Введение в математическую логику
Множества и отношения

Дашков Е. В.

6 декабря 2020 г.

ОГЛАВЛЕНИЕ

Предисловие

Настоящее учебное пособие представляет собой первую часть вводного курса математической логики, читаемого автором студентам-первокурсникам Физтех-школы прикладной математики и информатики Московского физико-технического института (национального исследовательского университета). Пособие содержит несколько больше материала, чем автору действительно удавалось прочесть в продолжение курса.

В этом и последующих планируемых пособиях предполагается изложить в основном традиционные для вводных курсов вопросы: основы теории множеств, логики высказываний и логики первого порядка, элементы теории моделей, теории доказательств и теории алгоритмов.

Настоящее пособие включает изложение аксиоматической теории множеств ZFC с извлечением следствий, нужных для обоснования курсов дискретной математики и информатики, читаемых студентам Физтех-школы. Предшествуя рассмотрению логики первого порядка, это изложение необходимо является неформальным. Тем не менее автор стремился достичь возможно большей строгости, не жертвуя краткостью и понятностью. Необходимые сведения из логики содержательных рассуждений сообщаются попутно.

В частности, не скрывается нужда в аксиоме выбора, возникающая уже в таких элементарных вопросах, как теория счетных множеств. Различные формы аксиомы выбора, а также аксиомы подстановки, нужные для рекурсивных конструкций, обсуждаются довольно подробно.

Строгие определения натуральных и вещественных чисел, вместе с вполне упорядоченными множествами, ординалами и рядом других традиционных теоретико-множественных тем, отложены до последующих частей курса. Взамен рассматриваются и обосновываются различные виды рекурсии, индуктивные определения множеств, а также основы теории формальных языков. Такой выбор продиктован ориентацией на дискретные математические науки.

Той же причиной объясняется несколько повышенное внимание к элементам универсальной алгебры, таким как операторы замыкания и соответствия Галуа.

В пособии разобрано значительное число примеров, а также предлагаются упражнения различной трудности.

Как и подобает элементарному курсу, все приводимые результаты хорошо известны (или являются незначительными вариациями таковых), а многие результаты — классические или «фольклорные». Поэтому точные ссылки при их формулировке и доказательстве не даются.

В списке литературы указаны как основные работы, использованные при составлении пособия, так и рекомендуемые читателю для углубленного изучения предмета или в качестве вспомогательных. В числе рекомендуемых книг имеется несколько относительно современных учебников на русском языке (весьма различных полнотой, сложностью и стилем изложения материала).

Изложение теории множеств в основном следует монографиям [7] и [18], а алгебраических вопросов (бинарных отношений, частичных порядков и пр.) — книгам [9] и [15]. При рассмотрении соответствий Галуа использованы заметки П. Смита [19]. Теория индуктивных определений представляет собой интерпретацию хорошо известных результатов универсальной алгебры, которые можно найти в [15].

Некоторые примеры и упражнения заимствованы из рекомендуемых читателю задачника [8] и брошюры [14].

Автор благодарит Л. Д. Беклемишева и В. Н. Крупского за полезные замечания, А. М. Райгородского, М. Н. Вялого, А. А. Глибичука, А. В. Бердникова, Д. В. Мусатова и всех сотрудников кафедры дискретной математики МФТИ, а также всех слушателей курса.

Глава 1. Множества, отношения и немного логики

§ 1.1. Математика и логика

Математическая логика — «логика по предмету, математика по методу» — изучает принятыми в математике методами различные *рассуждения* и прежде всего рассуждения самой математики[1]. В этой связи математическую логику нередко называют *метаматематикой*.

Рассуждения и истина. Рассуждения обычно стараются вести так, чтобы «сохранить истину», т. е. из истинных посылок получить истинные заключения, не совершив ошибок. В различении правильных и ошибочных рассуждений традиционно видели задачу собственно *логики*.

Пример 1.1.1. Рассуждение[2]:

> Каждый человек смертен. Сократ человек. Следовательно, Сократ смертен

является правильным, как и рассуждение:

> Каждое четное число, большее двух, есть сумма двух простых. Следовательно, Сократ смертен.

Почему? Потому что, как мы (считаем, что) знаем, заключение «Сократ смертен» является истинным, а значит, «истина» посылок (безотносительно к тому, была ли она там) не утратилась. При этом анализ

[1] Разумеется, как и всякая самостоятельная математическая наука, математическая логика обобщает и расчленяет свой «изначальный» предмет — реальные рассуждения, совершенно не ограничиваясь тем, что действительно находит в данный момент приложения в математике или где-либо еще. Иными словами, логика рассматривает некоторые абстрактные модели рассуждений и изучает их вполне свободно.

[2] До слова *следовательно* идут посылки, а после — заключение.

того, почему «Сократ смертен» и что́ есть истина, выходит за границы логики.

Однако в пользу правильности первого рассуждения можно привести и другой довод. Действительно, грамматика русского языка и определенный смысл слова «каждый» гарантируют: *если* посылки истинны, *то* обязательно истинно и заключение. Это рассуждение оказывается правильным лишь в силу своей *формы*: никакие сведения о «Сократе» не существенны.

Также по «формальным» причинам правильно рассуждение:

> Всякая ку́здра кудря́чит некоторого бокрёнка. Существует некоторая куздра. Следовательно, некоторого бокрёнка кудрячит некоторая куздра.

Что бы ни означала «куздра» и т. п., грамматика и «грамматические слова»: «всякая», «некоторая» и «существует» — свидетельствуют правильность рассуждения. *Формальная логика* (которая нас только и интересует) рассматривает свойства рассуждений, определенные их формой («грамматикой» в широком смысле), отвлекаясь от конкретного содержания, не требуя даже его уточнять.

Будет ли рассуждение:

> Всякая куздра смертна. Сократ смертен. Следовательно, Сократ куздра

правильным? Это зависит от смысла слова «куздра», а не только от «грамматики». Например, если «куздра» означает то же, что и «собака», истинные посылки дадут ложное заключение. В этом смысле последнее рассуждение «хуже» предшествующих.

Синтаксис и семантика. Как мы видим, рассуждения ведутся «о чем-то», причем упоминаемые объекты как-либо *обозначены*. В житейской и математической практике мы обычно думаем об объектах, не придавая обозначениям большого веса.

Пример 1.1.2.

> *Выражение* 16 означает число, делящееся на число, обозначаемое выражением 8.

В таком случае мы привыкли говорить: 16 *делится на* 8. Это высказывание *о значениях выражений*.

Употребляя те или иные выражения как в математической, так и обыденной речи, мы обыкновенно говорим именно об их значениях: *черный вам к лицу*. Однако иногда, особенно при логических или языковых исследованиях, нужно сказать *о самих выражениях*: 16 *состоит из двух цифр* (ср. также первое предложение этого примера) — или: *черный есть имя прилагательное*. В обыденной речи для этого часто употребляют кавычки: *«черный» есть имя прилагательное*. Но в математической практике систематическое употребление кавычек было бы слишком обременительным вследствие постоянного введения различных обозначений:

> Отношение длины к диаметру одинаково для всех окружностей. Обозначим это отношение греческой буквой π. Докажем, что $3 < \pi < 4$.

Поэтому мы впредь будем обозначать сами формальные выражения так же, как их значения. Такой способ обозначения называется *автонимным*. Разумеется, при этом нужно следить за контекстом, чтобы не оказалось, что *некоторые греческие буквы больше трех, но меньше четырех*[3].

В математической логике мы желаем построить *модель* математических рассуждений. Поэтому действующими лицами окажутся как обозначаемые объекты («семантика»), так и сами обозначения («синтаксис»). Легко понять, что объекты этих двух родов могут быть довольно различными. Например, выражение sin можно рассматривать как последовательность из трех букв конечного алфавита, в то время как «функция синус» естественно представляется бесконечной таблицей своих аргументов и значений (каждое из которых — вещественное число — требует для своего описания, вообще говоря, бесконечного числа цифр).

Вопрос о том, что означают те или иные *имена*, довольно непрост. Например, *что* означают имена «Сократ» (в частности, кого из носителей этого имени?) и «Шерлок Холмс», «золотая гора» и «круглый квадрат», «Утренняя звезда» и «Вечерняя звезда», «сегодня» и «здесь»?

В математическом исследовании мы пытаемся избежать затруднений, связанных со значением имен, давая *точные определения* и, когда требуется, *доказательства существования* обозначенных объектов[4].

[3] Придирчивый читатель мог бы еще заметить, что разные экземпляры буквы π в тексте, вообще говоря, следует отождествить.

[4] Если использовать естественный язык, достичь парадоксов весьма легко.

Итак, достаточно ясно, что означают имена 2, $3+2$, $\mathbb{N}$, $\sin$, $\sin 2$. Они подобны «именам собственным» обыкновенной грамматики. Но что означают выражения $3+x$ и $\sin x$? Можно считать, что они ничего не означают, пока не сделано никаких указаний о части x этих выражений, называемой *переменной*. В данном случае, если вместо переменной *подставить* имя какого-нибудь числа, мы вновь получим имя числа. Такие выражения с переменной называют *именными формами*.

Подобным образом, *высказывательные формы* обращаются в высказывания. Например, выражение $x^2 = 1$ высказыванием не является (истинно было бы такое высказывание или ложно?), но обращается в истинное высказывание при подстановке 1 вместо x и в ложное — при подстановке 2.

Основная ценность переменных, однако, в том, что они позволяют указывать на целые совокупности объектов. Скажем, выражение

$$x^2 = 1 \text{ для некоторого целого числа } x$$

есть (верное) высказывание. Здесь x играет чисто техническую роль, и данное высказывание относится вовсе не к какому-либо «числу x» (было бы такое число положительно или нет?), но ко всей совокупности целых чисел: утверждается, что она содержит решение уравнения. Приведенный пример заставляет вспомнить «имена нарицательные»: скажем, в выражении «каждый *человек* смертен» выделенное слово играет роль переменной, для которой, впрочем, указана еще *область* ее *значений* — люди.

Аналогичные конструкции применяются и для образования имен из именных форм: например, в выражениях $\lim_{x\to 0} \sin x$ и $\int_0^\pi \cos x\, dx$. Здесь два разных имени числа 0 образованы с помощью именных форм $\sin x$ и $\cos x$ без помощи подстановок.

В последних трех примерах подстановку имени числа вместо x можно считать бессмысленной. Такие употребления переменной называются *связанными*.

Обращаем еще внимание читателя на выражения, подобные *и*, *или*, $\lim_{x\to 0}$, *делится на*, *такой x, что*. Сами по себе они не являются ни

Именно, рассмотрим *наименьшее натуральное число, которое нельзя определить менее чем сотней русских слов*. Очевидно, таковое существует, поскольку достаточно коротких выражений русского языка лишь конечно много, а в каждой непустой совокупности натуральных чисел есть наименьшее. С другой стороны, мы, кажется, определили наше число короче (*парадокс Берри*). Интересно, что в формальном контексте этот и другие парадоксы дают начало глубоким теоремам.

именами, ни высказываниями[5]. Однако эти выражения задают способы образования новых имен и высказываний (именных и высказывательных форм) из имеющихся. Например, высказывание *Сократ смертен и Алкивиад смертен* образовано из двух, высказывание 2 *делится на* 4 образовано из имен 4 и 2, взятых в «неправильном» порядке, а имя *такой x, что $x+1=2$,* — из высказывательной формы $x+1=2$.

Вычисления. Рассмотрим выражения $1+1$ и $7-5$. С одной стороны, они различны, а с другой — им может быть поставлено в соответствие одно и то же «значение», которое еще обозначают выражением 2. А еще тем же значением можно наделить выражение «наибольшее натуральное число n, такое что уравнение $x^n+y^n=z^n$ имеет решение в целых положительных числах». Обратите внимание: понимание того, что значения всех этих выражений одинаковы, не достается даром — например, в последнем случае требуется использовать «великую теорему Ферма», чье доказательство потребовало трехсотлетних усилий. Напротив, в первом достаточно *вычислить* «значения выражений», скажем, преобразовав их к десятичной записи 2 по известным правилам, годящимся для *любых* выражений такого рода.

Вычисления, как преобразования обозначений по определенным «механическим» правилам, такие что *значение сохраняется*, а обозначение становится «достаточно простым» (скажем, является десятичной записью натурального числа), можно рассматривать как частный род рассуждений[6]. С развитием вычислительной техники этот частный случай приобрел особое значение. Поэтому органической частью курсов математической логики, не исключая нашего, является *теория алгоритмов* (или, если угодно, вычислений).

Основания математики. Если пытаться построить *модель* математики в целом, то, помимо обозначений, нужно проанализировать объекты, которыми она, собственно, занимается, «истинные» свойства этих объектов, на основании которых можно вести рассуждения, а также «сохраняющие истину» способы рассуждений. (Этот аспект мате-

[5]Кроме случая автонимного употребления, как в предыдущем нашем предложении.

[6]Любопытно, что Г. Лейбниц в XVII в. надеялся на обратное: заменить все рассуждения и споры философов (т.е. и математиков) вычислениями. Результаты математической логики не оставляют места такой возможности! Впрочем, если понимать программу Лейбница более ограниченно: вычисления не заменяют рассуждения, а только привлекаются для проверки их правильности, — следует отметить большие успехи в компьютерной проверке доказательств, переведенных на особый формальный язык.

матической логики называют *основаниями математики*). На рубеже XIX и XX вв. возобладал взгляд, что такими объектами можно считать *множества* и понятие *быть элементом множества*, которые вместо «определения» (неминуемо обращающегося к более простым объектам) снабжаются *аксиомами*, используемыми как базовые утверждения, и формальным языком записи понятий с некоторой «грамматикой».

Небезосновательно считают, что *внутри* формальной модели математики (как в некоторой игре с наперед заданными правилами) можно воспроизвести все ее наиболее значимые достижения (т. е. по формальным правилам *вывести* формальные «переводы» теорем). Однако, помимо *модели*, есть и «действительность», в которой модель строится.

Мы находимся как раз в этой действительности, а стало быть, не можем рассчитывать на формальное построение нашего инструментария *до* завершения работы: по ходу нашего курса мы будем использовать *внешние* (относительно модели) понятия: «множества», «натуральные числа», а также «логику» (что значит *и*?) без исчерпывающего объяснения, но с пояснениями, отражающими принятую практику.

Желательно, чтобы наш предмет, как и другие математические науки, мог быть развит в формальной модели математики. Это обстоятельство заставляет нас обращаться с *внешними* понятиями так, чтобы они были достаточно похожи на свои модели. В частности, используемые в следующих разделах без доказательств (или даже без явной формулировки) «очевидные» свойства множеств и натуральных чисел при формальном понимании оказываются следствиями «аксиом», а «разумные» приемы рассуждений выражаются «грамматическими правилами».

«Что мне в том?» Анализ математических (и иных) рассуждений любопытен с философской стороны и имеет давнюю историю. Например, классические задачи древности о возможности выполнить некоторое построение *ограниченными средствами* (скажем, «удвоение куба»: построить по ребру данного куба ребро куба вдвое большего объема — циркулем и линейной) и тем более о возможности вывести «пятый постулат Евклида» из прочих близки задачам математической логики[7].

Однако и с практической стороны методы математической логики могут быть полезны. В частности, их можно применять, когда требуется выяснить не возможности рассуждений математики в целом,

[7] Обе задачи получили отрицательное решение.

но только того, что доступно той или иной ограниченной формальной системе, скажем, что может или не может сделать некоторая компьютерная программа. (Уже древние греки располагали механическим «компьютером» — *нéвсисом*, позволявшим решить задачу об удвоении куба).

§ 1.2. Множества

Содержательно, множества нужны для того, чтобы рассматривать *многое* (быть может, *весьма* или *необозримо* многое) как нечто *одно*. Такие рассмотрения читатель легко обнаружит в довольно обыденных явлениях речи и мышления: *собака есть род животного*. Вопрос о смысле и возможности этих рассмотрений ставился уже Платоном и едва ли исчерпан теперь. Древняя идея оказывается весьма плодотворной в математике.

Будем считать, что *все* математические объекты, о которых мы говорим, являются *множествами*. Поскольку мы не дали множеству никакого определения, это нас ни к чему не обязывает, но упростит наши рассуждения. Такой подход оказывается достаточным для моделирования большей части математики.

Выражение $x \in A$ означает, что x является *элементом* множества A. Тогда еще говорят, что x *принадлежит* множеству A. Если x *не* является элементом A, будем писать $x \notin A$. Аналогичное правило «перечеркивания» станем применять и к другим символам.

Что означает «x принадлежит A»? Естественная интуиция тут, конечно, в том, что «объект» x содержится в «совокупности» A. Однако понятие принадлежности в нашей модели может отклоняться от этой интуиции. Как и множество, принадлежность не имеет никакого определения, а судить о свойствах этого понятия мы будем, постулировав некоторые из них.

Замечание 1.2.1. Читатель может спросить: что же будет элементами множеств? Очевидно, другие множества: ведь никаких иных математических объектов мы не допускаем. Возникают ли при этом бесконечные цепочки вида $\ldots x_{n+1} \in x_n \in \ldots \in x_1$? В частности, может ли быть $x \in x$? Обычно такие не вполне понятные интуитивно последовательности запрещают особой аксиомой; пока же заметим, что вскоре мы рассмотрим множества вовсе без элементов, на которых цепочка необходимо оборвется.

Напомним также, что множество натуральных чисел $\mathbb{N}$ мы считаем уже определенным. В качестве следствия (пока, скорее, в шут-

ку) можно заключить: хотя бы одно множество существует. Элементы множества $\mathbb{N}$ — знакомые нам натуральные числа 0, 1, 2 и т. д. — мы тоже считаем множествами. Каковы элементы этих множеств, нас не интересует постольку, поскольку мы пока принимаем простые свойства натуральных чисел, вроде $0 \neq 1$, без доказательства.

Замечание 1.2.2. Еще раз обратите внимание, что мы считаем $0 \in \mathbb{N}$. Такое соглашение можно оправдать, например, понимая натуральные числа как конечные количества: «ничего», «одно», «два» и т. д.

При необходимости (главным образом, в примерах) мы позволим себе «вспоминать» множества $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ целых, рациональных и вещественных чисел соответственно[8]. В неформальных примерах, которые придирчивый читатель может опустить, будут фигурировать и другие множества.

Равные множества. Мы говорим, что множество A есть *подмножество* (или *включено в*) B, и пишем $A \subseteq B$, если[9] для любого *множества* x из $x \in A$ следует $x \in B$. Тогда еще говорят, что B *надмножество* множества A. Иными словами, $A \subseteq B$ означает, что все элементы множества A принадлежат и множеству B.

В дальнейшем, если сказано «для любого x», «существует x» и т. п., но не указаны возможные значения переменной x (например, натуральные числа), то подразумевается соответственно «для любого *множества* x», «существует *множество* x» и пр.

Множества A и B *равны* (пишем $A = B$), если для любого x верно $x \in A$ тогда и только тогда, когда $x \in B$. Иначе говоря, множества равны, если и только если они состоят из одних и тех же элементов[10]. Мы пишем $A \subsetneq B$, если $A \subseteq B$, но $A \neq B$. Если $A \subsetneq B$, то говорят, что A есть *собственное* подмножество множества B.

Замечание 1.2.3. Понимая равенство интуитивно как «совпадение», мы ожидаем, что если $A \in X$ и $A = B$, то $B \in X$. При формальном подходе этот принцип — *аксиому равенства* — приходится постулировать.

[8] Элементы этих множеств также можно определить с помощью $\mathbb{N}$.

[9] Здесь и далее при введении различных обозначений и терминов слово «если», по традиции, означает «если и только если».

[10] Если считать равенство-«совпадение» (наряду с принадлежностью) исходным *неопределяемым* понятием, окажется, что элементы полностью определяют множество: скажем, тогда не может быть *различных* «красного» и «синего» множеств, состоящих точно из элементов $1, 2, 3$.

Отсюда будет видно, что равные множества в наших рассуждениях ведут себя совершенно одинаково и могут считаться «одним и тем же».

Лемма 1.2.4. *Для любых множеств A, B и C верно:*

1) $A \subseteq A$;

2) *если* $A \subseteq B$ *и* $B \subseteq C$, *то* $A \subseteq C$;

3) $A = B$ *тогда и только тогда, когда* $A \subseteq B$ *и* $B \subseteq A$.

Доказательство. Рассмотрим лишь п. 2. Итак, мы хотим показать, что для всякого $x \in A$ верно $x \in C$. Рассмотрим произвольный x и допустим $x \in A$. Тогда, в силу $A \subseteq B$, имеем $x \in B$. Аналогично, в силу $B \subseteq C$ заключаем $x \in C$. Раз для произвольного x из $x \in A$ следует $x \in C$, то это верно для всех x, что и требовалось. □

Следствие 1.2.5. *Для любых множеств A, B и C верно:*

1) $A = A$;

2) *если* $A = B$ *и* $B = C$, *то* $A = C$;

3) *если* $A = B$, *то* $B = A$.

Замечание 1.2.6. Такие свойства обосновывают использование традиционных цепочек равенств:

$$A_1 = A_2 = A_3 = \ldots = A_{n-1} = A_n.$$

Цепочка является сокращением для утверждения о том, что среди множеств $A_1, \ldots, A_n$ любые два равны. В самом деле, из равенств

$$A_1 = A_2,\ A_2 = A_3,\ \ldots,\ A_{n-1} = A_n$$

легко вывести любое равенство вида $A_i = A_j$. Например, равенство $A_1 = A_3$ будет следовать из первых двух.

Основные способы задания множеств. Множество можно задать, назвав *все* его элементы, когда число этих элементов конечно и все они уже определены: например, $\{1, 2, 3\}$ состоит точно из элементов 1, 2 и 3, а $\{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ — из элементов $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$.

Вообще, для любых множеств и x имеем

$$x \in \{a_1, \ldots, a_n\} \iff x = a_1 \text{ или } \ldots \text{ или } x = a_n,$$

где знак $\iff$ сокращает слова «тогда и только тогда, когда». (Строго говоря, здесь мы *постулируем*, что для любых $a_1, \ldots, a_n$ *существует* множество $\{a_1, \ldots, a_n\}$ с таким свойством.)

Пример 1.2.7. Обратите внимание, что $\mathbb{N} \in \{\mathbb{N}\}$, но $\mathbb{N} \not\subseteq \{\mathbb{N}\}$, ибо элемент 0 множества $\mathbb{N}$ (и всякий другой его элемент) не является множеством $\mathbb{N}$, а значит, не принадлежит множеству $\{\mathbb{N}\}$. С другой стороны, $\mathbb{N} \subseteq \mathbb{N}$, но $\mathbb{N} \notin \mathbb{N}$.

Пример 1.2.8. Имеет место $\{2, 2, 3\} = \{3, 2\}$. Действительно, если $x \in \{2, 2, 3\}$, то $x = 2$ или $x = 3$, и обратно. Этому же условию эквивалентно $x \in \{3, 2\}$. Таким образом, запись с символами $\{, \}$ содержит «лишнюю» информацию о порядке и кратности вхождения элементов, которая не учитывается понятием множества. Приведенные в начале записи следует считать синонимическими обозначениями одного и того же множества.

Другим важным способом задания множества является *выделение* всех элементов какого-нибудь *уже определенного множества* A, обладающих некоторым *точно определенным* свойством φ.

Если x обладает свойством φ, то пишут $\varphi(x)$. Скажем, четность(2). Для выделяемого множества B, очевидно, имеем

$$x \in B \iff x \in A \text{ и } \varphi(x)$$

при всех x и, следовательно, $B \subseteq A$. Такое множество B обозначают выражением $\{x \in A \mid \varphi(x)\}$.

Можно выделить, например, множество всех натуральных четных чисел:

$$\{x \in \mathbb{N} \mid \text{существует } y \in \mathbb{N},\ \text{т. ч. } x = 2y\}.$$

В формальной модели математики «свойства» окажутся выражениям особого искусственного языка. Мы же будем пока использовать в задании свойств любые разумные математические понятия (например, 2 или умножение), поскольку искусственный язык окажется достаточен для их записи, а также логические конструкции обыкновенного языка: «существует... т. ч. [такой что]», «и», «не» и др.

Пример 1.2.9. Существует *пустое* множество $\varnothing$, т. ч. $x \notin \varnothing$ для всех множеств x.

В самом деле, достаточно в любом множестве выделить подмножество элементов, удовлетворяющих какому-нибудь *противоречивому* свойству, например,

$$\varnothing = \{x \in \mathbb{N} \mid x = x \text{ и } x \neq x\}.$$

Пример 1.2.10. Пустое множество *единственно* в том смысле, что если N_1 и N_2 два пустых множества, то $N_1 = N_2$.[11]

Действительно, по определению пустого множества, условия $x \in$ $\in N_1$ и $x \in N_2$ ложны для всех x. Следовательно, для любого x верно $x \in N_1$ тогда и только тогда (никогда!), когда верно $x \in N_2$ (никогда!).

Пример 1.2.11. То, что новое множество состоит из элементов уже определенного, существенно. Снятие этого ограничения легко приводит к *парадоксу Рассела*: действительно, тогда существует множество

$$R = \{x \mid x \notin x\}$$

всех тех и только тех множеств, которые не являются своими элементами.

Верно ли, что $R \in R$? Пусть так. Тогда $R \notin R$. Противоречие заставляет заключить, что предположение неверно. Значит, $R \notin R$. Отсюда получаем $R \in R$ и новое противоречие — на этот раз без каких-либо предположений.

Исторически, именно это наблюдение побудило ограничивать способы образования новых множеств из имеющихся.

Упражнение 1.2.12. Приведите к противоречию предположение о существовании множества всех множеств.

Еще один способ получить новое множество B из данного множества A — рассмотреть множество всех подмножеств множества A. Иначе говоря, для всех x верно

$$x \in B \iff x \subseteq A.$$

Такое множество B обозначают выражением $\mathcal{P}(A)$. Множество $\mathcal{P}(A)$ еще называют *степенью* множества A.

Упражнение 1.2.13. Объясните, почему степень множества A единственна.

Пример 1.2.14. Множество

$$C = \{s \in \mathcal{P}(\mathbb{R}) \mid$$
$$\text{существует } x \in \mathbb{R}, \text{ т. ч. для всех } y \in \mathbb{R}\ (x \leqslant y \leqslant x+1 \iff y \in s)\}$$

[11] Обратите внимание, что так — обычным в математике образом — понимаемая единственность не влечет, вообще говоря, существования. (Хотя в данном случае пустое множество существует).

состоит из всевозможных отрезков числовой прямой $\mathbb{R}$, имеющих длину 1 (при этом точки x являются левыми их концами). Обратите внимание, что элементами C являются не точки прямой, но *множества* таковых.

Упражнение 1.2.15. Выпишите все элементы множества $\mathcal{P}(\{\varnothing, \{\varnothing\}\})$.

Пример 1.2.16. Пусть $\mathcal{P}(X) = \mathcal{P}(Y)$. Тогда $X = Y$.

Действительно, $X \subseteq X$, т. е. $X \in \mathcal{P}(X)$. Значит, $X \in \mathcal{P}(Y)$, откуда $X \subseteq Y$. Аналогично доказывается, что $Y \subseteq X$. Получаем $X = Y$ по лемме 1.2.4.

Располагая каким-нибудь множеством X, чьи элементы, как мы помним, тоже обязаны быть множествами, можно рассмотреть его *объединение*, обозначаемое $\cup X$ и состоящее из всевозможных элементов множеств, принадлежащих X. Точнее, для всех x имеет место

$$x \in \cup X \iff \text{существует } A \in X, \text{ т. ч. } x \in A.$$

Пример 1.2.17. Если выбрать на плоскости три круга положительного радиуса с попарно различными центрами, такое *множество кругов* будет иметь ровно три элемента, а его *объединением* будет фигура, состоящая из всех (бесконечно многих) точек, лежащих хотя бы в одном из кругов.

Пример 1.2.18. Для рассмотренного в примере 1.2.14 множества C имеем $\cup C = \mathbb{R}$. Действительно, если $x \in \cup C$, то $x \in s$ для некоторого отрезка $s \subseteq \mathbb{R}$. Тем более $x \in \mathbb{R}$. Обратно, если $x \in \mathbb{R}$, то $x \in [x, x+1]$. Отрезок $[x, x+1]$ имеет длину 1, а значит, $[x, x+1] \in C$. Следовательно, $x \in \cup C$.

Упражнение 1.2.19. Докажите, что $\cup\varnothing = \varnothing$ и $\cup\{A\} = A$ для всех A.

Упражнение 1.2.20. Докажите, что если $X \subseteq Y$, то $\cup X \subseteq \cup Y$ для любых множеств X и Y.

Пример 1.2.21. «Вассал моего вассала не мой вассал», — гласит принцип феодального права. Аналогичным образом, «элемент моего элемента не (всегда) мой элемент»: имеем $0 \in \cup\{\mathbb{N}\}$, поскольку $0 \in \mathbb{N}$, хотя $0 \notin \{\mathbb{N}\}$, так как $0 \neq \mathbb{N}$. Впрочем, довольно важны *транзитивные* множества, содержащие все элементы своих элементов (т. е. $\cup X \subseteq X$). Множества $\varnothing$ и $\{\varnothing\}$, очевидно, транзитивны.

Упражнение 1.2.22. Вычислите $\cup\{\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}\}$, $\cup\{\varnothing,\{\varnothing\},\{\{\varnothing\}\}\}$, а также $\cup\cup\{\{\varnothing\},\{\varnothing,\{\varnothing\}\}\}$.

Упражнение 1.2.23. Приведите к противоречию предположение о существовании множества всех *одноэлементных* (т. е. вида $\{x\}$) множеств.

Упражнение 1.2.24. Приведите пример множеств $X \neq Y$, т. ч. $\cup X = \cup Y$.

Пример 1.2.25. Покажем, что $\cup\mathcal{P}(X) = X$. В самом деле, если $x \in X$, то $x \in X \in \mathcal{P}(X)$, откуда $x \in \cup\mathcal{P}(X)$. Обратно, если $x \in \cup\mathcal{P}(X)$, то $x \in A$ для некоторого $A \in \mathcal{P}(X)$. Имеем $x \in A \subseteq X$, что влечет $x \in X$.

Упражнение 1.2.26. Докажите, что $X \subseteq \mathcal{P}(\cup X)$ для всех X. Приведите примеры множества X, т. ч. $\mathcal{P}(\cup X) \not\subseteq X$ и т. ч. $\mathcal{P}(\cup X) = X$.

Упражнение 1.2.27. Приведите пример транзитивного множества с нетранзитивным элементом. Докажите, что если X транзитивно, то таковы же $\cup X$ и $\mathcal{P}(X)$. Докажите, что X транзитивно тогда и только тогда, когда $X \subseteq \mathcal{P}(X)$.

Упражнение 1.2.28. Докажите, что для любых множеств X и Y верно

$$\cup X \subseteq Y \iff X \subseteq \mathcal{P}(Y).$$

Замечание 1.2.29. Понятие объединения позволяет свести определение множества «перечислением конечного числа элементов» к случаю, когда таких элементов не больше двух. Например, $\{1,2,3\} = \cup\{\{1,2\},\{3\}\}$.

Почему мы выделили именно эти способы задания множеств? Потому что они возникают в реальной математике. Некоторые другие практически важные способы сводятся к указанным — например, *пересечение* множества, о котором вскоре пойдет речь. С другой стороны, какие-то способы с ними логически несовместны: например, нельзя образовать множество всех множеств (упражнение 1.2.12).

При формальном построении математики встречаются еще способы образования новых множеств, сводимость которых к до сих пор рассмотренным неочевидна или даже опровергается в весьма общих предположениях. Какие из них следует принять, в конце концов, определяется лишь математической практикой.

Отметим, что «непринятие» непротиворечивого способа задания множеств отнюдь не означает, что такие множества объявляются несуществующими: просто в доказательствах не разрешается использовать их существование как данность.

О кванторах и королях. Выше нам часто встречались выражения «существует x» и «для всех x», а также их синонимы. Эти выражения, называемые *кванторами* (*существования* и *всеобщности* соответственно), чрезвычайно существенны для математики. (Следует заметить, что квантор всеобщности нередко опускают: пишут, например, $\sin x \leqslant 1$, имея в виду, что это верно *для всех* $x \in \mathbb{R}$.)

Пока же мы введем для кванторов символические обозначения: соответственно $\exists x$ и $\forall x$. Рассмотрим, например, вроде бы понятное утверждение «существует x, т. ч. $3x + 1 = 0$», или символически:

$$\exists x\,(3x + 1 = 0).$$

Верно ли оно? Иначе говоря, имеет ли уравнение $3x + 1 = 0$ решение? Очевидно, это зависит от того, в каком множестве решение ищется. Например, во множествах $\mathbb{N}$ и $\mathbb{Z}$ решений нет, а во множествах $\mathbb{Q}$ и $\mathbb{R}$ есть (единственное) решение $-\frac{1}{3}$.

Таким образом, существенно, из какой области берутся значения переменной x. Выше мы принимали за такую область все множества. Кроме того, в ряде случае мы эту область явно ограничивали некоторым множеством A с помощью выражений вида «существует $x \in A$». Такие выражения назовем *ограниченными кванторами*.

Нетрудно понять, что ограниченные кванторы сводятся к «неограниченным». Именно, имеет место

$$\exists x \in A\ \varphi(x) \iff \exists x\,(x \in A \text{ и } \varphi(x))$$

и

$$\forall x \in A\ \varphi(x) \iff \forall x\,(\text{если } x \in A,\ \text{то } \varphi(x)).$$

Важную роль в математике играет случай, когда множество A пусто. Условие $x \in \varnothing$ всегда ложно, а значит, ложно будет и утверждение $\exists x \in \varnothing\ \varphi(x)$.

Несколько менее интуитивно то обстоятельство, что утверждение $\forall x \in \varnothing\ \varphi(x)$ всегда истинно. В самом деле, $x \in \varnothing$ ложно, а из ложной посылки, как принято в математике[12], следует все, что угодно, — в частности, $\varphi(x)$.

Заметный философский интерес вызвали утверждения о «несуществующих» объектах: например, *нынешний король Франции лыс*. Если понимать это утверждение так:

[12]Напомним, что «правильные» рассуждения *сохраняют* истину. Если же условие было ложным, *любое* заключение сохраняет отсутствующую истину и делает рассуждение правильным.

всякий человек, если он нынешний король Франции, лыс,

окажется, что оно истинно. Но то, что «нынешний король Франции волосат», будет не менее истинным!

Упражнение 1.2.30. Докажите, что $\varnothing \subseteq A$ для любого множества A.

Пересечение множества. Аналогично объединению, определено и *пересечение* множества X

$$\cap X = \{x \in \cup X \mid \forall A \in X \; x \in A\}.$$

Обратите внимание, что это множество строится с помощью выделения подмножества в объединении X. Таким образом, перед нами не «основной», а производный способ получить новое множество. Если $X \neq \varnothing$, то для всех x верно

$$x \in \cap X \iff \forall A \in X \; x \in A.$$

Действительно, если существует $B \in X$ и $\forall A \in X \; x \in A$, то $x \in B \subseteq \subseteq \cup X$, откуда $x \in \cap X$. Напротив, условие $\forall A \in \varnothing \; x \in A$ выполнено для всех вообще x.

Упражнение 1.2.31. Вычислите $\cap\varnothing$ и $\cap\{\varnothing\}$.

Как мы видели, $X \subseteq Y$ влечет $\cup X \subseteq \cup Y$. «Двойственный» результат имеет место для пересечения, но с некоторой оговоркой.

Пример 1.2.32. Если $X \subseteq Y$, причем $X \neq \varnothing$, то $\cap Y \subseteq \cap X$. Действительно, пусть $z \in \cap Y$. Тогда $z \in A$ для всех $A \in Y$. Однако если $A \in X$, то $A \in Y$, а значит,

$$\forall A \, (A \in X \Longrightarrow z \in A).$$

(Символом $\alpha \Longrightarrow \beta$ мы заменяем выражение «если α, то β». Такие «условные суждения» называются *импликациями*. Если выполнено $\alpha \Longrightarrow \beta$, то говорят, что условие β *необходимо* для α, а условие α *достаточно* для β.)

Остается показать, что $z \in \cup X$. В самом деле, существует некоторое множество $B \in X$. Тогда $B \in Y$ и, следовательно, $z \in B$. Отсюда $z \in \cup X$.

Легко видеть, что требование $X \neq \varnothing$ необходимо. Например, при $\varnothing \subseteq \{\{\varnothing\}\}$ имеем $\cap\{\{\varnothing\}\} = \{\varnothing\} \not\subseteq \varnothing = \cap\varnothing$.

Замечание 1.2.33. Иногда пересечение $\cap\varnothing$ считают неопределенным.

Операции над множествами. Для произвольных множеств A и B обозначим символом $A \cup B$ множество $\cup\{A, B\}$, называемое *объединением множеств A и B*. Очевидно, что для всех x верно

$$x \in A \cup B \iff x \in A \text{ или } x \in B.$$

Обратите внимание, что «или» в математической практике понимается как *не* исключающее, т. е. допускается одновременное выполнение обеих возможностей.

Определим также *пересечение*

$$A \cap B = \{x \in A \mid x \in B\}$$

и *разность*

$$A \setminus B = \{x \in A \mid x \notin B\}$$

произвольных множеств A и B. Ясно, что для любого x имеем

$$x \in A \cap B \iff x \in A \text{ и } x \in B.$$

Кроме того, $A \cap B = \cap\{A, B\}$. Говорят, что множества A и B *не пересекаются*, если $A \cap B = \varnothing$.

Лемма 1.2.34. *Для любых множеств A и B верно $A \cap B \subseteq X \subseteq A \cup B$, если $X \in \{A, B\}$. Кроме того, $A \setminus B \subseteq A$ и $(A \setminus B) \cap B = \varnothing$.*

Лемма 1.2.35. *Для любых множеств A и B равносильны утверждения:*

1) $A \subseteq B$;

2) $A \cap B = A$;

3) $A \cup B = B$.

Доказательство. Достаточно показать, что из первого утверждения следует второе, из второго третье, и из третьего — первое.

Пусть $A \subseteq B$. По лемме 1.2.34, имеем $A \cap B \subseteq A$. Покажем, что $A \subseteq A \cap B$. Предположим для произвольного x, что $x \in A$. Тогда $x \in B$ в силу $A \subseteq B$. Следовательно, $x \in A \cap B$. Согласно лемме 1.2.4, утверждения $A \cap B \subseteq A$ и $A \subseteq A \cap B$ влекут $A \cap B = A$.

Пусть теперь $A \cap B = A$. По лемме 1.2.34, $B \subseteq A \cup B$. Остается проверить $A \cup B \subseteq B$. Если $x \in A \cup B$, то $x \in A$ или $x \in B$. В первом случае, в силу $A = A \cap B$, верно $x \in A \cap B$, откуда $x \in B$. Тем более $x \in B$ во втором случае.

Пусть, наконец, $A \cup B = B$. В силу леммы 1.2.34, имеем $A \subseteq A \cup B$ и, по предположению, $A \cup B \subseteq B$, откуда $A \subseteq B$. □

Упражнение 1.2.36. Докажите, что для любых A, B и C из $A \subseteq B$ следует $C \setminus B \subseteq C \setminus A$.

Нередко все рассматриваемые множества оказываются подмножествами какого-нибудь множества U (например, изучаются подмножества натурального ряда $\mathbb{N}$). Такое U называют тогда *универсумом*. Для каждого подмножества A заданного универсума U определено *дополнение*

$$\bar{A} = U \setminus A.$$

Упражнение 1.2.37. Докажите, что $A \setminus B = A \cap \bar{B}$ для любых A и B и любого универсума U, включающего эти множества.

Теорема 1.2.38 (Основные тождества алгебры множеств)**.** *Для любых множеств A, B, C и любого включающего их универсума U верно:*

1) $A \cap B = B \cap A$; $A \cup B = B \cup A$;

2) $(A \cap B) \cap C = A \cap (B \cap C)$; $(A \cup B) \cup C = A \cup (B \cup C)$;

3) $A \cap A = A$; $A \cup A = A$;

4) $A \cap (A \cup B) = A$; $A \cup (A \cap B) = A$;

5) $\bar{\bar{A}} = A$;

6) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$; $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;

7) $\overline{A \cap B} = \bar{A} \cup \bar{B}$; $\overline{A \cup B} = \bar{A} \cap \bar{B}$;

8) $A \cap \varnothing = \varnothing$; $A \cup \varnothing = A$; $A \cap U = A$; $A \cup U = U$; $\bar{\varnothing} = U$; $\bar{U} = \varnothing$;

9) $A \cap \bar{A} = \varnothing$; $A \cup \bar{A} = U$.

Доказательство. Проверим, например, что $\overline{A \cap B} = \bar{A} \cup \bar{B}$. Если $x \in \overline{A \cap B}$, то $x \in U$ и неверно, что $x \in A \cap B$. Т. е. неверно, что $x \in A$ и $x \in B$. Это значит, что выполнено хотя бы одно из двух условий: неверно $x \in A$ или неверно $x \in B$. Соответственно, получаем $x \in \bar{A}$ или $x \in \bar{B}$. Тогда $x \in \bar{A} \cup \bar{B}$. Итак, $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.

Установим обратное включение $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$. Пусть $x \in \bar{A} \cup \bar{B}$. Тогда $x \notin A$ или $x \notin B$. Допустим, что $x \in A \cap B$. Если $x \notin A$, имеем $x \in A$. Противоречие. В случае $x \notin B$ также приходим к противоречию. Значит, наше допущение противоречит условию, т. е. $x \notin A \cap B$, откуда $x \in \overline{A \cap B}$. $\square$

Замечание 1.2.39. Свойство $(A \cap B) \cap C = A \cap (B \cap C)$ *ассоциативности* пересечения множеств позволяет писать без скобок выражения вроде $A_1 \cap A_2 \cap \ldots \cap A_n$, поскольку безразлично, как скобки расставить. То же относится, конечно, к объединению множеств.

Замечание 1.2.40. Приведенные в теореме 1.2.38 тождества определяют структуру, состоящую из множества $\mathcal{P}(U)$, операций $\cap, \cup, \overline{(\cdot)}$ и выделенных элементов $\varnothing$, U, как *булеву алгебру* (при этом некоторые тождества можно вывести из других).

Пример 1.2.41. Если $A \subseteq C$ и $B \subseteq C$, то $A \cup B \subseteq C$. В самом деле, согласно лемме 1.2.35, имеем $C = A \cup C$ и $C = B \cup C$, откуда $C = A \cup (B \cup C) = (A \cup B) \cup C$, т. е. $A \cup B \subseteq C$.

Упражнение 1.2.42. Докажите, что если $A \subseteq B$ и $A \subseteq C$, то $A \subseteq B \cap C$.

Иногда, особенно при изучении свойств операций $\cap$, $\cup$ и $\setminus$, удобно предполагать, что некоторый универсум выбран, не уточняя, каков он. Заметим, что универсум всегда существует, если рассматривается «не слишком много» множеств, точнее, все они суть *элементы* некоторого множества X. Тогда достаточно положить $U = \cup X$. Например, в следующем примере можно считать $X = \{A, B, C\}$ для *каждого* возможного выбора множеств A, B, C.

Пример 1.2.43. Покажем, что $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$, используя уже известные тождества вместо непосредственной проверки. Для произвольных A, B и C имеем

$$A \setminus (B \setminus C) = A \cap \overline{B \cap \bar{C}} = A \cap (\bar{B} \cup \bar{\bar{C}}) =$$
$$= A \cap (\bar{B} \cup C) = (A \cap \bar{B}) \cup (A \cap C) = (A \setminus B) \cup (A \cap C).$$

Замечание 1.2.44. В последних примерах мы молчаливо использовали «устойчивость» операций относительно равенства: если $X = Y$, то $X \cap Z = Y \cap Z$, и т. п. Если понимать равенство как «совпадение», это само собою разумеется. Однако мы *определили* равенство через $\in$. Тогда «устойчивость» превращается в теорему, рутинное доказательство которой советуем провести читателю. (Это пример явления, о котором уже говорилось в замечании 1.2.3.) Впредь мы позволим себе не возвращаться к подобным вопросам.

Упражнение 1.2.45. Докажите, что для произвольных множеств A, B и C верно $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Декартово произведение. Кроме множеств, обычным объектом математики являются упорядоченные совокупности, в конечном случае называемые «наборами» или «кортежами». Например, при введении координат на плоскости точки отождествляются с *упорядоченными* парами вещественных чисел: так, $(0,1)$ и $(1,0)$ суть *разные* точки. Как мы увидим, такие объекты нетрудно моделировать с помощью множеств.

Для произвольных множеств a и b символом (a,b) обозначим множество

$$\{\{a\},\{a,b\}\},$$

называемое (*упорядоченной*) *парой множеств* a *и* b (*по Куратовскому*). Основным свойством пары является ее «упорядоченность», выражаемая следующей леммой.

Лемма 1.2.46. *Для любых множеств* a,b,c,d *имеет место*

$$(a,b)=(c,d) \iff a=c \text{ и } b=d.$$

Доказательство. Предположим, что $\{\{a\},\{a,b\}\}=\{\{c\},\{c,d\}\}$. Тогда $\{a\}\in\{\{c\},\{c,d\}\}$, т. е. $\{a\}=\{c\}$ или $\{a\}=\{c,d\}$. В первом случае $a\in\{c\}$, т. е. $a=c$. Во втором имеем $c\in\{a\}$, откуда $c=a$. Итак, $a=c$.

Из условия также получаем $\{a,b\}=\{c\}$ или $\{a,b\}=\{c,d\}$.

В первом случае $b\in\{c\}$, откуда $b=c=a$. Поскольку $\{c,d\}=\{a\}$ или $\{c,d\}=\{a,b\}$, получаем $d=a=b$. Значит, $b=d$.

Пусть теперь $\{a,b\}=\{c,d\}$. Если $d=b$, то все доказано. Иначе $d=a=c$, т. е. $\{a,b\}=\{d\}$, откуда вновь $b=d$.

Остается проверить обратную импликацию. Пусть $a=c$ и $b=d$. Если $x\in(a,b)$, то $x=\{a\}$ или $x=\{a,b\}$. Очевидно, тогда $x=\{c\}\in\in(c,d)$ или $x=\{c,d\}\in(c,d)$. Аналогично, $(c,d)\subseteq(a,b)$. □

Следствие 1.2.47. *Множества* (a,b) *и* (b,a) *равны тогда и только тогда, когда* $a=b$.

Замечание 1.2.48. Если $a,b\in X$, то $(a,b)\in\mathcal{P}(\mathcal{P}(X))$.

Декартовым (или *прямым*) *произведением* множеств A и B называется множество

$$A\times B=\{z\in\mathcal{P}(\mathcal{P}(A\cup B))\mid\exists a\in A\,\exists b\in B\ z=(a,b)\}.$$

Менее аккуратно, но более наглядно можно написать так:

$$A\times B=\{(a,b)\mid a\in A,\ b\in B\}.$$

Пример 1.2.49. Имеем $A \times \varnothing = \varnothing$ для любого A. Действительно, как мы помним, утверждение вида $\exists b \in \varnothing\, \varphi$ всегда ложно.

Упражнение 1.2.50. При каких условиях из $A \times B = C \times D$ следует $A = C$ и $B = D$?

Упражнение 1.2.51. Приведите примеры множеств A, B и C, для которых $A \times B \neq B \times A$ и $(A \times B) \times C \neq A \times (B \times C)$.

Мы будем опускать скобки в декартовых произведения по правилу «левой ассоциативности», что позволяет их при необходимости восстановить. Именно, будем писать $A \times B \times C$ вместо $(A \times B) \times C$, и, вообще,

$$A_1 \times A_2 \times A_3 \times \ldots \times A_{n-1} \times A_n$$

вместо

$$(\ldots((A_1 \times A_2) \times A_3) \times \ldots \times A_{n-1}) \times A_n$$

при всех натуральных $n \geqslant 3$.

Замечание 1.2.52. Если $(x, y) \in A \times B$, то $x \in A$ и $y \in B$, и обратно.

В самом деле, тогда по определению декартова произведения найдутся $a \in A$ и $b \in B$, т. ч. $(x, y) = (a, b)$. Согласно лемме 1.2.46, имеем $x = a$ и $y = b$, откуда вытекает $x \in A$ и $y \in B$ по аксиоме равенства (см. замечание 1.2.3). Обратная импликация очевидна из определения множества $A \times B$ и того что $(x, y) \in \mathcal{P}(\mathcal{P}(A \cup B))$ по замечанию 1.2.48.

Это утверждение может показаться почти бессодержательным, но мы предостережем читателя: пусть, например, $A, B \subseteq \mathbb{N}$ и $A + B = \{a + b \mid a \in A, b \in B\} = \{z \in \mathbb{N} \mid \exists a \in A\, \exists b \in B\ z = a + b\}$. Тогда, $2 + 3 = 4 + 1 \in \{1, 4, 0\} + \{5, 1\}$, хотя $2 \notin \{1, 4, 0\}$ и $3 \notin \{5, 1\}$. Таким образом, единственность определения компонент пары играет ключевую роль.

Пример 1.2.53. Установим, что для любых множеств A, B, C, D верно

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D).$$

Пусть $z \in (A \times B) \cap (C \times D)$. Тогда $z \in A \times B$ и $z \in C \times D$. Значит, $z = (a, b)$ для некоторых $a \in A$ и $b \in B$. Имеем $(a, b) \in C \times D$, откуда $a \in C$ и $b \in D$ по замечанию 1.2.52. Следовательно, $a \in A \cap C$ и $b \in B \cap D$, а значит, $z = (a, b) \in (A \cap C) \times (B \cap D)$.

Обратно, пусть $z \in (A \cap C) \times (B \cap D)$. Тогда существуют $x \in A \cap C$ и $y \in B \cap D$, т. ч. $z = (x, y)$. Поскольку $x \in A$ и $y \in B$, имеем $z \in A \times B$. Аналогично, $z \in C \times D$.

Упражнение 1.2.54. Докажите, что $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

Пример 1.2.55. Пусть множества A и B непусты. Тогда имеем

$$A \subseteq C \text{ и } B \subseteq D \iff A \times B \subseteq C \times D.$$

В самом деле, допустим, что $A \subseteq C$ и $B \subseteq D$. По лемме 1.2.35 имеем $A = A \cap C$ и $B = B \cap D$, а значит, $A \times B = (A \cap C) \times (B \cap D)$. Применяя пример 1.2.53, получаем

$$A \times B = (A \times B) \cap (C \times D) \subseteq C \times D.$$

Обратно. Пусть $A \times B \subseteq C \times D$ и $a \in A$. Поскольку $B \neq \varnothing$, существует $b \in B$, для которого $(a, b) \in A \times B$. Следовательно, $(a, b) \in C \times D$, откуда $a \in C$. Получаем, что $A \subseteq C$; второе включение устанавливается аналогично.

Пример 1.2.56. Пусть множества A и B непусты и $(A \times B) \cup (B \times A) = C \times D$. Тогда $A = B = C = D$.

Очевидно, что $A \times B \subseteq C \times D$, откуда, в силу примера 1.2.55, $A \subseteq C$ и $B \subseteq D$. Аналогично устанавливаем включения $B \subseteq C$ и $A \subseteq D$. Отсюда легко следует, что $A \cup B \subseteq C$ и $A \cup B \subseteq D$. (Действительно, учитывая лемму 1.2.35, имеем $(A \cup B) \cup C = A \cup (B \cup C) = A \cup C = C$.)

С другой стороны, $C \subseteq A \cup B$. В самом деле, $A \times B \neq \varnothing$, а значит, $C \times D \neq \varnothing$, откуда $C \neq \varnothing$ и $D \neq \varnothing$. Возьмем некоторый $d \in D$. Для произвольного $c \in C$ имеем $(c, d) \in A \times B$ или $(c, d) \in B \times A$, откуда $c \in A$ или $c \in B$. Аналогично, $D \subseteq A \cup B$. С учетом предыдущего получаем, что $C = A \cup B = D$.

Для произвольного $a \in A$ имеем $(a, a) \in C \times D$, а следовательно, $(a, a) \in A \times B$ или $(a, a) \in B \times A$. В каждом из этих случаев получаем $a \in B$. Итак, $A \subseteq B$. Аналогично, $B \subseteq A$. Окончательно, $A = B = A \cup B = C = D$.

Декартовы степени. Как и в случае обычного умножения, декартово произведение позволяет определить натуральные степени — для произвольного множества A и всех натуральных чисел $n \geqslant 2$ мы полагаем

$$\begin{aligned} A^0 &= \{\varnothing\}; \\ A^1 &= A; \\ A^n &= \underbrace{A \times A \times \ldots \times A}_{n \text{ вхождений } A}. \end{aligned}$$

Замечание 1.2.57. Почему $A^0 = \{\varnothing\}$, а не, скажем, $\varnothing$? Мы надеемся, что это соглашение станет ясным из обсуждения функций и натуральных чисел. Пока же отметим, что для натуральных чисел полагают $n^0 = 1$, а во множестве $\{\varnothing\}$ как раз *один* элемент.

Обратим также внимание, что $A^{n+1} = A^n \times A$ для всех $n \geqslant 1$.

Кроме пар множеств, можно говорить о тройках, четверках и т. д. Для $n \geqslant 2$ назовем *набором* (или *кортéжем*) *множеств* $a_1, \ldots, a_{n-1}$, a_n, множество

$$(a_1, \ldots, a_{n-1}, a_n) = ((\ldots((a_1, a_2), a_3), \ldots, a_{n-1}), a_n).$$

Множества a_i при этом будем называть *членами*, или *компонентами* набора $(a_1, \ldots, a_{n-1}, a_n)$.

Лемма 1.2.58. *Для любого натурального $n \geqslant 2$ и любых множеств $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ имеем*

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \iff a_i = b_i \text{ для всех } i \in \{1, \ldots, n\}.$$

Доказательство. Для каждого *конкретного* n утверждение получается $(n-1)$-кратным применением леммы 1.2.46. С помощью *индукции* и *рекурсии*, о которых речь пойдет далее, можно дать общее рассуждение, устанавливающее утверждение разом для всех n. □

Замечание 1.2.59. Для всех натуральных $n \geqslant 2$ для любого x имеем

$$x \in A_1 \times A_2 \times \ldots \times A_n \iff \exists a_1 \in A_1 \ldots \exists a_n \in A_n \; x = (a_1, \ldots, a_n)$$

и, в частности,

$$x \in A^n \iff \exists a_1 \in A \ldots \exists a_n \in A \; x = (a_1, \ldots, a_n).$$

Упражнение 1.2.60. Докажите, что если для какого-либо непустого множества A верно $A \subseteq A \times A$, то существует бесконечная последовательность множеств $\ldots x_{n+1} \in x_n \in \ldots \in x_1$.

Немного проще *аккуратно* вывести отсюда менее наглядное следствие: существует непустое множество X, т. ч. для любого $x \in X$ найдется $y \in X$ со свойством $y \in x$ [13].

Упражнение 1.2.61. Покажите, что для любых $A \neq \varnothing$ и $m, n \in \mathbb{N}$, если $m < n$, из $A^m \subseteq A^n$ следует тот же результат.

[13] Формально, утверждение про последовательность следует отсюда с помощью *принципа зависимого выбора*, о котором речь впереди.

Замечание 1.2.62. *Аксиома фундирования* гласит:

> Если множество A непусто, то найдется $x \in A$, т. ч. $y \notin x$ для всех $y \in A$.

При $A = \{x_1, \ldots, x_n, \ldots\}$ отсюда вытекает невозможность последовательности вида $\ldots x_{n+1} \in x_n \in \ldots \in x_1$, и мы приходим к важному выводу: если $A^m = A^n$, то $n = m$ или $A = \varnothing$.

§ 1.3. Отношения

Множество R называется *бинарным отношением* (или просто *отношением*, когда ясно, о чем речь), если каждый его элемент является упорядоченной парой множеств, т. е. если для всех x верно

$$x \in R \Longrightarrow \exists a \exists b\, x = (a, b).$$

Легко видеть, что если $(a, b) = \{\{a\}, \{a, b\}\} \in R$, то $\{a\} \in \cup R$ и $a \in \cup\cup R$. Аналогично, $b \in \cup\cup R$. Назовем *областью определения* отношения R множество

$$\operatorname{dom} R = \{a \in \cup\cup R \mid \exists b\, (a, b) \in R\}$$

и *областью значений* отношения R — множество

$$\operatorname{rng} R = \{b \in \cup\cup R \mid \exists a\, (a, b) \in R\}.$$

Это соответственно множества первых и вторых членов пар из R. Само множество $\cup\cup R$ называют *полем* отношения R.

Упражнение 1.3.1. Докажите, что $\cup\cup R = \operatorname{dom} R \cup \operatorname{rng} R$.

Лемма 1.3.2. *Для любых множеств R, A и B верно:*

1) *если $R \subseteq A \times B$, то R — бинарное отношение, причем* $\operatorname{dom} R \subseteq A$ *и* $\operatorname{rng} R \subseteq B$*;*

2) *если R — бинарное отношение, то $R \subseteq \operatorname{dom} R \times \operatorname{rng} R$.*

Таким образом, бинарные отношения суть в точности различные подмножества декартовых произведений $A \times B$ для всех возможных множеств A и B. Если $R \subseteq A \times B$, будем называть R *бинарным отношением между множествами A и B*.

Слово «бинарное» указывает, что берутся подмножества произведения *двух* множеств; легко также определить тернарные отношения как подмножества множества $A \times B \times C$ и т. д., чем мы пока не станем заниматься.

Пример 1.3.3. Множества $\varnothing$ и $A \times B$ являются бинарными отношениями между A и B. Пусть $A = \{0, 2, x, y\}$ и $B = \{z, 0, 1\}$ для любых x, y, z. Множество

$$R = \{(0, 0), (0, z), (x, 1), (y, 1)\}$$

является бинарным отношением между A и B. При этом $\operatorname{dom} R = \{0, x, y\} \subsetneq A$ (если x и y не равны 2) и $\operatorname{rng} R = B$.

Также говорят о *бинарных* (*тернарных, n-арных*) *отношениях на множестве* A, имея в виду множества $R \subseteq A^2$ ($R \subseteq A^3$, $R \subseteq A^n$).

Пример 1.3.4. На множестве $\mathbb{N}$ нам известно отношение строгого порядка $<$. Например, $(2, 3) \in <$, что традиционно записывают выражением $2 < 3$ (вообще, часто пишут xRy вместо $(x, y) \in R$). Очевидно, $(3, 2) \notin <$. Также на $\mathbb{N}$ нам знакомы отношения «меньше или равно» $\leqslant$, «больше» $>$ и «больше или равно» $\geqslant$.

Операции над отношениями. Пусть R — бинарное отношение. *Обратным* отношением к R называется отношение

$$R^{-1} = \{(b, a) \in \operatorname{rng} R \times \operatorname{dom} R \mid (a, b) \in R\}$$

(т. е. все пары в R «переворачиваются»).

Упражнение 1.3.5. Докажите, что $\cup\cup R^{-1} = \cup\cup R$, а затем $\operatorname{dom} R^{-1} = \operatorname{rng} R$ и $\operatorname{rng} R^{-1} = \operatorname{dom} R$.

Если фиксированы какие-либо множества A и B, т. ч. $R \subseteq A \times B$, определено *дополнение* $\bar{R}$ отношения R:

$$\bar{R} = (A \times B) \setminus R.$$

В частности, определено дополнение отношения *на множестве*.

Замечание 1.3.6. Согласно лемме 1.3.2, всегда можно рассматривать дополнение отношения R до множества $\operatorname{dom} R \times \operatorname{rng} R$, придав символу $\bar{R}$ смысл, не зависящий от выбора универсума, но мы не станем этого делать.

Пример 1.3.7. На множестве $\mathbb{N}$, очевидно, имеем $<^{-1} = >$ и $\bar{<} = \geqslant$ (если число m не меньше n, то m больше или равно n, и обратно).

Для любых отношений P и Q определена *композиция отношений* P *и* Q:

$$Q \circ P = \{(a, c) \in \operatorname{dom} P \times \operatorname{rng} Q \mid \exists b \big((a, b) \in P \text{ и } (b, c) \in Q\big)\}.$$

Замечание 1.3.8. Обратите внимание, что отношение, «действующее» первым, записывается справа (т. е. вторым). Это странное соглашение принято для сходства с композицией функций, о которой речь впереди, но которая, быть может, уже известна читателю: $(g \circ f)(x) = g(f(x))$.

Очевидно, что если $P \subseteq A \times B$ и $Q \subseteq B \times C$, то $Q \circ P \subseteq A \times C$. В частности, композиция отношений на множестве A сама является отношением на множестве A.

Пример 1.3.9. Поясним понятие композиции неформальной иллюстрацией. Пусть A и C суть две группы людей, читатели и писатели соответственно, а B — некоторая совокупность книг. Пусть отношения $P \subseteq A \times B$ и $Q \subseteq B \times C$ таковы, что aPb означает «a читал книгу b» и bQc означает «книга b написана автором c». Тогда $a(Q \circ P)c$ значит «a читал одну из книг писателя c».

Замечание 1.3.10. Наглядно бинарные отношения между A и B можно представить как множества «стрелок»: если $(a, b) \in R$, то в R имеется стрелка с началом в a и концом в b или, еще более наглядно, эта стрелка помечена буквой R: $a \xrightarrow{R} b$. Например, тогда $a(Q \circ P)c$ будет означать, что из a в c есть путь из двух стрелок через какую-то промежуточную точку b:

$$a \xrightarrow{P} b \xrightarrow{Q} c.$$

Упражнение 1.3.11. Пусть A — некоторая группа мужчин и aPb означает, что a сын b. Как понимать отношения $P \circ P$, P^{-1} и $P^{-1} \circ P$?

Пример 1.3.12. Имеем $\leqslant \circ < = \{(m, n) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N}\,(m < k \text{ и } k \leqslant n)\}$. Если $m < k$ и $k \leqslant n$, то $m < n$. Обратно, если $m < n$, то для $k = n$ имеем $m < k$ и $k \leqslant n$. Поэтому $\leqslant \circ < = <$.

Упражнение 1.3.13. Докажите, что $R \circ \varnothing = \varnothing \circ R = \varnothing$.

Теорема 1.3.14 (Ассоциативность композиции)**.** *Пусть P, Q и R суть бинарные отношения. Тогда*

$$R \circ (Q \circ P) = (R \circ Q) \circ P.$$

Доказательство. Для произвольной пары (a, d) имеем

$$\begin{array}{rcl}(a,d) \in R \circ (Q \circ P) & \iff & \exists c \big(a(Q \circ P)c \text{ и } cRd\big) \\ & \iff & \exists c \big(\exists b\,(aPb \text{ и } bQc) \text{ и } cRd\big) \\ & \iff & \exists c\, \exists b \big(aPb \text{ и } bQc \text{ и } cRd\big) \\ & \iff & \exists b\, \exists c \big(aPb \text{ и } bQc \text{ и } cRd\big) \\ & \iff & \exists b \big(aPb \text{ и } \exists c\,(bQc \text{ и } cRd)\big) \\ & \iff & \exists b \big(aPb \text{ и } b(R \circ Q)d)\big) \\ & \iff & (a,d) \in (R \circ Q) \circ P.\end{array}$$

□

Замечание 1.3.15. Ассоциативность композиции отношений позволяет опускать скобки при записи композиций: $P_1 \circ P_2 \circ \ldots \circ P_n$, поскольку безразлично, как эти скобки поставить.

Лемма 1.3.16. *Пусть P и Q — бинарные отношения. Тогда $(Q \circ P)^{-1} = P^{-1} \circ Q^{-1}$.*

Доказательство. Для произвольной пары (a, c) получаем

$$\begin{array}{rcl}(a,c) \in (Q \circ P)^{-1} & \iff & (c,a) \in Q \circ P \\ & \iff & \exists b\,(cPb \text{ и } bQa) \\ & \iff & \exists b\,((a,b) \in Q^{-1} \text{ и } (b,c) \in P^{-1}) \\ & \iff & (a,c) \in P^{-1} \circ Q^{-1}.\end{array}$$

□

Упражнение 1.3.17. Пусть $P \subseteq A \times B$, Q и R — бинарные отношения. Докажите:

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

2) $(P \cup Q)^{-1} = P^{-1} \cup Q^{-1}$.

3) $(\bar{P})^{-1} = \overline{P^{-1}}$.

4) $(P \cup Q) \circ R = (P \circ R) \cup (Q \circ R)$.

5) $(P \cap Q) \circ R \subseteq (P \circ R) \cap (Q \circ R)$.

