранью для $\{\varphi(x), \varphi(y)\}$, или, что то же, $\varphi(x \sqcap y) = \varphi(x) \sqcap \varphi(y)$.

Согласованность операции \sqcap относительно φ справедлива по двойственности. \square

Данная теорема позволяет не различать типы изоморфизма решёток и использовать для них единый символ \cong или \cong_{φ} , когда надо указать изоморфизм φ .

Теорема 4.5 (о неподвижной точке). Если φ — автоморфизм полной решётки $\langle L, \sqcup, \sqcap \rangle$, то $\varphi(x) = x$ для некоторого $x \in L$.

Доказательство. Пусть Y — множество всех таких элементов $y \in L$, что $y \sqsubseteq \varphi(y)$. Ясно, что $Y \neq \emptyset$, поскольку Y содержит, например, нуль решётки $x \in L$. Тогда существует элемент $x = \sup Y$ и для всякого $y \in Y$ имеем $y \sqsubseteq \varphi(y) \sqsubseteq \varphi(x)$, откуда $x \sqsubseteq \varphi(x)$. Но тогда $\varphi(x) \sqsubseteq \varphi(\varphi(x))$, что влечёт $\varphi(x) \in Y$, и значит, $\varphi(x) \sqsubseteq x = \sup Y$. Таким образом, $x \sqsubseteq \varphi(x) \sqsubseteq x$, т.е. $\varphi(x) = x$. \square

Доказанная теорема не допускает обращения: ч.у. множество Z_3 не является не только полной решёткой, но даже и просто решёткой, однако все его автоморфизмы, очевидно имеют неподвижную точку.

Следующая теорема показывает, как пополнить произвольное ч.у. множество до (полной) решётки.

Теорема 4.6 (Макнил). Всякое ч.у. множество можно вложить в подходящую полную решётку с сохранением всех точных граней.

Доказательство. Напомним, что через \widehat{R} мы обозначаем ч.у. множество R пополненное максимальным и/или минимальным элементами, если оно не имеет таковых.

Пусть дано ч.у. множество P . Для $X \subseteq \widehat{P}$ обозначим $G(X) = \widehat{X}^{\Delta}$ и $L(X) = \widehat{X}^{\nabla}$. Ясно, что они непусты, если $X \neq \emptyset$. Образует множество $Q = \{L(G(X)) \mid X \in \mathcal{P}^*(\widehat{P})\}$ с порядком по включению. Нетрудно установить, что Q есть искомая решётка. \square

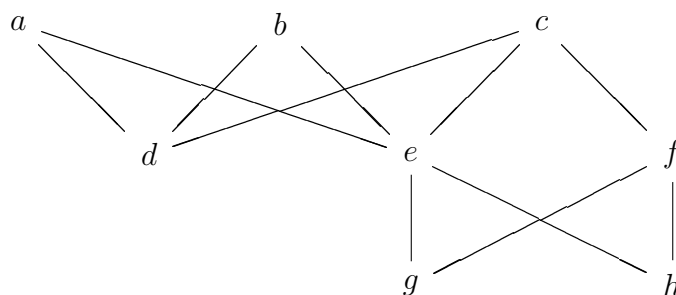
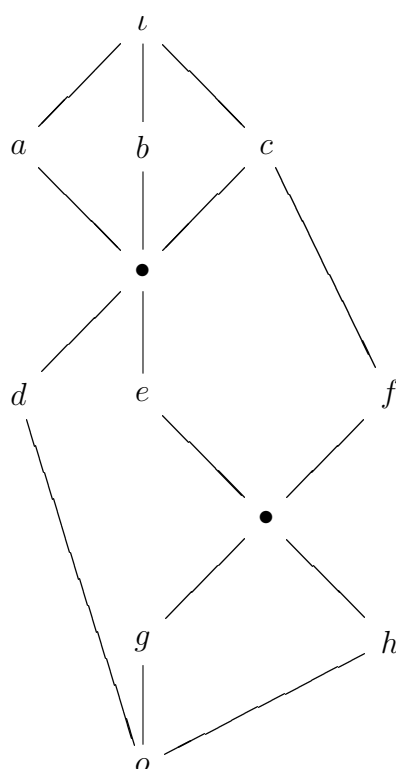
При построении решётки Q с указанным свойством по данному ч.у. множеству P говорят, что последнее пополняется сечениями Макнилла, а Q является замыканием (Макнилла) ч.у. множества P (символически $Q = \text{comp}(P)$). Доказано [54], что $\dim(P) = \dim(\text{comp}(P))$.

Пример замыкания показан на рис. 4.6 и 4.7. На последней диаграмме универсальные грани и элементы, отмеченные знаком \bullet суть сечения Макнилла.

Теорема 4.9 показывает, что знаменитое построение Р. Дедекиндом действительных чисел «сечениями» на самом деле применимо для любого ч.у. множества.

Определение 4.4. Непустое подмножество L' решётки $\langle L, \sqcup, \sqcap \rangle$ называется подрешёткой решётки L (символически $L' \leq L$), если L' устойчиво относительно сужений \sqcup и \sqcap .

Из определения следует, что подмножество элементов решётки L может быть решёткой относительно частичного порядка на L , но не подрешёткой L .

Рис. 4.6: Ч.у. множество P Рис. 4.7: Замыкание Макнила $\text{comp}(P)$ ч.у. множества P с рис. 4.6

- Пример 4.3.**
1. Любое одноэлементное подмножество решётки есть её подрешётка. Каждое подмножество решётки L является подрешёткой, если и только если L — цепь.
 2. Решётка $L' \cong N_5$, образованная элементами o, a, c, d, e (выделены жирным) не является подрешёткой решётки L (см. рис. 4.8), поскольку $c \sqcap d$ в L есть b , а в $L' = o$.
 3. Если L — решётка, то совокупность её подрешёток $\text{Sub } L$ — ч.у. множество, упорядоченное по включению.
 4. Любой интервал решётки есть её подрешётка, но не любая подрешётка есть интервал. Пересечение подрешёток либо пусто, либо является подрешёткой. В силу этого, оказывается удобным считать подрешёткой и пустое множество. Тогда пересечение любой совокупности подрешёток и любой интервал решётки оказываются подрешётками.

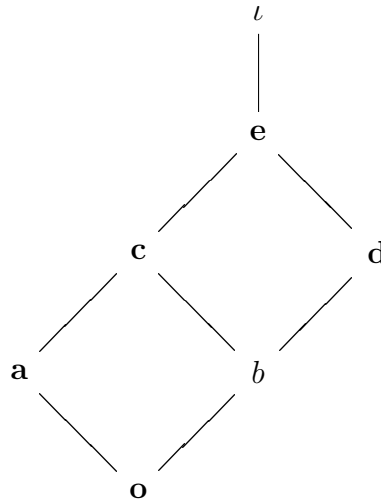


Рис. 4.8: Ч.у. подмножество (выделено жирным) — решётка, но не подрешётка исходной

5. Пусть $L = \langle L, \sqcup, \sqcap \rangle$ — решётка. Тогда совокупность её интервалов $Si(L)$ — также решётка относительно операций

$$[a, b] \cup [c, d] \triangleq [a \sqcap c, b \sqcup d] \quad \text{и} \quad [a, b] \cap [c, d] \triangleq [a \sqcup c, b \sqcap d], \quad a, b, c, d \in L.$$

Очевидно, $Si(L)$ — решётка с универсальными гранями: её единицей служит L , а нулём — пустой интервал.

6. Если φ — гомоморфизм решётки L в решётку L' , то $\text{Im } \varphi \leq L'$.
 7. Обозначим через \mathbb{N}° множество натуральных чисел, свободных от квадратов (см. пример 1.5.4), включая в него и 1. Тогда $\langle \mathbb{N}^\circ, \vee, \wedge \rangle \leq \langle \mathbb{N}, \vee, \wedge \rangle$.
 8. С помощью теоремы 4.4 устанавливается, что введённая выше решётка \mathbb{N}° изоморфна решётке $\mathcal{P}_0(A)$ всех конечных подмножеств счётного множества A .

Положим сначала $\varphi(1) = \emptyset$. Затем построим биекцию φ между множеством простых чисел и A . Для этого пронумеруем элементы A в произвольном порядке: $A = \{a_1, a_2, \dots\}$ и положим $\varphi(p_i) = a_i$, где p_i — i -е простое число. Таким образом, определено частичное инъективное отображение для простых чисел из \mathbb{N}° в A . Для остальных элементов $n = p_1 \cdot \dots \cdot p_k$ из \mathbb{N}° , где p_1, \dots, p_k — различные простые числа, положим $\varphi(n) = \{\varphi(p_1), \dots, \varphi(p_k)\}$. Понятно, что $\mathbb{N}^\circ \cong \mathcal{P}_0(A)$, если A — счётно.

9. Если G — группа, то множество всех её подгрупп $\text{Sub } G$ является, как известно, решёткой, однако $\text{Sub } G \not\leq \mathcal{P}(G)$.

Элемент e решётки L с универсальными гранями называют *центральной*, если при любом представлении $L = A \times B$ (A и B — решётки) имеет место либо $e = (o, \iota)$, либо $e = (\iota, o)$. Совокупность всех центральных элементов решётки называется её *центром*. Центр любой решётки оказывается её подрешёткой, и более того, булевой алгеброй.

Определение 4.5. Пусть $\langle L, \sqcup, \sqcap \rangle$ — решётка. Непустое подмножество I элементов L называется её (*решёточным*) *идеалом*, если

$$1) \ x \in I \ \& \ y \sqsubseteq x \Rightarrow y \in I \quad \text{и} \quad 2) \ x, y \in I \Rightarrow x \sqcup y \in I.$$

Двойственно, непустое подмножество F элементов L называется её *решёточным фильтром*, если

$$1) \ x \in F \ \& \ x \sqsubseteq y \Rightarrow y \in F \quad \text{и} \quad 2) \ x, y \in F \Rightarrow x \sqcap y \in F.$$

Мы видим, что решёточные идеалы [фильтры] суть непустые и устойчивые относительно операции \sqcup [\sqcap] порядковые идеалы [фильтры] решёток. Условия для решёточных идеалов и фильтров в приведённом определении часто заменяют на эквивалентные

$$x \in I \& y \in L \Rightarrow x \sqcap y \in I \quad \text{и} \quad x \in F \& y \in L \Rightarrow x \sqcup y \in F$$

соответственно. Непустое подмножество I [F] оказывается решёточным идеалом [фильтром], если и только если для любых её элементов x и y справедлива эквивалентность

$$x, y \in I \Leftrightarrow x \sqcup y \in I \quad [x, y \in F \Leftrightarrow x \sqcap y \in F].$$

Если решётка имеет наименьший [наибольший] элемент, то он будет её идеалом [фильтром]. Пусть a — элемент решётки L , тогда её главные порядковые идеал $J(a) = a^\nabla$ и фильтр a^Δ являются, очевидно, также и (*главными*) решёточными идеалом и фильтром. Легко видеть, что в конечной решётке все идеалы и фильтры — главные. Действительно, если I — идеал конечной решётки, то рассмотрим элемент $x = \bigsqcup_{a \in I} a$, для которого будем иметь $x \in I$ и $I = x^\nabla$ (аналогично для фильтров). Для бесконечных решёток построить элемент a , как это было сделано выше, вообще говоря, нельзя. Поэтому могут существовать и неглавные решёточные идеалы и фильтры.

Пример 4.4. 1. Если A — бесконечное множество, то совокупность $\mathcal{P}_0(A)$ всех его конечных подмножеств будет неглавным идеалом решётки $\mathcal{P}(A)$.

2. Рассмотрим цепь $[0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \dots, 5]$ и её подцепь $[0, 5]$. Исходная цепь есть решётка, а $I = \bigcup_{x \in [0,5)} x^\nabla$ — её неглавный идеал.

Сама решётка L всегда будет своим идеалом и фильтром. Все другие идеалы и фильтры L называют *собственными*. Понятно, что для решётки с единицей [нулём] идеал [фильтр] собственный, если и только если он не содержит единицу и [нуль]. Так, идеал I , построенный в п. 2 примера 4.4 собственный.

Множество всех собственных решёточных идеалов обозначим $J_*(L)$. Ясно, что это ч.у. множество, упорядоченное по включению. Если решётка содержит нуль o , то множество $\{o\}$ является наименьшим решёточным идеалом, в противном случае в число идеалов договариваются включать пустое множество. Поэтому $J_*(L)$ всегда имеет наименьший элемент. Максимальные элементы $J_*(L)$ называют *максимальными идеалами* решётки L ; таким образом максимальный идеал решётки не содержится ни в каком другом её собственном идеале. Существование максимальных решёточных идеалов и их связь с другими идеалами решётки определяет следующая

Теорема 4.7 (о собственных идеалах решётки с единицей). *Всякий собственный идеал решётки с единицей содержится в некотором её максимальном идеале.*

Доказательство. Пусть $\langle L, \sqsubseteq \rangle$ — решётка с единицей ι . Покажем, что в ч.у. множестве $\langle J_*(L), \subseteq \rangle$ всех собственных решёточных идеалов L каждая цепь имеет верхнюю грань и сошлёмся затем на лемму Куратовского-Цорна¹.

Пусть $C = [J_1, J_2, \dots]$ — некоторая (конечная или бесконечная) цепь собственных идеалов L . Обозначим $J = \bigcup_{J_k \in C} J_k$ и удостоверимся, что $J \in J_*(L)$, т.е. является собственным идеалом решётки L .

Действительно, если $x \in J$, то $x \in J_k \in C$ для некоторого k . Для любого $y \sqsubseteq x$ имеем $y \in J_k \subseteq J$. Пусть далее $x, y \in J$. Тогда $x \in J_k \in C$ и $y \in J_l \in C$ для некоторых k, l . Поскольку C — цепь, то J_k и J_l сравнимы в $J_*(L)$. Без ограничения общности считаем, что $J_k \subseteq J_l$. Тогда $x, y \in J_l$ и, поскольку J_l — идеал, то $x \sqcup y \in J_l \subseteq J$.

¹Эффективное доказательства данного факта неизвестно.

Таким образом, J — идеал решётки L . Более того, он собственный, поскольку $\iota \notin J_k \in C$ влечёт $\iota \notin J$. С другой стороны, поскольку $J_k \subseteq J$ для всех $J_k \in C$, то J будет верхней гранью цепи C . \square

Например, идеал I , построенный в п. 2 примера 4.4 максимальный.

Если имеется гомоморфизм φ решётки L на решётку с нулём 0 , то прообраз нуля $\varphi^\sharp(0)$ является идеалом L . Такой идеал называется *ядерным*. Решётки могут иметь и неядерные идеалы: например, идеал $\langle b \rangle = \{o, a, b, e\}$ решётки, изображённой на рис. 4.9, как можно показать, ядерным не является.

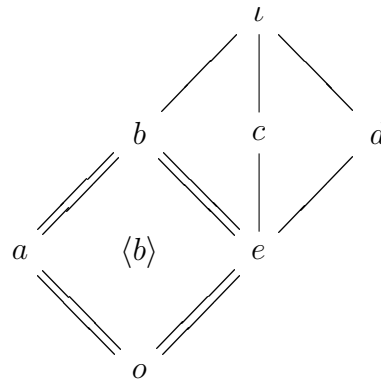


Рис. 4.9: Решётка с неядерным идеалом $\langle b \rangle$

Диаграммы Хассе остаются удобным способом описания решёток. Однако если решётка устроена слишком сложно, такие диаграммы становятся мало наглядными. Другие возможности представления решёток даёт следующая

Теорема 4.8 (о представлении решёток). *Всякая решётка может быть вложена с сохранением всех точных нижних граней в булеан подходящего множества.*

Доказательство. Пусть L — решётка. По теореме 3.7 о представлении ч.у. множеств отображение $\varphi(x) = x^\nabla$ осуществляет вложение L в $\mathcal{P}(L)$ как ч.у. множество. Осталось удостовериться, что φ сохраняет пересечения, т.е. $\varphi(x \sqcap y) = \varphi(x) \cap \varphi(y)$.

Для этого достаточно показать, что $(x \sqcap y)^\nabla = x^\nabla \cap y^\nabla$:

$$z \in (x \sqcap y)^\nabla \Leftrightarrow z \sqsubseteq (x \sqcap y) \Leftrightarrow \begin{cases} z \sqsubseteq x \\ z \sqsubseteq y \end{cases} \Leftrightarrow \begin{cases} z \in x^\nabla \\ z \in y^\nabla \end{cases} \Leftrightarrow z \in (x^\nabla \cap y^\nabla).$$

Поэтому

$$\varphi(x \sqcap y) = (x \sqcap y)^\nabla = x^\nabla \cap y^\nabla = \varphi(x) \cap \varphi(y)$$

и φ — искомое вложение. \square

Данная теорема позволяет представлять элементы любой решётки подмножествами некоторого множества A , пользуясь аналогами диаграмм Эйлера-Венна. В таких диаграммах результат операции пересечения отождествляют с теоретико-множественным пересечением в A , наибольшему элементу решётки (если он существует) соответствует само множество A , а наименьшему (если он есть) договариваются сопоставлять пустое множество (хотя по теореме 4.8 о представлении решёток имеем $\varphi(o) = o^\nabla = \{o\}$, но точка, соответствующая o , содержится во всех идеалах решётки, и её можно удалить без нарушения отношения включения идеалов).

Выясним, как следует обозначать результат объединения (точные верхние грани) на таких диаграммах. Имеем

$$z \in \varphi(x) \cup \varphi(y) = x^\nabla \cup y^\nabla \Leftrightarrow \begin{cases} z \in x^\nabla \\ z \in y^\nabla \end{cases} \Leftrightarrow \begin{cases} z \sqsubseteq x \\ z \sqsubseteq y \end{cases} \Rightarrow \\ \Rightarrow z \sqsubseteq x \sqcup y \Leftrightarrow z \in (x \sqcup y)^\nabla = \varphi(x \sqcup y).$$

Таким образом, $\varphi(x) \cup \varphi(y) \subseteq \varphi(x \sqcup y)$, причём равенство в этом выражении, как нетрудно видеть, будет лишь в случае сравнимости x и y . Поэтому при обозначении объединения элементов, изображаемых в виде связанных выпуклых областей, необходимо рисовать выпуклую область, покрывающую “с запасом” области, соответствующие данным элементам (см. рис. 4.10).

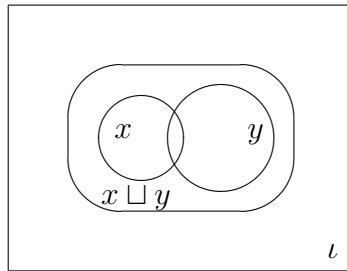


Рис. 4.10: Обозначение объединения элементов решётки

Приведём без доказательств ещё два утверждения относительно вложимости решёток.

Теорема 4.9 (Макнил). *Всякую решётку можно вложить в подходящую полную решётку с сохранением всех точных граней.*

Теорема 4.10. *Всякую конечную решётку можно вложить в конечную решётку разбиений.*

Далее мы рассмотрим специальные типы решёток.

4.3 Модулярные решётки

Определение 4.6. Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *модулярной*, если для любых $x, y, z \in L$ в ней выполняется следующий *модулярный закон*

$$Mod: x \sqsubseteq y \Rightarrow x \sqcup (y \sqcap z) = y \sqcap (x \sqcup z).$$

Ясно, что смысл модулярного закона состоит в выполнении следования, обратного утверждаемому в $Mod \sqsubseteq$. Двойственный к модулярному закон

$$x \sqsupseteq y \Rightarrow x \sqcap (y \sqcup z) = y \sqcup (x \sqcap z)$$

ему эквивалентен. Поэтому для модулярных решёток принцип двойственности остается справедливым.

Пример 4.5. 1. Модулярными являются все цепи, решётка $\langle \mathbb{N}, | \rangle$, булевы алгебры и их подрешётки. Впоследствии мы увидим, что для этих решёток справедливо более сильное условие дистрибутивности.

2. Решётка $\text{NSub } G$ всех нормальных подгрупп группы G образует модулярную решётку. Действительно, пусть X, Y, Z — произвольные нормальные подгруппы группы G и $X \subseteq Y$. Известно, что объединение $X \cup Z$ двух нормальных подгрупп X и Z группы G совпадает с их произведением $XZ \triangleq \{g \in G \mid \exists x \exists z (g = xz)\}$, а пересечение подгрупп всегда есть подгруппа. Поэтому нам нужно показать справедливость включения $Y \cap XZ \subseteq X(Z \cap Y)$ при условии $X \subseteq Y$. В самом деле, всегда найдутся такие $x \in X$ и $z \in Z$, что

$$t \in Y \cap XZ \Rightarrow \begin{cases} t \in Y \\ t = xz \end{cases} \stackrel{z=x^{-1}t \in Y}{\Rightarrow} \begin{cases} z \in Y \cap Z \\ t = xz \end{cases} \Rightarrow t \in X(Z \cap Y).$$

Модулярные решётки часто называют *дедекиндовыми*, поскольку указанное свойство нормальных подгрупп обнаружил в 1900 г. Р. Дедекинд.

3. Другим важным примером модулярной решётки является решётка всех подпространств векторного пространства. Под объединением подпространств понимается наименьшее подпространство, их содержащее. Доказательство этого факта полностью аналогично доказательству модулярности решётки $\text{NSub } G$. Точно так же доказывают, что решётка всех идеалов любого кольца модулярна.

Решётка всех эквивалентностей на данном множестве в общем случае не модулярна. Действительно, рассмотрим множество $M = \{1, 2, 3, 4\}$. Среди $\mathcal{E}(M)$ имеются эквивалентности α, β и γ со соответствующими разбиениями на смежные классы $D_\alpha = \{\{1\}, \{2\}, \{3, 4\}\}$, $D_\beta = \{\{1\}, \{2, 3\}, \{4\}\}$ и $D_\gamma = \{\{1, 2\}, \{3, 4\}\}$ соответственно. Вместе с диагональным отношением в качестве o и аморфной эквивалентностью в качестве ι они образуют решётку N_5 . Однако она немодулярна, поскольку $\alpha \sqsubseteq \gamma$, но

$$\alpha \sqcup (\gamma \sqcap \beta) = \alpha \sqcup o = \alpha \neq \gamma \sqcap (\alpha \sqcup \beta) = \gamma \sqcap \iota = \gamma.$$

Таким образом, решётка $\langle \mathcal{E}(M), \sqsubseteq \rangle$ может содержать немодулярную подрешётку, и, следовательно, в общем случае немодулярна сама.

Немодулярность N_5 оказывается ключевой: справедлива

Теорема 4.11 (критерий модулярности решётки). *Решётка модулярна, если и только если никакая её подрешётка не изоморфна пятиугольнику N_5 .*

Доказательство. (\Leftarrow) Поскольку пятиугольник не модулярен, то никакая решётка, содержащая изоморфную ему подрешётку, не может быть модулярной.

(\Rightarrow) Покажем, что немодулярная решётка L содержит подрешётку, изоморфную пятиугольнику N_5 .

Немодулярность L означает существование таких её элементов x, y и z , что $x \sqsubseteq y$, но $x \sqcup (y \sqcap z) \sqsubset y \sqcap (x \sqcup z)$. Покажем, что элементы $y \sqcap z, x \sqcup (y \sqcap z), y \sqcap (x \sqcup z), z, x \sqcup z$ образуют подрешётку в L , изоморфную N_5 .

В самом деле, должны иметь место соотношения

$$y \sqcap z \sqsubset z \sqsubset x \sqcup z \quad \text{и} \quad y \sqcap z \sqsubset x \sqcup (y \sqcap z) \sqsubset y \sqcap (x \sqcup z) \sqsubset x \sqcup z,$$

поскольку, заменив первый, второй, третий или пятый знак \sqsubset на $=$, получим $x \sqsubseteq z$ или $z \sqsubseteq y$, откуда сразу следует модулярный закон.

Далее

$$x \sqcup z = (x \sqcup z) \sqcup z \sqsubseteq (x \sqcup (y \sqcap z)) \sqcup z \sqsubseteq (y \sqcap (x \sqcup z)) \sqcup z \sqsubseteq (x \sqcup y) \sqcup z = x \sqcup z.$$

Это означает, что элементы $x \sqcup (y \sqcap z)$ и $y \sqcap (x \sqcup z)$ оба дают в объединении с z элемент $x \sqcup z$.

Кроме того,

$$y \sqcap z = (y \sqcap z) \sqcap z \sqsubseteq (x \sqcup (y \sqcap z)) \sqcap z \sqsubseteq (y \sqcap (x \sqcup z)) \sqcap z = y \sqcap ((x \sqcup z) \sqcap z) = y \sqcap z.$$

Это означает, что элементы $x \sqcup (y \sqcap z)$ и $y \sqcap (x \sqcup z)$ оба дают в пересечении с z элемент $y \sqcap z$. \square

Ясно, что невыполнение цепного условия Жордана–Дедекинда (3.2) для некоторой решётки означает существование у неё подрешётки, изоморфной N_5 , и, по доказанному критерию, её немодулярность. При этом выполнение указанного условия, очевидно, ещё не означает модулярности решётки.

Пример 4.6. 1. Для решётки, изображённой на рис. 4.11.1) цепное условия Жордана–Дедекинда не выполняется: длины её максимальных цепей между универсальными гранями элементами не совпадают, и, как следствие, она содержит подрешётку, изоморфную N_5 , что влечёт её немодулярность.

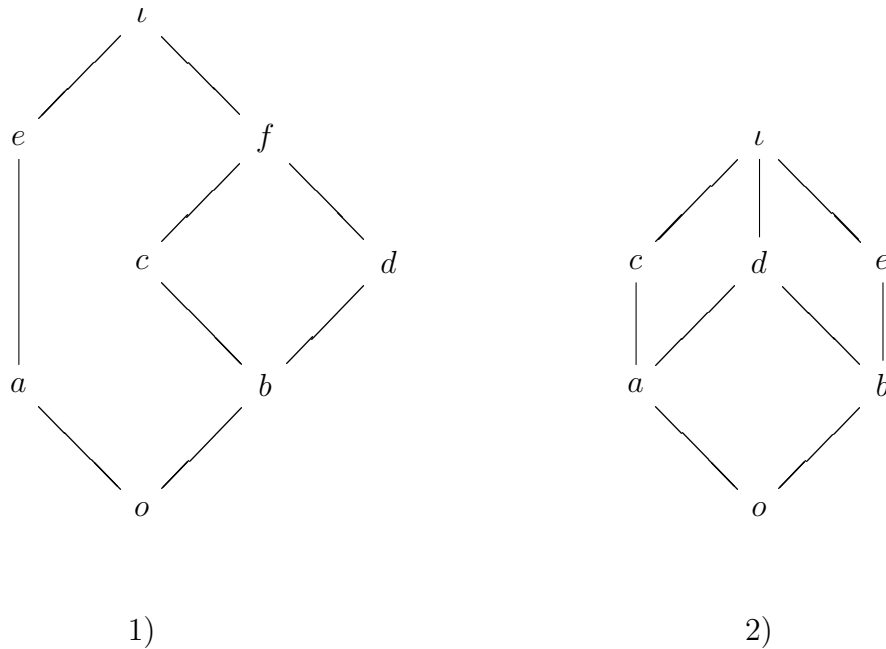


Рис. 4.11: Немодулярные решётки с невыполненным (1) и выполненным (2) условием Жордана–Дедекинда

2. Для решётки, изображённой на рис. 4.11.2) цепное условия Жордана–Дедекинда выполняется, однако она немодулярна, т.к. содержит подрешётку изоморфную N_5 .

В заключении раздела приведём ещё два критерия модулярности решёток.

Теорема 4.12. Решётка $\langle L, \sqcup, \sqcap \rangle$ модулярна, если и только если для любых её элементов x, y и z имеет место соотношение

$$x \sqcup ((x \sqcup y) \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$$

или эквивалентное двойственное ему

$$x \sqcap ((x \sqcap y) \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z).$$

Доказательство. Если решётка L модулярна, то первое тождество следует из отношения $x \sqsubseteq x \sqcup y$, если в модулярном законе заменить y на $x \sqcup y$. Обратно, при $x \sqsubseteq y$, т.е. при $x \sqcup y = y$, первое тождество превращается в $x \sqcup (y \sqcap z) = y \sqcap (x \sqcup z)$, что является заключением модулярного закона.

Справедливость второго тождества следует из принципа двойственности. \square

Можно показать, что решётка модулярна, если для любых двух её элементов x и y справедливо соотношение

$$x \sqcap y \leq x, y \Leftrightarrow x, y \leq x \sqcup y.$$

Пусть x, y и z — элементы решётки $\langle L, \sqcup, \sqcap \rangle$. Правило

$$Abbr(x, y) : \begin{cases} x \sqcup z = y \sqcup z \\ x \sqcap z = y \sqcap z \end{cases} \Rightarrow x = y. \quad (4.3)$$

называется *правилом сокращения для x и y* . В общем случае данное правило, конечно, несправедливо: например, для пятиугольника N_5 в обозначениях рис. 4.4 имеем $a \sqcup b = c \sqcup b = \iota$ и $a \sqcap b = c \sqcap b = o$, но $a \neq c$.

Теорема 4.13 (правило сокращения для модулярных решёток). *Решётка модулярна, если и только если при сравнимости её элементов x и y справедливо правило их сокращения.*

Доказательство.