Пример 1.3.18. Покажем, что в последнем утверждении упражнения включение не всегда можно заменить равенством. Рассмотрим отношения $R = \{(0,1),(0,2)\}$, $Q = \{(1,3)\}$ и $P = \{(2,3)\}$. Очевидно, что $(0,3) \in (P \circ R) \cap (Q \circ R)$, но $P \cap Q = \varnothing$.

Пример 1.3.19. Учитывая упражнение 1.3.17 и теорему 1.2.38, имеем

$$(P \cap Q)^{-1} = (\overline{\bar{P} \cup \bar{Q}})^{-1} = \overline{(\bar{P} \cup \bar{Q})^{-1}} = \\ = \overline{(\bar{P})^{-1} \cup (\bar{Q})^{-1}} = \overline{\overline{P^{-1}} \cup \overline{Q^{-1}}} = P^{-1} \cap Q^{-1}.$$

Пример 1.3.20. Пусть $P \subseteq Q$. Тогда $P \circ R \subseteq Q \circ R$. В самом деле, $P = P \cap Q$, откуда, по упражнению 1.3.17,

$$P \circ R = (P \cap Q) \circ R \subseteq (P \circ R) \cap (Q \circ R) \subseteq Q \circ R.$$

Аналогично имеем $P^{-1} \subseteq Q^{-1}$:

$$P^{-1} = (P \cap Q)^{-1} = P^{-1} \cap Q^{-1} \subseteq Q^{-1}.$$

Пример 1.3.21. Применяя упражнение 1.3.17 и лемму 1.3.16 к произвольным отношениям P, Q и R, получаем

$$(R \circ (P \cup Q))^{-1} = (P \cup Q)^{-1} \circ R^{-1} = \\ = (P^{-1} \cup Q^{-1}) \circ R^{-1} = (P^{-1} \circ R^{-1}) \cup (Q^{-1} \circ R^{-1}) = \\ = (R \circ P)^{-1} \cup (R \circ Q)^{-1} = ((R \circ P) \cup (R \circ Q))^{-1}.$$

Но тогда

$$R \circ (P \cup Q) = ((R \circ (P \cup Q))^{-1})^{-1} = \\ = (((R \circ P) \cup (R \circ Q))^{-1})^{-1} = (R \circ P) \cup (R \circ Q).$$

Аналогично устанавливается включение $R \circ (P \cap Q) \subseteq (R \circ P) \cap (R \circ Q)$.

Пример 1.3.22. Пусть $R \subseteq A \times B$, причем множества A и B непустые. Тогда $R^{-1} \neq \bar{R}$.

Рассуждая от противного, допустим, что $R^{-1} = \bar{R}$. Предположим вначале, что $A \cap B = \varnothing$. Если $R = \varnothing$, то $R^{-1} = \varnothing$. Однако $\bar{R} = (A \times B) \setminus \varnothing = A \times B \neq \varnothing$. Противоречие показывает, что $R \neq \varnothing$, т. е. $(a, b) \in R$ для некоторых $a \in A$ и $b \in B$. Но тогда $(b, a) \in R^{-1}$, откуда $(b, a) \in (A \times B) \setminus R$. Имеем $b \in A$, вопреки предположению $A \cap B = \varnothing$.

Итак, получили $A \cap B \neq \varnothing$. Рассмотрим некоторый $x \in A \cap B$. Если $(x, x) \in R$, то $(x, x) \in R^{-1} = \bar{R}$, т. е. $(x, x) \notin R$. Противоречие показывает, что $(x, x) \notin R$. Но тогда $(x, x) \in \bar{R} = R^{-1}$. Получаем $(x, x) \in R$ и новое противоречие. Следовательно, оставшееся предположение $R^{-1} = \bar{R}$ ложно.

На любом множестве A определено отношение

$$\mathrm{id}_A = \{(a,a) \mid a \in A\} = \{z \in A^2 \mid \exists a \in A\ z = (a,a)\}.$$

Упражнение 1.3.23. Докажите, что для любого отношения $R \subseteq A \times B$ верно $R \circ \mathrm{id}_A = R = \mathrm{id}_B \circ R$.

Пример 1.3.24. Пусть $R \subseteq A^2$. Всегда ли верно $R^{-1} \circ R = \mathrm{id}_A$? Отнюдь. Пусть $A = \mathbb{N}$ и $R = <$. Тогда

$$R^{-1} \circ R = > \circ < = \{(m,n) \in \mathbb{N}^2 \mid \exists k\,(m < k \text{ и } k > n)\}.$$

Очевидно, число k, большее и m, и n, существует для всех пар $(m,n) \in \in \mathbb{N}^2$. Иначе говоря, $R^{-1} \circ R = \mathbb{N}^2$.

Замечание 1.3.25. Множество $\mathcal{P}(A^2)$ (т. е. все отношения на A) с ассоциативной операцией $\circ$ образует *полугруппу с единицей* id_A. Операция $(\cdot)^{-1}$ не является групповой обратной в том смысле, что $R \circ R^{-1}$ не всегда есть id_A. Однако свойства $(R^{-1})^{-1} = R$ и $(R \circ Q)^{-1} = Q^{-1} \circ R^{-1}$, выполненные в группе, остаются верными. Такого рода структура называется *полугруппой (с единицей и) с инверсией.*

Образ множества. Пусть R — бинарное отношение и X — некоторое множество. Мы называем *образом под действием отношения* R (или, коротко, *R-образом*) *множества* X множество

$$R[X] = \{b \in \operatorname{rng} R \mid \exists a \in X\ aRb\}.$$

Множество $R^{-1}[X]$ традиционно называют *прообразом* множества X под действием R. Неформально, $R[X]$ есть концы всех тех R-стрелок, чьи начала лежат в X, а $R^{-1}[X]$ — соответственно начала всех тех R-стрелок, чьи концы лежат в X.

Замечание 1.3.26. Если $R \subseteq A \times B$, то $\operatorname{dom} R = R^{-1}[B]$ и $\operatorname{rng} R = R[A]$.

Пример 1.3.27. Пусть A есть некоторая совокупность городов, а xRy означает, что из города x можно проехать (по имеющимся дорогам) в город y. Тогда $R[X]$ есть все те города, куда можно добраться хотя бы из одного города $x \in X$.

Пример 1.3.28. Для натуральных чисел m и n запись $m \mid n$ означает, что существует $k \in \mathbb{N}$, т. ч. $n = mk$. Тогда говорят, что m *делит* n.

(Понятие делимости легко переносится на все целые числа. Например, $5 \mid -10$, поскольку $-10 = 5 \cdot (-2)$.)

Рассмотрим отношение $R = \{(m, n) \in \mathbb{N}^2 \mid m \mid n\}$. Тогда $R[\{2, 3\}]$ будет множество всех натуральных чисел, делящихся на 2 *или* на 3. Соответственно, $R^{-1}[\{2, 3\}]$ будут все числа, делящие 2 или 3. Очевидно, $R^{-1}[\{2, 3\}] = \{1, 2, 3\}$, $R[\{1\}] = \mathbb{N}$ и $R^{-1}[\{0\}] = \mathbb{N}$.

Пример 1.3.29. Покажем, что $R[X \cup Y] = R[X] \cup R[Y]$.

Пусть $b \in R[X]$. Тогда существует $a \in X$, т. ч. aRb. Тем более $a \in X \cup Y$. Значит, $b \in R[X \cup Y]$. Получили $R[X] \subseteq R[X \cup Y]$ и, аналогично, $R[Y] \subseteq R[X \cup Y]$. Отсюда $R[X] \cup R[Y] \subseteq R[X \cup Y]$.

Обратно. Пусть $b \in R[X \cup Y]$. Тогда найдется $a \in X \cup Y$, т. ч. aRb. Имеем $a \in X$ или $a \in Y$. В первом случае $b \in R[X]$, а во втором $b \in R[Y]$. В обоих случаях $b \in R[X] \cup R[Y]$.

Упражнение 1.3.30. Докажите, что из $X \subseteq Y$ следует $R[X] \subseteq R[Y]$.

Пример 1.3.31. Имеет место $R[X \cap Y] \subseteq R[X] \cap R[Y]$.

Действительно, если $b \in R[X \cap Y]$, то aRb для некоторого $a \in X \cap Y$. Имеем $a \in X$ и $a \in Y$, откуда $b \in R[X]$ и $b \in R[Y]$. Напротив, обратное включение верно не всегда. Например, возьмем $R = \{(0, 2), (1, 2)\}$. Для $X = \{0\}$ и $Y = \{1\}$ имеем $R[X] = R[Y] = R[X] \cap R[Y] = \{2\}$, но $R[X \cap Y] = R[\varnothing] = \varnothing$.

Упражнение 1.3.32. Докажите, что $(R \circ Q)[X] = R[Q[X]]$.

§ 1.4. Функции

Одним из важнейших понятий содержательной математики является функция. С помощью множеств можно аккуратно определить функции как отношения некоторого специального вида. Бинарное отношение R называется:

1) *функциональным*, если $\forall x \forall y \forall z\, ((xRy \text{ и } xRz) \Longrightarrow y = z)$;

2) *инъективным*, если $\forall x \forall y \forall z\, ((yRx \text{ и } zRx) \Longrightarrow y = z)$;

3) *тотальным для множества* Z, если $\forall x \in Z\, \exists y\, xRy$;

4) *сюръективным для множества* Z, если $\forall y \in Z\, \exists x\, xRy$.

Иначе говоря, инъективное отношение никогда не «склеивает» концы стрелок с разными началами, а функциональное, напротив, не допускает двух стрелок с общим началом и разными концами. Тотальность и сюръективность означают наличие R-стрелок с началами во всех точках Z или соответственно с концами во всех точках множества Z.

Замечание 1.4.1. Как видно, свойства функциональности и инъективности присущи самому отношению R как множеству пар. Напротив, свойства тотальности и сюръективности имеют дополнительный параметр — множество Z. (Например, любое отношение тотально и сюръективно относительно $\varnothing$.) Если мы рассматриваем R как отношение известных множеств A и B, просто *тотальное* отношение будет значить тотальное для A и просто *сюръективное* — сюръективное для множества B.

Пример 1.4.2. Отношение $<$ на множестве $\mathbb{N}$ тотально, поскольку для каждого m есть большее его n, но не функционально, так как такое n не единственно. Это отношение не инъективно, ибо $0 < 2$ и $1 < 2$, но $0 \neq 1$, и не сюръективно, потому что ни для какого n не верно $n < 0$. Напротив, отношение $\leqslant$ сюръективно, а $>$ не тотально.

Пусть $R = \{(x, y) \in \mathbb{R}_+ \times \mathbb{R} \mid x = y^2\}$, где $\mathbb{R}_+ = \{a \in \mathbb{R} \mid a > 0\}$. Тогда отношение R тотально, но не сюръективно (невозможно $xR0$). Далее, R инъективно: если $x = y^2$ и $z = y^2$, то $x = z$, но не функционально: имеем $(1, 1) \in R$ и $(1, -1) \in R$.

Лемма 1.4.3.

1) *R функционально $\iff$ R^{-1} инъективно;*

2) *R тотально для Z $\iff$ R^{-1} сюръективно для Z.*

Лемма 1.4.4. *Пусть $Q \subseteq A \times B$ и $R \subseteq B \times C$. Тогда:*

1) *если Q и R функциональны, то функционально $R \circ Q$;*

2) *если Q и R инъективны, то инъективно $R \circ Q$;*

3) *если Q и R тотальны, то тотально $R \circ Q$;*

4) *если Q и R сюръективны, то сюръективно $R \circ Q$.*

Доказательство. Проверим первое утверждение. Пусть $x(R \circ Q)y$ и $x(R \circ Q)z$. Тогда найдутся $u, v \in B$, для которых xQu, xQv, uRy и vRz. По функциональности Q имеем $u = v$, откуда uRy и uRz. Получаем $y = z$ по функциональности R.

Второе утверждение получается по лемме 1.4.3. Действительно, если $Q = (Q^{-1})^{-1}$ и $R = (R^{-1})^{-1}$ инъективны, то Q^{-1} и R^{-1} функциональны, а значит, функционально отношение $Q^{-1} \circ R^{-1} = (R \circ Q)^{-1}$. Следовательно, $R \circ Q$ инъективно.

Допустим теперь, что Q тотально для A и R тотально для B. Покажем, что отношение $R \circ Q$ тотально для A. Для произвольного $x \in A$

найдется u, т. ч. xQu. Однако $Q \subseteq A \times B$, а значит, $u \in B$. Но тогда существует y, т. ч. uRy. Итак, существует $u \in B$, для которого xQu и uRy, т.е. $x(R \circ Q)y$.

Последнее утверждение вновь получим по лемме 1.4.3. □

Упражнение 1.4.5. Пусть отношение $R \circ Q$ инъективно, а R тотально для $\operatorname{rng} Q$. Докажите, что тогда инъективно Q, но не всегда инъективно R.

Пример 1.4.6. Пусть отношение R функционально. Тогда $R^{-1}[X \cap Y] = R^{-1}[X] \cap R^{-1}[Y]$.

Включение слева направо мы уже установили в примере 1.3.31. Допустим, что $a \in R^{-1}[X]$ и $a \in R^{-1}[Y]$. Тогда найдутся $b \in X$ и $c \in Y$, т. ч. $bR^{-1}a$ и $cR^{-1}a$, т. е. aRb и aRc. В силу функциональности R имеем $b = c$. Но тогда $b \in X \cap Y$, а значит, $a \in R^{-1}[X \cap Y]$.

Пример 1.4.7. Пусть отношение $R \subseteq A \times B$ тотально. Тогда $X \subseteq$ $\subseteq R^{-1}[R[X]]$ для всех $X \subseteq A$.

Пусть $a \in X$. По тотальности, найдется $b \in B$, т. ч. aRb. Имеем $b \in R[X]$ и $bR^{-1}a$, откуда $a \in R^{-1}[R[X]]$.

Верно ли обратное включение? Не всегда: пусть $A = \{0, 1\}$, $B =$ $= \{2\}$, $R = \{(0, 2), (1, 2)\}$ и $X = \{1\}$. Тогда $R[X] = \{2\}$ и $R^{-1}[\{2\}] =$ $= \{0, 1\} \not\subseteq X$. Как видим, в приведенном примере R даже функционально.

Упражнение 1.4.8. Пусть отношение $R \subseteq A \times B$ функционально. Докажите, что $R[R^{-1}[X]] \subseteq X$ для любого множества X. Дополнительно потребовав тотальности R и $X \subseteq B$, приведите пример, когда нарушается обратное включение.

Функции и их значения. Функциональное отношение $f \subseteq A \times B$ называется *частичной функцией из множества A во множество B*. В таком случае пишем $f\colon A \xrightarrow{p} B$. Содержательно, частичные функции выражают «законы соответствия» элементов B элементам A, причем некоторым элементам A может ничего не соответствовать.

Пример 1.4.9. Отношение $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y^2 \text{ и } y \geqslant 0\}$ является известной частичной функцией «арифметический квадратный корень». Не у каждого вещественного числа есть (вещественный) квадратный корень, но ни у какого нет более одного неотрицательного корня. Соответственно, имеют место $f\colon \mathbb{R} \xrightarrow{p} \mathbb{R}$, $f\colon \mathbb{R} \xrightarrow{p} (\mathbb{R}_+ \cup \{0\})$ и $f\colon (\mathbb{R}_+ \cup \{0\}) \xrightarrow{p} (\mathbb{R}_+ \cup \{0\})$.

Пример 1.4.10. Отношение $f = \{(n, \frac{1}{n}) \in \mathbb{N} \times \mathbb{Q} \mid n \in \mathbb{N}_+\}$ является частичной функцией $\mathbb{N} \xrightarrow{p} \mathbb{Q}$, $\mathbb{N} \xrightarrow{p} [0,1]$, $\mathbb{N} \xrightarrow{p} \mathbb{R}$, $\mathbb{R} \xrightarrow{p} \mathbb{Q}$, $\mathbb{N}_+ \xrightarrow{p} [0,1]$ и т. д.

Пример 1.4.11. Пусть $f\colon \varnothing \xrightarrow{p} B$ для некоторого множества B. Когда это возможно?

Имеем $f \subseteq \varnothing \times B = \varnothing$, т. е. $f = \varnothing$. Легко проверить, что отношение $f = \varnothing$, действительно, функционально, инъективно и тотально для $\varnothing$. Очевидно, f будет сюръективно для B тогда и только тогда, когда $B = \varnothing$.

Элемент (т. е. множество) b назовем *значением* частичной функции $f\colon A \xrightarrow{p} B$ на элементе a, если afb. Функциональность гарантирует, что для каждого a существует не более одного такого значения b, причем $b \in B$. Значение f на элементе a обозначается $f(a)$.

Разумеется, значение на a может и не существовать. Тогда символ $f(a)$ не обозначает никакого множества. Это обстоятельство создает трудности в обращении с такими обозначениями. Если значение $f(a)$ существует, говорят, что функция f *определена* на элементе a, и пишут $f(a)\downarrow$. В противном случае пишут $f(a)\uparrow$. Очевидно, что $f(a)\downarrow$ равносильно $a \in \operatorname{dom} f$.

Замечание 1.4.12. Пусть $f\colon \varnothing \xrightarrow{p} B$ для некоторого множества B. Как мы видели в примере 1.4.11, это утверждение равносильно $f = \varnothing$. Ясно, что $\operatorname{dom} f = \varnothing$, а значит, $\forall a \in \varnothing\ f(a)\downarrow$. Тут возникает забавный парадокс: на всех элементах a пустого множества определено значение $f(a)$, притом что этот символ (для нашей f) никакого множества означать не может!

Разумеется, парадокс легко исчезает, если не использовать «бессмысленный» символ $f(a)$. (Собственно говоря, $f(a)$ есть типичный пример *«нынешнего короля Франции»*, о котором шла речь в § 1.2.) В самом деле, равносильное выражение

$$\forall a \in \varnothing\, \exists b \in B\ afb$$

истинно по тривиальным причинам и никак не парадоксально.

Аналогично, «неопределенный» символ $f(a)$ может быть устранен и в других случаях. Например, можно утверждать, что $f(a) = 1$ для всех $a \in \varnothing$, хотя выражение $f(a)$ при $a \in \varnothing$ не означает никакого множества, которое можно было бы сравнить с числом 1. Но мы считаем приведенное утверждение эквивалентным такому:

$$\forall a \in \varnothing\ \forall b\ ((a,b) \in f \Longrightarrow b = 1).$$

Последнее, очевидно, верно.

Если f и g суть частичные функции, то будем писать $f(x) \simeq g(y)$ (читаем: «f на x совпадает с g на y»), если

$$f(x)\downarrow \text{ и } g(y)\downarrow \text{ и } f(x) = g(y)$$

или

$$f(x)\uparrow \text{ и } g(y)\uparrow .$$

Частичные функции равны тогда и только тогда, когда они всюду совпадают. Убедимся в этом.

Лемма 1.4.13. *Пусть* $f\colon A \xrightarrow{p} B$ *и* $g\colon C \xrightarrow{p} D$. *Тогда*

$$f = g \iff \forall x\, f(x) \simeq g(x).$$

Доказательство. Пусть $f = g$. Тогда, очевидно, $\operatorname{dom} f = \operatorname{dom} g$ (если сомневаетесь, см. замечание 1.2.3).

Рассмотрим произвольное множество x. Если $x \notin \operatorname{dom} f$, то $x \notin \operatorname{dom} g$ и $f(x) \simeq g(x)$. Если же $x \in \operatorname{dom} f$, то $x \in \operatorname{dom} g$. В таком случае существуют $y \in B$ и $z \in C$, т. ч. $(x, y) \in f$ и $(x, z) \in g$. Из $f = g$ следует $(x, y), (x, z) \in f$, откуда $y = z$ по функциональности. Итак, $f(x) = y = z = g(x)$ и $f(x) \simeq g(x)$.

Обратно, пусть $f(x) \simeq g(x)$ для всех x. Предположим, что $(x, y) \in f$. Тогда $x \in \operatorname{dom} f$ и $f(x) = y$. По условию имеем также $x \in \operatorname{dom} g$ и $g(x) = f(x) = y$. Значит, $(x, y) \in g$. Обратное включение аналогично. □

Замечание 1.4.14. Если $f\colon A_1 \times A_2 \times \ldots \times A_n \xrightarrow{p} B$, где $n \geqslant 2$, и в частности, $f\colon A^n \xrightarrow{p} B$, то говорят, что f есть *частичная функция n аргументов*. Значение такой функции обычно обозначают $f(a_1, \ldots, a_n)$ вместо $f((a_1, \ldots, a_n))$. (Очевидно, любую функцию можно объявить *функцией одного аргумента*, но если множества $A_1, \ldots, A_n$ фиксированы, этот титул достанется функциям $A_i \xrightarrow{p} B$.)

Замечание 1.4.15. Ясно, что $\{f(a)\} = f[\{a\}]$ для любых $f\colon A \xrightarrow{p} B$ и $a \in \operatorname{dom} f$.

Замечание 1.4.16. Множество $R[X]$ — в частности, когда $R = f$ есть частичная функция, — обычно обозначают символом $R(X)$ (соответственно $f(X)$). Мы предпочли так не делать, чтобы не смешать значение $f(x)$ частичной функции $f\colon A \xrightarrow{p} B$ на $x \in A$ с образом $f(X)$ множества $X \subseteq A$ под действием f.

По лемме 1.4.4 из $f\colon A \xrightarrow{p} B$ и $g\colon B \xrightarrow{p} C$ следует $g \circ f\colon A \xrightarrow{p} C$, т. е. композиция частичных функций тоже частичная функция.

Пример 1.4.17. Для $f\colon A \xrightarrow{p} B$ и $g\colon B \xrightarrow{p} C$ имеем

$$\operatorname{rng}(g \circ f) = (g \circ f)[A] = g[f[A]] = g[\operatorname{rng} f]$$

и

$$\operatorname{dom}(g \circ f) = (g \circ f)^{-1}[C] = (f^{-1} \circ g^{-1})[C] = f^{-1}[g^{-1}[C]] = f^{-1}[\operatorname{dom} g].$$

Упражнение 1.4.18. Пусть $f\colon A \xrightarrow{p} B$ и $g\colon B \xrightarrow{p} C$. Докажите, что для всех $a \in A$ верно $(g \circ f)(a) \simeq g(f(a))$.

Частичная функция $f\colon A \xrightarrow{p} B$ называется *функцией из множества A во множество B*, если f тотальна для A. В таком случае пишем $f\colon A \to B$. Очевидно, композиция функций является функцией. Множество $\{f \in \mathcal{P}(A \times B) \mid f\colon A \to B\}$ всех функций из A в B обозначают символом B^A; аналогия с обозначением степени числа, как мы надеемся, станет ясной далее.

Упражнение 1.4.19. При каких условиях из $B^A = D^C$ следует $A = C$ и $B = D$?

Функции еще называют *отображениями* или *соответствиями*, а функции из $\mathbb{N}$ в какое-нибудь множество A — *последовательностями элементов A*. Например, функция $f\colon \mathbb{N} \to \mathbb{Q}$, т. ч. $f(n) = \frac{1}{1+n}$ для всех $n \in \mathbb{N}$, есть последовательность рациональных чисел.

Следствие 1.4.20. *Пусть $f\colon A \to B$ и $g\colon C \to D$. Тогда*

$$f = g \iff A = C \text{ и } \forall a \in A\ f(a) = g(a).$$

Итак, чтобы задать функцию, достаточно указать ее область определения и значение на каждом элементе этой области.

Замечание 1.4.21. Если $f\colon A^n \to B$ и $f\colon A^m \to B$, то $A^n = \operatorname{dom} f = A^m$. Если при этом $A \neq \varnothing$, то, как показывает замечание 1.2.62, $n = m$. Иначе говоря, в таком случае число аргументов функции (при фиксированном A) определено однозначно.

Упражнение 1.4.22. Пусть $f\colon A \to B$ и $X \subseteq A$. Докажите, что

$$f[X] \subseteq Y \iff X \subseteq f^{-1}[Y].$$

Пример 1.4.23. Пусть $f\colon A \to B$ и $g\colon A \to B$. Покажем, что $f \cap g\colon A \to \to B$ тогда и только тогда, когда $f = g$.

Если $f = g$, то, конечно, $f \cap g = f\colon A \to B$. Теперь предположим, что $f \cap g\colon A \to B$. Пусть $(a, b) \in f$. В силу тотальности $f \cap g$ найдется $c \in B$, т. ч. $(a, c) \in f \cap g$, откуда $(a, c) \in f$ и $(a, c) \in g$. По функциональности f имеем $b = c$, а значит, $(a, b) \in g$. Итак, $f \subseteq g$. Обратное включение устанавливается аналогично.

Упражнение 1.4.24. Когда, в условиях предыдущего примера, $f \cup g$ является функцией?

Ограничение функции. Пусть $f\colon A \xrightarrow{p} B$ и X — некоторое множество. *Ограничением* частичной функции f на X мы называем множество

$$f \restriction X = f \cap (X \times B).$$

Содержательно, в $f \restriction X$ остаются лишь те стрелки из f, чьи начала лежат в X. Формально $f \restriction X$ зависит от выбора множества B, но легко убедиться, что $f \restriction X = f \cap (X \times \operatorname{rng} f)$, а значит, любой выбор B с условием $f\colon A \xrightarrow{p} B$, т. е. $\operatorname{rng} f \subseteq B$, даст один и тот же результат.

Лемма 1.4.25. *Пусть $f\colon A \xrightarrow{p} B$. Тогда:*

1) $f \restriction X\colon X \xrightarrow{p} B$;

2) *если f инъективно, то инъективно и $f \restriction X$;*

3) *если f тотально для A и $X \subseteq A$, то $f \restriction X$ тотально для X.*

Доказательство. Достаточно заметить, что $f \restriction X = f \circ \mathrm{id}_X$, и воспользоваться леммой 1.4.4. □

Если $X \subseteq A$, частичная функция f называется *продолжением* частичной функции $f \restriction X$.

Замечание 1.4.26. Очевидно, $(f \restriction X) \restriction Y = f \restriction (X \cap Y)$.

Замечание 1.4.27. Можно рассмотреть понятие ограничения не только для частичных функций, но и для любых отношений. Тогда естественно возникают *ограничение R на X*, *ограничение R на X слева* и *ограничение R на X справа* — это соответственно отношения $R \cap X^2$, $R \cap (X \times \operatorname{rng} R)$ и $R \cap (\operatorname{dom} R \times X)$.

§ 1.5. Инъекции, сюръекции, биекции

Если функция $f\colon A \to B$ инъективна, она называется *инъекцией из A в B*. Если сюръективна, — называется *сюръекцией из A в B*. Наконец, если f инъективна и сюръективна, она называется *биекцией из A в B*.

Пример 1.5.1. Для любого множества A отношение id_A является биекцией из A в A.

На практике, вводя новые функции, часто используют некоторое сокращение. Например, пишут $f\colon \mathbb{N} \to \mathbb{N}$, $f\colon n \mapsto n+1$, имея в виду, что

$$f = \{(n, m) \in \mathbb{N}^2 \mid m = n + 1\}.$$

Иногда при этом опускают и само имя f. В обращении с таким сокращением нужна осторожность: скажем, $a^2 \mapsto a$ не задает функцию $\mathbb{Z} \to \mathbb{Z}$, т. к. числу 1 соответствуют 1 и -1.

Пример 1.5.2. Функция $x \mapsto e^x$ является инъекцией $\mathbb{R} \to \mathbb{R}$ и биекцией $\mathbb{R} \to \mathbb{R}_+$. Функция $x \mapsto x^2$ является сюръекцией $\mathbb{R} \to (\mathbb{R}_+ \cup \{0\})$, но не инъекцией. Функция $(n, m) \mapsto n + m$ является сюръекцией $\mathbb{N}^2 \to \mathbb{N}$, но не инъекцией.

Упражнение 1.5.3. Пусть $f\colon A \to B$ и $g\colon B \to C$. Докажите, что если $g \circ f$ инъекция, то f инъекция, а если $g \circ f$ сюръекция, то g — сюръекция.

Лемма 1.5.4. *Отношение $R \subseteq A \times B$ является биекцией из A в B тогда и только тогда, когда R^{-1} является биекцией из B в A.*

Доказательство. Требуемое легко следует из леммы 1.4.3. □

Упражнение 1.5.5. Докажите, что если $f\colon A \to B$ и $f^{-1}\colon B \to A$, то f есть биекция из A в B.

Теорема 1.5.6. *Отношение $R \subseteq A \times B$ является биекцией из A в B тогда и только тогда, когда*

$$R^{-1} \circ R = \mathrm{id}_A \quad \textit{и} \quad R \circ R^{-1} = \mathrm{id}_B.$$

Доказательство. Пусть $R\colon A \to B$ является биекцией. Допустим, что $(x, y) \in R^{-1} \circ R$. Тогда найдется $z \in B$, т. ч. xRz и $zR^{-1}y$, т. е. xRz и yRz. По инъективности R имеем $x = y$, т.е. $(x, y) \in \mathrm{id}_A$. Обратно, пусть

$(x, x) \in \mathrm{id}_A$. По тотальности R найдется $z \in B$, т. ч. xRz и, следовательно, $zR^{-1}x$. Значит, $(x, x) \in R^{-1} \circ R$. Второе равенство устанавливается аналогично с использованием функциональности и сюръективности R.

Предположим теперь, что наши равенства выполнены. Тогда для любого $z \in B$ имеем $(z, z) \in R \circ R^{-1}$, т. е. найдется $x \in A$, т. ч. xRz. Значит, R сюръективно. Пусть xRz и xRw. Тогда также $zR^{-1}x$, откуда $(z, w) \in R \circ R^{-1} = \mathrm{id}_B$. Следовательно, $z = w$ и R функционально. Инъективность и тотальность R извлекаются из первого равенства аналогичным образом. □

В свете установленных теорем ясно, почему биекции также называют *взаимно однозначными соответствиями*.

Замечание 1.5.7. Лемма 1.4.4 показывает, что композиция двух биекций есть всегда биекция, а лемма 1.5.4 и теорема 1.5.6 обеспечивают, что для любой биекции $f\colon A \to A$ обратное отношение f^{-1} не только является биекцией, но и «обратно» относительно композиции: $f \circ f^{-1} = \mathrm{id}_A = f^{-1} \circ f$. Таким образом, для любого A множество всех биекций из A в A с операциями $\circ$ и $(\cdot)^{-1}$ образует *группу*, называемую *симметрической группой* множества A.

Равномощность. Биекции очень важны в математике. Содержательно, наличие биекции между двумя множествами означает, что в них содержится «равное число элементов». Это понятие нетривиально для бесконечных множеств. Например, четных натуральных чисел «столько же», сколько всех натуральных, ибо имеется биекция $n \mapsto 2n$ из $\mathbb{N}$ во множество четных.

Будем писать $A \overset{f}{\sim} B$, если $f\colon A \to B$ есть биекция. Скажем, что множество A *равномощно* множеству B, если существует f, т. ч. $A \overset{f}{\sim} B$. Тогда пишем $A \sim B$.

Лемма 1.5.8. *Для любых A, B, C имеем:*

1) $A \sim A$;

2) *если* $A \sim B$, *то* $B \sim A$;

3) *если* $A \sim B$ *и* $B \sim C$, *то* $A \sim C$.

Доказательство. Очевидно, $A \overset{\mathrm{id}_A}{\sim} A$. Если $A \overset{f}{\sim} B$, то $B \overset{f^{-1}}{\sim} A$ по лемме 1.5.4. Если $A \overset{f}{\sim} B$ и $B \overset{g}{\sim} C$, то $A \overset{g \circ f}{\sim} C$ в силу леммы 1.4.4. □

Замечание 1.5.9. Пусть $f\colon A \to B$ — инъекция. Ясно, что $X \overset{f}{\sim} f[X]$ для любого множества $X \subseteq A$. Также нетрудно заметить, что $f \sim \operatorname{dom} f$ для каждой частичной функции f.

Пример 1.5.10. Убедимся, что $\mathbb{N}^2 \sim \mathbb{N}$, и явно укажем одну из биекций. То, что существует «достаточно простая» такая биекция, играет важную роль: это позволяет «достаточно свободно» переходить от пар (троек и т. д.) натуральных чисел, естественно возникающих в математике[14], к их «кодам» — натуральным числам, и обратно.

Итак, положим $f(m,n) = 2^m(2n+1)-1$ для всех $(m,n) \in \mathbb{N}^2$. Если $f(m,n) = f(m',n')$, то $2^m(2n+1) = 2^{m'}(2n'+1)$. Допустим, что $m \neq m'$ и, без ограничения общности[15], $m < m'$. Тогда $2n+1 = 2^{m'-m}(2n'+1)$, причем второе число четно, а первое нечетно. Противоречие показывает, что $m = m'$. Но тогда $2n+1 = 2n'+1$, откуда $n = n'$. Итак, f — инъекция. Установим сюръективность. Пусть некоторое *положительное* натуральное число не имеет вида $2^m(2n+1)$. Тогда найдется *наименьшее* такое число k. Это число четно (иначе оно имело бы вид $2^0(2n+1)$). Следовательно, $k = 2k'$. Однако $k' < k$, а значит, $k' = 2^{m'}(2n'+1)$ для некоторых $m', n' \in \mathbb{N}$. Но тогда $k = 2^{m'+1}(2n'+1)$. Противоречие. Итак, каждое положительное натуральное число имеет вид $f(m,n)+1$. Очевидно, тогда f — сюръекция из $\mathbb{N}^2$ в $\mathbb{N}$.

Как мы помним, вообще говоря, $A \times B \neq B \times A$. Однако, если вместо равенства рассматривать равномощность, декартово произведение ведет себя подобно обыкновенному умножению (скажем, натуральных чисел), причем B^A оказывается подобно возведению в степень. Следующие утверждения широко употребляются в математике.

Теорема 1.5.11. *Для любых множеств A, B и C имеет место:*

1) *если $A \sim B$, то $A \times C \sim B \times C$, $A^C \sim B^C$ и $C^A \sim C^B$;*

2) $A \times B \sim B \times A$;

3) $(A \times B) \times C \sim A \times (B \times C)$;

4) $(A \times B)^C \sim A^C \times B^C$;

5) $(C^B)^A \sim C^{A \times B}$.

[14] Например, рациональные числа можно рассматривать как тройки натуральных «числитель-знаменатель-знак» ($\frac{2}{4} = \frac{1}{2}$, так что некоторые тройки нужно отождествить).

[15] Такой способ речи означает, что остающиеся случаи вполне подобны разбираемым.

Доказательство.

1) Пусть $A \overset{\varphi}{\sim} B$. Положим $\psi\colon (a,c) \mapsto (\varphi(a),c)$ для всех $a \in A$ и $c \in C$ (напомним, по лемме 1.2.46 любой элемент множества $A \times C$ *однозначно* представляется в виде (a,c)). Тогда функции $\psi\colon A \times C \to B \times C$ есть биекция. Действительно, пусть $(a,c) \neq \neq (a',c')$. Тогда $a \neq a'$, и $\varphi(a) \neq \varphi(a')$ по инъективности φ, или же $c \neq c'$. В обоих случаях $\psi(a,c) \neq \psi(a',c')$. Следовательно, ψ есть инъекция. Для любого $(b,c) \in B \times C$ найдется $a \in A$, т. ч. $\varphi(a) = b$ по сюръективности φ, а значит, имеем $\psi(a,c) = (b,c)$ для этого a. Таким образом, ψ — сюръекция. Итак, $A \times C \overset{\psi}{\sim} B \times C$.

   Теперь положим $\psi\colon f \mapsto \varphi \circ f$ для всех $f \in A^C$. Имеем $(\varphi \circ f)\colon C \to \to B$. Таким образом, $\psi\colon A^C \to B^C$. Проверим, что ψ является биекцией. Если $f \neq f'$, то, согласно следствию 1.4.20, найдется $c \in C$, т. ч. $f(c) \neq f'(c)$. Поэтому, в силу инъективности φ,

$$(\psi(f))(c) = (\varphi \circ f)(c) = \varphi(f(c)) \neq \\ \neq \varphi(f'(c)) = (\varphi \circ f')(c) = (\psi(f'))(c),$$

   а значит, $\psi(f) \neq \psi(f')$. Итак, ψ инъективно. Пусть $g \in B^C$. Ясно, что $\varphi^{-1} \circ g \in A^C$. С другой стороны,

$$\psi(\varphi^{-1} \circ g) = \varphi \circ (\varphi^{-1} \circ g) = (\varphi \circ \varphi^{-1}) \circ g = \mathrm{id}_B \circ g = g.$$

   Поэтому функция ψ сюръективна. Имеем $A^C \overset{\psi}{\sim} B^C$.

   Наконец, положив $\psi\colon f \mapsto f \circ \varphi^{-1}$ для всех $f \in C^A$, имеем $C^A \overset{\psi}{\sim} \overset{\psi}{\sim} C^B$. Проверка оставляется читателю.

2) Рассматриваем биекцию $\psi\colon (a,b) \mapsto (b,a)$.

3) Рассматриваем биекцию $\psi\colon ((a,b),c) \mapsto (a,(b,c))$.

4) Рассмотрим функции-*проекторы* $\pi_1\colon A \times B \to A$ и $\pi_2\colon A \times B \to B$, т. ч. $\pi_1\colon (a,b) \mapsto a$ и $\pi_1\colon (a,b) \mapsto b$ для всех $a \in A$, $b \in B$ [16].

[16] Для удовольствия придирчивого читателя и для сравнения дадим более аккуратное определение π_1:

$$\pi_1 = \{z \in (A \times B) \times A \mid \exists a \in A\, \exists b \in B\ z = ((a,b),a)\}.$$

Пусть $(x,y),(x,y') \in \pi_1$. Тогда существуют $a,a' \in A$ и $b,b' \in B$, т. ч. $x = (a,b)$, $x = (a',b')$, $y = a$ и $y' = a'$. По лемме 1.2.46, $a = a'$, откуда $y = y'$. Следовательно, отношение π_1 функционально. Пусть $x \in A \times B$. Тогда найдутся $a \in A$ и $b \in B$, т. ч. $x = (a,b)$. Значит, $(x,a) \in \pi_1$ для этого a. Итак, π_1 тотально.

Положим теперь $\psi\colon f \mapsto (\pi_1 \circ f, \pi_2 \circ f)$ для всех $f \in (A \times B)^C$. Ясно, что $\psi\colon (A \times B)^C \to A^C \times B^C$. Проверим инъективность ψ. Пусть $f \neq f'$. Тогда $f(c) \neq f'(c)$ для некоторого $c \in C$. Допустим, что $f(c) = (a, b)$ и $f'(c) = (a', b')$. Имеем $a \neq a'$ или $b \neq b'$. В первом случае $(\pi_1 \circ f)(c) = a \neq a' = (\pi_1 \circ f)(c)$, т. е. $\pi_1 \circ f \neq \pi_1 \circ f'$. Значит, $\psi(f) \neq \psi(f')$. То же и во втором случае. Проверим сюръективность. Пусть $g_1 \in A^C$ и $g_2 \in B^C$. Тогда, полагая $f\colon c \mapsto (g_1(c), g_2(c))$ для всех $c \in C$, имеем $\pi_1 \circ f = g_1$ и $\pi_2 \circ f = g_2$, т. е. $\psi(f) = (g_1, g_2)$.

5) Для всех $f \in (C^B)^A$ и $z \in A \times B$ положим

$$\psi(f)\colon z \mapsto (f(\pi_1(z)))(\pi_2(z)).$$

Поскольку $f(\pi_1(z)) \in C^B$ и $\pi_2(z) \in B$, имеем $\psi(f)\colon A \times B \to C$. Следовательно, $\psi\colon (C^B)^A \to C^{A \times B}$. Пусть $f \neq f'$. Тогда найдется $a \in A$, т. ч. $f(a) \neq f'(a)$, а значит, также найдется $b \in B$, т. ч. $(f(a))(b) \neq (f'(a))(b)$. Положив $z = (a, b)$, имеем

$$(\psi(f))(z) = (f(\pi_1(z)))(\pi_2(z)) = (f(a))(b) \neq$$
$$\neq (f'(a))(b) = (f'(\pi_1(z)))(\pi_2(z)) = (\psi(f'))(z).$$

Итак, $\psi(f) \neq \psi(f')$, т. е. ψ есть инъекция. Проверим сюръективность. Пусть $g \in C^{A \times B}$. Для всех $a \in A$ положим $f(a)\colon b \mapsto g(a, b)$. Поскольку $f(a) \in C^B$, имеем $f \in (C^B)^A$. Далее, если $z = (a, b)$, то

$$(\psi(f))(z) = (f(\pi_1(z)))(\pi_2(z)) = (f(a))(b) = g(a, b) = g(z)$$

при всех $(a, b) \in A \times B$. Следовательно, $\psi(f) = g$.

□

Пример 1.5.12. Посмотрим, как выглядит биекция ψ (точнее, ψ^{-1}) для последнего утверждения теоремы в одном частном случае. Пусть $A = B = C = \mathbb{N}$ и функция $g \in \mathbb{N}^{\mathbb{N} \times \mathbb{N}}$ есть сложение. Положим $h_k\colon x \mapsto k + x$. Тогда $h_k \in \mathbb{N}^{\mathbb{N}}$ при всех $k \in \mathbb{N}$. Если $f\colon k \mapsto h_k$, то $f \in (\mathbb{N}^{\mathbb{N}})^{\mathbb{N}}$ и $(\psi(f))(k, x) = (f(k))(x) = h_k(x) = k + x = g(k, x)$, т. е. $\psi(f) = g$.

Обратите внимание, что биекция ψ^{-1} устраняет функцию двух аргументов g, «заменяя» ее семейством функций *одного* аргумента $h_0, h_1, \ldots$, которое, в свою очередь, задается функцией *одного* аргумента f. Такое преобразование, называемое *преобразованием Карри* (currying) играет важную роль в информатике и математике, включая отраженную в нашем курсе часть математической логики.

Замечание 1.5.13. Развивая аналогию декартова произведения с умножением, видим, что у первого тоже есть «единица», хотя и не единственная. Действительно, для произвольных множеств A и x верно $A \times \{x\} \sim A$.

Упражнение 1.5.14. Покажите, что в некотором смысле «показатели степеней» можно складывать: если $A \cap B = \varnothing$, то $C^{A \cup B} \sim C^A \times C^B$.

Вложения. По определению, множество A *не превосходит по мощности* (или *вкладывается во*) множество B, если существует инъекция $f\colon A \to B$. Тогда пишем $A \overset{f}{\lesssim} B$ и $A \lesssim B$.

Смысл понятия в том, что во множестве B «не меньше» элементов, чем в A. В самом деле, концы f-стрелок выделяют в B «копию» множества A, поскольку стрелки с разными началами имеют разные концы.

Пример 1.5.15. Если $A \subseteq B$, то $A \overset{\mathrm{id}_A}{\lesssim} B$. Пусть $2\mathbb{N}$ есть множество всех четных натуральных чисел. Имеем $\mathbb{N} \lesssim 2\mathbb{N}$ и тем более $2\mathbb{N} \lesssim \mathbb{N}$. При этом $\mathbb{N} \neq 2\mathbb{N}$, хотя $\mathbb{N} \sim 2\mathbb{N}$.

Лемма 1.5.16. *Для любых A, B, C имеем:*

1) $A \lesssim A$;

2) *если* $A \lesssim B$ *и* $B \lesssim C$, *то* $A \lesssim C$;

3) *если* $A \sim B$, *то* $A \lesssim B$ *и* $B \lesssim A$;

4) $A \lesssim B \iff \exists D \subseteq B\ A \sim D$.

Доказательство. В последнем утверждении, учитывая замечание 1.5.9, достаточно положить $D = f[A]$, где $f\colon A \to B$ есть некоторая инъекция. □

Упражнение 1.5.17. Докажите, что $A \lesssim \mathcal{P}(A)$ для любого A.

Теорема 1.5.18 (Кантора)**.** *Ни для какого множества A невозможно $\mathcal{P}(A) \lesssim A$.*

Доказательство. Пусть не так. Рассмотрим произвольную инъекцию $f\colon \mathcal{P}(A) \to A$. Положим

$$Y = \{a \in A \mid \forall X \in \mathcal{P}(A)\,(a = f(X) \Longrightarrow a \notin X)\}.$$

Очевидно, $Y \in \mathcal{P}(A)$. Если $f(Y) \in Y$, то, взяв $X = Y$, получаем $f(Y) \notin Y$. Противоречие показывает, что $f(Y) \notin Y$. Рассмотрим произвольное $X \in \mathcal{P}(A)$, т. ч. $f(Y) = f(X)$. В силу инъективности f имеем $X = Y$. Но тогда $f(Y) \notin X$ для всех таких X. По определению множества Y получаем $f(Y) \in Y$. Противоречие. □

Обратите внимание на сходство приведенных рассуждений с рассуждениями, приводящими к парадоксу Рассела. При «правильном применении» идеи парадоксов нередко дают любопытные теоремы!

Упражнение 1.5.19. Из теоремы 1.5.18 выведите, что не существует множества всех множеств.

Замечание 1.5.20. Из анализа известно, что $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. Множество $\mathcal{P}(\mathbb{N})$ называется *континуумом*, поскольку равномощно «непрерывной» совокупности точек прямой. Как видим, $\mathbb{N} \nsim \mathbb{R}$, т. е. невозможно взаимно однозначное соответствие между точками прямой и натурального ряда.

Континуум-гипотеза утверждает, что если $\mathbb{N} \lesssim X \lesssim \mathcal{P}(\mathbb{N})$, то $X \sim \mathbb{N}$ или $X \sim \mathcal{P}(\mathbb{N})$. Иначе говоря, нет «количества элементов», промежуточного между $\mathbb{N}$ и континуумом. Доказано, что ни это утверждение, ни его отрицание не приводят к противоречию при добавлении к прочим нашим постулатам о множествах (а значит, ни одно не следует из них), если сами эти постулаты непротиворечивы.

Итак, образование множества, промежуточного между $\mathbb{N}$ и $\mathcal{P}(\mathbb{N})$, представляет собой новый способ задания множеств, который можно принимать, не принимать или запрещать, в зависимости от того, кажутся ли получаемые при этом теоремы содержательной математики достоверными. Следуя принятой практике, мы будем консервативны и не станем принимать ни гипотезы, ни ее отрицания.

Теорема 1.5.21 (Кантора— Шрёдера— Бернштейна)**.** *Для любых множеств A и B, если $A \lesssim B$ и $B \lesssim A$, то $A \sim B$.*

Пусть U — какое-либо множество. Функцию $F\colon \mathcal{P}(U) \to \mathcal{P}(U)$ назовем *монотонной*, если $X \subseteq Y$ влечет $F(X) \subseteq F(Y)$ для всех $X, Y \subseteq U$.

Лемма 1.5.22 (о неподвижной точке монотонного оператора)**.** *Для любого множества U и любой монотонной функции $F\colon \mathcal{P}(U) \to \mathcal{P}(U)$ найдется $Z \subseteq U$, т. ч. $F(Z) = Z$.*

Доказательство. Рассмотрим множество

$$S = \{X \in \mathcal{P}(U) \mid X \subseteq F(X)\}.$$

Положим $Z = \bigcup S$. Ясно, что для всех $X \in S$ верно $X \subseteq F(X)$ и $X \subseteq Z$, откуда $F(X) \subseteq F(Z)$ в силу монотонности и, далее, $X \subseteq F(Z)$. Значит, $Z = \bigcup S \subseteq F(Z)$.

По монотонности из $Z \subseteq F(Z)$ получаем $F(Z) \subseteq F(F(Z))$, что означает $F(Z) \in S$. Но тогда $F(Z) \subseteq \bigcup S = Z$. Итак, $F(Z) = Z$. □

Доказательство теоремы 1.5.21. Пусть есть инъекции $f\colon A \to B$ и $g\colon B \to A$. Рассмотрим функцию $F\colon \mathcal{P}(A) \to \mathcal{P}(A)$, т. ч.

$$F(X) = g[B \setminus f[A \setminus X]]$$

для всех $X \subseteq A$. Проверим, что функция F монотонна.

В самом деле, пусть $X \subseteq Y$. Используя упражнения 1.2.36 и 1.3.30, последовательно получаем: $A \setminus Y \subseteq A \setminus X$, $f[A \setminus Y] \subseteq f[A \setminus X]$, $B \setminus f[A \setminus X] \subseteq B \setminus f[A \setminus Y]$ и, наконец, $g[B \setminus f[A \setminus X]] \subseteq g[B \setminus f[A \setminus Y]]$.

По лемме 1.5.22 найдется $Z \subseteq A$, т. ч. $F(Z) = Z$. Поскольку f есть инъекция, с учетом замечания 1.5.9 имеем

$$A \setminus Z \sim f[A \setminus Z].$$

Аналогично,

$$B \setminus f[A \setminus Z] \sim g[B \setminus f[A \setminus Z]] = F(Z) = Z.$$

Рассмотрим биекции $h_1\colon Z \to B \setminus f[A \setminus Z]$ и $h_2\colon A \setminus Z \to f[A \setminus Z]$. Определим функцию $h\colon A \to B$ следующим образом:

$$h(a) = \begin{cases} h_1(a), & \text{если } a \in Z; \\ h_2(a), & \text{если } a \in A \setminus Z. \end{cases}$$

Легко видеть, что $A \overset{h}{\sim} B$. □

Пример 1.5.23. Установленная теорема позволяет упростить доказательства равномощности. Довольно часто указать две инъекции проще, чем явно описать требуемую биекцию.

Например, очевидно, что $\mathbb{N} \lesssim \mathbb{Q}$. С другой стороны, $\mathbb{Q} \lesssim \mathbb{N}^3$: каждое положительное рациональное число q однозначно представляется *несократимой* дробью $\frac{m}{n}$, где $m, n \in \mathbb{N}$; отображение $f\colon q \mapsto \mapsto (m, n, 0), 0 \mapsto (0, 1, 0), -q \mapsto (m, n, 1)$ является тогда искомой инъекцией.

Далее, $\mathbb{N}^3 = \mathbb{N}^2 \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$ в силу теоремы 1.5.11 и примера 1.5.10. Отсюда $\mathbb{Q} \lesssim \mathbb{N}$. По теореме 1.5.21, $\mathbb{Q} \sim \mathbb{N}$.

Пример 1.5.24. На плоскости любой квадрат (с внутренностью) равномощен любому кругу. Действительно, с помощью сдвига и гомотетии можно «поместить» круг внутрь квадрата, и наоборот. Сдвиги и гомотетии — биекции плоскости в себя. Поэтому образ круга внутри квадрата равномощен исходному кругу, а значит, этот круг вкладывается в квадрат по лемме 1.5.16. Аналогично, квадрат вкладывается в круг. Следовательно, эти множества равномощны.

Упражнение 1.5.25. Пусть $A = \{0, 1\}$ и $B = \{0, 1, 2\}$. Докажите, что $A^{\mathbb{N}} \sim B^{\mathbb{N}}$.

Обратные функции и аксиома выбора. Пусть $f\colon A \to B$. Функция $g\colon B \to A$ называется *правой обратной* функции f, если $f \circ g = \mathrm{id}_B$. Аналогично, функция $h\colon B \to A$ называется *левой обратной* функции f, если $h \circ f = \mathrm{id}_A$.

Пример 1.5.26. Если $f\colon A \to B$ биекция, то, согласно лемме 1.5.4 и теореме 1.5.6, отношение $f^{-1} \subseteq B \times A$ является функцией, причем как правой, так и левой обратной функции f.

Упражнение 1.5.27. Пусть функция $f\colon A \to B$ имеет как левую обратную h, так и правую обратную g. Докажите, что f — биекция, причем $g = f^{-1} = h$.

Лемма 1.5.28. *Пусть $f\colon A \to B$. Правая обратная $g\colon B \to A$ функции f существует тогда и только тогда, когда f есть сюръекция.*

Доказательство. Пусть правая обратная g существует, т. е. $f \circ g = \mathrm{id}_B$. Для любого $b \in B$ имеем $(b, b) \in f \circ g$, а значит, найдется $a \in A$, для которого $(b, a) \in g$ и $(a, b) \in f$. Последнее означат сюръективность f.

Допустим теперь, что f сюръективна. Ясно, что тогда множества $f^{-1}[\{b\}]$ непусты для всех $b \in B$. Определим функцию $g\colon B \to A$, полагая

$$g(b) = \text{какой-либо элемент множества } f^{-1}[\{b\}]$$

при всех $b \in B$. Поскольку $g(b) \in f^{-1}[\{b\}]$, имеем $f(g(b)) = b$ для всех $b \in B$, т. е. $f \circ g = \mathrm{id}_B$. □

Определяя функцию g в доказательстве леммы 1.5.28, мы не смогли обойтись «основными способами задания множеств», описанными ранее, но были *вынуждены* определять каждое значение g *отдельно*

от других с помощью выражения «какой-либо». В самом деле, попытка написать что-то вроде

$$g = \{(b, a) \in B \times A \mid f(a) = b\}$$

наталкивается на возможность существования *многих* таких a, выделить какой-то один из которых некоторым свойством, в общем случае, не представляется возможным.

Широкое распространение такой ситуации в математической практике и зависимость многих важных (и признаваемых достоверными) теорем от существования множеств, подобных нашей функции g, заставили в начале XX в. выделить особую аксиому, называемую *аксиомой выбора*. Вот ее формулировка:

> Пусть множество A таково, что $\varnothing \notin A$. Тогда существует функция $f\colon A \to \cup A$, т. ч. $f(a) \in a$ для всех $a \in A$.

Вообще, функцию $f\colon A \to \cup A$ со свойством $f(a) \in a$ при всех $a \in A$ называют *функцией выбора* для множества A. В самом деле, эта функция *выбирает* какой-либо элемент $f(a)$ из каждого множества $a \in A$. Если все $a \in A$ непусты, аксиома выбора утверждает существование функции выбора для A.

Упражнение 1.5.29. Пусть множество A состоит из одноэлементных множеств, т. е. $\forall a \in A\, \exists x \in X\ a = \{x\}$. Докажите существование функции выбора $f\colon A \to \cup A$ без использования аксиомы выбора.

Пример 1.5.30. Поясним, как применить аксиому выбора к доказательству леммы 1.5.28. Пусть $\mathcal{P}_*(A) = \mathcal{P}(A) \setminus \{\varnothing\}$ и функция $G\colon B \to \mathcal{P}(A)$ определена равенством $G(b) = f^{-1}[\{b\}]$. В силу сюръективности f, имеем $G(b) \neq \varnothing$ для всех $b \in B$, а значит, $G\colon B \to \mathcal{P}_*(A)$.

Согласно аксиоме выбора, существует функция выбора $\xi\colon \mathcal{P}_*(A) \to \to \cup\mathcal{P}_*(A)$. С другой стороны, для всех $a \in A$ верно $a \in \{a\} \in \mathcal{P}_*(A)$, откуда $\cup\mathcal{P}_*(A) = A$. Итак, $\xi\colon \mathcal{P}_*(A) \to A$.

Остается положить $g = \xi \circ G$. Тогда для всякого $b \in B$ имеем $g(b) = \xi(G(b)) = \xi(f^{-1}[\{b\}]) \in f^{-1}[\{b\}]$, откуда $f(g(b)) = b$. Значит, $f \circ g = \mathrm{id}_B$, как и требовалось.

Упражнение 1.5.31. Пусть $f\colon A \to B$. Докажите, что левая обратная $h\colon B \to A$ функции f существует тогда и только тогда, когда f инъективна, причем $A \neq \varnothing$ или $B = \varnothing$. (Аксиома выбора тут не требуется.)

Упражнение 1.5.32. Допустим, что для любого X у множества $\mathcal{P}_*(X)$ есть функция выбора. Выведите отсюда аксиому выбора.

Попытаемся пояснить философский смысл и нужду в аксиоме выбора парой неформальных аналогий.

Пример 1.5.33. Если есть ($\exists$) ключ, подходящий к каждому ($\forall$) из замков в некоторой совокупности, то для каждого ($\forall$) замка найдется ($\exists$) подходящий ключ. Грубо говоря, логически допустимо преобразование

$$\exists\forall \to \forall\exists.$$

Обратное утверждение, конечно, верно не всегда: ключ от одного замка может не подойти к другому, т. е. преобразование

$$\forall\exists \to \exists\forall,$$

вообще говоря, некорректно. Аксиома выбора в некотором смысле исправляет это обстоятельство: в наших терминах, если для каждого ($\forall$) замка есть ($\exists$) подходящий ключ, аксиома утверждает существование ($\exists$) (помеченной) *связки ключей*, которая для каждого ($\forall$) замка «указывает» подходящий ключ.

«Связка», как будто, более сложный объект, чем «ключ», а потому представляется естественной потребность в «аксиоме» ее существования.

Пример 1.5.34. Представим себе, что имеется некоторая бесконечная совокупность «задач», для каждой ($\forall$) из которых есть ($\exists$) решающая ее компьютерная программа. Следует ли отсюда, что есть ($\exists$) программа, которая может решить каждую ($\forall$) задачу из совокупности, если ее подадут программе на вход?

С одной стороны, иногда такая программа вполне возможна. Действительно, пусть задачи суть вычисления квадратов всевозможных натуральных чисел. Легко представить программу, которая по *любому* входу «возвести n в квадрат», где $n \in \mathbb{N}$, выдает десятичную запись числа n^2.

С другой стороны, задачи могут быть «неоднородными», и единственным способом решить их все разом будет объединить все программы, решающие различные задачи, в одну. Тогда такая «библиотека» подпрограмм для каждой задачи окажется бесконечной, а следовательно, ее не удастся поместить в одну *конечную* программу[17].

Аксиома выбора утверждает, что есть *функция* (но не программа!), каждой задаче ставящая в соответствие некоторое ее решение просто

[17]Как будет видно из последующих частей курса, такая ситуация встречается при разумной формализации понятия программы.

по факту существования такового. В отличие от программы, функция не обязана «действительно решать» задачу, т. е. как-либо *определять* решение по «условию задачи».

Замечание 1.5.35. Почему же проблема выбора не затрудняла нас ранее, когда мы для произвольного непустого A говорили: *возьмем некоторый элемент* $a \in A$? Поясним этот момент немного более общим примером. Именно, пусть $A = \{a_1, a_2\}$ и $a_1 \neq a_2$, причем $\varnothing \notin A$, т. е. A есть *двуэлементное* множество непустых множеств. Покажем, что для A существует функция выбора $f\colon A \to \cup A$, *не используя аксиому выбора.*

Легко проверить следующее утверждение:

$$\forall x_1 \forall x_2 \big((x_1 \in a_1 \text{ и } x_2 \in a_2) \Longrightarrow \\ \Longrightarrow \{(a_1, x_1), (a_2, x_2)\} \text{ есть функция выбора для } A\big).$$

С другой стороны, $\exists x_1 \exists x_2\, (x_1 \in a_1 \text{ и } x_2 \in a_2)$. В силу логики, заключаем:

$$\exists x_1 \exists x_2\ \{(a_1, x_1), (a_2, x_2)\} \text{ есть функция выбора для } A,$$

откуда

$$\exists x_1 \exists x_2 \exists f\ f \text{ есть функция выбора для } A,$$

и, наконец,

$$\exists f\ f \text{ есть функция выбора для } A.$$

Совершенно аналогичные рассуждения проходят для любого конечного множества A: с ростом «числа элементов» последнего они станут, правда, длиннее (эту проблему можно решить при помощи индукции).

Настоящая трудность возникнет, когда A будет бесконечным. Очевидно, она сосредоточена в построении объекта, аналогичного множеству $\{(a_1, x_1), (a_2, x_2)\}$: работа с ним потребует «бесконечных рассуждений», чего мы не желаем допустить, или же — функции выбора!

Без аксиомы выбора бывает легко обойтись, когда элементы множества A являются подмножествами множества, где определена какая-нибудь дополнительная структура (такая как порядок), позволяющая явно описать выбираемые элементы.

Пример 1.5.36. В примере 1.2.14 нам встретилось множество

$$C = \{s \in \mathcal{P}(\mathbb{R}) \mid \exists x \in \mathbb{R}\ \forall y\ (x \leqslant y \leqslant x + 1 \iff y \in s)\}$$

всевозможных отрезков вещественной прямой длины один. Как мы показали, $\cup C = \mathbb{R}$. Убедимся теперь, что для C существует функция выбора $f\colon C \to \mathbb{R}$, не используя аксиому выбора.

Возьмем в качестве $f(s)$ левый конец x отрезка $s \in C$. Формально, положим

$$f = \{(s, x) \in C \times \mathbb{R} \mid \forall y\ (x \leqslant y \leqslant x + 1 \iff y \in s)\}.$$

Тотальность f следует из определения C, а функциональность, т. е. единственность левого конца отрезка, легко проверяется: если $(s, x) \in \in f$ и $(s, x') \in f$, то $x \leqslant y$ и $x' \leqslant y$ для всех $y \in s$, но $x, x' \in s$, откуда $x = x'$. Иначе говоря, в каждом отрезке есть наименьший в смысле естественного порядка вещественных чисел элемент — левый конец, выбор которого можно заложить в определение f.

Упражнение 1.5.37. Пусть $A \subseteq \mathcal{P}_*(\mathbb{Q})$. Не используя аксиому выбора, докажите, что существует функция выбора для множества A.

Упражнение 1.5.38. Предположим, что для любых множеств A и B любая сюръекция $f\colon A \to B$ имеет правую обратную. Выведите отсюда аксиому выбора. (Иначе говоря, лемма 1.5.28 равносильна аксиоме выбора.)

Индексированные семейства. В математической практике часто рассматриваются «семейства» объектов, которым приписаны «номера» из какого-либо множества. Например, *последовательность вещественных чисел* $(a_n)_{n\in\mathbb{N}}$ или *семейство интервалов* $\{(a_i, b_i)\}_{i\in I}$. В этих и подобных им случаях существенно, собственно, семейство объектов, а также то, что имеется некоторое соответствие между множеством номеров и объектами (в частности, объектов «не больше», чем номеров). Напротив, точное определение соответствия $n \mapsto a_n$ несущественно.

Опишем это на языке функций и множеств. Пусть I — некоторое множество *индексов*, а U — еще какое-либо множество. Назовем *индексированным семейством* произвольное отображение $F\colon I \to U$. Говорят, что A *принадлежит* семейству F, если $A \in F[I]$, и что A есть *i-й элемент* семейства F, если $i \in I$ и $A = F(i)$.

Обыкновенно пишут A_i вместо $F(i)$ и $\{A_i\}_{i\in I}$ вместо $F[I]$. Более того, символом $\{A_i\}_{i\in I}$ обозначают все семейство, так что отображение $F\colon i \mapsto A_i$ лишь подразумевается.

Замечание 1.5.39. Каждое множество X (чьи элементы, напомним, сами суть множества) можно представить как индексированное семейство. Действительно, положим $I = U = X$ и $F(A) = A$ для всех $A \in X$. Тогда $X = F[X] = \{A_A\}_{A\in X}$. Обратите внимание, что функция F здесь биекция.

Под *объединением* $\bigcup_{i\in I} A_i$ *индексированного семейства* множеств $\{A_i\}_{i\in I}$ мы понимаем множество $\cup F[I]$, а под *пересечением* $\bigcap_{i\in I} A_i$ соответственно множество $\cap F[I]$. Ожидаемо имеем

$$x \in \bigcup_{i\in I} A_i \iff \exists i \in I\ x \in A_i$$

и, если $I \neq \varnothing$,

$$x \in \bigcap_{i\in I} A_i \iff \forall i \in I\ x \in A_i.$$

Напомним, что в последней эквивалентности, если $I = \varnothing$, правая часть будет выполняться *для любого* x. Очевидно, $\bigcap_{i\in\varnothing} A_i = \cap F[\varnothing] = \cap\varnothing = \varnothing$.

Довольно часто множество индексов I само оказывается декартовым произведением: $I = J \times K$. Тогда обычно пишут $\{A_{jk}\}_{j\in J,k\in K}$ вместо $\{A_{(j,k)}\}_{(j,k)\in J\times K}$.

Пример 1.5.40. Покажем, что $\bigcup_{i\in I}\bigcap_{j\in J} A_{ij} = \bigcap_{f\in J^I}\bigcup_{i\in I} A_{i\,f(i)}$ (это свойство *полной дистрибутивности* обобщает одно из утверждений п. 6 теоремы 1.2.38).

В случае, когда $J = \varnothing$, тривиальная проверка оставляется читателю. Предположим, что $J \neq \varnothing$. Пусть $x \in \bigcup_{i\in I}\bigcap_{j\in J} A_{ij}$. Тогда найдется $i_0 \in I$, т. ч. $\forall j \in J\ x \in A_{i_0 j}$. Рассмотрим произвольную функцию $f\colon I \to J$. Имеем $x \in A_{i_0 f(i_0)}$. Поэтому $\forall f \in J^I\ \exists i \in I\ x \in A_{i\,f(i)}$, т. е. $x \in \bigcap_{f\in J^I}\bigcup_{i\in I} A_{i\,f(i)}$.