(\Rightarrow) Пусть для некоторых элементов x, y, z модулярной решётки справедливы и равенства $x \sqcup z = y \sqcup z$, $x \sqcap z = y \sqcap z$, и следование $x \sqsubseteq y$. Тогда

$$x \stackrel{Abs}{=} x \sqcup (x \sqcap z) = x \sqcup (y \sqcap z) \stackrel{Mod}{=} y \sqcup (x \sqcap z) = y \sqcup (y \sqcap z) \stackrel{Abs}{=} y.$$

(\Leftarrow) Доказательство достаточности может быть найдено в [34]. \square

Также может быть показано, что гомоморфный образ и любая подрешётка модулярной решётки модулярны и прямое произведение модулярных решёток есть модулярная решётка.

4.4 Дистрибутивные решётки

Определение 4.7. Решётка $\langle L, \sqcup, \sqcap \rangle$ называется *дистрибутивной*, если в ней выполняются дистрибутивные законы

$$\begin{aligned} Dtr1 : & (x \sqcup y) \sqcap z = (x \sqcap z) \sqcup (y \sqcap z); \\ Dtr2 : & (x \sqcap y) \sqcup z = (x \sqcup z) \sqcap (y \sqcup z). \end{aligned}$$

Ясно, что смысл дистрибутивных законов состоит в выполнении следований, обратных утверждаемым в соответствующих неравенствах полудистрибутивности. Так же понятно, что для дистрибутивных решёток принцип двойственности остается справедливым. В п. 1.1 было показано, что законы поглощения обеспечивают эквивалентность дистрибутивных законов. Так что рассматриваемая система аксиом для дистрибутивных решёток избыточна, и достаточно было потребовать выполнения лишь одного из дистрибутивных законов (обычно в таком случае постулируют выполнение $Dtr1$).

Пример 4.7. 1. Все цепи — дистрибутивны решётки: истинность тождества

$$\min \{ \max \{ x, y \}, z \} = \max \{ \min \{ x, z \}, \min \{ y, z \} \}$$

для них проверяется непосредственно.

Все булевы алгебры и максиминная алгебра (см. п. 2 примера 2) суть дистрибутивные решётки.

2. Покажем дистрибутивность решётки $\langle \mathbb{N}, \vee, \wedge \rangle$, т.е. справедливость для любых натуральных чисел x, y и z соотношения

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z),$$

где $x \wedge y$ — наибольший общий делитель, а $x \vee y$ — наименьшее общее кратное x и y . Воспользуемся каноническим представлением натуральных чисел в виде произведений их простых сомножителей

$$x = \prod_{i=1}^s p_i^{\alpha_i}, \quad y = \prod_{i=1}^s p_i^{\beta_i}, \quad z = \prod_{i=1}^s p_i^{\gamma_i},$$

считая, что некоторые показатели могут быть нулевыми. Тогда

$$\begin{aligned} x \wedge (y \vee z) &= \prod_{i=1}^s p_i^{\min\{\alpha_i, \max\{\beta_i, \gamma_i\}\}}, \\ (x \wedge y) \vee (x \wedge z) &= \prod_{i=1}^s p_i^{\max\{\min\{\alpha_i, \beta_i\}, \min\{\alpha_i, \gamma_i\}\}}, \end{aligned}$$

и требуемое равенство

$$\min\{\alpha, \max\{\beta, \gamma\}\} = \max\{\min\{\alpha, \beta\}, \min\{\alpha, \gamma\}\}$$

представляет собой дистрибутивный закон для цепи \mathbb{N}_0 .

Впоследствии будет показано, что любая конечная дистрибутивная решётка вложена в $\langle \mathbb{N}, \vee, \wedge \rangle$.

3. Решётка всех подпространств векторного пространства, упомянутая выше в качестве примера модулярной решётки, не является дистрибутивной. Для $n > 3$ решётка Π_n не дистрибутивна.
4. Непустая совокупность подмножеств некоторого множества, содержащая вместе с двумя подмножествами их объединение и пересечение называется *решёткой* или *кольцом множеств* (ср. с определением поля множеств на с. 10). Всякая решётка множеств дистрибутивна, поскольку дистрибутивны теоретико-множественные операции объединения и пересечения.
5. Решётка $\text{Sub } C$ всех подгрупп циклической группы C дистрибутивна. Заметим, что, однако, $\text{Sub } C$ не является решёткой множеств, поскольку объединение её элементов-подгрупп не совпадает (в отличие от пересечения) с теоретико-множественным.

Можно показать, что решётка дистрибутивна, если и только если она может быть представлен, как подрешётка B_n для некоторого n . Пятиугольник N_5 недистрибутивен: действительно (см. рис. 4.4),

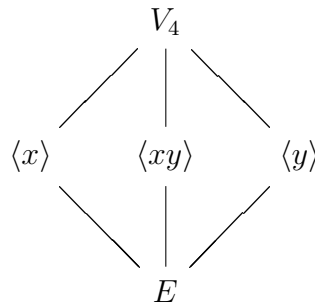
$$(a \sqcup b) \sqcap c = \iota \sqcap c = c \neq (a \sqcap c) \sqcup (b \sqcap c) = a \sqcup o = a.$$

Поэтому справедливо

Теорема 4.14. *Всякая дистрибутивная решётка модулярна.*

Это утверждение так же следует из того, что модулярный закон представляет собой ослабленную форму первого дистрибутивного закона: если $x \sqsubseteq y$, то $x \sqcup y = y$ и

$$x \sqcup (y \sqcap z) \stackrel{Dtr1}{=} (x \sqcup y) \sqcap (x \sqcup z) = y \sqcap (x \sqcup z).$$

Рис. 4.12: Решётка $\text{Sub } V_4$

Решётка $\text{NSub } G$ всех нормальных подгрупп группы G модулярна (см. пример 4.5.2), но в общем случае не дистрибутивна. Действительно, рассмотрим четверную группу Клейна $V_4 = \{e, x, y, xy\}$ с определяющими соотношениями $x^2 = y^2 = e$, $xy = yx$. Собственные её подгруппы суть $a = \{e, x\}$, $b = \{e, y\}$ и $c = \{e, xy\}$. Все они нормальны, поскольку V_4 абелева. Решётка $\text{Sub } V_4$ её подгрупп (см. рис. 4.12) изоморфна M_3 и модулярна, но не дистрибутивна, т.к. не дистрибутивен ромб M_3 :

$$(a \sqcup b) \sqcap c = e \sqcap c = c \neq (a \sqcap c) \sqcup (b \sqcap c) = e \sqcup e = e.$$

Недистрибутивность M_3 , оказывается ключевой: справедлива

Теорема 4.15. *Модулярная решётка является дистрибутивной, если и только если никакая её подрешётка не изоморфна ромбу M_3 .*

Доказательство. (\Leftarrow) Поскольку ромб M_3 не дистрибутивен, то никакая решётка, содержащая изоморфную ему подрешётку, не может быть дистрибутивной.

(\Rightarrow) Пусть решётка L модулярна и не содержит M_3 в качестве подрешётки. Для произвольных $x, y, z \in L$ рассмотрим следующие пять элементов

$$\begin{aligned} a &= (z \sqcap (x \sqcup y)) \sqcup (x \sqcap y); & b &= (y \sqcap (x \sqcup z)) \sqcup (x \sqcap z); \\ c &= (x \sqcap (y \sqcup z)) \sqcup (y \sqcap z); \\ u &= (x \sqcap y) \sqcup (y \sqcap z) \sqcup (z \sqcap x); & v &= (x \sqcup y) \sqcap (y \sqcup z) \sqcap (z \sqcup x). \end{aligned}$$

Покажем сначала, что

$$a \sqcup b = b \sqcup c = c \sqcup a = v \quad \text{и} \quad a \sqcap b = b \sqcap c = c \sqcap a = u.$$

Имеем

$$\begin{aligned} (z \sqcap (x \sqcup y)) \sqcup (y \sqcap (x \sqcup z)) &= (x \sqcup y) \sqcap ((y \sqcap (x \sqcup z)) \sqcup z) = \\ &= (x \sqcup y) \sqcap ((x \sqcup z) \sqcap (y \sqcup z)) = v. \end{aligned}$$

Вывод сделан с учётом модулярного закона, а также следований $y \sqcap (x \sqcup z) \sqsubseteq x \sqcup y$ и $z \sqsubseteq x \sqcup z$ для первого и второго равенств соответственно. Отсюда получаем, что $a \sqcup b = v$, и в силу симметрии, что $b \sqcup c = c \sqcup a = v$.

Учитывая модулярный закон и очевидное соотношение $x \sqcap y \sqsubseteq x \sqcup y$ получаем другое, двойственное к исходному, выражение для a :

$$a = (z \sqcup (x \sqcap y)) \sqcap (x \sqcup y).$$

Аналогично

$$b = (y \sqcup (z \sqcap x)) \sqcap (z \sqcup x), \quad c = (x \sqcup (y \sqcap z)) \sqcap (y \sqcup z).$$

Используя теперь принцип двойственности для модулярных решёток и учитывая, что u двойственно v , получим $a \sqcap b = b \sqcap c = c \sqcap a = u$.

Таким образом, если все элементы a , b и c попарно различны, то подрешётка $\{u, a, b, c, v\}$ в L изоморфна ромбу M_3 ($u \sqsubseteq a, b, c \sqsubseteq v$). Это невозможно, и, значит, $u = a = b = c = v$, но тогда

$$(x \sqcup y) \sqcap z \sqsubseteq a = u \sqsubseteq (x \sqcap z) \sqcup (y \sqcap z),$$

и, следовательно, в L выполняется дистрибутивный закон. \square

Следствие (Критерий дистрибутивности решётки). *Решётка дистрибутивна, если и только если никакая её подрешётка не изоморфна ни пятиугольнику N_5 , ни ромбу M_3 .*

В дистрибутивных решётках и только в них справедливо следующее правило.

Теорема 4.16 (правило сокращения для дистрибутивных решёток). *Решётка дистрибутивна, если и только если в ней справедливо правило сокращения Abbr (4.3).*

Доказательство необходимости совпадает с соответствующим в теореме 4.13, поскольку дистрибутивная решётка модулярна, а доказательство достаточности может быть найдено в [34]. \square

Отметим, что любая дистрибутивная решётка $\langle L, \sqcup, \sqcap \rangle$ является коммутативным полукольцом: обе операции ассоциативны и коммутативны, а пересечение дистрибутивно относительно объединения.

В дальнейшем нам понадобятся некоторые леммы, которые, впрочем, представляют и самостоятельный интерес.

Лемма 4.2. *Порядковые идеалы ч.у. множества P образуют подрешётку решётки $\langle \mathcal{P}(P), \cup, \cap \rangle$.*

Доказательство. Достаточно показать, что совокупность $J(P)$ устойчива относительно теоретико-множественных операций объединения и пересечения.

Пусть $I_1, I_2 \in J(P)$. Тогда для всех элементов $a, x \in P$ имеем

$$x \sqsubseteq a \ \& \ a \in I_1 \cup I_2 \Rightarrow \begin{cases} x \sqsubseteq a \ \& \ a \in I_1 \\ x \sqsubseteq a \ \& \ a \in I_2 \end{cases} \Rightarrow \begin{cases} x \in I_1 \\ x \in I_2 \end{cases} \Rightarrow x \in I_1 \cup I_2$$

и аналогично для $I_1 \cap I_2$. Следовательно, и $I_1 \cup I_2$, и $I_1 \cap I_2$ являются порядковыми идеалами. \square

Следствие. *Решётка $\langle J(P), \cup, \cap \rangle$ дистрибутивна.*

Понятно, что $J(P)$ — пример кольца множеств. В соответствии с данной леммой, решётка $J(P)$, построенная в примере 3.10 (рис. 3.7), дистрибутивна. Там она строилась “снизу вверх”, считая что если имеются два порядковых идеала, то должно существовать и их объединение. Ниже будет описан алгоритм построения диаграммы $J(P)$ по диаграмме конечного ч.у. множества P . Заметим, что установлена [45] справедливость соотношения

$$J(L^P) \cong (J(L))^P$$

для произвольных решётки L и ч.у. множества P .

В конечных дистрибутивных решётках атомы не играют такой роли, как в булевых алгебрах. Например, в конечной цепи всего один атом. Здесь гораздо большее значение имеют неразложимые в объединение элементы.

Определение 4.8. Ненулевой элемент z решётки назовём *неразложимым* (в объединении), если из $z = x \sqcup y$ следует $z = x$ или $z = y$.

Очевидно, неразложимый элемент нельзя записать в виде объединения содержащихся в нём и отличных от него элементов.

Пример 4.8. 1. Атомы любой решётки неразложимы, и в атомной булевой алгебре нет других неразложимых элементов.

2. В решётке $\langle \mathbb{N}, | \rangle$ неразложимы в точности степени простых чисел.

3. В цепи ни один элемент не является разложимым.

Ранее мы строили ч.у. множество $J(P)$ для некоторого ч.у. множества P , рассматривая все порядковые идеалы последнего и их взаимные включения. Теперь можно указать более эффективный алгоритм построения диаграммы Хассе для решётки порядковых идеалов конечного ч.у. множества по данной его диаграмме Хассе. Подробно алгоритм описан в монографии [36], вкратце он изложен ниже.

Пусть множество M минимальных элементов конечного ч.у. множества P имеет мощность m .

1. Построим диаграмму конечной булевой алгебры, изоморфной $J(M)$.
2. Выберем некоторый минимальный элемент x множества $P \setminus M$ и присоединим к $J(M)$ неразложимый в объединении элемент, содержащий порядковый идеал $J(x) \setminus \{x\}$.
3. Добавим все необходимые объединения элементов, содержащих идеал $J(x) \setminus \{x\}$, чтобы они образовывали булеву алгебру.
4. Если существуют элементы, содержащие множество $J(x) \setminus \{x\}$ и покрывающие элементы которых не имеют объединений, то изобразим последние так, чтобы образовалась булева алгебра.

Продолжая таким образом до тех пор, пока каждое множество элементов, содержащее данный элемент не будет иметь объединения, получим диаграмму дистрибутивной решётки $J(M \cup \{x\})$.

5. Выберем некоторый минимальный элемент y множества $\{P \setminus M\} \setminus \{x\}$ и присоединим к $J(M \cup \{x\})$ неразложимый в объединении элемент, содержащий порядковый идеал $J(x) \setminus \{y\}$.
6. Повторяя шаги 3 и 4, получим диаграмму дистрибутивной решётки $J(M \cup \{x, y\})$.
7. Продолжаем аналогично, пока не получим диаграмму решётки $J(P)$.

Построим по приведённому алгоритму решётку порядковых идеалов ч.у. множества Z_5 изображённого на рис. 4.13. Полученная решётка изображена на рис. 4.14.

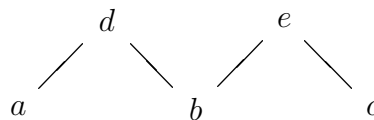
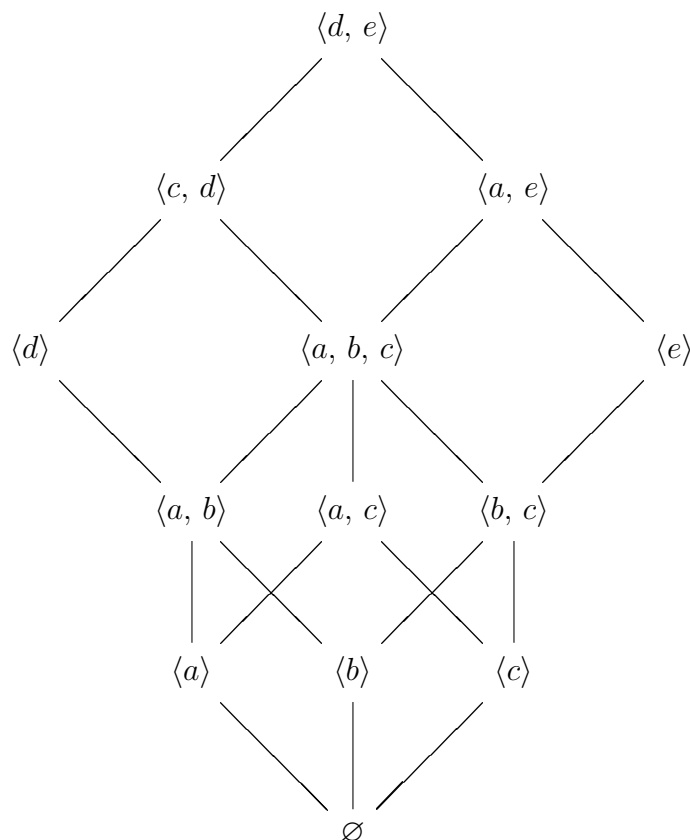


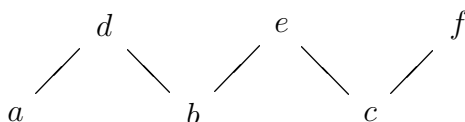
Рис. 4.13: Ч.у. множество Z_5

Продemonстрируем на построенной решётке вычисление некоторых характеристических чисел исходного ч.у. множества Z_5 . Известно, что зигзаг Z_n имеет F_{n+2} ($(n+2)$ -е число Фибоначчи) порядковых идеалов. Например, в нашем случае $|J(Z_5)| = F_7 = 13$.

Рис. 4.14: Решётка $J(Z_5)$

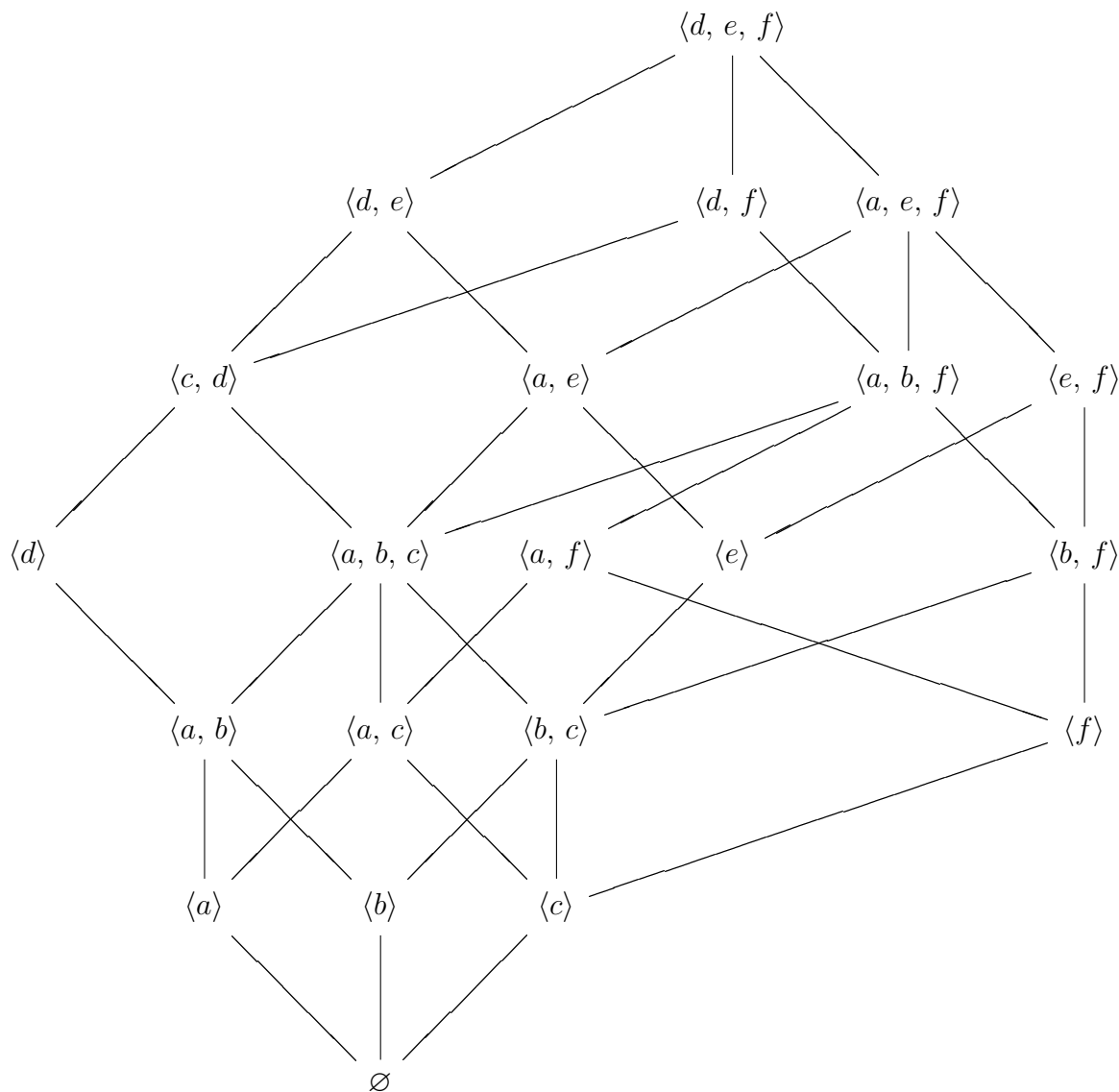
Кроме того доказано, что мощность $e(P)$ множества всех линейризаций конечного ч.у. множества P есть число максимальных восходящих (от наименьшего элемента \emptyset к наибольшему P^\vee) цепей в решётке $J(P)$. Для нашего примера можно подсчитать, что таких путей 16: проходящих через $\langle a, b, c \rangle$ — $6 \cdot 2 = 12$ (число максимальных восходящих путей в n -мерном кубе равно $n!$), а через $\langle d \rangle$ и $\langle e \rangle$ — по 2. Также, из формулы (3.5) следует, что $e(Z_5)$ есть $5!$ умноженное на 5-е число тангенса — коэффициент при x^5 в разложении $\operatorname{tg} x$ в ряд Маклорена. Поскольку данный коэффициент есть $\frac{2}{15}$, получим $e(Z_5) = 5! \cdot \frac{2}{15} = 16$.

Для примера, построим решётку порядковых идеалов ч.у. множества Z_6 изображённого на рис. 4.13. Полученная решётка изображена на рис. 4.16.

Рис. 4.15: Ч.у. множество Z_6

Теорема 4.17 ([14]).

$$\sum_{n \geq 1} \frac{e(s_n)}{n!} x^n = \frac{x}{\cos^2 x}.$$

Рис. 4.16: Решётка $J(Z_6)$

Доказательство. Для подсчёта числа максимальных цепей в $J(s_n)$ применим т.н. метод выделенного элемента, за который возьмём некоторый минимальный элемент Z_n . Задача сведётся к подсчёту числа b_n максимальных цепей в $J(Z_n)$, проходящих через данный минимальный элемент, т.к. $e(s_n) = n \cdot e_n$. Но b_n есть число максимальных цепей в $J(Z_{2n-1})$. Значение b_n известно — это n -е число тангенса $\frac{2^{2n}(2^{2n}-1)}{2^n} B_n$ (см. (3.5)). Здесь B_n — n -е число Бернулли в обозначениях [16]. Таким образом, имеем $e(s_n) = 2^{2n-1} \cdot (2^{2n} - 1) \cdot B_n$.

Утверждение теоремы следует из того, что $n \cdot e_n$ — коэффициент при x^{n-1} в разложении по степеням x функции $\operatorname{tg}'(x) = 1/\cos^2 x$. \square

Числа $e(s_n)$ и, для сравнения, числа секанса $e(Z_{2n})$ для первых значений n приведены в нижеследующей таблице.

n	2	3	4	5	6	7
$e(s_n)$	4	48	1088	39 680	2 122 752	156 577 855
$e(Z_{2n})$	5	61	1 385	50 521	2 702 765	199 360 981

На рис. 4.17 показана решётка порядковых идеалов для короны s_3 с рис. 3.23. По нему

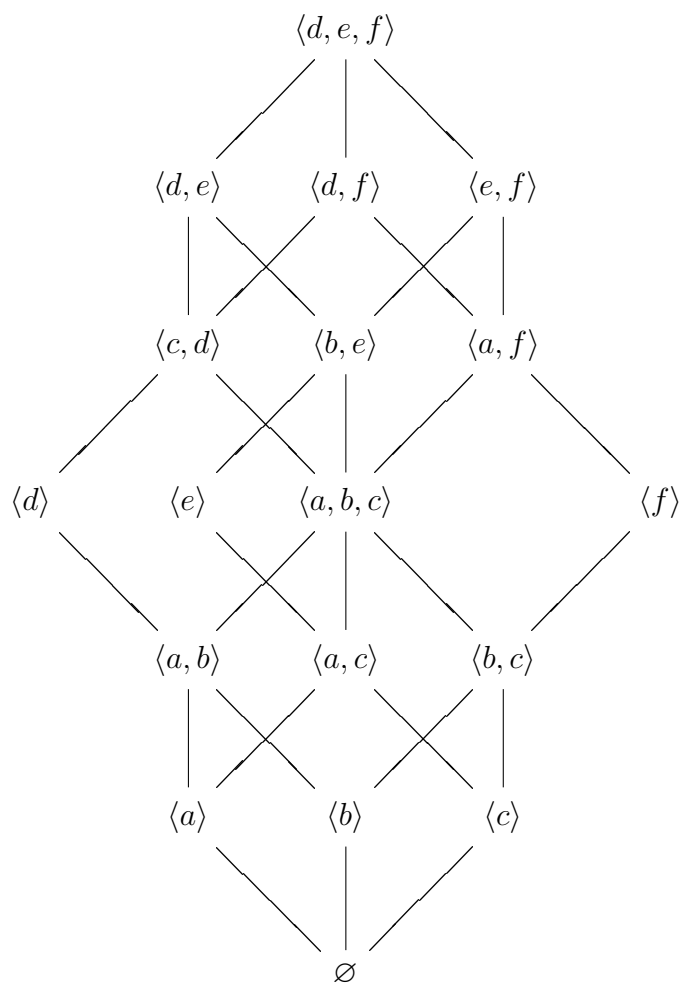


Рис. 4.17: Решётка $J(s_3)$

легко подсчитать, что число $e(s_3)$ максимальных путей в $J(s_3)$ равно 48 (через вершину $\langle a, b, c \rangle$ проходит $(3!)^2 = 36$ путей и через каждую из вершин $\langle d \rangle$, $\langle e \rangle$ и $\langle f \rangle$ — по $(2!)^2 = 4$), так же и по вышеприведённой таблице.

Лемма 4.3. *В конечной решётке каждый ненулевой элемент может быть представлен в виде объединения неразложимых элементов.*

Доказательство. Если элемент b неразложим, то $b = b \sqcup b$. Пусть $b = b_1 \sqcup b_2$ и $b_1 \neq b \neq b_2$. Если b_1 и b_2 неразложимы, то лемма доказана. В противном случае представляем b_1 и/или b_2 в виде объединения строго содержащихся в них элементов, и т.д. В силу конечности решётки указанный процесс закончится, и исходный элемент b будет представлен в виде объединения неразложимых элементов. \square

Множество неразложимых в объединение элементов (дистрибутивной) решётки L будем обозначать $\text{Irr } L$. Для элемента x решётки конечной L обозначим $\text{Irr}(a) = \{x \in \text{Irr } L \mid x \sqsubseteq a\}$ — множество неразложимых элементов L , содержащихся в x . Формально считаем, что $\text{Irr}(o) = \emptyset$.

Доказанная лемма утверждает, что в конечной решётке каждый ненулевой элемент x допускает (ср. с (1.8)) представление:

$$x = \bigsqcup_{a \in \text{Irr}(x)} a, \quad (4.4)$$

предполагая формально его справедливость и в случаях одноэлементности $\text{Irr}(x)$.

Ясно, что множество $\text{Irr} L$, наследуя порядок от решётки L , является ч.у. множеством.

Лемма 4.4. *Если P — ч.у. множество, то $\text{Irr} J(P) \cong P$.*

Доказательство. Пусть P — ч.у. множество и тогда $J(P)$ — дистрибутивная решётка его порядковых идеалов. Ясно, что порядковый идеал решётки неразложим, если и только если он является главным, вида x^∇ , и, таким образом, $\text{Irr} J(P) \cong J_0(P)$. Ранее (при доказательстве теоремы 3.7 о представлении ч.у. множеств) был установлен изоморфизм между ч.у. множеством и совокупностью его главных идеалов, поэтому $P \cong J_0(P) = \text{Irr} J(P)$. \square

Следствие. $J(P) \cong J(Q) \Leftrightarrow P \cong Q$.

Пример 4.9. 1. Для ч.у. множества P , заданного диаграммой на рис. 4.18.a множество порядковых идеалов $J(P)$ с выделенным множеством главных идеалов (элементы $x^\nabla \in J_0(P)$) представлено на рис. 4.18.b.

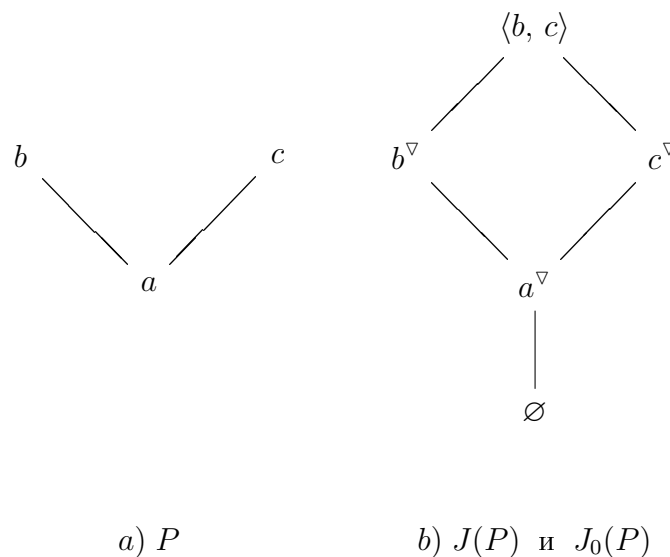


Рис. 4.18: Ч.у. множество P , дистрибутивная решётка $J(P)$ и ч.у. множество $J_0(P)$

2. См. рис. 3.7.

Нижеследующая теорема усиливает для дистрибутивных решёток теорему 4.8 и является аналогом теоремы Стоуна для булевых алгебр.

Теорема 4.18 (Биркгоф). *Всякая дистрибутивная решётка вложима в булеан подходящего множества с сохранением всех точных граней.*

Важным практическим следствием из данной теоремы является то, что при изучении дистрибутивных решёток можно пользоваться диаграммами Эйлера-Венна, интерпретируя элементы решёток подмножествами некоторого множества и отождествляя решёточные операции с соответствующими теоретико-множественными.

Доказательство данной теоремы можно найти, например, в [33]. Мы докажем эту теорему для конечных решёток, где она допускает важное усиление. Оно выражается в том, что утверждение следствия из леммы 4.2 «совокупность порядковых идеалов ч.у. множества есть дистрибутивная решётка» можно обратить, если решётка конечна. Следуя [36], назовём нижеприведённую теорему «фундаментальной теоремой для конечных дистрибутивных решёток (ФТКДР)».

Теорема 4.19 (ФТКДР, Биркгоф). *Всякая конечная дистрибутивная решётка изоморфна решётке порядковых идеалов ч.у. множества её неразложимых элементов.*

Доказательство. Пусть $\langle L, \sqcup, \sqcap \rangle$ — конечная дистрибутивная решётка с нулём o и $J(\text{Irr } L)$ — решётка порядковых идеалов ч.у. множества $\text{Irr } L$.

Рассмотрим отображение

$$\psi : L \rightarrow J(\text{Irr } L), \quad \psi(x) = \text{Irr}(x),$$

ставящее в соответствие каждому элементу x решётки множество её неразложимых в объединение элементов, содержащихся в x и покажем, что $L \stackrel{\psi}{\cong} J(\text{Irr } L)$. При этом, согласно теореме 4.4, достаточно установить изоморфизм между L и $J(\text{Irr } L)$, рассматриваемыми как ч.у. множества. Для доказательства будем пользоваться соотношением (4.4).

Во-первых, отображение ψ инъективно:

$$\psi(a) = \psi(b) \Leftrightarrow \text{Irr}(a) = \text{Irr}(b) \Rightarrow a = \bigsqcup_{z \in \text{Irr}(x)} z = \bigsqcup_{z \in \text{Irr}(y)} z = b.$$

Покажем, во-вторых, что оно сюръективно. Пусть $I = \{a_1, \dots, a_k\}$ — порядковый идеал ч.у. множества $\text{Irr } L$. Положим $a = \bigsqcup_{i=1}^k a_i$ и покажем, что $I = \text{Irr}(a)$. Действительно, с одной стороны, $x \sqsubseteq a$ для любого $x \in I$, откуда $I \in J(a)$. С другой, для $x \in \text{Irr}(a)$ имеем

$$x = x \sqcap a = x \sqcap \left(\bigsqcup_{i=1}^k a_i \right) = \bigsqcup_{i=1}^k (x \sqcap a_i).$$

Но x неразложим в L , и, следовательно, $x = x \sqcap a_i$ для подходящего i . Значит, $x \sqsubseteq a_i \in I$. Поскольку I — порядковый идеал, получаем, $x \in I$, откуда $\text{Irr}(a) \subseteq I$ и равенство $I = \text{Irr}(a)$ доказано.

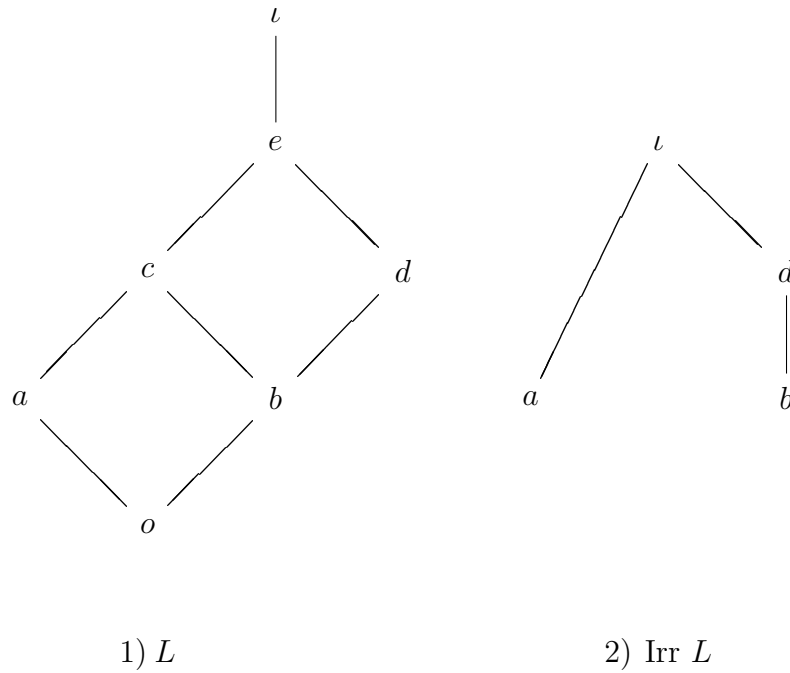
Кроме того, по свойствам взаимосвязанных операции объединения \sqcup и отношения порядка \sqsubseteq , имеем

$$x \sqsubseteq y \Leftrightarrow \text{Irr}(x) \subseteq \text{Irr}(y) \Leftrightarrow \psi(x) \subseteq \psi(y).$$

Это означает, что ψ — (порядковый) изоморфизм между L и $J(\text{Irr } L)$. \square

Следствие. *Если L_1 и L_2 — конечные дистрибутивные решётки, то $L_1 \cong L_2$, если только если $\text{Irr } L_1 \cong \text{Irr } L_2$.*

Отметим, что $J(\text{Irr } L) = \text{comp}(\text{Irr } L)$, т.е. решётка $J(\text{Irr } L)$ есть пополнение Макнила ч.у. множества $\text{Irr } L$ (см. с. 100).

Рис. 4.19: Дистрибутивная решётка L и ч.у. множество $\text{Irr } L$

Доказанная теорема играет большую роль в перечислительной комбинаторике, где конкретной задаче обычно неявно соответствует некоторое ч.у. множество².

Пример 4.10. 1. Рассмотрим диаграмму на рис. 4.18.b как диаграмму Хассе некоторой исходной конечной дистрибутивной решётки L . Тогда на рис. 4.18.a изображено ч.у. множество $\text{Irr } L$, и решётка всех порядковых идеалов которого $J(\text{Irr } L)$ совпадает изображённой на рис. 4.18.b.

2. На рис. 4.19 представлены диаграммы конечной дистрибутивной решётки L и ч.у. множества $\text{Irr } L$.

Диаграмма Хассе решётки порядковых идеалов $J(\text{Irr } L)$ повторяет диаграмму L с заменой $x \mapsto \psi(x)$, $x \in L$. При этом

$$\begin{aligned} \psi(o) &= \emptyset, & \psi(a) &= \langle a \rangle, & \psi(b) &= \langle b \rangle, & \psi(c) &= \langle a, b \rangle, \\ \psi(d) &= \langle d \rangle, & \psi(e) &= \langle a, d \rangle, & \psi(l) &= \langle l \rangle. \end{aligned}$$

Теорема Биркгофа позволяет представлять элементы любой дистрибутивной решётки подмножествами некоторого множества и пользоваться диаграммами Эйлера-Венна. Из неё также вытекает интересное

Следствие. *Всякая конечная дистрибутивная решётка вложима в упорядоченную делимостью решётку натуральных чисел.*

Доказательство. Из теоремы Биркгофа следует, что конечная дистрибутивная решётка L вкладывается в булеан $\mathcal{P}(A)$ некоторого конечного множества A . С другой стороны, пример 4.3.8 показывает, что $\mathcal{P}(A)$ вкладывается в $\langle \mathbb{N}^\circ, | \rangle$, а следовательно и в $\langle \mathbb{N}, | \rangle$. \square

Покажем, как конечная дистрибутивная решётка L может быть вложена в $\langle \mathbb{N}, \vee, \wedge \rangle$. Наименьшему элементу o решётки L сопоставляется число 1, а $n \geq 1$ её атомам — первые

²В упомянутой монографии [36] даже замечено, что «для комбинаторных целей было бы лучше всего определить конечную дистрибутивную решётку, как произвольное ч.у. множество вида $J(P)$, P конечно».

n простых чисел p_1, \dots, p_n . Пусть состоялось приписывание всем элементам множества $x^\vee \setminus \{x\}$ элемента x решётки L . Если элементу x непосредственно предшествует единственный элемент, которому сопоставлено число k , то сопоставляем x число kp , где p — первое из ещё не использованных простых чисел. Если элементу x непосредственно предшествуют несколько элементов, то сопоставляем x наименьшее общее кратное всех чисел, им соответствующих. Такое сопоставление для некоторых решёток приведено на рис. 4.20.

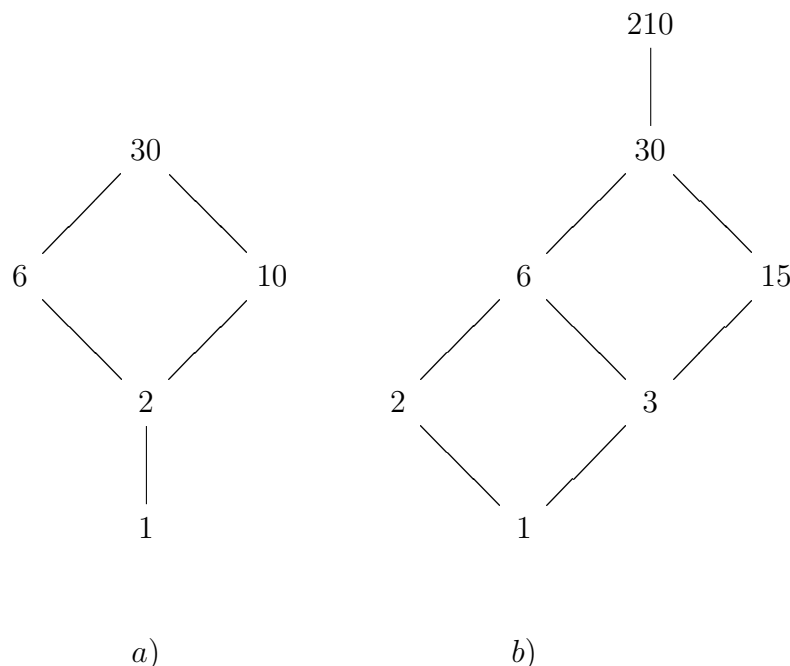


Рис. 4.20: Вложения конечных дистрибутивных решёток в решётку $\langle \mathbb{N}, | \rangle$

Приведём без доказательства ещё одну характеристику дистрибутивных решёток

Теорема 4.20. *Решётка L дистрибутивна, если и только если найдётся такое ч.у. множество P , что $L \cong \mathbf{2}^P$.*

Аналогично модулярным решёткам, может быть показано, что гомоморфный образ и любая подрешётка дистрибутивной решётки дистрибутивны и прямое произведение дистрибутивных решёток есть дистрибутивная решётка.

4.5 Факторрешётки. Решётки с дополнениями

Пусть L — решётка и на ней, как на множестве, имеется отношение эквивалентности \sim , сохраняющее объединения и пересечения, т.е.

$$\begin{cases} a \sim c \\ b \sim d \end{cases} \Rightarrow \begin{cases} (a \sqcup b) \sim (c \sqcup d) \\ (a \sqcap b) \sim (c \sqcap d) \end{cases} . \quad (4.5)$$

Такие эквивалентности называют *конгруэнциями*. Условия (4.5) позволяют рассматривать фактормножество L/\sim с операциями объединения и пересечения, применённые к его элементам (классам эквивалентности), т.е. *факторрешётку* L по конгруэнции \sim (символическое обозначение такое же, L/\sim).

Например, для гомоморфизма решёток $\varphi: L \rightarrow L'$ по (2.12) определяется ядерная эквивалентность $\text{Кер } \varphi$:

$$a(\text{Кер } \varphi)b \Leftrightarrow \varphi(a) = \varphi(b).$$

Далее имеем

$$\begin{cases} a(\text{Кер } \varphi)c \\ b(\text{Кер } \varphi)d \end{cases} \Leftrightarrow \begin{cases} \varphi(a \sqcup b) = \varphi(a) \sqcup \varphi(b) = \varphi(c) \sqcup \varphi(d) = \varphi(c \sqcup d), \\ \varphi(a \sqcap b) = \varphi(a) \sqcap \varphi(b) = \varphi(c) \sqcap \varphi(d) = \varphi(c \sqcap d). \end{cases}$$

Следовательно, $(a \sqcup b)(\text{Кер } \varphi)(c \sqcup d)$ и $(a \sqcap b)(\text{Кер } \varphi)(c \sqcap d)$, т.е. $\text{Кер } \varphi$ оказывается конгруэнцией. Эта конгруэнция называется *ядром гомоморфизма* φ .

Расстроим другой важный частный случай конгруэнций на решётках. Пусть I — идеал дистрибутивной решётки L . Рассмотрим бинарное отношение \sim_I на L , вводимое по правилу

$$a \sim_I b \Leftrightarrow \exists x (a \sqcup x = b \sqcup x). \quad (4.6)$$

Легко видеть, что это отношение есть эквивалентность. Действительно, его рефлексивность и симметричность очевидны. Покажем транзитивность. Пусть $a \sim_I b$ и $b \sim_I c$. Это означает существование $x, y \in I$ таких, что $a \sqcup x = b \sqcup x$ и $b \sqcup y = c \sqcup y$. Далее (объединяя левые и правые части первого равенства с y , а второго — с x), получим

$$\begin{cases} a \sqcup x = b \sqcup x \\ b \sqcup y = c \sqcup y \end{cases} \Rightarrow a \sqcup (x \sqcup y) = b \sqcup (x \sqcup y) = c \sqcup (x \sqcup y)$$

и $a \sim_I c$, поскольку $x \sqcup y \in I$.

Фактормножество по эквивалентности \sim_I обозначают L/I , соответствующие смежные классы — $[\cdot]_I$, причём, как легко установить, $[a]_I = a \sqcup I$ для элемента $a \in L$. Когда это не приводит к недоразумениям, индекс I у обозначения классов эквивалентности опускают.

Покажем теперь, что \sim_I — конгруэнция. Имеем

$$\begin{cases} a \sim c \\ b \sim d \end{cases} \Leftrightarrow \begin{cases} \exists x (a \sqcup x = c \sqcup x) \\ \exists y (b \sqcup y = d \sqcup y) \end{cases}. \quad (4.7)$$

Тогда, во-первых, для объединения получим

$$\exists x, y [(a \sqcup b) \sqcup (x \sqcup y) = (c \sqcup d) \sqcup (x \sqcup y)],$$

и, поскольку $x \sqcup y \in I$, то $(a \sqcup b) \sim_I (c \sqcup d)$. И, во-вторых, для пересечения —

$$\exists x, y [(a \sqcup x) \sqcap (b \sqcup y) = (c \sqcup x) \sqcap (d \sqcup y)].$$

Раскрывая по дистрибутивности равенство в данном соотношении, имеем

$$(a \sqcap b) \sqcup (a \sqcap y) \sqcup (x \sqcap b) \sqcup (x \sqcap y) = (c \sqcap d) \sqcup (c \sqcap y) \sqcup (x \sqcap d) \sqcup (x \sqcap y),$$

где все члены объединений в обеих частях равенства, кроме, быть может, $a \sqcap b$ и $c \sqcap d$, и, следовательно, и их объединения суть элементы идеала I . Осталось показать, что

$$(a \sqcap y) \sqcup (x \sqcap b) \sqcup (x \sqcap y) = (c \sqcap y) \sqcup (x \sqcap d) \sqcup (x \sqcap y).$$

Для этого берём пересечения с y первого и с x — второго равенства из правой части соотношения (4.7). Получим

$$\begin{cases} (a \sqcup x) \sqcap y = (c \sqcup x) \sqcap y \\ (b \sqcup y) \sqcap x = (d \sqcup y) \sqcap x \end{cases} \Leftrightarrow \begin{cases} (a \sqcap y) \sqcup (x \sqcap y) = (c \sqcap y) \sqcup (x \sqcap y) \\ (b \sqcap x) \sqcup (x \sqcap y) = (d \sqcap y) \sqcup (x \sqcap y) \end{cases},$$

и, производя объединение соответствующих левых и правых частей — требуемое равенство. Таким образом, для любого идеала I эквивалентность \sim_I , заданная по (4.6) является конгруэнцией.

Таким образом, L/I есть факторрешётка (с нулём). Гомоморфизм $\varphi: L \rightarrow L/I$ есть отображение $\varphi(x) = [x]_I$, имеющее своим ядром данный идеал I .

Пример 4.11. Рассмотрим решётку, представленную на рис. 4.21.1). Множество $I = \{o, a, b, c\}$ является, очевидно, её идеалом. При этом $e \sim_I d$, поскольку для $c \in I$ получим $e \sqcup c = d \sqcup c$, и, следовательно, элементы e и d находятся в одном классе эквивалентности по I .

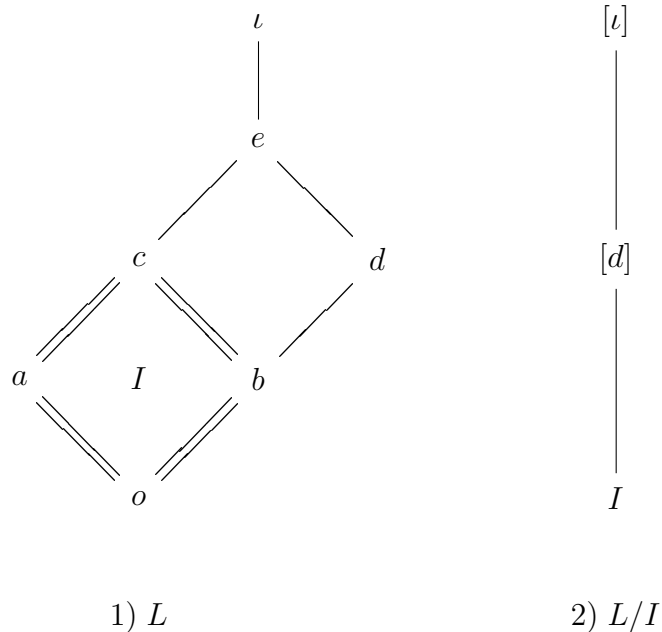


Рис. 4.21: Решётка L и факторрешётка L/I по идеалу $I = \{o, a, b, c\}$

Факторрешётка L/I изображена на рис. 4.21.2). Гомоморфизм $\varphi: L \rightarrow L/I$, есть отображение $\varphi(x) = [x]_I$ и идеал I есть нуль решётки L/I .

Решётка дистрибутивна, если и только если каждый её идеал ядерный. Заметим, что два разных гомоморфизма дистрибутивной решётки на одну и ту же решётку могут иметь совпадающие ядерные идеалы.

Определение 4.9. Если в решётке $\langle L, \sqcup, \sqcap \rangle$ с универсальными гранями для элемента x существует элемент y такой, что $x \sqcap y = o$ и $x \sqcup y = l$, то последний называется *дополнением элемента x* .

Решётка называется *решёткой с дополнениями*, если в ней каждый элемент имеет хотя бы одно дополнение. Если каждый элемент решётки обладает в точности одним дополнением, то её называют *решёткой с единственными дополнениями*.

Ясно, что если y — дополнение x , то и x — дополнение y , и что в любой ограниченной решётке o и l являются единственными дополнениями друг для друга.

Пример 4.12. 1. В решётке алгебры подмножеств множества A каждый элемент $X \subseteq A$ имеет единственное дополнение $\bar{X} = A \setminus \{X\}$. Это классический пример решётки с единственными дополнениями.

2. В решётке, представленной на рис. 4.20.а элемент 2 не имеет дополнения.

3. Пятиугольник N_5 — решётка с дополнениями. В ней (см. рис. 4.4) дополнениями a и c будет элемент b , а дополнениями b — элементы a и c .

Отметим, что критерий модулярности (теорема 4.11) для атомных решёток с дополнениями существенно упрощается, а именно, справедлива

Теорема 4.21 (Маклафлин). *Если атомная решётка с дополнениями не содержит в качестве подрешётки пятиугольник N_5 , наименьший и наибольший элементы которого совпадают с нулём и единицей решётки, то она модулярна.*

Доказательство имеется, например, в [33]. Из теоремы Маклафлина следует, что атомная решётка с единственными дополнениями модулярна. Более того, можно показать, что такая решётка дистрибутивна.

Следствием того, что в дистрибутивной решётке справедливо правило сокращения *Abbr* (см. теорему 4.16) является

Теорема 4.22. *Если ограниченная решётка дистрибутивна, то каждый её элемент имеет не более одного дополнения.*

Доказательство. Допустим, что элемент x дистрибутивной решётки имеет два дополнения — y_1 и y_2 . Тогда

$$\begin{cases} x \sqcup y_1 = x \sqcup y_2 = \iota \\ x \sqcap y_1 = x \sqcap y_2 = o \end{cases} \stackrel{\text{Abbr}}{\Rightarrow} y_1 = y_2.$$

□

Из теоремы Биркгофа 4.18 следует, что каждая дистрибутивная решётка вложима в дистрибутивную решётку с единственными дополнениями.

Вопрос о связи свойств дистрибутивности и наличия единственного дополнения у решёток является, как оказалось, достаточно глубоким и трудным. В начале XX века при формулировке систем аксиом для булевой алгебры естественной была попытка определить её как решётку с единственными дополнениями. Это стало бы возможным, если единственность дополнения у элементов решётки влекла бы её дистрибутивность. В связи с этим Э. Хантингтоном (см. с. 9) было высказано предположение о том, что *все решётки с единственными дополнениями дистрибутивны*. Вопрос о том, верна ли эта гипотеза и составлял знаменитую *проблему Хантингтона*.

К концу 30-х годов XX в. было исследовано значительное количество конкретных решёток с единственными дополнениями. Все они оказались дистрибутивными, в силу чего справедливость указанного предположения практически не вызвала сомнений у математиков. Поэтому большой неожиданностью было появление в 1945 г. работы американского математика Р. Дилуорса в которой была доказана

Теорема 4.23. *Всякая решётка может быть вложена в подходящую решётку с единственными дополнениями.*

В частности, можно взять пятиугольник N_5 , и тогда теорема Дилуорса даст немодулярную и, тем более, недистрибутивную решётку с единственными дополнениями. Таким образом, было доказано³, что существуют недистрибутивные решётки с единственными дополнениями. Отметим однако, что данный объект в доказательстве теоремы Дилуорса появляется лишь в результате некоторого предельного перехода, и до сих пор нет ни одного явного примера недистрибутивной решётки с единственными дополнениями. В классе полных решёток проблема Хантингтона до сих пор не имеет разрешения⁴.

³*Dilworth R.P.* Lattices with unique complements. — Trans. Amer. Math. Soc., 1945, **57**, p. 123-154. Современное доказательство данной теоремы имеется в [33].

⁴Данная проблематика подробно рассмотрена в [33].

Определение 4.10. Если $[a, b]$ — интервал решётки L , $x \in [a, b]$ и элемент y решётки L таков, что $x \sqcap y = a$ и $x \sqcup y = b$. То y называется *относительным дополнением* элемента x в интервале $[a, b]$.

Если в некоторой решётке все интервалы суть решётки с дополнениями, то она называется *решёткой с относительными дополнениями*.

Легко видеть, что если y — относительное дополнение элемента x в интервале $[a, b]$, то $y \in [a, b]$, и x , в свою очередь, также будет относительным дополнением элемента y в интервале $[a, b]$.

Пример 4.13. Решётка, изображенная ниже (мы повторяем рис. 4.9) не является решёткой с дополнениями, т.к., например, элемент b не имеет дополнения. В тоже время это решётка с относительными дополнениями: дополнениями элемента b в интервале $[e, \iota]$ являются элементы c и d , элементы a и e служат друг для друга единственными дополнениями в интервале $[o, b]$; в том же интервале дополнение b есть o .

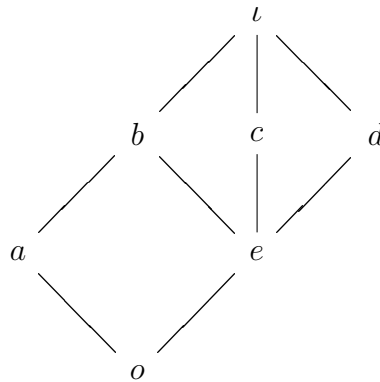


Рис. 4.22: Решётка с относительными дополнениями

Теорема 4.24 (Дилуорс). Любые две конгруэнции на решётке с относительными дополнениями перестановочны.

Доказательство. Пусть α и β — конгруэнции на на решётке L , $a, b, x \in L$, $a \alpha x$ и $x \beta b$.

Предварительно покажем, что если $a \sqsubseteq x \sqsubseteq b$, то для некоторого $y \in [a, b]$ справедливо $a \beta y$ и $y \alpha b$. Действительно, пусть y — дополнение элемента x в интервале $[a, b]$. Тогда

$$y = (b \sqcap y) \beta (x \sqcap y) = a \quad \text{и} \quad y = (a \sqcup y) \alpha (x \sqcup y) = b.$$

Теперь, отказавшись от ограничений $a \sqsubseteq x \sqsubseteq b$ и $y \in [a, b]$, получим

$$a = (a \sqcup a) \alpha (a \sqcup x) = (a \sqcup x \sqcup x) \beta (a \sqcup b \sqcup x) \alpha (x \sqcup b \sqcup x) = (b \sqcup x) \beta (b \sqcup b) = b$$

(для краткости, здесь и далее мы пишем $x\alpha y\beta z$ вместо $x\alpha y \& y\beta z$). Применяя полученное соотношение, будем иметь

$$a \beta u \alpha (a \sqcup b \sqcup x) \quad \text{и} \quad (a \sqcup b \sqcup x) \beta v \alpha b,$$

где $a \sqsubseteq u \sqsubseteq a \sqcup b \sqcup x$ и $b \sqsubseteq v \sqsubseteq a \sqcup b \sqcup x$. Отсюда

$$u = (u \sqcap a \sqcup b \sqcup x) \beta (u \sqcap v) \alpha (a \sqcup b \sqcup x) \sqcap v = v$$

и, следовательно, $a \beta (u \sqcap v)$ и $(u \sqcap v) \alpha b$. □

Теорема 4.25. *Модулярная решётка с дополнениями является решёткой с относительными дополнениями.*

Доказательство. Пусть $\langle L, \sqcup, \sqcap, ', o, \iota \rangle$ — модулярная решётка с дополнениями и a, b, x и y — такие её элементы, что $a \sqsubseteq x \sqsubseteq b$, $x \sqcup y = \iota$ и $x \sqcap y = o$, т.е. y есть (какое-то) дополнение x . С учётом модулярного закона получаем

$$\begin{aligned} x \sqcup (a \sqcup (y \sqcap b)) &= x \sqcup ((b \sqcap (a \sqcup y))) = b \sqcap (x \sqcup a \sqcup y) = b \sqcap \iota = b & \text{и} \\ x \sqcap (a \sqcup (y \sqcap b)) &= a \sqcup (x \sqcap y \sqcap b) = a \sqcup o = a. \end{aligned}$$

Поэтому $a \sqcup (y \sqcap b)$ есть относительное дополнение x в интервале $[a, b]$. \square

Приведём ещё одно важное свойство решёток.

Теорема 4.26. *Если $\langle L, \sqcup, \sqcap \rangle$ — решётка, а P — ч.у. множество, то L^P — решётка. При этом если L модулярна или дистрибутивна, то соответственно модулярной или дистрибутивной будет L^P .*

Доказательство. Пусть $f(x)$ и $g(x)$ — два изотонных отображение из P в L . Для любого $x \in P$ положим $h(x) = f(x) \sqcup g(x) \in P$. Тогда $h(x)$ — также изотонное отображение из P в L , являющееся при этом точной верхней гранью для $f(x)$ и $g(x)$ в L^P . Двойственно, изотонное отображение $h^*(x) = f(x) \sqcap g(x) \in P$ является точной нижней гранью для $f(x)$ и $g(x)$.

Этим доказано первое утверждение. Доказательство второго утверждения сводится к проверке выполнимости соответствующих тождеств для каждого $x \in P$. \square

Глава 5

Булевы алгебры (продолжение)

Продолжим изучение необыкновенной алгебры, которую мы назвали алгеброй Буля.

И.М. Яглом. Необыкновенная алгебра.

5.1 Булевы алгебры как решётки. Булевы гомоморфизмы и подалгебры

Определение 5.1. Дистрибутивная решётка с дополнениями называется *булевой алгеброй*.

Нетрудно установить, что оба определения булевой алгебры — данное только что и 1.1 — эквивалентны. Действительно, согласно первому определению, в булевой алгебре выполняются законы дистрибутивной решётки с дополнениями, а в последней дополнения (по теореме 4.22) единственны и справедливы аксиомы *Dtr* и *Abs* вместе с *Сmp'* и *Isl'*.

Теорема 5.1. Для любых элементов x и y булевой алгебры (с нулевым и единичным элементами o и ι соответственно) справедливо

- 1) $x \sqsubseteq y \Leftrightarrow x \sqcap y' = o \Leftrightarrow x' \sqcup y = \iota \Leftrightarrow x \sqcap y = x \Leftrightarrow x \sqcup y = y$;
- 2) $x \sqsubseteq y \Leftrightarrow x' \sqsupseteq y'$ — закон антиизотонности дополнения.