Обратно, допустим $\forall f \in J^I\ \exists i \in I\ x \in A_{i\,f(i)}$, но $x \notin \bigcup_{i\in I}\bigcap_{j\in J} A_{ij}$. Тогда для каждого $i \in I$ найдется $j \in J$, т. ч. $x \notin A_{ij}$. Из аксиомы выбора следует существование функции $f_0\colon I \to J$, т. ч. при всех $i \in I$ имеем $f_0(i) = j$, где $x \notin A_{ij}$. В самом деле, *определим* функцию $\varphi\colon I \to \mathcal{P}(J)$, для всех $i \in I$ положив $\varphi(i) = \{j \in J \mid x \notin A_{ij}\}$.

Поскольку $\forall i \in I\ \varphi(i) \neq \varnothing$, существует функция выбора $\xi\colon \varphi[I] \to \cup\varphi[I]$ (очевидно, $\cup\varphi[I] \subseteq J$), т. ч. $\xi(\varphi(i)) \in \varphi(i)$ при всех $i \in I$. Остается положить $f_0 = \xi \circ \varphi$. Итак, $x \notin A_{i\,f_0(i)}$ для всех $i \in I$.

С другой стороны, по исходному предположению для $f_0 \in J^I$ найдется $i_0 \in I$, т. ч. $x \in A_{i_0\,f_0(i_0)}$. Противоречие.

Упражнение 1.5.41. Докажите, что $\bigcap_{i\in I}\bigcup_{j\in J} A_{ij} = \bigcup_{f\in J^I}\bigcap_{i\in I} A_{i\,f(i)}$.

Несколько менее наглядно понятие *декартова произведения* индексированного семейства $\{A_i\}_{i\in I}$. Именно, положим

$$\prod_{i\in I} A_i = \{f \in (\bigcup_{i\in I} A_i)^I \mid \forall i \in I\ f(i) \in A_i\}.$$

Замечание 1.5.42. Элементы $f \in \prod_{i\in I} A_i$ тесно связаны с функциями выбора. Именно, композиции $\xi \circ F$, где ξ суть всевозможные функции выбора для множества $F[I] = \{A_i\}_{i\in I}$, принадлежат множеству $\prod_{i\in I} A_i$. В частности, если $A_i \neq \varnothing$ при всех $i \in I$, из аксиомы выбора следует $\prod_{i\in I} A_i \neq \varnothing$.

Упражнение 1.5.43. Проверьте, что если $I = \varnothing$, то $\prod_{i\in I} A_i = \{\varnothing\}$; если же $\exists i \in I$, т. ч. $A_i = \varnothing$, то $\prod_{i\in I} A_i = \varnothing$.

Пример 1.5.44. Пусть дано индексированное семейство $\{A_i\}_{i\in I}$, причем $A_i = A$ для всех $i \in I$. Покажем, что $A^I = \prod_{i\in I} A_i$.

Легко заметить, что $\bigcup_{i\in I} A_i \subseteq A$. Поэтому, если $f \in \prod_{i\in I} A_i$, то $f \in A^I$. Установим обратное включение. Если $I \neq \varnothing$, то $A \subseteq \bigcup_{i\in I} A_i$. Тогда из допущения $f \in A^I$ следует $f\colon I \to \bigcup_{i\in I} A_i$. С другой стороны, имеем $f(i) \in A = A_i$ для всех $i \in I$. Поэтому $f \in \prod_{i\in I} A_i$.

Пусть теперь $I = \varnothing$ и $f\colon \varnothing \to A$. Из примера 1.4.11 следует, что тогда $f = \varnothing$ и, более того, $f\colon \varnothing \to \bigcup_{i\in I} A_i$. С учетом замечания 1.4.12, $f(i) \in A_i$ для всех $i \in \varnothing$. Вновь $f \in \prod_{i\in I} A_i$.

Упражнение 1.5.45. Предположим, что для всякого индексированного семейства $\{A_i\}_{i\in I}$, т. ч. $A_i \neq \varnothing$ при всех $i \in I$, имеет место $\prod_{i\in I} A_i \neq \varnothing$. Выведите отсюда аксиому выбора.

Вообще, следует иметь в виду, что аксиома выбора очень часто требуется утверждениями о конструкциях, привлекающих бесконечные совокупности множеств произвольной природы (таких, как объединение и произведение).

В доказательстве теоремы 1.5.11 нам уже встречались функции-проекторы, отображающие пару в одну из ее компонент. Для семейства $\{A_i\}_{i\in I}$ определим семейство *проекторов* $\{\pi_i\}_{i\in I}$, т. ч. $\pi_j\colon \prod_{i\in I} A_i \to A_j$ и $\pi_j(f) = f(j)$ для всех $f \in \prod_{i\in I} A_i$ и $j \in I$.

Лемма 1.5.46. *Если $A_i \neq \varnothing$ при всех $i \in I$, то каждый проектор π_j является сюръекцией.*

Доказательство. В самом деле, тогда найдется какая-то $f \in \prod_{i\in I} A_i$, а значит, всякая функция

$$f_a^j(i) \quad = \quad \begin{cases} a, & \text{если } i = j; \\ f(i) & \text{иначе,} \end{cases}$$

где $a \in A_j$, тоже принадлежит $\prod_{i\in I} A_i$. Для каждого $a \in A_j$ имеем $\pi_j(f_a^j) = f_a^j(j) = a$. $\square$

Еще одной полезной конструкцией является *дизъюнктное объединение* (или *сумма*) $\bigsqcup_{i\in I} A_i$ индексированного семейства $\{A_i\}_{i\in I}$. Полагают

$$\bigsqcup_{i\in I} A_i = \bigcup_{i\in I} A_i \times \{i\} = \cup G[I],$$

где $G\colon I \to U \times I$ и $G(i) = F(i) \times \{i\}$ при всех $i \in I$. Смысл дизъюнктного объединения прост: мы помечаем множества A_i элементами i, чтобы получившиеся множества $A_i \times \{i\}$ попарно не пересекались. Это требуется, когда бывает нужно «склеить» несколько множеств.

Замечание 1.5.47. Очевидно, $(A_i \times \{i\}) \cap (A_j \times \{j\}) = \varnothing$, если $i \neq j$. Кроме того, $A_i \times \{i\} \sim A_i$.

Упражнение 1.5.48. Пусть $A_i = A$ при всех $i \in I$. Что есть $\bigsqcup_{i\in I} A_i$?

Для семейства $\{A_i\}_{i\in I}$ определим семейство *канонических*[18] *вложений* $\{\iota_i\}_{i\in I}$, т. ч. $\iota_j\colon A_j \to \bigsqcup_{i\in I} A_i$ и $\iota_j(a) = (a, j)$ для всех $a \in A_j$ и $j \in I$.

Замечание 1.5.49. Очевидно, все ι_j являются инъекциями.

Декартово произведение и дизъюнктное объединение обладают важными свойствами, «обратными» друг другу, являясь, как говорят, «двойственными» конструкциями.

Лемма 1.5.50. *Для любого множества X и любых индексированных семейств $\{A_i\}_{i\in I}$, $\{g_i\}_{i\in I}$, где $g_i\colon X \to A_i$, и $\{h_i\}_{i\in I}$, где $h_i\colon A_i \to X$,*

1) *существует единственная функция $g\colon X \to \prod_{i\in I} A_i$, т. ч. $g_j = \pi_j \circ g$ при всех $j \in I$;*

2) *существует единственная функция $h\colon \bigsqcup_{i\in I} A_i \to X$, т. ч. $h_j = h \circ \iota_j$ при всех $j \in I$.*

Доказательство. Положим $(g(x))(i) = g_i(x) \in A_i$ для всех $x \in X$ и $i \in I$. Очевидно, $g\colon X \to \prod_{i\in I} A_i$ и $\pi_j(g(x)) = (g(x))(j) = g_j(x)$. Если g' другая функция с таким свойством, то при любых $x \in X$ и $j \in I$ имеем $(g(x))(j) = \pi_j(g(x)) = g_j(x) = \pi_j(g'(x)) = (g'(x))(j)$, откуда $g(x) = g'(x)$ и $g = g'$.

[18] Слово «канонический» в математике выделяет самые естественные объекты среди многих возможных.

Также полагаем $h(a,j) = h_j(a) \in X$ при всех $a \in A_j$ и всех $j \in I$. Рассуждаем аналогично. $\square$

Содержательно, функции g и h представляют собой «произведение» $g(x) = (\ldots, g_i(x), \ldots)$ и «сумму» («склейку») $h(a,i) = h_i(a)$ семейств функций $\{g_i\}_{i\in I}$ и $\{h_i\}_{i\in I}$. Тот и другой объект «содержит» соответствующее семейство в том смысле, что из него можно «извлечь» члены семейства с помощью проекторов или вложений.

§ 1.6. Порядки

Помимо функций, важное место в математике занимают особые отношения, называемые *порядками* и *эквивалентностями*. Эти понятия, абстрактные по природе, естественным образом определяются в терминах множеств. Бинарное отношение R называется:

1) *рефлексивным для множества* Z, если $\forall x \in Z\, (x,x) \in R$;

2) *иррефлексивным*, если $\forall x\, (x,x) \notin R$;

3) *симметричным*, если $\forall x \forall y\, (xRy \Longrightarrow yRx)$;

4) *антисимметричным*, если $\forall x \forall y\, \big((xRy \text{ и } yRx) \Longrightarrow x = y\big)$;

5) *транзитивным*, если $\forall x \forall y \forall z\, \big((xRy \text{ и } yRz) \Longrightarrow xRz\big)$.

Как видно, свойство рефлексивности зависит от параметра Z, а прочие присущи самому множеству R. Отношение R на множестве A просто *рефлексивно*, если оно рефлексивно для A.

В терминах «стрелок» рефлексивность означает наличие петли в каждой точке множества A, иррефлексивность — отсутствие петель, симметричность означает наличие у каждой стрелки обратной, антисимметричность — отсутствие обратных стрелок, кроме, быть может, петель, а транзитивность означает, что любой путь из двух последовательных стрелок можно заменить одной стрелкой из его начала в конец.

Пример 1.6.1. Отношение id_A на множестве A рефлексивно, симметрично, антисимметрично и транзитивно. Отношение $\varnothing$ иррефлексивно, симметрично, антисимметрично и транзитивно. Действительно, например, условие $(x,y),(y,z) \in \varnothing$ всегда ложно, а потому влечет все, что угодно, включая $(x,z) \in \varnothing$.

Отношения $<$ и $\leqslant$ на множестве $\mathbb{N}$ транзитивны и антисимметричны (условие $x < y$ и $y < x$ невозможно, а значит, влечет $x = y$), причем $<$ иррефлексивно, а $\leqslant$ рефлексивно.

Отношение $\subseteq$ на множестве $\mathcal{P}(A)$ рефлексивно, транзитивно и антисимметрично. Отношения $\sim$ и $\lesssim$ на множестве $\mathcal{P}(A)$ рефлексивны и транзитивны, причем $\sim$ симметрично (по леммам 1.5.8 и 1.5.16); если в A есть два различных элемента a и b, то $\lesssim$ не симметрично ($\varnothing \lesssim \{a\}$, но $\{a\} \not\lesssim \varnothing$) и не антисимметрично ($\{a\} \lesssim \{b\}$ и $\{b\} \lesssim \{a\}$, но $\{a\} \neq \{b\}$).

Пример 1.6.2. Отношение перпендикулярности на множестве прямых плоскости иррефлексивно, симметрично и не транзитивно (если $a \perp b$ и $b \perp c$, то a и c параллельны или совпадают). Отношение параллельности на том же множестве симметрично и транзитивно. Рефлексивность же, т. е. параллельна ли прямая самой себе, зависит от деталей определения.

Упражнение 1.6.3. Какими из описанных свойств обладает отношение $\{(A, B) \in (\mathcal{P}(U))^2 \mid A \cap B \neq \varnothing\}$?

Практически удобно охарактеризовать наши свойства в терминах операций над множествами и отношениями.

Лемма 1.6.4. *Отношение $R \subseteq A^2$*

1) *рефлексивно* $\iff \mathrm{id}_A \subseteq R$;

2) *иррефлексивно* $\iff \mathrm{id}_A \cap R = \varnothing$;

3) *симметрично* $\iff R \subseteq R^{-1} \iff R = R^{-1} \iff R^{-1} \subseteq R$;

4) *антисимметрично* $\iff R \cap R^{-1} \subseteq \mathrm{id}_A$;

5) *транзитивно* $\iff R \circ R \subseteq R$.

Доказательство. Проверим три последних утверждения. Если R симметрично и $(x, y) \in R$, то, по определению, $(y, x) \in R$, откуда $(x, y) \in$ $\in R^{-1}$. Поэтому $R \subseteq R^{-1}$. Но отсюда имеем $R^{-1} \subseteq (R^{-1})^{-1} = R$, а значит, и $R = R^{-1}$, чего, в свою очередь, достаточно для симметричности.

Условие $R \cap R^{-1} \subseteq \mathrm{id}_A$ означает, что для любых x и y из xRy и $xR^{-1}y$ следует $x \,\mathrm{id}_A\, y$, или, равносильно, из xRy и yRx следует $x = y$. Это условие антисимметричности.

Пусть R транзитивно и $(x, y) \in R \circ R$. Тогда найдется z, т. ч. $(x, z) \in R$ и $(z, y) \in R$. По транзитивности, $(x, y) \in R$. Обратно, пусть

$R \circ R \subseteq R$, xRz и zRy. Но тогда $(x, y) \in R \circ R$ и xRy. Следовательно, R транзитивно. $\square$

Пример 1.6.5. Как устроены отношения $R \subseteq A^2$, симметричные и антисимметричные одновременно? Для каждого такого отношения имеем $R = R \cap R = R \cap R^{-1} \subseteq \mathrm{id}_A$. Значит, R обязательно состоит из пар одинаковых элементов. Обратно, пусть $R \subseteq \mathrm{id}_A$. Тогда $R \cap R^{-1} \subseteq R \subseteq \mathrm{id}_A$, и R антисимметрично. Также, если xRy, то $x = y$, откуда yRx и $xR^{-1}y$. Поэтому R симметрично.

Пример 1.6.6. Если отношения P и Q транзитивны, то таково же $P \cap Q$. В самом деле, согласно упражнению 1.3.17 и примеру 1.3.21,

$$\begin{aligned}(P \cap Q) \circ (P \cap Q) &\subseteq ((P \cap Q) \circ P) \cap ((P \cap Q) \circ Q) \subseteq \\ &\subseteq (P \circ P) \cap (Q \circ P) \cap (P \circ Q) \cap (Q \circ Q) \subseteq \\ &\subseteq (P \circ P) \cap (Q \circ Q) \subseteq P \cap Q.\end{aligned}$$

В последнем переходе использована транзитивность P и Q.

Упражнение 1.6.7. Докажите, что отношение $R \circ R^{-1}$ всегда симметрично.

Упражнение 1.6.8. Пусть отношения P и Q симметричны. Докажите, что отношение $P \circ Q$ симметрично тогда и только тогда, когда $P \circ Q = Q \circ P$.

Отношения порядка. Отношение R на каком-либо множестве называется *строгим частичным порядком* (или просто *строгим порядком*) на этом множестве, если R иррефлексивно и транзитивно.

Пример 1.6.9. На любом множестве A отношение $\varnothing$ есть строгий порядок. Отношения $<$ и $>$ на множестве $\mathbb{N}$ являются строгими частичными порядками, а рефлексивное отношение $\leqslant$ не является. Отношение $\subsetneq$ на множестве $\mathcal{P}(A)$ также строгий порядок.

Пример 1.6.10. Пусть A — некоторое множество, $f\colon A \to \mathbb{N}$ и отношение $R \subseteq A^2$ таково, что $xRy \iff f(x) < f(y)$ для всех $x, y \in A$ (например, $f(x)$ есть цена «товара» $x \in A$). Тогда отношение R является строгим частичным порядком. Очевидно, вместо отношения $<$ на $\mathbb{N}$ можно было бы рассмотреть любой строгий частичный порядок на любом множестве. Таким образом, функция $f\colon A \to B$ «переносит» порядок с B на A (или, как говорят, f *индуцирует* порядок на A).

Замечание 1.6.11. Строгий порядок R всегда антисимметричен. В самом деле, если xRy и yRx, то xRx в силу транзитивности. Иррефлексивность R показывает, что предположение ложно, а значит, влечет $x = y$. Мы получили даже больше: строгий порядок *асимметричен*: если xRy, то yRx неверно.

Отношение R на некотором множестве называется *нестрогим частичным порядком* (или просто *нестрогим порядком*) на этом множестве, если R рефлексивно, транзитивно и антисимметрично.

Пример 1.6.12. На любом множестве A отношение id_A есть нестрогий порядок. Отношения $\leqslant$ и $\geqslant$ на множестве $\mathbb{N}$ являются нестрогими частичными порядками, а иррефлексивное отношение $<$ не является. Отношение $\subseteq$ на множестве $\mathcal{P}(A)$ и отношение делимости $\mid$ на $\mathbb{N}$ также нестрогие порядки. Отношение делимости на $\mathbb{Z}$ порядком не является, поскольку $1 \mid -1$ и $-1 \mid 1$, но $1 \neq -1$.

Упражнение 1.6.13. В примере 1.6.10 положим $xQy \iff f(x) \leqslant f(y)$ для всех $x, y \in A$. Всегда ли Q будет нестрогим частичным порядком на A?

Обратите внимание: для любых элементов $n, m \in \mathbb{N}$ обязательно верно $n \leqslant m$ или $m \leqslant n$, а для порядка $\mid$ такое свойство неверно: $2 \nmid 3$ и $3 \nmid 2$. Говорят тогда, что элементы 2 и 3 в смысле порядка $\mid$ *несравнимы*. Именно эта возможность (не наблюдающаяся в таких знакомых случаях, как порядок $\leqslant$ натуральных чисел) выражена словами «*частичный* порядок».

Упражнение 1.6.14. Докажите, что если P и Q оба суть строгие (или нестрогие) частичные порядки на A, то отношения P^{-1} и $P \cap Q$ таковы же.

Если R есть строгий или нестрогий частичный порядок на множестве A, пара (A, R) называется *частично упорядоченным множеством* (ч. у. м.). Если ясно, какой порядок рассматривается, частично упорядоченным множеством называют и само A.

Связь строгих и нестрогих порядков. Между строгими и нестрогими порядками на заданном множестве A существует тесная взаимосвязь. Именно, у каждого строгого порядка P имеется нестрогий «напарник» $\varphi(P)$, а у нестрогого порядка Q — строгий «напарник» $\psi(Q)$.

Точнее, положим $S(A) = \{R \in \mathcal{P}(A^2) \mid R \text{ строгий порядок}\}$ и аналогично выделим множество $N(A)$ всех нестрогих порядков на A. Рассмотрим функции $\varphi\colon S(A) \to \mathcal{P}(A^2)$ и $\psi\colon N(A) \to \mathcal{P}(A^2)$, т. ч.

$$\varphi(P) = P \cup \mathrm{id}_A \quad \text{и} \quad \psi(Q) = Q \smallsetminus \mathrm{id}_A$$

для любых $P \in S(A)$ и $Q \in N(A)$. Иными словами,

$$(x,y) \in \varphi(P) \iff (xPy \text{ или } x = y) \quad \text{и}$$
$$(x,y) \in \psi(Q) \iff (xQy \text{ и } x \neq y).$$

Теорема 1.6.15. *Для любых $P \in S(A)$ и $Q \in N(A)$ верно:*

1) $\varphi(P) \in N(A)$ *и* $\psi(\varphi(P)) = P$;

2) $\psi(Q) \in S(A)$ *и* $\varphi(\psi(Q)) = Q$.

Доказательство. По определению, $\mathrm{id}_A \subseteq \varphi(P)$. Используя упражнение 1.3.17 и пример 1.3.21, а также транзитивность P, получаем

$$\begin{aligned}\varphi(P) \circ \varphi(P) &= (P \cup \mathrm{id}_A) \circ (P \cup \mathrm{id}_A) = \\ &= (P \circ P) \cup (\mathrm{id}_A \circ P) \cup (P \circ \mathrm{id}_A) \cup (\mathrm{id}_A \circ \mathrm{id}_A) = \\ &= (P \circ P) \cup P \cup \mathrm{id}_A \subseteq P \cup \mathrm{id}_A = \varphi(P).\end{aligned}$$

Остается проверить антисимметричность $\varphi(P)$. Воспользуемся тем, что P, согласно замечанию 1.6.11, антисимметрично:

$$\begin{aligned}\varphi(P) \cap (\varphi(P))^{-1} &= (P \cup \mathrm{id}_A) \cap (P \cup \mathrm{id}_A)^{-1} = \\ &= (P \cup \mathrm{id}_A) \cap (P^{-1} \cup \mathrm{id}_A^{-1}) = (P \cup \mathrm{id}_A) \cap (P^{-1} \cup \mathrm{id}_A) = \\ &= (P \cap P^{-1}) \cup \mathrm{id}_A = \mathrm{id}_A.\end{aligned}$$

Итак, $\varphi(P) \in N(A)$. Далее,

$$\begin{aligned}\psi(\varphi(P)) &= (P \cup \mathrm{id}_A) \cap \overline{\mathrm{id}}_A = (P \cap \overline{\mathrm{id}}_A) \cup (\mathrm{id}_A \cap \overline{\mathrm{id}}_A) = \\ &= (P \cap \overline{\mathrm{id}}_A) \cup \varnothing = (P \cap \overline{\mathrm{id}}_A) \cup (P \cap \mathrm{id}_A) = \\ &= P \cap (\overline{\mathrm{id}}_A \cup \mathrm{id}_A) = P \cap A^2 = P.\end{aligned}$$

Докажем второе утверждение. По определению, $\psi(Q) \cap \mathrm{id}_A = \varnothing$, т. е. $\psi(Q)$ иррефлексивно. Пусть $(x,y) \in \psi(Q)$ и $(y,z) \in \psi(Q)$. Тогда xQy и yQz, откуда xQz, но также $x \neq y$ и $y \neq z$. Предположим, что $x = z$. Имеем yQx, т. е. $xQ^{-1}y$. Но Q антисимметрично, а значит, $x = y$, что не

так. Следовательно, $x \neq z$ и $(x, z) \in Q \setminus \mathrm{id}_A = \psi(Q)$. Итак, отношение $\psi(Q)$ транзитивно и $\psi(Q) \in S(A)$. Наконец,

$$\varphi(\psi(Q)) = (Q \cap \overline{\mathrm{id}}_A) \cup \mathrm{id}_A = (Q \cup \mathrm{id}_A) \cap (\overline{\mathrm{id}}_A \cup \mathrm{id}_A) = \\ = (Q \cup \mathrm{id}_A) \cap A^2 = Q \cup \mathrm{id}_A = Q,$$

поскольку $\mathrm{id}_A \subseteq Q$. □

Как видим, функция $\psi\colon N(A) \to S(A)$ является левой и правой обратной функции $\varphi\colon S(A) \to N(A)$. Согласно упражнению 1.5.27, получаем

Следствие 1.6.16. *Функция $\varphi\colon S(A) \to N(A)$ является биекцией, причем $\psi = \varphi^{-1}$.*

Упражнение 1.6.17. Докажите, что $\varphi(P^{-1}) = (\varphi(P))^{-1}$ для всех $P \in S(A)$.

Таким образом, хотя строгие и нестрогие частичные порядки — это разные объекты, между ними всегда имеется естественное биективное соответствие (в частности, на любом множестве A тех и других «поровну»). Например, нам хорошо знакома пара соответствующих порядков $(<, \leqslant)$ на $\mathbb{N}$ или $(\subsetneq, \subseteq)$ на любом $\mathcal{P}(A)$.

Это позволяет, говоря о строгом порядке, всегда иметь к услугам соответствующий нестрогий, и наоборот. В частности, упоминая *частичный порядок*, можно вообще не уточнять без нужды, строгий или нестрогий его вариант имеется в виду. В нашем курсе, без уточнения, порядки будут считаться строгими.

При обозначении частичных порядков на различных множествах часто употребляют символ $<$ и ему подобные. Мы будем считать, что в парах $(<, \leqslant)$, $(\prec, \preceq)$ и т. п. первый символ обозначает строгий вариант порядка, а второй — нестрогий, т. е. $\leqslant = \varphi(<)$ и $< = \psi(\leqslant)$. Иногда, для большей ясности, для строгих вариантов применяют символы вроде $\subsetneq$ или $\lneq$.

Максимумы и минимумы. Если на множестве A задан строгий частичный порядок P, элемент $x \in A$ называется (P-)*максимальным*, если

$$\forall y \in A \text{ неверно } xPy.$$

В терминах «стрелок» максимальный элемент есть такой, *из которого* не выходит ни одной стрелки, «тупиковый». (Разумеется, это понятие

имеет смысл для любого иррефлексивного отношения P, а не только частичного порядка.) Аналогично определяется (P)-*минимальный* элемент x, т. ч.

$$\forall y \in A \text{ неверно } yPx,$$

или, иначе говоря, *в который* не ведет ни одна стрелка.

Если механически перенести это определение на *нестрогий* порядок $Q = \varphi(P)$, минимальных и максимальных элементов в нем не окажется вследствие рефлексивности. Но это не то, что имеется в виду! Мы желаем, чтобы «максимальными» для порядка Q оказались в точности максимальные элементы его строгого варианта P, для чего достаточно объявить элемент $x \in A$ Q-*максимальным*, если

$$\forall y \in A \; (xQy \Longrightarrow y = x)$$

(т.е. мы запрещаем выходить из x любым стрелкам, кроме петель). Аналогично изменится и понятие минимального элемента.

По существу, связанные с порядками понятия всегда определяются для пары $(P, \varphi(P))$ (она же $(\psi(Q), Q)$). Впредь мы не станем на этом останавливаться. Множество P-максимальных (они же Q-максимальные) элементов множества A мы обозначим $\max_P A$, или, если порядок P ясен, просто $\max A$.

Пример 1.6.18. Ожидаемо имеем $\min_< \mathbb{N} = \{0\}$ и $\max_< \mathbb{N} = \varnothing$, но также $\max_> \mathbb{N} = \{0\}$ и $\min_> \mathbb{N} = \varnothing$. Именно так: нет ни одного $y \in \mathbb{N}$, т. ч. $0 > y$. Из элемента 0 не выходит ни одной $>$-стрелки: он «тупиковый», максимальный в смысле понятия «больше», поскольку 0 не больше ни какого другого элемента!

Упражнение 1.6.19. Пусть R — частичный порядок на A. Докажите, что $\min_R A = \max_{R^{-1}} A$ и $\max_R A = \min_{R^{-1}} A$.

Пример 1.6.20. Пусть на множестве A задан строгий порядок $\varnothing$. Тогда $\min_\varnothing A = A = \max_\varnothing A$. В самом деле, ни в один элемент $x \in A$ не входит никакая стрелка, и никакая стрелка не выходит из него. Как видим, минимальных и максимальных элементов может быть много.

Пример 1.6.21. Пусть на множестве $A = \mathcal{P}(\mathbb{N}) \setminus \{\varnothing, \mathbb{N}\}$ задан порядок $\subseteq$. Найдем множества $\min A$ и $\max A$.

Легко видеть, что $x \subsetneq \{n\}$ невозможно ни для каких $x \in A$ и $n \in \mathbb{N}$. Поэтому все множества $\{n\}$ суть минимальные элементы A. Напротив, если во множестве $y \in A$ есть два различных элемента n и m, то $\{m\} \subsetneq y$, и такой y не минимальный. Итак, $\min A = \{\{n\} \mid n \in \mathbb{N}\}$. Аналогично, легко проверить, что $\max A = \{\mathbb{N} \setminus \{n\} \mid n \in \mathbb{N}\}$.

Упражнение 1.6.22. Найдите $\min_{|} \mathbb{N}$ и $\max_{|} \mathbb{N}$. Проделайте то же для $\mathbb{N} \setminus \{0, 1\}$.

Пусть дано ч. у. м. $(A, <)$. Понятие максимального и минимального элемента естественно распространить на любое подмножество $B \subseteq A$, положив $\max_< B = \{x \in B \mid \forall y \in B\, x \not< y\}$, и аналогично определяя $\min_< B$.

Замечание 1.6.23. С формальной точки зрения, можно также считать, что отображение $\mathrm{id}_B \colon B \to A$ индуцирует порядок $<_B$ на множестве B (при этом $<_B$ есть ограничение $<$ на B), а затем рассмотреть максимальные элементы ч. у. м. $(B, <_B)$.

Элемент $x \in B$ называется *наибольшим* в подмножестве B ч. у. м. $(A, <)$, если $\forall y \in B\ y \leqslant x$, и *наименьшим*, если $\forall y \in B\ x \leqslant y$.

Лемма 1.6.24. *Пусть $(A, <)$ ч. у. м. Если элемент x наибольший в $B \subseteq A$, то $\max_< B = \{x\}$. В частности, наибольший элемент B единствен.*

Доказательство. Допустим, $x \notin \max B$, т. е. $x < y$ для некоторого $y \in B$. Но также $y \leqslant x$, что означает $y = x$ или $y < x$ (поскольку $\leqslant = \varphi(<)$). В первом случае сразу имеем $y < y$, а во втором получаем это же по транзитивности $<$. Противоречие с иррефлексивностью $<$. Итак, $x \in \max B$.

Допустим, $x' \in \max B$. Тогда $x' \not< x$, но, с другой стороны, $x' \leqslant x$. Следовательно, $x' = x$. □

Упражнение 1.6.25. Сформулируйте и докажите аналогичное утверждение для наименьших элементов.

Упражнение 1.6.26. Допустим $\max_< A = \{x\}$. Всегда ли x есть наибольший элемент ч. у. м. $(A, <)$?

Пример 1.6.27. Рассмотрим множество $A = \mathcal{P}(\mathbb{N}) \setminus \{\varnothing, \mathbb{N}\}$ с порядком $\subseteq$. В A, как мы показали, более одного минимума и максимума, а значит, нет ни наименьшего, ни наибольшего элемента. Рассмотрим $B = \{X \in A \mid \{1, 2, 3\} \subseteq X\}$. Очевидно, элемент $\{1, 2, 3\}$ является наименьшим в B. С другой стороны, легко проверить, что

$$\max B = B \cap \max A = \{\mathbb{N} \setminus \{n\} \mid n \in \mathbb{N} \setminus \{1, 2, 3\}\}.$$

В частности, в B нет наибольшего элемента.

Пусть $(A, <)$ ч. у. м. и $B \subseteq A$. Элемент $x \in A$ назовем *верхней гранью* множества B, если $y \leqslant x$ для всех $y \in B$. Аналогично определяются *нижние грани*.

Пример 1.6.28. Верхними гранями множества $\{2, 3, 7\}$ в ч. у. м. $(\mathbb{N}, |)$ являются в точности натуральные числа, кратные 42. Единственной нижней гранью этого множества будет 1.

Упражнение 1.6.29. Пусть $(A, <)$ ч. у. м. и $B, C \subseteq A$. Обозначим $B^\triangle$ множество верхних и $B^\triangledown$ множество нижних граней множества B. Докажите, что

1) $(B \cup C)^\triangle = B^\triangle \cap C^\triangle$; $(B \cup C)^\triangledown = B^\triangledown \cap C^\triangledown$;

2) $B \subseteq C \Longrightarrow C^\triangle \subseteq B^\triangle$ и $C^\triangledown \subseteq B^\triangledown$;

3) $B \subseteq B^{\triangle\triangledown} \cap B^{\triangledown\triangle}$;

4) $B^\triangle = B^{\triangle\triangledown\triangle}$; $B^\triangledown = B^{\triangledown\triangle\triangledown}$.

Мы говорим, что $x \in A$ есть *точная верхняя грань* (или *супремум*) множества B, если x есть наименьшая верхняя грань множества B (т. е. наименьший элемент множества $B^\triangle$). Аналогично определяется *точная нижняя грань* (или *инфимум*) множества B — его наибольшая нижняя грань. Поскольку наибольший (наименьший) элемент единствен, осмысленно обозначение $x = \sup B$ для супремума и $x = \inf B$ для инфимума.

Замечание 1.6.30. Множество B имеет наибольший элемент тогда и только тогда, когда $\sup B \in B$, причем $\sup B$ является тем самым наибольшим элементом. Аналогично связаны инфимум и наименьший элемент.

Упражнение 1.6.31. Как соотносятся элементы $\sup B$ и $\inf B^\triangle$ (если они существуют)?

Пример 1.6.32. В естественном упорядочении вещественных чисел для множества $B = \{\frac{1}{n} \mid n \in \mathbb{N}_+\}$ имеем $\sup B = 1 \in B$ и $\inf B = 0 \notin B$.

Пример 1.6.33. Рассмотрим порядок $P = \{(0, 2), (0, 3), (1, 2), (1, 3)\}$ на множестве $A = \{0, 1, 2, 3\}$. Подмножество $B = \{2, 3\}$ имеет нижние грани 0 и 1, но эти грани несравнимы, а значит, *наибольшей* нижней грани у B нет, хотя каждая нижняя грань максимальная.

Пример 1.6.34. Рассмотрим ч. у. м. $(\mathcal{P}(A), \subseteq)$ и для произвольного семейства подмножеств $X \subseteq \mathcal{P}(A)$ найдем $\sup X$ и $\inf X$.

Если $B \in X$, то $B \subseteq \cup X \in \mathcal{P}(A)$, поэтому $\cup X$ есть верхняя грань множества X. Пусть $C \in \mathcal{P}(A)$ — какая-нибудь верхняя грань множества X. По определению, тогда $B \subseteq C$ для всех $B \in X$. Ясно, что в этом случае $\cup X \subseteq C$, а значит, верхняя грань $\cup X$ наименьшая. Итак, $\sup X = \cup X$.

Если $B \in X$, то $\cap X \subseteq B$ (напомним, по нашим определениям $\cap \varnothing = \varnothing$); следовательно, $\cap X$ есть нижняя грань X. Пусть $D \in \mathcal{P}(A)$ есть некоторая нижняя грань X, т. е. $D \subseteq B$ для всех $B \in X$. Если $X \neq \varnothing$, то найдется $B_0 \in X$, для которого $D \subseteq B_0$, а значит, $D \subseteq \cup X$. Тогда, по определению пересечения, $D \subseteq \cap X$ и, окончательно, $\inf X = \cap X$. Если же $X = \varnothing$, любое $D \in \mathcal{P}(A)$ является нижней гранью X. Наибольшим элементом $\mathcal{P}(A)$ является A, а значит, $\inf \varnothing = A$.

В простом случае, когда $X = \{B_1, B_2\}$, имеем $\sup X = B_1 \cup B_2$ и $\inf X = B_1 \cap B_2$. Таким образом, объединение двух множеств B_1 и B_2 является их *наименьшим* общим *над*множеством ($\subseteq$-верхней гранью), а пересечение — *наибольшим* общим *под*множеством ($\subseteq$-нижней гранью).

Важным классом упорядоченных множеств являются *решетки*, т. е. такие ч. у. м. $(A, <)$, где для любых $x, y \in A$ существуют $\sup\{x, y\}$ и $\inf\{x, y\}$. Ч. у. м. $(A, <)$ называется *полной решеткой*, если для всех $X \subseteq A$ существуют $\sup X$ и $\inf X$. Мы видели, что ч. у. м. $(\mathcal{P}(A), \subseteq)$ есть полная решетка.

Упражнение 1.6.35. Докажите, что ч. у. м. $(\mathbb{N} \setminus \{0\}, |)$ является решеткой, но не полной решеткой.

Упражнение 1.6.36. Докажите, что если в ч. у. м. $(A, <)$ для каждого $X \subseteq A$ существует $\sup X$, то для каждого $X \subseteq A$ существует $\inf X$, и наоборот.

Линейные порядки. Порядок $<$ на множестве A называется *линейным*, если любые два элемента A сравнимы, т. е.

$$\forall x, y \in A \quad x \leqslant y \text{ или } y \leqslant x.$$

Мы говорим, что ч. у. м. $(A, <)$ есть *линейно упорядоченное множество* (л. у. м.), если порядок $<$ линейный.

Пример 1.6.37. Естественные порядки на множествах $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ являются линейными, а порядки $\subseteq$ на $\mathcal{P}(A)$ (если в A есть хотя бы два различных элемента) и $|$ на $\mathbb{N}$ не являются.

Упражнение 1.6.38. Проверьте, что всякий линейный порядок есть решетка, но не всякий — полная решетка.

Замечание 1.6.39. Если порядок $<$ на A линейный, то

$$x \not< y \iff y \leqslant x$$

для всех $x, y \in A$. Отсюда следует, что относительно линейного порядка элемент x является наибольшим (наименьшим) во множестве $B \subseteq A$ тогда и только тогда, когда x максимальный (минимальный) в B. В частности, в линейном порядке множество может иметь не более одного максимального (минимального) элемента. Поэтому для л. у. м. можно писать $x = \max B$, если элемент x максимальный (т. е. и наибольший) во множестве B.

Поскольку наименьшая верхняя грань в случае линейного порядка есть то же, что минимальная, определение супремума (и инфимума) принимает особенно простой вид:

$$x = \sup B \iff (\forall y \in B\ y \leqslant x \quad \text{и} \quad \forall z < x\, \exists y \in B\ z < y).$$

(Ограниченный квантор $\forall z < x\, \varphi$ надо понимать как $\forall z\, (z < x \implies \varphi)$.)

Упражнение 1.6.40. Пусть $(B, <)$ л. у. м. и функция $f\colon A \to B$ индуцирует частичный порядок P на A. Докажите, что отношение $\bar{P}$ транзитивно.

Пусть $(A, <)$ ч. у. м. Множество $C \subseteq A$ называется *цепью* в A, если

$$\forall x, y \in C \ \ x \leqslant y \text{ или } y \leqslant x.$$

Иначе говоря, цепь — это подмножество, любые два элемента которого сравнимы, а порядок, при ограничении на него, становится линейным. Напротив, множество $D \subseteq A$ называется *антицепью*, если никакие два его (различных) элемента несравнимы, т. е.

$$\forall x, y \in D \ \ x \not< y \text{ и } y \not< x.$$

Пример 1.6.41. В ч. у. м. $(\mathbb{N}, |)$ множество $\{2^n \mid n \in \mathbb{N}\}$ образует цепь, а множество простых чисел — антицепь. Множество $\{\mathbb{N}_{\geqslant k} \mid k \in \mathbb{N}\}$, где $\mathbb{N}_{\geqslant k} = \{n \in \mathbb{N} \mid n \geqslant k\}$, есть цепь в $(\mathcal{P}(\mathbb{N}), \subseteq)$.

Упражнение 1.6.42. При каких условиях подмножество является цепью и антицепью одновременно? Найдите все цепи и все антицепи линейно упорядоченного множества.

Упражнение 1.6.43. Постройте в ч. у. м. $(\mathcal{P}(\mathbb{N}), \subseteq)$ непустую цепь, не имеющую ни наибольшего, ни наименьшего элемента.

Структуры и изоморфизм. Мы назвали пару (A, R) частично упорядоченным множеством, если R есть отношение частичного порядка на A. Вообще, подобные объекты, называемые *структурами*, — множества вместе с некоторой совокупностью отношений на них (необязательно бинарных) — иногда рассматривают как основной «предмет» математики. Например, арифметика изучает множество натуральных чисел вместе с функциям сложения и умножения (т. е. отношениями между $\mathbb{N}^2$ и $\mathbb{N}$), а также отношением «равно» (т. е. $\mathrm{id}_{\mathbb{N}}$).

Математика стремится выделить свойства структуры, заключающиеся во «взаимном расположении» элементов множества A в смысле имеющихся отношений, независимо от точной природы этих элементов. Например, умея «складывать яблоки», мы равно умеем складывать и груши[19]. Одинаково устроенные структуры называются *изоморфными* и зачастую не различаются.

В свое время мы дадим точное определение структуры и изоморфизма структур. Пока же ограничимся одним частным случаем. Именно, рассмотрим структуры вида $\mathcal{A} = (A, R)$, где есть только одно отношение $R \subseteq A^2$. При этом множество $A = |\mathcal{A}|$ называется *носителем* структуры $\mathcal{A}$. Структуры $\mathcal{A} = (A, R)$ и $\mathcal{B} = (B, Q)$ *изоморфны*, если существует функция $\alpha\colon A \to B$, т. ч. $A \overset{\alpha}{\sim} B$ и

$$xRy \iff \alpha(x)Q\alpha(y)$$

для всех $x, y \in A$. Сама функция α называется *изоморфизмом* структур $\mathcal{A}$ и $\mathcal{B}$. Соответственно мы пишем $\mathcal{A} \overset{\alpha}{\cong} \mathcal{B}$ и $\mathcal{A} \cong \mathcal{B}$.

Лемма 1.6.44. *Для любых структур $\mathcal{A}, \mathcal{B}, \mathcal{C}$ имеет место:*

1) $\mathcal{A} \overset{\mathrm{id}_A}{\cong} \mathcal{A}$;

2) *если* $\mathcal{A} \overset{\alpha}{\cong} \mathcal{B}$, *то* $\mathcal{B} \overset{\alpha^{-1}}{\cong} \mathcal{A}$;

3) *если* $\mathcal{A} \overset{\alpha}{\cong} \mathcal{B}$ *и* $\mathcal{B} \overset{\beta}{\cong} \mathcal{C}$, *то* $\mathcal{A} \overset{\beta\circ\alpha}{\cong} \mathcal{C}$.

Изоморфные структуры обладают одними и теми же свойствами, выразимыми в терминах имеющихся отношений. Впоследствии мы уточним и докажем это утверждение.

[19] «Человек, впервые формулировавший, что «два и два четыре», — великий математик, если даже он получил эту истину из складывания двух окурков с двумя окурками. Все дальнейшие люди, хотя бы они складывали неизмеримо большие вещи, например, паровоз с паровозом, — все эти люди — не математики». (*В. Маяковский.* Как делать стихи?)

Пример 1.6.45. Пусть (A, R) есть ч. у. м. и $(A, R) \cong (B, Q)$. Тогда структура (B, Q) также есть ч. у. м.

Действительно, если $\alpha\colon A \to B$ есть изоморфизм, то для всяких $u, v, w \in B$ найдутся $x, y, z \in A$, т. ч. $u = \alpha(x)$, $v = \alpha(y)$ и $w = \alpha(z)$. Поскольку $(x, x) \notin R$, имеем $(u, u) = (\alpha(x), \alpha(x)) \notin Q$. Итак, Q иррефлексивно. Если uQv и vQw, то xRy и yRz, откуда xRz, а значит, и uQw. Следовательно, Q транзитивно.

Ограничимся теперь лишь изоморфизмами частично упорядоченных множеств. Изоморфные ч. у. м. представляют, по существу дела, один и тот же порядок, а неизоморфные — существенно различные.

Пример 1.6.46. Имеем $(\mathbb{Z}, <) \cong (\mathbb{Z}, >)$. В самом деле, $x < y$ равносильно $-x > -y$, причем отображение $x \mapsto -x$ есть биекция $\mathbb{Z} \to \mathbb{Z}$. Значит, это искомый изоморфизм. С другой стороны, $(\mathbb{N}, <) \ncong (\mathbb{Z}, <)$ [20]. Иначе есть изоморфизм $\alpha\colon \mathbb{N} \to \mathbb{Z}$. Рассмотрим элемент $\alpha(0) \in \mathbb{Z}$. Найдется $u \in \mathbb{Z}$, т. ч. $u < \alpha(0)$, и $x \in \mathbb{N}$, т. ч. $\alpha(x) = u$. Имеем $\alpha(x) < \alpha(0)$, что дает $x < 0$, но в $\mathbb{N}$ таких x нет. Противоречие.

Упражнение 1.6.47. Докажите, что $(\mathbb{Q}, <) \ncong (\mathbb{Z}, <)$ и $(\mathbb{Q}, <) \ncong (\mathbb{R}, <)$, а также, что $(\mathbb{N}, |) \ncong (\mathcal{P}(U), \subseteq)$ для любого множества U [21].

Замечание 1.6.48. Легко проверить, что

$$(A, <_A) \overset{\alpha}{\cong} (B, <_B) \iff (A, \leqslant_A) \overset{\alpha}{\cong} (B, \leqslant_B).$$

Таким образом, любой изоморфизм ч. у. м. «уважает» связь между строгим и нестрогим вариантами порядка.

Мы уже видели, что изоморфные ч. у. м. обязаны одновременно иметь или не иметь наименьший элемент, причем изоморфизм переводит один в другой. То же относится и к другим понятиям, определяемым в терминах порядка.

Лемма 1.6.49. *Пусть* $(A, <_A) \overset{\alpha}{\cong} (B, <_B)$. *Тогда если* $(A, <_A)$ *л. у. м.* (*решетка*), *то и* $(B, <_B)$ *л. у. м.* (*решетка*). *Для всякого* $X \subseteq A$ *верно* $\max_{<_B} \alpha[X] = \alpha[\max_{<_A} X]$ *и, если существует* $\sup_{<_A} X$, *верно* $\sup_{<_B} \alpha[X] = \alpha(\sup_{<_A} X)$ (*аналогично для минимумов и инфимумов*).

[20] Мы злоупотребляем обозначениями: символ $<$ слева обозначает не то же отношение, что справа (а его собственное подмножество). Придирчивый читатель желал бы видеть тут, например, символы $<_{\mathbb{N}}$ и $<_{\mathbb{Z}}$. Мы будем допускать подобные вольности и впредь.

[21] Если эрудированного читателя искушает тот факт, что $\mathbb{N} \sim \mathcal{P}(U)$, предлагаем такой вариант задачи: пусть семейство $S \subseteq \mathcal{P}(U)$ таково, что $B \subseteq A \in S$ влечет $B \in S$; тогда $(\mathbb{N}_+, |) \ncong (S, \subseteq)$. В качестве такого S могут выступать, например, все конечные подмножества U.

Доказательство. Проверим лишь утверждение о супремуме. Пусть существует $\sup_{<_A} X$. Если $u \in \alpha[X]$, то $u = \alpha(x)$ для некоторого $x \in X$. Поскольку $x \leqslant_A \sup_{<_A} X$, имеем $u \leqslant_B \alpha(\sup_{<_A} X)$. С другой стороны, пусть $v = \alpha(y)$ есть произвольная верхняя грань множества $\alpha[X]$. Тогда для всех $x \in X$ верно $\alpha(x) \leqslant_B \alpha(y)$, откуда $x \leqslant_A y$. Значит, $\sup_{<_A} X \leqslant_A y$, и $\alpha(\sup_{<_A} X) \leqslant_B v$. □

Упражнение 1.6.50. Докажите, что для любого ч. у. м. $\mathcal{A} = (A, \leqslant)$ найдется $S \subseteq \mathcal{P}(A)$, т. ч. $\mathcal{A} \cong (S, \subseteq)$. Иначе говоря, любой порядок устроен так же, как включение на подходящем семействе подмножеств.

Соответствия Галуа. Помимо изоморфизма, в математической практике часто встречаются некоторые более слабые отношения между частично упорядоченными множествами.

Пусть $\mathcal{A} = (A, \leqslant_A)$ и $\mathcal{B} = (B, \leqslant_B)$ ч. у. м. Если для всех $x, y \in A$ из $x \leqslant_A y$ следует $\alpha(x) \leqslant_B \alpha(y)$, то отображение $\alpha\colon A \to B$ мы назовем *монотонным* (относительно данных порядков) или *гомоморфизмом* из $\mathcal{A}$ в $\mathcal{B}$. Если же $x \leqslant_A y$ равносильно $\alpha(x) \leqslant_B \alpha(y)$, то назовем α *изоморфным вложением* $\mathcal{A}$ в $\mathcal{B}$. Легко проверить, что изоморфное вложение является инъекцией, а значит, изоморфизмом ч. у. м. $\mathcal{A}$ и $\alpha[\mathcal{A}] = (\alpha[A], \leqslant_B)$.

Пример 1.6.51. Если порядок $<_A$ на множестве A индуцирован отображением $f\colon A \to B$ в ч. у. м. $(B, <_B)$, то f есть гомоморфизм из $(A, <_A)$ в $(B, <_B)$.

Пусть $A = \mathcal{P}(\{0, \ldots, N\})$ и $B = \{0, \ldots, N!\}$, где $N \in \mathbb{N}$. Отображение $\alpha\colon A \to B$, т. ч. $\alpha(\varnothing) = 1$ и $\alpha(\{k_1, k_2, \ldots, k_n\}) = k_1 k_2 \ldots k_n$ является гомоморфизмом ч. у. м $(A, \subseteq)$ и $(B, |)$, но не инъективно и не сюръективно при $N \geqslant 3$.

Если $\alpha(x) = \lfloor x \rfloor \in \mathbb{N}$ — целая часть числа $x \in \mathbb{R}_{\geqslant 0}$, то α есть гомоморфизм порядков $(\mathbb{R}_{\geqslant 0}, \leqslant)$ и $(\mathbb{N}, \leqslant)$.

Назовем пару (f_*, f^*) *соответствием Галуа* между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$, если $f_*\colon A \to B$ и $f^*\colon B \to A$, причем

$$f_*(x) \leqslant_B y \iff x \leqslant_A f^*(y)$$

при всех $x \in A$ и $y \in B$. Функции f_* и f^* называются *сопряженными*, причем f_* называется *левой* сопряженной ($к$ f^*), а f^* — *правой*.

Пример 1.6.52. Если $\mathcal{A} \overset{\alpha}{\cong} \mathcal{B}$, то (α, α^{-1}) есть соответствие Галуа между $\mathcal{A}$ и $\mathcal{B}$.

Зафиксируем $S \subseteq U$. Тогда функции f_* и f^*, т. ч. $f_*(X) = X \cap \cap S$ и $f^*(X) = X \cup \bar{S}$, образуют соответствие Галуа ч. у. м. $(\mathcal{P}(U), \subseteq)$ самого с собой. Как видим, соответствие Галуа может отличаться от изоморфизма даже при $\mathcal{A} = \mathcal{B}$.

Пусть $g\colon A \to B$. Функции $f_*\colon \mathcal{P}(A) \to \mathcal{P}(B)$ и $f^*\colon \mathcal{P}(B) \to \mathcal{P}(A)$ определим, полагая $f_*(X) = g[X]$ и $f^*(Y) = g^{-1}[Y]$. Тогда, согласно упражнению 1.4.22, $g[X] \subseteq Y \iff X \subseteq g^{-1}[Y]$, а значит, (f_*, f^*) будет соответствием Галуа между $(\mathcal{P}(A), \subseteq)$ и $(\mathcal{P}(B), \subseteq)$.

В упражнении 1.2.28 мы видели, что $\cup X \subseteq Y \iff X \subseteq \mathcal{P}(Y)$ для любых множеств X и Y. Если множеству U для каждого $X \in U$ также принадлежат $f_*(X) = \cup X$ и $f^*(X) = \mathcal{P}(X)$ [22], то (f_*, f^*) есть соответствие Галуа ч. у. м. $(U, \subseteq)$ самого с собой.

Пусть $\mathcal{A} = (A, \leqslant)$ решетка. Обозначим $\mathcal{A}' = (A^2, \leqslant')$, где $(x, z) \leqslant' (x', z') \iff x \leqslant_A x'$ и $z \leqslant_A z'$. Легко проверить, что $\mathcal{A}'$ есть ч. у. м. Имеем $\sup(x, z) \leqslant y \iff (x, z) \leqslant' (y, y)$ и $(y, y) \leqslant' (x, z) \iff y \leqslant \leqslant \inf(x, z)$. Поэтому $(\sup, \delta)$ есть соответствие Галуа между $\mathcal{A}'$ и $\mathcal{A}$, а $(\delta, \inf)$ — между $\mathcal{A}$ и $\mathcal{A}'$, где $\delta(y) = (y, y)$.

Пусть функции $\alpha, \beta\colon \mathbb{R}_{\geqslant 0} \to \mathbb{N}$ таковы, что $\alpha(x) = \lfloor x \rfloor$ и $\beta(x) = \lceil x \rceil$ (наименьшее натуральное не меньше x). Тогда $n \leqslant x \iff n \leqslant \lfloor x \rfloor$ и $\lceil x \rceil \leqslant n \iff x \leqslant n$; значит, пара $(\mathrm{id}_{\mathbb{N}}, \alpha)$ есть соответствие Галуа между $(\mathbb{N}, \leqslant)$ и $(\mathbb{R}_{\geqslant 0}, \leqslant)$, а пара $(\beta, \mathrm{id}_{\mathbb{N}})$ — между $(\mathbb{R}_{\geqslant 0}, \leqslant)$ и $(\mathbb{N}, \leqslant)$.

Лемма 1.6.53. *Пусть (f_*, f^*) — соответствие Галуа между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$. Тогда:*

1) $x \leqslant_A f^*(f_*(x))$ *и* $f_*(f^*(y)) \leqslant_B y$ *для всех* $x \in A$ *и* $y \in B$;

2) *функции f_* и f^* являются гомоморфизмами соответствующих ч. у. м.;*

3) $f_* = f_* \circ f^* \circ f_*$ *и* $f^* = f^* \circ f_* \circ f^*$.

Доказательство. Проверим лишь первую половину каждого утверждения, так как вторая устанавливается аналогично. Имеем $f_*(x) \leqslant_B \leqslant_B f_*(x)$, откуда $x \leqslant_A f^*(f_*(x))$. Далее, пусть $x \leqslant_A z$. Тогда $x \leqslant_A z \leqslant_A \leqslant_A f^*(f_*(z))$. Значит, $f_*(x) \leqslant_B f_*(z)$.

Поскольку $f_*(x) \in B$, в силу п. 1 имеем $f_*(f^*(f_*(x))) \leqslant_B f_*(x)$ при всех $x \in A$. С другой стороны, из $x \leqslant_A f^*(f_*(x))$ следует $f_*(x) \leqslant_B \leqslant_B f_*(f^*(f_*(x)))$ по монотонности f_*. □

[22] Такое непустое множество U можно определить с помощью *аксиом подстановки*, о которых речь впереди.

Упражнение 1.6.54. Пусть (f_*, f^*) — соответствие Галуа между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$. Докажите, что $f^* = f_*^{-1}$ тогда и только тогда, когда f_* есть изоморфизм $\mathcal{A} \to \mathcal{B}$.

Упражнение 1.6.55. Пусть (f_*, f^*) — соответствие Галуа между непустыми ч. у. м. $\mathcal{A}$ и $\mathcal{B}$. Докажите, что f_* инъективна тогда и только тогда, когда f^* сюръективна.

Оказывается, в соответствии Галуа каждая функция однозначно определяется сопряженной, явно через нее выражаясь.

Лемма 1.6.56. *Пусть (f_*, f^*) — соответствие Галуа между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$. Тогда*

$$f_*(x) = \min\{w \in B \mid x \leqslant_A f^*(w)\} \quad \text{и} \quad f^*(y) = \max\{z \in A \mid f_*(z) \leqslant_B y\}$$

для всех $x \in A$ и $y \in B$ (здесь min *и* max *означают наименьший и наибольший элемент соответственно).*

Доказательство. Как мы видели, $x \leqslant_A f^*(f_*(x))$ и $f_*(f^*(w)) \leqslant_B w$. Рассмотрим произвольный $w \in B$ со свойством $x \leqslant_A f^*(w)$. Используя монотонность, получаем $f_*(x) \leqslant_B f_*(f^*(w)) \leqslant_B w$. Поэтому $f_*(x)$ есть наименьший элемент B с этим свойством. Второе равенство получаем аналогично. □

Следствие 1.6.57. *Если (f, f^1) и (f, f^2) (или (f_1, f) и (f_2, f)) суть соответствия Галуа между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$, то $f^1 = f^2$ (соответственно, $f_1 = f_2$).*

Пример 1.6.58. Пусть $\mathcal{A} = (\mathbb{R}_{\geqslant 0}, \leqslant)$, $\mathcal{B} = (\mathbb{N}, \leqslant)$ и $\alpha(x) = \lfloor x \rfloor$. Тогда невозможно соответствие Галуа вида (α, f^*) между $\mathcal{A}$ и $\mathcal{B}$. В самом деле, иначе $f^*(n) = \max\{x \in \mathbb{R}_{\geqslant 0} \mid \lfloor x \rfloor \leqslant n\}$, что невозможно ни при каком $n > 0$.

Пример 1.6.59. Соответствия Галуа имеют фундаментальное значение для математической логики. Пока ограничимся неформальным примером. Пусть $\mathcal{A} = (\mathcal{P}(A), \subseteq)$ и $\mathcal{B} = (\mathcal{P}(B), \supseteq)$, где A есть некоторая совокупность «свойств», а B — совокупность «предметов», которые могут обладать или не обладать свойствами из A.

Пусть $f_*(\Phi)$ есть множество всех предметов, обладающих каждым свойством из Φ, а $f^*(Y)$ есть множество всех тех свойств, которыми обладает каждый предмет из Y. Ясно, что

$$f_*(\Phi) \supseteq Y \iff \Phi \subseteq f^*(Y),$$

а значит, (f_*, f^*) является соответствием Галуа между $\mathcal{A}$ и $\mathcal{B}$. Если, например, $A = \{\text{человек},\ \text{смертный}\}$ и B есть множество всех людей, то $f_*(\{\text{человек}\}) = B = f_*(A)$. Видим, что это соответствие не является, вообще говоря, изоморфизмом.

Особый интерес представляют такие множества свойств, которые полностью (относительно совокупностей A и B) характеризуют удовлетворяющие им предметы, т. е. $f^*(f_*(\Phi)) = \Phi$. Такие Φ можно считать «логически замкнутыми»: они *содержат* все свойства, которым *обязаны* удовлетворять предметы, удовлетворяющие всем свойствам из Φ. Каждый человек смертен, а потому множество $\{\text{человек}\}$ не замкнуто в отличие от $\{\text{человек},\ \text{смертный}\}$.

Лемма 1.6.60. *Пусть (f_*, f^*) — соответствие Галуа между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$, а $c = f^* \circ f_*$. Тогда при всех $x, y \in A$ верно:*

1) $x \leqslant_A c(x)$;

2) $x \leqslant_A y \Longrightarrow c(x) \leqslant_A c(y)$;

3) $c(c(x)) = c(x)$.

Доказательство. Первое и второе утверждения сразу следуют из леммы 1.6.53. Оттуда же $c \circ c = f^* \circ (f_* \circ f^* \circ f_*) = f^* \circ f_* = c$. □

Функция $d = f_* \circ f^*$ также обладает вторым и третьим свойствами, а вместо первого удовлетворяет неравенству $d(y) \leqslant_B y$. Мы неоднократно встретимся с такими свойствами отображений упорядоченного множества в себя в дальнейшем. Скажем, функции $x \mapsto \lceil x \rceil$ и $x \mapsto \lfloor x \rfloor$ на $(\mathbb{R}_{\geqslant 0}, \leqslant)$ представляют собой примеры функций c и d соответственно (что неудивительно в свете примера 1.6.52).

Неформально говоря, свойства отображения c отвечают идее «замыкания», «вытягивания» элемента x на максимальный доступный ему уровень. Наш пример с «логической замкнутостью» множества Φ как раз такого рода: $c(\Phi) = \Phi$. Еще один (шуточный) пример: $c(x)$ есть уровень знаний студента с изначальным уровнем x после *эффективного* обучения. Такое обучение не ухудшает ничьих знаний, не подавляет более подготовленных студентов и является исчерпывающим — повторное обучение (и пересдача) бесполезны.

Лемма 1.6.61. *Пусть (f_*, f^*) — соответствие Галуа между ч. у. м. $\mathcal{A}$ и $\mathcal{B}$, $c = f^* \circ f_*$ и $d = f_* \circ f^*$. Тогда $x \in \operatorname{rng} f^* \iff c(x) = x$ и $y \in \operatorname{rng} f_* \iff d(y) = y$.*

Доказательство. Очевидно, что $x \in \operatorname{rng} f^*$, если $f^*(f_*(x)) = x$. Обратно, $c(f^*(y)) = (f^* \circ f_* \circ f^*)(y) = f^*(y)$. □

В нашем примере это означает, что множество свойств Φ «логически замкнуто» тогда и только тогда, когда Φ есть все свойства, общие некоторому множеству предметов. Кроме того, если $\Psi \subseteq \Phi$ и Φ «логически замкнуто», то $\Psi \subseteq c(\Psi) \subseteq c(\Phi) = \Phi$ и $c(c(\Psi)) = c(\Psi)$, т. е. $c(\Psi)$ есть наименьшее «логически замкнутое» надмножество Ψ, множество всевозможных «следствий» свойств из Ψ.

§ 1.7. Эквивалентности

Отношение $R \subseteq A^2$ называется *отношением эквивалентности* (или просто *эквивалентностью*) на A, если R рефлексивно, симметрично и транзитивно.

Пример 1.7.1. Отношения A^2 и id_A суть эквивалентности. Отношение «x и y сравнимы по модулю $m > 0$» (т. е. $m \,|\, (x-y)$) на множестве $\mathbb{Z}$ есть отношение эквивалентности. Отношение параллельности прямых на плоскости, если считать, что каждая прямая параллельна самой себе, есть эквивалентность. Отношение равномощности $\sim$ на любом множестве (чьи элементы, напомним, тоже множества) есть эквивалентность.

Пример 1.7.2. Пусть $f\colon A \to B$. Тогда отношение

$$\ker f = \{(x, y) \in A^2 \mid f(x) = f(y)\},$$

называемое *ядерной эквивалентностью* (или *ядром*) функции f, есть, в самом деле, эквивалентность на множестве A.

Замечание 1.7.3. Понятие эквивалентности обобщает понятие равенства (которое на каждом множестве A совпадает с отношением id_A). При этом некоторые свойства равенства эквивалентность может утратить. Например, если R является эквивалентностью на множестве A и $f\colon A^n \to A$, то из $x_i R y_i$ для $1 \leqslant i \leqslant n$, вообще говоря, не следует, что $f(x_1, \ldots, x_n) R f(y_1, \ldots, y_n)$.

Впрочем, многие важные эквивалентности таким свойством обладают. Они называются *конгруэнциями* (относительно f). Например, отношение $\equiv_m$ сравнимости по модулю m является конгруэнцией относительно сложения и умножения целых чисел: если $x \equiv_m x'$ и $y \equiv_m y'$, то $x + y \equiv_m x' + y'$ и $xy \equiv_m x'y'$ (проверьте!).

Пример 1.7.4. Покажем, что $R \subseteq A^2$ есть эквивалентность тогда и только тогда, когда $(R \circ R^{-1}) \cup \mathrm{id}_A = R$.

Пусть R — эквивалентность. Тогда $R = \mathrm{id}_A \circ R \subseteq R \circ R \subseteq R$, а значит, $R = R \circ R = R \circ R^{-1}$. Отсюда $R = R \cup \mathrm{id}_A = (R \circ R^{-1}) \cup \mathrm{id}_A$.

Обратно. Пусть выполнено наше равенство. Тогда, очевидно, $\mathrm{id}_A \subseteq$ $\subseteq R$. Далее, $R^{-1} = (R \circ R^{-1})^{-1} \cup \mathrm{id}_A^{-1} = ((R^{-1})^{-1} \circ R^{-1}) \cup \mathrm{id}_A = R$. Наконец, $R \circ R = R \circ R^{-1} \subseteq R$.

Факторизация. Содержательно, эквивалентность элементов позволяет их отождествить, «склеить», пренебрегая несущественными в данном случае различиями. В результате получается новое множество «классов» исходных элементов. Например, если отождествить натуральные числа одной четности, получится всего два класса. А если отождествить одноцветные предметы в совокупности всевозможных белых, красных и зеленых, получится трехэлементное множество «цветов».[23] Подобные конструкции широко распространены в математике.

Итак, пусть E есть эквивалентность на множестве A и $x \in A$. Назовем множество

$$[x]_E = \{z \in A \mid xEz\}$$

классом эквивалентности элемента x по отношению E. Множество

$$A/E = \{\sigma \in \mathcal{P}(A) \mid \exists x \in A\ [x]_E = \sigma\} = \{[x]_E \mid x \in A\}$$

называется *фактор-множеством* множества A по отношению E.

Замечание 1.7.5. «Классы эквивалентности» суть знакомые нам образы множеств под действием E: именно $[x]_E = E[\{x\}]$. Это наблюдение обосновывает распространенное в алгебре обозначение xE для класса $[x]_E$.

Пример 1.7.6. Множество A/A^2 есть просто $\{A\}$, поскольку все элементы A^2-эквивалентны и попадают в один класс. Множество A/id_A есть множество всех одноэлементных подмножеств A. Следовательно, $A/\mathrm{id}_A \sim A$.