Доказательство.

1. См. определение отношения \sqsubseteq в решётках и лемму 1.1.
2. $x \sqsubseteq y \Leftrightarrow x \sqcap y = x \Leftrightarrow (x \sqcap y)' = x' \Leftrightarrow x' \sqcup y' = x' \Leftrightarrow y' \sqsubseteq x' \Leftrightarrow x' \sqsupseteq y'$.

□

Следующую простую теорему приведём без доказательства.

Теорема 5.2. Пусть $\langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра и A — произвольное непустое множество. Тогда множество B^A всех отображений из A в B также будет булевой алгеброй относительно «точечных» операций $\dot{\sqcup}$, $\dot{\sqcap}$ и $\dot{\ '}$, определяемых как

$$(f \dot{\sqcup} g)(x) = f(x) \sqcup g(x), \quad (f \dot{\sqcap} g)(x) = f(x) \sqcap g(x), \quad (f \dot{\ '})(x) = (f(x))'$$

для любых $f, g \in B^A$. Нулём и единицей B^A будут постоянные отображения $f_0(x) \equiv o$ и $f_1(x) \equiv \iota$ соответственно (везде x — произвольный элемент A).

Взяв в качестве A n -ю декартову степень B^n булевой алгебры B , получим булеву алгебру B^{B^n} всех функций из B^n в B , играющую важную роль в теории булевых многочленов. В частности, при $B = \mathbf{2}$ получаем булеву алгебру $\mathbf{2}^{2^n}$ всех булевых функций от n переменных.

До сих пор мы рассматривали только атомные булевы алгебры. Приведём пример булевой алгебры, не имеющих атомов. Рассмотрим совокупность всех конечных объединений всевозможных полуинтервалов вида $(x, y]$, содержащихся в промежутке $(0, 1]$:

$0 < x \leq y \leq 1$. Эта совокупность, очевидно, устойчива относительно теоретико-множественных операций объединения, пересечения и дополнения до $(0, 1]$, т.е. представляет собой булеву алгебру. Единицей в ней будет весь интервал $(0, 1]$, а нулём — пустое множество, представляемое в виде $(x, x]$. Легко видеть, что эта алгебра не имеет атомов: любой интервал $(x, y]$ рассматриваемого вида содержит в себе ненулевой подынтервал такого же вида.

Приведём без доказательства следующее утверждение: всякая полная не атомная булева алгебра будет представима в виде прямого произведения полной атомной и безатомной булевых алгебр, которые называют *дискретной* и *непрерывной компонентами* соответственно.

В п. 1.3 было введено понятие изоморфизма булевых алгебр. Дадим теперь определение булева гомоморфизма.

Определение 5.2. Булевым гомоморфизмом называют решёточный гомоморфизм φ между булевыми алгебрами, обеспечивающий равенство $\varphi(x') = \varphi(x)'$.

Инъективные булевы гомоморфизмы называют *булевыми мономорфизмами*.

Таким образом, булев гомоморфизм — это отображение одной булевой алгебры в другую, согласованное со всеми пятью булевыми операциями. Ясно, что, в частности, при любом булевом гомоморфизме φ обязательно имеет место $\varphi(o) = o$, $\varphi(\iota) = \iota$. Из определения видно, что булев гомоморфизм будет булевым изоморфизмом при биективности соответствующего отображения.

Пример 5.1. Пусть B — атомная булева алгебра и a — её атом. Тогда отображение $j_a : B \rightarrow \mathbf{2}$ такое, что

$$j_a(x) = \begin{cases} \iota, & \text{если } x \text{ содержит } a, \\ o, & \text{иначе,} \end{cases}$$

есть гомоморфизм. Такие гомоморфизмы булевой алгебры называют *двузначными* или *характерами*.

Понятно, что произвольный решёточный гомоморфизм одной булевой алгебры в другую может и не быть булевым гомоморфизмом. Например, если $A \subset B$, то естественное вложение $\mathcal{P}(A)$ в $\mathcal{P}(B)$ является решёточным мономорфизмом, но не булевым гомоморфизмом (и подавно, не булевым мономорфизмом), т.к. для произвольного подмножества A его дополнения в A и B различны.

Прообраз нуля $\varphi^\#(o)$ булева гомоморфизма φ называют его *ядром*. Ясно, что $\varphi^\#(o)$ есть смежный класс (ядро, см. определение на с. 36) $\text{Core}(o)$ ядерной эквивалентности $\text{Ker } \varphi$: для булева гомоморфизма φ имеем $x \in \text{Core}(o) \Leftrightarrow \varphi(x) = o$.

Определение 5.3. Булева алгебра B' называется *подалгеброй булевой алгебры B* (символически $B' \leq B$), если $B' \subseteq B$ и на B' устойчивы сужения всех операций B .

Понятно, что булева алгебра и её подалгебра имеют общие нули и единицы, поскольку они суть рассматриваться как некоторые нульместные операции на основном множестве.

Пример 5.2. 1. Булева алгебра P_2^n логических функций от n переменных является подалгеброй алгебры P_2 всех логических функций (см. п. 3 примера 1.5).

2. Пусть $A \subset B$. Тогда $\mathcal{P}(A) \not\leq \mathcal{P}(B)$, поскольку эти булевы алгебры имеют, например, разные единичные элементы (что повлечёт и несовпадение дополнений в $\mathcal{P}(A)$ и в $\mathcal{P}(B)$).

Непосредственно из определений и ранее доказанных фактов следует, что если $\varphi : B_1 \rightarrow B_2$ — булев гомоморфизм, то $\varphi(B_1) \leq B_2$.

5.2 Булевы кольца и структуры

Напомним, что (*алгебраическим*) *кольцом* называется АС $\langle R, +, \cdot, 0 \rangle$, где R — множество, содержащее элемент нуль (0), на котором определены две бинарные операции сложение ($+$) и умножение (\cdot) такие, что для любых $x, y, z \in R$ справедливы соотношения

$$(x + y) + z = x + (y + z), \quad x + y = y + x, \quad x + 0 = x \\ \exists(-x)(x + (-x) = 0),$$

(указанное означает, что редукт $\langle R, +, 0 \rangle$ кольца есть абелева группа по сложению),

$$(x + y) \cdot z = x \cdot z + y \cdot z, \quad x \cdot (y + z) = x \cdot y + x \cdot z$$

(дистрибутивность умножения по отношению к сложению).

Нуль кольца — единственный элемент, обладающий свойством $x + 0 = x$. Элемент $(-x)$ называют *обратным к x* ; он единственен. Заметим, что иногда при определении кольца исключают условие существования обратного элемента, но добавляют наличие унарной операции $(-)$, обладающей свойством $x + (-x) = 0$. Тогда все свойства задаются тождествами и кольцо оказывается многообразием (см. п. 6.1).

Если кольцевая операция умножения обладает свойством ассоциативности

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

и/или коммутативности

$$x \cdot y = x \cdot y,$$

то и кольцо называют соответствующе. Если кольцо содержит единицу (1) — элемент, для которого

$$x \cdot 1 = 1 \cdot x = x,$$

то говорят о *кольце с единицей*, его записывают как $\langle R, +, \cdot, 0, 1 \rangle$. Единица 1 — уникальный элемент с указанным свойством¹. В выкладках знак умножения обычно пускают и считают его приоритет выше приоритета сложения.

Определение 5.4. Ассоциативное кольцо, обладающие свойством $x^2 = x$ для любого своего элемента называется *булевым кольцом*.

Теорема 5.3. Булево кольцо $\langle R, +, \cdot, 0 \rangle$ коммутативно и $x + x = 0$ для всех $x \in R$.

Доказательство. Докажем сначала второе утверждение:

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = (x + x) + (x + x) \Rightarrow x + x = 0.$$

Отсюда

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y \Rightarrow xy + yx = 0$$

¹Доказательство приведённых свойств уникальности:

- если 0_1 и 0_2 — два элемента со свойствами нуля, то $0_1 = 0_1 + 0_2 = 0_2$;
- если y_1 и y_2 — обратные к x элементы, то

$$y_1 = y_1 + 0 = y_1 + (x + y_2) = (y_1 + x) + y_2 = 0 + y_2 = y_2;$$

- если 1_1 и 1_2 — два элемента со свойствами единицы, то $1_1 = 1_1 \cdot 1_2 = 1_2$.

и далее получаем

$$xy = xy + 0 = xy + (xy + yx) = (xy + xy) + yx = 0 + yx = yx.$$

□

Теорема 5.4. Пусть $\mathfrak{B} = \langle B, \sqcup, \sqcap, ', o, \iota \rangle$ — булева алгебра. Для любых $x, y \in B$ положим

$$x + y = (x \sqcap y') \sqcup (x' \sqcap y), \quad x \cdot y = x \sqcap y.$$

Тогда АС $\mathfrak{B}^* = \langle B, +, \cdot, o, \iota \rangle$ есть булево кольцо с единицей ι .

Доказательство. Коммутативность введённых операций сложения (+) и умножения (\cdot), ассоциативность умножения, справедливость равенства $x^2 = x$ и наличие единицы ι с её свойством $x \cdot \iota = x$ для всех x — очевидны.

Условия теоремы позволяют не различать операции умножения и пересечения. С учётом этого — $x + y = xy' \sqcup x'y$. Далее, используя законы булевой алгебры, получим

$$\begin{aligned} (x + y) + z &= (xy' \sqcup x'y)z' \sqcup (xy' \sqcup x'y)'z = xy'z' \sqcup x'yz' \sqcup (x' \sqcup y)(x \sqcup y')z = \\ &= xy'z' \sqcup x'yz' \sqcup x'y'z \sqcup xyz, \\ x + (y + z) &= x(yz' \sqcup y'z)' \sqcup x'(yz' \sqcup y'z) = x(y' \sqcup z)(y \sqcup z') \sqcup x'yz' \sqcup x''y = \\ &= xy'z' \sqcup xyz \sqcup x'yz' \sqcup x'y'z. \end{aligned}$$

Таким образом, $(x + y) + z = (x + y) + z$, и ассоциативность операции + показана. Затем

$$x + o = xo' \sqcup x'o = x\iota = x,$$

т.е. \mathfrak{B}^* оказывается абелевой группой по сложению.

И, наконец, выкладки

$$\begin{aligned} (x + y)z &= (xy' \sqcup x'y)z = xy'z \sqcup x'yz. \\ xz + yz &= xz(yz')' \sqcup (xz)'(yz) = xz(y' \sqcup z') \sqcup (x' \sqcup z')yz = xy'z \sqcup x'yz \end{aligned}$$

доказывают дистрибутивный закон умножения относительно сложения. □

Основным примером булева кольца и является как раз кольцо $\langle \mathcal{P}(A), \oplus, \cap, \emptyset, A \rangle$, получаемое указанным способом из тотальной алгебры множеств.

Теорема 5.5. Пусть $\mathfrak{K} = \langle R, +, \cdot, 0, 1 \rangle$ — булево кольцо с единицей. Для любых $x, y \in R$ положим

$$x \sqcup y = x + y + x \cdot y, \quad x \sqcap y = x \cdot y, \quad x' = x + 1.$$

Тогда АС $\mathfrak{K}^* = \langle R, \sqcup, \sqcap, ', 0, 1 \rangle$ — булева алгебра.

Доказательство. Ассоциативность введённых операций \sqcup, \sqcap и закон $Id \sqcup$ (с учётом $x + x = 0$ по теореме 5.3) проверяются непосредственно, а $Id \sqcap$ наследуется из \mathfrak{K} . Коммутативность булева кольца, установленная теоремой 5.4, обеспечивает коммутативность \sqcup и \sqcap . Далее в выкладках без пояснений используются свойства булева кольца.

Установим справедливость законов поглощения:

$$\begin{aligned} (x \sqcup y) \sqcap x &= (x + y + xy)x = x + xy + xy = x. \\ x \sqcup (x \sqcap y) &= x \sqcup (xy) = x + xy + xy = x. \end{aligned}$$

Таким образом, \mathfrak{B}^* — решётка.

Непосредственно проверяется выполнение пар законов $\sqcup 0$, $\sqcap \iota$ и $\sqcup \iota$, $\sqcap 0$, описывающих, соответственно, нейтральные и поглощающие свойства элементов 0 и 1 по отношению к \sqcup и \sqcap . В силу этого 0 и 1 суть нуль и единица решётки \mathfrak{B}^* .

Из равенств

$$\begin{aligned} x \sqcap x' &= x(1+x) = x+x = 0 && \text{и} \\ x \sqcup x' &= x \sqcup (1+x) = x+1+x+x(1+x) = 1+x+x = 1 \end{aligned}$$

вытекает, что \mathfrak{B}^* — решётка с дополнениями.

Равенства

$$(x \sqcup y) \sqcap z = (x+y+xy)z = xz+yz+xyz = (x \sqcap z) \sqcup (x \sqcap z)$$

доказывают справедливость в \mathfrak{B}^* первого дистрибутивного закона, а второй доказывается двойственно. \square

Таким образом, любое булево кольцо с единицей может быть задано с помощью булевой алгебры и наоборот. Легко проверяется, что справедливо

Следствие. $\mathfrak{B}^{**} = \mathfrak{B}$ и $\mathfrak{K}^{**} = \mathfrak{K}$.

Тем самым устанавливается т.н. *стоуновская двойственность между булевыми алгебрами и булевыми кольцами*.

Определение 5.5. АС $\langle B, \sqcup, \sqcap, ', \sqsubseteq, 0, \iota \rangle$ такая, что $\langle B, \sqcup, \sqcap, ', 0, \iota \rangle$ — булева алгебра, а отношение \sqsubseteq задаются по (4.1) называется *булевой структурой*.

Для многих приложений удобнее рассматривать не булевы алгебры, а сразу булевы структуры². Заметим, что при этом указанная булева алгебра есть *редукт* булевой структуры.

Покажем теперь, что справедливо следующее

Утверждение 5.1. *Элемент булевой алгебры является атомом, если и только если он непосредственно следует за нулём.*

Доказательство. С одной стороны, если элемент a непосредственно следует за нулём булевой алгебры, то любой её другой элемент x либо содержит элемент a , либо несравним с ним. В первом случае $a \sqcap x = a$, а во втором — $a \sqcap x = 0$, т.е. a удовлетворяет определению атома булевой алгебры B .

С другой стороны, если b — элемент B , покрывающий a , то $a \sqcap b = a \neq b$ и b не является атомом. \square

В булевой структуре легко доказываются лемма 1.4 из п. 1.4, утверждающая, что всякий ненулевой элемент конечной булевой алгебры может быть представлен в виде объединения содержащихся в нём атомов. Действительно, для конечной булевой алгебры как дистрибутивной решётки справедливо утверждение леммы 4.3 о представлении каждого ненулевого элемента в виде объединения неразложимых элементов, а таковыми в булевой алгебре, по доказанному утверждению, являются исключительно атомы.

Поскольку булева алгебра $\langle B, \sqcup, \sqcap, ', 0, \iota \rangle$ является модулярной решёткой с дополнениями, то для неё справедлива теорема 4.25, т.е. булева структура есть решётка с относительно дополнениями, и в ней единственное дополнение y элемента $x \in [a, b]$ относительно непустого интервала $[a, b]$ определяются по формуле

$$y = a \sqcup (b \sqcap x') = b \sqcap (a \sqcup x')$$

²В [40] для булевой структуры приведена (избыточная) система из 37 аксиом.

Если на интервале $[a, b]$, $a \sqsubset b$ по данной формуле определить операцию взятия дополнения \checkmark , то АС $\langle [a, b], \sqcup, \sqcap, \checkmark, a, b \rangle$ оказывается булевой алгеброй. Отметим, что полученная булева алгебра не будет (за исключением “собственного” случая $a = o, b = \iota$) являться подалгеброй исходной алгебры т.к. эти алгебры имеют, например, различные универсальные грани.

Отметим, что обычно рассматривают *булеву структуру множеств* $\langle \mathcal{P}(A), \cup, \cap, -, \subseteq, \emptyset, A \rangle$ дополняя тотальную алгебру множеств отношением включения \subseteq .

5.3 Идеалы, фильтры и конгруэнции в булевой алгебре

Определение 5.6. *Идеалом [фильтром] булевой алгебры называют её решёточные идеалы [фильтры]. Если I — идеал булевой алгебры B , то пишут $I \triangleleft B$.*

В силу данного определения, булевы идеалы и фильтры обладают всеми свойствами решёточных. Кроме того, идеала I и фильтра F булевой алгебры B добавляются следующие почти очевидные свойства

$$(x \in I) \& (x' \in I) \Rightarrow I = B \quad \text{и} \quad (x \in F) \& (x' \in F) \Rightarrow F = B.$$

Действительно, по определению идеала $\iota = x \sqcup x' \in I$, откуда $I = B$ и аналогично для фильтров.

На идеалы и фильтры булевой алгебры переносятся понятия, собственных, несобственных и главных идеалов и фильтров (см. п. 4.2). Так, идеалы и фильтры, описанные в предыдущем примере в п. 1 — главные, а в п. 2 — не главные. Поскольку булева алгебра есть решётка, то в конечной булевой алгебре все идеалы и фильтры — главные.

Пример 5.3. Рассмотрим тотальную алгебру множеств $\mathcal{P}(A)$ над множеством A .

1. Пусть $B \subseteq A$. Тогда совокупность всех подмножеств множества A , содержащихся в B есть идеал булевой алгебры $\mathcal{P}(A)$, а содержащих B — фильтр $\mathcal{P}(A)$. Это — главные идеалы и фильтры в бесконечной булевой алгебре.
2. Приведём пример неглавных идеалов и фильтров. Пусть A — бесконечное множество. Совокупность $\mathcal{P}_0(A)$ всех конечных подмножеств A есть неглавный идеал, а совокупность подмножеств, имеющих конечное дополнение до A — неглавный фильтр булевой алгебры $\mathcal{P}(A)$. Фильтр указанного вида называют *фильтром Фреше*.

То, что I — собственный идеал булевой алгебры B будем записывать $I \triangleleft B$.

Справедлива следующая простая

Теорема 5.6. *Пусть B — булева алгебра и $X \subseteq B$. Тогда множество $X' = \{x' \mid x \in X\}$ будет идеалом B , если X — фильтр B и фильтром B , если X — идеал B .*

Идеалы [фильтры] указанного вида называются *присоединёнными* к соответствующим фильтрам [идеалам].

Максимальные фильтры булевых алгебр будем называть *ультрафильтрами*. Точнее, ультрафильтр булевой алгебры B — это её собственный фильтр F , удовлетворяющий условию

$$\forall x (x \in F \vee x' \in F).$$

Однако, понятия «ультрафильтр» и «максимальный фильтр» (как собственный фильтр, не лежащий ни в каком другом собственном фильтре) оказываются эквивалентными

(см. ниже). Это позволяет максимальные фильтры булевых алгебр называть ультрафильтрами, что традиционно и делается.

Понятно, что если x — атом [коатом] конечной булевой алгебры, то x^Δ [x^∇] — её максимальный фильтр [идеал]. В конечных булевых алгебрах ультрафильтры других видов, очевидно, отсутствуют. Существование максимальных идеалов и фильтров в бесконечной булевой алгебре следует из теоремы 4.7 о собственных идеалах решётки с единицей.

Теорема 5.7 (свойства максимальных булевых идеалов и фильтров).

1. Каждый собственный идеал [фильтр] булевой алгебры содержится в некотором максимальном идеале [ультрафильтре].
2. Идеал [фильтр] булевой алгебры B является максимальным, если и только если для любого $x \in B$ в нём содержится в точности один из элементов x и x' .
3. Собственный идеал I [фильтр F] булевой алгебры B будет максимальным, если и только если для любых $x, y \in B$ из условия $(x \sqcup y) \in I$ [$(x \sqcap y) \in F$] следует, что либо x , либо y принадлежит I [F].
4. Собственный идеал [фильтр] булевой алгебры совпадает с пересечением всех максимальных идеалов [ультрафильтров], в которых он содержится.
5. Максимальный идеал [фильтр] булевой алгебры содержит все атомы [коатомы] булевой алгебры, кроме, быть может, одного.

Доказательство. В силу двойственности достаточно показать справедливость утверждений относительно идеалов.

1. Доказательство для идеалов совпадает с приведённым для теоремы 4.7 о собственных идеалах решётки с единицей.
2. Докажем данное утверждение для идеалов. Пусть I — максимальный идеал булевой алгебры $\langle B, \sqcup, \sqcap, ', o, \iota \rangle$. Он не может содержать ни одной пары элементов x и x' , т.к. иначе $x \sqcup x' = \iota \in I \Rightarrow I = B$, т.е. I — несобственный идеал. Противоречие.

Пусть теперь идеал I булевой алгебры B , $x \in B$ и I не содержит ни x , ни x' . Рассмотрим множество $I_1 = \{x \sqcup i \mid i \in I\}$. Легко видеть, что I_1 — идеал и $I \subseteq I_1$, т.е. I не максимален.

3. (\Rightarrow) Пусть идеал I булевой алгебры B максимален, т.е. $B/I \cong_b \mathbf{2} = \{o, \iota\}$. Тогда для любого $x \in B$ его смежный класс $[x]_I$ есть либо o , либо ι . В первом случае $x \in I$, во втором — $x' \in I$.

(\Leftarrow) Пусть для любого элемента булевой алгебры B либо он, либо его дополнение содержится в идеале $I \trianglelefteq B$. Пусть $I \subset I_1 \trianglelefteq B$. Тогда для $x \in I_1 \setminus I$ имеем $x' \in I_1$, откуда $x \sqcup x' = \iota \in I_1$, т.е. $I_1 = B$ и идеал I — максимальный.

Доказательство остальных утверждений можно найти, например, в [22], [27], [34]. \square

Замечания.

- К п. 1. Данное утверждение для фильтров часто называют *теоремой об ультрафильтрах* булевой алгебры.
- К п. 3. Собственный фильтр F булевой алгебры B , удовлетворяющий условию

$$(x \sqcup y) \in F \Rightarrow \begin{cases} x \in F \\ y \in F \end{cases}$$

называется *простым*. Таким образом данное утверждение доказывает эквивалентность понятий «ультрафильтр» и «простой фильтр» булевой алгебры.

Пусть B — булева алгебра, а \sim — конгруэнция на ней, как на решётке. Если при этом ещё и

$$x \sim y \Rightarrow x' \sim y',$$

то \sim — конгруэнция на данной булевой алгебре. Конгруэнции булевой алгебры B образуют полную дистрибутивную решётку $\text{Con } B$. Её наименьшим элементом является тождественная конгруэнция Δ_B , а наибольшим — аморфная конгруэнция ∇_B .

Важным отличием идеалов булевой алгебры от решёточных является то, что они находятся во взаимно-однозначном соответствии с конгруэнциями булевой алгебры. Именно, если $\sim = \sim_I$ — конгруэнция на булевой алгебре B и $I = [o]$ — класс эквивалентности, содержащий элемент o , то I — идеал B , причём выполняется соотношение

$$a \sim_I b \Leftrightarrow \exists_I x (a \sqcup x = b \sqcup x). \quad (5.1)$$

И обратно, если $I \trianglelefteq B$, то отношение \sim_I на B , определённое условием (5.1), будет конгруэнцией на B , причём $[o] = I$. Более того, покажем, что справедливо нижеследующее

Утверждение 5.2. Пусть a и b — элементы булевой алгебры B и $I \trianglelefteq B$.

$$a \sim_I b \Leftrightarrow (a \sqcap b') \sqcup (a' \sqcap b) \in I.$$

Доказательство. (\Rightarrow) Пусть существует $x \in I$ такой, что $a \sqcup x = b \sqcup x$. Тогда, беря пересечения с b' обеих частей равенства, получим $(a \sqcup x) \sqcap b' = (a \sqcap b') \sqcup (x \sqcap b') = x \sqcap b'$, т.е. $a \sqcap b' \sqsubseteq x \sqcap b' \in I$ и $a \sqcap b' \in I$. Аналогично $a' \sqcap b \in I$ и, по свойству идеала, $(a \sqcap b') \sqcup (a' \sqcap b) \in I$.

(\Leftarrow) Пусть $(a \sqcap b') \sqcup (a' \sqcap b) = z \in I$. Тогда $a \sqcap b' \sqsubseteq z$ и $a \sqcap b' \sqsubseteq z$, т.е. $a \sqcap b' = x \in I$ и $a \sqcap b' = y \in I$. Откуда, беря объединения с b обеих частей первого равенства и с a — второго равенства, получаем $a \sqcup b = x \sqcup b$ и $a \sqcup b = y \sqcup b$ соответственно. Отсюда $x \sqcup b = y \sqcup a$. \square

Конгруэнции на булевой алгебре естественным образом порождают факторалгебры. Пусть \sim — конгруэнция на булевой алгебре B , а I — идеал, соответствующий данной конгруэнции в указанном выше смысле. Фактормножество B/\sim обозначим B/I . На классах-элементах B/I могут быть введены булевы операции объединения, пересечения и дополнения, поскольку результат над элементами из фиксированных классов будет лежать в одном классе эквивалентности, вне зависимости от того, какие элементы будут выбраны из данных классов, т.к. конгруэнция как раз и обеспечивает это свойство. Таким образом, АС B/I будет факторалгеброй булевой алгебры B .

Отображение $\varphi : B \rightarrow B/\sim$, $\varphi(x) = [x]_{\sim}$, ставящее в соответствие элементу B его смежный класс по конгруэнции $\sim \in \text{Con}(B)$, является, очевидно, гомоморфизмом. Такой гомоморфизм, в соответствии с общим подходом, называется *естественным*. С другой стороны, если φ — гомоморфизм булевой алгебры B , то $\varphi(B) \cong_b B/\text{Ker } \varphi$ и $\text{Ker } \varphi \in \text{Con}(B)$.

Теорема 5.8 (Тарский). Идеал I булевой алгебры B максимален, если и только если $B/I \cong_b \mathbf{2}$.

Пример 5.4. Идеалом приведённого в примере 5.1 двузначного гомоморфизма j_a будет главный идеал $(a')^\nabla$, порождённый коатомом a' .

Для главных идеалов булевых алгебр справедлив изоморфизм $B/x^\nabla \cong_b [o, x']$.

Пример 5.5. Проиллюстрируем изоморфизм $B/x^\nabla \cong_b [o, x']$ для булевой алгебры B^3 . Её атомы будем обозначать a, b и c , а остальные элементы — указанием содержащихся

в них атомов. Если в качестве идеала I взять a^∇ , то классами эквивалентности по \sim_{a^∇} будут

$$[a] = a^\nabla = I = \{a, \emptyset\}, \quad [b] = \{ab, b\}, \quad [c] = \{ac, c\}, \quad [bc] = \{abc, bc\}.$$

Факторалгеброй булевой алгебры B^3 по выбранному идеалу будет изоморфная B^2 алгебра из указанных выше классов с нулём I , атомами $[b]$ и $[c]$ и единицей $[bc]$. Поскольку $bc = a'$ и $\emptyset \in I$, то $B/a^\nabla \cong_b [\emptyset, a']$.

На рис. 5.1.1), изображена булева алгебра B^3 , причём классы эквивалентности по \sim_{a^∇} выделены двойными линиями, а на рис. 5.1.2) — факторалгебра B^3/a^∇ .

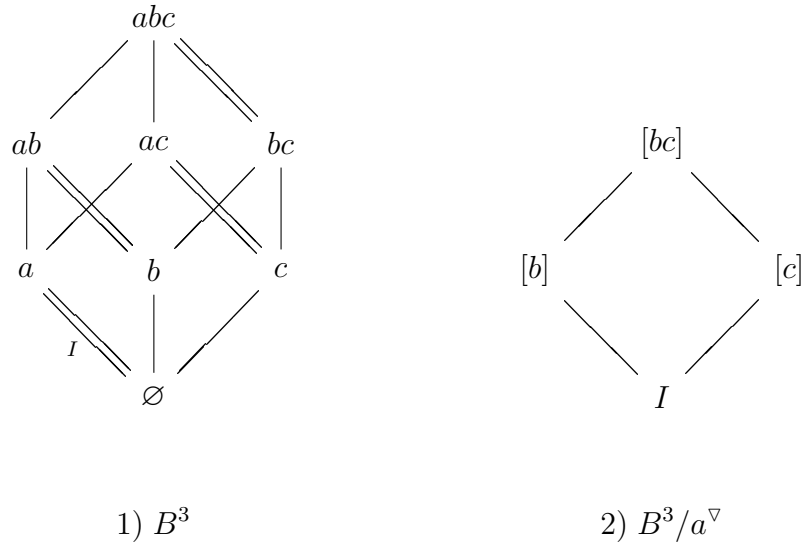
1) B^3 2) B^3/a^∇

Рис. 5.1: К примеру 5.5

Укажем теперь на связь идеалов [фильтров] булевой алгебры с булевыми гомоморфизмами.

Утверждение 5.3. *Ядро булева гомоморфизма есть собственный идеал. Каждый собственный идеал булевой алгебры представляет собой ядро некоторого её гомоморфизма.*

Прообраз единицы булева гомоморфизма есть собственный фильтр.

Доказательство. Докажем утверждения теоремы относительно идеалов, оставив последнее в качестве простого упражнения.

(\Rightarrow) Пусть φ — гомоморфизм из булевой алгебры B в булеву алгебру B' . Его ядро $\varphi^\#(0)$ непусто, поскольку всегда содержит $o \in B$. Пусть $x, y \in \varphi^\#(0)$. Тогда, во-первых, $\varphi(x \sqcup y) = \varphi(x) \sqcup \varphi(y) = o \sqcup o = o$, а во-вторых, если $z \sqsubseteq x$, то $\varphi(z) \sqsubseteq \varphi(x) = o$, и поэтому $\varphi(z) = 0$ и $z \in \varphi^\#(0)$.

(\Leftarrow) Если $I \triangleleft B$ и $\varphi : B \rightarrow B/I$ — гомоморфизм B на свою факторалгебру по конгруэнции, задаваемой идеалом I , то $I = \varphi^\#(B/I)$. \square

Мы видим, что для булевых алгебр понятия идеала, конгруэнции, факторалгебры и гомоморфизма оказываются тесно связанными и каждая из этих алгебраических конструкций определяет другую.

С помощью факторизации могут быть построены безатомные булевы алгебры. Рассмотрим $\langle \mathcal{P}(\mathbb{Z}), \cup, \cap, -, \emptyset, \mathbb{Z} \rangle$ — тотальную алгебру над множеством целых чисел \mathbb{Z} .

Определим отношение \simeq над элементами $\mathcal{P}(\mathbb{Z})$: будем считать, что $A \simeq B$, если симметрическая разность множеств A и B конечна. Ясно, что \simeq есть отношение эквивалентности. Поэтому можно образовать фактормножество $\mathcal{P}(\mathbb{Z})/\simeq$. Все конечные (включая пустое) подмножества $\mathcal{P}(\mathbb{Z})$ будут, очевидно, эквивалентными. Обозначим этот класс эквивалентности $[\emptyset]$. Также будут эквивалентными все подмножества целых чисел, имеющих конечные дополнения до \mathbb{Z} , включая само \mathbb{Z} ; этот класс эквивалентности обозначим $[\mathbb{Z}]$. Далее, легко проверить, что введенное отношение является также и стабильным относительно теоретико-множественных операций, т.е. для любых $A, B \in \mathcal{P}(\mathbb{Z})$ из $A \simeq A'$ и $B \simeq B'$ следует $A \cup B \simeq A' \cup B'$, $A \cap B \simeq A' \cap B'$ и $\overline{A} \simeq \overline{A'}$. Это означает, что АС $\langle \mathcal{P}(\mathbb{Z})/\simeq, \cup, \cap, -, [\emptyset], [\mathbb{Z}] \rangle$ будет являться булевой алгеброй.

Легко убедиться, что данная булева алгебра не имеет атомов. Действительно, любой отличный от $[\emptyset]$ элемент $\mathcal{P}(\mathbb{Z})/\simeq$ есть класс бесконечных множеств. Атом — элемент, непосредственно следующий за $[\emptyset]$, а таковые отсутствуют в $\mathcal{P}(\mathbb{Z})/\simeq$: действительно, в любом бесконечном множестве X можно (с помощью аксиомы выбора!) указать подмножество Y такое, что и оно, его дополнение бесконечны, и поэтому $[Y]$ строго содержится в $[X]$. Понятно, что подобная процедура может быть проведена для любой бесконечной алгебры множеств: если M — бесконечное множество, то $\mathcal{P}(M)/\mathcal{P}_0(M)$ — безатомная булева алгебра.

Говорят, что главные ультрафильтры алгебры множеств, поскольку все они имеют вид a^Δ , фиксированы в точке a множества. Их называют *тривиальными* ультрафильтрами. Совместно с фильтрами Фреше они играют важную роль при исследовании сходимости в анализе (топологическая система окрестностей данной точки является фиксированным в ней тривиальным ультрафильтром). Главные ультрафильтры также используют, например, при исследованиях полноты логических систем в *алгебрах Линденбаума–Тарского*, порождённых соответствующей логической теорией (см., например, [27] или [13]).

Пример 5.6. Рассмотрим множество $\mathcal{A} = \{A, B, \dots\}$ формул алгебры логики (формул над высказываниями). Если $A \equiv B$ есть тождественно истинная формула, то говорят, что формулы A и B *логически эквивалентны* или *равносильны*, что записывают как $A \sim B$. Ясно, что \sim есть отношение эквивалентности на \mathcal{A} . Класс эквивалентности, порождаемый формулой A будем обозначать $[A]$, классы тождественно истинных формул — \mathbf{T} , а тождественно ложных формул — \mathbf{F} .

На фактормножестве \mathcal{A}/\sim классов эквивалентности формул алгебры логики можно задать теоретико-множественные операции дополнения ($-$), объединения (\cup) и пересечения (\cap), причём

$$\overline{[A]} = [\neg A], \quad [A] \cup [B] = [A \vee B], \quad [A] \cap [B] = [A \& B].$$

Легко установить, что введенные операции над классами эквивалентностей имеют следующие свойства:

- операции \cup и \cap коммутативны и взаимно дистрибутивны;
- выполняются соотношения $[A] \cup \mathbf{F} = [A]$ и $[A] \cap \mathbf{T} = [A]$;
- справедливы законы $[A] \cup \overline{[A]} = \mathbf{T}$ и $[A] \cap \overline{[A]} = \mathbf{F}$.

Указанное означает, что АС $\langle \mathcal{A}/\sim, \cup, \cap, -, \mathbf{T}, \mathbf{F} \rangle$ является булевой алгеброй. Её называют *факторалгеброй логических формул*. Для классической алгебры высказываний она совпадает с соответствующей алгеброй Линденбаума–Тарского (в последней факторизация проводится по отношению \simeq такому, что $A \simeq B$ если и только если из формулы A выводится формула B и наоборот). С каждым элементом \mathcal{A}/\sim связана соответствующая функция алгебры логики.

Обозначим через \mathcal{A}_n множество формул алгебры логики над n элементарными высказываниями. Очевидно, \mathcal{A}_n бесконечно, а фактормножество \mathcal{A}_n/\sim — конечно (содержит 2^{2^n} элементов).

Рассмотрим уравнение

$$a(\tilde{x}) \& X(\tilde{x}) = \mathbf{F},$$

где $a(\tilde{x})$ и $X(\tilde{x})$ — формулы, реализующие соответственно известную и искомую булевы функции (для простоты указывают именно формулы, а не порождённые ими классы). Тогда решением данного уравнения будет любая функция, реализуемая формулами из главного идеала, порождённого формулой $\overline{a(\tilde{x})}$ в соответствующей алгебре Линденбаума–Тарского. Далее знак конъюнкции $\&$ будем для простоты опускать.

Например, пусть $a(\tilde{x}) = \bar{x}_1\bar{x}_2$, т.е. дано уравнение

$$\bar{x}_1\bar{x}_2X(x_1, x_2) = \mathbf{F}. \tag{*}$$

Имеем $\overline{\bar{x}_1\bar{x}_2} = x_1 \vee x_2$, и главный идеал алгебры Линденбаума–Тарского, порождённый классом формул $[x_1 \vee x_2]$, составляют классы $[x_1 \vee x_2]$, $[x_1]$, $[x_2]$, $[x_1\bar{x}_2 \vee \bar{x}_1x_2]$, $[x_1\bar{x}_2]$, $[x_1x_2]$, $[\bar{x}_1x_2]$ и \mathbf{F} . На рис. 5.2 показан данный идеал. Для каждого класса указан вектор значений соответствующей функции (подразумевается упорядочение наборов значений переменных сначала по x , затем по y).

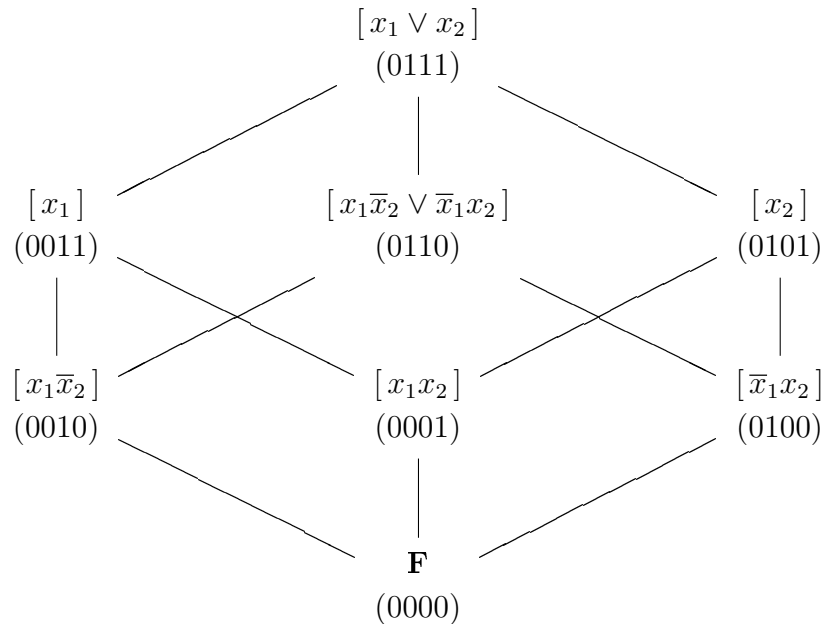


Рис. 5.2: Главный идеал L_2^* , порожденный классом конъюнкции

Решением уравнения (*) будет любая булева функция, реализуемая формулами из приведённых классов.

В бесконечных булевых алгебрах, могут существовать и неглавные (нетривиальные) ультрафильтры. Их также называют *свободными*, поскольку они не фиксированы ни в какой точке исходного множества. Пересечение всех элементов такого фильтра есть нулевой элемент.

Пример 5.7. Опишем в самом общем виде, как может быть построен неглавный ультрафильтр F булеана $\mathcal{P}(\mathbb{N})$. Сначала рассмотрим фильтр Фреше, который обозначим F_0 . Он не является максимальным, поскольку, например, ни множество чётных чисел $2\mathbb{N}$, ни его дополнение (множество нечётных чисел) не принадлежат F_0 . Поэтому надо принять решение, отнести $2\mathbb{N}$ к конструируемому ультрафильтру F или нет. Пусть принято решение о том, что $2\mathbb{N} \in F$. Это будет означать, что некоторые другие множества (все множества, содержащие $2\mathbb{N}$) также будут принадлежать F . Полученный фильтр обозначим F_1 . Понятно, что он также не будет являться искомым ультрафильтром, поскольку

относительно ряда множеств неопределённость останется: например, ни множество $3\mathbb{N}$, ни его дополнение не принадлежат F_1 . Здесь снова нужно принять решение о вхождении одного из указанных множеств в F_1 , построить F_2 и т.д. Показано, что в результате выполнения “трансфинитного числа шагов” будет построен искомый ультрафильтр F .

Хотя мы привели чрезвычайно грубый набросок способа построения фильтра F , надеемся, что читателю видна роль аксиомы выбора в данных рассуждениях: никакого способа указать, какое множество нужно рассматривать на каждом шаге для включения его или его дополнения в F , нет. Кроме того, на каждом шаге можно принять любую из указанных альтернатив. Мы видим, что процесс построения F существенно неоднозначен, и, на самом деле, до сих пор не указано ни одного неглавного ультрафильтра в явном виде, без применения аксиомы выбора.

Неглавные ультрафильтры над $\mathcal{P}(\mathbb{N})$ могут быть использованы, например, при построении поля гипердействительных чисел в нестандартном анализе.

Пример 5.8. Множество гипердействительных чисел ${}^*\mathbb{R}$, изучаемых в нестандартном анализе, представляет собой неархимедово упорядоченное поле, являющееся расширением поля \mathbb{R} действительных чисел³. Это означает, что ${}^*\mathbb{R}$ — цепь, в которую вложено множество \mathbb{R} (образ \mathbb{R} — стандартные гипердействительные числа) и содержащее, кроме того, множество т.н. нестандартных гипердействительных чисел. При этом в ${}^*\mathbb{R}$ выполняются все аксиомы поля, однако не выполняется справедливая в \mathbb{R} аксиома Архимеда: «для любых двух положительных чисел a и b существует натуральное n такое, что $n \cdot a > bB$ ».

Согласно принципу наследования свойств при расширении, аксиома Архимеда может нарушаться лишь когда хотя бы одно из чисел A и B нестандартное. Среди нестандартных чисел выделяют бесконечно большие и бесконечно малые. Так, если числа ε и I суть положительные бесконечно малое и бесконечно большое гипердействительные, а x — положительное действительное, то неравенства

$$\underbrace{\varepsilon + \dots + \varepsilon}_{n \text{ раз}} > x \quad \text{и} \quad \underbrace{x + \dots + x}_{n \text{ раз}} > I$$

не будут выполняться ни для какого натурального n .

Поле гипердействительных чисел ${}^*\mathbb{R}$ можно построить, используя некоторый неглавный ультрафильтр U в $\mathcal{P}(\mathbb{N})$. Рассмотрим всевозможные последовательности обычных действительных чисел. Будем говорить, что последовательности $a = (a_1, a_2, \dots)$ и $b = (b_1, b_2, \dots)$ эквивалентны, если равенство $a_i = b_i$ нарушается на множестве, не принадлежащем U .

Легко проверяется, что, в силу свойств ультрафильтров введённое отношения действительно является отношением эквивалентности и, например, все последовательности, отличающиеся в конечном числе членов, эквивалентны. Получающиеся классы эквивалентности назовём гипердействительными числами; они и будут являться элементами ${}^*\mathbb{R}$. Действительному числу a соответствует класс эквивалентности $[(a, a, \dots)]$, это — стандартное гипердействительное число.

Четыре арифметических действия производятся над последовательностями почленно. Будем считать, что $a < b$, если неравенство $a_i \geq b_i$ выполняется на каком-либо множестве, не входящем в U .

Нетрудно проверить, что, поскольку U — ультрафильтр, получено упорядоченное поле. В этом поле, однако, аксиома Архимеда не выполняется: например, $[(1, \frac{1}{2}, \frac{1}{3}, \dots)]$

³Создал нестандартный анализ американский математик А. Робинсон (1918–1974). Элементарному введению в дисциплину посвящена брошюра *Успенский В.А.* Нестандартный, или неархимедов, анализ. — М., 1983, откуда взяты этот и предыдущий примеры.

Последнее время вместо слова «нестандартный» часто пользуются термином «инфинитезимальный» (инфинитезимальными называют актуально рассматриваемые бесконечно большие и бесконечно малые величины) в противопоставление анализу бесконечно малых. Для дальнейшего изучения можно рекомендовать книгу *Гордон Е.И., Кусраев А.Г., Кутателадзе С.С.* Инфинитезимальный анализ. — Новосибирск, 2006.

есть бесконечно малое, а $[(1, 2, 3, \dots)]$ — бесконечно большое гипердействительные числа. При проверке этих свойств и требуется, чтобы U был неглавным ультрафильтром.

5.4 Булевы многочлены

Определение 5.7. Пусть $X_n = \{x_1, \dots, x_n\}$ — n -элементное множество *неизвестных* или *переменных*, не содержащее символов o и i . Тогда *булевы многочлены над X_n* суть объекты, удовлетворяющие следующим условиям:

- 1) $x_1, \dots, x_n, 0, 1$ — булевы многочлены;
- 2) если p и q — булевы многочлены, то таковыми являются и $(p) \sqcup (q)$, $(p) \sqcap (q)$, $(p)'$.

Множество всех булевых многочленов над X_n обозначим через P_n .

Понятно, что булевы многочлены — формальные строки символов (слова). Под записью $p = q$ мы будем понимать, что многочлены p и q совпадают как строки символов, т.е. их *синтаксическое тождество*, говоря при этом, что данные многочлены *равны*. Далее мы будем пользоваться известными правилами экономии скобок — вместо $(x_i)'$, $(0)'$ и $(1)'$ писать x_i' , $0'$ и $1'$ соответственно — и считать, что $p = q$, если данные многочлены совпадают при восстановлении всех скобок согласно определению 5.7. Любой булев многочлен над n переменными можно рассматривать как многочлен над $n + 1$ переменной, поэтому

$$P_1 \subset P_2 \subset \dots \subset P_n \subset P_{n+1} \subset \dots$$

Заметим, что P_n не является булевой алгеброй, поскольку $x_1 \sqcup x_2 \neq x_2 \sqcup x_1$ и $x_1 \sqcap x_2 \neq x_2 \sqcap x_1$. Для отождествления подобных выражений введём понятие полиномиальной функции, индуцированной многочленом на булевой алгебре B , обобщающее понятие булевой функции [39] (случай $B = \mathbf{2} = \{0, 1\}$).

Определение 5.8. Пусть B — булева алгебра и p — булев многочлен из P_n . Обозначим через $\widehat{p}_B(b_1, \dots, b_n)$ элемент из B , который получается из p заменой каждого x_i на $b_i \in B$, $i = 1, \dots, n$. Тогда отображение

$$\widehat{p}_B : B^n \rightarrow B, \quad (b_1, \dots, b_n) \mapsto \widehat{p}_B(b_1, \dots, b_n) \quad (5.2)$$

называется *полиномиальной функцией, индуцированной булевым многочленом p на B* .

Пример 5.9. 1. Пусть $B = \mathbf{2}$, $n = 2$, $p = x_1 \sqcup x_2$ и $q = x_2 \sqcup x_1$. Тогда $p \neq q$, $\widehat{p}_B = a \vee b$, $\widehat{q}_B = b \vee a$, где $a, b \in \{0, 1\}$ и $\widehat{p}_B = \widehat{q}_B$.

2. Пусть $B = \mathcal{P}(A)$, $n = 2$, $p = (x_1 \sqcup x_2)'$ и $q = x_1' \sqcap x_2'$. Тогда опять $p \neq q$, а $\widehat{p}_B = \overline{X \cup Y}$, $\widehat{q}_B = \overline{X} \cap \overline{Y}$, где $X, Y \subseteq A$ и снова $\widehat{p}_B = \widehat{q}_B$.

Определение 5.9. Два булевых многочлена $p, q \in P_n$ называются *эквивалентными* (символически $p \sim q$), если равны их полиномиальные функции на $\mathbf{2}$, т.е.

$$p \sim q \Leftrightarrow \widehat{p}_2 = \widehat{q}_2.$$

Легко видеть, что \sim действительно есть отношение эквивалентности на P_n , поскольку его свойства рефлексивности, симметричности и транзитивности наследуются из отношения равенства функций.

Обозначим $P_B^n = \{\widehat{p}_B \mid p \in P_n\}$ — множество всех полиномиальных функций, индуцированных многочленами из P_n на B .

Теорема 5.9. P_n / \sim есть булева алгебра, и $P_n / \sim \cong_b P_2^n$.

Доказательство. Определим отображение $\varphi: P_{\mathbf{2}}^n \rightarrow P_n / \sim$, которое переводит полиномиальную функцию $P_{\mathbf{2}}^n$, индуцированную многочленом p на $\mathbf{2}$ в класс эквивалентности $[p]_{\sim}$. Данное определение корректно, т.к. $\widehat{p}_{\mathbf{2}} = \widehat{q}_{\mathbf{2}} \Rightarrow p \sim q \Rightarrow [p]_{\sim} = [q]_{\sim}$. Легко проверить, что φ и есть искомым булев изоморфизм. \square

Теорема 5.10. Если B — булева алгебра, то и P_B^n — булева алгебра, причём $P_B^n \leq B^{B^n}$.

Доказательство. Необходимо убедиться в устойчивости P_B^n относительно операций объединения, пересечения и дополнения, а также, что P_B^n содержит указанные в теореме 5.2 постоянные функции $f_0 \equiv 0$ и $f_1 \equiv 1$.

Для \sqcup имеем

$$(\widehat{p}_B \sqcup \widehat{q}_B)(a) = \widehat{p}_B(a) \sqcup \widehat{q}_B(a) \stackrel{(5.2)}{=} (\widehat{p \sqcup q})_B(a) \in P_B^n$$

для произвольного $a \in B^n$. Для \sqcap и $'$ доказательство аналогично.

Кроме того, $f_0 \equiv 0$ и $f_1 \equiv 1$ для любой булевой алгебры B и по (5.2) эти функции содержатся в P_B^n . \square

С помощью теоремы Стоуна показывается, что полиномиальные функции, соответствующие эквивалентным многочленам, совпадают на любой булевой алгебре, а не только на $\mathbf{2}$, т.е. справедлива

Теорема 5.11. Пусть $p, q \in P_n$ и $p \sim q$. Тогда для произвольной булевой алгебры B справедливо $\widehat{p}_B = \widehat{q}_B$.

Доказательство можно найти в [22].

Часто возникает потребность заменить данный многочлен эквивалентным ему более простым многочленом. Данную проблему решают в два этапа. Сначала вводят т.н. нормальные формы многочленов. Совокупность нормальных форм обеспечивает наличие системы представителей для каждого класса эквивалентности множества P_n . Далее задача сводится к нахождению кратчайшего в том или ином смысле многочлена, эквивалентного данной нормальной форме.

Определение 5.10. Множество $N \subseteq P_n$ называется *системой совершенных нормальных форм*, если

- для любого элемента P_n найдётся эквивалентный ему элемент N ;
- два разных элемента N неэквивалентны.

Будем далее пользоваться обозначением x^σ , аналогичным введённому в п. 1.2 для множеств, а именно, для $\sigma \in \{0, 1\}$ и $x \in \{x_1, \dots, x_n, o, \iota\}$ положим

$$x_i^1 = x_i, \quad x_i^0 = x_i', \quad o^1 = 0, \quad o^0 = 1, \quad \iota^1 = 1, \quad \iota^0 = 0.$$

Последние равенства говорят о том, что мы будем далее в рамках данного раздела для простоты пользоваться символами 0 и 1 для обозначения нуля и единицы булевой алгебры соответственно. Выражения вида x_i, x_i' , а также 0 и 1 будем называть *литералами*.

Пусть B — булева алгебра, p — булев многочлен из P_n . Полиномиальную функцию $\widehat{p}_B(b_1, \dots, b_n) : \mathbf{2}^n \rightarrow \mathbf{2}$, индуцированную p на B , обозначим f_p . Элементы $\mathbf{2}^n$ будем обозначать $\tilde{\alpha}, \tilde{\beta}, \dots$. Таким образом, например, $\tilde{\alpha} = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in \{0, 1\}$, $i = \overline{1, n}$. Функции f_p сопоставлены два множества $N_{f_p}^1$ и $N_{f_p}^0$ её единичных и нулевых наборов. Следующие два булевых многочлена

$$p_d(f_p) = \bigsqcup_{\tilde{\alpha}=(\alpha_1, \dots, \alpha_n) \in N_{f_p}^1} (x_1^{\alpha_1} \sqcap \dots \sqcap x_n^{\alpha_n}) \quad \text{и}$$

$$p_c(f_p) = \prod_{\tilde{\alpha}=(\alpha_1, \dots, \alpha_n) \in N_{f_p}^0} (x_1^{\alpha_1} \sqcup \dots \sqcup x_n^{\alpha_n})$$

при $N_{f_p}^1 \neq \emptyset$ и $N_{f_p}^0 \neq \emptyset$ называются соответственно *совершенными дизъюнктивной и конъюнктивной нормальными формами* (СДНФ и СКНФ) многочлена p . При $N_{f_p}^1 = \emptyset$ полагают $p_d(f_p) = 0$, а при $N_{f_p}^0 = \emptyset$ — $p_c(f_p) = 1$. Ясно, что данные формы определены однозначно с точностью до порядка соответствующих членов. Заметим, что СДНФ для многочлена над $\{x_1\}$ называется разложением Шеннона по $x = x_1$: $(a \sqcap x) \sqcup (b \sqcap x')$, где a и b — известные элементы булевой алгебры B .

В многочисленных пособиях (см., например, [22] или [39]) показывается что совокупности СДНФ и СКНФ всех $p \in P_n$ есть системы совершенных нормальных форм. Как следствие, имеем

1. $P_2^n = \mathbf{2}^{2^n}$ и $|P_n / \sim| = 2^{2^n}$, т.е. любая функция из $\mathbf{2}^n$ в $\mathbf{2}$ является полиномиальной булевой функцией. Поэтому говорят, что алгебра $\mathbf{2}^n$ *полиномиально полна*.
2. Если $|B| = m > 2$, то $|P_B^n| = |P_n / \sim| = 2^{2^n} < m^{m^n} = |B^{B^n}|$, т.е. $\mathbf{2}^n$ — единственно полиномиально полная булева алгебра.

Полиномиальная полнота означает, что каждую функцию можно представить полиномом.

Пример 5.10. Пусть

$$p = ((x_1 \sqcup x_2) \sqcap x_1') \sqcup ((x_2')' \sqcap (x_1 \sqcup x_2')) \in P_2.$$

Поскольку $\widehat{p}_B(0, 0) = \widehat{p}_B(1, 0) = 0$ и $\widehat{p}_B(0, 1) = \widehat{p}_B(1, 1) = 1$, имеем

$$p \sim (x_1' \sqcap x_2) \sqcup (x_1 \sqcap x_2') = p_d(f_p).$$

Заметим, что применяя законы булевой алгебры, можно получить

$$p_d(f_p) \sim (x_1' \sqcup x_1) \sqcap x_2 \sim 1 \sqcap x_2 \sim x_2.$$

СДНФ булева многочлена p можно получить по следующему алгоритму.

Шаг 1. Применяя законы *DeM1,2* добиваемся, чтобы знаки дополнения относились только к литералам и константам.

Шаг 2. Применяя законы *Dtr1,2* выражаем p в виде объединения пересечений.

Шаг 3. Если в некотором пересечении отсутствуют как x_i , так и x_i' , в качестве множителя к p добавляем $x_i \sqcup x_i'$.

Шаг 4. Применяя (возможно неоднократно) *DeM1*, пока не будет получено объединение пересечений. Применяя закон *Id* \sqcap , получаем СДНФ p .

Пример 5.11. Пусть $a, b \in \mathbf{2}$ и

$$p = ((a \sqcap x_1) \sqcup (b \sqcap x_2)')' \sqcup (x_1 \sqcup b)'$$

Шаг 1. $p \sim ((a \sqcap x_1)' \sqcap (b \sqcap x_2)') \sqcup (x_1' \sqcap b') \sim ((a' \sqcup x_1') \sqcap (b \sqcap x_2)) \sqcup (x_1' \sqcap b')$.

Шаг 2.

$$\begin{aligned} ((a' \sqcup x_1') \sqcap (b \sqcap x_2)) \sqcup (x_1' \sqcap b') &\sim \\ &\sim ((a' \sqcap b \sqcap x_2) \sqcup (x_1' \sqcap b \sqcap x_2)) \sqcup (x_1' \sqcup b') \sim \\ &\sim (a' \sqcap b \sqcap x_2) \sqcup (x_1' \sqcap b \sqcap x_2) \sqcup (x_1' \sqcup b'). \end{aligned}$$

$$\text{Шаг 3. } \underbrace{(a' \sqcap b \sqcap x_2)}_1 \sqcup \underbrace{(x_1' \sqcap b \sqcap x_2)}_2 \sqcup \underbrace{(x_1' \sqcap b')}_3 = y.$$

В пересечении 1 отсутствует x_1 , поэтому в 1 добавляем $x_1 \sqcup x_1'$; в пересечении 2 встречаются как x_1 , так и x_2 , поэтому в 2 не добавляем ничего; в пересечении 3 отсутствует x_2 — добавляем $x_2 \sqcup x_2'$. Имеем

$$y \sim (a' \sqcap b \sqcap (x_1 \sqcup x_1') \sqcap x_2) \sqcup (x_1' \sqcap b \sqcap x_2) \sqcup (b' \sqcap x_1' \sqcap (x_2 \sqcup x_2')).$$

Шаг 4.

$$\begin{aligned} & (a' \sqcap b \sqcap (x_1 \sqcup x_1') \sqcap x_2) \sqcup (x_1' \sqcap b \sqcap x_2) \sqcup (b' \sqcap x_1' \sqcap (x_2 \sqcup x_2')) \sim \\ & \sim ((a' \sqcap b \sqcap x_1 \sqcup x_2) \sqcup (a' \sqcap b \sqcap x_1' \sqcup x_2) \sqcup (b \sqcap x_1' \sqcap x_2) \sqcup \\ & \quad \sqcup ((b' \sqcap x_1' \sqcap x_2) \sqcup (b' \sqcap x_1' \sqcap x_2'))) \sim \\ & \sim (a' \sqcap b \sqcap x_1 \sqcup x_2) \sqcup (a' \sqcap b \sqcap x_1' \sqcup x_2) \sqcup (b \sqcap x_1' \sqcap x_2) \sqcup \\ & \quad \sqcup (b' \sqcap x_1' \sqcap x_2) \sqcup (b' \sqcap x_1' \sqcap x_2'). \end{aligned}$$

Рассмотрим отдельно три средних пересечения, содержащие $x_1' \sqcup x_2$:

$$\begin{aligned} & ((a' \sqcap b) \sqcap (x_1' \sqcup x_2)) \sqcup (b \sqcap (\sqcap x_1' \sqcap x_2)) \sqcup (b' \sqcap (x_1' \sqcap x_2)) \sim \\ & \sim ((a' \sqcap b) \sqcup b \sqcup b') \sqcap (x_1' \sqcap x_2) \sim \\ & \sim ((a' \sqcap b) \sqcup 1) \sqcap (x_1' \sqcap x_2) \sim \sqcap 1 \sqcap (x_1' \sqcap x_2). \end{aligned}$$

Итак, окончательно получаем искомую СДНФ

$$p \sim (a' \sqcap b \sqcap x_1 \sqcap x_2) \sqcup (1 \sqcap x_1' \sqcap x_2) \sqcup (b' \sqcap x_1' \sqcap x_2').$$

Методы минимизации булевых многочленов мы не будем их здесь рассматривать, их можно найти, например, в [39].