Если $x \equiv_m y$, то, как легко проверить, x и y дают одинаковые остатки при делении на m, и наоборот. Поэтому класс $[x]_{\equiv_m}$ состоит в точности из чисел, делящихся на m с тем же остатком, что и x.

[23] На этом примере видна философская трудность, отягчающая понятие эквивалентности: после отождествления из совокупности *конкретных* предметов (таких как помидоры, огурцы и др.) получилось множество *абстрактных* свойств – цветов.

При делении на m возможны остатки $0, 1, \ldots, m-1$. Поэтому $\mathbb{Z}/{\equiv_m} \sim$ $\sim \{0, 1, \ldots, m-1\}$.

Если мы проведем на плоскости Π какую-либо прямую l и рассмотрим отношение «точки x и y лежат по одну сторону l или обе на ней», такое отношение L будет, очевидно, эквивалентностью. Множество Π/L состоит из трех элементов: двух полуплоскостей, на которые l рассекает Π, и самой прямой l.

Пример 1.7.7. Пусть $f\colon A \to B$. Что есть $A/\ker f$? Очевидно, $x \ker f = \{z \in A \mid f(z) = f(x)\} = f^{-1}[\{f(x)\}]$. Поэтому $\sigma \in A/\ker f$ тогда и только тогда, когда $\sigma = f^{-1}[\{y\}]$ для некоторого $y \in \operatorname{rng} f = f[A]$. Таким образом, $A/\ker f$ есть множество «полных прообразов» всевозможных значений функции f. Например, пусть $A = B = \mathbb{R}$ и $f = \cos$. Тогда

$$\mathbb{R}/\ker\cos = \{\{\pm\arccos\alpha + 2\pi k \mid k \in \mathbb{Z}\} \mid \alpha \in [0,1]\}.$$

Лемма 1.7.8. *Пусть E — эквивалентность на множестве A. Тогда для произвольных $x, y \in A$ верно:*

1) $x \in [x]_E$;

2) $[x]_E \cap [y]_E \neq \varnothing \iff xEy \iff [x]_E = [y]_E$.

Доказательство. Первое утверждение следует из xEx. Для второго допустим, что $z \in [x]_E \cap [y]_E$. Тогда xEz и yEz, откуда zEy и, далее, xEy. В свою очередь, пусть xEy и $z \in [x]_E$, т. е. xEz. Вновь применяя симметричность и транзитивность E, получаем yEz. Итак, $[x]_E \subseteq [y]_E$. Второе включение аналогично. Наконец, предположим, что $[x]_E = [y]_E$. Но тогда, по первому утверждению, $x \in [x]_E \cap [y]_E \neq \varnothing$. $\square$

Упражнение 1.7.9. Докажите, что для любого множества A и любой эквивалентности E на нем найдутся множество B и сюръекция $f\colon A \to$ $\to B$, т. ч. $E = \ker f$.

Упражнение 1.7.10. Пусть отношение $R \subseteq A^2$ рефлексивно и транзитивно. При всех $x, y \in A$ положим $xEy \iff xRy$ и yRx. Проверьте, что E есть эквивалентность на A. При всех $\sigma, \tau \in A/E$ положим $\sigma \leqslant \tau \iff \exists x \in \sigma\, \exists y \in \tau\ xRy$. Докажите, что $\leqslant$ есть нестрогий частичный порядок на множестве A/E.

Замечание 1.7.11. Рефлексивные транзитивные отношения называются *предпорядками*. Например, таково отношение $\lesssim$ на любом множестве A. Как мы знаем, $X \sim Y \iff X \lesssim Y$ и $Y \lesssim X$. Поэтому на фактор-множестве $A/\!\sim$, согласно предыдущему упражнению, $\lesssim$ определяет весьма естественный порядок, называемый *сравнением по мощности*. В последующих частях курса мы покажем, опираясь на аксиому выбора, что такой порядок всегда линейный.

Эквивалентности и разбиения. Как видим, классы эквивалентности покрывают все множество A, причем разные классы не пересекаются. Можно сказать, что отношение эквивалентности E «разбивает» множество A на попарно не пересекающиеся «куски». Точнее, назовем множество $\Sigma \subseteq \mathcal{P}(A)$ *разбиением* множества A, если

$$\varnothing \notin \Sigma, \quad \cup\Sigma = A \quad \text{и} \quad \forall \sigma, \tau \in \Sigma \, (\sigma \cap \tau \neq \varnothing \Longrightarrow \sigma = \tau).$$

Пример 1.7.12. Лемма 1.7.8 показывает, что любое фактор-множество A/E является разбиением A. Пусть $\mathbb{R}_-$ есть множество всех отрицательных вещественных чисел. Тогда $\{\mathbb{R}_-, \{0\}, \mathbb{R}_+\}$ есть разбиение $\mathbb{R}$. На плоскости множество окружностей с центром O всевозможных радиусов $0 \leqslant r \leqslant 1$ (окружность нулевого радиуса есть одна точка) является разбиением круга с центром O радиуса 1 (с границей).

Упражнение 1.7.13. Найдите все разбиения множества $\varnothing$.

Оказывается, что не только каждое фактор-множество есть разбиение, но и каждое разбиение будет фактор-множеством по подходящей эквивалентности, причем между теми и другими есть весьма естественное соответствие.

Итак, пусть $Eq(A)$ есть множество всех отношений эквивалентности на A, и $\Pi(A)$ есть множество всех разбиений множества A. Рассмотрим функции $\pi\colon Eq(A) \to \mathcal{P}(\mathcal{P}(A))$ и $\varepsilon\colon \Pi(A) \to \mathcal{P}(A^2)$, т. ч.

$$\pi(E) = A/E \quad \text{и} \quad \varepsilon(\Sigma) = \{(x, y) \in A^2 \mid \exists \sigma \in \Sigma \, (x \in \sigma \text{ и } y \in \sigma)\}$$

для всех $E \in Eq(A)$ и $\Sigma \in \Pi(A)$. Иначе говоря, отношение $\varepsilon(\Sigma)$ состоит из пар таких точек, что обе принадлежат какому-то одному элементу («куску») разбиения Σ.

Теорема 1.7.14. *Для любых $E \in Eq(A)$ и $\Sigma \in \Pi(A)$ верно:*

1) $\pi(E) \in \Pi(A)$ *и* $\varepsilon(\pi(E)) = E$;

2) $\varepsilon(\Sigma) \in Eq(A)$ *и* $\pi(\varepsilon(\Sigma)) = \Sigma$.

Доказательство. Как мы уже заметили, $\pi(E)$ есть разбиение A в силу леммы 1.7.8. Пусть $(x,y) \in \varepsilon(A/E)$. Тогда существует $\sigma \in A/E$, т. ч. $x, y \in \sigma$, т. е. $x, y \in [z]_E$ для некоторого $z \in A$. Значит, zEx и zEy, откуда $(x,y) \in E$. Обратно, пусть xEy. Тогда, согласно лемме 1.7.8, $y \in [y]_E = [x]_E$ и $x, y \in [x]_E \in A/E$. Следовательно, $(x,y) \in \varepsilon(A/E)$. Итак, $\varepsilon(\pi(E)) = E$.

Проверим теперь, что $\varepsilon(\Sigma)$ есть эквивалентность на A. Поскольку $\cup\Sigma = A$, для каждого $x \in A$ найдется $\sigma \in \Sigma$, т. ч. $x \in \sigma$; значит, $(x,x) \in \varepsilon(\Sigma)$. Симметричность $\varepsilon(\Sigma)$ очевидна. Допустим теперь, что $(x,y), (y,z) \in \varepsilon(\Sigma)$. Тогда для некоторых $\sigma, \tau \in \Sigma$ имеем $x \in \sigma$, $y \in \sigma$, $y \in \tau$ и $z \in \tau$. Из $\sigma \cap \tau \neq \varnothing$ получаем $\sigma = \tau$, откуда $x, z \in \sigma$ и $(x,z) \in \varepsilon(\Sigma)$.

Остается проверить, что $\pi(\varepsilon(\Sigma)) = \Sigma$. Докажем сначала, что для всех $\sigma \in \Sigma$ и всех $x \in \sigma$ верно $\sigma = [x]_{\varepsilon(\Sigma)}$. В самом деле, если $y \in \sigma$, получаем $x, y \in \sigma \in \Sigma$, откуда $(x,y) \in \varepsilon(\Sigma)$, т. е. $y \in [x]_{\varepsilon(\Sigma)}$. Имеем $\sigma \subseteq [x]_{\varepsilon(\Sigma)}$. Обратно, пусть $y \in [x]_{\varepsilon(\Sigma)}$. Тогда $x, y \in \sigma'$ для некоторого $\sigma' \in \Sigma$. Из $x \in \sigma \cap \sigma' \neq \varnothing$ следует, что $\sigma' = \sigma$, а значит, $y \in \sigma$. Получили $[x]_{\varepsilon(\Sigma)} \subseteq \sigma$.

Допустим теперь, что $\tau \in A/\varepsilon(\Sigma)$. Тогда $\tau = [x]_{\varepsilon(\Sigma)}$ для некоторого $x \in A$. С другой стороны, $x \in \sigma$ для некоторого $\sigma \in \Sigma$ в силу $\cup\Sigma = A$. По доказанному $\sigma = [x]_{\varepsilon(\Sigma)}$, а значит, $\tau = \sigma \in \Sigma$. Таким образом, $\pi(\varepsilon(\Sigma)) \subseteq \Sigma$.

Обратно, пусть $\tau \in \Sigma$. Поскольку $\tau \neq \varnothing$, можно выбрать $x \in \tau$. Имеем тогда $\tau = [x]_{\varepsilon(\Sigma)} \in A/\varepsilon(\Sigma)$. Итак, $\Sigma \subseteq \pi(\varepsilon(\Sigma))$. □

Из результата упражнения 1.5.27 получаем

Следствие 1.7.15. *Функция* $\pi\colon Eq(A) \to \Pi(A)$ *является биекцией, причем* $\varepsilon = \pi^{-1}$.

Решетка эквивалентностей. Отношения эквивалентности на A как подмножества A^2 можно частично упорядочить по включению. Сразу отметим, в ч. у. м. $(Eq(A), \subseteq)$ есть наибольший элемент A^2 и наименьший элемент id_A.

Оказывается, полученная биекция π множеств $Eq(A)$ и $\Pi(A)$ может рассматриваться как изоморфизм ч. у. м. Пусть, в самом деле, $\Sigma_1, \Sigma_2 \in \Pi(A)$. Будем писать $\Sigma_1 \leqslant \Sigma_2$ и говорить, что Σ_1 *мельче* Σ_2, если для каждого $\sigma \in \Sigma_1$ найдется $\tau \in \Sigma_2$, т. ч. $\sigma \subseteq \tau$. Иначе говоря, каждый Σ_1-кусок целиком попадает в некоторый Σ_2-кусок, т. е. Σ_1 представляет собой «более мелкую нарезку» множества A.

Лемма 1.7.16. $(\Pi(A), \leqslant)$ *есть ч. у. м.*

Доказательство. Проверим лишь антисимметричность. Пусть $\Sigma_1 \leqslant \Sigma_2$ и $\Sigma_2 \leqslant \Sigma_1$. Тогда если $\sigma \in \Sigma_1$, то найдется $\tau \in \Sigma_2$, т. ч. $\sigma \subseteq \tau$, но также найдется $\sigma' \in \Sigma_1$, т. ч. $\tau \subseteq \sigma'$. Из $\sigma \subseteq \tau \subseteq \sigma'$ следует $\sigma \cap \sigma' = \sigma \neq \varnothing$, откуда $\sigma = \sigma'$ и $\sigma = \tau \in \Sigma_2$. Итак, $\Sigma_1 \subseteq \Sigma_2$. Аналогично доказывая обратное включение, имеем $\Sigma_1 = \Sigma_2$. $\square$

Теорема 1.7.17. *Для всякого A верно $(Eq(A), \subseteq) \overset{\pi}{\cong} (\Pi(A), \leqslant)$.*

Доказательство. Мы уже показали, что π — биекция, так что достаточно проверить

$$E_1 \subseteq E_2 \iff A/E_1 \leqslant A/E_2$$

при всех $E_1, E_2 \in Eq(A)$. Итак, пусть $E_1 \subseteq E_2$ и $\sigma \in A/E_1$. Тогда $\sigma = [x]_{E_1}$ для некоторого $x \in A$. Если $y \in [x]_{E_1}$, то xE_1y и тем более xE_2y, т. е. $y \in [x]_{E_2}$. Значит, $\sigma \subseteq [x]_{E_2} \in A/E_2$. Итак, $A/E_1 \leqslant A/E_2$.

Обратно, пусть $A/E_1 \leqslant A/E_2$ и xE_1y. Тогда $y \in [x]_{E_1}$ и существует $\sigma \in A/E_2$, т. ч. $[x]_{E_1} \subseteq \sigma$. Значит, $x, y \in \sigma$, однако $\sigma = [z]_{E_2}$ для некоторого $z \in A$. Имеем zE_2x и zE_2y, откуда xE_2y. Получили $E_1 \subseteq E_2$. $\square$

Лемма 1.7.18. *Ч. у. м. $(Eq(A), \subseteq)$ и $(\Pi(A), \leqslant)$ суть решетки.*

Доказательство. Ввиду изоморфизма достаточно рассмотреть лишь $(Eq(A), \subseteq)$. Пусть $E_1, E_2 \in Eq(A)$. Очевидно, $E_1 \cap E_2$ есть нижняя грань $\{E_1, E_2\}$ в $(\mathcal{P}(A), \subseteq)$. Также для всякого F если $F \subseteq E_1$ и $F \subseteq E_2$, то $F \subseteq E_1 \cap E_2$. Поэтому $\inf\{E_1, E_2\}$ непременно включен в $E_1 \cap E_2$. Используя пример 1.6.6, легко проверить, что $E_1 \cap E_2 \in Eq(A)$. Поэтому $E_1 \cap E_2$ есть наибольшая нижняя грань $\{E_1, E_2\}$ в $(Eq(A), \subseteq)$.

Аналогичные рассуждения, однако, не приводят к успеху для супремума, поскольку $E_1 \cup E_2$ не всегда эквивалентность. Пусть $X_n = \{1, \ldots, n\}$ и $f\colon X_n \to \{1, 2\}$, т. е. f есть последовательность единиц и двоек длины n. Положим[24] $E_f = E_{f(1)} \circ E_{f(2)} \circ \ldots \circ E_{f(n)}$ и

$$E = \bigcup_{n \in \mathbb{N}_+} \{E_f \mid f\colon X_n \to \{1, 2\}\}.$$

Иначе говоря, множество E есть объединение всевозможных конечных композиций E_1 и E_2, взятых в произвольном порядке. (Например, $E_1 \circ \circ E_2 \circ E_2 \circ E_1 \subseteq E$. Ясно, что некоторые композиции можно «сократить», поскольку $F \circ F = F$ для всякой эквивалентности F.)

[24] Аккуратное определение фигурирующих здесь множеств использует *рекурсию*, о которой речь пойдет ниже.

Проверим, что $E \in Eq(A)$. Очевидно, что $\mathrm{id}_A \subseteq E_1 \subseteq E$. Пусть xEy. Тогда $(x,y) \in E_{f(1)} \circ E_{f(2)} \circ \ldots \circ E_{f(n)}$ для некоторых n и f. Имеем

$$(y,x) \in (E_{f(1)} \circ E_{f(2)} \circ \ldots \circ E_{f(n)})^{-1} = E_{f(n)}^{-1} \circ \ldots E_{f(2)}^{-1} \circ E_{f(1)}^{-1} = \\ = E_{f(n)} \circ \ldots E_{f(2)} \circ E_{f(1)} = E_{g(1)} \circ \ldots E_{g(n-1)} \circ E_{g(n)} \subseteq E,$$

где $g(k) = f(n+1-k)$ при всех $k \in X_n$. Наконец, пусть xEy и yEz, т. е. $(x,y) \in E_{f(1)} \circ E_{f(2)} \circ \ldots \circ E_{f(n)}$ и $(y,z) \in E_{g(1)} \circ E_{g(2)} \circ \ldots \circ E_{g(m)}$ для некоторых n, m, f, g. Тогда

$$(x,z) \in (E_{g(1)} \circ E_{g(2)} \circ \ldots \circ E_{g(m)}) \circ (E_{f(1)} \circ E_{f(2)} \circ \ldots \circ E_{f(n)}) = \\ = E_{h(1)} \circ E_{h(2)} \circ \ldots \circ E_{h(m+n)} \subseteq E,$$

где $h(k) = g(k)$ при $1 \leqslant k \leqslant m$ и $h(k) = f(k-m)$ при $m < k \leqslant m+n$. Итак, $E \in Eq(A)$.

Очевидно, что $E_1, E_2 \subseteq E$. Пусть $E_1, E_2 \subseteq F \in Eq(A)$. Тогда для всех $n \in \mathbb{N}_+$ и $f\colon X_n \to \{1,2\}$ имеем

$$E_{f(1)} \circ E_{f(2)} \circ \ldots \circ E_{f(n)} \subseteq F \circ F \circ \ldots \circ F \subseteq F.$$

Поэтому $E \subseteq F$. Итак, $E = \sup\{E_1, E_2\}$. □

Упражнение 1.7.19. Докажите, что ч. у. м. $(Eq(A), \subseteq)$ является полной решеткой, и выясните, как устроен $\sup_{i \in I} E_i$, где $E_i \in Eq(A)$ при всех $i \in I$.

Глава 2. Натуральные числа

§ 2.1. Индукция и рекурсия. Конечные множества

Напомним, что $\mathbb{N}$ означает *множество натуральных чисел*, которое мы пока принимали вместе с некоторой неуточняемой совокупностью «простейших свойств». Настало время выделить самое главное свойство натуральных чисел: *принцип индукции*.

Вообще, индукцией называют способ рассуждений, при котором свойства частных случаев как-либо переносятся на совокупность всех возможных случаев. Индукция — основа эмпирических наук[1].

В математической практике наиболее существенно то обстоятельство, что «совокупность всех возможных случаев» может оказаться бесконечной. Индукция же позволяет установить ее свойства некоторыми конечными рассуждениями о частных случаях. Мы уже сталкивались с подобным, изучая аксиому выбора: тогда из существования подходящего объекта в каждом случае заключалось существование бесконечной «последовательности» подходящих объектов (т. е. функции выбора). Индукция, аксиома выбора и бесконечность, как мы увидим, тесно связаны. В частности, множество $\mathbb{N}$ является в некотором смысле наименьшим бесконечным и наименьшим, удовлетворяющим принципу индукции.

Три формы принципа индукции. Мы полагаем, читателю известна «школьная» формулировка *принципа математической индукции* для множества $\mathbb{N}$:

> Для всякого свойства φ если $\varphi(0)$ и для каждого $n \in \mathbb{N}$ из $\varphi(n)$ следует $\varphi(n+1)$, то имеет место $\varphi(n)$ для всех $n \in \mathbb{N}$.

[1] «Такие свойства тел, ... которые оказываются присущи всем телам, над которыми возможно производить испытания, должны быть почитаемы за свойства всех тел вообще». (*И. Ньютон.* Математические начала натуральной философии. Кн. 3. О системе мира. Правила умозаключений в физике. Правило III.)

Утверждение $\varphi(0)$ называют *основанием* (или *базисом*, *базой*) индукции, утверждение $\forall n \in \mathbb{N}\,(\varphi(n) \Longrightarrow \varphi(n+1))$ называют *индукционным переходом* (или *шагом индукции*), а утверждение $\varphi(n)$ при каждом n — *индуктивным предположением* (или *гипотезой*).

Удобно переформулировать принцип математической индукции, не упоминая «свойства» вовсе:

> Для всякого множества $X \subseteq \mathbb{N}$ если $0 \in X$ и для каждого $n \in \mathbb{N}$ из $n \in X$ следует $n+1 \in X$, то $X = \mathbb{N}$.

В самом деле, для всякого свойства φ мы можем выделить в $\mathbb{N}$ подмножество $X = \{n \in \mathbb{N} \mid \varphi(n)\}$, и обратно, каждому множеству $X \subseteq \mathbb{N}$ можно поставить в соответствие свойство «$n \in X$» натурального числа n. Поэтому эта формулировка равносильна исходной.

Заметим, что название «*математическая* индукция» в нашем курсе не имеет иной цели, как только отличить приведенную формулировку принципа индукции от следующих ниже (и, как мы увидим, равносильных).

Пример 2.1.1. Покажем, что для каждого натурального $n \geqslant 3$ найдутся $a_1, \ldots, a_n \in \mathbb{N}_+$, т. ч.

$$1 = \frac{1}{a_1} + \ldots + \frac{1}{a_n},$$

причем $a_i \neq a_j$, если $i \neq j$.

Дадим подробное решение. Обозначив $A_n = \{k \in \mathbb{N} \mid 1 \leqslant k \leqslant n\}$, мы рассматриваем множество

$$X = \{n \in \mathbb{N} \mid n < 3 \text{ или } \exists \text{инъекция } f\colon A_n \to \mathbb{N}_+ \text{ т. ч. } \textstyle\sum_{k=1}^{n} \frac{1}{f(k)} = 1\}.$$

Проверим, выполнены ли для $X \subseteq \mathbb{N}$ посылки принципа математической индукции. Очевидно, $0 \in X$, так что основание индукции верно. Рассмотрим произвольное $n \in X$ и докажем, что $n+1 \in X$. Если $n+1 < 3$, то все ясно. Если $n+1 = 3$, то $n+1 \in X$, поскольку

$$1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}.$$

(Обратите внимание, что здесь мы не применяем бесполезное предположение $2 \in X$ (очевидно, если $1 = \frac{1}{a} + \frac{1}{b}$, то $a = b = 2$). Содержательно, именно $3 \in X$ является тут «основанием индукции»; однако, как видит читатель, легко обойтись индукцией от нуля, не усложняя формулировку принципа.) Пусть теперь $n+1 > 3$. Тогда $n \geqslant 3$, и,

по предположению $n \in X$, мы находим инъекцию $f\colon A_n \to \mathbb{N}_+$, т. ч. $\sum_{k=1}^{n} \frac{1}{f(k)} = 1$. Определим функцию $g\colon A_{n+1} \to \mathbb{N}_+$ так: $g(k) = 2f(k)$, если $k \in A_n$, и $g(n+1) = 2$. Имеем

$$\sum_{k=1}^{n+1} \frac{1}{g(k)} = \sum_{k=1}^{n} \frac{1}{2f(k)} + \frac{1}{2} = \frac{1}{2} \sum_{k=1}^{n} \frac{1}{f(k)} + \frac{1}{2} = \frac{1}{2} \cdot 1 + \frac{1}{2} = 1.$$

Остается убедиться, что g инъективна. Если различные $k, l \in A_n$, то $g(k) \neq g(l)$ в силу инъективности f. Если при этом $g(k) = g(n+1)$, то $f(k) = 1$. Однако тогда $\frac{1}{f(l)} = 0$ при всех $l \neq k$. Поскольку $n > 1$, такое невозможно. Следовательно, g — инъекция, и $n+1 \in X$.

Проверив для X основание и переход, по принципу математической индукции мы заключаем, что $X = \mathbb{N}$. Рассматривая $n \geqslant 3$, получаем требуемое свойство.

Довольно часто по индукции удается доказать лишь более сильное утверждение, чем требуется[2].

Пример 2.1.2. Покажем, что для всех $n \in \mathbb{N}$ выполнено

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \ldots \cdot \frac{2n+1}{2n+2} < \frac{1}{\sqrt{3n+3}}.$$

Положим $f(n) = \prod_{k=0}^{n} \frac{2k+1}{2k+2}$. Индукцией по n попробуем доказать неравенство $f(n) < \frac{1}{\sqrt{3n+3}}$. Очевидно, что $f(0) = \frac{1}{2} < \frac{1}{\sqrt{3}}$. Проверим индукционный переход: из $f(n) < \frac{1}{\sqrt{3n+3}}$ следует $f(n+1) < \frac{1}{\sqrt{3n+6}}$. Очевидно, *достаточно* доказать, что

$$\frac{f(n+1)}{f(n)} = \frac{2n+3}{2n+4} < \sqrt{\frac{n+1}{n+2}},$$

что, увы, неверно уже при $n = 0$ (и при всяком $n \in \mathbb{N}$). Таким образом, проверка индукционного перехода не кажется очевидной.

Дело можно поправить, если доказывать, что $f(n) \leqslant \frac{1}{\sqrt{3n+4}}$ при всех $n \in \mathbb{N}$, откуда сразу следует исходное утверждение. Основание индукции очевидно. Далее, при любом $n \in \mathbb{N}$ имеем

$$\frac{f(n+1)}{f(n)} = \frac{2n+3}{2n+4} \leqslant \sqrt{\frac{3n+4}{3n+7}},$$

[2]Причина в том, что вывод $\varphi(n+1)$ из слишком слабого (на первый взгляд) предположения $\varphi(n)$ может быть неочевиден, хотя, как становится потом ясным, свойством φ обладают все натуральные n.

в чем легко убедится читатель. Значит, если принять предположение индукции для n,

$$f(n+1)\sqrt{3n+7} \leqslant f(n)\sqrt{3n+4} \leqslant 1.$$

Тем самым, шаг индукции обоснован, и требуемое утверждение доказано.

Назовем множество $X \subseteq \mathbb{N}$ *прогрессивным*, если для каждого $n \in$ $\in \mathbb{N}$ из $\forall m < n\ m \in X$ следует $n \in X$.

Образно говоря, прогрессивное множество X «карабкается вверх» по ряду натуральных чисел: если оно завладело всеми m до некоторого n, то и n попадает в X. Будем писать $Prog(X)$, если X прогрессивно. Мы называем *принципом порядковой* (или *сильной*) *индукции* утверждение:

$$\forall X \subseteq \mathbb{N}\ (Prog(X) \Longrightarrow X = \mathbb{N}).$$

Содержательно принцип порядковой индукции отличается от принципа математической индукции тем, что допускает более сильное «индуктивное предположение»: именно, что $0, 1, \ldots, n \in X$, вместо $n \in X$. Таким образом, сам этот принцип не слабее принципа математической индукции.

Замечание 2.1.3. Утверждение $Prog(X)$, очевидно, соответствует индукционному переходу. Но где же основание индукции? Как нетрудно заметить, оно также содержится в $Prog(X)$, поскольку $Prog(X)$ влечет $0 \in X$. В самом деле, для прогрессивного X из $\forall m < 0\ m \in X$ следует $0 \in X$. Но натуральных чисел меньше нуля нет, а значит, утверждение $\forall m < 0\ m \in X$ истинно.

Пример 2.1.4. Пусть число $a + \dfrac{1}{a} \in \mathbb{Z}$ для некоторого $a \in \mathbb{R}$. Докажем, что тогда для любого $n \in \mathbb{N}$ верно $a^n + \dfrac{1}{a^n} \in \mathbb{Z}$.

Установим прогрессивность множества $X = \{n \in \mathbb{N} \mid a^n + \dfrac{1}{a^n} \in \mathbb{Z}\}$. Пусть некоторое $n \in \mathbb{N}$ таково, что $m \in X$ для всех $m < n$. Если $n \geqslant 2$, то натуральные числа $n-1, n-2 \in X$. Имеем тогда

$$a^n + \frac{1}{a^n} = \left(a + \frac{1}{a}\right)\left(a^{n-1} + \frac{1}{a^{n-1}}\right) - \left(a^{n-2} + \frac{1}{a^{n-2}}\right).$$

Произведение и разность целых чисел целые, поэтому $n \in X$. В случае $n \leqslant 1$ непосредственно видно, что $n \in X$. Итак, мы получили $Prog(X)$. В силу принципа порядковой индукции, $X = \mathbb{N}$.

Дополнительно стоит заметить, что в условиях нашей задачи $a^x + \frac{1}{a^x} \in \mathbb{Z}$ вообще для всех $x \in \mathbb{Z}$, поскольку $a^x + \frac{1}{a^x} = a^{|x|} + \frac{1}{a^{|x|}}$ и $|x| \in \mathbb{N}$ для всех $x \in \mathbb{Z}$.

Довольно часто задача, допускающая решение по индукции, не содержит прямого указания на «свойство натуральных чисел». Чтобы придумать такое решение, нужно найти натуральный параметр, распределяющий рассматриваемые объекты по «уровням сложности», и свести свойство более сложных к свойству более простых.

Пример 2.1.5. Пусть имеется $n \in \mathbb{N}_+$ городов, некоторые из которых соединены дорогами с двусторонним движением («дорожная сеть»), причем каждые два города соединены не более чем одной дорогой и каждая дорога имеет концы в разных городах. Покажем, что если из любого города можно проехать по дорогам в любой другой, но при перекрытии любой дороги это свойство теряется («условие У»), то всего имеется ровно $n-1$ дорога[3].

Удобно провести индукцию по числу дорог в сети. Точнее, мы докажем, что прогрессивно множество

$$X = \{m \in \mathbb{N} \mid \forall n \in \mathbb{N}_+ \text{ для любой дорожной сети с } n \text{ городами, } m \text{ дорогами и условием У верно } m = n-1\}.$$

Действительно, пусть $m' \in X$ для всех $m' < m$. Рассмотрим произвольную сеть S с m дорогами, n городами и условием У. Если $m = 0$, то условие У сразу влечет $n = 1$. Иначе есть дорога между разными городами A и B. Удалим ее. Все города, куда все еще можно добраться из A, образуют сеть S' с n' городами и m' дорогами, а куда можно добраться из B, — сеть S'' с n'' городами и m'' дорогами.

Ясно, что каждый город C из S попадает в одну из новых сетей (если C не в S', то путь из A в C включал дорогу AB; участок этого пути за последним проходом AB до C должен сохраниться, т. е. $C \in S''$), причем ровно в одну (иначе через C возникает объезд закрытой дороги AB). Поэтому $n = n' + n''$ и $m = m' + m'' + 1$.

Сеть S' удовлетворяет условию У: по определению, любые ее города связаны через A; если же удаление какой-то дороги в S' не нарушит связности, то тем более оно бы не нарушило ее в S, что не так. Аналогично, и S'' удовлетворяет У. Из $m', m'' < m$ получаем $m', m'' \in X$, откуда $m' = n'-1$ и $m'' = n''-1$. Значит, $m = (n'-1)+(n''-1)+1 = n-1$ и $m \in X$.

[3]Иначе говоря, в дереве на n вершинах ровно $n-1$ ребро.

С помощью порядковой индукции получаем $X = \mathbb{N}$, т. е. для любой сети с любым числом дорог и городов, а значит, просто для любой сети, имеет место требуемое утверждение.

Еще одна форма принципа индукции — это *принцип наименьшего числа*, гласящий:

> Для любого $X \subseteq \mathbb{N}$ если $X \neq \varnothing$, то в X существует наименьший элемент $\min X$.

Пример 2.1.6. Найдем все решения уравнения $8a^4 + 4b^4 + 2c^4 = d^4$ во множестве $\mathbb{Z}$.

Очевидно, набор $(0, 0, 0, 0)$ является решением. Покажем, что никаких иных решений нет. Ясно, что если (a, b, c, d) есть решение, то таков же набор $(|a|, |b|, |c|, |d|) \in \mathbb{N}^4$. Поэтому достаточно доказать, что нет ни одного ненулевого решения во множестве $\mathbb{N}$. Допустим противное. Тогда множество

$$Y = \{(a, b, c, d) \in \mathbb{N}^4 \mid 8a^4 + 4b^4 + 2c^4 = d^4 \text{ и } a + b + c + d > 0\}$$

непусто. Значит, множество $X = \{a + b + c + d \mid (a, b, c, d) \in Y\} \subseteq \mathbb{N}_+$ также непусто. В силу принципа наименьшего числа, существует $x = \min X > 0$, причем $x = a+b+c+d$ для некоторого решения (a, b, c, d). Поскольку $8a^4 + 4b^4 + 2c^4 = d^4$, число d^4 четно. Из арифметики известно, что тогда четно и d, т. е. $d = 2\delta$ для некоторого $\delta \in \mathbb{N}$. Имеем $8a^4 + 4b^4 + 2c^4 = 16\delta^4$, откуда $c^4 = 8\delta^4 - 4a^4 - 2b^4$. Видим, что тогда $c = 2\gamma$ и, рассуждая аналогично, $a = 2\alpha$, $b = 2\beta$ для некоторых $\alpha, \beta, \gamma \in \mathbb{N}$.

Подставляя полученное в исходное равенство, имеем $8\alpha^4 + 4\beta^4 + 2\gamma^4 = \delta^4$. Итак, набор $(\alpha, \beta, \gamma, \delta) \in \mathbb{N}^4$ также является решением. Однако $2(\alpha+\beta+\gamma+\delta) = a+b+c+d = x > 0$, а значит, $\alpha+\beta+\gamma+\delta > 0$. Тогда $(\alpha, \beta, \gamma, \delta) \in Y$ и $\alpha+\beta+\gamma+\delta \in X$. Но $\alpha+\beta+\gamma+\delta < x = \min X$. Противоречие.

Теперь мы покажем, что три сформулированных принципа равносильны, а значит, в качестве «принципа индукции» нам достаточно постулировать любой из них.

Теорема 2.1.7. *Следующие утверждения равносильны:*

1) *принцип порядковой индукции;*

2) *принцип наименьшего числа;*

3) *принцип математической индукции.*

Доказательство. Пусть принцип порядковой индукции выполнен. Тогда убедимся, что в каждом непустом $X \subseteq \mathbb{N}$ есть наименьший элемент. Предположим, что в некотором X нет наименьшего элемента. Покажем, что множество $\bar{X}$ прогрессивно. В самом деле, если $\forall m < n\ m \notin X$, то $n \notin X$, ибо иначе $n = \min X$, что невозможно. По принципу порядковой индукции, $\bar{X} = \mathbb{N}$, а значит, $X = \varnothing$.

Пусть принцип наименьшего числа выполнен. Установим, что для всякого множества $X \subseteq \mathbb{N}$ из предположений $0 \in X$ и $\forall n\,(n \in X \Longrightarrow$ $\Longrightarrow n+1 \in X)$ вытекает $X = \mathbb{N}$. Рассмотрим множество $\bar{X}$. Допустим, что $\bar{X} \neq \varnothing$. Тогда существует $n = \min \bar{X}$. По предположению, $n \neq$ $\neq 0 \notin \bar{X}$. Значит, $n = m + 1$ для некоторого $m \in \mathbb{N}$. Поскольку $m < n$, имеем $m \in X$. В силу предположения, $n = m + 1 \in X$, что не так. Следовательно, $\bar{X} = \varnothing$ и $X = \mathbb{N}$.

Пусть принцип математической индукции выполнен. Проверим, что для всякого множества $X \subseteq \mathbb{N}$ из предположения $Prog(X)$ следует $X = \mathbb{N}$. Рассмотрим множество

$$Y = \{n \in \mathbb{N} \mid \forall m < n\ m \in X\}.$$

Очевидным образом, $0 \in Y$. Допустим, что $n \in Y$. Тогда $\forall m < n\ m \in$ $\in X$, что, в силу прогрессивности X, влечет $n \in X$. Если $m < n+1$, то $m < n$ или $m = n$. В каждом из случаев $m \in X$, а значит, $n + 1 \in Y$. Для множества Y мы проверили основание и шаг индукции; по принципу математической индукции заключаем $Y = \mathbb{N}$. Для всякого $n \in \mathbb{N}$ имеем $n < n + 1 \in Y$, откуда $n \in X$. Следовательно, $X = \mathbb{N}$. □

Конечные множества. Натуральные числа, неформально говоря, выражающие «конечные количества», позволяют дать строгое определение конечного множества и, как мы увидим, развить теорию таковых на основе свойств натуральных чисел. Итак, при всех $n \in \mathbb{N}$ положим

$$\underline{n} = \{k \in \mathbb{N} \mid k < n\}.$$

В частности, имеем $\underline{0} = \varnothing$ и $\underline{n+1} = \underline{n} \cup \{n\}$ для всех $n \in \mathbb{N}$. Заметьте также, что $n \notin \underline{n}$ и $n = \max \underline{n+1}$.

Множества $\underline{n}$ будут рассматриваться нами как «эталонные» конечные множества[4]. Точнее, множество A *конечное*, если $A \sim \underline{n}$ для некоторого $n \in \mathbb{N}$. В противном случае множество A называется *бесконечным*.

[4]При формальном построении натуральных чисел в последующих частях курса окажется, что $n = \underline{n}$.

Пример 2.1.8. Множества $\varnothing \sim \underline{0}$, $\{\varnothing\} \sim \underline{1}$ и $\{\varnothing, \{\varnothing\}\} \sim \underline{2}$ конечные. Множество $A = \{x, y, z\}$ конечно. В зависимости от того, какие множества среди x, y, z равны, имеем $A \sim \underline{1}$, $A \sim \underline{2}$ или $A \sim \underline{3}$. Скажем, если $x = y \neq z$, то $A \sim \underline{2}$.

Следующее часто используемое утверждение устанавливает связь между подмножествами произвольного множества и определенными на этом множестве функциями с конечным множеством значений.

Лемма 2.1.9. *Для любого множества A имеет место $\mathcal{P}(A) \sim \underline{2}^A$.*

Доказательство. В самом деле, рассмотрим отображение $\varphi\colon \mathcal{P}(A) \to \to \underline{2}^A$, т. ч. $\varphi(B) = \chi_B$ при всех $B \subseteq A$, где $\chi_B\colon A \to \underline{2}$ есть *характеристическая функция* (или *индикатор*) подмножества B, определяемая так:

$$\chi_B(x) \quad = \quad \begin{cases} 1, \text{ если } x \in B; \\ 0, \text{ если } x \notin B. \end{cases}$$

Проверим инъективность φ. Пусть $B \neq C$. Без ограничения общности, существует $x \in B \setminus C$. Тогда $\chi_B(x) = 1 \neq 0 = \chi_C(x)$. Значит, $\varphi(B) = \chi_B \neq \chi_C = \varphi(C)$. Проверим сюръективность. Пусть $f\colon A \to \underline{2}$. Положим $B = f^{-1}[\{1\}]$. Очевидно, что $f = \chi_B = \varphi(B)$. Итак, $\mathcal{P}(A) \overset{\varphi}{\twoheadrightarrow} \underline{2}^A$. □

Пример 2.1.10. Как мы знаем, $\mathbb{R} \sim \mathcal{P}(\mathbb{N})$. Поэтому $\mathbb{R} \sim \underline{2}^{\mathbb{N}}$, откуда

$$\mathbb{R} \sim \mathbb{R} \times \{0\} \lesssim \mathbb{R} \times \mathbb{R} \sim \underline{2}^{\mathbb{N}} \times \underline{2}^{\mathbb{N}} \sim (\underline{2} \times \underline{2})^{\mathbb{N}} \sim$$
$$\sim \underline{4}^{\mathbb{N}} \lesssim \mathbb{N}^{\mathbb{N}} \lesssim \mathbb{R}^{\mathbb{N}} \sim (\underline{2}^{\mathbb{N}})^{\mathbb{N}} \sim \underline{2}^{\mathbb{N}\times\mathbb{N}} \sim \underline{2}^{\mathbb{N}} \sim \mathbb{R},$$

в силу теоремы 1.5.11 и примера 1.5.10. Используя теорему 1.5.21, заключаем $\mathbb{R}^2 \sim \mathbb{N}^{\mathbb{N}} \sim \mathbb{R}^{\mathbb{N}} \sim \mathbb{R}$. Утверждение $\mathbb{R}^2 \sim \mathbb{R}$ означает, что на прямой «столько же» точек, сколько и на плоскости. Г. Кантор в 1870-х гг. комментировал близкий этому факт словами: «Вижу, но не верю».

Пример 2.1.11. Покажем, что множество T всевозможных треугольников на плоскости равномощно $\mathbb{R}$.

Используем теорему 1.5.21, сначала проверив $T \lesssim \mathbb{R}$. Каждому треугольнику поставим в соответствие набор координат его вершин. Чтобы это соответствие было функциональным, зафиксируем порядок перечисления вершин. (Можно, скажем, перечислять вершины по возрастанию в смысле *лексикографического* линейного порядка $<_L$, т. ч.

$(x,y) <_L (x',y') \iff x < x'$ или $(x = x'$ и $y < y')$.) Ясно, что для разных треугольников такие наборы — элементы множества $(\mathbb{R}^2)^3$ — будут различны. Итак, $T \lesssim (\mathbb{R}^2)^3 \sim \mathbb{R}^3 = \mathbb{R}^2 \times \mathbb{R} \sim \mathbb{R} \times \mathbb{R} \sim \mathbb{R}$.

Вложение $\mathbb{R} \lesssim T$ легко получить, например, рассмотрев треугольники с вершинами $(-1,0),(1,0),(x,1)$ при всевозможных $x \in \mathbb{R}$.

Характеристические функции часто позволяют заменить рассуждения об операциях над множествами арифметическими вычислениями.

Упражнение 2.1.12. Докажите, что для любых $B, C \in \mathcal{P}(A)$ и $x \in A$ имеют место:

$$\begin{aligned} \chi_{B\cap C}(x) &= \chi_B(x) \cdot \chi_C(x); \\ \chi_{B\cup C}(x) &= \chi_B(x) + \chi_C(x) - \chi_B(x) \cdot \chi_C(x); \\ \chi_{\bar{B}}(x) &= 1 - \chi_B(x), \end{aligned}$$

а $B \subseteq C$ равносильно тому, что $\chi_B(x) \leqslant \chi_C(x)$ для всех $x \in A$.

Пример 2.1.13. Как мы видели, $\chi_B = \chi_C$ равносильно $B = C$. Поэтому с помощью характеристических функций можно, положив, например, $A = B \cup C$, доказывать тождества вроде $\bar{B} \cap \bar{C} = \overline{B \cup C}$. Действительно, для любого $x \in A$ имеем

$$\begin{aligned} \chi_{\bar{B}\cap\bar{C}}(x) = (1 - \chi_B(x))(1 - \chi_C(x)) = \\ = 1 - (\chi_B(x) + \chi_C(x) - \chi_B(x)\chi_C(x)) = \chi_{\overline{B\cup C}}(x). \end{aligned}$$

Пример 2.1.14. Докажем, что из $B \cap C = B \cup C$ следует $B = C$. Из условия для всех $x \in A$ получаем

$$\begin{aligned} 0 = \chi_{B\cup C}(x) - \chi_{B\cap C}(x) = \chi_B(x) + \chi_C(x) - 2\chi_B(x)\chi_C(x) = \\ = \chi_B^2(x) + \chi_C^2(x) - 2\chi_B(x)\chi_C(x) = (\chi_B(x) - \chi_C(x))^2. \end{aligned}$$

Отсюда $\chi_B(x) = \chi_C(x)$ для всех $x \in A$, а значит, $B = C$.

Конечные последовательности и наборы. Ранее мы для произвольного множества A и каждого $n \in \mathbb{N}$ определили множество A^n наборов длины n из элементов A. На такие наборы можно также посмотреть как на функции $\underline{n} \to A$. Между двумя этими интерпретациями имеется естественное биективное соответствие, которое имеют в виду, когда свободно и без пояснений переходят от одной интерпретации к другой.

Содержательно, каждой функции $f\colon \underline{n} \to A$ ставится в соответствие набор $(f(0), f(1), \ldots, f(n-1)) \in A^n$ или, с другой стороны, набору $(a_0, a_1, \ldots, a_{n-1})$ ставится в соответствие функция $k \mapsto a_k$ из $\underline{n}$ в A. Однако аккуратное воплощение этих идей использует индукцию. Как нетрудно понять, главной трудностью для аккуратного изложения является определение набора $(f(0), f(1), \ldots, f(n-1))$ (или функции $k \mapsto a_k$) с помощью «основных способов задания множеств».

Лемма 2.1.15. *Для произвольных $n \in \mathbb{N}$ и множества A верно $A^n \sim \sim A^{\underline{n}}$.*

Доказательство. Индукция по $n \in \mathbb{N}$. В силу определения, $A^0 = \{\varnothing\}$. С другой стороны, $A^{\underline{0}} = A^{\varnothing}$ есть множество функций $\varnothing \to A$. Согласно примеру 1.4.11, единственная такая функция — множество $\varnothing$. Значит, $A^{\underline{0}} = A^{\varnothing} = \{\varnothing\} = A^0$ и тем более $A^0 \sim A^{\underline{0}}$. Основание индукции проверено.

Допустим, что $A^n \overset{\varphi}{\sim} A^{\underline{n}}$. По определению $A^1 = A$ и, согласно замечанию 1.2.57, $A^{n+1} = A^n \times A$ при $n \geqslant 1$. Очевидно, что $A \sim \sim \{\varnothing\} \times A = A^0 \times A$. Следовательно, $A^{n+1} \sim A^n \times A$ при любом $n \in \mathbb{N}$. Определим отображение $\psi\colon A^n \times A \to A^{\underline{n+1}}$ следующим образом:

$$\psi(\alpha, x) = \varphi(\alpha) \cup \{(n, x)\}$$

для всех $\alpha \in A^n$ и $x \in A$. По предположению индукции, $\varphi(\alpha)\colon \underline{n} \to A$. Учитывая $\underline{n+1} = \underline{n} \cup \{n\}$ и $n \notin \underline{n}$, видим, что $\psi(\alpha, x)$, действительно, есть функция $\underline{n+1} \to A$.

Пусть $\psi(\alpha, x) = \psi(\beta, y)$, т. е. $\varphi(\alpha) \cup \{(n, x)\} = \varphi(\beta) \cup \{(n, y)\}$. Имеем $(n, x) \notin \varphi(\beta)$, откуда $(n, x) = (n, y)$ и $x = y$. Если $(k, z) \in \varphi(\alpha)$, то $k \neq n$, а значит, $(k, z) \in \varphi(\beta)$, т. е. $\varphi(\alpha) \subseteq \varphi(\beta)$. Аналогично получаем противоположное включение и $\varphi(\alpha) = \varphi(\beta)$, откуда $\alpha = \beta$ в силу инъективности φ. Итак, $(\alpha, x) = (\beta, x)$, а значит, отображение ψ инъективно.

Допустим, $f\colon \underline{n+1} \to A$. Очевидно, $f = g \cup \{(n, f(n))\}$, где $g = f \restriction \underline{n}$ и $f(n) \in A$. Поскольку $g\colon \underline{n} \to A$ и φ — сюръекция, найдется некоторый $\alpha \in A^n$, т. ч. $\varphi(\alpha) = g$. Тогда $\psi(\alpha, f(n)) = \varphi(\alpha) \cup \{(n, f(n))\} = f$. Итак, ψ сюръективно, а значит, является биекцией.

Итак, $A^{n+1} \sim A^n \times A \overset{\psi}{\sim} A^{\underline{n+1}}$, откуда $A^{n+1} \sim A^{\underline{n+1}}$. Индукционный переход проверен. По принципу математической индукции заключаем, что $A^n \sim A^{\underline{n}}$ при всех $n \in \mathbb{N}$. $\square$

Замечание 2.1.16. Мы, в частности, получили, что $A^1 = A \sim A^{\underline{1}} = A^{\{\varnothing\}}$. С другой стороны, $\{\varnothing\} = B^0$ для любого B. Согласно замечанию 1.4.14, мы называли функцию $B^n \to A$ при $n \geqslant 1$ функцией n аргументов. Логично тогда всякую функцию $f\colon B^0 \to A$ называть *функцией нуля аргументов*.

Очевидно, $f \subseteq \{\varnothing\} \times A$ для такой функции, а значит, $f = \{(\varnothing, x)\}$, где $x \in A$. Естественно отождествить всякую такую f с соответствующим элементом $x \in A$, что мы, собственно, и сделали, констатировав $A \sim A^{B^0}$.

Функции $B^0 \to A$ обычно называют *константами* и рутинным образом отождествляют с элементами множества A. Как видит читатель, выбор множества B здесь не играет никакой роли.

Принцип Дирихле и мощность конечного множества. Мы принимаем как известное, что $0 \neq 1$, поэтому $\underline{2} = \{0, 1\} \neq \{0\} = \underline{1}$. Но, быть может, $\underline{2} \sim \underline{1}$? В таком случае наше понятие конечного множества отнюдь не выражало бы интуицию «конечного числа элементов», ведь $2 \neq 1$!

По счастью, здесь все просто: если $\{0, 1\} \overset{\varphi}{\twoheadrightarrow} \{0\}$, то $\varphi(0) = 0 = \varphi(1)$ и, в силу инъективности, $0 = 1$, что не так. А что если $\underline{n} \sim \underline{m}$ для некоторых других неравных чисел n и m? Чтобы исключить такой случай, нам понадобится индукция.

Лемма 2.1.17. *Для каждого $n \in \mathbb{N}$, если $f\colon \underline{n+1} \to \underline{n}$, то f не инъекция.*

Доказательство. Предположим противное: пусть найдется $n \in \mathbb{N}$, для которого есть инъекция $f\colon \underline{n+1} \to \underline{n}$. Согласно принципу наименьшего числа, рассмотрим *наименьшее* такое n. Инъекция (и вообще, функция) $f\colon \underline{1} \to \underline{0}$ невозможна, потому что $f(0) \notin \underline{0}$. Значит, $n \neq 0$, т. е. $n = m + 1$ для некоторого $m \in \mathbb{N}$.

Пусть $f(n) = x \in \underline{n}$. Рассмотрим функцию $g\colon \underline{n} \to \underline{n}$, меняющую m и x местами. Точнее,

$$g(k) \quad = \quad \begin{cases} m, & \text{если } k = x; \\ x, & \text{если } k = m; \\ k & \text{иначе.} \end{cases}$$

Ясно, что g — инъекция и даже биекция. Функция $f \restriction \underline{n}\colon \underline{n} \to \underline{n}$, как показывает лемма 1.4.25, также является инъекцией. Значит, и $h = g \circ (f \restriction \underline{n})$ есть инъекция $\underline{n} \to \underline{n}$.

Если $h(k) = m$, то $(f \restriction \underline{n})(k) = x$. Но тогда $f(n) = x = f(k)$, хотя $n \neq k \in \underline{n}$. Это противоречит инъективности функции f. Выходит, h не принимает значения m и $\operatorname{rng} h \subseteq \underline{m}$. Тогда h есть инъекция $\underline{m+1} \to \underline{m}$. Однако такой инъекции нет, поскольку $m < n$, а число n наименьшее возможное. Противоречие. □

Теорема 2.1.18 (Принцип Дирихле)**.** *Если $m > n$ и $f\colon \underline{m} \to \underline{n}$, то f не инъекция (т. е. $\underline{m} \not\lesssim \underline{n}$).*

Доказательство. Допустим, инъекция $f\colon \underline{m} \to \underline{n}$ существует. Так как $m > n$, имеем $m \geqslant n + 1$, откуда $\underline{n+1} \subseteq \underline{m}$. Следовательно, функция $f \restriction \underline{n+1}\colon \underline{n+1} \to \underline{n}$ также является инъекцией, что невозможно. □

Неформально принцип Дирихле нередко представляют так:

> Если $m > n$, невозможно разложить m различных предметов по n различным ящикам так, чтобы в каждый ящик попало не более одного предмета.

Очевидно, такая формулировка сводится к нашей, если занумеровать предметы и ящики элементами множеств $\underline{m}$ и $\underline{n}$ соответственно, а затем рассмотреть функции, назначающие номеру предмета номер вмещающего его ящика.

Следствие 2.1.19. *Если $m \neq n$, то $\underline{m} \nsim \underline{n}$.*

Доказательство. Если $m \neq n$, то $m > n$ или $m < n$. В первом случае, по принципу Дирихле, невозможно $\underline{m} \lesssim \underline{n}$, а во втором — невозможно $\underline{n} \lesssim \underline{m}$. В каждом из случаев исключается $\underline{m} \sim \underline{n}$. □

Следствие 2.1.20. *Для каждого конечного множества A существует единственное $n \in \mathbb{N}$, т. ч. $A \sim \underline{n}$.*

Число n, т. ч. $A \sim \underline{n}$, называется *мощностью* конечного множества A. Мощность конечного множества A обозначим символом $|A|$. Очевидно, конечные A и B равномощны тогда и только тогда, когда их мощности равны.

Пример 2.1.21. Множество $\mathbb{N}$ бесконечно. В противном случае $\mathbb{N} \sim \underline{n}$ для некоторого $n \in \mathbb{N}$. Однако $\underline{n+1} \subseteq \mathbb{N}$ и тем более $\underline{n+1} \lesssim \mathbb{N}$. Тогда $\underline{n+1} \lesssim \underline{n}$, что невозможно по принципу Дирихле.

Лемма 2.1.22. *Пусть множества A и B конечны, причем $A \sim B$. Тогда для любой функции $f\colon A \to B$ верно: f инъективна тогда и только тогда, когда f сюръективна.*

Доказательство. Допустим $B \overset{\psi}{\sim} \underline{n} \overset{\varphi}{\sim} A$ и $f\colon A \to B$ — инъекция, но не сюръекция. Сразу отметим, что $n \neq 0$ (иначе функция $f = A = B = \varnothing$ является биекцией), а значит, $n = m + 1$ для некоторого $m \in \mathbb{N}$.

Согласно лемме 1.4.4, функция $f' = \psi \circ f \circ \varphi$ есть инъекция $\underline{n} \to \underline{n}$. Если f' является сюръекцией, то $f = \psi^{-1} \circ f' \circ \varphi^{-1}$ — также сюръекция, что неверно. Значит, f' не сюръекция, и существует $x < n$, т. ч. $x \notin \operatorname{rng} f'$. Как и в доказательстве леммы 2.1.17, рассмотрим биекцию $g\colon \underline{n} \to \underline{n}$, меняющую x и m местами. Функция $h = g \circ f'$ является инъекцией $\underline{n} \to \underline{n}$, причем $m \notin \operatorname{rng} h$. Следовательно, имеем инъекцию $h\colon \underline{m+1} \to \underline{m}$, что невозможно по принципу Дирихле. Противоречие.

Обратно, допустим теперь, что $f\colon A \to B$ — сюръекция. Согласно лемме 1.5.28, существует функция $g\colon B \to A$, т. ч. $f \circ g = \mathrm{id}_B$. Ясно, что g — инъекция, так как $g(x) = g(y)$ влечет $x = f(g(x)) = f(g(y)) = y$. По уже доказанному утверждению, g будет и сюръекцией, т. е. биекцией. В силу леммы 1.5.4 и теоремы 1.5.6, для биекции g^{-1} получаем $g^{-1} = \mathrm{id}_B \circ g^{-1} = (f \circ g) \circ g^{-1} = f \circ (g \circ g^{-1}) = f \circ \mathrm{id}_A = f$. Тогда f — тоже биекция, а значит, инъекция. □

Замечание 2.1.23. В доказательстве мы сослались на лемму 1.5.28, использующую аксиому выбора. Однако, поскольку речь здесь идет лишь о конечных множествах, то, в свете замечания 1.5.35, аксиому выбора можно заменить принципом индукции. Более того, правая обратная функция g к сюръекции $f\colon \underline{a} \to \underline{b}$ строится совсем просто: достаточно положить $g(k)$ равным *наименьшему* такому $l \in \underline{a}$, что $f(l) = k$. Индукция в форме принципа наименьшего числа обеспечивает тотальность g. Это легко переносится на произвольные конечные множества.

Упражнение 2.1.24. Докажите принцип, двойственный принципу Дирихле: если $m < n$ и $f\colon \underline{m} \to \underline{n}$, то f не сюръекция.

Упражнение 2.1.25. Индукцией по $n = |A|$ докажите «аксиому конечного выбора»:

> Для всякого конечного множества A, т. ч. $\varnothing \notin A$, существует функция выбора.

Упражнение 2.1.26. Докажите, что если функция $f\colon \underline{n} \to \underline{n}$ сюръективна, то она инъективна, непосредственно применяя принцип индукции. (Аналогично доказательству леммы 2.1.17 можно построить сюръекцию $h\colon \underline{n} \to \underline{n}$, т. ч. $h(n-1) = n-1$.)

Лемма 2.1.22 имеет изящные применения в математике конечных множеств. Рассмотрим одно из них.

Пример 2.1.27. Числа $m, n \in \mathbb{Z}$ *взаимно простые*, если из $k \,|\, m$, $k \,|\, n$ и $k \in \mathbb{N}$ следует, что $k = 1$. Например, таковы 12 и 35, но не 12 и 15. Пусть числа $m_1, \ldots, m_n \in \mathbb{N}_+$ попарно взаимно просты и $a_i \in \underline{m_i}$. Тогда существует единственное число $x \in \underline{M}$, где $M = m_1 \cdot \ldots \cdot m_n$, т. ч.

$$x \equiv_{m_1} a_1, \ \ldots, \ x \equiv_{m_n} a_n.$$

Таким образом, для любого набора остатков по заданным взаимно простым модулям есть число, дающее именно такие остатки. Это утверждение известно как *китайская теорема об остатках*.

Очевидно, $|\underline{M}| = M$. С другой стороны, если $X = \{(a_1, \ldots, a_n) \mid \mid\ a_i \in \underline{m_i}\}$, то $|X| = m_1 \cdot \ldots \cdot m_n = M$ (это понятно интуитивно; в следующем разделе мы дадим пояснения). Итак, $\underline{M} \sim X$.

Рассмотрим функцию $f\colon \underline{M} \to X$, т. ч. $f(x) = (x_1, \ldots, x_n)$, где x_i есть остаток от деления x на m_i. Если $f(x) = f(y)$, то $x_i = y_i$, а значит, $x \equiv_{m_i} y$, т. е. $m_i \,|(x-y)$ для всех i. Из взаимной простоты m_i нетрудно тогда получить $M \,|(x-y)$, т. е. $x = y + kM$ для $k \in \mathbb{Z}$. Поскольку $x, y \in \underline{M}$, имеем $k = 0$ и $x = y$. Значит, f — инъекция.

В силу леммы 2.1.22, функция f сюръективна. Следовательно, для каждого $(a_1, \ldots, a_n) \in X$ найдется $x \in \underline{M}$, т. ч. $f(x) = (a_1, \ldots, a_n)$. Это равносильно требуемому условию $x \equiv_{m_1} a_1, \ \ldots, \ x \equiv_{m_n} a_n$. Единственность x тогда следует из инъективности f.

Рекурсия. Читателю, вероятно, знакомы определения функций натуральных чисел «по рекурсии», когда «следующее» значение определяется «предыдущими». Например, функция $f\colon \mathbb{N} \to \mathbb{N}$ *факториал* задается условиями

$$f(0) = 1 \quad \text{и} \quad f(n+1) = (n+1) \cdot f(n)$$

при всех $n \in \mathbb{N}$. Однако почему функция, удовлетворяющая таким условиям, существует? И даже если существует, почему единственна? Какую из подходящих объявить факториалом?

Пример 2.1.28. Ни одна функция $f\colon \mathbb{N} \to \mathbb{N}$ не удовлетворяет условию

$$\forall n \in \mathbb{N}\ f(n) = 1 + f(n+1).$$

Действительно, иначе $f(n+1) < f(n)$ при всех $n \in \mathbb{N}$, и непустое множество $f[\mathbb{N}] \subseteq \mathbb{N}$ не имеет наименьшего элемента. С другой стороны, условию

$$\forall n \in \mathbb{N}\ f(n) = (f(n+1))^2$$

удовлетворяют функции $n \mapsto 0$ и $n \mapsto 1$ (и, как легко проверить, никакие другие).

Если попытаться переписать определение факториала в духе известных нам способов задания множеств, может получиться следующее:

$$f = \{(x, y) \in \mathbb{N}^2 \mid (x = 0 \text{ и } y = 1) \text{ или } (x > 0 \text{ и } y = x \cdot f(x-1))\}.$$

Как видим, свойство, выделяющее подмножество $f \subseteq \mathbb{N}^2$, явным образом использует само f. Возникающий здесь «порочный круг» препятствует нам счесть такое свойство «точно определенным» (что мы требовали). Покажем, как преодолеть эту трудность.

Теорема 2.1.29 (о рекурсии)**.** *Пусть U — некоторое множество, $u_0 \in U$ и $h\colon U \to U$. Тогда существует единственная функция $f\colon \mathbb{N} \to U$, т. ч.*

$$f(0) = u_0 \quad \text{и} \quad f(n+1) = h(f(n))$$

при всех $n \in \mathbb{N}$.

Доказательство. Рассмотрим множество

$$F = \{g \in \mathcal{P}(\mathbb{N} \times U) \mid \exists m \in \mathbb{N},\ \text{т. ч. } g\colon \underline{m} \to U \text{ и}$$
$$\forall k \left((0 \in \underline{m} \Longrightarrow g(0) = u_0) \text{ и } (k+1 \in \underline{m} \Longrightarrow g(k+1) = h(g(k)))\right)\}.$$

Иначе говоря, F состоит из всевозможных функций $\underline{m} \to U$, удовлетворяющим условиям для f на своей области определения. Как окажется, это будут, в точности, «начальные куски» $f \restriction \underline{m}$ функции f.

Пусть $g_1, g_2 \in F$, причем $g_1\colon \underline{m_1} \to U$ и $g_2\colon \underline{m_2} \to U$. Не ограничивая общности, считаем, что $m_1 \leqslant m_2$. Тогда $g_1(l) = g_2(l)$ при всех $k \in \underline{m_1}$ (т. е. $g_1 = g_2 \restriction \underline{m_1}$). В самом деле, иначе можно выбрать *наименьшее* такое $l \in \underline{m_1}$, что $g_1(l) \neq g_2(l)$. Случай $l = 0$ невозможен, ибо $g_1(0) = u_0 = g_2(0)$. Значит, $l = k+1$. Но и тогда $g_1(k+1) = h(g_1(k)) = h(g_2(k)) = g_2(k+1)$ в силу $g_1(k) = g_2(k)$. Противоречие.

Положим $f = \cup F$. Очевидно, $f \subseteq \mathbb{N} \times U$. Проверим функциональность отношения f. Пусть $(n, u_1), (n, u_2) \in f$. Тогда найдутся $g_1, g_2 \in$ $\in F$, где $g_1 \colon \underline{m_1} \to U$ и $g_2 \colon \underline{m_2} \to U$, т. ч. $(n, u_1) \in g_1$ и $(n, u_2) \in g_2$. Имеем $n \in \underline{m_1} \cap \underline{m_2}$, откуда, по доказанному, $u_1 = g_1(n) = g_2(n) = u_2$.

Теперь проверим тотальность f. Предположим противное и возьмем *наименьшее* $n \in \mathbb{N}$, т. ч. $(n, u) \notin f$ при всех $u \in U$. Случай $n = 0$ невозможен, поскольку для функции $g_1 \colon \underline{1} \to U$, т. ч. $g_1(0) = u_0$, имеем $(0, u_0) \in g_1 \in F$. Значит, $n = m + 1$. Однако, для $m < n$ найдется некоторое $u \in U$, т. ч. $(m, u) \in F$. Тогда найдется и функция $g \in F$, для которой $\underline{m+1} \subseteq \operatorname{dom} g$ и $g(m) = u$. Легко видеть, что $g \restriction \underline{m+1} \in F$. Если положить

$$g' = (g \restriction \underline{m+1}) \cup \{(m+1, h(g(m)))\},$$

также будем иметь $g' \in F$. Тем самым, $(n, h(g(m))) \in \cup F = f$, что противоречит предположению.

Наконец, проверим, что f удовлетворяет условиям теоремы. Вновь предполагая противное, выбираем *наименьшее* $n \in \mathbb{N}$, где условия нарушаются. Но тогда функция $f \restriction \underline{n}$ удовлетворяет условиям на своей области определения, а значит, $f \restriction \underline{n} \in F$. Если $n = m + 1$, то $f(n) \neq h(f(m))$, но для функции

$$f' = (f \restriction \underline{n}) \cup \{(m+1, h(f(m)))\}$$

имеем $f' \in F$, откуда $(n, h(f(m))) \in f$. Это противоречит функциональности f. Случай $n = 0$ аналогичен.

Итак, функция f, удовлетворяющая условию теоремы, построена. Если f_1 и f_2 суть любые такие функции, то $f_1 \restriction \underline{n}, f_2 \restriction \underline{n} \in F$ и, по доказанному, $f_1 \restriction \underline{n} = f_2 \restriction \underline{n}$ для всех $n \in \mathbb{N}$. Отсюда $f_1 = f_2$. Значит, искомая функция f единственна. □

Пример 2.1.30. Существует и единственна функция $f \colon \mathbb{N} \to \mathbb{N}$, т. ч. $f(0) = 1$ и $f(n+1) = 2f(n)$ при всех $n \in \mathbb{N}$. Очевидно, $f(n) = 2^n$.