5.5 Уравнения в булевых алгебрах

В булевых алгебрах можно решать уравнения. Удобнее всего рассматривать уравнения над булевыми многочленами.

Теперь можно перейти к булевым уравнениям и методам их решения. Прежде всего, нужно определить сам термин «булево уравнение», поскольку равенство $p = q$ говорит просто, что многочлены p и q идентичны.

Определение 5.11. Пусть p и q — булевы многочлены из P_n . Пару (p, q) назовём *(булевым) уравнением*.

Пусть B — произвольная булева алгебра. Элемент $(b_1, \dots, b_n) \in B^n$ называется решением уравнения (p, q) в булевой алгебре B , если $\widehat{p}_B(b_1, \dots, b_n) = \widehat{q}_B(b_1, \dots, b_n)$.

Множество уравнений $\{(p_i, q_i) \mid i \in I \subseteq \mathbb{N}\}$ образует *систему уравнений*. *Решением системы* называется общее решение всех уравнений системы.

Если не возникает путаницы, уравнение (p, q) допустимо записывать в виде $p = q$. Например, $x_1' x_2 \vee x_3 = x_1(x_2 \vee x_3)$ — булево уравнение, а (101) — его решение, поскольку в $(1' \& 0) \vee 1 = 1 \& (0 \vee 1) = 1$.

Далее в рамках данного раздела будем, следуя традиции, вместо $x \sqcup y$ и $x \sqcap y$ писать $x \vee y$ и $x y$ ($x \& y$) и называть данные выражения суммой и произведением соответственно. *Дизъюнктивной нормальной формой (ДНФ)* назовём булев многочлен, являющийся

суммой конечного числа произведений, которые в данном случае будем называть *элементарными конъюнкциями* или *конъюнктами*. *Конъюнктивной нормальной формой (КНФ)* назовём произведение конечного числа сумм, которые в данном случае будем называть *элементарными дизъюнкциями* или *дизъюнктами*.

Отметим известное свойство нормальных форм. Если $D = C_1 \vee \dots \vee C_l$ — ДНФ над $\{x_1, \dots, x_n\}$ и C_i — элементарные конъюнкции, $i = \overline{1, l}$, а $C = D_1 \vee \dots \vee D_m$ — КНФ над $\{x_1, \dots, x_n\}$ и D_i — элементарные дизъюнкции, $i = \overline{1, m}$, то

$$D = 0 \Leftrightarrow \bigwedge_{i=1}^l C_i = 0 \quad \text{и} \quad C = 0 \Leftrightarrow \bigvee_{i=1}^m D_i = 0. \quad (5.3)$$

Пусть $D = C_1 \vee \dots \vee C_l$, где C_i — элементарные конъюнкции, $i = \overline{1, l}$, есть СДНФ многочлена p . С помощью законов булевой алгебры преобразуем D в КНФ $C = D_1 \& \dots \& D_m$, где D_i — дизъюнкты, $i = \overline{1, m}$ (или сразу тем или иным путём получим КНФ, эквивалентную p). Тогда равенство $p = 0$ будет выполняться при выполнении любого из равенств $D_i = 0$, $i = \overline{1, m}$. Если $D_i = \bigsqcup_{j \in I_i} x_j^{\sigma_j}$, $I_i \subseteq \{1, \dots, n\}$, то любой набор $\beta = (\beta_1, \dots, \beta_n)$, где $\beta_k = \sigma_j$, $j \in I_i$ и $\beta_k \in \{1, 0\}$ $j \notin I_i$ будет решением уравнения $p = 0$.

Из этого ясно, что для дальнейшего удобно преобразовать $p = q$ к виду $R = 0$.

Теорема 5.12. Уравнения $p = q$ и $pq' \vee p'q = 0$ имеют одни и те же решения.

Доказательство. Пусть B — булева алгебра и $(b_1, \dots, b_n) \in B^n$. Для $x = \widehat{p}_B(b_1, \dots, b_n)$, $y = \widehat{q}_B(b_1, \dots, b_n)$ имеем $(x \vee y)(x' \vee y') = xy' \vee x'y$. С одной стороны,

$$x = y \Rightarrow xy' \vee x'y = 0.$$

С другой, если $xy' \vee x'y = 0$, то по теореме 5.1

$$x \vee y \sqsubseteq (x' \vee y')' = xy,$$

откуда $x = y$. □

По данной теореме система уравнений $\{(p_i, q_i) \mid i = 1, \dots, m\}$ эквивалентна единственному уравнению

$$p_1q_1 \vee p_1'q_1' \vee p_2q_2 \vee p_2'q_2' \vee \dots \vee p_mq_m \vee p_m'q_m' = 0.$$

Выразив левую часть в конъюнктивной форме, получим, что приведённое выше уравнение имеет решение, когда хотя бы один из сомножителей принимает значение 0. Таким образом, получают все решения системы.

Пример 5.12. Рассмотрим систему $\{(x_1x_2, x_1x_3 \vee x_2), (x_1 \vee x_2', x_3)\}$. Перепишем её в обычном виде

$$\begin{aligned} x_1x_2 &= x_1x_3 \vee x_2, \\ x_1 \vee x_2' &= x_3. \end{aligned}$$

По теореме 5.12 данная система эквивалентна единственному уравнению

$$(x_1x_2)(x_1x_3 \vee x_2)' \vee (x_1x_2)'(x_1x_3 \vee x_2) \vee (x_1 \vee x_2')x_3' \vee (x_1 \vee x_2')'x_3 = 0.$$

Преобразуя левую часть в СКНФ, получим уравнение

$$(x_1 \vee x_2 \vee x_3')(x_1' \vee x_2' \vee x_3') = 0,$$

которое имеет то же множество решений, что и исходная система. Эти решения являются нулями первого и второго сомножителей. Например, в **2** данная система имеет ровно два решения: (001) и (111).

В произвольной булевой алгебре решения записываются более сложно, но также доставляют 0 обоим сомножителям последнего уравнения.

Один из методов решения булевых уравнений относительно одного неизвестного элемента x булевой алгебры $\langle B, \sqcup, \sqcap, ', o, \iota \rangle$ состоит в последовательном выполнении следующих шагов.

Шаг 1. Приводим данное уравнение к равносильному уравнению с o в правой части (что обеспечивается теоремой 5.12).

Шаг 2. Приводим полученное уравнение к равносильному уравнению вида

$$(a \sqcap x) \sqcup (b \sqcap x') = o,$$

где a и b — известные элементы B . Понятно, что на данном шаге находится разложение Шеннона (см. 5.4) по переменной x .

Шаг 3. Заменяем полученное уравнение на эквивалентную систему

$$a \sqcap x = o, \quad b \sqcap x' = o$$

(используется свойство (5.3) СДНФ).

Шаг 4. Если $b \not\sqsubseteq a'$, то исходное уравнение решения не имеет. Иначе, любой x такой, что

$$b \sqsubseteq x \sqsubseteq a' \quad \text{или} \quad x = (b \sqcup u) \sqcap a' = (a' \sqcap u) \sqcup b,$$

где u — произвольный элемент B , есть искомое решение.

Последний шаг обосновывают следующие выкладки. Имеем

$$\begin{aligned} a \sqcap x = 0 &\Leftrightarrow (a \sqcap x) \sqcup a' = a' \Leftrightarrow (a \sqcup a') \sqcap (x \sqcup a') = a' \Leftrightarrow \\ &\Leftrightarrow x \sqcup a' = a' \Leftrightarrow x \sqsubseteq a'. \end{aligned}$$

Аналогично $b \sqcap x' = 0 \Leftrightarrow b \sqsubseteq x$. Справедливость формулы для x с использованием произвольного элемента B следует из

$$\left\{ \begin{array}{l} b \sqsubseteq x \\ x \sqsubseteq a' \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x = b \sqcup u \text{ для некоторого } u \in B \\ x \sqcap a' = x \end{array} \right\} \Leftrightarrow x = (b \sqcup u) \sqcap a'.$$

Вторая форма представления x следует из первой по модулярности.

Глава 6

Алгебраические системы

Теория универсальных алгебр уже оказывает и, нужно ожидать, ближайшее десятилетия будет оказывать всё возрастающее влияние на развитие всей общей алгебры.

А.Г. Курош. Курс общей алгебры.

6.1 Основные определения. Модели и алгебры

Мы уже пользовались одним из основных понятий современной математики — понятием алгебраической системы (АС). Неформально, АС — множество с определёнными на нём операциями и отношениями. Для формального задания АС \mathfrak{A} определим составляющие её элементы.

Пусть Op и Rel — некоторые непустые одновременно и не имеющие общих элементов совокупности символов произвольных операций и отношений соответственно. Если оба указанных множества конечны, то соответствующая алгебраическая система называется АС *конечного типа*. Мы будем рассматривать только такие системы. Мощности множеств Op и Rel обозначим N и M соответственно.

(Абстрактная) *сигнатура* σ есть упорядоченная пара $\langle Op, Rel \rangle$, символически $\sigma = sgnt \mathfrak{A}$. Если $Rel = \emptyset$, то АС называют (*универсальной*) *алгеброй*, а если $Op = \emptyset$ — то *реляционной системой* или *моделью*.

Каждому элементу $f_i \in Op$ сопоставлено натуральное число $n_i \geq 0$, $i = \overline{1, N}$, а элементу $r_j \in Rel$ — целое число $m_j > 0$, $j = \overline{1, M}$, выражающее «местность» или «арность» соответствующего функционального или предикатного символа.

Будем считать, что операции с ненулевыми арностями имеют номера с 1 по $N' \leq N$. Местности сигнатурных символов записывают в виде кортежа

$$\tau = \langle n_1, \dots, n_{N'}; m_1, \dots, m_M; 0, \dots, 0 \rangle,$$

который называют *типом АС*. Если оговаривают, что задается алгебра или модель, то их типы записывают, перечисляя арности лишь элементов из Op или, соответственно, из Rel .

При задании типа, последовательности арностей $n_1, \dots, n_{N'}$ и m_1, \dots, m_M принято упорядочивать так, чтобы они оказались невозрастающими. Задавая сигнатуру, её элементы перечисляют в соответствии с выбранной упорядоченностью. Если необходимо явно указывать арности элементов, их записывают в качестве верхних индексов: $f_i^{n_i}$, $i = \overline{1, N'}$, $r_j^{m_j}$, $j = \overline{1, M}$.

Рассмотрим теперь не имеющее общих элементов с Op и Rel непустое множество A . Оно будет называться *носителем* или *основным множеством* АС \mathfrak{A} , символически $A = Supp \mathfrak{A}$. Если A — конечно, то соответствующая алгебраическая система называется *конечной*.

Совокупности всех операций и отношений, которые можно определить на A будем обозначать $Op A$ и $Rel A$ соответственно. Понятно, что это — очень мощные множества, состоящие из большого числа элементов, даже если A — конечное множество небольшой мощности.

Определим далее понятие интерпретации данной абстрактной сигнатуры. *Интерпретация* ω есть пара функций $\langle \omega_1, \omega_2 \rangle$,

$$\omega_1 : Op \rightarrow \mathbf{Op} A \quad \text{и} \quad \omega_2 : Rel \rightarrow \mathbf{Rel} A,$$

сопоставляющих каждому символу из Op и Rel соответственно конкретные операции или отношения на A той же арности.

Окончательно, алгебраическая система \mathfrak{A} есть пятёрка

$$\mathfrak{A} = \langle A, Op, Rel, \omega_1, \omega_2 \rangle.$$

Образами интерпретации являются совокупности функций $Op A \subseteq \mathbf{Op} A$ и предикатов $Rel A \subseteq \mathbf{Rel} A$ на множестве A . Алгебраические системы с одинаковыми абстрактными сигнатурами называют *однотипными*. Однотипные АС различаются носителями и интерпретациями. Операции и отношения однотипных АС, являющиеся образами разных интерпретаций соответствующих символов сигнатуры называют *одноимёнными*.

При работе с конкретными АС их записывают короче, либо в общем виде как

$$\mathfrak{A} = \langle A, Op A, Rel A \rangle,$$

либо перечислением конкретных операций и отношений

$$\mathfrak{A} = \langle A, f_1^{n_1}, \dots, f_{N'}^{n_{N'}}, r_1^{m_1}, \dots, r_{M'}^{m_{M'}}, 0, \dots, 0 \rangle.$$

Элементы $Op A$ ненулевой арности называют *главными операциями*, элементы $Rel A$ — *главными отношениями*, а элементы $Op A$ нулевой арности — *главными элементами* АС. Элемент носителя A , отмечаемый нульарной операцией f_i^0 будем обозначать $f_i^0(A^0)$, опуская, возможно верхний и нижний индексы у символа функции. Пару $\langle Op A, Rel A \rangle$ будем называть сигнатурой на множестве A и обозначать σ_A .

Приведём примеры [29] алгебраических систем.

Пример 6.1. Для сигнатуры $\sigma = \langle f_1, f_2, f_3, r_1, c_1, c_2 \rangle$ типа $\langle 2, 2, 1; 2; 0, 0 \rangle$ построим различные однотипные АС, выбирая различные носители и по-разному задавая интерпретацию символов сигнатуры σ .

\mathfrak{A}_1 : $\text{supp } \mathfrak{A}_1 = \mathbb{N}_0$, а элементы сигнатуры интерпретируются (с переходом к инфиксной записи) следующим образом:

$$f_1 \mapsto +, \quad f_2 \mapsto \cdot, \quad f_3(n) = n + 1, \quad r \mapsto \leq, \quad c_1 \mapsto 0, \quad c_2 \mapsto 1.$$

Ясно, что такая АС описывает арифметику неотрицательных целых чисел.

\mathfrak{A}_2 : $\text{supp } \mathfrak{A}_2 = \text{supp } \mathfrak{A}_1$, но сигнатурные символы интерпретируются по-другому:

$$f_1 \mapsto 0, \quad f_2(m, n) = m^n, \quad f_3(n) = 2n, \\ r(m, n) \mapsto m \text{ и } n \text{ взаимно просты}, \quad c_1 \mapsto 1, \quad c_2 \mapsto 1.$$

Эта экзотичная АС не имеет специального названия.

\mathfrak{A}_3 : $\text{supp } \mathfrak{A}_3 = \mathcal{P}(A)$. Сигнатурные символы будем трактовать следующим образом:

$$f_1 \mapsto \cup, \quad f_2 \mapsto \cap, \quad f_3 \mapsto \bar{}, \quad r \mapsto \subseteq, \quad c_1 \mapsto \emptyset, \quad c_2 \mapsto A.$$

Ясно, что мы получили тотальную булеву структуру множеств.

\mathfrak{A}_4 : Носитель АС \mathfrak{A}_4 есть множество V всех векторов \vec{x} трёхмерного пространства, а сигнатурные символы интерпретируются так:

$$f_1(\vec{a}, \vec{b}) = \vec{a} + \vec{b}, \quad f_2(\vec{a}, \vec{b}) = \vec{a} \times \vec{b}, \quad f_3(\vec{a}) = -\vec{a}$$

$$r(\vec{a}, \vec{b}) \mapsto \langle \text{вектор } \vec{a} \text{ коллинеарен вектору } \vec{b} \rangle, \quad c_1, c_2 \mapsto \vec{0}.$$

До линейного трёхмерного пространства этой АС недостаёт требования возможности умножения векторов из V на элементы некоторого поля с выполнением законов унитарности, ассоциативности и дистрибутивности (см. с. 158).

Операции и отношения во всех приведённых примерах, соответствующие сигнатурным символам f_1, f_2, f_3 и r_1 будут одноимёнными. Везде мы предполагали, что введенные операции и отношения имеют обычный математический смысл.

Приведём примеры конкретных алгебраических систем различной сигнатуры.

Пример 6.2. 1. АС $\langle A, f \rangle$, где f — одноместная операция на множестве A называется *унаром*.

2. Поле действительных чисел $\langle \mathbb{R}, +, \cdot, -, 0, 1 \rangle$ есть алгебра типа $\langle 2, 2, 1, 0, 0 \rangle$. Заметим, что кортеж $\langle +, \cdot, -, {}^{-1}, 0, 1 \rangle$ нельзя рассматривать как сигнатуру поля, т.к. операция ${}^{-1}$ не определена для нуля.

Кольцо K с единицей есть алгебра сигнатуры $\sigma = \langle \cdot, +, -, 0, 1 \rangle$ типа $\langle 2, 2, 1, 0, 0 \rangle$.

Группа есть алгебра типа $\langle 2, 1, 0 \rangle$ сигнатуры $\sigma = \langle \circ, {}^{-1}, e \rangle$.

3. *Частично предпорядоченное множество* $\langle P, \leq \rangle$, где \leq — символ предпорядка есть модель типа $\langle 2 \rangle$.

4. Если одна АС может быть получена из другой удалением некоторых операций, отношений или констант, то первая АС называется *редуктом* второй.

Во всех приведённых выше примерах считалось, что приведённые операции и отношения обладают известными свойствами. В общем случае эти свойства необходимо задавать.

Совокупность АС фиксированной сигнатуры называется *классом* алгебраических систем. Класс \mathfrak{M} АС сигнатуры σ называется *многообразием*, если существует множество Σ тождеств сигнатуры σ такое, что АС сигнатуры σ принадлежит классу \mathfrak{M} если и только если в ней выполняются все тождества Σ . Совокупность тождеств Σ называют *аксиоматикой* данного класса.

Пример 6.3. 1. Булевы алгебры — многообразие сигнатуры $\langle \sqcup, \sqcap, ', 0, 1 \rangle$ типа $\langle 2, 2, 1, 0, 0 \rangle$, определяемой системой аксиом, приведённой в определении 1.1.

2. Полугруппы — это многообразия сигнатуры, состоящей из единственной бинарной операции \circ , удовлетворяющие тождеству $(x \circ y) \circ z = x \circ (y \circ z)$.

3. Ассоциативно-коммутативные кольца с единицей — это многообразия сигнатуры $\langle +, \cdot, -, 0, 1 \rangle$ типа $\langle 2, 2, 1, 0, 0 \rangle$ удовлетворяющие следующим тождествам Σ (знак \cdot опускаем):

$$\begin{aligned} (x + y) + z &= x + (y + z); & x + 0 &= 0 + x = x; \\ x + (-x) &= 0; & x + y &= y + x; \\ (x + y)z &= xz + yz; & x(y + z) &= xy + xz; \\ (xy)z &= x(yz); & x1 &= 1x = x; \\ xy &= yx. \end{aligned}$$

Отметим, что произвольной алгебре можно сопоставить адекватную ей модель, если каждую n -местную операцию f^n заменить на такое $(n + 1)$ -местное отношение r^{n+1} , что $r^{n+1}(x_1, \dots, x_n, y) \Leftrightarrow f^n(x_1, \dots, x_n) = y$. Такая модель называется *представляющей*.

Пример 6.4. Пусть задана группа $\langle \mathbb{Z}, +, -, 0 \rangle$. Если

$$r_1^3(m, n, k) \equiv (m + n = k), \quad r_2^2(m, n) \equiv (m = -n), \quad r_3^1(n) \equiv (n = 0),$$

то $\langle \mathbb{Z}, r_1^3, r_2^2, r_3^1 \rangle$ будет представляющей моделью для данной группы.

6.2 Подсистемы. Прямое произведение АС

Напомним, что множество X называется *устойчивым относительно отображения* $f: X^n \rightarrow X$, если $f(x_1, \dots, x_n) \in X$. Пусть $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$ — алгебраическая система и $\emptyset \neq B \subseteq A$. Назовём множество B *устойчивым относительно операций* из $\text{Op } A$, если оно устойчиво относительно сужений на B каждой операции из $\text{Op } A$.

Определение 6.1. Пусть $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$ — АС, $\emptyset \neq B \subseteq A$, а $\text{Op } B$ и $\text{Rel } B$ — совокупности сужений на B операций из $\text{Op } A$ и отношений из $\text{Rel } A$ соответственно. Если множество B устойчиво относительно всех операций из $\text{Op } A$, то АС $\mathfrak{B} = \langle B, \text{Op } B, \text{Rel } B \rangle$ называется *подсистемой* \mathfrak{A} (символически $\mathfrak{B} \leq \mathfrak{A}$).

Подсистему алгебры называют *подалгеброй*, а подсистему модели — *подмоделью*. Если $B \subset A$, то соответствующую подсистему называют *собственной* (символически $\mathfrak{B} < \mathfrak{A}$).

Ясно, что любое подмножество носителя определяет подмодель, но не любое — подалгебру. Для последнего требуется устойчивость подмножества относительно всех операций сигнатуры, в том числе и нульварных, т.е. подсистема должна содержать все главные элементы исходной системы, если таковые имеются.

Пример 6.5. 1. Поле рациональных чисел есть подалгебра поля действительных чисел (см. пример 6.2).

2. Если множество A — собственное подмножество множества B , то алгебра множеств $\mathcal{P}(A)$ не является подалгеброй $\mathcal{P}(B)$, поскольку такое сужение не сохраняет в $\mathcal{P}(A)$ единицу B из $\mathcal{P}(B)$.

3. Пусть F — множество дифференцируемых действительных функций. Тогда унар $\langle F, \frac{d}{dx} \rangle$, где $\frac{d}{dx}$ — оператор дифференцирования, есть алгебра. Множество полиномиальных функций будет её подалгеброй.

Заметим, что АС, носителем которой является множество функций, называют *функциональной системой*.

4. При любом натуральном n унар $\langle \mathbb{Z}, + \rangle$ содержит подалгебру $\langle n\mathbb{Z}, + \rangle$.

5. Подалгебрами циклической группы $\mathbb{Z}_6 = \langle \{0, 1, \dots, 5\}, +_6 \rangle$ будут подгруппы $\{0\} = E$, $\{0, 3\} \cong \mathbb{Z}_2$, $\{0, 2, 4\} \cong \mathbb{Z}_3$ и сама \mathbb{Z}_6 .

Совокупность всех подсистем АС \mathfrak{A} будем обозначать $\text{Sub } \mathfrak{A}$. Ясно, что это ч.у. множество, упорядоченное по включению (носителей подсистем).

Теорема 6.1. Пусть \mathfrak{A} — АС, I — произвольное множество индексов и $\{\mathfrak{A}_i\}_{i \in I}$ — некоторая совокупность её подсистем. Тогда $\bigcap_{i \in I} \mathfrak{A}_i$ либо пусто, либо является подсистемой.

Доказательство. Достаточно заметить, что пересечение носителей всех подсистем, если оно не пусто, устойчиво относительно всех операций любой подсистемы. \square

Следствие. Если АС \mathfrak{A} имеет главные элементы, то пересечение всех её подсистем непусто.

Справедливость данного следствия вытекает из условия принадлежности главных элементов АС \mathfrak{A} любой её подсистеме.

Наименьшую подсистему АС, в случае её существования, называют её *главной подсистемой*. Например, кольцо целых чисел $\langle \mathbb{Z}, +, \cdot, 0 \rangle$ и ч.у. множество $\langle \mathbb{Z}, \leq \rangle$ наименьших подсистем, очевидно, не имеют.

Пусть дана АС $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$ и $B \subseteq A$. Обозначим через $\mathfrak{B} = [B]$ пересечение всех подсистем из $\text{Sub } \mathfrak{A}$, содержащих B . \mathfrak{B} называют *подсистемой, порождённой множеством B* , а элементы B — *порождающими элементами*. АС \mathfrak{B} мы также будем записывать для простоты в виде $\mathfrak{B} = \langle [B], \text{Op } A, \text{Rel } A \rangle$, подразумевая здесь под $\text{Op } A$ и $\text{Rel } A$ соответствующие сужения операций и отношений. Если B — конечное множество, то \mathfrak{B} есть *конечнопорождённая система*. При $B = \{b\}$, то вместо $[\{b\}]$ пишут $[b]$.

Пример 6.6. 1. Подкольцо чётных кольца целых чисел порождается элементом 2.

2. Пусть $\mathfrak{A} = \langle \{a_1, a_1, \dots, a_n\}, f \rangle$ — унар, где $f(a_i) = a_{i+1}$ для $i = 1, 2, \dots, n-1$ и $f(a_n) = a_0$. Тогда \mathfrak{A} порождается любым элементом своего носителя.

3. $\langle \mathbb{N}, + \rangle = [1]$.

4. АС $\langle \mathbb{N}, \cdot \rangle$ не есть конечнопорождённая алгебра.

Итак, непустое пересечение подсистем АС всегда является её подсистемой. Поэтому часто для удобства рассматривают *пустую АС* — с пустым носителем и пустой сигнатурой, и тогда пересечение любых подсистем АС будет подсистемой.

Объединение подсистем АС, вообще говоря, подсистемой не является, что показывает нижеследующий

Пример 6.7. $\langle n\mathbb{Z}, + \rangle$ и $\langle m\mathbb{Z}, + \rangle$ при любых целых n и m суть подсистемы $\langle \mathbb{Z}, + \rangle$, однако при некратных друг другу n и m множество $n\mathbb{Z} \cup m\mathbb{Z}$ неустойчиво по отношению к сложению, и в этом случае $\langle n\mathbb{Z} \cup m\mathbb{Z}, + \rangle$ даже не есть АС. Например, при $n = 6$ и $m = 10$ множество $\{0, \pm 6, \pm 10, \pm 12, \pm 20, \dots\}$ не содержит элемента $4 = 10 - 6$.

Ниже сформулировано условие, когда объединение подсистем будет являться подсистемой.

Определение 6.2. Совокупность S подмножеств A называется *локальной*, если любое конечное подмножество A содержится в некотором элементе S .

Примером локальной подсистемы множества \mathbb{R} является совокупность интервалов вида $(-n, n)$, $n \in \mathbb{N}$.

Теорема 6.2 (об объединении подсистем АС). Пусть $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$ — алгебраическая система и $\{A_i \subseteq A \mid i \in I\}$ — локальная совокупность подмножеств её носителя A . Тогда $\langle \bigcup_{i \in I} A_i, \text{Op } A, \text{Rel } A \rangle \leq \mathfrak{A}$.

Доказательство. Надо показать устойчивость множества $U = \bigcup_{i \in I} A_i$ относительно операций из $\text{Op } A$. Рассмотрим произвольную n -местную операцию f из $\text{Op } A$. Для произвольного набора $(a_1, \dots, a_n) = a$ имеем: с одной стороны, $a \in U$, а с другой — найдется такое множество $A_i \subseteq U$, что $\{a \cup f(a)\} \in A_i$. Это означает, что U устойчиво относительно f . \square

Таким образом, устойчивость на объединении элементов локальной совокупности следует из того, что операции определены над конечным множеством аргументов.

Выше мы отмечали, что совокупность $\text{Sub } \mathfrak{A}$ всех подсистем АС \mathfrak{A} есть ч.у. множество. Более того, оно решёточно упорядочено, если для АС без главных элементов пустое множество считать устойчивым относительно произвольных операций. Тогда пересечение подсистем всегда есть подсистема (возможно пустая), и для $\mathfrak{A}_1, \mathfrak{A}_2 \in \mathfrak{A}$ можно положить $\inf \{\mathfrak{A}_1, \mathfrak{A}_2\} = \mathfrak{A}_1 \cap \mathfrak{A}_2$. Положим $\sup \{\mathfrak{A}_1, \mathfrak{A}_2\} = [\mathfrak{A}_1 \cup \mathfrak{A}_2]$. Поскольку кольцо множеств — полная решётка, то и $\text{Sub } \mathfrak{A}$ оказывается полной решёткой (см. с. 97).

Пример 6.8. Продолжая рассмотрение предыдущего примера укажем, что наименьшей подсистемой АС $\langle \mathbb{Z}, + \rangle$, содержащей её подсистемы $\langle n\mathbb{Z}, + \rangle$ и $\langle m\mathbb{Z}, + \rangle$ будет $\langle [m \wedge n], + \rangle$. Например, для $\langle 6\mathbb{Z}, + \rangle$ и $\langle 10\mathbb{Z}, + \rangle$ это $\langle 2\mathbb{Z}, + \rangle$.

Для двух однотипных АС \mathfrak{A}_1 и \mathfrak{A}_2 абстрактной сигнатуры σ с носителями A_1 и A_2 соответственно определяют *прямое произведение* $\mathfrak{A} = \mathfrak{A}_1 \times \mathfrak{A}_2$, также являющееся АС. Сигнатура АС \mathfrak{A} будет состоять из такого же числа тех же символов операций и отношений, что и σ , но их местности удваиваются. Пусть f_1 и f_2 — одноимённые операции, а r_1 и r_2 — одноимённые отношения из \mathfrak{A}_1 и \mathfrak{A}_2 соответственно. Соответствующие им операция f^\times и отношение r^\times в АС $\mathfrak{A}_1 \times \mathfrak{A}_2$ определяются как

$$f^\times(a, b) = (f_1(a), f_2(b)) \quad \text{и} \quad r^\times(a, b) = r_1(a) \& r_2(b).$$

Здесь a и b — произвольные наборы элементов из A_1 и A_2 соответственно длины n (для операций) или m (для отношений). Если c_1 и c_2 — главные одноимённые элементы из \mathfrak{A}_1 и \mathfrak{A}_2 соответственно, то

$$c^\times = (c_1, c_2)$$

— главный элемент из $\mathfrak{A}_1 \times \mathfrak{A}_2$.

Пример 6.9. 1. $\langle \mathbb{Z}_2, + \rangle \times \langle \mathbb{Z}_3, + \rangle$ состоит из шести элементов $(0, 0)$, $(0, 1)$, $(0, 2)$, $(1, 0)$, $(1, 1)$, $(1, 2)$. При этом, например, $(1, 1) + (1, 1) = (0, 2)$.