Различные виды рекурсии. Обоснованная нами форма рекурсии мало подходит для практического применения, поскольку, во-первых, функция h использует лишь значение $f(n)$, но «не имеет доступа» даже к самому числу n (как требует определение факториала)[5], а во-вторых, желательно позволить функции f иметь еще аргументы

[5]Такая рекурсия имеет преимущества в алгоритмической реализации (легко преобразуясь в т. н. «хвостовую» рекурсию).

помимо $n \in \mathbb{N}$. Тем не менее некоторые более сложные формы рекурсии могут быть сведены к рассмотренной за счет подходящего выбора множества U.

Следствие 2.1.31. *Пусть U есть некоторое множество, $u_0 \in U$ и $h\colon \mathbb{N} \times U \to U$. Тогда существует единственная функция $f\colon \mathbb{N} \to U$, т. ч.*

$$f(0) = u_0 \quad \text{и} \quad f(n+1) = h(n, f(n))$$

при всех $n \in \mathbb{N}$.

Доказательство. Рассмотрим множество $W = \mathbb{N} \times U$, положим $w_0 = (0, u_0) \in W$ и определим функцию $h'\colon W \to W$ так, что $h'(n,u) = (n+1, h(n,u))$ для всех $(n,u) \in W$. (Формально, удобно использовать функции-проекторы π_i, извлекающие компоненты пары, которые были введены в доказательстве теоремы 1.5.11. Тогда получится $h'(w) = (\pi_1(w) + 1, h(\pi_1(w), \pi_2(w)))$ для всех $w \in W$.)

По теореме о рекурсии, существует функция $f'\colon \mathbb{N} \to W$, для которой $f'(0) = w_0$ и $f'(n+1) = h'(f'(n))$ при всех $n \in \mathbb{N}$. Индукцией легко проверить, что $\pi_1(f'(n)) = n$ для всех $n \in \mathbb{N}$.

Положим $f = \pi_2 \circ f'$. Имеем $f(0) = \pi_2(f'(0)) = \pi_2(0, u_0) = u_0$ и, далее,

$$f(n+1) = \pi_2(f'(n+1)) = \pi_2(h'(f'(n))) = \\ = h(\pi_1(f'(n)), \pi_2(f'(n))) = h(n, f(n))$$

при всяком $n \in \mathbb{N}$. Итак, требуемая функция f существует. Ее единственность проверяется непосредственно: если $f_1 \neq f_2$ суть две подходящие функции, возьмем *наименьшее* n, т. ч. $f_1(n) \neq f_2(n)$. Поскольку $f_1(0) = u_0 = f_2(0)$, необходимо $n = m + 1$. Но $f_1(m) = f_2(m)$, а значит, $f_1(m+1) = h(m, f_1(m)) = h(m, f_2(m)) = f_2(m+1)$. Противоречие. $\square$

Пример 2.1.32. Существует и единственна функция «факториал», удовлетворяющая вышеприведенным условиям. Для произвольной функции $g\colon \mathbb{N} \to \mathbb{N}$ существует функция $f\colon \mathbb{N} \to \mathbb{N}$, однозначно определяемая условиями $f(0) = g(0)$ и $f(n+1) = f(n) + g(n+1)$ при всех $n \in \mathbb{N}$. В таком случае обычно пишут $f(n) = \sum_{k=0}^{n} g(k)$.

Следствие 2.1.33 (примитивная рекурсия)**.** *Пусть U и V — некоторые множества, $g\colon V \to U$ и $h\colon \mathbb{N} \times V \times U \to U$. Тогда существует единственная функция $f\colon \mathbb{N} \times V \to U$, т. ч.*

$$f(0, v) = g(v) \quad \text{и} \quad f(n+1, v) = h(n, v, f(n, v))$$

при всех $v \in V$ *и* $n \in \mathbb{N}$.

Доказательство. Рассмотрим множество $W = U^V$, положим $w_0 = g \in W$ и определим функцию $h' \colon \mathbb{N} \times W \to W$ так, что

$$(h'(n, \xi))(v) = h(n, v, \xi(v))$$

для всех $n \in \mathbb{N}$, $\xi \in W$ и $v \in V$. Согласно предыдущему следствию, существует функция $f' \colon \mathbb{N} \to W$, т. ч. $f'(0) = w_0$ и $f'(n+1) = h'(n, f'(n))$ при всех $n \in \mathbb{N}$. Определим функцию $f \colon \mathbb{N} \to W$ равенством[6]

$$f(n, v) = (f'(n))(v).$$

Тогда, очевидно, $f(0, v) = (f'(0))(v) = g(v)$ и

$$f(n+1, v) = (f'(n+1))(v) = (h'(n, f'(n)))(v) = \\ = h(n, v, (f'(n))(v)) = h(n, v, f(n, v))$$

при всех $n \in \mathbb{N}$ и $v \in V$. Требуемая функция построена. Допустим теперь, что условиям удовлетворяют функции $f_1 \neq f_2$. Возьмем *наименьшее* n, т. ч. $f_1(n, v) \neq f_2(n, v)$ для какого-либо $v \in V$. Если $n = 0$, то $f_1(0, v) = g(v) = f_2(0, v)$, что невозможно. Если же $n = m + 1$, то $f_1(m+1, v) = h(m, v, f_1(m, v)) = h(m, v, f_2(m, v)) = f_2(m+1, v)$, поскольку $f_1(m, v) = f_2(m, v)$. Противоречие показывает, что построенная нами f единственная подходящая. □

Пример 2.1.34. Существует и единственна функция $f \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, т. ч. $f(0, m) = m$ и $f(n+1, m) = f(n, m)+1$ при всех $n, m \in \mathbb{N}$. Ясно, что сложение удовлетворяет этим свойствам, а значит, $f(n, m) = n + m$.

Как видит читатель, рекурсия позволяет нам строго *определить* сложение натуральных чисел, коль скоро уже определена функция «последователь» $n \mapsto n + 1$. Это весьма полезно при формальном построении математики.

Тут же можно отметить *алгоритмический* аспект рекурсии: если некий «исполнитель» умеет вычислять по натуральному числу следующее и предыдущее, рекурсивное определение, по существу, дает такому исполнителю *программу* для вычисления суммы натуральных чисел. С помощью суммы можно программировать уже более сложные функции.

[6] Для педантов:

$$f = \{\alpha \in \mathbb{N} \times V \times U \mid \exists n \exists v \exists u \exists z \ (\alpha = (n, v, u) \text{ и } (n, z) \in f' \text{ и } (v, u) \in z)\}.$$

Упражнение 2.1.35. Предполагая, что определены функции $n \mapsto 0$ и $(n, m) \mapsto n + m$, дайте рекурсивное определение умножения натуральных чисел.

Во всех рассмотренных случаях значение $f(n+1)$ определялось с использованием лишь одного значения $f(n)$ функции f. Однако нередко желательно использовать несколько предыдущих значений. Вспомним, скажем, последовательность *чисел Фибоначчи* с условием $\varphi_{n+2} = \varphi_{n+1} + \varphi_n$.

Мы рассмотрим весьма общий случай, когда для каждого конкретного $v \in V$ значение $f(n+1, v)$ определяется с использованием всего уже построенного «куска» $f \restriction (\underline{n+1} \times \{v\}) \subseteq \mathbb{N} \times V \times U$ функции f (в частности, любых значений $f(m, v)$, где $m \leqslant n$, а v фиксировано).

Следствие 2.1.36 (возвратная рекурсия)**.** *Пусть U и V — некоторые множества, $g\colon V \to U$ и $h\colon \mathbb{N} \times V \times \mathcal{P}(\mathbb{N} \times V \times U) \to U$. Тогда существует единственная функция $f\colon \mathbb{N} \times V \to U$, т. ч.*

$$f(0, v) = g(v) \quad \text{и} \quad f(n+1, v) = h(n, v, f \restriction (\underline{n+1} \times \{v\}))$$

при всех $v \in V$ и $n \in \mathbb{N}$.

Доказательство. Рассмотрим множество $W = \mathcal{P}(\mathbb{N} \times V \times U)$, а также функции $g'\colon V \to W$ и $h'\colon \mathbb{N} \times V \times W \to W$, т. ч.

$$g'(v) = \{((0, v), g(v))\} \quad \text{и}$$

$$h'(n, v, \xi) = \xi \cup \{((n+1, v), h(n, v, \xi))\}$$

при всех $n \in \mathbb{N}$, $v \in V$, $\xi \in W$. Согласно предыдущему следствию, существует функция $f'\colon \mathbb{N} \times V \to W$, т. ч. $f'(0, v) = g'(v)$ и $f'(n+1, v) = h'(n, v, f'(n, v))$.

Индукцией по $n \in \mathbb{N}$ докажем, что $f'(n, v)\colon \underline{n+1} \times \{v\} \to U$ при всех $v \in V$. Понятно, что $f'(0, v) = g'(v)\colon \{(0, v)\} \to U$. Далее,

$$f'(n+1, v) = f'(n, v) \cup \{((n+1, v), h(n, v, f'(n, v)))\}.$$

Имеем $h(n, v, f'(n, v))) \in U$ и, по предположению индукции, для любого $v \in V$ имеем $f'(n, v)\colon \underline{n+1} \times \{v\} \to U$. Отсюда получаем, что $f'(n+1, v)\colon \underline{n+2} \times \{v\} \to U$. Основание и шаг индукции обоснованы.

Также легко видеть, что $(f'(n+1, v))(m, v) = (f'(n, v))(m, v)$ при всех $m \leqslant n$. Значит,

$$\begin{aligned}(f'(m, v))(m, v) &= (f'(m+1, v))(m, v) = \\ &= (f'(m+2, v))(m, v) = \ldots = (f'(m+k, v))(m, v).\end{aligned}$$

Индукцией по k легко показать, что $(f'(m,v))(m,v) = (f'(n,v))(m,v)$, если $m \leqslant n$.

Теперь положим $f(n,v) = (f'(n,v))(n,v) \in U$ при всех $n \in \mathbb{N}$ и всех $v \in V$. Имеем тогда

$$\begin{aligned} f \restriction (\underline{n+1} \times \{v\}) = \\ = \{\big((m,v), f(m,v)\big) \mid m \leqslant n\} = \{\big((m,v), (f'(m,v))(m,v)\big) \mid m \leqslant n\} = \\ = \{\big((m,v), (f'(n,v))(m,v)\big) \mid m \leqslant n\} = f'(n,v). \end{aligned}$$

Остается убедиться, что функция f удовлетворяет условиям нашего утверждения. Получаем $f(0,v) = (g'(v))(0,v) = g(v)$ и

$$\begin{aligned} f(n+1,v) = (f'(n+1,v))(n+1,v) = \\ = h(n,v,f'(n,v)) = h(n,v,f \restriction (\underline{n+1} \times \{v\})). \end{aligned}$$

Итак, функция f построена. Проверим единственность. Пусть имеются подходящие функции $f_1 \neq f_2$, и $n \in \mathbb{N}$ есть *наименьшее* число, т. ч. $f_1(n,v) \neq f_2(n,v)$ при некотором v. Тривиальным образом, $n \neq 0$. Пусть $n = m+1$. Тогда для всех $k \leqslant m$ и для всех $v \in V$ имеем $f_1(k,v) = f_2(k,v)$. Но это значит, что $f_1 \restriction (\underline{m+1} \times \{v\}) = f_2 \restriction (\underline{m+1} \times \times \{v\})$ при всех $v \in V$. Из условия на функции f_1 и f_2 видно, что $f_1(m+1,v) = f_2(m+1,v)$. Противоречие. $\square$

Пример 2.1.37. Существует и единственна функция $f\colon \mathbb{N} \to \mathbb{N}$, определенная условиями $f(0) = 0$, $f(1) = 1$ и $f(n+2) = f(n+1) + f(n)$ при всех $n \in \mathbb{N}$ (*числа Фибоначчи*).

Действительно, используем возвратную рекурсию, полагая $U = \mathbb{N}$ и $V = \{\varnothing\}$. Для простоты, мы будем вовсе игнорировать аргумент v (см. замечание 2.1.16). Применим рекурсию к функции $g = 0$ и функции $h\colon \mathbb{N} \times \mathcal{P}(\mathbb{N}^2) \to \mathbb{N}$, т. ч.

$$h(n,\xi) \quad = \quad \begin{cases} \xi(n) + \xi(n-1), & \text{если } n > 0 \text{ и } \xi\colon \underline{n+1} \to \mathbb{N}, \\ 1 & \text{иначе.} \end{cases}$$

Получится функция $f\colon \mathbb{N} \to \mathbb{N}$, т. ч. $f(0) = g = 0$, $f(1) = h(0, f \restriction \underline{1}) = 1$ и $f(n+2) = h(n+1, f \restriction \underline{n+2}) = (f \restriction \underline{n+2})(n+1) + (f \restriction \underline{n+2})(n) = f(n+1) + f(n)$.

Можно также использовать не два предыдущих значения, а все: существует и единственна функция $f\colon \mathbb{N} \to \mathbb{N}$, т. ч. $f(0) = 1$ и $f(n+1) = \sum_{k=0}^{n} (f(k))^n$.

Упражнение 2.1.38. Докажите следующую теорему о *совместной рекурсии*.

> Пусть U_i и V суть некоторые множества, $g_i\colon V \to U_i$ и $h_i\colon \mathbb{N} \times V \times U_1 \times U_2 \to U_i$. Тогда существует единственная пара (f_1, f_2) функций, т. ч. $f_i\colon \mathbb{N} \times V \to U_i$ и
>
> $$f_i(0, v) = g_i(v) \quad \text{и} \quad f_i(n+1, v) = h_i(n, v, f_1(n, v), f_2(n, v))$$
>
> при всех $v \in V$, $n \in \mathbb{N}$, $i \in \{1, 2\}$.

(Рассмотрите $W = U_1 \times U_2$.)

Мы показали, как обосновать существование и единственность рекурсивно определенной функции во многих важных случаях. В дальнейшем мы будем свободно использовать рекурсивные определения без особых пояснений.

Пример 2.1.39. Нетрудно указать способ определения функции, заслуживающий имени «рекурсивного», поскольку новые значения определяются через «предыдущие», но не имеющий очевидного сведения к рассмотренным нами. Например, существует *функция Аккермана* $A\colon \mathbb{N}^2 \to \mathbb{N}$, единственная удовлетворяющая при всех $m, n \in \mathbb{N}$ условиям

$$\begin{aligned} A(0, n) &= n + 1; \\ A(m+1, 0) &= A(m, 1); \\ A(m+1, n+1) &= A(m, A(m+1, n)). \end{aligned}$$

Попробуйте это доказать.

Аксиомы подстановки. В замечании 1.2.57 мы обратили внимание на то, что $A^{n+1} = A^n \times A$ при всех $n \geqslant 1$. Поскольку у нас *для каждого* натурального числа n было соответствующее определение множества A^n, это утверждение очевидно.

Кажется более естественным дать *одно* определение для всей «совокупности» множеств $A^0, A^1, A^2, \ldots$, проиндексировав ее элементами множества $\mathbb{N}$. Не можем ли мы тогда сказать, что соотношения $A^0 = \{\varnothing\}$, $A^1 = A$ и $A^{n+1} = A^n \times A$ для фиксированного A *определяют* функцию $n \mapsto A^n$, где $n \in \mathbb{N}$?

К сожалению, рассмотренные нами схемы рекурсии не позволяют дать такое определение. Дело в том, что мы строили функции со значениями в некотором *уже определенном* множестве U. В данном же

случае последовательность множеств A^n «растет слишком быстро», чтобы мы могли уместить ее в какое-либо U:

$$A^2 \in \mathcal{P}(\mathcal{P}(\mathcal{P}(A))),\ A^3 \in \mathcal{P}(\mathcal{P}(\mathcal{P}(A^2 \cup A)) \subseteq \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(A)) \cup A))), \ldots$$

Подходящее U можно бы определить «по рекурсии», итерируя «функцию» $X \mapsto \mathcal{P}(X)$, но тут возникает та же проблема.

Введение некоторого нового принципа позволит преодолеть это затруднение. Мы отложим более общее и более аккуратное рассмотрение до последующих частей курса, но уже теперь можем представить основную идею.

Будем рассматривать бинарные «свойства», т. е. осмысленные для пар множеств (например, $x \in y$, $x \sim y$ или $\exists z\ x \cup y \cup z = \mathbb{N}$). Мы не вправе назвать эти «свойства» отношениями, так как нет оснований считать, что подходящие пары образуют множество. Свойство $\varphi(x, y)$ назовем *функциональным*, если для любых множеств x, y, z из $\varphi(x, y)$ и $\varphi(x, z)$ следует $y = z$, и *тотальным*, если для любого x найдется y, т. ч. $\varphi(x, y)$.

Пример 2.1.40. Свойство $x \in y$ тотально, но не функционально, поскольку $x \in \{x\}$ и $x \in \{x, \{x\}\} \neq \{x\}$. Свойство $y \in x$ (пары множеств (x, y)) ни тотально, ни функционально. Свойство $y = \mathcal{P}(x)$ функционально и тотально. Таково же свойство $y = \cup x$.

Упражнение 2.1.41. Исследуйте «инъективность» этих свойств: верно ли, что из $\varphi(x, y)$ и $\varphi(z, y)$ следует $x = z$?

Для каждого бинарного свойства φ *аксиомой подстановки* называется утверждение:

> Если свойство φ функционально, то для любого *множества* X существует *множество* Y, т. ч. при всех y
>
> $$y \in Y \iff \exists x \in X\ \varphi(x, y).$$

Иначе говоря, существует «образ» $\varphi[X] = Y$ множества X под действием «частичной функции» φ. Мы постулируем такую аксиому для каждого свойства φ; совокупность всех этих утверждений называется *схемой аксиом подстановки*.

Замечание 2.1.42. Наши рассуждение приобретут более точный смысл, если отождествить свойства с «формулами» особого искусственного языка, которые могут «выполняться» или «не выполняться» для различных множеств.

Пример 2.1.43. Существуют множества $\{\mathcal{P}(n) \mid n \in \mathbb{N}\}$ и $\{\cup n \mid n \in \in \mathbb{N}\}$. Впрочем, когда нам станет известно определение натуральных чисел как множеств, это обстоятельство можно будет установить без аксиом подстановки.

Упражнение 2.1.44. С помощью аксиомы подстановки докажите, что для любого функционального свойства φ и множества X существует множество

$$\varphi \restriction X = \{(x, y) \mid \varphi(x, y) \text{ и } x \in X\}.$$

Обратно, из этого утверждения выведите схему аксиом подстановки.

Теперь мы можем сделать необходимое обобщение теоремы 2.1.29 о рекурсии.

Теорема 2.1.45. *Пусть бинарное свойство ψ функционально и тотально. Тогда существует и единственно множество f, т. ч. для некоторого множества U верно $f\colon \mathbb{N} \to U$ и $\psi(f \restriction \underline{n}, f(n))$ при всех $n \in \mathbb{N}$.*

Доказательство. Пусть $n \in \mathbb{N}$. Множество α назовем *правильной последовательностью длины n*, если для некоторого V верно $\alpha\colon \underline{n} \to V$ и

$$\forall m \in \underline{n}\ \psi(\alpha \restriction \underline{m}, \alpha(m)).$$

Индукцией по $n \in \mathbb{N}$ докажем, что для каждой длины n существует единственная правильная последовательность. В самом деле, при $n = 0$ и любом V единственной функцией $\underline{0} \to V$ является $\varnothing$. Пусть $\alpha\colon \underline{n} \to V$ — единственная правильная последовательность длины n. В силу тотальности ψ, найдется y, т. ч. $\psi(\alpha, y)$. Положим $V' = V \cup \{y\}$ и $\alpha' = \alpha \cup \{(n, y)\}$. Очевидно, что $\alpha'\colon \underline{n+1} \to V'$, $\alpha' \restriction \underline{m} = \alpha \restriction \underline{m}$ при $m \in \underline{n}$ и $\alpha' \restriction \underline{n} = \alpha$. Поэтому α' есть правильная последовательность длины $n + 1$. Допустим, α'' — другая такая последовательность. Ясно, что $\alpha'' \restriction \underline{n}$ должна быть правильной последовательностью длины n, а значит, $\alpha'' \restriction \underline{n} = \alpha$. Но тогда $\psi(\alpha, \alpha''(n))$. По функциональности ψ, $\alpha''(n) = y = \alpha'(n)$, откуда $\alpha'' = \alpha'$.

Теперь определим свойство φ, полагая

$$\varphi(n, y) \iff n \in \mathbb{N} \text{ и } \exists \alpha \big(\alpha \text{ есть правильная последовательность длины } n+1 \text{ и } \alpha(n) = y\big).$$

Свойство φ функционально, так как иначе для некоторого n существуют две различные правильные последовательности длины $n + 1$.

По аксиоме подстановки, существует множество $\varphi[\mathbb{N}]$, а значит, и множество

$$f = \{(n, y) \in \mathbb{N} \times \varphi[\mathbb{N}] \mid \varphi(n, y)\},$$

очевидно, являющееся частичной функцией $\mathbb{N} \xrightarrow{p} \varphi[\mathbb{N}]$. Ясно, что функция f тотальна, поскольку для каждого $n \in \mathbb{N}$ есть правильная последовательность α длины $n+1$, для которой $\varphi(n, \alpha(n))$. Индукцией по n также легко показать, что $f \restriction \underline{n}$ есть правильная последовательность длины n. Поэтому функция f удовлетворяет условию $\psi(f \restriction \underline{n}, f(n))$ при всех $n \in \mathbb{N}$. С другой стороны, если какая-либо функция $f' \colon \mathbb{N} \to U'$ удовлетворяет этому условию, все $f' \restriction n$ суть правильные последовательности. Из единственности правильной последовательности каждой длины вытекает $f' = f$. $\square$

Пример 2.1.46. Для каждого множества A существуют множество U и функция $f \colon \mathbb{N} \to U$, т. ч. $f(n) = A^n$ при всех $n \in \mathbb{N}$.

В самом деле, пусть свойство $\theta(x, n)$ означает, что $n \in \mathbb{N}$ и найдется множество V, для которого $x \colon \underline{n} \to V$. Тогда положим

$$\begin{aligned}\psi(x, y) \iff {} & (\theta(x, 0) \text{ и } y = \{\varnothing\}) \text{ или } (\theta(x, 1) \text{ и } y = A) \\ & \text{или } \exists n \in \mathbb{N}_{\geqslant 2}\, (\theta(x, n) \text{ и } y = x(n-1) \times A) \\ & \text{или } \forall n \in \mathbb{N}\, (\text{не } \theta(x, n) \text{ и } y = x).\end{aligned}$$

Свойство ψ тотально, так как подходящий y определен как при $x \colon \underline{n} \to \to V$, так и в любом другом случае.

Также это свойство функционально. Прежде заметим, что функционально θ, ибо $\underline{n} = \operatorname{dom} x = \underline{m}$ влечет $n = m$. Если $\theta(x, n)$ неверно при всех натуральных n, то подходящее $y = x$ единственно. Случаи $\theta(x, 0)$ и $\theta(x, 1)$ столь же ясны. Наконец, если $x \colon \underline{n} \to V$ при $n \geqslant 2$, то значение функции x в точке $n-1$ определено однозначно, как и его декартово произведение с A.

По теореме 2.1.45, существуют множество U и функция $f \colon \mathbb{N} \to U$, т. ч. $\psi(f \restriction \underline{n}, f(n))$ при всех n. Условие $f(n) = A^n$ проверяется индукцией по n. Имеем $\psi(f \restriction \underline{0}, f(0))$, откуда $f(0) = \{\varnothing\} = A^0$, и $\psi(f \restriction \underline{1}, f(1))$, откуда $f(1) = A$. При $n \geqslant 2$ получаем $f(n) = (f \restriction n)(n-1) \times A = = f(n-1) \times A = A^{n-1} \times A = A^n$. Единственность подходящей функции f очевидна.

Теперь мы можем свободно рассматривать такие множества, как $\bigcup_{n \in \mathbb{N}} A^n = \cup f[\mathbb{N}]$ или $\bigcup_{n \in \mathbb{N}} A^{A^n}$.

Упражнение 2.1.47. Докажите, что для любого A существует множество всех функций вида $A^n \to A$, где $n \in \mathbb{N}$.

Замечание 2.1.48. Видно, что из теоремы 2.1.45 легко следует теорема 2.1.29 о рекурсии, причем даже в форме «возвратной рекурсии» (следствие 2.1.36). Это неудивительно, поскольку мы ввели в действие весьма сильные аксиомы подстановки.

Упражнение 2.1.49. Докажите, что существует множество $A \neq \varnothing$, т. ч. $\cup A = A$. С учетом следующего раздела выясните, может ли такое A быть конечным.

Упражнение 2.1.50. Докажите, что существует множество $A \neq \varnothing$, т. ч. $A \times A \subseteq A$.

Упражнение 2.1.51. Докажите, что существует множество $A \neq \varnothing$, т. ч. для всех $X \in A$ выполнено $\cup X \in A$ и $\mathcal{P}(X) \in A$.

§ 2.2. Конечные и счетные множества

В этом разделе мы дадим аккуратные обоснования ряду интуитивно очевидных утверждений, имеющих самое широкое употребление.

Множество A называется *счетным*, если $A \sim \mathbb{N}$. Иногда счетными называют еще и конечные множества («между» теми и другими, как мы увидим, ничего нет).

Лемма 2.2.1. *Если множество A счетно (конечно, бесконечно) и $A \sim B$, то B таково же.*

Лемма 2.2.2. *Если множество A счетно и $A \lesssim B$, то B бесконечно.*

Доказательство. В противном случае, $\underline{n+1} \lesssim \mathbb{N} \lesssim B \sim \underline{n}$ для некоторого $n \in \mathbb{N}$. Но тогда $\underline{n+1} \lesssim \underline{n}$ вопреки принципу Дирихле. □

Лемма 2.2.3. *Если $A \subseteq \mathbb{N}$, то множество A конечно или счетно.*

Доказательство. Интуитивное доказательство просто: присвоим всем элементам A натуральные номера в порядке возрастания, так что $A = \{a_0, a_1, \ldots\}$ и $a_0 < a_1 < \ldots$ Если элементы A закончатся, то мы построили биекцию $k \mapsto a_k$ из $\underline{n}$ в A для некоторого $n \in \mathbb{N}$. Иначе получится биекция $\mathbb{N} \to A$. Реализуем эту интуицию с помощью формального построения множеств.

Согласно теореме 2.1.29 и принципу наименьшего числа, существует функция $\alpha\colon \mathbb{N} \to \mathcal{P}(A)$, т. ч. для всех $n \in \mathbb{N}$ верно

$$\begin{aligned} \alpha(0) &= A; \\ \alpha(n+1) &= \begin{cases} \alpha(n) \setminus \{\min \alpha(n)\}, & \text{если } \alpha(n) \neq \varnothing; \\ \varnothing & \text{иначе.} \end{cases} \end{aligned}$$

Легко видеть, что для всех $n \in \mathbb{N}$ верно $\alpha(n+1) \subseteq \alpha(n)$, причем $\alpha(n+1) \subsetneq \alpha(n)$, если $\alpha(n) \neq \varnothing$.

Допустим, функция α принимает значение $\varnothing$. Рассмотрим *наименьшее* n_0, т. ч. $\alpha(n_0) = \varnothing$. Тогда, полагая $f(m) = \min \alpha(m)$ при всех $m \in \underline{n_0}$, имеем функцию $f\colon \underline{n_0} \to A$. Если же $\alpha(n) \neq \varnothing$ при всех n, условие $f(n) = \min \alpha(n)$ определяет функцию $f\colon \mathbb{N} \to A$.

Проверим, что в каждом из случаев функция f является инъекцией. Ясно, что $f(n+1) > f(n)$, если $n+1 \in \operatorname{dom} f$. По индукции, отсюда легко получить $f(m) > f(n)$ при условии $m > n$. Если $m \neq n$, то без ограничения общности $m > n$, а значит, $f(m) \neq f(n)$.

Теперь проверим, что f сюръективна. Допустим, что найдется $a \in A \subseteq \mathbb{N}$, т. ч. $a \notin \operatorname{rng} f$. Индукцией легко показать, что $a \in \alpha(n)$ для всех $n \in \mathbb{N}$. Но тогда $\alpha(n_0) \neq \varnothing$, и в случае $f\colon \underline{n_0} \to A$ мы получили желаемое противоречие.

Остается случай $f\colon \mathbb{N} \to A$. Мы утверждаем, что найдется $k \in \mathbb{N}$, т. ч. $a \leqslant f(k)$. В самом деле, иначе $f\colon \mathbb{N} \to \underline{a}$, т.е. $\mathbb{N} \lesssim \underline{a}$, что невозможно по лемме 2.2.2. Очевидно, что $a \neq f(k) \in \operatorname{rng} f$. Значит, $a < f(k) = \min \alpha(k)$. С другой стороны, $a \in \alpha(k)$. Противоречие.

Итак, мы доказали, что f — биекция, причем в случае $\underline{n_0} \overset{f}{\sim} A$ множество A конечно, и счетно в случае $\mathbb{N} \overset{f}{\sim} A$. □

Следствие 2.2.4. *Если $A \lesssim B$ и множество B счетно, то A конечно или счетно.*

Следствие 2.2.5. *Если $A \lesssim B$ и множество B конечно, то A тоже конечно, причем $|A| \leqslant |B|$.*

Доказательство. Имеем $A \lesssim B \sim \underline{n} \lesssim \mathbb{N}$ для некоторого $n \in \mathbb{N}$. Тогда A конечно или счетно по предыдущему следствию. Однако счетность A противоречит лемме 2.2.2. Если $A \sim \underline{m}$ и $m > n$, то получаем $\underline{m} \lesssim \underline{n}$ вопреки принципу Дирихле. Значит, $m \leqslant n$. □

Со следующих *правил суммы и произведения* начинается *перечислительная комбинаторика*, посвященная подсчету объектов, образуемых конечными множествами (таких, как перестановки, сочетания, размещения, разбиения и пр.)

Теорема 2.2.6 (правило суммы)**.** *Пусть множества A и B конечны и $A \cap B = \varnothing$. Тогда множество $A \cup B$ тоже конечно, причем $|A \cup B| = |A| + |B|$.*

Доказательство. Допустим, что $A \overset{f}{\sim} \underline{n}$ и $B \overset{g}{\sim} \underline{m}$. Определим биекцию $h\colon A \cup B \to \underline{n+m}$, полагая

$$h(x) \quad = \quad \begin{cases} f(x), & \text{если } x \in A; \\ n + g(x), & \text{если } x \in B. \end{cases}$$

В силу $A \cap B = \varnothing$, действительно, получается функция, причем, очевидно, $h(x) < n + m$. Пусть $h(x) = h(y)$. Если $x, y \in A$, то $x = y$ по инъективности f. Если же $x, y \in B$, имеем $n + g(x) = n + g(y)$, откуда $g(x) = g(y)$ в силу свойств сложения и $x = y$ по инъективности g. Теперь допустим, что $x \in A$ и $y \in B$. Имеем $h(x) = f(x) < n \leqslant n + g(y) = h(y)$, что противоречит $h(x) = h(y)$. Итак, функция h инъективна.

Установим сюръективность. Пусть $k \in \underline{n+m}$. Тогда $k < n$ или $n \leqslant k < n + m$. В первом случае $k = f(x) = h(x)$ для некоторого $x \in A$ в силу сюръективности f. Во втором — по свойствам сложения замечаем, что $k = n + k'$ для некоторого $k' < m$. По сюръективности g, найдется $y \in B$, т. ч. $k' = g(y)$, но тогда $k = n + g(y) = h(y)$. □

Следствие 2.2.7. *Если множества A и B конечны, то множество $A \cup B$ тоже конечно, причем $|A \cup B| = |A| + |B| - |A \cap B|$.*

Доказательство. Имеем $A = (A \setminus B) \cup (A \cap B)$ и $A \cup B = (A \setminus B) \cup B$.

Множества $A \setminus B$, $A \cap B \subseteq A$ конечны в силу следствия 2.2.5. Множество $A \setminus B$ не пересекается ни с $A \cap B$, ни с B. Поэтому $|A| = |A \setminus B| + |A \cap B|$, и для конечного $A \cup B$ получаем

$$|A \cup B| = |A \setminus B| + |B| = (|A| - |A \cap B|) + |B| = |A| + |B| - |A \cap B|.$$

□

Следствие 2.2.8. *Если множества A и B конечны, то $|A \cup B| \leqslant |A| + |B|$.*

Замечание 2.2.9. Результат следствия 2.2.7 нетрудно обобщить на объединение трех конечных множеств:

$$\begin{aligned}|(A\cup B)\cup C| &= |A\cup B| + |C| - |(A\cup B)\cap C| = \\ &= |A\cup B| + |C| - |(A\cap C)\cup(B\cap C)| = |A| + |B| - |A\cap B| + \\ &\quad + |C| - (|A\cap C| + |B\cap C| - |A\cap C\cap B\cap C|) = \\ &= |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap C\cap B\cap C|.\end{aligned}$$

Дальнейшее обобщение с помощью индукции по $n \geqslant 2$ дает для конечных множеств $A_1, \ldots, A_n$ важный *принцип включений–исключений*:

$$|A_1\cup A_2\cup\ldots\cup A_n| = \sum_{k=1}^{n}(-1)^{k-1}\sum_{1\leqslant i_1<i_2<\ldots<i_k\leqslant n}|A_{i_1}\cap A_{i_2}\cap\ldots\cap A_{i_k}| =$$

$$= \sum_{1\leqslant i_1\leqslant n}|A_{i_1}| - \sum_{1\leqslant i_1<i_2\leqslant n}|A_{i_1}\cap A_{i_2}| + \sum_{1\leqslant i_1<i_2<i_3\leqslant n}|A_{i_1}\cap A_{i_2}\cap A_{i_3}| - \ldots$$

$$\ldots + (-1)^{n-1}|A_1\cap A_2\cap\ldots\cap A_n|.$$

Теорема 2.2.10 (правило произведения)**.** *Пусть множества A и B конечны. Тогда множество $A\times B$ тоже конечно, причем $|A\times B| = |A|\cdot|B|$.*

Доказательство. Пусть $A \overset{f}{\sim} \underline{n}$ и $B \overset{g}{\sim} \underline{m}$. Если $m = 0$, то $B = \varnothing$ и $A\times B = \varnothing \sim \underline{0}$. Пусть $m \neq 0$. Укажем биекцию $h\colon A\times B \to \underline{nm}$. Именно, положим

$$h(x,y) = mf(x) + g(y)$$

для всех $x\in A$, $y\in B$.

Из арифметики известна *теорема о делении с остатком*, согласно которой, для любых натуральных u и $v\neq 0$ существует единственная пара $(q,r)\in\mathbb{N}^2$, т. ч. $u = vq + r$ и $r < v$.

Проверим сюръективность функции h. Пусть $z\in\underline{nm}$. Тогда $z = mq + r$ для некоторых $q\in\mathbb{N}$ и $r\in\underline{m}$. Значит, найдется $y\in B$, т. ч. $r = g(y)$. Также $q\in\underline{n}$, поскольку иначе $z\geqslant nm$; поэтому найдется и $x\in A$, для которого $q = f(x)$. Итак, $z = mf(x) + g(y) = h(x,y)$.

Проверим инъективность. Пусть $mf(x) + g(y) = mf(x') + g(y') = z = mq + r$. Поскольку $g(y), g(y') < m$, по теореме о делении с остатком имеем $g(y) = g(y')$ и, учитывая свойства сложения и умножения, $f(x) = f(x')$. Тогда получаем $x = x'$ и $y = y'$ по инъективности f и g. $\square$

Замечание 2.2.11. Как видит читатель, мы вывели правила сложения и умножения из утверждений о сложении и умножении натуральных чисел. В свою очередь, сами эти утверждения можно доказать по индукции, используя рекурсивные определения сложения и умножения. В последующих частях курса мы установим такие утверждения в более общей форме.

Следствие 2.2.12. *Если множество A конечно, то при любом $n \in \mathbb{N}$ множество A^n тоже конечно, причем $|A^n| = |A|^n$.*

Доказательство. Индукция по n с учетом $A^{n+1} \sim A^n \times A$ при $n \geqslant 1$. □

Следствие 2.2.13. *Если множества A и B конечны, то множество B^A тоже конечно, причем $|B^A| = |B|^{|A|}$.*

Доказательство. Пусть $A \sim \underline{n}$. В силу теоремы 1.5.11 и леммы 2.1.15 имеем $B^A \sim B^{\underline{n}} \sim B^n$, откуда $|B^A| = |B^n| = |B|^{|A|}$. □

Следствие 2.2.14. *Если множество A конечно, то множество $\mathcal{P}(A)$ тоже конечно, причем $|\mathcal{P}(A)| = 2^{|A|}$.*

Доказательство. Согласно лемме 2.1.9, получаем $\mathcal{P}(A) \sim \underline{2}^A$, откуда $|\mathcal{P}(A)| = |\underline{2}^A| = |\underline{2}|^{|A|} = 2^{|A|}$. □

Пример 2.2.15. Напротив, если A бесконечно, тривиальное вложение $A \lesssim \mathcal{P}(A)$ влечет, по следствию 2.2.5, что $\mathcal{P}(A)$ также бесконечно.

Лемма 2.2.16. *Если множества A и B счетны, то множество $A \times \times B$ тоже счетно.*

Доказательство. Согласно примеру 1.5.10, $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. Затем используем теорему 1.5.11. □

Следствие 2.2.17. *Если множество A счетно и $n \in \mathbb{N}_+$, то множество A^n тоже счетно (а $A^0 = \{\varnothing\}$ конечно).*

Пример 2.2.18. Если множество A счетно, а B счетно или конечно, то счетно и $A \cup B$.

В самом деле, $A \subseteq A \cup B$, откуда $\mathbb{N} \lesssim A \cup B$. С другой стороны, $A \cup B \lesssim (\mathbb{N} \times \{0\}) \cup (\mathbb{N} \times \{1\})$. Действительно, пусть $A \overset{f}{\sim} \mathbb{N}$ и $B \overset{g}{\lesssim} \mathbb{N}$.

Тогда для всех $x \in A \cup B$ полагая

$$h(x) \quad = \quad \begin{cases} (f(x), 0), & \text{если } x \in A; \\ (g(x), 1), & \text{если } x \in B \setminus A, \end{cases}$$

получаем инъекцию $h\colon A \cup B \to (\mathbb{N} \times \{0\}) \cup (\mathbb{N} \times \{1\})$. Далее, имеем $(\mathbb{N} \times \{0\}) \cup (\mathbb{N} \times \{1\}) = \mathbb{N} \times \underline{2} \lesssim \mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. Итак, $A \cup B \lesssim \mathbb{N}$, и окончательно, $A \cup B \sim \mathbb{N}$.

Интуитивно ясно, что если есть сюръекция из A в B, то множество B «не больше», чем множество A, ибо из каждого элемента A в B идет ровно одна стрелка, а различных концов стрелок не больше, чем начал. В формальных терминах достаточно показать, что $B \lesssim A$. Это легко следует из леммы 1.5.28, поскольку правая обратная любой функции есть инъекция. Однако лемма использует аксиому выбора. В случае конечных и счетных множеств без аксиомы можно обойтись.

Лемма 2.2.19. *Пусть $f\colon A \to B$ и множество A конечно. Тогда множество $f[A]$ тоже конечно, причем $|f[A]| \leqslant |A|$.*

Доказательство. Проведем индукцию по $n = |A|$. Если $|A| = 0$, то $A = \varnothing$, откуда $f = \varnothing$ и $f[A] = \varnothing$. Пусть $|A| = n + 1$. Рассмотрим некоторый $x \in A$ и положим $A' = A \setminus \{x\}$. По правилу сложения $|A'| = n$, а значит, по предположению индукции для функции $f' = f \restriction A'$ имеем $|f'[A']| \leqslant |A'|$. С другой стороны, $f[A] = f'[A'] \cup \{f(x)\}$, откуда $|f[A]| \leqslant |f'[A']| + |\{x\}| \leqslant n + 1$. □

Лемма 2.2.20. *Пусть $f\colon A \to B$ и множество A счетно. Тогда множество $f[A]$ конечно или счетно.*

Доказательство. Пусть $\mathbb{N} \overset{\varphi}{\twoheadrightarrow} A$. Определим функцию $g\colon f[A] \to \mathbb{N}$, т. ч. для всех $y \in f[A]$

$$g(y) = \min\{k \in \mathbb{N} \mid f(\varphi(k)) = y\}.$$

Содержательно, $g(y)$ есть «наименьший» прообраз элемента y. В силу принципа наименьшего числа, функция g, действительно, тотальна. Если $g(y) = g(z) = k \in \mathbb{N}$, то $y = f(\varphi(k)) = z$. Значит, g — инъекция. Согласно следствию 2.2.4, множество $f[A]$ оказывается конечно или счетно. □

Зависимый и счетный выбор. Следующие результаты о счетных множествах используют аксиому выбора. Однако «в полную силу» аксиому можно здесь не применять, обходясь важным следствием — *принципом зависимого выбора*, гласящим:

> Пусть множество A непусто и отношение $R \subseteq A^2$ таково, что для всякого $a \in A$ найдется $b \in A$, т. ч. aRb. Тогда существует функция $f\colon \mathbb{N} \to A$, т. ч. $f(n)Rf(n+1)$ для всех $n \in \mathbb{N}$.

Иначе говоря, если для каждого элемента a можно выбрать b так, что aRb, то существует *бесконечная* (именно, счетная) последовательность $(a_n)_{n\in\mathbb{N}}$ таких выборов, где каждый элемент в находится отношении R к последующему. Как видим, логическая структура $\forall\exists \to \exists\forall$ аксиомы выбора сохранена.

Замечание 2.2.21. Индукцией по m легко доказать, что в условиях принципа зависимого выбора *для каждого* $m \in \mathbb{N}$ найдется функция $f\colon \underline{m} \to A$, т. ч. $f(n)Rf(n+1)$, если $n+1 \in \underline{m}$. Но вот «склеить» такие функции в одну $f\colon \mathbb{N} \to A$ без той или иной формы аксиомы выбора не получается.

Пример 2.2.22. Проверим, что принцип зависимого выбора следует из аксиомы выбора.

В самом деле, рассмотрим множество $X = \{R[\{a\}] \in \mathcal{P}(A) \mid a \in \in A\}$. По условию, для каждого $a \in A$ есть b, т. ч. aRb, а значит, $\varnothing \notin X$. Для множества X существует функция выбора $\xi\colon X \to A$ (учли $\cup X \subseteq A$). Поскольку $A \neq \varnothing$, можно взять некоторый $a_0 \in A$. Тогда, согласно теореме 2.1.29, существует функция $f\colon \mathbb{N} \to A$, т. ч.

$$f(0) = a_0 \quad \text{и} \quad f(n+1) = \xi(R[\{f(n)\}])$$

при всех $n \in \mathbb{N}$. Очевидно, функция f искомая.

Лемма 2.2.23. *Если множество A бесконечно, то $\mathbb{N} \lesssim A$.*

Доказательство. Рассмотрим множество

$$F = \{f \in \mathcal{P}(\mathbb{N} \times A) \mid \exists n \in \mathbb{N} \quad \underline{n} \overset{f}{\lesssim} A\}.$$

Попросту, F есть множество всевозможных инъекций из множеств $\underline{n}$ в A. Определим отношение $R \subseteq F^2$, для любых $f, g \in F$ полагая

$$fRg \iff \operatorname{dom} f \subsetneq \operatorname{dom} g \text{ и } g \restriction \operatorname{dom} f = f.$$

Иначе говоря, функция g продолжает функцию f, причем $f \neq g$. Заметим еще, что R транзитивно. Действительно, пусть fRg и gRh. Тогда $f = g \restriction \operatorname{dom} f = (h \restriction \operatorname{dom} g) \restriction \operatorname{dom} f = h \restriction (\operatorname{dom} g \cap \operatorname{dom} f) = h \restriction \operatorname{dom} f$.

Очевидно, что $\underline{0} \overset{\varnothing}{\lesssim} A$, а значит, $\varnothing \in F \neq \varnothing$. Покажем, что для каждого $f \in F$ найдется g, т. ч. fRg. Допустим, $f\colon \underline{n} \to A$. Если $\operatorname{rng} f = A$, то $\underline{n} \overset{f}{\sim} A$, что противоречит бесконечности A. Значит, найдется $x \in A \setminus \{\operatorname{rng} f\}$. Положим $g = f \cup \{(n, x)\}$. Ясно, что g есть искомая инъекция $\underline{n+1} \to A$.

Согласно принципу зависимого выбора, существует $\varphi\colon \mathbb{N} \to F$, т. ч. $\varphi(n) R \varphi(n+1)$ при всех $n \in \mathbb{N}$. Учтя транзитивность R, индукцией легко показать, что $\varphi(n) \restriction \operatorname{dom} \varphi(m) = \varphi(m)$ при $m \leqslant n$. Также по индукции проверим, что $\underline{n} \subseteq \operatorname{dom} \varphi(n)$. Основание очевидно. Пусть $\underline{n} \subseteq \operatorname{dom} \varphi(n)$. Имеем $\underline{n} \subsetneq \operatorname{dom} \varphi(n+1)$, с одной стороны, и $\operatorname{dom} \varphi(n+1) = \underline{m}$ при некотором $m \in \mathbb{N}$, с другой. Ясно, что тогда $m > n$, а значит, $m \geqslant n+1$ и $\underline{n+1} \subseteq \operatorname{dom} \varphi(n+1)$.

Положим $h = \cup\varphi[\mathbb{N}] = \bigcup_{n \in \mathbb{N}} \varphi(n)$. Достаточно проверить, что h есть инъекция $\mathbb{N} \to A$. Очевидно, что $h \subseteq \mathcal{P}(\mathbb{N} \times A)$. Пусть $(k, x), (k, y) \in h$. Тогда $(k, x) \in \varphi(m)$ и $(k, y) \in \varphi(n)$ для некоторых $m, n \in \mathbb{N}$. Без ограничения общности, $m \leqslant n$. По доказанному имеем $(k, x) \in \varphi(m) \subseteq \varphi(n)$. В силу функциональности $\varphi(n)$ получаем $x = y$. Итак, отношение h функционально. Аналогично, если $(k, x), (l, x) \in h$, а значит, $(k, x) \in \varphi(m)$, $(l, x) \in \varphi(n)$ и $m \leqslant n$, то $(k, x), (l, x) \in \varphi(n)$, что влечет $k = l$ по инъективности $\varphi(n)$. Инъективность h установлена.

Проверим, наконец, тотальность h. Для каждого $k \in \mathbb{N}$ по доказанному имеем $k \in \underline{k+1} \subseteq \operatorname{dom} \varphi(k+1) \subseteq \bigcup_{n \in \mathbb{N}} \operatorname{dom} \varphi(n) = \operatorname{dom} h$. $\square$

Следствие 2.2.24. *Всякое множество A бесконечно тогда и только тогда, когда $\mathbb{N} \lesssim A$.*

Как видим, множество $\mathbb{N}$ является «наименьшим» в смысле «отношения» $\lesssim$ бесконечным множеством.

Замечание 2.2.25. «Интуитивное» доказательство леммы 2.2.23 таково. Раз A бесконечно, $A \setminus B \neq \varnothing$ для любого конечного B. Поэтому можно выбрать a_0 в A, затем $a_1 \in A \setminus \{a_0\}$, $a_2 \in A \setminus \{a_0, a_1\}$ и т. д., т. ч. $f(n) = a_n$.

Применяя аксиому выбора ко множеству $\mathcal{P}_*(A) = \mathcal{P}(A) \setminus \{\varnothing\}$, легко придать этому рассуждению строгий характер. Поскольку A может быть сколь угодно велико, аксиома выбора применяется здесь к неограниченно большим множествам — в полной своей общности. Как мы видели, это оказывается избыточным.

Упражнение 2.2.26. Формализуйте интуитивное доказательство указанным способом.

Замечание 2.2.27. Лемму 2.2.23 можно также вывести из следующей *аксиомы счетного выбора*:

> Для всякого *счетного* множества A, т. ч. $\varnothing \notin A$, существует функция выбора.

Из аксиомы выбора тривиально следует аксиома счетного выбора.

Упражнение 2.2.28. Выведите лемму 2.2.23 из аксиомы счетного выбора. (Можно рассмотреть множества $\mathcal{P}_{2^n}(A) \neq \varnothing$ подмножеств A мощности 2^n при всех $n \in \mathbb{N}$. Если $A_i \in \mathcal{P}_{2^i}(A)$, то $A_n \setminus \bigcup_{i<n} A_i \neq \varnothing$.)

Упражнение 2.2.29. Выведите аксиому счетного выбора из принципа зависимого выбора. (Для счетного семейства множеств рассмотрите дизъюнктное объединение.)

Пример 2.2.30. Пусть множество A бесконечное, а множество B конечное или счетное. Тогда $A \cup B \sim A$.

Заметим, что $A \cup B = A \cup (B \setminus A)$. Согласно следствиям 2.2.5 и 2.2.4, множество $B \setminus A \subseteq B$ конечно или счетно. По лемме 2.2.23, в A есть счетное подмножество B'. Имеем

$$A \cup B = (A \setminus B') \cup B' \cup (B \setminus A),$$

причем множества в правой части попарно не пересекаются. Вследствие примера 2.2.18, множество $C = B' \cup (B \setminus A)$ счетно, т. е. существует биекция $f\colon C \to B'$. Учитывая $A \cup B = (A \setminus B') \cup C$, продолжим биекцию f до функции $g\colon A \cup B \to (A \setminus B') \cup B'$, т. ч.

$$g(x) \quad = \quad \begin{cases} f(x), & \text{если } x \in C; \\ x, & \text{если } x \in A \setminus B'. \end{cases}$$

Биективность g очевидна. Поскольку $(A \setminus B') \cup B' = A$, биекция g является искомой.

Упражнение 2.2.31. Докажите, что если множество $A \setminus B$ бесконечно, а B конечно или счетно, то $A \sim A \setminus B$.

В примере 2.2.18 мы видели, что объединение двух счетных множеств счетно. Оказывается, любое объединение «счетного числа» счетных множеств также оказывается счетно. Установим это часто используемое утверждение.

Теорема 2.2.32. *Пусть множество A конечно или счетно и каждое множество $X \in A$ конечно или счетно. Тогда множество $\cup A$ тоже конечно или счетно.*

Доказательство. Интуитивно, можно занумеровать каждый элемент $a \in \cup A = \cup\{X_0, X_1, \ldots\}$ парой чисел $(m, n) \in \mathbb{N}^2$, где $a = a_n^m \in X_m = \{a_0^m, a_1^m, \ldots\}$. Число m берем наименьшим подходящим, но аксиома выбора все же потребуется, ибо присвоить натуральные номера элементам множества X_m можно по-разному, а нам нужно зафиксировать такие нумерации для всех m сразу.

Определим функцию $\varphi\colon A \to \mathcal{P}(\mathcal{P}(\cup A \times \mathbb{N}))$, при всех $X \in A$ полагая

$$\varphi(X) = \{f \in \mathcal{P}(\cup A \times \mathbb{N}) \mid X \overset{f}{\lesssim} \mathbb{N}\}.$$

Как видно, $\varphi(X)$ есть множество всевозможных вложений X в $\mathbb{N}$ (каждое такое вложение является подмножеством множества $X \times \mathbb{N} \subseteq \cup A \times \times \mathbb{N}$). Все множества $X \in A$ конечны или счетны, а значит, вкладываются в $\mathbb{N}$, откуда $\varphi(X) \neq \varnothing$. По лемме 2.2.20, образ $\varphi[A]$ счетный или конечный. Применяя аксиому счетного выбора или в случае конечности индукцию (см. упражнение 2.1.25), получаем функцию выбора ξ для $\varphi[A]$.

Положим $g = \xi \circ \varphi$. Тогда для каждого $X \in A$ имеем инъекцию $g(X)\colon X \to \mathbb{N}$. Также существует инъекция $h\colon A \to \mathbb{N}$. Определим отношение $j \subseteq \cup A \times A$, для всех $a \in \cup A$ и $X \in A$ полагая

$$(a, X) \in j \iff a \in X \text{ и } \forall Y \in A\,(a \in Y \Longrightarrow h(X) \leqslant h(Y)).$$

Отношение j тотально, поскольку среди всех множеств Y, т. ч. $a \in Y$, есть X с наименьшим «номером» $h(X) \in \mathbb{N}$. Так как из $(a, X') \in j$ и $(a, X'') \in j$ следует $h(X') = h(X'')$, отношение j функционально по инъективности h. Итак, $j\colon \cup A \to A$, причем $a \in j(a)$.

Рассмотрим отображение $f\colon \cup A \to \mathbb{N} \times \mathbb{N}$, т. ч.

$$f(a) = (h(j(a)), (g(j(a)))(a))$$

для всех $a \in A$. Это инъекция. Действительно, если $h(j(a)) = h(j(a'))$, то $j(a) = j(a') = X \in A$, откуда $a, a' \in X$. Но тогда имеем $(g(X))(a) = = (g(X))(a')$ и $a = a'$. Остается использовать пример 1.5.10 и следствие 2.2.4. $\square$

Следствие 2.2.33. *Если множество I конечно или счетно и при каждом $i \in I$ конечно или счетно A_i, то $\bigcup_{i\in I} A_i$ тоже конечно или*

счетно, причем если A_i счетно при некотором $i \in I$, то и множество $\bigcup_{i\in I} A_i$ счетно.

Упражнение 2.2.34. Не используя никакой формы аксиомы выбора, докажите, что если множество A и все его элементы конечны, то множество $\cup A$ тоже конечно.

Упражнение 2.2.35. Не используя никакой формы аксиомы выбора, докажите, что если A бесконечно, то множество $\cup A$ тоже бесконечно.

Другие определения конечности. В нашем курсе понятие конечного множества оказалось зависимым от понятия натурального числа. Поскольку в последующих частях курса мы *определим* множество $\mathbb{N}$, это не большая беда. Тем не менее интересно рассмотреть альтернативные определения конечного множества, не упоминающие натуральные числа. Некоторые из таких определений эквивалентны нашему лишь в предположении аксиомы выбора.

Множество A назовем *конечным по Дедекинду* (или *D-конечным*), если всякая инъекция $A \to A$ является сюръекцией. Свойство *D-бесконечности*, таким образом, означает наличие биекции между множеством и его *собственным* подмножеством: скажем, между $\mathbb{N}$ и четными натуральными или квадратами натуральных чисел[7].

Лемма 2.2.36. *Множество A является D-бесконечным тогда и только тогда, когда $\mathbb{N} \lesssim A$.*

Доказательство. Пусть A не D-конечно. Тогда существует инъекция $g\colon A \to A$, не являющаяся сюръекцией, и найдется $x \in A \setminus g[A]$. По рекурсии определим функцию $f\colon \mathbb{N} \to A$, т. ч.

$$f(0) = x \quad \text{и} \quad f(n+1) = g(f(n))$$

при всех $n \in \mathbb{N}$. Покажем, что f — инъекция. В противном случае найдутся числа $m < n$, т. ч. $f(m) = f(n)$. Возьмем наименьшее m, для которого есть n с таким свойством. Если $m = 0$, то $x = f(n)$; так как $n = k + 1$, имеем $x = g(f(k)) \in g[A]$, что неверно. Если же $m = l + 1$ и $n = k + 1$, из $f(m) = g(f(l)) = g(f(k)) = f(n)$ по инъективности g получаем $f(l) = f(k)$ при $l < m \leqslant k$, что противоречит выбору m.

[7]Наблюдение о квадратах сделал Г. Галилей, впрочем, заключивший из него, что бесконечные совокупности бессмысленно сравнивать по величине. Мы же, разделив понятия $\subseteq$ и $\lesssim$, преодолеваем затруднение.

Обратно, пусть $\mathbb{N} \overset{f}{\lesssim} A$. Положив $B = f[\mathbb{N}]$, имеем $\mathbb{N} \overset{f}{\sim} B \subseteq A$. Определим функцию $g\colon A \to A$, для всех $x \in A$ полагая

$$g(x) \quad = \quad \begin{cases} f(2f^{-1}(x)), & \text{если } x \in B; \\ x, & \text{если } x \in A \setminus B. \end{cases}$$

Инъективность функции g очевидна. Однако $f(1) \notin \operatorname{rng} g$. Действительно, иначе $f(2f^{-1}(x)) = f(1) \in B$ для некоторого $x \in B$, откуда $2f^{-1}(x) = 1$, что невозможно для $f^{-1}\colon B \to \mathbb{N}$. Значит, инъекция g не сюръективна, а множество A не D-конечно. □

Замечание 2.2.37. Мы доказали лемму, не используя никакой формы аксиомы выбора. Напротив, в следующем утверждении мы ссылаемся на аксиому (счетного) выбора.

Следствие 2.2.38. *Множество конечно тогда и только тогда, когда оно D-конечно.*

Доказательство. Условие $\mathbb{N} \lesssim A$ равносильно бесконечности A в силу следствия 2.2.24. □

Множество A назовем *конечным по Тарскому* (или *T-конечным*), если в каждом непустом семействе $S \subseteq \mathcal{P}(A)$ есть $\subseteq$-максимальный элемент.

Упражнение 2.2.39. Не используя никакой формы аксиомы выбора, докажите, что в определении конечности по Тарскому можно равносильным образом заменить «максимальный элемент» на «минимальный».

Установим равносильность конечности и T-конечности, не используя никакой формы аксиомы выбора.

Лемма 2.2.40. *Множество A конечно тогда и только тогда, когда это множество T-конечно.*

Доказательство. Пусть $|A| = n$ и $\varnothing \neq S \subseteq \mathcal{P}(A)$. Если $B \in S$, то, согласно следствию 2.2.5, множество B конечно, причем $|B| \leqslant n$. Поэтому число n является верхней гранью непустого множества $S' = \{|B| \in \mathbb{N} \mid B \in S\}$. Тогда существует *наименьшая* верхняя грань $m = \sup S' \leqslant n$.

Покажем, что $m \in S'$, а значит, $m = \max S'$. Пусть не так. Если $m = 0$, то $S' = \varnothing$, что не верно. Значит, $m = l+1$. Но тогда $l < m$ тоже верхняя грань S', поскольку из $k < m$ следует $k \leqslant l$. Противоречие.

Рассмотрим какое-нибудь $C \in S$, т. ч. $|C| = m$. Мы утверждаем, что это множество максимальное в S. В противном случае, найдется $B \in S$, т. ч. $C \subsetneq B$. Тогда, с одной стороны, $|B| = |C| + |B \setminus C| > |C|$, поскольку $B \setminus C \neq \varnothing$. А с другой стороны, $|B| \leqslant |C|$ по максимальности $m \in S'$. Противоречие. Итак, A оказалось T-конечно.

В обратную сторону. Допустим, множество A бесконечно. Рассмотрим множество $\mathcal{P}_f(A) = \{B \in \mathcal{P}(A) \mid \exists n \in \mathbb{N}\ B \sim \underline{n}\}$, т. е. множество всех *конечных* подмножеств A. Имеем $\varnothing \in \mathcal{P}_f(A) \neq \varnothing$. Предположим $B \in \max \mathcal{P}_f(A)$. Раз A бесконечно, $B \neq A$, а значит, найдется $b' \in A \setminus B$. Для множества $B' = B \cup \{b\}$ имеем $B \subsetneq B'$. С другой стороны, как мы знаем, B' конечно, т. е. $B' \in \mathcal{P}_f(A)$. Получили противоречие с максимальностью B. Следовательно, в семействе $\mathcal{P}_f(A)$ нет максимальных элементов, и множество A не является T-конечным. □

На основе понятия T-конечности нетрудно обосновать многие из уже известных нам свойств конечных множеств.

Пример 2.2.41. Если T-конечны множества A и B, то T-конечно и $A \cup B$.

Пусть $\varnothing \neq S \subseteq \mathcal{P}(A \cup B)$. В семействе $S_1 = \{C \cap A \mid C \in S\} \subseteq \mathcal{P}(A)$ есть максимальный элемент $C_1 \cap A$, а в семействе

$$S_2 = \{C \cap B \mid C \in S \text{ и } C \cap A = C_1 \cap A\} \subseteq \mathcal{P}(B),$$

содержащем $C_1 \cap B$, есть максимальный элемент $C_2 \cap B$. Пусть $C_2 \subsetneq C' \in S$. Тогда $C_2 \cap B \subseteq C' \cap B$ и $C_1 \cap A = C_2 \cap A \subseteq C' \cap A$, причем хотя бы одно из включений строгое, что противоречит, однако, выбору C_1 и C_2. Значит, C_2 максимально в S.

Пример 2.2.42. Пусть $f\colon A \to B$ и T-конечно множество A. Тогда множество $f[A]$ тоже T-конечно.

Пусть $\varnothing \neq S \subseteq \mathcal{P}(f[A])$. Рассмотрим непустое семейство $S' = \{f^{-1}[D] \mid D \in S\} \subseteq \mathcal{P}(A)$. В силу T-конечности A, найдется $C_0 = f^{-1}[D_0] \in \max S'$. Допустим, $D_0 \subsetneq D' \in S$. Тогда $C_0 \subseteq f^{-1}[D'] \in S'$. Для $y \in D' \setminus D_0$ найдется x, т. ч. $f(x) = y$, а значит, $x \in f^{-1}[D'] \setminus C_0$. Это противоречит максимальности C_0. Следовательно, $D_0 \in \max S$, и множество $f[A]$ является T-конечным.

Упражнение 2.2.43. Рассуждая в терминах T-конечности, докажите, что если T-конечно множество A, то T-конечно и $\mathcal{P}(A)$.

Упражнение 2.2.44. Не используя никакой формы аксиомы выбора, докажите, что множество A конечно тогда и только тогда, когда множество $\mathcal{P}(\mathcal{P}(A))$ D-конечно. (Можно рассмотреть отображение $n \mapsto$ $\mapsto \{X \in \mathcal{P}(A) \mid |X| = n\}$ и применить лемму 2.2.36.)

§ 2.3. Формальные языки

Как мы уже отмечали, чтобы вести какие-либо рассуждения, нужны обозначения. В естественных языках, а также в их потомках, таких как языки программирования или язык формализованной математики, обозначения обычно предстают в виде *конечных последовательностей* неких различимых элементов: «букв» на письме, «звуков» в устной речи или «жестов» в языке глухонемых[8]. При этом различные комбинации известного набора элементов придают обозначению разный смысл.

В данном разделе мы сможем построить модель таких «линейных обозначений», поскольку конечные последовательности уже выразили в терминах множеств. Кроме логики, эта модель используется в информатике и лингвистике.

Алфавиты и слова. *Алфавитом* назовем произвольное непустое множество. Элементы алфавита A станем называть *символами* или *буквами*. Если $n \in \mathbb{N}$, любое отображение $\sigma\colon \underline{n} \to A$ мы называем *словом над алфавитом* (или *в алфавите*) A. Ясно, что $|\sigma| = n$. Число $|\sigma|$ называют также *длиной* слова σ. Как мощность конечного множества, длина определена однозначно.

Над любым алфавитом существует единственное слово длины 0, называемое *пустым* и обозначаемое ε. В самом деле, $A^{\underline{0}} = \{\varnothing\}$ и $\varepsilon = \varnothing$.

Множество всевозможных слов над A обозначается A^*. Иначе говоря, $A^* = \bigcup_{n\in\mathbb{N}} A^{\underline{n}}$. Индексированное семейство $\{A^{\underline{n}}\}_{n\in\mathbb{N}}$ определенно корректно, поскольку определена функция $F\colon n \mapsto A^{\underline{n}}$.

Упражнение 2.3.1. Педантам советуем определить такую функцию F с помощью основных способов задания множеств (без использования аксиом подстановки).

[8] Если стремиться к точности, нужно рассматривать не «буквы» и «звуки», а соответственно «графемы» и «фонемы», т. е. *классы эквивалентности*, возникающие при отождествлении изображений «одной» буквы и произношений «одного» звука, хотя и различных, но узнаваемых как «равнозначные».

Лемма 2.3.2. *Если алфавит A конечный или счетный, то множество A^* счетно.*

Доказательство. Согласно следствию 2.2.33, множество A^* конечно или счетно. Найдется некоторый символ $a \in A$. По рекурсии определим функцию $f\colon \mathbb{N} \to A^*$, т. ч.

$$f(0) = \varepsilon \quad \text{и} \quad f(n+1) = f(n) \cup \{(n, a)\}$$

при всех $n \in A$. Индукцией по n легко проверить, что $f(n) \in A^{\underline{n}}$ и, в частности, $|f(n)| = n$. Поэтому $\mathbb{N} \overset{f}{\lesssim} A^*$. Согласно лемме 2.2.2, множество A^* счетно. □

По лемме 2.1.15, имеем $A^{\underline{n}} \sim A^n$. Соответственно, мы будем отождествлять слово σ длины $n \geqslant 2$ и набор $(\sigma(0), \sigma(1) \ldots, \sigma(n-1)) \in \in A^n$, а слова длины 1 отождествим с элементами множества $A^1 = A$, т. е. с буквами алфавита. В таком контексте, если это не вызывает неясности, мы станем записывать наборы без скобок и запятых: $\sigma(0)\sigma(1)\ldots\sigma(n-1)$.