2. Рассмотрим две однотипные АС сигнатуры $\langle 2, 2, 0 \rangle$: $\mathfrak{A} = \langle \{0, 1, 2\}, +_3, \leq, 0 \rangle$ и $\mathfrak{B} = \langle \{0, 1\}, \max, <, 1 \rangle$, где \max — операция взятия максимального из двух чисел, а отношения \leq и $<$ понимаются в обычном смысле. Тогда

$$\mathfrak{A} \times \mathfrak{B} = \langle \{ (0, 0), (0, 1), (1, 0), (1, 1), (2, 0), (2, 1) \}, *, \leq, (0, 1) \rangle,$$

где бинарная операция $*$ и отношение \leq определены как

$$\begin{aligned} (a_1, b_1) * (a_2, b_2) &= ((a_1 +_3 a_2), \max \{b_1, b_2\}), \\ (a_1, b_1) \leq (a_2, b_2) &= (a_1 \leq a_2) \& (b_1 < b_2), \end{aligned}$$

где $a_1, a_2 \in \{0, 1, 2\}$, $b_1, b_2 \in \{0, 1\}$, а $(0, 1)$ — единица АС $\mathfrak{A} \times \mathfrak{B}$.

3. Прямое произведение булевых алгебр есть булева алгебра.

Ясно, что определено и прямое произведение любого конечного числа однотипных систем. Прямое произведение k АС \mathfrak{A} обозначают \mathfrak{A}^k .

6.3 Гомоморфизмы АС

Определение 6.3. Пусть $\langle A, Op A, Rel A \rangle$ и $\langle B, Op B, Rel B \rangle$ — две однотипные АС, а $f \in Op A$ и $f' \in Op B$ — пара одноимённых операций местности n . Тогда говорят, что отображение $\varphi: A \rightarrow B$ согласованно с данными операциями, если

$$\varphi(f(a_1, \dots, a_n)) = f'(\varphi(a_1), \dots, \varphi(a_n)) \quad \text{и} \quad \varphi(f(A^0)) = f'(\varphi(A^0)) \quad (6.1)$$

для $n > 0$ и при произвольных $a_1, \dots, a_n \in A$ и $n = 0$ соответственно.

Пример 6.10. Для алгебр $\langle \mathbb{R} \setminus \{0\}, \cdot \rangle$ и $\langle \mathbb{R}, + \rangle$ отображение $\varphi_a(x) = \log_a |x|$ при любом действительном $a > 0$, $a \neq 1$ согласованно с операциями \cdot и $+$ данных АС.

Если отображение φ окажется согласованным со всеми парами одноимённых операций двух АС, то будем говорить, что φ согласованно с операциями этих АС.

Определение 6.4. Пусть $\langle A, Op A, Rel A \rangle$ и $\langle B, Op B, Rel B \rangle$ — две однотипные АС, а $r \in Rel A$ и $r' \in Rel B$ — пара одноимённых отношений арности m . Тогда говорят, что отображение $\varphi: A \rightarrow B$ соответственно

- 1) *согласованно с данными отношениями*, если

$$r(a_1, \dots, a_m) \supset r'(\varphi(a_1), \dots, \varphi(a_m)); \quad (6.2)$$

- 2) *сильно согласованно с данными отношениями*, если

$$\begin{aligned} r'(\varphi(a_1), \dots, \varphi(a_m)) &\Rightarrow \\ &\Rightarrow \exists_A x_1, \dots, x_m [(\varphi(a_k) = \varphi(x_k), k = \overline{1, m}) \& r(x_1, \dots, x_m)]; \end{aligned} \quad (6.3)$$

- 3) *полностью (или тождественно) согласованно с данными отношениями*, если

$$r(a_1, \dots, a_m) \equiv r'(\varphi(a_1), \dots, \varphi(a_m)).$$

Если отображение φ окажется (сильно, тождественно) согласованным со всеми парами одноимённых отношений двух АС, то будем говорить, что φ (*сильно, тождественно*) *согласованно с отношениями* этих однотипных АС.

Пример 6.11. Рассмотрим две модели типа $\langle 1 \rangle$: $\langle \{a_1, a_2\}, r \rangle$ и $\langle \{b\}, r' \rangle$. Отображение φ из A на B (единственное возможное) задаётся равенствами $\varphi(a_1) = \varphi(a_2) = b$. Пусть $r'(b) = \mathbf{1}$. Тогда

- 1) если $r(a_1) = r(a_2) = \mathbf{0}$, то φ согласованно,
- 2) если $r(a_1) = \mathbf{1}$ и $r(a_2) = \mathbf{0}$, то φ сильно согласованно,
- 3) если $r(a_1) = r(a_2) = \mathbf{1}$, то φ тождественно согласованно

с парой (r, r') одноимённых отношений рассматриваемых моделей.

Определение 6.5. Пусть \mathfrak{A} и \mathfrak{B} — две однотипные АС. Тогда отображение $\varphi: A \rightarrow B$, согласованное с операциями этих АС называется соответственно

- 1) *гомоморфизмом из \mathfrak{A} в \mathfrak{B}* , если φ согласованно;
- 2) *взаимно-однозначным (или биективным) гомоморфизмом между \mathfrak{A} и \mathfrak{B}* , если φ — биекция, согласованная;
- 3) *сильным гомоморфизмом из \mathfrak{A} в \mathfrak{B}* , если φ сильно согласованно;
- 4) *изоморфизмом между \mathfrak{A} и \mathfrak{B}* , если φ — биекция, полностью согласованная

с отношениями этих АС.

Вместо термина «сильный» для гомоморфизма иногда употребляют термин *строгий*. Для алгебр понятие сильного гомоморфизма отсутствует, а взаимно-однозначный гомоморфизм всегда есть изоморфизм. АС \mathfrak{A} и \mathfrak{B} называют изоморфными, если существует изоморфизм между \mathfrak{A} и \mathfrak{B} , что записывают как $\mathfrak{A} \cong \mathfrak{B}$.

Пример 6.12. 1. Модель $\mathfrak{A} = \langle \mathbb{Z}, < \rangle$ не изоморфна, а лишь биективно гомоморфна модели $\mathfrak{B} = \langle 2\mathbb{Z}, \leq \rangle$: отображение $\varphi(n) = 2n$ есть взаимно-однозначный гомоморфизм из \mathfrak{A} в \mathfrak{B} . Он не сильный, поскольку отображение φ согласованно, но не тождественно согласованно с отношениями $<$ и \leq .

2. Для декартова произведения $\mathfrak{A} \times \mathfrak{B}$ алгебраических систем \mathfrak{A} и \mathfrak{B} определены отображения $\pi_1(a, b) = a$ и $\pi_2(a, b) = b$ из $\mathfrak{A} \times \mathfrak{B}$ на \mathfrak{A} и \mathfrak{B} соответственно. Из определения декартова произведения непосредственно видно, что π_1 и π_2 суть сильные гомоморфизмы.
3. $\langle \mathbb{Z}, \leq \rangle \cong \langle 2\mathbb{Z}, \leq \rangle$ и $\mathbb{Z}_2^2 \cong V_4$.

Замечание. Отметим важное свойство сильных гомоморфизмов, которое нам понадобится в дальнейшем. Соотношение (6.3) позволяет утверждать, что если (в введённых обозначениях) справедливо $r'(\varphi(a_1), \dots, \varphi(a_m))$, то в A найдутся такие x_1, \dots, x_m из ядра $\varphi^\#(0)$, что справедливо $r(x_1, \dots, x_m)$, и, таким образом, $r'(\varphi(a_1), \dots, \varphi(a_n)) \supset r(x_1, \dots, x_m)$. Можно сказать, что мы сохранили истинность на некотором подмножестве элементов, связанных отношением r' , переходя от него к одноимённому отношению r “при движении против отображения φ ”.

То, что φ — гомоморфизм из \mathfrak{A} в \mathfrak{B} записывают как $\varphi \in \text{Hom}(\mathfrak{A}, \mathfrak{B})$. Следующая теорема утверждает, что гомоморфные как образ, так и прообраз подсистем AC также суть подсистемы (соответствующих систем).

Теорема 6.3. Пусть $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$, $\mathfrak{B} = \langle B, \text{Op } B, \text{Rel } B \rangle$ — две однотипные AC, $\mathfrak{A}' \leq \mathfrak{A}$ и $\mathfrak{B}' \leq \mathfrak{B}$ (A' и B' — носители \mathfrak{A}' и \mathfrak{B}' соответственно) и $\varphi \in \text{Hom}(\mathfrak{A}, \mathfrak{B})$. Тогда $\text{Im } \varphi(A') \leq \mathfrak{B}$ и $\text{Im } \varphi^{-1}(B') \leq \mathfrak{A}$.

Доказательство. Нужно показать устойчивость главных операций и главных элементов из \mathfrak{A}' и \mathfrak{B}' на образе и прообразе φ соответственно.

Устойчивость главных элементов AC относительно гомоморфизмов и взятий подсистем очевидна. Рассмотрим теперь пару f, f' одноимённых операций местности $n > 0$ из $\text{Op } A$ и $\text{Op } B$ соответственно.

Пусть b_1, \dots, b_n — произвольные элементы из $\varphi(A')$. Тогда $\varphi(a_i) = b_i$ для некоторых $a_i \in A, i = \overline{1, n}$ и

$$f'(b_1, \dots, b_n) = f'(\varphi(a_1), \dots, \varphi(a_n)) = \varphi(f(a_1, \dots, a_n)) \in \varphi(A'),$$

поскольку $f(a_1, \dots, a_n) \in A'$ в силу устойчивости A' . Следовательно, подмножество $\varphi(A')$ устойчиво в AC B .

Если же a_1, \dots, a_n — произвольные элементы из $\varphi^{-1}(B')$, то $\varphi(a_i) \in B', i = \overline{1, n}$ и тогда

$$\varphi(f(a_1, \dots, a_n)) = f'(\varphi(a_1), \dots, \varphi(a_n)) \in \varphi(B'),$$

откуда $f(a_1, \dots, a_n) \in \varphi^{-1}(B')$ и, значит, $\varphi^{-1}(B')$ устойчиво в A . \square

Легко показывается, что если преобразование, обратное изоморфизму, есть изоморфизм и композиция гомоморфизмов [изоморфизмов] есть гомоморфизм [изоморфизм]. Также ясно, что отношение изоморфизма есть отношение эквивалентности на множестве алгебраических систем и, следовательно, все алгебраические системы распадаются на классы эквивалентности, содержащие изоморфные системы. Обычно изучают свойства алгебраической системы с точностью до изоморфизма. Такие свойства называют *абстрактными*.

Сюръективный гомоморфизм AC называют *эпиморфизмом*, а инъективный гомоморфизм — *мономорфизмом*¹, т.е. так же, как и соответствующее отображения. Гомоморфизм AC в себя называется *эндоморфизмом*. Изоморфизм AC на себя называют *автоморфизмом*. С каждой AC \mathfrak{A} связаны решётка подсистем $\text{Sub } \mathfrak{A}$, моноид эндоморфизмов $\text{End } \mathfrak{A}$ и группа автоморфизмов $\text{Aut } \mathfrak{A}$ (группа обратимых элементов моноида $\text{End } \mathfrak{A}$).

Класс алгебраических систем называется *абстрактным*, если вместе с каждой AC в нём лежат все системы, ей изоморфные. Для алгебр справедлива

Теорема 6.4 (Биркгоф). Класс алгебр является многообразием, если и только если он замкнут относительно взятия подалгебр, прямых произведений и гомоморфных образов.

¹Заметим, что в теории категорий термины «эпиморфизм» и «мономорфизм» имеют другие определения и, как следствие, несколько иные свойства. В частности, категорные эпиморфизмы не обязательно являются сюръективными гомоморфизмами.

Следующий факт часто используется на практике.

Теорема 6.5. *Всякий сюръективный эндоморфизм конечной системы есть изоморфизм.*

Доказательство. Рассмотрим АС $\langle A, Op A, Rel A \rangle$ с конечным носителем A и её сюръективный эндоморфизм φ . Пусть r — произвольное отношение арности m из $Rel A$. Поскольку φ — гомоморфизм, то для любого набора a_1, \dots, a_m из m элементов носителя A истина импликация $r(a_1, \dots, a_m) \supset r(\varphi(a_1), \dots, \varphi(a_m))$, т.е. для её посылки и заключения могут иметь место только следующие пары истинностных значений посылки и заключения: $(\mathbf{0}, \mathbf{0})$, $(\mathbf{0}, \mathbf{1})$, $(\mathbf{1}, \mathbf{1})$. Теорема будет доказана, если выяснится, что второй случай в наших условиях не реализуется.

Наложение множества на себя является биекцией и, в силу конечности A , перестановкой его элементов конечной степени. Тогда существует натуральное t такое, что φ^t есть тождественная перестановка. Пусть отношение $r(\varphi(a_1), \dots, \varphi(a_m))$ выполнено. Отсюда следует, что, поскольку φ — гомоморфизм, для любого натурального k выполнено $r(\varphi^k(a_1), \dots, \varphi^k(a_m))$. При $k = t$ получаем, что выполнено и $r(a_1, \dots, a_m)$. Таким образом, $r(\varphi(a_1), \dots, \varphi(a_m)) \supset r(a_1, \dots, a_m)$, и случай $(\mathbf{0}, \mathbf{1})$ невозможен.

В силу произвольности r мы показали тождественную согласованность φ со всеми отношениями из $Rel A$. \square

6.4 Конгруэнции и факторсистемы

Напомним, что однородное множество A отношение ρ стабильно относительно операции $f : A^n \rightarrow A$, если при $n > 0$ из $a_i \rho a_i'$, $i = \overline{1, n}$ для всех $a_1, a_1', \dots, a_n, a_n' \in A$ следует, что $f(a_1, \dots, a_n) \rho f(a_1', \dots, a_n')$, а при $n > 0$ — ρ рефлексивно (см. определение 2.7). Однородное отношение ρ на АС $\langle A, Op A, Rel A \rangle$ называется *стабильным* на этой АС, если оно стабильно относительно любой операции из $Op A$. Например, полное ∇ и диагональное Δ отношения стабильны на любой АС.

Определение 6.6. Стабильная на АС эквивалентность называется *конгруэнцией* на ней².

Ясно, что полное и диагональное отношения являются конгруэнциями на любой АС. Конгруэнция на АС \mathfrak{A} определяет подсистему АС \mathfrak{A}^2 . Совокупность всех конгруэнций $\text{Con } \mathfrak{A}$ есть ч.у. множество, упорядоченное по включению. $\text{Con } \mathfrak{A}$ имеет универсальные грани: это отмеченные выше диагональ (o) и аморфная конгруэнция (ι) .

Пример 6.13. В качестве АС \mathfrak{A} рассмотрим полугруппу $\langle \mathbb{Z}, \cdot \rangle$.

1. Отношение эквивалентности \equiv_2 (чётности) на множестве \mathbb{Z} есть конгруэнция на АС \mathfrak{A} . Действительно,

$$\begin{cases} k \equiv_2 m \\ l \equiv_2 n \end{cases} \Rightarrow kl \equiv_2 mn,$$

т.е. отношение \equiv_2 стабильно относительно операции умножения. Имеем $\mathfrak{A}^2 = \langle \mathbb{Z}^2, \cdot \rangle$, где $(k, l) \cdot (m, n) = (km, ln)$ и нетрудно видеть, что (для простоты указание на класс $\text{mod } 2$ опускаем)

$$\langle \{(0, 0), (0, 1), (1, 0), (1, 1)\}, \cdot \rangle \leq \mathfrak{A}^2.$$

2. Для конгруэнций \equiv_2 и \equiv_4 на АС \mathfrak{A} имеем $\equiv_4 \subseteq \equiv_2$, и вообще $\equiv_m \subseteq \equiv_n$, если $n \mid m$.

²Мы уже пользовались понятием конгруэнции на решётках — см. определение на с. 119

Нетрудно понять, что пересечение любого семейства конгруэнций само является конгруэнцией, притом наибольшей из всех, содержащихся в каждой из конгруэнций семейства. Из теоремы 4.2 следует, что ч.у. множество конгруэнций $\text{Con } \mathfrak{A}$ — полная решётка, называемая *решёткой конгруэнций* $AC \mathfrak{A}$. Понятно, что $\text{Con } \mathfrak{A} \subseteq \mathfrak{A}^2$. При этом можно показать, что для $\alpha, \beta \in \text{Con } \mathfrak{A}$ верно $\sup \{ \alpha, \beta \} = \{ \alpha, \beta \}^e \in \text{Con } \mathfrak{A}$ (ср. с п. 2 примера 4.2). Так же свойство $\{ \alpha, \beta \}^e = \alpha \cup \beta = \alpha \beta$ для перестановочных эквивалентностей α и β сохраняется и для конгруэнций AC .

Теорема 6.6. *Если на $AC \mathfrak{A}$ все конгруэнции перестановочны, то решётка $\text{Con } \mathfrak{A}$ модулярна.*

Доказательство. Пусть $\alpha, \beta, \gamma \in \text{Con } \mathfrak{A}$ и $\alpha \subseteq \beta$. Для того, чтобы в решётке конгруэнций выполнялся модулярный закон, достаточно показать, что справедливо включение

$$\alpha \subseteq \beta \Rightarrow \alpha \cup (\beta \cap \gamma) \supseteq \beta \cap (\alpha \cup \gamma),$$

обратное к неравенству полумодулярности.

Заменив объединение конгруэнций на их произведение, для произвольных подсистем A и B $AC \mathfrak{A}$ имеем

$$A(\beta \cap (\alpha \diamond \gamma))B \Leftrightarrow A\beta B \& \exists X (A\alpha X \& X\gamma B) \Leftrightarrow \exists X (A\beta B \& A\alpha X \& X\gamma B).$$

Здесь X — некоторая подсистема \mathfrak{A} .

Покажем теперь, что в данном случае $A\beta B$ можно заменить на $X\beta B$. Действительно,

$$A\alpha X \Rightarrow A\beta X \Leftrightarrow X\beta A$$

в силу симметричности конгруэнций. Вместе с $A\beta B$ это означает, что справедливо

$$X\beta A \& A\beta B \Rightarrow X\beta^2 B \Leftrightarrow X\beta B.$$

Таким образом,

$$\begin{aligned} \exists X (A\beta B \& A\alpha X \& X\gamma B) &\Rightarrow \exists X (A\alpha X \& X\beta B \& X\gamma B) \Leftrightarrow \\ &\Leftrightarrow \exists X (A\alpha X \& X(\beta \cap \gamma)B) \Leftrightarrow A(\alpha \diamond (\beta \cap \gamma))B, \end{aligned}$$

т.е. $\beta \cap (\alpha \cup \gamma) \subseteq \alpha \cup (\beta \cap \gamma)$. □

Пусть x, y — два различных элемента $AC \mathfrak{A}$. Наименьшая из конгруэнций, содержащих пару (x, y) , обозначается $\theta(x, y)$ и называется *главной конгруэнцией*, порождённой указанной парой. Таким образом,

$$\theta(x, y) \triangleq \bigcap_{(x, y) \in \alpha \in \text{Con } \mathfrak{A}} \alpha.$$

Роль главных конгруэнций раскрывает

Теорема 6.7. *Если $\alpha \in \text{Con } \mathfrak{A}$, то*

$$\alpha = \bigcup_{(x, y) \in \alpha} \theta(x, y).$$

Доказательство. 6.4

$$\bigcup_{(x,y) \in \alpha} \theta(x,y) = \bigcup_{(x,y) \in \alpha} \left(\bigcap_{(x,y) \in \alpha} \alpha \right) = \bigcap_{(x,y) \in \alpha} \left(\bigcup_{(x,y) \in \alpha} \alpha \right) = \bigcap_{(x,y) \in \alpha} \nabla = \alpha.$$

□

Таким образом, всякая конгруэнция α АС является теоретико-множественным объединением содержащихся в ней главных конгруэнций.

Теорема 6.8. *Ядро гомоморфизма АС есть конгруэнция на ней.*

Доказательство. Пусть φ — гомоморфное отображение АС с носителем A . Поскольку ядро $\varphi^\sharp(0)$ есть эквивалентность, нам достаточно показать его стабильность относительно операций данной АС.

Рассмотрим произвольную операцию f данной АС. Пусть местность f есть n .

Если $n > 0$, то возьмём $a_1, a_1', \dots, a_n, a_n' \in A$ такие, что $a_i(\text{Ker } \varphi) a_i'$, или иначе $\varphi(a_i) = \varphi(a_i')$ для всех $i = \overline{1, n}$. Поскольку φ — гомоморфизм, имеем:

$$\varphi(f(a_1, \dots, a_n)) = f'(\varphi(a_1), \dots, \varphi(a_n)) = f'(\varphi(a_1'), \dots, \varphi(a_n')) = \varphi(f(a_1', \dots, a_n')),$$

т.е. $f(a_1, \dots, a_n) (\text{Ker } \varphi) f(a_1', \dots, a_n')$.

Если $n = 0$, то заметим, что ядерная эквивалентность гомоморфизма — рефлексивное отношение, стабильное относительно нульместной операции по определению. □

Пусть на АС $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$ задана конгруэнция α . Тогда результаты операций из $\text{Op } A$ не изменяются при замене элемента a на какой-либо другой из класса эквивалентности $[a]_\alpha$, что позволяет корректно определить на фактормножестве A/α одноимённые относительно $\text{sgnt } \mathfrak{A}$ операции и отношения.

Операция f^* на A/α , одноимённая операции $f \in \text{Op } A$ арности n , задаётся равенством

$$f^*([a_1]_\alpha, \dots, [a_n]_\alpha) = [f(a_1, \dots, a_n)]_\alpha \quad (6.4)$$

при $n > 0$, а при $n = 0$ —

$$f^*((A/\alpha)^0) = [f(A^0)]_\alpha. \quad (6.5)$$

Отношение r^* , одноимённое отношению $r \in \text{Rel } A$ арности m , задаётся равенством

$$r^*([a_1]_\alpha, \dots, [a_m]_\alpha) = \exists_A x_1, \dots, x_m [(a_i \alpha x_i, i = \overline{1, m}) \& r(x_1, \dots, x_m)]. \quad (6.6)$$

Полученные множества операций и отношений на A/α будем обозначать $\text{Op}^* A/\alpha$ и $\text{Rel}^* A/\alpha$ соответственно. Таким образом, *факторсистема*

$$\mathfrak{A}/\alpha = \langle A/\alpha, \text{Op}^* A/\alpha, \text{Rel}^* A/\alpha \rangle$$

будет корректно определённой АС, однотипной с \mathfrak{A} . При этом ясно, что естественное отображение $\text{nat}(A, \alpha)$ в соответствии с (6.6) будет сильным гомоморфизмом из \mathfrak{A} в \mathfrak{A}/α и иметь α в качестве ядерной эквивалентности.

Замечание. Из сказанного следует, что теорема 6.8 допускает обращение: если α — конгруэнция на АС A , то естественное отображение $\text{nat}(A, \alpha)$ есть гомоморфизм (на её факторсистему).

Пример 6.14. 1. Для примера 6.13 имеем $\langle \mathbb{Z}/\equiv_2 \rangle = \langle \mathbb{Z}_2, \cdot \rangle$ и $\langle \mathbb{Z}/\equiv_4 \rangle = \langle \mathbb{Z}_4, \cdot \rangle$.

2. Для АС \mathfrak{A} имеем $\mathfrak{A}/\Delta \cong \mathfrak{A}$ и \mathfrak{A}/∇ — одноэлементная АС. В частности, для примера 6.13 имеем $\langle \mathbb{Z}/\Delta \rangle \cong \langle \mathbb{Z}, \cdot \rangle$ и $\langle \mathbb{Z}/\nabla \rangle \cong \langle \{[0]\}, \cdot \rangle$.

6.5 Теоремы о гомоморфизмах и изоморфизмах АС

Нижеследующая теорема описывает ситуацию, когда в качестве конгруэнции на АС берётся ядерная эквивалентность гомоморфизма.

Теорема 6.9 (о гомоморфизмах АС). Пусть φ — гомоморфизм из АС $\mathfrak{A} = \langle A, Op A, Rel A \rangle$ в (однотипную) АС $\mathfrak{B} = \langle B, Op B, Rel B \rangle$. Тогда

- 1) отображение ψ , задаваемое правилом $\psi([a]_{\text{Ker } \varphi}) = \varphi(a)$, есть биективный гомоморфизм из $\mathfrak{A}/\text{Ker } \varphi$ в $\text{Im } \varphi \leq \mathfrak{B}$;
- 2) если гомоморфизм φ сильный, то ψ — изоморфизм между $\mathfrak{A}/\text{Ker } \varphi$ и $\text{Im } \varphi$.

Доказательство. По теореме об основном свойстве отображений существует вложение $A/\text{Ker } \varphi \xrightarrow{\psi} B$ такое, что диаграмма

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \text{nat}(\text{Ker } \varphi) \searrow & & \nearrow \psi \\ & A/\text{Ker } \varphi & \end{array}$$

коммутативна. Это отображение задаётся правилом

$$\psi([a]_{\text{Ker } \varphi}) = \varphi(a). \quad (6.7)$$

Для доказательства утверждения 1) теоремы нам надо показать согласованность отображения ψ с операциями и отношениями АС $\mathfrak{A}/\text{Ker } \varphi$ и \mathfrak{B} .

Рассмотрим произвольную тройку одноимённых операций $f \in Op A$, $f' \in Op B$ и $f^* \in Op^* A/\text{Ker } \varphi$ местности n . При $n > 0$ имеем:

$$\begin{aligned} \psi(f^*([a_1], \dots, [a_n])) &\stackrel{(6.4)}{=} \psi([f(a_1, \dots, a_n)]) \stackrel{(6.7)}{=} \\ &= \varphi(f(a_1, \dots, a_n)) \stackrel{(6.1)}{=} f'(\varphi(a_1), \dots, \varphi(a_n)) \stackrel{(6.7)}{=} \\ &= f'(\psi([a_1]), \dots, \psi([a_n])) \end{aligned} \quad (6.8)$$

для любого набора элементов a_1, \dots, a_n из A , а при $n = 0$ —

$$\psi(f^*((A/\text{Ker } \varphi)^0)) \stackrel{(6.5)}{=} \psi([f(A^0)]) \stackrel{(6.7)}{=} \varphi(f(A^0)) \stackrel{(6.1)}{=} f'(\varphi(A^0)) = f'(\psi([A^0]))$$

(здесь все смежные классы — по эквивалентности $\text{Ker } \varphi$). Полученные равенства означают согласованность ψ с f^* и f' и — в силу их произвольности — со всеми операциями систем $\mathfrak{A}/\text{Ker } \varphi$ и \mathfrak{B} .

Теперь рассмотрим произвольную тройку одноимённых отношений $r \in Rel A$, $r' \in Rel B$ и $r^* \in Rel^* A/\text{Ker } \varphi$ арности m . Для любого набора элементов a_1, \dots, a_m из A имеем:

$$\begin{aligned} r^*([a_1], \dots, [a_m]) &\stackrel{(6.6)}{\Leftrightarrow} \exists_{\substack{x_1, \dots, x_m \\ A}} [(x_i(\text{Ker } \varphi)a_i, i = \overline{1, m}) \ \& \ r(x_1, \dots, x_m)] \stackrel{(6.2)}{\Rightarrow} \\ &\Rightarrow r'(\varphi(x_1), \dots, \varphi(x_m)) = r'(\varphi(a_1), \dots, \varphi(a_m)) \stackrel{(6.7)}{=} \\ &= r'(\psi([a_1]), \dots, \psi([a_m])) \end{aligned} \quad (6.9)$$

(все смежные классы — по эквивалентности $\text{Ker } \varphi$). Полученное равенство означает согласованность ψ с r^* и r' и — в силу их произвольности — со всеми отношениями систем $\mathfrak{A}/\text{Ker } \varphi$ и \mathfrak{B} .

Итак, показано, что ψ есть мономорфизм из $\mathfrak{A}/\text{Кег } \varphi$ в \mathfrak{B} и, следовательно, биективный гомоморфизм из $\mathfrak{A}/\text{Кег } \varphi$ в $\text{Im } \varphi$.

Для доказательства утверждения 2) теоремы заметим, что если гомоморфизм φ сильный, то следование $\stackrel{(6.2)}{\Rightarrow}$ в (6.9) можно обратить (см. замечание на с. 150) и, следовательно, заменить на \Leftrightarrow . В результате получим, что отображение ψ сильно согласованно с $r^* \in \text{Rel } A/\text{Кег } \varphi$ и $r' \in \text{Rel } B$ и отсюда — со всеми отношениями систем $\mathfrak{A}/\text{Кег } \varphi$ и $\text{Im } \varphi \subseteq \mathfrak{B}$. Поскольку отображение ψ биективно, то сильная согласованность означает согласованность тождественную и ψ — изоморфизм между $\mathfrak{A}/\text{Кег } \varphi$ и $\text{Im } \varphi$. \square

Теорема устанавливает, что если гомоморфизм φ — сильный, то $\text{Im } \varphi \cong \mathfrak{A}/\text{Кег } \varphi$ или, другими словами, образ сильного гомоморфизма АС изоморфен факторсистеме по его ядерной эквивалентности. С учётом замечания на с. 153, полученный результат можно переформулировать и так: совокупность всех сильно гомоморфных образов АС с точностью до изоморфизма совпадает с множеством всех факторсистем по различным конгруэнциям. Ясно, что для алгебр уточнение «сильного» в обоих случаях опускается.