Замечание 2.3.3. Здесь стоит соблюдать осторожность. Допустим, что $A = \{0, 1, 10\} \subseteq \mathbb{N}$. Какова длина слова $\sigma = 101$ над алфавитом A? Очевидно, это зависит от того, какое из слов: $(1, 0, 1)$ или $(10, 1)$ — имеется в виду. Чтобы еще больше запутать дело, мы могли бы считать, что $1, 0, 10$ обозначают не натуральные числа, но элементы множества $\{0, 1\}^*$. (Очевидно, ничто не мешает буквам быть словами какого-то другого алфавита.) Тогда имеем $|10| = 1$ (в смысле $10 \in A^{\underline{1}}$), хотя $|(1, 0)| = 2$.

Испытанные нами трудности со смыслом обозначения 10 относятся к *метаязыку*, т. е. к *внешнему* для нашей модели, тому *на*, а не *о* котором мы говорим. Тем не менее ситуацию двусмысленных обозначений полезно рассмотреть и *внутри* модели. Мы сделаем это в следующем разделе.

Конкатенацией слов σ и τ в алфавите A называется слово длины $|\sigma| + |\tau|$, обозначаемое $\sigma\tau$, т. ч.

$$(\sigma\tau)(i) \quad = \quad \begin{cases} \sigma(i), & \text{если } i < |\sigma|; \\ \tau(i - |\sigma|), & \text{если } i \geqslant |\sigma|. \end{cases}$$

Иначе говоря, $\sigma\tau = \sigma(0)\ldots\sigma(|\sigma|-1)\tau(0)\ldots\tau(|\tau|-1)$. При заданном A конкатенацию можно рассматривать как функцию $A^* \times A^* \to A^*$.

Пример 2.3.4. Пусть $A = \{a, b, c\}$, $\sigma = abbaca$ и $\tau = ccbab$. Тогда $\sigma\tau = abbacaccbab$ и $\tau\sigma = ccbababbaca$.

Лемма 2.3.5. *Для любых $\sigma, \tau, \rho \in A^*$ верно:*

1) $\sigma\varepsilon = \sigma = \varepsilon\sigma$;

2) $(\sigma\tau)\rho = \sigma(\tau\rho)$.

Доказательство. Допустим, что $|\sigma| = n$, $|\tau| = m$ и $|\rho| = l$. Тогда $|\sigma\varepsilon| = n + 0 = n = |\sigma|$. Так как $(\sigma\varepsilon)(i) = \sigma(i)$ для всех $i \in \underline{n}$, получаем $\sigma = \sigma\varepsilon \in A^{\underline{n}}$. Аналогично, $\varepsilon\sigma = \sigma$.

Слова $(\sigma\tau)\rho$ и $\sigma(\tau\rho)$ имеют одинаковую длину $n+m+l$. Если $i < n$, то также $i < n + m$, так что $((\sigma\tau)\rho)(i) = (\sigma\tau)(i) = \sigma(i) = (\sigma(\tau\rho))(i)$. Пусть теперь $n \leqslant i < n + m$. Тогда $i - n < m$. Имеем $((\sigma\tau)\rho)(i) = = (\sigma\tau)(i) = \tau(i - n) = (\tau\rho)(i - n) = (\sigma(\tau\rho))(i)$. Наконец, допустим $i \geqslant n + m$, откуда $i - n \geqslant m$. Получаем $((\sigma\tau)\rho)(i) = \rho(i - (n + m)) = = \rho((i - n) - m) = (\tau\rho)(i - n) = (\sigma(\tau\rho))(i)$. □

Замечание 2.3.6. Как и в случае мощностей конечных множеств, мы использовали арифметические свойства натуральных чисел.

Замечание 2.3.7. Ассоциативность конкатенации позволяет опускать скобки: $\sigma_1\sigma_2 \dots \sigma_n$, поскольку безразлично, как эти скобки поставить.

Кроме конкатенации, для слова $\sigma \in A^{\underline{n}}$ рассматривают *обращение* $\sigma^{\mathsf{R}} \in A^{\underline{n}}$, полагая $\sigma^{\mathsf{R}}(i) = \sigma(|\sigma| - 1 - i)$.

Пример 2.3.8. Пусть $A = \{a, b, c\}$ и $\sigma = abbacaccbab$. Тогда $\sigma^{\mathsf{R}} = = babccacabba$.

Упражнение 2.3.9. Докажите, что для любых $\sigma, \tau \in A^*$ верно:

1) $(\sigma^{\mathsf{R}})^{\mathsf{R}} = \sigma$;

2) $(\sigma\tau)^{\mathsf{R}} = \tau^{\mathsf{R}}\sigma^{\mathsf{R}}$.

Замечание 2.3.10. Видим, что на множестве A^* операция конкатенации задает полугруппу с нейтральным элементом ε и инверсией $(\cdot)^{\mathsf{R}}$. Подобная структура нам уже встречалась при рассмотрении бинарных отношений на множестве (см. замечание 1.3.25). Тем не менее, как показывает следующая лемма, полугруппы слов и отношений существенно различны (не изоморфны).

Лемма 2.3.11 (левый закон сокращения)**.** *Для любых $\sigma, \tau, \rho \in A^*$ из $\sigma\tau = \sigma\rho$ следует $\tau = \rho$.*

Доказательство. Имеем $|\sigma| + |\tau| = |\sigma\tau| = |\sigma\rho| = |\sigma| + |\rho|$, откуда $|\tau| = |\rho|$. Получаем $\tau(i) = (\sigma\tau)(i + |\sigma|) = (\sigma\rho)(i + |\sigma|) = \rho(i)$. □

Очевидно, имеет место и *правый* закон сокращения: $\tau\sigma = \rho\sigma \Longrightarrow \tau = \rho$.

Для функций $f\colon n \mapsto 0$ и $g\colon n \mapsto 1$ на множестве $\mathbb{N}$ имеет место $\mathbb{N}^2 \circ f = \mathbb{N}^2 = \mathbb{N}^2 \circ g$, хотя $f \neq g$. Поэтому левый закон сокращения не выполнен в полугруппе отношений на $\mathbb{N}$.

Упражнение 2.3.12. Докажите, что если $\sigma = \sigma^{\mathsf{R}}$, т. е. слово $\sigma \in A^*$ есть *палиндром*, то для некоторых $\tau \in A^*$ и $a \in A$ верно $\sigma = \tau\tau^{\mathsf{R}}$ или $\sigma = \tau a \tau^{\mathsf{R}}$.

Положим $\sigma^0 = \varepsilon$ и $\sigma^{k+1} = \sigma^k\sigma$ для всех $k \in \mathbb{N}$. (Формально, мы рекурсивно определяем функцию $f\colon \mathbb{N} \times A^* \to A^*$, где $\sigma^k = f(k, \sigma)$, с помощью следствия 2.1.33.)

Лемма 2.3.13. *Для всех $\sigma \in A^*$ и $k, l \in \mathbb{N}$ верно:*

1) $\sigma^k\sigma^l = \sigma^{k+l}$;

2) $\sigma^k\sigma^l = \sigma^l\sigma^k$.

Доказательство. Индукция по $l \in \mathbb{N}$. Имеем $\sigma^k\sigma^0 = \sigma^k\varepsilon = \sigma^k = \sigma^{k+0}$. Используя предположение индукции для l, получаем $\sigma^k\sigma^{l+1} = \sigma^k(\sigma^l\sigma) = (\sigma^k\sigma^l)\sigma = \sigma^{k+l}\sigma = \sigma^{(k+l)+1} = \sigma^{k+(l+1)}$.

По первому утверждению, $\sigma^k\sigma^l = \sigma^{k+l} = \sigma^{l+k} = \sigma^l\sigma^k$. □

Если $\sigma = \tau\rho$, то говорят, что τ есть *начало* (или *префикс*) слова σ, а ρ есть *окончание* (или *суффикс*) слова σ. Пишут соответственно $\tau \sqsubseteq \sigma$ и $\rho \sqsupseteq \sigma$. Если $\sigma = \tau\pi\rho$, то π есть *подслово* слова σ. Начало, окончание или подслово слова σ называется *собственным*, если оно не совпадает с σ. Тогда пишем $\tau \sqsubset \sigma$ или $\rho \sqsupset \sigma$ соответственно.

Замечание 2.3.14. Очевидно, длина префикса (суффикса, подслова) не больше длины всего слова, причем неравенство строгое, если и только если префикс (суффикс, подслово) собственный. Вообще, $\tau \sqsubseteq \sigma$ равносильно $\tau(i) = \sigma(i)$ при всех $i < |\tau|$, т. е. $\tau = \sigma \restriction \underline{|\tau|}$.

Пример 2.3.15. Очевидно, всегда $\varepsilon \sqsubseteq \sigma$ и $\varepsilon \sqsupseteq \sigma$. Пусть $A = \{a, b, c\}$ и $\sigma = abbacaccbab$. Тогда $abb \sqsubset \sigma$, $cbab \sqsupset \sigma$ и $cacc$ есть собственное подслово слова σ.

Лемма 2.3.16. *$(A^*, \sqsubseteq)$ есть ч. у. м. для любого алфавита A.*

Доказательство. Очевидно, $\sigma \sqsubseteq \sigma\varepsilon = \sigma$. Если $\rho \sqsubseteq \tau$ и $\tau \sqsubseteq \sigma$, то $\sigma = \tau\sigma'$ и $\tau = \rho\tau'$, откуда $\sigma = (\rho\tau')\sigma' = \rho(\tau'\sigma')$, а значит, $\rho \sqsubseteq \sigma$. Если $\tau \sqsubseteq \sigma$ и $\sigma \sqsubseteq \tau$, то $\sigma\varepsilon = \sigma = \tau\sigma' = (\sigma\tau')\sigma' = \sigma(\tau'\sigma')$, что дает $\varepsilon = \tau'\sigma'$ по закону сокращения. Имеем $|\tau'| + |\sigma'| = 0$ и, следовательно, $\tau' = \sigma' = \varepsilon$, откуда $\sigma = \tau\varepsilon = \tau$. Итак, $\sqsubseteq$ есть отношение нестрогого порядка. □

Замечание 2.3.17. $(A^*, \sqsubseteq) \cong (A^*, \sqsupseteq)$, причем в качестве изоморфизма можно взять $\sigma \mapsto \sigma^{\mathsf{R}}$.

Лемма 2.3.18. *Для произвольных непустого $X \subseteq A^*$ и $\sigma, \tau, \rho \in A^*$ верно:*

1) *существует* $\inf_{\sqsubseteq} X$;

2) *если $\sigma \sqsubseteq \rho$ и $\tau \sqsubseteq \rho$, то $\sigma \sqsubseteq \tau$ или $\tau \sqsubset \sigma$.*

Доказательство. По принципу наименьшего числа, в X есть слово θ наименьшей длины n. Если $\theta = \eta \restriction \underline{n}$ при всех $\eta \in X$, то $\theta \sqsubseteq \eta$, а значит, $\theta = \inf_{\sqsubseteq} X$. В противном случае возьмем наименьшее такое $m < n$, что для некоторого $\eta \in X$ выполнено $\theta(m) \neq \eta(m)$. Положим $\xi = \theta \restriction \underline{m}$. По выбору m имеем $\xi = \eta \restriction \underline{m}$, т. е. $\xi \sqsubseteq \eta$, для всех $\eta \in X$. Пусть ξ' тоже является нижней гранью X; тогда $|\xi'| = k \leqslant n$ и $\eta \restriction \underline{k} = \xi' = \theta \restriction \underline{k}$ для всех $\eta \in X$. Если $m < k$, то $\eta(m) = \theta(m)$ для всех $\eta \in X$, что не так. Значит, $k \leqslant m$ и $\xi' = \theta \restriction \underline{k} = \theta \restriction (\underline{m} \cap \underline{k}) = (\theta \restriction \underline{m}) \restriction \underline{k} = \xi \restriction \underline{k}$. Поэтому $\xi' \sqsubseteq \xi$.

Проверим второе утверждение. Пусть $|\sigma| = n$ и $|\tau| = m$. Если $m \leqslant n$, то $\tau = \rho \restriction \underline{m} = \rho \restriction (\underline{n} \cap \underline{m}) = (\rho \restriction \underline{n}) \restriction \underline{m} = \sigma \restriction \underline{n}$, откуда $\tau \sqsubseteq \sigma$. Иначе, очевидно, $\sigma \sqsubset \tau$. □

Как видим, порядок $\sqsubseteq$ является *нижней полурешеткой* (любые два элемента имеют инфимум), хотя, вообще, решеткой не является.

Упражнение 2.3.19. Какому хорошо известному упорядочению изоморфно ч. у. м. $(\{a\}^*, \sqsubseteq)$?

Мы видели, что слова вида ρ^k *коммутируют* (т. е. $\sigma\tau = \tau\sigma$ для любых таких слов σ, τ). Оказывается, коммутируют только они.

Пример 2.3.20. Если $\sigma\tau = \tau\sigma$, то найдутся слово ρ и числа $k, l \in \mathbb{N}$, т. ч. $\sigma = \rho^k$ и $\tau = \rho^l$.

Докажем утверждение индукцией по $n = |\sigma + \tau| \in \mathbb{N}$. При $n = 0$ оно очевидно. Предположим, что для любого $n' < n$ для любых σ' и τ',

если $n' = |\sigma' + \tau'|$ и $\sigma'\tau' = \tau'\sigma'$, то $\sigma' = (\rho')^{k'}$ и $\tau = (\rho')^{l'}$ при некоторых ρ' и k', l'.

Итак, пусть $\sigma\tau = \tau\sigma$. Тогда $\sigma \sqsubseteq \tau$ или $\tau \sqsubseteq \sigma$. Без ограничения общности допустим, что $\tau \sqsubseteq \sigma$, т. е. $\sigma = \tau\pi$. Тогда $\tau\pi\tau = \tau\tau\pi$, откуда $\pi\tau = \tau\pi$. Если $\tau \neq \varepsilon$, то $|\pi| + |\tau| < |\sigma| + |\tau| = n$ и, по предположению индукции, найдутся слово ρ и числа k, l, т. ч. $\tau = \rho^l$ и $\pi = \rho^k$. Тогда $\sigma = \rho^l\rho^k = \rho^{l+k}$. Если же $\tau = \varepsilon$, то, положив $\rho = \sigma$, имеем $\sigma = \rho^1$ и $\tau = \rho^0$.

Упражнение 2.3.21. Докажите *лемму Леви*: для любых $\sigma, \tau, \theta, \eta \in A^*$, если $\sigma\tau = \theta\eta$ и $|\sigma| \geqslant |\theta|$, то найдется ξ, т. ч. $\sigma = \theta\xi$ и $\eta = \xi\tau$.

Рекурсия по длине. Ранее мы обосновали рекурсивное определение функций, имеющих натуральный аргумент. Довольно часто эта процедура может быть обобщена и на функции, чьи аргументы, хотя и не принадлежат $\mathbb{N}$, но имеют некоторый естественный натуральный параметр. В случае слов таким параметром является длина.

Рассмотрим, например, *префиксную* рекурсию, где значение функции на слове σ определяется ее значением на длиннейшем собственном префиксе.

Лемма 2.3.22. *Если A и U суть некоторые множества, $u_0 \in U$ и $h\colon A \times U \to U$, то существует единственная функция $f\colon A^* \to U$, т. ч.*

$$f(\varepsilon) = u_0 \quad \text{и} \quad f(\sigma a) = h(a, f(\sigma))$$

при всех $\sigma \in A^*$ и $a \in A$.

Доказательство. С помощью примитивной рекурсии установим существование функции $f'\colon \mathbb{N} \times A^* \to A^*$, т. ч. $f'(0, \sigma) = u_0$ и

$$f'(n+1, \sigma) \quad = \quad \begin{cases} h(\sigma(n), f'(n, \sigma)), & \text{если } |\sigma| > n; \\ f'(n, \sigma) & \text{иначе} \end{cases}$$

при всех $\sigma \in A^*$ и $n \in \mathbb{N}$. Индукцией по n проверим, что $f'(n, \sigma) = f'(n, \sigma \restriction \underline{n})$ при всех $\sigma \in A^*$. В самом деле, случай $n = 0$ ясен. По определению, $f'(n+1, \sigma \restriction \underline{n+1}) = f'(n, \sigma \restriction \underline{n+1})$, если $|\sigma \restriction \underline{n+1}| \leqslant n$, т. е. $|\sigma| \leqslant n$, и $f'(n+1, \sigma \restriction \underline{n+1}) = h((\sigma \restriction \underline{n+1})(n), f'(n, \sigma \restriction \underline{n+1})) = h(\sigma(n), f'(n, \sigma \restriction \underline{n+1}))$, если $|\sigma \restriction \underline{n+1}| \geqslant n+1$, т. е. $|\sigma| \geqslant n+1$.

Имеем $f'(n, \sigma \restriction \underline{n+1}) = f'(n, (\sigma \restriction \underline{n+1}) \restriction \underline{n}) = f'(n, \sigma \restriction \underline{n}) = f'(n, \sigma)$ по предположению индукции. Значит, $f'(n+1, \sigma \restriction \underline{n+1})$ равно $f'(n, \sigma)$ при $|\sigma| \leqslant n$ и равно $h(\sigma(n), f'(n, \sigma))$ при $|\sigma| > n$, т. е. равно $f'(n+1, \sigma)$ во всяком случае.

Теперь полагаем $f(\sigma) = f'(|\sigma|, \sigma)$ и убеждаемся, что функция f подходит. Проверка единственности f оставляется читателю. $\square$

Пример 2.3.23. Существуют и единственны функции $f, g\colon \mathbb{N}^* \to \mathbb{N}$, т. ч. $f(\varepsilon) = 0$ и $f(\sigma n) = f(\sigma) + n$, а $g(\varepsilon) = 1$ и $g(n\sigma) = n^{g(\sigma)}$ при всех $\sigma \in \mathbb{N}^*$, $n \in \mathbb{N}$. (Имея префиксную рекурсию и операцию обращения, получаем «суффиксную» рекурсию.) Неформально, $f(\sigma) = \sigma(0) + \sigma(1) + \ldots + \sigma(m-1)$ и $g(\sigma) = \sigma(0)^{\sigma(1)^{\cdots^{\sigma(m-1)}}}$ при $m = |\sigma|$.

Полукольцо языков. *Языком над алфавитом* A назовем каждое подмножество $L \subseteq A^*$. Для языков над алфавитом A определим операции сложения и умножения:

$$L + M = L \cup M \quad \text{и} \quad L \cdot M = \{\sigma\tau \mid \sigma \in L \text{ и } \tau \in M\},$$

которые, очевидно, можно рассматривать как функции $(\mathcal{P}(A^*))^2 \to \to \mathcal{P}(A^*)$.

Пример 2.3.24. Пусть $a, b \in A$. Тогда $\{ab, b\}\cdot\{ba, \varepsilon\} = \{abba, ab, bba, b\}$ и $(\{aa\} \cdot A^*) \cdot \{a\} = \{\sigma \in A^* \mid \exists \tau \in A^*\ \sigma = aa\tau a\}$.

Лемма 2.3.25. *Для любых* $L, M, N \subseteq A^*$ *верно:*

1) $(L + M) + N = L + (M + N)$;
2) $L + M = M + L$;
3) $L + \varnothing = L = \varnothing + L$;
4) $(L \cdot M) \cdot N = L \cdot (M \cdot N)$;
5) $L \cdot \{\varepsilon\} = L = \{\varepsilon\} \cdot L$;
6) $(L + M) \cdot N = (L \cdot N) + (M \cdot N)$;
7) $N \cdot (L + M) = (N \cdot L) + (N \cdot M)$;
8) $L \cdot \varnothing = \varnothing = \varnothing \cdot L$.

Доказательство. Проверим, например, шестое свойство (*правой дистрибутивности*). Если $\sigma \in (L + M) \cdot N$, то найдутся $\tau \in L + M$ и $\rho \in N$, т. ч. $\sigma = \tau\rho$. Если, скажем, $\tau \in L$, то $\sigma \in L \cdot N \subseteq L \cdot N + M \cdot N$. Обратно, пусть $\sigma \in L \cdot N + M \cdot N$. Без ограничения общности, $\sigma \in L \cdot N$, т. е. $\sigma = \tau\rho$ для некоторых $\tau \in L \subseteq L + M$ и $\rho \in N$. $\square$

Замечание 2.3.26. Мы получили, что множество языков над алфавитом A с операциями $+$ и $\cdot$, «нулем» $\varnothing$ и «единицей» $\{\varepsilon\}$ образует *полукольцо* (т. е. полугруппу с нейтральными элементами по сложению и по умножению, коммутативную для сложения, удовлетворяющую также свойствам 6–8 — подобно натуральным числам с обыкновенными $+$, $\cdot$, 0 и 1). В отличие от натуральных чисел, сложение в полукольце языков *идемпотентно*: $L + L = L$. Также наше полукольцо, если $|A| \geqslant 2$, некоммутативно по умножению: $\{0\} \cdot \{1\} = \{01\} \neq \{1\} \cdot \{0\}$.

Пример 2.3.27. Покажем, что в полукольце языков для умножения не выполнен правый закон сокращения: из $L \cdot N = M \cdot N$, вообще говоря, не следует $L = M$.

Пусть $0, 1 \in A$, $N = \{0,1\}^*$, $L = \{\varepsilon\}$ и $M = \{0, 1, \varepsilon\}$. Очевидно, $M \cdot N \subseteq N = L \cdot N$. Обратно, допустим, что $\sigma \in N$. Если $\sigma = \varepsilon$, то $\sigma = \varepsilon\varepsilon \in M \cdot N$. Иначе $\sigma = 0\tau$ или $\sigma = 1\tau$ для некоторого $\tau \in N$. Вновь $\sigma \in M \cdot N$. Итак, $L \cdot N = M \cdot N$.

Упражнение 2.3.28. Выполнены ли законы сокращения для сложения? Левый закон для умножения?

Положив $L^0 = \{\varepsilon\}$ и $L^{k+1} = L^k \cdot L$ для всех $k \in \mathbb{N}$, легко получить следующее утверждение.

Лемма 2.3.29. *Для всех $L \subseteq A^*$ и $k, l \in \mathbb{N}$ верно:*

1) $L^k \cdot L^l = L^{k+l}$;

2) $L^k \cdot L^l = L^l \cdot L^k$.

Помимо сложения и умножения, часто рассматривают операции *итерации* (или *звездочки Клини*) и *положительной итерации* языка, соответственно полагая $L^* = \bigcup_{n\in\mathbb{N}} L^n$ и $L^+ = \bigcup_{n\in\mathbb{N}_+} L^n$. Та и другая задают функции $\mathcal{P}(A^*) \to \mathcal{P}(A^*)$.

Замечание 2.3.30. Педантичный читатель понимает, что «звездочка» в обозначениях итерации и множества всех слов над данным алфавитом должна иметь *разный* смысл. Но *вдумчивый* читатель заметит, что «омонимия» не случайна, и эти обозначения хорошо согласованы: если отождествить алфавит A со множеством однобуквенных слов над ним, итерация этого языка, очевидно, даст всевозможные слова над A. Аналогично, результат A^n n-кратной конкатенации такого языка с самим собой окажется множеством $A^{\underline{n}}$ всех слов длины n.

Пример 2.3.31. Пусть $A = \{0, 1\}$ и $L = \{00, 01, 10, 11\}$. Тогда $L^* = \{\sigma \in A^* \mid 2 \,|\, |\sigma|\}$.

Лемма 2.3.32. *Для всех $L, M \subseteq A^*$ верно:*

1) $L \subseteq L^*$;

2) $L \subseteq M \Longrightarrow L^* \subseteq M^*$;

3) $(L^*)^* = L^*$.

Доказательство. Очевидно, $L = L^1 \subseteq L^*$. Если $L \subseteq M$, индукцией по n легко установить $L^n \subseteq M^n$, откуда $L^* \subseteq M^*$. Также индукцией по n докажем $(L^*)^n \subseteq L^*$, откуда вытекает $(L^*)^* \subseteq L^*$. В самом деле, если $\sigma \in (L^*)^{n+1}$, то $\sigma = \tau\rho$, где $\tau \in (L^*)^n \subseteq L^*$ по предположению индукции и $\rho \in L^*$. Значит, $\tau \in L^k$ и $\rho \in L^l$ для некоторых $k, l \in \mathbb{N}$. Но тогда $\sigma \in L^k \cdot L^l = L^{k+l} \subseteq L^*$. □

Упражнение 2.3.33. Верны ли такие свойства для положительной итерации?

Примеры языков. Обратимся к содержательным примерам. Исследуем, скажем, какие употребляются *обозначения* для натуральных чисел.

Пример 2.3.34. Язык U *унарных записей* натуральных чисел есть множество $\{1\}^*$. В данном случае наделить наши обозначения смыслом очень просто. Именно, рассмотрим функцию $f\colon U \to \mathbb{N}$, т. ч. $f(\sigma) = |\sigma|$. Получаем $f(\varepsilon) = 0$ и $f(1111) = 4$. Мы понимаем число $f(\sigma)$ как *значение* выражения σ. Легко проверить, что f — биекция, а значит, каждое натуральное число имеет ровно одну унарную запись.

Перед нами наша первая модель синтаксиса и семантики некоторой системы обозначений. Функция f, отображающая обозначения в обозначаемые объекты, называется *интерпретацией* (языка U во множестве $\mathbb{N}$). При исследовании логики математическими средствами, к которому мы стремимся, подобные модели будут в изобилии.

Пример 2.3.35. Язык B *двоичных* (или *бинарных*) *записей* натуральных чисел есть множество $\{\sigma \in \underline{2}^+ \mid 0 \not\sqsubset \sigma\}$. Иначе говоря, языку принадлежат все те и только те непустые слова над $\underline{2}$, которые не начинаются с нуля или же совпадают с нулем. Мы не считаем выражения вроде 001 правильными двоичными записями, чтобы каждое число имело ровно одну запись.

Рекурсией по длине определяем функцию $f\colon \underline{2}^* \to \mathbb{N}$, т. ч. $f(\varepsilon) = 0$ и $f(\sigma a) = 2f(\sigma) + a$ для всех $\sigma \in \underline{2}^*$ и $a \in \underline{2}$. Например, $f(\varepsilon) = f(0) = f(000) = 0$ и $f(11) = 2f(1) + 1 = 3$. Убедимся, что $B \overset{g}{\sim} \mathbb{N}$, где $g = f \restriction B$.

Индукцией по $|\sigma|$ легко доказать, что $1 \sqsubseteq \sigma$ влечет $f(\sigma) \neq 0$. Если g не инъекция, то возьмем слово θ наименьшей длины, т. ч. $g(\theta) = g(\eta)$ для некоторого $\eta \neq \theta$. В частности, $|\theta| \leqslant |\eta|$. Поскольку $\varepsilon \notin B$, имеем $\theta = \sigma a$ и $\eta = \tau b$. Значит, $2f(\sigma) + a = 2f(\tau) + b$. Из соображений четности, $a = b$, откуда $f(\sigma) = f(\tau)$, причем $\sigma \neq \tau$.

Докажем теперь $\sigma, \tau \in B$, что противоречит выбору θ, ибо тогда $g(\sigma) = g(\tau)$ при $|\sigma| < |\theta|$. Итак, если $0 \sqsubseteq \sigma$, то $0 \sqsubset \theta$, что невозможно. Аналогично для τ. Остается еще случай $\sigma = \varepsilon$. Но тогда $f(\tau) = 0$, откуда $\tau(0) = 0$ или $\tau = \varepsilon$. Раз $0 \sqsubseteq \tau$ невозможно, остается $\tau = \varepsilon = \sigma$. Противоречие.

Проверим сюръективность g. В противном случае выберем наименьшее натуральное $n \notin \operatorname{rng} g$. Ясно, что $n > 1$, а значит, $n = 2m + 1$ или $n = 2m$, причем $0 < m < n$. Тогда $m = g(\sigma)$ для некоторого $\sigma \in B$ и соответственно $f(\sigma 1) = n$ или $f(\sigma 0) = n$. Остается убедиться, что эти, очевидно, непустые слова принадлежат B. Действительно, если $0 \sqsubset \sigma a$, то $0 \sqsubseteq \sigma$, откуда $\sigma = 0$. Но тогда $m = g(0) = 0$, что не так.

Пример 2.3.36. Язык D *десятичных записей* натуральных чисел над алфавитом «цифр» $\underline{10}$ (цифры мы отождествили с элементами множества $\underline{10}$) есть множество $\{\sigma \in \underline{10}^+ \mid 0 \not\sqsubset \sigma\}$.

Упражнение 2.3.37. Определите естественное биективное соответствие между десятичными записями и их значениями.

Пример 2.3.38. Язык N над алфавитом $\mathbb{N}$ состоит из всех однобуквенных слов, т. е. *почти* из натуральных чисел. Функция $\sigma \mapsto \sigma(0)$ задает интерпретацию языка N во множестве $\mathbb{N}$. Здесь в качестве обозначения натурального числа выступает *почти* оно само.

Такое положение вполне естественно для математики, но не для приложений: скажем, в программировании мы хотели бы выразить элементы *бесконечного* множества $\mathbb{N}$ с помощью *конечного* алфавита возможных состояний нашего вычислительного аппарата (положений костяшек счетов, символов в клетках тетрадного листа, содержимого ячеек памяти, и т. п.). В силу леммы 2.3.2, над конечным алфавитом достаточно слов для кодирования любого счетного языка. Поэтому бесконечные алфавиты необходимы лишь в контексте несчетных множеств.

Упражнение 2.3.39. Рассмотрим функцию $\varphi\colon \mathbb{N} \to \mathbb{N}$, для которой $\varphi(n) = f(n + 2)$, где f — последовательность Фибоначчи, и язык $F = \{\sigma \in \underline{2}^+ \mid 0 \not\sqsupset \sigma \text{ и } \forall i, k\ (\sigma(i) = \sigma(i + k) = 1 \Longrightarrow k \neq 1)\}$ (иначе говоря, не допускаются две единицы подряд и нули в конце слова, отличного от 0). Рекурсией по длине определим функцию $g\colon \underline{2}^* \to \mathbb{N}$,

т. ч. $g(\sigma) = \sum_{i<|\sigma|} \varphi(i) \cdot \sigma(i)$, т. е. сумму конечного множества чисел Фибоначчи, заданного σ.

Язык F и функция g представляют собой *фибоначчиеву систему счисления*. Убедитесь в этом, проверив $F \overset{g\restriction F}{\sim} \mathbb{N}$. (При доказательстве инъективности можно использовать лемму: сумма членов последовательности φ с наибольшим номером i, без повторов и подряд идущих членов, строго меньше числа $\varphi(i+1)$.)

Пусть $a \in A$. Рассмотрим функцию $|\cdot|_a \colon A^* \to \mathbb{N}$, т. ч.

$$|\sigma|_a = |\sigma^{-1}[\{a\}]| = |\{i \in \underline{|\sigma|} \mid \sigma(i) = a\}|$$

для всех $\sigma \in A^*$. Неформально говоря, эта функция возвращает *число вхождений* символа a в слово σ. Например, $|101|_1 = 2$.

Лемма 2.3.40. *Для всех $\sigma, \tau \in A^*$ верно $|\sigma\tau|_a = |\sigma|_a + |\tau|_a$.*

Доказательство. Пусть $|\sigma| = m$ и $|\tau| = n$. Имеем

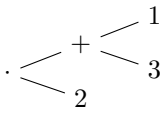
$$\{i \in \underline{m+n} \mid (\sigma\tau)(i) = a\} = \\ \{i \in \underline{m} \mid \sigma(i) = a\} \cup \{i \in \underline{m+n} \smallsetminus \underline{m} \mid \tau(i-m) = a\}.$$

Последние два множества не пересекаются, причем второе из них равномощно $\{i \in \underline{n} \mid \tau(i) = a\}$. Остается применить правило сложения. □

Упражнение 2.3.41. Определите функцию $|\cdot|_a$ рекурсией по длине и докажите эквивалентность нового определения исходному.

В математике и, скажем, языках программирования часто употребляются *скобки*. При этом обычно требуется, чтобы между числом открывающих и закрывающих скобок выполнялись некоторые соотношения, цель которых — обеспечить *однозначное* понимание выражения. Коль скоро мы желаем смоделировать язык математики, полезно изучить правила расстановки скобок.

Замечание 2.3.42. Скобки отражают *иерархию*, взаимную подчиненность частей обозначения, которая позволяет придать ему смысл. Например, в выражении $2 \cdot (3+1)$ скобки показывают, что умножение применяется *к результату* сложения, как бы «подчиняя» себе сложение. Таким образом, скобки возникают вследствие иерархичности интерпретации при линейности обозначений. Если отказаться от последней, например, изображая выражения в виде «деревьев»:



возможно обойтись без скобок. Такие деревья широко употребляются в информатике и лингвистике. С другой стороны, на примере употребления скобок видно, что любое конечное дерево легко закодировать словом конечного алфавита.

Заметим, наконец, что в случае, когда у каждой «операции» имеется фиксированное число «аргументов» (как в арифметике), легко и в линейных обозначениях обойтись без скобок: $\cdot\, 2 + 3\, 1$. В дальнейшем мы рассмотрим такую *польскую запись* подробнее.

Под «скобками», во избежание смешения с символами метаязыка, мы будем понимать элементы алфавита $\mathcal{B} = \{\langle, \rangle\}$. Определим функцию $b\colon \mathcal{B}^* \to \mathbb{Z}$ *скобочного итога*, полагая $b(\sigma) = |\sigma|_\langle - |\sigma|_\rangle$ для всех $\sigma \in \mathcal{B}^*$. Как видно из леммы 2.3.40, $b(\sigma\tau) = b(\sigma) + b(\tau)$.

Понятие скобочного итога легко распространить на слова в алфавитах, содержащих $\mathcal{B}$. Практический его смысл состоит в том, что в «правильно построенном выражении» — например, $(3{+}x){\cdot}(2{+}(y{+}(z)))$, но не $)3+((1+x)$ — скобки должны быть расставлены правильно: ни в каком префиксе закрывающих скобок не должно быть больше, чем открывающих, а во всем выражении должно быть поровну тех и других. Если оставить от «правильно построенного выражения» одни лишь скобки, получится *правильная скобочная последовательность*.

Пример 2.3.43. Язык R *правильных скобочных последовательностей* над алфавитом $\mathcal{B}$ есть множество

$$\{\sigma \in \mathcal{B}^* \mid b(\sigma) = 0 \text{ и } b(\tau) \geqslant 0 \text{ для всех } \tau \sqsubseteq \sigma\}.$$

Имеем $\varepsilon, \langle\rangle\langle\rangle, \langle\langle\rangle\rangle\langle\rangle\langle\rangle \in R$, однако $\langle\langle\langle, \langle\rangle\rangle\langle \notin R$.

Лемма 2.3.44. *Если $\sigma, \tau \in R$, то $\langle\sigma\rangle, \sigma\tau \in R$.*

Доказательство. Имеем $b(\langle\sigma\rangle) = b(\langle) + b(\sigma) + b(\rangle) = 1 + 0 - 1 = 0$ и $b(\sigma\tau) = b(\sigma) + b(\tau) = 0$.

Пусть $\rho \sqsubseteq \langle\sigma\rangle$, т. е. $\langle\sigma\rangle = \rho\tau'$. Тогда $\rho \sqsubset \langle$ или $\langle \sqsubseteq \rho$. В первом случае $\rho = \varepsilon$ и $b(\rho) = 0$. Во втором — имеем $\rho = \langle\rho'$, откуда $\rho'\tau' = \sigma\rangle$. Если теперь $\rho' \sqsubseteq \sigma$, то $b(\rho') \geqslant 0$ и $b(\rho) = 1 + b(\rho') > 0$. Если же $\sigma \sqsubset \rho'$, то $\rho' = \sigma\tau''$, причем $\tau'' \neq \varepsilon$. Получаем $\tau''\tau' = \rangle$, откуда $\tau'' = \rangle$. Имеем $\rho' = \sigma\rangle$ и $\rho = \langle\sigma\rangle$. Значит, $b(\rho) = 0$.

Допустим $\rho \sqsubseteq \sigma\tau$. Имеем $\rho \sqsubseteq \sigma$, откуда $b(\rho) \geqslant 0$, или же $\sigma \sqsubset \rho$. В последнем случае $\rho = \sigma\rho'$; тогда $\sigma\tau = \rho\tau' = \sigma\rho'\tau'$, откуда $\tau = \rho'\tau'$. Итак, $\rho' \sqsubseteq \tau$. Значит, $b(\rho) = b(\sigma) + b(\rho') = b(\rho') \geqslant 0$. □

Оказывается, полученные *достаточные* условия принадлежности языку R *определяют* его в некотором весьма естественном смысле. Действительно, мы могли бы сказать, что язык R есть такое подмножество $X \subseteq \mathcal{B}^*$, что:

1) $\varepsilon \in X$;

2) если $\sigma, \tau \in X$, то $\langle\sigma\rangle, \sigma\tau \in X$;

3) никакое слово, кроме образованных по предыдущим правилам, в X не лежит.

Такого рода *индуктивные определения*, имеющие широчайшее употребление, мы исследуем в следующем разделе. В частности, мы уточним весьма туманный третий пункт и строго докажем равносильность нового определения R исходному.

Пока же установим некоторые *необходимые* условия принадлежности R. Во-первых, каждая непустая правильная последовательность начинается с открывающей скобки и оканчивается закрывающей.

Лемма 2.3.45. *Для любого $\sigma \in R \setminus \{\varepsilon\}$ найдется $\tau \in \mathcal{B}^*$, т. ч. $\sigma = \langle\tau\rangle$.*

Доказательство. Поскольку $|\sigma| \neq 0$, определен элемент $\sigma(0) \in \mathcal{B}$. Если $\sigma(0) = \rangle$, то $\rangle \sqsubseteq \sigma$, хотя $b(\rangle) < 0$. Значит, $\sigma(0) = \langle$. Однако $b(\langle) \neq 0$, поэтому $|\sigma| = n > 1$. Имеем $0 = b(\sigma) = b(\sigma(0)\ldots\sigma(n-2)) + b(\sigma(n-1))$. Так как $\sigma(0)\ldots\sigma(n-2) \sqsubseteq \sigma$, первое слагаемое неотрицательно, а значит, второе неположительно. Поэтому случай $\sigma(n-1) = \langle$ невозможен; необходимо $\sigma(n-1) = \rangle$. □

Во-вторых, если потребовать, чтобы правильная последовательность σ не имела правильного собственного начала (помимо ε), последняя лемма может быть усилена до более полезного утверждения.

Лемма 2.3.46. *Для любого $\sigma \in R \setminus \{\varepsilon\}$, если ни для какого $\rho \in R \setminus \{\varepsilon\}$ не верно $\rho \sqsubset \sigma$, то найдется $\tau \in R$, т. ч. $\sigma = \langle\tau\rangle$.*

Доказательство. Заметим, что для всех непустых $\rho \sqsubset \sigma$ верно $b(\rho) > 0$. В самом деле, пусть не так. Для всех $\rho' \sqsubseteq \rho$ верно $\rho' \sqsubseteq \sigma$ и $b(\rho') \geqslant 0$. Учитывая $b(\rho) = 0$, получаем $\rho \in R$.

В силу леммы 2.3.45, $\sigma = \langle\tau\rangle$ для некоторого $\tau \in \mathcal{B}^*$. Покажем, что $\tau \in R$. Ясно, что $b(\tau) = b(\sigma) - 1 - (-1) = 0$. Пусть $\tau' \sqsubseteq \tau$. Тогда $\langle\tau' \sqsubseteq \langle\tau \sqsubset \sigma$, откуда $b(\langle\tau') = 1 + b(\tau') > 0$. Поэтому $b(\tau') \geqslant 0$. $\square$

§ 2.4. Индуктивные определения

Выше мы аккуратно обосновали процедуру рекурсивного определения функций натурального аргумента, хорошо знакомую читателю. Теперь же мы рассмотрим «рекурсивную» процедуру задания подмножества данного множества, называемую *индуктивным определением*, и сведем ее к нашим «основным способам задания множеств».

Такого рода определения уже встречались читателю в предыдущем разделе при обсуждении правильных скобочных последовательностей. Они весьма многочисленны в «дискретных» математических науках (алгебра, логика, комбинаторика, информатика и пр.) вообще и будут часто встречаться далее в нашем курсе. Начнем с примеров.

Пример 2.4.1. Множество $E \subseteq \mathbb{N}$ четных натуральных чисел, как известно, выделяется следующими равносильными свойствами:

$$n \in E \iff 2 \,|\, n \iff \exists m\ n = 2m \iff \exists m\ n = m + m.$$

Из свойств сложения и умножения видно, что $0 \in E$ и для любых $n, m \in E$ верно $n+2 \in E$ и $n+m \in E$. Оказывается, эти свойства можно положить в основу другого определения четности. Именно, рассмотрим множества $X \subseteq \mathbb{N}$, т. ч.

$$0 \in X \quad \text{и} \quad \forall n\,(n \in X \Longrightarrow n + 2 \in X).$$

Существует несколько таких множеств: в частности, подходят E и $\mathbb{N}$. Пусть $\mathcal{X} \subseteq P(\mathbb{N})$ есть множество всех подходящих X. Положим $E' = \cap\mathcal{X}$. Поскольку $\mathcal{X} \neq \varnothing$, для каждого $n \in \mathbb{N}$ имеем

$$n \in E' \iff \forall X \in \mathcal{X}\ n \in X.$$

Получаем $E' \subseteq X$ для каждого $X \in \mathcal{X}$. Раз $0 \in X$ для всех $X \in \mathcal{X}$, то $0 \in E'$. Для всех $X \in \mathcal{X}$ из $n \in X$ следует $n + 2 \in X$; поэтому $n \in E'$ влечет $n + 2 \in E'$. Значит, $E' \in \mathcal{X}$. Таким образом, множество E' является $\subseteq$-наименьшим подходящим.

Убедимся, что $E' = E$. Поскольку $E \in \mathcal{X}$, имеем $E' \subseteq E$. Обратно, предположим противное. Пусть $n = \min(E \smallsetminus E')$. Раз $0 \in E'$ и $1 \notin E$, то $n \geqslant 2$, т. е. $n = m + 2$. По минимальности n, число $m \in E$ должно принадлежать E'. Но тогда и $n = m + 2 \in E' \in \mathcal{X}$. Противоречие.

Упражнение 2.4.2. Пусть E'' есть наименьшее $X \subseteq \mathbb{N}$, т. ч.

$$\{0,2\} \subseteq X \quad \text{и} \quad \forall n \forall m\,(n,m \in X \Longrightarrow n+m \in X).$$

Убедитесь, что такое E'' действительно существует и что $E = E''$.

Упражнение 2.4.3. Выясните, как устроены все подходящие X из определений множеств E' и E''.

«Индуктивное определение» множества четных чисел не кажется ни естественным, ни особенно полезным (притом что сложение уже определено). Однако многие важные объекты задаются такими определениями естественным образом.

Пример 2.4.4. Пусть R — отношение на множестве A. *Транзитивным замыканием* $\hat{R}$ отношения R называется $\subseteq$-наименьшее отношение $Q \subseteq A^2$, т. ч.

$$R \subseteq Q \quad \text{и} \quad \forall x \forall y \forall z\,\big((xQy \text{ и } yQz) \Longrightarrow xQz\big).$$

Иными словами, $\hat{R}$ есть наименьшее транзитивное надмножество отношения R. Пусть $\mathcal{Q} \subseteq \mathcal{P}(A^2)$ будет множество всех транзитивных надмножеств R. Очевидно, $A^2 \in \mathcal{Q} \neq \varnothing$. Тогда легко проверить, что $\hat{R} = \cap\mathcal{Q}$.

Неформально говоря, транзитивное замыкание получится, если добавить к R все те и только те стрелки, которых не хватает для транзитивности. Например, если $R = \{(n, n+1) \in \mathbb{N}^2 \mid n \in \mathbb{N}\}$, то $\hat{R} = <$.

Добавлять стрелки можно «по шагам», однако новые стрелки создают новые нарушения транзитивности и влекут очередные шаги. Сейчас мы убедимся, что «шагать вдоль $\mathbb{N}$» достаточно, чтобы добавить *все* нужные стрелки.

Пусть $R \subseteq A^2$. Положим $(R)_1 = R$ и $(R)_{n+1} = (R)_n \circ R$ при всех $n > 0$. Индукцией легко доказать, что $(R)_m \circ (R)_n = (R)_{m+n}$.

Лемма 2.4.5. $\hat{R} = \bigcup_{n \in \mathbb{N}_+} (R)_n$.

Доказательство. Обозначим $U = \bigcup_{n \in \mathbb{N}_+} (R)_n \subseteq A^2$. Очевидно, $R \subseteq U$. Если $(x,y), (y,z) \in U$, то $x(R)_m y$ и $y(R)_n z$ при некоторых $m, n \in \mathbb{N}$. Тогда $(x,z) \in (R)_n \circ (R)_m = (R)_{m+n} \subseteq U$. Поэтому $U \in \mathcal{Q}$, откуда $\hat{R} = \cap\mathcal{Q} \subseteq U$. Обратно. Пусть $Q \in \mathcal{Q}$. Индукцией по n докажем, что $(R)_n \subseteq Q$. При $n = 1$ это ясно. Если $(R)_n \subseteq Q$, то $(R)_{n+1} = (R)_n \circ R \subseteq$ $\subseteq Q \circ Q \subseteq Q$ в силу транзитивности Q. Следовательно, $U \subseteq Q$ при всех

$Q \in \mathcal{Q}$, откуда $U \subseteq \cap\mathcal{Q} = \hat{R}$. $\square$

Как мы вскоре увидим, подобное «построение по шагам» возможно для любого индуктивного определения.

Упражнение 2.4.6. Определите «симметричное замыкание» отношения $R \subseteq A^2$ и выразите его через R с помощью операций над множествами и отношениями — в «конечном» виде, в отличие от транзитивного замыкания.

Индуктивные определения (и родственные им *порождающие грамматики*, о которых можно прочесть в [11]) являются естественными способами задания языков — особенно, не столь простых, как те, что мы смогли определить и без них.

Пример 2.4.7. Определим множество B' как $\subseteq$-наименьшее такое $X \subseteq \underline{2}^*$, что

$$\{0,1\} \subseteq X \quad \text{и} \quad \forall\sigma\,\big(\sigma \in X \setminus \{0\} \Longrightarrow \sigma 0, \sigma 1 \in X\big).$$

Как и в предыдущих примерах, $B' = \cap\mathcal{X}$, где $\mathcal{X}$ есть непустое (ибо $\underline{2}^* \in \mathcal{X}$) множество всех подходящих X. Ожидаемо, мы хотели бы доказать, что B' есть множество B двоичных записей натуральных чисел. Но пока отложим это.

Приведенное определение отражает естественный принцип образования новых двоичных записей из имеющихся: к любой ненулевой записи можно приписать справа еще один разряд.

Пример 2.4.8. Определим множество S как $\subseteq$-наименьшее такое $X \subseteq \mathcal{B}^*$, что

$$\varepsilon \in X \quad \text{и} \quad \forall\sigma\forall\tau\,\big(\sigma,\tau \in X \Longrightarrow \langle\sigma\rangle, \sigma\tau \in X\big).$$

Очевидно, это и есть обещанное индуктивное определение множества R всех правильных скобочных последовательностей. Доказательство равенства $R = S$ мы также пока отложим.

Как понимает читатель, расплывчатое требование о том, что язык не содержит «ничего лишнего», превратилось в условие, что он является $\subseteq$-наименьшим.

Пример 2.4.9. Определим язык *Ar замкнутых арифметических термов*, состоящий из выражений вроде $\langle\langle 3+2\rangle \cdot 5\rangle$, где натуральные числа сами выступают своими обозначениями. Итак, Ar есть наименьшее $X \subseteq (\mathbb{N} \cup \{+, \cdot, \langle, \rangle\})^*$, т. ч.

$$\forall n \in \mathbb{N}\ n \in Ar \quad \text{и} \quad \forall\sigma\forall\tau\,\big(\sigma,\tau \in X \Longrightarrow \langle\sigma+\tau\rangle, \langle\sigma\cdot\tau\rangle \in X\big).$$

«Неиндуктивное» определение столь естественного языка уже не кажется очевидным.

Одним из достоинств индуктивных определений являются простые и наглядные доказательства принадлежности элемента определяемому множеству. В самом деле, достаточно привести *построение* этого элемента по правилам нашего определения. Например,

$$5 \in Ar;\ 4 \in Ar;\ \langle 5+4\rangle \in Ar;\ \langle 4\cdot\langle 5+4\rangle\rangle \in Ar.$$

Общее понятие. Исследуем теперь индуктивные определения в общем виде. Как показали примеры, определение выделяет наименьшее подмножество X данного множества U, удовлетворяющее условиям вида «некоторое b принадлежит X» и «если некоторые $a_1,\dots,a_n$ принадлежат X, то и $b\in X$».

Эти условия удобно формализовать с помощью функций нескольких аргументов, которые ставят b в соответствие набору $a_1,\dots,a_n$. Если же элемент b «исходный», т. е. включается в X безусловно, используются функции нуля аргументов (см. замечание 2.1.16). Может быть и так, что b назначается не любым наборам $a_1,\dots,a_n$, но только некоторым: скажем, в определении транзитивного замыкания $(x,y)\in Q$ и $(w,z)\in Q$ влечет $(x,z)\in Q$ лишь при $y=w$. Самым наглядным решением будет рассмотреть *частичные* функции. Однако это не очень удобно технически, и, как увидит читатель, мы обойдемся функциями тотальными.

Итак, пусть U — некоторое непустое множество. Назовем (*финитарным*) *индуктивным определением над* U любое множество $\mathcal{F}$, т. ч. для каждого $f\in\mathcal{F}$ верно $f\colon U^n\to U$ при некотором $n\in\mathbb{N}$.

Замечание 2.4.10. «Финитарность» означает, что каждое b получается лишь из *конечного* набора a_i. Именно такие определения можно моделировать с помощью функций нескольких аргументов из U. В нашем курсе никакие другие индуктивные определения рассматриваться не будут.

Множество $X\subseteq U$ называется *замкнутым* относительно определения $\mathcal{F}$, если для каждой функции $f\in\mathcal{F}\cap U^{U^n}$ и всех наборов $\vec{u}=(u_0,\dots,u_{n-1})\in U^n$ из $\vec{u}\in X^n$ следует $f(\vec{u})\in X$. В частности, при $n=0$ имеем $\vec{u}=\varnothing\in X^0$, а значит, для функции-константы $f\colon\{\varnothing\}\to U$ должно быть $f(\varnothing)\in U$. В свете замечания 2.1.16, можно считать $f=f(\varnothing)$.

Замечание 2.4.11. Согласно замечаниям 1.2.62 и 1.4.21, при фиксированном $U\neq\varnothing$ число n членов набора $\vec{u}$ и аргументов функции f

определено однозначно. Запись $f^{(n)}$ означает, что у f ровно n аргументов, и может считаться синонимом[9] записи f.

Если нас число n не интересует, будем просто писать $f \in \mathcal{F}$ и даже $\vec{u} \in U$, считая, что n выбирается единственным допустимым образом.

Если $f(\vec{u}) = v \in U$, компоненты набора $\vec{u}$ называются *образующими* элемента v, а сама функция f — *правилом образования* этого элемента.

Для каждого $Y \subseteq U$ положим

$$\mathcal{X}(Y) = \{X \in \mathcal{P}(U) \mid Y \subseteq X \text{ и } X \text{ замкнутое относительно } \mathcal{F}\}.$$

Соответственно, $\mathcal{X} = \mathcal{X}(\varnothing)$ есть просто множество всех $\mathcal{F}$-замкнутых множеств. Смысл параметра Y в том, что бывает удобно немного варьировать индуктивное определение, добавляя новые «исходные» элементы.

Лемма 2.4.12. *Для каждого $Y \subseteq U$ существует единственный $\subseteq$-наименьший элемент $\mathcal{F}(Y)$ множества $\mathcal{X}(Y)$, причем $\mathcal{F}(Y) = \cap\mathcal{X}(Y)$.*

Доказательство. Единственность наименьшего элемента очевидна. Покажем, что множество $\mathcal{F}(Y) = \cap\mathcal{X}(Y)$ является таковым. Ясно, что $U \in \mathcal{X}(Y) \neq \varnothing$. Поэтому для всех $u \in U$ верно

$$u \in \mathcal{F}(Y) \iff \forall X \in \mathcal{X}(Y)\ u \in X.$$

Очевидно, $\mathcal{F}(Y) \subseteq X$ для всех $X \in \mathcal{X}(Y)$. Остается проверить $\mathcal{F}(Y) \in \in \mathcal{X}(Y)$. Поскольку $Y \subseteq X$ для всех $X \in \mathcal{X}(Y)$, имеем $Y \subseteq \mathcal{F}(Y)$. Предположим, что $f \in \mathcal{F}$ и $\vec{u} \in \mathcal{F}(Y)$. Но тогда $\vec{u} \in X$ для всех $X \in \mathcal{X}(Y)$. Каждое X является $\mathcal{F}$-замкнутым, а значит, содержит и $f(\vec{u})$. Поэтому $f(\vec{u}) \in \mathcal{F}(Y)$. □

Мы говорим, что множество $\mathcal{F}(Y)$ *порождается множеством Y под действием индуктивного определения $\mathcal{F}$*, а множество $\mathcal{F}(\varnothing)$ просто *порождается индуктивным определением $\mathcal{F}$*. Собственно говоря, $\mathcal{F}(\varnothing)$ и есть множество, задаваемое определением $\mathcal{F}$.

Замечание 2.4.13. Любое индуктивное определение можно избавить от констант, поместив их в Y. Но это не всегда оправдано с содержательной точки зрения: константы могут представлять «непременные» элементы определяемой совокупности.

[9] Обозначения 6 и *наименьшее натуральное число, равное сумме своих меньших делителей,* суть синонимы, ибо имеют одинаковое значение, хотя каждое дает некоторую новую информацию об этом значении.

Упражнение 2.4.14. Докажите, что для каждого $A \subseteq U$ существует индуктивное определение $\mathcal{F}$ над U, т. ч. $A = \mathcal{F}(\varnothing)$.

Пример 2.4.15. В нашей модели индуктивное определение множества четных чисел E' примет вид $\mathcal{F}' = \{f_1^{(0)}, f_2^{(1)}\}$, где $f_1(\varnothing) = 0$ и $f_2(n) = n + 2$ при всех $n \in \mathbb{N}$. Соответственно, определение множества E'' есть $\mathcal{F}'' = \{0^{(0)}, 2^{(0)}, +^{(2)}\}$. Понятно, что $\mathcal{F}'(\varnothing) = E = \mathcal{F}''(\varnothing)$.

Упражнение 2.4.16. Докажите, что $\mathcal{F}'(Y) = \mathcal{F}''(Y)$ для всех $Y \subseteq \mathbb{N}$.

Пример 2.4.17. Наше индуктивное определение транзитивного замыкания отношения $R \subseteq A^2$ есть $\mathcal{F}_R = \{t^{(2)}\} \cup \{(x, y)^{(0)} \mid (x, y) \in R\}$ над A^2, где для всех $(x, y), (w, z) \in A^2$ имеем

$$t((x, y), (w, z)) \quad = \quad \begin{cases} (x, z), & \text{если } y = w; \\ (x, y) & \text{иначе.} \end{cases}$$

Читатель видит изящное решение проблемы частичных функций: наша t добавляет стрелку (x, z), если ее аргументы в ней нуждаются, и просто возвращает первый аргумент в противном случае. При этом, очевидно, ничего лишнего во множество $\mathcal{F}(\varnothing)$ не добавляется.

В определении $\mathcal{F}_R$ присутствуют константы для каждой пары из R — быть может, бесконечно много констант. В данном случае от них уместно избавиться. Рассмотрим определение $\mathcal{F} = \{t^{(2)}\}$ над A^2. Тогда, очевидно, $\mathcal{F}(R) = \mathcal{F}_R(\varnothing) = \hat{R}$ для всех $R \subseteq A^2$. Таким образом, определение $\mathcal{F}$ с помощью параметра задает транзитивные замыкания всех вообще отношений на A.

Пример 2.4.18. Множество двоичных записей B' порождается определением $\{0^{(0)}, 1^{(0)}, f_0^{(1)}, f_1^{(1)}\}$ над множеством $\underline{2}^*$, где

$$f_i(\sigma) \quad = \quad \begin{cases} \sigma i, & \text{если } \sigma \neq 0; \\ \sigma & \text{иначе} \end{cases}$$

при всех $\sigma \in \underline{2}^*$.

Пример 2.4.19. Язык S над алфавитом $\mathcal{B}$ порождается индуктивным определением $\mathcal{S} = \{\varepsilon^{(0)}, p^{(1)}, c^{(2)}\}$ над $\mathcal{B}^*$, где $p(\sigma) = \langle\sigma\rangle$ и $c(\sigma, \tau) = \sigma\tau$ для всех $\sigma, \tau \in \mathcal{B}^*$.

Пример 2.4.20. Рассмотрим определение $\mathcal{F} = \{+^{(2)}\}$ над множеством $\mathbb{Z}$. Легко видеть, что $\mathcal{F}(\{1\}) = \mathbb{N}_+$, $\mathcal{F}(\{1, -1\}) = \mathbb{Z}$ и $\mathcal{F}(\{2, -2\}) = 2\mathbb{Z}$ (все четные целые).

Рассмотрим наименьшее по модулю число $n \in 2\mathbb{Z} \setminus \mathcal{F}(\{2,-2\})$. Очевидно, $n \neq 0 = 2+(-2) \in \mathcal{F}(\{2,-2\})$. Если $n > 0$, то $|n-2| < |n|$, а значит, $n-2 \in \mathcal{F}(\{2,-2\})$ и $n = (n-2)+2 \in \mathcal{F}(\{2,-2\})$. Аналогично получаем противоречие при $n < 0$. Следовательно, $2\mathbb{Z} \subseteq \mathcal{F}(\{2,-2\})$.

Чтобы установить $\mathcal{F}(\{2,-2\}) \subseteq 2\mathbb{Z}$, достаточно проверить, что множество $2\mathbb{Z}$ замкнуто относительно $\mathcal{F}$ и что $\{2,-2\} \subseteq 2\mathbb{Z}$. Последнее очевидно; столь же очевидно, что $m, n \in 2\mathbb{Z}$ влечет $m+n \in 2\mathbb{Z}$.

Пример 2.4.21. Рассмотрим определение $\mathcal{F} = \{1^{(0)}, +^{(2)}, \cdot^{(2)}, f^{(1)}, g^{(1)}\}$, где $f(x) = -x$, $g(x) = 1/x$ при $x \neq 0$ и $g(0) = 0$, над множеством $\mathbb{R}$. Нетрудно проверить, что $\mathcal{F}(\varnothing) = \mathbb{Q}$. (Доказываем $\mathbb{N} \subseteq \mathcal{F}(\varnothing)$ и замечаем, что всякое рациональное число имеет вид $\pm m \cdot 1/n$, где $m, n \in \mathbb{N}$.)

Множество $\mathcal{F}(\{\sqrt{2}\})$ обозначают символом $\mathbb{Q}(\sqrt{2})$. Это $\subseteq$-наименьшее включающее $\mathbb{Q}$ и замкнутое относительно сложения, умножения, вычитания и деления на ненулевое число подмножество $\mathbb{R}$, в котором уравнение $x^2 = 2$ имеет решение. Такого рода *расширения поля рациональных чисел* играют важную роль в алгебре.

Упражнение 2.4.22. Докажите, что $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Индукция по построению. В двух последних примерах мы применили метод рассуждений, называемый *индукцией по построению* и состоящий в следующем.

Теорема 2.4.23 (индукция по построению)**.** *Пусть $\mathcal{F}$ есть индуктивное определение над множеством U и $Y \subseteq U$. Тогда если множество Z является $\mathcal{F}$-замкнутым и $Y \subseteq Z$, то $\mathcal{F}(Y) \subseteq Z$.*

Доказательство. Поскольку $Z \in \mathcal{X}(Y)$, имеем $\mathcal{F}(Y) = \cap\mathcal{X}(Y) \subseteq Z$. □

Индукция по построению — основной способ доказать, что элементы порожденного индуктивным определением $\mathcal{F}$ множества удовлетворяют какому-либо свойству φ. В самом деле, достаточно проверить, что это свойство наследуется с образующих по каждому правилу образования, т. е. если $\varphi(u_i)$ для всех i, то $\varphi(f(\vec{u}))$ при каждом $f \in \mathcal{F}$.

Пример 2.4.24. Пусть отношение $R \subseteq A^2$ симметрично. Тогда его транзитивное замыкание $\hat{R}$ также симметрично.

Мы докажем, что любая пара $(x,y) \in \hat{R}$ такова, что $(y,x) \in \hat{R}$. Иначе говоря, $\hat{R} \subseteq Z = \{(x,y) \in A^2 \mid (y,x) \in \hat{R}\}$. Имеем $\hat{R} = \mathcal{F}(R)$, где $\mathcal{F} = \{t\}$. По условию, $R^{-1} \subseteq R \subseteq \hat{R}$, а значит, $R \subseteq Z$. Допустим, $(x,y),(w,z) \in Z$. Если $y \neq w$, то $t((x,y),(w,z)) = (x,y) \in Z$. Пусть $y = w$. Имеем $(y,x),(z,y) \in \hat{R}$, откуда $(z,x) \in \hat{R}$ по транзитивности.

Значит, $t((x,y),(y,z)) = (x,z) \in Z$, и множество Z замкнуто относительно $\mathcal{F}$. Применяя индукцию по построению, получаем $\hat{R} \subseteq Z$.

Упражнение 2.4.25. Выведите это утверждение из леммы 2.4.5. Обратите затем внимание, что лемма использует принцип индукции.

Индукция по построению дает способ доказать, что нечто *не* принадлежит множеству $\mathcal{F}(Y)$.

Пример 2.4.26. Имеем $\rangle \notin S = \mathcal{S}(\varnothing)$. В самом деле, рассмотрим множество $S' = S \setminus \{\rangle\}$. Очевидно, $\varepsilon \in S'$. Если $\sigma, \tau \in S' \subseteq S$, то $\sigma\tau \in S$ по $\mathcal{S}$-замкнутости S. Допустим, что $\sigma\tau = \rangle$. Тогда, из соображений длины, $\sigma = \rangle$ или $\tau = \rangle$, что противоречит $\sigma, \tau \in S'$. Значит, $c(\sigma,\tau) = \sigma\tau \in S'$.

Вновь, если $\sigma \in S'$, то $\langle\sigma\rangle \in S$, причем $\langle\sigma\rangle = \rangle$ влечет $\langle = \rangle$, а значит, $p(\sigma) \in S'$. Итак, множество S' является $\mathcal{S}$-замкнутым, откуда $S \subseteq S \setminus \{\rangle\}$ и $\rangle \notin S$.

Упражнение 2.4.27. Докажите, что $000 \notin B'$.

Упражнение 2.4.28. Докажите, что приведенные выше индуктивное и «неиндуктивное» определения множества двоичных записей натуральных чисел равносильны, т. е. что $B = B'$.

Замечание 2.4.29. Вдумчивый читатель, возможно, удивлен тем, как легко обосновать индукцию по построению — в частности, в доказательстве нами никак не использовался принцип математической индукции. Более того, при формальном определении натуральных чисел *сам* принцип индукции естественно доказать «индукцией по построению».

Точнее, множество $\mathbb{N}$ можно определить «индуктивно»: как пересечение всех множеств, содержащих $0 = \varnothing$ и замкнутых относительно операции $x \mapsto x + 1 = x \cup \{x\}$. Тогда любое такое замкнутое множество (в том числе и любое замкнутое подмножество $\mathbb{N}$, как в принципе математической индукции) обязано включать $\mathbb{N}$.

Чтобы эта конструкция сработала, остается только постулировать существование хотя бы одного замкнутого множества (ведь в «индуктивном определении» $\mathbb{N}$ не указано никакого U). Соответствующее утверждение называют *аксиомой бесконечности*[10]. Вот точная формулировка аксиомы:

[10] В самом деле, все нами явно и не явно использованные утверждения, не зависящие от существования множества $\mathbb{N}$ *всех* натуральных чисел, имели бы место и в мире, где есть только конечные множества.

Существует множество A, т. ч. $\varnothing \in A$ и для всех x из $x \in A$ следует $x \cup \{x\} \in A$.

Построения. Выше мы уже заметили, что элементы множества, порожденного индуктивным определением, можно «строить по шагам». С другой стороны, «индукция по построению» также намекает на некое «построение». Внесем ясность.

Пусть $\mathcal{F}$ есть индуктивное определение над множеством U и $Y \subseteq U$. Конечная последовательность $d \in U^*$ называется *$\mathcal{F}$-построением над Y*, если для каждого $i \in \underline{|d|}$ верно $d(i) \in Y$ или

$$\exists f^{(n)} \in \mathcal{F}\ \exists (j_0, \ldots, j_{n-1}) \in \underline{i}^n \quad d(i) = f(d(j_0), \ldots, d(j_{n-1})).$$

Если еще $u = d(|d|-1)$, то d есть *$\mathcal{F}$-построение элемента $u \in U$ над Y*. Иными словами, построение u оканчивается этим элементом, а каждый член построения принадлежит Y или получается из некоторых предшествующих с помощью одного из правил образования.

В таком случае пишем $Y \Rightarrow^d_{\mathcal{F}} u$. Будем также писать $Y \Rightarrow^d_{\mathcal{F}}$, если d есть некоторое $\mathcal{F}$-построение над Y. Назовем $\mathcal{F}$-построение над $\varnothing$ просто *$\mathcal{F}$-построением*; соответственно, пишем $\Rightarrow^d_{\mathcal{F}} u$. Наконец, мы пишем $Y \Rightarrow_{\mathcal{F}} u$, если у элемента u есть некоторое $\mathcal{F}$-построение над Y.

Пример 2.4.30. Для определения $\mathcal{S}$ языка S последовательность

$$\varepsilon,\ \langle\rangle,\ \langle\langle\rangle\rangle,\ \langle\langle\rangle\rangle\langle\rangle,\ \langle\rangle,\ \langle\langle\rangle\rangle\langle\rangle\rangle$$

является построением слова $\langle\langle\rangle\rangle\langle\rangle\rangle$. Видно, что это не единственное и даже не кратчайшее построение, поскольку предпоследний его член можно убрать.

Для определения транзитивного замыкания $\hat{R} = <$ отношения $R = \{(n, n+1) \in \mathbb{N}^2 \mid n \in \mathbb{N}\}$ последовательность

$$(3,4),\ (4,5),\ (1,2),\ (3,5),\ (2,3),\ (1,3),\ (1,5)$$

есть построение элемента $(1,5)$.

Упражнение 2.4.31. Докажите, что для любых $\mathcal{F}$, Y и u, если $Y \Rightarrow^d_{\mathcal{F}} u$, то для всякого $n > |d|$ найдется d', т. ч. $Y \Rightarrow^{d'}_{\mathcal{F}} u$ и $|d'| = n$. Иначе говоря, построение всегда можно искусственно удлинить.

Упражнение 2.4.32. Докажите, что если $Y \Rightarrow^{d'}_{\mathcal{F}}$, $Y \Rightarrow^{d''}_{\mathcal{F}} u$ и $d \sqsubseteq d'$, то $Y \Rightarrow^{d'd''}_{\mathcal{F}} u$ и $Y \Rightarrow^d_{\mathcal{F}}$. То есть любой префикс построения и конкатенация построений суть построения.

Теорема 2.4.33. *Для любого $u \in U$ имеет место $u \in \mathcal{F}(Y)$ тогда и только тогда, когда $Y \Rightarrow_{\mathcal{F}} u$.*

Доказательство. Для включения $\mathcal{F}(Y) \subseteq Z = \{u \in U \mid Y \Rightarrow_{\mathcal{F}} u\}$ достаточно проверить, что множество Z включает Y и является замкнутым относительно $\mathcal{F}$ (индукция по построению).

Очевидно, $Y \Rightarrow_{\mathcal{F}} y$ для всех $y \in Y$. Предположим, $u = f(\vec{v})$ для некоторых $\vec{v} = (v_0, \ldots, v_{s-1}) \in Z^s$ и $f^{(s)} \in \mathcal{F}$. Каждый элемент v_i имеет некоторое построение d_i над Y. Мы утверждаем, что последовательность $d = d_0 \cdot \ldots \cdot d_{s-1} \cdot (f(\vec{v}))$, где символ $\cdot$ обозначает конкатенацию, есть $\mathcal{F}$-построение u над Y. В силу упражнения 2.4.32, ее начало $d_0 \cdot \ldots \cdot d_{s-1}$ является $\mathcal{F}$-построением над Y. Если добавить в конец элемент $u = f(\vec{v})$, это по-прежнему будет такое построение, поскольку все v_i встречаются в начале $d_0 \cdot \ldots \cdot d_{s-1}$. Итак, $u \in Z$.

Теперь проверим $Z \subseteq \mathcal{F}(Y)$. Индукцией по $|d|$ установим, что при всех $u \in U$ из $Y \Rightarrow^d_{\mathcal{F}} u$ следует $u \in \mathcal{F}(Y)$. Если $|d| = 0$, то d не может быть построением элемента u. Пусть $|d| = n + 1$. Для элемента $d(n)$ имеем $d(n) \in Y \subseteq \mathcal{F}(Y)$ или же $d(n) = f(d(j_0), \ldots, d(j_{s-1}))$ при некоторых $j_0, \ldots, j_{s-1} < n$ и $f^{(s)} \in \mathcal{F}$. Согласно упражнению 2.4.32, каждый префикс $d \restriction \underline{j_i + 1}$ построения d является $\mathcal{F}$-построением элемента $d(j_i)$ над Y, причем его длина $j_i + 1 \leqslant n$, а значит, по предположению индукции, $d(j_0), \ldots, d(j_{s-1}) \in \mathcal{F}(Y)$. Но тогда и $u = d(n) \in \mathcal{F}(Y)$, поскольку множество $\mathcal{F}(Y)$ замкнутое. $\square$

Итак, множество, порожденное индуктивным определением, состоит из всех тех и только тех элементов, которые имеют построение. Наличие построения выражает интуитивную идею о том, что каждый элемент такого множества «получается» по одному из правил образования.

Пример 2.4.34. Имеем $\rangle \notin S$, поскольку это слово не может получиться ни по одному из правил образования, иначе как из самого себя: $\rangle = c(\rangle, \varepsilon)$. Но тогда мы придем к противоречию, рассмотрев его построение *наименьшей* длины.

При изучении свойств элементов порожденного множества иногда удобно использовать построения, а иногда — определение порожденного множества.

Лемма 2.4.35. *Пусть $\mathcal{F}$ — индуктивное определение над U и $Y, Z \subseteq U$. Тогда*

1) *если $Y \subseteq Z$ и $Y \Rightarrow^d_{\mathcal{F}} u$, то $Z \Rightarrow^d_{\mathcal{F}} u$;*

2) *если* $Y \subseteq Z$, *то* $\mathcal{F}(Y) \subseteq \mathcal{F}(Z)$;

3) *если* $Y \Rightarrow^d_{\mathcal{F}} u$, *то* $Y' \Rightarrow^d_{\mathcal{F}} u$ *для некоторого конечного* $Y' \subseteq Y$;

4) *если* $u \in \mathcal{F}(Y)$, *то* $u \in \mathcal{F}(Y')$ *для некоторого конечного* $Y' \subseteq Y$;

5) *если* $Z \Rightarrow_{\mathcal{F}} u$ *и* $Y \Rightarrow_{\mathcal{F}} v$ *для каждого* $v \in Z$, *то* $Y \Rightarrow_{\mathcal{F}} u$;

6) $\mathcal{F}(\mathcal{F}(Y)) \subseteq \mathcal{F}(Y)$.

Доказательство. Первое (а с ним и второе) утверждение очевидно. Для третьего (и четвертого) достаточно положить $Y' = Y \cap \operatorname{rng} d$ и применить лемму 2.2.19. Иначе говоря, в Y' попадают лишь те элементы Y, которые встретились в *конечном* построении d.

Шестое утверждение следует из того, что множество $\mathcal{F}(Y)$ является $\mathcal{F}$-замкнутым, притом что $\mathcal{F}(Y) \subseteq \mathcal{F}(Y)$. Отсюда выводится пятое утверждение: по теореме 2.4.33, $Z \subseteq \mathcal{F}(Y)$, откуда $\mathcal{F}(Z) \subseteq \mathcal{F}(\mathcal{F}(Y)) \subseteq$ $\subseteq \mathcal{F}(Y)$ в силу пп. 2 и 6. Тогда $u \in \mathcal{F}(Y)$, а значит, $Y \Rightarrow_{\mathcal{F}} u$. □

Кроме построений, находит применение несколько иной взгляд на образование элементов множества $\mathcal{F}(Y)$ «по шагам». Именно, определим отображение $\mathcal{E}\colon \mathcal{P}(U) \to \mathcal{P}(U)$, при всех $X \subseteq U$ полагая $\mathcal{E}(X) =$ $= X \cup \{f(\vec{u}) \mid f \in \mathcal{F} \text{ и } \vec{u} \in X\}$. Положим также $\mathcal{E}^0(X) = X$ и $\mathcal{E}^{n+1}(X) = \mathcal{E}(\mathcal{E}^n(X))$.

Упражнение 2.4.36. Докажите, что $\mathcal{F}(Y) = \bigcup_{n\in\mathbb{N}} \mathcal{E}^n(Y)$ для каждого $Y \subseteq U$.

Упражнение 2.4.37. Утверждение предыдущего упражнения напоминает лемму 2.4.5. Для соответствующего индуктивного определения докажите, что $\mathcal{E}^n(R) = \bigcup_{i=1}^{2^n} (R)_i$.

Операторы замыкания. Каждое индуктивное определение $\mathcal{F}$ над множеством U можно рассматривать как отображение $\mathcal{P}(U) \to \mathcal{P}(U)$, т. ч. $Y \mapsto \mathcal{F}(Y)$. Мы увидим, что это отображение является одним из *операторов замыкания*, широко распространенных в математике. Как увидит читатель, мы уже встречались с ними и еще не раз встретимся в продолжение нашего курса.

Для произвольного множества $U \neq \varnothing$ отображение $C\colon \mathcal{P}(U) \to$ $\to \mathcal{P}(U)$ называется *оператором замыкания над* U, если для любых $X, Y \subseteq U$ имеет место:

1) $X \subseteq C(X)$ (*экстенсивность*);

2) $X \subseteq Y \Longrightarrow C(X) \subseteq C(Y)$ (*монотонность*);

3) $C(C(X)) = C(X)$ (*идемпотентность*).

Пример 2.4.38. Согласно лемме 2.3.32, операция итерации языка над алфавитом A как отображение $\mathcal{P}(A^*) \to \mathcal{P}(A^*)$ является оператором замыкания.

Если W — подмножество линейного пространства V над полем $\mathbb{R}$, то *линейной оболочкой* множества W называется множество $\{\alpha_1 w_1 + + \ldots + \alpha_n w_n \mid w_i \in W,\ \alpha_i \in \mathbb{R}\}$. Легко проверить, что линейная оболочка W является наименьшим подпространством, содержащим W. Отображение подмножества W в его линейную оболочку есть оператор замыкания.

Пусть $X \subseteq \mathbb{R}^n$. *Топологическим замыканием* множества X мы называем множество всех таких точек пространства $\mathbb{R}^n$, чья любая окрестность пересекается с X. В частности, предел любой сходящейся последовательности элементов X принадлежит топологическому замыканию X. Отображение подмножества X в его топологическое замыкание есть оператор замыкания.

Пример 2.4.39. Свойства экстенсивности, монотонности и идемпотентности нам уже встречались при обсуждении соответствий Галуа. В самом деле, если (f_*, f^*) есть соответствие Галуа между ч. у. м. $(\mathcal{P}(U), \subseteq)$ и $(B, \leqslant)$, то отображение $C = f^* \circ f_*$ является, согласно лемме 1.6.60, оператором замыкания над U.

Подмножество $X \subseteq U$ называется *замкнутым* относительно оператора C, если $C(X) = X$. Часто рассматривают ч. у. м. $\mathcal{L}_C = (L_C, \subseteq)$, где $L_C = \{X \in \mathcal{P}(U) \mid C(X) = X\}$. Легко видеть, что $\mathcal{L}_C$ есть нижняя полурешетка, поскольку $X \cap Y = C(X \cap Y) \in L_C$ при $X, Y \in L_C$.

Упражнение 2.4.40. Докажите, что $\mathcal{L}_C$ есть полная решетка, и выясните, как устроен $\sup_{i \in I} A_i$, где все $A_i \in L_C$.

Упражнение 2.4.41. Докажите, что любая полная решетка $(A, \leqslant)$ изоморфна решетке $\mathcal{L}_C$ для некоторого оператора замыкания C. (Можно положить $C(X) = \{a \in A \mid a \leqslant \sup X\}$ для всех $X \subseteq A$.)

Оператор замыкания $C\colon \mathcal{P}(U) \to \mathcal{P}(U)$ называется *финитарным*, если

$$C(X) = \cup\{C(X') \mid X' \in \mathcal{P}_f(X)\},$$

где $\mathcal{P}_f(X)$ означает множество всех конечных подмножеств X. Включение справа налево имеет место для любого оператора замыкания в

силу монотонности, а включение слева направо означает, что каждый элемент $C(X)$ можно получить, «замкнув» лишь некоторое конечное подмножество X.

Упражнение 2.4.42. Докажите, что любое отображение $C\colon \mathcal{P}(U) \to \to \mathcal{P}(U)$, удовлетворяющее условию финитарности, а также условиям экстенсивности и идемпотентности, необходимо является монотонным.

Пример 2.4.43. Итерация языка финитарна. В самом деле, если $\sigma \in L^*$, то $\sigma \in L^n$ для некоторого $n \in \mathbb{N}$, т. е. $\sigma = \sigma_1\sigma_2\ldots\sigma_n$ при $\sigma_i \in L$. Очевидно, $\sigma \in (L')^*$, где язык $L' = \{\sigma_1, \ldots, \sigma_n\} \subseteq L$ конечный.

Упражнение 2.4.44. Докажите, что оператор линейной оболочки финитарный, а оператор топологического замыкания не финитарный уже для пространства $\mathbb{R}$.

Лемма 2.4.45. *Каждое индуктивное определение $\mathcal{F}$ над U является финитарным оператором замыкания над U.*

Доказательство. Очевидно из леммы 2.4.35. □

Замечание 2.4.46. Легко проверить, что множество $X \subseteq U$ является замкнутым относительно индуктивного определения $\mathcal{F}$ тогда и только тогда, когда $\mathcal{F}(X) = X$. Таким образом, два введенных нами понятия замкнутости вполне согласованы.

Любопытно, что каждый финитарный оператор замыкания можно рассматривать как некоторое индуктивное определение.

Теорема 2.4.47 (Биркгофа— Фринка)**.** *Для любого финитарного оператора замыкания C над U существует индуктивное определение $\mathcal{F}$ над U, т. ч. $C(X) = \mathcal{F}(X)$ при всех $X \subseteq U$.*

Доказательство. Для каждого конечного множества $A \subseteq U$ мощности n и каждого $a \in C(A)$ определим функцию $f_{A,a}\colon U^n \to U$, т. ч.

$$f_{A,a}(u_0, \ldots, u_{n-1}) \quad = \quad \begin{cases} a, & \text{если } A = \{u_0, \ldots, u_{n-1}\}; \\ u_0 & \text{иначе} \end{cases}$$

при всех $\vec{u} = (u_0, \ldots, u_{n-1}) \in U^n$. В частности, при $A = \varnothing$ для всех $\vec{u} \in U^0 = \{\varnothing\}$ имеем $f_{A,a}(\vec{u}) = a$. Положим

$$\mathcal{F} = \{f_{A,a} \in \bigcup_{n\in\mathbb{N}} U^{U^n} \mid A \in \mathcal{P}_f(U),\ a \in C(A)\}.$$

Чтобы доказать включение $\mathcal{F}(X) \subseteq C(X)$, достаточно проверить, что $X \subseteq C(X)$ (но оператор C экстенсивен) и что множество $C(X)$ является $\mathcal{F}$-замкнутым. В самом деле, пусть $\vec{u} \in C(X)$ и $f_{A,a} \in \mathcal{F}$. Тогда $f_{A,a}(\vec{u}) = u_0 \in C(X)$ или же $A = \{u_0, \ldots, u_{n-1}\}$ и $f_{A,a}(\vec{u}) = a \in$ $\in C(A) \subseteq C(C(X)) = C(X)$ по монотонности и идемпотентности C.

Докажем включение $C(X) \subseteq \mathcal{F}(X)$. Если $u \in C(X)$, то в силу финитарности C найдется конечное $A = \{a_0, \ldots, a_{n-1}\} \subseteq X$, т. ч. $u \in C(A)$. Значит, $f_{A,u} \in \mathcal{F}$, причем $f_{A,u}(a_0, \ldots, a_{n-1}) = u$. Поэтому $u \in \mathcal{F}(X)$. □

Упражнение 2.4.48. Дайте явные индуктивные определения операциям итерации языка и линейной оболочки подмножества линейного пространства.

Однозначность разбора. Напомним, над алфавитом $\mathcal{B} = \{\langle, \rangle\}$ язык R состоит, в точности, из правильных скобочных последовательностей, а язык S порождается индуктивным определением $\mathcal{S} = \{\varepsilon, p, c\}$, где $p(\sigma) = \langle\sigma\rangle$ и $c(\sigma, \tau) = \sigma\tau$.

Лемма 2.4.49. $S = R$.

Доказательство. Включение $S \subseteq R$ установим индукцией по построению для $\mathcal{S}$. Очевидно, $\varepsilon \in R$. Если $\sigma, \tau \in R$, то слова $p(\sigma) = \langle\sigma\rangle$ и $c(\sigma, \tau) = \sigma\tau$ также принадлежат R по лемме 2.3.44.

Проверим включение $R \subseteq S$. Индукцией по $|\sigma|$ установим, что $\sigma \in$ $\in S$, когда $\sigma \in R$. Если $|\sigma| = 0$, то $\sigma = \varepsilon \in S$. Пусть $|\sigma| > 0$. У слова σ есть непустое правильное начало (хотя бы само σ). Рассмотрим такое начало σ' *наименьшей длины*. Имеем $\sigma = \sigma'\sigma''$. Понятно, что $\sigma'' \in R$. В самом деле, $b(\sigma'') = b(\sigma) - b(\sigma') = 0$. Пусть $\rho \sqsubseteq \sigma''$. Тогда $\sigma'\rho \sqsubseteq \sigma$. Отсюда $0 \leqslant b(\sigma'\rho) = b(\sigma') + b(\rho) = b(\rho)$.

Если $|\sigma'| < |\sigma|$, то также $|\sigma''| < |\sigma|$. По предположению индукции, $\sigma', \sigma'' \in S$. Значит, и $\sigma = \sigma'\sigma'' \in S$.

Если же $|\sigma'| = |\sigma|$, то слово σ' не имеет непустого правильного собственного начала. В силу леммы 2.3.46, $\sigma = \sigma' = \langle\tau\rangle$ для некоторого $\tau \in R$. Но $|\tau| < |\sigma|$, откуда $\tau \in S$. Тогда и $\sigma = \langle\tau\rangle \in S$. □

Видим, что индуктивное определение $\mathcal{S}$ порождает язык правильных скобочных последовательностей R. Поэтому у каждой такой последовательности есть $\mathcal{S}$-построение. Как мы уже отмечали, оно не единственно. Например, построение всегда можно продлить, повторяя какой-нибудь член. Однако в случае определения $\mathcal{S}$ единственности

препятствует более серьезное обстоятельство: элементы S могут быть получены по разным правилам из разных наборов образующих. Например,

$$\langle\rangle\langle\rangle\langle\rangle = c(\langle\rangle\langle\rangle, \langle\rangle) = c(\langle\rangle, \langle\rangle\langle\rangle) = c(\langle\rangle\langle\rangle\langle\rangle, \varepsilon) \text{ и}$$

$$\langle\rangle = c(\langle\rangle, \varepsilon) = p(\varepsilon).$$

Устранение такой неоднозначности, как вскоре станет ясно, делает индуктивное определение существенно полезнее.

По определению, индуктивное определение $\mathcal{F}$ над U обладает свойством *однозначности разбора*, если для любых $\vec{u}, \vec{v} \in \mathcal{F}(\varnothing)$ и любых $f, g \in \mathcal{F}$ из $f(\vec{u}) = g(\vec{v})$ следует $f = g$ и $\vec{u} = \vec{v}$. Иначе говоря, для каждого элемента порожденного множества правило образования и набор образующих определены однозначно.

Упражнение 2.4.50. Для любого индуктивного определения докажите, что всякий элемент, имеющий построение, имеет и построение, в которое каждый член входит не более одного раза.

Упражнение 2.4.51. Пусть U — некоторое множество. Докажите, что тогда существует функция $g\colon U^n \to U$, т. ч. индуктивное определение $\mathcal{F} \cup \{g\}$ не обладает свойством однозначности разбора ни для какого индуктивного определения $\mathcal{F}$ над U с условием $\mathcal{F}(\varnothing) \neq \varnothing$.

Построим индуктивное определение языка R со свойством однозначности разбора. Положим $\mathcal{D} = \{\varepsilon^{(0)}, q^{(2)}\}$, где $q(\sigma, \tau) = \langle\sigma\rangle\tau$ для всех $\sigma, \tau \in \mathcal{B}^*$. Язык $D = \mathcal{D}(\varnothing)$ традиционно называют *языком Дика*.

Лемма 2.4.52. $D = R$.

Доказательство. Из $\sigma, \tau \in S$ следует $q(\sigma, \tau) = c(p(\sigma), \tau) \in S$. Также $\varepsilon \in S$. Поэтому $D \subseteq S = R$.

Покажем, что из $\sigma \in R$ вытекает $\sigma \in D$. Рассуждаем, как в лемме 2.4.49. Пусть σ' — непустое правильное начало слова σ наименьшей длины, т. ч. $\sigma = \sigma'\sigma''$. Как мы видели, $\sigma'' \in R$. По лемме 2.3.46, имеем $\sigma' = \langle\tau\rangle$ для некоторого $\tau \in R$. Так как $|\tau|, |\sigma''| < |\sigma|$, по предположению индукции получаем $\tau, \sigma'' \in D$. Значит, $\sigma = \langle\tau\rangle\sigma'' \in D$. □

Лемма 2.4.53. *Индуктивное определение $\mathcal{D}$ обладает свойством однозначности разбора.*

Доказательство. Очевидно, $q(\sigma, \tau) = \varepsilon$ невозможно. Поэтому достаточно показать, что для всех $\sigma, \sigma', \tau, \tau' \in D$ из $q(\sigma, \tau) = q(\sigma', \tau')$ следует

$\sigma = \sigma'$ и $\tau = \tau'$. Имеем $\sigma\rangle\tau = \sigma'\rangle\tau'$, откуда либо $\sigma\rangle = \sigma'\rangle$, что сразу влечет $\tau = \tau'$, либо же $\sigma\rangle \sqsubset \sigma'\rangle$ или $\sigma'\rangle \sqsubset \sigma\rangle$. Без ограничения общности допустим $\sigma\rangle \sqsubset \sigma'\rangle$. Но тогда $\sigma\rangle \sqsubseteq \sigma'$, хотя $b(\sigma\rangle) = b(\sigma) - 1 = -1$, вопреки $\sigma' \in R$. Противоречие. $\square$

Пример 2.4.54. Покажем, как однозначность разбора для $\mathcal{D}$ позволяет решить содержательную задачу: вычислить количество различных правильных скобочных последовательностей данной длины.

Положим $R_n = \{\sigma \in R \mid |\sigma| = n\}$. Сразу ясно, что $R_0 = \{\varepsilon\}$ и $R_1 = \varnothing$ (вообще, если n нечетно, то из $n = |\sigma| = |\sigma|_\langle + |\sigma|_\rangle$ следует $|\sigma|_\langle \neq |\sigma|_\rangle$, откуда $b(\sigma) = |\sigma|_\langle - |\sigma|_\rangle \neq 0$; значит, $R_n = \varnothing$). Если же длина слова $\sigma \in R = D$ не меньше двух, то это слово имеет $\mathcal{D}$-построение, причем является значением функции q. Значит, в силу однозначности разбора, для всякого $\sigma \in R_n$ при $n \geqslant 2$ существует единственная пара (τ, ρ) правильных последовательностей, т. ч. $\sigma = \langle\tau\rangle\rho$. Имеем $|\tau| + |\rho| + 2 = n$. С другой стороны, любая пара с таким условием задает слово $q(\tau, \rho) \in R_n$.

Это показывает, что при $n \geqslant 2$ существует биекция между множествами R_n и $\bigcup_{\{(k,m)\in\mathbb{N}^2 \mid k+m+2=n\}} R_k \times R_m$. Имеем $k, m \leqslant n$, а значит, таких пар (k, m) лишь конечно много. Тогда, применяя правила произведения и суммы, получаем $|R_n| = \sum_{k+m+2=n} |R_k| \cdot |R_m|$ при всех $n \geqslant 2$.

Обозначив $C_n = |R_{2n}|$ и учтя $|R_{2n+1}| = 0$, имеем

$$C_0 = 1 \quad \text{и} \quad C_{n+1} = \sum_{k+m=n} C_k \cdot C_m$$

при всех $n \in \mathbb{N}$. Последовательность $\{C_n\}_{n\in\mathbb{N}}$ с таким рекурсивным определением называется *числами Каталана*.

Помимо количества правильных скобочных последовательностей четной длины, числа Каталана имеют много других содержательных интерпретаций. Известны и более эффективные способы их вычисления.

Упражнение 2.4.55. Убедитесь, что индуктивное определение языка двоичных записей натуральных чисел из примера 2.4.18 не обладает свойством однозначности разбора, но если с помощью определения $\{1, f_0, f_1\}$ задать множество двоичных записей элементов $\mathbb{N}_+$, однозначность разбора будет иметь место.

Упражнение 2.4.56. Пусть язык L над алфавитом $\underline{2}$ задан таким определением: $0 \in L$; если $\sigma \in L$, то $\sigma 1 \in L$ и $\sigma\sigma \in L$. Докажите, что это определение обладает свойством однозначности разбора.

Беспрефиксные языки. Рассмотрим один частный метод доказательства однозначности разбора, важный для применений в математической логике. Язык L над алфавитом A называется *беспрефиксным*, если $\tau \sqsubset \sigma \in L$ влечет $\tau \notin L$. Иначе говоря, никакое собственное начало слова языка L этому языку не принадлежит.

Пример 2.4.57. Над алфавитом $\underline{2}$ язык $\{011, 0011, 11\}$ беспрефиксный, а язык $\{011, 01101\}$ нет. Языки двоичных записей натуральных чисел и правильных скобочных последовательностей не являются беспрефиксными.

Совершенно аналогично можно определить *бессуффиксные* языки и применить к ним все дальнейшие соображения.

Упражнение 2.4.58. Докажите, что язык L бессуффиксный тогда и только тогда, когда язык $L^{\mathsf{R}} = \{\sigma^{\mathsf{R}} \mid \sigma \in L\}$ беспрефиксный.

Пример 2.4.59. Проверим, что язык замкнутых арифметических термов Ar из примера 2.4.9 является беспрефиксным.

Индукцией по длине слова $\sigma \in Ar$ покажем, что $\tau \sqsubset \sigma$ влечет $\tau \notin Ar$. Рассмотрим какое-либо построение слова σ. Это слово состоит из одного символа алфавита $\mathbb{N}$ или же имеет вид $\langle \varphi \circ \psi \rangle$, где $\varphi, \psi \in Ar$ и $\circ \in \{+, \cdot\}$. В первом случае имеем $\tau = \varepsilon \notin Ar$.

Во втором случае $\tau \sqsubseteq \langle \varphi \circ \psi \rangle$. Предположим, что $\tau \in Ar$. Поскольку $\tau = \langle \tau'$, заключаем $\tau = \langle \varphi' * \psi' \rangle$ для некоторых $\varphi', \psi' \in Ar$ и $* \in \{+, \cdot\}$. Но тогда $\langle \varphi \circ \psi \rangle = \langle \varphi' * \psi' \rangle \theta$, откуда следует $\varphi = \varphi'$ или, без ограничения общности, $\varphi \sqsubset \varphi'$. Однако $|\varphi'| < |\sigma|$, и $\varphi \notin Ar$ по предположению индукции, что не так. Значит, $\varphi = \varphi'$, что дает $\circ \psi \rangle = * \psi' \rangle \theta$. Далее, $\circ = *$ и $\psi \rangle = \psi' \rangle \theta$. Вновь применяя предположение индукции, получаем $\psi = \psi'$, а значит, $\theta = \varepsilon$ и $\sigma = \tau$, что не так. Следовательно, $\tau \notin Ar$.

Пример 2.4.60. Индуктивное определение языка Ar обладает свойством однозначности разбора.

В самом деле, $\langle \sigma \circ \tau \rangle = n$, где $n \in \mathbb{N}$, невозможно, поскольку первое слово имеет длину не менее трех, а второе однобуквенное. Значит, остается для любых $\sigma, \sigma', \tau, \tau' \in Ar$ из $\langle \sigma \circ \tau \rangle = \langle \sigma' * \tau' \rangle$ вывести $\circ = *$ (т. е. что правило образования элемента определено однозначно), $\sigma = \sigma'$ и $\tau = \tau'$. Имеем $\sigma = \sigma'$ или $\sigma \sqsubset \sigma'$ или $\sigma' \sqsubset \sigma$. Второй и третий случаи противоречат беспрефиксности языка Ar, а значит, $\sigma = \sigma'$, откуда $\circ = *$ и $\tau = \tau'$.

Покажем теперь, как можно представить арифметические термы без скобок — посредством *польской* (или *префиксной*) *записи*. Мы же-

лаем определить язык Pl выражений вида $\cdot\ 2\ +\ 3\ 1$. Как обычно, Pl есть наименьшее множество, удовлетворяющее условиям

$$\forall n \in \mathbb{N}\ n \in Pl \quad \text{и} \quad \forall \sigma, \tau\, (\sigma, \tau \in Pl \Longrightarrow +\sigma\tau, \cdot\sigma\tau \in Pl).$$

Упражнение 2.4.61. Докажите, что язык Pl является беспрефиксным и его определение обладает свойством однозначности разбора.

Польская запись не вполне интуитивна и на практике применяется не часто. Однако она очень проста для анализа. Потому мы нередко будем давать определения различных языков в префиксной записи, но без комментариев переводить ее в привычную «инфиксную»: $+\ 2\ 3 \mapsto \langle 2 + 3 \rangle$ и т. п. — или же использовать дополнительные скобки и запятые: $+(2, 3)$. Такой перевод можно определить *рекурсивно*, в чем сейчас убедится читатель.

Рекурсия по построению. Важнейшим применением однозначности разбора в нашем курсе будет определение функций на индуктивно порожденных множествах с помощью *рекурсии по построению*. Идея состоит в определении значения функции на элементе по ее значениям на образующих этого элемента (набор которых единствен). При этом каждое правило образования задает отображение значения на образующих в значение на образованном элементе.

Пример 2.4.62. Функция $v\colon Pl \to \mathbb{N}$ ставит в соответствие арифметическом терму языка Pl его значение – натуральное число. Например, $v(\cdot\ 2\ +\ 3\ 1) = 8$. Очевидно, такая функция должна обладать свойствами

$$v(n) = n, \quad v(+\sigma\tau) = v(\sigma) + v(\tau) \quad \text{и} \quad v(\cdot\sigma\tau) = v(\sigma)v(\tau)$$

при всех $n \in \mathbb{N}$ и $\sigma, \tau \in Pl$.

Пример 2.4.63. Функция $t\colon Pl \to Ar$ ставит в соответствие арифметическом терму языка Pl его перевод в инфиксную запись. Например, $t(\cdot\ 2\ +\ 3\ 1) = \langle 2 \cdot \langle 3 + 1 \rangle \rangle$. При этом должно выполняться:

$$t(n) = n, \quad t(+\sigma\tau) = \langle t(\sigma) + t(\tau) \rangle \quad \text{и} \quad t(\cdot\sigma\tau) = \langle t(\sigma) \cdot t(\tau) \rangle$$

при всех $n \in \mathbb{N}$ и $\sigma, \tau \in Pl$.

Пример 2.4.64. Функция $t'\colon Ar \to Pl$ осуществляет обратный перевод. При этом должно выполняться:

$$t'(n) = n, \quad t'(\langle \sigma + \tau \rangle) = +\,t'(\sigma)\,t'(\tau) \quad \text{и} \quad t'(\langle \sigma \cdot \tau \rangle) = \cdot\,t'(\sigma)\,t'(\tau)$$

при всех $n \in \mathbb{N}$ и $\sigma, \tau \in Ar$.

Пример 2.4.65. Допустим, что такие функции t и t' существуют. Индукцией по построению легко доказать, что $t'(t(\sigma)) = \sigma$ для всех $\sigma \in Pl$, а значит, $t' \circ t = \mathrm{id}_{Pl}$. Аналогично устанавливается $t \circ t' = \mathrm{id}_{Ar}$. Тогда, согласно упражнению 1.5.27, перевод t является биекцией, причем $t' = t^{-1}$.

Интуитивно ясно, что функции v, t и t' с требуемыми свойствами существуют и определены однозначно. Мы теперь дадим строгое доказательство этому факту и в дальнейшем будем применять рекурсию по построению без особых пояснений.

Теорема 2.4.66 (рекурсия по построению)**.** *Пусть $\mathcal{F} = \{f_i\}_{i\in I}$, где $f_i = f_j$ влечет $i = j$, есть индуктивное определение над множеством U, обладающее свойством однозначности разбора, и $\{g_i\}_{i\in I}$ есть семейство функций*[11]*, т. ч. для некоторого множества V из $f_i\colon U^n \to U$ следует $g_i\colon V^n \to V$. Тогда существует единственная функция $f\colon \mathcal{F}(\varnothing) \to V$, т. ч.*

$$f(f_i(u_0, \ldots, u_{n-1})) = g_i(f(u_0), \ldots, f(u_{n-1}))$$

для всех $f_i^{(n)} \in \mathcal{F}$ и всех $u_0, \ldots, u_{n-1} \in \mathcal{F}(\varnothing)$.

Доказательство. Индуктивное определение Φ множества $f \subseteq \mathcal{F}(\varnothing) \times V$ зададим условиями:

- если $f_i^{(0)} \in \mathcal{F}$, то $(f_i, g_i) \in f$;
- если $f_i^{(n+1)} \in \mathcal{F}$ и $(u_0, v_0), \ldots, (u_n, v_n) \in f$, то $(f_i(\vec{u}), g_i(\vec{v})) \in f$.

Отношение f функционально и тотально. В самом деле, достаточно убедиться, что множество

$$Z = \{u \in \mathcal{F}(\varnothing) \mid \text{существует единственный } v \in V, \text{ т. ч. } (u, v) \in f\}$$

включает $\mathcal{F}(\varnothing)$. Для этого, в силу индукции по построению, достаточно проверить $\mathcal{F}$-замкнутость Z. Итак, пусть $f_i^{(n)} \in \mathcal{F}$ и $u_0, \ldots, u_{n-1} \in \in Z$. Тогда существуют и единственны такие элементы $v_0, \ldots, v_{n-1}$, что $(u_0, v_0), \ldots, (u_{n-1}, v_{n-1}) \in f$. Имеем $(f_i(\vec{u}), g_i(\vec{v})) \in f$. Предположим, что $(f_i(\vec{u}), w) \in f$ для некоторого $w \in V$. Рассматривая какое-нибудь Φ-построение этой пары, видим, что $f_i(\vec{u}) = f_j(\vec{u'})$ и $w = g_j(\vec{v'})$, где

[11] Мы говорим об индексированных семействах лишь для упрощения обозначений. Как показывает замечание 1.5.39, к такой формулировке тривиально сводятся другие.

$(u'_0, v'_0), \ldots, (u'_{m-1}, v'_{m-1}) \in f$. В силу однозначности разбора, $f_i = f_j$, $n = m$ и $\vec{u} = \vec{u}'$. Получаем $i = j$ и $g_i = g_j$, а также $\vec{v} = \vec{v}'$, вследствие $\vec{u} \in Z$. Но тогда $w = g_i(\vec{v})$, что означает $f_i(\vec{u}) \in Z$.

Итак, $f\colon \mathcal{F}(\varnothing) \to V$. Для любых $u_0, \ldots, u_{n-1} \in \mathcal{F}(\varnothing)$ имеет место $(u_k, f(u_k)) \in f$, а значит, $(f_i(\vec{u}), g_i(f(u_0), \ldots, f(u_{n-1}))) \in f$, что и требовалось.

Остается проверить единственность функции f. Пусть f' — другая функция с требуемым свойством. Среди элементов $u \in \mathcal{F}(\varnothing)$, где функции различаются, выберем некоторый, имеющий $\mathcal{F}$-построение d наименьшей длины. Пусть $u = f_i(u_0, \ldots, u_{n-1})$, где каждый элемент u_k встречается в построении d на месте $j_k < |d| - 1$. Поскольку $d \restriction \underline{j_k + 1}$ есть $\mathcal{F}$-построение u_k короче d, имеем $f(u_k) = f'(u_k)$. Но тогда $\underline{f(u)} = g_i(f(u_0), \ldots, f(u_{n-1})) = g_i(f'(u_0), \ldots, f'(u_{n-1})) = f'(u)$. Противоречие. □

Упражнение 2.4.67. С помощью рекурсии по построению определите функции: число вхождений символа $\langle$ в слово языка S; натуральное число — значение бинарной записи; перевод из бинарной записи в унарную.

Глава 3. Логика высказываний

§ 3.1. Что есть истина?

В предыдущих главах мы на основе понятия множества разработали наш инструментарий вполне достаточно, чтобы заняться, наконец, построением математической модели логики. Как уже отмечалось, с традиционной точки зрения, логика как таковая интересуется отделением правильных способов рассуждений от ошибочных — к первым относят ровно те, которые из истинных посылок всегда выводят истинные заключения.

Но что значит «истинные»? .....

§ 3.2. Функции и формулы

Назовем *булевой функцией n аргументов* всякую функцию $f\colon \underline{2}^n \to \underline{2}$, где $n \in \mathbb{N}$. Поскольку каждая такая функция является конечным множеством, она может быть описана перечислением всех своих элементов, которое удобно представить в форме таблицы.

Пример 3.2.1. Среди приведенных ниже функций читатель видит модели связок «не» (not, *отрицание*), «и» (and, *конъюнкция*), «или» (or, *дизъюнкция*), «если..., то...» (imp, *импликация*) и «равносильно» (eq, *эквивалентность*).

	not	$\mathbf{1}^{(1)}$	$\mathrm{id}_{\underline{2}}$
0	1	1	0
1	0	1	1

		and	or	imp	eq	+
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

Функция $+$ представляет собой сложение по модулю 2 и еще обозначается xor (exclusive or), что соответствует ее логической интерпретации связкой «либо…, либо…, но не то и другое вместе». Функция $\mathbf{1}^{(1)}$ имеет один аргумент, о чем говорит индекс в ее обозначении, и всегда возвращает единицу. Как будет вскоре видно, по алгебраическим причинам такая функция может быть удобнее константы $\mathbf{1}^{(0)}\colon \underline{2}^0 \to \underline{2}$.

Функция $\mathrm{id}_{\underline{2}}$ не нуждается в представлении, однако отметим, что она является частным случаем *проектора*, о которых нам уже случалось говорить в предыдущих главах, и которые в контексте булевых функций мы будем обозначать так: $\pi^i_n\colon \underline{2}^n \to \underline{2}$, где $\pi^i_n(x_1,\ldots,x_n) = x_i$ при $\vec{x} \in \underline{2}^n$, $n \in \mathbb{N}_+$ и $1 \leqslant i \leqslant n$. Действительно, тогда $\mathrm{id}_{\underline{2}} = \pi^1_1$.

Лемма 3.2.2. *Для любых $x, y, z \in \underline{2}$ имеет место:*

1) $\mathrm{and}(x,y) = \mathrm{and}(y,x)$; $\mathrm{or}(x,y) = \mathrm{or}(y,x)$; $x + y = y + x$;
2) $\mathrm{and}(\mathrm{and}(x,y),z) = \mathrm{and}(x,\mathrm{and}(y,z))$; $\mathrm{or}(\mathrm{or}(x,y),z) = \mathrm{or}(x,\mathrm{or}(y,z))$; $(x+y)+z = x+(y+z)$;
3) $\mathrm{and}(x,x) = x$; $\mathrm{or}(x,x) = x$; $x + x = 0$;
4) $\mathrm{and}(x,\mathrm{or}(x,y)) = x$; $\mathrm{and}(x,\mathrm{or}(x,y)) = x$;
5) $\mathrm{not}(\mathrm{not}(x)) = x$;
6) $\mathrm{and}(x,\mathrm{or}(y,z)) = \mathrm{or}(\mathrm{and}(x,y),\mathrm{and}(x,z))$; $\mathrm{or}(x,\mathrm{and}(y,z)) = \mathrm{and}(\mathrm{or}(x,y),\mathrm{or}(x,z))$; $\mathrm{and}(x,y+z) = \mathrm{and}(x,y) + \mathrm{and}(x,z)$;
7) $\mathrm{not}(\mathrm{and}(x,y)) = \mathrm{or}(\mathrm{not}(x),\mathrm{not}(y))$; $\mathrm{not}(\mathrm{or}(x,y)) = \mathrm{and}(\mathrm{not}(x),\mathrm{not}(y))$;
8) $\mathrm{and}(x,0) = 0$; $\mathrm{and}(x,1) = x$; $\mathrm{or}(x,0) = x$; $\mathrm{or}(x,1) = 1$; $x + 0 = x$; $x + 1 = \mathrm{not}(x)$; $\mathrm{not}(0) = 1$; $\mathrm{not}(1) = 0$;
9) $\mathrm{and}(x,\mathrm{not}(x)) = 0$; $\mathrm{or}(x,\mathrm{not}(x)) = 1$;
10) $\mathrm{imp}(x,y) = \mathrm{or}(\mathrm{not}(x),y)$; $\mathrm{not}(\mathrm{imp}(x,y)) = \mathrm{and}(x,\mathrm{not}(y))$; $\mathrm{imp}(0,x) = 1$; $\mathrm{imp}(1,x) = x$; $\mathrm{imp}(x,0) = \mathrm{not}(x)$; $\mathrm{imp}(x,1) = 1$;
11) $\mathrm{eq}(x,y) = \mathrm{and}(\mathrm{imp}(x,y),\mathrm{imp}(y,x))$.

Замечание 3.2.3. Если ограничить естественный порядок $(\mathbb{N},<)$ на множество $\underline{2}$ (т. е. попросту положить $0 < 1$), оказывается, что $\mathrm{and}(x,y) = \min(x,y)$, $\mathrm{or}(x,y) = \max(x,y)$ и $\mathrm{imp}(x,y) = 1$ тогда и только тогда, когда $x \leqslant y$. Отсюда еще видно, что ч. у. м. $(\underline{2},\leqslant)$ является решеткой, где $\sup\{x,y\} = \mathrm{or}(x,y)$ и $\inf\{x,y\} = \mathrm{and}(x,y)$.

Более того, как показывает сравнение с теоремой 1.2.38, структура $(\underline{2},\mathrm{and},\mathrm{or},\mathrm{not},0,1)$ является булевой алгеброй.

Упражнение 3.2.4. Для каких множеств X верно $(\mathcal{P}(X), \subseteq) \cong (\underline{2}, \leqslant)$?

Замечание 3.2.5. Легко видеть, что функция and совпадает с умножением по модулю 2. Иногда нам будет удобно обозначить эту функцию символом $\cdot$ (который, к тому же, традиционно опускают). Структура $(\underline{2}, +, \cdot, 0, 1)$ является *кольцом* (подобно целым числам с обыкновенными операциями сложения и умножения) и даже *полем* (подобно вещественным числам: умножение *коммутативно* ($xy = yx$) и у каждого элемента $x \neq 0$ есть обратный по умножению x^{-1}, т. ч. $xx^{-1} = 1$). Примечательно, что вычитание в этом поле совпадает со сложением, т. е. $-x = x$, поскольку $x + x = 0$, а единственный ненулевой элемент 1 обратный сам себе.

Замечание 3.2.6. Обратите внимание, что проектор, по существу, определяется «числом» своих аргументов (которое, как мы видели в разделе § 1.5., может быть и бесконечным) и «номером» того из них, который следует вернуть. Природа же самих элементов не существенна: скажем, мы имели бы равенство $\pi^i_n(x_1, \ldots, x_n) = x_i$ для $\pi^i_n \colon A^n \to A$ при *любом* A.

Таким образом, тут более плодотворна интуиция функции как *правила вычисления* значения из аргументов, а не «уже готового» множества пар. В частности, в нашем случае такое правило не зависит от множества A, и функцию π^i_n можно понимать как *полиморфную* — работающую с объектами произвольной природы.

Лемма 3.2.7. *Для любого $n \in \mathbb{N}$ множество B_n всевозможных булевых функций n аргументов имеет мощность 2^{2^n}.*

Доказательство. Как мы помним, $A^{\underline{k}} \sim A^k \sim \underline{|A|^k}$ для любого конечного A и $k \in \mathbb{N}$. Поэтому $B_n = \underline{2}^{\underline{2^n}} \sim \underline{2}^{\underline{2^n}} \sim \underline{2}^{2^n} \sim \underline{2^{2^n}}$. □

Пример 3.2.8. Имеем $B_1 = \{\mathbf{0}^{(1)}, \mathbf{1}^{(1)}, \pi^1_1, \mathrm{not}\}$ и $B_0 = \{\mathbf{0}^{(0)}, \mathbf{1}^{(0)}\}$. Согласно замечанию 2.1.16, можно считать $\mathbf{0}^{(0)} = 0$ и $\mathbf{1}^{(0)} = 1$.

Следствие 3.2.9. *Множество $\cup_{n\in\mathbb{N}} B_n$ всех булевых функций счетно.*

Булевы формулы. Во многих случаях важно, какие функции можно получить «комбинируя» уже имеющиеся. Например, в лемме 3.2.2 мы видели, что $\mathrm{imp}(x, y) = \mathrm{or}(\mathrm{not}(x), y)$, т. е. импликация получается из отрицания и дизъюнкции. Такой вопрос естествен как для логики, где мы хотим выяснить, какого рода высказывания можно получить

с помощью данного набора связок, так и для программирования, где может быть важно определить новую функцию, используя уже имеющиеся в «библиотеке».

Очевидно, само по себе *выражение* $\mathrm{or}(\mathrm{not}(x), y)$ представляет собой некоторую программу вычисления *значения* $\mathrm{imp}(x, y)$ по любым элементам $x, y \in \underline{2}$. При этом, разумеется, важно знать, что символ or обозначает известную функцию дизъюнкцию, а not — функцию отрицание.

Формализуем эту идею. Пусть фиксировано некоторое счетное множество $\mathrm{At} = \{p_0, p_1, p_2, \ldots\}$, чьи элементы назовем *атомарными высказываниями* или *атомами* (их логическая интерпретация — некоторые высказывания или предложения, дальнейший анализ которых не проводится). Также пусть дано некоторое множество $\hat{F} = \{\hat{f}, \ldots\}$, чьи элементы называем *связками*. Содержательно, это имена логических связок или операторы в «программе».

Будем считать, что $\hat{F} \cap \mathrm{At} = \varnothing$ и что каждой связке приписано[1] некоторое натуральное число, называемое ее *валентностью*. Если связка $\hat{f}$ имеет валентность n, пишем $\hat{f}^{(n)}$. Валентность равна числу аргументов функции, которую должна обозначать связка.

Множество $\mathrm{Fm}(\hat{F})$ *булевых формул над множеством связок* $\hat{F}$ задается индуктивным определением: это наименьшее $X \subseteq (\mathrm{At} \cup \hat{F})^*$, удовлетворяющее условиям:

$$p \in \mathrm{At} \Longrightarrow p \in X; \quad \hat{f}^{(n)} \in \hat{F},\ \varphi_1, \ldots, \varphi_n \in X \Longrightarrow \hat{f}\varphi_1 \ldots \varphi_n \in X.$$

Напоминаем, что выражение $\hat{f}\varphi_1 \ldots \varphi_n$ обозначает конкатенацию однобуквенного слова $\hat{f}$ и слов $\varphi_1, \ldots, \varphi_n$ над алфавитом $(\mathrm{At} \cup \hat{F})^*$. В «программистских» терминах, формула — это строка (массив) символов некоторого специального вида. Если $n = 0$, выражение $\hat{f}\varphi_1 \ldots \varphi_n$ понимается как $\hat{f}$. Это будет формула, поскольку связка $\hat{f}$ не требует аргументов.

Если множество связок $\hat{F}$ будет ясно из контекста, мы позволим себе писать Fm вместо $\mathrm{Fm}(\hat{F})$.

Пример 3.2.10. Пусть $\hat{F} = \{O^{(0)}, S^{(1)}, R^{(2)}, \circ^{(3)}\}$. Тогда последовательность

$$p_3,\ O,\ ROO,\ SO,\ p_1,\ Rp_1p_1,\ Rp_3SO,\ SSO,\ \circ Rp_3SO\,SSO\,Rp_1p_1.$$

[1] Разумеется, на языке множеств такое приписывание моделирует некоторая функция $\hat{F} \to \mathbb{N}$, но в этом и подобных случаях далее мы не станем загромождать изложение избыточной формалистикой, которую при желании легко восстановит педантичный читатель.

является построением для приведенного индуктивного определения, а значит, состоит из формул над $\hat{F}$. Как видит читатель, формулы даются в польской записи, что избавляет нас от употребления скобок.

Упражнение 3.2.11. Докажите, что язык $\mathrm{Fm}(\hat{F})$ является беспрефиксным, а приведенное его определение обладает свойством однозначности разбора.

Упражнение 3.2.12. Докажите, что $\mathrm{Fm}(\hat{F}) \sim \mathbb{N}$, если $\hat{F} \lesssim \mathbb{N}$, и $\mathrm{Fm}(\hat{F}) \sim \hat{F}$, если $\mathbb{N} \lesssim \hat{F}$.

Отметим, что в наших рассмотрениях множество $\hat{F}$ будет обычно конечным или счетным, а значит, и формул будет счетно много.

Технически важно сопоставить каждой формуле множество встречающихся в ней атомов. Это легко сделать, рекурсией по построению определив функцию $V\colon \mathrm{Fm}(\hat{F}) \to \mathcal{P}(\mathrm{At})$, т. ч.

$$V(p) = \{p\} \quad \text{и} \quad V(\hat{f}^{(n)}\varphi_1 \dots \varphi_n) = \cup_{1 \leqslant i \leqslant n} V(\varphi_i)$$

для всех $p \in \mathrm{At}, \hat{f} \in \hat{F}, \varphi_i \in \mathrm{Fm}(\hat{F})$. Как помнит читатель, однозначность разбора позволяет дать такое рекурсивное определение. Если $p \in V(\varphi)$, будем говорить, что *атом p входит*, или *имеет вхождение* в формулу φ.

Пример 3.2.13. Индукцией по построению докажем, что для любой $\varphi \in \mathrm{Fm}(\hat{F})$ множество $V(\varphi)$ конечно и, более того, $|V(\varphi)| \leqslant |\varphi|$.

Очевидно, достаточно проверить второе утверждение. Как помнит читатель, метод индукции по построению состоит в том, чтобы доказать, что множество Z формул $\varphi \in \mathrm{Fm}(\hat{F})$ со свойством $|V(\varphi)| \leqslant |\varphi|$ замкнуто относительно всех условий индуктивного определения множества $\mathrm{Fm}(\hat{F})$.

Это сводится к проверке того, что, во-первых, $|V(p)| \leqslant |p|$ для всех $p \in \mathrm{At}$ (что очевидно из определения V), а во-вторых, того что из $|V(\varphi_i)| \leqslant |\varphi_i|$ (т. е. $\varphi_i \in Z$) при всех $i \leqslant n$ следует $|V(\hat{f}\varphi_1 \dots \varphi_n)| \leqslant |\hat{f}\varphi_1 \dots \varphi_n|$ (т. е. $\hat{f}\varphi_1 \dots \varphi_n \in Z$) для любой связки $\hat{f}^{(n)}$.

Предположение вроде $\forall i \leqslant n\ \varphi_i \in Z$ о том, что «более простые» образующие формулы удовлетворяют требуемому свойству, в рассуждениях индукцией по построению мы будем называть *предположением индукции*, а вывод и него заключения вроде $\hat{f}\varphi_1 \dots \varphi_n \in Z$ будем называть *индукционным переходом* или *шагом индукции*. Таких шагов нужно проверить столько, сколько есть условий в индуктивном определении множества. В нашем случае для каждой связки $\hat{f}^{(n)}$ имеется

свой шаг. «Шаги», где предположение отсутствует, вроде $p \in Z$ при $p \in \mathrm{At}$, можно назвать *основанием* или *базисом индукции*.

Завершим проверку шага индукции. Имеем

$$|V(\hat{f}\varphi_1 \dots \varphi_n)| = |V(\varphi_1) \cup \dots \cup V(\varphi_n)| \leqslant$$
$$\leqslant |V(\varphi_1)| + \dots + |V(\varphi_n)| \leqslant |\varphi_1| + \dots + |\varphi_n| =$$
$$= |\varphi_1 \dots \varphi_n| < |\hat{f}\varphi_1 \dots \varphi_n|$$

в силу предположения индукции и следствия 2.2.8.

Пример 3.2.14. В условиях примера 3.2.10 имеем $V(p_3) = \{p_3\}$, $V(O) = V(ROO) = V(SO) = \varnothing$, $V(Rp_1p_1) = \{p_1\}$, $V(\circ Rp_3SO\,SSO\,Rp_1p_1) = \{p_1, p_3\}$.

Если $\vec{q} = (q_1, \dots, q_n)$ некоторый (*упорядоченный*) набор атомов, положим $\mathrm{Fm}(\hat{F}; \vec{q}) = \{\varphi \in \mathrm{Fm}(\hat{F}) \mid V(\varphi) \subseteq \{q_1, \dots, q_n\}\}$. Значение условия упорядоченности станет ясным позже. Кроме того, запись $\varphi(\vec{q})$, где φ означает какую-либо формулу над $\hat{F}$, будет предполагать, что $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$.

Пример 3.2.15. Имеем $Rp_1p_3 \in \mathrm{Fm}(\hat{F}; (p_1, p_2, p_3))$, однако $\circ p_1p_2p_4 \notin \mathrm{Fm}(\hat{F}; (p_1, p_2, p_3))$.

Множество связок $\hat{F}_{prop} = \{\wedge^{(2)}, \vee^{(2)}, \to^{(2)}, \leftrightarrow^{(2)}, \neg^{(1)}, \top^{(0)}, \bot^{(0)}\}$ традиционно используется в логике и имеет некоторое фиксированное значение, о котором мы скажем далее. Назовем множество $\mathrm{Fm}(\hat{F}_{prop})$ множеством *пропозициональных* формул и обозначим его символом Fm. Пропозициональные формулы мы будем без особых оговорок писать не только в польской, но и в инфиксной записи, которые станем рассматривать как синонимы, предполагая, что всегда выполним необходимый «перевод» (ср. пример 2.4.63 и последующие). Формально, множество инфиксных записей пропозициональных формул индуктивно определяется следующими свойствами:

$$\top, \bot \in \mathrm{Fm}_I;\ p \in \mathrm{At} \Longrightarrow p \in \mathrm{Fm}_I;$$
$$\varphi, \psi \in \mathrm{Fm}_I \Longrightarrow (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \to \psi), (\varphi \leftrightarrow \psi), \neg\varphi \in \mathrm{Fm}_I.$$

Упражнение 3.2.16. Докажите свойство беспрефиксности языка Fm_I и свойство однозначности разбора для его индуктивного определения. Сохранятся ли эти свойства, если отбросить скобки?

Упражнение 3.2.17. Дайте рекурсивные определения переводов $\mathrm{Fm} \to \mathrm{Fm}_I$ и $\mathrm{Fm}_I \to \mathrm{Fm}$.

Дополним соглашения о записи формул следующими положениями.

1) Буквы $p, q, r, s, p', q', q_i, \ldots$ и подобные обозначают в формулах некоторые элементы множества At, причем *разные* буквы, если не оговорено противное, обозначают *разные* элементы.

2) Разрешается в инфиксной записи опускать и добавлять внешние скобки. В польской записи разрешается добавлять внешние скобки и наследовать их в построении формулы (например, $(\wedge pq)$ и $\vee(\wedge pq)r$).

3) Разрешается писать $\varphi_1 * \varphi_2 * \ldots * \varphi_n$ вместо $((\ldots(\varphi_1 * \varphi_2) * \ldots) * \varphi_n)$ для $* \in \{\wedge, \vee\}$, т. е. символы $\wedge$ и $\vee$ *левоассоциативны*. Как мы увидим, это хорошо согласуется с естественным значением таких символов.

Пример 3.2.18. Слова $p \wedge q \wedge r$, $(((p \wedge q \wedge r)))$ и $\wedge \wedge pqr$ обозначает ту же формулу, что и слово $((p \wedge q) \wedge r)$. Имеет место $p \wedge q \wedge r = ((p \wedge q) \wedge r)$. Однако $p \wedge q \wedge r \neq (p \wedge (q \wedge r))$.

Значение формулы. Как мы уже сказали, формулу можно рассматривать как «программу» для вычисления функции, если придать связкам определенный смысл. Определим функцию, вычисляемую такой «программой» формально.

Прежде всего, допустим, что что каждой связке $\hat{f}^{(n)} \in \hat{F}$ поставлена в соответствие булева функция $f\colon \underline{2}^n \to \underline{2}$. Такое соответствие называется *интерпретацией* множества связок $\hat{F}$.

Любую функцию $\xi\colon \mathrm{At} \to \underline{2}$ назовем *оценкой*. Содержательно, оценка определяет значения, передаваемые «программе» на вход.

Для любой оценки ξ функция $[\cdot](\xi)\colon \mathrm{Fm}(\hat{F}) \to \underline{2}$ определяется рекурсией по построению элементов множества $\mathrm{Fm}(\hat{F})$, т. ч. она удовлетворяет условиям:

$$[p](\xi) = \xi(p); \quad [\hat{f}^{(n)}\varphi_1 \ldots \varphi_n](\xi) = f([\varphi_1](\xi), \ldots, [\varphi_n](\xi))$$

для всех $p \in \mathrm{At}, \hat{f} \in \hat{F}, \varphi_i \in \mathrm{Fm}(\hat{F})$.

Пример 3.2.19. Пусть $\hat{F} = \{O^{(0)}, S^{(1)}, R^{(2)}, \circ^{(3)}\}$ и фиксирована следующая интерпретация связок: $O \mapsto 0$, $S \mapsto \mathrm{not}$, $R \mapsto \mathrm{and}$ и $\circ \mapsto f$, где $f(x, y, z) = x + y + z$. Допустим также, что $\xi(p_1) = 1$ и $\xi(q) = 0$ для

всех $q \neq p_1$. Тогда

$$[\circ Rp_3SO\, SSO\, Rp_1p_1](\xi) = [Rp_3SO](\xi) + [SSO](\xi) + [Rp_1p_1](\xi) = \\ \mathrm{and}(\xi(p_1), \mathrm{not}(0)) + \mathrm{not}(\mathrm{not}(0)) + \mathrm{and}(\xi(p_1), \xi(p_1)) = \\ \mathrm{and}(0,1) + \mathrm{not}(1) + \mathrm{and}(1,1) = 0 + 0 + 1 = 1.$$

Мы будем называть *стандартной* следующую интерпретацию множества связок $\hat{F}_{prop}$:

$$\wedge \mapsto \mathrm{and},\ \vee \mapsto \mathrm{or},\ \to \mapsto \mathrm{imp},\ \leftrightarrow \mapsto \mathrm{eq},\ \neg \mapsto \mathrm{not},\ \top \mapsto 1,\ \bot \mapsto 0.$$

Если не оговорено иное, мы всегда предполагаем стандартную интерпретацию этих связок.

Немного злоупотребляя обозначениями, будем символом $\wedge$ обозначать не только связку, которую станем называть *конъюнкцией*, но и соответствующую ей функцию and. Аналогично поступим с другими связками. Также распространим на функции соглашение об инфиксной записи (что мы уже молчаливо сделали для $+$). Теперь, например, осмысленно выражение $0 \to (1 \wedge 0) = 1$ и т. п.

Замечание 3.2.20. Искушение смешать связки («имена») с функциями («значениями») весьма велико. До некоторой степени такое смешение технически удобно, но мы предостерегаем читателя: не следует забывать, что это, вообще говоря, *разные вещи*, хотя бы и обозначенные для краткости одним символом! (Скажем, интерпретация может и не быть стандартной.) В каждом контексте читатель должен иметь точный ответ на вопрос, что же именно имеется в виду.

Пример 3.2.21. Пусть $\varphi = \neg r \to (p \vee q)$ и оценка ξ такова, что $\xi(p) = 1$, $\xi(q) = 0$ и $\xi(r) = 0$. Тогда

$$[\varphi](\xi) = \mathrm{imp}([\varphi](\neg r), [\varphi](p \vee q)) = \\ \mathrm{imp}(\mathrm{not}([r](\xi)), \mathrm{or}([p](\xi), [q](\xi)) = \mathrm{imp}(\mathrm{not}(\xi(r)), \mathrm{or}(\xi(p), \xi(q))) = \\ \neg 0 \to (1 \vee 0) = 1 \to 1 = 1.$$

Как, быть может, уже заметил читатель, значение $[\varphi](\xi)$ зависит от значения оценки ξ лишь на атомах из $V(\varphi)$. Вот формальное выражение этой идеи.

Лемма 3.2.22. *Пусть* $\varphi \in \mathrm{Fm}(\hat{F})$ *и* $\xi, \eta \colon \mathrm{At} \to \underline{2}$. *Тогда если* $\xi \restriction V(\varphi) = \eta \restriction V(\varphi)$, *то* $[\varphi](\xi) = [\varphi](\eta)$.

Доказательство. Индукция по построению φ. Нужно убедиться, что множество формул, для которых верно равенство $[\varphi](\xi) = [\varphi](\eta)$ в предположении $\xi \restriction V(\varphi) = \eta \restriction V(\varphi)$, замкнуто относительно всех условий индуктивного определения $\mathrm{Fm}(\hat{F})$.

Действительно, если $\varphi = p \in \mathrm{At}$, то $[\varphi](\xi) = \xi(p)$ и $[\varphi](\eta) = \eta(p)$. Очевидно, $p \in V(\varphi)$, а значит, $\xi(p) = \eta(p)$ по условию, откуда $[\varphi](\xi) = [\varphi](\eta)$.

Предположим теперь, что для некоторых формул $\varphi_1, \ldots, \varphi_n$ из $\xi \restriction V(\varphi_i) = \eta \restriction V(\varphi_i)$ следует, что $[\varphi_i](\xi) = [\varphi_i](\eta)$. Тогда рассмотрим формулу $\varphi = \hat{f}^{(n)}\varphi_1 \ldots \varphi_n$ и допустим, что $\xi \restriction V(\varphi) = \eta \restriction V(\varphi)$. Заметим, что если $p \in V(\varphi_i)$, то $p \in V(\varphi_1) \cup \ldots \cup V(\varphi_n) = V(\varphi)$, а значит, $\xi(p) = \eta(p)$. Таким образом, $\xi \restriction V(\varphi_i) = \eta \restriction V(\varphi_i)$ при всех i, что по предположению индукции дает $[\varphi_i](\xi) = [\varphi_i](\eta)$. Отсюда

$$[\varphi](\xi) = [\hat{f}\varphi_1 \ldots \varphi_n](\xi) = f([\varphi_1](\xi), \ldots, [\varphi_n](\xi)) = \\ f([\varphi_1](\eta), \ldots, [\varphi_n](\eta)) = [\hat{f}\varphi_1 \ldots \varphi_n](\eta) = [\varphi](\eta).$$

□

Итак оценка ξ содержит информацию, излишнюю для вычисления значения $[\varphi](\xi)$. Очевидно, такой информацией являются значения переменных вне $V(\varphi)$. Если, например, $\varphi = \neg p \to (q \vee r)$, то достаточно задать функцию $\xi \restriction \{p, q, r\}$, которая, как функция из конечного множества, в свою очередь, задается набором своих значений. Например, набором $\vec{x} = (1, 0, 0)$. Таким образом, мы сможем определить *значение* $[\varphi](\vec{x})$ *формулы* φ *на наборе* $\vec{x}$. Это соответствует пониманию формулы как программы, которая принимает на вход значения своих аргументов-атомов — набор $\vec{x}$.