Отметим, что теорема носит название «о гомоморфизмах АС», а наиболее сильное её утверждение говорит об их изоморфизме. Приведённое традиционное название связано с тем, что первоначально теорема была сформулирована для алгебр.

Пример 6.15. 1. Рассмотрим две однотипные алгебры — $\mathfrak{A} = \langle \mathbb{N}_0, + \rangle$ и $\mathfrak{B} = \langle \{+1, -1\}, \cdot \rangle$ и отображение φ носителя \mathfrak{A} на носитель \mathfrak{B} , задаваемое правилом $\varphi(n) = (-1)^n$. Имеем:

$$\varphi(m+n) = (-1)^{m+n} = (-1)^m \cdot (-1)^n = \varphi(m) \cdot \varphi(n),$$

т.е. φ — гомоморфизм из \mathfrak{A} в \mathfrak{B} .

Ядерная эквивалентность φ разбивает \mathbb{N}_0 на два смежных класса — чётных (включая 0) и нечётных чисел, т.е. $m(\text{Кег } \varphi)n \Leftrightarrow m \equiv_2 n$. Далее получим

$$\begin{aligned} \mathfrak{A}/\text{Кег } \varphi &= \langle \{[0], [1]\}, \oplus \rangle \stackrel{\psi}{\cong} \mathfrak{B}, \quad \text{где} \\ \psi([1]) &= \varphi(1) = -1, \quad \psi([0]) = \varphi(0) = +1. \end{aligned}$$

2. Пусть $\varphi: L \rightarrow L'$ — сюръективный гомоморфизм решётки L в решётку L' . Тогда по теореме о гомоморфизмах существует такой изоморфизм ψ решёток L' и $L/\text{Кег } \varphi$, что $\psi(\varphi(a)) = \pi(a)$ для всех $a \in L$, где π — естественный гомоморфизм решётки L на её факторрешётку $L/\text{Кег } \varphi$.

Следствием теорем о гомоморфизмах АС и о фактормножествах является полезная

Теорема 6.10 (о факторсистемах). Пусть φ — гомоморфизм из АС $\mathfrak{A} = \langle A, \text{Op } A, \text{Rel } A \rangle$ в (однотипную) АС $\mathfrak{B} = \langle B, \text{Op } B, \text{Rel } B \rangle$ и \sim — эквивалентность на A такая, что $\sim \subseteq \text{Кег } \varphi$. Тогда:

- 1) отображение χ , задаваемое правилом $\chi([a]_{\sim}) = \varphi(a)$, есть эпиморфизм из \mathfrak{A}/\sim на $\text{Im } \varphi \subseteq \mathfrak{B}$;
- 2) если гомоморфизм φ сильный, то и χ — сильный гомоморфизм.

Доказательство. По теореме о фактормножествах существует отображение $A/\sim \xrightarrow{\chi} B$ такое, что диаграмма

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ \text{nat}(\sim) \searrow & & \nearrow \chi \\ & A/\sim & \end{array}$$

коммутативна. Это отображение задаётся правилом

$$\chi([a]_{\sim}) = \varphi(a). \quad (6.10)$$

Для доказательства утверждения теоремы надо показать согласованность отображения χ с операциями и отношениями АС \mathfrak{A}/\sim и \mathfrak{B} . Это проводится аналогично доказательству теоремы 6.9.

Пусть $f \in OpA$, $f' \in OpB$ и $f^* \in Op^*A/\sim$ — тройка одноимённых операций арности n . Для любого набора элементов a_1, \dots, a_n из A при $n > 0$ будем иметь цепочку равенств, совпадающую с (6.8), понимая под $[\cdot]$ классы эквивалентности по \sim и заменой (6.7) \mapsto (6.10). Также и для $n = 0$. Это означает согласованность χ с f^* и f' , и, следовательно, со всеми операциями систем \mathfrak{A}/\sim и \mathfrak{B} .

Теперь рассмотрим произвольную тройку одноимённых отношений $r \in RelA$, $r' \in RelB$ и $r^* \in Rel^*A/\sim$ арности m . Для любого набора элементов a_1, \dots, a_m из A будем иметь цепочку соотношений, совпадающую с (6.8), понимая под $[\cdot]$ классы эквивалентности по \sim и с заменой (6.7) \mapsto (6.10). Это означает согласованность χ с r^* и r' , и, следовательно, со всеми отношениями систем \mathfrak{A}/\sim и \mathfrak{B} .

Таким образом показано, что χ есть гомоморфизм из \mathfrak{A}/\sim в \mathfrak{B} и, следовательно, эпиморфизм \mathfrak{A}/\sim в $Im \varphi$.

Если гомоморфизм φ сильный, то соответствующую импликацию в последних соотношениях можно обратить. В результате получим, что отображение χ сильно согласованно с $r^* \in Rel A/\sim$ и $r' \in Rel B$ и, следовательно, χ — сильный гомоморфизм из $\mathfrak{A}/Ker \varphi$ в $Im \varphi$. \square

Пусть α — однородное на множестве A отношение, то его сужение на подмножество $B \subseteq A$ есть $B^2 \cap \alpha$. В этом случае легко видеть, что если α — конгруэнция на \mathfrak{A} и $\mathfrak{B} \leq \mathfrak{A}$, то $B^2 \cap \alpha$ — конгруэнция на \mathfrak{B} .

Теорема 6.11 (1-я первая об изоморфизмах АС). Пусть АС \mathfrak{A} с носителем A имеет подсистему \mathfrak{B} с носителем B , α — конгруэнция на \mathfrak{A} , $\varphi = nat(A, \alpha)$ и $\beta = B^2 \cap \alpha$ — конгруэнция на \mathfrak{B} . Тогда существует биективный гомоморфизм ψ факторсистемы \mathfrak{B}/β на $Im \varphi'$, где φ' — сужение φ на B .

Доказательство. Рассмотрим диаграмму

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A/\alpha \\ \downarrow \text{сужение} & & \downarrow \text{сужение} \\ B & \xrightarrow{\varphi'} & Im \varphi' \\ \searrow nat(B, \beta) & & \nearrow \psi \\ & & B/\beta \end{array}$$

Сужение φ' сильного гомоморфизма $\varphi = nat(A, \alpha)$ на $B \subseteq A$ есть гомоморфизм \mathfrak{B} . По теореме 6.9 о гомоморфизме АС отображение ψ , задаваемое правилом $\psi([x]_{Ker \beta}) = \varphi'(x)$ — взаимнооднозначный гомоморфизм $\mathfrak{B}/Ker \beta$ на $Im \varphi'$. \square

Заметим, что при сужении области задания свойство гомоморфизма «быть сильным» может быть потеряно, так что гомоморфизм φ' в вышеприведённой теореме, вообще говоря, не сильный. Поэтому в общем случае нельзя утверждать, что ψ — изоморфизм, и в данной теореме речь идёт лишь о биективном гомоморфизме АС, а не об их изоморфизме,

как можно было бы предположить из названия. Однако если \mathfrak{A} — алгебра, то ψ будет изоморфизмом, с чем связано традиционное название теоремы.

Вторая теорема об изоморфизмах АС связана с дробными эквивалентностями.

Теорема 6.12 (2-я об изоморфизмах АС). Пусть α и β — две конгруэнции на АС $\mathfrak{A} = AC$, причём $\beta \subseteq \alpha$. Тогда $(\mathfrak{A}/\beta)/(\alpha/\beta) \cong \mathfrak{A}/\alpha$.

Доказательство. Рассмотрим диаграмму

$$\begin{array}{ccc}
 & A & \\
 \text{nat } \beta \swarrow & & \searrow \text{nat } \alpha \\
 A/\beta & \xrightarrow{\varepsilon} & A/\alpha \\
 \text{nat } (\alpha/\beta) \searrow & & \swarrow \psi \\
 & (A/\beta)/(\alpha/\beta) &
 \end{array}$$

Зададим отображение ε правилом $\varepsilon([a]_\beta) = [a]_\alpha$. Тогда ε — сильный гомоморфизм из \mathfrak{A}/β в \mathfrak{A}/α . По теореме 6.9 отображение ψ , задаваемое правилом $\psi([a]_\beta)_{\alpha/\beta} = \varepsilon(a)$, есть изоморфизм между $(\mathfrak{A}/\beta)/(\alpha/\beta)$ и \mathfrak{A}/α . \square

Приведём без доказательства ещё одну теорему, описывающую свойства АС.

Теорема 6.13 (о соответствии). Если \mathfrak{A} — АС с носителем A и β — конгруэнция на ней, то решётка

$$L = \{ \alpha \in \text{Con } \mathfrak{A} \mid \beta \subseteq \alpha \}$$

изоморфна решётке $\text{Con } \mathfrak{A}/\beta$, причём $\mathfrak{A} \xrightarrow{\text{nat}(\alpha/\beta)} L$.

Укажем только, что здесь L и $\text{Con } \mathfrak{A}/\beta$ — полные решётки.

6.6 Многоосновные системы

Понятие АС может быть расширено. Например, если операции из $\text{Op } A$ — частичные, то говорят о *частичной АС*.

Другим возможным направлением расширения понятия АС является задание элементов сигнатуры не на одном, а на нескольких носителях. Так появляется понятие *многоосновной (многосортовой, гетерогенной, полидоменной)* системы. Рассмотрим некоторые примеры многоосновных алгебр.

Действие группы на множестве. Пусть дана группа $\mathfrak{G} = \langle G, \circ, e \rangle$. Действие α группы \mathfrak{G} на непустом множестве T обычно определяют как гомоморфизм из \mathfrak{G} в симметрическую группу $\text{Sym } T$ преобразований T . Мы дадим иное, как представляется, более простое определение действия группы на множестве.

Рассмотрим структуру из пяти элементов

$$\mathfrak{D} = \langle G, T, \circ, *, e \rangle,$$

у которой редукт $\langle G, \circ, e \rangle$ есть группа \mathfrak{G} , а операция $G \times T \xrightarrow{*} T$ подчиняется соотношениям

$$e * t = t, \quad (g \circ h) * t = h * (g * t)$$

для любых $g, h \in G$ и $t \in T$. Легко видеть, что указанные соотношения гарантируют, что соответствующее отображение \mathfrak{G} в $\text{Sym} T$ будет являться гомоморфизмом.

Введённая структура \mathfrak{D} представляет собой пример двухосновной алгебры с двумя бинарными операциями. Она имеет два носителя: G и T , причём групповая операция \circ определена на парах элементов из G , а операция $*$ — на парах элементов (g, t) , где $g \in G$, а $t \in T$. Константа e есть главный элемент \mathfrak{D} .

Конечные автоматы. Конечном детерминированным автоматом с начальным состоянием называется шестёрка объектов

$$\mathfrak{A} = \langle S, X, Y, \circ, *, s_0 \rangle,$$

где S, X, Y — конечные непустые множества, называемые соответственно множествами состояний, входных и выходных сигналов, \circ — функция переходов $S \times X \xrightarrow{\circ} S$, $*$ — функция выходов $S \times X \xrightarrow{*} Y$ и $s_0 \in S$ — начальное состояние.

Конечные автоматы являются примером трёхосновной алгебры, имеющей три носителя — S, X и Y , две бинарные функции — \circ и $*$ и главный элемент s_0 .

Линейное пространство. Пусть L — непустое множество и $\mathfrak{M} = \langle L, +, 0 \rangle$ — абелева группа (модуль). Пусть \mathfrak{K} — поле с носителем K , операцию сложения в котором будем обозначать тем же символом $+$, что и у модуля \mathfrak{M} , а символ операции умножения — опускать при записи. Единицу поля \mathfrak{K} будем обозначать, как обычно, 1 .

Введем новую операцию \cdot , действующую из $K \times L$ в L и подчиняющуюся правилам:

1. $1 \cdot x = x$ (унитальность),
2. $(\mu\lambda) \cdot x = \mu \cdot (\lambda \cdot x)$ (ассоциативность),³
3. $(\lambda + \mu) \cdot x = \lambda \cdot x + \mu \cdot x$,
4. $\lambda \cdot (x + y) = \lambda \cdot x + \mu \cdot x$ (дистрибутивные законы).

для любых $\lambda, \mu \in K$, $x, y \in L$.

Линейное пространство \mathfrak{L} элементов L над полем \mathfrak{K} можно определить как АС $\mathfrak{L} = \langle L, +, \{f_\lambda(x)\}_{\lambda \in K}, 0 \rangle$, где $f_\lambda(x) = \lambda \cdot x$. Это пример АС бесконечного типа.

В то же время ясно, что \mathfrak{L} можно мыслить как двухосновную алгебру с носителями L и K конечного типа.

Более формально, в качестве носителя в многоосновных системах выступают наборы множеств $\mathbf{A} = (A_i)_{i \in S}$, где A_i — множества, называемые *доменами*, а S — множество *сорт* доменов. Будем называть такие наборы множеств *комплектами*. При фиксированном множестве S будем говорить о S -комплектах.

Для S -комплекта покомпонентно (“посортно”) определяются понятие подкомплекта.

Покомпонентно определяются декартово произведение, а также образ и прообраз при рассмотрении отображений $\varphi: \mathbf{A} \rightarrow \mathbf{B}$ S -комплектов \mathbf{A} и \mathbf{B} . Также покомпонентно определяется умножение отображений. Ядром рассмотренного отображения φ будет являться набор $\phi = (\varphi_i)_{i \in S}$ ядер отображений $\varphi_i: A_i \rightarrow B_i$.

Набор эквивалентностей $\epsilon = (\sim_i)_{i \in S}$ комплекта $\mathbf{A} = (A_i)_{i \in S}$ определяет *факторкомплект* $\mathbf{A}/\epsilon \triangleq (A_i/\sim_i)_{i \in S}$. Ясно, что при этом для комплектов оказывается справедливым аналог теоремы 2.21 об основном свойстве отображений.

³Строго говоря, данный закон не есть закон ассоциативности, поскольку операции умножения поля и \cdot различны.

При определении многосортных алгебраических систем аналогом понятия арности операции или отношения служит их *тип*.

Тип многосортной операции f есть кортеж элементов множества сортов S вида $t = (s_1, \dots, s_n; s_0)$. Операция f вышеуказанного типа t на комплекте $\mathbf{A} = (A_i)_{i \in S}$ — это отображение

$$f: A_{s_1} \times \dots \times A_{s_n} \rightarrow A_{s_0}.$$

Тип нульарной операции, выделяющей элемент во множестве A_{s_0} , есть $t = (s_0)$.

Тип многосортного отношения r есть кортеж элементов множества сортов S вида $t = (s_1, \dots, s_m)$. Отношение r вышеуказанного типа t на комплекте $\mathbf{A} = (A_i)_{i \in S}$ — это отображение

$$r: A_{s_1} \times \dots \times A_{s_m} \rightarrow \{\mathbf{1}, \mathbf{0}\}.$$

Для данного комплекта $\mathbf{A} = (A_i)_{i \in S}$ совокупности $Op \mathbf{A}$ и $Rel \mathbf{A}$ суть объединения непересекающихся совокупностей операций $Op^t \mathbf{A}$ и $Rel^t \mathbf{A}$ типов t .

На многосортные алгебраические системы переносятся понятия согласованности отображений систем с операциями и отношениями (аналог определения 6.4), факторсистем и гомоморфизмов различных видов (аналог определения 6.5). При этом оказываются верны аналоги теорем о гомоморфизме и изоморфизмах систем, а также теорема 6.4 Биркгофа. Подробнее о многосортных алгебраических системах см. [27].

Приложение

Ниже приведены классические универсальные алгебраические системы. Указаны их сигнатура σ , тип τ и определяющие тождества и соотношения Σ . Для удобства обозначения операций унифицированы и считается, что приоритет \cdot (умножение или пересечение; может опускаться) выше приоритета $+$ (сложение или объединение).

Группоиды: $\sigma = \langle \cdot \rangle$; $\tau = \langle 1 \rangle$; $\Sigma :$

Полугруппы: $\sigma = \langle \cdot \rangle$; $\tau = \langle 1 \rangle$;

$$\Sigma : (1) \quad (xy)z = x(yz).$$

Моноиды: $\sigma = \langle \cdot, 1 \rangle$; $\tau = \langle 2, 0 \rangle$;

$$\Sigma : (1) \quad \text{и} \quad (2) \quad x \cdot 1 = 1 \cdot x = x.$$

Группы: $\sigma = \langle \cdot, {}^{-1}, 1 \rangle$; $\tau = \langle 2, 1, 0 \rangle$;

$$\Sigma : (1), (2) \quad \text{и} \\ (3) \quad x^{-1}x = xx^{-1} = 1.$$

Абелевы группы: $\sigma = \langle +, -, 0 \rangle$; $\tau = \langle 2, 1, 0 \rangle$;

$$\Sigma : (1^+) \quad (x + y) + z = x + (y + z), \\ (2^+) \quad x + 0 = 0 + x = x, \\ (3^+) \quad x + (-x) = 0, \\ (4^+) \quad x + y = y + x.$$

Полукольца: $\sigma = \langle +, \cdot \rangle$; $\tau = \langle 2, 2 \rangle$;

$$\Sigma : (1^+), (1), (4^+), \\ (5) \quad (x + y)z = xz + yz, \\ (6) \quad x(y + z) = xy + xz.$$

Кольца: $\sigma = \langle +, \cdot, -, 0 \rangle$; $\tau = \langle 2, 2, 1, 0 \rangle$;

$$\Sigma : (1^+) - (4^+), \\ (5) \quad (x + y)z = xz + yz, \\ (6) \quad x(y + z) = xy + xz.$$

Ассоциативные кольца: $\sigma = \langle +, \cdot, -, 0 \rangle$; $\tau = \langle 2, 2, 1, 0 \rangle$;

$$\Sigma : (1^+) - (4^+), (5), (6), (1).$$

Булевы кольца: $\sigma = \langle +, \cdot, -, 0 \rangle$; $\tau = \langle 2, 2, 1, 0 \rangle$;

$$\Sigma : (1^+) - (4^+), (5), (6), (1), \quad (9) \quad xx = x.$$

Ассоциативные кольца с единицей: $\sigma = \langle +, \cdot, -, 0, 1 \rangle$; $\tau = \langle 2, 2, 1, 0, 0 \rangle$;

$$\Sigma: (1^+) - (4^+), (5), (6), (1), (2).$$

Ассоциативно-коммутативные кольца с единицей: $\sigma = \langle +, \cdot, -, 0, 1 \rangle$;

$$\tau = \langle 2, 2, 1, 0, 0 \rangle;$$

$$\Sigma: (1^+) - (4^+), (5), (6), (1), (2), \quad (4) \quad xy = yx.$$

Тела: $\sigma = \langle +, \cdot, -, 0, 1 \rangle$; $\tau = \langle 2, 2, 1, 0, 0 \rangle$;

$$\Sigma: (1^+) - (4^+), (5), (6), (1), (2), \\ (3') \quad \forall x \neq 0 \exists x^{-1} (x^{-1}x = xx^{-1} = 1).$$

Поля: $\sigma = \langle +, \cdot, -, 0 \rangle$; $\tau = \langle 2, 2, 1, 0 \rangle$;

$$\Sigma: (1^+) - (4^+), (5), (6), (1), (2), (3'), (4).$$

Частично упорядоченные множества: $\sigma = \langle \leq \rangle$; $\tau = \langle 2 \rangle$;

$$\Sigma: (R) \quad x \leq x, \\ (AS) \quad (x \leq y) \& (y \leq x) \Rightarrow x = y, \\ (T) \quad (x \leq y) \& (y \leq z) \Rightarrow x \leq z,$$

Решётки: $\sigma = \langle +, \cdot \rangle$; $\tau = \langle 2, 2 \rangle$;

$$\Sigma: (1), (4), (1^+), (4^+), (9), \\ (9^+) \quad x + x = x, \\ (10) \quad x(x + y) = x, \quad (10^+) \quad x + yx = x.$$

Модулярные решётки: $\sigma = \langle +, \cdot \rangle$; $\tau = \langle 2, 2 \rangle$;

$$\Sigma: (1), (4), (1^+), (4^+), (9), (9^+), (10), (10^+), \\ (14) \quad x(x + y + z) = xy + xz.$$

Дистрибутивные решётки: $\sigma = \langle +, \cdot \rangle$; $\tau = \langle 2, 2 \rangle$;

$$\Sigma: (1), (4), (1^+), (4^+), (9), (9^+), (10), (10^+), \\ (15) \quad x(y + z) = xy + xz.$$

Булевы алгебры: $\sigma = \langle +, \cdot, ', 0, 1 \rangle$; $\tau = \langle 2, 2, 1, 0, 0 \rangle$;

$$\Sigma: (1), (4), (1^+), (4^+), (9), (9^+), \\ (10), (10^+), (5), \\ (11) \quad x0 = 0; \quad (11^+) \quad x + 1 = 1, \\ (12) \quad xx' = 0; \quad (12^+) \quad x + x' = 1, \\ (13) \quad x'' = x.$$

Булевы структуры: $\sigma = \langle +, \cdot, ', \leq, 0, 1 \rangle$; $\tau = \langle 2, 2, 1, 2, 0, 0 \rangle$;

$$\Sigma: (1), (4), (1^+), (4^+), (9), (9^+), \\ (10), (10^+), (5), (11), (11^+), (12), (12^+), (13), \\ (R), (AS), (T).$$

Список литературы

1. *Айгнер М.* Комбинаторная теория. — М.: Мир, 1982.
2. *Айзенберг Н.Н.* Спектральный анализ тестов и отношений толерантности: Методическая разработка по спецкурсам «Основы теории дискретных сигналов в произвольном базисе», «Дискретные спектральные разложения и тесты» для студентов математического факультета. — Ужгород: УжГУ, 1984.
3. *Богомолов А.М., Салий В.Н.* Алгебраические основы теории дискретных систем. — М.: Наука, 1997.
4. *Биркгоф Г.* Теория решёток. — М.: Наука, 1984.
5. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. — М.: Лань, 2005.
6. *Вагнер В.В.* Теория отношений и алгебра частичных отображений. / Теория полугрупп и её приложений. Сборник статей. Вып. 1. — Изд-во Саратов. ун-та, 1965. — С. 3–178.
7. *Валуце И.И.* Отображения. Алгебраические оопекты теории. — Кишенёв.: Штиинца, 1976.
8. *Владимиров Д.А.* Булевы алгебры. — М.: Наука, 1969.
9. *Войшвилло Е.К.* Алгебра двухполюсных сетей / Формальная логика и методология науки. — М.: Наука, 1964.
10. *Гретцер Г.* Общая теория решёток. — М.: Мир, 1982.
11. *Гуров С.И.* Упорядоченные множества и универсальная алгебра (вводный курс). — М.: Издательский отдел ф-та ВМиК МГУ, 2004.
12. *Гуров С.И.* Оценки числа монотонных булевых функций с данным числом нижних единиц / Математические методы распознавания образов (ММРО-12). Доклады 12-й Всероссийской конференции. — М.: МАКС Пресс, 2005. — С. 78–80.
13. *Гуров С.И.* Исчисления высказываний классической логики. — М.: Издательский отдел факультета ВМиК им. М.В.Ломоносова; МАКС Пресс. — 2007.
14. *Гуров С.И.* Нахождение некоторых характеристик частично упорядоченных множеств / Дискретные модели в теории управляющих систем: VIII Международная конференция, Москва, 6-9 апреля, 2009 г.: Труды. М.: Издательский отдел факультета ВМиК МГУ им. М.В. Ломоносова; МАКС Пресс, 2009. — С. 70-75.
15. *Грехем Р., Кнут Д., Паташник О.* Конкретная математика. Основания информатики. — М.: Мир, 1998.
16. *Двайт Г.Б.* Таблицы интегралов и другие математические формулы. — М.: Наука, 1948.
17. *Зарецкий К.А.* Полугруппа вполне эффективных бинарных отношений. / Теория полугрупп и её приложений. Сборник статей. Вып. 1. — Изд-во Саратов. ун-та, 1965. — С. 238–250.
18. *Кон П.* Универсальная алгебра. — М.: Мир, 1968.
19. *Кузнецов С.О.* Теория решёток для интеллектуального анализа данных: Учебное пособие. — Электронный ресурс <http://ami.hse.ru/data/165/315/1234/book.pdf>

20. Курош А.Г. Лекции по общей алгебре: Учебник. — СПб.: Издат-во «Лань», 2005⁴.
21. Курош А.Г. Общая алгебра (лекции 1969–1970 учебного года). — М.: Наука, 1974.
22. Лидл Р., Пильц Г. Прикладная абстрактная алгебра: Учебное пособие. — Екатеринбург: Изд.-во Урал. ун.-та, 1996.
23. Мальцев А.И. Алгебраические системы. — М.: Наука, 1970.
24. Ногин В.Д. Критериальная размерность задач векторной оптимизации / Модели и методы оптимизации, М.: ВНИИСИ, 1990, вып. 7. — С. 55–60.
25. Непейвода Н.Н. Прикладная логика. — Новосибирск: НГУ, 2000.
26. Оре О. Теория графов. — М.: Наука, 1980.
27. Плоткин Б.И. Универсальная алгебра, алгебраическая логика и базы данных. — М.: Наука, 1991.
28. Пропой А.И. О структуре частично упорядоченных множеств. // Докл. РАН. 2003, 390 (5). — С. 602–604.
29. Пинус А.Г. Основы универсальной алгебры. — Новосибирск: Изд-во НГТУ, 1998.
30. Риге Ж. Бинарные отношения, замыкания, соответствия Галуа. // Кибернетич. сборник № 7. — М.: Изд-во иностранной литературы, 1963. — С. 129–185.
31. Розен В.В. Частичные операции в упорядоченных множествах. — Саратов, 1973.
32. Розен В.В. Структура отношений предпочтения. — Саратов: Изд-во Саратов. ун.-та, 2007.
33. Саллий В.Н. Решётки с единственными дополнениями. — М.: Наука, 1984.
34. Скорняков Л.А. Элементы теории структур. — М.: Наука, 1970.
35. Скорняков Л.А. Элементы общей алгебры. — М.: Наука, 1983.
36. Стенли Р. Перечислительная комбинаторика (Volume I). — М.: Мир, 1990.
37. Шрейдер Ю.А. Равенство, сходство, порядок. — М.: Наука, 1971.
38. Шрейдер Ю.А. Пространства толерантности // Кибернетика, № 2, 1970. — С. 124–128.
39. Яблонский С.В. Введение в дискретную математику. — М.: Наука, 1986.
40. Яглом И.М. Булева структура и её модели. — М.: Сов. радио, 1980.
41. Bogart K.P., Trotter W.T. Maximal dimensional partially ordered sets II: characterization of $2n$ -element posets with dimension n // Discrete Math., **5**, 1973 — С. 33–43.
42. Brightwell G, Winkler P. Counting linear extensions // Order, **8**, 1991. — С. 225–242.
43. Burris S.N., Sunkappanavar H.P. A course of univrsal algebra. Springer Verlag. 1981.
44. Davey B. A., Priestley H. A. Introduction to Lattices and Order. Cambridge University Press, 1990.
45. Duffus D., Jónson B., Rival I. Structure results for fnction lattices. Canad. J. Math., 1978, 10, **2**, 392–400.
46. Demetrovics J., Rónyai L. Algebraic properties of crowns and fences // Order, № **6**, 1989. — С. 91–99.
47. Dushnik, B., Miller E.W. Partially ordered sets // Amer. J. Math. 63 (1941), 600–610.
48. Harzheim E. Ordered Sets (Chapter 7) / Advances in Mathematics. Volume 7. Springer US, 2005. — pp. 203–230.
49. Hiraguchi T. On the dimension of partially ordered sets. / Sci. Rep. Kanazawa Univ. 1, (1951). 77–94.

⁴Это издание включает и работу [21], которые автор намеревался объединить.

50. *Hiraguchi T.* On the dimension of orders. — Sci. Rep. Kanazawa Univ. 4, (1955). 1–20.
51. *Kelly D.* The 3-irreducible partially ordered sets // Canad. J. Math., **29**, 1977, 363–383.
52. *Kelly D.* On the dimension of partially ordered sets. Discrete Math., 1981, 35, 135–156.
53. *Kelly D., Trotter W. T.* Dimension theory for ordered sets / B Ordered sets [55].
54. *Novhk V.* Uber eine Eigenschaft der Dedekind-MacNeilleschen Hiille, Math. Ann. 179 (1969), 337–342.
55. *Ordered Sets.* Proc. NATO Adv. Study Inst. Banff (1981)(I. Rival, ed.). (Banff, Alta., Canada, 1981), NATO Ser. C: Math. Phys. Sci. Vol. 83 Dordrecht-Boston, Mass., 1982. 171–211.
56. *Ross J., Trotter W.T.* Every t -irreducible partial order is a subposet of a $t + 1$ -irreducible partial order, Annals of Discrete Math. 17 (1983), 613–621.
57. *Shepp L.* The XYZ conjecture and the FKG inequality // Ann. Prob., **10** (1982), 824–827.
58. *Shröder B.S.W.* Ordered sets: An introduction. Boston: Birkhauser, 2003.
59. *Szpilrajn E.* Sur l'extension de l'ordre partiel. Fund. Math. 16 (1930), 386–389.
60. *Stanley R.* Finite lattices and Jordan-Holder sets. // Algebra Universalis, **4** (1974), 361–371.
61. *Trotter W.T., Jr.* Dimension of the crown \mathbf{S}_n^k // Discrete Math, 8, 1974, 85–103.
62. *Trotter W.T.* Combinatorics and partially ordered sets: dimension theory. — Baltimore and Loondon: The Johnes Hopkins University Press, 1992.