Однако остается вопрос: *какая компонента набора какому атому соответствует?* Какие у нас есть основания оценить единицей именно p, а не q или r?

На этот вопрос легко ответить, если *упорядочить* множество переменных, встречающихся в формуле. Именно, если фиксирован некоторый набор $\vec{q} = (q_1, \ldots, q_n)$, где все $q_i \in \mathrm{At}$ попарно различны,[2] то для всякого $\vec{x} = (x_1, \ldots, x_n) \in \underline{2}^n$ положим

$$\xi_{\vec{x}}(p) \quad = \quad \begin{cases} x_i, & \text{если } p = q_i; \\ 0, & \text{если } p \neq q_i \text{ для всех } i. \end{cases}$$

[2]Напомним, что это следует из наших соглашений о записи формул, поскольку сами символы $q_1, \ldots, q_n$ попарно различные.

Если $\varphi \in \mathrm{Fm}(\hat{F};\vec{q})$, то положим $[\varphi](\vec{x}) = [\varphi](\xi_{\vec{x}})$. Очевидно, тогда $\xi \restriction V(\varphi) = \xi_{(\xi(q_1),\ldots,\xi(q_n))} \restriction V(\varphi)$ для любой оценки ξ.

Следствие 3.2.23. *Для любой формулы $\varphi \in \mathrm{Fm}(\hat{F};\vec{q})$ и любой оценки $\xi\colon \mathrm{At} \to \underline{2}$ верно*

$$[\varphi](\xi) = [\varphi](\xi(q_1),\ldots,\xi(q_n)).$$

Это еще одна формулировка того факта, что значение формулы при оценке определяется лишь значениями входящих в нее атомов.

Обратите внимание, что использование бесконечных оценок $\mathrm{At} \to \underline{2}$ вместо конечных наборов, как будто излишнее, дает техническое упрощение — избавляет нас от интереса к тому, какие атомы входят в формулу и в каком порядке их следует оценивать.

Теперь, наконец, мы можем определить булеву функцию, которую вычисляет формула-«программа». Пусть $\varphi \in \mathrm{Fm}(\hat{F};(q_1,\ldots,q_n))$. Формуле φ поставим в соответствие функцию $f_\varphi\colon \underline{2}^n \to \underline{2}$, т. ч.

$$f_\varphi(\vec{x}) = [\varphi](\vec{x})$$

при всех $\vec{x} \in \underline{2}^n$. Соответственно, скажем, что формула φ *представляет (*или *вычисляет)* функцию f, если $f = f_\varphi$.

Пример 3.2.24. Формулы p, $p\wedge p$, $p\vee(q\wedge\neg q)$ $\in \mathrm{Fm}(p,q)$ представляют функцию π^1_2. Если рассмотреть набор переменных (p), то формулы p и $p\wedge p$ из $\mathrm{Fm}(p)$ будут представлять функцию $\pi^1_1 \neq \pi^1_2$. Для формулы $p \to q \in \mathrm{Fm}(p,q)$ имеем $f_\varphi(1,0) = 0$, но если зафиксировать набор (q,p) (что *подразумевается* в выражении $p \to q \in \mathrm{Fm}(q,p)$), получится $f_\varphi(1,0) = 1$.

Итак, функция f_φ определяется не только формулой φ, но также выбранным порядком атомов и, конечно, интерпретацией связок.

Нормальные формы. Естественно возникает вопрос: всякую ли булеву функцию вычисляет некоторая формула? Ответ на этот вопрос тривиален, если мы никак не ограничены в выборе связок и их интерпретаций: любой функции $f \in B_n$ можно поставить в соответствие связку $\hat{f}^{(n)}$ и получить $f = f_\varphi$ для $\varphi = \hat{f}p_1\ldots p_n$.

Значительно более интересен случай, когда связки их интерпретация фиксированы. Оказывается, любая булева функция представима формулой в стандартной интерпретации, причем такой формуле можно придать весьма специальный вид.

Формула вида p или $\neg p$, где $p \in \mathrm{At}$, называется *литералом*. Формула вида $l_1 \wedge \ldots \wedge l_m$, где $m \geqslant 1$ и все l_i суть литералы, называется

элементарной конъюнкцией. Формула вида $c_1 \vee \ldots \vee c_k$, где $k \geqslant 1$ и все c_j суть элементарные конъюнкции, называется *дизъюнктивной нормальной формой (д. н. ф.).*

Пример 3.2.25. Формулы $\neg q$, $p \wedge r$, $(\neg q \wedge p) \vee \neg r \vee (p \wedge \neg p)$ являются д. н. ф., а формула $p \wedge (q \vee r)$ не является.

Теорема 3.2.26. *Для любой функции $f\colon \underline{2}^n \to \underline{2}$, где $n \geqslant 1$, существует д. н. ф. $\varphi \in \mathrm{Fm}(q_1, \ldots, q_n)$, т. ч. $f_\varphi = f$.*

Доказательство. Идея состоит в том, чтобы закодировать множество $U = \{\vec{x} \in \underline{2}^n \mid f(\vec{x}) = 1\}$ «единиц» функции f с помощью элементарных конъюнкций.

Если $U = \varnothing$, то $f(\vec{x}) = 0$ при всех $\vec{x} \in \underline{2}^n$, поэтому достаточно положить $\varphi = q_1 \wedge \neg q_1$, ибо эта формула всегда принимает значение 0. Допустим, что $U \neq \varnothing$. Для произвольных $p \in \mathrm{At}$ и $\sigma \in \underline{2}$ обозначим

$$p^\sigma \quad = \quad \begin{cases} p, & \text{если } \sigma = 1; \\ \neg p, & \text{если } \sigma = 0. \end{cases}$$

Непосредственно проверяется следующее утверждение:

$$[p^\sigma](x) = 1 \iff x = \sigma$$

для любых $x, \sigma \in \underline{2}$. Поскольку конъюнкция принимает значение 1, если и только если все ее члены приняли такое значение, имеем

$$[q_1^{\sigma_1} \wedge \ldots \wedge q_n^{\sigma_n}](\vec{x}) = 1 \iff \vec{x} = \vec{\sigma}$$

для всех $\vec{x}, \vec{\sigma} = (\sigma_1, \ldots, \sigma_n) \in \underline{2}^n$. Итак, элементарная конъюнкция $q_1^{\sigma_1} \wedge \ldots \wedge q_n^{\sigma_n}$ истинна только на наборе $\vec{\sigma}$ и, таким образом, может «кодировать» этот набор.

Положим $\varphi = \bigvee_{\vec{\sigma} \in U} q_1^{\sigma_1} \wedge \ldots \wedge q_n^{\sigma_n}$. Очевидно, это д. н. ф. (в формуле присутствует хотя бы одна элементарная конъюнкция). Поскольку дизъюнкция принимает значение 1, если и только если хотя бы один ее член принял такое значение, имеем

$$\begin{array}{rcl} f_\varphi(\vec{x}) = 1 & \iff & [\varphi](\vec{x}) = 1 \\ & \iff & \exists \vec{\sigma} \in U\ [q_1^{\sigma_1} \wedge \ldots \wedge q_n^{\sigma_n}](\vec{x}) = 1 \\ & \iff & \exists \vec{\sigma} \in U\ \vec{x} = \vec{\sigma} \\ & \iff & \vec{x} \in U \\ & \iff & f(\vec{x}) = 1. \end{array}$$

Так как булевы функции принимают не более двух значений, отсюда вытекает, что $f_\varphi(\vec{x}) = f(\vec{x})$ при всех $\vec{x} \in \underline{2}^n$, т. е. $f_\varphi = f$. $\square$

Замечание 3.2.27. Приведенное доказательство позволяет алгоритмически построить по функции (как конечному множеству пар) представляющую ее д. н. ф. Например, если функция $f\colon \underline{2}^4 \to \underline{2}$ принимает значение 1 лишь на наборах $(1,0,1,1), (1,1,0,1), (1,1,1,1)$, задавшись набором атомов (p,q,r,s), можно положить

$$\varphi = (p \wedge \neg q \wedge r \wedge s) \vee (p \wedge q \wedge \neg r \wedge s) \vee (p \wedge q \wedge r \wedge s).$$

Ясно также, что д. н. ф. для f не единственна даже во множестве $\mathrm{Fm}(p,q,r,s)$. Отступая от схемы из доказательства, мы могли бы взять еще

$$\varphi' = (p \wedge q \wedge s) \vee (p \wedge r \wedge s).$$

Замечание 3.2.28. То, что теорема 3.2.26 ограничивается функциями лишь ненулевого числа аргументов, несущественно. Во-первых, мы можем представить две константы с помощью д. н. ф. $q_1 \wedge \neg q_1$ и $q_1 \vee \neg q_1$ — разумеется, содержащими не нуль, а один атом каждая. А во-вторых, можно объявить д. н. ф. связки $\bot$ и $\top$.

Кроме д. н. ф., важную роль играют «двойственные» *конъюнктивные нормальные формы (к. н. ф.)*: мы называем таковой конъюнкцию нескольких элементарных дизъюнкций, под *элементарной дизъюнкцией* понимая дизъюнкцию нескольких литералов.

Пример 3.2.29. Формулы $\neg q$, $p \wedge r$, $(p \vee p) \wedge (\neg q \vee r)$ являются к. н. ф., а формула $(\neg q \wedge p) \vee \neg r \vee (p \wedge \neg p)$ не является.

Упражнение 3.2.30. Какие формулы являются вместе и д. н. ф., и к. н. ф.?

Упражнение 3.2.31. Сформулируйте и докажите для к. н. ф. аналог теоремы 3.2.26, причем используйте кодирование наборов, где функция принимает значение 0, с помощью к. н. ф.

§ 3.3. Логика высказываний

Формулы p и $p \wedge p$ различны, однако вычисляют одну и ту же функцию. Это вполне соответствует «программистской» интуиции: одну и ту же задачу могут решать весьма разные программы — разной длины или требующие различных затрат времени на исполнение. Тем не менее «эквивалентность» таких программ существенна и заслуживает рассмотрения. С логической точки зрения, эквивалентные формулы обозначают высказывания с одинаковым «смыслом».

Под *логикой высказываний* обычно понимают совокупность всех пар эквивалентных *пропозициональных* формул при *стандартной* их интерпретации. Мы, однако, сформулируем ряд утверждений для произвольного множества связок и произвольной его интерпретации.

До конца раздела мы считаем, что фиксирована некоторая интерпретация множества связок $\hat{F}$, а связки из $\hat{F}_{prop}$ всегда имеют стандартную интерпретацию.

Эквивалентность. Скажем, что формулы $\varphi, \psi \in \mathrm{Fm}(\hat{F})$ *эквивалентны*, если для всех оценок $\xi\colon \mathrm{At} \to \underline{2}$ верно

$$[\varphi](\xi) = [\psi](\xi).$$

Тогда пишем $\varphi \equiv \psi$. Эквивалентность — одно из центральных понятий логики.

Лемма 3.3.1. *Для всех $\varphi, \psi, \theta, \varphi_i, \psi_i \in \mathrm{Fm}(\hat{F})$ верно:*

1) $\varphi \equiv \varphi$;

2) *если* $\varphi \equiv \psi$, *то* $\psi \equiv \varphi$;

3) *если* $\varphi \equiv \psi$ *и* $\psi \equiv \theta$, *то* $\varphi \equiv \theta$;

4) *если* $\varphi_1 \equiv \psi_1, \ldots, \varphi_n \equiv \psi_n$ *и* $\hat{f}^{(n)} \in \hat{F}$, *то* $\hat{f}\varphi_1 \ldots \varphi_n \equiv \hat{f}\psi_1 \ldots \psi_n$.

Доказательство. Первые три утверждения очевидны и означают, что $\equiv$ в самом деле является отношением эквивалентности на множестве $\mathrm{Fm}(\hat{F})$. Проверим четвертое утверждение. Имеем

$$[\hat{f}\varphi_1 \ldots \varphi_n](\xi) = f([\varphi_1](\xi), \ldots, [\varphi_n](\xi)) = \\ = f([\psi_1](\xi), \ldots, [\psi_n](\xi)) = [\hat{f}\psi_1 \ldots \psi_n](\xi).$$

□

Если фиксирован набор переменных, эквивалентность формул в самом деле означает совпадение вычисляемых ими функций.

Лемма 3.3.2. *Пусть $\varphi, \psi \in \mathrm{Fm}(\hat{F}; \vec{q})$. Тогда $\varphi \equiv \psi$, если и только если $f_\varphi = f_\psi$.*

Доказательство. Для любого набора $\vec{x}$ из $\varphi \equiv \psi$ следует

$$f_\varphi(\vec{x}) = [\varphi](\vec{x}) = [\varphi](\xi_{\vec{x}}) = [\psi](\xi_{\vec{x}}) = [\psi](\vec{x}) = f_\psi(\vec{x}).$$

Обратно, предположив $f_\varphi = f_\psi$, в силу следствия 3.2.23, имеем

$$[\varphi](\xi) = [\varphi](\xi(\vec{q})) = f_\varphi(\xi(\vec{q})) = f_\psi(\xi(\vec{q})) = [\psi](\xi(\vec{q})) = [\psi](\xi)$$

для любой оценки ξ, где выражение $\xi(\vec{q})$ означает $(\xi(q_1), \ldots, \xi(q_n))$. □

Следствие 3.3.3. *Для всякой формулы $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$ существует д. н. ф. (к. н. ф.) $\psi \in \mathrm{Fm}(\{\neg, \wedge, \vee\}; \vec{q})$, т. ч. $\psi \equiv \varphi$.*

Доказательство. Согласно теореме 3.2.26 (соответственно, упражнению 3.2.31), существует д. н. ф. (к. н. ф.) $\psi \in \mathrm{Fm}(\{\neg, \wedge, \vee\}; \vec{q})$, т. ч. $f_\psi = f_\varphi$. Поскольку $\varphi, \psi \in \mathrm{Fm}(\hat{F} \cup \{\neg, \wedge, \vee\}; \vec{q})$, можно применить лемму 3.3.2, получая $\psi \equiv \varphi$. □

Таким образом, каждая формула, с точностью до эквивалентности, может рассматриваться как д. н. ф. (или к. н. ф.). Поскольку нормальные формы имеют очень простое строение, многие рассуждения при этом упрощаются.

С «программистской» точки зрения, наше следствие означает, что «язык программирования» с одними лишь отрицанием, конъюнкцией и дизъюнкцией «универсален», позволяя решить любую задачу, решаемую с помощью булевых формул.

Заметим, что это не единственный такой конечный «универсальный язык». По меньшей мере, возможно обойтись без конъюнкции либо дизъюнкции, используя эквивалентности $\varphi \wedge \psi \equiv \neg(\neg\varphi \vee \neg\psi)$ и $\varphi \vee \psi \equiv \neg(\neg\varphi \wedge \neg\psi)$. Более основательное исследование этих вопросов, относящееся, скорее, к алгебре, чем к логике, читатель найдет в § 3.5.

Мы видели, что $\equiv$ есть отношение эквивалентности на множестве формул. Как устроено соответствующее фактор-множество?

Лемма 3.3.4.

1) $|\mathrm{Fm}(\hat{F}; q_1, \ldots, q_n)/{\equiv}| \leqslant 2^{2^n}$, *причем неравенство обращается в равенство, если* $\{\neg, \wedge, \vee\} \subseteq \hat{F}$;

2) $\mathrm{Fm}(\hat{F})/{\equiv} \sim \mathbb{N}$.

Доказательство. Проверим первое утверждение. Каждой формуле $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$ соответствует функция $f_\varphi \in B_n$. Вообще говоря, это соответствие не инъективно, однако $f_\varphi = f_\psi$ равносильно $\varphi \equiv \psi$ по лемме 3.3.2. Поэтому если каждому классу $[\varphi]_\equiv$ поставить в соответствие функцию f_φ, получится инъекция из $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$ в B_n. В силу леммы 3.2.7 и принципа Дирихле, получаем требуемое неравенство. С

другой стороны, если $\{\neg, \wedge, \vee\} \subseteq \hat{F}$, то всякая функция $f \in B_n$ есть f_φ для некоторой $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$ вследствие теоремы 3.2.26. Это означает, что построенная инъекция является биекцией, а неравенство обращается в равенство.

Установим второе утверждение. Различные атомы не эквивалентны, а значит, $\mathbb{N} \sim \mathrm{At} \lesssim \mathrm{Fm}(\hat{F})/\equiv$. С другой стороны, рассмотрим произвольный класс $X \in \mathrm{Fm}(\hat{F})/\equiv$. Возьмем наименьшее такое $n \in \mathbb{N}$, что множество $X_n = X \cap \mathrm{Fm}(\hat{F}; p_0, \ldots, p_{n-1})$ непусто. Легко видеть, что $X_n \in \mathrm{Fm}(\hat{F}; p_0, \ldots, p_{n-1})/\equiv$. Поэтому отображение $X \mapsto X_n$ есть инъекция из $\mathrm{Fm}(\hat{F})/\equiv$ в $\bigcup_{n\in\mathbb{N}} \mathrm{Fm}(\hat{F}; p_0, \ldots, p_{n-1})/\equiv$. В силу первого утверждение и теоремы 2.2.33, последнее множество конечно или счетно, а значит, $\mathrm{Fm}(\hat{F})/\equiv \lesssim \mathbb{N}$. □

Подстановка. Еще одним важным логическим понятием является *подстановка*, которая для булевых формул понимается следующим образом. Если $\varphi, \psi \in \mathrm{Fm}(\hat{F})$ и $p \in \mathrm{At}$, то выражением $\varphi[\psi/p]$ мы обозначим результат замены всех вхождений p в φ на ψ.

Чтобы использовать это понятие в строгих доказательствах (и, в частности, доказать, что $\varphi[\psi/p] \in \mathrm{Fm}(\hat{F})$), полезно дать ему формальное определение. Именно, для всех ψ и p мы определим функцию $(\cdot)\,[\psi/p] \colon \mathrm{Fm}(\hat{F}) \to \mathrm{Fm}(\hat{F})$ рекурсией по построению элементов $\mathrm{Fm}(\hat{F})$:

$$p[\psi/p] = \psi; \quad q[\psi/p] = q, \text{ если } q \neq p;$$
$$(\hat{f}\varphi_1 \ldots \varphi_n)[\psi/p] = \hat{f}(\varphi_1[\psi/p]) \ldots (\varphi_n[\psi/p]).$$

Пример 3.3.5. $(p \to (q \to p))[(r \vee p)/p] = (r \vee p) \to (q \to (r \vee p))$.

Замечание 3.3.6. Обратите внимание, что порядок, в котором выполняются подстановки, существен. Например, $(p[q/p])[r/q] = r$, хотя $(p[r/q])[q/p] = q$. Поэтому, если требуется подставить сразу несколько формул на место нескольких атомов, удобно дать рекурсивное определение *одновременной подстановке* $\varphi[\psi_1/q_1, \ldots, \psi_n/q_n]$.

Упражнение 3.3.7. Дайте определение одновременной подстановки $(\cdot)[\psi_1/q_1, \ldots, \psi_n/q_n]$.

Упражнение 3.3.8. Покажите, как можно обойтись без одновременных подстановок, используя лишь подстановки вида $[\psi/q]$ и некоторый запас «свежих», не встречающихся в рассматриваемых формулах атомов. Иначе говоря, докажите, что для любых $q_1, \ldots, q_n \in \mathrm{At}$

и $\varphi, \psi_1, \ldots, \psi_n \in \mathrm{Fm}(\hat{F})$ существуют $r_1, \ldots, r_m \in \mathrm{At}$ и $\theta_1, \ldots, \theta_m \in \mathrm{Fm}(\hat{F})$, т. ч.

$$\varphi[\psi_1/q_1, \ldots, \psi_n/q_n] = \varphi[\theta_1/r_1] \ldots [\theta_m/r_m].$$

Можно достичь большей общности и объявить *(абстрактной) подстановкой* каждую функцию $\sigma\colon \mathrm{Fm}(\hat{F}) \to \mathrm{Fm}(\hat{F})$, коммутирующую со связками, т. е. такую что

$$\sigma(\hat{f}\varphi_1 \ldots \varphi_n) = \hat{f}\sigma(\varphi_1) \ldots \sigma(\varphi_n)$$

для любых $\hat{f} \in \hat{F}$, $\varphi_1, \ldots, \varphi_n \in \mathrm{Fm}(\hat{F})$. Ясно, что любая (одновременная) подстановка является абстрактной подстановкой.

Упражнение 3.3.9. Докажите, что любая абстрактная подстановка σ выражается через одновременную в следующем смысле: для любых $q_1, \ldots, q_n \in \mathrm{At}$ существуют формулы $\psi_1, \ldots, \psi_n \in \mathrm{Fm}(\hat{F})$ т. ч. $\sigma(\varphi) = \varphi[\psi_1/q_1, \ldots, \psi_n/q_n]$ для каждой $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$.

Подстановка, как показывает следующая лемма, в некотором смысле, коммутирует с оценкой переменных.

Лемма 3.3.10. *Для любых $\varphi, \psi \in \mathrm{Fm}(\hat{F})$, $p \in \mathrm{At}$ и $\xi\colon \mathrm{At} \to \underline{2}$ имеет место $[\varphi[\psi/p]](\xi) = [\varphi](\xi_p^\psi)$, где оценка ξ_p^ψ такова, что*

$$\xi_p^\psi(q) \quad = \quad \begin{cases} [\psi](\xi), & \text{если } q = p; \\ \xi(q) & \text{иначе.} \end{cases}$$

Доказательство. Индукция по построению формулы φ. Если $\varphi = p$, то $[\varphi[\psi/p]](\xi) = [\psi](\xi) = \xi_p^\psi(p) = [\varphi](\xi_p^\psi)$. Если же $\varphi = q \neq p$, имеем $[\varphi[\psi/p]](\xi) = [q](\xi) = \xi(q) = \xi_p^\psi(q) = [\varphi](\xi_p^\psi)$.

Допустим, наконец, что $\varphi = \hat{f}\varphi_1 \ldots f_n$. Тогда, используя предположение индукции для формул φ_i, получаем

$$\begin{aligned} [\varphi[\psi/p]](\xi) = [\hat{f}(\varphi_1[\psi/p]) \ldots (\varphi_n[\psi/p])](\xi) = \\ = f([\varphi_1[\psi/p]](\xi), \ldots, [\varphi_n[\psi/p]](\xi)) = f([\varphi_1](\xi_p^\psi), \ldots, [\varphi_n](\xi_p^\psi)) = \\ = [\hat{f}\varphi_1 \ldots \varphi_n](\xi_p^\psi) = [\varphi](\xi_p^\psi). \end{aligned}$$

□

Теперь мы можем сформулировать важное утверждение: эквивалентность сохраняется при подстановке.

Теорема 3.3.11. *Пусть* $\varphi, \psi, \psi' \in \mathrm{Fm}(\hat{F})$, $p \in \mathrm{At}$ *и* $\psi \equiv \psi'$. *Тогда*

1) $\varphi[\psi/p] \equiv \varphi[\psi'/p]$;

2) $\psi[\varphi/p] \equiv \psi'[\varphi/p]$.

Доказательство. Первое утверждение доказывается индукцией по построению φ с помощью леммы 3.3.1. Действительно, если $\varphi = p$, то $\varphi[\psi/p] = \psi \equiv \psi' = \varphi[\psi'/p]$. Если же $\varphi = q \neq p$, то $\varphi[\psi/p] = q = \varphi[\psi'/p]$. Остается предположить $\varphi = \hat{f}\varphi_1 \dots \varphi_n$ и воспользоваться предположением индукции для φ_i:

$$\varphi[\psi/p] = \hat{f}(\varphi_1[\psi/p]) \dots (\varphi_n[\psi/p]) \equiv \\ \equiv \hat{f}(\varphi_1[\psi'/p]) \dots (\varphi_n[\psi'/p]) = \varphi[\psi'/p].$$

Второе утверждение сразу следует из леммы 3.3.10, поскольку для каждой оценки ξ имеем:

$$[\psi[\varphi/p]](\xi) = [\psi](\xi_p^{\varphi}) = [\psi'](\xi_p^{\varphi}) = [\psi'[\varphi/p]](\xi).$$

□

Пример 3.3.12. Одно из применений первого утверждения теоремы — возможность заменять на эквивалентную любое вхождение подформулы в данную формулу (мы рассматриваем понятие *вхождение подформулы* интуитивно).

В самом деле, очевидно $p \equiv \neg\neg p$. Чтобы заменить в формуле

$$\varphi = (\neg\neg p \to (\neg\neg p \to (r \wedge (p \vee q)))) \vee (\neg\neg p \wedge q)$$

на p лишь самое левое и самое правое вхождения подформулы $\neg\neg p$, получая

$$\varphi' = (p \to (\neg\neg p \to (r \wedge (p \vee q)))) \vee (p \wedge q),$$

рассмотрим формулу

$$\theta = (s \to (\neg\neg p \to (r \wedge (p \vee q)))) \vee (s \wedge q).$$

Тогда, согласно теореме,

$$\varphi = \theta[\neg\neg p/s] \equiv \theta[p/s] = \varphi',$$

т. е. $\varphi \equiv \varphi'$, как того и требует наша интуиция.

Наконец, приведем некоторые эквивалентности, важные с логической точки зрения.

Лемма 3.3.13. *Для любых формул* $\varphi, \psi, \theta \in \mathrm{Fm}(\hat{F})$ *имеет место:*

$$\varphi \equiv \varphi \wedge \varphi; \quad \varphi \wedge \psi \equiv \psi \wedge \varphi; \quad (\varphi \wedge \psi) \wedge \theta \equiv \varphi \wedge (\psi \wedge \theta);$$
$$\varphi \equiv \varphi \vee \varphi; \quad \varphi \vee \psi \equiv \psi \vee \varphi; \quad (\varphi \vee \psi) \vee \theta \equiv \varphi \vee (\psi \vee \theta);$$
$$\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta); \quad \varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta);$$
$$\neg\neg\varphi \equiv \varphi; \quad \neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi; \quad \neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi;$$
$$\varphi \wedge \top \equiv \varphi; \quad \varphi \vee \top \equiv \top; \quad \varphi \wedge \bot \equiv \bot; \quad \varphi \vee \bot \equiv \varphi;$$
$$\neg\top \equiv \bot; \quad \neg\bot \equiv \top; \quad \varphi \wedge \neg\varphi \equiv \bot; \quad \varphi \vee \neg\varphi \equiv \top;$$
$$\varphi \to \psi \equiv \neg\varphi \vee \psi; \quad \neg(\varphi \to \psi) \equiv \varphi \wedge \neg\psi; \quad \varphi \to \psi \equiv \neg\psi \to \neg\varphi;$$
$$\varphi \to \top \equiv \top; \quad \bot \to \varphi \equiv \top; \quad \top \to \varphi \equiv \varphi; \quad \varphi \to \bot \equiv \neg\varphi;$$
$$\varphi \leftrightarrow \psi \equiv (\varphi \to \psi) \wedge (\psi \to \varphi); \quad \varphi \to (\psi \to \theta) \equiv (\varphi \wedge \psi) \to \theta.$$

Доказательство. Эти эквивалентности легко получить из равенств леммы 3.2.2. Например, при любой оценке ξ верно

$$[\varphi \wedge (\psi \vee \theta)](\xi) = \mathrm{and}([\varphi](\xi), \mathrm{or}([\psi](\xi), [\theta](\xi))) =$$
$$\mathrm{or}(\mathrm{and}([\varphi](\xi), [\psi](\xi)), \mathrm{and}([\varphi](\xi), [\theta](\xi))) = [(\varphi \wedge \psi) \vee (\varphi \wedge \theta)](\xi).$$

□

Тавтологии и выполнимость. Формула $\varphi \in \mathrm{Fm}(\hat{F})$ называется *тавтологией*, если *при любой* оценке ξ имеет место $[\varphi](\xi) = 1$.

Формула $\varphi \in \mathrm{Fm}(\hat{F})$ называется *выполнимой*, если *существует* оценка ξ, т. ч. $[\varphi](\xi) = 1$. Сама оценка ξ, для которой $[\varphi](\xi) = 1$, называется *выполняющей* формулу φ.

При наличии связки $\neg$ тавтологичность и выполнимость выражаются друг через друга.

Лемма 3.3.14. *Для любой формулы* $\varphi \in \mathrm{Fm}(\hat{F})$ *верно:*

1) φ *тавтология тогда и только тогда, когда* $\neg\varphi$ *не выполнима;*

2) φ *выполнима тогда и только тогда, когда* $\neg\varphi$ *не тавтология.*

Аналогичным образом, взаимно выражаются тавтологичность и эквивалентность.

Лемма 3.3.15. *Для любых формул* $\varphi, \psi \in \mathrm{Fm}(\hat{F})$ *верно:*

1) φ *тавтология тогда и только тогда, когда* $\varphi \equiv \top$*;*

2) $\varphi \equiv \psi$ *только тогда, когда* $\varphi \leftrightarrow \psi$ *тавтология.*

Доказательство. Для второго утверждения заметим, что $[\varphi \leftrightarrow \psi](\xi) = 1$ тогда и только тогда, когда $\mathrm{eq}([\varphi](\xi), [\psi](\xi)) = 1$, что, по определению функции eq, равносильно $[\varphi](\xi) = [\psi](\xi)$. □

Таким образом, нет существенной разницы, понимать ли под логикой высказываний множество пар эквивалентных формул, или множество тавтологий или же множество выполнимых формул.

Следствие 3.3.16. *Если* φ *тавтология, то для любых* ψ *и* p *формула* $\varphi[\psi/p]$ *также является тавтологией.*

Доказательство. Имеем $\varphi \equiv \top$, откуда $\varphi[\psi/p] \equiv \top[\psi/p] = \top$ по теореме 3.3.11. □

Упражнение 3.3.17. Сформулируйте и докажите аналогичное утверждение для выполнимости.

Как проверить, является ли формула $\varphi \in \mathrm{Fm}(\hat{F}; \vec{q})$ тавтологией? Очевидно, достаточно проверить, что $f_\varphi(\vec{x}) = 1$ при всех $\vec{x}$. Достаточно, таким образом, найти все значения булевой функции f_φ. Таблица таких значений называется *таблицей истинности* формулы φ.

Если $\vec{q} = (q_1, \ldots, q_n)$, то может потребоваться вычислить 2^n значений $f_\varphi(\vec{x})$ на наборах $\vec{x} \in \underline{2}^n$. Как видим, объем вычислений с ростом числа переменных растет экспоненциально. В настоящее время неизвестно, есть ли способ проверки на тавтологичность, требующий для *всех* пропозициональных формул существенно меньшей работы. Однако, во многих случаях без перебора всех $\vec{x}$ легко обойтись.

Пример 3.3.18. Является ли формула $\varphi = ((p \to q) \to p) \to p$ тавтологией?

Допустим, что существует оценка ξ, при которой φ ложна, и попытаемся найти одну из таких оценок. Из

$$[\varphi](\xi) = \mathrm{imp}([(p \to q) \to p](\xi), \xi(p)) = 0$$

следует $\xi(p) = 0$ и $[(p \to q) \to p](\xi) = 1$. Но тогда

$$[(p \to q) \to p](\xi) = \mathrm{imp}(\mathrm{imp}(0, \xi(q)), 0) = 1,$$

откуда $\mathrm{imp}(0, \xi(q)) = 0$, чего, очевидно, не может быть ни при каком значении q. Противоречие показывает, что оценки ξ, *опровергающей* формулу φ, не существует, т. е. это тавтология. Согласно следствию 3.3.16, любая формула вида $((\varphi \to \psi) \to \varphi) \to \varphi$ является

тавтологией. Этот факт называют *законом Пирса*, а каждую такую тавтологию *примером* закона Пирса.

Пример 3.3.19. Является ли формула

$$\varphi(p,q,r) = (p \to r) \to ((p \to q) \to (r \to q))$$

тавтологией?

Вновь предположим существование опровергающей оценки ξ. Имеем

$$[p \to r](\xi) = 1 \quad \text{и} \quad [(p \to q) \to (r \to q)](\xi) = 0,$$

откуда

$$[p \to q](\xi) = 1 \quad \text{и} \quad [r \to q](\xi) = 0.$$

Значит, $\xi(r) = 1$, $\xi(q) = 0$ и $\xi(p) = 0$. Формально говоря, нужно еще убедиться, что некоторая оценка с такими свойствами действительно обращает значение φ в ложь: ведь мы доказали лишь, что *если опровергающая оценка существует*, то она такая-то. Очевидно, впрочем, что оценка $\xi_{(0,0,1)}$ подходит. Следовательно, φ не является тавтологией.

Упражнение 3.3.20. Пусть $\hat{F} = \{\leftrightarrow, \neg\}$ при стандартной интерпретации этих связок. Докажите, что произвольная формула $\varphi \in \mathrm{Fm}(\hat{F})$ является тавтологией тогда и только тогда, когда связка $\neg$ и каждый атом из $V(\varphi)$ имеют в φ четное число вхождений. (Полезно использовать тождества $x \leftrightarrow y = x + y + 1$ и $\neg x = x + 1$.)

Таким образом, при некоторых ограничениях на используемые связки (или, как мы увидим далее, на структуру формулы) проверка тавтологичности может быть существенно ускорена.

Пример 3.3.21. Конъюнктивная нормальная форма является тавтологией тогда и только тогда, когда каждая ее элементарная дизъюнкция содержит литералы p и $\neg p$ для некоторого $p \in \mathrm{At}$.

Если такие вхождения действительно есть, то каждая элементарная дизъюнкция — тавтология, а значит, и вся к. н. ф. В противном случае найдется элементарная дизъюнкция вида $q_1 \vee \ldots \vee q_n \vee \neg r_1 \vee \ldots \vee \neg r_m$, причем всегда $q_i \neq r_j$. Существует оценка ξ, т. ч. $\xi(q_i) = 0$ и $\xi(r_j) = 1$ для всех i, j. Очевидно, ξ опровергает нашу элементарную дизъюнкцию, а значит, всю к. н. ф.

Упражнение 3.3.22. Найдите простой критерий выполнимости д. н. ф.

Тавтологии можно рассматривать как *законы логики* — сложные высказывания, истинные *безотносительно* истинности их составных частей.

Лемма 3.3.23. *Для любых $\varphi, \psi, \theta \in \mathrm{Fm}(\hat{F})$, следующие формулы являются тавтологиями:*

$\varphi \to \varphi$; $\varphi \to (\psi \to \varphi)$; $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$;
$\varphi \to (\psi \to (\varphi \wedge \psi))$; $(\varphi \wedge \psi) \to \varphi$; $(\varphi \wedge \psi) \to \psi$;
$(\varphi \to \theta) \to ((\psi \to \theta) \to ((\varphi \vee \psi) \to \theta))$; $\varphi \to (\varphi \vee \psi)$; $\psi \to (\varphi \vee \psi)$;
$\neg\varphi \to (\varphi \to \psi)$; $(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$;
$\bot \to \varphi$; $\varphi \to \top$;
$\varphi \vee \neg\varphi$; $\neg\neg\varphi \to \varphi$; $((\varphi \to \psi) \to \varphi) \to \varphi$.

Прокомментируем с содержательной точки зрения некоторые из этих законов. Закон $\varphi \to (\psi \to \varphi)$ говорит, что если φ высказывание истинно, то оно следует откуда угодно. Закон $(\varphi \to (\psi \to \theta)) \to ((\varphi \to \psi) \to (\varphi \to \theta))$ (*дистрибутивность импликации*) означает, что если из φ и ψ следует θ и из φ следует ψ, то из φ следует θ.

Закон $(\varphi \to \theta) \to ((\psi \to \theta) \to ((\varphi \vee \psi) \to \theta))$ (*разбор случаев*) утверждает, что если θ имеет место как при условии φ, так и при ψ, то для θ достаточно дизъюнкции этих условий.

Закон $\neg\varphi \to (\varphi \to \psi)$ говорит, что если мы имеем $\neg\varphi$ и φ, то получили противоречие, из которого вправе заключить что угодно (в частности, заведомую ложь $\bot$). Закон $(\varphi \to \psi) \to ((\varphi \to \neg\psi) \to \neg\varphi)$ (*приведение к абсурду*) разрешает заключить $\neg\varphi$, если предположение φ имеет противоречивые следствия.

Закон исключенного третьего $\neg\varphi \vee \varphi$ обязывает каждое утверждение быть истинным либо иметь истинное отрицание. Закон $\neg\neg\varphi \to \varphi$ (*снятие двойного отрицания*) выражает ту же мысль: если $\neg\varphi$ не истинно, то истинно φ.

Двойственность.

Унификация. Формула $p \to (q \to r)$.

Логическое следование. Пусть $\Gamma \subseteq \mathrm{Fm}(\hat{F})$ и $\varphi \in \mathrm{Fm}(\hat{F})$. Скажем, что оценка ξ *выполняет* множество Γ, если $[\gamma](\xi) = 1$ для всех $\gamma \in \Gamma$. Тогда пишем $[\Gamma](\xi) = 1$.

По определению, формула φ *логически следует* из множества (*гипотез*, *посылок* или *предположений*) Γ, если для любой оценки ξ, т. ч. $[\Gamma](\xi) = 1$, верно $[\varphi](\xi) = 1$. В таком случае пишем $\Gamma \models \varphi$.

Содержательно, логическое следование соответствует «правильному рассуждению», о котором шла речь в § 1.1.: при таком рассуждении,

если все посылки оказались истинны (при некоторой оценке — т. е., содержательно, при некотором «положении вещей»), то и заключение φ обязано быть истинным.

Принято писать $\Gamma, \psi \models \varphi$ вместо $\Gamma \cup \{\psi\} \models \varphi$ и $\models \varphi$ вместо $\varnothing \models \varphi$.

Лемма 3.3.24. *Для любой $\varphi \in \mathrm{Fm}(\hat{F})$ имеет место $\models \varphi$ тогда и только тогда, когда φ тавтология.*

Доказательство. В самом деле, $\varnothing \models \varphi$ равносильно тому, что любая оценка, выполняющая $\varnothing$, выполняет и φ. Однако пустое множество формул выполняется *любой* оценкой, поскольку утверждение $\forall \gamma \in \varnothing\, [\gamma](\xi) = 1$ всегда истинно. Стало быть, $\models \varphi$ тогда и только тогда, когда $[\varphi](\xi) = 1$ при всех ξ, т. е. когда φ является тавтологией. $\square$

Множество $\Gamma \subseteq \mathrm{Fm}(\hat{F})$ называется *противоречивым*, если $\Gamma \models \bot$.

Лемма 3.3.25. *Следующие условия равносильны:*

1) *для каждой оценки ξ найдется $\gamma \in \Gamma$, т. ч. $[\gamma](\xi) = 0$;*
2) *не существует оценки ξ, т. ч. $[\Gamma](\xi) = 1$;*
3) *$\Gamma \models \varphi$ для всех $\varphi \in \mathrm{Fm}(\hat{F})$;*
4) *$\Gamma \models \bot$;*
5) *$\Gamma \models \varphi$ и $\Gamma \models \neg\varphi$ для некоторой $\varphi \in \mathrm{Fm}(\hat{F})$.*

Эквивалентность, как нетрудно видеть, сохраняет логическое следование.

Лемма 3.3.26. *Если $\varphi \equiv \varphi'$ и $\psi \equiv \psi'$ и $\Gamma, \psi \models \varphi$, то $\Gamma, \psi' \models \varphi'$.*

Лемма 3.3.27. *Для любых $\varphi, \psi, \psi_i \in \mathrm{Fm}(\hat{F})$ и $\Gamma \subseteq \mathrm{Fm}(\hat{F})$ верно:*

1) $\Gamma, \psi \models \varphi \iff \Gamma \models \psi \to \varphi$;
2) $\Gamma, \psi_1, \psi_2, \ldots, \psi_n \models \varphi \iff \Gamma \models \psi_1 \to (\psi_2 \to (\ldots(\psi_n \to \varphi)\ldots))$;
3) $\Gamma, \psi_1, \psi_2, \ldots, \psi_n \models \varphi \iff \Gamma \models (\psi_1 \wedge \psi_2 \wedge \ldots \wedge \psi_n) \to \varphi$.

Доказательство. Пусть $\Gamma, \psi \models \varphi$ и $[\Gamma](\xi) = 1$. Если $[\psi](\xi) = 0$, то $[\psi \to \varphi](\xi) = 1$. Если же $[\psi](\xi) = 1$, то $[\Gamma, \psi](\xi) = 1$, а значит, $[\varphi](\xi) = 1$, откуда вновь получаем $[\psi \to \varphi](\xi) = 1$.

Второе и третье утверждения легко следуют из первого с применением эквивалентности $\varphi \to (\psi \to \theta) \equiv (\varphi \wedge \psi) \to \theta$. $\square$

Лемма 3.3.28. *Для любых* $\varphi, \psi, \theta \in \mathrm{Fm}(\hat{F})$ *и* $\Gamma \subseteq \mathrm{Fm}(\hat{F})$ *верно:*

1) $\Gamma, \varphi \models \varphi$;

2) $\Gamma \models \varphi$ *и* $\Gamma \models \psi \iff \Gamma \models \varphi \wedge \psi$;

3) $\Gamma, \varphi, \psi \models \theta \iff \Gamma, \varphi \wedge \psi \models \theta$;

4) $\Gamma \models \varphi$ *или* $\Gamma \models \psi \Longrightarrow \Gamma \models \varphi \vee \psi$;

5) $\Gamma, \varphi \models \theta$ *и* $\Gamma, \psi \models \theta \iff \Gamma, \varphi \vee \psi \models \theta$;

6) $\Gamma \models \varphi$ *и* $\Gamma, \psi \models \theta \Longrightarrow \Gamma, \varphi \to \psi \models \theta$;

7) $\Gamma, \varphi \models \bot \iff \Gamma \models \neg\varphi$.

Лемма 3.3.29. *Для любых* $\varphi \in \mathrm{Fm}(\hat{F})$ *и* $\Gamma, \Delta \subseteq \mathrm{Fm}(\hat{F})$ *верно:*

1) $\Gamma \models \varphi$ *и* $\Gamma \subseteq \Delta \Longrightarrow \Delta \models \varphi$;

2) $\Gamma \models \varphi$ *и* $\Delta \models \gamma$ *для всех* $\gamma \in \Gamma \Longrightarrow \Delta \models \varphi$.

Доказательство. Проверим второе утверждение. Пусть $[\Delta](\xi) = 1$. Но тогда $[\gamma](\xi) = 1$ для всех $\gamma \in \Gamma$, т. е. $[\Gamma](\xi) = 1$, откуда $[\varphi](\xi) = 1$. □

§ 3.4. Компактность

Назовем множество $\Gamma \subseteq \mathrm{Fm}(\hat{F})$ *выполнимым*, если существует выполняющая его оценка. Будем говорить также о *выполняющем наборе*[3] $\sigma \in \underline{2}^*$, если оценка ξ_σ выполняет Γ, где

$$\xi_\sigma(q) \quad = \quad \begin{cases} \sigma(i) & \text{если } q = p_i \text{ для } i < |\sigma|; \\ 0 & \text{иначе.} \end{cases}$$

Одним из важнейших свойств логики высказываний является следующая

Теорема 3.4.1 (о компактности)**.** *Если каждое конечное подмножество* $\Gamma' \subseteq \Gamma$ *выполнимо, то выполнимо и множество* Γ.

[3]Как видит педантичный читатель, мы производим отождествление наборов и слов на основе леммы 2.1.15.

Доказательство. Положим $\Gamma(p_0,\dots,p_{n-1}) = \Gamma \cap \mathrm{Fm}(\hat{F}; p_0,\dots,p_{n-1})$ (если $n=0$, останутся формулы без атомов, образованные с помощью связок вроде $\bot$ и $\top$). Хотя множество $\Gamma(p_0,\dots,p_{n-1})$ не обязано быть конечным, оно является таковым с «точностью до эквивалентности» в силу леммы 3.3.4. Точнее, мы факторизуем это множество по отношению эквивалентности, а затем выберем в каждом из классов по одному представителю (аксиома выбора не требуется, поскольку классов лишь конечно много). Назовем полученное конечное множество представителей $\Gamma_n \subseteq \Gamma(p_0,\dots,p_{n-1}) \subseteq \Gamma$.

По условию, для каждого $n \in \mathbb{N}$ множество Γ_n имеет какую-то выполняющую оценку ξ. В силу следствия 3.2.23, набор $\sigma = (\xi(p_0),\dots,\xi(p_{n-1}))$ является выполняющим для Γ_n. Положим

$$\Sigma = \{\sigma \in \underline{2}^* \mid \exists n \in \mathbb{N}\ (\sigma \text{ выполняет } \Gamma_n \text{ и } |\sigma| = n)\}.$$

Как видим, множество Σ бесконечно. Заметим также, что если σ выполняет Γ_n, то σ выполняет и все множество $\Gamma(p_0,\dots,p_{n-1})$. Поэтому, если $\sigma \in \Sigma$ и $\tau \sqsubseteq \sigma$, то для некоторого n набор σ длины n выполняет все формулы из $\Gamma(p_0,\dots,p_{n-1})$, а набор τ длины $m \leqslant n$ выполняет все формулы из $\Gamma(p_0,\dots,p_{m-1}) = \Gamma(p_0,\dots,p_{n-1}) \cap \mathrm{Fm}(\hat{F}; p_0,\dots,p_{m-1})$. В частности, τ выполняет Γ_m, а значит, $\tau \in \Sigma$. Таким образом, множество Σ «замкнуто вниз» относительно $\sqsubseteq$.

Назовем набор $\sigma \in \underline{2}^*$ *правильным*, если существует бесконечно много наборов $\tau \in \Sigma$, т. ч. $\sigma \sqsubseteq \tau$. Ясно, что каждый правильный набор сам лежит в Σ. Пустой набор ε правильный, поскольку $\varepsilon \sqsubseteq \sigma$ для любого $\sigma \in \Sigma$, а множество Σ бесконечно. Кроме того, если набор σ правильный, то правилен хотя бы один из наборов $\sigma 0$ или $\sigma 1$. В противном случае, оба эти набора имеют лишь конечно много продолжений в Σ (быть может, не имеют ни одного), а значит, и σ не может быть правильным.

С помощью рекурсии определим функцию $f\colon \mathbb{N} \to \underline{2}$, т. ч.

$$f(n) \quad = \quad \begin{cases} 1, & \text{если набор } f(0)\dots f(n-1)\,1 \text{ правильный;} \\ 0 & \text{иначе.} \end{cases}$$

Индукцией по $n \in \mathbb{N}$ покажем, что набор $f(0)\dots f(n-1)$ правилен при всех n. Если $n=0$, то, как мы знаем, пустой набор ε правильный. Пусть теперь набор $f(0)\dots f(n-1)$ правильный, а мы хотим доказать правильность $f(0)\dots f(n-1)f(n)$. Тогда $f(0)\dots f(n-1)\,1$ или $f(0)\dots f(n-1)\,0$ будет правильным; определение f обеспечивает требуемое.

Функция f естественным образом задает оценку ξ, т. ч. $\xi(p_n) = f(n)$. Каждый набор $(\xi(p_0), \ldots, \xi(p_{n-1}))$ правильный, а значит, выполняет $\Gamma(p_0, \ldots, p_{n-1})$. Таким образом, оценка ξ выполняет каждое из этих множеств, а значит, и $\Gamma = \bigcup_{n\in\mathbb{N}} \Gamma(p_0, \ldots, p_{n-1})$. □

Следствие 3.4.2. *Если* $\Gamma \models \varphi$, *то* $\Gamma' \models \varphi$ *для некоторого конечного подмножества* $\Gamma' \subseteq \Gamma$.

Доказательство. Предположим противное. Тогда для каждого конечного $\Gamma' \subseteq \Gamma$ имеем $\Gamma' \not\models \varphi$, т. е. существует оценка ξ, выполняющая Γ, для которой $[\varphi](\xi) = 0$. Значит, ξ выполняет $\Gamma' \cup \{\neg\varphi\}$. Поэтому каждое конечное подмножество множества $\Gamma \cup \{\neg\varphi\}$ выполнимо. По теореме 3.4.1, выполнимо и само это множество, т. е. для некоторой выполняющей Γ оценки ξ верно $[\varphi](\xi) = 0$, а значит, $\Gamma \not\models \varphi$. Противоречие.

Замечание 3.4.3. Следствие 3.4.2 тривиальным образом влечет теорему 3.4.1, т. е. может считаться ее переформулировкой.

В самом деле, допустив следствие и предположив, что каждое конечное подмножество $\Gamma' \subseteq \Gamma$ выполнимо, докажем выполнимость Γ. В противном случае имеем $\Gamma \models \bot$ по лемме 3.3.25. Но тогда $\Gamma' \models \bot$ для некоторого конечного Γ', т. е. Γ' не выполнимо. Противоречие.

Применения компактности. □

§ 3.5. Полные системы функций

§ 3.6. Дальнейшие свойства логики высказываний.

§ 3.7. Исчисление высказываний

§ 3.8. Другие интерпретации

Мы говорили, что пропозициональную формулу можно рассматривать как программу для вычисления булевой функции или, с другой стороны, как представление некоторого сложного высказывания, зависимость истинности которого от истинности более простых, как раз, задается этой функцией. Однако пропозициональным формулам можно давать и другие осмысленные интерпретации.

Теоретико-множественная интерпретация. Возможно, читатель заметил сходство между эквивалентностями в лемме 3.3.13 и тождествами из теоремы 1.2.38. Например, *закон де Моргана* $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$ естественным образом соответствует одноименному тождеству $\overline{(A \cap B)} = \bar{A} \cup \bar{B}$, верному для любых множеств A и B, если только фиксирован некоторый универсум U, включающий оба.

Соответствие тем более понятно, что мы, с одной стороны, *определяли* теоретико-множественные операции с опорой на естественное понимание слов «и», «или», «не», а с другой, мы *формализуем* это понимание с помощью функций and, or, not.

Понятие пропозициональной формулы позволяет придать нашему соответствию вполне строгий характер, когда выражения $\neg(A \wedge B)$ и $\overline{(A \cap B)}$ рассматриваются как одно, различные возможные смыслы которого определяются *интерпретацией*: в одном случае стандартной булевой, а в другом — теоретико-множественной.

Поскольку, как мы видели, все возможные булевы связки выражаются с помощью $\neg$ и $\wedge$, мы ограничимся для простоты только последними. Итак, полагаем далее $\mathrm{Fm} = \mathrm{Fm}(\neg, \wedge)$.

Пусть задано некоторое непустое множество U. Оно будет играть роль универсума для теоретико-множественных операций. Мы называем *U-оценкой* любую функцию $\alpha\colon \mathrm{At} \to \mathcal{P}(U)$. Значение $[\varphi](\alpha) \in \mathcal{P}(U)$ формулы $\varphi \in \mathrm{Fm}$ при U-оценке α определяется рекурсивно, т. ч. $[p](\alpha) = \alpha(p)$, $[\neg\varphi](\alpha) = \overline{[\varphi](\alpha)}$ и $[\varphi \wedge \psi](\alpha) = [\varphi](\alpha) \cap [\psi](\alpha)$.

Пример 3.8.1. Имеем $[p \wedge \neg p](\alpha) = \alpha(p) \cap \overline{\alpha(p)} = \varnothing$. Поскольку $\bot \equiv p \wedge \neg p$, было бы естественно положить $[\bot](\alpha) = \varnothing$ при рассмотрении более широкого набора связок. Впрочем, пока нами не исключена ситуация, когда какая-нибудь иная формула из $\mathrm{Fm}(\neg, \wedge)$, эквивалентная $\bot$, имеет другое теоретико-множественное значение.

Аналогично, $[\neg(\neg p \wedge \neg q)](\alpha) = \overline{\overline{\alpha(p)} \cap \overline{\alpha(q)}} = \alpha(p) \cup \alpha(q)$ и $[\neg(p \wedge \neg q)](\alpha) = \overline{\alpha(p)} \cup \alpha(q)$ для $p \vee q \equiv \neg(\neg p \wedge \neg q)$ и $p \to q \equiv \neg(p \wedge \neg q)$.

Формула φ называется *U-тавтологией*, если $[\varphi](\alpha) = U$ для всех U-оценок α, называется *U-выполнимой*, если $[\varphi](\alpha) \neq \varnothing$ для некоторой U-оценки α. Формулы φ и ψ *U-эквивалентны* (пишем $\varphi \equiv_U \psi$), если $[\varphi](\alpha) = [\psi](\alpha)$ для всех U-оценок α.

Лемма 3.8.2. *Формула φ есть U-тавтология тогда и только тогда, когда $\neg\varphi$ не является U-выполнимой. Имеет место $\varphi \equiv_U \psi$ тогда и только тогда, когда $\neg(\varphi \wedge \neg\psi) \wedge \neg(\psi \wedge \neg\varphi)$ есть U-тавтология.*

Доказательство. Проверим второе утверждение. Имеем $[\neg(\varphi \wedge \neg\psi) \wedge \neg(\psi \wedge \neg\varphi)](\alpha) = U$ тогда и только тогда, когда $[\varphi \wedge \neg\psi](\alpha) = [\psi \wedge$

$\wedge \neg\varphi](\alpha) = \varnothing$, т. е. $[\varphi](\alpha) \cap \overline{[\psi](\alpha)} = \varnothing$ и $[\psi](\alpha) \cap \overline{[\varphi](\alpha)} = \varnothing$, что равносильно $[\varphi](\alpha) \subseteq [\psi](\alpha)$ и $[\psi](\alpha) \subseteq [\varphi](\alpha)$. $\square$

Итак, понятия U-тавтологии и U-эквивалентности выражаются через U-выполнимость совершенно так же, как понятия тавтологии и эквивалентности выражаются через выполнимость.

Теорема 3.8.3. *Формула φ является U-выполнимой, если и только если φ выполнима.*

Доказательство. Допустим, что $[\varphi](\xi) = 1$ для некоторой оценки ξ. Рассмотрим U-оценку α, т. ч.

$$\alpha(q) \quad = \quad \begin{cases} U, & \text{если } \xi(q) = 1; \\ \varnothing, & \text{если } \xi(q) = 0. \end{cases}$$

Индукцией по построению проверим, что для любой формулы ψ верно $[\psi](\alpha) = U$, если $[\psi](\xi) = 1$, и $[\psi](\alpha) = \varnothing$, если $[\psi](\xi) = 0$. Случай, когда $\psi \in \mathrm{At}$, очевиден. Пусть $\psi = \neg\theta$. Тогда если $[\neg\theta](\xi) = 1$, то $[\theta](\xi) = 0$, откуда, по предположению индукции, $[\theta](\alpha) = \varnothing$ и $[\neg\theta](\alpha) = \overline{[\theta](\alpha)} = U$. Аналогично рассуждаем, если $[\neg\theta](\xi) = 0$.

Наконец, пусть $\psi = \theta_1 \wedge \theta_2$. Если $[\theta_1 \wedge \theta_2](\xi) = 1$, то $[\theta_1](\xi) = [\theta_2](\xi) = 1$, откуда $[\theta_1](\alpha) = [\theta_2](\alpha) = U$ по предположению индукции. Имеем $[\theta_1 \wedge \theta_2](\alpha) = [\theta_1](\alpha) \cap [\theta_2](\alpha) = U$. Если же $[\theta_1 \wedge \theta_2](\xi) = 0$, то, без ограничения общности, $[\theta_1](\xi) = 0$, откуда $[\theta_1](\alpha) = \varnothing$ и $[\theta_1 \wedge \theta_2](\alpha) = \varnothing \cap [\theta_2](\alpha) = \varnothing$.

Поскольку $[\varphi](\xi) = 1$, заключаем $[\varphi](\alpha) = U \neq \varnothing$, т. е. U-оценка α выполняет φ. Обратно, предположим, что некоторая U-оценка β выполняет φ, т. е. $[\varphi](\beta) \neq \varnothing$. Выберем произвольный элемент $x \in [\varphi](\beta)$ и рассмотрим оценку η, т. ч.

$$\eta(q) \quad = \quad \begin{cases} 1, & \text{если } x \in \beta(q); \\ 0, & \text{если } x \notin \beta(q). \end{cases}$$

Тогда для произвольной формулы ψ имеет место $[\psi](\eta) = 1$, если $x \in [\psi](\beta)$, и $[\psi](\eta) = 0$, если $x \notin [\psi](\beta)$. Индукция по построению ψ. Случай $\psi \in \mathrm{At}$ ясен. Допустим, что $\psi = \neg\theta$. Если $x \in [\neg\theta](\beta) = \overline{[\theta](\beta)}$, то $x \notin [\theta](\beta)$, а значит, $[\neg\theta](\eta) = \mathrm{not}([\theta](\eta)) = \mathrm{not}(0) = 1$ по предположению индукции. Рассуждаем аналогично при $x \notin [\neg\theta](\beta)$.

Пусть теперь $\psi = \theta_1 \wedge \theta_2$. Если $x \in [\theta_1 \wedge \theta_2](\beta) = [\theta_1](\beta) \cap [\theta_2](\beta)$, то $x \in [\theta_1](\beta)$ и $x \in [\theta_2](\beta)$. По предположению индукции, $[\theta_1](\eta) = [\theta_2](\eta) = 1$, откуда $[\theta_1 \wedge \theta_2](\eta) = 1$. Если же $x \notin [\theta_1 \wedge \theta_2](\beta) = [\theta_1](\beta) \cap$

$\cap[\theta_2](\beta)$, то, без ограничения общности, $x \notin [\theta_1](\beta)$, что дает $[\theta_1](\eta) = 0$ в силу индуктивного предположения, откуда $[\theta_1 \wedge \theta_2](\eta) = 0$.

Поскольку $x \in [\varphi](\beta)$, заключаем $[\varphi](\eta) = 1$, т. е. φ выполняется оценкой η. $\square$

Следствие 3.8.4. *Формула φ является U-тавтологией, если и только если φ тавтология. Имеет место $\varphi \equiv_U \psi$ тогда и только тогда, когда $\varphi \equiv \psi$.*

Итак, если U непусто, «U-логика высказываний» совпадает с обыкновенной логикой высказываний в отношении эквивалентностей, тавтологий и выполнимых формул. Заметим, что при этом «U-логика» может быть «бесконечнозначной» в том смысле, что значениями формулы при U-оценке могут быть бесконечно многие различные подмножества.

Более того, для любых непустых множеств U_1 и U_2 соответствующие логики совпадают.

Замечание 3.8.5. Теперь мы легко можем интерпретировать в U формулу φ над любым множеством связок. Для этого берем произвольную $\varphi' \in \mathrm{Fm}(\neg, \wedge)$, т. ч. $\varphi \equiv \varphi'$, и полагаем $[\varphi](\alpha) = [\varphi'](\alpha)$. Как видим, выбор конкретной φ' не играет роли, т. е. такое определение корректно: не нарушена функциональность $\overline{[\cdot](\alpha)}$.

Например, $\overline{[\top](\alpha)} = U$, $[p \to q](\alpha) = \overline{\alpha(p)} \cup \alpha(q)$, $[p \leftrightarrow q](\alpha) = (\overline{\alpha(p)} \cup \alpha(q)) \cap (\overline{\alpha(q)} \cup \alpha(p))$.

Пример 3.8.6. Если формула φ является U-выполнимой, то обязательно найдется U-оценка α, т. ч. $[\varphi](\alpha) = U$.

В самом деле, тогда φ выполняется некоторой оценкой ξ, которой, следуя доказательству теоремы 3.8.3, можно поставить в соответствие U-оценку α, т. ч. $[\varphi](\alpha) = U$.

Этот результат можно переформулировать. Пусть имеется (правильно построенное) выражение, составленное из букв $A_1, \ldots, A_n$ и символов операций $\cap, \cup, \overline{(\cdot)}$, вроде $A_1 \cup (A_3 \cap \overline{A_2})$. Тогда, если это выражение не означает тождественно пустое множество, то для всякого универсума $U \neq \varnothing$ можно выбрать множества $A_i \subseteq U$ так, что выражение будет означать все U.

Доказательство очевидно: выразив $\cup$ через $\cap$ и $\neg$, мы можем рассматривать наше выражение как формулу из $\mathrm{Fm}(A_1, \ldots, A_n)$. Раз она не всегда обозначает пустое множество, то для некоторого универсума U' (который всегда можно дополнить до непустого) есть U'-оценка,

выполняющая нашу формулу. Но тогда формула выполнима, и для любого непустого универсума U мы находим нужную оценку.

Пример 3.8.7. Пусть X и Y суть два выражения для множеств вышеописанного типа, не содержащие букв, кроме $A_1, \ldots, A_n$. Тогда если равенство $X = Y$ нарушается для некоторого выбора универсума U и множеств $A_1, \ldots, A_n$, то оно нарушается и для некоторых множеств $A'_1, \ldots, A'_n$ из произвольного *одноэлементного* универсума.

Вновь представим X и Y как формулы из $\mathrm{Fm}(A_1, \ldots, A_n)$. Нарушение равенства означает, что $X \not\equiv_{U_1} Y$ для некоторого непустого U_1. Поскольку логики для U_1 и U_2 совпадают, взяв любое одноэлементное множество U_2, имеем $X \not\equiv_{U_2} Y$, что влечет требуемое (т. е. можно взять $A'_i = [A_i](\alpha) \subseteq U_2$ для U_2-оценки α, при которой значения формул X и Y не совпадают).

Замечание 3.8.8. Какую роль играет требование непустоты U и что будет, если его отбросить?

Легко видеть, что всякая формула является $\varnothing$-тавтологией, любые две формулы эквивалентны в смысле $\equiv_\varnothing$, но ни одна формула не является $\varnothing$-выполнимой. Таким образом, «$\varnothing$-логика» устроена очень просто, но сильно отличается от обычной пропозициональной логики и логик непустых множеств (совпадающих между собой).

Если ввести понятие «M-тавтологии» (от слова «множество»), полагая формулу таковой, если она является U-тавтологией для любых U, включая пустое множество, то окажется, что M-тавтолгиями, попрежнему, являются все тавтологии и только они. Совершенно так же можно ввести понятие «M-эквивалентности», тождественное обычной эквивалентности. Чтобы сохранить «M-выполнимость» равной обычной выполнимости, правда, придется переменить квантор: формула M-выполнима, если *найдется* какое-либо U, для которого она будет U-выполнима. Определенная таким образом M-логика все еще совпадает с обычной логикой высказываний.

Совсем не так будет обстоять дело при допущении пустых множеств в интерпретации логики предикатов, о которой речь пойдет впоследствии.

Алгебраическая интерпретация.

Логические матрицы.

Интуиционисткая логика.

Литература

1. Бурбаки Н. Начала математики. Первая часть. Основные структуры анализа. Книга первая. Теория множеств. — М. : Мир, 1965.

2. Верещагин Н. К., Шень А. Лекции по математической логике и теории алгоритмов. Часть 1. Начала теории множеств. — 4-е изд. — М. : МЦНМО, 2012.

3. Ершов Ю. Л., Палютин Е. А. Математическая логика. — 2-е изд. — М. : Наука, 1987.

4. Колмогоров А. Н., Драгалин А. Г. Введение в математическую логику. — М. : Изд-во Московского ун-та, 1982.

5. Колмогоров А. Н., Драгалин А. Г. Математическая логика. Дополнительные главы. — М. : Изд-во Московского ун-та, 1984.

6. Крупский В. Н., Плиско В. Е. Математическая логика и теория алгоритмов. — М. : Изд. центр «Академия», 2013.

7. Куратовский К., Мостовский А. Теория множеств. — М. : Мир, 1970.

8. Лавров И. А., Максимова Л. Л. Задачи по теории множеств, математической логике и теории алгоритмов. — 5-е изд. — М. : Физматлит, 2002.

9. Мальцев А. И. Алгебраические системы. — Наука, 1970.

10. Мендельсон Э. Введение в математическую логику. — М. : Наука, 1971.

11. Пентус А. Е., Пентус М. Р. Теория формальных языков. — М. : Изд-во ЦПИ при механико-математическом факультете МГУ, 2004.

12. Френкель А. А., Бар-Хиллел И. Основания теории множеств. — М. : Мир, 1966.

13. Шенфилд Д. Математическая логика. — М. : Наука, 1975.

14. Шень А. Математическая индукция. — 3-е изд. — М. : МЦНМО, 2007.

15. Burris S., Sankappanavar H. P. A Course in Universal Algebra. — The Millennium edition. — 2012. — http://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html.

16. Ciesielski K. Set Theory for the Working Mathematician. — Cambridge University Press, 1997.

17. Herrlich H. Axiom of Choice. — Springer, 2006.

18. Jech T. Set Theory. — 3rd Millennium edition. — Springer, 2006.

19. Smith P. Category Theory: A Gentle Introduction. — http://www.logicmatters.net/categories.

Предметный указатель